

# Intelligent Operations Use Case Deployment Using vRealize Suite Lifecycle Manager

27 MAR 2018

VMware Validated Design 4.2

VMware Validated Design for Intelligent Operations 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 Intelligent Operations 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 Intelligent Operations 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	23
Configure the vRealize Suite Lifecycle Manager Appliance	25
Register vRealize Suite Lifecycle Manager with My VMware	34
OVA Configuration in vRealize Suite Lifecycle Manager	35
Add a Data Center to vRealize Suite Lifecycle Manager	37
<b>4 Pre-Deployment Tasks for the Intelligent Operations Use Case</b>	<b>39</b>
Generate Certificates for the Intelligent Operations Solution Path	39
Pre-Deployment Tasks for vRealize Operations Manager	41
Prerequisites for Deploying vRealize Log Insight	43
<b>5 Deployment Paths for the Intelligent Operations Use Case with vRealize Suite Lifecycle Manager</b>	<b>45</b>
Deploy the Intelligent Operations Use Case with the vRealize Suite Lifecycle Manager Installation Wizard	45
Deploy the Intelligent Operations Use Case with a vRealize Suite Lifecycle Manager JSON Configuration File	52
<b>6 Post-Deployment Tasks for vRealize Operations Manager</b>	<b>57</b>
Configure the Load Balancer for vRealize Operations Manager	58
Move vRealize Operations Analytics Cluster and Remote Collector Nodes to Virtual Machine Folders	62
Configure DRS Anti-Affinity Rules for vRealize Operations Manager	63

Proceed Using Evaluation Mode for vRealize Operations Manager	64
Replace vRealize Operations Manager Certificate	65
Group Remote Collector Nodes	66
Add an Authentication Source for the Active Directory	66
Configure User Access in vSphere for Integration with vRealize Operations Manager	67
Add vCenter Adapter Instances to vRealize Operations Manager	71
Connect vRealize Operations Manager to the NSX Manager Instances	73
Enable Storage Device Monitoring in vRealize Operations Manager	79
Enable vSAN Monitoring in vRealize Operations Manager	82
Configure Email Alerts for vRealize Operations Manager	84
<b>7 Post-Deployment Tasks for vRealize Log Insight</b>	<b>86</b>
Move vRealize Log Insight Cluster Nodes to a Virtual Machine Folder	87
Configure a DRS Anti-Affinity Rule for vRealize Log Insight	88
Configure the vRealize Log Insight Master node	88
Enable Active Directory Support for vRealize Log Insight	89
Replace the Certificate of vRealize Log Insight	90
Connect vRealize Log Insight to the vSphere Environment	91
Connect vRealize Log Insight to vRealize Operations Manager	96
Connect vRealize Log Insight to the NSX Instances	103
Install the vRealize Log Insight Content Pack for Linux	109
Configure a Log Insight Agent Group for the Management Virtual Appliances	110
Configure Log Retention and Archiving	111

# About Intelligent Operations Use Case Deployment Using vRealize Suite Lifecycle Manager

*Intelligent Operations 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 *Intelligent Operations 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:

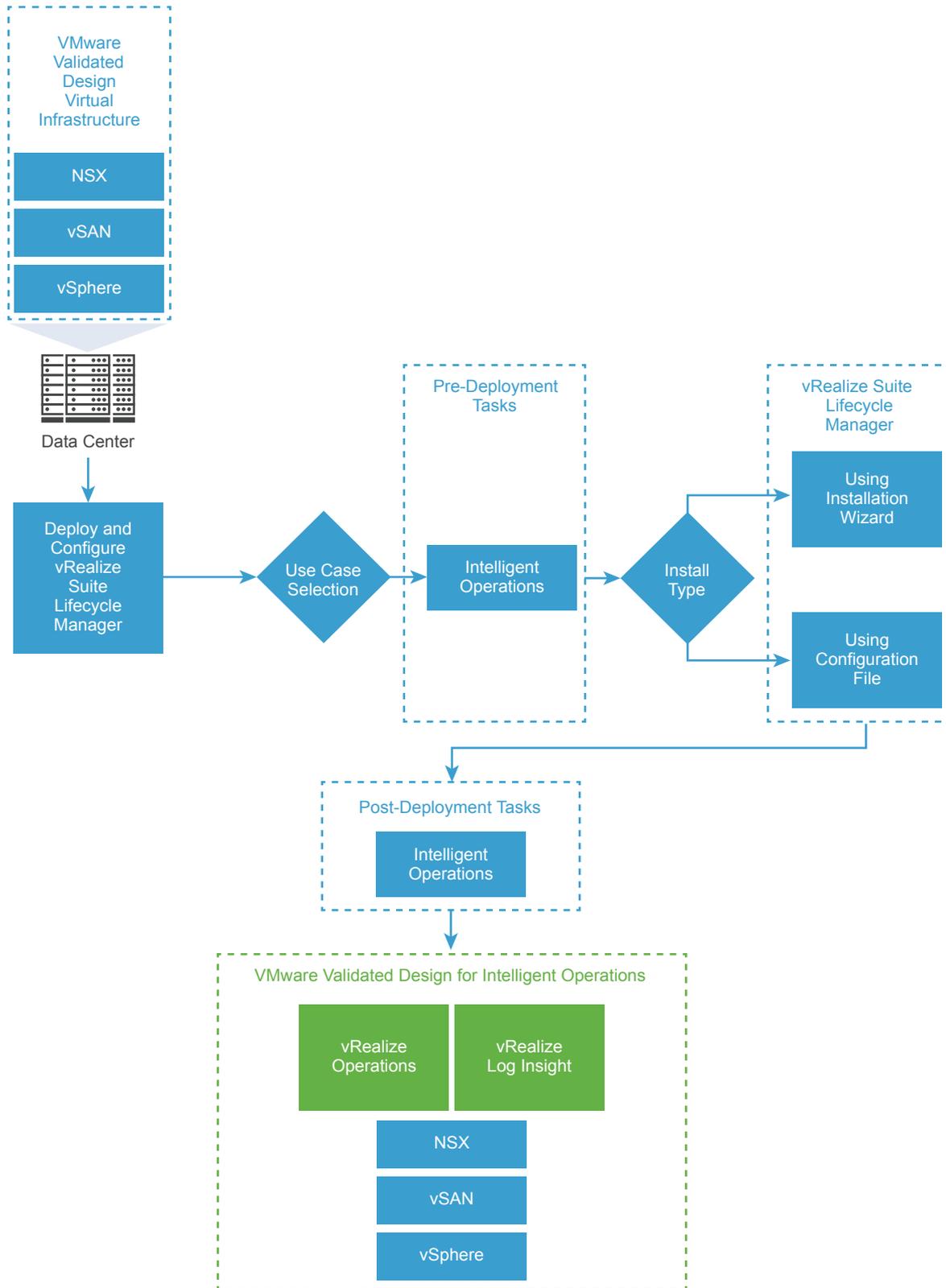
- 1 **IT Automating IT** – Enables automation and simplification of workload provisioning tasks of production-ready infrastructure and applications in the SDDC.
- 2 **Intelligent Operations** – Enables proactive identification and remediation of performance, capacity, and configuration issues in the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

# Intelligent Operations Solution Path

1

To deploy the Intelligent Operations 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 JSON configuration file. You can follow the step-by-step instructions in the *Monitoring and Alerting* documentation.

Figure 1-1. vRealize Suite Lifecycle Manager Solution Path for Intelligent Operations



## 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 A

In 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 Operations Manager](#).
- b [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 using the JSON file.

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

6 Perform post-deployment tasks for the products utilized in the use case:

- a Perform post-deployment tasks for vRealize Operations Manager.  
See [Chapter 6 Post-Deployment Tasks for vRealize Operations Manager](#).
- b Perform post-deployment tasks for vRealize Log Insight.  
See [Chapter 7 Post-Deployment Tasks for vRealize Log Insight](#).

- 7 Implement your Intelligent Operations scenarios using the products that you just installed. The *Monitoring and Alerting* documentation for step-by-step instructions about configuring vRealize Operations Manager and vRealize Log Insight. See <https://docs.vmware.com/en/VMware-Validated-Design/4.2/com.vmware.vvd.sddc-monitor.doc/GUID-8B4ADD7F-D56C-4A4E-A615-FBB533AA2695.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](#) 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 [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)
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/vr1cm**.
  - 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>vrs1cm_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)	vrsicm_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 Intelligent Operations 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>vrsicm_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 Intelligent Operations solution path, click the **Download** icon from the **Actions** column.

Solution Path	Product Name	Product Version
Intelligent Operations	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 Intelligent Operations 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 Intelligent Operations solution path.

Solution Path	Product Name	Product Version	Product OVA
Intelligent Operations	vRealize Operations Manager vRealize Log Insight	Refer to the Release Notes	vRealize Operations Manager .ova file vRealize Log Insight .ova file

- Create a directory on the vRealize Suite Lifecycle Manager appliance for product OVAs.
  - Open an SSH connection to `vrs011cm01.rainpole.local`.
  - Log in using the following credentials:

Setting	Value
Username	root
Password	<code>vrs/lcm_root_password</code>

- 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 **vrs01lcm01.rainpole.local**.

b Log in using following credentials:

Setting	Value
Username	root
Password	vrslcm_root_password

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://vrs01lcm01.rainpole.local/vr1cm**.
  - b Log in using the following credentials:

Setting	Value
User name	admin@localhost
Password	vrslcm_admin_password

- 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	/data/binaries/OVA

- 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
Product Binary Type	Install
Product Binary	vRealize Log Insight .ova file

- 8 Repeat the process for each product OVA required by the Intelligent Operations 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	<code>admin@localhost</code>
Password	<code>vrslcm_admin_password</code>

- 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	<code>sfo01-m01dc</code>
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	<code>sfo01m01vc01.sfo01.rainpole.local</code>
User Name	<code>svc-vrslcm-vsphere@rainpole.local</code>
Password	<code>svc-vrslcm-vsphere_password</code>
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 Intelligent Operations Use Case

# 4

Before deploying the Intelligent Operations use case, perform the following pre-deployment tasks.

## 1 [Generate Certificates for the Intelligent Operations Solution Path](#)

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

## 2 [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.

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

## Generate Certificates for the Intelligent Operations Solution Path

Use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates that are 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 Intelligent Operations Solution Path**

Host Name or Service	Configuration Files
Operations Management Layer	
vRealize Operations Manager	<ul style="list-style-type: none"> <li>■ vrops01svr01.rainpole.local</li> <li>■ vrops01svr01a.rainpole.local</li> <li>■ vrops01svr01b.rainpole.local</li> <li>■ vrops01svr01c.rainpole.local</li> </ul>
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>

6 Verify that each configuration file includes FQDNs and host names in the dedicated sections.

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 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 4-2. 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 4-3. 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 4-4. 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>
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>

Prerequisite	Value
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 4-5. 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 4-6. 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
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>	ntp.sfo01.rainpole.local

## 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>
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 <code>rainpole.local</code> 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 Intelligent Operations Use Case with vRealize Suite Lifecycle Manager

# 5

vRealize Suite Lifecycle Manager provides two paths for deploying the Intelligent Operations use case.

You can deploy the Intelligent Operations 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 Intelligent Operations Use Case with the vRealize Suite Lifecycle Manager Installation Wizard](#)
- [Deploy the Intelligent Operations Use Case with a vRealize Suite Lifecycle Manager JSON Configuration File](#)

## Deploy the Intelligent Operations Use Case with the vRealize Suite Lifecycle Manager Installation Wizard

You can deploy all components required for the Intelligent Operations 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 Intelligent Operations with the Installation Wizard

When you deploy the Intelligent Operations 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 Intelligent Operations 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	Intelligent Operations
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 Intelligent Operations 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)
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 Operations Manager with vRealize Suite Lifecycle Manager](#)
  - b [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 Intelligent Operations use case by using the vRealize Suite Lifecycle Manager web interface.

## 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	vrops01svr01a
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
Master Hostname	vrops01svr01a.rainpole.local
Master IP Address	192.168.11.31
Extended Storage (1 TB)	sfo01-m01-vsan01
Deploy Option	<b>medium</b>

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	<b>medium</b>

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

Option	Value
Data IP Address	192.168.11.33
Extended Storage (1 TB)	sfo01-m01-vsan01
Deploy Option	<b>medium</b>

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
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

Option	Value
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01b
Gateway	192.168.31.1
Deploy Option	medium

- 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
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 Intelligent Operations in vRealize Suite Lifecycle Manager

You can monitor the status of the Intelligent Operations 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/vrlicm**.
  - 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: Intelligent Operations 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: Intelligent Operations 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 Intelligent Operations Use Case with a vRealize Suite Lifecycle Manager JSON Configuration File

You can deploy all components required for the Intelligent Operations 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 Intelligent Operations with a JSON Configuration File

You can deploy the products that are used by the Intelligent Operations 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, click **Using Configuration File**.
- 4 On the **Data Center and Environment** page, enter the following information.

Setting	Value
Data Center	sfo01-m01dc
Environment Type	Production

Setting	Value
Environment Name	Intelligent Operations
Administrator Email	<i>default_deployment_administrator_email</i>
Default Password	<i>default_deployment_password</i>
Confirm Default Password	<i>default_deployment_password</i>
Customer Experience Improvement Program	Selected

- 5 On the **Product Config JSON** section, copy and paste the example JSON configuration file below.

**Note** You are responsible for reviewing and supplying the license, certificate, keyphrases, portgroups, and key information.

- 6 Click **Create Environment**.

### Example: Example JSON Configuration File for Intelligent Operations

```
{
  "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": "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"
    }
  },
  {
    "type": "replica",
    "properties": {
      "name": "vrops01svr01b",
      "ipAddress": "192.168.11.32",
      "hostname": "vrops01svr01b.rainpole.local",
      "extendedStorage": "sfo01-m01-vsan01"
    }
  },
  {
    "type": "data",
    "properties": {
      "name": "vrops01svr01c",
      "ipAddress": "192.168.11.33",
      "hostname": "vrops01svr01c.rainpole.local",
      "extendedStorage": "sfo01-m01-vsan01"
    }
  },
  {
    "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"
    }
  },
  {
    "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"
    }
  }
],
"contents": []
},

```

```

{
  "id": "vrli",
  "version": "4.5.1",
  "clusterVIP": [],
  "properties": {
    "vrliClusterVips": "192.168.31.10#sfo01vrli01.sfo01.rainpole.local"
  },
  "nodes": [
    {
      "type": "vrli-master",
      "properties": {
        "vrliAdminEmail": "admin@rainpole.local",
        "vrliLicenseKey": "xxxxx-xxxxx-xxxxx-xxxxxx-xxxxx",
        "name": "sfo01vrli01a",
        "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"
      }
    },
    {
      "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"
      }
    },
    {
      "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"
      }
    }
  ],
  "contents": []
}

```

## Monitor the Deployment for Intelligent Operations in vRealize Suite Lifecycle Manager

You can monitor the status of the Intelligent Operations 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>vrs1cm_admin_password</i>

- 2 In the **Navigator**, click **Requests** and validate that CREATE\_ENVIRONMENT for Environment Name: Intelligent Operations 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: Intelligent Operations 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 Operations Manager

# 6

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 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.

**12 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.

**13 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 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

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	<i>vrops_admin_password</i>

- 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	<i>svc-vrops_password</i>	<i>svc-vrops_password</i>
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

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>■ <b>Virtual Machine.Configuration.Change CPU Count</b></li> <li>■ <b>Virtual Machine.Configuration. Change Resource</b></li> <li>■ <b>Virtual Machine.Configuration. Memory</b></li> <li>■ <b>Virtual Machine.Interaction. Power Off</b></li> <li>■ <b>Virtual Machine.Interaction. Power On</b></li> <li>■ <b>Virtual Machine.Snapshot Management. Create Snapshot</b></li> <li>■ <b>Virtual Machine.Snapshot Management. Remove Snapshot</b></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-vmware 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-vmware@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://vroops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vroops_admin_password</i>

- 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	<i>svc-vrops-vsphere-password</i>

- 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	nsx_admin_password

- 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	<i>svc-vrops-nsx_password</i>
vCenter User Name	svc-vrops-nsx@rainpole.local
vCenter Password	<i>svc-vrops-nsx_password</i>

- 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	<i>vrops_admin_password</i>

- 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**.

## 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

# 7

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 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.

## 10 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.

## 11 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	<i>vri_admin_password</i>

- 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	<i>vsphere_admin_password</i>

- 2 Update the host profile for the 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 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.

## 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	<code>vrops_admin_password</code>

- 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	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Integration**, click **vRealize Operations**.
- 4 On the **vRealize Operations Manager** page, configure the integration settings for vRealize Operations Manager.

Setting	Value
Hostname	vrops01svr01.rainpole.local
Username	svc-vrli-vrops@rainpole.local
Password	svc-vrli-vrops_password
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	Value
Display Name	Log Insight Adapter - sfo01vrl01
Description	vRealize Log Insight for sfo01
Log Insight server	sfo01vrl01.sfo01.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 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	vrops_root_password

- 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=sfo01vr1i01.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":"vR0ps", "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	vrli_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	<i>vri_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 - 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>

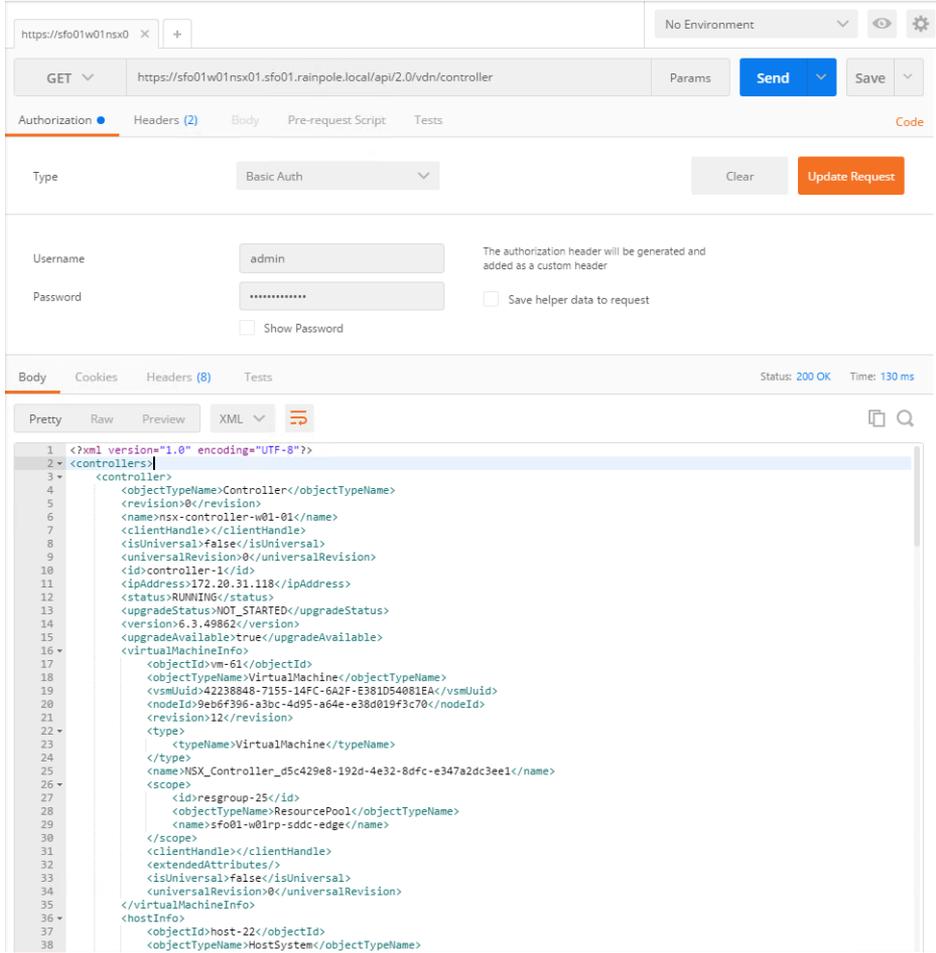
The Postman application sends a query to the NSX Manager about the installed NSX controllers.

- 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.

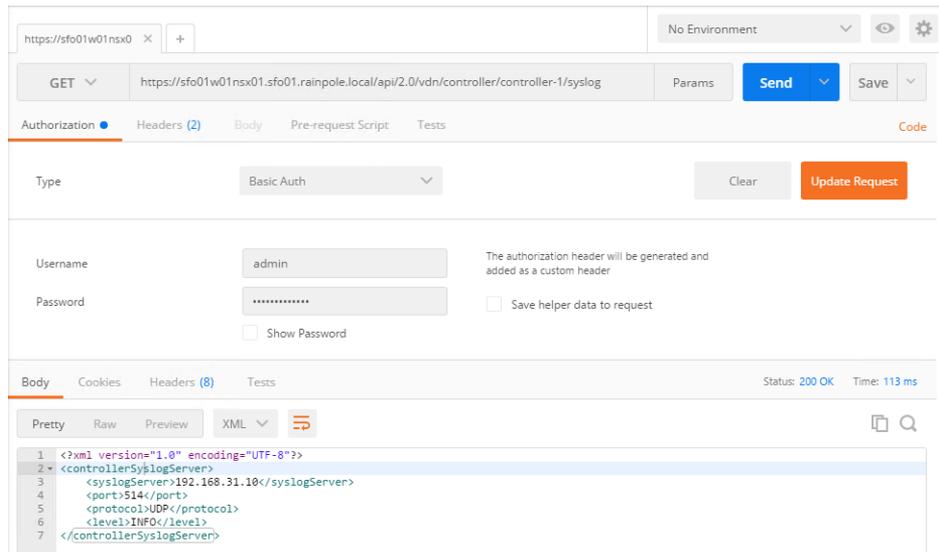
a In the **Request** pane, from the **Method** drop-down menu, select **GET**, in the **URL** text box, enter the controller-specific syslog URL from [Step 5](#), and click the **SEND** button.

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.

## 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>vri_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>vri_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> </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	vri_admin_password

- 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**.