Planning and Preparation

25 SEP 2018
VMware Validated Design 4.3
VMware Validated Design for Remote Office Branch Office 4.3

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 Remote Office and Branch Office

1

VMware Validated Design Planning and Preparation for VMware Validated Design™ Remote Office and Branch Office provides detailed information about the software, tools and external services required to successfully implement the remote office and branch office (ROBO), whose design extends VMware Validated Design™ for Software-Defined Data Center.

Before deploying the components of this VMware Validated Design, you must have deployed the VMware Validated Design for SDDC. In addition, you must set up a remote office and branch office environment that has a specific compute, storage, and network configuration, and that provides services to the components of the remote office and branch office SDDC (ROBO SDDC). Carefully review the *VMware Validated Design Planning and Preparation for Remote Office and Branch Office* documentation at least 2 weeks prior to deploying this remote office and branch office solution to avoid costly re-work and delays.

Intended Audience

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

Required VMware Software

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

Hardware Requirements in ROBO

2

To implement the *VMware Validated Design for Remote Office and Branch Office*, your hardware must meet certain requirements.

Consolidated Workload Domain

When implementing the *VMware Validated Design for Remote Office and Branch Office*, the consolidated workload domain contains the consolidated cluster which must meet or exceed the following minimum requirements.

Table 2-1. Minimum Hardware Requirements for the ROBO Cluster

Component	Minimum 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	192 GB

Storage per server	■ 16 GB SSD for booting
	■ 200 GB of Flash Device capacity for the caching tier
	  ■ Class D Endurance
	  ■ Class E Performance
	■ 4 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 in ROBO

3

To implement the VMware Validated Design for ROBO, you must download and license the following VMware and third-party software.

1 VMware Scripts and Tools in ROBO

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

2 Third-Party Software in ROBO

Download and license the following third-party software products.

VMware Scripts and Tools in ROBO

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

Table 3-1. 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 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 in ROBO

Download and license the following third-party software products.

Table 3-2. Third-Party Software Required for the VMware Validated Design for ROBO

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
		Nginx	Nginx	1.4
	vRealize Operations Manager and vRealize Log Insight	Postman	Postman App	https://www.getpostman.com
Cloud Management	vRealize Automation	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 (64-bit)

External Services in ROBO

4

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

1 External Services Overview in ROBO

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).

2 Physical Network Requirements in ROBO

3 VLANs, IP Subnets, and Application Virtual Networks in ROBO

4 Host Names and IP Addresses in ROBO

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.

5 Time Synchronization in ROBO

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.

6 Active Directory Users and Groups in ROBO

Before you deploy and configure the SDDC in this VMware Validated Design, you must provide 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.

7 Certificate Replacement in ROBO

Before you deploy the SDDC, you must configure a certificate authority and generate certificate files for the management products. According to this validated design, you replace the default VMCA- or self-signed certificates of the SDDC management products with certificates signed by a certificate authority (CA) during deployment.

8 Datastore Requirements in ROBO

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

External Services Overview in ROBO

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.

You must provide a domain controller in each ROBO location.

Table 4-1. 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, universal groups, and service accounts.
Active Directory users and groups	-		All user accounts and groups from the Active Directory Users and Groups in ROBO 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 4-2. 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 ROBO deployment, you must provide a root domain which contains the DNS records.

Table 4-3. DNS Server Requirements

Requirement	Domain Instance	Description
DNS host entries	rainpole.local	Resides in the 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 listed in the Host Names and IP Addresses in ROBO 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 in ROBO.

Table 4-4. 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.rainpole.local.

SMTP Mail Relay

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

Table 4-5. 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 4-6. 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 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.

SFTP Server

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

Table 4-7. 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 4-8. 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 in ROBO

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

Table 4-9. 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 in ROBO

Before you start deploying the ROBO SDDC, you must allocate VLANs and IP subnets to the different types of traffic in the ROBO, 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 in ROBO

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 in ROBO.

Table 4-10. VLAN and IP Subnet Configuration in ROBO

Cluster	VLAN Function	VLAN ID	Subnet	Gateway
ROBO Cluster	ESXi Management	1811	172.18.11.0/24	172.18.11.253
	vSphere vMotion	1812	172.18.12.0/24	172.18.12.253
	vSAN	1813	172.18.13.0/24	172.18.13.253
	VXLAN (NSX VTEP)	1814	172.18.14.0/24	172.18.14.253
	Secondary Storage	1815	172.18.15.0/24	172.18.15.253
	Uplink01	1816	172.18.16.0/24	172.18.16.253
	Uplink02	1817	172.18.17.0/24	172.18.17.253

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 in ROBO

You must allocate an IP subnet to the application virtual network in each ROBO location.

Table 4-11. IP Subnets for the Application Virtual Networks

Application Virtual Network	Subnet
Mgmt-NYC01-VXLAN	172.18.19.0/24

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

Host Names and IP Addresses in ROBO

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.

1 Host Names and IP Addresses for External Services in ROBO

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

2 Host Names and IP Addresses for the Virtual Infrastructure Layer in ROBO

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.

3 Host Names and IP Addresses for the Operations Management Layer in ROBO

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.

4 Host Names and IP Addresses for the Cloud Management Layer in ROBO

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 in ROBO

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

Each ROBO site must have a local Active Directory domain controller and an NTP server. This ensures authentication and time synchronization still work in the event of breaking the connection between the Hub and the ROBO site.

Table 4-12. Host Names and IP Addresses for the External Services

Component Group	Host Name	DNS Zone	IP Address	Description
NTP	ntp.rainpole.local	rainpole.local	■ 172.18.11.251 ■ 172.18.11.252	■ NTP server selected using Round Robin ■ NTP server on a ToR switches.
AD/DNS	dc03rpl.rainpole.local	rainpole.local	172.18.11.4	Windows 2012 R2 host that contains the Active Directory configuration and DNS server for the rainpole.local domain.

Host Names and IP Addresses for the Virtual Infrastructure Layer in ROBO

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
vCenter Servers	X
NSX Managers	X
NSX Edge Services Gateways	-

Table 4-13. Host Names and IP Addresses for the Virtual Infrastructure Components in ROBO

Component Group	Host Name	DNS Zone	IP Address	Description
vSphere	nyc01r01vc01	rainpole.local	172.18.11.61	vCenter Server
	nyc01r01esx01	rainpole.local	172.18.11.101	ESXi host
	nyc01r01esx02	rainpole.local	172.18.11.102	ESXi host
	nyc01r01esx03	rainpole.local	172.18.11.103	ESXi host
	nyc01r01esx04	rainpole.local	172.18.11.104	ESXi host
NSX for vSphere	nyc01r01nsx01	rainpole.local	172.18.11.65	NSX Manager
	nyc01r01nsxc01	rainpole.local	172.18.11.118	NSX Controllers
	nyc01r01nsxc02	rainpole.local	172.18.11.119	
	nyc01r01nsxc03	rainpole.local	172.18.11.120	
	nyc01r01esg01	-	■ 172.18.16.2 ■ 172.18.17.3 ■ 172.18.18.1	ECMP-enabled NSX Edge device for North-South traffic
	nyc01r01esg02	-	■ 172.18.16.3 ■ 172.18.17.2 ■ 172.18.18.2	ECMP-enabled NSX Edge device for North-South traffic
	nyc01r01dlr01	-	172.18.18.3	Distributed Logical Router (DLR) for East-West traffic

Host Names and IP Addresses for the Operations Management Layer in ROBO

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 Operations Manager	X
vRealize Log Insight	X

Table 4-14. Host Names and IP Addresses for Operations Management Components in ROBO

Component Group	Host Name	DNS Zone	IP Address	Description
vSphere Update Manager	nyc01umds01	rainpole.local	172.18.19.67	vSphere Update Manager Download Service (UMDS)
vRealize Operations Manager	nyc01vropsc01a	rainpole.local	172.18.19.31	Remote Collector 1 of vRealize Operations Manager
	nyc01vropsc01b	rainpole.local	172.18.19.32	Remote Collector 2 of vRealize Operations Manager
vRealize Log Insight	nyc01vrli01	rainpole.local	172.18.19.10	VIP address of the integrated load balancer of vRealize Log Insight
	nyc01vrli01a	rainpole.local	172.18.19.11	Master node of vRealize Log Insight
	nyc01vrli01b	rainpole.local	172.18.19.12	Worker node 1 of vRealize Log Insight
	nyc01vrli01c	rainpole.local	172.18.19.13	Worker node 2 of vRealize Log Insight

Host Names and IP Addresses for the Cloud Management Layer in ROBO

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
vRealize Business for Cloud	X

Table 4-15. Host Names and IP Addresses for the Cloud Management Components in ROBO

Component Group	Host Name	DNS Zone	IP Address	Description
vRealize Automation	nyc01ias01a	rainpole.local	172.18.19.52	vRealize Automation Proxy Agents
	nyc01ias01b	rainpole.local	172.18.19.53	
vRealize Business for Cloud	nyc01vrbc01	rainpole.local	172.18.19.54	vRealize Business for Cloud Data Collector

Time Synchronization in ROBO

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.

1 Requirements for Time Synchronization in ROBO

2 Configure NTP-Based Time Synchronization on Windows Hosts in ROBO

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

Requirements for Time Synchronization in ROBO

All management components in ROBO deployment must be configured to use NTP for time synchronization.

NTP Server Configuration

- Configure two time sources that are external to the ROBO SDDC stack but local to the ROBO site. 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 4-16. NTP Server FQDN and IP Configuration

NTP Server FQDN	Mapped IP Address
ntp.rainpole.local	■ 172.18.11.251 ■ 172.18.11.252
2.ntp.rainpole.local	172.18.11.251
3.ntp.rainpole.local	172.18.11.251

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

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 in ROBO

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/.

Active Directory Users and Groups in ROBO

Before you deploy and configure the SDDC in this VMware Validated Design, you must provide 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.

The Active Directory service and user accounts required have already been configured as part of the deployment of VMware Validated Design for Software-Defined Data Center. You can reuse these service and user accounts for ROBO deployments.

Active Directory Administrator Account

Certain installation and configuration tasks require a domain administrator account that is referred to as `svc-domain-join` in the Active Directory domain.

Certificate Replacement in ROBO

Before you deploy the SDDC, you must configure a certificate authority and generate certificate files for the management products. According to this validated design, you replace the default VMCA- or self-signed certificates of the SDDC management products with certificates 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.

Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components in ROBO

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

For information about the VMware Validated Design Certificate Generation Utility, see VMware Knowledge Base article 2146215.

Prerequisites

- Provide a Window Server 2012 host that is part of the rainpole.local domain.
- Install a Certificate Authority server on the rainpole.local domain.

Procedure

1. Log in to a Windows host that has access to your data center.
2. Download the `CertGenVVD-`*`version`*`.zip` file of the Certificate Generation Utility from VMware Knowledge Base article 2146215 on the Windows host where you connect to the data center and extract the ZIP file 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=NYC
ST=NY
CC=US
CN=VMware_VVD
keysize=2048
```

5. Verify that the `C:\CertGenVVD-`*`version`*`\ConfigFiles` folder contains only the following files.

Table 4-17. Certificate Generation Files for ROBO

Host Name or Service in ROBO		Configuration Files
Virtual Infrastructure Layer		
vCenter Server	nyc01r01vc01.rainpole.local	nyc01r01vc01.txt
NSX Manager	nyc01r01nsx01.rainpole.local	nyc01r01nsx01.txt
Operations Management Layer		
vRealize Log Insight	■ nyc01vrli01.rainpole.local ■ nyc01vrli01a.rainpole.local ■ nyc01vrli01b.rainpole.local ■ nyc01vrli01c.rainpole.local	nyc01vrli01.txt

6 Verify that each configuration file includes FQDNs and host names in the dedicated sections.

For example, the configuration files for the vCenter Server instance must contain the following properties:

nyc01r01vc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=NYC
ST=default
CC=default
CN=nyc01r01vc01.rainpole.local
keysize=default
[SAN]
nyc01r01vc01
nyc01r01vc01.rainpole.local
```

7 Open a Windows PowerShell prompt and navigate to the `CertGenVVD` folder.

```
cd C:\CertGenVVD-version
```

8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

9 Validate if you can run the utility using the configuration on the host and verify if VMware is included in the printed CA template policy.

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

10 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` subfolder.

Datastore Requirements in ROBO

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

For information about the approximate sizes of all management components, see Chapter 6 Management Workload Footprint in ROBO. Consider these sizes in the storage requirements for your VMware vSphere Storage APIs for Data Protection-based backup solution.

This VMware Validated Design uses NFS as its secondary storage. vRealize Log Insight requires NFS storage for archiving purposes.

NFS Exports for Management Components

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

Table 4-18. NFS Export Configuration for Consolidated ROBO

VLAN	Server	Export	Size	Map As	Cluster	Component
1615	172.16.15.251	/VVD_vRLI_ROBO_250GB	250 GB	NFS datastore for log archiving in vRealize Log Insight	ROBO	vRealize Log Insight

Virtual Machine Specifications in ROBO

5

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 machine for Update Manager Download Service (UMDS) before you start the deployment of this management component in ROBO

Table 5-1. Specifications of Management Virtual Machines in ROBO

Attribute	vSphere Update Manager Download Service
Number of virtual machines	1
Guest OS	Ubuntu Server 14.04 LTS
VM name	nyc01umds01
VM folder	nyc01-r01fd-mgmt
Cluster	nyc01-r01-robo01
Datastore	nyc01-r01-vsan01
Number of CPUs	2
Memory (GB)	2
Disk space (GB)	120
SCSI Controller	LSI Logic SAS
Virtual machine network adapter	VMXNET3
Virtual machine network	Mgmt-NYC01-VXLAN
Active Directory Domain	rainpole.local
Service account	svc-umds
VMware Tools	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 5-2. 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

Management Workload Footprint in ROBO

6

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

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

Virtual Infrastructure Layer

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

Table 6-1. Virtual Infrastructure Layer Footprint for ROBO

Management Component	Operating System	vCPUs	Memory (GB)	Storage (GB)
vCenter Server	Virtual Appliance	4	16	270
NSX Manager	Virtual Appliance	4	16	60
NSX Controller 01	Virtual Appliance	4	4	28
NSX Controller 02	Virtual Appliance	4	4	28
NSX Controller 03	Virtual Appliance	4	4	28
NSX Edge Services Gateway 1 - ECMP	Virtual Appliance	2	1	2
NSX Edge Services Gateway 2 - ECMP	Virtual Appliance	2	1	2
NSX Edge Services Gateway 1 - DLR	Virtual Appliance	2	0.5	2
NSX Edge Services Gateway 2 - DLR	Virtual Appliance	2	0.5	2
Total		28 vCPU	47 GB	422 GB

Operations Management Layer

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

Table 6-2. Operations Management Layer Footprint for ROBO

Management Component	Operating System	vCPUs	Memory (GB)	Storage (GB)
Update Manager Download Service	Linux Virtual Machine	2	2	120
vRealize Operations Manager Remote Collector 1	Virtual Appliance	2	4	274
vRealize Operations Manager Remote Collector 2	Virtual Appliance	2	4	274
vRealize Log Insight Node 1	Virtual Appliance	8	16	530
vRealize Log Insight Node 2	Virtual Appliance	8	16	530
vRealize Log Insight Node 3	Virtual Appliance	8	16	530
Total		30 vCPU	58 GB	2,258 GB

Cloud Management Layer

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

Table 6-3. Cloud Management Layer Footprint for ROBO

Management Component	Operating System	vCPUs	Memory (GB)	Storage (GB)
vRealize Automation Proxy Agent 1	Windows Server Virtual Machine	2	8	60
vRealize Automation Proxy Agent 2	Windows Server Virtual Machine	2	8	60
vRealize Business for Cloud Data Collector	Virtual Appliance	4	2	50
Total		8 vCPU	18 GB	170 GB