Dell EMC VxRail Appliance

Cloud Builder Deployment Guide for VVD Version 5.1.1 in Region B

Abstract

This deployment guide provides detailed instructions for installing, configuring, and operating a software-defined data center (SDDC) for Cloud Builder on VxRail. It is based on the VMware Validated Design 5.1.1.

January 2020

H18098

Table of contents

1 About VMware Validated Design Deployment

The *VMware Validated Design Deployment* on VxRail documentation provides step-by-step instructions for installing, configuring, and operating a software-defined data center (SDDC) on the Dell EMC VxRail Hyperconverged Infrastructure platform. This document is based on the VMware Validated Design (VVD) for SDDC, using VxRail infrastructure and the VVD Cloud Builder to automate the implementation of Region B.

This document is focused on deployment of the SDDC. Post-deployment tasks for tenant customization depend on customer requirements, therefore, this document does not contain step-by-step instructions for performing all required post-configuration tasks.

1.1 Intended audience

The VVD of Region B Deployment Guide is intended for cloud architects, infrastructure administrators, and cloud administrators familiar with VxRail and VMware software, and interested in deploying an SDDC on Dell EMC VxRail infrastructure.

1.2 Required VMware software

The VVD of Region B Deployment Guide is compliant and validated with certain product versions. See the *VMware Validated Design v5.1 Planning Guide* and *Release Notes* for more information about supported product versions.

1.3 Required VxRail software

VVD 5.1.1 was qualified using VxRail 4.7.410. It is supported in the 4.7.4xx releases of VxRail.

What's changed:

VxRail supports a Domain Join option to federate SSO across both Regions during Region B bring-up.

1.4 Before you apply this guidance

The sequence of the documentation of VVD follows the stages for implementing and maintaining an SDDC. See Documentation Map for VMware Validated Design.

To use VVD in Region B, you must be familiar with the following:

- VxRail Installation and Administration
- VVD Architecture and Design
- VVD Planning and Preparation
- VVD Deployment of Region A

2 Hardware Requirements

To implement the SDDC from this VVD, your hardware must meet the requirements listed in this section.

2.1 Management Workload Domain

When implementing a dual-region SDDC, the management workload domain in each region contains a management cluster which must meet the following hardware requirements.

Table 1 **Hardware Requirements for the Management Cluster**

Component	Requirement per Region
VxRail Nodes	Minimum of 4 VxRail Nodes. Supported Models are E, P, and G Series. Recommend E or P for this Domain.
CPU per server	Dual-socket, 8 cores per socket
Memory per server	256 GB*
Storage per server	16 GB SSD for booting One 400 GB SSD for the caching tier – Class D Endurance – Class E Performance Two 1 TB HDD for the capacity tier – 10K RPM See Designing and Sizing a vSAN Cluster from the VMware vSAN documentation for guidelines about cache sizing.
NICs per server	– Two 10 GbE or two 26 GbE NICs – One 1 GbE BMC NIC

*Note: VMware 5.1 guidance states that the minimum memory requirement for Management nodes is 256 GB which is intended to support new features in future releases.

VxRail Dell Nodes have six memory slots which should be configured symmetrically to maximize performance. The minimum requirement of 192 GB is supported; however, 384 GB will be recommended in future releases.

2.2 Virtual Infrastructure Workload Domain

When implementing a dual-region, the virtual infrastructure workload domain contains a shared edge and compute cluster which must meet the following requirements.

Table 2 **Hardware Requirements for the Shared Edge and Compute Cluster**

Component	Requirement per Region
Servers	Minimum of four VxRail Nodes. Recommend E- or P- Series for Compute Cluster.
CPU, memory, and storage per server	Supported configurations

Component	Requirement per Region
NICs per server	Two 10 GbE or 25 GbE NICs One 1 GbE BMC NIC

For information about supported servers, CPU, storage, I/O devices, and so on, see the Dell EMC VxRail hardware information in the VMware Compatibility Guide.

Note: When scaling compute-only VVD clusters, ensure that each new VxRail node contains the same hardware profile as the existing nodes in the cluster.

3 Known issues within this release

This VVD Region B deployment on VxRail document is certified and updated with each release of the product, or when necessary.

Setting VM priority mappings for recovery plan in SRM might fail

Assignment of VM priority within SRM Recovery Plan fails intermittently. This is reflected in the UI by the task name and also within the `vcf-bringup-debug.log` file with a message similar to the following:

```
ERROR [0000000000000000,0000]
[c.v.e.s.o.model.error.ErrorFactory,threadPoolExecutor-4] [E9J7R5]
CONFIGURE_VM_PRIORITIES_FAILED Configuration for VM priorities for SRM
172.16.64.22 failed
```

Workaround:

1. Log in to the SRM Management UI with an administrative account.
2. Select the **Recovery Plan** tab and open the **SDDC Cloud Management** RP (Recovery Plan).
3. Confirm that the VM startup priority for each VM matches the following table.

Table 3 **SDDC Cloud Management VM Startup Priority**

VM Name	Priority
vra01svr01a	2
vra01svr01b	2
vra01svr01c	2
vra01iws01a	3
vra01iws01b	3
vra01ims01a	4
vra01ims01b	4
vra01dem01a	5
vra01dem01b	5

4. Select the **Recovery Plan** tab and open the **SDDC Operations Management** RP.
5. Confirm that the startup priority for each VM matches the following table.

Table 4 **SDDC Operations Management VM Startup Priority**

VM Name	Priority
vrops01svr01a	1
vrops01svr01a	2
vrops01svr01a	3
vrs01lcm01	4

6. Open the Active Cloud Build deployment and select **Retry** to restart the task.
7. Confirm that Cloud Builder completes the task successfully.

Deployment of the Region B Workload Domain sets the host security profile to Lockdown Mode.

Lockdown mode prevents VxRail PT Agent and other services from communicating to the host. Follow the Post-Deployment task to disable Lockdown mode on all of the VxRail hosts.

4 VVD Region B Deployment Flow

The flowchart in Figure 1 illustrates the high-level deployment tasks required for the deployment of the VxRail clusters for the Cloud Builder automated SDDC deployment.

Preparation for the deployment requires the creation of two VxRail clusters in the Region B environment. Similar to Region A, there is an embedded VxRail cluster which includes an integrated vCenter and Platform services controller, and a second VxRail cluster which is deployed to a vCenter instance that is hosted in the Management cluster.

In order to federate the SSO domain, we must join the PSC in Region B to Region A. That task is automated through the VxRail Manager initialization utility.

The Region B workload domain PSC is deployed into that management domain, and joined to the SSO domain, through the Region A workload domain PSC. In this way, we establish a daisy-chain deployment of PSC. After the cloud builder deployment is completed, each PSC is configured with multiple partners for redundant replication.

The workload vCenter is deployed to support the second VxRail cluster for the Region B workload domain. The vCenter deployment can be performed using the CLI on the Cloud Builder VM, or from the or the UI installer from the vCenter ISO which is included in the Cloud Builder software bundle.

Once the base configuration has been established, the vCenter servers are repointed to the Region B load balanced address for fault tolerance.

Completion of the Phase 1 tasks establishes the foundation for the Cloud Builder Region B deployment.

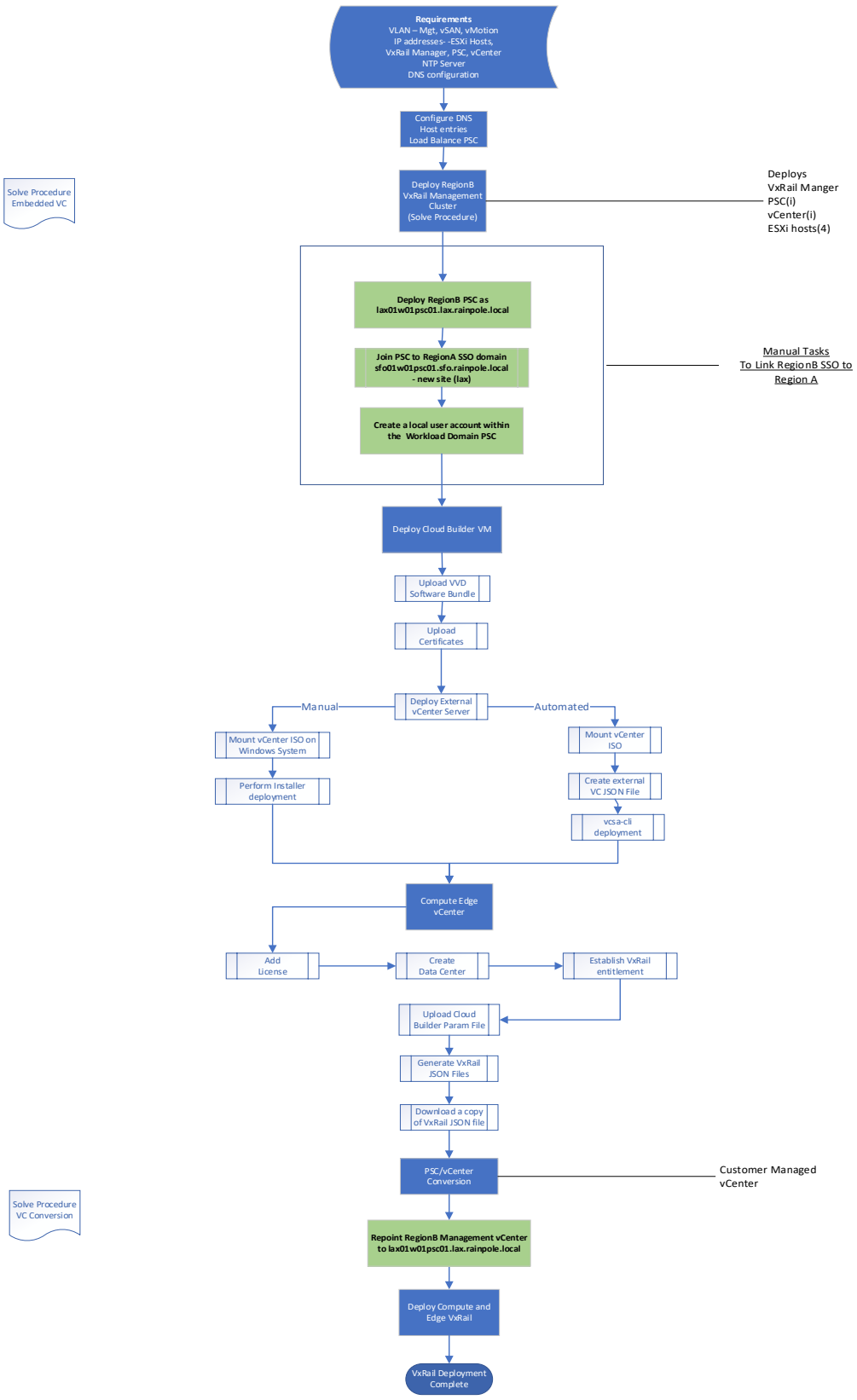


Figure 1. VxRail Cluster Deployment for Region B

4.1 Preparation for Cloud Builder

The following Region B dependencies must be established before proceeding to the Cloud builder validation and deployment.

- Cloud Builder requires SSH access to all ESXi Hosts, therefore enable SSH on all hosts.
- A Windows 2016 virtual machine template is required for the IaaS components of the deployment. Details on the configuration of the template are listed within this document.
- The Cloud Builder parameter file must be completed and validated. Since the deployment is dependent on properties defined within the file, the properties should also be validated.

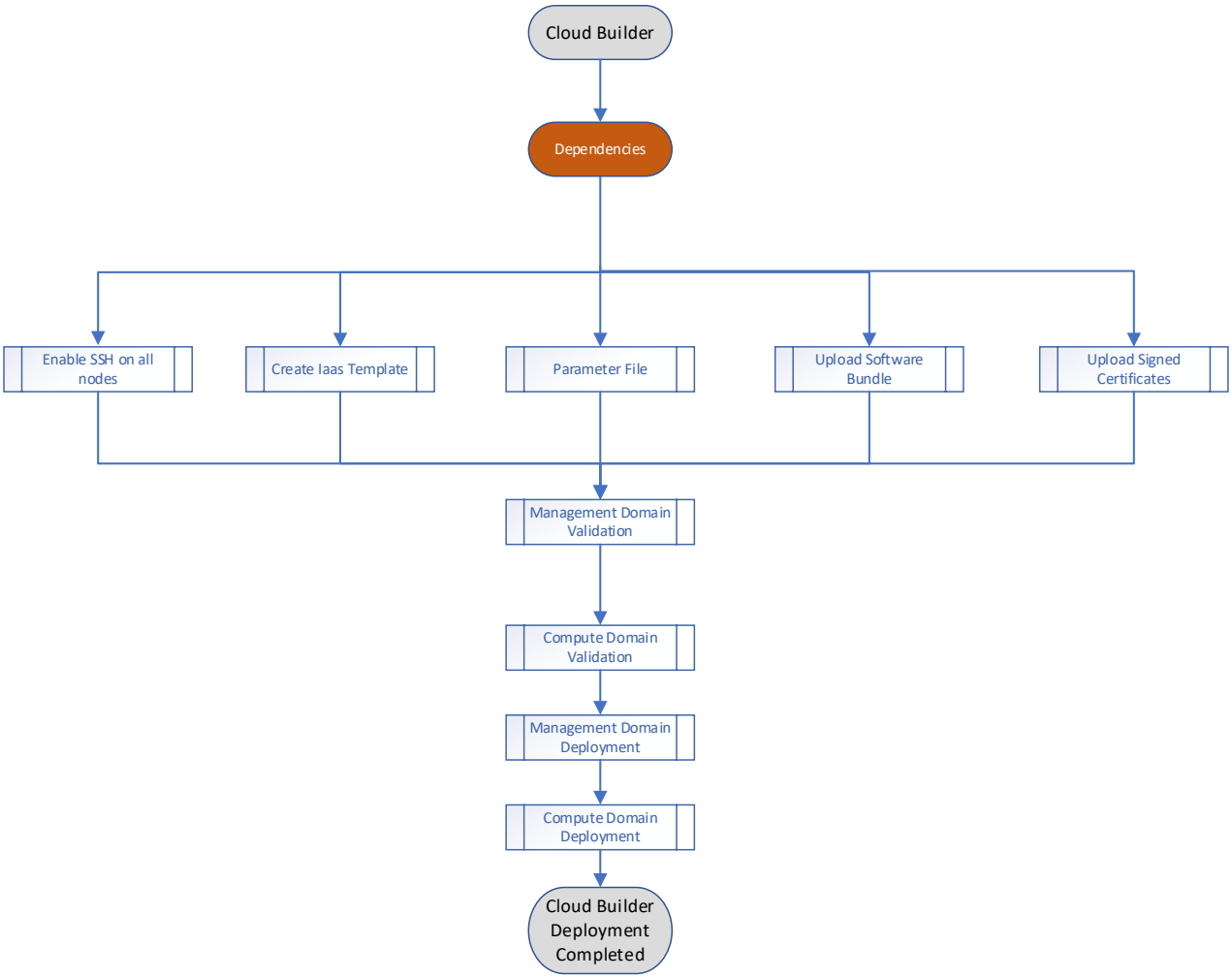


Figure 2. Cloud Builder Dependencies

4.2 vRealize automation post-deployment tasks

Finalize the deployment by setting the monitoring policies, and configuring the vRealize tenant and service catalog to verify that the environment is functional.

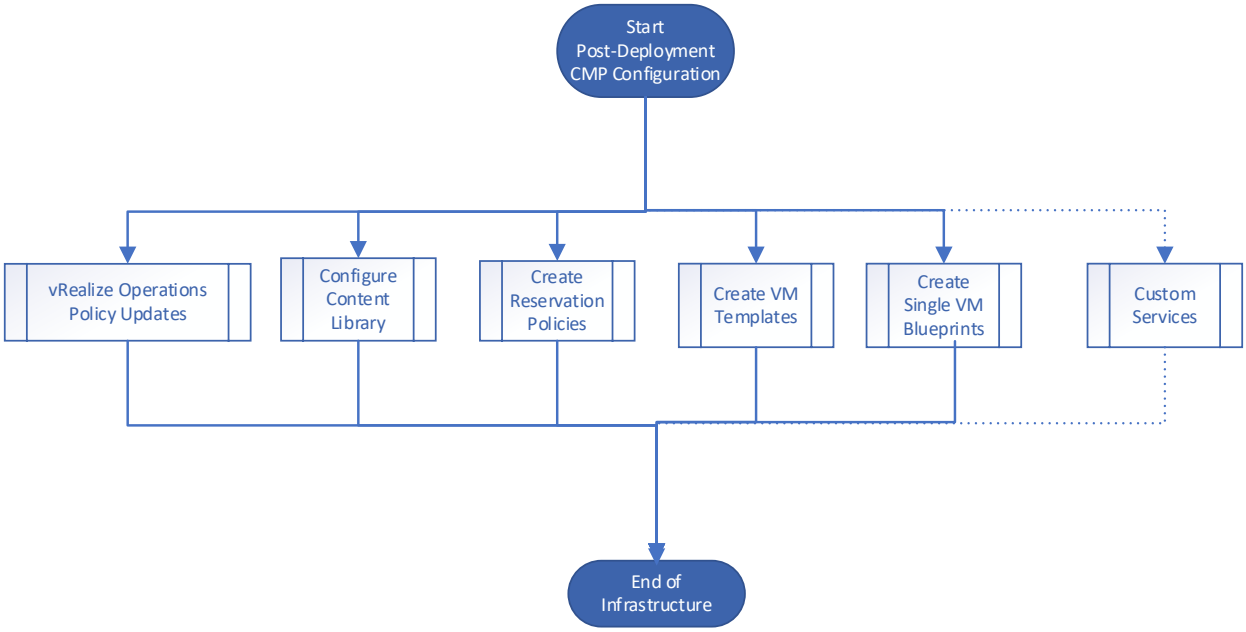


Figure 3. Post-Deployment Tasks

5 Prepare the Environment for Automated Deployment

Prepare the environment for automated deployment before you start the automated SDDC deployment. Verify that your environment fulfills the requirements listed in the following section. Prepare each layer of the SDDC by deploying and configuring the necessary infrastructure, operational, and management components.

5.1 Prerequisites for automated SDDC deployment

Table 5 **Automated SDDC Deployment Prerequisites**

Prerequisite	Value
Environment	Verify that your environment is configured for deployment of the SDDC. See Prepare the Environment for 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 is configured with VxRail and SDDC entries within the root and child domains.
NTP Services	Verify that two external 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 VVD to your local file system.

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

5.2 Pre-deployment assessment and data collection preparation

The SDDC deployment is dependent on established network services and configuration. A seamless deployment depends upon reliable and verified environmental details.

There are two documents which are used to capture details for the deployment:

- Dell *EMC Pre-Engagement Questionnaire* (PEQ) - provides a documentation tool to collect details for the VxRail deployment.

  The purpose of this document is to prepare the environment for the VxRail cluster deployment. It includes sections for environmental readiness as well as cluster configuration details. This document is familiar to the VxRail delivery team and used to plan the deployment with the customers and ensure that requirements are communicated and verified prior to the VxRail cluster deployment. The document is available from Solve.emc.com.

- *VMware Cloud Builder Deployment Parameters spreadsheet* - captures the configuration details for the SDDC deployment.

  The VVD parameter document is provided to gather details about the entire SDDC environment. It is used as the source file for the cloud builder deployment. The document is the definition file for the cloud builder deployment. Properties and services defined within this file govern the delivery of the SDDC deployment. This information might overlap information gathered by the PEQ, so it is important to review and familiarize yourself with both documents.

The parameter file and additional details on the values are available at the following URL: https://docs.vmware.com/en/VMware-Validated-Design/5.0/com.vmware.vvd.sddc-plan.doc/GUID-C4AC2482-98B2-4050-BB81-A6FE3D0F15ED.html

Note: Parameter files are version-dependent. Ensure you are using the VVD 5.1.1 version of the document to be consistent with the VVD 5.1.1 version of Cloud Builder.

5.2.1 Procedure

1. Obtain the relevant documents from SolVe and the VMware website or Cloud Builder.
2. Thoroughly complete the documents and verify the details of the user accounts, DNS entries, and network configuration contained within the file.
3. Get help with the review.

   These documents should be completed prior to delivery. The ISBU and Dell EMC are available to review the documents prior to the engagement.

5.3 Configure DNS settings

Confirm that all DNS entries for SDDC and VxRail have been added to the DNS servers prior to the engagement. A list of systems and addresses are included in the Networks and Deployment tabs of the parameter file.

5.3.1 Perform the DNS configuration for the Platform Services load balancer

Configure the DNS load balancer record to emulate the NSX-V load balancer.

5.3.2 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 6 **Platform Services Controller Load Balancer and Management Cluster Settings**

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

5.3.3 Procedure

1. Log in to the `dc01rpl.rainpole.local` DNS server.
2. Open the Windows Start menu and enter `dnsmgmt.msc` in the Search bar. Press **Enter**.

   The **DNS Manager** dialog box opens.
3. Create an A record for the Platform Services Controller Load Balancer Name VIP.
   a In the **DNS Manager** dialog 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**.

Table 7 **Forward Lookup Zone Settings**

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

Note: 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**.

Table 8 **New Pointer Settings**

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

5.4 Generate certificates for the SDDC components

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

Use the Certificate Generation Utility for VVD (`CertGenVVD`) to create certificate configuration files based on the Deployment Parameters file for Region A. The files are used to generate new certificates signed by the Microsoft certificate authority (MSCA) for all management products.

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 VVD Certificate Generation Utility, see VMware Knowledge Base article 2146215.

5.4.1 Prerequisites for generating signed certificates for the SDDC components

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

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

Table 9 **Signed Certificate Prerequisites**

Prerequisite	Value
Active Directory	• The Certificate Authority Service and the Certificate Authority Web Enrolment roles are installed and configured on the Active Directory Server. • A new Microsoft Certificate Authority template is created and enabled. • Use a hashing algorithm of SHA-256 or higher on the certificate authority. • 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.

5.4.2 Create and add a Microsoft Certificate Authority template

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

Create and configure the VMware CA 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.

5.4.3 Procedure

1. Log in to the Active Directory server using a Remote Desktop Protocol (RDP) client with username ***Active Directory administrator*** and 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**.

5.5 Generate signed certificates for the SDDC components

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

5.5.1 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.

Table 10 **Default Settings**

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`.

6 Deploy VxRail Clusters for Management and Shared Edge/Compute Domain

To prepare for the SDDC environment, two VxRail Clusters are deployed:

- A management cluster for the SDDC cloud management services, vCenter services, NSX managers, and the cloud builder virtual appliance
- A shared edge and compute cluster that hosts the NSX controllers, edge services, and workload domain virtual machines.

The first VxRail cluster establishes the foundation for the SDDC environment. It supports the Management domain where all of the core infrastructure services and are deployed. It also provides the services for federation of the Single Sign On (SSO) domain across both SDDC regions. VxRail version 4.7.300 and later include the ability to join an SSO domain during first run. That feature is used to federate the SSO domain and identity across domains during the Region B deployment. The VxRail Management cluster is deployed using the embedded services procedure. The resulting cluster hosts the platform services controller and vCenter instance which manage its resources.

Those services will be converted from VxRail-managed to customer-managed after the initialization is completed. Once converted, the vCenter and PSC are no longer managed or included in the VxRail Manager Lifecycle Management processes.

A second instance of vCenter and PSC is deployed within the Management vCenter for the Shared Edge and Compute cluster management. The Platform Services controllers are federated and abstracted through an NSX load balancer.

Network services, DNS, and NTP must be configured prior to performing this task.

6.1 Prerequisites for installation of VxRail clusters

The VxRail Clusters provide the infrastructure for the SDDC deployment. Prepare for the installation and configuration of each cluster by performing the PEQ for the VxRail environment.

The PEQ process captures all service information and configuration details of the environment and is used to validate that the environment is prepared for the VxRail deployment.

The installation requires a system connected to the network with a supported web client, and remote connectivity tools for RDP, SSH and SCP.

The VxRail Clusters are deployed in a specific order, meaning the Management Cluster must be deployed first and configured with the necessary services to support the deployment of the second cluster.

6.1.1 Before you start

- Make sure that you have a Windows host with access to your data center. Use this support host to connect to the SDDC environment to perform the 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.

6.1.2 IP addresses, hostnames, and network configuration

The following values are required to configure your hosts.

Table 11 **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.sfo1.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

6.2 Install and configure the management domain VxRail

VxRail Manager provides automated deployment to initialize a cluster for the VVD environment. The cluster initialization configures ESXi Hosts, PSC, vCenter, vDS, and vSAN to accelerate the SDDC deployment. The detailed steps are included in the VxRail Initialization SolVe procedure on the Dell EMC support site.

Note: This VxRail cluster will use the Domain JOIN feature to join the PSC within the VxRail Management domain to the existing SSO domain in the Region A environment

Reference the details in the pre-deployment qualification (PEQ) assessment. Work with the customer to obtain the details to complete the VxRail deployment.

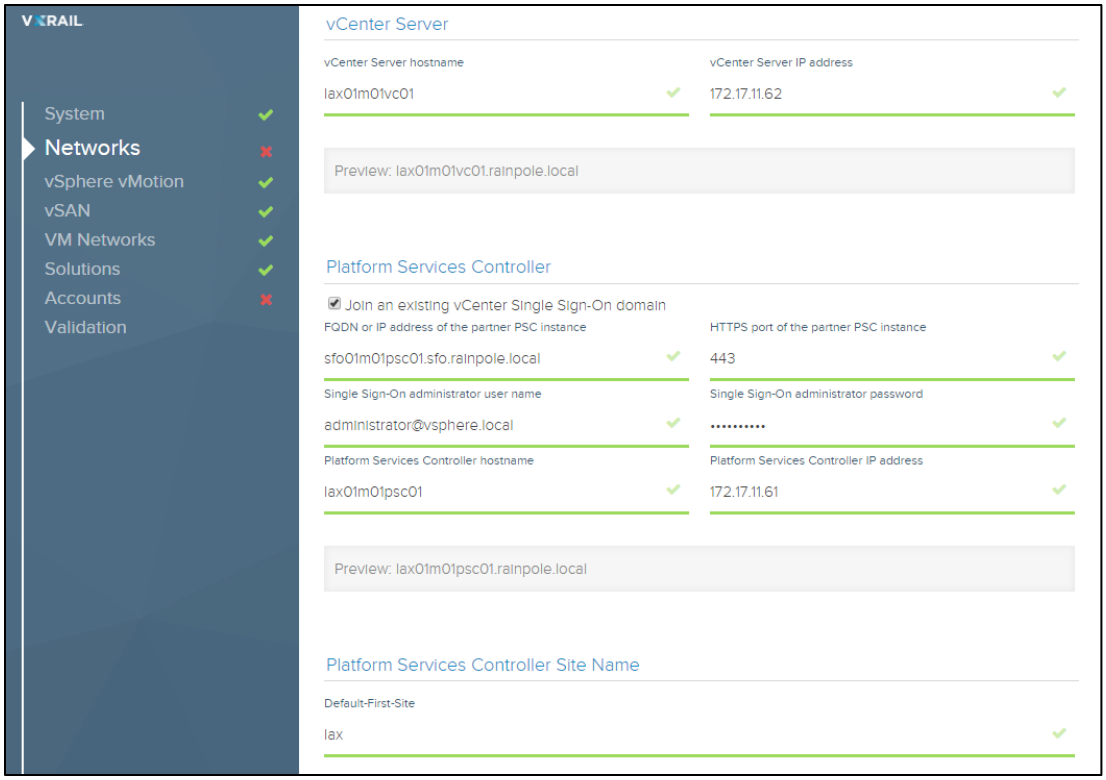
1. Download the current VxRail SolVe procedure from the SolVe Desktop or Dell EMC SolVe Online (currently available at https://solveonline.emc.com/solve/products) for VxRail-embedded vCenter deployment.

Note: This procedure requires that the VxRail Management cluster be joined to the Platform Services Controller of the Region A Domain.

---

   a. During the first run process select the option to join an existing SSO domain”
   b. Enter the fully qualified domain name and login credentials for Platform Services Controller.

      sfo01m01psc01.sfo.rainpole.local



6.3 Deploy the VxRail Management cluster

Table 12 **VxRail Manager, vCenter, and Platform Services Controller Details**

FQDN	IP	VLAN ID	Default Gateway	NTP Server
lax01m01vxm01.lax01.rainpole.local	172.17.11.100	1711	172.17.11.253	ntp.sfo01.rainpole.local
lax01m01psc01.lax01.rainpole. local	172.17.11.61	1711	172.17.11.253	ntp.sfo01.rainpole.local
lax01m01vc01.lax01.rainpole.local	172.17.11.62	1711	172.17.11.253	ntp.sfo01.rainpole.local

Table 13 **Management Cluster Hosts**

Hostname Range	IP Range	VLAN ID	Default Gateway
lax01m01esx01.lax01.rainpole.local – lax01m01esx04.lax01.rainpole.local	172.17.11.101 - 172.17.11.104	1711	172.17.11.253

Table 14 **vSAN Host Configuration**

Hostname Range	IP	VLAN ID	Default Gateway
lax01m01esx01.lax01.rainpole.local – lax01m01esx04.lax01.rainpole.local	172.17.12.101 - 172.17.12.104	1712	172.17.12.253

Table 15 **vMotion Host Configuration**

FQDN	IP	VLAN ID	Default Gateway
lax01m01esx01.lax01.rainpole.local – lax01m01esx04.lax01.rainpole.local	172.17.13.101 - 172.17.13.104	1713	172.17.13.253

Table 16 **VM Network Host Configuration**

FQDN	IP	VLAN ID	Default Gateway
lax01m01esx01.lax01.rainpole.local – lax01m01esx04.lax01.rainpole.local	172.17.14.101 - 172.17.14.104	1714	172.17.14.253

6.4 Deploy VMware Cloud Builder virtual appliance

Deploy the VMware Cloud Builder virtual appliance in Region B. Cloud Builder provides the management framework to orchestrate the automated deployment of the SDDC environment. The VVD software bundle and parameters file are uploaded to the system to prepare it for the deployment task.

6.4.1 Procedure

1. Log in to the Management vCenter in Region A.
   a Open a Web browser and go to `https://lax01m01esx01.lax01.rainpole.local`.
   b Log in with username `administrator@vsphere.local` and password `admin_password`.
2. In the navigator, select the Data Center and click **Create / Register** VM.
3. The New virtual machine wizard appears.
4. In the Select creation type dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
5. In 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**.
6. In the Select storage dialog box, select **VxRail Manager vSAN Datastore-<uniqueID>**, and click **Next**.
7. On the License agreements page, click **I agree** to accept the license agreement, and click **Next**.
8. On the Deployment options page, enter the following values and click **Next**.

Table 17 **Cloud Builder Virtual Appliance Disk deployment settings**

Setting	Value
Network mappings	VxRail vCenter Server-<uniqueid>
Disk provisioning	Thin
Power on automatically	Selected

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

Table 18 **Cloud Builder Virtual Appliance settings**

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	*sfo01cb01_admin_password*
Confirm password	*sfo01cb01_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.sfo01.rainpole.local,ntp.lax01.rainpole.local

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

6.5 Deploy the shared edge and compute vCenter server

The shared edge and compute cluster uses and external vCenter for deployment. Once the shared edge and compute PSC has been configured and validated, deploy the vCenter and prepare if for the shared edge and compute VxRail Cluster.

6.5.1 Procedure

1. Obtain a copy of the vCenter VMware-VCSA-all-6.7.0-15132721.iso file from myvmware or the Cloud Builder Appliance.
2. Alternatively, use a tool such as WinSCP to log into the cloud builder appliance
   a Login with user root user root and the corresponding root_password
   b Change directory to `/mnt/iso/sddc-foundation-bundle-3.9.1.0-15253477/vcenter_ova.`
   c Copy the `VMware-VCSA-all-6.7.0-15132721.iso` file to the local Windows system.
3. Mount the ISO file on Windows VM and open the drive where the ISO is mounted.
   a Change directory to the location of the Windows installer, for example: `E:\vcsa-ui-installer\win32`
4. Select the installation application to launch the deployment wizard.
5. Select the **Installer** option and click **Next.**
6. Accept the license agreement and continue.

7. Select the **Deploy a vCenter Server** option from the External Platform Services Controller section of the form and click **Next** .
8. Enter the **Fully Qualified Domain Name** of the Region B management vCenter Server `lax01m01vc01.lax01.rainpole.local`
9. Select the folder to install the VM.
10. Select the compute resource and click **Next**.
11. Enter the VM name `lax01w01vc01` and the root password and click **Next**.
12. Select the vSAN datastore for the desired storage location and click **Next**.
13. Select the port group that begins with `vCenter`, and specify the FQDN, IP address, and other system properties and click **Next**.
14. Confirm that the values are correct and click **Finish**.

    When the vCenter has been deployed, select **Continue** to join it to the `lax01m01psc01` Platform Services Controller in Region B.
15. Start the configuration process and select join and existing domain option by entering the target PSC that you would like to join `lax01m01psc01.sfo01.rainpole.local`.
16. Select the configuration option
    a Specify the `lax01m01vc01.lax.rainpole.local` platform services controller instance.
    b Provide the SSO administrative credentials.
    c Select **Next** to proceed to the summary screen.
    d Review the details and select **FINISH** to deploy the vCenter.

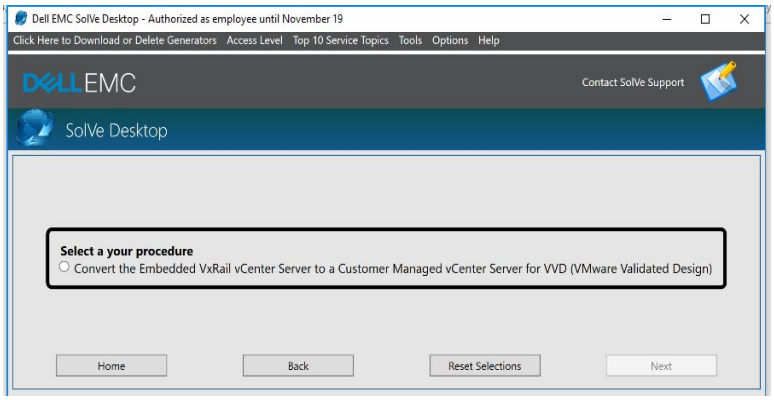
7 Convert the VxRail Management Cluster Internal vCenter and PSC VMs – New process using the UI

Before proceeding with the deployment, convert the PSC and vCenter to customer-managed systems. That task is performed through a vCenter Plugin for VxRail Management. The plugin exposes the conversion option through the Cluster Configure page of the Management vCenter Server. The purpose of this task is to:

- Disassociate the services from VxRail Manager and prepare the vCenter to join the Region A SSO
- Enable the use of enhanced linked mode and cross-site vCenter NSX.
- Provide better alignment with VVD for the Lifecycle Management processes.

This process is dependent on the Dell EMC SolVe procedure *Migrate VxRail Cluster from embedded VC to External vCenter*.

Access the SolVe Desktop tool or SolVe Online (solveonline.emc.com) to download the *Migrate Embedded VxRail vCenter to VVD vCenter and Platform Services Controller* procedure.



Follow the instructions in that document to convert the embedded vCenter and PSC instance.

7.1 Repoint the management cluster to the federated SSO domain

In order to get all vCenter servers to share the same identity source, we must repoint the Region B management vCenter to the PSC which we manually deployed (`lax01w01psc01`). That task is performed from the Management vCenter command line using the `cmsso` utility.

7.1.1 Procedure

1. Log into the management vcenter UI.
2. Create snapshots of the following VMs:
    - lax01m01vc01.`lax.rainpole.local`
    - lax01m01psc01.`lax.rainpole.local`
    - lax01w01psc01.`lax.rainpole.local`
3. SSH or log into vCenter `lax01m01vc01` as the root user.
4. Enter the following command to view the current configuration of the vCenter:

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-ls-location --server-name localhost
```

Note: This command should return `lax01m01psc01.lax01.rainpole.local`.

5. Use the `cmsso domain-repoint` command with pre-check option to test the ability to perform the repoint the management vCenter server.

```
cmsso-util domain-repoint --mode pre-check --src-psc-admin
administrator --dest-psc-fqdn lax01w01psc01.lax01.rainpole.local --
dest-psc-admin administrator --dest-domain-name vsphere.local --dest-
vc-fqdn lax01w01vc01.lax01.rainpole.local
```

6. Enter the passwords for the source and destination PSCs.
7. Review the warning and Click **Y** to proceed.
8. Confirm that the pre-check is successful.

Note: If the task fails or results in an error for any reason, STOP and get some assistance from support or a knowledgeable PS resource. Do not proceed until the pre-check is successful.

---

9. Once the pre-check is successful, alter the command replacing the value of mode from `pre-check` to `execute`.
10. When completed, re-run the `get-ls-location` command to confirm the vCenter is now pointed at the linked PSC.

```
# /usr/lib/vmware-vmafd/bin/vmafd-cli get-ls-location --server-name
localhost
```

11. A second validation task is to log into vCenter using the vCenter web client and confirm all vCenters within the environment are visible in the vCenter UI.

7.2 (Optional) Obtain the VxRail JSON configuration file from Cloud Builder.

Cloud includes a JSON utility that generates VxRail JSON configuration files. Details for the VxRail environment are entered into the vvd-vxrail-regb-deployment.xls parameter file. The “Generate JSON” utility in the Cloud Builder UI produces files for the VVD deployment as well as the VxRail configuration files. Download a copy of the `vvd-vxrail-comp-mgt.json` file to automate the deployment of the VxRail Cluster for the Shared Edge and Compute Domain.

1. If you have not already done so, connect to the cloud builder server
    a. From a web browser, connect to https://lax01cb01.lax01.rainpole.local
    b. Login with user name ***admin*** and password ***admin_password*.**
    c. Select the Deployment Wizard Icon → Upload Config File.
    d. Under Select Architecture – click **VVD-for SDDC 5.1.1 on DellEMC VxRail (Region B)**.
    e. Locate the **vvd-vxrail-regb** parameter file and upload it to the system.
    f. Click **Generate JSON** to create the JSON files.
2. Use a secure copy tool such as WinSCP to connect to the system.
    a. Login with user name ***root***.
    b. Password ***root_password***.
3. Change directory to /opt/vmware/sddc-support/cloud_admin_tools/Resources/vxrail-regb
4. Copy the **vxrail-regb-comp-manager.json** file to the local desktop.
5. Use this file when prompted for an input file during the VxRail Initialization.

7.3 Create shared edge vCenter datacenter for VxRail external vCenter deployment

Create a VCenter required datacenter on `laxw01vc01.lax01.rainpole.local`.

7.3.1 Procedure

1. Log into the vCenter Server.
2. Locate the `lax01w01vc01` vCenter Server from the global inventory list.
3. Right-click on the **vCenter** and select **New Data Center**.
4. Enter the value for the data center defined within the PEQ and/or parameter file.
5. Click **OK** and proceed to the next task.

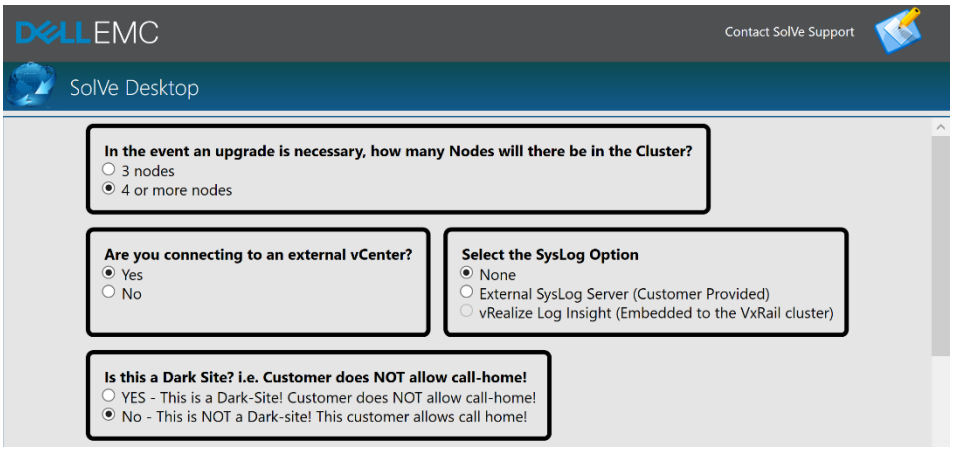
7.4 Deploy the shared edge and compute VxRail cluster

Refer to the VxRail *External vCenter* installation procedures from the Dell EMC SolVe site or SolVe desktop tool and ensure the following:

- Shared edge compute vCenter server is deployed in Region B.
- Network and top-of-rack switches configured with requisite VLANs and BGP peer interfaces.
- Windows host that has access to VxRail Manager within your data center.
- (Optional) VxRail deployment JSON file

7.4.1 Procedure

1. Download the *VxRail External vCenter Installation Guide* from the Solve Desktop or Solve Online through the Dell EMC Support web site.



   The SolVe tool produces the deployment guide with detailed instructions and dependencies for deploying the VxRail external cluster.
2. Follow the procedures within the SolVe deployment documentation to complete the shared edge and compute VxRail cluster deployment.
3. Deploy the VxRail using Cloud Builder Generated JSON input file (Optional)

a. VxRail deployment supports two options for defining the configuration properties. A manual process where details are manually entered, and a JSON configuration file which is pre-populated with configuration details.

b. Cloud Builder produces multiple JSON files from the parameter file, including a VxRail input file for both clusters. If the parameter file is available, log into Cloud Builder and follow the process to generate the JSON files.

c. Obtain the `vxrail-regb-comp-manager.json` file from Cloud Builder using ftp or SCP. The file is available in the `/opt/vmware/sddc-support/cloud_admin_tools/Resources/vxrail-regb` directory.

See *Generate the JSON Deployment Files for the Management and the Shared Edge and Compute Clusters in Region A* for steps to upload and create the json file.

4. Reference the following information for either manual or Cloud Builder VxRail deployment.

The NTP server is `ntp.lax01.rainpole.local`.

Table 19 **VxRail Manager, vCenter, and Platform Services Controller Details**

FQDN	IP	VLAN ID	Default Gateway
lax01w01vxm01.lax01.rainpole.local	172.17.31.69	1731	172.17.11.253
lax01w01psc01.lax01.rainpole.local	172.17.11.63	“”	“”
lax01w01vc01.lax01.rainpole.local	172.17.11.64	1731	172.17.11.253

Table 20 **Management Cluster Hosts**

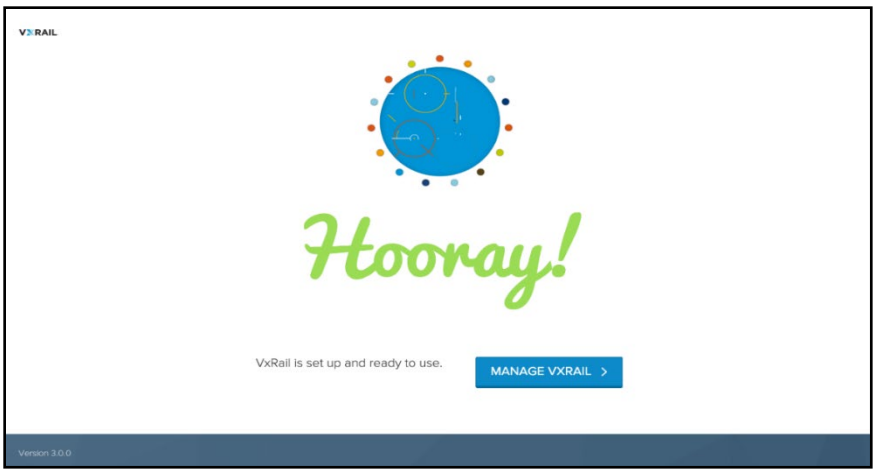
FQDN	IP	VLAN ID	Default Gateway
lax01w01esx01 … lax01w01esx04	172.17.31.101 … 172.17.31.104	1731	172.17.31.253

Table 21 **vSAN Host Configuration**

FQDN	IP	VLAN ID	Default Gateway
lax01w01esx01… lax01w01esx04	172.17.33.101… 172.17.33.104	1733	172.17.33.253

Table 22 **vMotion Host Configuration**

FQDN	IP	VLAN ID	Default Gateway
lax01w01esx01 … lax01w01esx04	172.17.32.101… 172.17.32.104	1732	172.17.32.253



After completion of the VxRail Manager deployment, connect to VxRail Manager and confirm the health of all components in the cluster.

8 Configure SSH on all hosts

Complete the initial configuration of all ESXi hosts by enabling the SSH service to allow Cloud Builder remote connectivity.

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

8.1 Procedure

1. Log in to the vSphere host by using the VMware Host Client.
   a. Open a Web browser and go to **https://lax01m01vc01.lax01.rainpole.local/ui**.
   b. Log in with user name *administrator@vsphere.local* and password *administrator_password*.
2. Expand the cluster and list the ESXi Hosts.
3. Select lax01m01esx01.lax01.rainpole.local.
4. Select System > Services
   a. Select the **SSH** service, and click the **Actions** menu.
   b. Select **Policy** and click **Start and stop with host**.
   c. Click **Start** to start the service.
5. Repeat Steps 3 and 4 for all ESXi hosts in the cluster.
6. Repeat Steps 1 – 4 on the workload domain vCenter **https://lax01w01vc01.lax01.rainpole.local/ui**.

9 Set the MTU Size for the vDS and VMKernel Host Adapters

The Cloud Builder 5.1.1 performs validation of the MTU settings on the vDS as well as the VMkernel interfaces for VSAN and vMotion. The MTU properties for these network devices and their corresponding TOR ports, VLANS, etc., will have been established during the pre-deployment planning, and documented in the VVD parameter guide. The VVD validation tasks will compare the configured settings for these devices to the properties identified on the networks tab of the parameter document.

If there is a disparity between the values, the network pre-validation will fail and require remediation. In order to avoid that, set the properties prior to performing the validation.

Log into the Management Cluster and set the vDS MTU size to 9000 (or specific value defined for the customer environment). Note: VXLAN requires an MTU size of at least 1600 bytes.

Repeat this procedure for all hosts in the management and shared edge and compute clusters.

9.1 Procedure

1. Log in to the vSphere Management Server.
   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui/`.
   b Log in using the user name *administrator@vsphere.local* and the administrator password.
2. Select the Networking Object and locate the vDS (for example sfo01m01vds01)
3. Use the right mouse button to display the switch management option.
4. Select **Settings > Edit Settings.**
   a Click **Advanced configuration**.
   b Replace the existing MTU value of 1500 bytes with the documented value (i.e., 9000).
   c Click **OK** to apply the settings.
5. Select the Hosts and Clusters Tab
6. Expand the cluster and list the ESXi hosts.
7. Select **sfo01m01esx01.sfo01.rainpole.local**
8. Select **Configured**
9. Select **VMkernel adapters**
   a Select the VMkenel adapter for the vSAN interface (i.e. sfo01m01vsan) and click **Edit**.
   b Set the MTU property to the documented value (i.e. 9000). Note; This value must not exceed the MTU size defined for the vDS.
   c Click **OK**.
10. Repeat steps 5 through 9 for all ESXi hosts in the cluster.
11. Repeat steps 1 through 9 on the workload domain vCenter. **https://sfo01w01vc01.sfo01.rainpole.local/ui.**

10 Prerequisites for Cloud Management Layer

To prepare the cloud management layer for automated deployment of the SDDC components using Cloud Builder, 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.

10.1 Deploy and configure the master Windows system for vRealize automation IaaS nodes in Region B

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

Create a virtual machine on the `lax01m01vc01.lax01.rainpole.local` host for the Master Windows system with the following virtual machine, software, and network configuration.

Table 23 **Virtual Machine Requirements for the Master Windows System**

Setting	Value
ESXi Host	lax01m01vc01
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	lax01m01-vSAN
Network Interface	vCenter-<unique hex id>
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 24 **Software Requirements for the Master Windows System**

Component	Requirement
Operating System	Windows Server 2016
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.

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.

10.2 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 with user name ***Windows administrator user*** and password ***windows_administrator_password***.
3. Click **Start**, right-click **Windows PowerShell** and select **More > Run as Administrator**.
3. Set the PowerShell execution policy by running the following command.

   ```
   Set-ExecutionPolicy Unrestricted
   ```

   When prompted, confirm the execution policy change.
4. Disable User Account Control (UAC) by running the following command.

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

5. Disable IPv6 protocol.

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

6. 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.

7. 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
   ```

8. 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 with user name ***rainpole\svc-vra*** and password ***svc-vra_password***.

9. Shut down the master Windows system virtual machine.

11 Deploy the SDDC Components

After you deploy and configure the VMware Cloud Builder appliance, generate the JSON deployment files based on the values populated in the Deployment Parameters XLS file. 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.

11.1 Upload the VVD software bundle and signed certificates to VMware Cloud Builder in Region B

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

11.1.1 Procedure

1. Log in to the VMware Cloud Builder virtual appliance.
   a Open a connection to `lax01cb01.lax01.rainpole.local` using an SCP software such as WinSCP.
   b Log in with user name ***admin*** and password ***cloudbuilder_admin_password***.
2. Upload the VVD software bundle files to the`/mnt/hgfs` directory on the Cloud Builder appliance.
   - sddc-vrealize-bundle-5.1.1.0-15121189.iso
   - sddc-dr-bundle-5.1.1.0-15121189.iso
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 VVD software bundle`.iso` file.
   a Open an SSH connection to `lax01cb01.lax01.rainpole.local`.
   b Log in with user name ***admin*** and password ***cloudbuilder_admin_password***.
   c Switch to the **root** user by running the `su` command.
   d Mount the VVD 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.

12 Generate the JSON Deployment Files for the Shared Edge and Compute Cluster

After you have populated all required configuration values in the Deployment Parameters XLS file, 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.

12.1 Procedure

1. Log in to VMware Cloud Builder.
   a Open a Web browser and go to **https://lax01cb01.lax01.rainpole.local**.
   b Log in with user name ***admin*** and 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 25 **Region B JSON Deployment Files**

Architecture Type	JSON Filename	Workload Domain	Deployment Order
VVD for SDDC Region B	`vvd-vxrail-regb-mgmt.json`	Management	1
	`vvd-vxrail-regb-comp.json`	Compute	2

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

Table 26 **VMware Cloud Builder JSON Generator Log File Location**

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

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

13 Validate the Deployment Parameters and Environment Prerequisites for the VVD Clusters

Perform validation of both JSON deployment files and target environment to ensure that prerequisites have been met and you can successfully deploy the management and the shared edge/compute clusters using VMware Cloud Builder.

Validate the JSON deployment files for both the management and the shared edge and compute clusters. If 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 27 **VMware Cloud Builder Platform Audit Log File Location**

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

13.1 Procedure

1. Log in to VMware Cloud Builder.
   a. Open a Web browser and go to `https://lax01cb01.lax01.rainpole.local.`
   b. Log in with user name ***admin*** and 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-vxrail-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*.

   If validation fails with a `user input error` message, remediate the Deployment Parameters XLS file.
6. 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.
7. Navigate to the updated Deployment Parameters XLS file and click **Open**.
8. In the Overwrite Existing JSON File(s) dialog box, select **Yes**.
9. Select the Validate Environment tab, from the Select File to Validate drop-down menu, select the `vvd-vxrail-regb-mgmt.json` file and click **Validate**.

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

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

    The `vvd-vxrail-regb-comp.json` file successfully validates against the predefined run parameters.

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

13.2 Start the automated deployment of the management cluster

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

13.2.1 Procedure

1. Log in to VMware Cloud Builder.
   a Open a Web browser and go to **https://lax01cb01.lax01.rainpole.local**.
   b Log in with user name ***admin*** and 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-vxrail-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 15. 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`

13.3 Start the automated deployment for the shared edge and compute cluster

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

13.3.1 Procedure

1. Log in to VMware Cloud Builder.
   a Open a Web browser and go to **https://lax01cb01.lax01.rainpole.local**.
   b Log in with user name ***admin*** and password ***cloudbuilder_admin_password***.
2. In the Cloud BuilderNavigator, select the **Deployment Wizard** icon.
3. Select the **Deploy an SDDC** tab.
4. From the Select Deployment File drop-down menu, select the **vvd-vxrail-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 16. 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

14 Post-Deployment Create a local VxRail Admin account on the workload PSC

During the VxRail first run, VxRail Manager created a local account on the platform services controller and granted the VMware HCIA Management entitlement to that account.

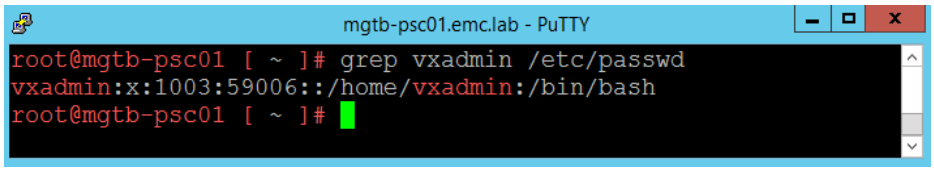
To support the condition where the primary PSC may be unavailable, add a localos account to the second PSC. The account is used to support the VxRail Management administrative functions and was defined when we deployed the initial cluster within this region. Use the following procedure to create the account on the second PSC.

- The VxRail manager administrative account name in this example is `vxadmin`.
- UID and GID values were obtained from the initial PSC.

14.1.1 Procedure

1. SSH into the `lax01m01psc01.lax01.rainpole.local` PSC as root.
   a Run the following command to verify the existing user ID and group ID values:

   ```
   grep vxadmin /etc/passwd
   ```

2. Open an SSH session to the `lax01w01psc01.lax01.rainpole.local` PSC.
3. Run the following commands to add the group and user:

   ```
   groupadd -g 59006 vxadmins
   useradd vxadmin -u 1003 -g 59006 -d /home/vxadmin -s /bin/bash
   ```

4. Set the password of the vxadmin to match the existing password on the PSC1

   ```
   passwd vxadmin
   ```

5. Log in to the DCUI of the Workload Domain vCenter Server to enable the global privilege for the Account.
6. Select **Administration > Workload vCenter Server** from the drop-down menu.
7. Select **Global Permissions** and click the + to add a new permission.
8. Select **localos** from the Domain drop down and locate the vxadmin@localos account. Click **Add**.
9. From the Assign Role, select **VMware HCIA Management** global privilege to the local account, select **Propagate to children**, and click **OK**.

15 Post-Deployment Disable Host Lockdown Mode

The Region B Management workflows within this release inadvertently set the Security Profile Lockdown Mode on hosts within the management clusters of both regions. This will impact the network services that are running between VxRail Manager and the hosts.

To correct this issue, the security profile host lockdown mode setting must be verified and disabled on all hosts in the VxRail clusters.

15.1.1 Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
2. From the Menu select **Hosts and Clusters**.
3. In the Navigator, Expand vCenter Server > Datacenter > Cluster.
4. In the Navigator, select the ESXi host.
5. In the main page select the Configure tab.
6. In the navigator of the main page, select **System > Security Profile**.
7. Under Lockdown Mode, click **Edit**.
8. In the Lockdown Mode dialog, select the **Disabled** radio button and click **OK**.
9. Repeat for all remaining ESXi hosts in the cluster.

16 Post-Deployment Operations Management Configuration

After the operations management applications are deployed in Region B, perform post-deployment tasks for the operations management layer. Reconfigure the automatic synchronization of authentication sources in vRealize Operations Manager, and enable define monitoring goals for the default policy.

16.1 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. Enable an automatic synchronization of the user membership for configured groups and enable define monitoring goals for the default policy.

16.1.1 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.

16.1.2 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 with user name ***admin*** and 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** > **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**.

16.2 Define monitoring goals for the default policy in vRealize Operations Manager

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

16.2.1 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 with user name ***admin*** and 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 opens.
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 Steps 5 to 10 for the Compute vCenter Server adapter.
12. In the Manage Solution - VMware vSphere dialog box, click **Close**.

17 Post-Deployment Cloud Management Platform Configuration

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

17.1 Configure content library

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.

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

17.2 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.

17.2.1 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 with user name ***administrator@vsphere.local*** and 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 with user name ***administrator@vsphere.local*** and password ***vsphere_admin_password***.
6. From the Home menu, select **Content Libraries**, and click the **+** icon.

   The **New Content Library** wizard opens.
7. On the Name and location page, enter the following settings and click **Next**.

Table 28 **Name and Location Settings**

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**.

Table 29 **Subscribed Content Library Settings**

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.

17.3 Create reservation policies

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.

17.3.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. Navigate to **Infrastructure > Reservations > Reservation Policies**.
3. Click the **New** icon, configure the following settings, and click **OK**.

Table 30 **Production Policy Settings**

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**.

Table 31 **Development Policy Settings**

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**.

Table 32 **Edge Policy Settings**

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

17.4 Create reservations for the shared edge and compute cluster

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 33 **Business Group Names**

Group	Name
Production	LAX01-Comp01-Prod-Res01
Development	LAX01-Comp01-Dev-Res01

17.4.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
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.

Table 34 **Reservation Settings**

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

Setting	Production Group Value	Development Group Value
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 a network path listed in the following table, 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.

Table 35 **Production Network Path and Profile**

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.

Table 36 **Development Network Path and Profile**

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.

17.5 Create reservations for the user edge resources

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 37 **Business Group Names**

Group	Name
Production	LAX01-Edge01-Prod-Res01
Development	LAX01-Edge01-Dev-Res01

17.5.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
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.

Table 38 **New Reservation Settings**

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. From the Network Profile drop-down menu, select the corresponding network profile for the business group whose reservation you are configuring.

Table 39 **Production Network Paths**

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

Table 40 **Development Network Paths**

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.

17.6 Create virtual machines using VM templates in the content library

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 41 **VM Templates and Their Guest Operating Systems**

VM Template Name	Guest OS
windows-server-2016	Windows Server 2016
windows-server-2016-sql-server-2017	Windows Server 2016
ubuntu-server-1804	Ubuntu Server 18.04

17.6.1 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 with user name ***administrator@vsphere.local*** and 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-2016** 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.

17.7 Convert virtual machines to VM templates

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 42 **VM templates and Their Guest Operating Systems**

VM Template Name	Guest OS
windows-server-2016	Windows Server 2016
windows-server-2016-sql-server-2017	Windows Server 2016
ubuntu-sever-1804	Ubuntu 18.04

17.7.1 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 with user name ***administrator@vsphere.local*** and 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-server-2016** virtual machine located in the **VM Templates** folder, and click **Template > Convert to Template**.
5. Click **Yes** and confirm the template conversion.

18 Configure Single-Machine Blueprints

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

18.1 Create a service catalog

A service catalog provides a common interface for you to request services, track your requests, and manage your provisioned service items.

18.1.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. Navigate to **Administration > Catalog Management > Services > New**.

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

Table 43 **Service Settings**

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)

18.2 Create a single-machine blueprint

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.

Table 44 **Blueprint Values**

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2016 - LAX Prod	windows-server-2016 (lax01w01vc01.lax01.rainpole.local)	os-windows-joindomain-custom-spec	LAX-Production-Policy

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2016 With SQL Server 2017 - LAX Prod	windows-server-2016-sql-server-2017 (lax01w01vc01.lax01.rainpole.local)	os-windows-joindomain-custom-spec	LAX-Production-Policy
Ubuntu Server 18.04 - LAX Prod	ubuntu-server-1804 (lax01w01vc01.lax01.rainpole.local)	os-linux-custom-spec	LAX-Production-Policy

18.2.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. From the main navigation bar, select the **Design tab**
3. In the left pane, click **Blueprints > New**.
4. In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

Table 45 **New Blueprint Values**

Setting	Value
Name	Windows Server 2016 - LAX Prod
Deployment limit	Default setting (blank)
Lease (days): Minimum	30
Lease (days): Maximum	270
Archive (days)	15

5. From the Categories pane, click **Machine types**, select **vSphere (vCenter) Machine** and drag it to the **Design Canvas**.
6. On the virtual machine specification section click the **General** tab, configure the following settings, and click **Save**.

Table 46 **Virtual Machine Settings**

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

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

Table 47 **Build Information Settings**

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	windows-server-2016
Customization spec	**os-windows-joindomain-custom-spec**

Note: If the value of the **Clone from** setting does not list **windows-server-2016** template, you must perform a data collection on the **lax01-w01-comp01** Compute Resource.

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

Table 48 **Machine Resources Settings**

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

9. Configure the network for the virtual machine blueprint.
   a From the Categories pane, click **Network & security**, select the **Existing network** component and drag it into the **Design Canvas**.
   b On the General tab of the existing network component, select the **Ext-Net-Profile-Production- Web** network profile, and click **Save**.
   c In the Design Canvas, select the **vSphere_vCenter_Machine** object
   d Click the **Network** tab, click **New**, configure the following settings, and click **OK**

Table 49 **Blueprint Network Values**

Blueprint Name	Existing network
Network	Ext-Net-Profile-Production-Web
Assignment type	Static IP
Address	Default setting (blank)

   e To save the blueprint, click **Finish**.

   On the Blueprints page, select the **Windows Server 2016 - LAX Prod** blueprint and click **Publish.**

10. Repeat this procedure to create the remaining blueprints of Production environment.

    To test blueprints in a Development environment, or according to your business needs, create Development blueprints using the same process as for Production blueprints.

18.3 Configure entitlements of blueprints

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 entitlements.

Table 50 **Blueprint Entitlements**

Blueprint Name	Service Catalog	Add to Entitlement
Windows Server 2016 - LAX Prod	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2016 With SQL Server 2017 - LAX Prod	LAX Service Catalog	Prod-SingleVM-Entitlement
Ubuntu Server 18.04	LAX Service Catalog	Prod-SingleVM-Entitlement

18.3.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. Configure the service catalog for the blueprint.
   a On the main navigation bar, click the **Administration** tab.
   b In the left pane, navigate to **Catalog Management > Catalog Items**.
   c On the Catalog Items pane, select the **Windows Server 2016 - LAX Prod** blueprint.
3. The **Configure Catalog Item** page opens.
   a On the General tab, from the Service drop-down menu, select **LAX Service Catalog**, and click **OK**.
   b Repeat this step to configure service catalog for the remaining blueprints
4. Associate the blueprint with an entitlement.
   a In the left Catalog Management pane, Click **Entitlements.**

      The **Edit Entitlement** pane opens.
   b Select the **Items & Approvals** tab
   c Under Entitled Items, click **Add items**, select the **Windows Server 2016 - LAX Prod** blueprint, and click OK.
   d Click **Finish**.
5. Repeat this procedure to associate all the blueprints with their entitlements.

18.4 Test the deployment of a single-machine blueprint

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.

18.4.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.

2. From the main navigation bar, click the **Catalog** tab.
3. On the Catalog page, click the **Click here to apply filters icon.**
4. In the left pane, select **LAX Service Catalog** check box.
5. On one of the blueprint cards, click **Request** and **Submit**.
6. Verify that the request finishes successfully.
   a Click the **Deployments** tab.
   b Click the deployment you submitted, click **History**, and wait for the request to complete.
   c Under Status, verify that the virtual machine is successfully provisioned.
7. 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 with user name ***administrator@vsphere.local*** and password ***vsphere_admin_password***.
8. Verify that the virtual machine provisions in the shared edge and compute cluster.
   a In the Hosts and Clusters inventory, expand the **lax01w01vc01.lax01.rainpole.local** tree and expand the **lax01-w01dc** data center.
   b Expand the **lax01-w01-comp01** cluster and select the **lax01-w01rp-user-vm** resource pool.
   c Verify that the provisioned virtual machine is present and operational.

19 Configure Unified Single-Machine Blueprints for Cross-Region Deployment

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.

19.1 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, edit an XML file on the vRealize Automation server.

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

19.1.1 Procedure

1. Log in to the virtual machine of the vRealize Automation IaaS Web server by using a Remote Desktop Protocol (RDP) client with the following credentials.

   Table 51 **RDP Credentials**

Setting	Value
FQDN	vra01iws01a.rainpole.local
User name	rainpole\svc-vra
Password	*svc-vra_password*

2. 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 Modify the `Data Name` and `Description` attributes to use the following settings.

   ```
   <CustomDataType>
      <Data Name="SFO" Description="San Francisco Data Center"/>
      <Data Name="LAX" Description="Los Angeles Data Center"/>
   </CustomDataType>
   ```

   c Save and close the file.

3. Restart the vra01iws01a virtual machine.

   Wait until the virtual machine restarts and is successfully running.

4. Repeat this procedure for the vra01iws01b virtual machine.

19.2 Associate compute resources with a location

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.

Table 52 **vCenter Server Compute Locations**

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

19.2.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. From the main navigation bar, select the **Infrastructure** tab.
3. Navigate to **Compute Resources > Compute Resources** and click **sfo01-w01-comp01.**
4. From the Location drop-down menu, select the **SFO** data center and click **OK**.
5. Repeat this procedure and set the data center location for the lax01-w01-comp01 cluster.

19.3 Add a property group and a property definition for data center location

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.

19.3.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. From the main navigation bar, click **Administration.**
3. Navigate to **Property Dictionary > Property definitions**.
4. 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.

Table 53 **Property Settings**

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.

5. Navigate to **Administration > Property Dictionary > Property Groups**, and click **New**.
6. Enter **Select Location** in the Name text box.
7. The ID text box is populated with the same value, after you enter the **Name** value.
8. In the Visibility section, select the **All tenants** radio button and specify with which tenant the property is to be available.
9. (Optional) Enter a description of the property group.
10. Add a property to the group by using the **Properties** box.

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

Table 54 **Group Property Settings**

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

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

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

19.4 Create a reservation policy for the unified blueprint

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.

19.4.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.

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**.

19.5 Specify reservation information for the unified blueprint

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.

Table 55 **Reservation Values for the Unified Blueprint**

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)

19.5.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.

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:

Table 56 **New Reservation Settings**

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

Setting	Production Business Group Value
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.

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

Table 57 **Network Paths**

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

6. Click **OK** and save the reservation.
7. Repeat the procedure and create a reservation for Region B.

19.6 Create a service catalog for the unified blueprint

The service catalog provides a common interface for consumers of IT services to request 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 entitlements allow members of a particular business group, for example, the production business group, to use the blueprint. Without an entitlement, users cannot use the blueprint.

19.6.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. From the main navigation bar, click **Administration > Catalog Management > Services**.
3. Click **New**.
4. In the **New Service** dialog box, enter the following

Table 58 **New Service Settings**

Setting	Value
Name	Unified Single-Machine Catalog
Description	Default Setting (blank)
Status	Active

19.7 Create an entitlement for the Unified Blueprint catalog

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.

19.7.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. From the main navigation bar, click the **Administration** tab.
3. In the left pane, navigate to **Catalog Management > Entitlements**.
4. Click **Prod-SingleVM-Entitlement**.

   The Edit Entitlement window appears.
5. Select the **Items & Approvals** tab, navigate to **Entitled Services** and click the **Add** icon.
   c Select **Unified Single-Machine Catalog** and click **OK**.
   d Click **Finish**.

19.8 Create unified single-machine blueprints

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.

Table 59 **Unified Single-Machine Blueprints**

Blueprint Name	VM Template	Reservation Policy	Customization Specification	Service Catalog
Windows Server 2016 - Unified Prod	windows-server-2016 (sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	os-windows-joindomain-custom-spec	Unified Single-Machine Catalog

Blueprint Name	VM Template	Reservation Policy	Customization Specification	Service Catalog
Windows Server 2016 with SQL Server 2017 - Unified Prod	windows-server-2016 -sql-server-2017 (sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	os-windows-joindomain-custom-spec	Unified Single-Machine Catalog
Ubuntu Server 18.04 - Unified Prod	ubuntu-serer-1804(sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	os-linux-custom-spec	Unified Single-Machine Catalog

19.8.1 Procedure

5. 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
6. From the main navigation bar, click the **Design tab.**
7. In the left pane, click **Blueprints > Blueprints > New**.
8. In the New Blueprint dialog box, configure the following settings on the General tab, and click **OK**.

Table 60 **New Blueprint Settings**

Setting	Value
Name	Windows Server 2016 - Unified Prod
Deployment limit	Default setting (blank)
Lease (days): Minimum	30
Lease (days): Maximum	270
Archive (days)	15

9. From the Categories pane, click **Machine types**, select the vSphere (vCenter) machine component and drag it in the **Design Canvas**.
10. On the virtual machine specification section, click the **General** tab, configure the following settings, and click **Save**.

Table 61 **Virtual Machine Settings**

Setting	Value
ID	Default setting (vSphere_vCenter_Machine_1)
Display location on request	Deselected
Reservation Policy	UnifiedBlueprint-Policy
Machine Prefix	Use group default
Instances: Minimum	Default setting
Instances: Maximum	1

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

Table 62 **Build Information Settings**

Setting	Value
Blueprint Type	Server
Action	Clone
Provisioning Workflow	CloneWorkflow
Clone from	windows-server-2016
Customization spec	**os-windows-joindomain-custom-spec**

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

Table 63 **Machine Resources Settings**

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

13. Configure the network for the virtual machine blueprint.
    a From the Categories pane, click **Network & security**, select the Existing network component and drag it in the **Design Canvas**.
    b On the General tab of the existing network component, select the **Ext-Net-Profile-Production- Web** network profile , and click **Save**.
    c In the **Design Canvas**, select the **vSphere_vCenter_Machine** object.
    d Click the **Network** tab, click **New**, configure the following settings, and click **OK.**

Table 64 **Blueprint Network Properties**

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

14. Click the **Properties** tab.
    a On the Property groups tab, click **Add**.
    b Select the property group **Select Location** and click **OK**.
15. To save the blueprint, on the **New blueprint** dialog box, click **Finish** Click **OK**.
16. On the Blueprints page, select the Windows Server 2016 - Unified Prod blueprint and click Publish.
17. Configure the service catalog for the blueprint.
18. Navigate to **Administration > Catalog Management > Catalog Items** and add the blueprint to the **Unified Single-Machine Catalog**.
    a On the main navigation bar, click the **Administration** tab.
    b In the left pane, navigate to **Catalog management > Catalog items**.
    c On the Catalog items page, click the **Windows Server 2016 - Unified Prod** blueprint.
    The Configure catalog item page opens.

d On the General tab, from the Service drop-down menu, select **Unified Single-Machine Catalog**, and click **OK.**

19.9 Test the cross-region deployment of the single-machine blueprints

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.

Table 65 **Site Locations**

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

19.9.1 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 to the rainpole.local domain with user name ***vra-admin-rainpole*** and password ***vra-admin-rainpole_password***.
2. From the main navigation bar, click the **Catalog** tab.
3. On the Catalog page, click the **Click here to apply filters** icon.
4. In the left pane, select the **Unified Single-Machine Catalog** check box.
5. On one of the blueprint cards, click **Request.**
6. Select vSphere_vCenter_Machine_1.
7. From the Select a region drop-down menu, select **San Francisco** and click **Submit**.
8. Verify the request finishes successfully.
   a On the main navigation bar, click the **Deployments** tab.
   b Click the deployment that you submitted, click the **History** tab and wait for the process to finish.
   c Under **Status**, verify that the virtual machine successfully provisioned.
9. Log in to the Compute vCenter Server https://sfo01w01vc01.sfo01.rainpole.local/ui by using the vSphere client with username ***administrator@vsphere.local*** and password ***vsphere_admin_password***.
10. Verify the virtual machine provisions in the Region A vCenter Server compute cluster.
    a In the **Hosts and Clusters** inventory, expand the **sfo01w01vc01.sfo01.rainpole.local** tree and expand the **sfo01-w01dc** data center.
    b Expand the **sfo01-w01-comp01** cluster and select the **sfo01-w01rp-user-vm** resource pool.
    c Verify that the provisioned virtual machine is present and operational.
11. Repeat this procedure for Region B.