VMware Validated Design™ for Micro-Segmentation Planning and Preparation Guide

VMware Validated Design
for Micro-Segmentation 3.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002253-00

vmware®

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com

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

Contents

1. Purpose and Intended Audience

VMware Validated Design for Micro-Segmentation Planning and Preparation Guide provides detailed information about the requirements to software, tools and external services required to successfully implement the VMware Validated Design for Micro-Segmentation platform.

Before you start deploying the components of the VMware Validated Design, you must set up an environment that has a specific compute, storage and network configuration, and that provides services to the components in the data center. Carefully review the *VMware Validated Design Planning and Preparation Guide* documentation to avoid costly rework and delays.

Note The *VMware Validated Design for Micro-Segmentation Planning and Preparation Guide* is compliant and validated with certain product versions. See *Introducing the VMware Validated Design for Micro-Segmentation* for more information about supported product versions.

VMware Validated Design for Micro-Segmentation Planning and Preparation Guide 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, and extensibility for backup and restore, and disaster recovery support.

1.1 About Regions Mentioned in This Document

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

2. Software Requirements

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

Download the software to a Windows host machine that is connected to the ESXi management network in the management pod.

2.1 VMware Software

Download and license the following VMware software products.

Table 1. VMware Software Required for the VMware Validated Design

Layer	Product Group & Edition	Product Name	Product Version
Virtual Infrastructure	VMware vSphere Enterprise Plus	VMware ESXi™	6.0 Update 2
	VMware vCenter Server Standard	vCenter® Server Appliance™ (ISO)	6.0 Update 2
	VMware NSX for vSphere Enterprise	NSX for vSphere	6.2.4
Service Management	VMware vRealize Log Insight™	vRealize Log Insight	3.3.2
		vRealize Log Insight Content Pack for NSX for vSphere	3.3

2.2 VMware Scripts and Tools

Download the following script that this VMware Validated Design uses.

Table 2. VMware Scripts and Tools Required for the VMware Validated Design

Script/Tool	Download Location	Description
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..

2.3 Third-Party Software

Download and license the following third-party software products.

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

Layer	Required by	Vendor	Product Item	Product Version
Virtual Infrastructure	Windows host that connects to the management network and has access to the data center	Microsoft	Windows OS for the vSphere Client. See VMware Knowledge Base article 2100436.	Version of the Windows OS that is supported for the vSphere Client 6.0 U2

3. External Service Dependencies

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

3.1 Active Directory

This validated design uses Microsoft Active Directory (AD) for authentication and authorization to resources within the **`rainpole.local`** domain. Using a domain and forest structure to store and manage Active Directory objects will facilitate expansion to a multi-region deployment later.

Table 4. Requirements for the Active Directory Service

Requirement	Domain Instance	Domain Name	Description
Active Directory configuration	Parent Active Directory	rainpole.local	Contains Domain Name System (DNS) server, time server, and universal groups that contain global groups from the child domains and are members of local groups in the child domains.
	Region-A child Active Directory	sfo01.rainpole.local	Contains DNS records that replicate to all DNS servers in the forest. This child domain contains all users of this design, and global and local groups.
Active Directory users and groups	-		All user accounts and groups from the Active Directory Users and Groups documentation must exist in the Active Directory before installing and configuring the data center.
Active Directory connectivity	-		All Active Directory domain controllers must be accessible by all components within the management pod.

3.2 DHCP

This validated design requires Dynamic Host Configuration Protocol (DHCP) support for the configuration of each VMkernel port of an ESXi host with an IPv4 address. The configuration includes the VMkernel ports for the ESXi management network, vSphere vMotion, VXLAN (VTEP) and NFS.

Table 5. DHCP Requirements

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

3.3 DNS

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

Table 6. DNS Configuration Requirements

Requirement	Domain Instance	Description
DNS host entries	`rainpole.local`	Resides in the `rainpole.local` domain.
	`sfo01.rainpole.local`	DNS server that resides in the `sfo01.rainpole.local` domains. Configure the 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 servers in this forest** • Create all hosts listed in the *DNS Names* documentation.

If you configure the DNS servers properly, all nodes from the validated design are resolvable by FQDN.

3.4 NTP

All components must be synchronized against a common time by using the Network Time Protocol (NTP) on all nodes. Important components, such as vCenter Single Sign-On, are sensitive to time drift between distributed components. See *Time Synchronization* in the *Architecture Reference*.

Table 7. 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. Use the ToR switches in the management pods as the NTP servers or the upstream physical router. Ensure that these switches synchronize with different upstream NTP servers and provide time synchronization capabilities within the environment. As a best practice, make the NTP servers available under a friendly FQDN, for example, `ntp.sfo01.rainpole.local`.

3.5 SMTP Mail Relay

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

Table 8. 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 component over plain SMTP (no SSL/TLS encryption). As a best practice, limit the relay function to the IP range of the deployment.

3.6 Certificate Authority

The majority of the components in the VMware Validate Design for Micro-Segmentation 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. You can use the CertGenVVD tool to generate the CSRs.

Table 9. CA Requirements for Signing Certificates of Management Applications

Requirement	Description
Certificate Authority	CA must be able to ingest a Certificate Signing Request (CSR) 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.

3.7 FTP Server

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

Table 10. 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.

3.8 Windows Host Machine

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

Table 11. Requirements for a Windows Host Machine

Requirement	Description
Windows host machine	Microsoft Windows virtual machine or physical server that can connect to the data center and store software downloads. The host must be connected to the external network and to the ESXi management network. For information about the Windows OS requirements for the host and the software downloads for this validated design, see *Software Requirements*.

4. Physical VLANs, IP Subnets and Application Virtual Networks

Before you start deployment, you must allocate VLANs and IP subnets to the different types of traffic, such as ESXi management, vSphere vMotion, and others.

4.1 VLAN IDs and IP Subnets for System Traffic

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

4.1.1 VLANs and IP Subnets

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

Table 12. VLAN and IP Subnet Configuration

POD	VLAN Function	VLAN	Subnet	Gateway
Management Pod	ESXi Management	1611	172.16.11.0/24	172.16.11.253
	vSphere vMotion	1612	172.16.12.0/24	172.16.12.253
	VXLAN (VTEP)	1614	172.16.14.0/24	172.16.14.253
	NFS	1615	172.16.15.0/24	172.16.15.253
	Uplink01	2711	172.27.11.0/24	172.27.11.253
	Uplink02	2712	172.27.12.0/24	172.27.12.253
	External Management Connectivity	130	10.158.130.0/24	10.158.130.253
Shared Edge and Compute Pod	ESXi Management	1631	172.16.31.0/24	172.16.31.253
	vSphere vMotion	1632	172.16.32.0/24	172.16.32.253
	VXLAN (VTEP)	1634	172.16.34.0/24	172.16.34.253
	NFS	1625	172.16.25.0/24	172.16.25.253
	External Tenant Connectivity	140	10.158.140.0/24	10.158.140.253

4.2 Names and IP Subnets of Application Virtual Networks

This VMware Validated Design uses the following IP subnets in the application virtual networks for the management applications.

Table 13. Application Network Names and IP Subnets

Application Virtual Networks	Subnet
Mgmt-RegionA01-VXLAN	192.168.31.0/24

5. DNS Names

Before you deploy this validated design, you must create a DNS configuration of fully qualified domain names (FQDNs) and map them to the IP addresses of the management application nodes.

This section presents the design for two domains in case the use case is scaled to a two-region design. You can perform the setup for only one domain initially.

If you expand to a multi-region deployment, you assign IP subnets and DNS configuration to each sub-domain, **`sfo01.rainpole.local`** and **`lax01.rainpole.local`**

5.1 DNS Names and IP Addresses

Provide DNS names and IP addresses for your deployment.

5.1.1 Host Names and IP Addresses for External Services

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

Table 14. Host Names and IP Addresses for External Services

Component Group	DNS Name	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 pod
	0.ntp.sfo01.rainpole.local	172.16.11.251	NTP server on a ToR switch in the management pod
	1.ntp.sfo01.rainpole.local	172.16.11.252	NTP server on a ToR switch in the management pod
AD/DNS/CA	dc01rpl.rainpole.local	172.16.11.4	Windows 2012 R2 host that contains the Active Directory configuration and DNS server for the rainpole.local domain, and the Microsoft Certificate Authority for signing management SSL certificates
	dc01sfo.sfo01.rainpole.local	172.16.11.5	Active Directory and DNS server for the sub-domains

5.1.2 Host Names and IP Addresses for the Virtual Infrastructure Components

Allocate DNS names and IP addresses to ESXi hosts, vCenter Server instances and connected Platform Services Controller instances, and NSX components. If you expand to a dual-region deployment of the full VMware Validated Design for the Software-Defined Data Center, you also allocate host names and IP addresses to the nodes that run Site Recovery Manager and vSphere Replication in each region.

Table 15. Host Name and IP addresses for the Virtual Infrastructure Components

Component Group	DNS Name	IP Address	Description
vSphere	mgmt01esx01.sfo01.rainpole.local	172.16.11.101	ESXi host in the management pod
	mgmt01esx02.sfo01.rainpole.local	172.16.11.102	ESXi host in the management pod
	mgmt01esx03.sfo01.rainpole.local	172.16.11.103	ESXi host in the management pod
	mgmt01esx04.sfo01.rainpole.local	172.16.11.104	ESXi host in the management pod
	comp01esx01.sfo01.rainpole.local	172.16.31.101	ESXi host in the shared edge and compute pod
	comp01esx02.sfo01.rainpole.local	172.16.31.102	ESXi host in the shared edge and compute pod
	comp01esx03.sfo01.rainpole.local	172.16.31.103	ESXi host in the shared edge and compute pod
	comp01esx04.sfo01.rainpole.local	172.16.31.104	ESXi host in the shared edge and compute pod
	mgmt01psc01.sfo01.rainpole.local	172.16.11.61	Platform Services Controller for the Management vCenter Server
	mgmt01vc01.sfo01.rainpole.local	172.16.11.62	Management vCenter Server
	comp01psc01.sfo01.rainpole.local	172.16.11.63	Platform Services Controller for the Compute vCenter Server
	comp01vc01.sfo01.rainpole.local	172.16.11.64	Compute vCenter Server
NSX for vSphere	mgmt01nsxm01.sfo01.rainpole.local	172.16.11.65	NSX Manager for the management cluster
	mgmt01nsxc01.sfo01.rainpole.local	172.16.11.118	Reserved.
	mgmt01nsxc02.sfo01.rainpole.local	172.16.11.119	NSX Controllers for the management cluster
	mgmt01nsxc03.sfo01.rainpole.local	172.16.11.120	
	comp01nsxm01.sfo01.rainpole.local	172.16.11.66	NSX Manager for the shared edge and compute cluster
	comp01nsxc01.sfo01.rainpole.local	172.16.31.118	Reserved
	comp01nsxc02.sfo01.rainpole.local	172.16.31.119	
	comp01nsxc03.sfo01.rainpole.local	172.16.31.120	NSX Controllers for the compute and edge clusters

Component Group	DNS Name	IP Address	Description
	SFOMGMT-ESG01	172.27.11.2 172.27.12.3 192.168.10.1	ECMP-enabled NSX Edge device for North-South management traffic
	SFOMGMT-ESG02	172.27.11.3 172.27.12.2 192.168.10.2	ECMP-enabled NSX Edge device for North-South management traffic
	UDLR01	192.168.10.3	Universal Distributed Logical Router (UDLR) for East-West management traffic.
	SFOCOMP-ESG01	172.16.35.2 172.27.13.3 192.168.100.1	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	SFOCOMP-ESG02	172.16.35.3 172.27.13.2 192.168.100.2	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	UDLR01	192.168.100.3	Universal Distributed Logical Router (UDLR) for East-West compute and edge traffic.
	SFOMGMT-LB01	192.168.11.2	NSX Edge device for load balancing management applications.

5.1.3 Host Names and IP Addresses for vRealize Log Insight

Allocate DNS names and IP addresses to vRealize Log Insight.

Table 16. Host Name and IP address for vRealize Log Insight

DNS Name	IP Address	Description
vrli-cluster-01.sfo01.rainpole.local	192.168.31.10	VIP address of the integrated load balancer of vRealize Log Insight
vrli-mstr-01.sfo01.rainpole.local	192.168.31.11	Master node of vRealize Log Insight
vrli-wrkr-01.sfo01.rainpole.local	192.168.31.12	Worker node 01 of vRealize Log Insight
vrli-wrkr-02.sfo01.rainpole.local	192.168.31.13	Worker node 02 of vRealize Log Insight

6. Time Synchronization

Consistent system clocks are critical for the proper operation because some components rely on vCenter Single Sign-On, which requires synchronized components.

NTP also makes it easier to correlate log files from multiple sources during troubleshooting, auditing, or inspection of log files to detect attacks.

6.1 Requirements for Time Synchronization

Use the following approach to reduce the impact of time synchronization issues.

- Configure two external time sources. 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 NTP dispersion.
- Configure a DNS CNAME that maps the two time sources to one DNS name.

Table 17. 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

- Synchronize the time with the NTP servers on the following systems:
  - ESXi hosts
  - AD domain controllers
  - Virtual appliances of the management applications
- Configure each system with the regional NTP server alias `ntp.sfo01.rainpole.local`
- Verify that the default configuration on the Windows VMs is active, that is, any Windows VMs is 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. NTP is an industry standard and ensures accurate timekeeping in the guest operating system.

6.2 Configure NTP-Based Time Synchronization on Windows Hosts

On Windows, enable NTP-based synchronization.

1. Open the command prompt as Administrator.
2. Run the following console command to enable time synchronization with the NTP servers on the ToR switches.

```
w32tm /config /manualpeerlist:"ntp.sfo01.rainpole.local"
/syncfromflags:manual /reliable:YES /update
```

3. Restart the Windows Time service to apply the changes.

```
net stop w32time
net start w32time
```

4. Verify the time synchronization configuration.
   a. Run the following console.

```
w32tm /query /status
```

   b. Verify that the `ReferenceId:` attribute in the output contains one of these servers in each region: 172.16.11.251, 172.16.11.252.
   c. If the `ReferenceId:` attribute contains `LOCL` instead of the IP address of at least one of the 4 NTP servers, run the following command and wait for the re-synchronization to complete.

```
w32tm /resync
```

   d. Query the status of the Windows Time service again:

```
w32tm /query /status
```

7. Active Directory Users and Groups

Before you deploy this validated design, set up Active Directory users and groups.

To prepare for expansion to a multi-region environment that has parent and child domains in a single forest, store service accounts in the parent domain and user accounts in each of the child domains. By using the group scope attribute of Active Directory groups you manage resource access across domains.

7.1 Active Directory Administrator Account

Certain installation and configuration tasks require a domain administrator account in the Active Directory domain (`ad_admin_acct`).

7.2 Active Directory Groups

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

1. Add user and service accounts to universal groups in the parent domain.
2. Add the universal groups to global groups in each child domain.
3. Assign access right and permissions to the local groups in the child domains according to their role.

7.3 Universal Groups in the Parent Domain

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

Table 18. Universal Groups in the rainpole.local Parent Domain

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

7.4 Global Groups in the Child Domain

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

Table 19. Local Groups in the sfo01.rainpole.local Child Domain

Group Name	Group Scope	Description	Member of Groups
SDDC-Admins	Global	Administrative group.	RAINPOLE\ug-SDDC-Admins
SDDC-Ops	Global	Operators group	RAINPOLE\ug-SDDC-Ops
vCenterAdmins	Global	Group with accounts that are assigned vCenter Server administrator privileges	RAINPOLE\ug-vCenterAdmins

7.5 Active Directory Users

7.5.1 Service Accounts

A service account provides components of the deployment with non-interactive and non-human access to services and APIs. A service account is a standard Active Directory account that you configure in the following way:

- The password never expires.
- The user cannot change the password.
- The account must have the right to join computers to the Active Directory domain.

7.5.2 Service Accounts in the Parent Domain

Create the following service accounts in the parent Active Directory domain `rainpole.local` to provide centralized authentication of the products in this validated design.

Table 20. Service Accounts in the rainpole.local Parent Domain

User Name	Description	Service Account	Member of Groups
svc-loginsight	Read-only service account for using the Active Directory as an authentication source in vRealize Log Insight and for forwarding log information from vCenter Server and ESXi to vRealize Log Insight.	Yes	
svc-nsxmanager	Service account for registering NSX Manager with vCenter Single Sign-on on the Platform Services Controller and vCenter Server for the management cluster and for the shared edge and compute cluster.	Yes	RAINPOLE\ug-vCenterAdmins

7.5.3 User Accounts in the Child Domains

Create the following accounts for user access in each of the child Active Directory domain, **`sfo01.rainpole.local`**, to provide centralized user access in this VMware Validated Design. In the Active Directory, you do not assign any special rights to these accounts other than the default ones.

Table 21. User Accounts in the sfo01.rainpole.local Child Domain

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

8. Datastore Requirements

For certain features, such as log archiving, you must provide NFS exports as storage. You must also provide a validated datastore to the shared edge and compute cluster for storing NSX Controller and Edge instances and tenant workloads.

8.1 NFS Exports for Management Components

The management applications use NFS exports with the following paths.

Table 22. NFS Export Configuration

VLAN	Server	Export	Size	Map As	Cluster	Component
1615	172.16.15.251	/V2D_vRLI_MgmtA_1TB	1TB	NFS datastore for vRealize Log Insight log archiving	Management cluster	vRealize Log Insight

8.2 Customer-Specific Datastore for the Shared Edge and Compute Clusters

To enable the deployment of virtual appliances that are a part of the NSX deployment before you begin implementing this design, you must set up datastores for the shared edge and compute cluster. This validated design contains guidance for datastore setup only for the management components. For more information about the datastore types that are supported for the shared and edge cluster, see *Shared Storage Design* in the *VMware Validated Design for Micro-Segmentation Reference Architecture* guide.