Planning and Preparation for Consolidated SDDC

19 MAR 2019

VMware Validated Design 5.0

VMware Validated Design for Management and Workload Consolidation 5.0

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Validated Design Planning and Preparation for Consolidated SDDC

VMware Validated Design Planning and Preparation for Management and Workload 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 Management and Workload Consolidation* documentation at least 2 weeks ahead of deployment to avoid costly rework and delays.

Intended Audience

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

Before You Apply This Guidance

The sequence of the documentation of VMware Validated Design follows the stages for implementing and maintaining an SDDC. See Documentation Map for VMware Validated Design.

To use *VMware Validated Design Planning and Preparation for Management and Workload Consolidation*, you must be acquainted with the following guidance:

- *Introducing VMware Validated Designs*
- Optionally *VMware Validated Design Architecture and Design for Consolidated SDDC*

Hardware Requirements for Consolidated SDDC

1

To implement the SDDC from this VMware Validated Design, your hardware must meet certain requirements.

Consolidated Workload Domain

When implementing the *VMware Validated Design for Management and Workload Consolidation*, the consolidated workload domain contains the consolidated cluster which must meet the following requirements.

Table 1-1. Hardware Requirements for the Consolidated Cluster

Component	Requirement
Servers	Four vSAN ReadyNodes with hybrid (HY) profile. For information about vSAN ReadyNodes, see the VMware Compatibility Guide.
CPU per server	Dual-socket, 8 cores per socket
Memory per server	256 GB

Storage per server	■ 16 GB SSD for booting
	■ 600 GB of Flash Device capacity for the caching tier
	  ■ Class D Endurance
	  ■ Class E Performance
	■ 12 TB of magnetic HDD capacity for the capacity tier
	  ■ 10K RPM
	See Designing and Sizing a vSAN Cluster from the VMware vSAN documentation for guidelines about cache sizing.

NICs per server	■ Two 10 GbE NICs ■ One 1 GbE BMC NIC

Primary Storage Options

This design uses and is validated against vSAN as primary storage. However, in a workload domain you can use a supported storage solution that matches the requirements of your organization. Verify that the storage design supports the capacity and performance capabilities of the vSAN configuration in this design. Appropriately adjust the deployment and operational guidance.

Software Requirements for Consolidated SDDC 2

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

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

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 the SDDC implementation.

Table 2-1. VMware Scripts and Tools Required for VMware Validated Design

SDDC Layer	Product Group	Script/Tool	Download Location	Description
SDDC	VMware Cloud Builder	Consolidated Deployment Parameters XLS file: ■ `vvd-consolidated-deployment-parameter.xlsx`	■ my.vmware.com ■ User interface of VMware Cloud Builder.	The Deployment Parameters XLS file is a Microsoft® Excel® workbook that provides the deployment specification. You use this file as an input for an automated deployment of the Consolidated SDDC components with VMware Cloud Builder.
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 that are 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 2-2. Third-Party Software Required for the VMware Validated Design for Consolidated SDDC

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.	Microsoft	Any Supported	Operating system for vSphere deployment.
Operations Management	Update Manager Download Service (UMDS)	Ubuntu	Ubuntu Server 18.04	Ubuntu Server 18.04 LTS
		Nginx	Nginx	1.4
	vRealize Operations Manager and vRealize Log Insight	Postman	Postman App	https://www.getpostman.com
Cloud Management	vRealize Automation	Microsoft	Windows 2016	Windows Server 2016 (64-bit)
		Microsoft	SQL Server 2017	SQL Server 2017 Standard or higher edition (64-bit)
		Redhat	Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6 (64-bit)

External Services for Consolidated SDDC

3

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 (AD), Dynamic Host Control Protocol (DHCP), Domain Name Services (DNS), Network Time Protocol (NTP), Simple Mail Transport Protocol (SMTP) Mail Relay, File Transfer Protocol (FTP), and Certificate Authority (CA).

Active Directory

This VMware Validated Design uses Active Directory (AD) for authentication and authorization to resources in the rainpole.local domain.

Table 3-1. Active Directory Requirements

Requirement	Domain Instance	DNS Zone	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.

Table 3-1. Active Directory Requirements (Continued)

Requirement	Domain Instance	DNS Zone	Description
Active Directory users and groups	-		All user accounts and groups from the User Accounts and Groups for Consolidated SDDC 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 3-2. DHCP Requirements

Requirement	Description
DHCP server	The subnets and associated VLANs that provide IPv4 transport for VXLAN (VTEP) VMkernel ports must be configured for IPv4 address auto-assignment by using DHCP.

DNS

For a single-region deployment, you must provide a root domain and a child domain that contain separate DNS records.

Table 3-3. DNS Server 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 both DNS servers with the following settings: ■ Dynamic updates for the domain set to **Nonsecure and secure**. ■ Zone replication scope for the domain set to **All DNS server in this forest**. ■ Create all hosts listed in the Host Names and IP Addresses for Consolidated SDDC documentation.

If you configure the DNS servers properly, all nodes from the Validated Design are resolvable by FQDN as well as IP address.

NTP

All components in 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.

Table 3-4. NTP Server Requirements

Requirement	Description
NTP	An 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 in 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 3-5. SMTP Server Requirements

Requirement	Description
SMTP mail relay	An 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 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 3-6. Certificate Authority Requirements

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 VMware Validated Design, use the Microsoft Windows Enterprise CA that is available in the Windows Server 2016 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.

SFTP Server

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

Table 3-7. SFTP Server Requirements

Requirement	Description
SFTP server	An SFTP server must host NSX Manager backups. The server must support SFTP and FTP. NSX Manager instances must have connection to the remote SFTP server.

Windows Host Machine

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

Table 3-8. Windows Host Machine Requirements

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 SDDC, provide certain physical network configuration.

Table 3-9. Requirements for the SDDC Physical Network

Requirement	Feature
IGMP snooping querier	Required for the following traffic types: ■ 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

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 SDDC.

To meet the requirements of this VMware Validated Design, you must have the following VLANs and IP subnets for Consolidated SDDC.

Table 3-10. VLAN and IP Subnet Configuration for Consolidated SDDC

Cluster	VLAN Function	VLAN ID	Portgroup Name	Subnet	Gateway
Consolidated Cluster	ESXi Management	1631	sfo01-w01-vds01-management	172.16.31.0/24	172.16.31.253
	Management Virtual Machines	1611	sfo01-w01-vds01-management-vm	172.16.11.0/24	172.16.11.253
	vSphere vMotion	1632	sfo01-w01-vds01-vmotion	172.16.32.0/24	172.16.32.253
	vSAN	1633	sfo01-w01-vds01-vsan	172.16.33.0/24	172.16.33.253
	VXLAN (NSX VTEP)	1634	VXLAN (VTEP) - DHCP Network	172.16.34.0/24	172.16.34.253
	Secondary Storage	1625	sfo01-w01-vds01-SecondaryStorage	172.16.25.0/24	172.16.25.253
	Uplink01	1635	sfo01-w01-vds01-uplink01	172.16.35.0/24	172.16.35.253
	Uplink02	2713	sfo01-w01-vds01-uplink02	172.27.13.0/24	172.27.13.253

Note Use these VLAN IDs and IP subnets as examples. Configure the actual VLAN IDs and IP subnets according to your environment.

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 3-11. IP Subnets for the Application Virtual Networks

Application Virtual Network	Subnet
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

In the SDDC, you must define the host names and IP addresses of the management components before the SDDC deployment. For some components, you must configure fully qualified domain names (FQDN) that map to their IP addresses on the DNS servers.

- Host Names and IP Addresses for External Services for Consolidated SDDC

  Allocate host names and IP addresses to all external services required by the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Virtual Infrastructure Layer for Consolidated SDDC

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

- Host Names and IP Addresses for the Operations Management Layer for Consolidated SDDC

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

- Host Names and IP Addresses for the Cloud Management Layer for Consolidated SDDC

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

Host Names and IP Addresses for External Services for Consolidated SDDC

Allocate host names and IP addresses to all external services required by the SDDC according to this VMware Validated Design.

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

Components	Requires DNS Configuration
NTP	X
Active Directory	X

Table 3-12. Host Names and IP Addresses for the External Services

Component Group	Host Name	DNS Zone	IP Address	Description
NTP	ntp	sfo01.rainpole.local	■ 172.16.11.251 ■ 172.16.11.252	■ NTP server selected using Round Robin ■ NTP server on a ToR switch in the management cluster
	0.ntp	sfo01.rainpole.local	172.16.11.251	NTP server on a ToR switch in the management cluster
	1.ntp	sfo01.rainpole.local	172.16.11.252	NTP server on a ToR switch in the management cluster
AD/DNS/CA	dc01rpl	rainpole.local	172.16.11.4	Windows 2016 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 Layer for Consolidated SDDC

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

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

Components	Requires DNS Configuration
VMware Cloud Builder	X
Platform Services Controller	X
vCenter Server	X
NSX Manager	X
NSX Edge Services Gateways	-

Table 3-13. Host Names and IP Addresses for the Virtual Infrastructure Components in Consolidated SDDC

Component Group	Host Name	DNS Zone	IP Address	Description
VMware Cloud Builder	sfo01cb01	sfo01.rainpole.local	172.16.11.60	Automation appliance for deployment and configuration of SDDC components
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 3-13. 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 Operations Management Layer for Consolidated SDDC

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

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

Components	Requires DNS Configuration
vSphere Update Manager Download Service	X
vRealize Suite Lifecycle Manager	X
vRealize Operations Manager	X
vRealize Log Insight	X

Table 3-14. Host Names and IP Addresses for Operations Management Components in Consolidated SDDC

Component Group	Host Name	DNS Zone	IP Address	Description
vSphere Update Manager	sfo01umds01	sfo01.rainpole.local	■ 172.16.11.67 (VM Network) ■ 192.168.31.67 (VXLAN)	vSphere Update Manager Download Service (UMDS)
vRealize Suite Lifecycle Manager	vrslcm01svr01a	rainpole.local	192.168.11.20	vRealize Suite Lifecycle Manager 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
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

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

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

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

Components	Requires DNS Configuration
vRealize Automation	X
Microsoft SQL Server for vRealize Automation	X
vRealize Business for Cloud	X

Table 3-15. Host Names and IP Addresses for the Cloud Management Components in Consolidated SDDC

Component Group	Host Name	DNS Zone	IP Address	Description
vRealize Automation	vra01svr01a	rainpole.local	192.168.11.51	vRealize Automation Server Appliance
	vra01svr01	rainpole.local	192.168.11.53	VIP address of the vRealize Automation Server
	vra01iws01a	rainpole.local	192.168.11.54	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, DEM Worker, and Proxy Agent
	vra01ims01	rainpole.local	192.168.11.59	VIP address of the vRealize Automation IaaS Manager Service
Microsoft SQL Server	vra01mssql01	rainpole.local	■ 172.16.11.72 (VM Network) ■ 192.168.11.62 (VXLAN)	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

Time Synchronization for Consolidated SDDC

Synchronized systems over NTP are essential for the validity of vCenter Single Sign-On and other certificates. Consistent system clocks are important for the proper operation of the components in the SDDC because in certain cases they rely on vCenter Single Sign-on.

Using 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 must 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 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 3-16. 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 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 for Consolidated SDDC

Ensure that NTP has been configured properly in your Microsoft Windows Domain.

See https://blogs.technet.microsoft.com/nepapfe/2013/03/01/its-simple-time-configuration-in-active-directory/.

User Accounts and Groups for Consolidated SDDC

Before you deploy and configure the SDDC in this VMware Validated Design, you must provide a specific configuration of Active Directory users and groups. You use these users and Active Directory groups for application login, for assigning roles in a tenant organization and for authentication in cross-application communication.

Active Directory Service Accounts

In a multi-region or single-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 account `svc-domain-join` with elevated permissions to add computer objects to the Active Directory domain.

Active Directory Groups for Consolidated SDDC

To grant user and service accounts the access that is required to perform their task, create Active Directory groups according to certain rules.

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 global groups in each child domain to the universal groups.

3 Where applicable, assign access rights and permissions to the global groups, located in the child domains, and the universal groups, located in the parent domain (rainpole.local) to specific products according to their role.

Universal Groups in the Parent Domain

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

Table 3-17. 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.
ug-vra-admins-rainpole	Universal	Tenant administrators group
ug-vra-archs-rainpole	Universal	Tenant blueprint architects group
ug-vROAdmins	Universal	Groups with vRealize Orchestrator Administrator privileges

Global Groups in the Child Domains

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

Table 3-18. Global Groups in the Child Domains

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

Active Directory User Accounts 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.

In addition, a special service account is also required to perform domain join operations if a component registers itself in Active Directory as a computer object. This account must have the right to join computers to the Active Directory domain.

Service Accounts in VMware Validated Design

This Validated Design introduces a set of service accounts that are used in a one- or bidirectional 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 3-1. Service Accounts in VMware Validated Design for Consolidated SDDC

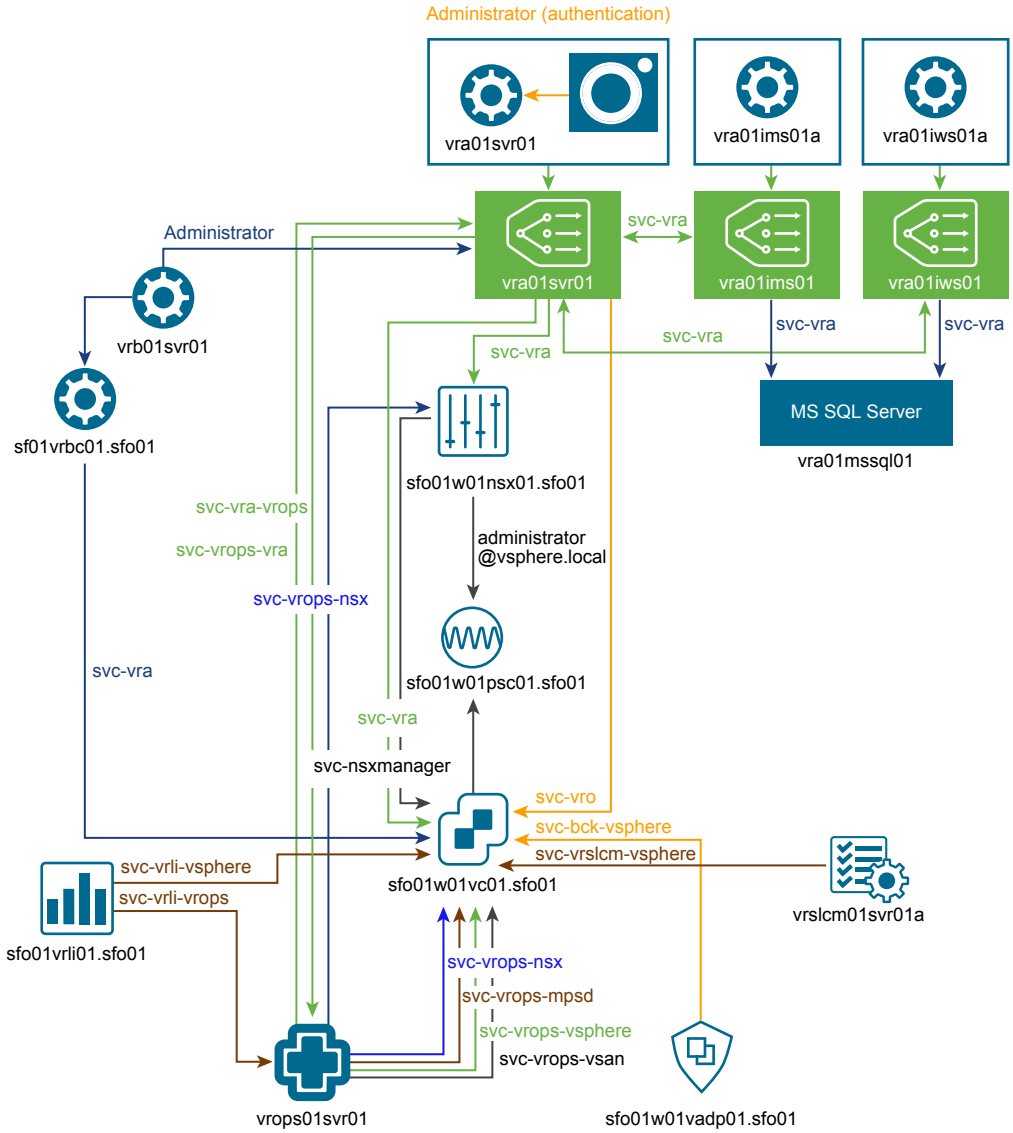

Table 3-19. Application-to-Application or Application Service Accounts in VMware Validated Design

User Name	Source	Destination	Description	Required Role	Password Complexity Category
svc-domain-join	Various management components (one-time domain join action)	Active Directory	Service account for performing domain-join operations from certain SDDC management components.	■ Account Operators Group ■ Delegation to Join Computers to Domain for both the parent and child domains	Standard
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 shared compute and edge cluster	Administrator	Standard
svc-vrli	vRealize Log Insight	Active Directory	Service account for using the Active Directory as an authentication source in vRealize Log Insight	-	Standard
svc-vrli-vsphere	vRealize Log Insight	vCenter Server	Service account for connecting vRealize Log Insight to vCenter Server and ESXi for forwarding log information	Log Insight User (vCenter Server)	Standard
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 for Launch in Context integration	Administrator	Standard
svc-vrslcm-vsphere	vRealize Suite Lifecycle Manager	vCenter Server	A service account for deploying and managing the lifecycle of vRealize Suite components on the Software-Defined Data Center management cluster	vRealize Suite Lifecycle Manager User (Custom)	Standard

Table 3-19. Application-to-Application or Application Service Accounts in VMware Validated Design (Continued)

User Name	Source	Destination	Description	Required Role	Password Complexity Category
svc-bck-vsphere	vSphere Storage API - Data Protection	vCenter Server	Service account for performing backups using the vSphere Storage API - Data Protection with vCenter Server for the management cluster	VADP Backup Solution Requirements	Standard
svc-vra	vRealize Automation	■ vCenter Server ■ vRealize Automation	Service account for access from vRealize Automation to vCenter Server and NSX. This account is part of the vRealize Automation setup process.	■ Administrator ■ vRealize Orchestrator Administrator	Standard
svc-vro	vRealize Orchestrator	vCenter Server	Service account for access from vRealize Orchestrator to vCenter Server	Administrator	Standard
svc-vrops	vRealize Operations Manager	Active Directory	Service account for integration of Active Directory in vRealize Operations Manager for user authentication	-	Standard
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 vCenter Server in to vRealize Operations Manager. Also to perform some actions or tasks on the objects it manages in vCenter Server	vSphere Actions User	Standard
svc-vrops-nsx	vRealize Operations Manager	■ vCenter Server ■ NSX for vSphere	Service account that is available in the Active Directory domain and locally on NSX Manager for collecting data in vRealize Operations Manager from the NSX Manager instances about virtual networking.	■ Read-Only (vCenter Server) ■ Enterprise Administrator (NSX)	Standard

Table 3-19. Application-to-Application or Application Service Accounts in VMware Validated Design (Continued)

User Name	Source	Destination	Description	Required Role	Password Complexity Category
svc-vrops-vsan	vRealize Operations Manager	vCenter Server	Service account for monitoring and collecting metrics about vSAN datastores from vCenter Server in to vRealize Operations Manager	MPSD Metrics User	Standard
svc-vrops-mpsd	vRealize Operations Manager	vCenter Server	Service account for storage device monitoring of the vCenter Server instances in the SDDC from vRealize Operations Manager	MPSD Metrics User	Standard
svc-vrops-vra	vRealize Operations Manager	vRealize Automation	Service account for collecting data in vRealize Operations Manager about the workloads in vRealize Automation	■ IaaS Administrator ■ Infrastructure Architect ■ Software Architect ■ Tenant Administrator ■ Fabric Administrator	Standard
svc-vra-vrops	vRealize Automation	vRealize Operations Manager	Service account for retrieving statistics from vRealize Operations Manager in vRealize Automation for workload reclamation	Read-Only	Standard
svc-umds	vSphere Update Manager Download Service	--	Local service account for configuring the Update Manager Download Service on the host virtual machine	Administrator	Standard

User Accounts in the Parent Domain

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

Table 3-20. User Accounts in the rainpole.local Parent Domain

User Name	Description	Service Account	Member of Groups
vra-admin-rainpole	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-vra-admins-rainpole ■ RAINPOLE\ug-vROAdmins
vra-arch-rainpole	Tenant blueprint architect role in the SDDC for creating the blueprints that tenants request from the service catalog	No	RAINPOLE\ug-vra-archs-rainpole

Users in the Child Domains

Create the following accounts for user access in each of the child Active Directory domain 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 3-21. User Accounts in the Child Domains

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

Local Application User Accounts for Consolidated SDDC

Local application user accounts enable you to perform system and application administration. You set the passwords for local root and administrative accounts with the required password complexity in the **Users and Groups** tab of the Deployment Parameters XLS file before you start the deployment of the SDDC components with VMware Cloud Builder.

All passwords must meet the specific requirements for their complexity category. For password complexity, see Password Complexity for Application and Service Accounts. Passwords can be the same or different across components.

Table 3-22. Local Application Accounts in VMware Validated Design

SDDC Layer	Component	User Account	Description	Password Complexity Category
Virtual Infrastructure Layer	Single Sing-On	administrator@vsphere.local	Default Single-Sign On Domain User	SSO
	ESXi	root	ESXi root account	ESXi
	vCenter Server	root	Virtual appliance root account	Standard

Table 3-22. Local Application Accounts in VMware Validated Design (Continued)

SDDC Layer	Component	User Account	Description	Password Complexity Category
	Platform Services Controller	root	Virtual appliance root account	Standard
	NSX for vSphere	admin	NSX Manager default administrator account	Standard
		admin	NSX Controller Privileged user account to perform console commands	Standard
		admin	NSX Edge device default administrator account	ESG
Operations Management Layer	vRealize Suite Lifecycle Manager	root	Virtual appliance root account	Standard
		admin@localhost	Default administrator account	Standard
	vRealize Operations Manager	admin	Default administrator account	Standard
		root	Virtual appliance root account	Standard
	vRealize Log Insight	root	Virtual appliance root account	vRealize Log Insight
		admin	Default administrator account	Standard
Cloud Management Layer	vRealize Automation	root	Virtual appliances root account	Standard
		administrator@vsphere.local	Administrator account for the default tenant in vRealize Automation	Standard
		Administrator	Local account with membership to the local Administrators Group on the master Windows virtual machine for the IaaS components	Standard
		TenantArchitect	Tenant architect account	Standard
		TenantAdmin	Tenant administrator account	Standard
	vRealize Business	root	Virtual appliances root account	Standard

Password Complexity for Application and Service Accounts

You must consider the requirements for password complexity of each management product in the stack. Because VMware Cloud Builder deploys the SDDC in a single operation, provide the default passwords for the products according to the requirements before you run the deployment operation.

You enter the default passwords for the application and service accounts on the **Users and Groups** tab of the Consolidated Deployment Parameters XLS file for the region.

Passwords can be different per account or common across multiple accounts.

You set passwords for both the required local accounts and Active Directory users. For information on the use, names, and required roles for the accounts, see Active Directory User Accounts for Consolidated SDDC and Local Application User Accounts for Consolidated SDDC.

Table 3-23. Categories of Password Complexity Requirements

Password Category Type	Password Property	Requirements for Complexity
ESXi	Length	8-40 characters
	Characters	■ Must include the following characters: ■ A mix of upper-case and lower-case letters ■ A number ■ A special character such as `@ ! # $ % ^ ?` ■ Must not include characters such as `{ } [ ] ( ) / \ ' " ` ~ , ; : . < >`
Standard	Length	8-12 characters
	Characters	■ Must include the following characters: ■ A mix of upper-case and lower-case letters ■ A number ■ A special character such as `@ ! # $ % ^ ?` ■ Must not include characters such as `{ } [ ] ( ) / \ ' " ` ~ , ; : . < >`
SSO (accounts in vsphere.local)	Length	8-20 characters
	Characters	Must include the following characters: ■ A mix of upper-case and lower-case letters ■ A number ■ A special character such as `@ ! # $ % ^ ?`
ESG	Length	12-255 characters
	Characters	■ Must include the following characters: ■ A mix of upper-case and lower-case letters ■ A number ■ A special character such as `@ ! # $ % ^ ?` ■ Must not include the following characters: ■ Characters such as `{ } [ ] ( ) / \ ' " ` ~ , ; : . < >` ■ Words, for example, `admin` ■ Characters repeated subsequently more than three times
vRealize Log Insight	Length	8-12 characters
	Characters	■ Must include the following types of characters: ■ A mix of upper-case and lower-case letters ■ A number ■ A special character such as `@ ! # $ % ^ ?` ■ Must not include a character repeated subsequently more than four times

Datastore Requirements for Consolidated SDDC

For certain features of the SDDC, such as back up and restore, log archiving, and content library, you must provide secondary storage.

This VMware Validated Design uses NFS as its secondary storage. While vRealize Automation supports any type of secondary storage, using vRealize Log Insight requires NFS storage for archive purposes.

NFS Exports for Management Components

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

Table 3-24. NFS Export Configuration for Consolidated SDDC

VLAN	Server	Export	Size	Map As	Cluster	Component
1625	172.16.25.251	/VVD_vRLI_Consolidated_250GB	250 GB	NFS datastore for log archiving in vRealize Log Insight	Consolidated	vRealize Log Insight
1625	172.16.25.251	/VVD_backup01_nfs01_Consolidated_6TB	6 TB	sfo01-w01-bkp01	Consolidated	VADP-based Backup Solution

Deployment Specification for Consolidated SDDC

4

As part of the preparation for deploying the SDDC, you configure the physical infrastructure, network, storage, and external services, and obtain the product licenses. You provide this data to VMware Cloud Builder as a deployment specification. A deployment specification is presented as a Microsoft® Excel® spreadsheet (XLS) file.

Fill in the Deployment Parameters Spreadsheet for Consolidated SDDC

Before you run an automated deployment for Consolidated SDDC by using VMware Cloud Builder, provide a deployment specification through the Deployment Parameters XLS file.

You configure a Consolidated Deployment Parameters XLS file for the region. The parameters in the spreadsheet are pre-configured according to the VMware Validated Design documentation. You modify them according to your environment. If you use the default values, VMware Cloud Builder deploys a Consolidated SDDC according to the original design in this VMware Validated Design.

Procedure

1 Download the Deployment Parameters XLS file for the region from my.vmware.com.

Region	Deployment Parameters XLS File
Consolidated SDDC	vvd-consolidated-deployment-parameter.xlsx

2 In the spreadsheet, change the pre-defined values of the deployment parameters according to the hardware, software, and external services requirements of VMware Validated Design.

Parameters	Tab in the Deployment Spreadsheet	Requirements
■ Footprint of the management workloads ■ License keys	Management Workloads	■ Footprint data is automatically calculated. ■ Obtain license keys for the VMware products in the management stack.
■ Service accounts in Active Directory and default passwords ■ Default passwords for local application accounts	Users and Groups	■ Password Complexity for Application and Service Accounts

Parameters	Tab in the Deployment Spreadsheet	Requirements
■ VLAN ID, gateway address, MTU, and IP subnet for each network for the consolidated cluster ■ Network-specific IP addresses for each host in the consolidated cluster	Hosts and Networks	■ VLANs, IP Subnets, and Application Virtual Networks for Consolidated SDDC ■ Host Names and IP Addresses for the Virtual Infrastructure Layer for Consolidated SDDC
■ Deployment and configuration of the external services, such as Active Directory, DNS, and SMTP ■ Deployment and configuration of the management components of the Consolidated SDDC	Deploy Parameters	■ External Services Overview for Consolidated SDDC ■ Host Names and IP Addresses for Consolidated SDDC ■ Active Directory Groups for Consolidated SDDC ■ Active Directory User Accounts for Consolidated SDDC ■ Requirements for Time Synchronization for Consolidated SDDC
Configuration of the infrastructure components for the Rainpole tenant in vRealize Automation	vRA Configuration	-
■ Deployment of management components and features in the Consolidated SDDC ■ Size configuration of the management components	Run Parameters	Leave default values selected
List of certificate files that VMware Cloud Builder uses to upload CA-signed certificates on the management products. You generate these files at deployment by using the VMware Validated Design certificate utility.	CertConfig	The setup of configuration files is automatically filled in.

My VMware Account Requirements

5

You register vRealize Suite Lifecycle Manager with My VMware to access product licenses and download product binaries to the local repository used during deployment and upgrade operations. The My VMware account is used to download content from the VMware Marketplace API service through the vRealize Suite Lifecycle Manager integration.

You use the *My VMware* integration to simplify, automate, organize, and update the repository. If your organization restricts outbound traffic from the management components of the SDDC, you can download the product binaries from *My VMware* and discover them in the vRealize Suite Lifecycle Manager user interface for inclusion in the repository.

To register vRealize Suite Lifecycle Manager with *My VMware*, invite a designated user to the entitlement account and limit the folder level permissions for the user.

- Refer to KB 2070555 for details on inviting a user to a *My VMware* account.
- Refer to KB 2006977 for details on assigning user permissions in a *My VMware* account.

You can structure the folders, user, and permissions in a *My VMware* entitlement account in any way that best serves the asset management and operations support needs of your business. The minimum requirements and permissions for the My VMware account used by vRealize Suite Lifecycle Manager include:

- A folder with the vRealize Suite product entitlements
- View License Keys & User Permissions
- Download Products

Table 5-1. My VMware Account for vRealize Suite Lifecycle Manager

First Name	Last Name	User Email	Minimum Folder Permissions	Folder	Product Entitlement in Folder
vRealize Suite Lifecycle Manager User	at Rainpole	vvd-vrslcm@rainpole.local	■ View License Keys & User Permissions ■ Download Products	■ Home folder ■ Child folder	vRealize Suite

Virtual Machine Specifications for Consolidated SDDC

6

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 Update Manager Download Service (UMDS) and Microsoft SQL Server before you start the deployment of these management components.

Table 6-1. Specifications of Management Virtual Machines in Consolidated SDDC

Attribute	vSphere Update Manager Download Service	Microsoft SQL Server
Number of virtual machines	1	1
Guest OS	Ubuntu Server 18.04 LTS	Windows Server 2016 (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
Active Directory Domain	sfo01.rainpole.local	rainpole.local
Service account	svc-umds	svc-vra
VMware Tools	Latest version	Latest version

Specifications for vRealize Automation IaaS and Tenant Blueprints Virtual Machines

To create a IaaS virtual machines and tenant blueprint in vRealize Automation, this Validated Design uses a set of virtual machines according to predefined specifications.

Table 6-2. Specifications for the vRealize Automation IaaS and Blueprint VMs Templates

Required by VMware Component	VM Template Name	Guest OS	CPUs	Memory (GB)	Virtual Disk (GB)	SCSI Controller	Virtual Machine Network Adapter	VMware Tools
vRealize Automation	redhat6-enterprise-64	Red Hat Enterprise Linux 6 (64-bit)	1	6	20	LSI Logic SAS	VMXNET3	Latest version
	windows-2012r2-64	Windows Server 2012 R2 (64-bit)	1	4	60	LSI Logic SAS	VMXNET3	Latest version
	windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)	1	8	100	LSI Logic SAS	VMXNET3	Latest version