VMware Validated Design for Micro-Segmentation Planning and Preparation Guide

VMware Validated Design for Micro-Segmentation 3.0.0

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-002253-01

vmware®

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

http://www.vmware.com/support/

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 Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware Validated Design for Micro-Segmentation Planning and Preparation 5

Updated Information 7

1 Software Requirements 9

VMware Software 9

VMware Scripts and Tools 10

Third-Party Software 10

2 External Service Dependencies 11

Physical VLANs, IP Subnets, and Application Virtual Networks 14

DNS Names 15

Time Synchronization 17

Active Directory Users and Groups 18

Certificate Replacement for a Single-Region Environment 20

Datastore Requirements 25

Index 27

About VMware Validated Design for Micro-Segmentation Planning and Preparation

The *VMware Validated Design for Micro-Segmentation Planning and Preparation* document provides detailed information about the requirements to software, tools and external services required to successfully implement the VMware Validated Design for Micro-Segmentation 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 in the data center. Carefully review the *VMware Validated Design Planning and Preparation* documentation to avoid costly rework and delays

Intended Audience

This information is intended for anyone who wants to install, upgrade, or use ESX. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

About Regions Mentioned in this Document

The VMware Validated Design for Micro-Segmentation use case uses a single-region design. However, some of the guidance in this document is forward-looking to support an expansion to dual region later.

Updated Information

This *VMware Validated Design for Micro-Segmentation Planning and Preparation Guide* is updated with each release of the product or when necessary.

This table provides the update history of the *VMware Validated Design for Micro-Segmentation Planning and Preparation Guide*.

Revision	Description
EN-002253-01	Updated the document to remove some VMware software and some Third-Party software that is not related to the micro-segmentation use case.
EN-002253-00	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 Software," on page 9
- "VMware Scripts and Tools," on page 10
- "Third-Party Software," on page 10

VMware Software

Download and license the following VMware software products.

Table 1-1. VMware Software Required for the VMware Validated Design

SDDC Layer	Product Group and Edition	Product Name	Product Version
Virtual Infrastructure	VMware vSphere Enterprise Plus	ESXi	6.0 Update 2
	VMware vCenter Server Standard	vCenter Server Appliance (ISO)	6.0 Update 2
	VMware Virtual SAN Standard or higher	Virtual SAN	6.2
	VMware NSX for vSphere Enterprise	NSX for vSphere	6.2.4
Service Management	vRealize Log Insight	vRealize Log Insight	3.3.2
		vRealize Log Insight Content Pack for NSX for vSphere	3.3

VMware Scripts and Tools

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

Table 1-2. 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 1-3. 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

External Service Dependencies 2

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

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 can use a domain and forest structure to store and manage Active Directory objects per region.

Table 2-1. Requirements for the Active Directory Service

Requirement	Domain Instance	Domain Name	Description
Active Directory configuration	Parent Active Directory	rainpole.local	Contains Domain Name System (DNS) server, time server, and universal groups that contain global groups from the child domains and are members of local groups in the child domains.
	Region-A child Active Directory	sfo01.rainpole.local	Contains DNS records that replicate to all DNS servers in the forest. This child domain contains all SDDC users, and global and local groups.
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.

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 2-2. 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.

DNS

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

Table 2-3. DNS Configuration Requirements

Requirement	Domain Instance	Description
DNS host entries	rainpole.local	Resides in the rainpole.local domain.
	sfo01.rainpole.local	DNS servers reside in the sfo01.rainpole.local domain. 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," on page 15 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," on page 17.

Table 2-4. NTP Server Configuration Requirements

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

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	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.

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. For information about the Windows OS requirements for the host and the software downloads for this SDDC validated design, see "Third-Party Software," on page 10.

This chapter includes the following topics:

- "Physical VLANs, IP Subnets, and Application Virtual Networks," on page 14
- "DNS Names," on page 15
- "Time Synchronization," on page 17
- "Active Directory Users and Groups," on page 18
- "Certificate Replacement for a Single-Region Environment," on page 20
- "Datastore Requirements," on page 25

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.

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
	Virtual SAN	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
	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 (NSX VTEP)	1634	172.16.34.0/24	172.16.34.253
	NFS	1625	172.16.25.0/24	172.16.25.253
	Uplink01	1635	172.16.35.0/24	172.16.35.253
	Uplink02	2713	172.27.13.0/24	172.27.13.253
	External Tenant Connectivity	140	10.158.140.0/24	10.158.140.253

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 2-10. IP Subnets for the Application Virtual Networks

Application Virtual Network	Subnet in Region A
Mgmt-RegionA01-VXLAN	192.168.31.0/24

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.

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 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.

Host Names and IP Addresses for vSphere

DNS Name in Region A	IP Address in Region A	Description
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

DNS Name in Region A	IP Address in Region A	Description
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

Host Names and IP Addresses for NSX for vSphere

DNS Name in Region A	IP Address in Region A	Description
mgmt01nsxm01.sfo01.rainpole.local	172.16.11.65	NSX Manager for the management cluster
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	
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

Host Names and IP Addresses for vRealize Log Insight in Region A

Allocate DNS names and IP addresses to vRealize Log Insight in Region A before you deploy the application.

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

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 2-11. NTP Server FQDN and IP Configuration

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

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 regional NTP server alias ntp.sfo01.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

On Windows, enable NTP-based synchronization.

Procedure

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" /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.

  c If the ReferenceId: attribute contains LOCL instead of the IP address of at least one of the NTP servers, run the following command and wait for the resynchronization to complete.

  ```
  w32tm /resync
  ```

  d Query the status of the Windows Time service again.

  ```
  w32tm /query /status
  ```

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

When creating Active Directory groups, follow account rules and create prespecified universal groups in the parent domain and global groups in the child domain.

Account Rules

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 2-12. Universal Groups in the rainpole.local Parent Domain

Group Name	Group Scope	Description
ug-SDDC-Admins	Universal	Administrative group for the SDDC
ug-SDDC-Ops	Universal	SDDC operators group
ug-vCenterAdmins	Universal	Group with accounts that are assigned vCenter Server administrator privileges.

Global Groups in the Child Domains

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

Table 2-13. Global Groups in the sfo01.rainpole.local Child Domain

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

Active Directory Users

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 the Parent Domain

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

Table 2-14. 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-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 compute and edge clusters.	Yes	RAINPOLE\ug-vCenterAdmins

Users in the Child Domains

Create the following accounts for user access in the child Active Directory domain sfo01.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 2-15. 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 for a Single-Region Environment

By default, virtual infrastructure management components use TLS/SSL certificates that are signed by the VMware Certificate Authority (VMCA). These certificates are not trusted by end-user devices. For example, a certificate warning might appear when a user connects to a vCenter Server system by using the vSphere Web Client.

Infrastructure administrators connect to different SDDC components, such as vCenter Server systems or a Platform Services Controller from a Web browser to perform configuration, management and troubleshooting. The authenticity of the network node to which the administrator connects must be confirmed with a valid TLS/SSL certificate.

In this design, you replace user-facing certificates with certificates that are signed by a Microsoft Certificate Authority (CA). You can use other Certificate Authorities according to the requirements of your organization. You do not replace certificates for machine-to-machine communication. If necessary, you can manually mark these certificates as trusted.

Certificate replacement covers the following VMware products from the virtual infrastructure layer:

- Platform Services Controller in both management pod and shared edge and compute pod
- vCenter Server system in both management pod and shared edge and compute pod
- VMware NSX Manager in both management pod and shared edge and compute pod

Product Order for Certificate Replacement

After set up your Microsoft CA, create a custom template, and add the custom template to the set of available templates, replace certificates on the virtual infrastructure products as follows:

1. Management Platform Services Controller
2. Management vCenter Server
3. Management NSX Manager
4. Compute Platform Services Controller
5. Compute vCenter Server
6. Compute NSX Manager

Options for Certificate Generation and Replacement

You have two options to create and replace certificates while deploying this VMware Validated Design.

- Use the CertGenVVD tool 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 tool that you can use to save time in creating signed certificates. The tool generates CSRs, OpenSSL CA-signed certificates, and Microsoft CA-signed certificates. See VMware Knowledge Base article 2146215.

- If the CertGenVVD tool is not an option for deployment, follow the validated manual steps to create and replace certificates.

1. Create and Add a Microsoft Certificate Authority Template on page 21

   As a part of the certificate replacement process, you submit Certificate Signing Requests (CSRs) to the intermediate Certificate Authority (CA) server. You then replace the VMCA-signed or self-signed certificates with CA-signed certificates.

2. Generate CA-Signed Certificates for the Management Components in Region A on page 22

   For each certificate that you want to replace, you need a certificate file that is signed by the intermediate certificate authority (CA) that you set up earlier on the Active Directory server.

Create and Add a Microsoft Certificate Authority Template

As a part of the certificate replacement process, you submit Certificate Signing Requests (CSRs) to the intermediate Certificate Authority (CA) server. You then replace the VMCA-signed or self-signed certificates with CA-signed certificates.

This VMware Validated Design uses a Microsoft Certificate Authority server, however other Certificate Authorities can also be used.

- 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 it to the certificate templates of the Microsoft Certificate Authority.

Prerequisites

This VMware Validated Design sets up the CA on the Active Directory (AD) server `dc01sfo.sfo01.rainpole.local`, which is running Microsoft Windows Server 2012 R2.

- Verify that you installed Microsoft Server 2012 R2 with Active Directory Services enabled.
- Verify that your AD Server is installed and configured with the Certificate Authority Service role and the Certificate Authority Web Enrolment role.

If a different Microsoft CA already exists in your environment, you can use that CA instead.

Procedure

1 Use Remote Desktop Protocol to connect to the CA server `dc01sfo.sfo01.rainpole.local` as the AD administrator with the *ad_admin_password* password.

2 Click **Start > Run**, type **`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 **Start > Run**, type **`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, in the **Name** column, select the VMware certificate that you just created and click **OK.**

Generate CA-Signed Certificates for the Management Components in Region A

For each certificate that you want to replace, you need a certificate file that is signed by the intermediate certificate authority (CA) that you set up earlier on the Active Directory server.

You perform these tasks, in sequence:

1 Generate a CSR for the certificate that you want to replace. You generate the CSR on the machine where the certificate lives. For vCenter Server and Platform Services Controller certificate replacement, you use the vSphere Certificate Manager utility.

2 Submit the certificate request to your AD server for signing by the CA on the server and export the signed certificate.

3 Copy the certificate and the associated root certificate to the virtual machine where you want to replace the certificate.

4 Replace the existing certificates with the new certificates.

For additional details, see VMware Knowledge Base article 2112014.

You obtain custom certificates for the Platform Services Controllers, vCenter Server instances and NSX Managers.

This example illustrates how you generate the signed certificate for the `mgmt01psc01.sfo01.rainpole.local` Platform Services Controller instance.

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	domain administrator
Password	*ad_admin_password*

   c Click the **Request a certificate** link.

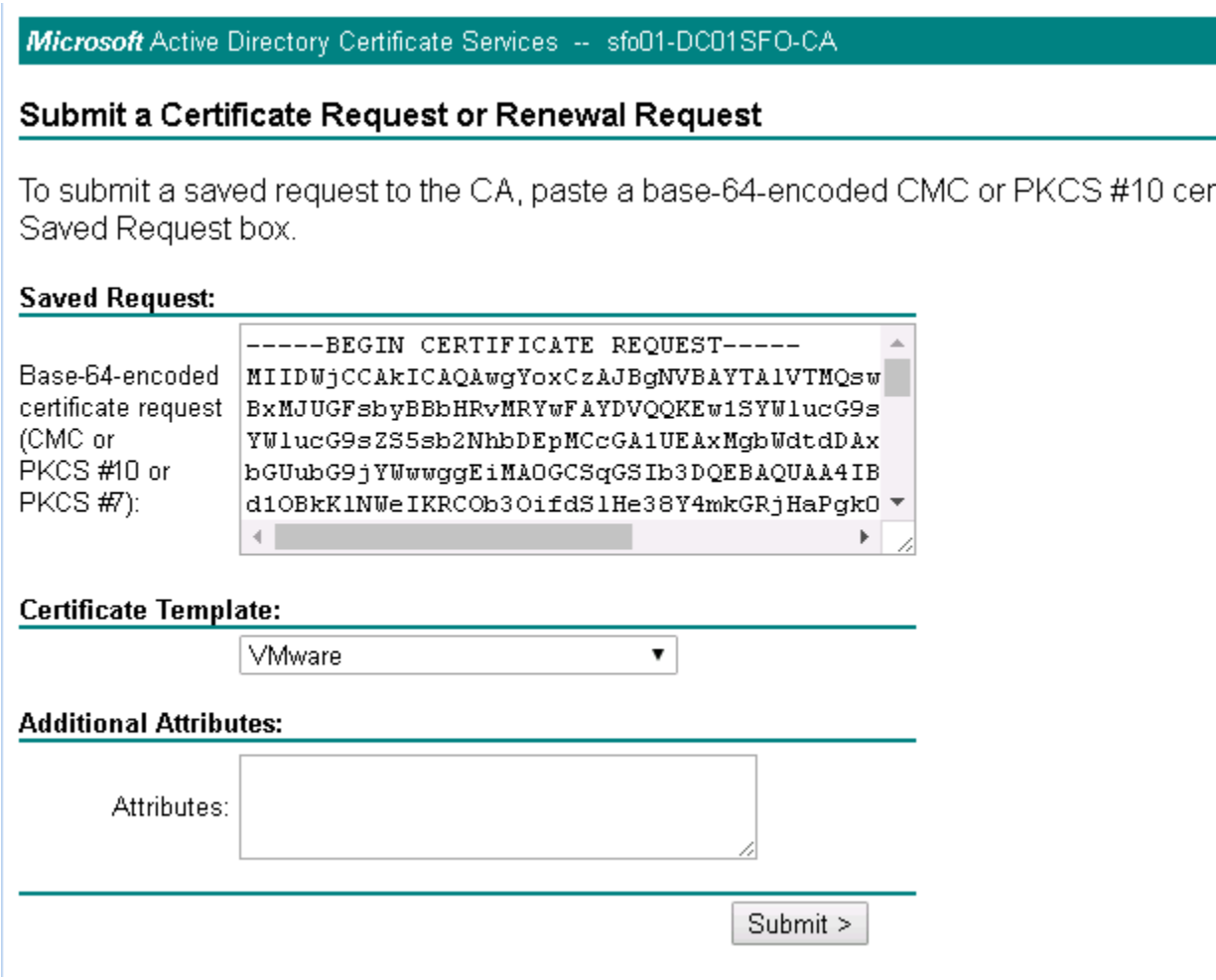
   d Click **advanced certificate request**.

   e Open the CSR file `mgmt01psc01.sfo01_ssl.csr` in a plain text editor.

   f Copy everything from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----` to the clipboard.

   g On the Submit a Certificate Request or Renewal Request page, paste the contents of the CSR file into the **Saved Request** box.

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



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

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

3 Export the machine certificate to the correct format.

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

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

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

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

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

f Browse to `C:\certs` and specify the certificate named `mgmt01psc01.sfo01` in the **File name** text box.

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

The `mgmt01psc01.sfo01.cer` 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 2-16. 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

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, you must set up datastores for the shared edge and compute cluster for each region before you begin implementing your SDDC. 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*.

Index

U
updated information **7**