Deployment of Region B

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 B

1

The *VMware Validated Design Deployment of Region B* 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 Validated Design Cloud Builder virtual appliance to automate the implementation of this Validated Design.

The *VMware Validated Design Deployment of Region B*documentation does not contain step-by-step instructions for performing all required post-configuration tasks because they often depend on customer requirements.

Intended Audience

The *VMware Validated Design Deployment of Region B* 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 B* 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 B*, 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*
- *VMware Validated Design Deployment of Region A*

Updated Information

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

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

Revision	Description
19 MAR 2019	■ Changed the login method during the postdeployment configuration of the vShere Update Manager Download Service virtual machine from SSH to virtual console. See Reconfigure Update Manager Download Service in Region B. ■ Added a post-deployment procedure for the Virtual Infrastructure layer to update the distributed firewall to exclude vCenter Server instances from firewall protection. See Update the Distributed Firewall Configuration for Region B. ■ Added a post-deployment procedure for the Virtual Infrastructure layer to edit the DNS entry for the Platform Services Controller load balancer to point to the virtual IP address of the load balancer. See Update the DNS Records for the Platform Services Controller Load Balancer in Region B.
12 FEB 2019	■ Clarified requirements for primary and secondary storage capacity. See Prerequisites for Automated SDDC Deployment in Region B. ■ 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 B.
22 JAN 2019	Initial Release

Prepare the Environment for Automated Deployment in Region B

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 B

  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 compute cluster, configure the management network, DNS, NTP, and SSH services.

- Prerequisites for Operations Management Layer Implementation in Region B

  To prepare the operations management layer for an automated deployment of the 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 B

  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 B

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

- Generate Certificates for the SDDC Components in Region B

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

Prerequisites for Virtual Infrastructure Layer Implementation in Region B

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 compute cluster, configure the management network, DNS, NTP, and SSH services.

Procedure

1 Prerequisites for Installation of ESXi Hosts in Region B

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 B

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

3 Configure the Network on All Hosts in Region B

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 B

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

5 Configure SSH and NTP on All Hosts in Region B

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 B

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

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

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 a DNS configuration to emulate an existing load balancer IP address.

Prerequisites for Installation of ESXi Hosts in Region B

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 your hosts and perform configuration steps.
- Ensure that routing is in place between the two regional management networks 172.16.11.0/24 and 172.17.11.0/24 as it is necessary to join the common SSO domain.

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
lax01m01esx01.lax01.rainpole.local	172.17.11.101	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01m01esx02.lax01.rainpole.local	172.17.11.102	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01m01esx03.lax01.rainpole.local	172.17.11.103	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01m01esx04.lax01.rainpole.local	172.17.11.104	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local

Table 2-2. Shared Edge and Compute Cluster Hosts

FQDN	IP	VLAN ID	Default Gateway	NTP Server
lax01w01esx01.lax01.rainpole.local	172.17.31.101	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01w01esx02.lax01.rainpole.local	172.17.31.102	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01w01esx03.lax01.rainpole.local	172.17.31.103	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01w01esx04.lax01.rainpole.local	172.17.31.104	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local

Install ESXi Interactively on All Hosts in Region B

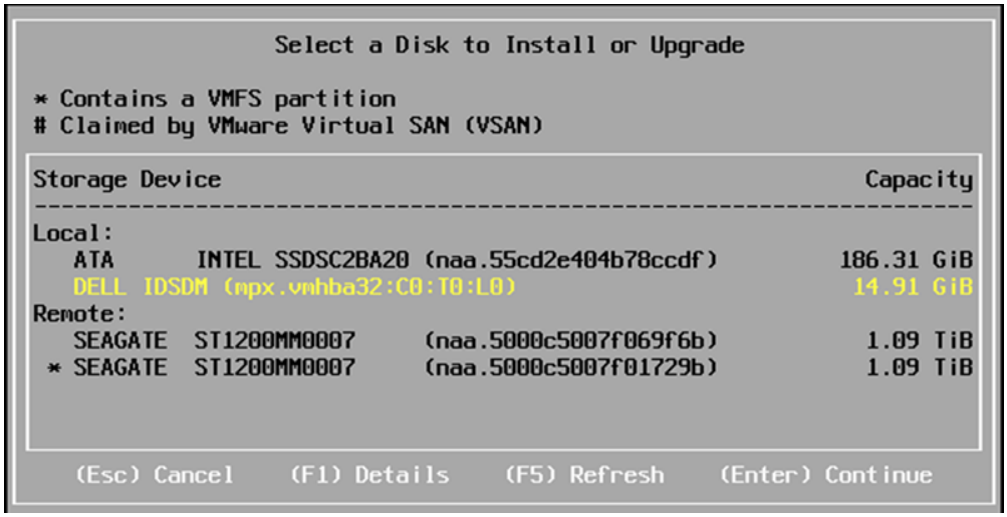
Install ESXi on all hosts in the management and the shared edge and compute clusters interactively.

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 B

Procedure

1. Power on the **lax01m01esx01** 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 or SD card 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 B

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 B.

Procedure

1 Open the DCUI on the physical ESXi host **lax01m01esx01.lax01.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 **1711** 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	172.17.11.101
Subnet Mask	255.255.255.0
Default Gateway	172.17.11.253

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	172.17.11.5
Alternate DNS Server	172.17.11.4
Hostname	lax01m01esx01.lax01.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 B

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

You configure the VLAN ID of the VM network port group 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
lax01m01esx01.lax01.rainpole.local	1711
lax01m01esx02.lax01.rainpole.local	1711
lax01m01esx03.lax01.rainpole.local	1711
lax01m01esx04.lax01.rainpole.local	1711
lax01w01esx01.lax01.rainpole.local	1731
lax01w01esx02.lax01.rainpole.local	1731
lax01w01esx03.lax01.rainpole.local	1731
lax01w01esx04.lax01.rainpole.local	1731

Procedure

1. Log in to the vSphere host by using the VMware Host Client.
   a. Open a Web browser and go to `https://lax01m01esx01.lax01.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 `1711` for **VLAN ID**, and click **Save**.

Configure SSH and NTP on All Hosts in Region B

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. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts in Region B

Procedure

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

   a Open a Web browser and go to **`https://lax01m01esx01.lax01.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 enter **`ntp.lax01.rainpole.local,ntp.sfo01.rainpole.local`** as NTP servers.

   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 B

This VMware Validated Design uses NFS storage as the secondary storage for the SDDC management components. You mount the NFS storage to provide the 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 B.

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://lax01m01esx01.lax01.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 the Management Cluster	Value for the Shared Edge and Compute Cluster
Port Group	New port group	New port group
New Port Group	Storage	Storage
Virtual Switch	vSwitch0	vSwitch0
VLAN ID	1715	1725
MTU	9000	9000
IP version	IPv4 only	IPv4 only
IPv4 settings	Static	Static
Address	172.17.15.101	172.17.25.101
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 the Management Cluster	Value for the Shared Edge and Compute Cluster
Name	lax01-m01-bkp01	lax01-w01-lib01
NFS server	172.17.15.251	172.17.25.251
NFS share	`/VVD_backup01_nfs01_Mgmt_6TB`	`/VVD_vRA_ComputeB_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 B

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 a 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	lax01psc01	172.17.11.71	lax01.rainpole.local
Platform Services Controller for the Management Cluster	lax01m01psc01	172.17.11.61	lax01.rainpole.local

Procedure

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

2 Open the Windows **Start** menu, and 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 **lax01.rainpole.local** zone, and select **New Host (A or AAAA)**.

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

Setting	Value
Name	lax01psc01
Fully qualified domain name (FQDN)	lax01psc01.lax01.rainpole.local
IP address	172.17.11.61
Create associate pointer (PTR) record	Deselected

Attention To create an operational network configuration for lax01psc01.lax01.rainpole.local, Cloud Builder requires forward lookup with IP 172.17.11.61 and reverse lookup with IP 172.17.11.71 (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 **11.17.172.in-addr.arpa** zone and select **New Pointer (PTR)**.

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

Setting	Value
Host IP address	172.17.11.71
Fully qualified domain name (FQDN)	**71.11.17.172.in-addr.arpa**
Host name	lax01psc01.lax01.rainpole.local

Prerequisites for Operations Management Layer Implementation in Region B

To prepare the operations management layer for an automated deployment of the 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 B

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 lax01m01esx01.lax01.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	lax01m01esx01
VM Name	lax01umds01
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	lax01-m01-bkp01

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

Setting	Value
Host Name	lax01umds01
Static IPv4 Address	172.17.11.67
Default Gateway	172.17.11.253
Subnet Mask	255.255.255.0
DNS Server	172.17.11.5, 172.17.11.4
DNS Domain	lax01.rainpole.local
DNS Search	lax01.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://lax01m01esx01.lax01.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 **lax01umds01** 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 B

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.

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

You deploy and configure a single Master Windows system virtual machine which is cloned and reconfigured during the SDDC deployment to provision all 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 lax01m01esx01.lax01.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	lax01m01esx01
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	lax01-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 that 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 lax01.rainpole.local domain.
Internet Explorer Enhanced Security Configuration	Turn off ESC.
Remote Desktop Protocol	Enable RDP access.

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

Component	Requirement
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 the Secondary Logon service and set the 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 PowerShell 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 the `sources\sxs` directory 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 name	rainpole\svc-vra
Password	*svc-vra_password*

10 Shut down the Master Windows system virtual machine.

Prerequisites for Business Continuity Layer Implementation in Region B

To prepare the business continuity layer for automated deployment of the SDDC components using VMware 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 B

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 lax01m01esx01.lax01.rainpole.local host for Site Recovery Manager with the following virtual machine, software, and network configuration.

Table 2-9. Virtual Machine Requirements for Site Recovery Manager VM

Setting	Value
ESXi Host	lax01m01esx01
VM Name	lax01m01srm01
Guest OS	Windows Server 2016 (64-bit)
vCPU	2
Memory	2 GB
Virtual Disk	40 GB
SCSI Controller	LSI Logic SAS
Datastore	lax01-m01-bkp01
Network Interface	VM Network
Network Adapter Type	1 x VMXNET3

Table 2-10. Network Requirements for Site Recovery Manager VM

Setting	Value
Host Name	sfo01m01srm01
Static IPv4 Address	172.17.11.124
Subnet Mask	255.255.255.0
Default Gateway	172.17.11.253
DNS Server	172.17.11.5
FQDN	lax01m01srm01.lax01.rainpole.local
Open Ports	■ 9086 ■ 5678

Table 2-11. 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 lax01.rainpole.local domain.

Table 2-11. Software Requirements for the Site Recovery Manager VM (Continued)

Setting	Value
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 lax01m01srm01.lax01.rainpole.local 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 B

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

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 for 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 B

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

(Optional) 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 B

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 B

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 for Region B. See Deployment Specification in the *VMware Validated Design Planning and Preparation* 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

(Optional) 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.

You create and configure the `VMware` certificate authority template to generate and sign the certificates for the management components in Region A. If the `VMware` certificate authority template exists and is added to the certificate templates of the Microsoft CA, you can skip this procedure.

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 B

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	LAX
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.

   - lax01m01nsx01.txt
   - lax01m01srm01.txt
   - lax01m01vc01.txt
   - lax01m01vrs01.txt
   - lax01psc01.txt
   - lax01w01nsx01.txt
   - lax01w01vc01.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-lax-jd`.

VMware Cloud Builder Implementation in Region B

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 B

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 Management Host in Region B

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

Prerequisites for VMware Cloud Builder Implementation in Region B

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	172.17.11.60
Host name	lax01cb01
Default gateway	172.17.11.253
DNS servers	■ 172.17.11.5 ■ 172.17.11.4
DNS domain	lax01.rainpole.local
DNS search	lax01.rainpole.local,rainpole.local

Setting	Value
Subnet mask	255.255.255.0
NTP servers	■ ntp.lax01.rainpole.local ■ ntp.sfo01.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 Prepare the Environment for Deployment in Region B.
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 B

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

Procedure

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

  a Open a Web browser and go to **`https://lax01m01esx01.lax01.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 **`lax01cb01`** for the virtual machine name, select the VMware Cloud Builder `.ova` file , and click **Next**.

5 In the **Select storage** dialog box, select **lax01-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	*lax01cb01_root_password* Note : The passwords must be at least 8 characters, must contain uppercase, lowercase, digits, and special characters.
Confirm root password	*lax01cb01_root_password*
Enter admin user name	admin
Enter admin password	*lax01cb01_admin_password*
Confirm password	*lax01cb01_admin_password*
IP address	172.17.11.60
Subnet mask	255.255.255.0
Default Gateway	172.17.11.253
VM hostname	lax01cb01
Domain name	lax01.rainpole.local
Domain search path	lax01.rainpole.local,rainpole.local
DNS	172.17.11.5,172.17.11.4
NTP	ntp.lax01.rainpole.local,ntp.sfo01.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 B

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 deployment files against 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 B.

Procedure

1 Prerequisites for Automated SDDC Deployment in Region B

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 Builder in Region B

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 B

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 B

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 B

After you successfully validate the `vvd-std-regb-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 Cluster in Region B

After you successfully validate the `vvd-std-regb-comp.json` file, you start the automated deployment of the components in the shared edge and compute cluster.

Prerequisites for Automated SDDC Deployment in Region B

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 B.
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 B. 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 B.
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 Builder in Region B

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 **`lax01cb01.lax01.rainpole.local`** using an SCP 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-lax-jd` to the `/opt/vmware/vvd/certificates` directory on the Cloud Builder appliance.
4. Upload the `vra01svr01`, `vrb01svr01`, `vrops01svr01`, and `vrs01lcm01` folders and their content, that you generated during Region A deployment (`C:\CertGenVVD-*version*\SignedByMSCACerts-sfo-jd`) , to the `/opt/vmware/vvd/certificates` directory on the Cloud Builder appliance in Region B.
5. Configure the Cloud Builder appliance and mount the VMware Validated Design software bundle `.iso` file.
   a. Open an SSH connection to lax01cb01.lax01.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 B

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://lax01cb01.lax01.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 file 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 B** 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 B JSON Deployment Files

Architecture Type	JSON Filename	Workload Domain	Deployment Order
VVD for SDDC Region B	`vvd-std-regb-mgmt.json`	Management	1
	`vvd-std-regb-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 B 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 B

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 for both the management and the shared edge and compute clusters. 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://lax01cb01.lax01.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-regb-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 lax01cb01.lax01.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 B** 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-regb-mgmt.json` file and click **Validate**.

   The `vvd-std-regb-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-regb-comp.json` file and click **Validate**

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

What to do next

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

Start the Automated Deployment of the Management Cluster in Region B

After you successfully validate the `vvd-std-regb-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://lax01cb01.lax01.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 Cluster in Region B

After you successfully validate the `vvd-std-regb-comp.json` file, 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://lax01cb01.lax01.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-regb-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 B

5

After a successful deployment using VMware Cloud Builder, perform post-deployment tasks to finish the SDDC configuration in Region B. For the virtual infrastructure layer, you update the host profiles for the management cluster and for the shared edge and compute cluster.

Procedure

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

   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 Update the Distributed Firewall Configuration for Region B

   After deploying vCenter Server, add the vCenter Server instance to the distributed firewall exclusion list.

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

   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.

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

   You must modify the DNS address of the Platform Services Controller load balancer in Region B.

Update the Host Profile for the Management Cluster in Region B

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 the Virtual Appliance Management Interface (VAMI) of the vCenter Server appliance.

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Update the host profile.

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

   b Right-click **lax01-m01hp-mgmt01**, and select **Copy settings from Host**.

   c Select **lax01m01esx01.lax01.rainpole.local** and click **OK**.

3 Edit the lax01-m01hp-mgmt01 host profile customizations.

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

   b Right-click **lax01-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 in **User Name** and **Password**.

ESXi Host	Active Directory Configuration user name	Active Directory Configuration Password
lax01m01esx01.lax01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
lax01m01esx02.lax01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
lax01m01esx03.lax01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
lax01m01esx04.lax01.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 **lax01-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 lax01m01esx01.lax01.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 `Compliant` status in the **Host Compliance** column.

Update the Distributed Firewall Configuration for Region B

After deploying vCenter Server, add the vCenter Server instance to the distributed firewall exclusion list.

Procedure

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

a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local/ui`**.

b Log in using the following credentials.

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

2 Exclude the management vCenter Server instance from the firewall protection.

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

b Click **Firewall Settings** and click the **Exclusion List** tab.

c From the **NSX Manager** drop-down menu, select **172.17.11.65**.

d Under **User Excluded VMs**, click the **Add** button.

e On the **Select VM(s) to exclude** dialog box, move **lax01m01vc01** to the **Selected Objects** section, and click **OK**.

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

a In the **Navigator** pane, click **Firewall**.

b From the **NSX Manager** drop-down menu, select **172.17.11.65**.

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

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

e Click **Save** and click **Publish**.

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

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 the Compute vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/ui`**.

   b Log in using the following credentials.

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

2 Update the lax01-w01hp-comp01 host profile.

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

   b Click **Host Profiles**, right-click on **lax01-w01-comp01**, and select **Copy settings from Host**.

   c Select **lax01w01esx01.lax01.rainpole.local** and click **OK**.

3 Edit the lax01-w01hp-comp01 host profile customizations.

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

   b Right-click **lax01-w01hp-comp01**, and select **Host Profiles > 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 in **User Name** and **Password**.

ESXi Host	Active Directory Configuration user name	Active Directory Configuration Password
lax01w01esx01.lax01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
lax01w01esx02.lax01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
lax01w01esx03.lax01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
lax01w01esx04.lax01.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 **lax01-w01hp-comp01** and click the **Monitor** tab.

   b Click the **Monitor** tab and click **Compliance**.

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

   On the **Host profile** page, the **Host Profile Compliance** column shows lax01w01esx01.lax01.rainpole.local as `Compliant`, and the other hosts as `Not Compliant`.

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

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

f Click **OK**.

All hosts show as `Compliant`.

UpdatetheDNS Records for the Platform Services Controller Load Balancer in Region B

You must modify the DNS address of the Platform Services Controller load balancer in Region B.

For the Platform Services Controller Load Balancer, you must edit the DNS entry of lax01psc01.lax01.rainpole.local to point to the virtual IP address (VIP) of the Load Balancer (172.17.11.71) instead of pointing to the IP address of lax01m01psc01.

Procedure

1 Log in to the DNS server that resides in the lax01.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 **lax01.rainpole.local** domain and locate the **lax01psc01** record on the right.

4 Double-click **lax01psc01**, enter the following settings, and click **OK**.

Setting	Value
Fully Qualified Domain Name (FQDN)	IP Address
IP Address	172.17.11.71
Update Associated Pointer (PTR) record	Deselected

Post-Deployment Operations Management Configuration in Region B

6

After the operations management applications are deployed in Region B, 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 B

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.

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

After vRealize Operations Manager nodes are deployed in Region B, perform post deployment tasks for vRealize Operations Manager. You enable an automatic synchronization of the user membership for configured groups and enable define monitoring goals for the default policy.

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

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.

Reconfigure Update Manager Download Service in Region B

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

Procedure

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

a Open a Web browser and go to **`https://lax01m01vc01.lax01.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 **lax01m01vc01.lax01.rainpole.local** tree.

3 Connect the Update Manager Download Service VM to the **Mgmt-RegionB01-VXLAN** port group.

a Right-click **lax01umds01**, and select **Edit Settings**.

b Log in by using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc_umds_password*

c 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-RegionB01-VXLAN`

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

a Right-click **lax01umds01**, and select **Open Console**.

b Open the `01-netcfg.yaml` file by running the following command.

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

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

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

Setting	Value
addresses	[192.168.32.67/24]
gateway4	192.168.32.1

d Apply the changes by running the following command.

```
sudo netplan apply
```

5 Log in to the **dc51rpl.rainpole.local** DNS server by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the **`dc51rpl.rainpole.local`** DNS server.

   b Log in by using the following credentials.

Setting	Value
User name	Active Directory administrator
Password	*ad_admin_password*

6 Click the **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 **lax01.rainpole.local** domain and in the right pane, locate **lax01umds01**.

8 Double-click the **lax01umds01** record, modify the IP address , and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	lax01umds01.lax01.rainpole.local
IP Address	192.168.32.67
Update associated pointer (PTR) record.	Selected

Post-Deployment Configuration for vRealize Operations Manager in Region B

After vRealize Operations Manager nodes are deployed in Region B, perform post deployment tasks for vRealize Operations Manager. You enable an automatic synchronization of the user membership for configured groups and enable define monitoring goals for the default policy.

Procedure

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

   vRealize Operations Manager maps imported LDAP users to user groups after you enable "Automatically synchronize user membership for configured groups" for the lax01.rainpole.local Active Directory instance.

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

   Enable the "Define monitoring goals" option for the default policy for each vCenter Adapter instance in vRealize Operations Manager.

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

vRealize Operations Manager maps imported LDAP users to user groups after you enable "Automatically synchronize user membership for configured groups" for the lax01.rainpole.local Active Directory 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 Configure the authentication sources to enable an automatic synchronization for the **lax01.rainpole.local** Active Directory instance.

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

   b On the **Authentication Sources** page, select **lax01.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**.

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

Enable the "Define monitoring goals" option for the default policy for each vCenter Adapter instance in vRealize Operations Manager.

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 **lax01m01vc01** 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 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 B

7

After the Cloud Management Platform (CMP) is deployed in Region B, 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 Content Library in Region B

   Content libraries are container objects for VM templates, vApp templates, and other types of files. vSphere administrators can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. Sharing templates and files across multiple vCenter Server instances in same or different locations brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

2 Create Reservation Policies in Region B

   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.

3 Create Reservations for the Shared Edge and Compute Cluster in Region B

   Before members of a business group can request machines, fabric administrators 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.

4 Create Reservations for the User Edge Resources in Region B

   Before members of a business group can request virtual machines, fabric administrators must allocate 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.

5 Create Virtual Machines Using VM Templates in the Content Library in Region B

   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 Servers compute clusters you add to vRealize Automation, including the first vCenter Server compute instance.

6 Convert Virtual Machines to VM Templates in Region B

   You can convert a virtual machine directly to a template instead of making a copy by cloning.

7 Configure Single Machine Blueprints in Region B

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

8 Configure Unified Single Machine Blueprints for Cross-Region Deployment in Region B

To provision blueprints from a specific vRealize Automation deployment to multiple regions, you define the additional regions in vRealize Automation, and associate the blueprints with those locations.

Configure Content Library in Region B

Content libraries are container objects for VM templates, vApp templates, and other types of files. vSphere administrators can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. Sharing templates and files across multiple vCenter Server instances in same or different locations 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 to other vCenter Server instances, provided the HTTP(S) traffic is allowed between them.

Connect to Content Library of Region A Compute vCenter Server Instance in Region B

Synchronize templates among different Compute vCenter Server instances by connecting to the content library in Region A, so that all the templates in your environment are consistent.

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 In the **Navigator** pane, click the **sfo01-w01cl-vra01** content library that was created in the Compute vCenter Server in Region A.

4 Under**Publication**, click the **Copy Link** button.

The subscription URL is copied to the clipboard.

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

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local/ui`**.

   b Log in using the following credentials.

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

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

   The **New Content Library** wizard appears.

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

Setting	Value
Name	lax01-w01cl-vra01
vCenter Server	lax01w01vc01.lax01.rainpole.local

8 On the **Configure content library** page, select **Subscribed content library**, enter the following settings, and click **Next**.

Setting	Value
Subscription URL	*sfo01-w01cl-vra01_subscription_URL*
Enable authentication	Selected
Password	*sfo01-w01cl-vra01_password*
Download all library content immediately	Selected

9 On the **Add storage** page, click the **Select a datastore** radio button , select the **sfo01-m01-vsan01** datastore to store the content library, and click **Next**.

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

   In the **Recent Tasks** pane, a **Transfer Files** status indicates the time to finish the file transfer.

Create Reservation Policies in Region B

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. You can add multiple reservations to a reservation

policy, but a reservation can belong to only one policy. You can assign a single reservation policy to more than one blueprint. A blueprint can have only one reservation policy. 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 Policies**.

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

Setting	Value
Name	LAX-Production-Policy
Description	Reservation policy for Production Business Group in LAX

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

Setting	Value
Name	LAX-Development-Policy
Description	Reservation policy for Development Business Group in LAX

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

Setting	Value
Name	LAX-Edge-Policy
Description	Reservation policy for Tenant Edge resources in LAX

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

Before members of a business group can request machines, fabric administrators 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.

Perform this procedure twice to create compute resource reservations for both the production and development business groups.

Table 7-1. Business Group Names

Group	Name
Production	LAX01-Comp01-Prod-Res01
Development	LAX01-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 > Reservations > Reservations** and select **New > vSphere (vCenter)**.

3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for each group.

Setting	Production Group Value	Development Group Value
Name	LAX01-Comp01-Prod-Res01	LAX01-Comp01-Dev-Res01
Tenant	**rainpole**	**rainpole**
Business Group	Production	Development
Reservation Policy	LAX-Production-Policy	LAX-Development-Policy
Priority	100	100
Enable this reservation	Selected	Selected

4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.

   a Select **lax01-w01-comp01 (lax01w01vc01.lax01.rainpole.local)** from the **Compute resource** drop-down menu.

   b In the **This Reservation** column of the **Memory (GB)** table, enter **`200`**.

   c In the **Storage (GB)** table, select the check box for your primary datastore, for example, **lax01-w01-vsan01**, enter **`2000`** in the **This Reservation Reserved** text box, enter **`1`** in the **Priority** text box, and click **OK**.

   d Select **lax01-w01rp-user-vm** from the **Resource pool** drop-down menu.

5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

6 On the **Network** tab, select the following network path 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

7 Click **OK**.

8 Repeat this procedure and create a reservation for the Development Business Group.

Create Reservations for the User Edge Resources in Region B

Before members of a business group can request virtual machines, fabric administrators must allocate 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 Edge reservations for both the Production and Development business groups.

Table 7-2. Business Group Names

Group	Name
Production	LAX01-Edge01-Prod-Res01
Development	LAX01-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)**.

3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for your business group.

Setting	Production Group Value	Development Group Value
Name	LAX01-Edge01-Prod-Res01	LAX01-Edge01-Dev-Res01
Tenant	**rainpole**	**rainpole**
Business Group	Production	Development
Reservation Policy	LAX-Edge-Policy	LAX-Edge-Policy
Priority	100	100
Enable this reservation	Selected	Selected

4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.

   a Select **lax01-w01-comp01(lax01w01vc01.lax01.rainpole.local)** from the **Compute resource** drop-down menu.

   b Enter **`200`** in the **This Reservation** column of the **Memory (GB)** table.

   c In the **Storage (GB)** table, select the check box for your primary datastore, for example, **lax01-w01-vsan01**, enter **`2000`** in the **This Reservation Reserved** text box, enter **`1`** in the **Priority** text box, and click **OK**.

   d Select **lax01-w01rp-user-edge** from the **Resource pool** drop-down menu.

5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

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

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

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

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

8 Repeat the procedure to create an edge reservation for the development business group.

Create Virtual Machines Using VM Templates in the Content Library in Region B

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 Servers compute clusters you add to vRealize Automation, including the first vCenter Server compute instance.

Repeat this procedure three times for each VM Template in the content library. The following table lists the VM Templates and the guest OS each template uses to create a virtual machine.

Table 7-3. VM Templates and Their Guest Operating Systems

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://lax01w01vc01.lax01.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 **lax01w01vc01.lax01.rainpole.local** vCenter Server.

4 Right-click the **lax01-w01dc** data center and select **New Folder > New VM and Template Folder**.

5 Create a folder and label it **`VM Templates`**.

6 Navigate to **Menu > Content Libraries**.

7 Click **lax01-w01cl-vra01> Templates**.

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

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

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

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

10 Expand the **lax01-w01dc** data center, select **VM Templates** as the folder for this virtual machine, and click **Next**.

11 On the **Select a resource** page, expand cluster **lax01-w01-comp01**, select the **lax01-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 **lax01-w01-lib01** datastore and **Thin Provision** from the **Select virtual disk format** drop-down menu and click **Next**.

14 On the **Select networks** page, select **lax01-w01-vds01-management** for the **Destination Network**, and click **Next**.

Note vRealize Automation changes the network according to the blueprint configuration.

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

A new task for creating the virtual machine appears in the **Recent Tasks** pane. The new virtual machine is created after the task finishes.

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

Convert Virtual Machines to VM Templates in Region B

You can convert a virtual machine directly to a template instead of making a copy by cloning.

Repeat this procedure three times for each of the VM templates in the content library. The following table lists the VM templates and the guest OS each template uses to create a virtual machine.

Table 7-4. VM Templates and Their Guest Operating Systems

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://lax01w01vc01.lax01.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 **lax01w01vc01.lax01.rainpole.local>lax01-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** and confirm the template conversion.

Configure Single Machine Blueprints in Region B

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

Procedure

1 Create a Service Catalog in Region B

   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 B

   Create a blueprint for cloning virtual machines using the specified resources on the Compute vCenter Server. Tenants can later use this blueprint 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 Configure Entitlements of Blueprints in Region B

   You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

4 Test the Deployment of a Single Machine Blueprint in Region B

   Test your environment and confirm the successful provisioning of virtual machines using the blueprints that have been created. 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 B

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 Navigate to **Administration > Catalog Management > Services > New**.

3 In the **New Service** page, configure the following settings and click **OK**.

Setting	Value
Name	LAX Service Catalog
Description	Default setting (blank)
Icon	Default setting (blank)
Status	Active
Hours	Default setting (blank)
Owner	Default setting (blank)
Support Team	Default setting (blank)
Change Window	Default setting (blank)

Create a Single Machine Blueprint in Region B

Create a blueprint for cloning virtual machines using the specified resources on the Compute vCenter Server. Tenants can later use this blueprint 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 three blueprints.

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2012 R2 - LAX Prod	windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)	**os-windows-joindomain-custom-spec**	LAX-Production-Policy
Windows Server 2012 R2 With SQL2012 - LAX Prod	windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)	**os-windows-joindomain-custom-spec**	LAX-Production-Policy
Redhat Enterprise Linux 6 - LAX Prod	redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)	**os-linux-custom-spec**	LAX-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 **Infrastructure > Compute Resources > Compute Resources**.

3 In the **Name** column, point to the compute cluster **lax01-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 **Design > Blueprints > New**.

7 In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - LAX Prod
Deployment limit	Default setting (blank)
Lease (days): Minimum	30
Lease (days): Maximum	270
Archive (days)	15

8 Select and drag the **vSphere (vCenter) Machine** icon to the **Design Canvas**.

9 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	LAX-Production-Policy
Machine prefix	Use group default
Instances: Minimum	Default setting
Instances: Maximum	Default setting

10 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	Name: windows-2012r2-64 Endpoint: lax01w01vc01.lax01.rainpole.local
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 **lax01-w01-comp01** Compute Resource.

11 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	2	4
Memory (MB)	4096	16384
Storage (GB)	Default setting	Default setting

12 In the **Categories** section of the page, select **Network & Security** to display the list of available network and security components.

a Select the **Existing Network** component, drag it onto the **Design Canvas** and click the **Existing network** component from design canvas.

b Under the **General** tab, click the browse icon and select the **Ext-Net-Profile-Production-Web** network profile and click **Save**.

Blueprint Name	Existing network
Windows Server 2012 R2 - LAX Prod	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 With SQL2012 - LAX Prod	Ext-Net-Profile-Production-DB
Redhat Enterprise Linux 6 - LAX Prod	Ext-Net-Profile-Production-App

c Select the **vSphere_vCenter_Machine_1** properties from the design canvas.

d Select the **Network** tab, click **New**, configure the following settings, and click **OK**.

Network	Assignment Type	Address
ExtNetProfileProductionWeb	Static IP	Default setting (blank)
ExtNetProfileProductionDB	Static IP	Default setting (blank)
ExtNetProfileProductionApp	Static IP	Default setting (blank)

e Click **Finish** to save the blueprint.

13 Select the blueprint **Windows Server 2012 R2 - LAX Prod** and click **Publish**.

Configure Entitlements of Blueprints in Region B

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 three blueprints with their entitlement.

Blueprint Name	Service Catalog	Add to Entitlement.
Windows Server 2012 R2 - LAX Prod	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Prod	LAX Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Prod	LAX 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 Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.

3 On the **Catalog Items** pane, select the **Windows Server 2012 R2 - LAX Prod** blueprint in the **Catalog Items** list and click **Configure**.

4 On the **General** tab of the **Configure Catalog Item** dialog box, select **LAX 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 and add the **Windows Server 2012 R2 - LAX Prod** blueprint to the **Entitled Items** list.

   c Click **Finish**.

6 Repeat this procedure to associate all the blueprints with their entitlement.

Test the Deployment of a Single Machine Blueprint in Region B

Test your environment and confirm the successful provisioning of virtual machines using the blueprints that have been created. 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 select **LAX Service Catalog** from the catalog of available services.

3 Click the **Request** button for the **Windows Server 2012 R2 - LAX Prod** blueprint 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 complete.

     Click the **Refresh** icon after a few minutes until a `Successful` message appears.

   c Under **Status**, verify that the virtual machine is successfully provisioned.

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/ui`**.

   b Log in using the following credentials.

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

6 Verify that the virtual machine provisions in the shared edge and compute cluster.

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

   b In the **Navigator** pane, navigate to **lax01w01vc01.lax01.rainpole.local > lax01-w01-comp01 > lax01-w01rp-user-vm**, and verify that the virtual machine exists.

Configure Unified Single Machine Blueprints for Cross-Region Deployment in Region B

To provision blueprints from a specific vRealize Automation deployment to multiple regions, you define the additional regions in vRealize Automation, and associate the blueprints with those locations.

Procedure

1 Add Data Center Locations to the Compute Resource Menu

   You can configure new data center locations and resources in the Compute Resource menu of the vRealize Automation deployment selection screen, allowing you to more easily select new compute resources for deployment. To add a new location to the Compute Resource menu, you edit an XML file on the vRealize Automation server.

2 Associate Compute Resources with a Location in Region B

   Each data center location has its own compute resources, which you associate with that site for its dedicated use.

3 Add a Property Group and a Property Definition for Data Center Location in Region B

   Property definitions let you more easily control which location to deploy a blueprint, and based on that choice, which storage and network resources to use with that blueprint.

4 Create a Reservation Policy for the Unified Blueprint in Region B

   When you as a tenant administrator and business group manager create a blueprint, the option to add a reservation policy becomes available. To add a reservation policy to an existing blueprint, you must edit the blueprint.

5 Specify Reservation Information for the Unified Blueprint in Region B

   Each reservation is configured for a specific business group to grant them access to request specific physical machines.

6 Create a Service Catalog for the Unified Blueprint in Region B

The service catalog provides a common interface for consumers of IT services to request and manage the services and resources they need. Users can browse the catalog to request services, track their requests, and manage their provisioned service items.

7 Create an Entitlement for the Unified Blueprint Catalog in Region B

Entitle all blueprints in the Unified Blueprint Catalog to the Production business group. Entitlements determine which users and groups can request specific catalog items or perform specific actions. Entitlements are specific to a business group, and allow users in different business groups to access the blueprint catalog.

8 Create Unified Single Machine Blueprints in Region B

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. Create three blueprints from which to clone the virtual machine for your environment using pre-configured resources on the vCenter Server compute cluster in both Region A and Region B. Tenants use these blueprints to provision virtual machines automatically.

9 Test the Cross-Region Deployment of the Single Machine Blueprints in Region B

The data center environment is now ready for the multi-site deployment of virtual machines using vRealize Automation. Test your environment and confirm the successful provisioning of virtual machines using the blueprints you created to both Region A and Region B.

Add Data Center Locations to the Compute Resource Menu

You can configure new data center locations and resources in the Compute Resource menu of the vRealize Automation deployment selection screen, allowing you to more easily select new compute resources for deployment. To add a new location to the Compute Resource menu, you edit an XML file on the vRealize Automation server.

Perform this procedure for both vra01iws01a and vra01iws01b IaaS Web server virtual machines.

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 Open a VM console to the IaaS Web server virtual machine vra01iws01a, and log in using administrator credentials.

3 Add the data centers for the two regions of the SDDC.

   a Open the `C:\Program Files (x86)\VMware\VCAC\Server\Website\XmlData\DataCenterLocations.xml` file in a text editor.

   b Update the `Data Name` and `Description` attributes to use the following settings.

Data Name	Description
SFO	San Francisco data center
LAX	Los Angeles data center

   c Save and close the file.

4 Restart the vra01iws01a virtual machine.

   Wait until the virtual machine restarts and is successfully running.

5 Repeat this procedure for the vra01iws01b virtual machine.

Associate Compute Resources with a Location in Region B

Each data center location has its own compute resources, which you associate with that site for its dedicated use.

Repeat this procedure two times, for each vCenter Server compute cluster and region.

Location	vCenter Server Compute Cluster
SFO	sfo01-w01-comp01
LAX	lax01-w01-comp01

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 Select the **sfo01-w01-comp01** compute resource and click **Edit**.

4 From the **Location** drop-down menu, select the **SFO** data center location for sfo01-w01-comp01.

5 Click **OK**.

6 Repeat this procedure and set the data center location for lax01-w01-comp01.

Add a Property Group and a Property Definition for Data Center Location in Region B

Property definitions let you more easily control which location to deploy a blueprint, and based on that choice, which storage and network resources to use with that blueprint.

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 > Property Dictionary > Property Definitions**.

3 Click **New** and create a property definition.

a Enter **`Vrm.DataCenter.Location`** in the **Name** text box.

Note The property definition name is case-sensitive, and must exactly match the property name used in the blueprint or the build profile.

b Enter **`Select a Region`** in the **Label** text box.

c In the **Visibility** section, select the **All tenants** radio button and specify to which tenant the property is available.

d (Optional) Enter a property description in the **Description** text box.

Describe the intent of the property and any information that might help the consumer best use the property.

e Leave default setting for **Display order**.

f Select **String** from the **Data type** drop-down menu.

g Select **Yes** from the **Required** drop-down menu.

h Select **Dropdown** from the **Display as** drop-down menu.

i Select the **Static list** radio button for **Values**.

j Deselect **Enable custom value entry**.

k Click **New** in the **Static list** area and enter a property name and value from the following table.

Name	Value
San Francisco	SFO
Los Angeles	LAX

l Click **OK** and save both predefined values.

m Click **OK** and save the property definition.

The property is created and available on the **Property Definitions** page.

4 Navigate to **Administration > Property Dictionary > Property Groups**, and click **New**.

5 Enter `Select Location` in the **Name** text box.

6 The **ID** text box is populated with the same value, after you enter the **Name** value.

7 In the **Visibility** section, select the **All tenants** radio button and specify with which tenant the property is to be available.

8 (Optional) Enter a description of the property group.

9 Add a property to the group by using the **Properties** box.

a Click **New** and enter the following settings.

Setting	Value
Name	Vrm.DataCenter.Location
Encrypted	Deselected
Show in Request	Selected

b Click **OK** and add the property to the group.

10 Click **OK** and save the property group.

Create a Reservation Policy for the Unified Blueprint in Region B

When you as a tenant administrator and business group manager create a blueprint, the option to add a reservation policy becomes available. To add a reservation policy to an existing blueprint, you must edit the blueprint.

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**.

   a Click **New**.

   b Type **`UnifiedBlueprint-Policy`** in the **Name** text box.

   c Select **Reservation Policy** from the **Type** drop-down menu.

   d Type **`Reservation policy for Unified Blueprint`** in the **Description** text box.

   e Click **OK**.

Specify Reservation Information for the Unified Blueprint in Region B

Each reservation is configured for a specific business group to grant them access to request specific physical machines.

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

Repeat this procedure twice to create reservations for the production business group on the shared edge and compute clusters in both Region A and Region B.

Region	Business Group	Reservation Name	Reservation Policy	Compute Resource.
Region A	Production	SFO01-Comp01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	sfo01-w01-comp01(sfo01w01vc01.sfo01.rainpole.local)
Region B	Production	LAX01-Comp01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	lax01-w01-comp01(lax01w01vc01.lax01.rainpole.local)

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)**.

3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values.

Setting	Production Business Group Value
Name	SFO01-Comp01-Prod-UnifiedBlueprint
Tenant	**rainpole**
Business Group	Production
Reservation Policy	UnifiedBlueprint-Policy
Priority	100
Enable This Reservation	Selected

4 On the **New Reservation - vSphere** page, click the **Resources** tab.

   a Select **sfo01-w01-comp01(sfo01w01vc01.sfo01.rainpole.local)** from the **Compute Resource** drop-down menu.

   b Enter **`200`** in the **This Reservation** column of the **Memory (GB)** table.

   c In the **Storage (GB)** table, select your primary datastore, for example, **sfo01-w01-vsan01**, enter **`2000`** in the **This Reservation Reserved** text box, enter **`1`** in the **Priority** text box, and click **OK**.

   d Select **sfo01-w01rp-user-vm** from the **Resource Pool** drop-down menu.

5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

6 Select the following network path check boxes and select the corresponding network profiles for the Production business group whose reservation you are configuring.

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

7 Click **OK** and save the reservation.

8 Repeat the procedure and create a reservation for Region B.

Create a Service Catalog for the Unified Blueprint in Region B

The service catalog provides a common interface for consumers of IT services to request and manage the services and resources they need. Users can browse the catalog to request services, track their requests, and manage their provisioned service items.

After the service catalog is created, business group managers can create entitlements for services, catalog items, and resource actions to groups of users. The entitlement allows members of a particular business group, for example, the production business group, to use the blueprint. Without an entitlement, users cannot use the blueprint.

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 > Catalog Management > Services**.

3 Click **New**.

   a In the **New Service** dialog box, enter **`Unified Single Machine Catalog`** in the **Name** text box.

   b Select **Active** from the **Status** drop-down menu.

   c Click **OK**.

Create an Entitlement for the Unified Blueprint Catalog in Region B

Entitle all blueprints in the Unified Blueprint Catalog to the Production business group. Entitlements determine which users and groups can request specific catalog items or perform specific actions. Entitlements are specific to a business group, and allow users in different business groups to access the blueprint catalog.

Perform this procedure and associate the Unified Blueprint Catalog with the Prod-SingleVM-Entitlement 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 Associate the **Unified Blueprint Catalog** with the **Prod-SingleVM-Entitlement entitlement** that you created earlier.

   a Navigate to **Administration > Catalog Management > Entitlements**.

   b Click **Prod-SingleVM-Entitlement**.

   The **Edit Entitlement** window appears.

   c Select the **Items & Approvals** tab.

   d Navigate to **Entitled Services** and click the **Add** icon.

   e Select the box next to **Unified Single Machine Catalog** and click **OK**.

   f Click **Finish** and save your changes.

Create Unified Single Machine Blueprints in Region B

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. Create three blueprints from which to clone the virtual machine for your environment using pre-configured resources on the vCenter Server compute cluster in both Region A and Region B. Tenants use these blueprints to provision virtual machines automatically.

Repeat this procedure and create the following three Unified Single Machine blueprints.

Blueprint Name	VM Template	Reservation Policy	Customization Specification	Service Catalog
Windows Server 2012 R2 - Unified Prod	windows-2012r2-64 (sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	**os-windows-joindomain-custom-spec**	Unified Single Machine Catalog
Windows Server 2012 R2 With SQL2012 - Unified Prod	windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	**os-windows-joindomain-custom-spec**	Unified Single Machine Catalog
Redhat Enterprise Linux 6 - Unified Prod	redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	**os-linux-custom-spec**	Unified Single Machine Catalog

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 > New**.

3 In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - Unified Prod
Deployment limit	Default setting (blank)
Lease (days): Minimum	30
Lease (days): Maximum	270
Archive (days)	15

4 Select and drag the **vSphere (vCenter) Machine** icon to the Design Canvas.

5 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Value
ID	Default setting (vSphere_vCenter_Machine_1)
Reservation Policy	UnifiedBlueprint-Policy
Machine Prefix	Use group default

Setting	Value
Instances: Minimum	Default setting
Instances: Maximum	Default setting

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**

7 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	1	4
Memory (MB)	4096	16384
Storage (GB)	Default setting	Default setting

8 Click the **Network** tab.

a Select **Network & Security** in the **Categories** section and display the list of available network and security components.

b Select the **Existing Network** component and drag it onto the design canvas.

c Click in the **Existing network** component in the Design Canvas, click the **Browse** icon, and select the **Ext-Net-Profile-Production-Web** network profile under **General** tab.

Blueprint Name	Existing Network
Windows Server 2012 R2 - Unified Prod	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 With SQL2012 - Unified Prod	Ext-Net-Profile-Production-DB
Redhat Enterprise Linux 6 - Unified Prod	Ext-Net-Profile-Production-App

d Click **Save**.

e Select the **vSphere_Machine** properties from the design canvas.

f Click the **Network** tab, click **New**, configure the following settings, and click **OK**.

Setting	Value
Network	ExtNetProfileProductionWeb
Assignment Type	Static IP
Address	Default setting (blank)

9 Click the **Properties** tab.

   a Click **Add** on the **Property Groups** tab.

   b Select the property group **Select Location** and click **OK**.

10 Click **OK**.

11 Click **Finish** and save the blueprint.

12 Select the blueprint **Windows Server 2012 R2 - Unified** and click **Publish**.

13 Navigate to **Administration > Catalog Management > Catalog Items** and add the blueprint to the **Unified Single Machine Catalog**.

   a In the **Catalog Items** list, click the blueprint labeled **Windows Server 2012 R2 - Unified**.

   b In the **Configure Catalog Item** dialog box, set **Service** to **Unified Single Machine Catalog**, and click **OK**.

Test the Cross-Region Deployment of the Single Machine Blueprints in Region B

The data center environment is now ready for the multi-site deployment of virtual machines using vRealize Automation. Test your environment and confirm the successful provisioning of virtual machines using the blueprints you created to both Region A and Region B.

Repeat this procedure twice and provision virtual machines in both the Region A and Region B Compute vCenter Server instances.

Region	Compute vCenter Server.
San Francisco	sfo01w01vc01.sfo01.rainpole.local
Los Angeles	lax01w01vc01.lax01.rainpole.local

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 Select the **Catalog** tab, click **Click here to apply filters**, and click **Unified Single Machine Catalog** from the catalog of available services.

3 Click the **Request** button for one of the blueprints.

4 Select **vSphere_vCenter_Machine_1**.

5 Select **San Francisco** from the **Select a Region** drop-down menu, and click **Submit**.

6 Click **Submit**.

7 Verify the request finishes successfully.

   a Select the **Deployments** tab.

   b Select the deployment that you submitted, click **History**, and wait several minutes for the request to complete.

   Click the **Refresh** icon every few minutes until a `Successful` message appears.

   c Under **Status**, verify that the virtual machine successfully provisioned.

8 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*

9 Verify the virtual machine provisions in the Region A vCenter Server compute cluster.

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

   b In the **Navigator** pane, navigate to **sfo01w01vc01.sfo01.rainpole.local>**, **sfo01-w01dc> VRM** and verify the existence of the virtual machine.

10 Repeat this procedure for Region B.

   a Provision virtual machines to the Region B vCenter Server compute cluster.

   b Verify that the request finishes successfully and that the virtual machine is provisioned in the Region B vCenter Server compute cluster.

You have successfully performed a cross-region deployment of vRealize Automation single machine blueprints, provisioning virtual machines in both Region A and Region B.