

# IT Automating IT Use Case Deployment Using vRealize Suite Lifecycle Manager

27 MAR 2018

VMware Validated Design 4.2

VMware Validated Design for IT Automating IT 4.2



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

About IT Automating IT Use Case Deployment Using vRealize Suite Lifecycle Manager	5
vRealize Suite Lifecycle Manager Overview	5
vRealize Suite Lifecycle Manager Solution Path Installation Methods and Deployment Types	6
<b>1 IT Automating IT Solution Path</b>	<b>8</b>
<b>2 Before You Deploy vRealize Suite Lifecycle Manager</b>	<b>12</b>
Configure User Access in vSphere for Integration with vRealize Suite Lifecycle Manager	12
Hostname and IP Address for vRealize Suite Lifecycle Manager	15
Distributed Firewall Configuration for vRealize Suite Lifecycle Manager	16
My VMware Account for vRealize Suite Lifecycle Manager	19
Create a Certificate for the vRealize Suite Lifecycle Manager Appliance	20
<b>3 Deploy and Configure the vRealize Suite Lifecycle Manager Appliance</b>	<b>23</b>
Deploy the vRealize Suite Lifecycle Manager Appliance	24
Configure the vRealize Suite Lifecycle Manager Appliance	25
Register vRealize Suite Lifecycle Manager with My VMware	35
OVA Configuration in vRealize Suite Lifecycle Manager	36
Download Marketplace Content in vRealize Suite Lifecycle Manager	39
Add a Data Center to vRealize Suite Lifecycle Manager	39
<b>4 Pre-Deployment Tasks for the IT Automating IT Use Case</b>	<b>41</b>
Generate Certificates for the IT Automating IT Solution Path	41
Pre-deployment Tasks for vRealize Automation	43
Pre-Deployment Tasks for vRealize Operations Manager	66
Prerequisites for Deploying vRealize Log Insight	68
<b>5 Deployment Paths for the IT Automating IT Use Case with vRealize Suite Lifecycle Manager</b>	<b>70</b>
Deploy the IT Automating IT Use Case with the vRealize Suite Lifecycle Manager Installation Wizard	70
Deploy the IT Automating IT Use Case with a vRealize Suite Lifecycle Manager JSON Configuration File	80
<b>6 Post-Deployment Tasks for vRealize Automation</b>	<b>90</b>
Move vRealize Automation and vRealize Business for Cloud Appliances to Virtual Machine Folders	91
Set Up NTP on the vRealize Automation Appliance	92

Create Anti-Affinity Rules for vRealize Automation Virtual Machines	93
Replace the vRealize Automation Certificate	94
vRealize Automation Default Tenant Configuration	95
vRealize Automation Tenant Creation	97
Embedded vRealize Orchestrator Configuration	104
vRealize Business Installation	112
Cloud Management Platform Post-Installation Tasks	117
Content Library Configuration	122
Tenant Content Creation	124
<b>7 Post-Deployment Tasks for vRealize Operations Manager</b>	<b>151</b>
Configure the Load Balancer for vRealize Operations Manager	152
Move vRealize Operations Analytics Cluster and Remote Collector Nodes to Virtual Machine Folders	156
Configure DRS Anti-Affinity Rules for vRealize Operations Manager	157
Proceed Using Evaluation Mode for vRealize Operations Manager	158
Replace vRealize Operations Manager Certificate	159
Group Remote Collector Nodes	160
Add an Authentication Source for the Active Directory	160
Configure User Access in vSphere for Integration with vRealize Operations Manager	162
Add vCenter Adapter Instances to vRealize Operations Manager	165
Connect vRealize Operations Manager to the NSX Manager Instances	167
Connect vRealize Operations Manager to vRealize Automation	173
Connect vRealize Operations Manager with vRealize Business	178
Enable Storage Device Monitoring in vRealize Operations Manager	180
Enable vSAN Monitoring in vRealize Operations Manager	183
Configure Email Alerts for vRealize Operations Manager	185
<b>8 Post-Deployment Tasks for vRealize Log Insight</b>	<b>187</b>
Move vRealize Log Insight Cluster Nodes to a Virtual Machine Folder	188
Configure a DRS Anti-Affinity Rule for vRealize Log Insight	189
Configure the vRealize Log Insight Master node	189
Enable Active Directory Support for vRealize Log Insight	190
Replace the Certificate of vRealize Log Insight	191
Connect vRealize Log Insight to the vSphere Environment	192
Connect vRealize Log Insight to vRealize Operations Manager	197
Connect vRealize Log Insight to the NSX Instances	204
Connect vRealize Log Insight to vRealize Automation	211
Install the vRealize Log Insight Content Pack for Linux	219
Configure a Log Insight Agent Group for the Management Virtual Appliances	220
Configure Log Retention and Archiving	221

# About IT Automating IT Use Case Deployment Using vRealize Suite Lifecycle Manager

*IT Automating IT Use Case Deployment by Using vRealize Suite Lifecycle Manager* provides an alternative method of deploying and configuring a VMware Validated Design use case by using VMware vRealize Suite Lifecycle Manager. You can use vRealize Suite Lifecycle Manager to deploy three common use cases: IT Automating IT, Intelligent Operations, and Micro-segmentation.

This guide helps you deploy and configure the products for each use case and provides step-by-step instructions for the following tasks:

- Deployment and configuration of the vRealize Suite Lifecycle Manager appliance
- Pre-deployment tasks for products utilized by the use case
- Deployment of the products utilized by the use case using vRealize Suite Lifecycle Manager
- Post-deployment tasks for products utilized the use case

---

**Note** This guide does not include instructions for deploying the VMware Validated Design for Software-Defined Data Center foundation products. See the *Deployment for Region A* document in the VMware Validated Design for the Software-Defined Data Center documentation.

---

## Intended Audience

The *IT Automating IT Use Case Deployment by Using vRealize Suite Lifecycle Manager* document is for cloud architects, infrastructure administrators, and cloud administrators who are familiar with VMware Validated Design for Software-Defined Data Center and want to use vRealize Suite Lifecycle Manager to deploy VMware Validated Design use cases.

## vRealize Suite Lifecycle Manager Overview

vRealize Suite Lifecycle Manager automates the deployment, patching, and upgrade of the vRealize Suite solutions, resulting in simplified operational experience for customers.

### Overview

vRealize Suite Lifecycle Manager automates the lifecycle management of the vRealize Suite through both a web-based management application and an API, freeing you to focus on business-critical initiatives and improving time to value, reliability, and consistency.

The vRealize Suite Lifecycle Manager solution supports the deployment, patching, and upgrade of following VMware vRealize Suite products:

- VMware vRealize Automation (with Embedded vRealize Orchestrator)
- VMware vRealize Business for Cloud
- VMware vRealize Operations Manager
- VMware vRealize Log Insight

## Deployment Model

vRealize Suite Lifecycle Manager is available as a self-contained virtual appliance shipped as an OVA (Open Virtual Appliance) image for a seamless deployment experience within an on-premises, vSphere-based, private cloud platform. You access vRealize Suite Lifecycle Manager as a web-based application through a local user or VMware Identity Manager single sign-on integration.

Once deployed, the appliance is registered with one or more vCenter Server instances where an administrator can automate the following operations for the lifecycle management of the vRealize Suite.

- Management of a vRealize Suite Product Repository (Installation and Upgrade Media)
- Create Environments with Solution or Product-based Structures (Greenfield)
- Ingest Existing vRealize Suite-based Environments (Brownfield)
- Analysis of Configuration Drift within Environments
- Scale-out of Environments
- Upgrade of Environments

## vRealize Suite Lifecycle Manager Solution Path Installation Methods and Deployment Types

Using vRealize Suite Lifecycle Manager, you create an environment with a prescriptive solution path configuration for the SDDC through an installation wizard or a configuration file.

### Installation Methods

vRealize Suite Lifecycle Manager provides two installation methods for an environment creation:

- Installation Wizard
- JSON Configuration File

When creating a new environment using the installation wizard, you provide a target datacenter, an environment type, and an environment name. When creating a new environment using the configuration file, you provide a target datacenter, an environment type, an environment name, as well as a properly formatted product JSON configuration file.

## Deployment Types

vRealize Suite Lifecycle Manager provides two options to create install vRealize Suite components:

- **Product Path** – as the default option in vRealize Suite Lifecycle Manager, you select the individual vRealize Suite products you would like to include in an SDDC. The product path allows you to perform a new greenfield installation or to import an existing brownfield installation of the vRealize Suite components. For a greenfield deployment, you select the product version and size to install for each component.
- **Solution Path** – you use the solution path for a new greenfield installation of use case-based components in an SDDC. The solution path based deployment allows vRealize Suite Lifecycle Manager to install and configure a specific set of vRealize Suite products suited for a VMware Validated Design use case. Within each solution path, you can view the specific products and product versions included in the selected use case.

The Solution Paths included in vRealize Suite Lifecycle Manager are:

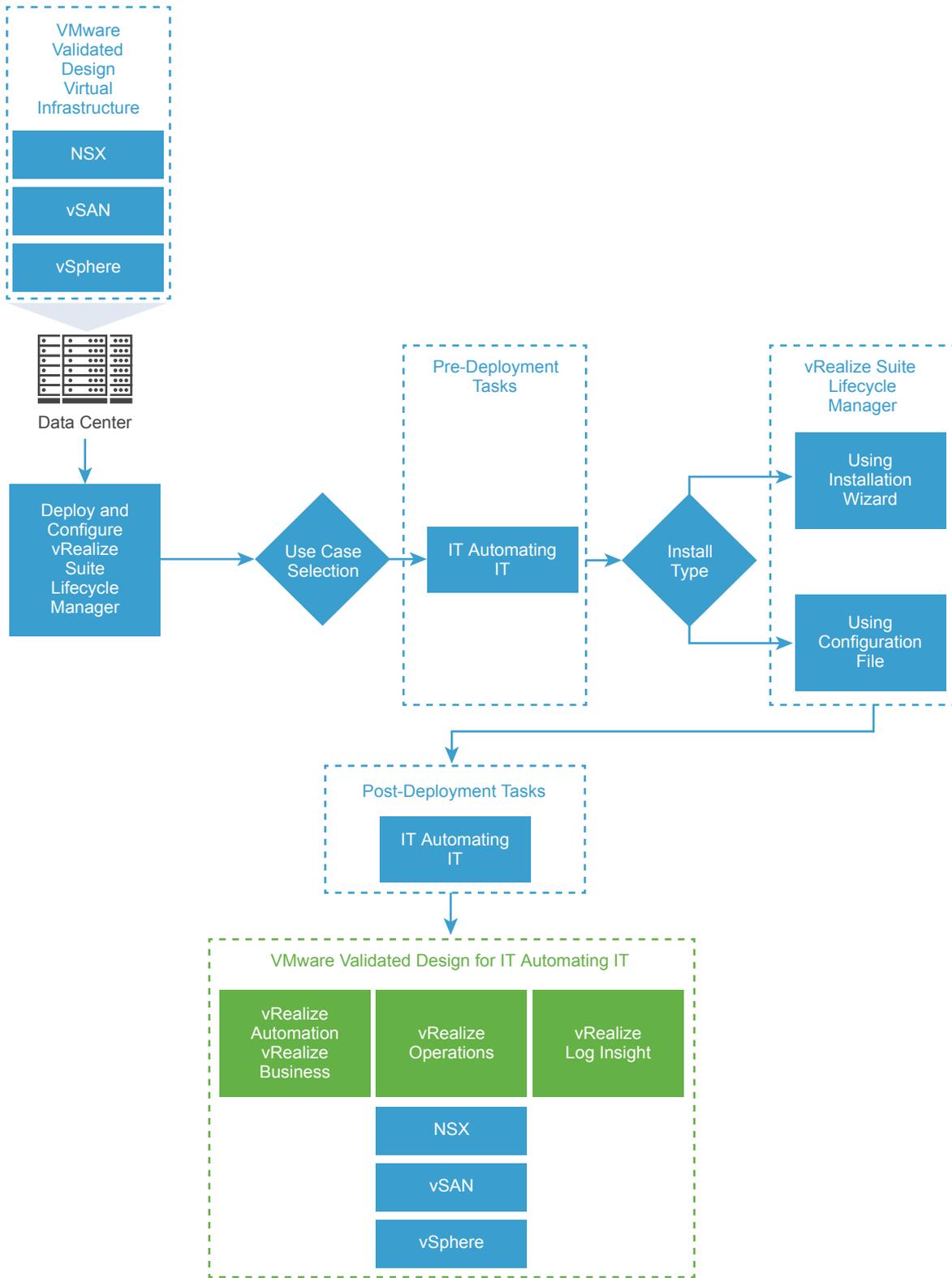
- 1 **IT Automating IT** – Enables automation and simplification of workload provisioning tasks of production-ready infrastructure and applications in the SDDC.
- 2 **Intelligent Operations** – Enables proactive identification and remediation of performance, capacity, and configuration issues in the SDDC.
- 3 **Micro-segmentation** – Enables distributed firewall and isolation policies to create better network security in the SDDC.

# IT Automating IT Solution Path

1

To deploy the IT Automating IT use case, you perform pre-deployment tasks that include installing the VMware Validated Design Software-Defined Data Center Virtual Infrastructure Layer. You deploy the vRealize Suite products needed by this solution path using the vRealize Suite Lifecycle Manager installation wizard or configuration file. Afterwhich, you can select from the use cases in the *scenarios* guide and follow the step-by-step instructions in that document.

Figure 1-1. vRealize Suite Lifecycle Manager Solution Path for IT Automating IT



## Procedure

- 1 As your basis, you deploy the virtual infrastructure, as discussed in *Deployment for Region A* at <https://docs.vmware.com/en/VMware-Validated-Design/4.2/com.vmware.vvd.sddc-deploya.doc/GUID-657DB777-D919-4C23-BA5E-B98D8A91CA8B.html>.
  - a Install and Configure ESXi Hosts in Region A
  - b Deploy and Configure the Platform Services Controller and vCenter Server Components in Region A
  - c Deploy and Configure the NSX Instance for the Management Cluster in Region A
  - d Deploy and Configure the Shared Edge and Compute Cluster Components in Region A
  - e Deploy and Configure Shared Edge and Compute Cluster NSX Instance in Region AIn the *Deployment for Region A* guide, each task is for Region A. Because this is a single-region deployment, we use the Region A task.
- 2 Perform pre-deployment tasks for vRealize Suite Lifecycle Manager appliance.  
See [Chapter 2 Before You Deploy vRealize Suite Lifecycle Manager](#).
- 3 Deploy the vRealize Suite Lifecycle Manager appliance, upload the OVA file for your use case, and complete certificate setup.  
See [Chapter 3 Deploy and Configure the vRealize Suite Lifecycle Manager Appliance](#).
- 4 Perform pre-deployment tasks for the products that are used by this use case.
  - a [Pre-deployment Tasks for vRealize Automation](#).
  - b [Pre-Deployment Tasks for vRealize Operations Manager](#).
  - c [Prerequisites for Deploying vRealize Log Insight](#).

---

**Note** No other pre-deployment tasks are required for this use case. Not all of the products require pre-deployment tasks.

---
- 5 Deploy the required products by running the installation wizard or by using the JSON file.
  - [Deploy the IT Automating IT Use Case with the vRealize Suite Lifecycle Manager Installation Wizard](#).
  - [Create the Environment for IT Automating IT with a JSON Configuration File](#).

- 6 Perform post-deployment tasks for the products that this use case uses:
  - a Perform post-deployment tasks for the vRealize Automation suite of products, which includes vRealize Orchestrator and vRealize Business for Cloud.  
See [Chapter 6 Post-Deployment Tasks for vRealize Automation](#).
  - b Perform post-deployment tasks for vRealize Operations Manager.  
See [Chapter 7 Post-Deployment Tasks for vRealize Operations Manager](#).
  - c Perform post-deployment tasks for vRealize Log Insight.  
See [Chapter 8 Post-Deployment Tasks for vRealize Log Insight](#).
- 7 Select one or more of the scenarios for IT Automating IT and implement them.  
See the *Scenarios* guide for IT Automating IT <https://docs.vmware.com/en/VMware-Validated-Design/4.2/com.vmware.vvd.it.automation-usecases.doc/GUID-2BA1821B-7F87-4CA8-B0E4-15EA28D12128.html>.

# Before You Deploy vRealize Suite Lifecycle Manager

# 2

Before you deploy vRealize Suite Lifecycle Manager, you configure a least privilege service account for the Management vCenter Server instance, enable additional distributed firewall configurations to the existing VMware Validated Design for Software-Defined Data Center virtual infrastructure layer, establish a My VMware account, and generate a certificate for the vRealize Suite Lifecycle Manager appliance.

## 1 [Configure User Access in vSphere for Integration with vRealize Suite Lifecycle Manager](#)

Configure an operations service account with the required permissions to enable vRealize Suite Lifecycle Manager to deploy and manage the Software-Defined Data Center (SDDC) solutions on the Management vCenter Server.

## 2 [Hostname and IP Address for vRealize Suite Lifecycle Manager](#)

Before deploying and configuring vRealize Suite Lifecycle Manager in this VMware Validated Design, allocate a hostname and IP address for the appliance.

## 3 [Distributed Firewall Configuration for vRealize Suite Lifecycle Manager](#)

Configuring a distributed firewall for use with your SDDC increases the security level of your environment by allowing only the network traffic that is required for the SDDC to run. In this design, additional policies are defined that allow access to vRealize Suite Lifecycle Manager.

## 4 [My VMware Account for vRealize Suite Lifecycle Manager](#)

You can register vRealize Suite Lifecycle Manager to access vRealize Suite product licenses and download product OVAs to the repository.

## 5 [Create a Certificate for the vRealize Suite Lifecycle Manager Appliance](#)

Use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates that are signed by the Microsoft certificate authority (MSCA) for vRealize Suite Lifecycle Manager.

## Configure User Access in vSphere for Integration with vRealize Suite Lifecycle Manager

Configure an operations service account with the required permissions to enable vRealize Suite Lifecycle Manager to deploy and manage the Software-Defined Data Center (SDDC) solutions on the Management vCenter Server.

## Active Directory User Service Account for vRealize Suite Lifecycle Manager

A service account provides non-interactive and non-human access to services and APIs to the components of the SDDC. You must create a service account for vRealize Suite Lifecycle Manager to deploy and manage the life cycle of vRealize Suite components in the SDDC.

---

**Note** A service account is a standard Active Directory account that you configure with a non-expiring password that cannot be changed by the account itself.

---

The vRealize Suite Lifecycle Manager service account is used in a one-directional fashion to enable secure application-to-application communication to the Management vCenter Server instance. A custom role ensures that the service account has the least required permissions for authentication, data collection, and life cycle management operations.

You associate the `svc-vrslcm-vsphere` service account in the Active Directory with a custom vRealize Suite Lifecycle Manager user role that has specific privileges. You assign the user to the vCenter Server instance in the inventory.

**Table 2-1. Application-to-Application Service Account for vRealize Suite Lifecycle Manager**

Username	Source	Destination	Description	Required Role
svc-vrslcm-vsphere	vRealize Suite Lifecycle Manager	Management vCenter Server	A service account for deploying and managing the life cycle of vRealize Suite components on the Software-Defined Data Center management cluster.	vRealize Suite Lifecycle Manager User (Custom)

---

## Define a User Role in vSphere for vRealize Suite Lifecycle Manager

Create a user role in the vSphere Web Client with the required privileges for vRealize Suite Lifecycle Manager.

## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page, under **Administration**, click **Roles**.
- 3 Create a role for all application-to-application interactions between vRealize Suite Lifecycle Manager and vSphere.
  - a On the **Roles** page, click the **Create Role action** icon.
  - b In the **Create Role** dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role Name	vRealize Suite Lifecycle Manager User
Privilege	<ul style="list-style-type: none"> <li>▪ <b>Datastore.Allocate Space</b></li> <li>▪ <b>Datastore.Browse Datastore</b></li> <li>▪ <b>Datastore.Update Virtual Machine Files</b></li> <li>▪ <b>Host.Local.Operations.Add Host to vCenter</b></li> <li>▪ <b>Host.Local.Operations.Create Virtual Machine</b></li> <li>▪ <b>Host.Local.Operations.Delete Virtual Machine</b></li> <li>▪ <b>Host.Local.Operations.Reconfigure Virtual Machine</b></li> <li>▪ <b>Network.Assign Network</b></li> <li>▪ <b>Resource.Assign vApp to Resource Pool</b></li> <li>▪ <b>Resource.Assign Virtual Machine to Resource Pool</b></li> <li>▪ <b>vApp.* (All privileges.)</b></li> <li>▪ <b>Virtual Machine.* (All privileges.)</b></li> </ul>

This role inherits the **System.Anonymous**, **System.View**, and **System.Read** privileges.

- 4 The Management vCenter Server propagates the role to the other linked vCenter Server instances.

## Configure User Privileges in vSphere for Integration with vRealize Suite Lifecycle Manager

Assign permissions to the operations service account to deploy and manage SDDC components on the Management vCenter Server with vRealize Suite Lifecycle Manager.

- The svc-vrslcm-vsphere user has the required privileges established for the Management vCenter Server.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Assign permissions to the service account according to its roles.
  - a From the **Home** menu, select **Host and Clusters**.
  - b In the Navigator, select `sfo01m01vc01.sfo01.rainpole.local`.
  - c Navigate to **Permissions > Add permission**.
  - d In the **Add Permission** dialog box, click **Add** to associate a user or a group with a role.
  - e In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select `rainpole.local`, in the filter box type `svc-vrs1cm-vsphere`, and press Enter.
  - f From the list of users and groups, select `svc-vrs1cm-vsphere`, click **Add**, and click **OK**.
  - g In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **vRealize Suite Lifecycle Manager User**, ensure that **Propagate to children** is selected, and click **OK**.

## Hostname and IP Address for vRealize Suite Lifecycle Manager

Before deploying and configuring vRealize Suite Lifecycle Manager in this VMware Validated Design, allocate a hostname and IP address for the appliance.

Allocate a hostname and IP address for each component. Configure both forward and reverse DNS records with the designated fully qualified domain name (FQDN) and IP address.

**Table 2-2. Hostname and IP Address for vRealize Suite Lifecycle Manager Appliance**

Component	IP Address	DNS A Record	Create DNS PTR Record
vRealize Suite Lifecycle Manager Appliance	192.168.11.20	vrs01lcm01.rainpole.local	Yes

# Distributed Firewall Configuration for vRealize Suite Lifecycle Manager

Configuring a distributed firewall for use with your SDDC increases the security level of your environment by allowing only the network traffic that is required for the SDDC to run. In this design, additional policies are defined that allow access to vRealize Suite Lifecycle Manager.

You define additional explicit policies for the distributed firewall, which allow communication between vRealize Suite Lifecycle Manager and the necessary SDDC components.

## Create IP Set for vRealize Suite Lifecycle Manager

Create an IP set for the vRealize Suite Lifecycle Manager appliance in the management cluster. You use the IP set later to create a security group for use with the additional distributed firewall rules established for vRealize Suite Lifecycle Manager.

A single IP set is added to support vRealize Suite Lifecycle Manager.

**Table 2-3. IP Set for vRealize Suite Lifecycle Manager**

Name	IP Addresses
vRealize Suite Lifecycle Manager	<i>vRealize-Suite-Lifecycle-Manager_IP's</i>

### Prerequisites

Before configuring the additional distributed firewall policies for vRealize Suite Lifecycle Manager, ensure that the distributed firewall configuration for the management cluster is in place as defined in the VMware Validated Design for Software-Defined Data Center. See *Deployment for Region A*.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create the IP set for vRealize Suite Lifecycle Manager.
  - a In the **Navigator**, click **Networking & Security**.
  - b Click **NSX Managers** and select the **172.16.11.65** instance.
  - c Click **Manage**, click **Grouping Objects**, and click **IP Sets**.

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

For all IP sets that you configure, select the **Mark this object for Universal Synchronization** check box.

Setting	Value
Name	vRealize Suite Lifecycle Manager
IP Addresses	192.168.11.20
Mark this object for Universal Synchronization	Selected

## Create Security Group for vRealize Suite Lifecycle Manager

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 together.

You perform this procedure multiple times to configure all the necessary security groups. In addition, you create the VMware Appliances and Windows Servers groups from the security groups you add in the previous repetitions of this procedure.

**Table 2-4. Security Group for vRealize Suite Lifecycle Manager**

Name	Object Type	Selected Object
vRealize Suite Lifecycle Manager	IP Sets	vRealize Suite Lifecycle Manager
VMware Appliances	Security Groups	vRealize Suite Lifecycle Manager

### Prerequisites

An IP set for the vRealize Suite Lifecycle Manager appliance is created.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking & Security** and click **NSX Managers**.
- 3 Select the **172.16.11.65** NSX Manger instance, and click the **Manage** tab.

- 4 Click **Grouping Objects**, select **Security Group**, and click the **Add new Security Group** icon.  
The **Add Security Group** wizard appears.
- 5 On the **Name and description** page, enter **vRealize Suite Lifecycle Manager** in the **Name** text box, select the **Mark this object for Universal Synchronization** check box, and click **Next**.  
For all security groups that you configure, select the **Mark this object for Universal Synchronization** check box.
- 6 On the **Select objects to include** page, select **IP Sets** from the **Object Type** drop-down menu, select **vRealize Suite Lifecycle Manager** from the list of available objects, click the **Add** button, and click **Next**.
- 7 On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.
- 8 In **Security Group**, select the group label **VMware Appliances** and click the **Edit Security Group** icon.  
The **Edit Security Group** wizard appears.
- 9 On the **Name and description** page, click **Next**.
- 10 On the **Select objects to include** page, select **Security Group** from the **Object Type** drop-down menu, select **vRealize Suite Lifecycle Manager** from the list of available objects, click the **Add** button, and click **Next**.
- 11 On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.

## Add Distributed Firewall Rule for vRealize Suite Lifecycle Manager

A firewall rule consists of a section to segregate the firewall rules and the rule itself, which defines what network traffic is blocked or allowed.

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

### Prerequisites

- The IP sets, security groups, and distributed firewall rules from the VMware Validated Design for Software-Defined Data Center foundation are implemented.
- The IP set for vRealize Suite Lifecycle Manager is created.
- The Security Group for vRealize Suite Lifecycle Manager is created.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a distributed firewall rule to allow administrative access to the vRealize Suite Lifecycle Manager user.

Name	Source	Destination	Service / Port
Allow vRSLCM to Admins	Administrators	vRealize Suite Lifecycle Manager	HTTPS

- a In the **VMware Management Services** section, click **Add rule**.
- b In the **Name** cell, click the **Edit** icon to change the rule name to **Allow vRSLCM to Admins**.
- c Click the **Edit** icon in the **Source** column, change the **Object Type** to **Security Groups**, add **Administrators** to the **Selected Objects** list, and click **OK**.
- d Click the **Edit** icon in the **Destination** column, change the **Object Type** to **Security Groups**, add **VMware Appliances** and **Update Manager Download Service** to the **Selected Objects** list, and click **OK**.
- e Click the **Edit** icon in the **Service** column, enter **HTTPS** in the filter, add **HTTPS** to the **Selected Objects** list, and click **OK**.
- f Click **Publish Changes**.

## My VMware Account for vRealize Suite Lifecycle Manager

You can register vRealize Suite Lifecycle Manager to access vRealize Suite product licenses and download product OVAs to the repository.

**Note** Using the My VMware integration allows you to download vRealize Suite product OVAs to the vRealize Suite Lifecycle Manager appliance and is the recommended path to simplify, automate, and organize the repository. If your organization must restrict outbound traffic from the management components of the SDDC, you can download the vRealize Suite product OVAs from My VMware and upload them to the vRealize Suite Lifecycle Manager repository.

My VMware provides an integrated, self-service, account-based interface focused on simplifying and streamlining your online product license and support management experience. It allows you to:

- View and manage product licenses and support details by account.

- Get help and file support requests.
- View and manage evaluations.
- View orders and support contract details.
- Create folders to better organize license keys.
- Manage user rights and permissions for license key management and support details.
- Request a renewal quote for support contracts.

[Learn more](https://my.vmware.com) about My VMware or visit <https://my.vmware.com>.

vRealize Suite Lifecycle Manager registers an account with My VMware to download the product OVAs to its repository. You can select an available license key from a product entitlement during an environment creation.

You can structure the folders, user, and permissions in a My VMware entitlement account in any way that best serves the asset management and operations support needs of your business. The minimum requirements and permissions include:

- A folder with a vRealize Suite product entitlement.
  - View License Keys & User Permissions
  - Download Products

To register vRealize Suite with My VMware, invite a designated user to the entitlement account and limit the folder level permissions for the user.

- Refer to [KB 2070555](#) for details on inviting a user to a My VMware account.
- Refer to [KB 2006977](#) for details on assigning user permissions in a My VMware account.

**Table 2-5. vRealize Suite Lifecycle Manager User Product Entitlement Example**

First Name	Last Name	User Email	Minimum Folder Permissions	Folder	Product Entitlement in Folder
vRealize Suite Lifecycle Manager User	at Rainpole	vvd- vrslcm@rainpole.local	<ul style="list-style-type: none"> <li>■ View License Keys &amp; User Permissions</li> <li>■ Download Products</li> </ul>	<ul style="list-style-type: none"> <li>■ Home folder or</li> <li>■ Child folder</li> </ul>	vRealze Suite

## Create a Certificate for the vRealize Suite Lifecycle Manager Appliance

Use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates that are signed by the Microsoft certificate authority (MSCA) for vRealize Suite Lifecycle Manager.

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

## Prerequisites

- Provide a Windows Server 2012 host that is part of the sfo01.rainpole.local domain.
- Install a Certificate Authority server on the rainpole.local domain.

## Procedure

- 1 Log in to a Windows host that has access to your data center.
- 2 Download the CertGenVVD-*version*.zip file of the Certificate Generation Utility from VMware Knowledge Base article [2146215](#) on the Windows host where you connect to the data center and extract the ZIP file to the C: drive.
- 3 In the C:\CertGenVVD-*version* folder, open the default.txt file in a text editor.
- 4 Verify that following properties are configured.

```
ORG=Rainpole Inc.
OU=Rainpole.local
LOC=SFO
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
```

- 5 Delete all files in the C:\CertGenVVD-*version*\ConfigFiles folder
- 6 In the C:\CertGenVVD-*version*\ConfigFiles folder, create a text file named vrs01lcm01.txt with the following content.

For example, the configuration files for the vRealize Suite Lifecycle Manager instance must contain the following properties:

### vrslcm.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=vrs01lcm01.rainpole.local
keysize=default
[SAN]
vrs01lcm01
vrs01lcm01.rainpole.local
```

- 7 Open a Windows PowerShell prompt and navigate to the CertGenVVD folder.

```
cd C:\CertGenVVD-version
```

- 8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

- 9 Validate if you can run the utility using the configuration on the host and verify if VMware is included in the printed CA template policy.

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

- 10 Generate MSCA-signed certificates.

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

- 11 In the C:\CertGenVVD-*version* folder, verify that the utility created the SignedByMSCACerts subfolder.

# Deploy and Configure the vRealize Suite Lifecycle Manager Appliance

# 3

In this section, you deploy the vRealize Suite Lifecycle Manager appliance, configure the common settings, replace the appliance certificate, generate a certificate for solution path deployments, configure the OVA sources, and download solutions content from the VMware Marketplace.

## Procedure

### 1 [Deploy the vRealize Suite Lifecycle Manager Appliance](#)

The vRealize Suite Lifecycle Manager appliance is deployed on an existing VMware Validated Design for the Software-Defined Data Center environment. As part of the appliance deployment, you specify storage, networking, and other key appliance attributes.

### 2 [Configure the vRealize Suite Lifecycle Manager Appliance](#)

In the vRealize Suite Lifecycle Manager user interface, you configure the common settings, replace the appliance certificate, generate a certificate for solution path deployments, configure the OVA sources, and download solutions content from the VMware Marketplace.

### 3 [Register vRealize Suite Lifecycle Manager with My VMware](#)

You can integrate vRealize Suite Lifecycle Manager directly with a My VMware account to access vRealize Suite licenses within an entitlement account and manage the download of product OVAs for install, patch, and upgrade. The My VMware account registration is also used to download content from the VMware Marketplace.

### 4 [OVA Configuration in vRealize Suite Lifecycle Manager](#)

vRealize Suite Lifecycle Manager provides two methods to retrieve and store product OVAs for install, patch, and upgrade of the vRealize Suite components.

### 5 [Download Marketplace Content in vRealize Suite Lifecycle Manager](#)

Use vRealize Suite Lifecycle Manager to add and manage content from Marketplace, such as the vRealize Operations Manager management packs, and vRealize Log Insight content packs for a specific solution path.

### 6 [Add a Data Center to vRealize Suite Lifecycle Manager](#)

Before you can create an environment for a solution path deployment, you must add a data center in using vRealize Suite Lifecycle Manager and associate the Management vCenter Server instance.

# Deploy the vRealize Suite Lifecycle Manager Appliance

The vRealize Suite Lifecycle Manager appliance is deployed on an existing VMware Validated Design for the Software-Defined Data Center environment. As part of the appliance deployment, you specify storage, networking, and other key appliance attributes.

## Prerequisites

Before deploying the vRealize Suite Lifecycle Manager appliance, you must complete deployment of the foundation Software-Defined Data Center.

**Note** This guide refers to SDDC components based on the VMware Validated Design for Software-Defined Data Center. See Virtual Infrastructure Deployment in the *Deployment for Region A* document at <https://docs.vmware.com/en/VMware-Validated-Design/4.2/com.vmware.vvd.sddc-deploya.doc/GUID-657DB777-D919-4C23-BA5E-B98D8A91CA8B.html>.

## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Global Inventory Lists > vCenter Servers**.
- 3 Right-click `sfo01m01vc01.sfo01.rainpole.local` and select **Deploy OVF Template**.
- 4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Suite Lifecycle Manager OVA file, and click **Next**.
- 5 On the **Select name and location** page, enter the following information, and click **Next**.

Setting	Value
Name	vrs01lcm01
Select a folder or datacenter	sfo01-m01fd-mgmt

- 6 On the **Select a resource** page, select `sfo01-m01-mgmt01` and click **Next**.
- 7 On the **Review details** page, review the virtual appliance details, such as product, version, download size, and size on disk, and then click **Next**.
- 8 On the **Accept license agreements** page, read and accept the End User License Agreement, and click **Next**.

- 9 On the **Select storage** page, select the datastore.
  - a From the **Select virtual disk format** drop-down menu, select **Thin Provision**.
  - b From the **VM storage policy** drop-down menu, select **vSAN Default Storage Policy**.
  - c From the datastore table, select the **sfo01-m01-vsan01** vSAN datastore and click **Next**.
- 10 On the **Select networks** page, select the distributed port group that ends with Mgmt-xRegion01-VXLAN from the **Destination Network** drop-down menu and click **Next**.
- 11 On the **Customize template** page, configure the following values and click **Next**.

Option	Value
Hostname	vrs01lcm01.rainpole.local
Join the VMware Customer Experience Improvement Program	Selected
Common Name	vrs01lcm01.rainpole.local
Country Code	US
Organization Name	Rainpole
Organization Unit	Rainpole
Default Gateway	192.168.11.1
Domain Name	rainpole.local
Domain Name Servers	172.16.11.4,172.16.11.5
Domain Name Path	rainpole.local,sfo01.rainpole.local
Network 1 IP Address	192.168.11.20
Network 1 Netmask	255.255.255.0

- 12 On the **Ready to complete** page, click **Finish** and wait for process to complete.
- 13 Power on vRealize Suite Lifecycle Manager appliance.
  - a From the **Home** menu, select **Hosts and Clusters** .
  - b Expand the sfo01m01vc01.sfo01.rainpole.local tree, select the **vrs01lcm01** virtual machine, and click **Power on**.

## Configure the vRealize Suite Lifecycle Manager Appliance

In the vRealize Suite Lifecycle Manager user interface, you configure the common settings, replace the appliance certificate, generate a certificate for solution path deployments, configure the OVA sources, and download solutions content from the VMware Marketplace.

## Set Common Configuration Settings in vRealize Suite Lifecycle Manager

After the deployment of the vRealize Suite Lifecycle Manager appliance, you perform an initial login and set common configuration settings, such as the appliance passwords, the configuration drift interval, enablement of SSH, and joining the VMware Customer Experience Improvement Program.

### Prerequisites

Complete the deployment of the vRealize Suite Lifecycle Manager appliance on a VMware Validated Design for Software-Defined Data Center foundation environment.

### Procedure

- 1 Open a browser and go to **`https://vrs01lcm01.rainpole.local/vr1cm`**.
- 2 Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password (default)	vmware

- 3 On **Choose a new LCM Appliance Password** page, enter a new password, click **Update Password**, and close the **Welcome** dialog box.

**Note** During initial login to the vRealize Suite Lifecycle Manager, you must change the default appliance password.

The password must be at least 8 characters long and contain at least one lowercase, uppercase, numeric, and special character.

- 4 On the **Navigator** pane, click **Settings**.
- 5 Under **Settings**, click **Common Configuration** and enter the following values.

Option	Value
Root Password	<i>vrs1cm_root_password</i>
Confirm Root Password	<i>vrs1cm_root_password</i>
Admin Password	<i>vrs1cm_admin_password</i>
Confirm Admin Password	<i>vrs1cm_admin_password</i>
SSH User Password	<i>vrs1cm_ssh_password</i>
Confirm SSH User Password	<i>vrs1cm_ssh_password</i>
Configuration Drift Interval	24 (default)
Restart Server	Deselected (default)

Option	Value
SSH Service Enabled	Selected (default)
Join the VMware Customer Experience Improvement Program	Selected (default)

## 6 Click **Save**.

The administrative user is logged out and returned to the vRealize Suite Lifecycle Manager login screen, where the updated password for **admin@localhost** is used.

## Generate Certificate for vRealize Suite Lifecycle Manager Environments

Before deploying a product or solution path with vRealize Suite Lifecycle Manager, you generate a self-signed certificate that is used during an installation wizard or configuration file based deployment.

### Procedure

- 1 Open a browser and go to **https://vrs01lcm01.rainpole.local/vr1cm**.
- 2 Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password (default)	vrlscm_admin_password

- 3 On the **Navigator** pane, click **Settings**.
- 4 Under **Settings**, click the **Generate Certificates** tab, enter the following values, and click **Generate Certificate**. A dialogue appears with the message Certificate generate request triggered successfully.

Option	Value
Enter Organization Name	Rainpole
Enter Organizational Unit	Rainpole
Enter Domain Name	rainpole.local
Enter Locality	San Francisco
Enter State	California
Enter Country Code	US
Enter Passphrase	vrlscm_generated_certificate_passphrase

- 5 On the **Navigator**, click **Requests** and validate that ACTION#GENERATE\_CERTIFICATE displays COMPLETED.
- 6 Under **Settings**, click the **Generate Certificates** tab and click **View Certificate**.

- 7 (Optional) In the **View Certificate**, copy and save the text output of the **Private Key** and **Certificate Chain**.

*Step 7* is only required if you are using the configuration file option to deploy products using vRealize Lifecycle Manager.

## Replace Certificate on the vRealize Suite Lifecycle Manager Appliance

To establish a trusted connection to vRealize Suite Lifecycle Manager, you replace the SSL certificate on the appliance with a custom certificate that is signed by a certificate authority available on the parent Active Directory or on the intermediate Active Directory. See *Certificate Replacement* guide for additional information.

**Table 3-1. Certificate Files for vRealize Suite Lifecycle Manager**

vRealize Suite Lifecycle Manager Appliance	Certificate File Name
vrs01lcm01.rainpole.local	<ul style="list-style-type: none"> <li>■ vrs01lcm01.2.chain.pem</li> <li>■ vrs01lcm01-orig.key</li> </ul>

### Prerequisites

- A certificate signed by a certificate authority, generated using VMware Validated Design Certificate Generation Utility (CertGenVVD).
- A host with an SSH terminal access software such as PuTTY and an SCP software such as WinSCP installed.

### Procedure

- 1 Rename the certificates generated using the VMware Validated Design Certificate Generation Utility for vrs01lcm01.rainpole.local.

Original Certificate File Name	New Certificate File Name
vrs01lcm01.2.chain.pem	server.crt
vrs01lcm01-orig.key	server.key

- 2 Open a Secure Shell connection to the vRealize Suite Lifecycle Manager appliance
  - a Open an SSH connection to vrs01lcm01.rainpole.local.
  - b Log in using the following credentials.

Setting	Value
Username	root
Password	vrslcm_root_password

- 3 Copy the certificate files `server.crt` and `server.key` to the `/opt/vmware/vlcm/cert` folder. You can use an SCP software like WinSCP on Windows.

- 4 After copying the certificates, restart the vRealize Suite Lifecycle Manager services to update the appliance certificate.

- a Restart the system services by executing the following command in the SSH session:

```
systemctl restart vlcM-xserver
```

- b Check the status of the system services by executing the following command in the SSH session:

```
systemctl status vlcM-xserver
```

- 5 After restarting the services, verify that the certificate is updated on the appliance.

- a Open a browser and go to **https://vrs01lcm01.rainpole.local/vrlcm**.
- b Verify that you see the new certificate in the browser.

## Configure NTP on the vRealize Suite Lifecycle Manager Appliance

Configuring NTP on the vRealize Suite Lifecycle Manager appliance.

### Prerequisites

Verify that the vRealize Suite Lifecycle Manager appliance is deployed, with SSH enabled and an SSH user password set.

### Procedure

- 1 Connect to the vRealize Suite Lifecycle Manager appliance.
  - a Open a terminal and SSH to **vrs01lcm01.rainpole.local**.
  - b Log in using following credentials:

Setting	Value
Username	root
Password	<i>vrslcm_root_password</i>

- 2 Configure the NTP source for the vRealize Suite Lifecycle Manager appliance.
  - a Open `/etc/systemd/timesync.conf` in vi editor.
 

```
# vi /etc/systemd/timesyncd.conf
```
  - b Uncomment the **NTP** configuration and add **ntp.sfo01.rainpole.local**.
 

```
NTP=ntp.sfo01.rainpole.local
```
- 3 Enable the `systemd-timesyncd` service and verify the status.
  - a At the prompt, enter `timedatectl set-ntp true` to start the service
  - b Next, enter `timedatectl status` to verify the state of the service
- 4 Logout of the session by typing **logout**.

## Configure the Proxy Settings for vRealize Suite Lifecycle Manager

(Optional) You configure a proxy server for the vRealize Suite Lifecycle Manager appliance if your organization restricts outbound access. vRealize Suite Lifecycle Manager requires outbound access to communicate with My VMware for product OVAs and licenses, Marketplace content, and appliance updates.

### Procedure

- 1 Open a browser and go to `https://vrs01lcm01.rainpole.local/vr1cm`.
- 2 Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password (default)	vrslcm_admin_password

- 3 On the **Navigator** pane, click **Settings**.
- 4 Under **Settings**, click the **Proxy** tab, enter the following values, and click **Save**.

Option	Value
Enable / Disable Proxy	Selected
HTTP Proxy Server	<i>proxy_server_fqdn_or_ip</i> (for example, proxy.rainpole.local)
Proxy Port	<i>proxy_server_port</i> (for example, 3128)
Proxy Username	<i>proxy_server_username</i>
Proxy Password	<i>proxy_server_password</i>

## Update the VMware Validated Design Solution Path Policies on the vRealize Suite Lifecycle Manager Appliance

Before you can deploy the IT Automating IT use case, you must update the solution path policies on the vRealize Suite Lifecycle Manager appliance.

### Prerequisites

The vRealize Suite Lifecycle Manager Appliance must be deployed.

## Procedure

- 1 Connect to the vRealize Suite Lifecycle Manager appliance.
  - a Open a terminal and SSH to **vrs011cm01.rainpole.local**.
  - b Log in using following credentials:

Setting	Value
Username	root
Password	<i>vrs/cm_root_password</i>

## 2 Update the VMware Validate Design solution path policies on the vRealize Suite Lifecycle Manager appliance.

a Open `/var/lib/vlcm/policy/vvd.json` in `vi` editor.

# **vi /var/lib/vlcm/policy/vvd.json**

b Delete the contents of the file and replace with the following policy configurations:

```
{
  "vlds": [
    {
      "version": "4.1",
      "sizes": [
        "small",
        "smallha",
        "medium",
        "large"
      ],
      "solutions": [
        {
          "id": "itait",
          "name": "IT Automating IT",
          "iconSrc": "images/IT_automating_IT.png",
          "products": [
            {
              "id": "vra",
              "iconSrc": "images/vRA_icon.png",
              "name": "vRealize Automation",
              "version": "7.3.0"
            },
            {
              "id": "vrbc",
              "iconSrc": "images/vrb.jpeg",
              "name": "vRealize Business for Cloud",
              "version": "7.3.0"
            },
            {
              "id": "vrops",
              "iconSrc": "images/vrops.png",
              "name": "vRealize Operations Manager",
              "version": "6.6.1"
            },
            {
              "id": "vrli",
              "iconSrc": "images/vrli.png",
              "name": "vRealize Log Insight",
              "version": "4.5.0"
            }
          ]
        },
        {
          "description": "Enable automation and simplification of workload provisioning tasks of production-ready infrastructure and applications across multi-cloud environments.",
          "detailsHref": "http://www.vmware.com/info?id=1427"
        }
      ]
    }
  ]
}
```

```

    {
      "id": "micseg",
      "name": "Micro-Segmentation",
      "iconSrc": "images/microsegmentation.png",
      "products": [
        {
          "id": "vrli",
          "iconSrc": "images/vrli.png",
          "name": "vRealize Log Insight",
          "version": "4.5.0"
        }
      ],
      "description": "Enable distribution of firewall and isolation policies to
create better network security built inside the data center.",
      "detailsHref": "http://www.vmware.com/info?id=1426"
    },
    {
      "id": "intelligentops",
      "name": "Intelligent Operations",
      "iconSrc": "images/microsegmentation.png",
      "products": [
        {
          "id": "vrops",
          "iconSrc": "images/vrops.png",
          "name": "vRealize Operations Manager",
          "version": "6.6.1"
        },
        {
          "id": "vrli",
          "iconSrc": "images/vrli.png",
          "name": "vRealize Log Insight",
          "version": "4.5.0"
        }
      ],
      "description": "Enabling proactive identification and remediation of
performance, capacity, and configuration issues of the infrastructure.",
      "detailsHref": "http://www.vmware.com/info?id=1428"
    }
  ]
},
{
  "version": "4.2",
  "sizes": [
    "small",
    "smallha",
    "medium",
    "large"
  ],
  "solutions": [
    {
      "id": "itait",
      "name": "IT Automating IT",
      "iconSrc": "images/IT_automating_IT.png",
      "products": [
        {

```

```

        "id": "vra",
        "iconSrc": "images/vRA_icon.png",
        "name": "vRealize Automation",
        "version": "7.3.0"
    },
    {
        "id": "vrbc",
        "iconSrc": "images/vrb.jpeg",
        "name": "vRealize Business for Cloud",
        "version": "7.3.1"
    },
    {
        "id": "vrops",
        "iconSrc": "images/vrops.png",
        "name": "vRealize Operations Manager",
        "version": "6.6.1"
    },
    {
        "id": "vrli",
        "iconSrc": "images/vrli.png",
        "name": "vRealize Log Insight",
        "version": "4.5.1"
    }
],
    "description": "Enable automation and simplification of workload provisioning tasks of production-ready infrastructure and applications across multi-cloud environments.",
    "detailsHref": "http://www.vmware.com/info?id=1427"
},
{
    "id": "micseg",
    "name": "Micro-Segmentation",
    "iconSrc": "images/microsegmentation.png",
    "products": [
        {
            "id": "vrli",
            "iconSrc": "images/vrli.png",
            "name": "vRealize Log Insight",
            "version": "4.5.1"
        }
    ]
},
    "description": "Enable distribution of firewall and isolation policies to create better network security built inside the data center.",
    "detailsHref": "http://www.vmware.com/info?id=1426"
},
{
    "id": "intelligentops",
    "name": "Intelligent Operations",
    "iconSrc": "images/microsegmentation.png",
    "products": [
        {
            "id": "vrops",
            "iconSrc": "images/vrops.png",
            "name": "vRealize Operations Manager",
            "version": "6.6.1"
        }
    ]
}

```

```

    },
    {
      "id": "vrli",
      "iconSrc": "images/vrli.png",
      "name": "vRealize Log Insight",
      "version": "4.5.1"
    }
  ],
  "description": "Enabling proactive identification and remediation of
performance, capacity, and configuration issues of the infrastructure.",
  "detailsHref": "http://www.vmware.com/info?id=1428"
}
]
}
]
}

```

- 3 Save the contents of the updated policy configuration and exit vi editor.

```
:wq!
```

- 4 Logout of the SSH session by typing **logout**.

```
# logout
```

## Register vRealize Suite Lifecycle Manager with My VMware

You can integrate vRealize Suite Lifecycle Manager directly with a My VMware account to access vRealize Suite licenses within an entitlement account and manage the download of product OVAs for install, patch, and upgrade. The My VMware account registration is also used to download content from the VMware Marketplace.

### Prerequisites

Before registering vRealize Suite Lifecycle Manager with My VMware, ensure that you have created a My VMware account with permissions to view licenses and download products from your entitlement account.

### Procedure

- 1 Open a browser and go to **<https://vrs01lcm01.rainpole.local/vr1cm>**.
- 2 Log in using the following credentials.

Setting	Value
Username	admin@localhost
Password	vrs1cm_admin_username

- 3 On the **Navigator** pane, click **Settings**

- 4 Under **Settings**, click the **My VMware** tab, enter your My VMware credentials, and click **Submit**.  
vRealize Suite Lifecycle Manager is successfully registered with My VMware if the Service registered with My VMware credentials provided. message appears.
- 5 When the **Download OVA** dialogue appears prompting to start a content download, select **No** to close the action.

## OVA Configuration in vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager provides two methods to retrieve and store product OVAs for install, patch, and upgrade of the vRealize Suite components.

### Download Product OVAs to vRealize Suite Lifecycle Manager with My VMware

You can integrate vRealize Suite Lifecycle Manager directly with a My VMware account to access vRealize Suite entitlements. You can download all or select product OVAs for install, patch, and upgrade.

---

**Note** Using the My VMware integration to download vRealize Suite product OVAs to the vRealize Suite Lifecycle Manager appliance is the recommended path to simplify, automate, and organize the repository. If your organization must restrict outbound traffic from the management components of the Software-Defined Data Center, as an alternative you can upload vRealize Suite product OVAs to the vRealize Suite Lifecycle Manager appliance directly.

---

#### Prerequisites

- vRealize Suite Lifecycle Manager has been registered with My VMware.
- The registered My VMware account has product entitlement to the vRealize Suite.
- If your organization requires the use of an HTTP Proxy, ensure that it has been enabled.

#### Procedure

- 1 Log in to the vRealize Suite Lifecycle Manager user interface.
  - a Open a browser and go to **https://vrs01lcm01.rainpole.local/vr1cm**.
  - b Log in using following credentials:

Setting	Value
Username	admin@localhost
Password	vrs1cm_admin_password

- 2 Click **Settings** and click **OVA Configuration**.
- 3 In the **Select a source location or download from My VMware** section, select **My VMware**.
- 4 At the bottom of the **OVA Configuration** page, enable **Auto Refresh**.

- For each product and version in the IT Automating IT solution path, click the **Download** icon from the **Actions** column.

Solution Path	Product Name	Product Version
IT Automating IT	vRealize Automation vRealize Business for Cloud vRealize Operations vRealize Log Insight	Refer to the Release Notes

- When downloading, the **Download Status** column changes to an INPROGRESS status. Monitor the **Download Status** column as each product transitions from INPROGRESS to COMPLETED. Due to the size of each product download for install, patch, and upgrade, the process can take some time to complete.

## Upload Product OVAs to vRealize Suite Lifecycle Manager

Before you can trigger a solution path deployment for IT Automating IT by using vRealize Suite Lifecycle Manager, you download product OVAs and create mappings between each product and the associated OVA.

**Note** Using the My VMware integration to download vRealize Suite product OVAs to the vRealize Suite Lifecycle Manager appliance path simplifies, automates, and organizes the repository. If your organization restricts outbound traffic from the management components of the Software-Defined Data Center, as an alternative you can upload the vRealize Suite product OVAs to the vRealize Suite Lifecycle Manager appliance directly.

### Prerequisites

Verify that the vRealize Suite Lifecycle Manager appliance is deployed, SSH is enabled and an SSH user password is set.

### Procedure

- Download the product OVAs for the IT Automating IT solution path.

Solution Path	Product Name	Product Version	Product OVA
IT Automating IT	vRealize Automation vRealize Business for Cloud vRealize Operations Manager vRealize Log Insight	Refer to the Release Notes	vRealize Automation .ova file vRealize Business for Cloud .ova file vRealize Operations Manager .ova file vRealize Log Insight .ova file

- 2 Create a directory on the vRealize Suite Lifecycle Manager appliance for product OVAs.
  - a Open an SSH connection to **vrs011cm01.rainpole.local**.

- b Log in using the following credentials:

Setting	Value
Username	root
Password	<i>vrslcm_root_password</i>

- c Create the `/data/binaries/OVA` directory, and exit.

- 3 Upload the product OVAs to the vRealize Suite Lifecycle Manager appliance.

- a Open an SCP client and connect to **vrs011cm01.rainpole.local**.
  - b Log in using following credentials:

Setting	Value
Username	root
Password	<i>vrslcm_root_password</i>

- c Upload the product `.ova` files to the `/data/binaries/OVA` directory and exit.

- 4 Log in to the vRealize Suite Lifecycle Manager Web interface.

- a Open Web a browser and go to **https://vrs011cm01.rainpole.local/vr1cm**.
  - b Log in using the following credentials:

Setting	Value
User name	admin@localhost
Password	<i>vrslcm_admin_password</i>

- 5 Click **Settings** and click **OVA Configuration**.

- 6 Enter the following parameter to identify the source type and click **Get**.

Option	Value
Select OVA source location or Download OVA from My VMware	Source Location
Select Location Type	Local
Base Location	<code>/data/binaries/OVA</code>

- 7 Create a mapping to associate each OVA file with the solution path in Step 1 and for each product click **Save**.

For example, if a solution path includes vRealize Log Insight simply add product information.

Option	Value
Product Name	vRealize Log Insight
Product Version	Select Version - Refer to Release Notes

Option	Value
Product Binary Type	Install
Product Binary	vRealize Log Insight .ova file

- 8 Repeat the process for each product OVA required by the IT Automating IT solution path.

## Download Marketplace Content in vRealize Suite Lifecycle Manager

Use vRealize Suite Lifecycle Manager to add and manage content from Marketplace, such as the vRealize Operations Manager management packs, and vRealize Log Insight content packs for a specific solution path.

## Add a Data Center to vRealize Suite Lifecycle Manager

Before you can create an environment for a solution path deployment, you must add a data center in using vRealize Suite Lifecycle Manager and associate the Management vCenter Server instance.

### Prerequisites

Ensure the operations service account `svc-vrslcm-vsphere` for the integration between vRealize Suite Lifecycle Manager and vSphere is:

- added to the Management vCenter Server.
- assigned the custom vRealize Suite Lifecycle Manager User role.

### Procedure

- 1 Log in to the vRealize Suite Lifecycle Manager Web interface.
  - a Open a browser and go to `https://vrs01lcm01.rainpole.local/vr1cm`.
  - b Log in using following credentials:

Setting	Value
Username	admin@localhost
Password	<i>vrslcm_admin_password</i>

- 2 In the **Navigator**, click **Manage Data Centers** and click **Add Data Center**.
- 3 In the **Add Data Center** dialog box, enter the following information and click **Add**.

Setting	Value
Name	sfo01-m01dc
Location	San Francisco, California, US

**4** Add the vCenter Server.

- a Click **Manage vCenter Servers**.
- b In the *Select Data Center*, click the drop-down menu and select sfo01-m01dc.
- c Click **Add vCenter Server**.
- d Enter the following vCenter Server information and click **Submit**.

Setting	Value
Host Name	sfo01m01vc01.sfo01.rainpole.local
User Name	svc-vrslcm-vsphere@rainpole.local
Password	<i>svc-vrslcm-vsphere_password</i>
vCenter Server Type	Management

- 5** In the **Navigator**, click **Requests** and validate that VC\_DATA\_COLLECTION for the vCenter Server shows COMPLETED.

# Pre-Deployment Tasks for the IT Automating IT Use Case

# 4

Before deploying the IT Automating IT use case, perform the following pre-deployment tasks.

## 1 [Generate Certificates for the IT Automating IT Solution Path](#)

Use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates signed by the Microsoft certificate authority (MSCA) for all life cycle products with a single operation.

## 2 [Pre-deployment Tasks for vRealize Automation](#)

Before using vRealize Suite Lifecycle Manager to deploy use cases or solution paths that include vRealize Automation, you must perform pre-deployment tasks.

## 3 [Pre-Deployment Tasks for vRealize Operations Manager](#)

Before using vRealize Suite Lifecycle Manager to deploy use cases or solution paths that include vRealize Operations Manager, you must perform pre-deployment tasks.

## 4 [Prerequisites for Deploying vRealize Log Insight](#)

## Generate Certificates for the IT Automating IT Solution Path

Use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates signed by the Microsoft certificate authority (MSCA) for all life cycle products with a single operation.

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

### Prerequisites

- Provide a Windows Server 2012 host that is part of the sfo01.rainpole.local domain.
- Install a Certificate Authority server on the rainpole.local domain.

### Procedure

- 1 Log in to a Windows host that has access to your data center.
- 2 Download the `CertGenVVD-version.zip` file of the Certificate Generation Utility from VMware Knowledge Base article [2146215](#) on the Windows host where you connect to the data center and extract the ZIP file to the C: drive.

- 3 In the C:\CertGenVVD-*version* folder, open the default.txt file in a text editor.
- 4 Verify that following properties are configured.

```

ORG=Rainpole Inc.
OU=Rainpole.local
LOC=SFO
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
    
```

- 5 Verify that the C:\CertGenVVD-*version*\ConfigFiles folder contains only following files.

**Table 4-1. Certificate Configuration Files for the IT Automating IT Solution Path**

Host Name or Service	Configuration Files	
Cloud Management Platform Layer		
vRealize Automation	<ul style="list-style-type: none"> <li>■ vra01svr01.rainpole.local</li> <li>■ vra01svr01a.rainpole.local</li> <li>■ vra01svr01b.rainpole.local</li> <li>■ vra01iws01.rainpole.local</li> <li>■ vra01iws01a.rainpole.local</li> <li>■ vra01iws01b.rainpole.local</li> <li>■ vra01ims01.rainpole.local</li> <li>■ vra01ims01a.rainpole.local</li> <li>■ vra01ims01b.rainpole.local</li> <li>■ vra01dem01a.rainpole.local</li> <li>■ vra01dem01b.rainpole.local</li> </ul>	vra.txt
vRealize Business Server	vrb01svr01.rainpole.local	vrb.txt
Operations Management Layer		
vRealize Operations Manager	<ul style="list-style-type: none"> <li>■ vroops01svr01.rainpole.local</li> <li>■ vroops01svr01a.rainpole.local</li> <li>■ vroops01svr01b.rainpole.local</li> <li>■ vroops01svr01c.rainpole.local</li> </ul>	vroops.txt
vRealize Log Insight	<ul style="list-style-type: none"> <li>■ sfo01vrli01.sfo01.rainpole.local</li> <li>■ sfo01vrli01a.sfo01.rainpole.local</li> <li>■ sfo01vrli01b.sfo01.rainpole.local</li> <li>■ sfo01vrli01c.sfo01.rainpole.local</li> </ul>	vrli.sfo01.txt

- 6 Verify that each configuration file includes FQDNs and host names in the dedicated sections.  
For example, the configuration files for the vRealize Operations Manager instances must contain the following properties:

**vrops.txt**

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01vrops01svr01.rainpole.local
keysize=default
[SAN]
sfo01vrops01svr01
sfo01vrops01svr01a
sfo01vrops01svr01b
sfo01vrops01svr01c
sfo01vrops01svr01.rainpole.local
sfo01vrops01svr01a.rainpole.local
sfo01vrops01svr01b.rainpole.local
sfo01vrops01svr01c.rainpole.local
```

- 7 Open a Windows PowerShell prompt and navigate to the CertGenVVD folder.

```
cd C:\CertGenVVD-version
```

- 8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

- 9 Validate if you can run the utility using the configuration on the host and verify if VMware is included in the printed CA template policy.

```
.\CertgenVVD-version.ps1 -validate
```

- 10 Generate MSCA-signed certificates.

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

- 11 In the C:\CertGenVVD-*version* folder, verify that the utility created the SignedByMSCACerts subfolder.

## Pre-deployment Tasks for vRealize Automation

Before using vRealize Suite Lifecycle Manager to deploy use cases or solution paths that include vRealize Automation, you must perform pre-deployment tasks.

### DNS Entries and IP Address Mappings

Verify that your DNS and IP environment fulfills the requirements for this SDDC deployment.

## IP Addresses and Host Names

**Table 4-2. IP Addresses and FQDNs for the vRealize Automation Instance in Region A**

Role	IP Address	FQDN
vRealize Automation Server Appliances	192.168.11.51	vra01svr01a.rainpole.local
	192.168.11.52	vra01svr01b.rainpole.local
vRealize Automation Server VIP	192.168.11.53	vra01svr01.rainpole.local
vRealize Automation IWS	192.168.11.54	vra01iws01a.rainpole.local
	192.168.11.55	vra01iws01b.rainpole.local
vRealize Automation IWS VIP	192.168.11.56	vra01iws01.rainpole.local
vRealize Automation IMS	192.168.11.57	vra01ims01a.rainpole.local
	192.168.11.58	vra01ims01b.rainpole.local
vRealize Automation IMS VIP	192.168.11.59	vra01ims01.rainpole.local
vRealize DEM Workers	192.168.11.60	vra01dem01a.rainpole.local
	192.168.11.61	vra01dem01b.rainpole.local
MS SQL Server for vRealize Automation	192.168.11.62	vra01mssql01.rainpole.local
vRealize Business for Cloud Server Appliance	192.168.11.66	vrbc01svr01.rainpole.local

**Table 4-3. IP Addresses and Host Name for the Supporting Infrastructure**

Role	IP Address	FQDN
vRealize Automation Proxy Agent	192.168.31.52	sfo01ias01a.sfo01.rainpole.local
	192.168.31.53	sfo01ias01b.sfo01.rainpole.local
vRealize Business for Cloud Data Collector	192.168.31.54	sfo01vrbc01.sfo01.rainpole.local
Default gateway	192.168.31.1	
DNS server	172.16.11.5	
Subnet mask	255.255.255.0	
NTP	172.16.11.251	ntp.sfo01.rainpole.local
	172.16.11.252	
	172.17.11.251	ntp.lax01.rainpole.local
	172.17.11.252	

## vRealize Automation Deployment Prerequisites

Before you install and use vRealize Automation, your environment must meet the following prerequisites.

Prerequisite	Value
Storage	<ul style="list-style-type: none"> <li>■ Virtual disk provisioning.</li> <li>■ Required storage per node.</li> </ul>
Operating System	Windows 2012 R2 Standard
Database	Microsoft SQL Server 2012 Standard Edition
Installation Package	<p>Download the vRealize Automation virtual appliance .ova file.</p> <p>Download the vRealize Business for Cloud virtual appliance .ova file.</p>
License	<p>Verify that you have obtained a license that covers the use of vRealize Automation.</p> <p>Verify that you have obtained a license that covers the use of vRealize Business for vRealize Automation.</p>
Active Directory	<p>Verify that you have a parent Active Directory instance with the SDDC user roles configured for the rainpole.local domain.</p> <p>Verify the existence of the ug-vra-admins-rainpole group in the rainpole.local domain.</p> <p>Verify the existence of the ug-vra-archs-rainpole group in the rainpole.local domain.</p> <p>Verify the existence of the svc-domain-join user in the rainpole.local domain.</p> <p>Verify the existence of the vra-admin-rainpole user in the rainpole.local domain.</p> <p>Verify the existence of the svc-vra-vrops user in the rainpole.local domain.</p> <p>Verify the existence of the svc-vrops-vra user in the rainpole.local domain.</p> <p>Verify the existence of the svc-vra user in the rainpole.local domain.</p> <p>Verify the existence of the ug-vROadmins group in the rainpole.local domain.</p> <p>Verify the existence of the svc-vro user in the rainpole.local domain.</p> <p>The Microsoft SQL Server virtual machine should join the rainpole.local domain.</p>
Certification Authority	Configure the root Active Directory domain controller as a certificate authority for the environment.
Java	Install Java SE Development Kit (JDK), which is required to run the vRealize Orchestrator Client.

## Create Virtual Machine Folders for vRealize Automation and vRealize Business

Use the vSphere Web Client to create virtual machine folders for the organization and ease of management of vRealize Automation and vRealize Business virtual machines.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

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

- 3 Navigate to the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server and **sfo01-m01dc** data center.
- 4 Create two new VM and Template folders named **sfo01-m01fd-vra** and **sfo01-m01fd-vraias**.

## SQL Server Configuration for the Cloud Management Platform

The Cloud Management Platform uses a Microsoft SQL Server database to store data for vRealize Automation.

### Microsoft SQL Server Recommendations

vRealize Automation and other VMware components use Microsoft SQL Server as a database to store information. The specific configuration of SQL Server for use in your environment is not addressed in this implementation guide. High-level guidance is provided to ensure more reliable operation of your VMware components.

- Microsoft SQL Server must be configured with separate Operating System Level volumes (drive letters) for each of the following items. The separation of these items into separate logical volumes (drive letters) helps prevent database corruption if a single volume reaches capacity.
  - Operating System
  - Database Application
  - SQL User Database Data Files
  - SQL User Database Log Files
  - SQL TempDB
  - SQL Backup Files
- To provide optimal performance for VMware vRealize databases, configure the SQL Server virtual machine (vra01mssql01.rainpole.local) with 8 vCPU and 16 GB vRAM.

For further guidance on the deployment and operation of a production installation of Microsoft SQL Server, see the Microsoft SQL Server documentation, or consult with a qualified Microsoft SQL Server database administrator.

### Assign the SQL Server System Role to vRealize Automation

Assign the SQL Server system role **sysadmin** to the vRealize Automation service account.

vRealize Automation uses the SQL Server system role privilege to create and run scripts on the SQL Server database. By default, only users who are members of the **sysadmin** system role, or the **db\_owner** and **db\_ddladmin** database roles, can create objects in the database.

## Procedure

- 1 Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client.
  - a Open an RDP connection to the `vra01mssql01.rainpole.local` virtual machine.
  - b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	<code>windows_administrator_password</code>

- 2 From the **Start** menu, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.

**Note** If SQL Server Management Studio does not appear in your **All Programs** menu, you may not have successfully installed SQL Server Management Studio. Verify that you have successfully installed SQL Server Management Studio, and then continue with this procedure.

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

**Note** During the SQL Server installation, the **Database Engine** configuration wizard prompts you to provide the user name and password for the SQL Server administrator. If this user was not added during the SQL Server installation, select **SQL Authentication** from the **Authentication** drop-down menu, and enter the user name `sa` in the **User name** text box, and the password `sa_password` in the **Password** text box.

- 4 In the **Object Explorer** pane, expand the **VRA01MSSQL01** server instance .
- 5 Right-click the **Security** folder, click **New**, and click **Login**.
- 6 In the **Login Properties** dialog box, click the **General** page and enter `rainpole\svc-vra` in the **Login name** text box.
- 7 Click the **Server Roles** page, select the **sysadmin** check box, and click **OK**.

## Configure Network Access for Distributed Transaction Coordinator

You configure network access and security between vRealize Automation and your Microsoft SQL Server database using Microsoft Distributed Transaction Coordinator (MSDTC). MSDTC coordinates transactions that update two or more transaction-protected resources, such as databases, message queues, file systems. These transaction-protected resources may be on a single computer, or distributed across many networked computers.

**Procedure**

- 1 Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client.
  - a Open an RDP connection to the `vra01mssql01.rainpole.local` virtual machine.
  - b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	<code>windows_administrator_password</code>

- 2 From the **Start** menu, click **Run**, type `comexp.msc` in the **Open** text box, and click **OK**.  
The **Component Services** manager displays. Component Services lets you manage Component Object Model (COM+) applications.
- 3 Using the navigation tree in the left-side pane, expand **Component Services > Computers > My Computer > Distributed Transaction List > Local DTC**.
- 4 Right-click **Local DTC** and click **Properties**.  
The **Local DTC Properties** dialog box displays.
- 5 Click the **Security** tab in the **Local DTC Properties** dialog box.
- 6 On the **Security** tab, configure the following values, and click **OK**.

Setting	Value
Network DTC Access	Selected
Allow Remote Clients	Selected
Allow Remote Administration	Deselected
Allow Inbound	Selected
Allow Outbound	Selected
Mutual Authentication Required	Selected
Enable XA Transactions	Deselected
Enable SNA LU 6.2 Transactions	Selected
Account	Leave the default setting (NT AUTHORITY\NetworkService)
Password	Leave blank

- 7 Click **Yes** to restart the MSDTC Service, click **OK** to confirm that the service has successfully restarted, and close the **Component Services** manager.

## Allow MS SQL Server and MSDTC Access Through Windows Firewall for vRealize Automation

You can configure Windows Firewall to allow or block specific traffic. For vRealize Automation to function correctly, ensure that network access to Microsoft Distributed Transaction Coordinator (MSDTC) and SQL Server is configured to allow access.

## Procedure

- 1 Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client.
  - a Open an RDP connection to the `vra01mssql01.rainpole.local` virtual machine.
  - b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	<code>windows_administrator_password</code>

- 2 From the **Start** menu, click **Run**, type `WF.msc` in the **Open** text box, and click **OK**.

The Windows Firewall with Advanced Security dialog box appears. You use Windows Firewall with Advanced Security to configure firewall properties for each network profile.

- 3 Allow Access for Microsoft SQL Server on TCP Port 1433.
  - a In the navigation pane, under **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.  
The **New Inbound Rule Wizard** appears.
  - b On the Rule Type page of the **New Inbound Rule Wizard**, select the **Port** radio button, and click **Next**.
  - c On the Protocol and Ports page, select **TCP** and enter the port number **1433** in the **Specific local ports** text box, and click **Next**.
  - d On the Action page, select **Allow the connection**, and click **Next**.
  - e On the Profile page, select the **Domain, Private**, and **Public** profiles, and click **Next**.
  - f On the Name page, enter a *Name* and *Description* for this rule, and click **Finish**.
- 4 Allow access for Microsoft Distributed Transaction Coordinator.
  - a In the navigation pane, under **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.
  - b On the Rule Type page click **Predefined**, click **Distributed Transaction Coordinator**, and click **Next**.
  - c On the Predefined Rules page, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, **Distributed Transaction Coordinator (TCP-In)**, and click **Next**.
  - d On the Action page, select **Allow the connection**, and click **Finish**.
- 5 Exit the **Windows Firewall with Advanced Security** wizard.

## Configure Service Account Privileges

To provision virtual machines and logical networks, configure privileges for vRealize Automation for the service account `svc-vra@rainpole.local` on both the vCenter Server and the NSX instance in the cluster. If you add more vCenter Server instances in the future, perform this procedure on those instances as well.

### Configure Service Account Privileges on the vCenter Server

Configure Administrator privileges for the `svc-vra` and `svc-vro` users on the vCenter Server.

#### Procedure

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

a Open a Web browser and go to

`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 In the **Navigator** pane, select **Global Inventory Lists > vCenter Servers**.

3 Right-click the `sfo01m01vc01.sfo01.rainpole.local` instance and select **Add Permission**.

4 In the **Add Permission** dialog box, click the **Add** button.

The **Select Users/Groups** dialog box appears.

5 Select **RAINPOLE** from the **Domain** drop-down menu, and enter `svc` in the **Show Users First** text box to filter user and group names.

6 Select `svc-vra` and `svc-vro` from the **User/Group** list, click the **Add** button, and click **OK**.

7 In the **Add Permission** dialog box, select **Administrator** from the **Assigned Role** drop-down menu, and click **OK**.

The `svc-vra` and `svc-vro` users now have **Administrator** privilege on the vCenter Server.

### Configure the Service Account Privilege on the NSX Instance

Configure Enterprise Administrator privileges for the `svc-vra@rainpole.local` service account.

**Procedure**

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Networking & Security**.
- 3 In the **Navigator** pane, select **Users and Domains**.
- 4 Select the NSX Manager from the drop-down menu.
- 5 Under the **Users** tab, click the **Add** icon.  
The **Assign Role** wizard appears.
- 6 On the **Identify User** page, select the **Specify a vCenter User** radio button, enter **svc-vra@rainpole.local** in the **User** text box, and click **Next**.
- 7 On the **Select Roles** page, select the **Enterprise Administrator** radio button, and click **Finish**.

## Load Balancing the Cloud Management Platform

You configure load balancing for all services and components related to vRealize Automation and vRealize Orchestrator by using an NSX Edge load balancer.

You must configure the load balancer before you deploy the vRealize Automation appliance. This is because you need the virtual IP (VIP) addresses to deploy the vRealize Automation appliance.

### Add Virtual IP Addresses to the NSX Load Balancer

As the first step of configuring load balancing, you add virtual IP Addresses to the edge interfaces.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.

- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to edit its network settings.
- 5 Click the **Manage** tab, click **Settings**, and select **Interfaces**.
- 6 Select the **OneArmLB** interface and click the **Edit** icon.
- 7 In the **Edit NSX Edge Interface** dialog box, add the VIP addresses of the vRealize Automation nodes in the **Secondary IP Addresses** text box.

Setting	Value
Secondary IP Address	192.168.11.53,192.168.11.56,192.168.11.59

The screenshot shows the 'Edit NSX Edge Interface' dialog box with the following configuration:

- VNIC#:** 0
- Name:** OneArmLB
- Type:** Internal
- Connected To:** Mgmt-xRegion01-VXLAN
- Connectivity Status:** Connected
- Configure Subnets:**

Primary IP Address	Secondary IP Address	Subnet Prefix Length
192.168.11.2	168.11.53,192.168.11.56,192.168.11.59,192.168.11.65	24
- MAC Addresses:** (Two empty text boxes)
- MTU:** 9000
- Options:**
  - Enable Proxy ARP
  - Send ICMP Redirect
  - Reverse Path Filter: Enabled
- Fence Parameters:** (Empty text box)

Example: ethernet0.filter1.param1=1

- 8 Click **OK** to save the configuration.

## Create Application Profiles

To define the behavior of a particular type of network traffic, you create an application profile. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

You repeat this procedure twice to create two application profiles.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.
- 6 Click the **Add** icon and in the **New Profile** dialog box, enter the following values.

Setting	Value
Name	vra-https-persist
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800

- 7 Click **OK** to save the configuration.
- 8 Repeat the same steps to create the following application profile.

Setting	Value
Name	vra-https
Type	HTTPS

Setting	Value
Enable SSL Passthrough	Selected
Persistence	None

## Create Service Monitoring

The service monitor defines health check parameters for the load balancer. You create a service monitor for each component.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Service Monitoring**.
- 6 Click the **Add** icon and in the **New Service Monitor** dialog box, configure the values for the service monitor you are adding, and click **OK**.

Setting	vra-svr-443-monitor	vra-iws-443-monitor	vra-ims-443-monitor	vra-vro-8283-monitor
Name	vra-svr-443-monitor	vra-iws-443-monitor	vra-ims-443-monitor	vra-vro-8283-monitor
Interval	3	3	3	3
Timeout	10	10	10	10
Max Retries	3	3	3	3
Type	HTTPS	HTTPS	HTTPS	HTTPS
Expected	204			
Method	GET	GET	GET	GET
URL	/vcac/services/api/health	/wapi/api/status/web	/VMPSProvision	/vco-controlcenter/docs
Receive		REGISTERED	ProvisionService	

**New Service Monitor**

Name: \* vra-svr-443-monitor

Interval: 3 (seconds)

Timeout: 10 (seconds)

Max Retries: 3

Type: HTTPS

Expected: 204

Method: GET

URL: /cac/services/api/health

Send:

Receive:

Extension:

OK Cancel

- Repeat [Step 6](#) to create a service monitor for each component.

Upon completion, verify that you have successfully entered the monitor names and their respective configuration values.

## Create Server Pools

A server pool consists of back-end server members. After you create a server pool, you associate a service monitor with the pool to manage and share the back-end servers flexibly and efficiently.

The following considerations explain the design of the server pools configuration.

- The configuration uses NONE as a health monitor for all server pools. Until vRealize Automation is fully installed and started, the health monitor marks pool members as offline. Health monitors indicate the status of pool members correctly, only after vRealize Automaton is fully installed and initialized.

- The configuration disables the second pool member of three vRealize Automation VIPs (vra-svr-443, vra-iaas-web-443, vra-iaas-mgr-443). During the installation or power cycle of vRealize Automation, the service inside the second node might not be installed or initialized yet. In this period, if the load balancer passes a request to the second node, the request fails. If the second pool member is not disabled, you can experience random failures during a vRealize Automation installation, and service initialization or registration failure during a vRealize Automation power cycle.

Perform the procedure multiple times to configure five different server pools.

**Table 4-4. Server Pools for the Cloud Management Platform**

Pool Name	Algorithm	Monitors	Enable Member	Member Name	IP Address	Port	Monitor Port
vra-svr-443	ROUND-ROBIN	NONE	Yes	vra01svr01a	192.168.11.51	443	
			No	vra01svr01b	192.168.11.52	443	
vra-iws-443	ROUND-ROBIN	NONE	Yes	vra01iws01a	192.168.11.54	443	
			No	vra01iws01b	192.168.11.55	443	
vra-ims-443	ROUND-ROBIN	NONE	Yes	vra01ims01a	192.168.11.57	443	
			No	vra01ims01b	192.168.11.58	443	
vra-svr-8444	ROUND-ROBIN	NONE	Yes	vra01svr01a	192.168.11.51	8444	443
			Yes	vra01svr01b	192.168.11.52	8444	443
vra-vro-8283	ROUND-ROBIN	NONE	Yes	vra01svr01a	192.168.11.51	8283	
			No	vra01svr01b	192.168.11.52	8283	

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

6 Click the **Add** icon, and in the **New Pool** dialog box, enter the following values.

Setting	Value
Name	vra-svr-443
Algorithm	ROUND-ROBIN
Monitors	NONE

7 In the **New Members** dialog box, click the **Add** icon to add the first pool member.

8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Value
Name	vra01svr01a
IP Address/VC Container	192.168.11.51
State	Enable
Port	443
Monitor Port	
Weight	1

9 Repeat the previous two steps to create the second member of the pool.

10 Repeat the procedure to create the remaining server pools.

## Create Virtual Servers

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all the configured server pools.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.

- 6 Click the **Add** icon, and in the **New Virtual Server** dialog box configure the values for the virtual server you are adding, and click **OK**.

Setting	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283
Enable Virtual server	Selected	Selected	Selected	Selected	Selected
Application Profile	vra-https-persist	vra-https-persist	vra-https	vra-https-persist	vra-https-persist
Name	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283
Description	vRealize Automation Appliance UI	vRealize Automation IaaS Web UI	vRealize Automation IaaS Manager	vRealize Automation Remote Console Proxy	vRealize Orchestrator Control Center
IP Address	192.168.11.53	192.168.11.56	192.168.11.59	192.168.11.53	192.168.11.53
Protocol	HTTPS	HTTPS	HTTPS	HTTPS	HTTPS
Port	443	443	443	8444	8283
Default Pool	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283

- 7 Repeat [Step 6](#) to create a virtual server for each component. Upon completion, verify that you have successfully entered the virtual server names and their respective configuration values.

## Deploy Windows Virtual Machines for vRealize Automation

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration.

### Create vSphere Image Customization Specifications

Create vSphere image customization specifications to use with your deployments. The customization specification you create customizes the guest operating systems of the virtual machines.

Customization specifications are XML files that contain guest operating system settings for virtual machines. You create customization specifications with the **Guest Customization** wizard, and manage specifications using the Customization Specification Manager. vCenter Server saves the customized configuration parameters in the vCenter Server database. When you clone a virtual machine or deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties such as the computer name, network settings, and license settings. When you apply an image customization specification to the guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

### Create a Customization Specification File for IaaS Servers

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Servers deployment.

You can supply a custom sysprep answer file as an alternative to specifying many of the settings in the **Guest Customization** wizard. The vSphere Image Customization template sysprep answer file stores a number of customization settings such as computer name, licensing information, and workgroup or domain settings.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From **Home** page, under **Policies and Profiles**, click **Customization Specification Manager**.
- 3 Select **sfo01m01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu.
- 4 Click the **Create a new specification** icon.  
The **Guest Customization** wizard opens.
- 5 On the **Specify Properties** page, configure the following values, and click **Next**.

Setting	Value
Target VM Operating System	Windows
Use custom SysPrep answer file	Deselected
Customization Spec Name	vra7-template

- 6 On the **Set Registration Information** page, configure the following values, and click **Next**.

Setting	Value
Name	Rainpole
Organization	Rainpole IT

- 7 On the **Set Computer Name** page, select the **Enter a name in the Clone/Deploy wizard** radio button, and click **Next**.

- 8 On the **Enter Windows License** page, configure the following values, and click **Next**.

If you are using Microsoft License Server, or have multiple single license keys, leave the **Product Key** text box blank.

Setting	Value
Product Key	<i>volume_license_key</i>
Include Server License Information	Selected
Server License Mode	Per seat

- 9 On the **Set Administrator Password** page, configure the following values, and click **Next**.

Setting	Value
Password	<i>local_administrator_pwd</i>
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

- 10 On the **Time Zone** page, select **(GMT) Coordinated Universal Time** from the **Time Zone** drop-down menu, and click **Next**.

- 11 On the **Run Once** page, type `net localgroup administrators rainpole\svc-vra /add` in the text box and click **Add**. This command will add service account rainpole\svc-vra into virtual machine's local administrators group. Click **Next**.

- 12 On the **Configure Network** page, select the **Manually select custom settings** radio button, select **NIC1** from the list of network interfaces in the virtual machine, and click **Edit**.

The **Edit Network** dialog box opens.

- 13 In the **Edit Network** dialog box, on the **IPv4** page, configure the following values and click **DNS**.

Setting	Value
Prompt the user for an address when the specification is used	Selected
Subnet Mask	255.255.255.0
Default Gateway	192.168.11.1

- 14 On the **DNS** page, provide DNS servers and search suffixes.

- a Specify the following DNS server settings.

Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.16.11.4
Alternate DNS Server	172.16.11.5

- b Enter `rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

- c Enter `sfo01.rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- d Click **OK** to save settings and close the Edit Network dialog box, and click **Next**.

**15** On the **Set Workgroup or Domain** page, enter credentials that have privileges to join the domain, and click **Next**.

Setting	Value
Windows Server Domain	rainpole.local
Username	svc-domain-join@rainpole.local
Password	<i>svc-domain-join_password</i>

**16** On the **Set Operating System Options** page, select the **Generate New Security ID (SID)** check box, and click **Next**.

**17** On the **Ready to complete** page, review the configuration settings that you entered, and click **Finish**.

The customization specification you created is listed in the Customization Specification Manager and can be used to customize virtual machine guest operating systems.

### Create a Customization Specification File for IaaS Proxy Agent Server

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Proxy Agent deployment.

#### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 From the **Home** page, under **Policies and Profiles** click **Customization Specification Manager**.
- 3 Select `sfo01m01vc01.sfo01.rainpole.local` from the **vCenter Server** drop-down menu.
- 4 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard opens.

- 5 On the **Specify Properties** page, enter the following settings, and click **Next**.

Setting	Value
Target VM Operating System	Windows
Use custom SysPrep answer file	Deselected
Customization Spec Name	vra7-proxy-agent-template

- 6 On the **Set Registration Information** page, enter the following settings, and click **Next**.

Setting	Value
Name	Rainpole
Organization	Rainpole IT

- 7 On the **Set Computer Name** page, select the **Enter a name in the Clone/Deploy wizard** radio button, and click **Next**.

- 8 On the **Enter Windows License** page, enter the following settings, and click **Next**.

If you are using Microsoft License Server, or have multiple single license keys, leave the **Product Key** text box blank.

Setting	Value
Product Key	<i>volume_license_key</i>
Include Server License Information	Selected
Server License Mode	Per seat

- 9 On the **Set Administrator Password** page, enter the following settings, and click **Next**.

Setting	Value
Password	<i>local_administrator_pwd</i>
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

- 10 On the **Time Zone** page, select **(GMT) Coordinated Universal Time** from the **Time Zone** drop-down menu, and click **Next**.

- 11 On the **Run Once** page, type **net localgroup administrators rainpole\svc-vra /add** in the text box and click **Add**. This command will add service account rainpole\svc-vra into the virtual machine's local administrators group. Click **Next**.

- 12 On the **Configure Network** page, select the **Manually select custom settings** radio button, select **NIC1** from the list of network interfaces in the virtual machine, and click **Edit**.

The **Network Properties** dialog box displays.

- 13 In the **Edit Network** dialog box, on the IPv4 page, specify the following settings and click **DNS**.

Setting	Value
Prompt the user for an address when the specification is used	Selected
Subnet Mask	255.255.255.0
Default Gateway	192.168.31.1

- 14 On the **DNS** page, provide DNS servers and search suffixes.

- a Specify the following DNS server settings.

Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.16.11.4
Alternate DNS Server	172.16.11.5

- b Enter **sfo01.rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- c Enter **rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- d Click **OK** to save settings and close the **Edit Network** dialog box, and click **Next**.
- 15 On the **Set Workgroup or Domain** page, enter credentials that have privileges to join the domain, and click **Next**.

Setting	Value
Windows Server Domain	sfo01.rainpole.local
Username	svc-domain-join@rainpole.local
Password	svc-domain-join_password

- 16 On the **Set Operating System** options page, select the **Generate New Security ID (SID)** check box, and click **Next**.
- 17 On the **Ready to Complete** page, review the settings that you entered, and click **Finish**.

The customization specification you created is listed in the **Customization Specification Manager** and can be used to customize virtual machine guest operating systems.

## Create Windows Virtual Machines for vRealize Automation

vRealize Automation requires multiple Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

To facilitate cloning, this design uses the customization specification templates and the windows-2012r2-64 VM template. Repeat this procedure by using the information in the following table to create all needed VMs.

Name for Virtual Machine	NetBIOS name	vCenter Folder	IP	vCPU number	Memory Size	Image Customization Specification Template	Network
vra01iws01a	vra01iws01a	sfo01-m01fd-vra	192.168.11.54	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01iws01b	vra01iws01b	sfo01-m01fd-vra	192.168.11.55	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01ims01a	vra01ims01a	sfo01-m01fd-vra	192.168.11.57	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01ims01b	vra01ims01b	sfo01-m01fd-vra	192.168.11.58	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01dem01a	vra01dem01a	sfo01-m01fd-vra	192.168.11.60	2	6 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01dem01b	vra01dem01b	sfo01-m01fd-vra	192.168.11.61	2	6 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
sfo01ias01a	sfo01ias01a	sfo01-m01fd-vraias	192.168.31.52	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-RegionA01-VXLAN
sfo01ias01b	sfo01ias01b	sfo01-m01fd-vraias	192.168.31.53	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-RegionA01-VXLAN

### Prerequisites

- Verify that you have created the Windows 2012 R2 VM template named **windows-2012r2-64**.
- Verify that windows-2012r2-64 was created with the latest version of VM Tools installed and is updated with the latest Windows updates.
- SHA512 is disabled in Windows for TLS 1.2 by default. If SHA512 certificates are used for vRealize Automation, verify that you have installed the Windows update in Microsoft KB2973337.

## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator** pane, select **Global Inventory Lists > vCenter Servers** and click the **sfo01m01vc01.sfo01.rainpole.local** instance.
- 3 Click **VM Templates in Folders**, right-click the IaaS Windows template **windows-2012r2-64**, and select **New VM from this Template**.
- 4 On the **Select a name and folder** page of the **Deploy From Template** wizard, specify a name and location for the virtual machine.
  - a Enter vra01iws01a in the **Enter a name for the virtual machine** text box.
  - b In the **Select a location for the virtual machine** pane, select the **sfo01-m01fd-vra** folder in the **sfo01-m01dc** data center under **sfo01m01vc01.sfo01.rainpole.local**, and click **Next**.
- 5 On the **Select a compute resource** page, expand **sfo01-m01-mgmt01**, select the **sfo01-m01fd-vra** folder, and click **Next**.
- 6 On the **Select storage** page, select the datastore on which to create the virtual machine's disks.
  - a From the **VM Storage Policy** drop-down menu, select **vSAN Default Storage Policy**.
  - b Select the **sfo01-m01-vsan01** vSAN datastore from the datastore table and click **Next**.
- 7 On the **Select Clone options** page, select the **Customize the operating system** check box, and click **Next**.
- 8 On the **Customize guest OS** page, select the **vra7-template** from the table, and click **Next**.
- 9 On the **User Settings** page, enter the following values, and click **Next**.

Setting	Value
NetBIOS name	vra01iws01a
IPv4 address	192.168.11.54
IPv4 subnet mask	255.255.255.0

- 10 On the **Ready to Complete** page, review your settings and click **Finish**.  
When the deployment of the virtual machine completes, you can customize the virtual machine.
- 11 In the Navigator, select **VMs and Templates**.
- 12 Right-click the **vra01iws01a** virtual machine and select **Edit Settings**.

- 13 Click **Virtual Hardware** and configure the settings for **CPU**, **Memory**, and the **Network adapter 1**.
  - a Select **2** from the **CPU** drop-down menu.
  - b Set the **Memory** settings to **4096 MB**.
  - c Expand **Network adapter 1** and select **vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN** from the drop-down menu and click **OK**.
- 14 Right-click the virtual machine **vra01iws01a**, and select **Power > Power on**.
- 15 From the Virtual Machine Console, verify that vra01iws01a reboots, and uses the configuration settings that you specified.
- 16 Log in to the Windows operating system and perform final verification and customization.
  - a Verify that the IP address, computer name, and domain are correct.
  - b Verify vRealize Automation service account svc-vra@rainpole.local has been added to the Local Administrators Group.
  - c Right click PowerShell, select **Run as Administrator**, run the following command: `Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value "0"`, and reboot the virtual machine.
- 17 Repeat this procedure to deploy and configure the remaining virtual machines.

## Pre-Deployment Tasks for vRealize Operations Manager

Before using vRealize Suite Lifecycle Manager to deploy use cases or solution paths that include vRealize Operations Manager, you must perform pre-deployment tasks.

### Prerequisites for Deploying vRealize Operations Manager

Before you deploy vRealize Operations Manager, verify that your environment satisfies the requirements for this deployment.

#### IP Addresses and Host Names

Verify that static IP addresses and FQDNs for the application virtual networks are available for the SDDC deployment.

For the analytics cluster application virtual network, allocate three static IP addresses and FQDNs for the nodes, one for the load balancer, and map host names to the IP addresses. For the remote collector group, allocate two static IP addresses and FQDNs and map host names to the IP addresses.

**Table 4-5. Application Virtual Network Names for vRealize Operations Manager**

vRealize Operations Manager Component	Application Virtual Network
Analytics Cluster	Mgmt-xRegion01-VXLAN
Remote Collector Group	Mgmt-RegionA01-VXLAN

**Table 4-6. IP Addresses and Host Names for the Analytics Cluster in Region A**

Role	IP Address	FQDN
External load balancer VIP address	192.168.11.35	vrops01svr01.rainpole.local
Master node	192.168.11.31	vrops01svr01a.rainpole.local
Master replica node	192.168.11.32	vrops01svr01b.rainpole.local
Data node 1	192.168.11.33	vrops01svr01c.rainpole.local
Default gateway	192.168.11.1	-
DNS server	<ul style="list-style-type: none"> <li>■ 172.16.11.4</li> <li>■ 172.17.11.4</li> </ul>	-
Subnet mask	255.255.255.0	-
NTP servers	<ul style="list-style-type: none"> <li>■ 172.16.11.251</li> <li>■ 172.16.11.252</li> </ul>	<ul style="list-style-type: none"> <li>■ ntp.sfo01.rainpole.local</li> </ul>

**Table 4-7. IP Addresses and Host Names for the Remote Collectors in Region A**

Role	IP Address	FQDN
Remote collector node 1	192.168.31.31	sfo01vropsc01a.sfo01.rainpole.local
Remote collector node 2	192.168.31.32	sfo01vropsc01b.sfo01.rainpole.local
Default gateway	192.168.31.1	-
DNS server	172.16.11.5	-
Subnet mask	255.255.255.0	-

## Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for the deployment of vRealize Operations Manager.

Prerequisite	Value
Storage	<ul style="list-style-type: none"> <li>■ Virtual disk provisioning. <ul style="list-style-type: none"> <li>■ Thin</li> </ul> </li> <li>■ Required storage per analytics cluster node. <ul style="list-style-type: none"> <li>■ Initial storage for the analytics cluster node: 274 GB</li> <li>■ Additional storage for monitoring data per analytics cluster node: 750 GB</li> </ul> </li> <li>■ Required storage per remote collector group node. <ul style="list-style-type: none"> <li>■ Initial storage per node: 274 GB</li> </ul> </li> </ul>
Software Features	<ul style="list-style-type: none"> <li>■ Verify that vCenter Server is operational.</li> <li>■ Verify that the vSphere cluster has vSphere DRS and HA enabled.</li> <li>■ Verify that the NSX Manager is operational.</li> <li>■ Verify that the application virtual networks are available.</li> <li>■ Verify that the Load Balancer service is enabled on the NSX Edge services gateway.</li> <li>■ Verify that Postman App is installed.</li> </ul>

Prerequisite	Value
Installation Package	<ul style="list-style-type: none"> <li>Download the .ova file of the vRealize Operations Manager virtual appliance on the machine where you use the vSphere Web Client.</li> <li>Download the .pak file for the vRealize Operations Manager Management Pack for NSX for vSphere from VMware Solutions Exchange.</li> <li>Download the .pak file for the vRealize Operations Manager Management Pack for Storage Devices from VMware Solutions Exchange.</li> <li>Download the .pak file for the vRealize Operations Manager Management Pack for Site Recovery Manager from VMware Solutions Exchange.</li> </ul>
License	<ul style="list-style-type: none"> <li>Verify that you have obtained a license that covers the use of vRealize Operations Manager.</li> </ul>
Active Directory	<ul style="list-style-type: none"> <li>Verify that you have a parent active directory with the SDDC user roles configured for the rainpole.local domain.</li> </ul>
Certificate Authority	<ul style="list-style-type: none"> <li>Configure the root Active Directory domain controller as a certificate authority for the environment.</li> <li>Download the CertGenVVD tool and generate the signed certificate for the analytics cluster. See the <i>VMware Validated Design Planning and Preparation</i> documentation.</li> </ul>
External Services	<ul style="list-style-type: none"> <li>Verify that you have access to an SMTP server.</li> <li>Verify that SNMP is enabled in your network environment, to monitor network devices.</li> <li>Verify that Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP) is enabled on each network device for complete monitoring of your environment.</li> </ul>

## Prerequisites for Deploying vRealize Log Insight

Before you use vRealize Suite Lifecycle Manager to deploy vRealize Log Insight, verify that your environment satisfies the requirements for this deployment.

### IP Addresses and Host Names

Verify that static IP addresses and FQDNs for vRealize Log Insight are available in the region-specific application virtual network.

For the application virtual network, allocate three static IP addresses for the vRealize Log Insight nodes and one IP address for the integrated load balancer. Map host names to the IP addresses in DNS.

**Table 4-8. Application Virtual Network Names for vRealize Log Insight**

vRealize Log Insight Component	Application Virtual Network
Analytics Cluster Nodes	Mgmt-RegionA01-VXLAN

**Note** Region A must be routable via the vSphere management network.

**Table 4-9. IP Addresses and Host Names for vRealize Log Insight**

Role	IP Address	FQDN
Integrated load balancer VIP address	192.168.31.10	sfo01vrli01.sfo01.rainpole.local
Master node	192.168.31.11	sfo01vrli01a.sfo01.rainpole.local
Worker node 1	192.168.31.12	sfo01vrli01b.sfo01.rainpole.local

**Table 4-9. IP Addresses and Host Names for vRealize Log Insight (Continued)**

Role	IP Address	FQDN
Worker node 2	192.168.31.13	sfo01vrli01c.sfo01.rainpole.local
Default gateway	192.168.31.1	-
DNS server	<ul style="list-style-type: none"> <li>■ 172.16.11.5</li> <li>■ 172.16.11.4</li> </ul>	-
Subnet mask	255.255.255.0	-
NTP servers	<ul style="list-style-type: none"> <li>■ 172.16.11.251</li> <li>■ 172.16.11.252</li> </ul>	<ul style="list-style-type: none"> <li>■ ntp.sfo01.rainpole.local</li> </ul>

## Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for deploying vRealize Log Insight.

Prerequisite	Value
Storage	<ul style="list-style-type: none"> <li>■ Virtual disk provisioning. <ul style="list-style-type: none"> <li>■ Thin</li> </ul> </li> <li>■ Required storage per node <ul style="list-style-type: none"> <li>■ Initial storage for node deployment: 510 GB</li> </ul> </li> <li>■ Required storage for cluster archiving <ul style="list-style-type: none"> <li>■ Initial storage for archiving: 400 GB</li> </ul> </li> </ul>
Software Features	<ul style="list-style-type: none"> <li>■ Verify that the vCenter Server instances are operational.</li> <li>■ Verify that the vSphere cluster has DRS and HA enabled.</li> <li>■ Verify that the NSX Manager instances are operational.</li> <li>■ Verify that vRealize Operations Manager is operational.</li> <li>■ Verify that the application virtual network is available.</li> <li>■ Verify that the Postman application is installed.</li> <li>■ Verify the following NFS datastore requirements: <ul style="list-style-type: none"> <li>■ Create an NFS share of 400 GB and export it as /V2D_vRLI_MgmtA_400GB.</li> <li>■ Verify that the NFS server supports NFS v3.</li> <li>■ Verify that the NFS partition allows read and write operations for guest accounts.</li> <li>■ Verify that the mount does not require authentication.</li> <li>■ Verify that the NFS share is directly accessible to vRealize Log Insight</li> <li>■ If using a Windows NFS server, allow unmapped user Unix access (by UID/GID).</li> </ul> </li> </ul>
Installation Package	Download the .ova file of the vRealize Log Insight virtual appliance on the machine where you use the vSphere Web Client.
License	Obtain a license that covers the use of vRealize Log Insight.
Active Directory	Verify that you have a parent and child Active Directory domain controllers configured with the role-specific SDDC users and groups for the rainpole.local domain.
Certificate Authority	Configure the Active Directory domain controller as a certificate authority for the environment.
E-mail account	Provide an email account to send vRealize Log Insight notifications.

# Deployment Paths for the IT Automating IT Use Case with vRealize Suite Lifecycle Manager

# 5

vRealize Suite Lifecycle Manager provides two paths for deploying the IT Automating IT use case.

You can deploy the IT Automating IT use case using either of the following methods.

- **Using Installation Wizard:** You can use the installation wizard to deploy the vRealize Suite products for the use case by entering each configuration parameter in the vRealize Suite Lifecycle Manager user interface.
- **Using Configuration File:** You can use the JSON configuration file to deploy the vRealize Suite products for the use case to provide a pre-built configuration to vRealize Suite Lifecycle Manager.

This chapter includes the following topics:

- [Deploy the IT Automating IT Use Case with the vRealize Suite Lifecycle Manager Installation Wizard](#)
- [Deploy the IT Automating IT Use Case with a vRealize Suite Lifecycle Manager JSON Configuration File](#)

## Deploy the IT Automating IT Use Case with the vRealize Suite Lifecycle Manager Installation Wizard

You can deploy all components required for the IT Automating IT use case by using the installation wizard in vRealize Suite Lifecycle Manager.

The installation wizard will prompt you for information about your deployment such as name, location, licensing, virtual machine names, IP addresses, and more.

### Prerequisites

Deploy and configure the vRealize Suite Lifecycle Manager virtual appliance and perform pre-deployment tasks.

## Create the Environment for IT Automating IT with the Installation Wizard

When you deploy the IT Automating IT use case by using the vRealize Suite Lifecycle Manager web interface, you first create a new environment. As part of the task, you input parameters such as the administrator email, network and storage information, and other environment information that is required for the deployment.

**Prerequisites**

vRealize Suite Lifecycle Manager deployed and product OVA sources configured for the IT Automating IT use case.

**Procedure**

1 Login to vRealize Suite Lifecycle Manager

- a Open a Web browser and go to **https://vrs01lcm01.rainpole.local/vr1cm**.
- b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	vrslcm_admin_password

2 To start a new deployment, on the **Home** page, click **Create Environment**.

3 In the **Select Installation Type** window, click **Using Installation Wizard**.

4 On the **Create New Environment** page, enter the following information and click the **Solutions** tab.

Setting	Value
Data Center	sfo01-m01dc
Environment Type	Production
Environment Name/Id	IT Automating IT
Administrator Email	default_deployment_administrator_email
Default Password	default_admin_password
Confirm Default Password	default_admin_password
Customer Experience Improvement Program	Selected

5 On the **Solutions** tab, select **VVD Version 4.2** from the drop-down menu.

6 Select the check box for IT Automating IT and click **Create Environment**.

7 On the **End User License Agreement** page, read the EULA, check **I agree to the terms and conditions**, and click **Next**.

8 On the **License Details** page, add or select the vRealize Suite license.

- a From the drop-down menu provided through the My VMware product entitlement, select **Select vRealize Suite License**, select the license, and click **Next**.
- b Or select **Add vRealize Suite License**, provide the vRealize Suite License key, and click **Next**.

9 On the **Infrastructure Details** page, enter the following information, and click **Next**.

Setting	Value
Select vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Select Cluster	sfo01-m01-mgmt01 (sfo01-m01dc)

Setting	Value
Select Network	Distributed port group that ends with Mgmt-xRegion01-VXLAN
Select Datastore	sfo01-m01-vsan01
Select Disk Format	Thin

10 On the **Network Details** page, enter the following information and click **Next**.

Setting	Value
Default Gateway	192.168.11.1
Domain Name	rainpole.local
Domain Search Path	rainpole.local,sfo01.rainpole.local
Domain Name Server	172.16.11.4,172.16.11.5
Netmask	255.255.255.0

11 On the **Certificate Details** page, select **Use Generated Certificate** and click **Next**.

12 Specify information for each product that is part of this use case:

- a [Configure vRealize Automation with vRealize Suite Lifecycle Manager](#)
- b [Configure vRealize Business for Cloud with vRealize Suite Lifecycle Manager](#)
- c [Configure vRealize Operations Manager with vRealize Suite Lifecycle Manager](#)
- d [Configure vRealize Log Insight with vRealize Suite Lifecycle Manager](#)

13 On the **Summary** page, click **Pre-Validate Configuration**, wait for the Validation successful message, and click **Submit** to start the deployment.

#### What to do next

Monitor the deployment of the IT Automating IT use case by using the vRealize Suite Lifecycle Manager web interface.

## Configure vRealize Automation with vRealize Suite Lifecycle Manager

You configure deployment details for vRealize Automation in the the vRealize Suite Lifecycle Manager installation wizard.

#### Procedure

- 1 On the **Product Details** page, select the **vRealize Automation** tab.
- 2 Enter the following information for **Product Properties**.

Setting	Value
windowsPassword	<i>svc-vra_password</i>
windowsUsername	<i>RAINPOLE\svc-vra</i>

3 Enter the following information for **Cluster Virtual IPs**.

Component	Option	Value
vRA Appliance	Hostname	vra01svr01.rainpole.local
	IP Address	192.168.11.53
IaaS Web	Hostname	vra01iws01.rainpole.local
	IP Address	192.168.11.56
IaaS Manager	Hostname	vra01ims01.rainpole.local
	IP Address	192.168.11.59

4 Configure the **vra-server-primary** and **vra-server-secondary** VMs:

- a Select the **vra-server-primary** VM and click the **Advanced Settings** icon.
- b On **Advanced Configuration for vra-server-primary** page, enter the **vRA Hostname**, **vRA IP Address**, and **vRA VM Name** from the following table.
- c Click **Done**.
- d Repeat for **vra-server-secondary** VM.

Component	vRA Hostname	vRA IP Address	vRA VM Name
vra-server-primary	vra01svr01a.rainpole.local	192.168.11.51	vra01svr01a
vra-server-secondary	vra01svr01b.rainpole.local	192.168.11.52	vra01svr01b

5 Configure the **db** settings:

- a Select the **db** and click the **Advanced Settings** icon.
- b On **Advanced Configuration for db** page, enter the values from the following table.

Setting	Value
Database Name	VRADB-01
Database IP Address	192.168.11.62
To use SQL authentication, deselect this option.	Selected
Database Hostname	vra01mssql01.rainpole.local
VM Name	vra01mssql01

- c Click **Done**.

6 Configure the **iaas-web-01** and **iaas-web-02** VMs:

- a Select the **iaas-web-01** VM and click the **Advanced Settings** icon.
- b On **Advanced Configuration for iaas-web-01** page, enter the **IP Address**, **Windows Web Hostname**, and **Web Name** from the following table.

- c Click **Done**.
- d Repeat for the **iaas-web-02** VM.

Component	IP Address	Windows Web Hostname	Web Name
iaas-web-01	192.168.11.54	vra01iws01a.rainpole.local	vra01iws01a.rainpole.local
iaas-web-02	192.168.11.55	vra01iws01b.rainpole.local	vra01iws01b.rainpole.local

**7** Configure the **iaas-manager-active** and **iaas-manager-passive** VMs:

- a Select the **iaas-manager-active** VM and click the **Advanced Settings** icon.
- b On **Advanced Configuration for iaas-manager-active** page, enter the **IP Address**, **Windows MS Hostname**, and **MS Name** from the following table.
- c Click **Done**.
- d Repeat for the **iaas-manager-passive** VM.

Component	IP Address	Windows MS Hostname	MS Name
iaas-manager-active	192.168.11.57	vra01ims01a.rainpole.local	vra01ims01a.rainpole.local
iaas-manager-passive	192.168.11.58	vra01ims01b.rainpole.local	vra01ims01b.rainpole.local

**8** Configure the **Demworker-01** to **Demworker-06** VMs:

- a Select a **Demworker-01** VM and click the **Advanced Settings** icon.
- b On **Advanced Configuration for Demworker-01** page enter the **IP Address**, **Windows DEM Hostname**, and **DEM Worker Name**.
- c Click **Done**.
- d Repeat for all remaining **Demworker** VMs.

Component	IP Address	Windows DEM Hostname	DEM Worker Name
Demworker-01	192.168.11.60	vra01dem01a.rainpole.local	DEM-WORKER-01
Demworker-02	192.168.11.60	vra01dem01a.rainpole.local	DEM-WORKER-02
Demworker-03	192.168.11.60	vra01dem01a.rainpole.local	DEM-WORKER-03
Demworker-04	192.168.11.61	vra01dem01b.rainpole.local	DEM-WORKER-04
Demworker-05	192.168.11.61	vra01dem01b.rainpole.local	DEM-WORKER-05
Demworker-06	192.168.11.61	vra01dem01b.rainpole.local	DEM-WORKER-06

**9** Configure the **Demorchestrator-01** and **Demorchestrator-02** VMs:

- a Select the **Demorchestrator-01** VM and click the **Advanced Settings** icon.
- b On **Advanced Configuration for Demorchestrator-01** page, enter **IP Address**, **Windows DEM Hostname**, and **DEM Orchestrator Name** from the following table.

- c Click **Done**.
- d Repeat for the **Demorchestrator-02** VM.

Component	IP Address	Windows DEM Hostname	DEM Orchestrator Name
Demorchestrator-01	192.168.11.57	vra01ims01a.rainpole.local	DEM-ORCHESTRATOR-01
Demorchestrator-02	192.168.11.58	vra01ims01b.rainpole.local	DEM-ORCHESTRATOR-02

**10** Configure the **proxy-agent-vsphere-01** and **proxy-agent-vsphere-02** VMs:

- a Select the **proxy-agent-vsphere-01** VM and click the **Advanced Settings** icon.
- b On **Advanced Configuration for proxy-agent-vsphere-01** page, enter the **IP Address**, **Windows Agent Hostname**, and **Agent Name** from the following table.
- c Click **Done**.
- d Repeat for the **proxy-agent-vsphere-02** VM.

Component	IP Address	Windows Agent Hostname	Agent Name	vSphere Endpoint Name
proxy-agent-vsphere-01	192.168.31.52	sfo01ias01a.sfo01.rainpole.local	VSPHERE-AGENT-01	sfo01w01vc01.sfo01.rainpole.local
proxy-agent-vsphere-02	192.168.31.53	sfo01ias01b.sfo01.rainpole.local	VSPHERE-AGENT-01	sfo01w01vc01.sfo01.rainpole.local

## Configure vRealize Business for Cloud with vRealize Suite Lifecycle Manager

You configure deployment details for vRealize Business for Cloud in the vRealize Suite Lifecycle Manager installation wizard.

### Procedure

- 1 On the **Product Details** page, select the **vRealize Business for Cloud** tab.
- 2 Enter the following information for **Product Properties**.

Option	Value
Currency	Select a currency

- 3 Select the **vrbs-server** VM and click the **Advanced Settings** icon.
- 4 On the **Advanced Configuration for vrbs-server** page, enter the following information and click **Done**.

Option	Value
Hostname	vrbs01svr01.rainpole.local
IP Address	192.168.11.66
VM Name	vrbs01svr01

- 5 Select the **vrbc-collector** VM and click **Advanced Settings** icon.
- 6 On **Advanced Configuration for vrbc-collector** page, enter the following information and click **Done**.

Option	Value
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with Mgmt-RegionA01-VXLAN
Hostname	sfo01vrbc01.sfo01.rainpole.local
IP Address	192.168.31.54
Domain	sfo01.rainpole.local
DNS	172.16.11.4,172.16.11.5
Search Path	rainpole.local,sfo01.rainpole.local
VM Name	sfo01vrbc01
Gateway	192.168.31.1

## Configure vRealize Operations Manager with vRealize Suite Lifecycle Manager

You configure deployment details for vRealize Operations Manager in the vRealize Suite Lifecycle Manager installation wizard. You set advanced settings for the required VMs that are part of vRealize Operations Manager.

### Procedure

- 1 On the **Product Details** page, select the **vRealize Operation** tab.
- 2 Enter the following information for **Product Properties**.

Option	Value
NTP Server IP / Hostname	ntp.sfo01.rainpole.local

- 3 Select the **master** VM and click the **Advanced Settings** icon.
- 4 On **Advanced Configuration for master** page, enter the following information and click **Done**.

Option	Value
VM Name	vroops01svr01a
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
Master Hostname	vroops01svr01a.rainpole.local
Master IP Address	192.168.11.31

Option	Value
Extended Storage (1 TB)	sfo01-m01-vsan01
Deploy Option	medium

5 Select the **replica** VM and click the **Advanced Settings** icon.

6 On **Advanced Configuration for replica** page, enter the following information and click **Done**.

Option	Value
VM Name	vrops01svr01b
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
Replica Hostname	vrops01svr01b.rainpole.local
Replica IP Address	192.168.11.32
Extended Storage (1 TB)	sfo01-m01-vsan01
Deploy Option	medium

7 Select the **data-01** VM and click the **Advanced Settings** icon.

8 On **Advanced Configuration for data-01** page, enter the following information and click **Done**.

Option	Value
VM Name	vrops01svr01c
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
Data Hostname	vrops01svr01c.rainpole.local
Data IP Address	192.168.11.33
Extended Storage (1 TB)	sfo01-m01-vsan01
Deploy Option	medium

9 Select the **remotecollector-01** VM and click the **Advanced Settings** icon.

10 On **Advanced Configuration for remotecollector-01** page, enter the following information and click **Done**.

Option	Value
VM Name	sfo01vropsc01a
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with Mgmt-RegionA01-VXLAN
Remote Collector Hostname	sfo01vropsc01a.sfo01.rainpole.local
Remote Collector IP address	192.168.31.31

Option	Value
Domain	sfo01.rainpole.local
Gateway	192.168.31.1
Deploy Option	<b>smallrc</b>

- 11 Select the **remotecollector-02** VM and click the **Advanced Settings** icon.
- 12 On **Advanced Configuration for remotecollector-02** page, enter the following information and click **Done**.

Option	Value
VM Name	sfo01vropsc01b
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with Mgmt-RegionA01-VXLAN
Remote Collector Hostname	sfo01vropsc01b.sfo01.rainpole.local
Remote Collector IP Address	192.168.31.32
Domain	sfo01.rainpole.local
Gateway	192.168.31.1
Deploy Option	<b>smallrc</b>

## Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

You configure deployment details for vRealize Log Insight in the vRealize Suite Lifecycle Manager installation wizard.

### Procedure

- 1 On the **Product Details** page, select the **vRealize Log Insight** tab.
- 2 Enter the following information for **Product Properties**.

Option	Value
Configure Cluster Virtual IPs	Selected
FQDN	sfo01vrli01.sfo01.rainpole.local
Virtual IP Address	192.168.31.10

- 3 Select the **vrli-master** VM and click the **Advanced Settings** icon.

- 4 On **Advanced Configuration for vrli-master** page, enter following information and click **Done**.

Option	Value
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	Distributed port group that ends with Mgmt-RegionA01-VXLAN
Hostname	sfo01vrli01a.sfo01.rainpole.local
IP Address	192.168.31.11
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01a
Gateway	192.168.31.1
Deploy Option	<b>medium</b>

- 5 Select the **vrli-worker-01** VM and click the **Advanced Settings** icon.

- 6 On **Advanced Configuration for vrli-worker-01** page, enter the following information and click **Done**.

Option	Value
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
IP Address	192.168.31.12
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	Distributed port group that ends with Mgmt-RegionA01-VXLAN
Hostname	sfo01vrli01b.sfo01.rainpole.local
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01b
Gateway	192.168.31.1
Deploy Option	<b>medium</b>

- 7 Select the **vrli-worker-02** VM and click the **Advanced Settings** icon.

- 8 On **Advanced Configuration for vrli-worker-02** page, enter the following information and click **Done**.

Option	Value
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
IP Address	192.168.31.13
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	Distributed port group that ends with Mgmt-RegionA01-VXLAN
Hostname	sfo01vrli01c.sfo01.rainpole.local
Domain	sfo01.rainpole.local

Option	Value
VM Name	sfo01vrli01c
Gateway	192.168.31.1
Deploy Option	medium

- 9 Click **Next** and review the configuration details on the **Summary** page.
- 10 Click **Submit** to create the environment.

## Monitor the Deployment for IT Automating IT in vRealize Suite Lifecycle Manager

You can monitor the status of the IT Automating IT deployment in the vRealize Suite Lifecycle Manager user interface.

### Procedure

- 1 Login to vRealize Suite Lifecycle Manager
  - a Open a Web browser and go to <https://vrs01lcm01.rainpole.local/vr1cm>.
  - b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	vrslcm_admin_password

- 2 In the **Navigator**, click **Requests** and validate that CREATE\_ENVIRONMENT for Environment Name:IT Automating IT in the **Request Info** is INPROGRESS. It can take a moment for the process to progress from SUBMITTED to INPROGRESS state.
- 3 Select the INPROGRESS for Environment Name:IT Automating IT in the **Request Info** column.
- 4 In **Requests** page, monitor the steps of the deployment graph until the request is marked as COMPLETED.

## Deploy the IT Automating IT Use Case with a vRealize Suite Lifecycle Manager JSON Configuration File

You can deploy all components required for the IT Automating IT use case by providing a JSON configuration file in vRealize Suite Lifecycle Manager.

The process prompts you for information about your deployment such as name, location, password, and the JSON configuration file.

## Create the Environment for IT Automating IT with a JSON Configuration File

You can deploy the products required by the IT Automating IT use case by importing a JSON configuration file into vRealize Suite Lifecycle Manager.

### Prerequisites

Deploy and configure the vRealize Suite Lifecycle Manager virtual appliance and perform pre-deployment tasks.

### Procedure

- 1 Login to vRealize Suite Lifecycle Manager
  - a Open a Web browser and go to **https://vrs01lcm01.rainpole.local/vr1cm**.
  - b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	vrslcm_admin_password

- 2 On the **Home** page, click **Create Environment**.
- 3 In **Select Installation Type** dialog, select **Using Configuration File**.
- 4 On the **Data Center and Environment** page, enter the following information.

Setting	Value
Data Center	sfo01-m01dc
Environment Type	Production
Environment Name	IT Automating IT
Administrator Email	default_deployment_administrator_email
Default Password	default_deployment_password
Confirm Default Password	default_deployment_password
Customer Experience Improvement Program	Selected

- 5 On the **Product Config JSON** section, copy and paste the example JSON configuration file below.
  - a Update the license with your vRealize Suite license key value.
  - b Provide the masterCertificateChain, masterPrivateKey, masterKeyPassphrase, certificateChain, privateKey, and keyPassphrase values.
  - c Provide the vcPassword value.

- d Provide the vmNetwork and network with requisite dvPortGroup value.
- e Review all name/value pairs for your deployment.

**Note** The certificate chain and private key values must be provided in a single line with \n for each line break.

```
"masterCertificateChain": "-----BEGIN CERTIFICATE-----\nLine 1\nLine 2\n-----END CERTIFICATE-----"
```

## 6 Click **Create Environment**.

### Example: Example JSON Configuration File for IT Automating IT

```
{
  "encoded": false,
  "infrastructure": {
    "properties": {
      "acceptEULA": true,
      "diskFormat": "Thin",
      "license": "xxxxx-xxxxx-xxxxx-xxxxxx-xxxxx",
      "vcUsername": "svc-vrslcm-vsphere@rainpole.local",
      "vcPassword": "vsphere_admin_password",
      "vcHostname": "sfo01m01vc01.sfo01.rainpole.local",
      "clusterName": "sfo01-dc#sfo01-m01-mgmt01",
      "datastoreName": "sfo01-m01-vsan01",
      "vmNetwork": "dvPortgroup ending with Mgmt-xRegion01-VXLAN",
      "netmask": "255.255.255.0",
      "gateway": "192.168.11.1",
      "dnsServers": "172.16.11.4,172.16.11.5",
      "domain": "rainpole.local",
      "searchpath": "rainpole.local,sfo01.rainpole.local",
      "masterCertificateChain": "-----BEGIN CERTIFICATE-----\n\n-----END CERTIFICATE-----",
      "masterPrivateKey": "-----BEGIN RSA PRIVATE KEY-----\n\n-----END RSA PRIVATE KEY-----",
      "masterKeyPassphrase": "master_key_passphrase",
      "certificateChain": "-----BEGIN CERTIFICATE-----\n\n-----END CERTIFICATE-----",
      "privateKey": "-----BEGIN RSA PRIVATE KEY-----\n\n-----END RSA PRIVATE KEY-----",
      "keyPassphrase": "key_passphrase"
    }
  },
  "products": [
    {
      "id": "vra",
      "version": "7.3.0",
      "clusterVIP": [
        {
          "type": "vra",
          "hostname": "vra01svr01.rainpole.local",
          "ipAddress": "192.168.11.53"
        },
        {
          "type": "iaas-web",
          "hostname": "vra01iws01.rainpole.local",
          "ipAddress": "192.168.11.56"
        }
      ]
    }
  ]
}
```

```

    },
    {
      "type": "iaas-manager",
      "hostname": "vra01ims01.rainpole.local",
      "ipAddress": "192.168.11.59"
    }
  ],
  "properties": {
    "windowsUsername": "rainpole\\svc-vra",
    "windowsPassword": "svc-vra_password"
  },
  "nodes": [
    {
      "type": "vra-server-primary",
      "properties": {
        "name": "vra01svr01a",
        "ipAddress": "192.168.11.51",
        "hostname": "vra01svr01a.rainpole.local",
        "vidmVraDisabledAdvanced": "false"
      }
    },
    {
      "type": "vra-server-secondary",
      "properties": {
        "name": "vra01svr01b",
        "ipAddress": "192.168.11.52",
        "hostname": "vra01svr01b.rainpole.local"
      }
    },
    {
      "type": "db",
      "properties": {
        "name": "vra01mssql01",
        "ipAddress": "192.168.11.162",
        "hostname": "vra01mssql01.rainpole.local",
        "databaseName": "VRADB-01",
        "useWindowsAuthentication": "true"
      }
    },
    {
      "type": "iaas-web",
      "properties": {
        "name": "vra01iws01a.rainpole.local",
        "ipAddress": "192.168.11.54",
        "hostname": "vra01iws01a.rainpole.local"
      }
    },
    {
      "type": "iaas-web",
      "properties": {
        "name": "vra01iws01b.rainpole.local",
        "ipAddress": "192.168.11.55",
        "hostname": "vra01iws01b.rainpole.local"
      }
    }
  ],

```

```

{
  "type": "iaas-manager-active",
  "properties": {
    "name": "vra01ims01a.rainpole.local",
    "ipAddress": "192.168.11.57",
    "hostname": "vra01ims01a.rainpole.local"
  }
},
{
  "type": "iaas-manager-passive",
  "properties": {
    "name": "vra01ims01b.rainpole.local",
    "ipAddress": "192.168.11.58",
    "hostname": "vra01ims01b.rainpole.local"
  }
},
{
  "type": "iaas-dem-worker",
  "properties": {
    "name": "DEM-WORKER-01",
    "ipAddress": "192.168.11.60",
    "hostname": "vra01dem01a.rainpole.local"
  }
},
{
  "type": "iaas-dem-worker",
  "properties": {
    "name": "DEM-WORKER-02",
    "ipAddress": "192.168.11.60",
    "hostname": "vra01dem01a.rainpole.local"
  }
},
{
  "type": "iaas-dem-worker",
  "properties": {
    "name": "DEM-WORKER-03",
    "ipAddress": "192.168.11.60",
    "hostname": "vra01dem01a.rainpole.local"
  }
},
{
  "type": "iaas-dem-worker",
  "properties": {
    "name": "DEM-WORKER-04",
    "ipAddress": "192.168.11.61",
    "hostname": "vra01dem01b.rainpole.local"
  }
},
{
  "type": "iaas-dem-worker",
  "properties": {
    "name": "DEM-WORKER-05",
    "ipAddress": "192.168.11.61",
    "hostname": "vra01dem01b.rainpole.local"
  }
}

```

```

    },
    {
      "type": "iaas-dem-worker",
      "properties": {
        "name": "DEM-WORKER-06",
        "ipAddress": "192.168.11.61",
        "hostname": "vra01dem01b.rainpole.local"
      }
    },
    {
      "type": "iaas-dem-orchestrator",
      "properties": {
        "name": "DEM-ORCHESTRATOR-01",
        "ipAddress": "192.168.11.57",
        "hostname": "vra01ims01a.rainpole.local"
      }
    },
    {
      "type": "iaas-dem-orchestrator",
      "properties": {
        "name": "DEM-ORCHESTRATOR-02",
        "ipAddress": "192.168.11.58",
        "hostname": "vra01ims01b.rainpole.local"
      }
    },
    {
      "type": "proxy-agent-vsphere",
      "properties": {
        "name": "VSPHERE-AGENT-01",
        "ipAddress": "192.168.31.52",
        "agentName": "VSPHERE-AGENT-01",
        "vsphereEndpointName": "sfo01w01vc01.sfo01.rainpole.local",
        "hostname": "sfo01ias01a.sfo01.rainpole.local"
      }
    },
    {
      "type": "proxy-agent-vsphere",
      "properties": {
        "name": "VSPHERE-AGENT-01",
        "agentName": "VSPHERE-AGENT-01",
        "vsphereEndpointName": "sfo01w01vc01.sfo01.rainpole.local",
        "ipAddress": "192.168.31.53",
        "hostname": "sfo01ias01b.sfo01.rainpole.local"
      }
    }
  ],
  "contents": [],
},
{
  "id": "vrbc",
  "version": "7.3.1",
  "clusterVIP": [],
  "properties": {
    "currency": "USD - US Dollar"
  }
},

```

```

"nodes": [
  {
    "type": "vrb-server",
    "properties": {
      "name": "vrb01svr01",
      "ipAddress": "192.168.11.66",
      "hostname": "vrb01svr01.rainpole.local"
    }
  },
  {
    "type": "vrb-collector",
    "properties": {
      "name": "sfo01vrbc01",
      "ipAddress": "192.168.31.54",
      "hostname": "sfo01vrbc01.sfo01.rainpole.local",
      "network": "dvPortgroup ending with Mgmt-RegionA01-VXLAN",
      "domain": "sfo01.rainpole.local",
      "searchpath": "sfo01.rainpole.local,rainpole.local",
      "gateway": "192.168.31.1"
    }
  }
],
"contents": [],
{
  "id": "vrops",
  "version": "6.6.1",
  "clusterVIP": [],
  "properties": {
    "ntpServerIP": "ntp.sfo01.rainpole.local"
  },
  "nodes": [
    {
      "type": "master",
      "properties": {
        "name": "vrops01svr01a",
        "ipAddress": "192.168.11.31",
        "hostname": "vrops01svr01a.rainpole.local",
        "extendedStorage": "sfo01-m01-vsan01",
        "deployOption": "medium"
      }
    },
    {
      "type": "replica",
      "properties": {
        "name": "vrops01svr01b",
        "ipAddress": "192.168.11.32",
        "hostname": "vrops01svr01b.rainpole.local",
        "extendedStorage": "sfo01-m01-vsan01",
        "deployOption": "medium"
      }
    },
    {
      "type": "data",
      "properties": {

```

```

        "name": "vrops01svr01c",
        "ipAddress": "192.168.11.33",
        "hostname": "vrops01svr01c.rainpole.local",
        "extendedStorage": "sfo01-m01-vsan01",
        "deployOption": "medium"
    }
},
{
    "type": "remotecollector",
    "properties": {
        "name": "sfo01vropsc01a",
        "ipAddress": "192.168.31.31",
        "hostname": "sfo01vropsc01a.sfo01.rainpole.local",
        "network": "dvPortgroup ending with Mgmt-RegionA01-VXLAN",
        "domain": "sfo01.rainpole.local",
        "searchpath": "sfo01.rainpole.local,rainpole.local",
        "gateway": "192.168.31.1",
        "deployOption": "smallrc"
    }
},
{
    "type": "remotecollector",
    "properties": {
        "name": "sfo01vropsc01b",
        "ipAddress": "192.168.31.32",
        "hostname": "sfo01vropsc01b.sfo01.rainpole.local",
        "network": "dvPortgroup ending with Mgmt-RegionA01-VXLAN",
        "domain": "sfo01.rainpole.local",
        "searchpath": "sfo01.rainpole.local,rainpole.local",
        "gateway": "192.168.31.1",
        "deployOption": "smallrc"
    }
}
],
"contents": []
},
{
    "id": "vrli",
    "version": "4.5.1",
    "clusterVIP": [],
    "properties": {
        "vrliClusterVips": "192.168.31.10#sfo01vrli01.sfo01.rainpole.local"
    },
    "nodes": [
        {
            "type": "vrli-master",
            "properties": {
                "name": "sfo01vrli01a",
                "vrliAdminEmail": "admin@rainpole.local",
                "vrliLicenseKey": "xxxxx-xxxxx-xxxxx-xxxxxx-xxxxx",
                "ipAddress": "192.168.31.11",
                "hostname": "sfo01vrli01a.sfo01.rainpole.local",
                "network": "dvPortgroup ending with Mgmt-RegionA01-VXLAN",
                "domain": "sfo01.rainpole.local",
                "searchpath": "sfo01.rainpole.local,rainpole.local",
            }
        }
    ]
}

```

```

    "gateway": "192.168.31.1",
    "deployOption": "medium"
  }
},
{
  "type": "vrli-worker",
  "properties": {
    "name": "sfo01vrli01b",
    "ipAddress": "192.168.31.12",
    "hostname": "sfo01vrli01b.sfo01.rainpole.local",
    "network": "dvPortgroup ending with Mgmt-RegionA01-VXLAN",
    "domain": "sfo01.rainpole.local",
    "searchpath": "sfo01.rainpole.local,rainpole.local",
    "gateway": "192.168.31.1",
    "deployOption": "medium"
  }
},
{
  "type": "vrli-worker",
  "properties": {
    "name": "sfo01vrli01c",
    "ipAddress": "192.168.31.13",
    "hostname": "sfo01vrli01c.sfo01.rainpole.local",
    "network": "dvPortgroup ending with Mgmt-RegionA01-VXLAN",
    "domain": "sfo01.rainpole.local",
    "searchpath": "sfo01.rainpole.local,rainpole.local",
    "gateway": "192.168.31.1",
    "deployOption": "medium"
  }
}
],
"contents": []
}
]
}

```

### What to do next

Monitor the deployment of the IT Automating IT solution path deployment by using the vRealize Suite Lifecycle Manager web interface.

## Monitor the Deployment for IT Automating IT in vRealize Suite Lifecycle Manager

You can monitor the status of the IT Automating IT deployment in the vRealize Suite Lifecycle Manager user interface.

## Procedure

### 1 Login to vRealize Suite Lifecycle Manager

- a Open a Web browser and go to **https://vrs01lcm01.rainpole.local/vr1cm**.
- b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	<i>vrslcm_admin_password</i>

- 2 In the **Navigator**, click **Requests** and validate that CREATE\_ENVIRONMENT for Environment Name:IT Automating IT in the **Request Info** is INPROGRESS. It can take a moment for the process to progress from SUBMITTED to INPROGRESS state.
- 3 Select the INPROGRESS for Environment Name:IT Automating IT in the **Request Info** column.
- 4 In **Requests** page, monitor the steps of the deployment graph until the request is marked as COMPLETED.

# Post-Deployment Tasks for vRealize Automation

# 6

Post-deployment tasks for vRealize Automation include configuration of vRealize Automation, an embedded vRealize Orchestrator, and vRealize Business for Cloud.

vRealize Automation incorporates virtual machine provisioning and a self-service portal. vRealize Business enables billing and chargeback functions. vRealize Orchestrator provides workflow optimization. The following procedures describe the validated flow of post configuration for use case deployment.

Post-deployment tasks include customizing the installation environment and configuring one or more tenants. By using the secure portal Web interface, administrators, developers, or business users can then request IT services and manage specific cloud and IT resources based on their roles and privileges.

## Procedure

### 1 [Move vRealize Automation and vRealize Business for Cloud Appliances to Virtual Machine Folders](#)

Use the vSphere Web Client to move vRealize Automation and vRealize Business for Cloud appliances to virtual machine folders for organization and ease of management.

### 2 [Set Up NTP on the vRealize Automation Appliance](#)

Time synchronization in your environment is essential. If different SDDC components are out of sync, authentication might no longer work. After deployment with vRealize Suite Lifecycle Manager, you have to connect each vRealize Automation appliance to the NTP server.

### 3 [Create Anti-Affinity Rules for vRealize Automation Virtual Machines](#)

A VM-Host anti-affinity (or affinity) rule specifies the relationship between a group of virtual machines and a group of hosts. Anti-affinity rules force selected virtual machines to remain hosted on different hosts during failover actions, and are a requirement for high availability.

### 4 [Replace the vRealize Automation Certificate](#)

Replace the existing certificate for all vRealize Automation services from the vRealize Automation Management Console. You replace the certificate on the vRealize Automation Appliance, IaaS Web server and IaaS Manager server to maintain trusted communication between the vRealize Automation nodes.

### 5 [vRealize Automation Default Tenant Configuration](#)

In shared cloud environments, where multiple companies, divisions or independent groups are using a common infrastructure fabric, it is necessary to set up virtual private clouds where authentication, resources, policy are customized to the needs of each group. Tenants are useful for isolating the users, resources, and services of one tenant from those of other tenants.

## 6 vRealize Automation Tenant Creation

You create additional vRealize Automation tenants so that users can access the applications and resources that they need to complete their work assignments.

## 7 Embedded vRealize Orchestrator Configuration

VMware Embedded vRealize Orchestrator is a platform that provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage the VMware vSphere infrastructure and other VMware and third-party technologies.

## 8 vRealize Business Installation

vRealize Business is an IT financial management tool that provides clarity and control over the costs and quality of IT services, enabling alignment with the business and acceleration of IT transformation.

## 9 Cloud Management Platform Post-Installation Tasks

After you deploy vRealize Automation and vRealize Orchestrator, you enable health monitors to check the health status of individual servers, and remove the snapshots created during the vRealize Automation installation.

## 10 Content Library Configuration

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

## 11 Tenant Content Creation

To provision virtual machines in the Compute vCenter Server, you must configure the tenant to use compute resources within vCenter Server.

# Move vRealize Automation and vRealize Business for Cloud Appliances to Virtual Machine Folders

Use the vSphere Web Client to move vRealize Automation and vRealize Business for Cloud appliances to virtual machine folders for organization and ease of management.

vRealize Suite Lifecycle Manager deploys:

- Two vRealize Automation appliances. Server 01a and Server 01b
- Two vRealize Business for Cloud appliances: Server 01 and Remote Collector 01

### Prerequisites

Verify that the virtual machine folders **sfo01-m01fd-vra** and **sfo01-m01fd-vraias** were previously created in the **sfo01-m01dc** data center during the vRealize Automation pre-deployment tasks.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the Home menu, select **VMs and Templates**.
- 3 Navigate to the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server and **sfo01-m01dc** data center.
- 4 Move the vRealize Automation and vRealize Business for Cloud server appliances.
  - a Select the virtual machines **vra01svr01a**, **vra01svr01b**, and **vrb01svr01**.
  - b Right click and select **Move to...** and select **sfo01-m01fd-vra** under VM Folders.
  - c Click **OK**.
- 5 Move the vRealize Business for Cloud remote collector virtual machine.
  - a Select the virtual machine **sfo01vrbc01**.
  - b Right click and select **Move to...** and select **sfo01-m01fd-vraias** under VM Folders
  - c Click **OK**.

## Set Up NTP on the vRealize Automation Appliance

Time synchronization in your environment is essential. If different SDDC components are out of sync, authentication might no longer work. After deployment with vRealize Suite Lifecycle Manager, you have to connect each vRealize Automation appliance to the NTP server.

**Procedure**

- 1 Log in to the first vRealize Automation appliance.
  - a Open a Web browser and go to **https://vra01svr01a.rainpole.local:5480/**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vra_appA_root_password

- 2 On the **VMware vRealize Appliance** page, click the **Admin** tab.
- 3 On the **Admin** tab, click **Time Settings**.

- 4 On the **Time Settings** tab, select **Use Timer Server** as the Time Sync. Mode and specify the time server:

Setting	Value
Time Server	ntp.sfo01.rainpole.local

- 5 Click **Save Settings**.
- 6 Repeat the steps for the second vRealize Automation appliance, <https://vra01svr01b.rainpole.local:5480/>

**Note** The Time Offset column shows the time delta between the vRealize Automation appliance and the Windows IaaS VMs. Time synchronization is critical. If there are values outside of the acceptable boundaries, remediate those before you proceed.

## Create Anti-Affinity Rules for vRealize Automation Virtual Machines

A VM-Host anti-affinity (or affinity) rule specifies the relationship between a group of virtual machines and a group of hosts. Anti-affinity rules force selected virtual machines to remain hosted on different hosts during failover actions, and are a requirement for high availability.

**Table 6-1. Anti-Affinity Rules for the Cloud Management Platform**

Name	Type	Members
anti-affinity-rule-vra-svr	Separate Virtual Machines	vra01svr01a, vra01svr01b
anti-affinity-rule-vra-iws	Separate Virtual Machines	vra01iws01a, vra01iws01b
anti-affinity-rule-vra-ims	Separate Virtual Machines	vra01ims01a, vra01ims01b
anti-affinity-rule-vra-dem	Separate Virtual Machines	vra01dem01a, vra01dem01b
anti-affinity-rule-vra-ias	Separate Virtual Machines	sfo01ias01a, sfo01ias01b

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** page, click **Hosts and Clusters**.
- 3 Under **sfo01m01vc01.sfo01.rainpole.local**, click **sfo01-m01dc**, and click **sfo01-m01-mgmt01**.

- 4 Click the **Configure** tab, and under **Configuration**, select **VM/Host Rules**.
- 5 Under **VM/Host Rules**, click **Add** to create a virtual machine anti-affinity rule.
- 6 In the **Create VM/Host Rule** dialog box, specify the first rule for the vRealize Automation virtual appliances.
  - a In the **Name** text box, enter **anti-affinity-rule-vra-svr**.
  - b Select the **Enable rule** check box.
  - c Select **Separate Virtual Machines** from the **Type** drop-down menu.
  - d Click **Add**, select the **vra01svr01a** and **vra01svr01b** virtual machines, click **OK**, and click **OK**.
- 7 Repeat the procedure to configure the remaining anti-affinity rules.

## Replace the vRealize Automation Certificate

Replace the existing certificate for all vRealize Automation services from the vRealize Automation Management Console. You replace the certificate on the vRealize Automation Appliance, IaaS Web server and IaaS Manager server to maintain trusted communication between the vRealize Automation nodes.

### Procedure

- 1 Log in to the vRealize Automation appliance management console.
  - a Open a Web Browser and go to **https://vra01svr01a.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vra_appA_root_password

- 2 On **vRA Settings** tab, click the **Host Settings** tab.
- 3 Under **SSL Configuration**, select **Import** next **Certificate Action**.
- 4 From a text editor on the Windows host where you run the CertGenVVD utility, copy the content of the following certificate files and paste it in the corresponding text boxes in the user interface, and click **Save Settings**.

Source Content	Target Text Box
vra.key	RSA Private Key
vra.3.pem	Certificate Chain
Passphrase that you optionally entered at generation	Passphrase

- 5 Scroll down on the page and verify that all cluster nodes have been successfully updated.
- 6 Click the **Certificates** tab and repeat the procedure to configure the IaaS Web server and IaaS Manager Service with the new certificate details.

IaaS Component	Component Type
IaaS Web server	IaaS Web
IaaS Manager Service	Manager Service

## vRealize Automation Default Tenant Configuration

In shared cloud environments, where multiple companies, divisions or independent groups are using a common infrastructure fabric, it is necessary to set up virtual private clouds where authentication, resources, policy are customized to the needs of each group. Tenants are useful for isolating the users, resources, and services of one tenant from those of other tenants.

### Create a Local Tenant Administrator

To support Integrated Windows Authentication, join the VMware Identity Manager connectors to the Active Directory domain. Perform this operation in the default tenant **vsphere.local**.

Create a local user for the default tenant in vRealize Automation and assign the Tenant Administrator role to the default tenant.

### Procedure

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 On the **Tenants** page, click the default tenant **vsphere.local** to edit its settings.
- 3 Click the **Local users** tab and click **New** to add a local user to the default tenant.
- 4 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	vRA
Last name	LocalDefaultAdmin
Email	vra-localdefaultadmin@vsphere.local
User name	vra-localdefaultadmin
Password	<i>vra-localdefaultadmin_password</i>
Confirm password	<i>vra-localdefaultadmin_password</i>

- 5 On the **Administrators** tab, specify tenant and infrastructure administrators.
  - a In the **Tenant administrators** search text box, enter **vra-localdefaultadmin** and press Enter.
  - b In the **laaS administrators** search text box, enter **vra-localdefaultadmin** and press Enter.
  - c Click **Finish**.
- 6 Log out of the vRealize Automation portal.

## Join Connectors to an Active Directory Domain

To use an Active Directory domain for tenant authentication, you must join a VMware Identity Manager connector to vRealize Automation.

Each vRealize Automation appliance includes a connector that supports user authentication. By default, one connector is typically configured to perform a directory synchronization. Perform the procedure by using the **vra-localdefaultadmin** that you configured in the previous procedure.

**Procedure**

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/vsphere.local**.
  - b Log in using the following credentials.

Setting	Value
User name	vra-localdefaultadmin
Password	vra-localdefaultadmin_password

- 2 Navigate to **Administration > Directories Management > Connectors**.
- 3 For the **first.connector**, click **Join Domain**, specify the following settings, and click **Join Domain**.

Setting	Value
Domain	Custom Domain rainpole.local
Domain User	svc-domain-join
Domain Password	svc-domain-join_password

- 4 Log out from the vRealize Automation portal.

## vRealize Automation Tenant Creation

You create additional vRealize Automation tenants so that users can access the applications and resources that they need to complete their work assignments.

A tenant is a group of users with specific privileges who work within a software instance. Administrators can create additional tenants so that users can log in and complete their work assignments. Administrators can create as many tenants as needed for system operation. Administrators must specify basic configuration such as name, login URL, local users, and administrators. The tenant administrator must also log in and set up an appropriate Active Directory connection and apply a custom branding to tenants.

### Create the Rainpole Tenant

The vRealize Automation Identity Manager provides Single-Sign On (SSO) capability for vRealize Automation users.

vRealize Automation Identity Manager is an authentication broker and security token exchange that interacts with the Active Directory to authenticate users. As the system administrator, you configure Identity Manager to provide access to vRealize Automation by the Rainpole tenant. The Rainpole tenant is the tenant through which you manage system-wide configuration, that includes global system defaults for branding, notifications, and monitor system logs.

**Procedure**

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 On the **Tenants** page, click **New** to configure a new tenant.
- 3 On the **General** tab, enter the following settings for the Rainpole tenant, and click **Submit and Next**.

Setting	Value
Name	Rainpole
URL Name	rainpole
Contact email	administrator@rainpole.local

- 4 On the **Local Users** tab, click **New** to add a local user for the tenant.
- 5 In the **User Details** dialog box, configure the following settings, click **OK**, and click **Next**.

Setting	Value
First name	vRA
Last name	LocalRainpoleAdmin
Email	vra-localrainpoleadmin@rainpole.local
User name	vra-localrainpoleadmin
Password	<i>vra-localrainpoleadmin_password</i>
Confirm password	<i>vra-localrainpoleadmin_password</i>

- 6 On the **Administrators** tab, specify tenant and infrastructure administrators.
  - a Enter **vra-localrainpoleadmin** in the **Tenant administrators** search text box and press **Enter**.
  - b Enter **vra-localrainpoleadmin** in the **IaaS administrators** search text box and press **Enter**.
  - c Click **Finish**.
- 7 Log out of vRealize Automation portal.

## Configure Identity Management for the vRealize Automation Tenant

vRealize Automation uses VMware Identity Manager to authenticate users.

Each tenant must be associated with at least one directory as part of the tenant creation. You can add more directories if necessary. Perform the procedure by using the `vra-localrainpoleadmin` that you configured.

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
  - b Log in using the following credentials.

Setting	Value
User name	<code>vra-localrainpoleadmin</code>
Password	<code>vra-localrainpoleadmin_password</code>

- 2 Navigate to **Administration > Directories Management > Directories**.
- 3 Click **Add Directory** and select **Add Active Directory over LDAP/IWA**, specify the following settings, and click **Save & Next**.

Setting	Value
Directory Name	<code>rainpole.local</code>
Directory Type	Active Directory (Integrated Windows Authentication)
Sync Connector	<code>vra01svr01a.rainpole.local</code>
Authentication	Yes
Directory Search Attribute	<code>sAMAccountName</code>
Certificates	Deselected
Domain Name	<code>rainpole.local</code>
Domain Admin Username	<code>domain administrator</code>
Domain Admin Password	<code>domain_admin_password</code>
Bind User UPN	<code>svc-vra@rainpole.local</code>
Bind DN Password	<code>svc-vra_password</code>

- 4 On the **Select the Domains** page, select **rainpole.local (RAINPOLE)**, and click **Next**.
- 5 On the **Map User Attributes** page, click **Next**.
- 6 On the **Select the groups (users) you want to sync** page, enter the group DNs to sync.
  - a Click the **Add** icon to add the distinguished name to the search criteria.
  - b In the **Specify the group DNs** text box, enter `dc=rainpole,dc=local` and click **Find Groups**.
  - c After the **Groups to sync** value updates, click the **Select** button.

- d Select the following groups and click **Save**.
    - ug-vra-admins-rainpole
    - ug-vra-archs-rainpole
    - ug-SDDC-Admins
    - ug-SDDC-Ops
    - ug-vROAdmins
  - e Click **Next**.
- 7 On the **Select the Users you would like to sync** page, enter the user DNs to sync.
    - a Click the **Add** icon to add the distinguished name to the search criteria.
    - b In the **Specify the user DNs** text box, enter **cn=users,dc=rainpole,dc=local**, click the **Add** icon on the same row, and click **Next**.
  - 8 On the **Review** page, click **Sync Directory**.

## Configure Directories Management for High Availability

Each vRealize Automation appliance includes a connector that supports user authentication, although only one connector is typically configured to perform directory synchronization.

To support Directories Management high availability, you must configure a second connector that corresponds to your second vRealize Automation appliance. That second connector connects to the same Identity Provider and, through VMware Identity Manager, points to the same Active Directory instance. With this configuration, if one appliance fails, the other can take over management of user authentication.

In a high availability environment, all nodes must serve the same set of users, authentication methods, and other Active Directory constructs. The most direct method to accomplish this is to promote the Identity Provider to the cluster by setting the load balancer host as the Identity Provider host. With this configuration, all authentication requests are directed to the load balancer, which forwards the request to either connector as appropriate.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	vra-localrainpoleadmin
Password	vra-localrainpoleadmin_password

- 2 Navigate to **Administration > Directories Management > Identity Providers**.

- 3 Click **WorkspaceIDP\_1** to edit its settings.
- 4 Under **Connector(s)**, specify the following settings and click **Add Connector**.

Setting	Value
Add a Connector	vra01svr01b.rainpole.local
Bind DN Password	<i>svc-vra_password</i>
Domain Admin Password	<i>domain_admin_password</i>

- 5 In the **Idp Hostname** text box, enter **vra01svr01.rainpole.local**, the host name of the load balancer, and click **Save**.

## Assign Tenant Administrative Roles to Active Directory Users

After vRealize Automation Directories Management is associated with your Active Directory domain, domain users can administer the tenant. Assign domain user groups for tenant and infrastructure administrators.

### Procedure

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 On the **Tenants** page, click the Rainpole tenant to edit its settings.
- 3 Click the **Administrators** tab to assign domain user groups for tenant and infrastructure administrators.
  - a Enter **ug-vra-admins-rainpole** in the **Tenant administrators** search text box and press **Enter**.
  - b Enter **ug-vra-admins-rainpole** in the **laaS administrators** search text box and press **Enter**.
  - c Click **Finish**.

## Brand the Tenant Login Pages

You can apply custom branding on a per-customer basis to the vRealize Automation tenant login pages.

System administrators control the default branding for all tenants. As a tenant administrator, you change the branding of the portal. That includes the logo, the background color, and the information in the header and footer. If the branding for a tenant is changed, a tenant administrator can revert to the system defaults.

## Procedure

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 Navigate to **Administration > Branding** and deselect the **Use default** check box.
- 3 On the **Header** tab, specify the following settings for the header branding.

Setting	Value
Company Name	Rainpole
Product Name	Infrastructure Service Portal
Background hex color	<i>3989C7</i>
Text hex color	<i>FFFFFF</i>

- 4 Click the **Footer** tab, specify the following settings for the footer branding, and click **Finish**.

Setting	Value
Copyright notice	Copyright Rainpole. All Rights Reserved.
Privacy policy link	<a href="https://www.rainpole.local">https://www.rainpole.local</a>
Contact link	<a href="https://www.rainpole.local/contact">https://www.rainpole.local/contact</a>

## Configure the Default Email Servers

System administrators configure inbound and outbound email servers to handle email notifications about events involving tenants machines. System administrators can create only one inbound email server and one outbound email server. These servers are the defaults for all tenants.

If tenant administrators do not override the default email server settings before they enable notifications, vRealize Automation uses the globally configured email server.

**Procedure**

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 Navigate to **Administration > Email Servers**, and click **New**.
- 3 In the **New Email Server** dialog box, select **Email - Inbound**, and click **OK**.
- 4 On the **New Inbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

Setting	Value
Name	Rainpole-Inbound
Security	Deselected
Protocol	IMAP
Server Name	email.rainpole.local
Server Port	143
Folder Name	INBOX
Processed Email	Deselected
User Name	administrator@rainpole.local
Password	<i>vra_administrator_password</i>
Email Address	svc-vra@rainpole.local

- 5 On the **Email Servers** page, click **New** to configure the outbound server settings.
- 6 In the **New Email Server** dialog box, select **Email - Outbound**, and click **OK**.
- 7 On the **New Outbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

Setting	Value
Name	Rainpole-Outbound
Server Name	email.rainpole.local
Encryption Method	None
Server Port	25
Authentication	Selected
User Name	administrator@rainpole.local

Setting	Value
Password	<i>vra_administrator_password</i>
Sender Address	svc-vra@rainpole.local

8 Log out of vRealize Automation portal.

## Embedded vRealize Orchestrator Configuration

VMware Embedded vRealize Orchestrator is a platform that provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage the VMware vSphere infrastructure and other VMware and third-party technologies.

vRealize Orchestrator is composed of three distinct layers: an orchestration platform that provides the common features required for an orchestration tool, a plug-in architecture to integrate control of subsystems, and a library of workflows. vRealize Orchestrator is an open platform that can be extended with new plug-ins and libraries, and can be integrated into larger architectures through a REST API.

### Configure the Embedded vRealize Orchestrator Service in the vRealize Automation Appliance

To create a highly available Embedded vRealize Orchestrator cluster, configure two vRealize Automation virtual appliances.

Perform this procedure twice to configure two appliances using the respective values in the following table for the different hosts.

vRealize Orchestrator Appliance	IP Address	FQDN
Host A	192.168.11.51	vra01svr01a.rainpole.local
Host B	192.168.11.52	vra01svr01b.rainpole.local

## Procedure

- 1 Log in to the vRealize Automation Appliance by using Secure Shell (SSH) client to configure the embedded vRealize Orchestrator.

- a Open an SSH connection to `vra01svr01a.rainpole.local` using the following credentials.

Setting	Value
User name	root
Password	<i>hostA_root_password</i>

- b Start `vco-configurator` service using the command `service vco-configurator start`.



```
vra01svr01a.rainpole.local - PuTTY
vra01svr01a:~ # service vco-configurator start
Starting tcServer
Using CATALINA_BASE:   /var/lib/vco/configuration
Using CATALINA_HOME:   /opt/pivotal/pivotal-tc-server-standard/tomcat-8.5.4.B.RELEASE
Using CATALINA_TMPDIR: /var/lib/vco/configuration/temp
Using JRE_HOME:        /usr/java/jre-vmware
Using CLASSPATH:       /opt/pivotal/pivotal-tc-server-standard/tomcat-8.5.4.B.RELEASE/bin/bootstrap.jar:/opt/pivotal/pivotal-tc-server-standard/tomcat-8.5.4.B.RELEASE/bin/tomcat-juli.jar
Using CATALINA_PID:    /var/lib/vco/configuration/logs/tcserver.pid
Tomcat started.
Status:                RUNNING as PID=3742
vra01svr01a:~ #
```

- c Verify the status of `vco-configurator` using the command `service vco-configurator status`.



```
vra01svr01a:~ # service vco-configurator status
Status-ing tcServer
Instance name:        configuration
Runtime version:     8.5.4.B.RELEASE
tc Runtime Base:     /var/lib/vco/configuration
Status:              RUNNING as PID=3742
vra01svr01a:~ #
```

- d Run the command `chkconfig vco-configurator on` to enable automatic restart of the `vco-configurator` service upon subsequent reboots of the vRealize Automation appliance.

- 2 Repeat the procedure to configure the vRealize Orchestrator for Host B `vra01svr01b.rainpole.local`.

## Configure Authentication Provider for vRealize Orchestrator

Configure vRealize Orchestrator to use the Rainpole local tenant in vRealize Automation for authentication. By associating vRealize Orchestrator authentication to a non-default tenant, vRealize Orchestrator runs workflows with end-user permissions. If vRealize Orchestrator authenticates using the default tenant, Orchestrator users always have administrative rights.

**Procedure**

- 1 Log in to the vRealize Orchestrator Control Center.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local:8283/vco-controlcenter**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 Configure vRealize Automation as a vRealize Orchestrator authentication provider.
  - a On the **Home** page, under **Manage**, click **Configure Authentication Provider**.
  - b In the **Default Tenant** text box, click the **Change** button, enter **rainpole**, and click **Apply**.
  - c In the **Admin group** text box, enter **ug-vR0** and click **Search**.
  - d From the drop-down menu, select **rainpole.local\ug-vROAdmins** and click **Save Changes**.

The control center logs you out.

- 3 Verify that the role-based access control (RBAC) is enabled in the control center by logging in as svc-vra.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local:8283/vco-controlcenter**.
  - b Log in using the following credentials.

Setting	Value
Domain	rainpole.local
User name	svc-vra
Password	<i>svc-vra_password</i>

- c Log out of the control center.
- 4 Restart the vRealize Orchestrator services.
  - a Open an SSH connection to **vra01svr01a.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>hostA_root_password</i>

- c Run the following commands.

```
service vco-server restart
service vco-configurator restart
```

- d Repeat the steps to restart the services on vra01svr01b.rainpole.local.

- 5 Log back in to the control center as the svc-vra user.

---

**Note** The log in process might be delayed due to the vRealize Orchestrator services restarting.

---

- a Open a Web browser and go to <https://vra01svr01.rainpole.local:8283/vco-controlcenter>.
- b Log in using the following credentials.

Setting	Value
Domain	rainpole.local
User name	svc-vra
Password	svc-vra_password

## Validate the Configuration of vRealize Orchestrator

You can verify that Embedded vRealize Orchestrator is configured properly by opening the **Validate Configuration** page in the Control Center.

### Procedure

- 1 Log in to the Embedded vRealize Orchestrator Control Center.
  - a Open a Web browser and go to <https://vra01svr01.rainpole.local:8283/vco-controlcenter>.
  - b Log in using the following credentials.

Setting	Value
Domain	rainpole.local
User name	svc-vra
Password	svc-vra_password

- 2 On the **Home** page, under **Manage**, click **Validate Configuration**, and verify that all check marks are green.

## Add Compute vCenter Server Instance to Embedded vRealize Orchestrator

Add each vCenter Server instance that contributes resources to vRealize Automation and uses vRealize Orchestrator workflows to allow for communication.

## Procedure

- 1 Download and Install the vRealize Orchestrator Client.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local**.
  - b Click **vRealize Orchestrator Client**.
  - c On the **VMware vRealize Orchestrator Login** page, log in to the Embedded vRealize Orchestrator by using the following hostname and credentials.

Setting	Value
Host name	vra01svr01.rainpole.local:443
User name	svc-vra
Password	svc-vra_password

- 2 In the left pane, click **Workflows**, and navigate to **Library > vCenter > Configuration**.
- 3 Right-click the **Add a vCenter Server instance** workflow, and click **Start Workflow**.
  - a On the **Set the vCenter Server Instance** page, configure the following settings, and click **Next**.

Setting	Value
IP or hostname of the vCenter Server instance to add	sfo01w01vc01.sfo01.rainpole.local
HTTPS port of the vCenter Server instance	443
Location of SDK that you use to connect	/sdk
Will you orchestrate this instance	Yes
Do you want to ignore certificate warnings	Yes

- b On the **Set the connection properties** page, configure the following settings, and click **Submit**.

Setting	Value
Use a session per user	No
vCenter Server user name	rainpole.local\svc-vro
vCenter Server user password	svc-vro_password

- 4 To verify that the workflow completed successfully, click the **Inventory** tab, and expand the **vSphere vCenter Plugin** tree control.

The vCenter Server instance you added is now visible in the inventory.

## Integrate vRealize Orchestrator with vRealize Automation

Configure vRealize Automation to work with the embedded vRealize Orchestrator instance.

### Configure Embedded vRealize Orchestrator Server

To use vRealize Automation workflows to call vRealize Orchestrator workflows, you must configure vRealize Orchestrator to act as an endpoint.

**Procedure**

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 Click **Administration > vRO Configuration > Server Configuration**.
- 3 Select the **Use the default Orchestrator server** radio button and click **Test Connection**.
- 4 Once the **Successfully connected to the Orchestrator server** message appears, click **OK** to complete the configuration.

**Create a vRealize Orchestrator Endpoint**

IaaS administrators are responsible for creating the endpoints that allow vRealize Automation to communicate with your infrastructure. You create a vRealize Orchestrator endpoint for use by Realize Automation to communicate workflows.

**Procedure**

- 1 Log in to the Rainpole Infrastructure Service Portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b From the **Select your domain** drop-down menu, select **Rainpole.local** and click **Next**.
  - c Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	<i>vra-admin-rainpole_password</i>
Domain	rainpole.local

## 2 Create an endpoint for vRealize Orchestrator.

- a Select **Infrastructure > Endpoints > Endpoints**.
- b Click **New > Orchestration > vRealize Orchestrator**, enter the following values, and click **OK** to complete the process.

Setting	Value
Name	vra01svr01.rainpole.local
Address	<a href="https://vra01svr01.rainpole.local/vco">https://vra01svr01.rainpole.local/vco</a>
User name	svc-vra@rainpole.local
Password	svc-vra_password
Priority	1

## 3 Start the data collection for the newly created endpoint.

- a Select the vRealize Orchestrator endpoint in the Endpoints list and click **Actions > Data Collection**.
- b Click **Start** to begin the vRealize Orchestrator data collection process. Wait several minutes for the data collection process to complete.
- c Click **Refresh** to verify that the data collection successfully complete.

When a data collection succeeded status message appears, the configuration process is complete.

## Add vRealize Automation Host in vRealize Orchestrator

To call vRealize Automation Plugin workflows, you configure the vRealize Automation host in vRealize Orchestrator.

### Procedure

- 1 Log in to the vRealize Orchestrator Client.
  - a Open a Web browser and go to <https://vra01svr01.rainpole.local/vco>.
  - b Click **Start Orchestrator Client**.
  - c On the VMware vRealize Orchestrator login page, log in to vRealize Orchestrator using the following hostname and credentials.

Setting	Value
Host name	vra01svr01.rainpole.local:443
User name	svc-vra
Password	svc-vra_password

- 2 In the left pane, click **Workflows**, and navigate to **Library > vRealize Automation > Configuration**.

- 3 Right-click the **Add a vRA host using component registry** workflow and click **Start Workflow**.
  - a On the **Common parameters** page, configure the following settings, and click **Submit**.

Setting	Value
Name of the vCAC host	vra01svr01.rainpole.local
Connection timeout	30.0
Operation timeout	60.0
Maximum page size for objects retrieved from this host	100.0

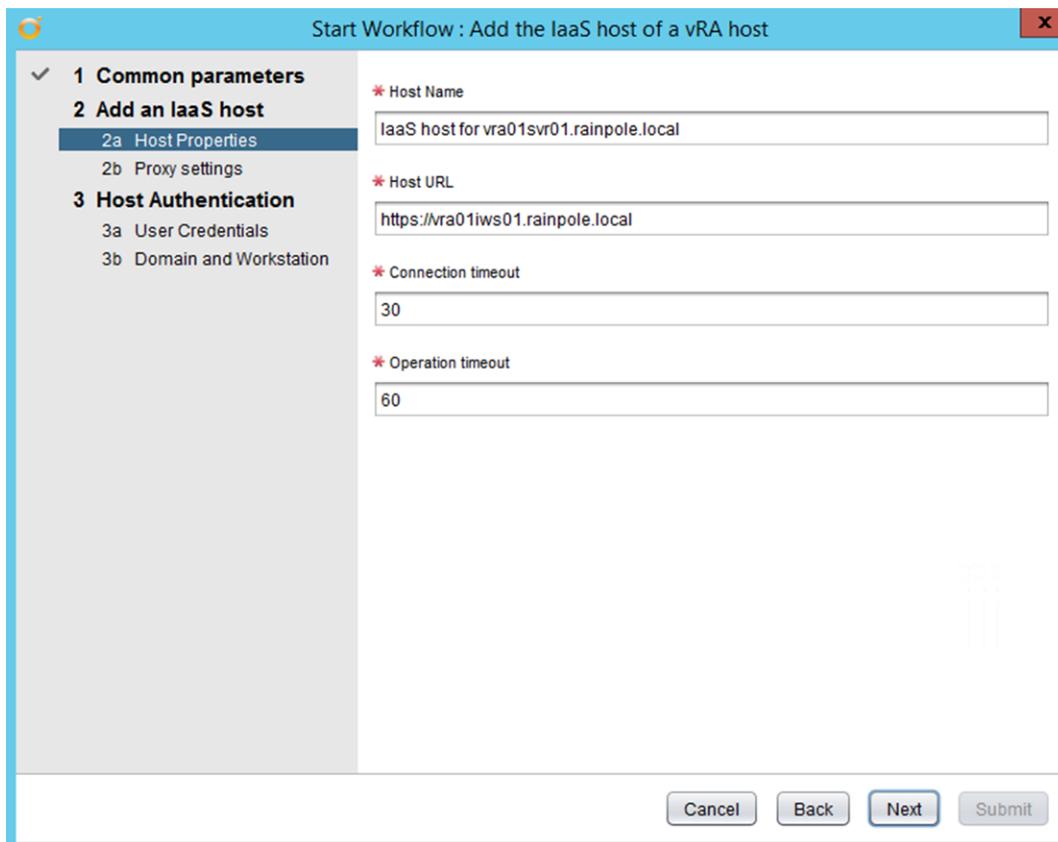
- 4 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vRealize Automation** tree control.

The vRealize Automation Server instance that you just added is visible in the inventory.

- 5 In the left pane, click **Workflows**, and navigate to **Library > vRealize Automation > Configuration**.

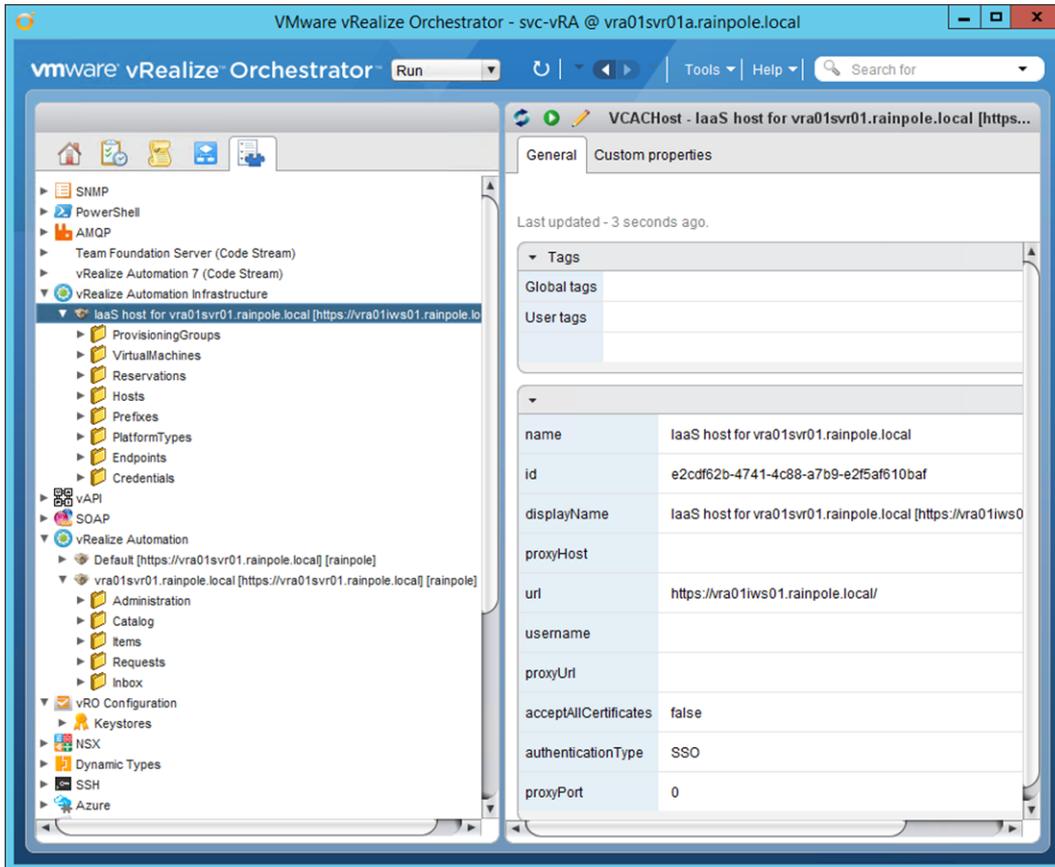
- 6 Right-click the **Add the IaaS host of a vRA host** workflow and click **Start Workflow**.

- a On the **Common parameters** page, click the search icon labelled **Not set**. Select **vra01svr01.rainpole.local [https://vra01svr01.rainpole.local] [rainpole]** for **vCAC host** and click **Next**.
- b On the **Add an IaaS host** page, keep the default settings for **Host Properties**, and click **Next**.



- c On the **Add an IaaS host** page, keep the default settings for the **Proxy Settings**, and click **Next**.
  - d On the **Host Authentication** page, select **SSO** for **Host's authentication type**, and click **Submit**.
- 7 To verify that the workflow completed successfully, click the **Inventory** tab, and expand the **vRealize Automation Infrastructure** tree control.

The vRealize Automation IaaS Server instance you added is visible in the inventory.



## vRealize Business Installation

vRealize Business is an IT financial management tool that provides clarity and control over the costs and quality of IT services, enabling alignment with the business and acceleration of IT transformation.

Install vRealize Business and integrate it with vRealize Automation to continuously monitor the cost of each individual Virtual Machine and the cost of their data center.

The following values are different in a vRealize Suite Lifecycle Manager deployment for sfo01vrbc01.sfo01.rainpole.local.

VMware Validated Design Value	2 GB RAM virtual appliance
Lifecycle Manager Deployed Value	8 GB RAM virtual appliance

## Configure NTP for vRealize Business

Configure the network time protocol (NTP) on the vRealize Business appliances from the virtual appliance management interface (VAMI).

Perform the procedure on both vRealize Business Server and vRealize Business Data Collector virtual appliances.

Host	VAMI URL
Server	<a href="https://vrb01svr01.rainpole.local:5480">https://vrb01svr01.rainpole.local:5480</a>
Data Collector	<a href="https://sfo01vrbc01.sfo01.rainpole.local:5480">https://sfo01vrbc01.sfo01.rainpole.local:5480</a>

### Procedure

- 1 Log in to the vRealize Business Server appliance management console.
  - a Open a Web browser and go to **<https://vrb01svr01.rainpole.local:5480>**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_server_root_password</i>

- 2 Configure the appliance to use a time server.
  - a Click the **Administration** tab and click **Time Settings**.
  - b On the **Time Settings** page, enter the following settings and click **Save Settings**.

Setting	Value
Time Sync. Mode	Use Time Server
Time Server #1	ntp.sfo01.rainpole.local

- 3 Repeat the procedure on the vRealize Business Data Collector virtual appliance `sfo01vrbc01.sfo01.rainpole.local`.

## Integrate vRealize Business with vRealize Automation

To prepare vRealize Business for use, you must register the vRealize Business Server to vRealize Automation by using the management interface.

## Procedure

- 1 Log in to the vRealize Business Server appliance management console.
  - a Open a Web browser and go to **https://vrb01svr01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_server_root_password</i>

- 2 On the **Registration > vRA** subtab, enter the following credentials to register with the vRealize Automation server.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	vsphere.local
SSO Admin User	administrator
SSO Admin Password	<i>vra_administrator_password</i>
Accept "vRealize Automation" certificate	Selected

- 3 Click **Register** to connect to vRealize Automation and get its certificate.  
 A failure message may appear at the top of the page. Wait until the SSO Status changes to The certificate of "vRealize Automation" is not trusted. Please view and accept to register.
- 4 Click the **View "vRealize Automation" certificate** link to download the vRealize Automation certificate.
- 5 Select the **Accept "vRealize Automation" certificate** check box and click **Register**.  
**SSO Status** changes to Connected to vRealize Automation.

## Register the vRealize Business Data Collector with the Server

As part of the vRealize Business installation, you connect the Data Collectors with the vRealize Business Server.

Because the tenant is configured in vRealize Automation, you register the vRealize Business Data Collector appliance with the vRealize Business Server using the following procedure.

- Grant an added role to the tenant admin, enter the product license key, and generate a one-time key from vRealize Automation.
- Register the Data Collector to the vRealize Business Server.

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Navigate to **Administration > Users & Groups > Directory Users and Groups**.
- 3 Generate a one-time use key for connecting the two vRealize Business appliances.
  - a Expand the **Manage Data Collector > Remote Data Collection** section.
  - b Click **Generate a new one time use key**.
  - c Save the one time use key as you need it at a later stage in the implementation sequence.
- 4 Log in to the vRealize Business Data Collector console.
  - a Open a Web browser and go to **https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vrbc_collector_root_password

- 5 Register the Data Collector with the vRealize Business Server.
  - a Expand the **Registration with the vRealize Business Server** section.
  - b Enter the following values and click **Register**.

Setting	Value
Enter the vRB Server Url	https://vrbc01svr01.rainpole.local
Enter the One Time Key	one_time_use_key

After you click **Register**, a warning message informs you that the certificate is not trusted.

- c Click **Install** and click **OK**.

The vRealize Business appliances are now connected.

## Replace the SSL Certificate on vRealize Business Server

Replace the default or existing SSL certificate of vRealize Business with a new one using the vRealize Business appliance management console. This certificate is used when you access the Web interface of the vRealize Business server.

## Procedure

- 1 Log in to the vRealize Business Server appliance management console.
  - a Open a Web browser and go to **https://vrb01svr01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_server_root_password</i>

- 2 Click the **Administration** tab and click **SSL**.
- 3 On the **Replace SSL Certificate** page, upload the certificate files that you previously generated for vRealize Business and click **Replace Certificate**.

Use the *vrb.key* file as the **RSA Private Key (.key)** and the *vrb.3.pem* file for the **Certificate(s) (.pem)** entry. These files are in the *vrb* folder that you created during certificate generation.

Setting	Value
Choose mode	Import PEM encoded Certificate
RSA Private Key (.key)	<pre>-----BEGIN RSA PRIVATE KEY----- private_key_value -----END RSA PRIVATE KEY-----</pre>
Certificate(s) (.pem)	<pre>-----BEGIN CERTIFICATE----- Server_certificate_value -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- Intermediate_CA -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- Root_CA_certificate_value -----END CERTIFICATE-----</pre>
Private Key Passphrase	<i>vrb_cert_passphrase</i>

A message that the SSL certificate was successfully configured appears.

- 4 Click the **System** tab and click **Reboot** for the changes to take effect.

## Connect vRealize Business with the Compute vCenter Server

vRealize Business requires a connection with the vCenter Server to collect data from the entire cluster. You add the vCenter Server to vRealize Business by using the vRealize Business Data Collector console.

## Procedure

- 1 Log in to the vRealize Business Data Collector console.
  - a Open a Web browser and go to **https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_collector_root_password</i>

- 2 Click **Manage Private Cloud Connections**, select **vCenter Server**, and click the **Add** icon.
- 3 In the **Add vCenter Server Connection** dialog box, enter the following settings, and click **Save**.

Setting	Value
Name	sfo01w01vc01.sfo01.rainpole.local
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
Username	svc-vra@rainpole.local
Password	<i>svc_vra_password</i>

- 4 In the **SSL Certificate warning** dialog box, click **Install**.
- 5 In the **Success** dialog box, click **OK**.

## Cloud Management Platform Post-Installation Tasks

After you deploy vRealize Automation and vRealize Orchestrator, you enable health monitors to check the health status of individual servers, and remove the snapshots created during the vRealize Automation installation.

### Create VM Groups to Define the Startup Order of the Cloud Management Platform

VM Groups allow you to define the startup order of virtual machines. The startup order you define ensures that vSphere HA powers on virtual machines in the correct order.

## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, select **Host and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.
- 3 Create a VM Group for the vRealize Automation IaaS Database.
  - a Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.
  - b On the **Configure** page, click **VM/Host Groups**.
  - c On the **VM/Host Groups** page, click the **Add** button.
  - d In the **Create VM/Host Group** dialog box, enter **vRealize Automation IaaS Database** in the **Name** field, select **VM Group** from the **Type** drop-down menu, and click the **Add** button.
  - e In the **Add VM/Host Group Member** dialog box, select **vra01mssql01** and click **OK**.
  - f Click **OK** to save the VM/Host Group.
- 4 Repeat *Step 3* to create the following VM/Host Groups.

VM/Host Group Name	VM/Host Group Member
vRealize Automation Virtual Appliances	vra01svr01a
	vra01svr01b
vRealize Automation IaaS Web Servers	vra01iws01a
	vra01iws01b
vRealize Automation IaaS Managers	vra01ims01a
	vra01ims01b
vRealize Automation IaaS DEM Workers	vra01dem01a
	vra01dem01b
vRealize Automation IaaS Proxy Agents	sfo01ias01a
	sfo01ias01b
vRealize Business Servers	vr01svr01
vRealize Business Remote Collectors	sfo01vrbc01

- 5 Create a rule to power on the vRealize Automation Database before the vRealize Automation Virtual Appliances.
  - a Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.
  - b On the **Configure** page, click **VM/Host Rules**.
  - c On the **VM/Host Rules** page, click the **Add** button.
  - d In the **Create VM/Host Rule** dialog box, enter **SDDC Cloud Management Platform 01** in the **Name** text box, ensure the **Enable Rule** check box is selected, and select **Virtual Machines to Virtual Machines** from the **Type** drop-down menu.
  - e Select **vRealize Automation IaaS Database** from the **First restart VMs in VM group** drop-down menu.
  - f Select **vRealize Automation Virtual Appliances** from the **Then restart VMs in VM group** drop-down menu, and click **OK**.
- 6 Repeat *Step 5* to create the following VM/Host Rules to ensure the correct restart order for your Cloud Management Platform.

VM/Host Rule Name	First restart VMs in VM group	Then restart VMs in VM group
SDDC Cloud Management Platform 02	vRealize Automation Virtual Appliances	vRealize Automation IaaS Web Servers
SDDC Cloud Management Platform 03	vRealize Automation IaaS Web Servers	vRealize Automation IaaS Managers
SDDC Cloud Management Platform 04	vRealize Automation IaaS Managers	vRealize Automation IaaS DEM Workers
SDDC Cloud Management Platform 05	vRealize Automation IaaS Managers	vRealize Automation IaaS Proxy Agents
SDDC Cloud Management Platform 06	vRealize Automation IaaS Managers	vRealize Business Servers
SDDC Cloud Management Platform 07	vRealize Business Servers	vRealize Business Remote Collectors

## Enable Load Balancer Health Monitoring

Previously you disabled health monitoring for the **sfo01m01lb01** load balancer to complete configuration of vRealize Automation. You may now re-enable health monitoring for the **sfo01m01lb01** load balancer.

Perform this procedure multiple times to configure the health monitor and to enable the second member for the server pools as described in the following table.

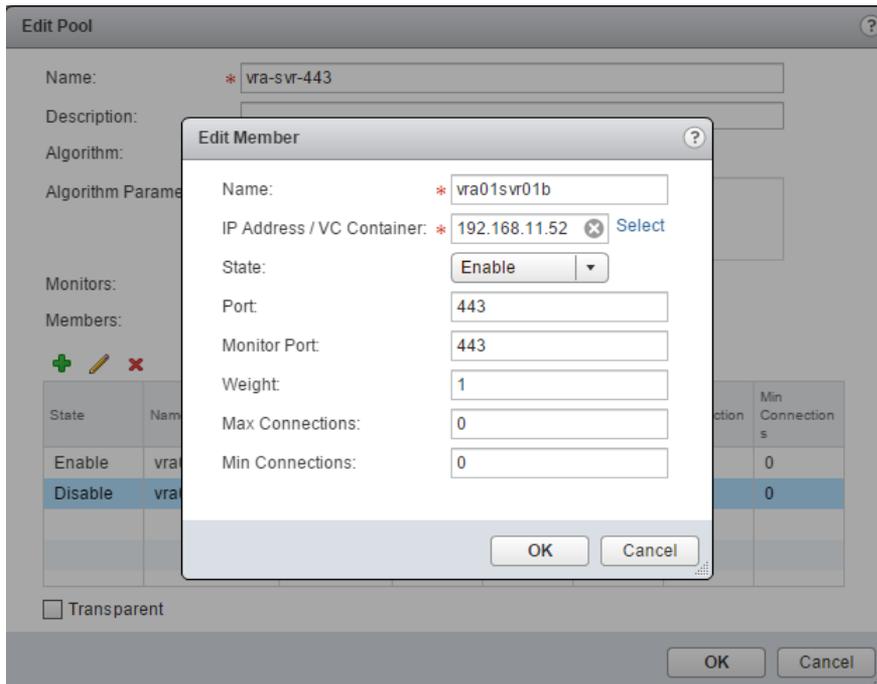
Pool Name	Monitor	Enable Pool Member
vra-svr-443	vra-svr-443-monitor	vra01svr01b
vra-iws-443	vra-iws-443-monitor	vra01iws01b
vra-ims-443	vra-ims-443-monitor	vra01ims01b
vra-svr-8444	vra-svr-443-monitor	vra01svr01b
vra-vro-8283	vra-vro-8283-monitor	vra01svr01b

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking & Security**, and select **NSX Edges**.
- 3 Select **172.16.11.65** from the **NSX Manager** drop-down menu, and double-click **sfo01m01b01** to edit its settings.
- 4 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.
- 5 From the pools table, select the **vra-svr-443** server pool, and click **Edit** icon.
- 6 In the **Edit Pool** dialog box, configure the monitor, and enable the member that is not enabled.
  - a From the **Monitors** drop-down menu, select **vra-svr-443-monitor**.
  - b From the **Members** table, select **vra01svr01b** and click **Edit** icon.
  - c In the **Edit Member** dialog box, from the **State:** drop-down menu, select **Enable** and click **OK**.
  - d Click **OK** to close the **Edit Pool** dialog box.



- 7 Repeat the procedure to configure the health monitor and enable the second member for the remaining server pools.
- 8 Click **Show Pool Statistics** and make sure all the server pools **Status** show as **UP**.

## Clean up the vRealize Automation VM Snapshots

You made snapshots of each vRealize virtual machine during the vRealize Automation installation process. After you successfully complete the installation, you can delete these snapshots.

Repeat this procedure to remove all the vRealize Automation virtual machine snapshots you created during the implementation. The virtual machine names and their respective folders are listed in the following table.

Virtual Machines	vCenter Folder
vra01svr01a	sfo01-m01fd-vra
vra01svr01b	sfo01-m01fd-vra
vra01mssql01	sfo01-m01fd-vra
vra01iws01a	sfo01-m01fd-vra
vra01iws01b	sfo01-m01fd-vra
vra01ims01a	sfo01-m01fd-vra
vra01ims01b	sfo01-m01fd-vra
vra01dem01a	sfo01-m01fd-vra
vra01dem01b	sfo01-m01fd-vra
sfo01ias01a	sfo01-m01fd-vraias
sfo01ias01b	sfo01-m01fd-vraias

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** page, click **VMs and Templates**.
- 3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** folder.
- 4 Right-click the **vra01dem01a** VM and select **Snapshots > Manage Snapshots**.
- 5 Select the **Prior to vRA IaaS Component Installation** snapshot and click the **Delete** icon.

- 6 Repeat this procedure to remove all the remaining vRealize Automation virtual machine snapshots.

## Content Library Configuration

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

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

### Configure a Content Library in the First Compute vCenter Server Instance

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 of the templates in your environment are consistent.

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

#### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** page, click **Content Libraries** and click the **Create a new content library** icon. The **New Content Library** wizard opens.
- 3 On the **Name** page, specify the following settings and click **Next**.

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

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

Setting	Value
Local content library	Selected
Publish externally	Selected
Enable authentication	Selected
Password	<i>sfo01-w01cl-vra01_password</i>
Confirm password	<i>sfo01-w01cl-vra01_password</i>

- 5 On the **Add storage** page, click the **Select a datastore** radio button, select the **sfo01-w01-lib01** datastore to store the content library, and click **Next**.
- 6 On the **Ready to complete** page, click **Finish**.

## Import the OVF Files for the Virtual Machine Templates

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

You repeat this procedure three times to import the virtual machine templates listed in [Table 6-2](#).

**Table 6-2. VM Templates to Import**

VM Template Name	Description
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)

### Prerequisites

Verify that you have prepared the OVF templates, as specified in the *Virtual Machine Template Specifications* section.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 From the **Home** page, click **Content Libraries** and click the **Objects** tab.

- 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 **OK**.

Setting	Value
Source file	redhat6-enterprise-64.ovf
Item name	redhat6-enterprise-64
Notes	Red Hat Enterprise Server 6 (64-bit)

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

## Tenant Content Creation

To provision virtual machines in the Compute vCenter Server, you must configure the tenant to use compute resources within vCenter Server.

### Prerequisites

- Verify that a vCenter Server cluster has been deployed and configured. See
- Verify that an NSX instance has been configured for use by the vCenter Server cluster.
- Proxy agents have been deployed.

## Create Logical Switches for Business Groups

For each vCenter Server compute instance, you create three logical switches for each business group which simulate networks for the web, database, and application tiers.

You repeat this procedure six times to create six logical switches.

**Table 6-3. Logical Switch Names and Descriptions**

Logical Switch Name	Description
Production-Web-VXLAN	Logical switch for the Web tier of Product Business Group
Production-DB-VXLAN	Logical switch for the Database tier of Product Business Group
Production-App-VXLAN	Logical switch for the Application tier of Product Business Group
Development-Web-VXLAN	Logical switch for the Web tier of Development Business Group
Development-DB-VXLAN	Logical switch for the Database tier of Development Business Group
Development-App-VXLAN	Logical switch for the Application tier of Development Business Group

## Procedure

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

- a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Create a logical switch.

- a Click **Networking & Security**.
- b In the Navigator, select **Logical Switches**.
- c From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager.
- d Click the **New Logical Switch** icon.

The **New Logical Switch** dialog box appears.

- e In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Production-Web-VXLAN
Description	Logical switch for Web tier of Production Business Group
Transport Zone	Comp Universal Transport Zone
Replication Mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

3 Repeat this procedure to create the remaining logical switches.

## Configure User Roles in vRealize Automation

You assign user roles in the context of a specific tenant. However, some roles for the default tenant can manage system-wide configuration settings that apply to multiple tenants.

Roles are sets of privileges that you associate with users to determine what tasks they can perform. Based on their responsibilities, individuals might have one or more roles associated with their user account.

You assign tenant architect and administrator roles to the **ug-vra-admins-rainpole** and **ug-vra-archs-rainpole** user groups.

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 On the **Administration** tab, navigate to **Users & Groups > Directory Users and Groups**.
- 3 Enter **ug-vra-admins-rainpole** in the search box and press Enter.  
The ug-vra-admins-rainpole (ug-vra-admins-rainpole@rainpole.local) group name appears in the **Name** text box.
- 4 Click the **ug-vra-admins-rainpole (ug-vra-admins-rainpole@rainpole.local)** user group.
- 5 In the **Add Roles to this Group** list, select the following roles, and click **Finish**.
  - Application Architect
  - Approval Administrator
  - Business Management Administrator
  - Catalog Administrator
  - Container Administrator
  - Container Architect
  - Infrastructure Architect
  - Software Architect
  - Tenant Administrator
  - XaaS Architect
- 6 Search for **ug-vra-archs-rainpole** in the **Tenant Administrators** search box .  
The ug-vra-archs-rainpole (ug-vra-archs-rainpole@rainpole.local) group appears in the **Name** text box.
- 7 Click the **ug-vra-archs-rainpole (ug-vra-archs-rainpole@rainpole.local)** user group.
- 8 In the **Add Roles to this Group** list, select the following user groups, and click **Finish**.
  - Application Architect
  - Container Architect
  - Infrastructure Architect

- Software Architect
- XaaS Architect

## Create Fabric Groups

IaaS administrators can organize virtualization compute resources and cloud endpoints into fabric groups by type and intent. One or more fabric administrators manage the resources in each fabric group.

Fabric administrators are responsible for creating reservations on the compute resources in their groups to allocate fabric resources to specific business groups. Fabric groups are created in a specific tenant, but their resources can be made available to users who belong to business groups in all tenants.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Select **Infrastructure > Endpoints > Fabric Groups**.
- 3 Click **New Fabric Group**, enter the following settings, and click **OK**.

Setting	Value
Name	SFO Fabric Group
Fabric administrators	ug-vra-admins-rainpole@rainpole.local

---

**Note** You have not yet configured a vCenter Endpoint, so no compute resource is available for you to select. You configure the vCenter Endpoint later.

---

- 4 Log out of the vRealize Automation portal and close your browser.

## 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 to be followed by a counter of a specified number of digits. When the digits are all used, vRealize Automation rolls back to the first number.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Select **Infrastructure > Administration > Machine Prefixes**.
- 3 Click the **New** icon to create a default machine prefix for the Production group using the following settings, and click the **Save** icon.

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

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

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

## Create Business Groups

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

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

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Navigate to **Administration > Users and Groups > Business Groups**.
- 3 Click the **New** icon.
- 4 On the **General** tab, enter the following values and click **Next**.

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

- 5 On the **Members** tab, enter **ug-vra-admins-rainpole.local** in the **Group manager role** text box, and click **Next**.
- 6 On the **Infrastructure** tab, select **Prod-** from the **Default machine prefix** drop-down menu and click **Finish**.
- 7 Click the **New** icon.
- 8 On the **General** tab, configure the following values, and click **Next**.

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

- 9 On the **Members** tab, enter **ug-vra-admins-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

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

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

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

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

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

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

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

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

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

## Create a vSphere Endpoint in vRealize Automation

As an IaaS administrator, to allow vRealize Automation to manage the infrastructure, create endpoints and configure user credentials for those endpoints. When you create a vSphere Endpoint, vRealize Automation can communicate with the vSphere environment and discover vCenter Server-managed compute resources, collect data, and provision machines.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Navigate to **Infrastructure > Endpoints > Endpoints**, and click **New > Virtual > vSphere (vCenter)**.
- 3 On the **New Endpoint - vSphere (vCenter)** page, create a vSphere Endpoint with the following settings, and click **Test Connection**.

Setting	Value
Name	sfo01m01vc01.sfo01.rainpole.local
Address	https://sfo01m01vc01.sfo01.rainpole.local/sdk
User Name	rainpole\svc-vra
Password	svc-vra_password

**Note** The vSphere Endpoint name must be the same as the endpoint name configured during the installation of the vRealize Automation environment. See the *VMware Validated Design Deployment for Region A* documentation.

- 4 If a **Security Alert** window appears, click **OK**.
- 5 Click **OK** to create the Endpoint.

## Create an NSX Endpoint in vRealize Automation

When you create an endpoint for NSX for the shared edge and compute cluster, vRealize Automation can communicate with NSX Manager to discover networking resources.

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Navigate to **Infrastructure > Endpoints > Endpoints** and click **New > Network and Security > NSX**.
- 3 On the **General** page, configure the vRealize Automation Endpoint with the following settings.

Setting	Value
Name	SFO-NSXEndpoint
Address	https://sfo01w01nsx01.sfo01.rainpole.local
User Name	rainpole\svc-vra
Password	svc_vra_password

- 4 Click **Test Connection**.
- 5 Click the **Associations** tab, click **New**, select **sfo01w01vc01.sfo01.rainpole.local** from the **Name** drop-down menu, and click **OK**.
- 6 If a **Security Alert** window appears, click **OK**.
- 7 Click **OK**.

## Add Compute Resources to a Fabric Group

You allocate compute resources to fabric groups so that vRealize Automation can use the resources in that compute resource for that fabric group when provisioning virtual machines.

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Navigate to **Infrastructure > Endpoints > Fabric Groups**.
- 3 In the **Name** column, point to the fabric group name **SFO Fabric Group**, and click **Edit**.
- 4 On the **Edit Fabric Group** page, select **sfo01-w01-comp01** from the **Compute resources** table, and click **OK**.

---

**Note** It might take several minutes for vRealize Automation to connect to the Compute vCenter Server system and associated clusters. If you are unable to see the compute cluster after sufficient time has passed, restart both proxy agent services in the virtual machines `sfo01ias01a.sfo01.rainpole.local` and `sfo01ias01b.sfo01.rainpole.local`.

---

- 5 Navigate to **Infrastructure > Compute Resources > Compute Resources**.
- 6 In the **Compute Resource** column, point to the compute cluster **sfo01-w01-comp01**, and click **Data Collection**.
- 7 Click the **Request now** buttons in each field on the page.  
Wait a few seconds for the data collection process to complete.
- 8 Click **Refresh**, and verify that **Status** for both **Inventory** and **Network and Security Inventory** shows **Succeeded**.

## 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 external network profiles.

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

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to <https://vra01svr01.rainpole.local/vcac/org/rainpole>.
  - b Log in using the following credentials.

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

- 2 Navigate to **Infrastructure > Reservations > Network Profiles**, and click **New > External**.
- 3 On the **New Network Profile - External** page, specify the network profiles on the **General** tab.
  - a Add the values for the Production Group External Network Profile.

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

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

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

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

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

- 5 Click the **Network Ranges** tab.

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

a Enter the following values for Production Business Network Range.

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 Production Group	Static IP range for DB Tier of Production Group	Static IP range for App Tier of 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 Enter the following values for Development Business Network Range.

Setting	Development Web Value	Development DB Value	Development App Value
Name	Development-Web	Development-DB	Development-App
Description	Static IP range for Web Tier of Development Group	Static IP range for DB Tier of Development Group	Static IP range for App Tier of 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.

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

8 Repeat this procedure to create additional external network profiles.

When all the network profiles have been added, the **Network Profiles** page displays six 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.

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

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

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

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

Setting	Production 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

- 4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.
  - a Select **sfo01-w01-comp01(sfo01w01vc01.sfo01.rainpole.local)** from the **Compute resource** drop-down menu.
  - b In the **This Reservation** column of the **Memory (GB)** table, enter **200**.
  - c In the **Storage (GB)** table, select the check box for your primary datastore, for example, **sfo01-w01-vsan01**, enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
  - d Select **sfo01-w01rp-user-vm** from the **Resource pool** drop-down menu.
- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

- 6 On 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
vxx-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxx-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxx-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
vxx-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxx-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxx-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App

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

## Create Reservations for the User Edge Resources

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

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

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

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
- a Open a Web browser and go to **<https://vra01svr01.rainpole.local/vcac/org/rainpole>**.
- b Log in using the following credentials.

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

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

Setting	Production Group Value	Development Group Value
Name	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 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.
  - a Select **sfo01-w01-comp01(sfo01w01vc01.sfo01.rainpole.local)** from the **Compute resource** drop-down menu.
  - b Enter **200** in the **This Reservation** column of the **Memory (GB)** table.
  - c In the **Storage (GB)** table, select the check box for your primary datastore, for example, **sfo01-w01-vsan01**, enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
  - d Select **sfo01-w01rp-user-edge** from the **Resource pool** drop-down menu.
- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.
- 6 On the **Network** tab, select the 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.

Production Business Group

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

Development Business Group

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

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

- 8 Repeat the procedure to create an Edge reservation for the Development Business Group.

## Create Blueprint Customization Specifications in Compute vCenter Server

Create two customization specifications, one for Linux and one for Windows, for use by the virtual machines you deploy. Customization specifications are XML files that contain system configuration settings for the guest operating systems used by virtual machines. When you apply a specification to a guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

You will later use the customization specifications you create when you create blueprints for use with vRealize Automation.

### Create a Customization Specification for Linux Blueprints

Create a Linux guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

#### Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > Policies and Profiles > Customization Specification Manager**.
- 3 Select the vCenter Server **sfo01w01vc01.sfo01.rainpole.local** from the drop-down menu.
- 4 Click the **Create a new specification** icon.
 

The **New VM Guest Customization Spec** wizard appears.
- 5 On the **Specify Properties** page, select **Linux** from the **Target VM Operating System** drop-down menu, enter **os-linux-custom-spec** for the **Customization Spec Name**, and click **Next**.
- 6 On the **Set Computer Name** page, select **Use the virtual machine name**, enter **sfo01.rainpole.local** in the **Domain Name** text box, and click **Next**.

- 7 On the **Time Zone** page, specify the time zone as shown in the following table for the virtual machine, and click **Next**.

Setting	Value
Area	America
Location	Los Angeles
Hardware Clock Set To	Local Time

- 8 On the **Configure Network** page, click **Next**.
- 9 On the **Enter DNS and domain settings** page, leave the default settings, and click **Next**.
- 10 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

## Create a Customization Specification for Windows Blueprints

Create a Windows guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

### Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > Policies and Profiles > Customization Specification Manager**.
- 3 Select the vCenter Server **sfo01w01vc01.sfo01.rainpole.local** from the drop-down menu.
- 4 Click the **Create a new specification** icon.  
The **New VM Guest Customization** wizard appears.
- 5 On the **Specify Properties** page, select **Windows** from the **Target VM Operating System** drop-down menu, enter **os-windows-joindomain-custom-spec** for the **Customization Spec Name**, and click **Next**.
- 6 On the **Set Registration Information** page, enter **Rainpole** for the virtual machine owner's **Name** and **Organization**, and click **Next**.

- 7 On the **Set Computer Name** page, select **Use the virtual machine name**, and click **Next**.

The operating system uses this name to identify itself on the network.

- 8 On the **Enter Windows License** page, provide licensing information for the Windows operating system, enter the *volume\_license\_key*, and click **Next**.

- 9 Specify the administrator password for use with the virtual machine, and click **Next**.

- 10 On the **Time Zone** page, select **(GMT-08:00) Pacific Time(US & Canada)**, and click **Next**.

- 11 On the **Run Once** page, click **Next**.

- 12 On the **Configure Network** page, click **Next**.

- 13 On the **Set Workgroup or Domain** page, select **Windows Server Domain**, configure the following settings, and click **Next**.

Setting	Value
Windows Server Domain	sfo01.rainpole.local
Username	svc-domain-join@rainpole.local
Password	svc-domain-join_password

- 14 On the **Set Operating System Options** page, select **Generate New Security ID (SID)**, and click **Next**.

- 15 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

## Create Virtual Machines Using VM Templates in the Content Library

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

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

VM Template Name	Guest OS
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)

## Procedure

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

a Open a Web browser and go to

**`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`** .

b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Navigate to **Home > 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 Create a new folder and label it **VM Templates**.

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

7 Click **> Templates**.

8 Right-click the VM Template **redhat6-enterprise-64** and click **New VM from This Template**.

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

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

---

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

---

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

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

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 and select **Thin Provision** from the **Select virtual disk format** drop-down menu.

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

---

**Note** vRealize Automation will change the network according to the blueprint configuration.

---

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

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

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

## Convert Virtual Machines to VM Templates

You need to 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. The table below lists the VM Templates and the guest OS that each template uses to create a virtual machine.

VM Template Name	Guest OS
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)

### Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > VMs and Templates**.
- 3 In the **Navigator** pane, expand **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01dc > VM Templates**.
- 4 Right-click the **redhat6-enterprise-64** virtual machine located in the VM Templates folder, and click **Template > Convert to Template**.
- 5 Click **Yes** to confirm the template conversion.
- 6 Repeat this procedure for all of 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 a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

### 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 using the following credentials.

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

- 2 Navigate to the **Administration** tab, click **Catalog Management > Services**, and click **New**.  
The **New Service** page appears.
- 3 In the **New Service** page, configure the following settings and click **OK**.

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

**Create a Single Machine Blueprint**

Create a blueprint for cloning the windows-2012r2-64 virtual machine template using the specified resources on the Compute vCenter Server. Tenants can later use this blueprint for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Repeat this procedure to create the following six blueprints.

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2012 R2 - SFO Prod	windows-2012r2-64 (sfo01m01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Production-Policy
Windows Server 2012 R2 - SFO Dev	windows-2012r2-64 (sfo01m01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Development-Policy

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2012 R2 With SQL2012 - SFO Prod	windows-2012r2-64-sql2012(sfo01m01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Production-Policy
Windows Server 2012 R2 With SQL2012 - SFO Dev	windows-2012r2-64-sql2012(sfo01m01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Development-Policy
Redhat Enterprise Linux 6 - SFO Prod	redhat6-enterprise-64(sfo01m01vc01.sfo01.rainpole.local)	os-linux-custom-spec	SFO-Production-Policy
Redhat Enterprise Linux 6 - SFO Dev	redhat6-enterprise-64(sfo01m01vc01.sfo01.rainpole.local)	os-linux-custom-spec	SFO-Development-Policy

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

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

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

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

Setting	Default
ID	Default setting (vSphere_vCenter_Machine_1)
Description	Default setting (blank)
Display location on request	Deselected

Setting	Default
Reservation policy	SFO-Production-Policy
Machine prefix	Use group default
Instances: Minimum	Default setting
Instances: Maximum	Default setting

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

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	os-windows-joindomain-custom-spec

**Note** If the value of the **Clone from** setting does not list **windows-2012r2-64** template, you must perform a data collection on the **sfo01-w01-comp01** Compute Resource.

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

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

9 Click the **Network** tab.

- a Select **Network & Security** in the **Categories** section to display the list of available network and security components.
- b Select the **Existing Network** component and drag it onto the design canvas.
- c Click in the **Existing network** text box and select the **Ext-Net-Profile-Production-Web** network profile.

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

d Click **Save**.

- e Select the **vSphere\_vCenter\_Machine** object from the design canvas.
- f Select the **Network** tab, click **New**, and configure the following settings. Click **OK**.

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

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

10 Select the blueprint **Windows Server 2012 R2 - SFO Prod** and click **Publish**.

11 Repeat this procedure to create additional blueprints.

### Create Entitlements for Business Groups

You add a service, catalog item, or action to an entitlement, allowing 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 twice to create entitlements for both the Production and Development business groups.

Entitlement Name	Status	Business Group	User & Groups
Prod-SingleVM-Entitlement	Active	Production	ug-vra-admins-rainpole
Dev-SingleVM-Entitlement	Active	Development	ug-vra-admins-rainpole

#### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

2 Click the **Administration** tab, and click **Catalog Management > Entitlements**.

3 Click **New**.

The **New Entitlement** page appears.

4 On the **New Entitlement** page, select the **Details** tab, configure the following values, and click **Next**.

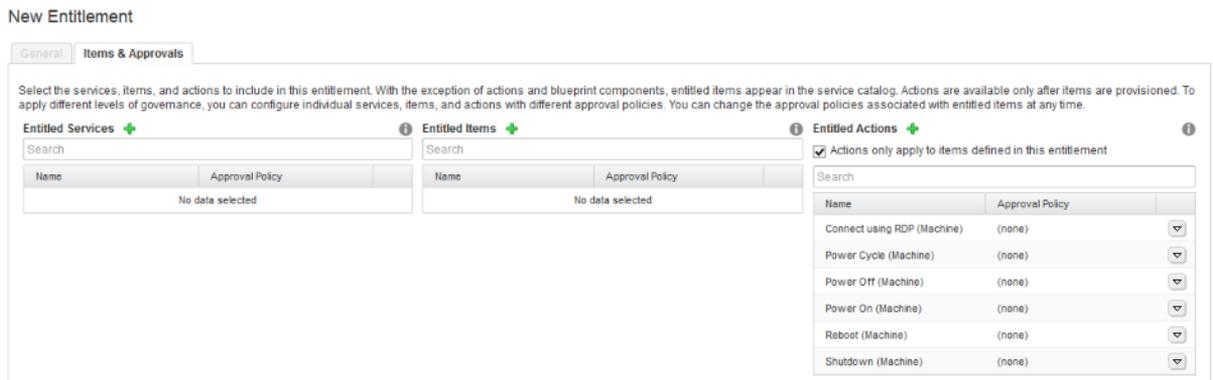
Setting	Production Value	Development Value
Name	Prod-SingleVM-Entitlement	Dev-SingleVM-Entitlement
Description	Default setting (blank)	Default setting (blank)
Expiration Date	Default setting (blank)	Default setting (blank)
Status	Active	Active
Business Group	Production	Development
All Users and Groups	Unselected	Unselected
Users & Groups	ug-vra-admins-rainpole	ug-vra-admins-rainpole

5 Click the **Items & Approvals** tab.

a On the **Entitlement Actions** page, click the **Add Action** 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**.



6 Repeat this procedure to create an entitlement for the Development business group.

Use the same Entitled Actions as for the Production business group.

## Configure Entitlements for Blueprints

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

Repeat this procedure to associate the blueprints with their entitlement.

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

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to <https://vra01svr01.rainpole.local/vcac/org/rainpole>.
  - b Log in using the following credentials.

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

- 2 Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.
- 3 On the **Catalog Items** pane, select the **Windows Server 2012 R2 - SFO Prod** blueprint in the **Catalog Items** list and click **Configure**.
- 4 On the **General** tab of the **Configure Catalog Item** dialog box, select **SFO Service Catalog** from the **Service** drop-down menu, and click **OK**.
- 5 Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement.
  - a Click **Entitlements** and select **Prod-SingleVM-Entitlement**.  
The **Edit Entitlement** pane appears.
  - b Select the **Items & Approvals** tab, add the **Windows Server 2012 R2 - SFO Prod** blueprint to the **Entitled Items** list, and click **OK**.
  - c Click **Finish**.
- 6 Select the **Catalog** tab and verify that the blueprints are listed in the Service Catalog.
- 7 Repeat this procedure to associate all the blueprints with their entitlements.

### Test the Deployment of a Single Machine Blueprint

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

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Select the **Catalog** tab, and click **SFO Service Catalog** from the catalog of available services.
- 3 Click the **Request** button for the **Windows Server 2012 R2 - SFO Prod** blueprint.
- 4 Click **Submit**.
- 5 Verify the request finishes successfully.
  - a Select the **Requests** tab.
  - b Select the request you submitted and wait several minutes for the request to complete.  
Click the **Refresh** icon every few minutes until a Successful message appears under **Status**.
  - c Click **View Details**.
  - d Under **Status Details**, 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/vsphere-client**.
  - b Log in using the following credentials.

Option	Description
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c Select **Home > VMs and Templates**.
- d In the Navigator panel, expand the vCenter Server cluster **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01-comp01 > sfo01-w01rp-user-vm**, and verify the existence of the virtual machine.

# Post-Deployment Tasks for vRealize Operations Manager

# 7

After you deploy vRealize Operations Manager with vRealize Suite Lifecycle Manager, you perform post-deployment tasks to complete the configuration.

## Procedure

### 1 [Configure the Load Balancer for vRealize Operations Manager](#)

Configure load balancing for the analytics cluster on the dedicated NSX Edge services gateway. The remote collector group does not require load balancing.

### 2 [Move vRealize Operations Analytics Cluster and Remote Collector Nodes to Virtual Machine Folders](#)

Use the vSphere Web Client to move the vRealize Operations analytics cluster nodes and remote collectors nodes to virtual machine folders for organization and ease of management.

### 3 [Configure DRS Anti-Affinity Rules for vRealize Operations Manager](#)

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run both the virtual machines of the analytics cluster and of the remote collectors on different hosts in the management cluster.

### 4 [Proceed Using Evaluation Mode for vRealize Operations Manager](#)

When you deploy vRealize Operations Manager with vRealize Suite Lifecycle Manager, the license is applied to the product. You can therefore use evaluation mode instead of applying a new license.

### 5 [Replace vRealize Operations Manager Certificate](#)

Use the PEM file that is generated using the CertGenVVD utility to replace the current certificate on the vRealize Operations Manager administrator user interface. You reconnect vRealize Automation to vRealize Operations Manager to update the certificate in the workload reclamation connection.

### 6 [Group Remote Collector Nodes](#)

### 7 [Add an Authentication Source for the Active Directory](#)

Connect vRealize Operations Manager to the Active Directory of the SDDC for central user management and access control.

### 8 [Configure User Access in vSphere for Integration with vRealize Operations Manager](#)

### 9 [Add vCenter Adapter Instances to vRealize Operations Manager](#)

**10 Connect vRealize Operations Manager to the NSX Manager Instances**

Install and configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in the clusters in the region and view the vSphere hosts in the NSX transport zones.

**11 Connect vRealize Operations Manager to vRealize Automation**

Configure the vRealize Operations Manager Management Pack for vRealize Automation to monitor the health and capacity risk of your cloud infrastructure in the context of the tenant's business groups.

**12 Connect vRealize Operations Manager with vRealize Business**

Configure the vRealize Operations Manager Management Pack for vRealize Business to view your infrastructure performance, cost information, and troubleshooting tips. You can connect vRealize Operations Manager to a single instance of vRealize Business for Cloud.

**13 Enable Storage Device Monitoring in vRealize Operations Manager**

Install and configure the vRealize Operations Management Pack for Storage Devices to view the storage topology in the SDDC and to monitor the capacity and problems on storage components.

**14 Enable vSAN Monitoring in vRealize Operations Manager**

Configure the vRealize Operations Management Pack for vSAN to view the vSAN topology, and to monitor the capacity and problems.

**15 Configure Email Alerts for vRealize Operations Manager**

You configure email notifications in vRealize Operations Manager so that users and applications receive the administrative alerts from vRealize Operations Manager about certain situations in the data center.

## Configure the Load Balancer for vRealize Operations Manager

Configure load balancing for the analytics cluster on the dedicated NSX Edge services gateway. The remote collector group does not require load balancing.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.

- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** and double-click the **sfo01m01lb01** NSX Edge to open its network settings.
- 5 Configure the VIP address for load balancing for the analytics cluster.
  - a On the **Manage** tab, click the **Settings** tab and click **Interfaces**.
  - b Select the **OneArmLB** interface and click **Edit**.
  - c In the **Edit NSX Edge Interface** dialog box, click the **Edit** and in the **Secondary IP Addresses** text box enter the **192.168.11.35** VIP address.
  - d Click **OK** to save the configuration.
- 6 Create an application profile.
  - a On the **Manage** tab for the sfo01m01lb01 device, click the **Load Balancer** tab.
  - b Click **Application Profiles**, and click **Add**.
  - c In the **New Profile** dialog box, configure the profile using the following configuration settings, and click **OK**.

Setting	Value
Name	vrops-https
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800
Client Authentication	Ignore

- 7 Create a service monitoring entry.
  - a On the **Load Balancer** tab for the of the sfo01m01lb01 device, click **Service Monitoring** and click **Add**.
  - b In the **New Service Monitor** dialog box, configure the health check parameters using the following configuration settings, and click **OK**.

Setting	Value
Name	vrops-443-monitor
Interval	3
Timeout	5
Max Retries	2
Type	HTTPS
Method	GET
URL	/suite-api/api/deployment/node/status
Receive	ONLINE (must be upper case)

## 8 Add a server pool.

- a On the **Load Balancer** tab of the sfo01m01lb01 device, select **Pools**, and click **Add**
- b In the **New Pool** dialog box, configure the load balancing profile using the following configuration settings.

Setting	Value
Name	vrops-svr-443
Algorithm	LEASTCONN
Monitors	vrops-443-monitor

- c Under **Members**, click **Add** to add the pool members.
- d In the **New Member** dialog box, add one member for each node of the analytics cluster and click **OK**.

Setting	Value
Name	<ul style="list-style-type: none"> <li>■ vrops01svr01a</li> <li>■ vrops01svr01b</li> <li>■ vrops01svr01c</li> </ul>
IP Address	<ul style="list-style-type: none"> <li>■ 192.168.11.31</li> <li>■ 192.168.11.32</li> <li>■ 192.168.11.33</li> </ul>
State	Enable
Port	443
Monitor Port	443
Weight	1
Max Connections	8
Min Connections	8

- e In the **New Pool** dialog box, click **OK**.

## 9 Add a virtual server.

- a On the **Load Balancer** tab of the sfo01m01lb01 device, select **Virtual Servers** and click **Add**.
- b In the **New Virtual Server** dialog box, configure the settings of the virtual server for the analytics cluster and click **OK**.

Setting	Value
Enable Virtual Server	Selected
Application Profile	vrops-https
Name	vrops-svr-443
Description	vRealize Operations Manager Cluster
IP Address	192.168.11.35 Click <b>Select IP Address</b> , select <b>OneArmLB</b> from the drop-down menu, and select <b>192.168.11.35</b> IP for the virtual NIC.
Protocol	HTTPS
Port	443
Default Pool	vrops-svr-443
Connection Limit	0
Connection Rate Limit	0

You can now connect to the analytics cluster using the public Virtual Server IP address over HTTPS at the **https://vrops01svr01.rainpole.local** address.

## 10 Configure auto-redirect from HTTP to HTTPS requests.

The NSX Edge can redirect users from HTTP to HTTPS without entering another URL in the browser.

- a On the **Load Balancer** tab of the sfo01m01lb01 device, select **Application Profiles** and click **Add**.
- b In the **New Profile** dialog box, configure the application profile settings and click **OK**.

Setting	Value
Name	vrops-http-redirect
Type	HTTP
HTTP Redirect URL	https://vrops01svr01.rainpole.local/vcops-web-ent/login.action
Persistence	Source IP
Expires in (Seconds)	1800

- c On the **Load Balancer** tab of the sfo01m01lb01 device, select **Virtual Servers** and click **Add**.
- d Configure the settings of the virtual server for HTTP redirects and click **OK**.

Setting	Value
Enable Virtual Server	Selected
Application Profile	vrops-http-redirect
Name	vrops-svr-80-redirect
Description	HTTP Redirect for vRealize Operations Manager
IP Address	192.168.11.35
Protocol	HTTP
Port	80
Default Pool	NONE
Connection Limit	0
Connection Rate Limit	0

You can connect to the analytics cluster at the public Virtual Server IP address over HTTP at the `http://vrops01svr01.rainpole.local` address.

- 11 Verify the pool configuration by examining the pool statistics that reflect the status of the components behind the load balancer.
  - a Log out and log in again to the vSphere Web Client.
  - b From the **Home** menu, select **Networking & Security**.
  - c On the **NSX Home** page, click **NSX Edges** and select **172.16.11.65** from the **NSX Manager** drop-down menu at the top of the **NSX Edges** page.
  - d On the **NSX Edges** page, double-click the **sfo01m01lb01** NSX Edge.
  - e On the **Manage** tab, click the **Load Balancer** tab.
  - f Select **Pools** and click **Show Pool Statistics**.
  - g In the **Pool and Member Status** dialog box, select the **vrops-svr-443** pool.
  - h Verify that the load balancer pool is up.

## Move vRealize Operations Analytics Cluster and Remote Collector Nodes to Virtual Machine Folders

Use the vSphere Web Client to move the vRealize Operations analytics cluster nodes and remote collectors nodes to virtual machine folders for organization and ease of management.

vRealize Suite Lifecycle Manager deploys:

- Three vRealize Operations analytics cluster VMs: Master, Master Replica, and Data.
- Two vRealize Operations remote collector VMs: Remote Collector 1 and Remote Collector 2

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the Home menu, select **VMs and Templates**.
- 3 Navigate to the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server and **sfo01-m01dc** data center.
- 4 Create two new VM and Template folders named **sfo01-m01fd-vrops** and **sfo01-m01fd-vropsrc**.
- 5 Move the vRealize Operations Manager analytics cluster VMs to the **sfo01-m01fd-vrops**.
  - a Select the virtual machines **vrops01svr01a**, **vrops01svr01b**, and **vrops01svr01c**.
  - b Right click and select **Move to...**, and select **sfo01-m01fd-vrops** under VM Folders.
  - c Click **OK**.
- 6 Move the vRealize Operations Manager Analytics remote collector VMs to the **sfo01-m01fd-vropsrc**.
  - a Select the virtual machines **sfo01vropsc01a** and **sfo01vropsc01b**.
  - b Right click and select **Move to...** and select **sfo01-m01fd-vropsrc** under VM Folders.
  - c Click **OK**.

## Configure DRS Anti-Affinity Rules for vRealize Operations Manager

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run both the virtual machines of the analytics cluster and of the remote collectors on different hosts in the management cluster.

You use two anti-affinity rules for the vRealize Operations Manager virtual machines: one for the analytics nodes and one for the remote collector nodes. This rule configuration also accommodates the case when you place a host from the management cluster in maintenance mode.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the sfo01m01vc01.sfo01.rainpole.local vCenter Server object, and under the sfo01-m01dc data center object select the **sfo01-m01-mgmt01** cluster.
- 3 Click the **Configure** tab.
- 4 Under the **Configuration** group of settings, select **VM/Host Rules**.
- 5 Create the new anti-affinity rules for the vRealize Operations Manager analytics cluster and remote collectors using the following settings.

Setting	Value for the Analytics Nodes	Value for the Remote Collectors
Name	anti-affinity-rule-vropsm	anti-affinity-rule-vropsr
Enable rule	Selected	Selected
Type	Separate Virtual Machines	Separate Virtual Machines
Members	<ul style="list-style-type: none"> <li>■ vrops01svr01a</li> <li>■ vrops01svr01b</li> <li>■ vrops01svr01c</li> </ul>	<ul style="list-style-type: none"> <li>■ sfo01vropsc01a</li> <li>■ sfo01vropsc01b</li> </ul>

- a In the **VM/Host Rules** list, click **Add** above the rules list.
- b In the **Create VM/Host Rule** dialog box, add the new anti-affinity rule for the virtual machines of the vRealize Operations Manager analytics cluster, and click **OK**.
- c Repeat the step to add the anti-affinity rule for the remote collector virtual machines of the vRealize Operations Manager.

## Proceed Using Evaluation Mode for vRealize Operations Manager

When you deploy vRealize Operations Manager with vRealize Suite Lifecycle Manager, the license is applied to the product. You can therefore use evaluation mode instead of applying a new license.

**Procedure**

- 1 Log in to vRealize Operations Manager by using the administration interface.
  - a Open a Web browser and go to **https://vrops01svr01a.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the **Welcome** page of the **vRealize Operations Manager Configuration** wizard, examine the process overview, and click **Next**.
- 3 On the **Accept EULA** page, accept the end user license agreement, and click **Next**.
- 4 On the **Enter Product License Key** page, select **Product Evaluation (no key required)** and click **Next**.
- 5 (Optional) On the **Customer Experience Improvement Program** page, select **Join the VMware Customer Experience Improvement Program** to send technical information for product improvement, and click **Next**.
- 6 On the **Ready to Complete** page, click **Finish**.

## Replace vRealize Operations Manager Certificate

Use the PEM file that is generated using the CertGenVVD utility to replace the current certificate on the vRealize Operations Manager administrator user interface. You reconnect vRealize Automation to vRealize Operations Manager to update the certificate in the workload reclamation connection.

**Procedure**

- 1 Log in to the vRealize Operations Manager administrator user interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local/admin**
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 At the upper right corner of the UI, click the yellow **SSL Certificate** icon.
- 3 In the **SSL Certificate** dialog box, click **Install New Certificate**.
- 4 Click **Browse**, locate the `vrops.2.chain.pem` PEM file, and click **Open**.
- 5 Verify the certificate details and click **Install**.

## Group Remote Collector Nodes

After you start vRealize Operations Manager and assign it a license, join the remote collectors in a group for adapter resiliency in the cases where the collector experiences network interruption or becomes unavailable.

### Procedure

- 1 Log in to vRealize Operations Manager by using the administration interface.
  - a Open a Web browser and go to **https://vrops01svr01a.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Management** and click **Collector Groups**.
- 4 Click **Add**.
- 5 In the **Add New Collector Group** dialog box, configure the following settings, and click **Save**.

Setting	Value
Name	sfo01-remote-collectors
Description	Remote collector group for sfo01
sfo01vropsc01a	Selected
sfo01vropsc01b	Selected

The sfo01-remote-collectors group appears on the **Collector Groups** page under the **Administration** view of the user interface.

## Add an Authentication Source for the Active Directory

Connect vRealize Operations Manager to the Active Directory of the SDDC for central user management and access control.

**Procedure**

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Access** and click **Authentication Sources**.
- 4 On the **Authentication Sources** page, click **Add**.
- 5 In the **Add Source for User and Group Import** dialog box, enter the settings for the rainpole.local and sfo01.rainpole.local Active Directories, and click **OK**.

Active Directory Settings	rainpole.local Value	sfo01.rainpole.local Value
Source Display Name	RAINPOLE.LOCAL	SFO01.RAINPOLE.LOCAL
Source Type	Active Directory	Active Directory
Integration Mode	Basic	Basic
Domain/Subdomain	RAINPOLE.LOCAL	SFO01.RAINPOLE.LOCAL
Use SSL/TLS	Deselected	Deselected
User Name	svc-vrops@rainpole.local	svc-vrops@rainpole.local
Password	svc-vrops_password	svc-vrops_password
Settings under the <b>Details</b> section		
Automatically synchronize user membership for configured groups	Selected	Selected
Host	dc01rpl.rainpole.local	dc01sfo.sfo01.rainpole.local
Port	3268	389
Base DN	dc=RAINPOLE,dc=LOCAL	dc=SFO01,dc=RAINPOLE,dc=LOCAL
Common Name	userPrincipalName	userPrincipalName

- 6 Click the **Test** button to test the connection to the domain controller and in the **Info** dialog click **OK**.
- 7 In the **Add Source for User and Group Import** dialog box, click **OK**.

The users and user groups in the two Active Directories are added to vReliaze Operations Manager.

## Configure User Access in vSphere for Integration with vRealize Operations Manager

Configure operations service accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the vCenter Server instances in the region.

You associate the `svc-vrops-solution` service accounts in the Active Directory with user roles that have certain privileges and you assign the users to the vCenter Server instances in the inventory by using global permissions.

### Define a User Role in vSphere for vCenter Adapters in vRealize Operations Manager

In vSphere, create a user role with privileges that are required to query information from vCenter Server and receive metric data in vRealize Operations Manager. In vRealize Operations Manager, you can also run actions or tasks on the objects it manages in vCenter Server. Add the privileges to the role that are required for typical virtual machine lifecycle operations, such as snapshot management and virtual machine resource configuration.

#### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, click **Roles** under **Administration**.

- 3 Create a role for collecting data from and performing actions on vCenter Server.
  - a On the **Roles** page, click the **Create role action** icon.
  - b In the **Create Role** dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role name	vSphere Actions User
Privilege	<ul style="list-style-type: none"> <li>■ Virtual Machine.Configuration.Change CPU Count</li> <li>■ Virtual Machine.Configuration. Change Resource</li> <li>■ Virtual Machine.Configuration. Memory</li> <li>■ Virtual Machine.Interaction. Power Off</li> <li>■ Virtual Machine.Interaction. Power On</li> <li>■ Virtual Machine.Snapshot Management. Create Snapshot</li> <li>■ Virtual Machine.Snapshot Management. Remove Snapshot</li> </ul>

This role inherits the **System.Anonymous**, **System.View**, and **System.Read** privileges.

## Define a User Role in vSphere for Storage Devices Adapters in vRealize Operations Manager

In vSphere, create a user role with privileges that are required for collecting data about storage devices in vRealize Operations Manager.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, click **Roles** under **Administration**.

- 3 Create a new role for collecting storage device data.
  - a On the **Roles** page, click the **Create role action** icon.
  - b In the **Create Role** dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role name	MPSD Metrics User
Privilege	<ul style="list-style-type: none"> <li>■ Host.CIM.CIM interaction</li> <li>■ Host.Configuration.Storage partition configuration</li> <li>■ Profile-driven storage.Profile-driven storage view</li> <li>■ Storage views.View</li> </ul>

This role inherits the **System.Anonymous**, **System.View**, and **System.Read** privileges.

## Configure User Privileges in vSphere for Integration with vRealize Operations Manager

Assign global permissions to the operations service accounts to access monitoring data from vCenter Server instances in vRealize Operations Manager.

- The svc-vrops-vsphere user has the rights that are specifically required to collect data from and perform actions on vCenter Server from vRealize Operations Manager.
- The svc-vrops-nsx user has read-only access on all objects in vCenter Server.
- The svc-vrops-mpsd and svc-vrops-vsan users have rights that are specifically required for access to storage device and vSAN information, respectively, in vRealize Operations Manager on all objects in vCenter Server.

You assign global permissions that are based on the following roles to these service accounts:

Service Account	Role
svc-vrops-vsphere@rainpole.local	vSphere Actions User
svc-vrops-nsx@rainpole.local	Read-only
svc-vrops-mpsd@rainpole.local	MPSD Metrics User
svc-vrops-vsan@rainpole.local	MPSD Metrics User

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Click **Global Permissions** under **Access Control**.
- 4 On the **Manage** tab, click **Add permission**.
- 5 In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate the service account with the role that contains the privileges for accessing data from the inventory.
- 6 Add the service account.
  - a In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc-vrops**, and press Enter.
  - b From the list of users and groups, select **svc-vrops-vmware**, click **Add**, and click **OK**.
- 7 Associate the service account with the role.
  - a In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **vSphere Actions User**.
  - b Verify that **Propagate to children** is selected and click **OK**.
- 8 Repeat the steps to assign global permissions to the other service accounts.

## Add vCenter Adapter Instances to vRealize Operations Manager

After you deploy the analytics and the remote collector nodes of vRealize Operations Manager and start vRealize Operations Manager, pair a vCenter Adapter instance with each vCenter Server instance in the region.

**Procedure**

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 From the solution table on the **Solutions** page, select the **VMware vSphere** solution, and click the **Configure** icon at the top.

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

- 5 Under **Instance Settings**, enter the settings for connection to vCenter Server.
  - a If you already have added another vCenter Adapter, click the **Add** icon on the left side to add adapter settings.
  - b Enter the display name, description, and FQDN of the vCenter Server instance.

Setting	Value for Management vCenter Server	Value for Compute vCenter Server
Display Name	vCenter Adapter - sfo01m01vc01	vCenter Adapter - sfo01w01vc01
Description	Management vCenter Server for sfo01	Compute vCenter Server for sfo01
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	sfo01w01vc01.sfo01.rainpole.local

- c Click the **Add** icon on the right side, configure the collection credentials for connection to the vCenter Server instance, and click **OK**.

vCenter Server Credentials Attribute	Value
Credential name	■ vCenter Adapter Credentials - sfo01m01vc01
User Name	svc-vrops-vsphere@rainpole.local
Password	svc-vrops-vsphere-password

- d Leave **Enable Actions** set to **Enable** so that vCenter Adapter can run actions on objects in vCenter Server from vRealize Operations Manager.
  - e Click **Test Connection** to validate the connection to the vCenter Server instance.  
The vCenter Server certificate appears.
  - f In the **Review and Accept Certificate** dialog box, verify the certificate information, and click **Accept**.
  - g Click **OK** in the **Info** dialog box.

- h Expand the **Advanced Settings** section of settings.
- i From the **Collectors/Groups** drop-down menu, select the **sfo01-remote-collectors** group.
- j Specify a user account with administrator privileges to register vRealize Operations Manager with the vCenter Server instance.

Setting	Value
Registration user	administrator@vsphere.local
Registration password	vsphere_admin_password

- 6 Click **Define Monitoring Goals**.
- 7 In the **Define Monitoring Goals** page, under **Enable vSphere Hardening Guide Alerts?**, select **Yes**, leave the default configuration for the other options, and click **Save**.
- 8 Click **OK** in the **Success** dialog box.
- 9 Click **Save Settings**.
- 10 In the **Info** dialog box, click **OK**.
- 11 Repeat [Step 5](#) to [Step 10](#) for the Compute vCenter Server.
- 12 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.
- 13 On the **Solutions** page, select **VMware vSphere** from the solution table to view the collection state and collection status.

The collection state indicates whether the adapter should be collecting data. The collection status value indicates whether vRealize Operations Manager is receiving data about a certain object type. An adapter instance has a status value only if its collection state is `Collecting`.

The **Collection State** column for the vCenter Adapter displays `Collecting`, and the **Collection Status** column displays `Data receiving`.

## Connect vRealize Operations Manager to the NSX Manager Instances

Install and configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in the clusters in the region and view the vSphere hosts in the NSX transport zones.

You can also access end-to-end logical network topologies between two virtual machines or NSX objects. You can isolate problems in the logical or physical network by using the physical host - network device relationship.

## Install the vRealize Operations Manager Management Pack for NSX for vSphere

Install the .pak file for the management pack for NSX for vSphere to add the management pack as a solution to vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the **Solutions** page, click the **Add** icon.
- 5 On the **Select Solution** page from the **Add Solution** wizard, browse to the .pak file of the vRealize Operations Manager Management Pack for NSX for vSphere and click **Upload**.  
After the NSX management pack file has been uploaded, you see details about the management pack.
- 6 After the upload is complete, click **Next**.
- 7 On the **End User License Agreement** page, accept the license agreement and click **Next**.  
The installation of the management pack starts. You see its progress on the **Install** page.
- 8 After the installation is complete, click **Finish** on the **Install** page.

The Management Pack for NSX-vSphere solution appears on the **Solutions** page of the vRealize Operations Manager user interface.

## Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager

Assign the permissions to the service account svc-vrops-nsx that are required to access monitoring data from the NSX Manager in vRealize Operations Manager.

**Procedure**

- 1 Log in to the NSX Manager by using a Secure Shell (SSH) client.

- a Open an SSH connection to the NSX Manager virtual machine.

NSX Manager	Host name
NSX Manager for the management cluster	sfo01m01nsx01.sfo01.rainpole.local
NSX Manager for the shared compute and edge cluster	sfo01w01nsx01.sfo01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 2 Create the local service account svc-vrops-nsx on the NSX Manager instance.

- a Run the following command to switch to Privileged mode of NSX Manager.

```
enable
```

- b Enter the admin password when prompted and press Enter.
- c Switch to Configuration mode.

```
configure terminal
```

- d Create the service account svc-vrops-nsx.

```
user svc-vrops-nsx password plaintext svc-vrops-nsx_password
```

- e Assign the svc-vrops-nsx user access to NSX Manager from the vSphere Web Client.

```
user svc-vrops-nsx privilege web-interface
```

- f Commit these updates to the NSX Manager.

```
write memory
```

- g Exit Configuration mode.

```
exit
```

- 3 Assign the **security\_admin** role to the svc-vrops-nsx service account.

- a Log in to the Windows host that has access to your data center.
- b Launch the Postman application and log in.

- c Select **POST** from the drop-down menu that contains the HTTP request methods.
- d In the URL text box next to the selected method, enter the following URL.

NSX Manager	POST URL
NSX Manager for the management cluster	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true
NSX Manager for the shared edge and compute cluster	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true

- e On the **Authorization** tab, configure the following authorization settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	<i>nsx_admin_password</i>

- f On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Value	text/xml

- g In the **Body** tab, select **raw** and paste the following request body in the **Body** text box and click **Send**.

```
<accessControlEntry>
  <role>security_admin</role>
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```

The Status changes to 204 No Content.

- 4 Repeat the procedure for the other NSX Manager instance.

## Add NSX-vSphere Adapter Instances to vRealize Operations Manager

After you install the management pack, configure an NSX-vSphere Adapter for each NSX Manager instance in the region.

**Procedure**

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the **Solutions** page, select **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.
- 5 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.
- 6 Under **Instance Settings**, enter the settings for connection to the NSX Manager instance.
  - a If you already have added another NSX-vSphere Adapter, click the **Add** icon to add an adapter settings.
  - b Enter the display name, the FQDN of the NSX Manager, and the FQDN of the vCenter Server instance that is connected to the NSX Manager.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Display Name	NSX Adapter - sfo01m01nsx01	NSX Adapter - sfo01w01nsx01
Description	Management NSX Manager for sfo01	Compute NSX Manager for sfo01
NSX Manager Host	sfo01m01nsx01.sfo01.rainpole.local	sfo01w01nsx01.sfo01.rainpole.local
VC Host	sfo01m01vc01.sfo01.rainpole.local	sfo01w01vc01.sfo01.rainpole.local
Enable Log Insight integration if configured	false	false

- c Click the **Add** icon next to the **Credential** text box, configure the credentials for the connection to NSX Manager and vCenter Server, and click **OK**.

vCenter Server Credentials Attribute	Value
Credential name	■ NSX Adapter Credentials - sfo01m01nsx01
NSX Manager User Name	svc-vrops-nsx
NSX Manager Password	svc-vrops-nsx_password
vCenter User Name	svc-vrops-nsx@rainpole.local
vCenter Password	svc-vrops-nsx_password

- d Click **Test Connection** to validate the connection to the NSX Manager instance.  
The NSX Manager certificate appears.
- e In the **Review and Accept Certificate** dialog box, verify the certificate information and click **Accept**.
- f Click **OK** in the **Info** dialog.
- g Expand the **Advanced Settings** section of settings.
- h From the **Collectors/Groups** drop-down menu, select the remote collector group.
- i Click **Save Settings**.
- j Click **OK** in the **Info** dialog box that appears.

7 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The NSX-vSphere adapter appears on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Add Network Devices Adapter to vRealize Operations Manager

Configure a Network Devices Adapter to monitor the switches and routers in your environment, and view related alerts, metrics and object capacity.

The Network Devices Adapter collects data across all network devices that you want to monitor using vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the **Solutions** page, select the **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.
- 5 In **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **Network Devices Adapter**.

6 Under **Instance Settings**, enter the settings for SNMP connection to the network devices for the management cluster.

- a Enter the display name, SNMP version and credentials.

Setting	Value
Display Name	Network Devices Adapter
Description	Global Network Devices Adapter
SNMP Ports	161
SNMP Version	SNMPv2
SNMPv3 Privacy Protocol	AES
SNMPv3 Authentication Protocol	MD5

- b Click the **Add** icon, and configure the credentials for connecting the Network Devices Adapter to the network devices, and click **OK**.

Credential	Value
Credential Kind	SNMPv1, SNMPv2 Credential
Credential Name	Network Devices Credentials
SNMP Read Community Strings	public

For SNMPv1 and SNMPv2 devices, enter a comma-separated list of community names (default is public).

- c Click **Test Connection** to verify the settings, and if the test is successful click the **OK** button.
- d Expand the **Advanced Settings** section of settings, and verify that the **Collectors/Groups** option is set to **Default collector group**.
- e Click **Save Settings**.
- f Click **OK** in the **Info** dialog box that appears.

7 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The Network Devices Adapter appears on the **Solutions** page of the vRealize Operations Manager user interface. The adapter is collecting data about the network devices in all regions of the SDDC.

The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Connect vRealize Operations Manager to vRealize Automation

Configure the vRealize Operations Manager Management Pack for vRealize Automation to monitor the health and capacity risk of your cloud infrastructure in the context of the tenant's business groups.

The vRealize Operations Manager Management Pack for vRealize Automation is installed by default on the version of vRealize Operations Manager in this validated design.

## Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager

Assign the permissions that are required to access monitoring data from the vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account. The svc-vrops-vra user has rights that are specifically required for access to vRealize Automation in vRealize Operations Manager.

### Procedure

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 On the **Tenants** tab, click the **Rainpole** tenant.
- 3 Click the **Administrators** tab to assign tenant administrator and IaaS administrator roles to the svc-vrops-vra service account.
  - a Enter **svc-vrops-vra** in the **Tenant administrators** search text box, click the **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** user that shows in the search result list to assign the role to the account.
  - b Enter **svc-vrops-vra** in the **IaaS administrators** search text box, click the **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** user that shows in the search result list to assign the role to the account.
  - c Click **Finish**.
- 4 Log out of the vRealize Automation portal for the default tenant.
- 5 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	<i>vra-admin-rainpole_password</i>
Domain	rainpole.local

- 6 Navigate to **Administration > Users & Groups > Directory Users and Groups** to assign the software architect role to the svc-vrops-vra service account.
  - a Enter **svc-vrops-vra** in the search box, click the **Search** icon and click the **svc-vrops-vra (svc-vrops-vra@rainpole.local)** user.
  - b The setting of the svc-vrops-vra account appear.
  - c On the **General** tab, select **Infrastructure Architect** and **Software Architect** under **Add roles to this User**, and click **Finish**.
- 7 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign the fabric administrator role to the svc-vrops-vra service account.
  - a On the **Fabric Groups** page, click **SFO Fabric Group**.
  - b On **Edit Fabric Group** page, enter **svc-vrops-vra** in **Fabric administrators** search text box and click the **Search** icon.
  - c Click **svc-vrops-vra@rainpole.local** in the search result list to assign the fabric administrator role to the account, and click **OK**.

## Add a vRealize Automation Adapter to vRealize Operations Manager

Configure a vRealize Automation adapter to collect monitoring data from vRealize Automation.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 From the solution table on the **Solutions** page, select **VMware vRealize Automation** and click **Configure**.

The Manage Solution - VMware vRealize Automation dialog box appears.

5 In the Manage Solution - VMware vRealize Automation dialog box, under **Instance Settings**, enter the settings for the connection to vRealize Automation.

- a Enter the display name, description and FQDN of the vRealize Automation front-end portal, and turn on data collection for the Rainpole tenant.

Setting	Value
Display Name	vRealize Automation Adapter - vra01svr01 (Rainpole)
Description	vRealize Automation - Rainpole Tenant
vRealize Automation Appliance URL	https://vra01svr01.rainpole.local

- b Click the **Add** icon next to the **Credential** text box, configure the credentials for the connection to vRealize Automation, and click **OK**.

Credential	Value
Credential name	vRA Adapter Credentials - vra01svr01
SysAdmin Username	administrator@vsphere.local
SysAdmin Password	vra_administrator_password
SuperUser Username	svc-vrops-vra@rainpole.local
SuperUser Password	svc_vrops_vra_password

- c Click **Test Connection** to validate the connection to vRealize Automation.
- d In the **Review and Accept Certificate** dialog box, verify the vRealize Automation certificate information, and click **Accept**.
- e Click **OK** in the **Info** dialog box.
- f Expand the **Advanced Settings** section, and verify the following configuration.

Advanced Setting	Value
Collectors/Groups	Default collector group
Tenants	rainpole
vRA Endpoint Monitoring	Enabled
Auto Discovery	true

- g Click **Save Settings** and click **OK** in the **Info** box that appears.

6 In the **Manage Solution - VMware vRealize Automation** dialog box, click **Close**.

The **vRealize Automation Adapter** appears on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation

Configure read-only privileges for the svc-vra-vrops@rainpole.local service account on vRealize Operations Manager. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, expand **Access**, and click **Access Control**.
- 4 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.
- 5 On the **Import Users** page, import the svc-vra-vrops@rainpole.local service account.
  - a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.
  - b Select the **Basic** option for the search query.
  - c In the **Search String** text box, enter **svc-vra-vrops** and click **Search**.  
The search results contain the svc-vra-vrops user account.
  - d Select **svc-vra-vrops@rainpole.local** and click **Next**.
- 6 On the **Assign Groups and Permissions** page, to assign the ReadOnly role to the svc-vra-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings, and click **Finish**.

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

## Add vRealize Operations Manager as a Metrics Provider in vRealize Automation

Integrate vRealize Automation with vRealize Operations Manager to pull metrics for the reclamation of tenant workloads.

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

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

- 2 Navigate to **Administration > Reclamation > Metrics Provider**.
- 3 On the **Metrics Provider** page, configure the vRealize Operations Manager settings.
  - a Select **vRealize Operations Manager endpoint**.
  - b Configure the following settings for vRealize Operations Manager.

Setting	Value
URL	https://vrops01svr01.rainpole.local/suite-api/
Username	svc-vra-vrops@rainpole.local
Password	svc-vra-vrops_password

- c Click **Test Connection**, verify that the test connection is successful, and click **Save**.
  - d In the certificate warning message box, click **OK**.

The vSphere metrics provider updated successfully message appears.

## Connect vRealize Operations Manager with vRealize Business

Configure the vRealize Operations Manager Management Pack for vRealize Business to view your infrastructure performance, cost information, and troubleshooting tips. You can connect vRealize Operations Manager to a single instance of vRealize Business for Cloud.

### Configure vRealize Business Adapter in vRealize Operations

Configure a vRealize Business for Cloud adapter to collect monitoring data from vRealize Business for Cloud in vRealize Operations Manager.

**Procedure**

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 From the solution table on the **Solutions** page, select **VMware vRealize Business for Cloud** solution, and click **Configure**.

The **Manage Solution - VMware vRealize Business for Cloud** dialog box appears.

- 5 In the **Manage Solution - VMware vRealize Business for Cloud** dialog box, under **Instance Settings**, enter the settings for the connection to vRealize Business for Cloud.
  - a Enter the display name, description, and FQDN of the vRealize Business for Cloud server.

Setting	Value for vRealize Business for Cloud Server
Display Name	vRealize Business Adapter - vrb01svr01
Description	vRealize Business for Cloud Server
vRealize Business for Cloud server	vrb01svr01.rainpole.local

- b Click **Test Connection** to validate the connection to the vRealize Business server instance.
  - c Click **OK** in the **Info** dialog box.
  - d Expand the **Advanced Settings** section of settings
  - e From the **Collectors/Groups** drop-down menu, make sure that the **Default collector group** is selected.
- 6 Click **Save Settings**.
- 7 Click **OK** in the **Info** dialog box.
- 8 In the **Manage Solution - VMware vRealize Business for Cloud** dialog box, click **Close**.

The **vrBC Adapter** appears on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

# Enable Storage Device Monitoring in vRealize Operations Manager

Install and configure the vRealize Operations Management Pack for Storage Devices to view the storage topology in the SDDC and to monitor the capacity and problems on storage components.

## Install the vRealize Operations Manager Management Pack for Storage Devices

Install the .pak file of the management pack for storage devices to add the management pack as a solution to vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the **Solutions** page, click the **Add** icon.
- 5 On the **Select Solution** page from the **Add Solution** wizard, browse to the .pak file of the vRealize Operations Manager Management Pack for Storage Devices and click **Upload**.
- 6 After the upload is complete, click **Next**.
- 7 On the **End User License Agreement** page, accept the license agreement and click **Next**.  
The installation of the management pack starts. You see its progress on the **Install** page.
- 8 After the installation is complete, click **Finish** on the **Install** page.

The **Management Pack for Storage Devices** solution appears on the **Solutions** page of the vRealize Operations Manager user interface.

## Disable the vSAN Dashboards of the Management Pack for Storage Devices

Use the vRealize Operations Management Pack for Storage Devices to monitor fabric-based storage such as the NFS datastores in this validated design. To monitor the vSAN datastores for the management applications, disable the vSAN dashboards of management pack for Storage Devices and use the dashboards of the vRealize Operations Management Pack for vSAN. The management pack for vSAN comes pre-installed with vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using Secure Shell (SSH) client.
  - a Open an SSH connection to `vrops01svr01a.rainpole.local`.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrops_root_password</i>

- 2 Disable the vSAN dashboards provided by the vRealize Operations Manager Management Pack for Storage Devices by running the following commands.

```
cd /usr/lib/vmware-vcops/tools/opscli
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Heatmap'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Entity Usage'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Cluster Insights'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Device Insights'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Troubleshooting'
```

- 3 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to <https://vrops01svr01.rainpole.local>.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 4 On the main navigation bar, click **Dashboards** and verify that the following dashboards are no longer visible.
  - VirtualSAN Heatmap
  - VirtualSAN Entity Usage
  - VirtualSAN Cluster Insights
  - VirtualSAN Device Insights

- VirtualSAN Troubleshooting

## Add Storage Devices Adapters in vRealize Operations Manager

After you install the management pack, configure a Storage Devices adapter to collect monitoring data about the storage devices in the SDDC. Each adapter communicates with a vCenter Server instance to retrieve data about the storage devices from the vCenter Server inventory.

### Procedure

- Log in to vRealize Operations Manager by using the operations interface.
  - Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- On the main navigation bar, click **Administration**.
- In the left pane of vRealize Operations Manager, click **Solutions**.
- On the **Solutions** page, select **Management Pack for Storage Devices** from the solution table and click **Configure**.

The **Manage Solution - Management Pack for Storage Devices** dialog box appears.

- Under **Instance Settings**, enter the settings for connection to the vCenter Server instance.
  - If you already have added another Storage Devices adapter, click the **Add** icon on the left side to add an adapter settings.
  - Enter the display name, description, and name of the vCenter Server instance.

Setting	Value for the Management vCenter Server	Value for the Compute vCenter Server
Display Name	Storage Devices Adapter - sfo01m01vc01	Storage Devices Adapter - sfo01w01vc01
Description	Storage Devices in Management vCenter for sfo01	Storage Devices in Compute vCenter for sfo01
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	sfo01w01vc01.sfo01.rainpole.local
SNMP Community Strings	-	-

- c Click the **Add** icon on the right side, configure the collection credentials for connection to the vCenter Server instance, and click **OK**.

vCenter Server Credentials Attribute	Value
Credential name	■ Storage Devices Adapter Credentials - sfo01m01vc01
User Name	svc-vrops-mpsd@rainpole.local
Password	svc-vrops-mpsd-password

- d Click **Test Connection** to validate the connection to the vCenter Server.  
The vCenter Server certificate appears.
- e In the **Review and Accept Certificate** dialog box, verify the vCenter Server certificate information and click **Accept**.
- f Click **OK** in the **Info** dialog box.
- g Expand the **Advanced Settings** section of settings.
- h From the **Collectors/Groups** drop-down menu, select the **sfo01-remote-collectors** remote collector group.
- i Click **Save Settings**.
- j Click **OK** in the **Info** dialog box that appears.
- k Repeat the procedure for the other vCenter Server instance.

- 6 In the **Manage Solution - Management Pack for Storage Devices** dialog box, click **Close**.

The Storage Devices adapter appears on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Enable vSAN Monitoring in vRealize Operations Manager

Configure the vRealize Operations Management Pack for vSAN to view the vSAN topology, and to monitor the capacity and problems.

The vRealize Operations Management Pack for vSAN is installed by default in the vRealize Operations Manager version that is used in this version of VMware Validated Design.

### Turn On vSAN Performance Service

When you create a vSAN cluster, the performance service is disabled. Turn on the vSAN performance service to monitor the performance of vSAN clusters, hosts, disks, and VMs.

When you turn on the performance service, vSAN places a Stats database object in the datastore to collect statistical data. The Stats database is a namespace object in the vSAN datastore of the cluster.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, expand the **sfo01-m01dc** data center object.
- 3 Click the **sfo01-m01-mgmt01** cluster object and click the **Configure** tab.
- 4 Under **vSAN**, select **Health and Performance**.
- 5 Next to the **Performance Service** settings, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Turn ON vSAN performance service	Selected
Storage policy	vSAN Default Storage Policy

## Add a vSAN Adapter in vRealize Operations Manager

Configure the vSAN adapter to collect monitoring data about vSAN usage in the SDDC.

**Procedure**

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the **Solutions** page, select **VMware vSAN** from the solution table, and click **Configure**.  
The **Manage Solution - VMware vSAN** dialog box appears.

5 Under **Instance Settings**, enter the settings for the connection to the vCenter Server instance.

- a Enter the settings for connection to the vCenter Server.

Setting	Value for the vCenter Server
Display Name	vSAN Adapter - sfo01m01vc01
Description	vCenter Server vSAN Adapter for
vCenter Server	sfo01m01vc01.sfo01.rainpole.local

- b Click the **Add** icon next to the **Credential** text box, and configure the credentials for connection to vCenter Server, and click **OK**.

Setting	Value for the vCenter
Credential name	vSAN Adapter Credentials - sfo01m01vc01
vCenter User Name	svc-vrops-vsan@rainpole.local
vCenter Password	svc-vrops-vsan-password

- c Click **Test Connection** to validate the connection to vCenter Server.

The vCenter Server certificate appears.

- d In the **Review and Accept Certificate** dialog box, verify the vCenter Server certificate information, and click **Accept**.

- e Click **OK** in the **Info** dialog box.

- f Expand the **Advanced Settings** section of settings.

- g From the **Collectors/Groups** drop-down menu, select the collector group.

- h Make sure **Auto Discovery** is set to **true**.

- i Click **Save Settings**.

- j Click **OK** in the **Info** dialog box that appears.

6 In the **Manage Solution - VMware vSAN** dialog box, click **Close**.

The vSAN Adapter appears on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Configure Email Alerts for vRealize Operations Manager

You configure email notifications in vRealize Operations Manager so that users and applications receive the administrative alerts from vRealize Operations Manager about certain situations in the data center.

**Procedure**

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Management** and click **Outbound Settings**.
- 4 On the **Outbound Settings** page, click the **Add** icon to create an outbound alert instance.
- 5 In the **Add/Edit Outbound Instance** dialog box, configure the settings for the Standard Email Plug-in, and click **OK**.

Alert Instance Setting	Value
Plugin Type	Standard Email Plugin
Instance Name	SMTP Alert Mail Relay
Use Secure Connection	Selected
SMTP Host	<i>FQDN of the SMTP server</i>
SMTP Port	<i>Server port for SMTP requests</i>
Secure Connection Type	TLS
Sender Email Address	<i>Address that appears as the sender of the email</i>
Sender Name	<i>Name that appears as the sender of the email</i>

- 6 Click **Test** to verify the connection with the SMTP server and click **OK**.
- 7 Click **Save**.

# Post-Deployment Tasks for vRealize Log Insight

# 8

After you deploy vRealize Log Insight with vRealize Suite Lifecycle Manager, you perform post-deployment tasks to complete the configuration.

## 1 [Move vRealize Log Insight Cluster Nodes to a Virtual Machine Folder](#)

Use the vSphere Web Client to move the vRealize Log Insight cluster nodes to a virtual machine folder for organization and ease of management.

## 2 [Configure a DRS Anti-Affinity Rule for vRealize Log Insight](#)

To protect the vRealize Log Insight cluster from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the cluster.

## 3 [Configure the vRealize Log Insight Master node](#)

Configure the general properties of the vRealize Log Insight Master Node.

## 4 [Enable Active Directory Support for vRealize Log Insight](#)

To use service accounts in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, enable Active Directory support.

## 5 [Replace the Certificate of vRealize Log Insight](#)

Update the certificate chain of vRealize Log Insight to use a trusted non-default certificate after deployment or to replace a certificate that is soon to expire. In this way, connection to the vRealize Log Insight user interface remains trusted.

## 6 [Connect vRealize Log Insight to the vSphere Environment](#)

Start collecting log information about the ESXi and vCenter Server instances in the SDDC.

## 7 [Connect vRealize Log Insight to vRealize Operations Manager](#)

Connect vRealize Log Insight to vRealize Operations Manager so that you can use the Launch in Context functionality between the two applications to troubleshoot management nodes and vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

## 8 [Connect vRealize Log Insight to the NSX Instances](#)

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

**9** [Connect vRealize Log Insight to vRealize Automation](#)

Connect vRealize Log to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight user interface.

**10** [Install the vRealize Log Insight Content Pack for Linux](#)

Install the content pack for Linux to add dashboards for viewing log information in vRealize Log Insight from the operating system of the management virtual appliances in the region.

**11** [Configure a Log Insight Agent Group for the Management Virtual Appliances](#)

After you install the content pack for Linux, configure an agent group to apply common settings to the agents on the appliances in the region.

**12** [Configure Log Retention and Archiving](#)

Set log retention to one week and archive logs for 90 days according to the *VMware Validated Design Architecture and Design* documentation.

## Move vRealize Log Insight Cluster Nodes to a Virtual Machine Folder

Use the vSphere Web Client to move the vRealize Log Insight cluster nodes to a virtual machine folder for organization and ease of management.

vRealize Suite Lifecycle Manager deploys three vRealize Log Insight nodes - one master node and two worker nodes. You move them to a single VM folder to simplify management.

### Procedure

- Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- From the Home menu, select **VMs and Templates**.
- Navigate to the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server and **sfo01-m01dc** data center.
- Create a new VM and Template folder named **sfo01-m01fd-vrli**.
- Move the vRealize Log Insight cluster VMs.
  - a Select the virtual machines **sfo01vrli01a**, **sfo01vrli01b**, and **sfo01vrli01c**.
  - b Right click and select **Move to...** and select **sfo01-m01fd-vrli** under **VM Folders**.
  - c Click **OK**.

## Configure a DRS Anti-Affinity Rule for vRealize Log Insight

To protect the vRealize Log Insight cluster from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the cluster.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the sfo01m01vc01.sfo01.rainpole.local vCenter Server object, and under the sfo01-m01dc data center object select the **sfo01-m01-mgmt01** cluster.
- 3 On the **Configure** tab, select **VM/Host Rules**.
- 4 In the **VM/Host Rules** list, click **Add** above the rules list, add a new anti-affinity rule using the following details, and click **OK**.

Rule Attribute	Value
Name	anti-affinity-rule-vrli
Enable rule	Yes
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> <li>▪ sfo01vrli01a</li> <li>▪ sfo01vrli01b</li> <li>▪ sfo01vrli01c</li> </ul>

## Configure the vRealize Log Insight Master node

Configure the general properties of the vRealize Log Insight Master Node.

vRealize Suite Lifecycle Manager performs the deployment for you, but you have to perform additional configuration.

### Prerequisites

You need information about the email server for sending notifications from vRealize Log Insight. Contact your system administrator for details about the email server.

**Procedure**

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01a.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrlj_admin_password

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Configuration**, click **General**, enter the following settings and click **Save**.

Setting	Value
Email System Notifications to	email_address_to_receive_system_notifications
Send HTTP Post System Notifications To	https://sfo01vrli01.sfo01.rainpole.local

- 4 Under **Configuration** page, click **SMTP**, specify the properties of an SMTP server to enable outgoing alerts and system notification emails, and to test the email notification.
  - a Set the connection setting for the SMTP server that will send the email messages from vRealize Log Insight.

SMTP Option	Description
SMTP Server	FQDN of the SMTP server
Port	Server port for SMTP requests
SSL (SMTPS)	Sets whether encryption should be enabled for the SMTP transport option connection.
STARTTLS Encryption	Enable or disable the STARTTLS encryption.
Sender	Address that appears as the sender of the email.
Username	User name on the SMTP server
Password	Password for the SMTP server you specified in Username

- b To verify that the SMTP configuration is correct, type a valid email address and click **Send Test Email**.  
vRealize Log Insight sends a test email to the address that you provided.
    - c Click **Save**.

## Enable Active Directory Support for vRealize Log Insight

To use service accounts in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, enable Active Directory support.

**Procedure**

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 From the Administration page, under **Configuration**, click **Authentication**.
- 3 On the **Authentication Configuration** page, select the **Active Directory** tab.
- 4 Slide the toggle button to enable the support for Active Directory and configure the Active Directory settings.
  - a Configure the Active Directory connection settings according to the details from your IT administrator.

Setting	Value
Enable Active Directory support	Selected
Default Domain	rainpole.local
Domain Controller(s)	dc01rpl.rainpole.local
User Name	svc-vrli
Password	<i>svc_vrli_password</i>
Connection Type	Standard
Require SSL	Yes or No according to the instructions from the IT administrator

- b Click **Test Connection** to verify the connection, and click **Save**.

## Replace the Certificate of vRealize Log Insight

Update the certificate chain of vRealize Log Insight to use a trusted non-default certificate after deployment or to replace a certificate that is soon to expire. In this way, connection to the vRealize Log Insight user interface remains trusted.

**Procedure**

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Configuration**, click **SSL**.
- 4 On the **SSL Configuration** page, next to **New Certificate File (PEM format)** click **Choose File**, browse to the location of the PEM file on your computer, and click **Save**.

Certificate Generation Option	Certificate File
Using the CertGenVVD tool	vrli.sfo01.2.chain.pem

The certificate is uploaded to vRealize Log Insight.

- 5 Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**  
A warning message that the connection is not trusted appears.
- 6 To review the certificate, click the padlock  in the address bar of the browser, and verify that **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.
- 7 Import the certificate in your Web browser.  
For example, in Google Chrome under the HTTPS/TLS settings click **Manage certificates**, and in the **Certificates** dialog box import `vrli-chain.pem`.

You can also use Certificate Manager on Windows or Keychain Access on MAC OS X.

## Connect vRealize Log Insight to the vSphere Environment

Start collecting log information about the ESXi and vCenter Server instances in the SDDC.

### Configure User Privileges in vSphere for Integration with vRealize Log Insight

Assign global permissions to the service account `svc-vrli-vsphere` to collect log information from the vCenter Server instances and ESXi hosts with vRealize Log Insight. The `svc-vrli-vsphere` user account is dedicated to collecting log information from vCenter Server and ESXi.

#### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Under **Access Control**, click **Roles**.
- 4 Create a role for vRealize Log Insight.
  - a From **Roles provider** drop-down menu, select sfo01m01vc01.sfo01.rainpole.local
  - b Select **Read-only** and click the **Clone role action** icon.

You clone the Read-only role because it includes the **System.Anonymous**, **System.View**, and **System.Read** privileges. vRealize Log Insight requires those privileges for accessing log information related to the vCenter Server instances.

- c In the **Clone Role Read-only** dialog box, complete the configuration of the role and click **OK**.

Setting	Description
Role name	Log Insight User
Privilege	<ul style="list-style-type: none"> <li>■ Host.Configuration.Advanced settings</li> <li>■ Host.Configuration.Change settings</li> <li>■ Host.Configuration.Network configuration</li> <li>■ Host.Configuration.Security profile and firewall</li> </ul>

These host privileges allow vRealize Log Insight to configure the syslog service on the ESXi hosts.

The Log Insight User role is propagated to other linked vCenter Server instances.

- 5 Assign global permissions to the svc-vrli-vsphere@rainpole.local service account.
  - a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Global Permissions** under **Access Control**.
  - b On the **Manage** tab, click **Add Permission**.
  - c In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
  - d In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
  - e From the list of users and groups, select the **svc-vrli-vsphere** user, click **Add**, and click **OK**.
  - f In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Log Insight User**, select **Propagate to children**, and click **OK**.

The global permissions of the svc-vrli-vsphere@rainpole.local user propagate to all vCenter Server instances.

## Connect vRealize Log Insight to vSphere

After you configure the svc-vrli-vsphere Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, connect vRealize Log Insight to vSphere in the vRealize Log Insight user interface.

## Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Integration**, click **vSphere**.
- 4 In the **vCenter Servers** pane, enter the connection settings for the vCenter Server instances in the region.
  - a Enter the host name, user credentials, and collection options for the vCenter Server instances, and click **Test Connection**.

vCenter Server Option	Value
Hostname	<ul style="list-style-type: none"> <li>■ sfo01m01vc01.sfo01.rainpole.local for Management vCenter Server</li> <li>■ sfo01w01vc01.sfo01.rainpole.local for Compute vCenter Server</li> </ul>
Username	svc-vrli-vsphere@rainpole.local
Password	<i>svc-vrli-vsphere_user_password</i>
Collect vCenter Server events, tasks and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected

- b Click **Advanced Options** and examine the list of ESXi hosts that are connected to the vCenter Server instance to verify that you connect to the correct vCenter Server.
  - c In the **Advanced Options** configuration window, select **Configure all ESXi hosts**, select **UDP** under **Syslog protocol**, and click **OK**.
- 5 Click **Add vCenter Server** to add a new settings form and repeat the steps to add the settings for the second vCenter Server instance in Region A.
- 6 Click **Save**.  
A progress dialog box appears.
- 7 Click **OK** in the confirmation dialog box that appears after vRealize Log Insight contacts the vCenter Server instances.

You see the vSphere dashboards under the **VMware - vSphere** content pack dashboard category.

## Configure vCenter Server to Forward Log Events to vRealize Log Insight

Configure vCenter Server and Platform Services Controller appliances to forward system logs and events to the vRealize Log Insight. You can then view and analyze all syslog information in the vRealize Log Insight Web interface.

You configure the following vCenter Server and Platform Services Controller instances:

Appliance Type	Appliance Management Interface URL
vCenter Server instances	https://sfo01m01vc01.sfo01.rainpole.local:5480
	https://sfo01w01vc01.sfo01.rainpole.local:5480
Platform Services Controller instances	https://sfo01m01psc01.sfo01.rainpole.local:5480
	https://sfo01w01psc01.sfo01.rainpole.local:5480

### Procedure

- 1 Redirect the log events from the vCenter Server Appliance to vRealize Log Insight.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vc_root_password

- c In the **Navigator**, click **Syslog Configuration**.
- d On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	sfo01vrli01.sfo01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

- e Repeat the steps for the other appliances.

- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vri_admin_password

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** under **Content Pack Dashboards**.
- d Verify that the vCenter Server nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

## Update the Host Profiles with Syslog Settings

To have a consistent logging configuration across all ESXi hosts, update the host profile in each cluster to accommodate the syslog settings for connection to vRealize Log Insight.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Update the host profile for the management cluster.
  - a From the vSphere Web Client **Home** menu, select **Home**.
  - b In the **Navigator**, click **Policies and Profiles** and click **Host Profiles**.
  - c Right-click **sfo01-m01hp-mgmt01** and select **Copy Settings from Host**.
  - d Select **sfo01m01esx01.sfo01.rainpole.local** and click **OK**.
- 3 Verify that the syslog host settings have been updated.
  - a On the **Host Profiles** page in the **Navigator**, click **sfo01-m01hp-mgmt01**.
  - b On the **Configure** tab, click **Settings**.
  - c In **Filter** search box, enter **Syslog.global.logHost**.
  - d Select the **Syslog.global.logHost** entry from the results list and verify that value of the option is **udp://sfo01vrli01.sfo01.rainpole.local:514**

- 4 Verify the compliance of the hosts in the management cluster.
  - a From the vSphere Web Client **Home** menu, select **Hosts and Clusters**.
  - b Click the **sfo01-m01hp-mgmt01** cluster, click the **Monitor** tab, and click **Profile Compliance**.
  - c Click the **Check Compliance Now** button.
  - d Verify that all hosts are compliant with the attached profile.
- 5 Repeat the procedure with a host in the shared edge and compute cluster.

## Connect vRealize Log Insight to vRealize Operations Manager

Connect vRealize Log Insight to vRealize Operations Manager so that you can use the Launch in Context functionality between the two applications to troubleshoot management nodes and vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

## Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight

Configure administrator privileges for the `svc-vrli-vrops@rainpole.local` service account for vRealize Log Insight on vRealize Operations Manager. You must assign administrator privileges to the service account for the Launch in Context integration between the two management components.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigator bar, click **Administration**.
- 3 On the left of vRealize Operations Manager, expand **Access** and click **Access Control**.
- 4 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.
- 5 On the **Import Users** page, import the `svc-vrli-vrops@rainpole.local` service account.
  - a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.
  - b Select the **Basic** option for the search query.

- c In the **Search String** text box, enter **svc-vrli-vrops** and click **Search**.  
The search results contain the svc-vrli-vrops user account.
  - d Select **svc-vrli-vrops@rainpole.local** and click **Next**.
- 6 On the **Assign Groups and Permissions** page, to assign the Administrator role to the svc-vrli-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings, and click **Finish**.

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

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

## Enable the vRealize Log Insight Integration with vRealize Operations Manager

Connect vRealize Log Insight in the region with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager and to send alerts to vRealize Operations Manager.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 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, configure the integration settings for vRealize Operations Manager.

Setting	Value
Hostname	vrops01svr01.rainpole.local
Username	svc-vrli-vrops@rainpole.local
Password	<i>svc-vrli-vrops_password</i>
Enable alerts integration	Selected
Enable launch in context	Selected

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

A progress dialog box appears.

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

## Connect vRealize Operations Manager to vRealize Log Insight

Configure a vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager in your environment. You can access unstructured log data about any object in your environment by using Launch in Context in vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the **Solutions** page, select **VMware vRealize Log Insight** from the solution table, and click **Configure**.

The **Manage Solution - VMware vRealize Log Insight** dialog box appears.

- 5 Under **Instance Settings**, enter the settings for connection to vRealize Log Insight.
  - a Enter the display name, description and the FQDN of the vRealize Log Insight instance.

Setting	vRealize Log Insight in Region A	vRealize Log Insight in Region B
Display Name	Log Insight Adapter - sfo01vrli01	Log Insight Adapter - lax01vrli01
Description	vRealize Log Insight for sfo01	vRealize Log Insight for lax01
Log Insight server	sfo01vrli01.sfo01.rainpole.local	lax01vrli01.lax01.rainpole.local

- b Click **Save Settings**.
  - c Click **OK** in the **Info** box.
- 6 Validate the connection to vRealize Log Insight.
  - a Click **Test Connection** to validate the connection to vRealize Log Insight.
  - b Click **OK** in the **Info** dialog box.

- 7 Expand the **Advanced Settings** pane and select the collector group from the **Collectors/Groups** drop-down menu.
- 8 Click **Save Settings** and click **OK** in the **Info** dialog box that appears.
- 9 Repeat the procedure to create an adapter for the vRealize Log Insight in Region B.
- 10 In the **Manage Solution - VMware vRealize Log Insight** dialog box, click **Close**.

The vRealize Log Insight Adapter is available on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight

After you connect vRealize Operations Manager to vRealize Log Insight for Launch in Context, configure the Log Insight agent on vRealize Operations Manager to send audit logs and system events to vRealize Log Insight.

### Procedure

- 1 Enable Secure Shell (SSH) on each node of vRealize Operations Manager.
  - a Open a Web browser and go to **<https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client>**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c Under the sfo01m01vc01.sfo01.rainpole.local vCenter Server, navigate to the virtual appliance for the node.

Virtual Appliance Name	Role
vrops01svr01a	Master node
vrops01svr01b	Master replica node
vrops01svr01c	Data node 1
sfo01vropsc01a	Remote collector 1
sfo01vropsc01b	Remote collector 2

- d Right-click the appliance node and select **Open Console** to open the remote console to the appliance.
    - e Press ALT+F1 to switch to the command prompt.

- f Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrops_root_password</i>

- g Start the SSH service by running the following command.

```
service sshd start
```

- h Close the virtual appliance console.

- i Repeat the step for other nodes.

**2** Configure the Log Insight agent in vRealize Operation Manager.

- a Open an SSH connection to the vRealize Operations Manager appliances using the following settings.

Setting	Value
Host name	<ul style="list-style-type: none"> <li>■ vrops01svr01a.rainpole.local</li> <li>■ vrops01svr01b.rainpole.local</li> <li>■ vrops01svr01c.rainpole.local</li> <li>■ sfo01vropsc01a.sfo01.rainpole.local</li> <li>■ sfo01vropsc01b.sfo01.rainpole.local</li> </ul>
User name	root
Password	<i>vrops_root_password</i>

- b Edit the `liagent.ini` file on each vRealize Operations Manager node using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

- c Locate the [server] section, uncomment the following parameters and input the following values.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=sfo01vrli01.sfo01.rainpole.local
; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
;
proto=cfapi
; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000
;ssl - enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
ssl=no
; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30
```

- d After the [server] section, add the following block on each vRealize Operations Manager node.

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"<vROPS Node Role Here>",
"vmw_vr_ops_nodename":"<Your vROPS Node Name Here>",
"vmw_vr_ops_hostname":"<Your vROPS Hostname Here>"}
```

- e Modify the following parameters specifically for each node.

Parameter	Description	Location in liagent.ini
vmw_vr_ops_clusterrole	Role of the vRealize Operations Manager node	Set to <b>Master</b> or <b>Remote Collector</b> according to the role of the node.
vmw_vr_ops_nodename	IP address or FQDN of the vRealize Operations Manager node	Replace each <Your VR0PS Node Name Here> with the following names: <ul style="list-style-type: none"> <li>■ vrops01svr01a</li> <li>■ vrops01svr01b</li> <li>■ vrops01svr01c</li> <li>■ sfo01vropsc01a</li> <li>■ sfo01vropsc01b</li> </ul>
vmw_vr_ops_hostname	Name of the vRealize Operations Manager node that is set during node initial configuration	Replace each <Your VR0PS Hostname Here> with the following names: <ul style="list-style-type: none"> <li>■ vrops01svr01a.rainpole.local</li> <li>■ vrops01svr01b.rainpole.local</li> <li>■ vrops01svr01c.rainpole.local</li> <li>■ sfo01vropsc01a.sfo01.rainpole.local</li> <li>■ sfo01vropsc01b.sfo01.rainpole.local</li> </ul>

For example, on the master node you change the [common|filelog] section to add a context to the logs that are sent to the vRealize Log Insight cluster:

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vR0ps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"Master", "vmw_vr_ops_nodename":"vrops01svr01a",
"vmw_vr_ops_hostname":"vrops01svr01a.rainpole.local"}
```

- f Press Esc and enter **:wq!** to save the file.
- g Restart the Log Insight agent on node by running the following console command.

```
/etc/init.d/liagentd restart
```

- h Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

- i Stop the SSH service on the virtual appliance by running the following command.

```
service sshd stop
```

- 3 Repeat the steps for each of the remaining vRealize Operations Manager nodes.

#### 4 Configure the Agent Group for the vRealize Operations Manager components in the vRealize Log Insight Web user interface.

- a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vri_admin_password

- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under **Management**, click **Agents**.
- e From the drop-down menu at the top, select **vRops 6.4 or higher - Sample** from the **Available Templates** section and click the **Copy Template** button at the bottom.
- f In the **Copy Agent Group** dialog box, enter **vROPs – Appliance Agent Group** in the **Name** text box and click **Copy**.
- g In the **agent filter** fields, enter the following values pressing Enter after each host name.

Filter	Operator	Values
Hostname	Matches	<ul style="list-style-type: none"> <li>■ vrops01svr01a.rainpole.local</li> <li>■ vrops01svr01b.rainpole.local</li> <li>■ vrops01svr01c.rainpole.local</li> <li>■ sfo01vropsc01a.sfo01.rainpole.local</li> <li>■ sfo01vropsc01b.sfo01.rainpole.local</li> </ul>

- h Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.
- i Click **Save New Group** at the bottom of the page.
- j Click the **Dashboard** tab and select the **VMware - vRops 6.x** dashboard under the **Content Pack Dashboards** on the left.

All **VMware - vRops 6** dashboards become available on the home page of vRealize Log Insight. You see the **Total number of vRops Clusters** showing 1 and **Total number of vRops nodes over time** showing the host names of the vRealize Operations Manager nodes.

## Connect vRealize Log Insight to the NSX Instances

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

## Install the vRealize Log Insight Content Pack for NSX for vSphere

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vri_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - NSX-vSphere** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, accept the **License Agreement**, and click **Install**.
- 6 In the **VMware - NSX-vSphere Setup Instructions** dialog box, click **OK**.

After the installation is complete, the VMware - NSX-vSphere content pack appears in the **Installed Content Packs** list on the left.

## Configure NSX Manager to Forward Log Events to vRealize Log Insight

Configure the NSX Manager instances in the region to send audit logs and system events to vRealize Log Insight.

**Procedure**

- 1 Log in to the Management NSX Manager appliance user interface.

- a Open a Web browser and go to following URL.

NSX Manager	URL
NSX Manager for the management cluster	<a href="https://sfo01m01nsx01.sfo01.rainpole.local">https://sfo01m01nsx01.sfo01.rainpole.local</a>
NSX Manager for the shared compute and edge cluster	<a href="https://sfo01w01nsx01.sfo01.rainpole.local">https://sfo01w01nsx01.sfo01.rainpole.local</a>

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 2 On the main page of the appliance user interface, click **Manage Appliance Settings**.
- 3 Under **Settings**, click **General**, and in the **Syslog Server** pane, click **Edit**.
- 4 In the **Syslog Server** dialog box, configure vRealize Log Insight as a syslog server by specifying the following settings and click **OK**.

Syslog Server Setting	Value
Syslog Server	sfo01vrli01.sfo01.rainpole.local
Port	514
Protocol	UDP

- 5 Repeat the steps for the other NSX Manager.

## Configure the NSX Controllers to Forward Events to vRealize Log Insight

Configure the NSX Controller instances to forward log information to vRealize Log Insight by using the NSX REST API. To enable log forwarding, you can use a REST client, such as the Postman application.

**Procedure**

- 1 Log in to the Windows host that has access to your data center.
- 2 Start the Postman application and log in.

3 Specify the headers for requests to the NSX Manager.

- a On the **Authorization** tab, configure the following authorization settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	<i>nsx_admin_password</i>

The `Authorization:Basic XXX` header appears in the **Headers** pane.

- b On the **Headers** tab, enter the following header details.

Request Header Attribute	Value
Content-Type	application/xml

The `Content-Type:application/xml` header appears in the **Headers** pane.

4 Contact NSX Manager to retrieve the IDs of the associated NSX Controllers.

- a Select **GET** from the drop-down menu that contains the HTTP request methods.
- b In the **URL** text box next to the selected method, enter the following URL, and click **Send**.

NSX Manager	URL
NSX Manager for the management cluster	<code>https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller</code>
NSX Manager for the shared edge and compute cluster	<code>https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller</code>

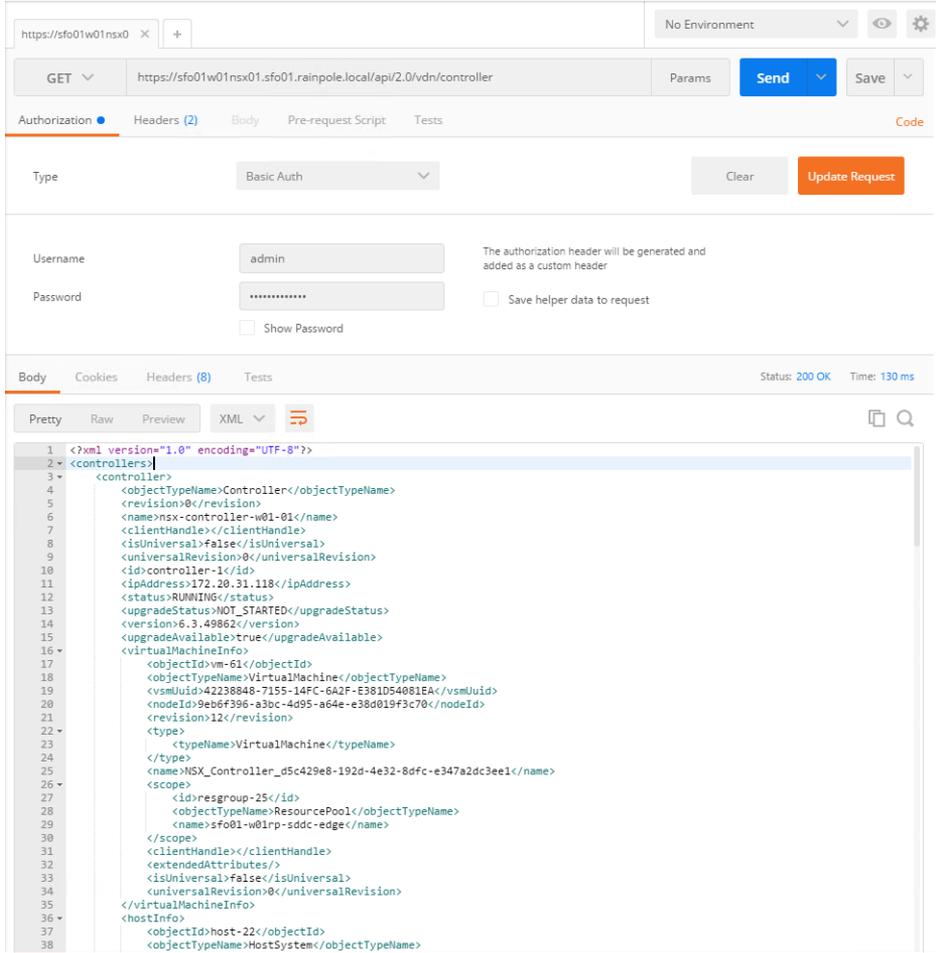
The Postman application sends a query to the NSX Manager about the installed NSX controllers.

- c After the NSX Manager sends a response back, click the **Body** tab in the response pane.

The response body contains a root `<controllers>` XML element that groups the details about the three controllers that form the controller cluster.

- d Within the <controllers> element, locate the <controller> element for each controller and write down the content of the <id> element.

Controller IDs have the controller-*id* format where *id* represents the sequence number of the controller in the cluster, for example, controller-1 in the following image.



- e Repeat the steps for the other NSX Manager.

- 5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.
  - a In the request pane at the top, select **POST** from the drop-down menu that contains the HTTP request methods, and in the **URL** text box, enter the following URL.

Replace *controller-ID* with the controller IDs you have written down.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 1	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/ <b>controller-1</b> /syslog
	NSX Controller 2	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/ <b>controller-2</b> /syslog
	NSX Controller 3	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/ <b>controller-3</b> /syslog
NSX Manager for the shared edge and compute cluster	NSX Controller 1	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/ <b>controller-1</b> /syslog
	NSX Controller 2	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/ <b>controller-2</b> /syslog
	NSX Controller 3	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/ <b>controller-3</b> /syslog

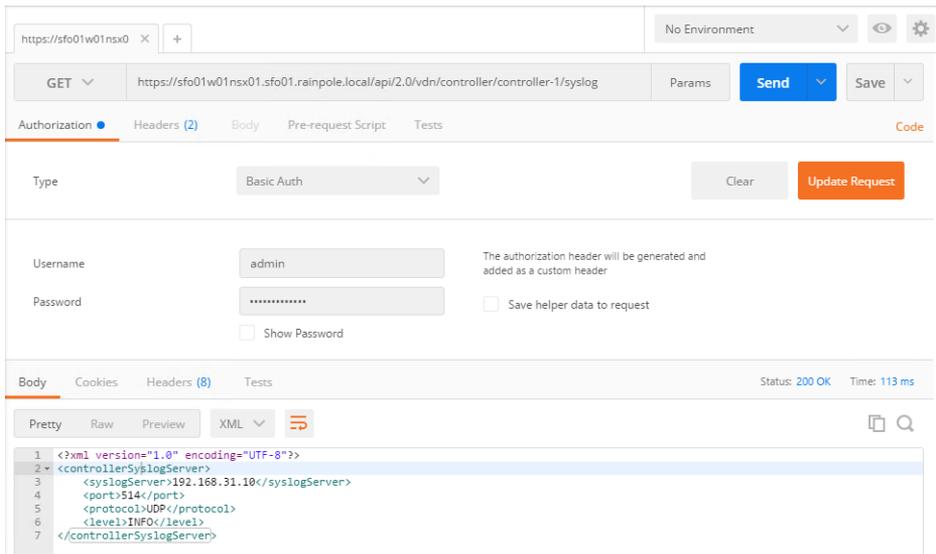
- b In the **Request** pane, click the **Body** tab, select **Raw**, and using the drop-down menu, select **XML (Application/XML)**.
- c Paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
  <syslogServer>192.168.31.10</syslogServer>
  <port>514</port>
  <protocol>UDP</protocol>
  <level>INFO</level>
</controllerSyslogServer>
```

- d Repeat the steps for the other NSX Controllers in the management cluster and in the shared edge and compute cluster.

**6** Verify the syslog configuration on each NSX Controller.

- a In the **Request** pane, from the **Method** drop-down menu, select **GET**, in the **URL** text box, enter the controller-specific syslog URL from [Step 5](#), and click the **SEND** button.
- b After the NSX Manager sends a response back, click the **Body** tab under **Response**.  
The response body contains a root <controllerSyslogServer> element, which represents the settings for the remote syslog server on the NSX Controller.
- c Verify that the value of the <syslogServer> element is 192.168.31.10.
- d Repeat the steps for the other NSX Controllers to verify the syslog configuration.



## Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight

Redirect log information from the edge services gateways, universal distributed logical router, and load balancer to vRealize Log Insight.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.

- 3 In the **Navigator**, click **NSX Edges**.
- 4 On the **NSX Edges** page, select the NSX Manager instance from the **NSX Manager** drop-down menu.

NSX Manager Instance	IP Address
NSX Manager for the management cluster	172.16.11.65
NSX Manager for the shared edge and compute cluster	172.16.11.66

The edge devices in the scope of the NSX Manager appear.

- 5 Configure the log forwarding on each edge service gateway instance.
  - a Double-click the edge device to open its user interface.

Traffic	Management NSX Edge Services Gateway	Compute NSX Edge Services Gateway
North-South Routing	sfo01m01esg01	sfo01w01esg01
North-South Routing	sfo01m01esg02	sfo01w01esg02
East-West Routing	sfo01m01udlr01	sfo01w01udlr01
East-West Routing	-	sfo01w01dlr01
Load Balancer	sfo01m01lb01	-
PSC Load Balancer	sfo01psc01	-

- b On the NSX Edge device page, click the **Manage** tab, click **Settings**, and click **Configuration**.
  - c In the **Details** pane, click **Change** next to **Syslog servers**.
  - d In the **Edit Syslog Servers Configuration** dialog box, configure the following settings and click **OK**.

Setting	Value
Syslog Server 1	192.168.31.10
Protocol	udp

- e Click **OK**.
  - f Repeat the steps for the remaining NSX Edge devices for management and shared edge and compute clusters.

The vRealize Log Insight user interface starts showing log data in the **NSX-vSphere-Overview** dashboard available under the VMware - NSX-vSphere group of content pack dashboards.

## Connect vRealize Log Insight to vRealize Automation

Connect vRealize Log to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight user interface.

## Install the vRealize Log Insight Content Packs for the Cloud Management Platform

Install the content packs for vRealize Automation, vRealize Orchestrator, and Microsoft SQL Server to add the dashboards for viewing log information about the Cloud Management Platform in vRealize Log Insight.

You install the following content packs:

- VMware - vRA 7
- VMware - Orchestrator 7.0.1+
- Microsoft - SQL Server

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - vRA 7** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, click **Install**.
- 6 Repeat the procedure to install the **VMware - Orchestrator** and **Microsoft - SQL Server** content packs.

After the installation is complete, the VMware - vRA, VMware - Orchestrator 7.0.1+ and Microsoft - SQL Server content packs appear in the **Installed Content Packs** list on the left.

## Install vRealize Log Insight Windows Agents

Install the vRealize Log Insight agent on the Windows virtual machines for the Distributed Execution Manager, IaaS Manager Service, IaaS Web Server, IaaS SQL Server, and the vSphere proxy agents. The agents forward log data to vRealize Log Insight that appears in the dashboards for vRealize Automation.

## Procedure

- 1 Log in to the Windows virtual machines of the vRealize Automation component.
  - a Open a Remote Desktop Protocol (RDP) connection to each of the following vRealize Automation virtual machines.

vRealize Automation Component	Host Name or VM Name
laaS Web Server	vra01iws01a.rainpole.local
laaS Web Server	vra01iws01b.rainpole.local
laaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
laaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
laaS DEM Worker	vra01dem01a.rainpole.local
laaS DEM Worker	vra01dem01b.rainpole.local
vSphere Proxy Agent	sfo01ias01a.sfo01.rainpole.local
vSphere Proxy Agent	sfo01ias01b.sfo01.rainpole.local
Microsoft SQL Server	vra01mssql01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	Rainpole\svc-vra
Password	svc-vra-user-password

- 2 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 3 Click the configuration drop-down menu icon  and select **Administration**.
- 4 Under **Management**, click **Agents**.
- 5 On the **Agents** page, click the **Download Log Insight Agent Version** link.
- 6 In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the .msi file on the vRealize Automation virtual machine.
- 7 Double-click the .msi file to run the installer.
- 8 With the Log Insight host name sfo01vrli01.sfo01.rainpole.local selected in the **Host** text box, click **Install**.
- 9 After the installation is complete, click **Finish**.

All VMware vRA 7 dashboards become available on the home page of vRealize Log Insight.

## Configure vRealize Log Insight Linux Agents in the vRealize Automation Appliances

vRealize Log Insight Agent comes pre-installed on the vRealize Automation Appliance. On each virtual appliance in the region, by updating the `liagent.ini` configuration file, configure the agent with the location of the vRealize Log Insight deployment.

Agent configuration for the vRealize Automation Appliances includes the following tasks:

- In the management interface of the vRealize Automation Appliances, enable log forwarding to vRealize Log Insight.
- Create an agent group for configuring log forwarding from the vRealize Automation modules on the appliances.
- Create an agent group for configuring log forwarding from the operating system of the appliances.

### Procedure

- 1 Open a Web browser and log in to the management interface of the vRealize Automation Appliance.

Setting	Value for vRealize Appliance A	Value for vRealize Appliance B
URL	<code>https://vra01svr01a.rainpole.local:5480</code>	<code>https://vra01svr01b.rainpole.local</code>
User name	<code>root</code>	<code>root</code>
Password	<code>vra_applianceA_root_password</code>	<code>vra_applianceB_root_password</code>

Setting	Value
URL	<code>https://vra01svr01a.rainpole.local:5480</code>
Username	<code>root</code>
Password	<code>vra_applianceA_root_password</code>

- 2 Configure log forwarding to vReliaze Log Insight.
  - a On the **VRA Settings** tab, click the **Logs** tab.
  - b Scroll down to the **Log Insight Agent Configuration** section.

- c Enter the following values and click **Save Settings**

Setting	Value
Host	sfo01vrli01.sfo01.rainpole.local
Port	9000
Protocol	CFAPI
SSL Enabled	Unchecked
Reconnect	30
Max Buffer Size	2000

- d Log in to the other appliance and verify that these settings have been replicated to vRealize Automation appliance vra01svr01b.rainpole.local.

- 3 Log in to the vRealize Log Insight user interface.

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

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 4 Click the configuration drop-down menu icon  and select **Administration**.

- 5 Under **Management**, click **Agents**.

- 6 Create the agent group for vRealize Automation appliances on vRealize Log Insight.

- a From the drop-down menu on the top, select **vRealize Automation 7 - Linux** from the **Available Templates** section.

- b Click **Copy Template** at the bottom of the page.

- c In the **Copy Agent Group** dialog box, enter **vRA7 – Appliance Agent Group** in the name field and click **Copy**.

- d In the agent filter fields, enter the following values pressing Enter after each host name.

Filter	Operator	Values
Hostname	Matches	<ul style="list-style-type: none"> <li>■ vra01svr01a.rainpole.local</li> <li>■ vra01svr01b.rainpole.local</li> </ul>

- e Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.

- f Click **Save New Group** at the bottom of the page.

- 7 To verify the configuration, click the **Dashboards** tab, under the **VMware - vRA 7** category click **General - Overview**.

The dashboard shows log data from the components of the vRealize Automation Appliances.

## Configure the vRealize Log Insight Linux Agents on vRealize Business

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. On each virtual appliance, by updating `liagent.ini` configuration file, configure the agent with the location of the vRealize Log Insight deployment in the region.

### Procedure

- 1 Enable Secure Shell (SSH) on the vRealize Business appliances.

- a Open a Web browser and go to the following URL.

vRealize Business Node	Virtual Appliance Management Interface URL
vRealize Business Server Appliance	<code>https://vrb01svr01.rainpole.local:5480</code>
vRealize Business Data Collector	<code>https://sfo01vrbc01.sfo01.rainpole.local:5480</code>

- b Log in using the following credentials.

Setting	Value
User name	<code>root</code>
Password	<code>vrb_server_root_password</code>

The appliance management interface of the appliance opens.

- c Click the **Administration** tab and click **Administration**.
  - d Under the **Actions** section, click **Toggle SSH setting**.
  - e Verify that the **SSH service status** is Enabled.
  - f Repeat the step for the second vRealize Business appliance.
- 2 Configure the vRealize Log Insight agent in the vRealize Business appliance.
    - a Open an SSH connection to the vRealize Business appliance using the following settings.

Setting	Value
Hostname	<ul style="list-style-type: none"> <li>■ <code>vrb01svr01.rainpole.local</code></li> <li>■ <code>sfo01vrbc01.sfo01.rainpole.local</code></li> </ul>
User name	<code>root</code>
Password	<code>vrb_server_appliance_root_password</code>

- b Edit the `liagent.ini` file using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

- c Add the following information under the [server] section.

```
[server]
hostname=sfo01vrli01.sfo01.rainpole.local
proto = cfapi
port = 9000
ssl = no
```

- d Replace all instances of the FQDN\_localhost parameter located after agent\_name with **vr01svr01.rainpole.local**.

```
[server]
hostname=sfo01vrli01.sfo01.rainpole.local
proto=cfapi
port=9000
ssl=no

; itfm server log
[filelog]ItfmServer
directory=/var/log/vrb/itfm-server
include=*
tags={"appname":"vrb", "service":"itfm_server", "agent_name":"vr01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}|\d{1,3}
.\d{1,3}\.\d{1,3}\.\d{1,3})

; itfm tomcat log
[filelog]ItfmCatalina
directory=/usr/local/ccserver/vfabric-tc-server-standard/itbm-server/logs
include=*
tags={"appname":"vrb", "service":"itfm_catalina", "agent_name":"vr01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}|\d{1,3}
.\d{1,3}\.\d{1,3}\.\d{1,3})

; data collector log
[filelog]DataCollector
directory=/var/log/vrb/data-collector
include=*
tags={"appname":"vrb", "service":"data_collector", "agent_name":"vr01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}|\d{1,3}
.\d{1,3}\.\d{1,3}\.\d{1,3})
```

- e Press Esc and type :wq! to save the file.
- f Start the Log Insight agent.

```
/etc/init.d/liagentd start
```

- g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

- h Turn on autorun by default for the Log Insight agent.

```
chkconfig liagentd on
```

- i Repeat the procedure to configure the vRealize Business Data Collector at sfo01vrbc01.sfo01.rainpole.local.

## Configure the vRealize Log Insight Linux Agents on vRealize Business

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. On each virtual appliance, by updating liagent.ini configuration file, configure the agent with the location of the vRealize Log Insight deployment in the region.

**Procedure****1** Enable Secure Shell (SSH) on the vRealize Business appliances.

- a Open a Web browser and go to the following URL.

<b>vRealize Business Node</b>	<b>Virtual Appliance Management Interface URL</b>
vRealize Business Server Appliance	https://vrb01svr01.rainpole.local:5480
vRealize Business Data Collector	https://sfo01vrbc01.sfo01.rainpole.local:5480

- b Log in using the following credentials.

<b>Setting</b>	<b>Value</b>
User name	root
Password	<i>vrb_server_root_password</i>

The appliance management interface of the appliance opens.

- c Click the **Administration** tab and click **Administration**.
  - d Under the **Actions** section, click **Toggle SSH setting**.
  - e Verify that the **SSH service status** is Enabled.
  - f Repeat the step for the second vRealize Business appliance.
- 2** Configure the vRealize Log Insight agent in the vRealize Business appliance.

- a Open an SSH connection to the vRealize Business appliance using the following settings.

<b>Setting</b>	<b>Value</b>
Hostname	<ul style="list-style-type: none"> <li>■ vrb01svr01.rainpole.local</li> <li>■ sfo01vrbc01.sfo01.rainpole.local</li> </ul>
User name	root
Password	<i>vrb_server_appliance_root_password</i>

- b Edit the `liagent.ini` file using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

- c Add the following information under the `[server]` section.

```
[server]
hostname=sfo01vrli01.sfo01.rainpole.local
proto = cfapi
port = 9000
ssl = no
```

- d Replace all instances of the `FQDN_localhost` parameter located after `agent_name` with `vr01svr01.rainpole.local`.

```
[server]
hostname=sfo01vrli01.sfo01.rainpole.local
proto=cfapi
port=9000
ssl=no

; itfm server log
[filelog|ItfmServer]
directory=/var/log/vrb/itfm-server
include=*
tags={"appname":"vrb", "service":"itfm_server", "agent_name":"vr01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})

; itfm tomscat log
[filelog|ItfmCatalina]
directory=/usr/local/tcserver/vfabric-tc-server-standard/itbm-server/logs
include=*
tags={"appname":"vrb", "service":"itfm_catalina", "agent_name":"vr01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})

; data collector log
[filelog|DataCollector]
directory=/var/log/vrb/data-collector
include=*
tags={"appname":"vrb", "service":"data_collector", "agent_name":"vr01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})
```

- e Press Esc and type `:wq!` to save the file.
- f Start the Log Insight agent.

```
/etc/init.d/liagentd start
```

- g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

- h Turn on autorun by default for the Log Insight agent.

```
chkconfig liagentd on
```

- i Repeat the procedure to configure the vRealize Business Data Collector at `sfo01vrbc01.sfo01.rainpole.local`.

## Install the vRealize Log Insight Content Pack for Linux

Install the content pack for Linux to add dashboards for viewing log information in vRealize Log Insight from the operating system of the management virtual appliances in the region.

**Procedure**

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **Linux** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, accept the License Agreement, and click **Install**.

After the installation is complete, the **Linux** content pack appears in the **Installed Content Packs** list on the left.

## Configure a Log Insight Agent Group for the Management Virtual Appliances

After you install the content pack for Linux, configure an agent group to apply common settings to the agents on the appliances in the region.

**Procedure**

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Agents**.
- 4 From the drop-down at the top, select **Linux** from the **Available Templates** section.
- 5 Click **Copy Template**.
- 6 In the **Copy Agent Group** dialog box, enter **VA – Linux Agent Group** in the **Name** text box and click **Copy**.

- 7 In the agent filter fields, use the following selections.

Press Enter to separate the host name values.

Filter	Operator	Values
Hostname	matches	<ul style="list-style-type: none"> <li>■ vrops01svr01a.rainpole.local</li> <li>■ vrops01svr01b.rainpole.local</li> <li>■ vrops01svr01c.rainpole.local</li> <li>■ sfo01vropsc01a.sfo01.rainpole.local</li> <li>■ sfo01vropsc01b.sfo01.rainpole.local</li> <li>■ vra01svr01a.rainpole.local</li> <li>■ vra01svr01b.rainpole.local</li> <li>■ vrb01svr01.rainpole.local</li> <li>■ sfo01vrbc01.sfo01.rainpole.local</li> </ul>

- 8 Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.
- 9 Click **Save New Group** at the bottom of the page.
- 10 Verify that log data is showing up on the Linux dashboards.

- a On the main navigation bar, click **Dashboards**.
- b Expand **Linux** and click **Security - Overview**.

You see events that have occurred over the past 48 hours.

## Configure Log Retention and Archiving

Set log retention to one week and archive logs for 90 days according to the *VMware Validated Design Architecture and Design* documentation.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

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

3 Configure notification about reaching a retention threshold of one week.

Log Insight continually estimates how long data can be retained with the currently available pool of storage.

If the estimation drops below the retention threshold of one week, Log Insight immediately notifies the administrator that the amount of searchable log data is likely to drop.

- a Under **Configuration**, click **General**.
- b On the **General Configuration** page, under the **Alerts** section, select the **Send a notification when capacity drops below** check box next to **Retention Notification Threshold**, and enter a 1-week period in the text box.
- c Click **Save**.

4 Configure data archiving.

- a Under **Configuration**, click **Archiving**.
- b Toggle **Enable Data Archiving** on.
- c In the **Archive Location** text box, enter the path in the form of `nfs://nfs-server-address/V2D_vRLI_MgmtA_400GB` to an NFS partition where logs will be archived.
- d Click **Test** next to the **Archive Location** text box to verify that the share is accessible.
- e Click **Save**.