Planning and Preparation

VMware Validated Design 4.0
VMware Validated Design for Remote Office Branch Office 4.0

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

Required VMware Software

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

Software Requirements in ROBO

2

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

Download the software for building the ROBO SDDC to a compatible client machine that is connected to the ESXi management network in the management pod.

This chapter includes the following topics:

VMware Scripts and Tools in ROBO

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

Table 2-1. 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 in ROBO

Download and license the following third-party software products.

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

SDDC Layer	Required by VMware Component	Vendor	Product Item	Product Version
Virtual Infrastructure	An end user machine in the data center that has access to the ESXi management network.	Any Supported	Operating system that is supported for deploying VMware vSphere. See System Requirements for the vCenter Server Appliance Installer.	Operating system for vSphere deployment.
Operations Management	Update Manager Download Service (UMDS)	Ubuntu	Ubuntu Server 14.04	Ubuntu Server 14.04 LTS
		PostgreSQL	PostgreSQL	9.3
		Nginx	Nginx	1.4
Cloud Management	vRealize Automation	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 Update (64-bit)

External Services in ROBO 3

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

This chapter includes the following topics:

External Services Overview in ROBO

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

Active Directory

This validated design uses Microsoft Active Directory (AD) for authentication and authorization to resources within the rainpole.local domain. You must ensure a domain controller is available in each ROBO location.

Table 3-1. Requirements for the Active Directory Service

Requirement	Domain Name	Description
Active Directory configuration	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* documentation must exist in the Active Directory before installing and configuring the ROBO SDDC.
Active Directory connectivity		All Active Directory domain controllers must be accessible by all management components within the consolidated pod.

DHCP

This validated design requires Dynamic Host Configuration Protocol (DHCP) support for the configuration of the VTEP (VXLAN) VMkernel ports on the ESXi hosts.

Table 3-2. DHCP Requirements

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

DNS

DNS is an important component for the operation of the ROBO SDDC.

Table 3-3. DNS Configuration Requirements

Requirement	Domain Instance	Description
DNS host entries	rainpole.local	Resides in the rainpole.local domain. Configure DNS zones with the following settings: ■ Dynamic updates for the zone set to **Nonsecure and secure**. ■ Zone replication scope for the domain set to **All DNS server in this forest.** ■ Create all hosts listed in the DNS Names 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 within the ROBO SDDC must be synchronized against a common time by using the Network Time Protocol (NTP) on all nodes. Important components of the ROBO SDDC, such as, vCenter Single Sign-On, are sensitive to a time drift between distributed components. See Time Synchronization in ROBO.

Table 3-4. 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 ROBO SDDC. Use the top of rack (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 ROBO 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 3-5. 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 ROBO SDDC component over plain SMTP (no SSL/TLS encryption). As a best practice, limit the relay function to the IP range of the ROBO SDDC deployment.

Certificate Authority

The majority of the components of the ROBO 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 3-6. 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 ROBO 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.

Table 3-7. FTP Server Requirements

Requirement	Description
FTP server	Space for NSX Manager backups must be available on an FTP server. The server must support SFTP and FTP. The NSX Manager instances must have connection to the remote FTP server.

Windows Host Machine

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

Table 3-8. Requirements for a Windows Host Machine

Requirement	Description
Windows host machine	Microsoft Windows virtual machine or physical server must be available to provide connection to the data center and store software downloads. The host must be connected to the external network and to the ESXi management network.

VLANs, IP Subnets, and Application Virtual Networks in ROBO

Before you start deploying the ROBO SDDC, you must allocate VLANs and IP subnets to the different types of traffic in the remote office and branch office, such as ESXi management, vSphere vMotion, and others. For application virtual networks, you must plan separate IP subnets for these networks.

VLAN IDs and IP Subnets for System Traffic in ROBO

This VMware Validated Design requires that the following VLAN IDs and IP subnets be allocated for the traffic types in the ROBO SDDC.

VLANs and IP Subnets in the first ROBO site

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

Table 3-9. VLAN and IP Subnet Configuration in the First ROBO site

VLAN Function	VLAN ID	Subnet	Gateway
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 These VLAN IDs and IP subnets are examples. The actual implementation depends on 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 3-10. IP Subnet for the Application Virtual Network

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

Note Use this IP subnet as a sample. Configure the actual IP subnet according to your environment.

DNS Names and IP Addresses in ROBO

You must provide the necessary DNS names and IP addresses required by the ROBO SDDC deployment.

Before you deploy the ROBO SDDC, create forward and reverse DNS records for all of the management components

Host Names and IP Addresses for External Services in ROBO

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

Each ROBO site must have a local Active Directory domain controller and NTP server. This ensures authentication and time sync still works in the event the connection between the hub and ROBO site is down.

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

Note These FQDN's and IP addresses are examples. Use the FQDN and IP addresses for Active Directory and NTP you currently have configured in your environment.

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

Allocate DNS names and IP addresses to the vSphere and NSX components.

Table 3-11. Host Names and IP Addresses for the Virtual Infrastructure Components

Component Group	DNS Name	IP Address	Description
vSphere	nyc01esx01.rainpole.local	172.18.11.101	ESXi host
	nyc01esx02.rainpole.local	172.18.11.102	ESXi host
	nyc01esx03.rainpole.local	172.18.11.103	ESXi host
	nyc01esx04.rainpole.local	172.18.11.104	ESXi host
	nyc01vc01.rainpole.local	172.18.11.62	vCenter Server
NSX for vSphere	nyc01nsxm01.rainpole.local	172.18.11.65	NSX Manager
	nyc01nsxc01.rainpole.local	172.18.11.118	Reserved. NSX Controllers
	nyc01nsxc02.rainpole.local	172.18.11.119	
	nyc01nsxc03.rainpole.local	172.18.11.120	

Table 3-11. Host Names and IP Addresses for the Virtual Infrastructure Components (Continued)

Component Group	DNS Name	IP Address	Description
	NYC01-ESG01	■ 172.18.16.2 ■ 172.18.17.3 ■ 172.18.18.1	ECMP-enabled NSX Edge device for North-South traffic
	NYC01-ESG02	■ 172.18.16.3 ■ 172.18.17.2 ■ 172.18.18.2	ECMP-enabled NSX Edge device for North-South traffic
	NYC01-DLR01	172.18.18.3	Distributed Logical Router (DLR) for East-West traffic

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

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

For the Cloud Management Platform, this design uses specific IP addresses and DNS names for the following nodes:

- Proxy Agents
- vRealize Business nodes

Component Group	DNS Name	IP Address	Description
vRealize Automation Proxy Agents	nyc01ias01.rainpole.local	172.18.19.52	vRealize Automation Proxy Agent
	nyc01ias02.rainpole.local	172.18.19.53	vRealize Automation Proxy Agent
vRealize Business Data Collectors	nyc01buc01.rainpole.local	172.18.19.54	vRealize Business Data Collector

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

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

Component Group	DNS Name	IP Address	Description
vSphere Data Protection	nyc01vdp01.rainpole.local	172.18.11.81	vSphere Data Protection primary appliance
vRealize Operations Manager	nyc01rmtcol01.rainpole.local	172.18.19.31	Remote Collector 1 of vRealize Operations Manager
	nyc01rmtcol02.rainpole.local	172.18.19.32	Remote Collector 2 of vRealize Operations Manager
vSphere Update Manager	nyc01umds01.rainpole.local	172.18.19.67	vSphere Update Manager Download Service (UMDS)

Component Group	DNS Name	IP Address	Description
vRealize Log Insight	nyc01vrli01-cluster01.rainpole.local	172.18.19.10	VIP address of the integrated load balancer of vRealize Log Insight
	nyc01vrli01.rainpole.local	172.18.19.11	Master node of vRealize Log Insight
	nyc01vrli02.rainpole.local	172.18.19.12	Worker node 1 of vRealize Log Insight
	nyc01vrli03.rainpole.local	172.18.19.13	Worker node 2 of vRealize Log Insight

Time Synchronization in ROBO

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 ROBO 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 in ROBO

All management components in your ROBO deployment need to 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 3-12. 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	172.18.11.252

Time Synchronization on the Management Nodes

- Synchronize the time with the NTP servers on the following systems:
  - ESXi hosts

- 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 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 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 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 in ROBO

Before you deploy and configure the ROBO 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.

The Active Directory service and user accounts required have already been configured as part of the VMware Validated Design for SDDC deployment. These service and user accounts can be re-used for ROBO deployments.

Active Directory Administrator Account

Certain installation and configuration tasks require a domain administrator or an account that has the required rights delegated to it, that is referred to as `ad_admin_acct` of the Active Directory domain.

Certificate Replacement in ROBO

Before you deploy the ROBO 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 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.

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

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

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

Procedure

1. Log in to a Windows Server 2012 host that has access to the data center as AD administrator and is part of rainpole.local domain.
2. Download and extract the Certificate Generation Utility from VMware Knowledge Base article 2146215.
   a. Open the VMware Knowledge Base article in a Web browser.
   b. Extract `CertGenVVD-3.0.zip` to the `C:` drive.
3. In the `c:\CertGenVVD-3.0` 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
```

   Note These are default values and should be updated to reflect your orginization.

5. Verify that only the following files are available in the `c:\CertGenVVD-3.0\ConfigFiles` folder and `LOC=NYC` is in the text files.
   - nyc01nsxm01.txt
   - nyc01vc01.txt
   - nyc01vdp01.txt
   - nyc01vrb.txt
   - nyc01vrli.txt

   Note The vRealize Automation Proxy Agents use the same certificate generated for the Proxy Agents in the VMware Validated Design for SDDC deployment.

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

```
cd c:\CertGenVVD-3.0
```

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

```
Set-ExecutionPolicy RemoteSigned
```

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

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

```
.\CertgenVVD-3.0.ps1 -validate
```

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

```
.\CertGenVVD-3.0.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
```

10 In the `c:\CertGenVVD-3.0` 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.