Deployment of Region A

19 MAR 2019
VMware Validated Design 5.0
VMware Validated Design for Software-Defined Data Center 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 Deployment of Region A

1

The *VMware Validated Design Deployment of Region A* documentation provides step-by-step instructions for installing, configuring, and operating a software-defined data center (SDDC) based on the VMware Validated Design for Software-Defined Data Center, using the VMware Cloud Builder virtual appliance to automate the implementation of this Validated Design.

The *VMware Validated Design Deployment of Region A* documentation does not contain step-by-step instructions for performing all required post-configuration tasks because their nature often depends on the requirements of your organization.

Intended Audience

The *VMware Validated Design Deployment of Region A* 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 Deployment of Region A* documentation is compliant and validated with certain product versions. See *VMware Validated Design 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 Deployment of Region A*, you must be acquainted with the following guidance:

- *Introducing VMware Validated Designs*
- Optionally *VMware Validated Design Architecture and Design*
- *VMware Validated Design Planning and Preparation*

Updated Information

This *VMware Validated Design Deployment of Region A* document is updated with each release of the product or when necessary.

This table provides the update history of the *Deployment of Region A* document.

Revision	Description
19 MAR 2019	■ Changed login method during post deployment configuration of the vShere Update Manager Download Service virtual machine from SSH to virtual console. See Reconfigure Update Manager Download Service in Region A.
12 FEB 2019	■ Clarified requirements for primary and secondary storage capacity . See Prerequisites for Automated SDDC Deployment in Region A. ■ Added a step to run again the `/opt/vmware/vvd/cloud-builder/install/reconfigure.sh` script on the VMware Cloud Builder appliance if validation of the deployment `.json` files fails because of issues with the signed certificate files you previously uploaded. See Validate the Deployment Parameters and Target Environment Prerequisites for the Management Cluster and the Shared Edge and Compute Cluster in Region A.
22 JAN 2019	Initial Release

Prepare the Environment for Automated Deployment in Region A

2

Before you start the automated deployment of VMware Validated Design for Software-Defined Data Center using VMware Cloud Builder, your environment must meet target prerequisites and be in a specific starting state. Prepare each layer of the SDDC by deploying and configuring the necessary infrastructure, operational, and management components.

- Prerequisites for Virtual Infrastructure Layer Implementation in Region A

  To prepare the virtual infrastructure layer of the SDDC, you first install ESXi on all hosts for the management cluster and for the shared edge and computecluster, configure the management network, DNS, NTP, and SSH services.

- Prerequisites for Operations Management Layer Implementation in Region A

  To prepare the operations management layer for automated deployment of SDDC components using Cloud Builder, you deploy and configure a Linux virtual machine for vSphere Update Manager Download Service.

- Prerequisites for Cloud Management Layer Implementation in Region A

  To prepare the cloud management layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure the Master Windows system for vRealize Automation Infrastructure as a Service (IaaS) nodes and deploy and configure the external SQL server for vRealize Automation.

- Prerequisites for Business Continuity Layer Implementation in Region A

  To prepare the business continuity layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure the Site Recovery Manager Windows virtual machine.

- Generate Certificates for the SDDC Components in Region A

  To ensure secure and operational connectivity between the SDDC components, you generate new signed certificates for the SDDC components in Region A.

Prerequisites for Virtual Infrastructure Layer Implementation in Region A

To prepare the virtual infrastructure layer of the SDDC, you first install ESXi on all hosts for the management cluster and for the shared edge and computecluster, configure the management network, DNS, NTP, and SSH services.

Procedure

1 Prerequisites for Installation of ESXi Hosts in Region A

You prepare for the installation and configuration of all ESXi hosts in the management cluster and the shared edge and compute cluster. You use the same process to install and configure the hosts for both clusters.

2 Install ESXi Interactively on All Hosts in Region A

Install ESXi on all hosts in the management and the shared edge and computeclusters interactively.

3 Configure the Network on all Hosts in Region A

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

4 Configure the Virtual Machine Network Port Group on All Hosts in Region A

You perform network configuration for each ESXi host using the VMware Host Client.

5 Configure SSH and NTP on All Hosts in Region A

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service. You then configure the NTP service to avoid time synchronization issues in the SDDC.

6 Mount NFS Storage on all ESXi Hosts in Region A

This VMware Validated Design uses NFS storage as secondary storage for the SDDC management components. You mount the NFS storage to provide storage capacity for archiving log data, backup, and application templates.

7 Configure DNS Settings for the Platform Services Controller Load Balancer in Region A

This VMware Validated Design deploys two Platform Services Controllers behind a load balancer implemented through NSX for vSphere. When you prepare your environment for automated deployment using Cloud Builder, NSX for vSphere is not yet available. You perform DNS configuration to emulate an existing load balancer IP address.

Prerequisites for Installation of ESXi Hosts in Region A

You prepare for the installation and configuration of all ESXi hosts in the management cluster and the shared edge and compute cluster. You use the same process to install and configure the hosts for both clusters.

Before you start:

- Make sure that you have a Windows host that has access to your data center. You use this host to connect to the data center and perform configuration steps.

You must also prepare the installation files.

- Download the ESXi ISO installer.
- Create a bootable USB drive that contains the ESXi Installation. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade" in *vSphere Installation and Setup*.

IP Addresses, Hostnames, and Network Configuration

The following values are required to configure your hosts.

Table 2-1. Management Cluster Hosts

FQDN	IP	VLAN ID	Default Gateway	NTP Server
sfo01m01esx01.sfo01.rainpole.local	172.16.11.101	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo01m01esx02.sfo01.rainpole.local	172.16.11.102	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo01m01esx03.sfo01.rainpole.local	172.16.11.103	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo01m01esx04.sfo01.rainpole.local	172.16.11.104	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Table 2-2. Shared Edge and Compute Cluster Hosts

FQDN	IP	VLAN ID	Default Gateway	NTP Server
sfo01w01esx01.sfo01.rainpole.local	172.16.31.101	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo01w01esx02.sfo01.rainpole.local	172.16.31.102	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo01w01esx03.sfo01.rainpole.local	172.16.31.103	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo01w01esx04.sfo01.rainpole.local	172.16.31.104	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

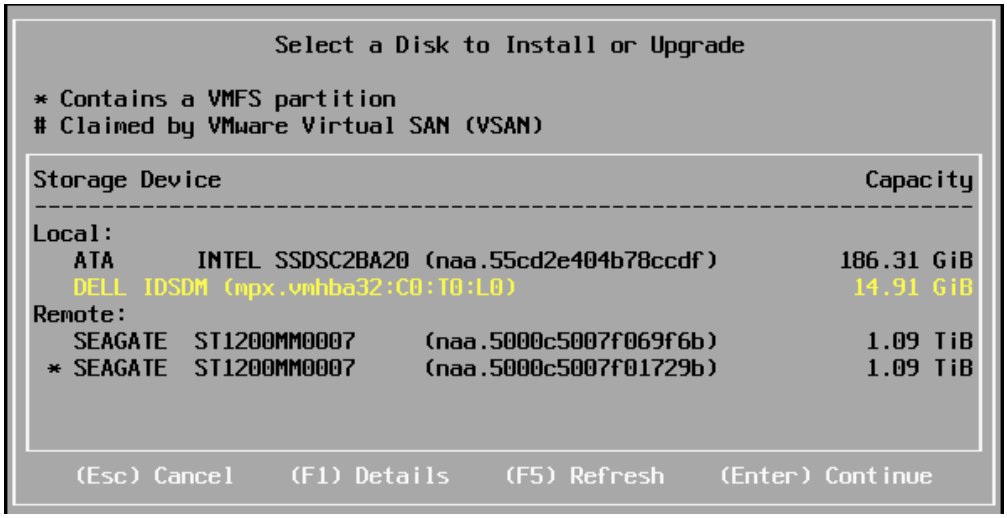
Install ESXi Interactively on All Hosts in Region A

Install ESXi on all hosts in the management and the shared edge and computeclusters interactively.

Repeat this procedure for all hosts in the management and shared edge and compute clusters. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts in Region A.

Procedure

1. Power on the **`sfo01m01esx01`** host.
2. Mount the USB drive containing the ESXi ISO file and boot from that USB drive.
3. On the **Welcome to the VMware 6.7 U1 Installation** screen, press Enter to start the installation.
4. On the **End User License Agreement (EULA)** screen, press F11 to accept the EULA.
5. On the **Select a Disk to Install or Upgrade** screen, select the USB drive under local storage to install ESXi and press Enter to continue.



6 Select the keyboard layout and press Enter.

7 Enter the ***esxi_root_user_password***, enter the password a second time to confirm the spelling and press Enter.

8 On the **Confirm Install** screen, press **F11** to start the installation.

9 After the installation completes successfully, unmount the USB drive and press Enter to reboot the host.

Configure the Network on all Hosts in Region A

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

Perform the following tasks to configure the host network settings:

- Configure the network adapter (vmk0) and VLAN ID for the Management Network.
- Configure the IP address, subnet mask, gateway, DNS server, and FQDN for the ESXi host.

Repeat this procedure for all hosts in the management and shared edge and compute clusters. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts in Region A.

Procedure

1 Open the DCUI on the physical ESXi host **sfo01m01esx01.sfo01.rainpole.local**.

a Open a console window to the host.

b Press F2 to enter the DCUI.

c Log in using the following credentials.

Setting	Value
User name	**root**
Password	***esxi_root_user_password***

2 Configure the network.

a Select **Configure Management Network** and press Enter.

b Select **VLAN (Optional)** and press Enter.

c Enter **1611** as the VLAN ID for the Management Network and press Enter.

d Select **IPv4 Configuration** and press Enter.

e Configure the IPv4 network using the following settings and press Enter.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.16.11.101
Subnet Mask	255.255.255.0
Default Gateway	172.16.11.253

f Select **DNS Configuration** and press Enter.

g Configure DNS using the following settings and press Enter.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.16.11.5
Alternate DNS Server	172.16.11.4
Hostname	sfo01m01esx01.sfo01.rainpole.local

h Select **Custom DNS Suffixes** and press Enter.

i Ensure that there are no suffixes listed and press Enter.

3 Press Escape to exit and press Y to confirm the changes.

Configure the Virtual Machine Network Port Group on All Hosts in Region A

You perform network configuration for each ESXi host using the VMware Host Client.

You configure the VLAN ID of the VM Network portgroup on the vSphere Standard Switch. This configuration provides connectivity and common network configuration for virtual machines that reside on each host.

You repeat this procedure for all hosts in the management and the shared edge and compute cluster with the following VLAN IDs.

Table 2-3. Default VM Network Port Group for the Management and the Shared Edge and Compute Clusters

Host	VLAN ID
sfo01m01esx01.sfo01.rainpole.local	1611
sfo01m01esx02.sfo01.rainpole.local	1611
sfo01m01esx03.sfo01.rainpole.local	1611
sfo01m01esx04.sfo01.rainpole.local	1611
sfo01w01esx01.sfo01.rainpole.local	1631
sfo01w01esx02.sfo01.rainpole.local	1631
sfo01w01esx03.sfo01.rainpole.local	1631
sfo01w01esx04.sfo01.rainpole.local	1631

Procedure

1. Log in to the vSphere host by using the VMware Host Client.
   a. Open a Web browser and go to `https://sfo01m01esx01.sfo01.rainpole.local`.
   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2. Click **OK** to Join the Customer Experience Improvement Program.
3. Configure a VLAN for the VM Network port group.
   a. In the Navigator, click **Networking**, click the **Port Groups** tab, select the **VM Network** port group, and click **Edit Settings**.
   b. On the **Edit port group - VM Network** window, enter `1611` for **VLAN ID**, and click **Save**.

Configure SSH and NTP on All Hosts in Region A

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service. You then configure the NTP service to avoid time synchronization issues in the SDDC.

Repeat this procedure for all hosts in the management and shared edge and compute clusters. See Prerequisites for Installation of ESXi Hosts in Region A.

Procedure

1 Log in to the vSphere host by using the VMware Host Client.

   a Open a Web browser and go to **`https://sfo01m01esx01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Configure and start the TSM-SSH service.

   a In the Navigator, click **Manage** and click the **Services** tab.

   b Select the **TSM-SSH** service, and click the **Actions** menu.

   c Select **Policy** and click **Start and stop with host**.

   d Click **Start** to start the service.

3 Configure and start the NTP service.

   a In the Navigator, click **Manage**, click the **System** tab.

   b Click **Time & date** and click **Edit Settings**.

   c In the **Edit time configuration** dialog box, select the **Use Network Time Protocol (enable NTP client)** radio button, change the NTP service startup policy to **Start and stop with host**, and in the **NTP servers** text box, enter**`ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local`**.

   d Click **Save**.

   e Start the service by clicking **Actions**, select **NTP service**, and click **Start**.

Mount NFS Storage on all ESXi Hosts in Region A

This VMware Validated Design uses NFS storage as secondary storage for the SDDC management components. You mount the NFS storage to provide storage capacity for archiving log data, backup, and application templates.

Repeat this procedure for all hosts in the management and shared edge and compute clusters. See Prerequisites for Installation of ESXi Hosts in Region A.

Prerequisites

Verify that you have allocated static IP addresses for each ESXi VMkernel storage port.

Procedure

1 Log in to the vSphere host by using the VMware Host Client.

   a Open a Web browser and go to **`https://sfo01m01esx01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Configure the Maximum Transmission Units (MTU) on the standard virtual switch.

   a In the **Navigator**, select **Networking > Virtual switches > vSwitch0 > Edit**.

   b In the **Edit standard virtual switch** dialog box, enter the following values, and click **Save**.

Setting	Value
MTU	9000
Uplink1	vmnic0

3 Configure a VMkernel storage port on all ESXi hosts.

   a In the **Navigator**, select **Networking**.

   b Select the **VMkernel NICs** and click **Add VMkernel NIC**.

   c In the **Add VMkernel NIC** dialog box, enter the following values, and click **Create**.

Setting	Value for Management Cluster	Value for Shared Edge and Compute Cluster
Port Group	New port group	New port group
New Port Group	Storage	Storage
Virtual Switch	vSwitch0	vSwitch0
VLAN ID	1615	1625
MTU	9000	9000
IP version	IPv4 only	IPv4 only
IPv4 settings	Static	Static
Address	172.16.15.101	172.16.25.101
Subnet mask	255.255.255.0	255.255.255.0
TCP/IP stack	Default TCP/IP stack	Default TCP/IP stack
Services	Deselected	Deselected

4 Mount the NFS datastore on the ESXi host.

a In the **Navigator**, select **Storage > Datastores > New datastore**.

The **New datastore** dialog box appears.

b On the **Select creation type** dialog box, select **Mount NFS datastore** and click **Next**.

c On the **Provide NFS mount details** dialog box, enter the following values.

Setting	Value for Management Cluster	Value for Shared Edge and Compute Cluster
Name	sfo01-m01-bkp01	sfo01-w01-lib01
NFS Server	172.16.15.251	172.16.25.251
NFS Share	`/VVD_backup01_nfs01_MgmtA_6TB`	`/VVD_vRA_ComputeA_1TB`
NFS Version	NFS 3	NFS 3

d Click **Next**.

e On the **Ready to complete** dialogue box, click **Finish**.

Configure DNS Settings for the Platform Services Controller Load Balancer in Region A

This VMware Validated Design deploys two Platform Services Controllers behind a load balancer implemented through NSX for vSphere. When you prepare your environment for automated deployment using Cloud Builder, NSX for vSphere is not yet available. You perform DNS configuration to emulate an existing load balancer IP address.

Prerequisites

Verify that the following static IP addresses are allocated.

- Static IP address for the Management Platform Services Controller
- Static IP address for the Platform Services Controller Load Balancer Virtual IP

Table 2-4. IP Addresses and Host Names for the Platform Services Controller Load Balancer and the Platform Services Controller for the Management Cluster

Component	Hostname	IP Address	Domain
Platform Services Controller Load Balancer	sfo01psc01	172.16.11.71	sfo01.rainpole.local
Platform Services Controller for the Management Cluster	sfo01m01psc01	172.16.11.61	sfo01.rainpole.local

Procedure

1 Log in to the **`dc01rpl.rainpole.local`** DNS server.

2 Open the Windows **Start** menu, in the **Search** bar, enter **`dnsmgmt.msc`**, and press Enter.

The **DNS Manager** dialogue box appears.

3 Create an **A Record** for the Platform Services Controller Load Balancer Name VIP.

a In the **DNS Manager** dialogue box, expand **Forward Lookup Zones**.

b Right click the **sfo01.rainpole.local** zone and select **New Host (A or AAAA)**.

c Enter the following values and click **Add Host**.

Setting	Value
Name	sfo01psc01
Fully qualified domain name (FQDN)	sfo01psc01.sfo01.rainpole.local
IP address	172.16.11.61
Create associate pointer (PTR) record	Deselected

Attention To create an operational network configuration for sfo01psc01.sfo01.rainpole.local , Cloud Builder requires forward lookup with IP 172.16.11.61 and reverse lookup with IP 172.16.11.71 (the load balancer VIP). Ensure that the A Record and the pointer (PTR) record are not associated and point to different IPs.

4 Create a pointer (PTR) record for the Platform Services Controller Load Balancer VIP and point it to the **A Record** of the Platform Services Controller Load Balancer VIP.

a Expand **Reverse Lookup Zones**.

b Right click the **11.16.172.in-addr.arpa** zone and select **New Pointer (PTR)**…

c Enter the following values and click **OK**.

Setting	Value
Host IP address	172.16.11.71
Fully qualified domain name (FQDN)	71.11.16.172.in-addr.arpa
Host name	sfo01psc01.sfo01.rainpole.local

Prerequisites for Operations Management Layer Implementation in Region A

To prepare the operations management layer for automated deployment of SDDC components using Cloud Builder, you deploy and configure a Linux virtual machine for vSphere Update Manager Download Service.

Deploy and Configure a Linux Virtual Machine for vSphere Update Manager Download Service in Region A

Before you deploy vSphere Update Manager Download Service with Cloud Builder, you deploy and configure a virtual machine with an Ubuntu Server operating system.

You create a virtual machine on the sfo01m01esx01.sfo01.rainpole.local host for vSphere Update Manager Download Service with the following virtual machine and network configuration requirements. Ensure that the virtual machine has access to the Internet.

Table 2-5. Virtual Machine Requirements for the vSphere Update Manager Download Service Linux VM

Setting	Value
ESXi Host	sfo01m01esx01
VM Name	sfo01umds01
Guest OS	Ubuntu Server 18.04 LTS
CPU	2
Memory	2 GB
Hard Disk	120 GB
SCSI Controller	LSI Logic SAS
Network Interface	VM Network
Network Adapter Type	VMXNET3
Datastore	sfo01-m01-bkp01

Table 2-6. Network Requirements for the vSphere Update Manager Download Service Linux VM

Setting	Value
Host Name	sfo01umds01
Static IPv4 Address	172.16.11.67
Default Gateway	172.16.11.253
Subnet Mask	255.255.255.0
DNS Server	172.16.11.5, 172.16.11.4
DNS Domain	sfo01.rainpole.local
DNS Search	sfo01.rainpole.local

Procedure

1 Deploy the vSphere Update Manager Download Service Linux VM with the specified configuration.

2 Log in to the vSphere host by using the VMware Host Client.

   a Open a Web browser and go to **`https://sfo01m01esx01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

3 In the **Navigator**, click **Virtual Machines**.

4 Select the **sfo01umds01** virtual machine, click the **Console** button, and select **Open browser console**.

5 Create the **svc-umds** service account for vSphere Update Manager Download Service by running the following command.

```
adduser svc-umds
```

   When prompted, enter the password, confirm it, and give the full name of the **svc-umds** user.

6 Assign administrative privileges to the **svc-umds** service account by running the following command.

```
usermod -aG sudo svc-umds
```

7 Install Secure Shell (SSH) server by running the following command.

```
sudo apt-get update
sudo apt-get -y install ssh
```

8 Verify the status of SSH service by running the following command.

```
service ssh status
```

9 Install Expect and Nginx packages for Ubuntu by running the following commands.

```
sudo apt-get install -y expect
sudo apt-get install -y nginx
```

Prerequisites for Cloud Management Layer Implementation in Region A

To prepare the cloud management layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure the Master Windows system for vRealize Automation Infrastructure as a Service (IaaS) nodes and deploy and configure the external SQL server for vRealize Automation.

Procedure

1 Deploy and Configure the Master Windows System for vRealize Automation IaaS Nodes in Region A

You deploy and configure a single Master Windows system virtual machine which is cloned and reconfigured during SDDC deployment to provision the vRealize Automation IaaS components - IaaS Web Servers, IaaS Manager Service Servers, IaaS DEM Servers, and IaaS Proxy Servers.

2 Deploy and Configure the External SQL Server for vRealize Automation in Region A

You deploy and configure a Windows-based virtual machine to host the SQL Server database required for the vRealize Automation IaaS components. After you install the SQL instance, you perform additional configuration to allow Cloud Builder to perform initial validation and deploy the necessary vRealize Automation components.

Deploy and Configure the Master Windows System for vRealize Automation IaaS Nodes in Region A

You deploy and configure a single Master Windows system virtual machine which is cloned and reconfigured during SDDC deployment to provision the vRealize Automation IaaS components - IaaS Web Servers, IaaS Manager Service Servers, IaaS DEM Servers, and IaaS Proxy Servers.

You create a virtual machine on the sfo01m01esx01.sfo01.rainpole.local host for the Master Windows system with the following virtual machine, software, and network configuration.

Table 2-7. Virtual Machine Requirements for the Master Windows System

Setting	Value
ESXi Host	sfo01m01esx01
VM Name	master-iaas-vm
Guest OS	Microsoft Windows Server 2016 (64-bit)
vCPU	2
Memory	8 GB
Virtual Disk	60 GB
SCSI Controller	LSI Logic SAS
Datastore	sfo01-m01-bkp01
Network Interface	VM Network
Network Adapter Type	1 x VMXNET3

Network Requirements:

- Verify that you have allocated a static or DHCP IP address for the Master Windows system.
- Verify the Master Windows system has access to the Internet.

Table 2-8. Software Requirements for the Master Windows System

Component	Requirement
Operating System	Windows Server 2016 (64-bit)
VMware Tools	Latest version
Active Directory	Join the virtual machine to the sfo01.rainpole.local domain.
Internet Explorer Enhanced Security Configuration	Turn off ESC.
Remote Desktop Protocol	Enable RDP access.
Java	■ Java Runtime Environment (JRE) executable jre-8u191-windows-x64 or later. ■ Set the *JAVA_HOME* environment variable to the Java installation directory. ■ Update the *PATH* system variable to include the `bin` folder of Java installation directory.
Secondary Logon Service	Start Secondary Logon service and set start-up type to Automatic.

Procedure

1 Deploy the Master Windows System for vRealize Automation with the specified configuration.

2 Log in to the vRealize Automation Master Windows virtual machine by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine.

   b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

3 Click **Start**, right-click **Windows PowerShell**, and select **More > Run as Administrator**.

4 Set the execution policy by running the following command.

```
Set-ExecutionPolicy Unrestricted
```

   When prompted, confirm the execution policy change.

5 Disable User Account Control (UAC) by running the following command.

```
set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"EnableLUA" -Value "0"
```

6 Disable IPv6 protocol.

```
set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\TCPIP6\Parameters" -Name
"DisabledComponents" -Value 0xff
```

7 Verify that the source path for Microsoft Windows Server is available.

   a Mount the Microsoft Windows Server ISO file on the Master Windows system virtual machine.

   b Create the `\sources\sxs` directory by running the following command in Windows PowerShell.

   ```
   mkdir C:\sources\sxs
   ```

   c Copy the Microsoft Windows Server source files from `sources\sxs` on the ISO file to the `C:\sources\sxs` directory on the virtual machine.

   d Update the registry with the full system path of the Microsoft Windows Server source files by running the following command in Windows PowerShell.

   ```
   New-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Servicing"
   ```

   ```
   set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Servicing\" -
   Name "LocalSourcePath" -value "c:\sources\sxs"
   ```

   e Unmount the Microsoft Windows Server ISO file.

8 Add the **svc-vra** service account to the Local Administrators group.

   a Click **Start**, right-click **Windows PowerShell**, and select **More > Run as Administrator**.

   b Run the following command.

   ```
   net localgroup administrators rainpole\svc-vra /add
   ```

9 Create the **svc-vra** user profile by logging in to the vRealize Automation Master Windows virtual machine.

   a Open an RDP connection to the virtual machine.

   b Log in using the following credentials.

Settings	Value
User ame	rainpole\svc-vra
Password	*svc-vra_password*

10 Shut down the Master Windows system virtual machine.

Deploy and Configure the External SQL Server for vRealize Automation in Region A

You deploy and configure a Windows-based virtual machine to host the SQL Server database required for the vRealize Automation IaaS components. After you install the SQL instance, you perform additional configuration to allow Cloud Builder to perform initial validation and deploy the necessary vRealize Automation components.

You create a virtual machine on the sfo01m01esx01.sfo01.rainpole.local host for the Microsoft SQL Server with the following virtual machine, software, and network configuration requirements.

Table 2-9. Virtual Machine Requirements for the External vRealize Automation SQL Server

Setting	Value
ESXi Host	sfo01m01esx01
VM Name	vra01mssql01
Guest OS	Microsoft Windows Server 2016 (64-bit)
vCPU	8
Memory (GB)	16
Hard Disk (GB)	200
SCSI Controller	LSI Logic SAS
Datastore	sfo01-m01-bkp01
Network Interface	VM Network
Network Adapter Type	1 x VMXNET3

Table 2-10. Network Requirements for the External vRealize Automation SQL Server

Setting	Value
Host Name	vra01mssql01
Static IPv4 Address	172.16.11.72
Subnet Mask	255.255.255.0
Default Gateway	172.16.11.253
DNS Server	172.16.11.5
FQDN	vra01mssql01.rainpole.local

Table 2-11. Software Requirements for the External vRealize Automation SQL Server

Component	Requirement
Operating System	Windows Server 2016 (64-bit)
VMware Tools	Latest version
SQL Server	SQL Server 2017 Standard or later (64-bit) Microsoft SQL Server Management Studio **Important** During the SQL Server installation, the Database Engine configuration wizard prompts you to provide the user name and password for the SQL Server administrator. If this user is not added during the SQL Server installation, select **SQL Authentication** from the **Authentication** drop-down menu, enter ***sa*** in the **User name** text box, and *sa_password* in the **Password** text box.
Active Directory	Join the virtual machine to the rainpole.local domain.
Remote Desktop Protocol	Enable RDP access.

Procedure

1 Deploy the the External vRealize Automation SQL Server VM with the specified configuration.

2 Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the **`vra01mssql01.rainpole.local`** virtual machine.

   b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

3 Enable Microsoft Distributed Transaction Coordinator (MSDTC).

   a Click the Windows **Start** button, type **`comexp.msc`**, and press Enter.

   The **Component Services** window opens.

   b In the **Console Root** on the left pane, navigate to **Component Services > Computers > My Computer > Distributed Transaction Coordinator**.

   c Right click **Local DTC** and select **Properties**.

   d In the **Local DTC Properties** dialog box, click the **Security** tab, configure the following values, and click **OK**.

Setting	Value
Network DTC Access	Selected
Allow Remote Clients	Selected
Allow Inbound	Selected
Allow Outbound	Selected

   e In **MSDTC Service** dialog box, select **Yes** to restart the MSDTC service.

4 Create the vRealize Automation account in the SQL Server instance.

   a Click the Windows **Start** button and open Microsoft SQL Server Management Studio.

   b In the **Connect to Server** dialog box, leave the default value for the **Server Name** text box, from the drop-down menu select **Windows Authentication**, and click **Connect**.

   c In the **Object Explorer** tree, expand the **VRA01MSSQL01** server instance, right click the**Security** folder, and select **New > Login**.

   d In the **Login** dialog box, under **General**, enter **`rainpole\svc-vra`** in the **Login name** text box.

   e On the **Server Roles** page, select **sysadmin** and click **OK**.

5 Create the new vRealize Automation database.

a Click the Windows **Start** button and open Microsoft SQL Server Management Studio.

b Right click the **Databases** folder and select **New Database**.

The **New Database** wizard appears.

c In the **General** page, enter **VRADB01** for **Database name** and **rainpole\svc-vra** for **Owner**.

d On the **Options**page, configure the following recovery model settings, and click **OK**.

Setting	Value
Recovery model	Simple
Compatibility level	SQL Server 2014 (120)
Other options > Miscellaneous > Allow Snapshot Isolation	True
Other options > Miscellaneous > Is Read Committed Snapshot On	True

6 Allow access to Microsoft SQL Server on TCP port 1433.

a Click the Windows **Start** button, type **WF.msc**, and press Enter.

The **Windows Firewall with Advanced Security** window appears.

b In the navigation pane, right click **Inbound Rules** and select **New Rule**.

The **New Inbound Rule Wizard** appears.

c On the **Rule Type** page, select the **Port** radio button, and click **Next**.

d On the **Protocol and Ports** page, select **TCP**, enter the port number **1433** in the **Specific local ports** text box, and click **Next**.

e On the **Action** page, select **Allow the connection**, and click **Next**.

f On the **Profile** page, select the **Domain**,**Private**, and **Public** profiles, and click **Next**.

g On the **Name** page, enter **Microsoft SQL Server Port (1433)** and click **Finish**.

7 Allow access for Microsoft Distributed Transaction Coordinator.

a Click the Windows **Start** button, type **WF.msc** and press Enter.

The **Windows Firewall with Advanced Security** window appears.

b In the navigation pane, select **Inbound Rules > New RuleInbound Rules**.

The **New Inbound Rule Wizard** appears.

c On the **Rule Type** page, select the **Predefined** radio button, select**Distributed Transaction Coordinator**, and click **Next**.

d On the **Predefined Rules** page, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, **Distributed Transaction Coordinator (TCP-In)**, and click **Next**.

e On the **Action** page, select **Allow the connection**, and click **Finish**.

8 Unmount any ISO files mounted to the virtual machine.

Prerequisites for Business Continuity Layer Implementation in Region A

To prepare the business continuity layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure the Site Recovery Manager Windows virtual machine.

Deploy and Configure the Windows Virtual Machine for Site Recovery Manager in Region A

You deploy and configure a Windows-based virtual machine to create the necessary infrastructure to facilitate deployment of Site Recovery Manager with VMware Cloud Builder. This virtual machine must meet specific configuration and software requirements.

You create a virtual machine on the sfo01m01esx01.sfo01.rainpole.local host for Site Recovery Manager with the following virtual machine, software, and network configuration.

Table 2-12. Virtual Machine Requirements for Site Recovery Manager VM

Setting	Value
ESXi Host	sfo01m01esx01
VM Name	sfo01m01srm01
Guest OS	Windows Server 2016 (64-bit)
vCPU	2
Memory	2 GB
Virtual Disk	40 GB
SCSI Controller	LSI Logic SAS
Datastore	sfo01-m01-bkp01
Network Interface	VM Network
Network Adapter Type	1 x VMXNET3

Table 2-13. Network Requirements for Site Recovery Manager VM

Setting	Value
Host Name	sfo01m01srm01
Static IPv4 Address	172.16.11.124
Subnet Mask	255.255.255.0
Default Gateway	172.16.11.253

Table 2-13. Network Requirements for Site Recovery Manager VM (Continued)

Setting	Value
DNS Server	172.16.11.5
FQDN	sfo01m01srm01.sfo01.rainpole.local
Open Ports	■ 9086 ■ 5678

Table 2-14. Software Requirements for the Site Recovery Manager VM

Setting	Value
Operating System	Windows Server 2016 (64-bit)
VMware Tools	Latest version.
Active Directory	Join the virtual machine to the sfo01.rainpole.local domain.
License	Verify that you have obtained a VMware Site Recovery Manager license that satisfies the requirements of this design.
Internet Explorer Enhanced Security Configuration	Turn off ESC.
Remote Desktop Protocol	Enable RDP access.

Procedure

1 Deploy the Site Recovery Manager virtual machine with the specified configuration.

2 Log in to the Site Recovery Manager virtual machine by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the sfo01m01srm01 virtual machine.

   b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

3 Click **Start**, right-click **Windows PowerShell**, and select **More > Run as Administrator**.

4 Add the **svc-srm** service account to the local Administrators group by running the following command.

```
net localgroup administrators rainpole\svc-srm /add
```

5 Configure NTP settings.

a Enable Windows Time Service and start by running the following commands.

```
w32tm /config /manualpeerlist:“ntp.sfo01.rainpole.local
ntp.lax01.rainpole.local” /syncfromflags:manual /reliable:YES /update
```

b Restart the Windows Time Service by running the following command.

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

c Verify the time synchronization configuration by running the following command.

```
w32tm /query /status
```

Generate Certificates for the SDDC Components in Region A

To ensure secure and operational connectivity between the SDDC components, you generate new signed certificates for the SDDC components in Region A.

You use the Certificate Generation Utility for VMware Validated Design (`CertGenVVD`) to generate the certificate configuration files based on the deployment specification configured in the Deployment Parameters XLS file in Region A. You then generate new certificates signed by the Microsoft certificate authority (MSCA) for all management products.

You later upload the newly generated and signed certificates to VMware Cloud Builder as part of the deployment and configuration procedure of the virtual appliance.

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

Procedure

1 Prerequisites for Generating Signed Certificates for the SDDC Components in Region A

Before you generate MSCA signed certificates for the SDDC components, verify that your environment fulfills the requirements for this process.

2 Create and Add a Microsoft Certificate Authority Template in Region A

You first set up a Microsoft Certificate Authority template on the Active Directory (AD) servers for the region. The template contains the certificate authority (CA) attributes for signing certificates for the SDDC components. After you create the template, you add it to the certificate templates of the Microsoft CA.

3 Generate Signed Certificates for the SDDC Components in Region A

Use the Certificate Generation Utility for VMware Validated Design (`CertGenVVD`) to generate new signed certificates for the SDDC components.

Prerequisites for Generating Signed Certificates for the SDDC Components in Region A

Before you generate MSCA signed certificates for the SDDC components, verify that your environment fulfills the requirements for this process.

This VMware Validated Design sets the Certificate Authority service on the Active Directory (AD) dc01rpl.rainpole.local (root CA) server. Verify that your environment satisfies the following prerequisites generating signed certificates for the components of the SDDC.

Certificate Generation Prerequisites

Prerequisite	Value
Active Directory	■ Verify that the Certificate Authority Service role and the Certificate Authority Web Enrollment role are installed and configured on the Active Directory Server. ■ Verify that a new Microsoft Certificate Authority template is created and enabled. ■ Use a hashing algorithm of SHA-256 or higher on the certificate authority. ■ Verify that relevant firewall ports relating to the Microsoft Certificate Authority and related services are open.
Windows Host	■ Ensure the Windows host system where you connect to the data center and generate the certificates is joined to the domain of the Microsoft Certificate Authority. ■ Install Java Runtime Environment version 1.8 or later. ■ Configure the *JAVA_HOME* environment variable to the Java installation directory. ■ Update the *PATH* system variable to include the `bin` folder of Java installation directory. ■ Install OpenSSL toolkit version 1.0.2 for Windows. ■ Update the *PATH* system variable to include the `bin` folder of the OpenSSL installation directory.
Software Features	■ Fill in the Deployment Parameters XLS file in Region A. See Deployment Specification in the *VMware Validated Design Planning and Preparation for Consolidated SDDC* documentation.
Installation Packages	■ Download the `CertGenVVD-`*`version`*`.zip` file of the Certificate Generation Utility from VMware Knowledge Base article 2146215 and extract the ZIP file to the `C:` drive.

Create and Add a Microsoft Certificate Authority Template in Region A

You first set up a Microsoft Certificate Authority template on the Active Directory (AD) servers for the region. The template contains the certificate authority (CA) attributes for signing certificates for the SDDC components. After you create the template, you add it to the certificate templates of the Microsoft CA.

Procedure

1 Log in to the Active Directory server using a Remote Desktop Protocol (RDP) client.

   a Log in using the following credentials.

Setting	Value
User	Active Directory administrator
Password	*ad_admin_password*

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

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

4 In the **Duplicate Template** dialog box, leave **Windows Server 2003 Enterprise** selected for backward compatibility and click **OK**.

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

6 In the **Template display name** text box, enter **`VMware`**.

7 Click the **Extensions** tab and configure the following.

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

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

   c If the **Client Authentication** policy is present, select it, click **Remove**, and click **OK**.

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

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

   f Leave the default for all other options.

   g Click **OK**.

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

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

   a Click **Start > Run**, enter **`certsrv.msc`**, and click **OK**

   b In the **Certification Authority** window, expand the left pane, right-click **Certificate Templates**, and select **New > Certificate Template to Issue**.

   c In the **Enable Certificate Templates** dialog box, select **VMware**, and click **OK**.

Generate Signed Certificates for the SDDC Components in Region A

Use the Certificate Generation Utility for VMware Validated Design (`CertGenVVD`) to generate new signed certificates for the SDDC components.

Procedure

1. Log in to the Windows host that has access to your data center.
2. Set the execution policy to Unrestricted.
   a. Click **Start**, right click **Windows PowerShell**, and select **More > Run as Administrator**.
   b. Set the execution policy by running the following command.

      ```
      Set-ExecutionPolicy Unrestricted
      ```

   c. Enter **Y** to confirm the execution policy change.
3. Use the `CertConfig` utility to generate the certificate configuration files.
   a. Open the populated Deployment Parameters XLS file and select the **CertConfig** worksheet.
   b. From the **File** menu, select **Save As…**, set the file format to **Comma delimited (*.csv)**, rename the file to **`SDDC-CertConfig.csv`**, and click **Save**.
   c. Rename the `C:\CertGenVVD-`*`version`*`\ConfigFiles` folder to `ConfigFiles.Old`.
   d. Create a new `C:\CertGenVVD-`*`version`*`\ConfigFiles` folder.
   e. In the Windows PowerShell terminal, navigate to the `C:\CertGenVVD-`*`version`* folder and run the following command.

      ```
      .\Certconfig-version.ps1 SDDC-Certconfig.csv
      ```

f Follow the on-screen instructions and set the following values.

Setting	Value
Default Organization	Rainpole Inc
Default OU	Rainpole
Default Location	SFO
Default State	CA
Default Country	US
Default Key Size	2048

g Verify that the `C:\CertGenVVD-version\ConfigFiles` folder is populated with the necessary certificate configuration files.

- sfo01psc01.txt
- sfo01m01vc01.txt
- sfo01w01vc01.txt
- sfo01m01nsx01.txt
- sfo01w01nsx01.txt
- vrops01svr01.txt
- vra01svr01.txt
- vrb01svr01.txt
- sfo01vrli01.txt
- sfo01m01srm01.txt
- sfo01m01vrs01.txt
- vrs01lcm01.txt

4 In the Windows PowerShell terminal, navigate to the `C:\CertGenVVD-version` folder and validate the configuration by running the following command.

```
.\CertGenVVD-version.ps1 -validate
```

The local machine configuration is validated successfully.

5 Use the `CertGenVVD` utility to generate the signed certificate files.

   a In the Windows PowerShell terminal, navigate to the `C:\CertGenVVD-version` folder and generate the signed certificates by running the following command.

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

   b Follow the on-screen instruction and enter a passphrase for PEM/P12 file encryption.

   All MSCA signed certificates are generated in the `C:\CertGenVVD-version\SignedByMSCACerts` folder.

6 Rename the `C:\CertGenVVD-version\SignedByMSCACerts` folder to `SignedByMSCACerts-sfo-jd`.

7 Copy the `vra01svr01`, `vrb01svr01`, and `vrs01lcm01` folder and their content to a location that you can access during the deployment of Region B.

VMware Cloud Builder Implementation in Region A

3

You deploy and configure the VMware Cloud Builder virtual appliance to start the automated implementation of the SDDC components.

You deploy dedicated VMware Cloud Builder virtual appliances for both Region A and Region B. You use each region's dedicated virtual appliance to deploy the SDDC components.

Procedure

1 Prerequisites for VMware Cloud Builder Implementation in Region A

Before you deploy the virtual appliance of VMware Cloud Builder, verify that your environment fulfills the requirements for this deployment.

2 Deploy the Virtual Appliance of VMware Cloud Builder on a ManagementHost in Region A

You deploy the virtual appliance of VMware Cloud Builder in Region A and configure the appliance to start the automated implementation of the SDDC components for the region.

Prerequisites for VMware Cloud Builder Implementation in Region A

Before you deploy the virtual appliance of VMware Cloud Builder, verify that your environment fulfills the requirements for this deployment.

IP Addresses and Host Names

Verify that the static IP address and FQDN for the VMware Cloud Builder virtual appliance are available.

Setting	Value
IP address	172.16.11.60
Host name	sfo01cb01
Default gateway	172.16.11.253
DNS servers	■ 172.16.11.5 ■ 172.16.11.4
DNS domain	sfo01.rainpole.local
DNS search	sfo01.rainpole.local,rainpole.local

Setting	Value
Subnet mask	255.255.255.0
NTP servers	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for the deployment of the virtual appliance of VMware Cloud Builder.

Prerequisite	Value
Environment	■ Verify that your environment is configured for deployment of VMware Cloud Builder and of the SDDC. See Chapter 2 Prepare the Environment for Automated Deployment in Region A.
Storage	■ Virtual disk provisioning: ■ Thin ■ Required storage: 28 GB
Installation Packages	■ Download the `.ova` file for VMware Cloud Builder.

Deploy the Virtual Appliance of VMware Cloud Builder on a Management Host in Region A

You deploy the virtual appliance of VMware Cloud Builder in Region A and configure the appliance to start the automated implementation of the SDDC components for the region.

Procedure

1 Log in to the vSphere host by using the VMware Host Client.

  a Open a Web browser and go to **`https://sfo01m01esx01.sfo01.rainpole.local`**.

  b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 In the **Navigator**, select **Host** and click the **Create / Register VM** button.

  The **New virtual machine** wizard appears.

3 On the **Select creation type** dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

4 On the **Select OVF and VMDK files** dialog box, enter **`sfo01cb01`** for the virtual machine name, select the VMware Cloud Builder `.ova` file, and click **Next**.

5 In the **Select storage** dialog box, select **sfo01-m01-bkp01**, and click **Next**.

6 On the **License agreements** page, click **I agree** to accept the license agreement, and click **Next**.

7 On the **Deployment options** page, enter the following values and click **Next**.

Setting	Value
Network mappings	VM network
Disk provisioning	Thin
Power on automatically	Selected

8 In the **Additional settings** dialog box, expand **Application** ,enter the following values, and click **Next**.

Option	Value
Root password	*sfo01cb01_root_password* Note : The passwords must be at least 8 characters, must contain uppercase, lowercase, digits, and special characters.
Confirm root password	*sfo01cb01_root_password*
Admin username	admin
Admin password	*sfo01cb01_admin_password*
Confirm admin password	*sfo01cb01_admin_password*
Network 1 IP address	172.16.11.60
Network 1 Subnet mask	255.255.255.0
Default Gateway	172.16.11.253
Enter VM hostname	sfo01cb01
Domain name	sfo01.rainpole.local
Domain search path	sfo01.rainpole.local,rainpole.local
DNS	172.16.11.5,172.16.11.4
NTP	ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local

9 On the **Ready to complete** dialog box, review the virtual machine configuration and click **Finish**.

Deploy the Software-Defined Data Center Components in Region A

4

After you deploy and configure the VMware Cloud Builder appliance, you generate the JSON deployment files based on the values populated in the Deployment Parameters XLS file. You then validate the necessary run parameters and start the automated deployment of the SDDC components for the management cluster and for the shared edge and compute cluster in Region A.

Procedure

1 Prerequisites for Automated SDDC Deployment in Region A

Before you start the automated SDDC deployment, verify that your environment fulfills the requirements for this deployment.

2 Upload the VMware Validated Design Software Bundle and Signed Certificates to VMware Cloud Builderin Region A

After you deploy the Cloud Builder virtual appliance, you prepare for an automated deployment of the SDDC components by uploading the software bundle and the generated signed certificates. You then mount the software bundle and configuring application properties.

3 Generate the JSON Deployment Files for the Management and the Shared Edge and Compute Clusters in Region A

After you have populated all required configuration values in the Deployment Parameters XLS file, you upload it to the VMware Cloud Builder appliance and generate the JSON files that automate the deployment of the SDDC components in the management and the shared edge and compute clusters.

4 Validate the Deployment Parameters and Target Environment Prerequisites for the Management Cluster and the Shared Edge and Compute Cluster in Region A

You perform validation of both JSON deployment files and specific target environment prerequisites to ensure that you can successfully deploy the components of the management and the shared edge and compute clusters using VMware Cloud Builder.

5 Start the Automated Deployment of the Management Cluster in Region A

After you successfully validate the `vvd-std-rega-mgmt.json` file, you start the automated deployment of the components in the management cluster.

6 Start the Automated Deployment for the Shared Edge and Compute Clusterin Region A

After you have successfully validated the `vvd-std-rega-comp.json` file and deployed the management cluster, you start the automated deployment of the components in the shared edge and compute cluster.

Prerequisites for Automated SDDC Deployment in Region A

Before you start the automated SDDC deployment, verify that your environment fulfills the requirements for this deployment.

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for the automated SDDC deployment.

Prerequisite	Value
Environment	■ Verify that your environment is configured for deployment of the SDDC. See Chapter 2 Prepare the Environment for Automated Deployment in Region A.
Physical Network	■ Verify that your environment meets all physical network requirements, all host names and IP addresses are allocated for external services and SDDC components.
Active Directory	■ Verify that Active Directory is configured with all child domains, all service accounts and groups are created and configured.
DNS	■ Verify that DNS entries are configured for the root and child domains.
NTP Services	■ Verify that two external to the SDDC NTP servers are configured and time synchronization is configured on all ESXi hosts and AD domain controllers.

Storage	■ Primary vSAN storage:
	  ■ Verify that the necessary primary storage capacity is allocated. See Deployment Parameters XLS file for Region A for automatic capacity calculation.
	■ Secondary NFS storage:
	  ■ Verify that NFS storage is mounted.
	  ■ Verify that you have allocated the necessary storage capacity. See Datastore Requirements in the *VMware Validated Design Planning and Preparation* documentation.

Software Features	■ Fill in the Deployment Parameters XLS file for Region A. See Deployment Specification in the *VMware Validated Design Planning and Preparation* documentation. ■ Verify that you have generated CA-signed certificates for the management components of the SDDC. See Generate Signed Certificates for the SDDC Components in Region A.
Installation Packages	■ Download the `.iso` file for the software bundle for VMware Validated Design to your local file system.

For additional information, see the VMware Validated Design Planning and Preparation documentation.

Upload the VMware Validated Design Software Bundle and Signed Certificates to VMware Cloud Builderin Region A

After you deploy the Cloud Builder virtual appliance, you prepare for an automated deployment of the SDDC components by uploading the software bundle and the generated signed certificates. You then mount the software bundle and configuring application properties.

Procedure

1 Log in to the VMware Cloud Builder virtual appliance.

   a Open a connection to **sfo01cb01.sfo01.rainpole.local** using an Secure Copy Protocol software like WinSCP.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2 Upload the VMware Validated Design software bundle file `vvd-bundle-johndory-x.x.x-xxxxxxx.iso` to the `/mnt/hgfs` directory on the Cloud Builder appliance.

3 Upload all folders and their content from the `CertGenVVD` folder `C:\CertGenVVD-version\SignedByMSCACerts-sfo-jd` to the `/opt/vmware/vvd/certificates` directory on the Cloud Builder appliance.

4 Configure the Cloud Builder appliance and mount the VMware Validated Design software bundle `.iso` file.

   a Open an SSH connection to sfo01cb01.sfo01.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

   c Switch to the **root** user by running the `su` command.

   d Mount the VMware Validated Design software bundle `.iso` file and configure application properties by running the following command.

```
/opt/vmware/vvd/cloud-builder/install/reconfigure.sh
```

   The script sets the full system path to each application's installation file, configures specific application properties, and restarts the bring-up service.

Generate the JSON Deployment Files for the Management and the Shared Edge and Compute Clusters in Region A

After you have populated all required configuration values in the Deployment Parameters XLS file, you upload it to the VMware Cloud Builder appliance and generate the JSON files that automate the deployment of the SDDC components in the management and the shared edge and compute clusters.

Procedure

1 Log in to VMware Cloud Builder.

   a Open a Web browser and go to **`https://sfo01cb01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2 On the **End User License Agreement** page, click **Accept License Agreement**.

3 Generate the JSON files used for automated deployment of the SDDC components.

   a In the Cloud Builder**Navigator**, select the **Deployment Wizard** icon.

   b In the **Upload Config File** tab, from the **Select Architecture Type** drop-down menu, select the **VVD for SDDC Region A** architecture and click the **Upload Config File** button.

   c Navigate to the Deployment Parameters XLS file and click **Open**.

   d Click the **Generate JSON** button.

   Cloud Builder generates one JSON file for the management cluster and one JSON file for the shared edge and compute cluster.

Table 4-1. Region A JSON Deployment Files

Architecture Type	JSON Filename	Workload Domain	Deployment Order
VVD for SDDC Region A	`vvd-std-rega-mgmt.json`	Management	1
	`vvd-std-rega-comp.json`	Compute	2

4 Monitor the process and check the following log files for errors.

Table 4-2. VMware Cloud Builder JSON Generator Log File Location

Cloud Builder Component	Location
JSON Generator	`/opt/vmware/sddc-support/cloud_admin_tools/logs/JsonGenerator.log`

What to do next

After the JSON files for Region A are generated, you validate their content for configuration, application, and bring-up readiness, and perform validation of the target platform.

Validate the Deployment Parameters and Target Environment Prerequisites for the Management Cluster and the Shared Edge and Compute Cluster in Region A

You perform validation of both JSON deployment files and specific target environment prerequisites to ensure that you can successfully deploy the components of the management and the shared edge and compute clusters using VMware Cloud Builder.

You validate the JSON deployment files `vvd-std-rega-mgmt.json` for the management cluster and `vvd-std-rega-comp.json` for the shared edge and compute cluster. In case any of the tests fail, you must remediate any errors and perform the validation process again. Additional information can be found in the audit log file.

Table 4-3. VMware Cloud Builder Platform Audit Log File Location

Cloud Builder Component	Location
Platform Audit	`/opt/vmware/sddc-support/cloud_admin_tools/logs/PlatformAudit.log`

Procedure

1. Log in to VMware Cloud Builder.
   a. Open a Web browser and go to **`https://sfo01cb01.sfo01.rainpole.local`**.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2. In the Cloud Builder**Navigator**, click the **Deployment Wizard** icon.
3. Select the Validate Environment tab.
4. From the **Select File to Validate** drop-down menu, select the `vvd-std-rega-mgmt.json` file and click **Validate**.

5 If validation fails because of issues with the signed certificate files, resolve the issues and reupload the modified certificate files.

   a Upload the modified certificate files to the Cloud Builder appliance using an SCP software like WinSCP.

   b Open an SSH connection to sfo01cb01.sfo01.rainpole.local.

   c Run the following command.

   ```
   su /opt/vmware/vvd/cloud-builder/install/reconfigure.sh
   ```

   When prompted, enter the *cloudbuilder_root_password*.

6 If validation fails with an `user input errors` message, remediate the Deployment Parameters XLS file.

7 In the **Upload Config File** tab, from the **Select Architecture Type** drop-down menu, select the **VVD for SDDC Region A** architecture and click the **Upload Config File** button.

8 Navigate to the updated Deployment Parameters XLS file and click **Open**.

9 On the **Overwrite Existing JSON File(s)dialog box**, select **Yes**.

10 Select the **Validate Environment tab**, from the **Select File to Validate** drop-down menu, select the `vvd-std-rega-mgmt.json` file and click **Validate**.

   The `vvd-std-rega-mgmt.json` file is successfully validated against the predefined run parameters.

11 Click the **Back** button, from the **Select File to Validate** drop-down menu, select the `vvd-std-rega-comp.json` file and click **Validate**

   The `vvd-std-rega-comp.json` file is successfully validated against the predefined run parameters.

What to do next

After successful validation of `vvd-std-rega-mgmt.json` and `vvd-std-rega-comp.json` files, click **Next** to start the deployment of the management cluster.

Start the Automated Deployment of the Management Cluster in Region A

After you successfully validate the `vvd-std-rega-mgmt.json` file, you start the automated deployment of the components in the management cluster.

Procedure

1 Log in to VMware Cloud Builder.

a Open a Web browser and go to **`https://sfo01cb01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2 In the Cloud Builder **Navigator**, select the **Deployment Wizard** icon.

3 Select the **Deploy an SDDC** tab.

4 From the **Select Deployment File** drop-down menu, select the `vvd-std-rega-mgmt.json` file and click **Deploy**.

The automated deployment of the components in the management cluster starts.

5 Monitor the deployment and check the following log files for errors.

Table 4-4. VMware Cloud Builder Bring Up Service Log File Location

Cloud Builder Component	Location
Bring Up Service	`/opt/vmware/bringup/logs/vcf-bringup.log`
	`/opt/vmware/bringup/logs/vcf-bringup-debug.log`

Start the Automated Deployment for the Shared Edge and Compute Clusterin Region A

After you have successfully validated the `vvd-std-rega-comp.json` file and deployed the management cluster, you start the automated deployment of the components in the shared edge and compute cluster.

Procedure

1 Log in to VMware Cloud Builder.

a Open a Web browser and go to **`https://sfo01cb01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2 In the Cloud Builder**Navigator**, select the **Deployment Wizard** icon.

3 Select the **Deploy an SDDCtab**.

4 From the **Select Deployment File** drop-down menu, select the `vvd-std-rega-comp.json` file and click **Deploy**.

   The automated deployment of the components in the shared edge and compute cluster starts.

5 Monitor the deployment and check the following log files for errors.

Table 4-5. VMware Cloud Builder Bring Up Service Log File Location

Cloud Builder Component	Location
Bring Up Service	`/opt/vmware/bringup/logs/vcf-bringup.log`
	`/opt/vmware/bringup/logs/vcf-bringup-debug.log`

Post-Deployment Virtual Infrastructure Configuration in Region A

5

After a successful deployment using VMware Cloud Builder, perform post-deployment tasks to finish the SDDC configuration in Region A. For the virtual infrastructure layer, update the host profiles, configure the distributed firewall for traffic from the management applications and update the DNS records for the Platform Services Controller Load Balancer.

Procedure

1 Update the Host Profile for the Management Cluster in Region A

   Cloud Builder configures the VMkernels of the ESXi hosts and adds them to the domain. You update the user name and password in the customizations for the hosts to be compliant as the host profile does not contain credentials information.

2 Distributed Firewall Configuration for Management Applications in Region A

   To increase the security level of your environment by allowing only the network traffic that the SDDC requires, you configure a distributed firewall. The explicit firewall rules you define allow access to management applications.

3 Update the Host Profile for the Shared Edge and Compute Cluster in Region A

   Update the user name and password in the customizations for the hosts in the shared edge and computecluster to be compliant as the host profile does not contain credentials information.

4 Update DNS Records for the Platform Services Controller Load Balancer in Region A

   After setting up load balancing, you modify the DNS address of the Platform Services Controller load balancer in Region A.

Update the Host Profile for the Management Cluster in Region A

Cloud Builder configures the VMkernels of the ESXi hosts and adds them to the domain. You update the user name and password in the customizations for the hosts to be compliant as the host profile does not contain credentials information.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Update the sfo01-m01hp-mgmt01 host profile.

   a From the **Home** menu, select **Policies and Profiles** and click **Host Profiles**.

   b Right-click **sfo01-m01hp-mgmt01**, and select **Copy Settings from Host**.

   c Select **sfo01m01esx01.sfo01.rainpole.local**, and click **OK**.

3 Edit the sfo01-m01hp-mgmt01 host profile customizations.

   a From the **Home** menu, select **Policies and Profiles** and click **Host Profiles**.

   b Right-click **sfo01-m01hp-mgmt01**, and select **Edit Host Customizations**.

   The **Edit Host Customizations** wizard appears.

   c Under **Select Hosts**, select all hosts and click **Next**.

   d Under **Edit Host Customizations**, update the following values for **User Name** and **Password**.

ESXi Host	Active Directory Configuration user name	Active Directory Configuration Password
sfo01m01esx01.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01m01esx02.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01m01esx03.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01m01esx04.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*

   e Click **Finish**.

4 Verify compliance and remediate the hosts.

   a On the **Host Profiles** page, click **sfo01-m01hp-mgmt01** and click the **Monitor** tab.

   b Click **Compliance**, click **Actions**, and select **Check Host Profile Compliance**.

   On the **Host profile** page, the **Host Profile Compliance** column shows sfo01m01esx01.sfo01.rainpole.local as `Compliant`, and the other hosts as `Not Compliant`.

   c Select each of the non-compliant hosts and click **Remediate**.

d In the **Remediate** dialog box, select **Automatically reboot hosts that require remediation**.

e Click **OK**.

All hosts show as `Compliant`.

Distributed Firewall Configuration for Management Applications in Region A

To increase the security level of your environment by allowing only the network traffic that the SDDC requires, you configure a distributed firewall. The explicit firewall rules you define allow access to management applications.

Procedure

1 Add vCenter Server Instances to the NSX Distributed Firewall Exclusion List in Region A

To ensure that network access between vCenter Server and NSX is not blocked, you exclude vCenter Server from all the distributed firewall rules.

2 Create IP Sets for Components of the Management Cluster in Region A

Create IP sets for all management applications . You use the IP sets later to create security groups for use with the distributed firewall rules.

3 Create Security Groups in Region A

Create security groups for use in configuring firewall rules for the groups of applications in the SDDC.

4 Create Distributed Firewall Rules in Region A

You create firewall rules to allow administrators to connect to the various VMware solutions, to allow for user access to the vRealize Automation portal, and to provide the external connectivity to the SDDC.

Add vCenter Server Instances to the NSX Distributed Firewall Exclusion List in Region A

To ensure that network access between vCenter Server and NSX is not blocked, you exclude vCenter Server from all the distributed firewall rules.

You configure the NSX distributed firewall by using a vCenter Server. If a rule prevents access between NSX Manager and vCenter Server, you are not able to manage the distributed firewall. You must exclude vCenter Server from all the distributed firewall rules and ensure that access between the two products is not blocked.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Exclude vCenter Server instances from the distributed firewall rules.

   a From the **Home** menu, select **Networking & Security**.

   b In the **Navigator** pane, click **Firewall Settings** and click the **Exclusion List** tab.

   c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

   d Click the **Add** button.

   The **Select VM(s) to exclude** dialog box appears.

   e Select **sfo01m01vc01**, add it to the **Selected Objects** list, and click **OK**.

Create IP Sets for Components of the Management Cluster in Region A

Create IP sets for all management applications . You use the IP sets later to create security groups for use with the distributed firewall rules.

You perform this procedure multiple times to configure all the necessary IP sets. For applications that are load balanced, include their VIP in the IP set.

Table 5-1. IP Sets for the Management Components

Name	IP Addresses
Platform Services Controller Instances	*Platform-Service-Controller_IP's*
vCenter Server Instances	*vCenter-Server_IP's*
vRealize Automation Appliances	*vRealize-Automation-Appliances_IP's*
vRealize Automation Windows	*vRealize-Automation-Windows _IP's*
vRealize Automation Proxy Agents	*vRealize-Automation-Proxy-Agents-IP's*
vRealize Business Server	*vRealize-Business_IP's*
vRealize Business Data Collector	*vRealize-Business-Data-Collector_IP*'s
VMware VADP Solution	*vStorage-API for Data-Protection-Solution_IP's*
vRealize Operations Manager	*vRealize-Operations-Manager_IP's*
vRealize Operations Manager Remote Collectors	*vRealize-Operations-Manager-Remote-Collectors_IP's*
vRealize Log Insight	*vRealize-Log-Insight_IP's*

Table 5-1. IP Sets for the Management Components (Continued)

Name	IP Addresses
vRealize Suite Lifecycle Manager	*vRealize-Suite-Lifecycle-Manager_IP's*
Site Recovery Manager	*Site-Recovery-Manger_IP's*
vSphere Replication	*vSphere-Replication_IP's*
Update Manager Download Service	*UMDS_IP's*
SDDC	*Management-VLAN_Subnets, Management-VXLAN_Subnets*
Administrators	*Administrators_Subnet*

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Create an IP set.

   a From the **Home** menu, select **Networking & Security**.

   b In the Navigator pane, click **Groups and Tags**, and click the **IP Sets** tab.

   c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

   d Click **Add**.

   e In the **New IP Set** dialog box, configure the values for the IP set that you are adding, and click **Add**.

Setting	Value
Name	vCenter Server Instances
IP Addresses	172.16.11.62 172.16.11.64
Universal Synchronization	On

3 Repeat the previous step to create IP sets for all remaining components.

Create Security Groups in Region A

Create security groups for use in configuring firewall rules for the groups of applications in the SDDC.

A security group is a collection of assets (or objects) from your vSphere inventory that you group. You perform this procedure multiple times to configure all the necessary security groups. In addition, you create the VMware Appliances and Windows Servers groups from the security groups you add in the previous repetitions of this procedure.

Table 5-2. Security Groups for the Management Clusters Components in the SDDC

Name	Object Type	Selected Object
Platform Services Controller Instances	IP Sets	Platform Services Controller Instances
vCenter Server Instances	IP Sets	vCenter Server Instances
vRealize Automation Appliances	IP Sets	vRealize Automation Appliances
vRealize Automation Windows	IP Sets	vRealize Automation Windows
vRealize Business Server	IP Sets	vRealize Business Server
vRealize Automation Proxy Agents	IP Sets	vRealize Automation Proxy Agents
vRealize Business Data Collector	IP Sets	vRealize Business Data Collector
VMware Storage API for VADP Solution	IP Sets	VMware VADP
vRealize Operations Manager	IP Sets	vRealize Operations Manager
vRealize Operations Manager Remote Collectors	IP Sets	vRealize Operations Manager Remote Collectors
vRealize Suite Lifecycle Manager	IP Sets	vRealize Suite Lifecycle Manager
Site Recovery Manager	IP Sets	Site Recovery Manager
vSphere Replication	IP Sets	vSphere Replication
vRealize Log Insight	IP Sets	vRealize Log Insight
Update Manager Download Service	IP Sets	Update Manager Download Service
SDDC	IP Sets	SDDC
Administrators	IP Sets	Administrators
Windows Servers	Security Groups	■ Site Recovery Manger ■ vRealize Automation Windows ■ vRealize Automation Proxy Agents
VMware Appliances	Security Groups	■ Platform Services Controller Instances ■ vCenter Server Instances ■ vSphere Replication ■ vRealize Automation Appliances ■ vRealize Business Server ■ vRealize Business Data Collector ■ VMware vStorage API for Data Protection Solution ■ vRealize Operations Manager ■ vRealize Operations Manager Remote Collectors ■ vRealize Suite Lifecycle Manager ■ vRealize Log Insight

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Networking & Security** and click **Groups and Tags**.

3 Click the **Security Groups** tab and select the **172.16.11.65** from the **NSX Manager** drop-down menu.

4 Click **Add**.

   The **Create Security Group** wizard appears.

5 On the **Name and Description** page, enter the following settings and click **Next**.

Setting	Value
Name	**`Platform Services Controller Instances`**
Universal Synchronization	On

6 On the **Select Objects to Include** page, select **IP Sets** from the **Object Type** drop-down menu, add **Platform Services Controller Instances** from **Available Objects** to **Selected Objects**, and click **Next**.

7 On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.

8 Repeat this procedure to create all the necessary security groups.

Create Distributed Firewall Rules in Region A

You create firewall rules to allow administrators to connect to the various VMware solutions, to allow for user access to the vRealize Automation portal, and to provide the external connectivity to the SDDC.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Add a section of rules for the management applications.

a From the **Home** menu, select **Networking & Security** and click **Firewall**.

b From the **NSX Manager** drop-down menu, select **172.16.11.65**.

c Click **Add Section**.

The **Add New Section** dialog box appears.

d Enter **`VMware Management Services`** in the **Section Name** text box, click the **Universal Synchronization** toggle to **On**, and click **Add**.

3 Create a distributed firewall rule to allow an SSH access to administrators for the different VMware appliances.

a Click **Add rule**.

b Enter **`Allow SSH to admins`** in the **Name** column of the new rule.

c Click the **Edit** icon in the **Source** column, select **Security Group** from the **Object Type** drop-down menu , add **Administrators** to the **Selected Objects** list, and click **Save**.

d Click the **Edit** icon in the **Destination** column, select **Security Group** from the **Object Type** drop-down menu, add **VMware Appliances** and **Update Manager Download Service** to the **Selected Objects** list, and click **Save**.

e Click the **Edit** icon in the **Service** column, add **SSH** to the **Selected Objects** list, and click **Save**.

f Click the **Publish** button.

4 Repeat the previous step to create the following distributed firewall rules.

Name	Source	Destination	Service / Port
Allow vRA Portal to end users.	* any	■ vRealize Automation Appliances ■ vRealize Automation Windows ■ vRealize Business Server	HTTP, HTTPS
Allow vRA Console Proxy to end users	* any	vRealize Automation Appliances	TCP:8444
Allow SDDC to any.	SDDC	* any	* any
Allow PSC to admins.	Administrators	Platform Services Controller Instances	HTTPS
Allow SSH to admins.	Administrators	■ VMware Appliances ■ Update Manager Download Service	SSH
Allow RDP to admins.	Administrators	Windows Servers	RDP
Allow Orchestrator to admins.	Administrators	vRealize Automation Appliances	TCP:8281,8283
Allow vRB Data Collector to admins.	Administrators	vRealize Business Data Collector	HTTP, HTTPS
Allow vROPs to admins.	Administrators	■ vRealize Operations Manager ■ vRealize Operations Manager Remote Collectors	HTTP, HTTPS
Allow vRLI to admins.	Administrators	vRealize Log Insight	HTTP, HTTPS
Allow vRSLCM to admins.	Administrators	vRealize Suite Lifecycle Manager	HTTPS

Name	Source	Destination	Service / Port
Allow VAMI to admins.	Administrators	VMware Appliances	TCP:5480
Allow VMware VADP Solution to admins.	Administrators	VMware Appliances	TCP:8543

5 Change the default rule action from Allow to **Block**.

a From the **NSX Manager** drop-down menu, select **172.16.11.65**.

b On the **General** tab, expand the **Default Section Layer3** section.

c In the **Action** column, for the **Default Rule**, change the action to **Block**.

d Click **Save** and click **Publish**.

Network security improves by allowing only required by the SDDC network traffic to pass.

Update the Host Profile for the Shared Edge and Compute Cluster in Region A

Update the user name and password in the customizations for the hosts in the shared edge and computecluster to be compliant as the host profile does not contain credentials information.

Procedure

1 Log in to the Compute vCenter Server by using the vSphere Client.

a Open a Web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/ui` .

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Update the sfo01-w01hp-comp01 host profile.

a From the **Home** menu, select **Policies and Profiles** and click **Host Profiles**.

b Right-click **sfo01-w01hp-comp01**, and select **Copy Settings from Host**.

c Select **sfo01w01esx01.sfo01.rainpole.local**, and click **OK**.

3 Edit the **sfo01-w01hp-comp01** host profile customizations.

a From the **Home** menu, select **Policies and Profiles** and click **Host Profiles**.

b Right-click **sfo01-w01hp-comp01**, and select **Edit Host Customizations**.

The **Edit Host Customizations** wizard appears.

c Under **Select Hosts**, select all hosts and click **Next**.

d Under **Edit Host Customizations**, update the following values for **User Name** and **Password**.

ESXi Host	Active Directory Configuration user name	Active Directory Configuration Password
sfo01w01esx01.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01w01esx02.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01w01esx03.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01w01esx04.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*

e Click **Finish**.

4 Verify compliance and remediate the hosts.

a On the **Host Profiles** page, click **sfo01-w01hp-comp01**, and click the **Monitor** tab.

b Click **Compliance**, click **Actions**, and select **Check Host Profile Compliance**.

On the **Host profile** page, the **Host Profile Compliance** column shows the first host as `Compliant`, and the other hosts as `Not Compliant`.

c Select each of the non-compliant hosts and click **Remediate**.

d In the **Remediate** dialog box, select **Automatically reboot hosts that require remediation**.

e Click **OK**.

All hosts show as **Compliant**.

Update DNS Records for the Platform Services Controller Load Balancer in Region A

After setting up load balancing, you modify the DNS address of the Platform Services Controller load balancer in Region A.

For the Platform Services Controller Load Balancer, you edit the sfo01psc01.sfo01.rainpole.local DNS entry to point to the virtual IP address (VIP) of the 172.16.11.71 load balancer, instead of pointing to the sfo01m01psc01 IP address.

Procedure

1 Log in to the DNS server that resides in the sfo01.rainpole.local domain.

2 Open the Windows **Start** menu, enter **`dnsmgmt.msc`** in the **Search** text box, and press Enter.

The **DNS Manager** dialog box appears.

3 In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the **sfo01.rainpole.local** domain and on the right locate the sfo01psc01 record .

4 Double-click **sfo01psc01**, enter the following settings, and click **OK**.

Setting	Value
Fully Qualified domain name (FQDN)	sfo01psc01.sfo01.rainpole.local
IP Address	172.16.11.71
Update Associated Pointer (PTR) record	Deselected

Post-Deployment Operations Management Configuration in Region A

6

After the operations management applications are deployed in Region A, perform post-deployment tasks for the operations management layer. You reconfigure the UMDS application virtual network, enable the automatic synchronization of authentication sources in vRealize Operations Manager, and enable define monitoring goals for the default policy.

Procedure

1 Post-Deployment Configuration for Update Manager Download Service in Region A

After Update Manager Download Service (UMDS) is deployed, perform post-deployment tasks. You allocate a static IP and connect UMDS to the application virtual network in Region A.

2 Post-Deployment Configuration for vRealize Operations Manager in Region A

After deploying vRealize Operations Manager, enable an automatic synchronization of the user membership for configured groups and remove the existing service accounts. You add the service accounts to integrate vRealize Operations Manager with vRealize Log Insight and with vRealize Automation, and for the default policy you enable define monitoring goals.

Post-Deployment Configuration for Update Manager Download Service in Region A

After Update Manager Download Service (UMDS) is deployed, perform post-deployment tasks. You allocate a static IP and connect UMDS to the application virtual network in Region A.

Reconfigure Update Manager Download Service in Region A

After deploying Update Manager Download Service (UMDS), it is outside of the application virtual network. You add the UMDS virtual machine to the application virtual network in Region A and update the UMDS VM IP address.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Connect the Update Manager Download Service VM to the **Mgmt-RegionA01-VXLAN** port group.

   a Right-click **sfo01umds01**, and select **Edit Settings**.

   b On the **Edit Settings** page, browse to the following network and click **OK**.

Setting	Value
Network adapter 1	distributed port group that ends with `Mgmt-RegionA01-VXLAN`

4 Change the IP address of the Update Manager Download Service virtual machine.

   a Right-click **sfo01umds01**, and select **Open Console**.

   b Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc_umds_password*

   c Run the following command to open the `01-netcfg.yaml` file.

```
sudo vi /etc/netplan/01-netcfg.yaml
```

   When prompted, provide the password for the **svc-umds** account.

   d In the `01-netcfg.yaml` file, enter the following settings and save the file.

Setting	Value
addresses	[192.168.31.67/24]
gateway4	192.168.31.1

   e Run the following command to apply the changes.

```
sudo netplan apply
```

5 Log in to the **dc01rpl.rainpole.local** DNS server by using a Remote Desktop Protocol (RDP) client.

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

   b Log in using the following credentials.

Setting	Value
User name	Active Directory administrator
Password	*ad_admin_password*

6 Open the Windows **Start** menu, enter **`dnsmgmt.msc`** in the **Search** text box, and press Enter.

   The **DNS Manager** dialog box appears.

7 Under **Forward Lookup Zones**, select the **sfo01.rainpole.local** domain and in the right pane locate **sfo01umds01**.

8 Double-click the **sfo01umds01** record, modify the IP address, and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	sfo01umds01.sfo01.rainpole.local
IP Address	192.168.31.67
Update associated pointer (PTR) record	Selected

Post-Deployment Configuration for vRealize Operations Manager in Region A

After deploying vRealize Operations Manager, enable an automatic synchronization of the user membership for configured groups and remove the existing service accounts. You add the service accounts to integrate vRealize Operations Manager with vRealize Log Insight and with vRealize Automation, and for the default policy you enable define monitoring goals.

Procedure

1 Enable Automatic Synchronization of Authentication Sources in vRealize Operations Manager in Region A

   vRealize Operations Manager maps imported LDAP users to user groups after you enable the automatic synchronization of user membership for the rainpole.local and sfo01.rainpole.local Active Directory instances.

2 Remove Existing Service Accounts in vRealize Operations Manager in Region A

   After enabling automatic synchronization of authentication sources, you remove the **svc-vrli-vrops** and **svc-vra-vrops** service accounts and later add them. vRealize Operations Manager does not provide an API to perform an automatic synchronization.

3 Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight in Region A

   Assign an administrator role to the **svc-vrli-vrops** service account for the Launch in Context integration of vRealize Operations Manager with vRealize Log Insight.

4 Enable Integration of vRealize Log Insight with vRealize Operations Manager in Region A

Connect vRealize Log Insight in Region A with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager. Use the launch in context functionality between the two management applications to troubleshoot management nodes and vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

5 Configure User Privileges on vRealize Operations Manager for Integration with vRealize Automation in Region A

Configure read-only privileges for the **svc-vra-vrops** service account on vRealize Operations Manager. vRealize Automation uses this account to collect metrics from vRealize Operations Manager for reclamation of tenant workloads that have a low use of CPU, memory, or disk space.

6 Verify the Integration of vRealize Operations Manager as a Metrics Provider in vRealize Automation in Region A

In vRealize Automation, verify that vRealize Operations Manager is integrated as a metrics provider so that vRealize Automation can pull metrics for the reclamation of tenant workloads.

7 Define Monitoring Goals for the Default Policy in vRealize Operations Manager in Region A

Define the default policy settings for monitoring the vCenter Server instances in the region in vRealize Operations Manager. vRealize Operations Manager uses these settings to analyze and monitor the objects associated with a vCenter Server instance.

Enable Automatic Synchronization of Authentication Sources in vRealize Operations Manager in Region A

vRealize Operations Manager maps imported LDAP users to user groups after you enable the automatic synchronization of user membership for the rainpole.local and sfo01.rainpole.local Active Directory instances.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2 On the main navigation bar, click **Administration**.

3 Configure the authentication sources to enable an automatic synchronization for the **rainpole.local** Active Directory instance.

a In the left pane, click **Access** and click **Authentication Sources**.

b On the **Authentication Sources** page, select **rainpole.local** and click **Edit**.

c In the **Edit Source for User and Group Import** dialog box, expand **Details** and select **Automatically synchronize user membership for configured groups**.

d Click **OK**.

4 Repeat the previous step for the **sfo01.rainpole.local** Active Directory.

Remove Existing Service Accounts in vRealize Operations Manager in Region A

After enabling automatic synchronization of authentication sources, you remove the **svc-vrli-vrops** and **svc-vra-vrops** service accounts and later add them. vRealize Operations Manager does not provide an API to perform an automatic synchronization.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2 On the main navigation bar, click **Administration**.

3 On the left of vRealize Operations Manager, click **Access** and click **Access Control**.

4 Remove the existing **svc-vrli-vrops** and **svc-vra-vrops** service accounts.

a On the **Access Control** page, select **svc-vrli-vrops** and click **Delete**.

b In the **Delete User** dialog box, click **Yes**.

c Repeat this step for the **svc-vra-vrops** service account and remove it.

Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight in Region A

Assign an administrator role to the **svc-vrli-vrops** service account for the Launch in Context integration of vRealize Operations Manager with vRealize Log Insight.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2 On the main navigator bar, click **Administration**.

3 On the left, expand **Access** and click **Access Control**.

4 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.

5 On the **Import Users** page, import the **svc-vrli-vrops** service account.

   a From the **Import From** drop-down menu, select **rainpole.local**.

   b Select the **Basic** option for the search query.

   c In the **Search String** text box, enter **`svc-vrli-vrops`** and click **Search**.

   d Select **svc-vrli-vrops@rainpole.local** and click **Next**.

6 On the **Assign Groups and Permissions** page, click the **Objects** tab, configure the following settings, and click **Finish**.

Setting	Value
Select Role	Administrator
Assign this role to the user	Selected
Allow access to all objects in the system	Selected

7 When prompted with the warning about allowing access to all objects on the system, click **Yes**.

Enable Integration of vRealize Log Insight with vRealize Operations Manager in Region A

Connect vRealize Log Insight in Region A with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager. Use the launch in context functionality between the two management applications to troubleshoot management nodes and vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Administration**.

3 Under **Integration**, click **vRealize Operations**.

4 On the **vRealize Operations Manager** page, select **Enable launch in context**.

5 Click **Test Connection** to validate the connection and click **Save**.

   A progress dialog box appears.

6 Click **OK** to close the dialog box.

Configure User Privileges on vRealize Operations Manager for Integration with vRealize Automation in Region A

Configure read-only privileges for the **svc-vra-vrops** service account on vRealize Operations Manager. vRealize Automation uses this account to collect metrics from vRealize Operations Manager for reclamation of tenant workloads that have a low use of CPU, memory, or disk space.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2 On the main navigator bar, click **Administration**.

3 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.

4 On the **Import Users** page, import the **svc-vra-vrops** service account.

   a From the **Import From** drop-down menu, select **rainpole.local**.

   b Select the **Basic** option for the search query.

c In the **Search String** text box, enter `svc-vra-vrops` and click **Search**.

d Select **svc-vra-vrops@rainpole.local** and click **Next**.

5 On the **Assign Groups and Permissions** page, click the **Objects** tab, configure the following settings, and click **Finish**.

Setting	Value
Select Role	ReadOnly
Assign this role to the user	Selected
Select Object	**vCenter Adapter > vCenter Adapter - sfo01w01vc01**

Verify the Integration of vRealize Operations Manager as a Metrics Provider in vRealize Automation in Region A

In vRealize Automation, verify that vRealize Operations Manager is integrated as a metrics provider so that vRealize Automation can pull metrics for the reclamation of tenant workloads.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Administration > Reclamation > Metrics Provider**.

3 Click **Test Connection** to verify that the test connection is successful.

Define Monitoring Goals for the Default Policy in vRealize Operations Manager in Region A

Define the default policy settings for monitoring the vCenter Server instances in the region in vRealize Operations Manager. vRealize Operations Manager uses these settings to analyze and monitor the objects associated with a vCenter Server instance.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 From the solution table on the **Solutions** page, select the **VMware vSphere** solution, and click the **Configure** icon at the top.

   The **Manage Solution - VMware vSphere** dialog box appears.

5 Under **Instance Settings**, select the **sfo01m01vc01** vCenter adapter.

6 Click **Define Monitoring Goals**.

7 Under **Enable vSphere Hardening Guide Alerts**, click **Yes**, leave the default configuration for the other options, and click **Save**.

8 In the **Success** dialog box, click **OK**.

9 Click **Save Settings**.

10 In the **Info** dialog box, click **OK**.

11 Repeat steps Step 5 to Step 10 for the Compute vCenter Server adapter.

12 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.

Post-Deployment Cloud Management Platform Configuration in Region A

7

After the Cloud Management Platform (CMP) is deployed in Region A, perform post-deployment tasks for the cloud management layer. You finish the SDDC configuration in your environment and confirm a successful provisioning of virtual machines using newly created blueprints.

Procedure

1 Configure vRealize Automation for a Large-Scale Deployment in Region A

   Increase the values of the `ProxyAgentServiceBinding` attributes to configure the vRealize Automation Manager Service to contain many data objects, for example, 3000 or more virtual machines from vCenter Server.

2 Configure Content Library in Region A

   Content libraries are containers for VM templates, vApp templates, and other resources used for the vRealize Automation deployment of virtual machines and vApps. Sharing templates and files across multiple vCenter Server instances brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

3 Create Machine Prefixes in Region A

   As a fabric administrator, you create machine prefixes that are used to create names for machines provisioned through vRealize Automation. Tenant administrators and business group managers select these machine prefixes and assign them to provisioned machines through blueprints and business group defaults.

4 Create Business Groups in Region A

   Tenant administrators create business groups to associate a set of services and resources to a set of users that often correspond to a line of business, department, or other organizational unit. Users must belong to a business group to request machines.

5 Create Reservation Policies in Region A

   You use reservation policies to group similar reservations together. Create the reservation policy tag first, then add the policy to reservations to allow a tenant administrator or business group manager to use the reservation policy in a blueprint.

6 Create External Network Profiles in Region A

Before members of a business group can request virtual machines, fabric administrators must create network profiles to define the subnet and routing configuration for those virtual machines. Each network profile is configured for a specific network port group or virtual network to specify the IP address and the routing configuration for virtual machines provisioned to that network.

7 Create Reservations for the Shared Edge and Compute Cluster in Region A

Before members of a business group can request machines, as a fabric administrator, you must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource.

8 Create Reservations for the User Edge Resources in Region A

Before members of a business group can request virtual machines, as a fabric administrator, you must allocate NSX Edge resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

9 Create Virtual Machines Using VM Templatesin the Content Libraryin Region A

vRealize Automation cannot directly access virtual machine templates in the content library. You must create a virtual machine using the virtual machine templates in the content library, then convert the template in vCenter Server. Perform this procedure on all vCenter Server compute clusters that you add to vRealize Automation, including the first vCenter Server compute instance.

10 Convert Virtual Machines to VM Templates in in Region A

You convert the virtual machines directly to templates instead of making a copy by cloning.

11 Configure Single Machine Blueprints in Region A

Virtual machine blueprints determine the virtual machine attributes, the manner in which it is provisioned, and its policy and management settings.

12 Reconfigure the Microsoft SQL Server for vRealize Automation in Region A

When you deploy vRealize Automation, the Microsoft SQL Server is outside of the vRealize Automation application virtual network and you reconfigure the Microsoft SQL Server.

Configure vRealize Automation for a Large-Scale Deployment in Region A

Increase the values of the `ProxyAgentServiceBinding` attributes to configure the vRealize Automation Manager Service to contain many data objects, for example, 3000 or more virtual machines from vCenter Server.

Procedure

1 Log in to the virtual machine of the vRealize Automation IaaS Manager Service by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the **`vra01ims01a.rainpole.local`** virtual machine.

   b Log in using the following credentials.

Settings	Value
User name	rainpole\svc-vra
Password	*svc-vra_password*

2 Open the `C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config` file in a text editor, with Administrative rights.

3 Locate the following line in the `ManagerService.exe.config` file.

```
<binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">
<readerQuotas maxStringContentLength="13107200" />
```

4 Edit the values of the following parameters, increasing them by a factor of 10 as in the following table.

Setting	Value
maxReceivedMessageSize	131072000
maxStringContentLength	131072000

5 Save your changes to the `ManagerService.exe.config` file, and close the text editor.

6 Open the Windows**Start** menu, and select **Restart** to restart the virtual machine.

7 Repeat this procedure for the vra01ims01b.rainpole.local virtual machine.

Configure Content Library in Region A

Content libraries are containers for VM templates, vApp templates, and other resources used for the vRealize Automation deployment of virtual machines and vApps. Sharing templates and files across multiple vCenter Server instances brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

You create and manage a content library from a single vCenter Server instance, but you can share the library items with other vCenter Server instances if the HTTP(S) traffic is allowed between them.

Procedure

1 Configure a Content Library in the First Compute vCenter Server Instance in Region A

   Create a content library and populate it with templates that you can use to deploy virtual machines in your environment. Content libraries let you synchronize templates among different vCenter Server instances so that all the templates in your environment are consistent.

2 Import the OVF Files for the Virtual Machine Templates in Region A

You can import OVF packages that you previously prepared to use as templates for deploying virtual machines. The virtual machine templates that you add to the content library are used as vRealize Automation blueprints.

Configure a Content Library in the First Compute vCenter Server Instance in Region A

Create a content library and populate it with templates that you can use to deploy virtual machines in your environment. Content libraries let you synchronize templates among different vCenter Server instances so that all the templates in your environment are consistent.

There is only one Compute vCenter Server in this VMware Validated Design, but if you deploy more instances for use by the compute cluster they can also use this content library.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Content Libraries** and click the **+** icon.

The **New Content Library** wizard opens.

3 On the **Name and location** page, enter the following settings and click **Next**.

Setting	Value
Name	sfo01-w01cl-vra01
vCenter Server	sfo01w01vc01.sfo01.rainpole.local

4 On the **Configure content library** page, enter the following settings, and click **Next**.

Setting	Value
Local content library	Selected
Publish externally	Selected
Enable authentication	Selected
Password	*sfo01-w01cl-vra01_password*
Confirm password	*sfo01-w01cl-vra01_password*

5 On the **Add storage** page, select the **sfo01-w01-lib01** datastore to store the content library, and click **Next**.

6 On the **Ready to complete** page, click **Finish**.

Import the OVF Files for the Virtual Machine Templates in Region A

You can import OVF packages that you previously prepared to use as templates for deploying virtual machines. The virtual machine templates that you add to the content library are used as vRealize Automation blueprints.

You repeat this procedure three times to import the following virtual machine templates.

VM Template Name	Operating System Type
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit) with SQL 2012

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Content Libraries**.

3 Right-click the content library **sfo01-w01cl-vra01** and select **Import Item**.

4 In the **Import Library Item** dialog box, specify the settings for the first template and click **Import**.

Setting	Value
Source file	URL or local path to `redhat6-enterprise-64.ovf` and `.vmdk` file
Item name	redhat6-enterprise-64
Notes	Red Hat Enterprise Server 6 (64-bit)

5 Repeat the procedure to import the remaining virtual machine templates.

Create Machine Prefixes in Region A

As a fabric administrator, you create machine prefixes that are used to create names for machines provisioned through vRealize Automation. Tenant administrators and business group managers select these machine prefixes and assign them to provisioned machines through blueprints and business group defaults.

Machine prefixes are shared across all tenants. Every business group has a default machine prefix. Every blueprint must have a machine prefix or use the group default prefix. Fabric administrators are responsible for managing machine prefixes. A prefix consists of a base name to be followed by a counter of a specified number of digits. When the digits are all used, vRealize Automation rolls back to the first number.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Click **Infrastructure > Administration** > **Machine Prefixes**.

3 Click **New**, to create a default machine prefix for the Production group using the following settings, and click the **Save** icon.

Setting	Value
Name	Prod-
Number of Digits	5
Next Number	1

4 Click **New**, to create a default machine prefix for the Development group using the following settings, and click the **Save** icon.

Setting	Value
Name	Dev-
Number of Digits	5
Next Number	1

Create Business Groups in Region A

Tenant administrators create business groups to associate a set of services and resources to a set of users that often correspond to a line of business, department, or other organizational unit. Users must belong to a business group to request machines.

For this implementation create two business groups, a Production business group and a Development business group.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Administration > Users and Groups > Business Groups**.

3 Click **New**.

4 On the **General** tab, enter the following values and click **Next**.

Setting	Value
Name	Production
Send capacity alert emails to	vra-admin-rainpole@rainpole.local

5 On the **Members** tab, enter **`ug-vra-admins-rainpole@rainpole.local`** in the **Group manager role** text box, press Enter, select the displayed group, and click **Next**.

6 On the **Infrastructure** tab, select **Prod-** from the **Default machine prefix** drop-down menu and click **Finish**.

7 Click **New**.

8 On the **General** tab, configure the following values, and click **Next**.

Setting	Value
Name	Development
Send capacity alert emails to	vra-admin-rainpole@rainpole.local

9 On the **Members** tab, enter **`ug-vra-admins-rainpole@rainpole.local`** in the **Group manager role** text box and click **Next**.

10 On the **Infrastructure** tab, select **Dev-** from the **Default machine prefix** drop-down menu, and click **Finish**.

Create Reservation Policies in Region A

You use reservation policies to group similar reservations together. Create the reservation policy tag first, then add the policy to reservations to allow a tenant administrator or business group manager to use the reservation policy in a blueprint.

When you request a machine, it can be provisioned on any reservation of the appropriate type that has sufficient capacity for the machine. You can apply a reservation policy to a blueprint to restrict the machines provisioned from that blueprint to a subset of available reservations. A reservation policy is often used to collect resources into groups for different service levels, or to make a specific type of resource easily available for a particular purpose. A reservation policy can include reservations of different types, but only reservations that match the blueprint type are considered when selecting a reservation for a particular request.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservations > Reservation Polices**.

3 Click **New**, configure the following settings, and click **OK**.

Setting	Value
Name	SFO-Production-Policy
Type	Reservation Policy
Description	Reservation policy for Production Business Group

4 Click **New**, configure the following settings, and click **OK**.

Setting	Value
Name	SFO-Development-Policy
Type	Reservation Policy
Description	Reservation policy for Development Business Group

5 Click **New**, configure the following settings, and click **OK**.

Setting	Value
Name	SFO-Edge-Policy
Type	Reservation Policy
Description	Reservation policy for Tenant Edge resources

Create External Network Profiles in Region A

Before members of a business group can request virtual machines, fabric administrators must create network profiles to define the subnet and routing configuration for those virtual machines. Each network profile is configured for a specific network port group or virtual network to specify the IP address and the routing configuration for virtual machines provisioned to that network.

You repeat this procedure six times to create the following six external network profiles.

- Ext-Net-Profile-Production-App
- Ext-Net-Profile-Production-DB
- Ext-Net-Profile-Production-Web
- Ext-Net-Profile-Development-App
- Ext-Net-Profile-Development-DB
- Ext-Net-Profile-Development-Web

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservations > Network Profiles**, and click **New > External**.

3 On the **New Network Profile - External** page, specify the network profiles on the **General** tab.

a Add the values for the Production Group External Network Profile.

Setting	Production Web Value	Production DB Value	Production App Value
Name	Ext-Net-Profile-Production-Web	Ext-Net-Profile-Production-DB	Ext-Net-Profile-Production-App
Description	External Network profile for Web Tier of Production Business Group	External Network profile for DB Tier of Production Business Group	External Network profile for App Tier of Production Business Group
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	172.11.10.1	172.11.11.1	172.11.12.1

b Add the values for the Development Group External Network Profile.

Setting	Development Web Value	Development DB Value	Development App Value
Name	Ext-Net-Profile-Development-Web	Ext-Net-Profile-Development-DB	Ext-Net-Profile-Development-App
Description	External Network profile for Web Tier of Development Business Group	External Network profile for DB Tier of Development Business Group	External Network profile for App Tier of Development Business Group
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	172.12.10.1	172.12.11.1	172.12.12.1

4 On the **DNS** tab, enter the following values for the profile you are creating.

Setting	Value
Primary DNS	172.16.11.4
Secondary DNS	172.17.11.4
DNS suffix	sfo01.rainpole.local
DNS search suffixes	sfo01.rainpole.local

5 Click the **Network Ranges** tab, click the **New** button and enter the following values for the profile you are creating.

a Configure the Production Business Network Range with the following values.

Setting	Production Web Value	Production DB Value	Production App Value
Name	Production-Web	Production-DB	Production-App
Description	Static IP range for Web Tier of the Production Group	Static IP range for DB Tier of the Production Group	Static IP range for App Tier of the Production Group
Start IP	172.11.10.20	172.11.11.20	172.11.12.20
End IP	172.11.10.250	172.11.11.250	172.11.12.250

b Configure the Production Development Business Network Range with the following values.

Setting	Development Web Value	Development DB Value	Development App Value
Name	Development-Web	Development-DB	Development-App
Description	Static IP range for Web Tier of the Development Group	Static IP range for DB Tier of the Development Group	Static IP range for App Tier of the Development Group
Start IP	172.12.10.20	172.12.11.20	172.12.12.20
End IP	172.12.10.250	172.12.11.250	172.12.12.250

c Click **OK** to save the network range.

6 Click **OK** to save the network profile.

7 Repeat this procedure to create all external network profiles.

Create Reservations for the Shared Edge and Compute Cluster in Region A

Before members of a business group can request machines, as a fabric administrator, you must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource.

For the scenarios, you perform this procedure twice to create reservations for both the Production and Development business groups.

Group	Name
Production	SFO01-Comp01-Prod-Res01
Development	SFO01-Comp01-Dev-Res01

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Compute Resources > Compute Resources**.

3 In the **Name** column, point to the compute cluster **sfo01-w01-comp01**, and select **Data Collection** from the drop-down menu.

4 Click the four **Request now** buttons in each field on the page.

   Wait for the data collection process to complete.

5 Click **Refresh**, and verify that **Status** shows `Succeeded` for both **Inventory** and **Network and Security Inventory**.

6 Navigate to **Infrastructure > Reservations** > **Reservations**, and click **New > vSphere (vCenter)**.

   The **New Reservation - vSphere (vCenter)** page appears.

7 Click the **General** tab and configure the following values.

Setting	Production Group Value	Development Group Value
Name	SFO01-Comp01-Prod-Res01	SFO01-Comp01-Dev-Res01
Tenant	Rainpole	Rainpole
Business Group	Production	Development
Reservation Policy	SFO-Production-Policy	SFO-Development-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

8 Click the **Resources** tab and configure the following values.

Setting	Value
Compute resource	**sfo01-w01-comp01 (sfo01w01vc01.sfo01.rainpole.local)**
Memory (GB)	**This Reservation `200`**
Storage (GB)	■ Select the **sfo01-w01-lib01** check box. ■ **This Reservation Reserved `2000`** ■ **Priority `1`**
Resource Pool	**sfo01-w01rp-user-vm**

9 Click the **Network** tab, select the network path check boxes listed in the following table from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

   a Configure the Production Business Group with the following values.

Production Network Path	Production Group Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

   b Configure the Development Business Group with the following values.

Development Network Path	Development Group Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App

10 Click **OK** to save the reservation.

11 Repeat this procedure to create a reservation for the Development Business Group.

Create Reservations for the User Edge Resources in Region A

Before members of a business group can request virtual machines, as a fabric administrator, you must allocate NSX Edge resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

Perform this procedure twice to create reservations for both the Production and Development business groups.

Group	Name
Production	SFO01-Edge01-Prod-Res01
Development	SFO01-Edge01-Dev-Res01

Procedure

1 Log in to the vRealize Automation Rainpole portal.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservations> Reservations**, and click **New > vSphere (vCenter)**.

The **New Reservation - vSphere (vCenter)** page appears.

3 Click the **General** tab, and configure the following values.

Setting	Production Group Value	Development Group Value
Name	SFO01-Edge01-Prod-Res01	SFO01-Edge01-Dev-Res01
Tenant	Rainpole	Rainpole
Business Group	Production	Development
Reservation Policy	SFO-Edge-Policy	SFO-Edge-Policy
Priority	100	100
Enable This Reservation.	Selected	Selected

4 Click the **Resources** tab and configure the following values.

Setting	Value
Compute resource	**sfo01-w01-comp01 (sfo01w01vc01.sfo01.rainpole.local)**
Memory (GB)	**This Reservation `200`**
Storage (GB)	■ Select the **sfo01-w01-vsan01** check box. ■ **This Reservation Reserved `2000`** ■ **Priority `1`**
Resource Pool	**sfo01-w01rp-user-edge**

5 Click the **Network** tab, select the network path check boxes listed in the following tables from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

   a Configure the Production Business Group with the following values.

Production Port Group	Production Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

   b Configure the Development Business Group with the following values.

Development Port Group	Development Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App

6 Click **OK** to save the reservation.

7 Repeat this procedure to create a reservation for the Development Business Group.

Create Virtual Machines Using VM Templates in the Content Libraryin Region A

vRealize Automation cannot directly access virtual machine templates in the content library. You must create a virtual machine using the virtual machine templates in the content library, then convert the template in vCenter Server. Perform this procedure on all vCenter Server compute clusters that you add to vRealize Automation, including the first vCenter Server compute instance.

Repeat this procedure three times for each of the VM templates in the content library.

VM Template Name	Guest OS
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)

Procedure

1 Log in to the Compute vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`** .

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **VMs and Templates**.

3 Expand the **sfo01w01vc01.sfo01.rainpole.local** vCenter Server.

4 Right-click the **sfo01-w01dc** data center and select **New Folder > New VM and Template Folder**.

5 Enter the folder name as **`VM Templates`** and click **OK**.

6 From the **Home** menu, select **Content Libraries**.

7 Click **sfo01-w01cl-vra01** > **Templates**.

8 Right-click the VM Template **windows-2012r2-64** and click **New VM from This Template**.

   The **New Virtual Machine from Content Library** wizard opens.

9 On the **Select a name and folder** page, use the same template name.

   You use the same template name to create a common service catalog that works across different vCenter Server instances within your data center environment.

10 Select **VM Templates** as the folder for this virtual machine, and click **Next**.

11 On the **Select a compute resource** page, expand the **sfo01-w01-comp01** cluster, select the **sfo01-w01rp-user-vm** resource pool, and click **Next**.

12 On the **Review details** page, verify the template details and click **Next**.

13 On the **Select storage** page, select the **sfo01-w01-lib01** datastore, select **Thin Provision** from the **Select virtual disk format** drop-down menu, and click **Next**.

14 On the **Select networks** page, select **sfo01-w01-vds01-management** for the **Destination Network**, and click **Next**.

   vRealize Automation changes the network according to the blueprint configuration.

15 On the **Ready to complete** page, review the configurations that you have made for the virtual machine, and click **Finish**.

   A new task for creating the virtual machine appears in the **Recent Tasks** pane. After the task is complete, the new virtual machine is created.

16 Repeat this procedure for all the VM templates in the content library.

Convert Virtual Machines to VM Templates in in Region A

You convert the virtual machines directly to templates instead of making a copy by cloning.

Repeat this procedure for each of the VM templates in the content library.

Table 7-1. VM Templates and Guest OS for Each Template

VM Template Name	Guest OS
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)

Procedure

1 Log in to the Compute vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`** .

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **VMs and Templates**.

3 In the **Navigator** pane, expand **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01dc > VM Templates**.

4 Right-click the **windows-2012r2-64** virtual machine located in the `VM Templates` folder, and click **Template > Convert to Template**.

5 Click **Yes** to confirm the template conversion.

6 Repeat this procedure for all the VM templates in the content library, verifying that each VM template appears in the `VM Templates` folder.

Configure Single Machine Blueprints in Region A

Virtual machine blueprints determine the virtual machine attributes, the manner in which it is provisioned, and its policy and management settings.

Procedure

1 Create a Service Catalog in Region A

   A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

2 Create a Single Machine Blueprint in Region A

Create blueprints for cloning the virtual machine templates using the specified resources on the Compute vCenter Server. Tenants can later use these blueprints for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

3 Create Entitlements for Business Groups in Region A

You add a service, catalog item, or action to an entitlement, to allow the users and groups identified in the entitlement to request provisionable items in the service catalog. The entitlement allows members of a particular business group (for example, the Production business group) to use the blueprint. Without the entitlement, users cannot use the blueprint.

4 Configure Entitlements for Blueprints in Region A

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

5 Test the Deployment of a Single Machine Blueprint in Region A

Test your environment and confirm the successful provisioning of virtual machines using the newly created blueprints. If multiple availability zones have been configured, you must manually place all the virtual machines provisioned by vRealize Automation into the appropriate VM group for the availability zone.

Create a Service Catalog in Region A

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Click the **Administration** tab, click **Catalog Management > Services**, and click **New**.

3 In the **New Service** page, configure the following settings and click **OK**.

Setting	Value
Name	SFO Service Catalog
Description	Default setting (blank)

Setting	Value
Icon	Default setting (blank)
Status	Active

Create a Single Machine Blueprint in Region A

Create blueprints for cloning the virtual machine templates using the specified resources on the Compute vCenter Server. Tenants can later use these blueprints for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Repeat this procedure to create the following three blueprints.

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2012 R2 - SFO Prod	windows-2012r2-64 (sfo01w01vc01.sfo01.rainpole.local)	**os-windows-joindomain-custom-spec**	SFO-Production-Policy
Windows Server 2012 R2 With SQL2012 - SFO Prod	windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local)	**os-windows-joindomain-custom-spec**	SFO-Production-Policy
Redhat Enterprise Linux 6 - SFO Prod	redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)	**os-linux-custom-spec**	SFO-Production-Policy

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Design > Blueprints** and click **New**.

3 In the **New Blueprint** dialog box, on the **General** tab, configure the following settings, and click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - SFO Prod
Deployment limit	Default setting (blank)
Lease (days): Minimum	30
Lease (days): Maximum	270
Archive (days)	15

4 Select the **vSphere (vCenter) Machine** icon and drag it in the **Design Canvas**.

5 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Default
ID	Default setting (vSphere_vCenter_Machine_1)
Description	Default setting (blank)
Display location on request	Deselected
Reservation policy	SFO -Production-Policy
Machine prefix	Use group default.
Instances: Minimum	Default setting
Instances: Maximum	1

6 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	**os-windows-joindomain-custom-spec**

Note If the value of the **Clone from** setting does not list **windows-2012r2-64** template, you must perform a data collection on the **sfo01-w01-comp01** Compute Resource.

Verify that the required customization spec is available in vSphere Client under **Menu > Policies and Profiles > VM Customization Specifications**.

7 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPUs	2	4
Memory (MB)	4096	16384
Storage (GB)	Default setting	Same value as Minimum

8 Click the **Network** tab.

a In the **Categories** section, select **Network & Security** to display the list of available network and security components.

b Select the **Existing Network** component and drag it in the **Design Canvas**.

c Click the **Existing network** object and on the **General** tab, select the **Ext-Net-Profile-Production-Web** network profile , and click **OK**.

Blueprint Name	Existing network
Windows Server 2012 R2 - SFO Prod	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 With SQL2012 - SFO Prod	Ext-Net-Profile-Production-DB
Redhat Enterprise Linux 6 - SFO Prod	Ext-Net-Profile-Production-App

d Click **Save**.

e In the **Design Canvas**, select the **vSphere_vCenter_Machine** object.

f Select the **Network** tab, click **New**, configure the following settings, and click **OK**.

Network	Assignment Type	Address
Ext-Net-Profile-Production-Web	Static IP	Default setting (blank)
Ext-Net-Profile-Production-DB	Static IP	Default setting (blank)
Ext-Net-Profile-Production-App	Static IP	Default setting (blank)

g Click **Finish** to save the blueprint.

9 Select the blueprint **Windows Server 2012 R2 - SFO Prod** and click **Publish**.

10 Repeat this procedure to create additional blueprints.

To test blueprints in a development environment, or according to your business needs, create development blueprints using the same process as for production blueprints.

Create Entitlements for Business Groups in Region A

You add a service, catalog item, or action to an entitlement, to allow the users and groups identified in the entitlement to request provisionable items in the service catalog. The entitlement allows members of a particular business group (for example, the Production business group) to use the blueprint. Without the entitlement, users cannot use the blueprint.

Perform this procedure to create an entitlement for the Production business group.

Entitlement Name	Status	Business Group	User & Groups
Prod-SingleVM-Entitlement	Active	Production	**ug-vra-admins-rainpole**

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Click the **Administration** tab, and click **Catalog Management > Entitlements**.

3 Click **New**.

   The **New Entitlement** page appears.

4 Click the **General** tab, configure the following values, and click **Next**.

Setting	Value
Name	Prod-SingleVM-Entitlement
Description	Default setting (blank)
Expiration Date	Default setting (blank)
Status	Active
Business Group	Production
All Users and Groups	Unselected
Users & Groups	**ug-vra-admins-rainpole**

5 On the **Items & Approvals** tab, add the actions that the users from the Production business group are entitled to.

   a On the **Entitled Actions** page, click the **Add Actions** icon, add the following actions, and click **OK**.

   - Connect using RDP (Machine).
   - Power Cycle (Machine)
   - Power off (Machine)
   - Power on (Machine)
   - Reboot (Machine).
   - Shutdown (Machine)

   b Click **Finish**.

Configure Entitlements for Blueprints in Region A

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

Repeat this procedure to associate the blueprints with their entitlement.

Blueprint Name	Service Catalog	Add to Entitlement.
Windows Server 2012 R2 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement
Red hat Enterprise Linux 6 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Click the **Administration** tab and navigate to **Catalog Management > Catalog Items**.

3 On the **Catalog Items** pane, select the **Windows Server 2012 R2 - SFO Prod** blueprint in the **Catalog Items** list and click **Configure**.

4 On the **General** tab of the **Configure Catalog Item** dialog box, select **SFO Service Catalog** from the **Service** drop-down menu, and click **OK**.

5 Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement.

   a Click **Entitlements** and select **Prod-SingleVM-Entitlement**.

   The **Edit Entitlement** pane appears.

   b Select the **Items & Approvals** tab, add the **Windows Server 2012 R2 - SFO Prod** blueprint to the **Entitled Items** list, and click **OK**.

   c Click **Finish**.

6 Click the **Catalog** tab and verify that the blueprints are listed in the Service Catalog.

7 Repeat this procedure to associate all the blueprints with their entitlements.

Test the Deployment of a Single Machine Blueprint in Region A

Test your environment and confirm the successful provisioning of virtual machines using the newly created blueprints. If multiple availability zones have been configured, you must manually place all the virtual machines provisioned by vRealize Automation into the appropriate VM group for the availability zone.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Click the **Catalog** tab, click **Click here to apply filters**, and click **SFO Service Catalog** from the catalog of available services.

3 Click the **Request** button for one of the blueprints and click **Submit**.

4 Verify that the request finishes successfully.

   a Click the **Deployments** tab.

   b Select the deployment that you submitted, click **History**, and wait several minutes for the request to finish.

   Click the **Refresh** icon every few minutes until a `Successful` message appears.

   c Under **Status**, verify that the virtual machine successfully provisioned.

5 Verify that the virtual machine provisions in the shared edge and compute cluster.

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`** .

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

   c From the **Home** menu, select **Hosts and Clusters**.

   d In the **Navigator** pane, expand **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01-comp01 > sfo01-w01rp-user-vm**, and verify that the virtual machine is present.

Reconfigure the Microsoft SQL Server for vRealize Automation in Region A

When you deploy vRealize Automation, the Microsoft SQL Server is outside of the vRealize Automation application virtual network and you reconfigure the Microsoft SQL Server.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Shut down the vRealize Automation components.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Right-click the following VMs, according to their shutdown order and select **Power > Shut Down Guest OS**.

Table 7-2. Shutdown Order

Product	Virtual Machine Name in Region A	Shutdown Order
vRealize Business for Cloud	Total Number of VMs (2)	1
	sfo01vrbc01	1
	vrb01svr01	2
vRealize Automation	Total Number of VMs (12)	2
	vra01dem01b	1
	vra01dem01a	1
	sfo01ias01b	1
	sfo01ias01a	1
	vra01ims01b	2
	vra01ims01a	3
	vra01iws01b	4
	vra01iws01a	5
	vra01svr01c	6
	vra01svr01b	7
	vra01svr01a	8
	vra01mssql01	9

3 Migrate the Microsoft SQL Server virtual machine to the sfo01-m01fd-vra folder and connect to the Mgmt-xRegion01-VXLAN port group.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Right-click **vra01mssql01**, select **Move to folder > sfo01-m01fd-vra**, and click **OK**.

c Right-click **vra01mssql01**, and select **Edit Settings**.

d On the **Edit Settings** page, browse the following network and click **OK**.

Setting	Value
Network adapter 1	distributed port group that ends with `Mgmt-xRegion01-VXLAN`

e Right-click **vra01mssql01** and select **Power > Power on**.

4 Change the IP address of the vra01mssql01 virtual machine.

a Right click **vra01mssql01**, and select **Open Console**.

b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

c From the Windows **Start Menu**, select **Control Panel > Network and Internet > Network and Sharing Center**.

d Click **Change adapter settings**.

e Right-click the Ethernet adapter and select **Properties**.

f Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

g Enter the following settings and click **OK**.

Setting	Value
IP address	192.168.11.62
Subnet mask	255.255.255.0
Default gateway	192.168.11.1

5 Change the IP address in the DNS for the vra01mssql01 virtual machine.

a Log in to the DNS server that resides in the sfo01.rainpole.local domain by using a Remote Desktop Protocol (RDP) client.

b Open an RDP connection to the **`dc01rpl.rainpole.local`** DNS server.

c Log in using the following credentials.

Setting	Value
User name	Active Directory administrator
Password	*ad_admin_password*

d Open the Windows **Start** menu, enter **`dnsmgmt.msc`** in the **Search** text box, and press Enter.

The **DNS Manager** dialog box appears.

e Under **Forward Lookup Zones**, select the **rainpole.local** domain and in the right pane locate vra01mssql01.

f Double-click the **vra01mssql01** record, modify the **IP Address**, and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	vra01mssql01.rainpole.local
IP Address	192.168.11.62
Update associated pointer (PTR) record	Selected

6 Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client.

a Open an RDP connection to the **`vra01mssql01.rainpole.local`** virtual machine.

b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

7 Install vRealize Log Insight Windows Agents in vra01mssql01.

From the vra01mssql01 Windows environment, log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

c Click the configuration drop-down menu icon and select **Administration**.

d Under **Management**, click **Agents** and click the **Download Log Insight Agent Version** link.

e In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the `.msi` file on the vra01mssql01 virtual machine.

f Open an administrative command prompt, and navigate to the directory where you saved the `.msi` file.

g Run the following command and install the vRealize Log Insight agent with custom values.

```
VMware-Log-Insight-Agent-4.7.0-build_number_192.168.31.10.msi SERVERPORT=9000 AUTOUPDATE=yes
LIAGENT_SSL=no
```

h In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.

i Select sfo01vrli01.sfo01.rainpole.local in the **Host** text box, and click **Install**.

j Click **Finish**.

8 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

9 Power on the remaining vRealize Automation components.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Right-click the following VMs, according to their startup order and select **Power > Power on**.

Table 7-3. Startup Order

Product	Virtual Machine Name in Region A	Startup Order
vRealize Automation	Total Number of VMs (11)	1
	vra01svr01a	1
	vra01svr01b	2
	vra01svr01c	3
	vra01iws01a	4
	vra01iws01b	5
	vra01ims01a	6
	vra01ims01b	7
	sfo01ias01a	8
	sfo01ias01b	8
	vra01dem01a	8
	vra01dem01b	8
vRealize Business for Cloud	Total Number of VMs (2)	2
	vrb01svr01	1
	sfo01vrbc01	2

10 Test your environment and confirm the successful provisioning of virtual machines.

Follow the steps in the following procedure and Test the Deployment of a Single Machine Blueprint in Region A.