VMware Validated Design for SDDC v5.1.1 on Dell EMC VxRail

VMware Cloud Builder Deployment for Region A

Deployment Guide

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. It uses the VMware Cloud Builder virtual appliance to automate the implementation of this validated design on Dell EMC VxRail appliances.

January 2020

CONTENTS

Table of Contents

CHAPTER 1

Executive Summary

This chapter presents the following topics:

Document purpose

This deployment guide provides detailed instructions for installing, configuring, and operating a software-defined data center (SDDC) based on the VMware Validated Design (VVD) for SDDC. It uses the VMware Cloud Builder virtual appliance to automate the implementation of this validated design on Dell EMC VxRail appliances.

This deployment guide does not contain instructions for performing all required post-configuration tasks, which are specific to the requirements of your organization.

Audience

This deployment guide is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with VMware software. It enables them 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.

We value your feedback

Dell EMC and the authors of this document welcome your feedback on the solution and the solution documentation.

Contact the Dell EMC Solutions team by email or provide your comments by completing our documentation survey.

CHAPTER 2

VVD on VxRail Deployment Overview

This chapter presents the following topics:

Introduction

This deployment uses VMware Cloud Builder for VxRail, which is designed to expedite the delivery of VVD on VxRail hyperconverged infrastructure (HCI) appliances.

Cloud Builder for VVD automates the deployment and configuration of most SDDC systems and services. The deployment flow for Cloud Builder VVD on VxRail is designed to better support services alignment. The deployment is logically separated into three phases with distinct start and end points so that you can complete each phase according to skill set or service definition agreement.

Phase 1—Deploy VxRail clusters

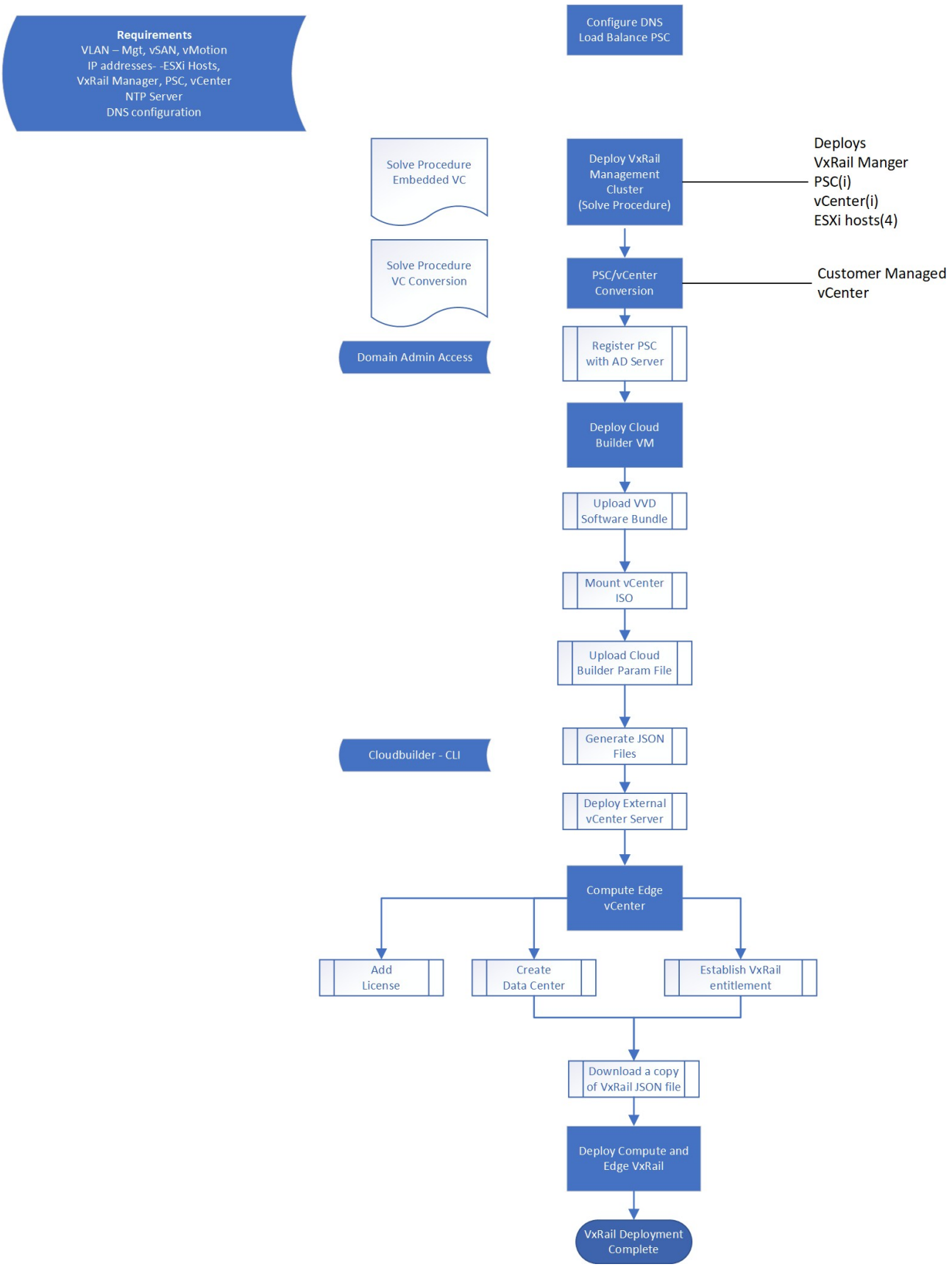
Set up the VxRail infrastructure for the SDDC environment.

Phase 1 includes the following tasks, which are detailed in Deploying VxRail on page 15:

- Deploy two VxRail clusters for the Management and Shared Edge and Compute domains. Each cluster requires a minimum of four Dell 14 G nodes.
- Deploy the VxRail Management cluster with embedded vCenter and Platform Services Controller (PSC) virtual machines. After the cluster is deployed, use the VxRail vCenter conversion utility to convert the systems to customer-managed systems.
- Deploy the Cloud Builder VM to establish the external vCenter for the VxRail Shared Edge and Compute cluster. Deploy the second vCenter Server using the ISO or a scripted process.
- Complete the following additional tasks on the VxRail Shared Edge and Compute vCenter: Procedures for these tasks are available in the *VxRail External vCenter deployment* SolVe procedure at https://solveonline.emc.com.
  - Create a data center that matches the parameter file.
  - Create a vCenter user account for the VxRail administrator.
  - Assign the vCenter VMware HCIA entitlement to the account.

The following figure represents the phase 1 tasks:

Figure 1 Phase 1 deployment flow



Phase 2—Deploy the Cloud Builder SDDC clusters

Phase 2 validates the environment readiness for the Management and Shared Edge and Compute clusters. It automates the deployment of the SDDC using the details that are defined in the parameter file.

Complete and verify the following prerequisites before the Cloud Builder preparation:

- Configure the network switches.
- Populate the parameter file.
- Obtain machine certificates.
- Add the Active Directory user and service accounts.

Phase 2 includes the following tasks, which are detailed in Deploying the SDDC Components on page 40:

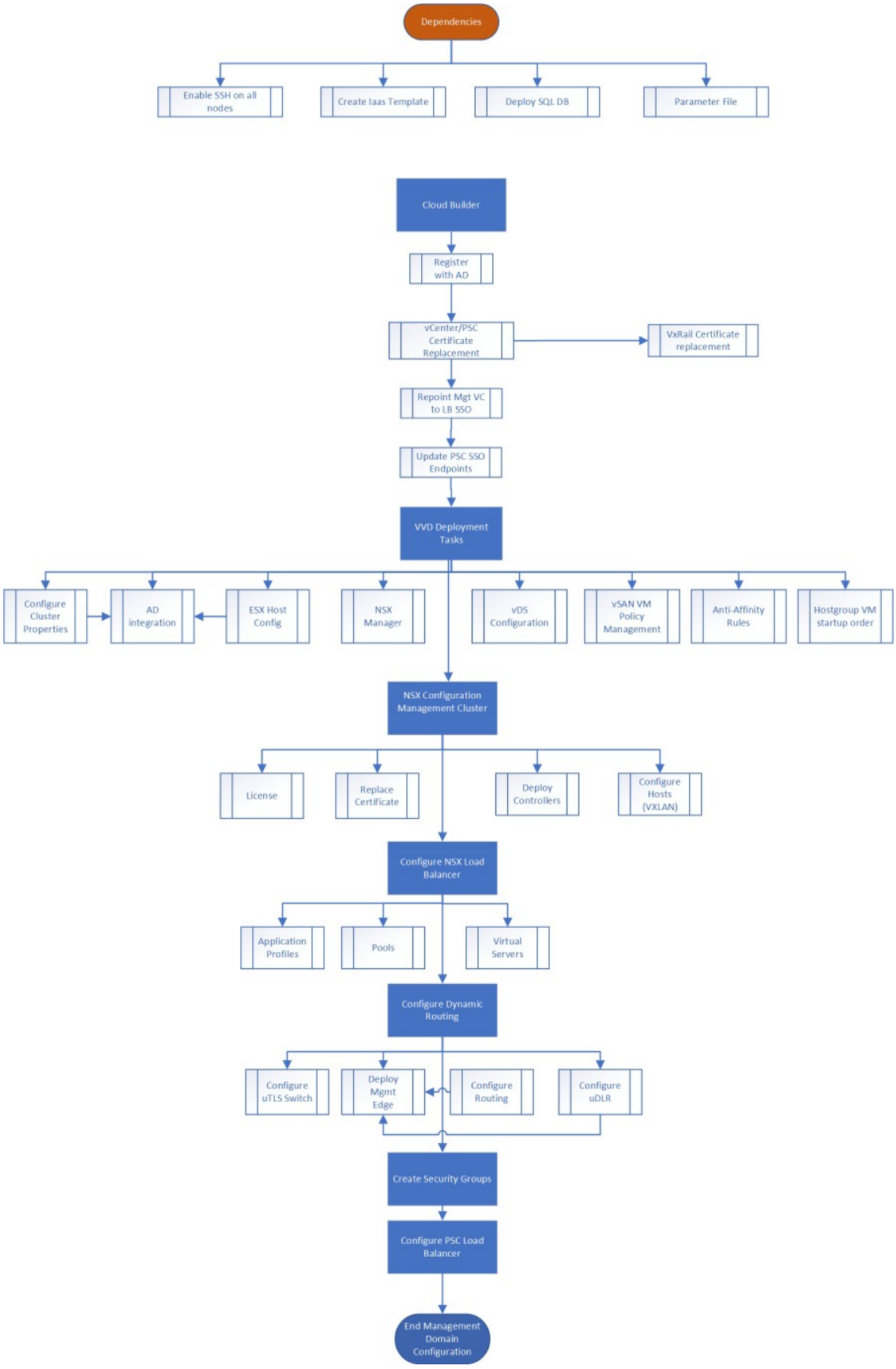
- Deploy and configure SQL Database for vRealize Automation.
- Deploy and configure Cloud Builder Virtual Appliance.
- Validate the environment
- Generate certificates for the VVD systems within the environment.
- Deploy NSX Manager, Controllers, and Edge Services.
- Configure dynamic routing.
- Deploy vRealize Suite (vRealize Automation, vRealize Operations, Log Insight, vRealize Business).

Note

Some components, such as VMware vCenter Update Manager, are optional for VVD on VxRail. Cloud Builder enables you to select deployment components by using the parameter file.

The following figure represents the phase 2 tasks:

Figure 2 Phase 2 deployment flow



Phase 3—Complete post-deployment tasks

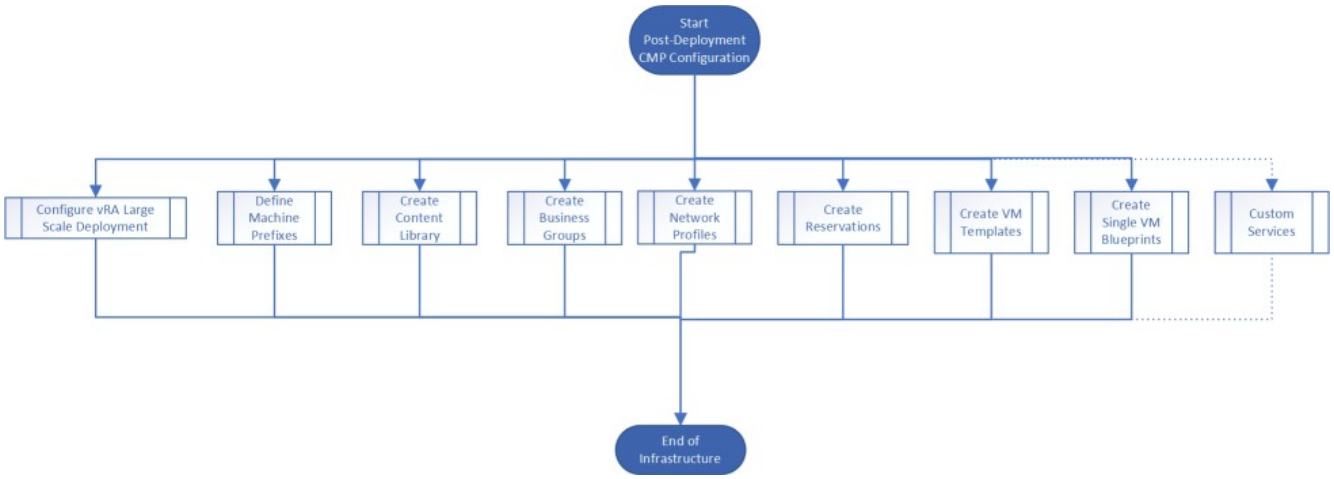
Phase 3 consists of Cloud Builder post-deployment tasks, including Cloud Management Platform configuration to prepare for monitoring, logging, and reporting operations.

Phase 3 includes the following tasks, which are detailed in Post-deployment: Configuring the Virtual Infrastructure on page 44, Post-deployment: Configuring vRealize Operations Manager on page 52, and Post-deployment: Configuring the Cloud Management Platform on page 56:

- Configure the Cloud Management Platform to provide templates, blue prints, and consumable catalog services.
- Complete the tasks to establish monitoring, logging, and reporting operations.
- (Optional) Complete custom services for complex workflows and services (not covered in this document.)

The following figure represents the phase 3 tasks:

Figure 3 Phase 3 deployment workflow



CHAPTER 3

Requirements and Prerequisites

This chapter presents the following topics:

Required software

Ensure that the software in your environment meets the requirements for this deployment.

Dell software

The products that are described in this document have been validated with the VxRail 4.7.111 software release. Version 5.01 is supported on VxRail 4.7.1 release versions.

VMware software

The *VMware Validated Design Deployment of Region A* documentation is compliant and validated with certain product versions. See *VMware Validated Design Release* Notes for more information about supported product versions.

Required hardware

Ensure that your environment meets the requirements for this deployment.

The following table lists the hardware specifications for the management domain and the compute domain:

Table 2 VxRail appliance specifications per domain

Hardware	Description
Servers	Four VxRail Dell 14G Appliances (Nodes)
CPU (per server)	Dual-socket, 8 cores per socket
Memory (per server)	192 GB* Recommended: 384 GB
Storage (per server)	BOSS with 2 x 240 GB SATA M.2
	One 400 GB SSD - caching tier
	Two 1.2 TB hard drive @ 10 K RPM - capacity tier
NICs per server	Four 10 GbE or 25 GbE NICs One 1 GbE BMC network adapter

*__Note__: The VVD documentation has a recommended memory configuration of 256 GB. The VxRail DIMM architecture does not support a 256GB configuration. The next memory increment with fully populated DIMM slots is 384 GB.

Complete the pre-engagement qualification form

Ensure that you have obtained all the deployment requirements.

Capture the installation details for the VxRail deployment by using the Dell EMC VxRail pre-engagement qualification (PEQ) form, available in the **Enablement Tools** section of Dell EMC SolVe Online for VxRail. Use the VxRail information in the PEQ to populate the Cloud Builder parameters file.

Required SolVe procedures

Download the SolVe procedures that you need for the deployment. Go to Dell EMC SolVe Online for VxRail, and download the following procedures:

- *VxRail Installation procedure for Embedded vCenter*
- *VxRail Installation procedure for External vCenter*
- VVD procedures:
  - *Convert the Embedded VxRail vCenter Server to a Customer-Managed- vCenter Server for VVD.*
  - *Enable VVD Cloud Builder for VxRail.*

CHAPTER 4

Deploying VxRail

This chapter presents the following topics:

Configure DNS settings for VxRail clusters

Configure DNS settings for Management and Shared Edge and Compute cluster hosts.

See the following tables to configure DNS settings for hosts in the Management domain and Shared Edge and Compute domain:

Table 3 Management cluster host values

FQDN	IP address
sfo01m01vxm01.sfo01.rainpole.local	172.16.11.100
sfo01m01psc01.sfo01.rainpole.local	172.16.11.61
sfo01m01vc01.sfo01.rainpole.local	172.16.11.62

Table 4 Management domain ESXi host values

Management ESXi Hosts	IP
sfo01m01esx01.sfo01.rainpole.local	172.16.11.101
sfo01m01esx02.sfo01.rainpole.local	172.16.11.102
sfo01m01esx03.sfo01.rainpole.local	172.16.11.103
sfo01m01esx04.sfo01.rainpole.local	172.16.11.104

Table 5 Shared Edge/Compute cluster host values

FQDN	IP address
sfo01w01vxm01.sfo01.rainpole.local	172.16.11.69
sfo01w01psc01.sfo01.rainpole.local	172.16.11.63
sfo01w01vc01.sfo01.rainpole.local	172.16.11.64

Table 6 Shared Edge/Compute domain ESXi host values

ESXi Hosts	IP
sfo01w01esx01.sfo01.rainpole.local	172.16.31.101
sfo01w01esx02.sfo01.rainpole.local	172.16.31.102
sfo01w01esx03.sfo01.rainpole.local	172.16.31.103
sfo01w01esx04.sfo01.rainpole.local	172.16.31.104

Configure DNS Settings for PSC load balancer

This VVD deploys two PSCs behind a load balancer that is implemented through NSX for vSphere. When you prepare your environment for automated deployment using Cloud Builder, NSX for vSphere is not yet available. Perform DNS configuration to emulate an existing load balancer IP address for the PSC load balancer in Region A.

Before you begin

Verify that the following static IP addresses are allocated:

- Static IP address for the Management PSC
- Static IP address for the PSC Load Balancer Virtual IP

Table 7 IP addresses and host names for the PSC load balancer and the PSC for the management cluster

Component	Host name	IP address	Domain
PSC Load Balancer	sfo01psc01	172.16.11.71	sfo01.rainpole.local
PSC for the Management Cluster	sfo01m01psc01	172.16.11.61	sfo01.rainpole.local

Procedure

1. Log in to the `dc01rpl.rainpole.local` DNS server.
2. From the Windows **Start** menu **Search** bar, type **`dnsmgmt.msc`** and press Enter.
3. In the **DNS Manager** dialog box, create an **A Record** for the PSC load balancer name VIP:
   a. Expand **Forward Lookup Zones**.
   b. Right-click the sfo01.rainpole.local zone, and select **New Host (A or AAAA)**.
   c. Enter the following values, and then click **Add Host**:
      - Name: **`sfo01psc01`**
      - Fully qualified domain name (FQDN): **`sfo01psc01.sfo01.rainpole.local`**
      - IP address: **`172.16.11.61`**
      - Clear **Create associate pointer (PTR) record**

      Note

      To create an operational network configuration for `sfo01psc01.sfo01.rainpole.local`, Cloud Builder requires forward lookup with IP 172.16.11.61 and reverse lookup with IP 172.16.11.71 (the load balancer VIP). Ensure that the A Record and the pointer (PTR) record are not associated and hover over different IP addresses.
4. Create a pointer (PTR) record for the PSC Load Balancer VIP and point it to the A Record of the PSC Load Balancer VIP:
   a. Expand **Reverse Lookup Zones**.
   b. Right-click the 11.16.172.in-addr.arpa zone, and select **New Pointer (PTR)**.
   c. Type the following values, and then click **OK**:

Host IP address: `172.16.11.71`

Fully qualified domain name (FQDN): `71.11.16.172.in-addr.arpa`

Host name: `sfo01psc01.sfo01.rainpole.local`

Deploy the VxRail Management cluster

Use the VxRail Installation with embedded vCenter Server SolVe procedure to deploy the management cluster.

Before you begin

Ensure that you have:

- A Windows host that has access to your data center. Use this host to connect to the data center and perform configuration steps.
- Downloaded the VxRail SolVe Installation procedure from Dell EMC Solve Online for VxRail embedded vCenter deployment
- Populated DNS with forward and reverse lookup records of the VxRail PSC, vCenter, and ESXi hosts.

See the system properties in the following tables to deploy the VxRail cluster:

Table 8 VxRail first-run host requirements

FQDN	IP address	VLAN ID	Default gateway	NTP server
sfo01m01vxm01.sfo01.rainpole.local	172.16.31.100	1611	172.16.11.253	ntp.sfo01.rainpole.local
sfo01m01psc01.sfo01.rainpole.local	172.16.31.61			
sfo01m01vc01.sfo01.rainpole.local	172.16.31.62			

Table 9 VxRail Management cluster hosts

Hostname FQDN range	IP range	VLAN ID	Default gateway	NTP server
sfo01m01esx01.sfo01.rainpole.local – sfo01m01esx04.sfo01.rainpole.local	172.16.11.101 – 172.16.11.104	1611	172.16.11.253	▪ ntp.sfo01.rainpole.local ▪ ntp.lax01.rainpole.local

Table 10 vSAN host configuration

Hostname FQDN range	IP range	VLAN ID	Default gateway
sfo01m01esx01.sfo01.rainpole.local – sfo01m01esx04.sfo01.rainpole.local	172.16.12.101 – 172.16.12.104	1612	172.16.12.253

Table 11 vMotion host configuration

Hostname FQDN range	IP range	VLAN ID	Default gateway
sfo01m01esx01.sfo01.rainpole.local – sfo01m01esx04.sfo01.rainpole.local	172.16.13.101 – 172.16.13.104	1613	172.16.13.253

Table 12 VM network host configuration

Hostname FQDN range	IP range	VLAN ID	Default gateway
sfo01m01esx01.sfo01.rainpole.local – sfo01m01esx04.sfo01.rainpole.local	172.16.14.101 – 172.16.14.104	1614	172.16.14.253

The management cluster provides management services for both domains. Use the initialization wizard to deploy the management cluster.

VxRail Manager provides automated deployment to initialize a vCenter cluster for the VVD environment. The initialization process deploys and configures ESXi Hosts, vDS networking, vSAN storage, PSC, and vCenter during this task.

Procedure

Follow the steps in the VxRail Installation SolVe procedure for Embedded vCenter on Dell EMC Solve Online.

Convert embedded vCenter and PSC to customer-managed systems

Use the SolVe procedure to RE-ESTABLISH the PSC and vCenter as customer-managed systems.

Before you begin

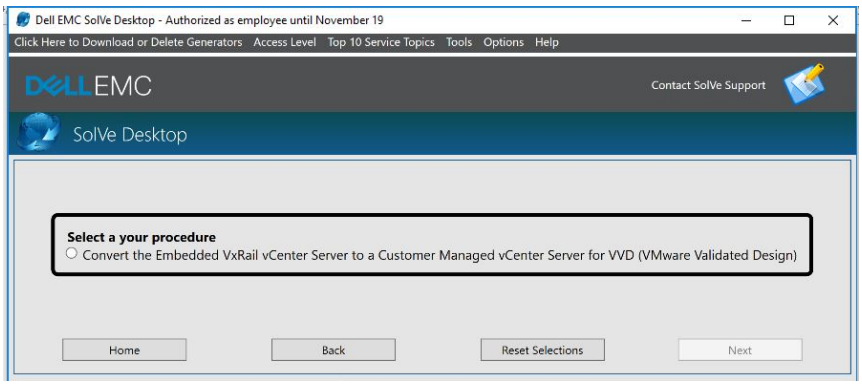
Download the SolVe procedure, *Migrate Embedded VxRail vCenter to VVD vCenter and Platform Services Controller*.

This task establishes the foundation for the VVD IaaS deployment. This conversion has the following benefits:

- It establishes a common identity-management system (SSO) for vCenter Server enhanced linked mode and cross-site vCenter Server for dual-region deployments.
- It provides better alignment with VVD for life cycle management.

Procedure

- Follow the steps in the SolVe procedure, *Convert the Embedded VxRail vCenter Server to a Customer-Managed vCenter Server for VMware Validated Design (VVD)*.



Configure CEIP on vCenter and PSC Servers

Ensure that the Customer Experience Improvement Program (CEIP) settings are enabled on all PSCs in the environment for consistent convergence of PSC objects across PSCs.

The automated PSC deployment is configured with the CEIP option enabled. Both PSC instances must be configured with the same CEIP value in order for replication to work properly.

Procedure

1. Log in to the `sfo01m01vc01.sfo.rainpole.local` DNS server.
2. From the Home tab, select **Customer Experience Improvement Program**.
3. In the right pane, select **Join.**
4. Confirm that the Customer Experience Improvement Program status is enabled.

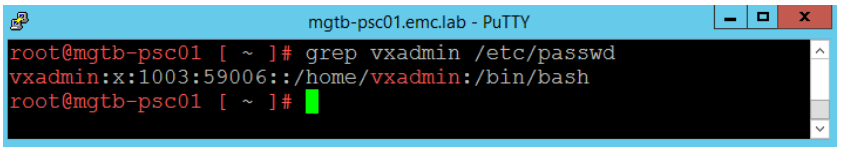
Create a local user account on the second PSC for VxRail administration

The Management Cluster deployment established a trusted user account for interaction between the VxRail Manager system and the primary PSC. The account must also be defined within the second PSC to provide an HA configuration. This account allows VxRail Manager to access the VMware HCIA Manager privilege through either PSC in the event of a PSC service interruption.

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

Perform the following tasks to create the account:

1. SSH into the primary psi sfo01m01psc01.sfo01.rainpole.local 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 second PSC `sfo01w01psc01.sfo01.rainpole.local.`
3. Run the following commands to add the group and user:

   ```
   Groupadd -g 59006 admins
   ```

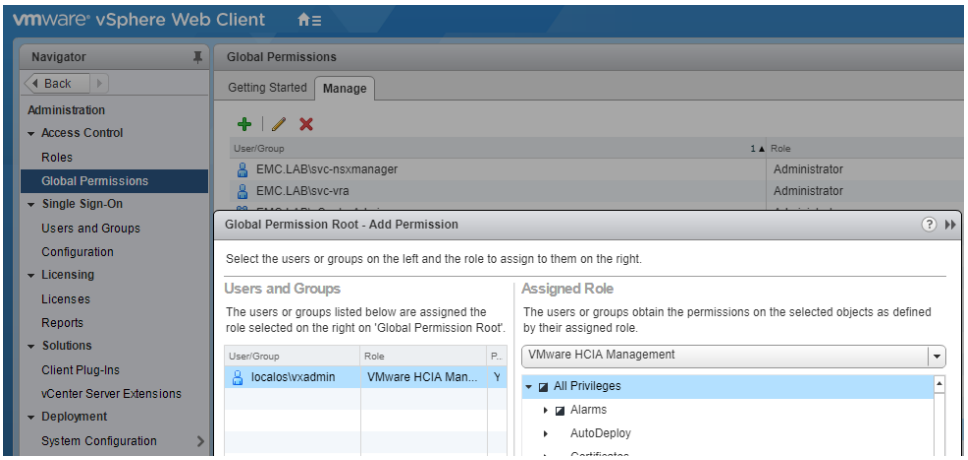
   ```
   Useradd vxadmin -u 1003 -g 59006 -d /home/vxadmin -s /bin/bash
   ```

4. Set the password of the vxadmin to match the existing password on the PSC1 (passwd `vxadmin`).
5. Connect the DCUI of the Workload Domain vCenter Server to enable the global privilege for the Account.
6. Select **Administration**, and then select the **Workload vCenter Server** from the drop- down menu.

7 Select **Global Permissions** and click the + icon to add a new permission.

8 Select **locals** from the **Domain** drop-down menu, locate the **vxadmin@localos** account, and click **Add.**

9 From the **Assign Role,** select **VMware HCIA Management** global privilege to the local account, select **Propagate to children**, and click **OK.**



To confirm the credential, log out of the DCUI and log in using the vxadmin@local account and password.

Deploy the Cloud Builder virtual appliance

The VMware Cloud Builder virtual appliance automates the implementation of the SDDC components.

Before you begin

Verify that your environment fulfills the requirements for this deployment:

- Verify that the following static IP addresses and FQDNs for the VMware Cloud Builder virtual appliance are available:
  - IP Address—172.16.11.60
  - Host Name—sfo01cb01
  - Default Gateway—172.16.11.253
  - DNS Servers—172.16.11.5 and 172.16.11.4
  - DNS Domain—sfo01.rainpole.local
  - DNS Search—sfo01.rainpole.local
  - Subnet Mask—255.255.255.0
  - NTP Servers—ntp.sfo01.rainpole.local and ntp.lax01.rainpole.local
- Verify that your environment satisfies the following prerequisites for the deployment of the virtual appliance of VMware Cloud Builder:
  - Environment—Verify that your environment is configured for deployment of VMware Cloud Builder and of the SDDC as described in Deploying VxRail on page 15.
  - Storage—Virtual disk provisioning: Thin, Required storage: 25 GB
  - Installation packages—Download the `.ova` file for VMware Cloud Builder.

Procedure

1. Log in to the Management vCenter in Region A.
   a. Open a web browser and go to `https://sfo01m01esx01.sfo01.rainpole.local`.
   b. Log in using the username **`administrator@vsphere.local`** and the administrator password.
2. In the Navigator, select the data center and click **Create/Register VM**.

   The **New virtual machine** wizard appears.
3. In the **Select creation type** dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
4. In the **Select OVF and VMDK files** dialog box, enter **`sfo01cb01`** for the virtual machine name, select the VMware Cloud Builder `.ova` file, and click **Next**.
5. In the **Select storage** dialog box, select **VxRail Manager vSAN Datastore-<*uniqueID*>** and click **Next**.
6. On the **License agreements** page, click **I agree** to accept the license agreement, and click **Next**.
7. On the **Deployment options** page, enter the following values, and then click **Next**:
   - **Network mappings**—VxRail vCenter Server-<*uniqueid*>
   - **Disk provisioning**—Thin
   - **Power on automatically**—Selected
8. In the **Additional settings** dialog box, expand **Application**, enter the following values, and then click **Next**:

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

9. In the **Ready to complete** dialog box, review the virtual machine configuration and click **Finish**.
10. See the *Enable VVD Cloud Builder for VxRail* Solve procedure to enable VxRail configuration tasks.

Generate the JSON deployment files

Generate the VxRail and VVD JSON files that automate the deployment of the IaaS and SDDC components in the management and the shared edge and compute clusters.

Before you begin

Verify that you have populated the Deployment Parameters .xls file.

Procedure

1. Log in to VMware Cloud Builder:
   a. Open a web browser and go to `https://sfo01cb01.sfo01.rainpole.local`.
   b. Log in using the username **`admin`** and the Cloud Builder administrator password.
2. 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 > **Select Architecture Type** list, select the **VVD for SDDC 5.0 on Dell EMC VxRail (Region A)** architecture and click **Upload Config File**.
   c. Go to the Deployment Parameters .xls file and click **Open**.
   d. Click **Generate JSON**.

   Cloud Builder generates two JSON files for the management and the shared edge and compute clusters, as listed in the following table:

Architecture type	JSON filename	Workload domain	Deployment order
VVD for SDDC Region A	vvd-std-rega-mgmt.json	Management	1
	vvd-std-rega-comp.json	Compute	2
	vxrail-rega-comp-manager.json	VxRail management cluster	3
	vxrail-rega-mgmt-comp.json	VxRail compute cluster	4

3. Monitor the process and check for errors in the JSON Generator log files at `/opt/vmware/sddc-support/cloud_admin_tools/logs/JsonGenerator.log`.

Mount the VVD software bundle on Cloud Builder

Prepare for an automated deployment of the SDDC components by uploading the software bundle and the generated signed certificates, and configuring application properties.

Procedure

1. Log in to the VMware Cloud Builder virtual appliance.
   a. Open a connection to `sfo01cb01.sfo01.rainpole.local` using an SCP software like WinSCP.
   b. Log in using the username **admin** and the Cloud Builder administrator password.
2. Upload the VVD software bundle files to the `/mnt/hgfs` directory on the Cloud Builder appliance.
   a. Sddc-vrealize-bundle-5.1.1.0-15121189.iso
   b. sddc-dr-bundle-5.1.1.0-15121189.iso
3. Upload all folders and their content from the `CertGenVVD` folder `C:\CertGenVVD-3.0.4\SignedByMSCACerts` to the `/opt/vmware/vvd/certificates` directory on the Cloud Builder appliance.
4. Configure the Cloud Builder appliance, and mount the VVD software bundle `.iso` file:
   a. Open an SSH connection to `sfo01cb01.sfo01.rainpole.local`.
   b. Log in using the username **admin** and the Cloud Builder administrator password.
5. Switch to the **root** user by running the **su** command.
6. Mount the VVD software bundle .iso file, and configure application properties by running the following command: `/opt/vmware/vvd/cloud-builder/install/reconfigure.sh`

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

Deploy the vCenter Server for the Shared Edge/Compute cluster

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

Procedure

1. Obtain a copy of the vCenter VMware-VCSA-all-6.7.0-15132721.iso file from myvmware or the Cloud Builder Appliance.
2. Alternatively, the vCenter ISO can be obtained from the Cloud Builder Appliance using a file copy tool such as WinSCP.
   a. Log in to the cloud builder appliance with user *root* and the corresponding root_password.
   b. Change directory to `/mnt/iso/sddc-foundation-bundle-3.9.1.0-15253477/vcenter_ova.`

c. Copy the `VMware-VCSA-all-6.7.0-15132721.iso` file to the local Windows system.

3. Mount the ISO file on Windows VM and open the drive where the ISO is mounted.
   a. Change directory to the location of the Windows installer, for example: `E:\vcsa-ui-installer\win32`
4. Select the installation application to launch the deployment wizard.
5. Select the **Installer** option, and click **Next.**
6. Accept the license agreement, and continue.
7. Select the **Deploy a vCenter Server** option from the External Platform Services Controller section of the form and click **Next**.
8. Enter the **Fully Qualified Domain Name** of the Region B management vCenter Server `lax01m01vc01.lax01.rainpole.local`.
9. Select the folder to install the VM.
10. Select the compute resource, and click **Next**.
11. Enter the VM name `sfo01w01vc01`, and the root password, and click **Next.**
12. Select the vSAN datastore for the desired storage location and click **Next.**
13. Select the port group that begins with `vCenter`, and specify the FQDN, IP address, and other system properties and click **Next**.
14. Confirm that the values are correct and click **Finish**.
    When the vCenter has been deployed, select **Continue** to join it to the `lax01m01psc01` Platform Services Controller in Region B.
15. Start the configuration process and select join and existing domain option by entering the target PSC that you would like to join `sfo01m01psc01.sfo.rainpole.local`.
16. Select the configuration option.
    a. Specify the `sfo01m01vc01.sfo.rainpole.local` platform services controller instance.
    b. Provide the SSO administrative credentials.
    c. Select **Next** to go to the summary screen.
    d. Review the details and select FINISH to deploy the vCenter.

Deploy the Shared Edge and Compute VxRail cluster

Follow the instructions in the SolVe procedure to install this cluster.

Before you begin

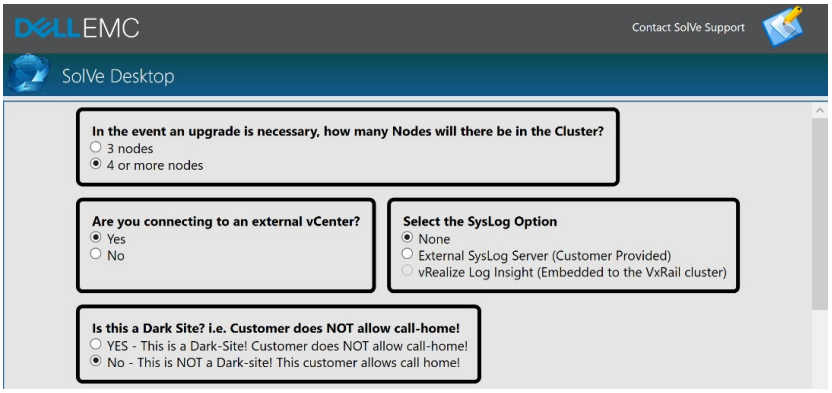
Ensure that the following tasks are complete:

- The Shared Edge and Compute vCenter Server is deployed in Region A.
- Network and top-of-rack switches are configured with the required VLANs and BGP peer interfaces.
- A Windows host exists that has access to VxRail Manager within your data center.
- (Optional) VxRail deployment JSON file exists.

Procedure

1. Download the VxRail Installation with External vCenter procedure from SolVe Online using the selections shown in the following figure:

   Figure 4 Installation guide selections

   The SolVe Tool produces the deployment guide with the detailed instructions and dependencies for deploying the VxRail external cluster.

2. Follow the procedures in the SolVe deployment documentation to complete the Shared Edge and Compute VxRail cluster deployment.

3. (Optional) Deploy the VxRail using the Cloud Builder generated JSON input file:

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

   - 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 in to the Cloud Builder and follow the process to generate the .json files.
   - Obtain the `vxrail-rega-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-rega` directory.

4. See the information in the following tables for either manual or Cloud Builder VxRail deployment:

   Table 13 VxRail Manager, vCenter, and PSC details

FQDN	IP address	VLAN ID	Default gateway
sfo01w01vxm01.sfo01.rainpole.local	172.16.11.69	1611	172.16.11.253
sfo01m01psc01.sfo01.rainpole.local [a]	172.16.11.63	1611	172.16.11.253
sfo01w01vc01.sfo01.rainpole.local	172.16.11.64	1611	172.16.11.253

   [a] The second PSC has not been deployed yet, so you must join the management PSC during this process. Repointing is completed by Cloud Builder.

Table 14 Management cluster hosts

FQDN	IP address	VLAN ID	Default gateway
sfo01w01esx01 … sfo01w01esx04	172.16.31.101 … 172.16.31.104	1631	172.16.31.253

Table 15 vSAN host configuration

FQDN	IP address	VLAN ID	Default gateway
sfo01w01esx01 … sfo01w01esx04	172.16.33.101 … 172.16.33.104	1633	172.16.33.253

Table 16 vMotion host configuration

FQDN	IP address	VLAN ID	Default gateway
sfo01w01esx01 … sfo01w01esx04	172.16.32.101 … 172.16.32.104	1632	172.16.32.253

After completion of the VxRail Manager deployment, connect to VxRail Manager and confirm that the health of the system.

Configure SSH on all hosts in Region A

Enable the SSH service to allow Cloud Builder remote connectivity.

Repeat this procedure for all hosts in the management and shared edge and compute clusters. Use the values in the table in Configure DNS settings for VxRail clusters on page 16.

Procedure

1. Log in to the vSphere host by using the VMware Host Client:
   a. Open a web browser and go to `https://sfo01m01esx01.sfo01.rainpole.local`.
   b. Log in using the username `root` and the esxi root user password.
2. Configure and start the SSH service:
   a. In the Navigator, click **Manage** > **Services**.
   b. Select **SSH service** > **Actions** > **Policy** > **Start and stop with host**.
   c. Click **Start** to start the service.

CHAPTER 5

Preparing the Environment for Automated Deployment

This chapter presents the following topics:

Deploy and configure the master Windows system

Deploy and configure a single Master Windows system virtual machine to provision the vRealize Automation IaaS components.

Before you begin

Ensure that the following network requirements are met:

- 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.

The single master Windows system virtual machine is cloned and reconfigured during SDDC deployment to provision the vRealize Automation IaaS components: IaaS web servers, IaaS Manager service servers, IaaS DEM servers, and IaaS proxy servers. Create a virtual machine on the `sfo01m01vc01.sfo01.rainpole.local` vCenter Server for the master Windows system with the virtual machine, software, and network configuration listed in the following tables:

Table 17 Virtual machine requirements for the master Windows system

Setting	Value
ESXi host	mgt-vcenter.rainpole.local
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	VxRail-Virtual-SAN-Datastore-<hexid>
Network interface	VM Network
Network adapter type	1 x VMXNET3

Table 18 Software requirements for the master Windows system

Component	Requirement
Operating system	Windows Server 2016 (64-bit)
VMware Tools	Latest version
Active Directory	Join the virtual machine to the sfo01.rainpole.local domain.
Internet Explorer Enhanced Security Configuration	Turn off ESC.
Remote Desktop Protocol	Enable RDP access.

Table 18 Software requirements for the master Windows system (continued)

Component	Requirement
Java	• Java Runtime Environment (JRE) executable jre-8u191-windows-x64 or later • Set the JAVA_HOME environment variable to the Java installation directory. • Update the PATH system variable to include the bin folder of Java installation directory.
Secondary Logon service	Start Secondary Logon service, and set start-up type to Automatic.

Procedure

1. Deploy the Master Windows System for vRealize Automation with the specified configuration.
2. Log in to the vRealize Automation Master Windows virtual machine by using a Remote Desktop Protocol (RDP) client:
   a. Open an RDP connection to the virtual machine.
   b. Log in using the Windows administrator username and password.
3. Click **Start**, right-click **Windows PowerShell**, and select **More** > **Run as Administrator**.
4. Set the execution policy by running the following command: `Set-ExecutionPolicy Unrestricted` Confirm the execution policy change at the prompt.
5. Disable User Account Control (UAC) by running the following command:

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

6. Disable IPv6 protocol:

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

7. Verify that the source path for Microsoft Windows Server is available:
   a. Mount the Microsoft Windows Server ISO file on the Master Windows system virtual machine.
   b. Create the \sources\sxs directory by running the following command in Windows PowerShell: `mkdir C:\sources\sxs`
   c. Copy the Microsoft Windows Server source files from `sources\sxs` on the ISO file to the `C:\sources\sxs` directory on the virtual machine.

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

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

e. Unmount the Microsoft Windows Server ISO file.

8. Add the `svc-vra` service account to the Local Administrators group.
   a. Click **Start**, right-click **Windows PowerShell**, and select **More** > **Run as Administrator**.
   b. Run the following command: `net local group administrators rainpole\svc-vra /add`.
9. Create the `svc-vra` user profile by logging in to the vRealize Automation Master Windows virtual machine:
   a. Open an RDP connection to the virtual machine.
   b. Log in using the username, `rainpole\svc-vra`, and the svc-vra password.
10. Shut down the Master Windows system virtual machine

Deploy and configure the external SQL Server

Deploy and configure a Windows-based virtual machine to host the SQL Server database required for the vRealize Automation IaaS components.

Create a virtual machine on the `sfo01m01esx01.sfo01.rainpole.local` host for the Microsoft SQL Server with the virtual machine, software, and network configuration requirements listed in the following tables:

Table 19 Virtual machine requirements for the external vRealize automation SQL Server

Setting	Value
ESXi host	sfo01m01vc01.sfo01.rainpole.local
VM name	vra01mssql01
Guest operating system	Microsoft Windows Server 2016 (64-bit)
vCPU	8
Memory (GB)	16
Hard disk (GB)	200
SCSI Controller	LSI Logic SAS
Datastore	VxRail-Virtual-SAN-Datastore-<hexid>
Network interface	vCenter Server Network-<hexid>
Network adapter type	1 x VMXNET3

Table 20 Network requirements for the external vRealize automation SQL Server

Setting	Value
Host name	vra01mssql01
Static IPv4 address	172.16.11.72
Subnet mask	255.255.255.0
Default gateway	172.16.11.253
DNS server	172.16.11.5
FQDN	vra01mssql01.rainpole.local

Table 21 Software requirements for the external vRealize automation SQL Server

Component	Requirement
Operating system	Windows Server 2016 (64-bit)
VMware Tools	Latest version
SQL Server	SQL Server 2017 Standard or later (64-bit) Microsoft SQL Server Management Studio. **Note:** During the SQL Server installation, the Database Engine configuration wizard prompts you to provide the username and password for the SQL Server administrator. If this user was not added during the SQL Server installation, select SQL Authentication from the Authentication drop-down menu. Type **sa** in the username text box and the sa password in the Password text box.
Active Directory	Join the virtual machine to the `sfo01.rainpole.local domain`.
Remote Desktop Protocol	Enable RDP access.

Procedure

1. Deploy the External vRealize Automation SQL Server VM with the specified configuration.
2. Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client:
   a. Open an RDP connection to the `vra01mssql01.rainpole.local` virtual machine.
   b. Log in using the Windows administrator username and password.
3. Enable Microsoft Distributed Transaction Coordinator (MSDTC):
   a. Click the Windows **Start** button, type **comexp.msc**, and press **Enter**. The **Component Services** window opens.
   b. In the **Console root** in the left pane, select **Component Services** > **Computers** > **My Computer** > **Distributed Transaction Coordinator**.
   c. Right-click **Local DTC,** and select **Properties**.

d. In the **Local DTC Properties** dialog box, click **Security**, select the following options, and then click **OK**:

- **Network DTC Access**
- **Allow Remote Clients**
- **Allow Inbound**
- **Allow Outbound**

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

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

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

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

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

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

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

5. Create the new vRealize Automation database.

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

b. Right-click the **Databases** folder, and select **New Database**. The **New Database** wizard opens.

c. On the **General** page, type **`VRADB01`** for **Database name** and `rainpole\svc-vra` for **Owner**.

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

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

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

a. Click the Windows **Start** button, type **`WF.msc`**, and press Enter. The **Windows Firewall with Advanced Security** window appears.

b. In the Navigation pane, right-click **Inbound Rules** and select **New Rule**. The **New Inbound Rule** wizard opens.

c. For Rule **Type**, select **Port** and click **Next**.

d. For Protocol **and Ports**, select **TCP**, type the port number **`1433`** in the **Specific local ports** text box and click **Next**.

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

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

g. For Name, type **`Microsoft SQL Server Port (1433)`** and click **Finish**.

Allow access for Microsoft Distributed Transaction Coordinator.

h. Click the Windows **Start** button, type `WF.msc` and press Enter. The **Windows Firewall with Advanced Security** window appears.

i. In the Navigation pane, select **Inbound Rules** > **New Rule Inbound Rules**. The **New Inbound Rule** wizard opens.

j. For **Rule Type**, select **Predefined** > **Distributed Transaction Coordinator**, and click **Next**.

k. For **Predefined Rules**, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, and **Distributed Transaction Coordinator (TCP-In)**, and then click **Next**.

l. For **Action**, select **Allow the connection** and click **Finish**.

7. Unmount any ISO files that are mounted to the virtual machine.

Deploy and configure the Windows system for Site Recovery Manager

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.

Note

This procedure is optional for Single Region deployments, but required for Dual Region deployments.

Create a virtual machine on the `sfo01m01vc01.sfo01.rainpole.local` vCenter server for Site Recovery Manager with the following virtual machine, software, and network configuration:

Table 22 Virtual machine requirements for Site Recovery Manager VM

Setting	Value
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
VM Name	sfo01m01srm01
Guest OS	Windows Server 2016 (64-bit)
vCPU	2
Memory (GB)	2
Virtual Disk (GB)	40
SCSI Controller	LSI Logic SAS
Datastore	VxRail-Virtual-SAN-Datastore-<hexid>
Network Interface	vCenter Server Network-<hexid>
Network Adapter Type	1 x VMXNET3

Table 23 Network requirements for Site Recovery Manager VM

Setting	Value
Host Name	sfo01m01srm01
Static IPv4 Address	172.16.11.124
Subnet Mask	255.255.255.0
Default Gateway	172.16.11.253
DNS Server	172.16.11.5
FQDN	sfo01m01srm01.sfo01.rainpole.local
Open Ports	9086, 5678

Table 24 Software requirements for the Site Recovery Manager VM

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

Procedure

1. Deploy the Site Recovery Manager virtual machine with the specified configuration.
2. Log in to the Site Recovery Manager virtual machine by using a Remote Desktop Protocol (RDP) client:
   a. Open an RDP connection to the `sfo01m01srm01` virtual machine.
   b. Log in using the Windows administrator username and password.
3. Click **Start**, right-click **Windows PowerShell**, and select **More** > **Run as Administrator.**
4. Add the svc-srm service account to the local Administrators group by running the following command: `net local group administrators rainpole\svc-srm /add`
5. Configure NTP settings:
   a. Enable Windows Time Service and start by running the following commands:

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

net stop w32time && net start w32time
```

b. Verify the time synchronization configuration by running the following command:

```
w32tm /query /status
```

Generate and replace certificates for the SDDC components

In an SDDC, the security of the environment depends on the validity and trust of the management certificates. To ensure secure and operational connectivity between the SDDC components, generate new signed certificates to prepare for replacing the temporary self-signed certificates.

The high-level steps are as follows:

1. Create and add a Microsoft certificate authority template on page 37
2. Generate signed certificates for the SDDC components on page 38

Create and add a Microsoft certificate authority template

Set up a Microsoft Certificate Authority template on the Active Directory (AD) servers for the region.

Before you begin:

- This VVD sets the Certificate Authority service on the Active Directory (AD) `dc01rpl.rainpole.local` (root CA) server. Verify that the Certificate Authority Service role and the Certificate Authority web Enrollment role are installed and configured on the Active Directory Server.
- 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.

The template contains the certificate authority (CA) attributes for signing certificates of VMware SDDC solutions. After you create the template, you add it to the certificate templates of the Microsoft CA.

Procedure

1. Log in to the Active Directory server using a Remote Desktop Protocol (RDP) client using the Active Directory administrator username and password.
2. Select **Start** > **Run**, type **`certtmpl.msc`**, and click **OK**.
3. In the **Certificate Template** console, under **Template Display Name**, right-click **web Server** and click **Duplicate Template**.
4. In the **Duplicate Template** window, 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, type **`VMware`** as the name of the new template.
7. Click the **Extensions** tab, and specify the extensions information:
   a. Select **Application Policies** and click **Edit**.
   b. Select **Server Authentication** > **Remove** > **OK**.
   c. If the Client Authentication policy is present, select it, click **Remove**, and click **OK**.
   d. Select **Key Usage** > **Edit**.

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

f. Leave the default for all other options.

g. Click **OK**.

8. Click the **Subject Name** tab, ensure that **Supply in the request** is selected, and click **OK** to save the template.
9. To add the new template to your CA, click **Start** > **Run**, enter `certsrv.msc`, and click **OK**.
10. In the **Certification Authority** window, expand the left pane if it is collapsed.
11. Right-click Certificate Templates, and select **New** > **Certificate Template to Issue**.
12. In the **Enable Certificate Templates** dialog box, in the **Name** column, select **VMware certificate**, and click **OK**.

Generate signed certificates for the SDDC components

Use the Certificate Generation Utility for VVD (`CertGenVVD`) and VMware Cloud Builder to generate new signed certificates and replace the default, self-signed certificates for the SDDC components.

Before you begin

- 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.
- 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.

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
   ```

3. Use the `CertConfig` utility to generate the certificate configuration files:
   a. Open the completed 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. Transfer the `SDDC-CertConfig.csv` file to the Windows host.

d. Rename the current `ConfigFiles` folder located in `C:\CertGenVVD-3.0.4` to `ConfigFiles.Old`.

e. Create a `ConfigFiles` folder in the `C:\CertGenVVD-3.0.4` directory.

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

g. Go to the `C:\CertGenVVD-3.0.4` folder, and run the following command: `.\Certconfig-1.1.0.ps1 SDDC-Certconfig.csv`

h. Follow the on-screen instructions, and set the following values:

- **Default Organization**—Rainpole Inc
- **Default OU**—Rainpole
- **Default Location**—SFO
- **Default State**—CA
- **Default Country**—US
- **Default Key Size**—2048

i. Verify that the `C:\CertGenVVD-3.0.4\ConfigFiles` folder is populated with the necessary certificate configuration files.

4. Validate the local machine configuration:

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

b. Go to the `C:\CertGenVVD-3.0.4` folder, and validate the configuration by running the following command: `.\CertGenVVD-3.0.4.ps1 -validate`

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

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

b. Go to the `C:\CertGenVVD-3.0.4` folder, and generate the signed certificates by running the following command: `.\CertGenVVD-3.0.4.ps1 -MSCASigned -at trib 'CertificateTemplate:VMware'`

c. Follow the on-screen instruction, and type a passphrase for PEM/P12 file encryption.

CHAPTER 6

Deploying the SDDC Components

This chapter presents the following topics:

Automated SDDC deployment prerequisites

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

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

Environment
Verify that:

- Your environment is configured for deployment of the SDDC as documented in Deploying VxRail on page 18.
- Active Directory is configured with all child domains and all service accounts, and groups are created and configured.
- DNS entries are configured for the root and child domains.
- Two servers external to the SDDC NTP are configured and time synchronization is configured on all ESXi hosts and AD domain controllers.
- Your environment meets all physical network requirements and that all host names and IP addresses are allocated for external services and virtual infrastructure components.
- Secondary storage for certain SDDC features is mounted.

For additional information, see the *VMware Validated Design on Dell EMC VxRail Appliances Planning Guide*.

Software
Ensure that the following tasks have been completed:

- Enter the Deployment Parameters .xls file for Region A.
- Verify that you have generated CA-signed certificates for the management components of the SDDC. See Generate and replace certificates for the SDDC components on page 37.

Installation packages
Download the `.iso` file for the software bundle for VVD to your local file system.

Audit deployment parameters and target environment

Perform an audit 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.

Before you begin:

Enable SSH on all VxRail nodes before performing the audit.

Validate the JSON deployment files for both the management and the shared edge and compute clusters. In case any of the tests fail, you must fix any errors and perform the validation process again. Additional information can be found in the Cloud Builder Platform Audit log file, `/opt/vmware/sddc-support/cloud_admin_tools/logs/PlatformAudit.log`.

Procedure

1. Log in to VMware Cloud Builder:
   a. Open a web browser and go to `https://sfo01cb01.sfo01.rainpole.local`.
   b. Log in using the username **admin** and the Cloud Builder administrator password.
2. In the Cloud Builder Navigator, click the **Deployment Wizard** icon.
3. Select the **Validate Environment** tab.
4. From the **Select File to Validate** drop-down menu, select the `vvd-std-rega-mgmt.jsonfile` and click **Validate**.
5. (Optional) If the Validation fails due to user input errors, perform the validation process again with .xls file modification:
   a. Fix input errors in the .xls file.
   b. In the **Upload Config File** tab > **Select Architecture Type** drop- down menu, select the **VVD for SDDC Region A** architecture, and click **Upload Config File**.
   c. Go to the Updated Deployment Parameters .xls file, and click **Open**.
   d. On **Overwrite Existing JSON Files**, select **Yes** to replace.
   e. Click the **Back** button and repeat Step 4.
6. Repeat step 5, if necessary, until all validation tasks have completed successfully.

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

After you finish:

After successful validation of `vvd-std-rega-mgmt.json` and `vvd-std-rega-comp.json` files, click **Next** to start the deployment process. The clusters are deployed in dependent order.

Note

You must deploy the management cluster first. Deploy the workload domain only after successful completion of the management cluster.

Start automated deployment for the Management cluster

After you successfully validate the `vvd-std-rega-mgmt.json` 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://sfo01cb01.sfo01.rainpole.local`.
   b. Log in using the username **admin** and the Cloud Builder administrator password.
2. In the Cloud Builder Navigator, select the **Deployment Wizard** icon.

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

   Automated deployment of the components in the management cluster begins.
5. Monitor the deployment, and check the following log files for errors:

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

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

Start automated deployment for the shared edge and compute cluster

After you have deployed the management cluster, you start the automated deployment of the components in the shared edge and compute cluster.

Procedure

1. Log in to VMware Cloud Builder:
   a. Open a web browser and go to `https://sfo01cb01.sfo01.rainpole.local`.
   b. Log in using the username **`admin`** and the Cloud Builder administrator password.
2. In the Cloud Builder Navigator, select the **Deployment Wizard** icon.
3. Select the **Deploy an SDDC** tab.
4. From the **Select Deployment File** drop-down menu, select the `vvd-std-rega-comp.json` JSON file and click **Deploy**.

   Automated deployment of the components in the shared edge and compute cluster begins.
5. Monitor the deployment, and check the following log files for errors:

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

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

CHAPTER 7

Post-deployment: Configuring the Virtual Infrastructure

This chapter presents the following topics:

Configure a distributed firewall for management applications

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

Procedure

1. Add vCenter Server instances to the NSX distributed firewall exclusion list on page 45

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

2. Create IP sets for management cluster components on page 46

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

3. Create security groups on page 47

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

4. Create distributed firewall rules on page 48

   Create firewall rules to allow administrators to connect to the various VMware solutions. Firewall rules allow users to access to the vRealize Automation portal, and to provide the external connectivity to the SDDC.

Add vCenter Server instances to the NSX distributed firewall exclusion list

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

Configure the NSX distributed firewall by using a vCenter Server. You must exclude vCenter Server from all the distributed firewall rules and ensure that access between the two products is not blocked.

Procedure

1. Use the vSphere Client to log in to the vCenter Server:
   a. Open a web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
2. Exclude vCenter Server instances from the distributed firewall rules:
   a. From the **Home** menu, select **Networking & Security**.
   b. In the Navigator pane, select **Firewall Settings** > **Exclusion List**.
   c. Select **172.16.11.65** from the **NSX Manager** drop-down menu.
   d. Click **Add**.
   e. In the **Select VM(s) to exclude** dialog box, select **sfo01m01vc01**, add it to the **Selected Objects** list, and click **OK**.

Create IP sets for management cluster components

Create IP sets for all management applications.

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

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

The following table lists the IP sets required for the management components:

Table 25 Required IP sets for management components

Name	IP addresses
PSC Instances	Platform-Service-Controller_IPs
vCenter Server Instances	vCenter-Server_IPs
vRealize Automation Appliances	vRealize-Automation-Appliances_IPs
vRealize Automation Windows	vRealize-Automation-Windows _IPs
vRealize Automation Proxy Agents	vRealize-Automation-Proxy-Agents-IPs
vRealize Business Server	vRealize-Business_IPs
vRealize Business Data Collector	vRealize-Business-Data-Collector_IPs
VMware VADP Solution	vStorage-API for Data-Protection-Solution_IPs
vRealize Operations Manager	vRealize-Operations-Manager_IPs
vRealize Operations Manager Remote Collectors	vRealize-Operations-Manager-Remote-Collectors_IPs
vRealize Log Insight	vRealize-Log-Insight_IPs
vRealize Suite Lifecycle Manager	vRealize-Suite-Lifecycle-Manager_IPs
Site Recovery Manager	Site-Recovery-Manger_IPs
vSphere Replication	vSphere-Replication_IPs
SDDC	Management-VLAN_Subnets, Management-VXLAN_Subnets
Administrators	Administrators_Subnet

Procedure

1. Use the vSphere Client to log in to the vCenter Server:
   a. Open a web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
2. Create an IP set:
   a. From the **Home** menu, select **Networking & Security**.
   b. In the Navigator pane, select **Groups and Tags** > **IP Sets**.
   c. Select **172.16.11.65** from the **NSX Manager** drop-down menu.
   d. Click **Add**.

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

- **Name**—vCenter Server Instances
- **IP Addresses**—172.16.11.62, 172.16.11.64
- **Universal Synchronization**—On

3. Repeat Step 2 to create IP sets for all remaining components.

Create security groups

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

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

Table 26 Security groups for the management cluster components in the SDDC

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

Table 26 Security groups for the management cluster components in the SDDC (continued)

Name	Object Type	Selected Object
VMware Appliances	Security Groups	• PSC Instances • vCenter Server Instances • vSphere Replication • vRealize Automation Appliances • vRealize Business Server • vRealize Business Data Collector • VMware vStorage API for Data Protection Solution • vRealize Operations Manager • vRealize Operations Manager Remote Collectors • vRealize Suite Lifecycle Manager • vRealize Log Insight

Procedure

1. Use the vSphere Client to log in to the vCenter Server:
   a. Open a web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
2. From the **Home** menu, select **Networking & Security** > **Groups and Tags** > **Security Groups**.
3. Select **172.16.11.65** from the **NSX Manager** drop-down menu.
4. Click **Add**.

   The **Create Security Group** wizard appears.
5. On the **Name and Description** page, enter the following settings, and then click **Next**.
   - **Name**—PSC Instances
   - **Universal Synchronization**—On
6. On the **Select Objects to Include** page, select **IP Sets** from the **Available Objects > Object Type** drop-down menu. Add **PSC Instances** to **Selected objects**, and click **Next**.
7. On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.
8. Repeat this procedure to create all the necessary security groups.

Create distributed firewall rules

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

Procedure

1. Use the vSphere Client to log in to the vCenter Server:
   a. Open a web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
2. Add a section of rules for the management applications:
   a. From the Home menu, select **Networking & Security** > **Firewall**.
   b. From the **NSX Manager** drop-down menu, select **172.16.11.65**.
   c. Click **Add Section**.
3. In the **Add New Section** dialog box, enter the following information, and then click **Add**:
   - **Section Name**—VMware Management Services
   - **Universal Synchronization**—On
4. Create a distributed firewall rule to allow an SSH access to administrators for the different VMware appliances:
   a. Click **Add rule**.
   b. In the **Name** column of the new rule, type **`Allow SSH to admins`**.
   c. In the **Source** column, select Edit, select **Security Group** from the **Object Type** drop-down menu, add **Administrators** to the **Selected Objects** list, and click **Save**.
   d. In the Destination column, click Edit, select Security Group from the **Object Type** drop-down menu. Add **VMware Appliances** and **Update Manager Download Service** to the **Selected Objects** list, and click **Save**.
   e. In the **Service** column, click **Edit**, add **SSH** to the **Selected Objects** list, and click **Save**.
   f. Click **Publish**.
5. Repeat the previous step to create the following distributed firewall rules:

Name	Source	Destination	Service/ Port
Allow vRA Portal to end users.	* any	• vRealize Automation Appliances • vRealize Automation Windows • vRealize Business Server	HTTP, HTTPS
Allow vRA Console Proxy to end users.	* any	vRealize Automation Appliances	TCP: 8444
Allow SDDC to any.	SDDC	* any	* any
Allow PSC to admins.	Administrators	PSC Instances	HTTPS
Allow SSH to admins.	Administrators	VMware Appliances Update Manager Download Service	SSH

Name	Source	Destination	Service/Port
Allow RDP to admins.	Administrators	Windows Servers	RDP
Allow Orchestrator to admins.	Administrators	vRealize Automation Appliances	TCP: 8281, 8283
Allow vRB Data Collector to admins.	Administrators	vRealize Business Data Collector	HTTP, HTTPS
Allow vROPs to admins.	Administrators	• vRealize Operations Manager • vRealize Operations Manager Remote Collectors	HTTP, HTTPS
Allow vRLI to admins.	Administrators	vRealize Log Insight	HTTP, HTTPS
Allow vRSLCM to admins.	Administrators	vRealize Suite Lifecycle Manager	HTTPS
Allow VAMI to admins.	Administrators	VMware Appliances	TCP: 5480
Allow VMware VADP Solution to admins.	Administrators	VMware Appliances	TCP: 8543

6. Change the default rule action from Allow to **Block**:
   a. From the NSX Manager drop-down menu, select 172.16.11.65.
   b. Under **Default Section Layer3**, in the **Action** column for the **Default Rule**, change the action to **Block**, and then click **Save**.
   c. Click **Publish**.

   Network security allows only the network traffic that is required by the SDDC to pass.

Update DNS records for the PSC load balancer

Modify the DNS address of the PSC load balancer.

Edit the `sfo01psc01.sfo01.rainpole.local` DNS entry to point to the virtual IP address (VIP) of the 172.16.11.71 load balancer, instead of pointing to the `sfo01m01psc01` IP address.

Procedure

1 Log in to the DNS server that resides in the `sfo01.rainpole.local` domain.
2 From the Windows **Start** menu **Search** text box, type `dnsmgmt.msc` and press Enter.
3 In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the **sfo01.rainpole.local** domain and, on the right, locate the **sfo01psc01** record.
4 Double-click **sfo01psc01**, enter the following settings, and then click **OK**:
   - **Fully Qualified domain name (FQDN)**—sfo01psc01.sfo01.rainpole.local
   - **IP Address**—172.16.11.71
   - **Update Associated Pointer (PTR) record**—Not selected

CHAPTER 8
Post-deployment: Configuring vRealize Operations Manager

This chapter presents the following topics:

Enable automatic synchronization of authentication sources

Enable the automatic synchronization of authentication sources in vRealize Operations Manager and define monitoring goals for the default policy.

vRealize Operations Manager maps import LDAP users to user groups after you enable **Automatically synchronize user membership for configured groups** for the `rainpole.local` and `sfo01.rainpole.local` Active Directory instances.

Procedure

1. Log in to vRealize Operations Manager.
   a. Open a web browser and go to `https://vrops01svr01.rainpole.local`.
   b. Log in using the username **`admin`** and the deployment administrator password.
2. On the main navigation bar, click **Administration**.
3. Configure the authentication sources to enable an automatic synchronization for the `rainpole.local` Active Directory instance:
   a. In the left pane, click **Access** > **Authentication Sources**.
   b. On the **Authentication Sources** page, select **rainpole.local** and click **Edit**.
   c. In the **Edit Source for User and Group Import** dialog box, expand **Details** and select **Automatically synchronize user membership for configured groups**.
   d. Click **OK**.
4. Repeat the previous step for the `sfo01.rainpole.local` Active directory.

Remove existing service accounts in vRealize Operations Manager

After enabling automatic synchronization of authentication sources, remove the `svc-vrli-vrops` and `svc-vra-vrops` service accounts. Add them later because vRealize Operations Manager does not provide an API to synchronize in an automated way.

Procedure

1. Log in to vRealize Operations Manager.
   a. Open a web browser and go to `https://vrops01svr01.rainpole.local`.
   b. Log in using the username **`admin`** and the deployment administrator password.
2. On the main navigation bar, click **Administration**.
3. On the left side, click **Access** > **Access Control**.
4. Remove the existing `svc-vrli-vrops` and `svc-vra-vrops` service accounts:
   a. On the **Access Control** page, select svc-vrli-vrops and click **Delete**.
   b. In the **Delete User** dialog box, click **Yes**.

c. Repeat steps a and b for the svc-vra-vrops service account to remove it.

Configure user privileges on vRealize Operations Manager

Assign an administrator role to the `svc-reli-vrops` service account for the **launch in context** integration of vRealize Operations Manager with vRealize Log Insight.

Procedure

1. Log in to vRealize Operations Manager.
   a. Open a web browser and go to `https://vrops01svr01.rainpole.local`.
   b. Log in using the username **`admin`** and the deployment administrator password.
2. On the main navigation bar, click **Administration**.
3. In the left pane, click **Access** > **Access Control**.
4. On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.
5. On the **Import Users** page, import the `svc-vrli-vrops` service account:
   a. From the **Import From** drop-down menu, select **rainpole.local**.
   b. Select the **Basic** option for the search query.
   c. In the **Search String** text box, type **`svc-vrli-vrops`** and click **Search**.
   d. Select **svc-vrli-vrops@rainpole.local,** and click **Next**.
6. On the **Assign Groups and Permissions** page, click the **Objects** tab, configure the following settings, and then click **Finish:**
   - **Select Role**—Administrator
   - **Assign this role to the user**—Selected
   - **Allow access to all objects in the system**—Selected
7. When prompted with the warning about allowing access to all objects on the system, click **Yes**.

Integrate vRealize Log Insight with vRealize Operations Manager

Connect vRealize Log Insight in Region A with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager.

Use the **launch in context** functionality between the two management applications to troubleshoot management nodes and vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

Procedure

1. Log in to the vRealize Log Insight user interface.
   a. Open a web browser and go to `https://sfo01vrli01.sfo01.rainpole.local`.
   b. Log in with the username **`admin`** and the deployment administrator password.
2. In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Administration**.
3. Under **Integration**, click **vRealize Operations**.
4. On the **vRealize Operations Manager** page, select **Enable launch in context**.

5. Click **Test Connection** to validate the connection and click **Save**.
6. Click **OK** to close the progress dialog box.

Configure user privileges for integration with vRealize Automation

Configure read-only privileges for the `svc-vra-vrops` service account on vRealize Operations Manager for integration with vRealize Automation.

vRealize Automation can collect metrics from vRealize Operations Manager for reclamation of tenant workloads that have a low use of CPU, memory, or disk space.

Procedure

1. Log in to vRealize Operations Manager.
   a. Open a web browser and go to `https://vrops01svr01.rainpole.local`.
   b. Log in using the username **`admin`** and the deployment administrator password.
2. On the main navigator bar, click **Administration**.
3. On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.
4. On the **Import Users** page, import the `svc-vra-vrops` service account:
   a. From the **Import From** drop-down menu, select **rainpole.local**.
   b. Select the **Basic** option for the search query.
   c. In the **Search String** text box, type **`svc-vra-vrops`** and click **Search**.
   d. Select **svc-vra-vrops@rainpole.local,** and click **Next**.
5. On the **Assign Groups and Permissions** page, click the **Objects** tab, configure the following settings, and then click **Finish**:
   - **Select Role**—ReadOnly
   - **Assign this role to the user**—Selected
   - **Select Object—vCenter Adapter** > **vCenter Adapter - sfo01w01vc01**

Verify integration of vRealize Operations Manager as a metrics provider

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

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. Select **Administration** > **Reclamation** > **Metrics Provider**.
3. Click **Test Connection** to verify that the connection is successful.

Define default policy monitoring goals

In vRealize Operations Manager, enable the **Define monitoring goals** option for the default policy for each vCenter Adapter instance.

Procedure

1. Log in to vRealize Operations Manager.
   a. Open a web browser and go to `https://vrops01svr01.rainpole.local`.
   b. Log in using the username **`admin`** and the deployment administrator password.
2. On the main navigation bar, click **Administration**.
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. In the solution table, select the **VMware vSphere** solution and click the **Configure** icon.

   The **Manage Solution - VMware vSphere** dialog box appears.
5. Under **Instance Settings**, select the **sfo01m01vc01** vCenter adapter.
6. Click **Define Monitoring Goals**.
7. Under **Enable vSphere Hardening Guide Alerts**, click **Yes**, leave the default configuration of the other options, and click **Save**.
8. In the **Success** dialog box, click **OK**.
9. Click **Save Settings**.
10. In the **Info** dialog box, click **OK**.
11. Repeat steps 5 to 10 for the Compute vCenter Server adapter.
12. In the **Manage Solution - VMware vSphere** dialog box, click **Close**.

CHAPTER 9
Post-deployment: Configuring the Cloud Management Platform

This chapter presents the following topics:

Configure vRealize Automation for a large-scale deployment

Increase the values of the `ProxyAgentServiceBinding` attributes to configure the vRealize Automation Manager Service to contain many data objects.

Procedure

1. Log in to the virtual machine of the vRealize Automation IaaS Manager Service by using a Remote Desktop Protocol (RDP) client:
   a. Open an RDP connection to the `vra01ims01a.rainpole.local` virtual machine.
   b. Log in with the username **`rainpole\svc-vra`** and the svc-vra password.
2. Open the `C:\Program Files (x86)\VMware\vCAC\Server \ManagerService.exe.config` file in a text editor with administrative rights.
3. Locate the following line in the `ManagerService.exe.config` file:

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

4. Edit the values of the following parameters, increasing them by a factor of 10 as shown:
   - **maxReceivedMessageSize**—131072000
   - **maxStringContentLength**—131072000
5. Save your changes to the `ManagerService.exe.config` file, and close the text editor.
6. Open the Windows **Start** menu and select **Restart** to restart the virtual machine.
7. Repeat this procedure for the `vra01ims01b.rainpole.local` virtual machine.

Configure the content library

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

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

Procedure

1. Use the vSphere Client to log in to the Compute vCenter Server:
   a. Open a web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/ui`.

b. Log in using the username `administrator@vsphere.local` and the vSphere administrator password.

2. From the **Home** menu, select **Content Libraries** and click the **+** icon. The **New Content Library** wizard opens.
3. On the **Name and location** page, enter the following settings and click **Next**:
   - **Name**—sfo01-w01cl-vra0
   - **vCenter Server**—sfo01w01vc01.sfo01.rainpole.local
4. On the **Configure content library** page, enter the following settings and click **Next**:
   - **Local content library**—Selected
   - **Publish externally**—Selected
   - **Enable authentication**—Selected
   - **Password**—*sfo01-w01cl-vra01_password*
   - **Confirm password**—*sfo01-w01cl-vra01_password*
5. On the **Add storage** page, select the `sfo01-w01-lib01` datastore to store the content library and click **Next**.
6. In the **Ready to Complete** page, click **Finish**.

Import .ovf files for virtual machine templates

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

Before you begin:

Verify that you have prepared the OVF templates, as specified in the "Virtual Machine Template Specifications" section of the *VMware Validated Design on VxRail Appliance Planning Guide*.

Repeat this procedure three times to import the virtual machine templates listed in the following table:

Table 27 Virtual machine templates

VM template name	Operating system type
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit) with SQL 2012

Procedure

1. Use the vSphere Client to log in to the Compute vCenter Server:
   a. Open a web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username `administrator@vsphere.local` and the vSphere administrator password.
2. From the Home menu, select Content Libraries.

3. Right-click the content library **sfo01-w01cl-vra01,** and select **Import Item**.
4. In the **Import Library Item** dialog box, specify the settings for the first template and click **Import**.
   - **Source file**—URL or local path to `redhat6-enterprise-64.ovf` and `.vmdk` file
   - **Item name**—redhat6-enterprise-64
   - **Notes**—Red Hat Enterprise Server 6 (64-bit)
5. Repeat the procedure to import the remaining virtual machine templates.

Create machine prefixes

As a fabric administrator, you create machine prefixes that are used to create names for machines provisioned through vRealize Automation.

Tenant administrators and business group managers select these machine prefixes and assign them to provisioned machines through blueprints and business group defaults.

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

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. Click **Infrastructure** > **Administration** > **Machine Prefixes**.
3. Click **New** and specify the following settings to create a default machine prefix for the Production group, and then click **Save**:
   - **Name**—Prod-
   - **Number of Digits**—5
   - **Next Number**—1
4. Click **New** and specify the following settings to create a default machine prefix for the Development group, and then click **Save**:
   - **Name**—Dev-
   - **Number of Digits**—5
   - **Next Number**—1

Create business groups

Tenant administrators create business groups to associate services and resources to users that often correspond to a line of business, department, or other organizational unit.

Users must belong to a business group to request machines. For this implementation, create two business groups:

- Production

Development 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 with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. Select **Administration** > **Users and Groups** > **Business Groups**.
3. Click **New**.
4. On the **General** tab, enter the following values and click **Next**:
   - **Name**—Production
   - **Send capacity alert email messages to**—`vra-admin-rainpole@rai ..pole.local`
5. On the **Members** tab, type **`ug-vra-admins-rainpole@rainpole.local`** in the **Group manager role** text box, press Enter, select the displayed group, and click **Next**.
6. On the **Infrastructure** tab, select **Prod-** from the **Default machine prefix** drop-down menu and click **Finish**.
7. Click **New**.
8. On the **General** tab, configure the following values, and click **Next**:
   - **Name**—Development
   - **Send capacity alert email messages to**—`vra-admin-rainpole@rai ..pole.local`
9. On the **Members** tab, type **`ug-vra-admins-rainpole@rainpole.local`** in the **Group manager role** text box, and click **Next**.
10. On the **Infrastructure** tab, select **Dev-** from the **Default machine prefix** drop- down menu and click **Finish**.

Create reservation policies

A reservation policy is often used to collect resources into groups for different service levels, or to make a resource easily available for a particular purpose. Reservation policies 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 that are provisioned from that blueprint to a subset of available reservations. A reservation policy can include reservations of different types, but only reservations that match the blueprint type are considered when selecting a reservation for a particular request.

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. Select **Infrastructure** > **Reservations** > **Reservation Policies**.
3. Click **New**, configure the following settings, and click **OK**:
   - **Name**—SFO-Production-Policy
   - **Type**—Reservation Policy
   - **Description**—Reservation policy for Production Business Group
4. Click **New**, configure the following settings, and click **OK**:
   - **Name**—SFO-Development-Policy
   - **Type**—Reservation Policy
   - **Description**—Reservation policy for Development Business Group
5. Click **New**, configure the following settings, and click **OK**:
   - **Name**—SFO-Edge-Policy
   - **Type**—Reservation Policy
   - **Description**—Reservation policy for Tenant Edge resources

Create external network profiles

Before members of a business group can request virtual machines, fabric administrators must create network profiles to define the subnet and routing configuration for those virtual machines

Each network profile is configured for a specific network port group or virtual network to specify the IP address and the routing configuration for virtual machines provisioned to that network.

Repeat this procedure six times to create the following six external network profiles

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

Development-Web

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

b. Log in with the username `vra-admin-rainpole` and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.

2. Select **Infrastructure** > **Reservations** > **Network Profiles** > **New** > **External**.
3. On the **New Network Profile - External** page, specify the network profiles on the **General** tab.

   a. Add the values in the following table for the Production Group External Network Profile:

Table 28 Production Group external network profile values

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

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

Table 29 Development Group external network profile values

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

4. On the **DNS** tab, enter the following values for the profile you are creating:
   - P**rimary DNS**—172.16.11.4
   - **Secondary DNS**—172.17.11.4
   - **DNS suffix**—sfo01.rainpole.local
   - **DNS search suffixes**—sfo01.rainpole.local
5. On the **Network Ranges** tab, click **New** and enter the following values for the profile you are creating:

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

Table 30 Production Business Network Range values

Setting	Production web value	Production DB value	Production App value
Name	Production-Web	Production-DB	Production-App
Description	Static IP range for web tier of the Production Group	Static IP range for DB tier of the Production Group	Static IP range for App tier of the Production Group

Start IP	172.11.10.20	172.11.11.20	172.11.12.20
End IP	172.11.10.250	172.11.11.250	172.11.12.250

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

Table 31 Production Development Business Network Range values

Setting	Production web value	Production DB value	Production App value
Name	Development-Web	Development-DB	Development-App
Description	Static IP range for web tier of the Development Group	Static IP range for DB tier of the Development Group	Static IP range for App tier of the Development Group
Start IP	172.12.10.20	172.12.11.20	172.12.12.20
End IP	172.12.10.250	172.12.11.250	172.12.12.250

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

6. Click **OK** to save the network profile.
7. Repeat this procedure to create all external network profiles.

Create reservations for the shared edge and compute cluster

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

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

Table 32 Reservation names

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

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. Select **Infrastructure** > **Compute Resources** > **Compute Resources**.
3. In the **Name** column, select the compute **cluster sfo01-w01-comp01** and select
   Data Collection from the drop-down menu.
4. Click the four **Request now** buttons in each field on the page. Wait for the

data collection process to complete.

5. Click **Refresh** and verify that **Status** shows `Succeeded` for both **Inventory** and **Network and Security Inventory**.
6. Select **Infrastructure** > **Reservations** > **Reservations** > **New** > **vSphere (vCenter)**.

   The **New Reservation - vSphere (vCenter)** page appears.
7. Select the **General** tab and configure the following values:

   Table 33 Values for the General tab

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

8. Select the **Resources** tab and configure the following values:

   Table 34 Values for the Resources tab

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

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

   a. Configure the Production Business Group with the following values:

Production network path	Production Group network profile
vxw-dvs-*xxxxx*-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-*xxxxx*-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-*xxxxx*-Production-App-VXLAN	Ext-Net-Profile-Production-App

   b. Configure the Development Business Group with the following values:

Development network path	Development Group network profile
vxw-dvs-*xxxxx*-Development-Web-VXLAN	Ext-Net-Profile-Development-Web

vxw-dvs-*xxxxx*-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-*xxxxx*-Development-App-VXLAN	Ext-Net-Profile-Development-App

10. Click **OK** to save the reservation.
11. Repeat this procedure to create a reservation for the Development Business Group.

Create reservations for user edge resources

Before members of a business group can request virtual machines, as a fabric administrator, you must allocate NSX Edge resources to that business group by creating a reservation.

Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

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

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

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. Select **Infrastructure** > **Reservations** > **Reservations** > **New**> **vSphere (vCenter)**.

   The **New Reservation - vSphere (vCenter)** page appears.
3. Select the **General** tab and configure the following values:

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

4. Select the **Resources** tab and configure the following values:

Setting	Value

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

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

   a. Configure the Production Business Group with the following values:

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

   b. Configure the Development Business Group with the following values:

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

6. Click **OK** to save the reservation.
7. Repeat this procedure to create a reservation for the Development Business Group.

Create virtual machines using 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 Server compute clusters that you add to vRealize Automation, including the first vCenter Server compute instance.

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

Table 35 VM templates

VM template name	Guest OS
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)

Procedure

1. Use the vSphere Client to log in to the Compute vCenter Server:
   a. Open a web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
2. From the **Home** menu, select **VMs and Templates**.
3. Expand the `sfo01w01vc01.sfo01.rainpole.local` vCenter Server.
4. Right-click the **sfo01-w01dc** data center and select **New Folder** > **New VM and Template Folder**.
5. Type the folder name **`VM Templates`** and click **OK**.
6. From the **Home** menu, select **Content Libraries**.
7. Select **sfo01-w01cl-vra01** > **Templates**.
8. Right-click the VM Template **windows-2012r2-64** and click **New VM from This Template**.

   The **New Virtual Machine from Content Library** wizard opens.
9. On the **Select a name and folder** page, user the same template name.

   You use the same template name to create a common service catalog that works across different vCenter Server instances within your data center environment.
10. Select **VM Templates** as the folder for this virtual machine and click **Next**.
11. On the **Select a compute resource** page, expand the **sfo01-w01-comp01** cluster, select the **sfo01-w01rp-user-vm** resource pool, and click **Next**.
12. On the **Review details** page, verify the template details and click **Next**.
13. On the **Select storage** page, select the **sfo01-w01-lib01** datastore, select **Thin Provision** from the **Select virtual disk format** drop-down menu, and click **Next**.
14. On the **Select networks** page, select **sfo01-w01-vds01-management** for the **Destination Network**, and click **Next**.

    vRealize Automation changes the network according to the blueprint configuration.
15. On the **Ready to complete** page, review your configurations for the virtual machine, and click **Finish**.

    A new task for creating the virtual machine appears in the **Recent Tasks** pane. After the task is complete, the new virtual machine is created.
16. Repeat this procedure for all the VM templates in the content library.

Convert virtual machines to VM templates

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

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

Table 36 VM templates

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

Procedure

1. Use the vSphere Client to log in to the Compute vCenter Server:
   a. Open a web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
2. From the **Home** menu, select **VMs and Templates**.
3. In the Navigator pane, expand **sfo01w01vc01.sfo01.rainpole.local** > **sfo01-w01dc** > **VM Templates**.
4. In the `VM Templates` folder, right-click the **windows-2012r2-64** virtual machine and click **Template** > **Convert to Template**.
5. Click **Yes** to confirm the template conversion.
6. Repeat this procedure for all the VM templates in the content library, verifying that each VM template appears in the `VM Templates` folder.

Configure single machine blueprints

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

Procedure

1. Create a service catalog on page 68
2. Create a single machine blueprint on page 69
3. Create entitlements for business groups on page 71
4. Configure entitlements for blueprints on page 72
5. Test the deployment of a single machine blueprint on page 73

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.

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 with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. From the **Administration** tab, select **Catalog Management** > **Services** > **New**.
3. In the **New Service** page, configure the following settings and click **OK**.

- **Name**—SFO Service Catalog
- **Description**—Default setting (blank)
- **Icon**—Default setting (blank)
- **Status**—Active

Create a single machine blueprint

Create blueprints for cloning the virtual machine templates using the specified resources on the Compute vCenter Server.

Tenants can later use these blueprints for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Repeat this procedure to create the following three blueprints:

Table 37 Blueprints to create

Blueprint name	VM template	Customization specification	Reservation policy
Windows Server 2012 R2 - SFO Prod	windows-2012r2-64 (sfo01w01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Production-Policy
Windows Server 2012 R2 With SQL2012 - SFO Prod	windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Production-Policy
Redhat Enterprise Linux 6 - SFO Prod	redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)	os-linux-custom-spec	SFO-Production-Policy

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

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 with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. Select **Design** > **Blueprints** > **New**.
3. In the **New Blueprint** dialog box, on the **General** tab, configure the following settings, and click **OK**.
   - **Name**—Windows Server 2012 R2 -SFO Prod
   - **Deployment limit**—Default setting (blank)
   - **Lease (days): Minimum**—30
   - **Lease (days): Maximum**—270
   - **Archive (days)**—15
4. Select the **vSphere (vCenter) Machine** icon and drag it in the **Design Canvas**.
5. Select the **General** tab, configure the following settings, and then click **Save**.
   - **ID**—Default setting (vSphere_vCenter_Machine_1)

- **Description**—Default setting (blank)
- **Display location on request**—Not selected
- **Reservation policy**—SFO -Production-Policy
- **Machine prefix**—Use group default
- **Instances: Minimum**—Default setting
- **Instances: Maximum**—1

6. Select the **Build Information** tab, configure the following settings, and then click **Save**.
   - Blueprint type—Server
   - Action—Clone
   - Provisioning workflow—CloneWorkflow
   - Clone from—Windows-2012r2-64
   - Customization spec—s-windows-joindomain-custom-spec

   Note
   - If the value of the **Clone from** setting does not list **windows-2012r2-64** template, you must perform a data collection on the **sfo01-w01-comp01** Compute Resource.
   - Verify that the required customization spec is available in vSphere Client under **Menu** > **Policies and Profiles** > **VM Customization Specifications**.

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

   Table 38 Machine Resources tab values

Setting	Minimum	Maximum
CPUs	2	4
Memory (MB)	4096	16384
Storage (GB)	Default setting	Same value as Minimum

8. Select the **Network** tab.
   a. In the **Categories** section, select **Network & Security** to display the list of available network and security components.
   b. Select the **Existing Network** component and drag it in the **Design Canvas**.
   c. Click the **Existing network** object and on the **General** tab, select the **Ext-Net-Profile-Production-Web** network profile, and click **OK**.

   Use the following table to create subsequent blueprints.

   Table 39 Network names for blueprints

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

d. Click **Save**.

e. In the **Design Canvas**, select the **vSphere_vCenter_Machine** object.

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

Table 40 Network tab values

Network	Assignment type	Address
Ext-Net-Profile-Production-Web	Static IP	Default setting (blank)
Ext-Net-Profile-Production-DB	Static IP	Default setting (blank)
Ext-Net-Profile-Production-App	Static IP	Default setting (blank)

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

9. Select the blueprint **Windows Server 2012 R2 -SFO Prod** and click **Publish**.
10. Repeat this procedure to create additional blueprints.

Create entitlements for business groups

Add a service, catalog item, or action to an entitlement, to allow the users and groups identified in the entitlement to request provisionable items in the service catalog.

The entitlement allows members of a particular business group (for example, the Production business group) to use the blueprint. Without the entitlement, users cannot use the blueprint.

Perform this procedure to create an entitlement for the Production business group.

Table 41 Production group parameters

Entitlement name	Status	Business group	User & groups
Prod-SingleVM-Entitlement	Active	Production	ug-vra-admins-rainpole

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. On the **Administration** tab, select **Catalog Management** > **Entitlements**.
3. Click **New**.
   The **New Entitlement** page appears.
4. On the **General** tab, configure the following values, and click **Next**.
   - **Name**—Prod-SingleVM-Entitlement
   - **Description**—Default setting (blank)
   - **Expiration Date**—Default setting (blank)

- **Status**—Active
- **Business Group**—Production
- **All Users and Groups**—Not selected
- **Users and Groups**—ug-vra-admins-rainpole

5. On the **Items & Approvals tab**, add the actions that the users from the Production business group are entitled to.
   a. On the **Entitled Actions** page, click the **Add Actions** icon, add the following actions, and click **OK**.
      - **Connect using RDP (Machine)**
      - **Power Cycle (Machine)**
      - **Power off (Machine)**
      - **Power on (Machine)**
      - **Reboot (Machine)**
      - **Shutdown (Machine)**
   b. Click **Finish**.

Configure entitlements for blueprints

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

Repeat this procedure to associate the blueprints with their entitlement.

Table 42 Blueprint entitlement configuration

Blueprint name	Service catalog	Add to entitlement
Windows Server 2012 R2 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement
Red hat Enterprise Linux 6 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. On the **Administration** tab, select **Catalog Management** > **Catalog Items**.
3. On the **Catalog Items** pane, select the **Windows Server 2012 R2 - SFO Prod** blueprint in the **Catalog Items** list and click **Configure**.
4. On the **General** tab of the **Configure Catalog Item** dialog box, select **SFO Service Catalog** from the **Service** drop-down menu, and click **OK**.
5. Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement:
   a. Select **Entitlements** > **Prod-SingleVM-Entitlement**.
   b. In the **Edit Entitlement** window, select the **Items & Approvals** tab, add

the **Windows Server 2012 R2 - SFO Prod** blueprint to the **Entitled Items** list, and click **OK**.

c. Click **Finish**.

6. On the **Catalog** tab, verify that the blueprints are listed in the Service Catalog.
7. Repeat this procedure to associate all the blueprints with their entitlements.

Test the deployment of a single machine blueprint

Test your environment and confirm the successful provisioning of virtual machines using the newly created blueprints.

If multiple availability zones have been configured, you must manually place all the virtual machines provisioned by vRealize Automation into the appropriate VM group for the availability zone.

Procedure

1. Log in to the vRealize Automation Rainpole portal.
   a. Open a web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
   b. Log in with the username **`vra-admin-rainpole`** and the vRealize Automation rainpole administrator password. Domain is `rainpole.local`.
2. On the Catalog tab, click **Click here to apply filters** and select **SFO Service Catalog** from the catalog of available services.
3. Click **Request** for one of the blueprints.
4. Click **Submit**.
5. Verify that the request finishes successfully:
   a. On the **Deployments** tab, 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.

   b. Under **Status**, verify that the virtual machine successfully provisioned.
6. Verify that the virtual machine provisions in the shared edge and compute cluster:
   a. Open a web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
   c. From the **Menu** option, select **Hosts and Clusters**.
   d. In the Navigator pane, expand **sfo01w01vc01.sfo01.rainpole.local** > **sfo01- w01-comp01** > **sfo01-w01rp-user-vm** and verify that the virtual machine is present.

Reconfigure the Microsoft SQL Server instance

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

Before you begin

Allocate a static IP address on the cross-region application virtual network.

Procedure

1. Use the vSphere Client to log in to the vCenter Server:
   a. Open a web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.
2. Shut down the vRealize Automation components:
   a. From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.
   b. Right-click the following VMs according to their shutdown order and select Power > Shut Down Guest OS.

   Table 43 Virtual machine shutdown order

Product	Virtual machine name in Region A	Shutdown order
vRealize Business for Cloud	Total Number of VMs (2)	1
	sfo01vrbc01	1
	vrb01svr01	2
vRealize Automation	Total Number of VMs (12)	2
	vra01dem01b	1
	vra01dem01a	1
	sfo01ias01b	1
	sfo01ias01a	1
	vra01ims01b	2
	vra01ims01a	3
	vra01iws01b	4
	vra01iws01a	5
	vra01svr01c	6
	vra01svr01b	7
	vra01svr01a	8
	vra01mssql01	9

3. Migrate the Microsoft SQL Server virtual machine to the sfo01-m01fd-vra folder and connect to the Mgmt-xRegion01-VXLAN port group:
   a. From the Home menu, select Hosts and Clusters and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.
   b. Right-click **vra01mssql01**, select **Move to folder** > **sfo01-m01fd-vra**, and click **OK**.
   c. Right-click **vra01mssql01** and select **Edit Settings**.

d. On the **Edit Settings** page, browse to the Network Adapter 1 distributed port group that ends with `Mgmt-xRegion01-VXLAN` and click **OK**.

e. Right-click **vra01mssql01** and select **Power** > **Power on**.

4. Change the IP address of the vra01mssql01 virtual machine:

a. Right-click **vra01mssql01**, and select **Open Console**.

b. Log in with the Windows administrator username and password.

c. From the Windows **Start** menu, select **Control Panel** > **Network and Sharing Center**.

d. Click **`Change adapter settings`**.

e. Right-click the Ethernet adapter and select **Properties**.

f. Select **Internet Protocol Version 4 (TCP/IPv4)** > **Properties**.

g. Enter the following settings and click **OK**:

- **IP Address**—192.168.11.62
- **Subnet Mask**—255.255.255.0
- **Default Gateway**—192.168.11.1

5. Change the IP address in the DNS for the vra01mssql01 virtual machine:

a. Log in to the DNS server that resides in the sfo01.rainpole.local domain by using a Remote Desktop Protocol (RDP) client.

b. Open an RDP connection to the `dc01rpl.rainpole.local` DNS server.

c. Log in with the Active Directory administrator username and password.

d. From the Windows **Start** menu, type **`dnsmgmt.msc`** in the Search text box and press Enter.

e. In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the rainpole.local domain.

f. In the right pane, double-click the **vra01mssql01** record, modify the **IP Address** using the following settings, and click **OK**

- **Fully qualified domain name (FQDN)**—vra01mssql01.rainpole.local
- **IP Address**—192.168.11.62
- **Update associated pointer (PTR) record**—Selected

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

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

b. Log in with the Windows administrator username and password.

7. Install vRealize Log Insight Windows Agents in vra01mssql01:

a. From the vra01mssql01 Windows environment, log in to the vRealize Log Insight user interface:

- Open a web browser and go to `https://sfo01vrli01.sfo01.rainpole.local`.
- Log in with the username **`admin`** and the deployment administrator password.

b. Click the configuration drop-down menu icon and click **Administration**.

c. Under **Management**, select **Agents** and click the **Download Log Insight Agent Version** link.

d. In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the `.msi` file on the vra01mssql01 virtual machine.

e. Open an administrative command prompt, and navigate to the directory where you saved the `.msi` file.

f. Run the following command to install the vRealize Log Insight agent with custom values:

```
VMware-Log-Insight-Agent-4.7.0-
build_number_192.168.31.10.msi SERVERPORT=9000
AUTOUPDATE=yes LIAGENT_SSL=no
```

g. In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.

h. In the **Host** text box, select **sfo01vrli01.sfo01.rainpole.local** and click **Install**.

i. Click **Finish**.

8. Use the vSphere Client to log in to the vCenter Server:

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

   b. Log in using the username **`administrator@vsphere.local`** and the vSphere administrator password.

9. Power on the remaining vRealize Automation components:

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

   b. Right-click the following VMs, according to their startup order and select **Power** > **Power on**.

Table 44 Virtual machine startup order

Product	Virtual machine name in Region A	Startup order
vRealize Automation	Total Number of VMs (11)	1
	vra01svr01a	1
	vra01svr01b	2
	vra01svr01c	3
	vra01iws01a	4
	vra01iws01b	5
	vra01ims01a	6
	vra01ims01b	7
	sfo01ias01a	8
	sfo01ias01b	8

	vra01dem01a	8
	vra01dem01b	8
vRealize Business for Cloud	vRealize Business for Cloud	2
	vrb01svr01	1
	sfo01vrbc01	2

10. Test your environment and confirm the successful provisioning of virtual machines.

    See Test the deployment of a single machine blueprint on page 73.

APPENDIX A
Using the Cloud Builder VM to Deploy vCenter Server

Use the following script to deploy a vCenter Server instance using the Cloud Builder VM.

```
   "_version": "2.13.0",
    "new_vcsa": {
        "vc": {
            "hostname": "mgt-vcenter.lab3.local",
            "username":
            "administrator@vsphere.local",
            "password": "VMw@re1!",
            "deployment_network": "vCenter Server Network-ad9cf3d1-72a2-
4729- beff-723c2876225b",
            "datacenter": "VxRail-Datacenter",
            "datastore": "VxRail-Virtual-SAN-Datastore-ad9cf3d1-72a2-
4729- beff-723c2876225b",
            "target": "VxRail-Virtual-SAN-Cluster-ad9cf3d1-72a2-4729-beff-723c2876225b"
        },
        "appliance": {
            "thin_disk_mode":
            true,
            "deployment_option": "management-
            small", "name": "wld-vcenter"
        },
        "network": {
            "ip_family": "ipv4",
            "mode": "static",
            "ip":
            "172.16.64.20",
            "dns_servers": [
            "172.16.64.4" ], "prefix":
            "24",
            "gateway": "172.16.64.1",
            "system_name": "wld-vcenter.lab3.local"
        },
        "os": {
            "password": "VMw@re1!",
            "ntp_servers": [
            "ntp.lab3.local" ],
            "ssh_enable": true
        },
        "sso": {
            "password": "VMw@re1!",
            "domain_name":
            "vsphere.local",
            "platform_services_controller": "mgt-
            psc01.lab3.local", "sso_port": 443
        }
    }
}
```