Planning and Preparation

22 AUG 2017

VMware Validated Design 4.1

VMware Validated Design for Management and Workload Consolidation 4.1

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

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

Contents

About VMware Validated Design Planning and Preparation for Workload and Management Consolidation

VMware Validated Design Planning and Preparation for Workload and Management Consolidation provides detailed information about the software, tools and external services that are required to implement a Software-Defined Data Center (SDDC) whose management and tenant workloads run on a consolidated pod.

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

Intended Audience

The *VMware Validated Design Planning and Preparation for Workload and Management Consolidation* 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.

Required VMware Software

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

Software Requirements for Consolidated SDDC 1

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

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

This chapter includes the following topics:

VMware Scripts and Tools for Consolidated SDDC

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 for Consolidated SDDC

Download and license the following third-party software products.

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

SDDC Layer	Required by VMware Component	Vendor	Product Item	Product Version
Virtual Infrastructure	Windows host machine in the data center that has access to the ESXi management network.	Any Supported	Operating system that is supported for deploying VMware vSphere. See System Requirements for the vCenter Server Appliance Installer.	Operating system for vSphere deployment.
Operations Management	Update Manager Download Service (UMDS)	Ubuntu	Ubuntu Server 14.04	Ubuntu Server 14.04 LTS
		PostgreSQL	PostgreSQL	9.3.17
		Nginx	Nginx	1.4.6
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	Red Hat Enterprise Linux 6 (64-bit)

External Services for Consolidated SDDC 2

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

This chapter includes the following topics:

External Services Overview 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 for Consolidated SDDC," on page 17 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 "Host Names and IP Addresses for Consolidated SDDC," on page 13 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 for Consolidated SDDC," on page 16.

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.

Physical Network Requirements for Consolidated SDDC

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

Table 2-9. Requirements for the SDDC Physical Network

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

VLANs, IP Subnets, and Application Virtual Networks for Consolidated SDDC

Before you start deploying the Consolidated 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 Consolidated SDDC

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

According to the VMware Validated Design, you have the following VLANs and IP subnets for Consolidated SDDC.

Table 2-10. VLAN and IP Subnet Configuration for Consolidated SDDC

Pod in Consolidated SDDC	VLAN Function	VLAN ID	Subnet	Gateway
Consolidated Pod	ESXi Management	1631	172.16.31.0/24	172.16.31.253
	Management Virtual Machines	1611	172.16.11.0/24	172.16.11.253
	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
	Secondary Storage	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 for Consolidated SDDC

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 Consolidated SDDC
Mgmt-xRegion01-VXLAN	192.168.11.0/24
Mgmt-RegionA01-VXLAN	192.168.31.0/24

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

Host Names and IP Addresses for Consolidated SDDC

Before you deploy the Consolidated SDDC following this validated design, you must define the host names and IP addresses for the each of the management components deployed. Some of these host names must also be configured in DNS with fully qualified domain names (FQDNs) that map them to the IP addresses.

- Host Names and IP Addresses for External Services for Consolidated SDDC on page 13

  Allocate DNS names and IP addresses to the NTP and Active Directory servers in the Consolidated SDDC.

- Host Names and IP Addresses for the Virtual Infrastructure Components for Consolidated SDDC on page 14

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

- Host Names and IP Addresses for the Cloud Management Components for Consolidated SDDC on page 15

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

- Host Names and IP Addresses for the Data Protection and Operations Management Components for Consolidated SDDC on page 15

  Allocate host names and IP addresses to the data protection and operations management components of the Consolidated SDDC according to this VMware Validated Design.

Host Names and IP Addresses for External Services for Consolidated SDDC

Allocate DNS names and IP addresses to the NTP and Active Directory servers in the Consolidated SDDC.

Component Group	Host Name	DNS Zone	IP Address	Description
NTP	ntp	sfo01.rainpole.local	■ 172.16.11.251 ■ 172.16.11.252	■ NTP server selected using Round Robin ■ NTP server on a ToR switch in the consolidated pod
	0.ntp	sfo01.rainpole.local	172.16.11.251	NTP server on a ToR switch in the consolidated pod
	1.ntp	sfo01.rainpole.local	172.16.11.252	NTP server on a ToR switch in the consolidate pod

Component Group	Host Name	DNS Zone	IP Address	Description
AD/DNS/CA	dc01rpl	rainpole.local	172.16.11.4	Windows 2012 R2 host that contains the Active Directory configuration and DNS server for the rainpole.local domain and the Microsoft Certificate Authority for signing management SSL certificates
	dc01sfo	sfo01.rainpole.local	172.16.11.5	Active Directory and DNS server for the sfo01 child domain

Host Names and IP Addresses for the Virtual Infrastructure Components for Consolidated SDDC

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

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

Components	Requires DNS Configuration
Platform Services Controller instances	X
vCenter Server instances	X
NSX Manager instances	X
NSX Edge services gateways	-

Table 2-12. Host Names and IP Addresses for the Virtual Infrastructure Components in Consolidated SDDC

Component Group	Host Name	DNS Zone	IP Address	Description
vSphere	sfo01w01psc01	sfo01.rainpole.local	172.16.11.63	Platform Services Controller
	sfo01w01vc01	sfo01.rainpole.local	172.16.11.64	vCenter Server
	sfo01w01esx01	sfo01.rainpole.local	172.16.31.101	ESXi hosts
	sfo01w01esx02	sfo01.rainpole.local	172.16.31.102	
	sfo01w01esx03	sfo01.rainpole.local	172.16.31.103	
	sfo01w01esx04	sfo01.rainpole.local	172.16.31.104	
NSX for vSphere	sfo01w01nsx01	sfo01.rainpole.local	172.16.11.66	NSX Manager
	sfo01w01nsxc01	-	172.16.31.118	NSX Controllers
	sfo01w01nsxc02	-	172.16.31.119	
	sfo01w01nsxc03	-	172.16.31.120	
	sfo01w01esg01	-	■ 172.16.35.2 ■ 172.27.13.3 ■ 192.168.100.1	ECMP-enabled NSX Edge device for North-South traffic
	sfo01w01esg02	-	■ 172.16.35.3 ■ 172.27.13.2 ■ 192.168.100.2	ECMP-enabled NSX Edge device for North-South traffic

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

Component Group	Host Name	DNS Zone	IP Address	Description
	sfo01w01udlr01	-	■ 192.168.100.3 ■ 192.168.11.1 ■ 192.168.31.1	Universal Distributed Logical Router (UDLR) for East-West traffic
	sfo01w01lb01	-	192.168.11.2	NSX Edge device for load balancing management applications

Host Names and IP Addresses for the Cloud Management Components for Consolidated SDDC

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

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

- vRealize Automation
- Microsoft SQL Server for vRealize Automation
- vRealize Business for Cloud

Table 2-13. Host Names and IP Addresses for the Cloud Management Components in Consolidated SDDC

Component Group	Host Name	DNS Zone	IP Address	Description
vRealize Automation	vra01svr01	rainpole.local	192.168.11.53	VIP address of the vRealize Automation Appliance
	vra01svr01a	rainpole.local	192.168.11.51	vRealize Automation Appliance
	vra01iws01	rainpole.local	192.168.11.56	VIP address of the vRealize Automation IaaS Web Server
	vra01iws01a	rainpole.local	192.168.11.54	vRealize Automation IaaS Web Server
	vra01ims01	rainpole.local	192.168.11.59	VIP address of the vRealize Automation IaaS Manager Service
	vra01ims01a	rainpole.local	192.168.11.57	vRealize Automation IaaS Manager Service, DEM Orchestrator, DEM Worker and Proxy Agent
Microsoft SQL Server	vra01mssql01	rainpole.local	192.168.11.62	Microsoft SQL Server for vRealize Automation
vRealize Business for Cloud	vrb01svr01	rainpole.local	192.168.11.66	vRealize Business for Cloud Server
	sfo01vrbc01	sfo01.rainpole.local	192.168.31.54	vRealize Business for Cloud Data Collector

Host Names and IP Addresses for the Data Protection and Operations Management Components for Consolidated SDDC

Allocate host names and IP addresses to the data protection and operations management components of the Consolidated SDDC according to this VMware Validated Design.

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

- vSphere Data Protection

- vRealize Operations Manager
- vSphere Update Manager Download Service
- vRealize Log Insight

Table 2-14. Host Names and IP Addresses for the Data Protection and Operations Management Components in Consolidated SDDC

Component Group	Host Name	DNS Zone	IP Address	Description
vSphere Data Protection	sfo01w01vdp01	sfo01.rainpole.local	172.16.11.81	vSphere Data Protection primary appliance
vRealize Operations Manager	vrops01svr01	rainpole.local	192.168.11.35	VIP address of load balancer for the analytics cluster of vRealize Operations Manager
	vrops01svr01a	rainpole.local	192.168.11.31	Master node of vRealize Operations Manager
	sfo01vropsc01a	sfo01.rainpole.local	192.168.31.31	Remote Collector of vRealize Operations Manager
vSphere Update Manager	sfo01umds01	sfo01.rainpole.local	192.168.31.67	vSphere Update Manager Download Service (UMDS)
vRealize Log Insight	sfo01vrli01	sfo01.rainpole.local	192.168.31.10	VIP address of the integrated load balancer of vRealize Log Insight
	sfo01vrli01a	sfo01.rainpole.local	192.168.31.11	Master node of vRealize Log Insight

Time Synchronization for Consolidated SDDC

Configure a common NTP server source for synchronized operation of vCenter Single Sign-On and log correlation.

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 for Consolidated SDDC

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

NTP Server Configuration

- Configure two time sources 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 switches.
- 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 2-15. 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 ntp.sfo01.rainpole.local NTP server alias

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

Configure NTP-Based Time Synchronization on Windows Hosts for Consolidated SDDC

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 for Consolidated SDDC

Before you deploy and configure the Consolidated 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 an environment that has parent and child domains in a single forest, store service accounts in the parent domain and user accounts in 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` in the Active Directory domain.

Active Directory Groups for Consolidated SDDC

To grant user and service accounts the access that is required to perform their tasks, create Active Directory groups whose scope reflects the permissions to perform these tasks.

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 rights 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 2-16. 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 Domain

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

Table 2-17. 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
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 for Consolidated SDDC

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

Figure 2-1. Service Accounts in VMware Validated Design for Consolidated SDDC

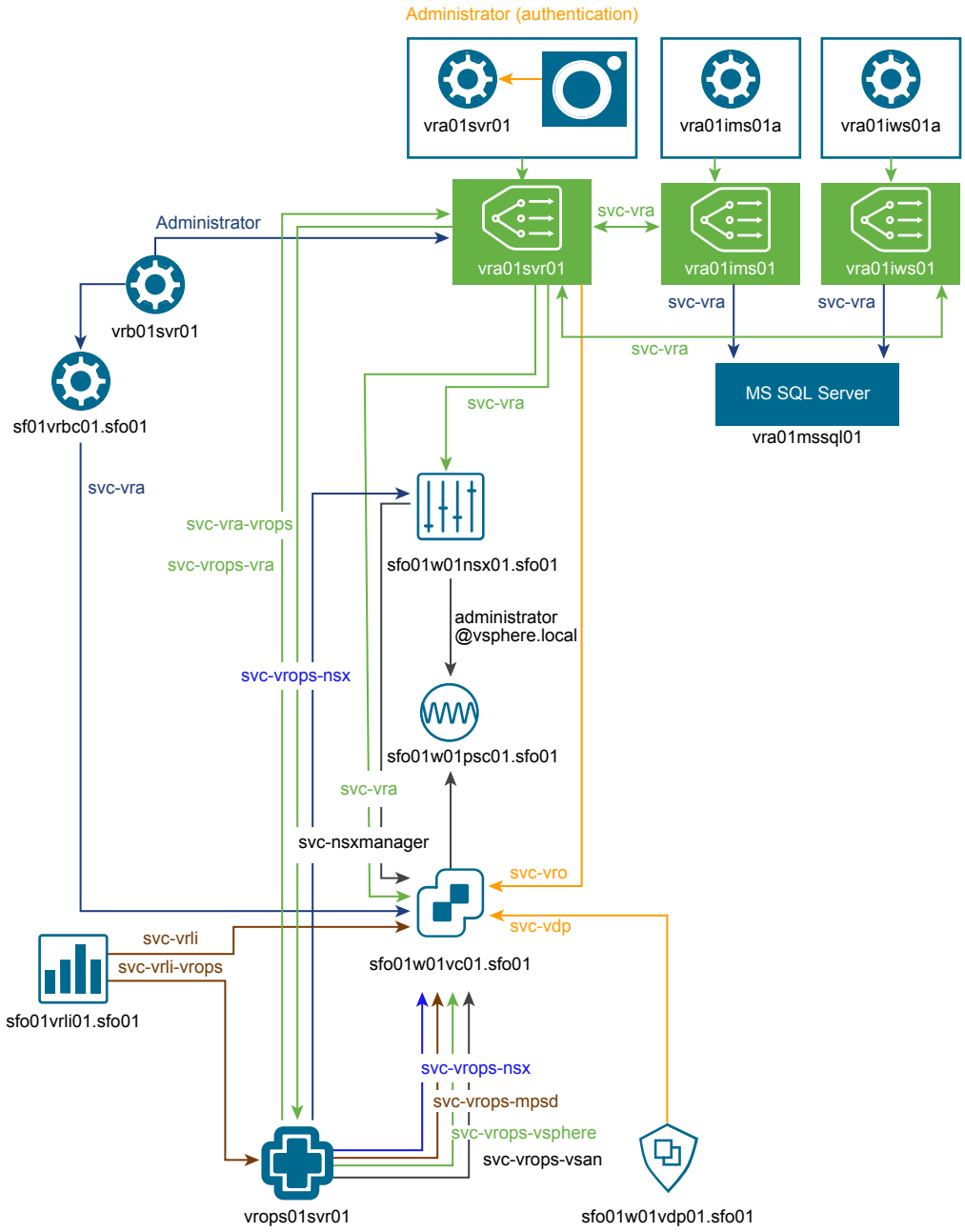

Table 2-18. Application-to-Application or Application Service Accounts in the VMware Validated Design

Username	Source	Destination	Description	Required Role
svc-nsxmanager	NSX for vSphere Manager	vCenter Server	Service account for registering NSX Manager with vCenter Single Sign-on on the Platform Services Controller and vCenter Server for the management cluster and for the compute and edge clusters.	Administrator
svc-vrli	vRealize Log Insight	■ vCenter Server ■ Active Directory	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 Service account for Active Directory integration from vRealize Log Insight for user authentication.	Log Insight User (vCenter Server)
svc-vrli-vrops	vRealize Log Insight	vRealize Operations Manager	Service account for connecting vRealize Log Insight to vRealize Operations Manager for log forwarding, alerts and Launch in Context integration.	Administrator
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-vra	vRealize Automation	■ vCenter Server ■ NSX for vSphere ■ vRealize Automation	Service account for access from vRealize Automation to vCenter Server and NSX for vSphere. This account is a part of the vRealize Automation setup process.	■ Administrator ■ vRealize Orchestrator Administrator
svc-vro	vRealize Orchestrator (embedded in vRealize Automation)	vCenter Server	Service account for access from vRealize Orchestrator to vCenter Server.	Administrator
svc-vrops	vRealize Operations Manager	Active Directory	Service account for Active Directory integration in vRealize Operations Manager for user authentication.	--
svc-vrops-vsphere	vRealize Operations Manager	vCenter Server	Service account for monitoring and collecting general metrics about vSphere objects, including infrastructure and virtual machines, from the Consolidated vCenter Server in to vRealize Operations Manager	Read-Only

Table 2-18. 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	■ vCenter Server ■ NSX for vSphere	■ Service account for monitoring and collecting metrics about NSX components from the Consolidated vCenter Server in to vRealize Operations Manager ■ Local service account for connecting the NSX for vSphere adapter for vRealize Operations Manager to the Management and Compute NSX Managers	■ Read-Only (vCenter Server) ■ Enterprise Administrator (NSX)
svc-vrops-vsan	vRealize Operations Manager Management Pack: VMware vSAN	vCenter Server	Service account for monitoring and collecting metrics about vSAN components from the Consolidated vCenter Server in to vRealize Operations Manager.	MPSD Metrics User
svc-vrops-mpsd	vRealize Operations Manager Management Pack: MPSD	vCenter Server	Service account for monitoring and collecting metrics about storage devices from the Consolidated vCenter Server in to vRealize Operations Manager.	MPSD Metrics User
svc-vrops-vra	vRealize Operations Manager Management Pack: vRA	vRealize Automation	Service account for monitoring and collecting metrics about vRealize Automation objects from vRealize Automation in to vRealize Operations Manager.	■ IaaS Administrator ■ Infrastructure Architect ■ Software Architect ■ Tenant Administrator ■ Fabric 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 2-19. 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 in the child Active Directory domain, sfo01.rainpole.local, to provide centralized user access in the SDDC. In Active Directory, you do not assign any special rights to these accounts other than the default ones.

Table 2-20. User Accounts in the sfo01.rainpole.local Child Domain

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

Certificate Replacement for Consolidated SDDC

Before you deploy the Consolidated 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 for Consolidated SDDC on page 24

  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 Management Certificates for Consolidated SDDC on page 25

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

Create and Add a Microsoft Certificate Authority Template for Consolidated SDDC

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

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

1 Set up a Microsoft Certificate Authority template.

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

Prerequisites

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

- Verify that you installed Microsoft Server 2012 R2 VM with Active Directory Domain Services enabled.
- Verify that the Certificate Authority Service role and the Certificate Authority Web Enrollment role are installed and configured on Active Directory server.
- Use a hashing algorithm of SHA-2 or higher on the certificate authority.

Procedure

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

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

b Use the following credentials.

Setting	Value
User name	Active directory administrator
Password	*ad_admin_password*

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

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

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

5 In the Properties of New Template dialog box, click the **General** tab.

6 In the **Template display name** text box, enter **`VMware`** as the name of the new template.

7 Click the **Extensions** tab and specify extensions information.

a Select **Application Policies** and click **Edit**.

b Select **Server Authentication**, click **Remove**, and click **OK**.

c Select **Key Usage** and click **Edit**.

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

e Leave the default for all other options.

f Click **OK**.

8 Click the **Subject Name** tab, ensure that the **Supply in the request** option is selected, and click **OK** to save the template.

9 To add the new template to your CA, click Windows **Start > Run**, enter **`certsrv.msc`**, and click **OK**.

10 In the Certification Authority window, expand the left pane if it is collapsed.

11 Right-click **Certificate Templates** and select **New** > **Certificate Template to Issue**.

12 In the **Name** column of the Enable Certificate Templates dialog box, select the VMware certificate that you have just created and click **OK.**

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

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

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.

Hostnames or Services	Configuration Files
SFO01 Plaform Services Controller ■ sfo01psc01.sfo01.rainpole.local ■ sfo01w01psc01.sfo01.rainpole.local SFO01 vCenter Server ■ sfo01w01vc01.sfo01.rainpole.local SFO01 NSX Manager ■ sfo01w01nsx01.sfo01.rainpole.local SFO01 VDP ■ sfo01m01vdp01.sfo01.rainpole.local	SFO01 Plaform Services Controller ■ sfo01psc01.txt SFO01 vCenter Server ■ sfo01w01vc01.txt SFO01 NSX Manager ■ sfo01w01nsx01.txt SFO01 VDP ■ sfo01m01vdp01.txt
SFO01 CMP vRealized Automation ■ vra01svr01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01iws01.rainpole.local ■ vra01iws01a.rainpole.local ■ vra01ims01.rainpole.local ■ vra01ims01a.rainpole.local SFO01 CMP vRealized Business Server ■ vrb01svr01.rainpole.local	SFO01 CMP vRealized Automation ■ vra.txt SFO01 CMP vRealized Business Server ■ vrb.txt
SFO01 Operations vRealize Operation ■ vrops01svr01.rainpole.local ■ vrops01svr01a.rainpole.local SFO01 Operations vRealize Log Insight ■ sfo01vrli01.rainpole.local ■ sfo01vrli01a.rainpole.local	SFO01 Operations vRealize Operation ■ vrops-for1pod.txt SFO01 Operations vRealize Log Insight ■ vrli.sfo01.txt

6 Please verify each configuration file includes FQDN and hostnames of its corsponding column.

a An example of sfo01psc01.txt configuration file is listed below

sfo01psc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01psc01.sfo01.rainpole.local
keysize=default
[SAN]
sfo01psc01
sfo01w01psc01
sfo01psc01.sfo01.rainpole.local
sfo01w01psc01.sfo01.rainpole.local
```

7 Open a Windows PowerShell prompt and navigate to the `c:\CertGenVVD-version` folder.

```
cd c:\CertGenVVD-version
```

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

```
Set-ExecutionPolicy Unrestricted
```

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

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

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

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

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

11 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.

Datastore Requirements

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

NFS Exports for Consolidated Pod Components

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

Table 2-21. NFS Export Configuration

VLAN	Server	Export	Size	Map As	Cluster	Component
1615	172.16.15.251	/V2D_vRLI_Consolidated_250GB	250 GB	NFS datastore for log archiving in vRealize Log Insight	Consolidated	vRealize Log Insight
1615	172.16.15.251	/V2D_vDP_Consolidated_6TB	6 TB	sfo01-w01-vdp01	Consolidated	vSphere Data Protection

Virtual Machine Specifications for Consolidated SDDC 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 a virtual machines for Update Manager Download Service (UMDS) and Microsoft SQL Server before you start the deployment of these management components.

For information on the networking configuration of the virtual machines, such as host name, IPv4 address, default gateway, and so on, see "Host Names and IP Addresses for the Data Protection and Operations Management Components for Consolidated SDDC," on page 15.

Table 3-1. Specifications of UMDS and Microsoft SQL Server Management Virtual Machines

Attribute	Update Manager Download Service	Microsoft SQL Server
Number of virtual machines	1	1
Guest OS	Ubuntu Server 14.04 LTS	Windows Server 2012 R2 (64-bit)
VM name	sfo01umds01	vra01mssql01
VM folder	sfo1-w01fd-mgmt	sfo1-w01fd-vra
Cluster	sfo01-w01-consolidated01	sfo01-w01-consolidated01
Resource Pool	sfo01-w01rp-sddc-mgmt	sfo01-w01rp-sddc-mgmt
Datastore	sfo01-w01-vsan01	sfo01-w01-vsan01
Number of CPUs	2	8
Memory (GB)	2	16
Disk space (GB)	120	200
SCSI Controller	LSI Logic SAS	LSI Logic SAS
Virtual machine network adapter	VMXNET3	VMXNET3
Virtual machine network	Mgmt-RegionA01-VXLAN	Mgmt-xRegion01-VXLAN
AD domain	sfo01.rainpole.local	rainpole.local
User account	svc-umds	svc-vra
VMware Tools	Latest version	Latest version

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 (64-bit)	1	6	20	LSI Logic SAS	VMXNET3
	windows-2012r2-64	Windows Server 2012 R2 (64-bit)	1	4	50	LSI Logic SAS	VMXNET3
	windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)	1	8	100	LSI Logic SAS	VMXNET3

Management Workload Footprint for Consolidated SDDC

4

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

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

Virtual Infrastructure Footprint

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

Table 4-1. Virtual Infrastructure Footprint

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Consolidated vCenter Server	Virtual Appliance	4	16	260
Platform Services Controller for the Consolidated vCenter Server	Virtual Appliance	2	4	55
NSX Manager for the consolidated cluster	Virtual Appliance	4	16	60
NSX Controller 01 for the consolidated cluster	Virtual Appliance	4	4	20
NSX Controller 02 for the consolidated cluster	Virtual Appliance	4	4	20
NSX Controller 03 for the consolidated cluster	Virtual Appliance	4	4	20
NSX Edge Services Gateway 1 - ECMP	Virtual Appliance	2	1	1
NSX Edge Services Gateway 2 - ECMP	Virtual Appliance	2	1	1
NSX Edge Services Gateway 1 - Load Balancer	Virtual Appliance	2	1	1

Table 4-1. Virtual Infrastructure Footprint (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
NSX Edge Services Gateway 2 - Load Balancer	Virtual Appliance	2	1	1
NSX Edge Services Gateway 1 - UDLR	Virtual Appliance	2	1	1
NSX Edge Services Gateway 2 - UDLR	Virtual Appliance	2	1	1
Update Manager Download Service	Linux Virtual Machine	2	2	120
Total	-	36	56	561

Cloud Management Platform

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

Table 4-2. Cloud Management Platform Footprint

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Automation Appliance	Virtual Appliance	4	18	65
vRealize Automation IaaS Web Server	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS Manager Server	Windows Server Virtual Machine	4	8	60
vRealize Business for Cloud Server	Virtual Appliance	4	8	50
vRealize Business for Cloud Data Collector	Virtual Appliance	4	2	50
Microsoft SQL Server	Windows Server Virtual Machine	8	16	200
Total	-	26	56	485

Operations Management

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

Table 4-3. Operations Management Footprint

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Operations Manager Master	Virtual Appliance	8	32	274
vRealize Operations Manager Remote Collector	Virtual Appliance	2	4	274

Table 4-3. Operations Management Footprint (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Log Insight Master	Virtual Appliance	4	8	530.5
vSphere Data Protection	Virtual Appliance	4	8	6,200
Total	-	14	52	7,278.5