Dell EMC VxRail Appliance

Cloud Builder Deployment Guide for VVD Version 5.0 in Region B

Abstract

This deployment guide provides detailed instructions for installing, configuring, and operating a software-defined data center (SDDC) based on the VMware Validated Design for SDDC, using the VMware Cloud Builder virtual appliance to automate the implement.

June 2019

H17783

Table of contents

1 About VMware Validated Design Deployment

The *VMware Validated Design Deployment for Region B* 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 for SDDC, using VxRail infrastructure and the VMware Validated Design Cloud Builder to automate the implementation of Region B.

This document is focused on deployment. Since the post-deployment tasks for tenant customization depend on customer requirements, this document provides general guidance, but it does not contain step-by-step instructions for performing all required post-configuration tasks.

1.1 Intended Audience

The *VMware Validated Design Deployment of Region B* documentation is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with and want to use VMware software to quickly deploy and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

1.2 Required VMware Software

The *VMware Validated Design Deployment of Region B* documentation is compliant and validated with certain product versions. See the *VMware Validated Design v5.0 Planning Guide and Release Notes* for more information about supported product versions.

1.3 Required VxRail Software

VVD 5.0 was qualified using VxRail 4.7.100. It is supported for the 4.7.1xx releases of VxRail.

1.4 Before You Apply This Guidance

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

To use VMware Validated Design Deployment of Region B, you must be acquainted with the following:

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

2 Hardware Requirements

To implement the SDDC from this VMware Validated Design, 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 per Region

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	192 GB*

Storage per server	▪ 16 GB SSD for booting
	▪ One 200 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 5.0 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 per Region

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, IO devices, and so on, see the Dell EMC VxRail hardware information in the VMware Compatibility Guide.

Note If you scale out the environment with compute-only clusters, each server must meet the same requirements as a server in the shared edge and compute cluster. You can use as many compute servers as required.

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.

Cloud Builder fails to deploy Site Recovery Manager

The SRM automated deployment fails to install the site recovery manager software on the Windows VM. The Cloud Builder UI reports that the SRM deployment has failed.

Workaround: Perform the manual deployment of Site Recovery Manager on the `ax01-srm01.lax01.rainpole.local` virtual machine.

1. Connect to the Windows SRM VM through vCenter or a Remote Desktop Client using the `svc-srm` account.
2. Open the c:\ folder and locate the srm.bat file.
3. Right-click that file and select **Run as administrator**.
4. Monitor the batch file and wait for SRM deployment to complete.
5. Go to the Cloud Builder Web UI Deployment tab and select **Retry** to restart the Management deployment.

Setting VM priority mappings for recovery plan in SRM fails

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.

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.

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.

4 Deployment Overview

This section provides a brief overview of the deployment process. It is intended as a preparation tool to orient you with the process, and as a reference to quickly identifying where you are in the process flow as you proceed through the deployment.

The process has three distinct sections.

- Section 1 focuses on deploying the infrastructure services and preparing for the cloud builder deployment.
- Section 2 covers the cloud builder tasks and deployment.
- Section 3 describes the post deployment tasks which are conducted within the vRealize Suite.

4.1 VVD VxRail infrastructure and network services

Figure 1 illustrates the high-level deployment tasks required for the deployment of the VxRail Clusters for the Cloud Builder automated SDDC deployment.

This phase of 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, and establish replication between PSCs within the SSO domain, the Region B workload domain SC is joined to the workload domain PSC in Region A. That task is performed manually after the VxRail Cluster for the management domain has been deployed.

The Region B workload domain PSC is deployed into that management domain, and joined to the existing 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 embedded vCenter is repointed to the Region B workload PSC and the original Region B management PSC is recreated to join the SSO domain.

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

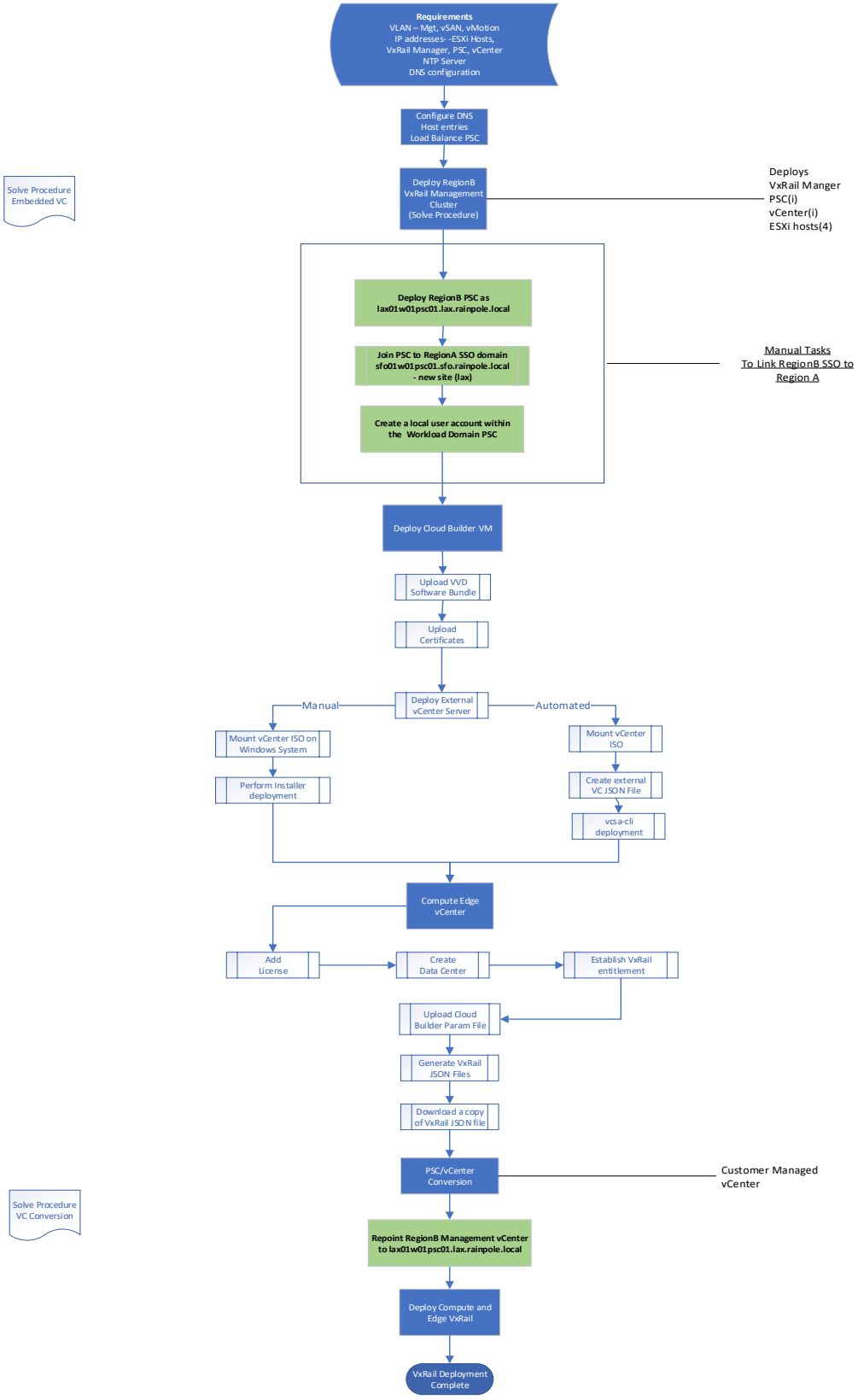


Figure 1. VxRail Cluster Deployment for Region B.

4.2 Preparation for Cloud Builder

Similar to the Region A document, the following dependencies must be established before proceeding to the Cloud builder validation and deployment.

- Cloud Builder requires SSH access to all ESXi Hosts, therefore we must 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.
- If the deployment includes data protection with SRM, a Windows VM must be deployed and configured to support the SRM services.
- 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.

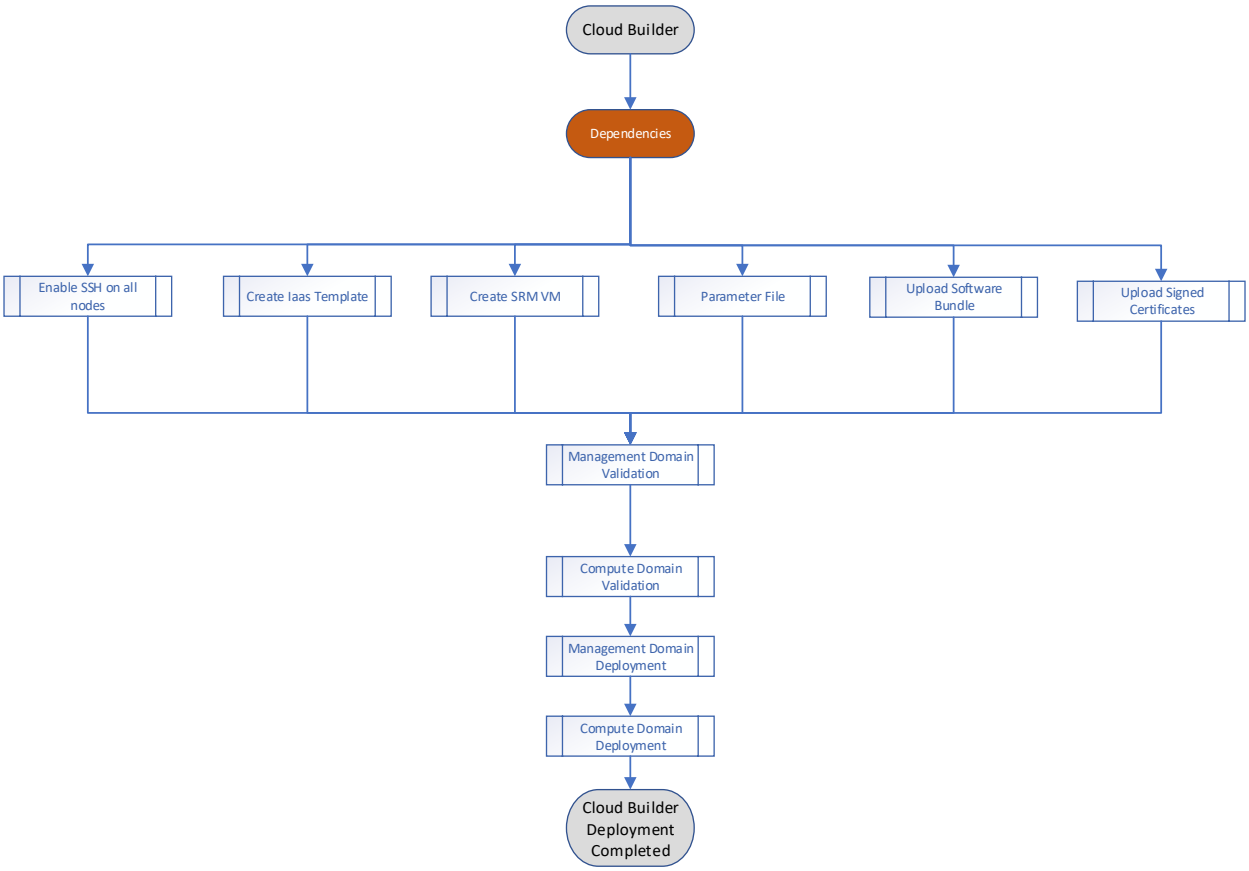


Figure 2. Cloud Builder dependencies

Finalize the deployment by setting the monitoring policies, and configuring the vRealize tenant and Service Catalog to verify the environment is functional.

The tasks in this section are related to creation of VM templates, vRA blueprints, and catalog services. Custom services are out-of-scope for this deployment and would be completed after phase three.

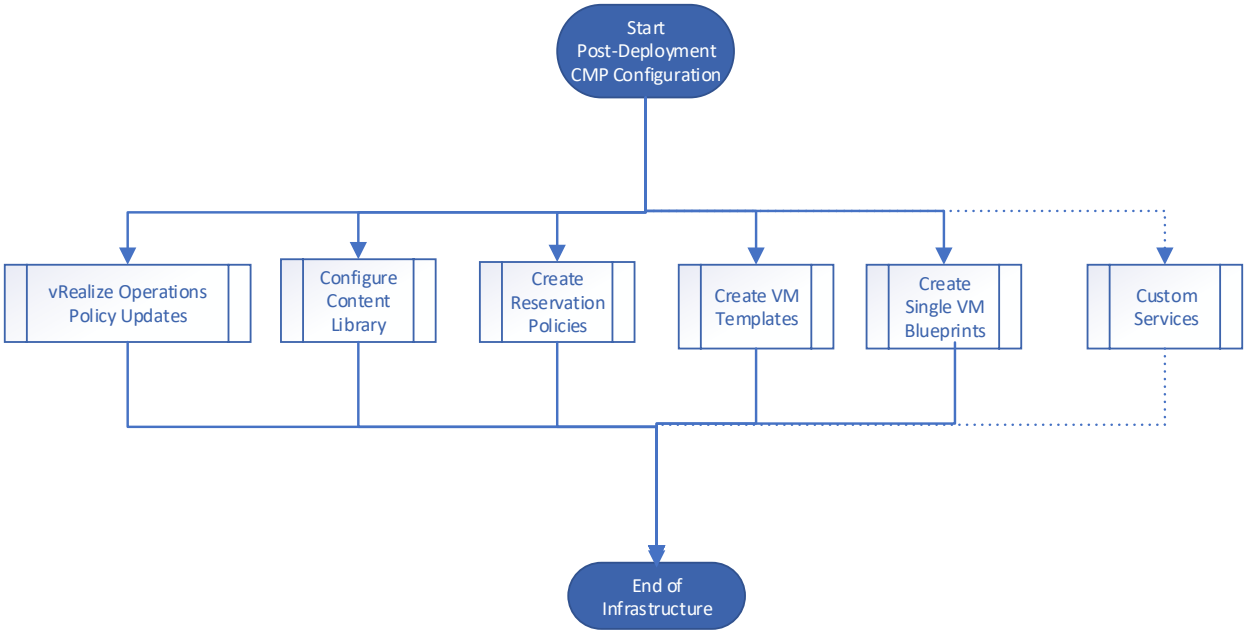


Figure 3. Post-deployment tasks

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

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 VMware Validated Design 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 - provides a documentation tool to collect details for the VxRail deployment.
- VMware Cloud Builder Deployment Parameters spread sheet - captures the configuration details for the SDDC deployment.

5.2.1 Dell EMC PEQ document

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.

5.2.2 VMware parameter excel document

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 is 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

5.2.3 Procedure

1. Obtain the relevant documents from Solve and the VMware Web Site 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 4. IP addresses and host names for the Platform Services controller load balancer and the Platform Services controller for the Management Cluster

Component	Hostname	IP Address	Domain
Platform Services Controller Load Balancer	lax01psc01	172.17.11.71	lax01.rainpole.local
Platform Services Controller for the Management Cluster	lax01m01psc01	172.17.11.61	lax01.rainpole.local

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

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

   b Right-click the **lax01.rainpole.local** zone, and select **New Host (A or AAAA)**.

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

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

   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**.

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 new signed certificates for the SDDC components in Region B.

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

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

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

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

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

5.4.2 Create and add a Microsoft Certificate Authority template

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

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

5.4.3 Procedure

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

Setting	Value
User	Active Directory administrator
Password	*ad_admin_password*

2. Click **Start** > **Run**, enter **certtmpl.msc**, and click **OK**.
3. In the Certificate Template console, under Template Display Name, right-click **Web Server** and select **Duplicate Template**.
4. In the Duplicate Template dialog box, leave Windows Server 2003 Enterprise selected for backward compatibility and click **OK**.
5. In the Properties of New Template dialog box, click the **General** tab.
6. In the Template display name text box, enter **VMware**.
7. Click the **Extensions** tab and configure the following:
    a. Select **Application Policies** and click **Edit**.
    b. Select **Server Authentication**, click **Remove**, and click **OK**.
    c. If the **Client Authentication** policy is present, select it, click **Remove**, and click **OK**.
    d. Select **Key Usage** and click **Edit**.
    e. Select the **Signature is proof of origin (nonrepudiation)** check box.
    f. Leave the default for all other options.
    g. Click **OK**.
8. Click the **Subject Name** tab, ensure that the Supply in the request option is selected, and click **OK** to save the template.
9. Add the new template to the certificate templates of the Microsoft CA.
    a. Click **Start > Run**, enter **certsrv.msc**, and click **OK.**
    b. In the **Certification Authority** window, expand the left pane, right-click **Certificate Templates**, and select **New > Certificate Template to Issue**.
    c. In the **Enable Certificate Templates** dialog box, select **VMware**, and click **OK**.

5.5 Generate signed certificates for the SDDC Components

Use the Certificate Generation Utility for VMware Validated Design (`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.

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 that hosts 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 and Edge Services for the Workload domain.

The first cluster, for the management Domain, provides the foundation for the SDDC environment. It is deployed using the VxRail embedded deployment procedure, resulting in the cluster hosting the platform services controller and vCenter instance which manage its resources. Those services are converted from VxRail Managed to customer managed after the VxRail cluster initialization is complete using a VxRail Manager conversion utility. 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 are 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 Pre-engagement qualification for the VxRail environment.

That 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.

Before you start:

- Make sure that you have a Windows host that has access to your data center. Use this host to connect to your hosts and perform configuration steps.
- Ensure that routing is in place between the two regional management networks 172.16.11.0/24 and 172.17.11.0/24 as it is necessary to join the common SSO domain.

6.1.1 IP addresses, hostnames, and network configuration

The following values are required to configure your hosts.

Table 1. Management Cluster Hosts

FQDN	IP	VLAN ID	Default Gateway	NTP Server
lax01m01esx01.lax01.rainpole.local	172.17.11.101	1711	172.17.11.253	ntp.lax01.rainpole.local ntp.sfo01.rainpole.local

FQDN	IP	VLAN ID	Default Gateway	NTP Server
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 VxRail management domain

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

4. Reference the details in the pre-deployment qualification (PEQ) assessment

   Work with the customer to obtain the details to complete the VxRail deployment.

5. 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.

6.3 Deploy the VxRail management cluster

Table 38. VxRail Manager, vCenter, and Platform Services controller details

FQDN	IP	VLAN ID	Default Gateway	P 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	l72.17.11.62	1711	172.17.11.253	ntp.sfo01.rainpole. local

Table 39. 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 40. 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 41. 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 42. 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 virtual appliance of VMware Cloud Builder in Region B and configure the appliance to support the infrastructure services deployment. 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.

Cloud builder also includes an option to generate VxRail configuration files in JSON format. Those files can be downloaded and used as input during the VxRail cluster initialization. At this point in the procedure, cloud builder is optionally deployed to generate the json file for the VxRail shared edge and compute cluster.

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 using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*Administrator password*

2. In the navigator, select the Data Center and click **Create / Register** VM.

3. The New virtual machine wizard appears.
4. On the Select creation type dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
5. On the Select OVF and VMDK files dialog box, enter **lax01cb01** for the virtual machine name, select the **VMware Cloud Builder.ova** file, and click **Next**.
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**.

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**.

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

6.5 Deploy the shared compute and edge platform service controller

VVD relies upon two platform services controllers for high availability and redundancy. In a dual-region deployment, the PSCs are federated providing configuration details including services accounts and vCenter service details across both regions.

The goal of this task is to deploy the necessary PSC services in Region B while also joining the PSCs to the Region A SSO domain.

In order to establish that linkage, we deploy the PSC for the Region B Shared Edge and Compute into the Region B Management vCenter. We then join that PSC to the shared edge and compute PSC in Region A (sfo01w01psc01.sfo01.rainpole.local)

This process enables the use of a common SSO domain for all components of the SDDC supporting vCenter enhance linked mode, as well as providing a common identity source to the Active Directory service accounts.

The embedded PSC in the Region B Management Domain will be replaced and linked to Region A during the automated workflows. It is in use supporting the Region B.

6.5.1 Procedure

1. Obtain a copy of the `vvd-bundle-johndory-5.0.0-13453959` software bundle.
    a. On a windows machine mount the ISO and extract the vCSA image from `<drive>:\vvd-bundle-johndory-5.0.0-13453959\vcenter_ova`
    b. Copy the ISO to the local drive.
2. 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`
3. Select the installation application to launch the deployment wizard.
4. Select the **Installer** option and click **Next.**
5. Accept the license agreement and continue.
6. Select the **deploy a Platform Services Controller** option from the External Platform Services Controller section of the form and click **Next**.
7. Enter the Fully Qualified Domain Name of the Region B Management vCenter Server `lax01m01vc01.lax01.rainpole.local`
8. Select the folder to install the VM.
9. Select the compute resource and click **Next**.
10. Enter the VM name `lax01w01psc01.lax01.rainpole.local` and the root password and click **Next**.
11. Select the vSAN datastore for the desired storage location and click **Next**.
12. Select the port group that begins with `vCenter`, and specify the FQDN, IP address, and other system properties and click **Next**.
13. Confirm that the values are correct and click **Finish**.

6.5.2 Join the PSC to the Region A SSO domain

When the PSC has completed deployment, perform the following tasks to configure the network properties and join it to the existing SSO domain in Region A. Note: The PSC will Join the workload PSC in Region A, and establish a new Site ID.

1. From the PSC configuration UI, select **Join and existing domain**.
2. Register the system with the shared edge and compute PSC in Region A.
    - `sfo01w01psc01.sfo01.rainpole.local`
3. Select **Add a new Site** and specify the site name for Region B, i.e. `Lax01`.
4. Enter `vsphere.local` as the SSO Domain name.

5. Confirm the join the VMWare CEIP check is selected and click **Next**.
6. Confirm the details and click **Finish** to deploy.
7. Log into the vCenter Server.
8. Select the **Administration option → System Configuration** interface
    a. Ensure that the `lax01w01psc01.lax01.rainpole.local` is listed in the node view.

6.6 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.

6.6.1 Procedure

1. Using the same Windows VM that was used to deploy the PSC, select the installer application to launch the deployment wizard.
2. Select the Installation option and click **Next**.
3. Accept the license agreement and continue
4. Select the deploy a vCenter Server option from the `External Platform Services Controller` section of the form and click **Next**.
5. Enter the **Fully Qualified Domain Name** of the Region B management vCenter Server `lax01m01vc01.lax01.rainpole.local`
6. Select the VM placement values, folder, compute resource, and click **Next**.
7. Enter the VM name `lax01w01psc01.lax01.rainpole.local` and the root password and click **Next**.
8. Select the vSAN datastore for the desired storage location and click **Next**.
9. Select the port group that begins with “vCenter, and specify the FQDN, IP address, and other system properties and click **Next**.
10. Confirm that the values are correct and click **Finish**.
    When the vCenter has been deployed, select **Continue** to join it to the `lax01w01psc01` Platform Services Controller in Region B.
11. Start the configuration process and select join and existing domain option by entering the target PSC that you would like to join `sfo01w01psc01.sfo01.rainpole.local`.
12. Select the configuration option
    a. Specify the `lax01w01psc01.lax.rainpole.local` platform services controller instance.
    b. Provide the SSO administrative credentials.
    c. Select **Next** to deploy the vCenter.

6.7 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.

For the second cluster a global account and entitlement were created within the vsphere.local domain. To support cases where the primary PSC becomes unavailable, we need to add the local account to the second PSC so vsphere.local account was created for the second Cluster initial configuration. Mirror that account on the second PSC so that you can perform VxRail Manager tasks if the primary PSC is unavailable.

The VxRail manager administrative account name in this example is `vxadmin`.

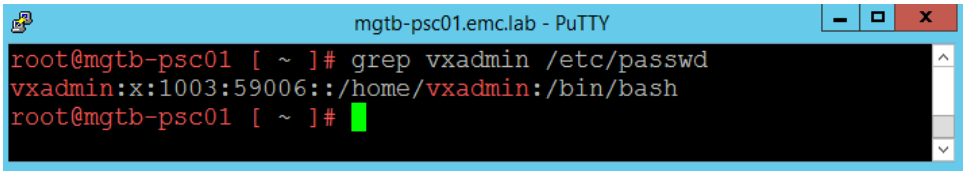
UID and GID values were obtained from the initial PSC.

6.7.1 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

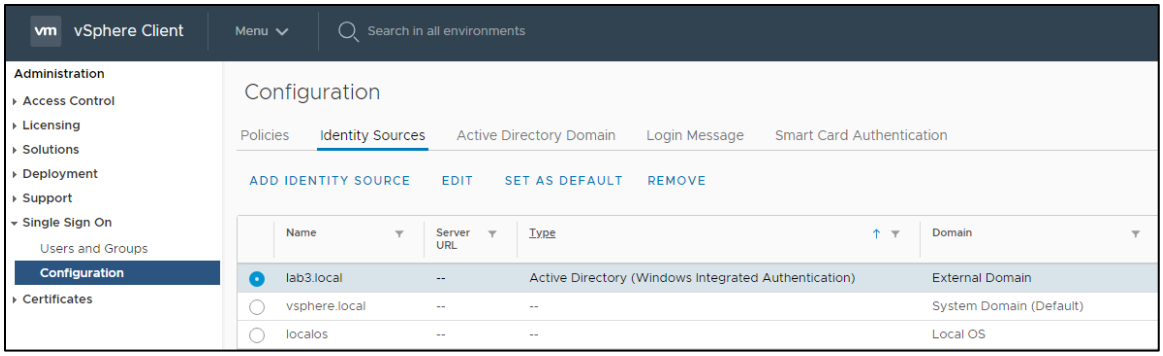
   ```
   passwd vxadmin
   ```

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**.

6.8 Join the PSC to Active Directory domain

To leverage the service accounts created in Region A, the newly created PSC must be joined to the Active Director Domain.

1. SSH or open the vCenter DCUI to access the `lax01w01psc01.lax01.rainpole.local` console.
2. Log in with the root account.
3. From the command line execute the following command to join the PSC to the Active Directory domain: `/opt/likewise/bin/domainjoin-cli join lax01.rainpole.local administrator [password]`
4. Reboot the PSC.
5. Log in to vCenter to set the domain as the default identity Source.
6. Log in to the vCenter client using the administrator account.
7. Select **Administration.**
8. Select **Single Sign On Configuration.**
9. Select **Identity Sources**.
10. If the domain does not appear, Select the **+** sign to add it.
    a. Select **Active Directory** and click **Next.**
    b. Click **Finish**.
11. Highlight the Active Directory from the identity source list and select **Set AS Default** to make it the default identity source.


vSphere Client
Menu
Search in all environments
Administration
Access Control
Licensing
Solutions
Deployment
Support
Single Sign On
Users and Groups
Configuration
Certificates
Configuration
Policies
Identity Sources
Active Directory Domain
Login Message
Smart Card Authentication
ADD IDENTITY SOURCE
EDIT
SET AS DEFAULT
REMOVE
Name
Server URL
Type
Domain
lab3.local
--
Active Directory (Windows Integrated Authentication)
External Domain
vsphere.local
--
--
System Domain (Default)
localos
--
--
Local OS

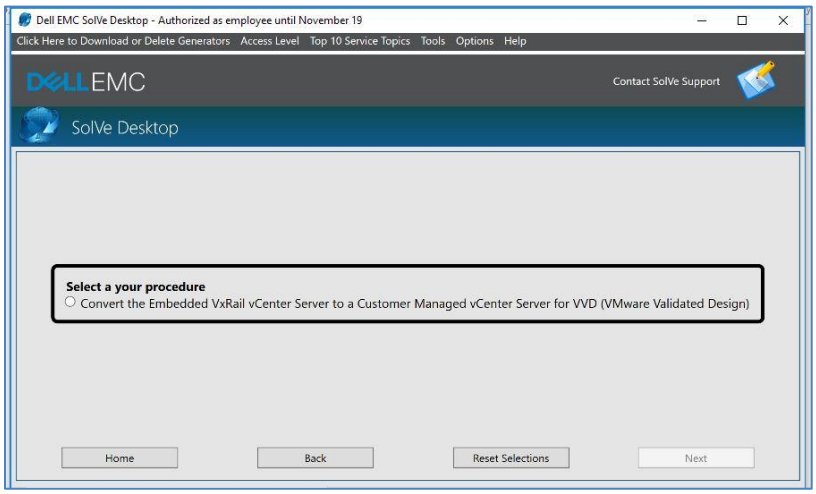
7 Convert the VxRail Management Cluster Internal vCenter and Platform Services Systems to Customer-Managed Systems

Before proceeding with the deployment, you must convert the PSC and vCenter to customer-managed systems. That task is performed through a python utility on the VxRail Manager server. The purpose of this task is to:

- Disassociate the services from VxRail Manager and prepares 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 l`ax01m01vc01` 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 Create shared edge vCenter datacenter for VxRail external vCenter deployment

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

7.2.1 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.

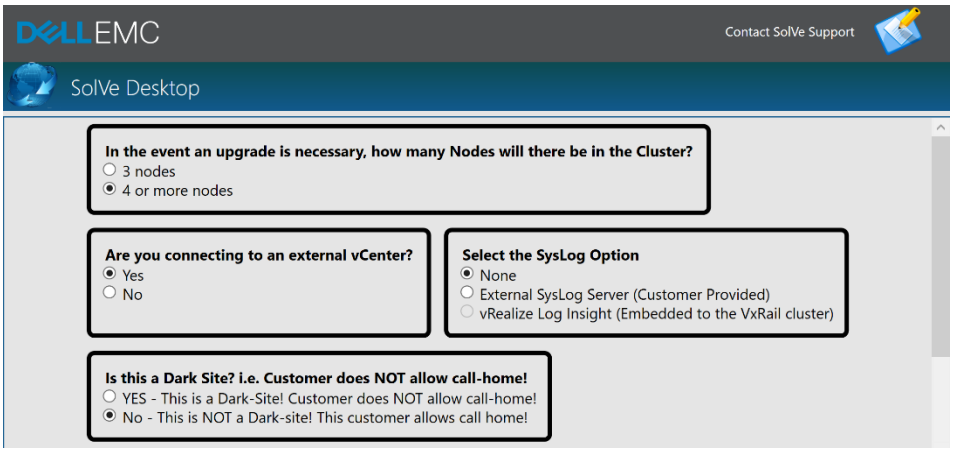
7.3 Deploy the shared edge and compute VxRail cluster

Reference 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

7.3.1 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 the 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 53. 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 54. Management cluster hosts

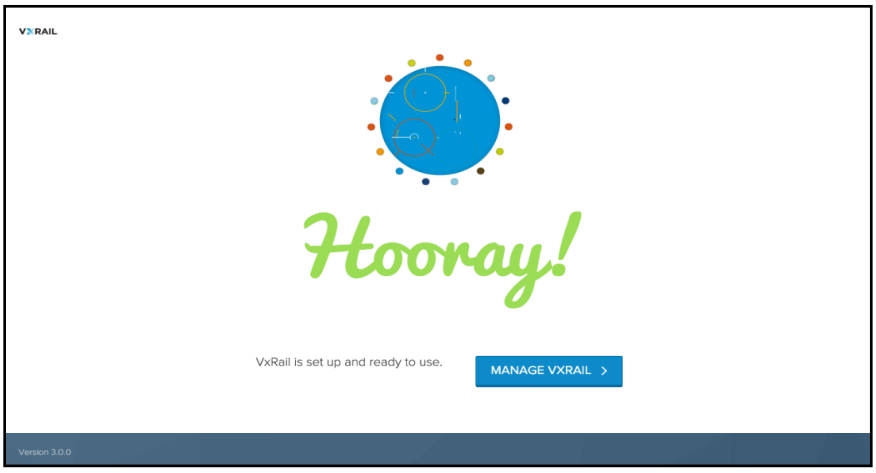
FQDN	IP	VLAN ID	Default Gateway
lax01w01esx01	172.17.31.101	1731	172.17.31.253
…	…		
lax01w01esx04	172.17.31.104		

Table 55. vSAN host configuration

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

Table 56. vMotion host configuration

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



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://lax01m01esx01.lax01.rainpole.local**.
   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2. Configure and start the SSH service.
   a. In the Navigator, click **Manage** and click the **Services** tab.
   b. Select the **SSH** service, and click the **Actions** menu.
   c. Select **Policy** and click **Start and stop with host**.
   d. Click **Start** to start the service.

9 Prerequisites for Cloud Management Layer

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

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

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

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 7. 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 8. Software requirements for the master Windows system

Component	Requirement
Operating System	Windows Server 2016 (64-bit)
VMware Tools	Latest version
Active Directory	Join the virtual machine to the lax01.rainpole.local domain.
Internet Explorer Enhanced Security Configuration	Turn off ESC.

Component	Requirement
Remote Desktop Protocol	Enable RDP access.
Java	▪ Java Runtime Environment (JRE) executable jre-8u191-windows-x64 or later. ▪ Set the *JAVA_HOME* environment variable to the Java installation directory. ▪ Update the *PATH* system variable to include the `bin` folder of Java installation directory.
Secondary Logon Service	Start the Secondary Logon service and set the start-up type to Automatic.

9.2 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 using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

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

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

9. Shut down the master Windows system virtual machine.

10 Prerequisites for Business Continuity Layer

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

10.1 Deploy and configure the Windows virtual machine for Site Recovery Manager

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

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

Table 9. Virtual machine requirements for Site Recovery Manager VM

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

Table 10. Network requirements for Site Recovery Manager VM

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

Table 11. Software requirements for the Site Recovery Manager VM

Setting	Value
Operating System	Windows Server 2016 (64-bit)
VMware Tools	Latest version.
Active Directory	Join the virtual machine to the lax01.rainpole.local domain.
License	Verify that you have obtained a VMware Site Recovery Manager license that satisfies the requirements of this design.
Internet Explorer Enhanced Security Configuration	Turn off ESC.
Remote Desktop Protocol	Enable RDP access.

10.2 Procedure

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

1. Log in to the Site Recovery Manager virtual machine by using a Remote Desktop Protocol (RDP) client.
   a Open an RDP connection to the lax01m01srm01.lax01.rainpole.local virtual machine.
   b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2. Click **Start**, right-click **Windows PowerShell**, and select **More > Run as Administrator**.
3. Add the `svc-srm` service account to the local Administrators group by running the following command.

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

4. Configure NTP settings.
   a Enable Windows Time Service and start by running the following commands.

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

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

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

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

```
w32tm /query /status
```

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. You then validate the deployment files against the necessary run parameters and start the automated deployment of the SDDC components for the management cluster and for the shared edge and compute cluster in Region B.

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

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

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 like WinSCP.
   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

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

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

   c Switch to the **root** user by running the `su` command.
   d Mount the VMware Validated Design software bundle `.iso` file and configure application properties by running the following command.

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

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

12 Generate the JSON Deployment Files for the Management and the Shared Edge and Compute Clusters

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 using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2. On the End User License Agreement page, click **Accept License Agreement**.
3. Generate the JSON file used for automated deployment of the SDDC components.
   a In the Cloud Builder Navigator, select the **Deployment Wizard** icon.
   b In the Upload Config File tab, from the **Select Architecture Type** drop-down menu, select the **VVD for SDDC Region B** architecture and click the **Upload Config File** button.
   c Navigate to the Deployment Parameters XLS file and click **Open**.
   d Click the **Generate JSON** button.

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

Table 12. Region B JSON Deployment Files

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

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

Table 13. 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 Target Environment Prerequisites

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

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 14. 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 using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2. In the Cloud Builder Navigator, click the **Deployment Wizard** icon.
3. Select the **Validate Environment** tab.
4. From the Select File to Validate drop-down menu, select the `vvd-std-regb-mgmt.json` file and click **Validate**.
5. If validation fails because of issues with the signed certificate files, resolve the issues and reupload the modified certificate files.
   a Upload the modified certificate files to the Cloud Builder appliance using an SCP software like WinSCP.
   b Open an SSH connection to lax01cb01.lax01.rainpole.local.
   c Run the following command.

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

   When prompted, enter the *cloudbuilder_root_password*.

   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. On 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-std-regb-mgmt.json` file and click **Validate**.
   The `vvd-std-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-std-regb-comp.json` file and click **Validate**
    The `vvd-std-regb-comp.json` file is successfully validated against the predefined run parameters.
11. After successful validation of `vvd-std-regb-mgmt.json` and `vvd-std-regb-comp.json` files, click **Next** to start the deployment of the management cluster.

13.2 Start the automated deployment of the management cluster

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

Procedure

1. Log in to VMware Cloud Builder.
   a Open a Web browser and go to **https://lax01cb01.lax01.rainpole.local**.
   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2. In the Cloud 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-std-rega-mgmt.json` file and click **Deploy**.

   The automated deployment of the components in the management cluster starts.
5. Monitor the deployment and check the following log files for errors.

Table 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-std-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 using the following credentials.

Setting	Value
User name	admin
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-std-regb-comp.json** file and click **Deploy**.
   The automated deployment of the components in the shared edge and compute cluster starts.
5. Monitor the deployment and check the following log files for errors.

Table 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 Operations Management Configuration

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

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

14.1.1 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.

14.1.2 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 using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2. On the main navigation bar, click **Administration**.
3. Configure the authentication sources to enable an automatic synchronization for the `lax01.rainpole.local` Active Directory instance.
   a In the left pane, click **Access** and click **Authentication Sources**.
   b On the Authentication Sources page, select **lax01.rainpole.local** and click **Edit**.
   c In the Edit Source for User and Group Import dialog box, expand **Details** and select **Automatically synchronize user membership for configured groups**.
   d Click **OK**.

14.2 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.

14.2.1 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 using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2. On the main navigation bar, click **Administration**.
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. From the solution table on the Solutions page, select the **VMware vSphere** solution, and click the **Configure** icon at the top.
   The **Manage Solution - VMware vSphere** dialog box appears.
5. Under Instance Settings, select the **lax01m01vc01** vCenter adapter.
6. Click **Define Monitoring Goals**.
7. Under Enable vSphere Hardening Guide Alerts, click **Yes**, leave the default configuration for the other options, and click **Save**.
8. In the Success dialog box, click **OK**.
9. Click **Save Settings**.
10. In the Info dialog box, click **OK**.
11. Repeat Step 5 to Step 10 for the Compute vCenter Server adapter.
12. In the Manage Solution - VMware vSphere dialog box, click **Close**.

15 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. You finish the SDDC configuration in your environment and confirm a successful provisioning of virtual machines using newly created blueprints.

15.1 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.

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

15.2 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.

15.2.1 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 using the following credentials.

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

2. From the Home menu, select **Content Libraries**.
3. In the Navigator pane, click the **sfo01-w01cl-vra01** content library that was created in the Compute vCenter Server in Region A.
4. Under Publication, click the **Copy Link** button.
   The subscription URL is copied to the clipboard.
5. Log in to vCenter Server by using the vSphere Client.
   a Open a Web browser and go to **https://lax01m01vc01.lax01.rainpole.local/ui**.
   b Log in using the following credentials.

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

6. From the Home menu, select **Content Libraries**, and click the **+** icon.
   The **New Content Library** wizard appears.
7. On the Name and location page, enter the following settings and click **Next**.

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

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

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

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

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

15.3 Create reservation policies

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

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

15.3.1 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 using the following credentials.

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

2. Navigate to **Infrastructure > Reservations > Reservation Policies**.
3. Click the **New** icon, configure the following settings, and click **OK**.

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

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

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

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

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

15.4 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 17. Business Group Names

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

15.4.1 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 using the following credentials.

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

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

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

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

4. On the New Reservation - vSphere (vCenter) page, click the **Resources** tab.
   a Select **lax01-w01-comp01 (lax01w01vc01.lax01.rainpole.local)** from the Compute resource drop-down menu.
   b In the **This Reservation** column of the **Memory (GB)** table, enter **200**.
   c In the **Storage (GB)** table, select the check box for your primary datastore, for example, `lax01-w01-vsan01`, enter **2000** in the **This Reservation Reserved** text box. Enter **1** in the **Priority** text box, and click **OK**.
   d Select **lax01-w01rp-user-vm** from the **Resource pool** drop-down menu.
5. On the New Reservation - vSphere (vCenter) page, click the **Network** tab.
6. On the Network tab, select 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.

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

   b Configure the Development Business Group with the following values.

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

7. Click **OK**.
8. Repeat this procedure and create a reservation for the Development Business Group.

15.5 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 18. Business Group Names

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

15.5.1 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 using the following credentials.

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

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

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

4. On the New Reservation - vSphere (vCenter) page, click the **Resources** tab.
   a. Select **lax01-w01-comp01(lax01w01vc01.lax01.rainpole.local)** from the **Compute resource** drop-down menu.
   b. Enter **200** in the **This Reservation** column of the **Memory (GB)** table.
   c. In the **Storage (GB)** table, select the check box for your primary datastore, for example, `lax01-w01-vsan01`, enter **2000** in the **This Reservation Reserved** text box. Enter **1** in the **Priority** text box, and click **OK**.

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

5. On the New Reservation - vSphere (vCenter) page, click the **Network** tab.
6. From the **Network Paths** list, select the network path check boxes listed in the following table, and from the **Network Profile** drop-down menu select the corresponding network profile for the business group whose reservation you are configuring.

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

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

7. Click **OK** to save the reservation.
8. Repeat the procedure to create an edge reservation for the development business group.

15.6 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 19. VM Templates and Their Guest Operating Systems

VM Template Name	Guest OS
Windows-2012r2-64	Windows Server 2012 R2 (64-bit)
Windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)
Redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)

15.6.1 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 using the following credentials.

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

2. From the Home menu, select **VMs and Templates**.
3. Expand the **lax01w01vc01.lax01.rainpole.local** vCenter Server.
4. Right-click the **lax01-w01dc** data center and select **New Folder > New VM and Template Folder**.
5. Create a folder and label it **VM Templates**.
6. Navigate to **Menu > Content Libraries**.
7. Click **lax01-w01cl-vra01> Templates**.
8. Right-click the **windows-2012r2-64** VM Template and click **New VM from This Template**.
   The **New Virtual Machine from Content Library** wizard opens.
9. On the Select name and location page, use the same template name.
   Note Use the same template name to create a common service catalog that works across different vCenter Server instances within your data center environment.
10. Expand the **lax01-w01dc** data center, select **VM Templates** as the folder for this virtual machine, and click **Next**.
11. On the Select a resource page, expand cluster **lax01-w01-comp01**, select the **lax01-w01rp-user-vm** resource pool, and click **Next**.
12. On the Review details page, verify the template details, and click **Next**.
13. On the Select storage page, select the **lax01-w01-lib01** datastore and **Thin Provision** from the Select virtual disk format drop-down menu and click **Next**.
14. On the Select networks page, select **lax01-w01-vds01-management** for the **Destination Network**, and click **Next**.
    Note vRealize Automation changes the network according to the blueprint configuration.
15. On the Ready to complete page, review the configurations you made for the virtual machine, and click **Finish**.
    A new task for creating the virtual machine appears in the Recent Tasks pane. The new virtual machine is created after the task finishes.
16. Repeat this procedure for all the VM templates in the content library.

15.7 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 20. VM templates and their guest operating systems

VM Template Name	Guest OS
Windows-2012r2-64	Windows Server 2012 R2 (64-bt)
Windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)
Redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)

15.7.1 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 using the following credentials.

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

2. From the **Home** menu, select **VMs and Templates**.
3. In the **Navigator** pane, expand **lax01w01vc01.lax01.rainpole.local>lax01-w01dc> VM Templates**.
4. Right-click the **windows-2012r2-64** virtual machine located in the **VM Templates** folder, and click **Template > Convert to Template**.
5. Click **Yes** and confirm the template conversion.

16 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.

16.1 Create a service catalog

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

16.1.1 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 using the following credentials.

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

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

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

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

16.2 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.

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

16.2.1 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 using the following credentials.

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

2. Navigate to **Infrastructure > Compute Resources > Compute Resources**.
3. In the **Name** column, point to the compute cluster **lax01-w01-comp01**, and select **Data Collection** from the drop-down menu.
4. Click the four **Request now** buttons in each field on the page.

   Wait for the data collection process to complete.

5. Click **Refresh**, and verify that **Status** shows `Succeeded` for both **Inventory** and **Network and Security Inventory**.
6. Navigate to **Design > Blueprints > New**.
7. In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

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

8. Select and drag the **vSphere (vCenter) Machine** icon to the **Design Canvas**.
9. Click the **General** tab, configure the following settings, and click **Save**.

Setting	Default
ID	Default setting (vSphere_vCenter_Machine_1)
Description	Default setting (blank)
Display location on request	Deselected
Reservation policy	LAX-Production-Policy
Machine prefix	Use group default
Instances: Minimum	Default setting
Instances: Maximum	Default setting

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

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	Name: windows-2012r2-64 Endpoint: lax01w01vc01.lax01.rainpole.local
Customization spec	**os-windows-joindomain-custom-spec**

Note If the value of the **Clone from** setting does not list **windows-2012r2-64** template, you must perform a data collection on the **lax01-w01-comp01** Compute Resource.

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

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

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

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

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

Blueprint Name	Existing network
Windows Server 2012 R2 - LAX Prod	Ext-Net-Profile-Production-Web

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

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

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

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

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

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

16.3 Configure entitlements of blueprints

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

Repeat this procedure to associate the three blueprints with their entitlement.

Blueprint Name	Service Catalog	Add to Entitlement.
Windows Server 2012 R2 - LAX Prod	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Prod	LAX Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Prod	LAX Service Catalog	Prod-SingleVM-Entitlement

16.3.1 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 using the following credentials.

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

2. Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.
3. On the **Catalog Items** pane, select the **Windows Server 2012 R2 - LAX Prod** blueprint in the **Catalog Items** list and click **Configure**.
4. On the **General** tab of the **Configure Catalog Item** dialog box, select **LAX Service Catalog** from the **Service** drop-down menu, and click **OK**.
5. Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement.

    a Click **Entitlements** and select **Prod-SingleVM-Entitlement**.

    The **Edit Entitlement** pane appears.

    b Select the **Items & Approvals** tab and add the **Windows Server 2012 R2 - LAX Prod** blueprint to the **Entitled Items** list.

    c Click **Finish**.

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

16.4 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.

16.4.1 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 using the following credentials.

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

2. Click the **Catalog** tab, click **Click here to apply filters**, and select **LAX Service Catalog** from the catalog of available services.
3. Click the **Request** button for the **Windows Server 2012 R2 - LAX Prod** blueprint and click **Submit**.
4. Verify that the request finishes successfully.

    a Click the **Deployments** tab.

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

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

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

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

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

b Log in using the following credentials.

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

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

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

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

17 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.

17.1 Add data center locations to the Compute Resource Menu

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

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

17.1.1 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 using the following credentials.

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

2. Open a VM console to the IaaS Web server virtual machine vra01iws01a, and log in using administrator credentials.
3. Add the data centers for the two regions of the SDDC.

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

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

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

   c Save and close the file.

4. Restart the vra01iws01a virtual machine.

   Wait until the virtual machine restarts and is successfully running.

5. Repeat this procedure for the vra01iws01b virtual machine.

17.2 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.

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

17.2.1 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 using the following credentials.

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

2. Navigate to **Infrastructure > Compute Resources > Compute Resources**.
3. Select the **sfo01-w01-comp01** compute resource and click **Edit**.
4. From the **Location** drop-down menu, select the **SFO** data center location for sfo01-w01-comp01.
5. Click **OK**.
6. Repeat this procedure and set the data center location for lax01-w01-comp01.

17.3 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.

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 using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*

Setting	Value
Domain	rainpole.local

2. Navigate to **Administration > Property Dictionary > Property Definitions**.
3. Click **New** and create a property definition.

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

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

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

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

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

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

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

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

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

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

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

   j Deselect **Enable custom value entry**.

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

Name	Value
San Francisco	SFO
Los Angeles	LAX

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

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

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

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

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

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

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

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

17.4 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.

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 using the following credentials.

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

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

   a Click **New**.

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

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

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

   e Click **OK**.

17.5 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.

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)

17.5.1 Procedure

3. Log in to the vRealize Automation Rainpole portal.

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

   b Log in using the following credentials.

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

4. Navigate to **Infrastructure > Reservations > Reservations** and click **New > vSphere (vCenter)**.
5. On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values.

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

6. 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.

7. 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.

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

8. Click **OK** and save the reservation.
9. Repeat the procedure and create a reservation for Region B.

17.6 Create a service catalog for the unified blueprint

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

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

17.6.1 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 using the following credentials.

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

2. Navigate to **Administration > Catalog Management > Services**.
3. Click **New**.

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

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

   c Click **OK**.

17.7 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.

17.7.1 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 using the following credentials.

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

2. Associate the **Unified Blueprint Catalog** with the **Prod-SingleVM-Entitlement entitlement** that you created earlier.

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

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

   The **Edit Entitlement** window appears.

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

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

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

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

17.8 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.

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

17.8.1 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 using the following credentials.

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

2. Navigate to **Design > Blueprints > New**.
3. In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

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

4. Select and drag the **vSphere (vCenter) Machine** icon to the Design Canvas.
5. Click the **General** tab, configure the following settings, and click **Save**.

Setting	Value
ID	Default setting (vSphere_vCenter_Machine_1)

Setting	Value
Reservation Policy	UnifiedBlueprint-Policy
Machine Prefix	Use group default
Instances: Minimum	Default setting
Instances: Maximum	Default setting

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

Setting	Value
Blueprint Type	Server
Action	Clone
Provisioning Workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	**os-windows-joindomain-custom-spec**

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

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

8. Click the **Network** tab.

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

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

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

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

   d Click **Save**.

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

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

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

9. Click the **Properties** tab.

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

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

10. Click **OK**.
11. Click **Finish** and save the blueprint.
12. Select the blueprint **Windows Server 2012 R2 - Unified** and click **Publish**.
13. Navigate to **Administration > Catalog Management > Catalog Items** and add the blueprint to the **Unified Single Machine Catalog**.

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

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

17.9 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.

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

17.9.1 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 using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*

Setting	Value
Domain	rainpole.local

2. Select the **Catalog** tab, select **Click here to apply filters**, and click **Unified Single Machine Catalog** from the catalog of available services.
3. Click the **Request** button for one of the blueprints.
4. Select vSphere_**vCenter**_**Machine**_**1**.
5. Select San **Francisco** from the **Select a Region** drop-down menu, and click **Submit**.
6. Click Submit.
7. Verify the request finishes successfully.

   a Select the **Deployments** tab.

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

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

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

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

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

   b Log in using the following credentials.

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

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

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

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

10. Repeat this procedure for Region B.

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

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

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

A.1 Appendix A - Troubleshooting

In many cases a failed task can be mitigated by logging into the system where the task was being performed and either observing the current state and log information that may be present from the failed effort, or by attempting to perform the task manually and observing the result.

Cloud Build can detect the presence of the corrected task and continue its execution flow.

A.1.1 Cloud Builder deployment logs

The following log is useful for monitoring and identifying additional details related to a failed task.

`/opt/vmware/bringup/logs/vcf-bringup-debug.log`

If a task fails, view the most recent exception which includes a java exception and additional messages.

If the task fails and support is required, extract a copy of the `vcf-bringup` log files and the `rest-api` log file. I include these files in the SR case.

A.1.2 BGP pairing fails

If the BGP pairing task fails, it is like the result of an incorrect network or password configuration for the ESGs,

At this point in the workflow the NSX controllers and ESGs have been deployed, so it is possible to log into them and observer the configuration.

It is further possible to log into the ESGs and manually view the BGP pairing details by running a command such as

```
show ip bgp neighbors.
```

Each interface should be paired and have a state of `Established`.

If there is an error in this task, isolate it to the interface which is not in the established state, and then troubleshoot the configuration details on both the switch and NSX ESG.

A.1.3 Cloud Builder Web UI reports REST API not started

In certain cases, the Cloud Builder Web UI might behave unexpectedly such as not uploading the config file or performing an auto-logout. If you experience any similar issues, close the web browser and start a new session with a fresh browser.