Use Case Deployment Using vRealize Suite Lifecycle Manager

Modified on 21 DEC 2017
VMware Validated Design 4.1

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Use Case Deployment Using vRealize Suite Lifecycle Manager

Use Case Deployment Using vRealize Suite Lifecycle Manager describes an alternative method to deploy and configure a VMware Validated Design use case by using 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. Additional documentation is available for each use case.

This guide helps you deploy and configure the products for each use case. See Chapter 1 vRealize Suite Lifecycle Manager Solution Paths. This guide provides step-by-step instructions for the following tasks:

- Deployment and configuration of the vRealize Suite Lifecycle Manager appliance.
- Pre-deployment tasks for some of the products that are used by the use case.
- Deployment of the products needed by a use case using vRealize Suite Lifecycle Manager.
- Post-deployment tasks for products that are required by a use case.

Note This guide does not include instructions for deploying the foundation products (ESXi, vCenter Server, VMware NSX, vSphere Update Manager Download Service). See the *Deployment for Region A* document in the VMware Validated Design for the Software-Defined Data Center documentation.

Intended Audience

The *Use Case Deployment 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 the base for a use case.

vRealize Suite Lifecycle Manager Solution Paths

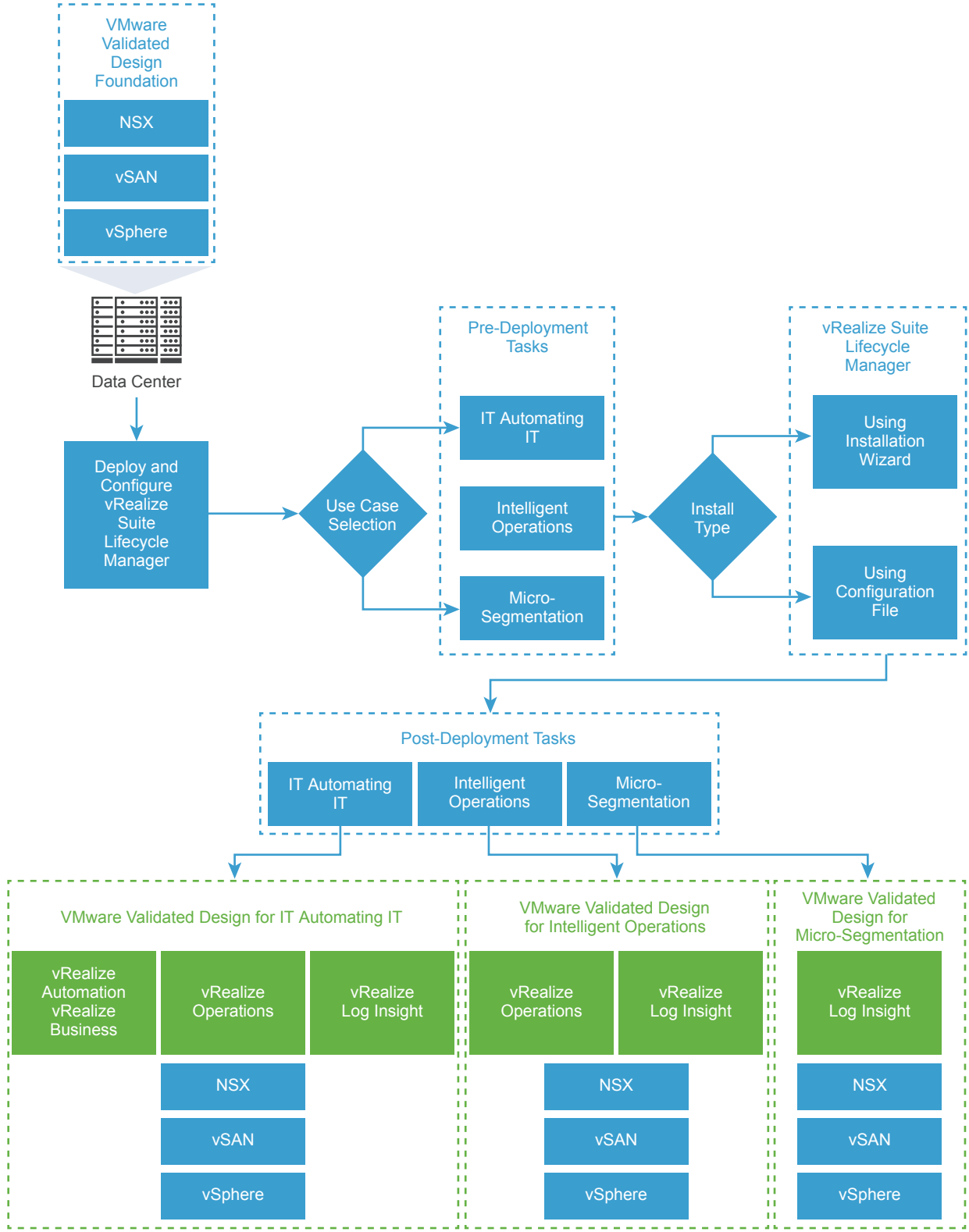
1

Use Case Deployment Using vRealize Suite Lifecycle Manager deploys use case solutions on the SDDC foundation which consist of VMware vSphere and VMware NSX for vSphere components.

vRealize Suite Lifecycle Manager can deploy all applications that are needed by a VMware Validated Design use case. You can run a wizard and provide input, as prompted by the GUI, or you can import a JSON file for the use case with predefined parameters. In either case, you customize the size, host names, networking information, and so on as part of deployment, as discussed in this guide.

Each use case requires some pre-deployment and post-deployment configuration depending on the products included in the use case. The following overview of all solution paths is followed by details for each solution path.

Figure 1-1. vRealize Suite Lifecycle Manager Solution Paths for Use Cases

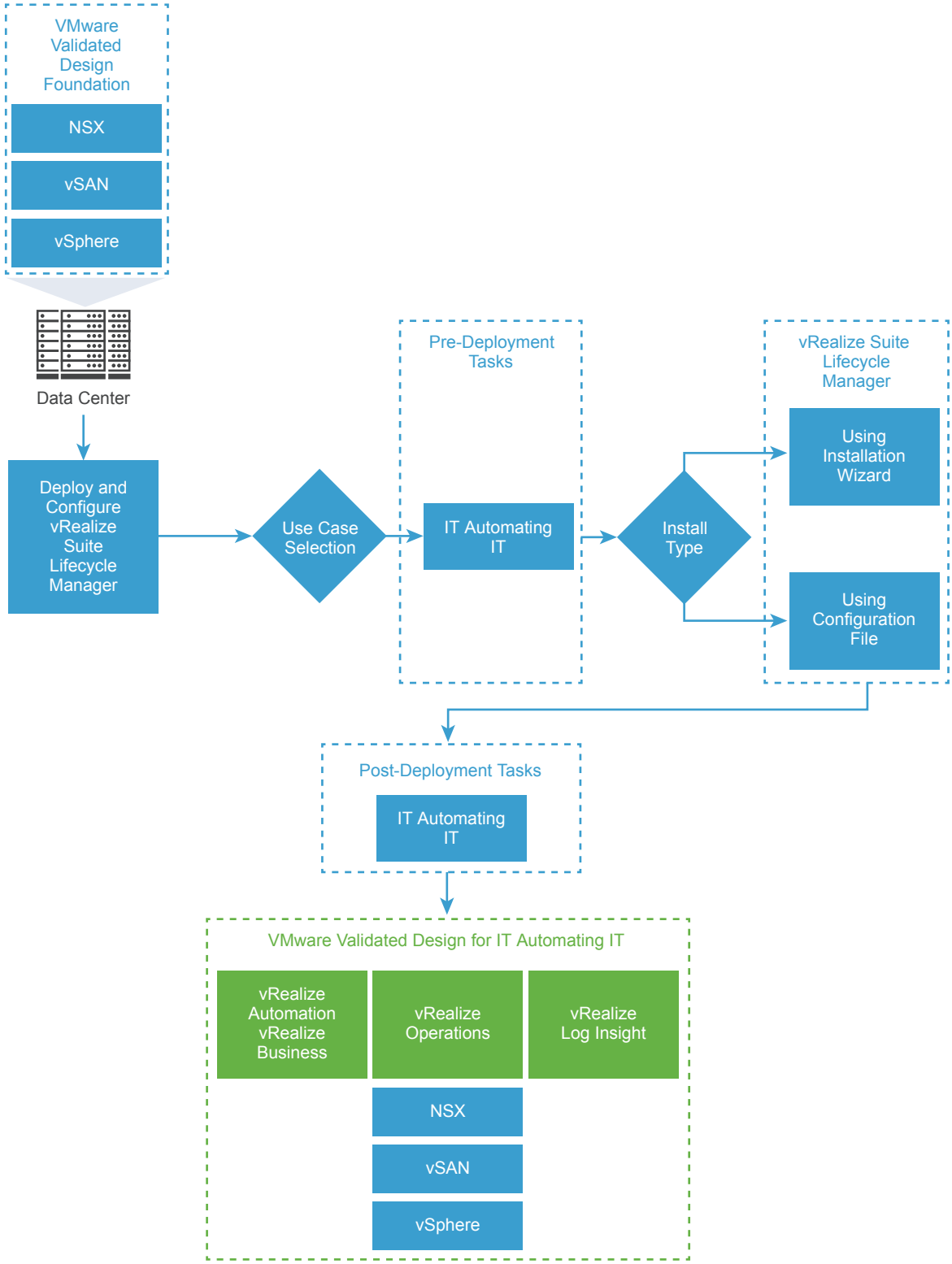


This chapter includes the following topics:

IT Automating IT Solution Path

To deploy the IT Automating IT use case, you perform pre-deployment tasks that include installing the SDDC foundation. Then you deploy the applications needed by this solution path using the vRealize Suite Lifecycle Manager GUI or by importing a JSON file. After that, you can select from the use cases in the *Scenarios* guide for the VMware Validated Design for IT Automating IT and follow the step-by-step instructions in that document.

Figure 1-2. vRealize Suite Lifecycle Manager Solution Path for IT Automating IT



Procedure

1 As your basis, you deploy the virtual infrastructure, as discussed in *Deployment for Region A* at http://pubs.vmware.com/vmware-validated-design-41/topic/com.vmware.vvd.sddc-deploya.doc/GUID-657DB777-D919-4C23-BA5E-B98D8A91CA8B.html.

   a Install and Configure ESXi Hosts.

   b Deploy and Configure the Platform Services Controller and vCenter Server Component

   c Deploy and Configure the Management Cluster NSX Instance

   d Deploy and Configure the Shared Edge and Compute Cluster Components

   e Deploy and Configure Shared Edge and Compute Cluster NSX Instance

   f Replace Certificates

   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 tasks.

   Note The VMware Validated Design for the Software-Defined Data Center *Deployment for Region A* includes vSphere Data Protection. That product is not needed here.

2 Deploy the vRealize Suite Lifecycle Manager appliance, upload the OVA file for your use case, and complete certificate setup.

   See Chapter 2 Deploy and Configure the vRealize Suite Lifecycle Manager Appliance.

3 Perform pre-deployment tasks for the products that are used by this use case.

   a Pre-deployment Tasks for vRealize Automation.

   b Pre-Deployment Tasks for vRealize Operations Manager.

   c Pre-Deployment Tasks for vRealize Log Insight.

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

4 Deploy the required products by running the installation wizard or by using the JSON file.

   - Run the IT Automating IT Installation Wizard from vRealize Suite Lifecycle Manager.
   - Chapter 7 Import a JSON File to Deploy IT Automating IT.

5 Replace certificate for the products that this use case uses:

   a Perform certificate replacement for vRealize Automation suite of products, which includes vRealize Orchestrator and vRealize Business for Cloud.

   See http://pubs.vmware.com/vmware-validated-design-41/index.jsp#com.vmware.vvd.sddc-certificate.doc/GUID-2B8F9D8F-00C9-404B-ABDC-9F1C78A21480.html

   b Perform certificate replacement for vRealize Operations Manager.

   See http://pubs.vmware.com/vmware-validated-design-41/index.jsp#com.vmware.vvd.sddc-certificate.doc/GUID-9D6F0E22-A772-40E5-A840-2F025B74C4EE.html

   c Perform certificate replacement for vRealize Log Insight.

   See http://pubs.vmware.com/vmware-validated-design-41/index.jsp#com.vmware.vvd.sddc-certificate.doc/GUID-E52991A8-A938-4044-87BF-19B5C85861FA.html

6 Perform post-deployment tasks for the products that this use case uses:

   a Perform post-deployment tasks for the vRealize Automation suite of products, which includes vRealize Orchestrator and vRealize Business for Cloud.

   See Post-Deployment Tasks for vRealize Automation.

   b Perform post-deployment tasks for vRealize Operations Manager.

   See Post-Deployment Tasks for vRealize Operations Manager.

   c Perform post-deployment tasks for vRealize Log Insight.

   See Post-Deployment Tasks for vRealize Log Insight.

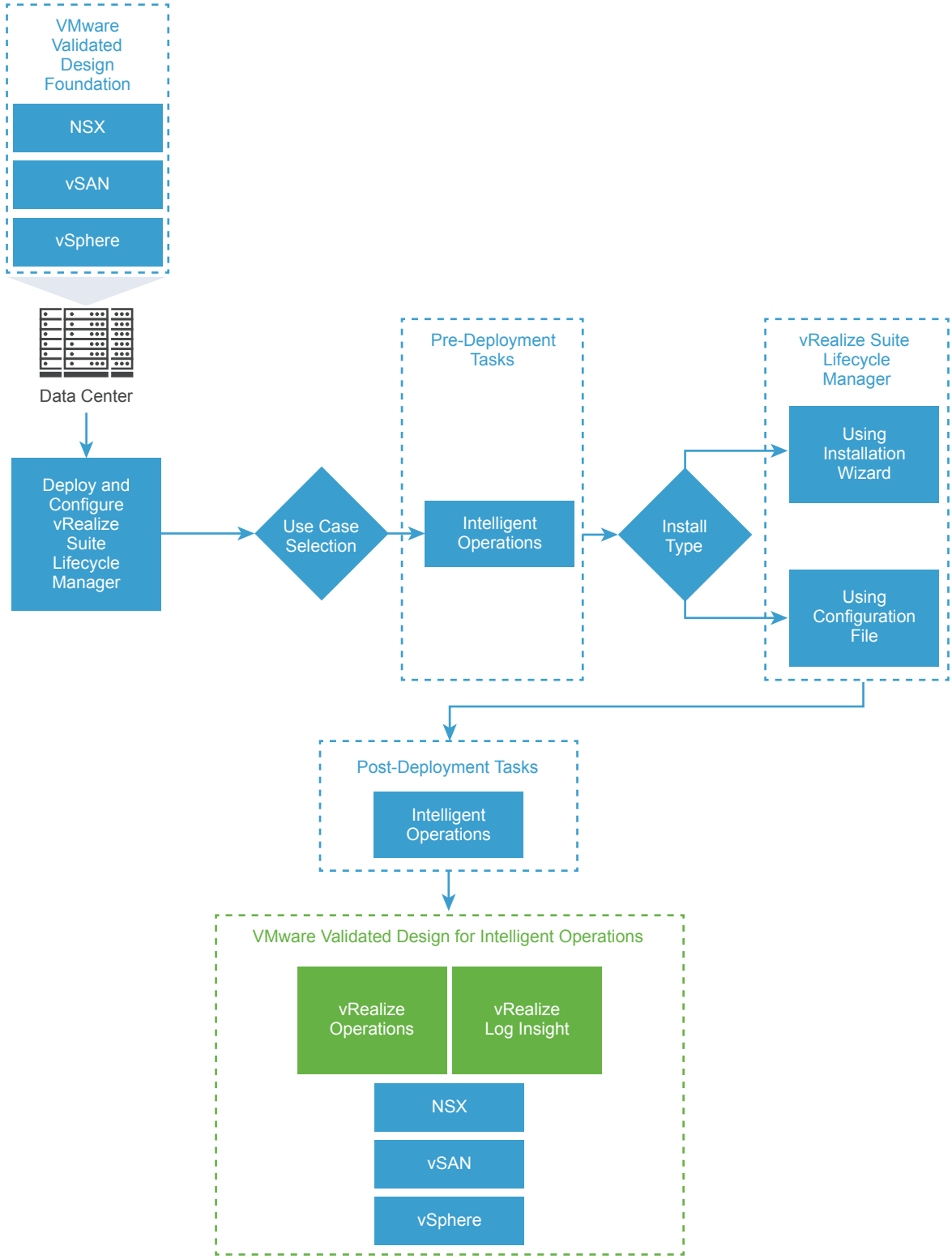
7 Select one or more of the scenarios for IT Automating IT and implement them.

   See the *Scenarios* guide for IT Automating IT http://pubs.vmware.com/vmware-validated-design-41/topic/com.vmware.vvd.it.automation-usecases.doc/GUID-2BA1821B-7F87-4CA8-B0E4-15EA28D12128.html.

Intelligent Operations Solution Path

To deploy the Intelligent Operations use case, you perform pre-deployment tasks that include installing the SDDC foundation. Then you deploy the applications needed by this solution path using the vRealize Suite Lifecycle Manager GUI or by importing a JSON file. After that, you can follow the step-by-step instructions in the *Monitoring and Alerting* documentation.

Figure 1-3. 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 http://pubs.vmware.com/vmware-validated-design-41/topic/com.vmware.vvd.sddc-deploya.doc/GUID-657DB777-D919-4C23-BA5E-B98D8A91CA8B.html.

   a Install and Configure ESXi Hosts.

   b Deploy and Configure the Platform Services Controller and vCenter Server Component

   c Deploy and Configure the Management Cluster NSX Instance

   d Deploy and Configure the Shared Edge and Compute Cluster Components

   e Deploy and Configure Shared Edge and Compute Cluster NSX Instance

   f Replace Certificates

   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.

   Note The VMware Validated Design for the Software-Defined Data Center *Deployment for Region A* includes vSphere Data Protection. That product is not needed here.

2 Deploy the vRealize Suite Lifecycle Manager appliance, upload the OVA file for your use case, and complete certificate setup.

   See Chapter 2 Deploy and Configure the vRealize Suite Lifecycle Manager Appliance.

3 Perform pre-deployment tasks for the products that are used by this use case.

   a Pre-Deployment Tasks for vRealize Operations Manager.

   b Pre-Deployment Tasks for vRealize Log Insight.

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

4 Deploy the required products by running the installation wizard or using the JSON file.

   - Chapter 5 Run the Intelligent Operations Installation Wizard with vRealize Suite Lifecycle Manager.
   - Chapter 8 Import a JSON File to Deploy Intelligent Operations.

5 Replace certificate for the products that this use case uses:

   a Perform certificate replacement for vRealize Operations Manager.

   See http://pubs.vmware.com/vmware-validated-design-41/index.jsp#com.vmware.vvd.sddc-certificate.doc/GUID-9D6F0E22-A772-40E5-A840-2F025B74C4EE.html

   b Perform certificate replacement for vRealize Log Insight.

   See http://pubs.vmware.com/vmware-validated-design-41/index.jsp#com.vmware.vvd.sddc-certificate.doc/GUID-E52991A8-A938-4044-87BF-19B5C85861FA.html

6 Perform post-deployment tasks for the products that this use case uses:

   a Perform post-deployment tasks for vRealize Operations Manager.

   See Post-Deployment Tasks for vRealize Operations Manager.

   b Perform post-deployment tasks for vRealize Log Insight.

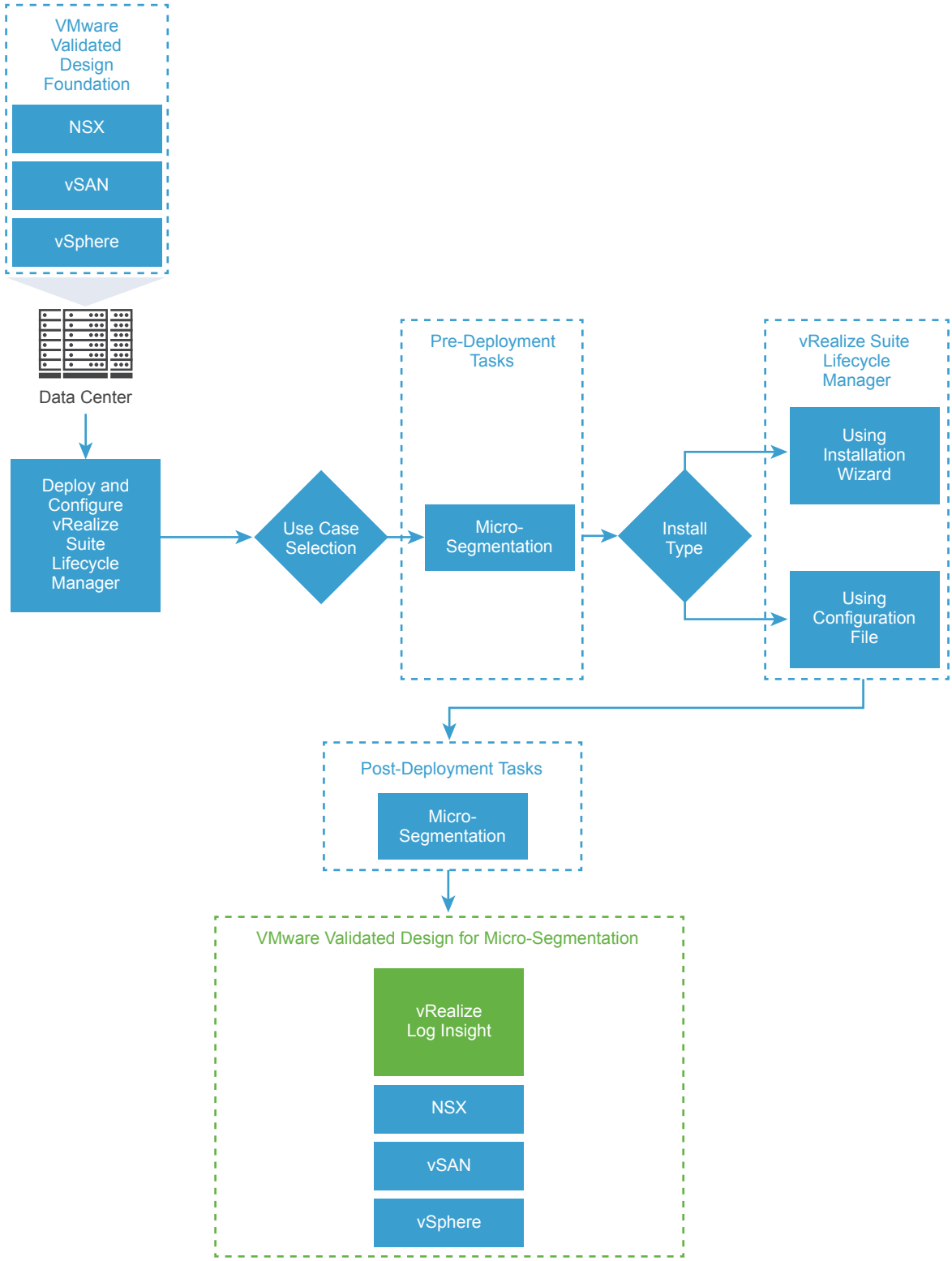
   See Post-Deployment Tasks for vRealize Log Insight.

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 http://pubs.vmware.com/vmware-validated-design-41/topic/com.vmware.vvd.sddc-monitor.doc/GUID-8B4ADD7F-D56C-4A4E-A615-FBB533AA2695.html.

Micro-Segmentation Solution Path

To deploy the Micro-Segmentation use case, you perform pre-deployment tasks that include installing the SDDC foundation. Then you deploy the applications needed by this solution path using the vRealize Suite Lifecycle Manager GUI or by importing a JSON file. After that, you can configure security groups and perform other Micro-Segmentation tasks.

Figure 1-4. vRealize Suite Lifecycle Manager Solution Path for Micro-Segmentation



Procedure

1 As your basis, you deploy the virtual infrastructure, as discussed in *Deployment for Region A* at http://pubs.vmware.com/vmware-validated-design-41/topic/com.vmware.vvd.sddc-deploya.doc/GUID-657DB777-D919-4C23-BA5E-B98D8A91CA8B.html.

   a Install and Configure ESXi Hosts.

   b Deploy and Configure the Platform Services Controller and vCenter Server Component

   c Deploy and Configure the Management Cluster NSX Instance

   d Deploy and Configure the Shared Edge and Compute Cluster Components

   e Deploy and Configure Shared Edge and Compute Cluster NSX Instance

   f Replace Certificates

   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.

   Note The VMware Validated Design for the Software-Defined Data Center *Deployment for Region A* includes vSphere Data Protection. That product is not needed here.

2 Deploy the vRealize Suite Lifecycle Manager appliance, upload the OVA file for your use case, and complete certificate setup.

   See Chapter 2 Deploy and Configure the vRealize Suite Lifecycle Manager Appliance.

3 Perform pre-deployment tasks for vRealize Log Insight.

   See Pre-Deployment Tasks for vRealize Log Insight.

   Note No other pre-deployment tasks are required for this use case.

4 Deploy the required products by running the installation wizard or using the JSON file.

   - Chapter 6 Run the Micro-Segmentation Installation Wizard with vRealize Suite Lifecycle Manager.
   - Chapter 9 Import a JSON File to Deploy the Micro-Segmentation Use Case.

5 Replace certificate for the products that this use case uses:

   a Perform certificate replacement for vRealize Log Insight.

   See http://pubs.vmware.com/vmware-validated-design-41/index.jsp#com.vmware.vvd.sddc-certificate.doc/GUID-E52991A8-A938-4044-87BF-19B5C85861FA.html

6 Perform post-deployment tasks for vRealize Log Insight.

   See Post-Deployment Tasks for vRealize Log Insight.

   Note No other post-deployment tasks are required for this use case.

7 Set up Micro-Segmentation in your environment. See the VMware NSX documentation for details.

Deploy and Configure the vRealize Suite Lifecycle Manager Appliance

2

You have to deploy the vRealize Suite Lifecycle Manager appliance, upload one or more OVA files depending on the use case, and prepare certificates.

This chapter includes the following topics:

Deploy the vRealize Suite Lifecycle Manager Appliance

You deploy the vRealize Suite Lifecycle Manager appliance on top of an existing VMware Validated Design for the Software-Defined Data Center deployment. As part of appliance deployment, you specify storage, networking, and other appliance attributes.

Prerequisites

Complete deployment of the foundation SDDC components of before you start appliance deployment. The names of vCenter Server nodes, storage, and so on that are used in this guide expect a VMware Validated Design deployment.

Note This guide refers to vCenter Server nodes, storage, and so on based on the VMware Validated Design for Software-Defined Data Center

---

See Virtual Infrastructure Deployment in *Deployment for Region A* document at http://pubs.vmware.com/vmware-validated-design-41/topic/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 Life Cycle Manager OVA file, and click **Next**.

5 On the **Select name and location** page, enter the following information, and click **Next**.

Setting	Value
Name	sfo01m01vrlcm01
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, examine 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 agreements and click **Next**.

9 On the **Select storage** page, select the datastore.

   a Select **Thin Provision** from the **Select virtual disk format** drop-down menu.

   b Select **vSAN Default Storage Policy** from the **VM storage policy** drop-down menu.

   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 **sfo01-m01-vds01-management** 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	sfo01m01vrlcm01.rainpole.local
Join the VMware Customer Experience Improvement Program	Selected
Common Name	sfo01m01vrlcm01.rainpole.local
Country Code	US

Option	Value
Organization Name	Rainpole
Organization Unit	Rainpole
Default Gateway	172.16.11.253
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	172.16.11.85
Network 1 Netmask	255.255.255.0

12 On the **Ready to complete** page, click **Finish** and wait for deployment to complete.

13 From the **Home** menu:

a Select **Hosts and Clusters** .

b Expand the sfo01m01vc01.sfo01.rainpole.local tree.

c Select the **sfo01m01vrlcm01** VM and click **Power on**.

14 Open a web browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

15 Log in using the following credentials.

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

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

Note In the first login, you must change the default appliance password before proceeding.

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

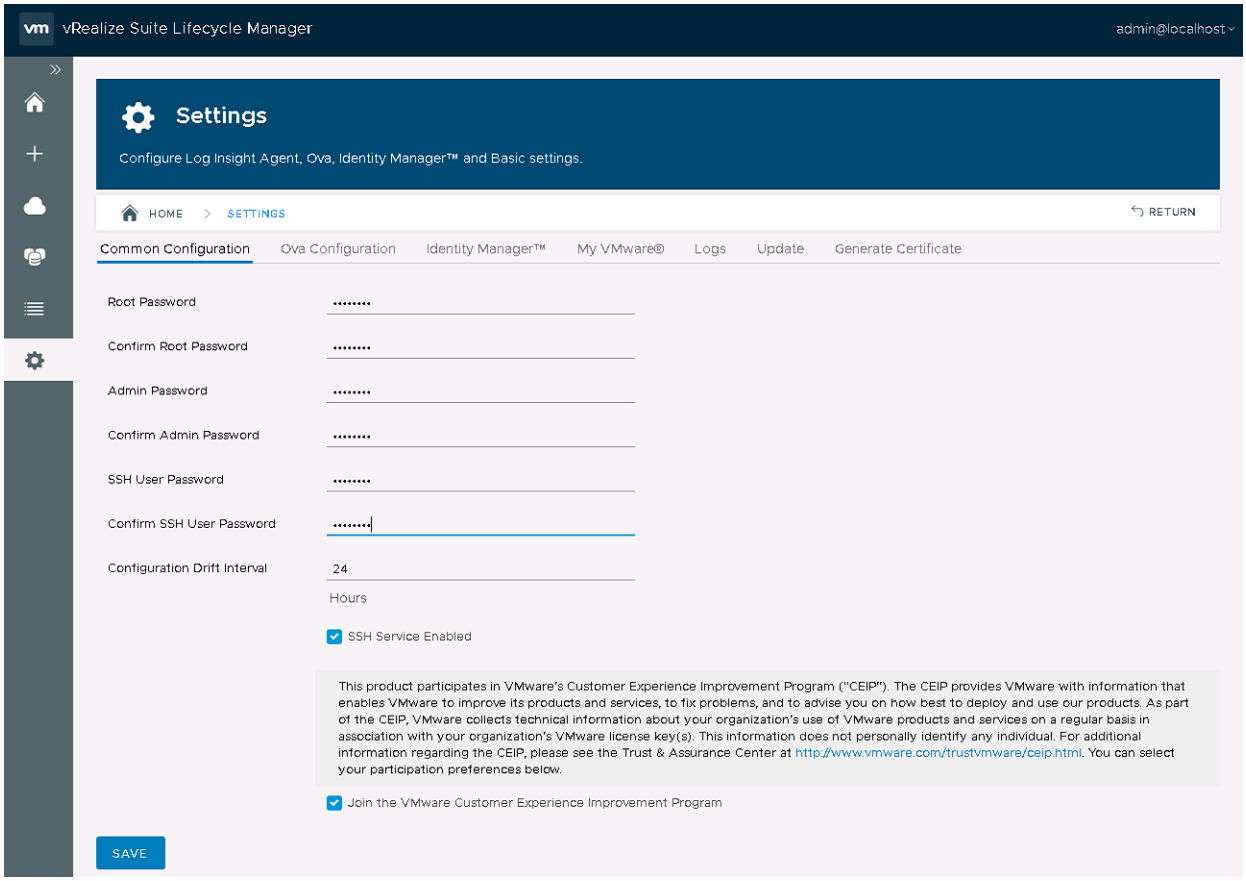
17 On the Navigator pane, click **Settings**.

18 Under **Settings**, click **Common Configuration**, enter the following values.

Option	Value
Root Password	*vrlcm_root_password*
Confirm Root Password	*vrlcm_root_password*
Admin Password	*vrlcm_admin_password*
Confirm Admin Password	*vrlcm_admin_password*
SSH User Password	*vrlcm_ssh_password*
Confirm SSH User Password	*vrlcm_ssh_password*

Option	Value
Configuration Drift Interval	24 (default)
SSH Service Enabled	Selected
Join the VMware Customer Experience Improvement Program	Selected

Figure 2-1. vRealize Suite Lifecycle Manager Settings



19 Click the **Generate Certificates** tab, enter the following values, click **Generate Certificate**, and click **Save**.

Option	Value
Enter Organization	Rainpole
Enter Organizational Unit	Rainpole
Enter Domain Name	*.rainpole.local
Enter locality	SFO
Enter state	CA
Enter Country Code	US
Enter Passphrase	*vrlcm_certificate_passphrase*

20 Click **admin@localhost** at the top right and click **Logout**.

Upload Product OVAs to vRealize Suite Lifecycle Manager

Before you can trigger a use case deployment by using vRealize Suite Lifecycle Manager, you download product OVAs and create mappings between each product and the associated OVA.

You can download product OVAs in the following ways:

- Manual download.
- Download directly from MyVMware into vRealize Suite Lifecycle Manager.

This design explains how to perform the task with a manual download.

Prerequisites

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

Procedure

1 Download the OVA binaries depending on the target use case.

Use Case	Product Name	Product Version	Product OVA
Micro-Segmentation	vRealize Log Insight	4.5.0	vRealize Log Insight `.ova` file
IT Automating IT	vRealize Automation	7.3.0	vRealize Automation `.ova` file
	vRealize Business for Cloud	7.3.0	vRealize Business `.ova` file
	vRealize Log Insight	4.5.0	vRealize Log Insight `.ova` file
	vRealize Operations	6.6.1	vRealize Operations Manager `.ova` file
Intelligent Operations	vRealize Log Insight	4.5.0	vRealize Log Insight `.ova` file
	vRealize Operations	6.6.1	vRealize Operations Manager `.ova` file

2 Use SSH to connect to **`sfo01m01vrlcm01.rainpole.local`**, create a `/data/binaries/OVA` directory, and exit.

3 Use SCP to connect to **`sfo01m01vrlcm01.rainpole.local`** and upload the product OVAs to default location (**`/data/binaries/OVA`**).

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

   a Open a Web Browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials:

Setting	Value
User name	admin@localhost
Password	*vrlcm_admin_password*

5 Click **Settings** and click **Ova Configuration**.

6 Enter the following parameter to identified 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 for each OVA file associate to the use case on the table in Step 1 and click **Save** for each entry.

For example, for the Micro-Segmentation use case, you add vRealize Log Insight product information.

Option	Value
Product Name	vRealize Log Insight
Product Version	4.5.0
Product Binary Type	Install
Product Binary	VMware-vRealize-Log-Insight-4.5.0-xxxxx.ova

8 Repeat the process for each OVA file required by your use case.

9 In the **Navigator**, click **Managed Data Center** and click **Add Data Center** (the three vertical dots on the right).

10 In the **Add Data Center** dialog box, enter the following information and click **Add**.

Setting	Value
Name	sfo01-m01dc
Location	San Francisco

11 Add the vCenter Server, as follows:

a Click **Manage VCenters**.

b In the *Select Data Center*, use the drop down and select **sfo01-m01dc**.

c Click **Add vCenter**.

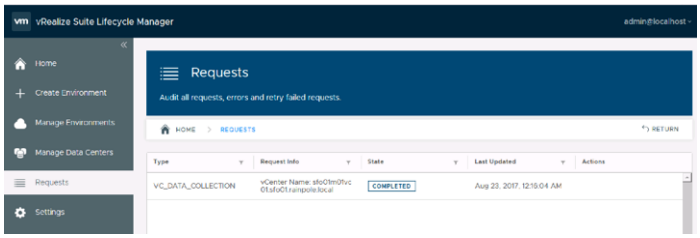
d Enter the following vCenter Server information and click **Submit**.

Setting	Value
Host Name	sfo01m01vc01.sfo01.rainpole.local
User Name	administrator@vsphere.local
Password	*vsphere_admin_password*
vCenter Server type	Management

12 In the **Navigator**, click **Requests** and validate that `VC_DATA_COLLECTION` for the vCenter Server shows `COMPLETED`.

It may take some time for the process to complete.

Figure 2-2. vRealize Suite Lifecycle Manager Requests Validation



13 Click **admin@localhost** and click **Logout**.

Certificate Replacement

Before you deploy use cases with vRealize Suite Lifecycle Manager, you must specify a certificate authority and generate certificate files for the vRealize Suite management products. In this validated design, you replace the default VMCA-signed (self-signed) certificates of the management products with certificates that are signed by a Certificate Authority (CA).

VMware Validated Design comes with a Certificate Generation Utility, `CertGenVVD`.

Use the `CertGenVVD` utility to generate CSRs and CA-signed certificate files for all VMware management products that are deployed in this design. See the *Certificate Replacement* guide that is part of the VMware Validated Design for the Software-Defined Data Center at http://pubs.vmware.com/vmware-validated-design-41/topic/com.vmware.vvd.sddc-certificate.doc/GUID-FA99EBD8-CE1C-405A-96C8-7B5EA9F79D23.html.

Pre-Deployment Tasks for vRealize Suite Lifecycle Manager Use Cases

3

Before you can deploy a use case with vRealize Suite Lifecycle Manager, you have to perform pre-deployment tasks on some of the products that vRealize Suite Lifecycle Manager installs.

Which pre-deployment tasks you perform depends on the use case you want to deploy. See Chapter 1 vRealize Suite Lifecycle Manager Solution Paths for details.

This chapter includes the following topics:

Pre-deployment Tasks for vRealize Automation

Before you can use vRealize Suite Lifecycle Manager to deploy a use case that includes vRealize Automation, you have to perform some pre-deployment tasks.

1 IP Address Mappings and Other Prerequisites for vRealize Automation

Before you deploy the vRealize Automation suite of products, verify that your environment satisfies the requirements for this deployment. Requirements include storage, Active Directory setup and IP addresses and host names.

2 SQL Server Configuration for vRealize Automation

The vRealize Automation suite of products uses a Microsoft SQL Server database to store data.

3 Configure Service Account Privileges

For you to provision virtual machines and logical networks, configure privileges for vRealize Automation for the service account svc-vra@rainpole.local on both the Compute vCenter Server and the Compute Cluster NSX instance.

4 Configure Load Balancing for vRealize Automation Components

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

5 Deploy Windows Virtual Machines for vRealize Automation

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

IP Address Mappings and Other Prerequisites for vRealize Automation

Before you deploy the vRealize Automation suite of products, verify that your environment satisfies the requirements for this deployment. Requirements include storage, Active Directory setup and IP addresses and host names.

vRealize Automation Deployment Prerequisites

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

Prerequisite	Value
Storage	■ Virtual disk provisioning. ■ Required storage per node.
Operating system	Windows 2012 R2 Standard
Database	Microsoft SQL Server 2012 Standard Edition
Active directory	Verify that you have a parent Active Directory instance with the SDDC user roles configured for the rainpole.local domain. Verify the existence of the svc-vra user in the `rainpole.local` domain. Verify the existence of the svc-vro user in the `rainpole.local` domain. The Microsoft SQL Server virtual machine should join the `rainpole.local` domain.
Certification authority	Configure the root Active Directory domain controller as a certificate authority for the environment.
Java	Install Java SE Development Kit (JDK), which is required to run the vRealize Orchestrator Client.

IP Addresses and Host Names

Verify that the static IP address and FQDNs that are listed in the table below are available for the vRealize Automation application virtual network for the first region of the SDDC deployment.

Table 3-1. IP Addresses and FQDNs for the vRealize Automation Instance

Role	IP Address	FQDN
vRealize Automation Server Appliances	192.168.11.51	vra01svr01a.rainpole.local
	192.168.11.52	vra01svr01b.rainpole.local
vRealize Automation Server VIP	192.168.11.53	vra01svr01.rainpole.local
vRealize Automation IWS	192.168.11.54	vra01iws01a.rainpole.local
	192.168.11.55	vra01iws01b.rainpole.local
vRealize Automation IWS VIP	192.168.11.56	vra01iws01.rainpole.local
vRealize Automation IMS	192.168.11.57	vra01ims01a.rainpole.local

Table 3-1. IP Addresses and FQDNs for the vRealize Automation Instance (Continued)

Role	IP Address	FQDN
	192.168.11.58	vra01ims01b.rainpole.local
vRealize Automation IMS VIP	192.168.11.59	vra01ims01.rainpole.local
vRealize DEM Workers	192.168.11.60	vra01dem01a.rainpole.local
	192.168.11.61	vra01dem01b.rainpole.local
MS SQL Server for vRealize Automation	192.168.11.62	vra01mssql01.rainpole.local
vRealize Business for Cloud Server Appliance	192.168.11.66	vrb01svr01.rainpole.local

Table 3-2. IP Addresses and Host Name for the Supporting Infrastructure

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

SQL Server Configuration for vRealize Automation

The vRealize Automation suite of products uses a Microsoft SQL Server database to store data.

Microsoft SQL Server Recommendations

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

- Microsoft SQL Server should be configured with separate Operating System Level volumes (drive letters) for each of the following items. The separation of these items into separate logical volumes (drive letters) will help prevent database corruption should a single volume reach capacity.
  - Operating System
  - Database Application
  - SQL User Database Data Files
  - SQL User Database Log Files

  - SQL TempDB
  - SQL Backup Files
- To provide optimal performance for VMware vRealize databases, configure the SQL Server virtual machine (`vra01mssql01.rainpole.local`) with 8 vCPU and 16GB vRAM.
- Configure the DNS of the SQL Server virtual machine (`vra01mssql01.rainpole.local`) :
  - The primary DNS points to 172.16.11.4 (region A's primary DNS).
  - secondary DNS to point to 172.17.11.4 (region B's primary DNS)

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

Assign the SQL Server System Role to vRealize Automation

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

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

Prerequisites

Verify that you successfully installed SQL Server Management Studio.

Procedure

1 Log in to `vra01mssql01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to `vra01mssql01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	*Windows administrator user*
Password	*windows_administrator_password*

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

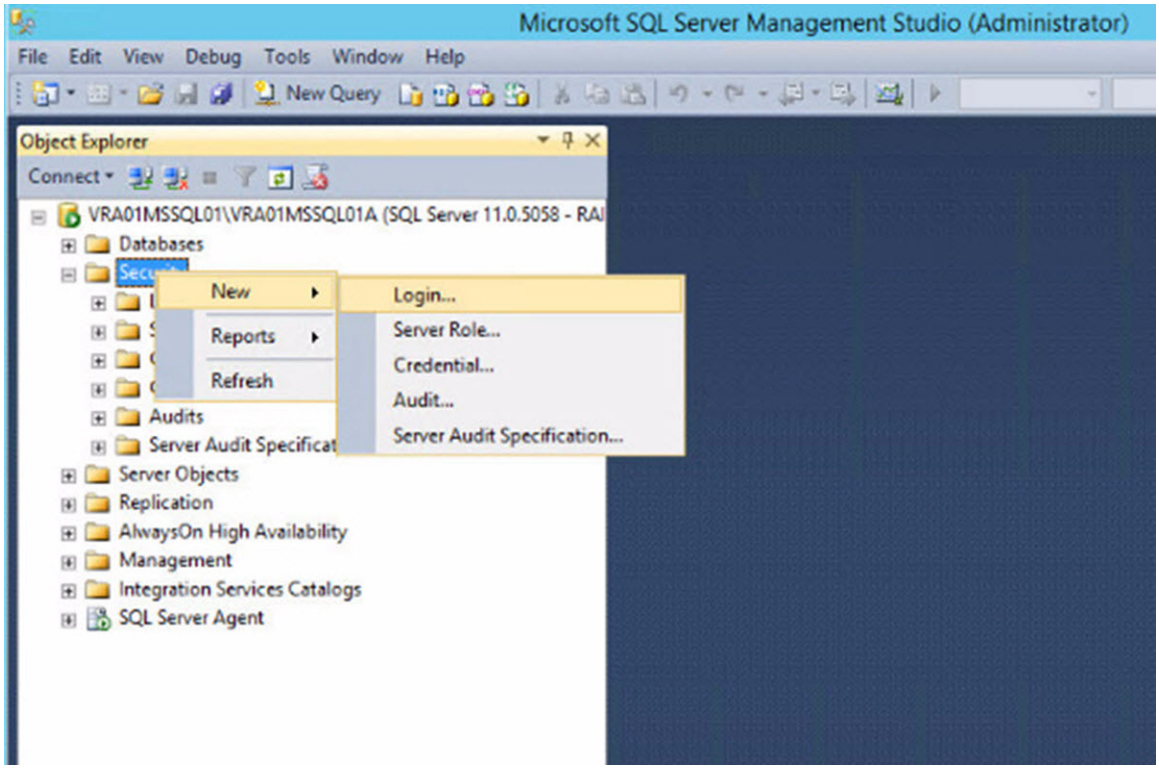
   Note If SQL Server Management Studio doesn't appear in your **All Programs** menu, verify that you successfully installed SQL Server Management Studio.

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

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

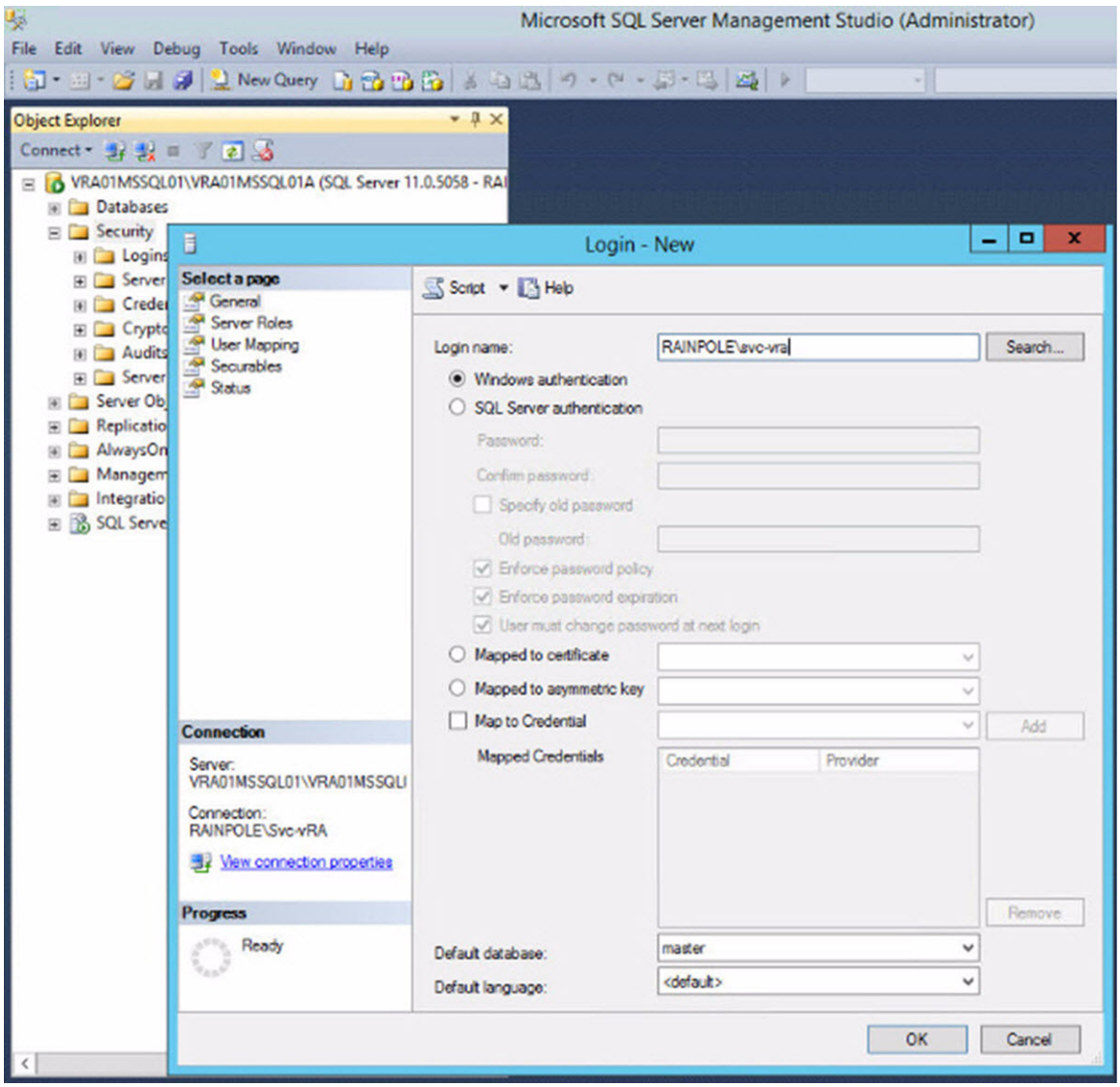
4 In Object Explorer, expand the server instance **VRA01MSSQL01**.

5 Right-click the **Security** folder, click **New**, and click **Login**.



6 In the **Login Properties** dialog box, click **General** on the navigator men.

7 Enter **Rainpole\Svc-vRA** in the **Login name** text box.



8 In the **Login Properties** dialog box, select the **Server Role** on the navigator menu.

9 In the Server roles field, select the **sysadmin** check box, and click **OK**.

Configure Network Access for Distributed Transaction Coordinator

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

Procedure

1 Log in to `vra01mssql01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.

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

   b Log in using the following credentials.

Setting	Value
User name	*Windows administrator user*
Password	*windows_administrator_password*

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

   The Component Services manager displays. Component Services lets you manage Component Object Model (COM+) applications.

3 Using the navigation tree in the left-side pane, expand **Component Services > Computers > My Computer > Distributed Transaction List > Local DTC**.

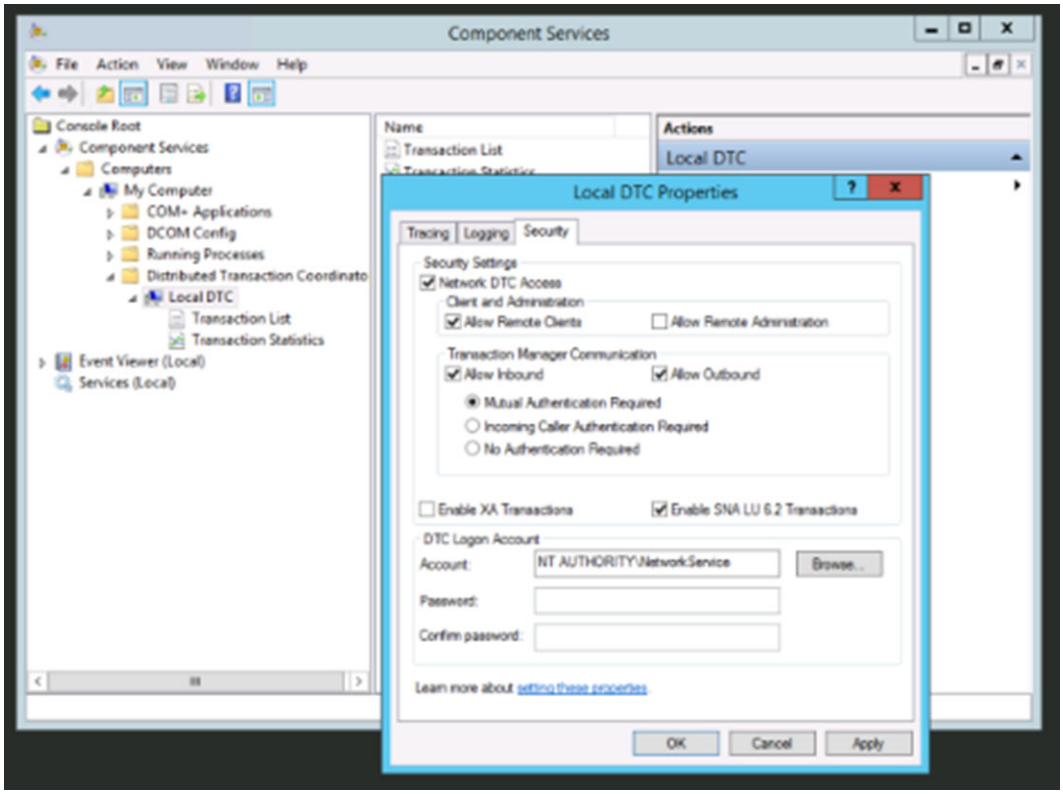
4 Right-click **Local DTC** and click **Properties**.

   The **Local DTC Properties** dialog box displays.

5 Click the **Security** tab in the **Local DTC Properties** dialog box.

6 On the **Security** tab, configure the following values, and click **OK**.

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



7 Click **Yes** to restart the MSDTC Service.

8 Click **OK** to confirm that the MSDTC Service has successfully restarted.

9 Close the Component Services Manager.

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

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

Procedure

1 Log in to the `vra01mssql01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.

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

   b Log in using the following credentials.

Setting	Value
User name	*Windows administrator user*
Password	*windows_administrator_password*

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

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

3 Allow Access for Microsoft SQL Server on TCP Port 1433.

a In the navigation pane, under **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.

The **New Inbound Rule Wizard** appears.

b On the Rule Type page of the **New Inbound Rule Wizard**, select the **Port** radio button, and click **Next**.

c On the Protocol and Ports page, select **TCP** and enter the port number `1433` in the **Specific local ports** text box, and click **Next**.

d On the Action page, select **Allow the connection**, and click **Next**.

e On the Profile page, select the **Domain**,**Private**, and **Public** profiles, and click **Next**.

f On the Name page, enter a name and description for this rule and click **Finish**.

4 Allow access for Microsoft Distributed Transaction Coordinator.

a In the navigation pane, under **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the Action pane.

b On the Rule Type page click **Predefined**, click **Distributed Transaction Coordinator**, and click **Next**.

c On the Predefined Rules page, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, **Distributed Transaction Coordinator (TCP-In)**, and click **Next**.

d On the Action page, select **Allow the connection**, and click **Finish**.

5 Exit the **Windows Firewall with Advanced Security** wizard.

Configure Service Account Privileges

For you to provision virtual machines and logical networks, configure privileges for vRealize Automation for the service account svc-vra@rainpole.local on both the Compute vCenter Server and the Compute Cluster NSX instance.

Procedure

1 Configure Service Account Privileges on the Compute vCenter Server

The svc-vra and svc-vro users must have Administrator privileges on the Compute vCenter Server. You can set up the privileges by using the vSphere Web Client.

2 Configure the Service Account Privilege on the NSX Instance for Consolidated SDDC

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

Configure Service Account Privileges on the Compute vCenter Server

The svc-vra and svc-vro users must have Administrator privileges on the Compute vCenter Server. You can set up the privileges by using the vSphere Web Client.

If you add more Compute vCenter Server instances in the future, perform this procedure on those instances as well.

Procedure

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

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

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

3 Right-click the **sfo01w01vc01.sfo01.rainpole.local** instance and select **Add Permission**.

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

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

5 Select **RAINPOLE** from the **Domain** drop-down menu.

6 In the **Show Users First** text box enter **`svc`** to filter user and group names.

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

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

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

Configure the Service Account Privilege on the NSX Instance for Consolidated SDDC

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

Procedure

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

   a Open a Web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

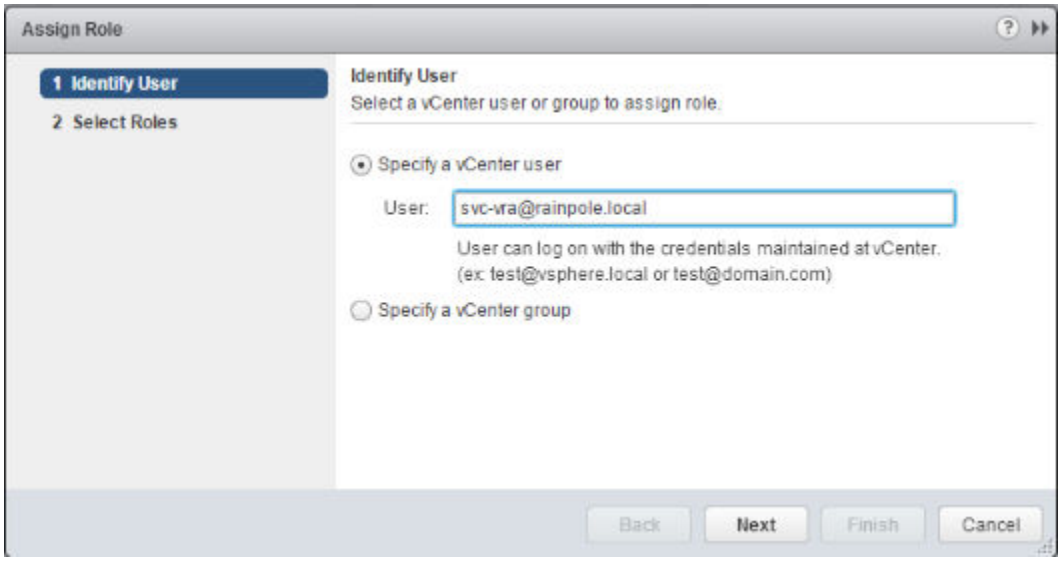
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, select **Networking & Security > NSX Managers**.

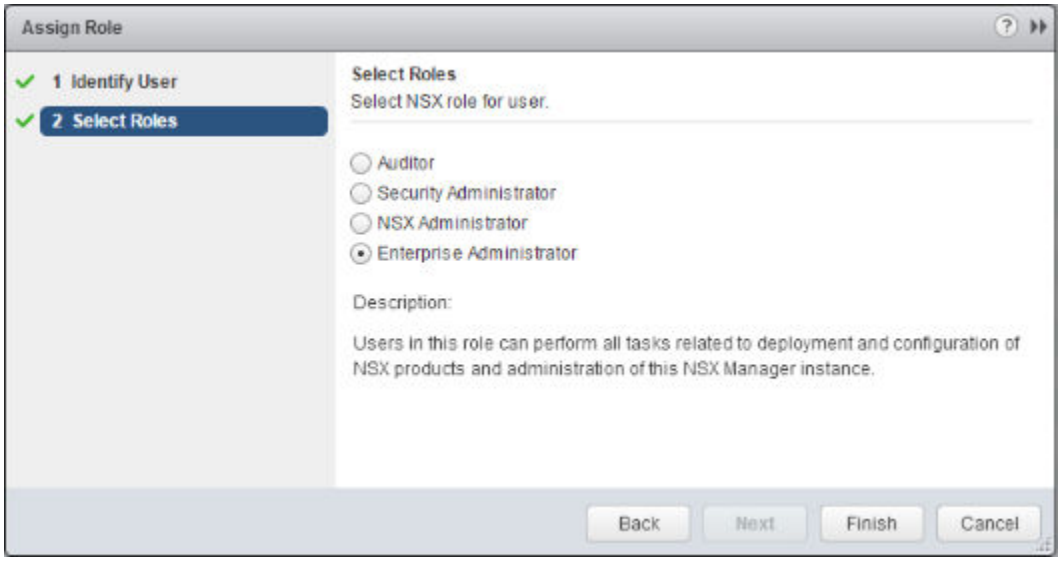
3 Double-click the NSX Manager **172.16.11.66**.

4 Click **Manage**, click **Users**, and click the **Add** icon. The **Assign Role** wizard appears.

5 On the **Identify User** page, select the **Specify a vCenter User** radio button, enter `svc-vra@rainpole.local` in the **User** text box, and click **Next**.



6 On the **Select Roles** page, select the **Enterprise Administrator** radio button, and click **Finish**.



The **rainpole\svc-vra** user is now configured as an Enterprise Administrator for the NSX instance and appears in the lists of users and roles.

Configure Load Balancing for vRealize Automation Components

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

You must configure the load balancer before you deploy the vRealize Automation appliance. Load balancer configuration must come first because you need the virtual IP (VIP) addresses when you deploy the vRealize Automation appliance.

Procedure

1 Add Virtual IP Addresses to the NSX Load Balancer

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

2 Create Application Profiles

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

3 Create Service Monitoring

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

4 Create Server Pools

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

5 Create Virtual Servers

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

Add Virtual IP Addresses to the NSX Load Balancer

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

Procedure

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

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

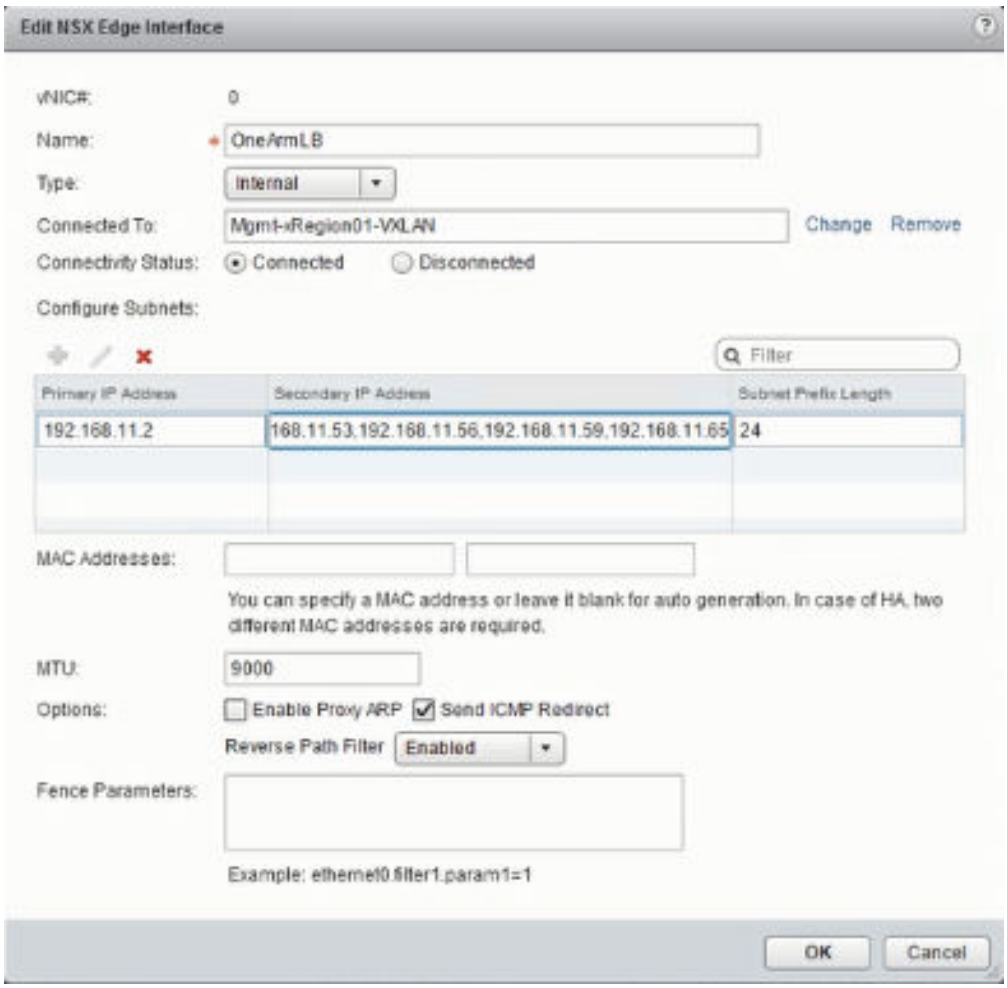
4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to edit its network settings.

5 Click the **Manage** tab, click **Settings**, and select **Interfaces**.

6 Select the **OneArmLB** interface and click the **Edit** icon.

7 In the **Edit NSX Edge Interface** dialog box, add the VIP addresses of the vRealize Automation nodes in the **Secondary IP Addresses** text box.

Setting	Value
Secondary IP Address	192.168.11.53,192.168.11.56,192.168.11.59



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

Create Application Profiles

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

You repeat this procedure twice to create two application profiles.

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Click **Networking & Security**.

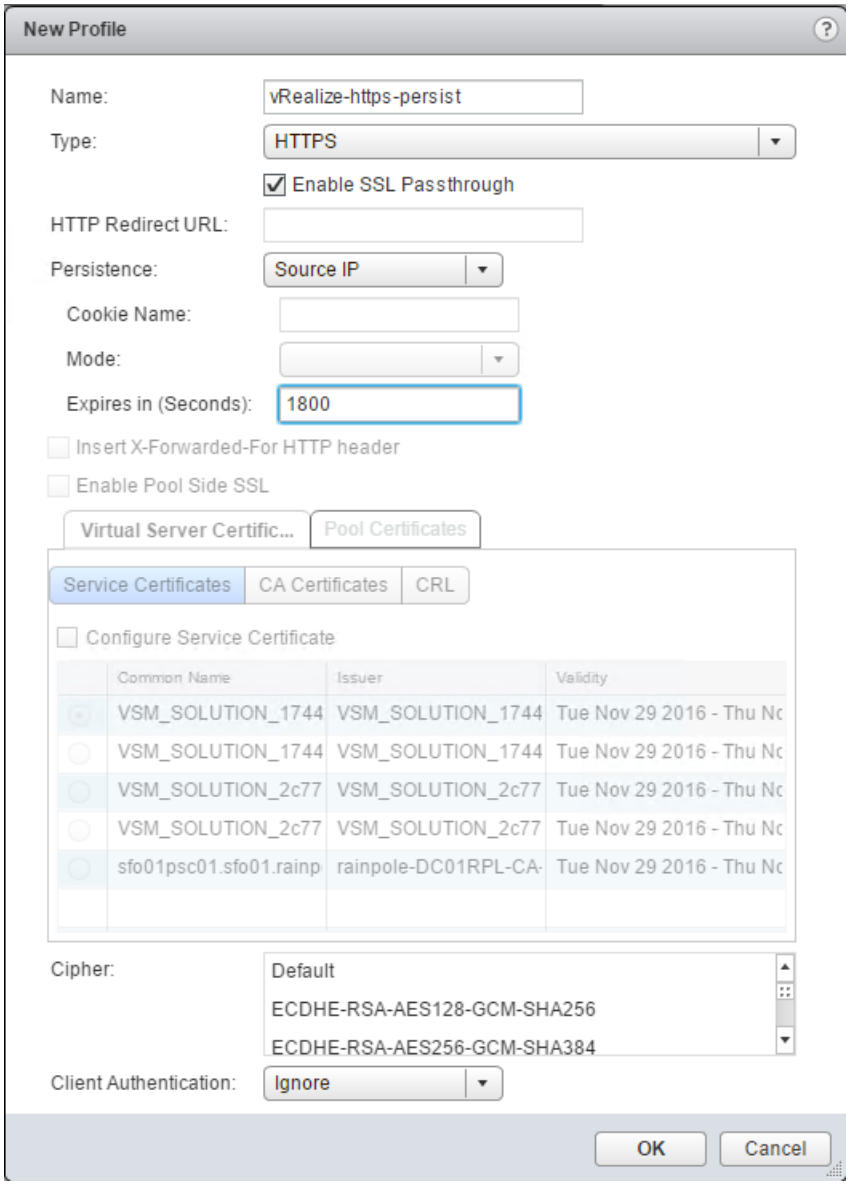
3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.

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

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



7 Click **OK** to save the configuration.

8 Repeat the same steps to create the following application profile.

Setting	Value
Name	vRealize-https
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	None

Create Service Monitoring

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

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Service Monitoring**.

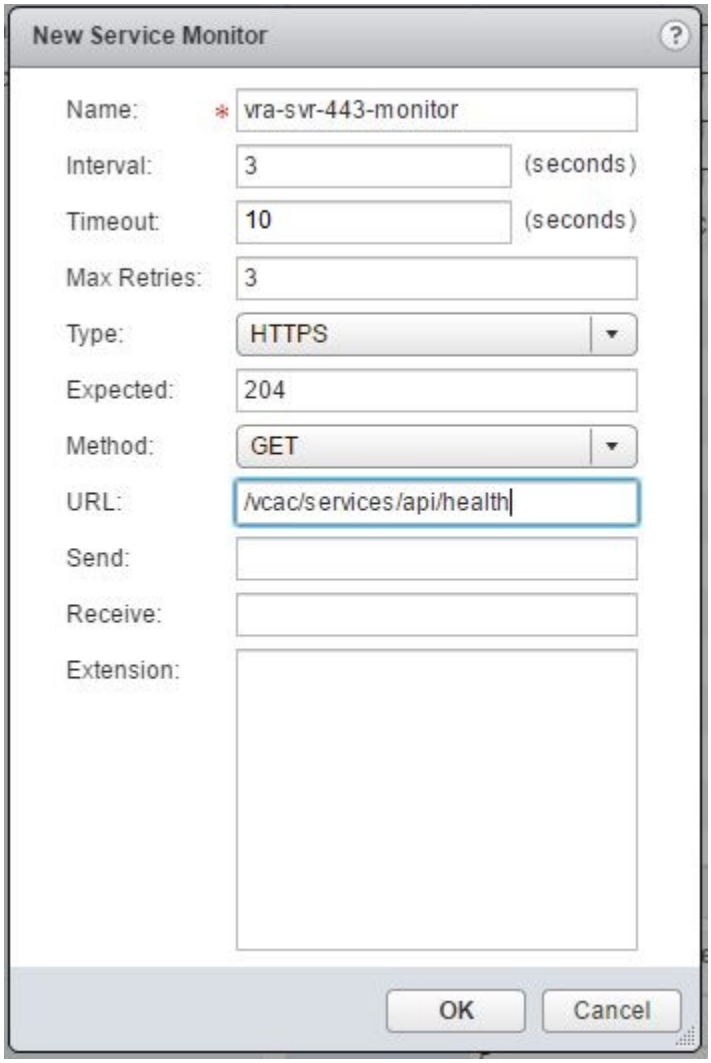
6 Configure the service monitors.

   a Click the **Add** icon.

   b In the **New Service Monitor** dialog box, configure the values for the service monitor that you are adding.

   c Click **OK**.

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



7 Repeat Step 6 to create a service monitor for each component.

Create Server Pools

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

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

- The configuration uses `NONE` as health monitor for all server pools. Until vRealize Automation is fully installed and started, the health monitor marks pool members as offline. Health monitors indicate the status of pool members correctly only after vRealize Automaton is fully installed and initialized.
- The configuration disables the second pool member of three vRealize Automation VIPs (vra-svr-443, vra-iaas-web-443, vra-iaas-mgr-443). During the installation or power cycle of vRealize Automation, the service inside the second node might not be installed or initialized yet. In this period of time, if the load balancer passes a request to the second node, the request fails. If the second pool member is not disabled, you might experience random failures during vRealize Automation installation, and service initialization or registration failure during a vRealize Automation power cycle.

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

Table 3-3. Server Pools for vRealize Automation

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

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

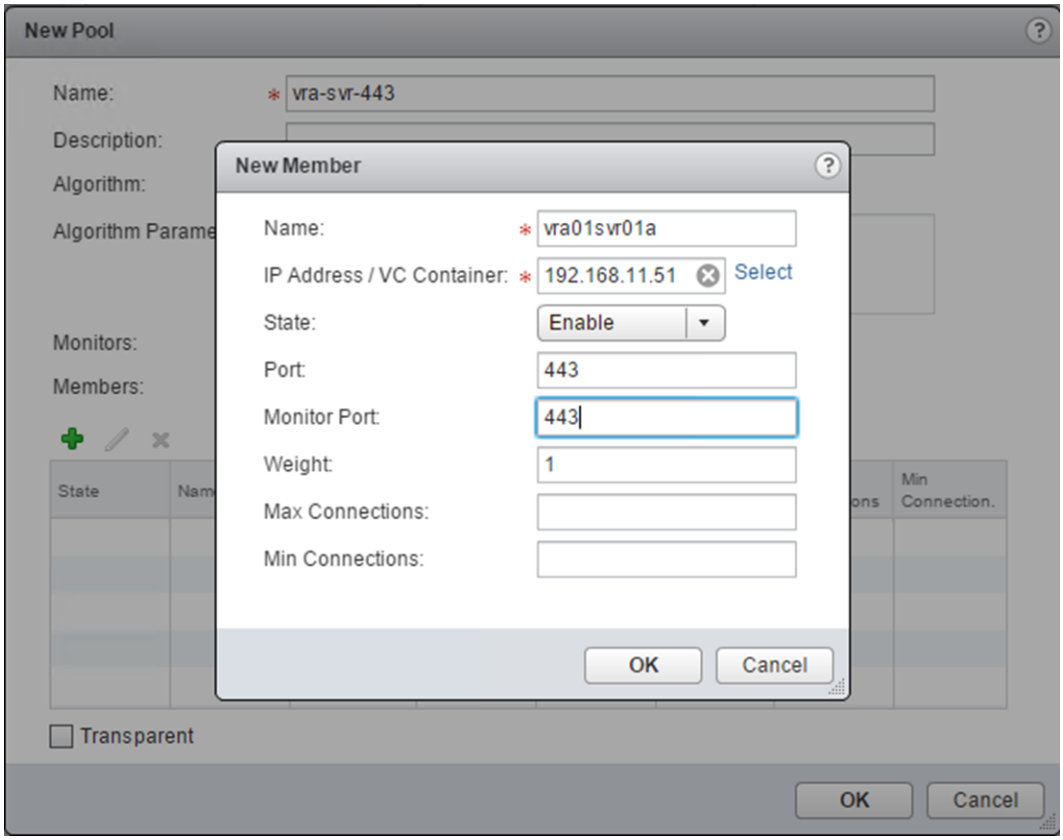
6 Click the **Add** icon and in the **New Pool** dialog box, enter the following values.

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

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

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

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



9 Under **Members**, click the **Add** icon to add the second pool member.

10 In the **New Member** dialog box, enter the following values, click **OK** and click **OK** to save the vRealize Automation server pool.

Setting	Description
Name	vra01svr01b
IP Address/VC Container	192.168.11.52
State	Disable
Port	443

Setting	Description
Monitor Port	443
Weight	1

11 Repeat the procedure to create the remaining server pools.

Create Virtual Servers

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

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

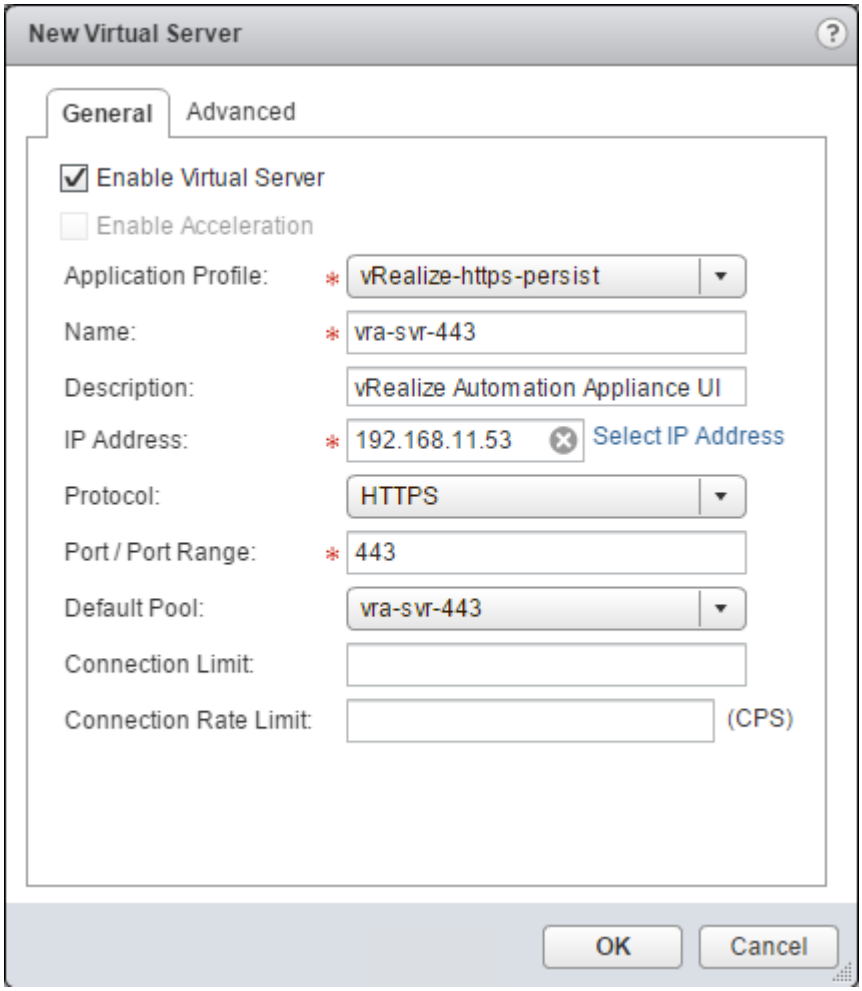
4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **sfo01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.

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

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

Setting	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283
Port	443	443	443	8444	8283
Default Pool	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283



7 Repeat Step 6 to create a virtual server for each component.

Deploy Windows Virtual Machines for vRealize Automation

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

Procedure

1 Create vSphere Image Customization Specifications

Create vSphere image customization specifications to use with your vRealize Automation IaaS Servers and Proxy Agent deployments. The customization specification you create customizes the guest operating systems of the virtual machines that host the vRealize Automation IaaS Web Server and IaaS Manager Services.

2 Create Windows Virtual Machines for vRealize Automation

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

Create vSphere Image Customization Specifications

Create vSphere image customization specifications to use with your vRealize Automation IaaS Servers and Proxy Agent deployments. The customization specification you create customizes the guest operating systems of the virtual machines that host the vRealize Automation IaaS Web Server and IaaS Manager Services.

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

Create a Customization Specification File for IaaS Servers

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

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

Procedure

1 Log in to the Management 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 **Operations and Policies**, click **Customization Specification Manager**.

3 Select **sfo01m01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu.

4 Click the **Create a new specification** icon.

The **Guest Customization** wizard opens.

5 On the **Specify Properties** page, set the following values, and click **Next**.

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

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

Setting	Value
Name	Rainpole
Organization	Rainpole IT

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

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

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

Setting	Value
Product Key	*volume_license_key*
Include Server License Information	Selected
Server License Mode	Per seat

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

Setting	Value
Password	*local_administrator_pwd*
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

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

11 On the **Run Once** page, type **`net localgroup administrators rainpole\svc-vra /add`** in the text box, click **Add**, and click **Next**.

This command will add the service account rainpole\svc-vra into virtual machine's local administrators group.

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

The **Edit Network** dialog box opens.

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

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

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

a Specify the following DNS server settings.

Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.16.11.4
Alternate DNS Server	172.17.11.4

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

c Enter **`sfo01.rainpole.local`** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

d Enter **`lax01.rainpole.local`** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

e Click **OK** to save settings, close the **Edit Network** dialog box, and click **Next**.

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

Setting	Value
Windows Server Domain	rainpole.local
Username	ad_admin_acct@rainpole.local
Password	*ad_admin_password*

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

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

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

Create a Customization Specification File for IaaS Proxy Agent Servers

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

Procedure

1 Log in to the Management 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, click **Customization Specification Manager**.

3 Select **sfo01m01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu.

4 Click the **Create a new specification** icon.

   The **New VMGuest CustomizationSpec** wizard opens.

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

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

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

Setting	Value
Name	Rainpole
Organization	Rainpole IT

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

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

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

Setting	Value
Product Key	*volume_license_key*
Include Server License Information	Selected
Server License Mode	Per seat

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

Setting	Value
Password	*local_administrator_pwd*
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

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

11 On the **Run Once** page, type **`net localgroup administrators rainpole\svc-vra /add`** in the text box, click **Add**, and click **Next**.

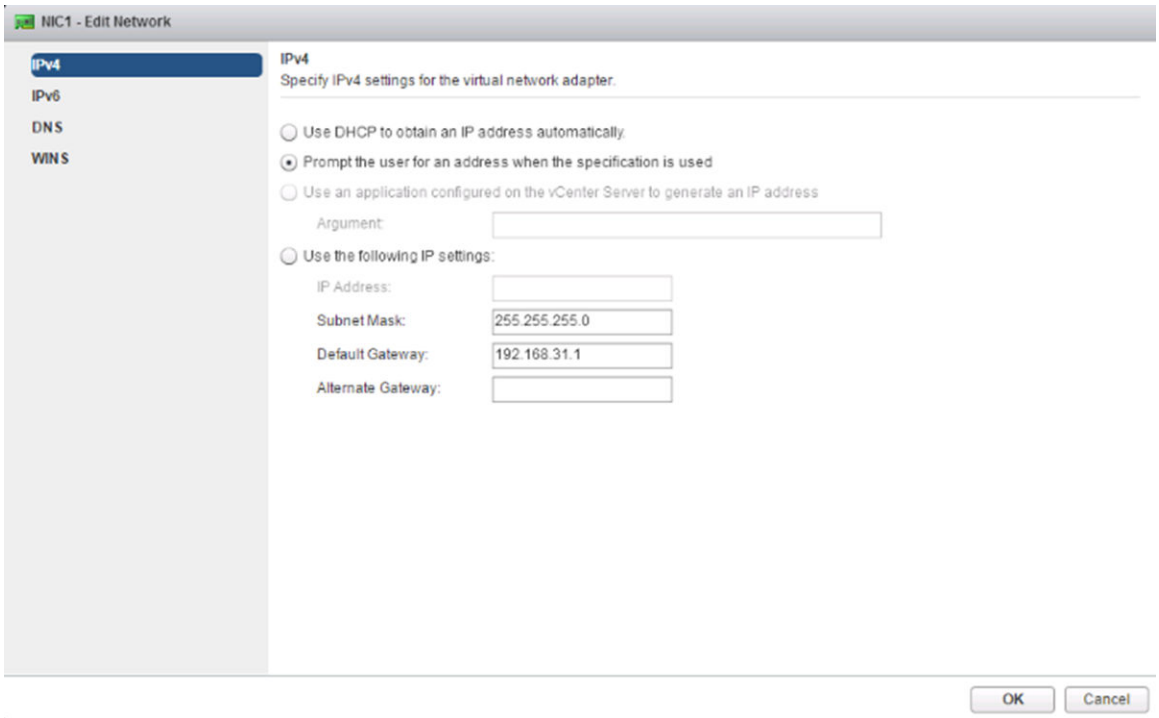
This command will add the service account rainpole\svc-vra into the virtual machine's local administrators group.

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

The **Network Properties** dialog box displays.

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

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



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

a Specify the following DNS server settings.

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

b Enter **`sfo01.rainpole.local`** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

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

d Enter **`lax01.rainpole.local`** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

e Click **OK** to save settings, close the **Edit Network** dialog box, and click **Next**.

15 On the **Set Workgroup or Domain** page, enter credentials for a user who has administrative privileges in the domain, and click **Next**.

Setting	Value
Windows Server Domain	sfo01.rainpole.local
Username	ad_admin_acct@sfo01.rainpole.local
Password	*ad_admin_password*

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

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

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

Create Windows Virtual Machines for vRealize Automation

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

To facilitate cloning, this design uses the vra7-template and the vra7-proxy-agent-template image customization specification templates and the windows-2012r2-64 VM template. A fully redundant vRealize Automation deployment requires eight virtual machines that run on Windows. Repeat this procedure eight times by using the information in the following table to create eight VMs.

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

Prerequisites

- Verify that you have created the Windows 2012 R2 VM template, windows2012r2-template.
- SHA512 is disabled in Windows for TLS 1.2 by default. If SHA512 certificates will be used for vRealize Automation, you need to install the windows update in Microsoft KB2973337.

Procedure

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

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 In the Navigator pane, select **Global Inventory Lists** > **vCenter Servers** and click the **sfo01m01vc01.sfo01.rainpole.local**.

3 Click **VM Templates in Folders**, right-click the IaaS windows template **win2012r2-template** in the VM Templates in Folders pane, and select **New VM from this Template**.

4 On the **Select a name and folder** page of the **Deploy From Template** wizard, specify a name and location for the virtual machine.

   a Enter `vra01iws01a.rainpole.local` in the **Enter a name for the virtual machine** text box.

   b In the **Select a location for the virtual machine** pane, select the **sfo01-m01fd-vra** folder in the **sfo01-m01dc** datacenter under **sfo01m01vc01.sfo01.rainpole.local**, and click **Next**.

5 On the **Select a compute resource** page, select **sfo01-m01-mgmt01**, and click **Next**.

6 On the **Select storage** page, select the datastore on which to create the virtual machine's disks.

   a Select **vSAN Default Storage Policy** from the **VM Storage Policy** drop-down menu.

   b Select the **sfo01-m01-vsan01** vSAN datastore from the datastore table and click **Next**.

7 On the **Select Clone options** page, select the **Customize the operating system** check box, and click **Next**.

8 On the **Customize guest OS** page, select the **vra7-template** from the table, and click **Next**.

9 On the **User Settings** page, enter the following values, and click **Next**.

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

10 On the **Ready to Complete** page, review your settings and click **Finish**.

   When the deployment of the virtual machine completes, you can customize the virtual machine.

11 In the Navigator, select **VMs and Templates**.

12 Right-click the **vra01iws01a.rainpole.local** virtual machine and select **Edit Settings**.

13 Click **Virtual Hardware** and configure the following settings:

Setting	Value
CPU	2
Memory	4096 MB
Network adapter 1	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN

14 Right-click the virtual machine **vra01iws01a.rainpole.local**, and select **Power > Power on**.

15 From the Virtual Machine Console, verify that vra01iws01a.rainpole.local reboots, and uses the configuration settings that you specified.

After the Windows customization process completes, a clean desktop appears.

16 Log in to the Windows operating system and perform final verification and customization.

a Verify that the IP address, computer name, and domain are correct.

b Verify vRealize Automation service account svc-vra@rainpole.local has been added to the Local Administrators Group.

Note You may notice that the virtual machine failed to execute all the steps in the customization specification. When this occurs:

- Delete the virtual machine and its customization specification.
- Retry creating the Windows virtual machines for the IaaS components by creating a new customization specification and provisioning a virtual machine using the newly recreated customization specification.

17 Repeat this procedure to deploy and configure the remaining virtual machines.

Pre-Deployment Tasks for vRealize Operations Manager

Before you can deploy vRealize Operations Manager as part of a vRealize Suite Lifecycle Manager deployment, you prepare for the deployment.

Configure the Load Balancer for vRealize Operations Manager

Configure load balancing for the analytics cluster on the dedicated sfo01m01lb01 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, select **Networking & Security**.

3 On the **NSX Home** page, click **NSX Edges** and select **172.16.11.65** from the **NSX Manager** drop-down menu .

4 On the **NSX Edges** page, double-click **sfo01m01lb01**.

5 Configure the load balancing VIP address for 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 **Edit**.

   d In the **Secondary IP Addresses** text box enter the **`192.168.11.35`** VIP address.

   e 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 `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 the **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	■ vrops01svr01a ■ vrops01svr01b ■ vrops01svr01c
IP Address	■ 192.168.11.31 ■ 192.168.11.32 ■ 192.168.11.33
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	1 Click **Select IP Address**. 2 Select **OneArmLB** from the drop-down menu. 3 Select **192.168.11.35** IP as the virtual NIC.
Protocol	HTTPS
Port	443
Default Pool	vrops-svr-443
Connection Limit	0
Connection Rate Limit	0

10 Configure auto-redirect from HTTP to HTTPS requests.

The NSX Edge can redirect users from HTTP to HTTPS.

a On the **Load Balancer** tab of the `sfo01m01lb01` device, select **Application Profiles** and click the **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

Verify vRealize Operations Manager Requirements

Before you deploy vRealize Operations Manager, verify that your environment satisfies the requirements for this deployment. Prerequisites include storage, software features, external services, IP addresses and host names, and more.

Deployment Prerequisites

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

Prerequisite	Value
Storage	■ Virtual disk provisioning: Thin ■ Required storage per analytics cluster node. ■ Initial storage for the analytics cluster node: 274 GB ■ Additional storage for monitoring data per analytics cluster node: 750 GB ■ Required storage per remote collector group node. ■ Initial storage per node: 274 GB
Software Features	■ Verify that vCenter Server is operational. ■ Verify that the vSphere cluster has vSphere DRS and HA enabled. ■ Verify that the NSX Manager is operational. ■ Verify that the application virtual networks are available. ■ Verify that the Load Balancer service is enabled on the NSX Edge services gateway.
Installation Package	■ Download the `.pak` file for the vRealize Operations Manager Management Pack for NSX for vSphere from VMware Solutions Exchange. ■ Download the `.pak` file for the vRealize Operations Manager Management Pack for Storage Devices from VMware Solutions Exchange.
Active Directory	■ Verify that you have a parent active directory with the SDDC user roles configured for the rainpole.local domain.
Certification Authority	■ Configure the root Active Directory domain controller as a certificate authority for the environment. ■ Download the CertGenVVD tool and generate the signed certificate for the analytics cluster. See the *Planning and Preparation* documentation for VMware Validated Design for the Software-Defined Data Center.
External Services	■ Verify that you have access to a SMTP server. ■ Verify that SNMP is enabled in your network environment, to monitor network devices. ■ Verify that Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP) is enabled on each network device, for complete monitoring of your environment.

IP Addresses and Host Names

Verify that static IP addresses and FQDNs for the application virtual network are available for the first region of the SDDC deployment.

For the analytics cluster application virtual network, allocate 3 static IP addresses and FQDNs for the nodes and one for the load balancer, and map host names to the IP addresses. For the remote collector group, allocate 2 static IP addresses and FQDNs.

Table 3-4. 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 3-5. IP Addresses and Host Names for the Analytics Cluster

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

Table 3-5. IP Addresses and Host Names for the Analytics Cluster (Continued)

Role	IP Address	FQDN
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	■ 172.16.11.4 ■ 172.17.11.4	--
Subnet mask	255.255.255.0	--
NTP servers	■ 172.16.11.251 ■ 172.17.11.251	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Table 3-6. IP Addresses and Host Names for the Remote Collectors

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	--

Pre-Deployment Tasks for 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 the vRealize Log Insight are available in the application virtual network.

For the application virtual network, allocate 3 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.

Table 3-7. Application Virtual Network Names for vRealize Log Insight

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

Table 3-8. IP Addresses and Host Names for the vRealize Log Insight Instance

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

Table 3-8. IP Addresses and Host Names for the vRealize Log Insight Instance (Continued)

Role	IP Address	FQDN
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	■ 172.16.11.5 ■ 172.16.11.4	-
Subnet mask	255.255.255.0	-
NTP servers	■ 172.16.11.251 ■ 172.16.11.252 ■ 172.17.11.251 ■ 172.17.11.252	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Deployment Prerequisites

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

Prerequisite	Value

Storage	■ Virtual disk provisioning: Thin.
	■ Required storage per node
	  ■ Initial storage for node deployment: 510 GB
	■ Required storage for cluster archiving
	  ■ Initial storage for archiving: 400 GB

Software Features	■ Verify that vCenter Server is operational.
	■ Verify that the vSphere cluster has DRS and HA enabled.
	■ Verify that the Management NSX Manager is operational.
	■ Verify that the application virtual network for the 3-node vRealize Log Insight cluster is available.
	■ Verify the following NFS datastore requirements:
	  ■ Create an NFS share of 400 GB in Region and export it as `/V2D_vRLI_MgmtA_400`GB.
	  ■ Verify that the NFS server supports NFS v3.
	  ■ Verify that the NFS partition allows read and write operations for guest accounts.
	  ■ Verify that the mount does not require authentication.
	  ■ Verify that the NFS share is directly accessible to vRealize Log Insight
	  ■ If using a Windows NFS server, allow unmapped user Unix access (by UID/GID).

Active Directory	Verify that you have a parent and child Active Directory domain controllers configured with the role-specific SDDC users and groups for the `rainpole.local` domain.
Certification 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 from.

Run the IT Automating IT Installation Wizard from vRealize Suite Lifecycle Manager

4

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

The installation wizard will prompt you for information about your deployment such as virtual machine names, IP addresses, and so on.

Prerequisites

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

See IT Automating IT Solution Path.

Procedure

1 Create the Environment for the IT Automating IT Installation Wizard

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

2 Configure vRealize Automation with vRealize Suite Lifecycle Manager

   The vRealize Suite Lifecycle Manager wizard prompts you for information about the vRealize Automation deployment.

3 Configure vRealize Business for Cloud with vRealize Suite Lifecycle Manager

   As part of use case deployment, vRealize Suite Lifecycle Manager prompts you for information for vRealize Business for Cloud virtual appliances.

4 Configure vRealize Operations Manager with vRealize Suite Lifecycle Manager

   You can configure vRealize Operations Manager by specifying information on the vRealize Suite Lifecycle Manager **Product Details** page for vRealize Operations Manager. You set advanced settings for the different VMs that are part of vRealize Operations Manager.

5 Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

   vRealize Suite Lifecycle Manager prompts you for information for the virtual appliances for vRealize Log Insight.

Create the Environment for the IT Automating IT Installation Wizard

When you deploy the IT Automating IT use case by using the vRealize Suite Lifecycle Manager web interface, you first create a new environment. As part of that 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 OVA files configured for corresponding product or solutions.

Procedure

1 Login to vRealize Suite Lifecycle Manager

   a Open a Web browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	*vrlcm_admin_password*

2 On the **Home** page, click **Create Environment** to start a new deployment.

3 In the **Select Installaton 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	VVD-ITAIT
Administrator Email	admin@rainpole.local
Default Password	**`default_admin_password`**
Customer Experience Improvement Program	Selected

5 On the **Solutions** tab, select **VVD Version 4.1** from the drop-down menu.

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

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

8 On the **License Details** page, 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
vCenter Host Name	sfo01m01vc01.sfo01.rainpole.local
Cluster	sfo01-m01-mgmt01 (sfo01-m01dc)
Network	distributed switch that ends with `Mgmt-xRegion01-VXLAN`
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, as follows:

a Configure vRealize Automation with vRealize Suite Lifecycle Manager

b Configure vRealize Business for Cloud with vRealize Suite Lifecycle Manager

c Configure vRealize Operations Manager with vRealize Suite Lifecycle Manager

d Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

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

Configure vRealize Automation with vRealize Suite Lifecycle Manager

The vRealize Suite Lifecycle Manager wizard prompts you for information about the vRealize Automation deployment.

Procedure

1 On the **Product Details** page, select the **vRealize Automation** tab.

2 Enter the following information for **Product Properties**.

Setting	Value
windowsPassword	*windows_vm_domain_password*
windowsUsername	*RAINPOLE\svc-vra*

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

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

4 Specify the following information for **vra-server-primary** and **vra-server-secondary**.

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

a Click **vra-server-primary** and click **Advanced Settings**.

b In **Advanced Configuration for vra-server-primary**, enter vRA Hostname, vRA IP Address, and vRA VM Name.

c Click **Done**.

d Repeat for **vra-server-secondary** component.

5 Click **Advanced Settings** for **db**, enter the following information, and click **Done**.

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

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

a Select the **iaas-web-*XX*** VM and click **Advanced Settings** for .

b Enter the IP Address, Windows Web Hostname, and Web Name from the table below.

c Click **Done**.

d Repeat for the **iaas-web-02** VM.

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

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

a Select the **iaas-manager-active** VM and click **Advanced Settings** .

b Enter the IP Address, Windows MS Hostname, and MS Name from the table below.

c Click **Done**.

d Repeat for the **iaas-manager-passive** VM.

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

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

a Select a **Demworker-*XX*** VM and click **Advanced Settings**.

b Enter the IP Address, Windows DEM Hostname, and DEM Worker Name.

c Click **Done**.

d Repeat for the other Demworker VMs.

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

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

a Select the **Demorchestrator-01** VM and click **Advanced Settings**.

b Enter IP Address, Windows DEM Hostname, and DEM Orchestrator Name shown in the table below.

c Click **Done**.

d Repeat for the **Demorchestrator-02** VM.

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

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

a Select the **proxy-agent-vsphere-01** VM and click **Advanced Settings**.

b Enter the IP Address, Windows Agent Hostname, and Agent Name shown in the table below.

c Click **Done**.

d Repeat for the **proxy-agent-vsphere-02** VM.

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

Configure vRealize Business for Cloud with vRealize Suite Lifecycle Manager

As part of use case deployment, vRealize Suite Lifecycle Manager prompts you for information for vRealize Business for Cloud virtual appliances.

Procedure

1 On the **Product Details** page, select the **vRealize Business for Cloud** tab.

2 Enter the following information for **Product Properties**.

Option	Value
Currency	USD - US Dollar

3 Click **Advanced Settings** for the **vrb-server** VM.

4 On the **Advanced Configuration for vrb-server** page, enter the following information and click **Done**.

Option	Value
Hostname	vrb01svr01.rainpole.local
IP Address	192.168.11.66
VM Name	vrb01svr01.rainpole.local

5 Click **Advanced Settings** for the **vrb-collector** VM.

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

Option	Value
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrbc01.sfo01.rainpole.local
IP Address	192.168.31.54
Domain	sfo01.rainpole.local

Option	Value
VM Name	sfo01vrbc01.sfo01.rainpole.local
Gateway	192.168.31.1

Configure vRealize Operations Manager with vRealize Suite Lifecycle Manager

You can configure vRealize Operations Manager by specifying information on the vRealize Suite Lifecycle Manager **Product Details** page for vRealize Operations Manager. You set advanced settings for the different 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 Click **Advanced Settings** for the **master** VM.

4 Enter the following information and click **Done**.

Option	Value
VM Name	vrops01svr01a.rainpole.local
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
Hostname	vrops01svr01a.rainpole.local
IP Address	192.168.11.31
Extended Storage (1 TB)	sfo01-m01-vsan01

5 Click **Advanced Settings** for the **replica** VM.

6 Enter the following information and click **Done**.

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

7 Click **Advanced Settings** for the **data-01** VM.

8 Enter the following information and click **Done**.

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

9 Click **Advanced Settings** for the **remotecollector-01** VM.

10 Enter the following information and click **Done**.

Option	Value
VM Name	sfo01vropsc01a.sfo01.rainpole.local
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vropsc01a.sfo01.rainpole.local
IP address	192.168.31.31
Domain	sfo01.rainpole.local
Gateway	192.168.31.1

11 Click **Advanced Settings** for the **remotecollector-02** VM.

12 Enter the following information and click **Done**.

Option	Value
VM Name	sfo01vropsc01b.sfo01.rainpole.local
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vropsc01b.sfo01.rainpole.local
IP Address	192.168.31.32
Domain	sfo01.rainpole.local
Gateway	192.168.31.1

Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager prompts you for information for the virtual appliances for vRealize Log Insight.

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 Click **Advanced Settings** for **vrli-master** VM.

4 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01a.sfo01.rainpole.local
IP Address	192.168.31.11
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01a.sfo01.rainpole.local
Gateway	192.168.31.1

5 Click **Advanced Settings** for the **vrli-worker-01** VM.

6 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01b.sfo01.rainpole.local
Domain	sfo01.rainpole.local

Option	Value
VM Name	sfo01vrli01b.sfo01.rainpole.local
Gateway	192.168.31.1

7 Click **Advanced Settings** for the **vrli-worker-02** VM.

8 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01c.sfo01.rainpole.local
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01c.sfo01.rainpole.local
Gateway	192.168.31.1

Run the Intelligent Operations Installation Wizard with vRealize Suite Lifecycle Manager

5

Deploy the Intelligent Operations use case using the vRealize Suite Lifecycle Manager installation wizards. The installation wizard will prompt you for information about your deployment such as virtual machine names, IP addresses, and so on.

Prerequisites

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

See Intelligent Operations Solution Path for details.

Procedure

1 Create the Environment for the Intelligent Operations

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 that task, you input parameters such as the administrator email, network and storage information, and other environment information that is required for the deployment.

2 Configure vRealize Operations Manager with vRealize Suite Lifecycle Manager

You can configure vRealize Operations Manager by specifying information on the vRealize Suite Lifecycle Manager **Product Details** page for vRealize Operations Manager. You set advanced settings for the different VMs that are part of vRealize Operations Manager.

3 Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager prompts you for information for the virtual appliances for vRealize Log Insight.

Create the Environment for the Intelligent Operations

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 that task, you input parameters such as the administrator email, network and storage information, and other environment information that is required for the deployment.

Procedure

1 Login to vRealize Suite Lifecycle Manager

   a Open a Web browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	*vrlcm_admin_password*

2 On the **Home** page, click **Create Environment** to start a new deployment.

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

4 On the **Create New Environment** page, enter the following information.

Setting	Value
Data Center	sfo01-m01dc
Environment Type	Production
Environment Name	VVD-Intelligent-Operation
Administrator Email	admin@rainpole.local
Default Password	*default_admin_password*
Customer Experience Improvement Program	Selected

5 Click the **Solutions** tab and select **VVD Version 4.1** 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, 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
vCenter Host Name	sfo01m01vc01.sfo01.rainpole.local
Cluster	sfo01-m01-mgmt01 (sfo01-m01dc)
Network	distributed switch that ends with `Mgmt-xRegion01-VXLAN`
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**.

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

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 deployment.

Configure vRealize Operations Manager with vRealize Suite Lifecycle Manager

You can configure vRealize Operations Manager by specifying information on the vRealize Suite Lifecycle Manager **Product Details** page for vRealize Operations Manager. You set advanced settings for the different 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 Click **Advanced Settings** for the **master** VM.

4 Enter the following information and click **Done**.

Option	Value
VM Name	vrops01svr01a.rainpole.local
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
Hostname	vrops01svr01a.rainpole.local
IP Address	192.168.11.31
Extended Storage (1 TB)	sfo01-m01-vsan01

5 Click **Advanced Settings** for the **replica** VM.

6 Enter the following information and click **Done**.

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

7 Click **Advanced Settings** for the **data-01** VM.

8 Enter the following information and click **Done**.

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

9 Click **Advanced Settings** for the **remotecollector-01** VM.

10 Enter the following information and click **Done**.

Option	Value
VM Name	sfo01vropsc01a.sfo01.rainpole.local
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vropsc01a.sfo01.rainpole.local
IP address	192.168.31.31
Domain	sfo01.rainpole.local
Gateway	192.168.31.1

11 Click **Advanced Settings** for the **remotecollector-02** VM.

12 Enter the following information and click **Done**.

Option	Value
VM Name	sfo01vropsc01b.sfo01.rainpole.local
vCenter Host	sfo01m01vc01.sfo01.rainpole.local
vCenter Cluster Name	sfo01-m01-mgmt01 (sfo01-m01dc)
VM Network	distributed switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vropsc01b.sfo01.rainpole.local
IP Address	192.168.31.32
Domain	sfo01.rainpole.local
Gateway	192.168.31.1

Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager prompts you for information for the virtual appliances for vRealize Log Insight.

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 Click **Advanced Settings** for **vrli-master** VM.

4 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01a.sfo01.rainpole.local
IP Address	192.168.31.11
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01a.sfo01.rainpole.local
Gateway	192.168.31.1

5 Click **Advanced Settings** for the **vrli-worker-01** VM.

6 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01b.sfo01.rainpole.local
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01b.sfo01.rainpole.local
Gateway	192.168.31.1

7 Click **Advanced Settings** for the **vrli-worker-02** VM.

8 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01c.sfo01.rainpole.local
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01c.sfo01.rainpole.local
Gateway	192.168.31.1

Run the Micro-Segmentation Installation Wizard with vRealize Suite Lifecycle Manager

6

Deploy Micro-Segmentation use case using the installation wizards in vRealize Suite Lifecycle Manager. The installation wizard prompts you for information about your deployment.

The installation wizard will prompt you for information about your deployment such as virtual machine names, IP addresses, and so on.

Prerequisites

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

See Micro-Segmentation Solution Path.

Procedure

1 Create the Environment for the Micro-Segmentation Use Case

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

2 Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

   vRealize Suite Lifecycle Manager prompts you for information for the virtual appliances for vRealize Log Insight.

Create the Environment for the Micro-Segmentation Use Case

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

Procedure

1 Login to vRealize Suite Lifecycle Manager

   a Open a Web browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	*vrlcm_admin_password*

2 On the **Home** page, click **Create Environment** to start a new deployment.

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

4 On the **Create New Environment** page, enter the following information.

Setting	Value
Data Center	sfo01-m01dc
Environment Type	Production
Environment Name	VVD-Micro-segmentation
Administrator Email	admin@rainpole.local
Default Password	**`default_admin_password`**
Customer Experience Improvement Program	Selected

5 Click the **Solutions** tab and select **VVD Version 4.1** from the drop down.

6 Select the check box for **Micro-Segmentation** 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, 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
vCenter Host Name	sfo01m01vc01.sfo01.rainpole.local
Cluster	sfo01-m01-mgmt01 (sfo01-m01dc)
Network	distributed switch that ends with `Mgmt-xRegion01-VXLAN`
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**.

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

a 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 deployment.

Configure vRealize Log Insight with vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager prompts you for information for the virtual appliances for vRealize Log Insight.

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 Click **Advanced Settings** for **vrli-master** VM.

4 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01a.sfo01.rainpole.local
IP Address	192.168.31.11
Domain	sfo01.rainpole.local

Option	Value
VM Name	sfo01vrli01a.sfo01.rainpole.local
Gateway	192.168.31.1

5 Click **Advanced Settings** for the **vrli-worker-01** VM.

6 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01b.sfo01.rainpole.local
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01b.sfo01.rainpole.local
Gateway	192.168.31.1

7 Click **Advanced Settings** for the **vrli-worker-02** VM.

8 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 switch that ends with `Mgmt-RegionA01-VXLAN`
Hostname	sfo01vrli01c.sfo01.rainpole.local
Domain	sfo01.rainpole.local
VM Name	sfo01vrli01c.sfo01.rainpole.local
Gateway	192.168.31.1

Import a JSON File to Deploy IT Automating IT

7

You can deploy the products that are used by the IT Automating IT use case by importing the IT Automating IT JSON file into vRealize Suite Lifecycle Manager.

Prerequisites

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

See IT Automating IT Solution Path.

Procedure

1 Login to vRealize Suite Lifecycle Manager

   a Open a Web browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	*vrlcm_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
Environment Name	VVD-ITAIT-JSON
Administrator Email	administrator@vsphere.local
Default Password	*default_admin_password*
Customer Experience Improvement Program	Selected

5 On the **Product Config JSON** section, copy and paste the sample JSON file below.

Note You are responsible for supplying the license, certificate, and key information.

6 Click **Create Environment**.

Example: IT Automating IT Example JSON File

```
{
  "requestId": null,
  "environmentId": "f3c8969d4a574e75558e64e985228",
  "infrastructure": {
    "sourceLink": "f3c8969d4a574e75558e64e985228",
    "properties": {
      "bindPassword": "",
      "dataCenterName": "sfo01-m01dc",
      "vcHostname": "sfo01m01vc01.sfo01.rainpole.local",
      "environmentId": "f3c8969d4a574e75558e64e985228",
      "masterVidmAdminUserName": "",
      "netmask": "255.255.255.0",
      "environmentName": "VVD-ITAIT",
      "clusterName": "sfo01-m01dc#sfo01-m01-mgmt01",
      "enableTelemetry": "true",
      "dnsServers": "172.16.11.4,172.16.11.5",
      "diskFormat": "Thin",
      "baseDN": "",
      "vcPassword": "vsphere_admin_password",
      "defaultPassword": "vsphere_admin_password",
      "adminEmail": "admin@rainpole.local",
      "adName": "",
         "certificateChain":
                                  "-----BEGIN CERTIFICATE-----
                           CERTIFICATE CHAIN CONTENTS HERE
          -----END CERTIFICATE-----\n
          -----BEGIN CERTIFICATE-----
          CERTIFICATE CONTENTS HERE
          -----END CERTIFICATE-----",
      "masterKeyPassphrase": "",
      "datastoreName": "sfo01-m01-vsan01",
      "masterVidmAdminPassword": "",
      "masterVidmEnabled": "",
      "uberAdmin": "",
      "license": "xxxx-xxxx-xxxx-xxxx-xxxx",
      "privateKey": "-----BEGIN RSA PRIVATE KEY-----
                    RSA PRIVATE KEY HERE
                    -----END RSA PRIVATE KEY-----",
      "bindDN": "",
      "vmNetwork": "distributed switch that ends with Mgmt-xRegion01-VXLAN",
      "masterPrivateKey": "",
      "masterVidmHostName": "",
      "groupDN": "",
      "masterVidmCloudAdminGroup": "",
      "vcUsername": "administrator@vsphere.local",
```

```
      "domain": "rainpole.local",
      "acceptEULA": true,
      "keyPassphrase": "Certificate_Passphrase",
      "gateway": "192.168.11.1",
      "searchpath": "rainpole.local,sfo01.rainpole.local",
      "masterCertificateChain": ""
    }
  },
  "encoded": true,
  "products": [
    {
      "sourceLink": null,
      "id": "vra",
      "version": "7.3.0",
      "clusterVIP": [
        {
          "type": "vra",
          "hostname": "vra01svr01.rainpole.local",
          "ipAddress": "192.168.11.53"
        },
        {
          "type": "iaas-web",
          "hostname": "vra01iws01.rainpole.local",
          "ipAddress": "192.168.11.56"
        },
        {
          "type": "iaas-manager",
          "hostname": "vra01ims01.rainpole.local",
          "ipAddress": "192.168.11.59"
        }
      ],
      "properties": {
        "windowsPassword": "vsphere_admin_password",
        "windowsUsername": "RAINPOLE\\svc-vra"
      },
      "nodes": [
        {
          "type": "vra-server-primary",
          "sourceLink": "",
          "properties": {
            "name": "vra01svr01a.rainpole.local",
            "ipAddress": "192.168.11.51",
            "hostname": "vra01svr01a.rainpole.local",
            "cluster": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "",
            "netmask": "",
            "sshEnabled": "",
            "dns": "",
            "licenseKey": "",
            "domain": "",
            "gateway": "",
            "searchpath": "",
            "vidmVraDisabledAdvanced": "false",
```

```
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "vra-server-secondary",
          "sourceLink": "",
          "properties": {
            "name": "vra01svr01b.rainpole.local",
            "ipAddress": "192.168.11.52",
            "hostname": "vra01svr01b.rainpole.local",
            "cluster": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "",
            "netmask": "",
            "sshEnabled": "",
            "dns": "",
            "domain": "",
            "gateway": "",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "db",
          "sourceLink": "",
          "properties": {
            "name": "vra01mssql01.rainpole.local",
            "ipAddress": "192.168.11.62",
            "hostname": "vra01mssql01.rainpole.local",
            "databaseName": "VRADB-01",
            "databaseUserName": "",
            "useWindowsAuthentication": "true",
            "useExistingDatabase": "",
            "databasePassword": ""
          }
        },
        {
          "type": "iaas-web",
          "sourceLink": "",
          "properties": {
            "name": "vra01iws01a.rainpole.local",
            "ipAddress": "192.168.11.54",
            "hostname": "vra01iws01a.rainpole.local",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "webPassword": "",
            "webUserName": "",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
```

```
            "type": "iaas-web",
            "sourceLink": "",
            "properties": {
              "name": "vra01iws01b.rainpole.local",
              "ipAddress": "192.168.11.55",
              "hostname": "vra01iws01b.rainpole.local",
              "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
              "webPassword": "",
              "webUserName": "",
              "installationPath": "",
              "userName": "administrator@vsphere.local",
              "password": "vsphere_admin_password"
            }
          },
          {
            "type": "iaas-manager-active",
            "sourceLink": "",
            "properties": {
              "name": "vra01ims01a.rainpole.local",
              "ipAddress": "192.168.11.57",
              "hostname": "vra01ims01a.rainpole.local",
              "msUserName": "",
              "msPassword": "",
              "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
              "installationPath": "",
              "userName": "administrator@vsphere.local",
              "password": "vsphere_admin_password"
            }
          },
          {
            "type": "iaas-manager-passive",
            "sourceLink": "",
            "properties": {
              "name": "vra01ims01b.rainpole.local",
              "ipAddress": "192.168.11.58",
              "hostname": "vra01ims01b.rainpole.local",
              "msUserName": "",
              "msPassword": "",
              "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
              "installationPath": "",
              "userName": "administrator@vsphere.local",
              "password": "vsphere_admin_password"
            }
          },
          {
            "type": "iaas-dem-worker",
            "sourceLink": "",
            "properties": {
              "name": "DEM-WORKER-01",
              "ipAddress": "192.168.11.60",
              "hostname": "vra01dem01a.rainpole.local",
              "demUserName": "",
              "demPassword": "",
              "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
              "installationPath": "",
```

```
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "iaas-dem-worker",
          "sourceLink": "",
          "properties": {
            "name": "DEM-WORKER-02",
            "ipAddress": "192.168.11.60",
            "hostname": "vra01dem01a.rainpole.local",
            "demUserName": "",
            "demPassword": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "iaas-dem-worker",
          "sourceLink": "",
          "properties": {
            "name": "DEM-WORKER-03",
            "ipAddress": "192.168.11.60",
            "hostname": "vra01dem01a.rainpole.local",
            "demUserName": "",
            "demPassword": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "iaas-dem-worker",
          "sourceLink": "",
          "properties": {
            "name": "DEM-WORKER-04",
            "ipAddress": "192.168.11.61",
            "hostname": "vra01dem01b.rainpole.local",
            "demUserName": "",
            "demPassword": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "iaas-dem-worker",
          "sourceLink": "",
          "properties": {
            "name": "DEM-WORKER-05",
            "ipAddress": "192.168.11.61",
```

```
            "hostname": "vra01dem01b.rainpole.local",
            "demUserName": "",
            "demPassword": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "iaas-dem-worker",
          "sourceLink": "",
          "properties": {
            "name": "DEM-WORKER-06",
            "ipAddress": "192.168.11.61",
            "hostname": "vra01dem01b.rainpole.local",
            "demUserName": "",
            "demPassword": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "iaas-dem-orchestrator",
          "sourceLink": "",
          "properties": {
            "name": "DEM-ORCHESTRATOR-01",
            "ipAddress": "192.168.11.57",
            "hostname": "vra01ims01a.rainpole.local",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "demUserName": "",
            "demPassword": "",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "iaas-dem-orchestrator",
          "sourceLink": "",
          "properties": {
            "name": "DEM-ORCHESTRATOR-02",
            "ipAddress": "192.168.11.58",
            "hostname": "vra01ims01b.rainpole.local",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "demUserName": "",
            "demPassword": "",
            "installationPath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
```

```
          "type": "proxy-agent-vsphere",
          "sourceLink": "",
          "properties": {
            "name": "VSPHERE-AGENT-01",
            "ipAddress": "192.168.31.52",
            "hostname": "sfo01ias01a.sfo01.rainpole.local",
            "agentUserName": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "agentPassword": "",
            "installationPath": "",
            "vsphereEndpointName": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "proxy-agent-vsphere",
          "sourceLink": "",
          "properties": {
            "name": "VSPHERE-AGENT-02",
            "ipAddress": "192.168.31.53",
            "hostname": "sfo01ias01b.sfo01.rainpole.local",
            "agentUserName": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "agentPassword": "",
            "installationPath": "",
            "vsphereEndpointName": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        }
      ]
    },
    {
      "sourceLink": null,
      "id": "vrbc",
      "version": "7.3.0",
      "clusterVIP": [],
      "properties": {
        "currency": "USD - US Dollar"
      },
      "nodes": [
        {
          "type": "vrb-server",
          "sourceLink": "",
          "properties": {
            "name": "vra01bus01.rainpole.local",
            "ipAddress": "192.168.11.66",
            "hostname": "vra01bus01.rainpole.local",
            "cluster": "",
            "vrbTelemetryEnabled": "",
            "tenantPassword": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "",
```

```
            "tenantUser": "",
            "netmask": "",
            "diskFormat": "",
            "vrbCurrency": "",
            "sshEnabled": "",
            "dns": "",
            "vrbLicenseKey": "",
            "isTelemetryEnable": "",
            "domain": "",
            "gateway": "",
            "searchpath": "",
            "isStandalone": "",
            "masterVidmEnabled": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "vrb-collector",
          "sourceLink": "",
          "properties": {
            "name": "vra01buc01.sfo01.rainpole.local",
            "ipAddress": "192.168.31.54",
            "hostname": "vra01buc01.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vrbTelemetryEnabled": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "diskFormat": "",
            "vrbCurrency": "",
            "sshEnabled": "",
            "dns": "",
            "vrbLicenseKey": "",
            "isTelemetryEnable": "",
            "domain": "sfo01.rainpole.local",
            "gateway": "192.168.31.1",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        }
      ]
    },
    {
      "sourceLink": null,
      "id": "vrops",
      "version": "6.6.1",
      "clusterVIP": [],
      "properties": {
        "ntpServerIP": "ntp.sfo01.rainpole.local"
      },
      "nodes": [
        {
```

```
            "type": "master",
            "sourceLink": "",
            "properties": {
              "name": "vrops01svr01a.rainpole.local",
              "ipAddress": "192.168.11.31",
              "hostname": "vrops01svr01a.rainpole.local",
              "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
              "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
              "storage": "",
              "network": "",
              "netmask": "",
              "diskFormat": "",
              "ntpServer": "",
              "dns": "",
              "timeZone": "",
              "license": "",
              "domain": "",
              "gateway": "",
              "deployOption": "",
              "extendedStorage": "sfo01-m01-vsan01",
              "searchpath": "",
              "masterVidmEnabled": "",
              "masterVidmHostName": "",
              "masterVidmSourceName": "",
              "masterVidmTenant": "",
              "masterVidmAdminUserName": "",
              "masterVidmAdminPassword": "",
              "userName": "administrator@vsphere.local",
              "password": "vsphere_admin_password"
            }
          },
          {
            "type": "replica",
            "sourceLink": "",
            "properties": {
              "name": "vrops01svr01b.rainpole.local",
              "ipAddress": "192.168.11.32",
              "hostname": "vrops01svr01b.rainpole.local",
              "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
              "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
              "storage": "",
              "network": "",
              "netmask": "",
              "diskFormat": "",
              "dns": "",
              "timeZone": "",
              "domain": "",
              "gateway": "",
              "deployOption": "",
              "extendedStorage": "sfo01-m01-vsan01",
              "searchpath": "",
              "userName": "administrator@vsphere.local",
              "password": "vsphere_admin_password"
            }
          },
```

```
        {
          "type": "data",
          "sourceLink": "",
          "properties": {
            "name": "vrops01svr01c.rainpole.local",
            "ipAddress": "192.168.11.33",
            "hostname": "vrops01svr01c.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "",
            "netmask": "",
            "diskFormat": "",
            "dns": "",
            "timeZone": "",
            "domain": "",
            "gateway": "",
            "deployOption": "",
            "extendedStorage": "sfo01-m01-vsan01",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "remotecollector",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vropsc01a.sfo01.rainpole.local",
            "ipAddress": "192.168.31.31",
            "hostname": "sfo01vropsc01a.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "diskFormat": "",
            "ntpServer": "",
            "dns": "",
            "timeZone": "",
            "domain": "sfo01.rainpole.local",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "extendedStorage": "",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "remotecollector",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vropsc01b.sfo01.rainpole.local",
            "ipAddress": "192.168.31.32",
```

```
            "hostname": "sfo01vropsc01b.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "diskFormat": "",
            "ntpServer": "",
            "dns": "",
            "timeZone": "",
            "domain": "sfo01.rainpole.local",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "extendedStorage": "",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        }
      ]
    },
    {
      "sourceLink": null,
      "id": "vrli",
      "version": "4.5.0",
      "clusterVIP": [],
      "properties": {
        "vrliClusterVips": "192.168.31.10#sfo01vrli01.sfo01.rainpole.local"
      },
      "nodes": [
        {
          "type": "vrli-master",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01a.sfo01.rainpole.local",
            "ipAddress": "192.168.31.11",
            "hostname": "sfo01vrli01a.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "vrliAdminEmail": "",
            "netmask": "",
            "vrliAdminUser": "",
            "diskFormat": "",
            "vrliLicenseKey": "",
            "dns": "",
            "domain": "sfo01.rainpole.local",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "masterVidmEnabled": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
```

```
        },
        {
          "type": "vrli-worker",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01b.sfo01.rainpole.local",
            "ipAddress": "192.168.31.12",
            "hostname": "sfo01vrli01b.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "dns": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "domain": "sfo01.rainpole.local",
            "diskFormat": "",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "vrli-worker",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01c.sfo01.rainpole.local",
            "ipAddress": "192.168.31.13",
            "hostname": "sfo01vrli01c.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "dns": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "domain": "sfo01.rainpole.local",
            "diskFormat": "",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        }
      ]
    }
  ]
}
```

Import a JSON File to Deploy Intelligent Operations

8

You can deploy all products that are required for the Intelligent Operations use case by importing the Intelligent Operations JSON file into vRealize Suite Lifecycle Manager.

Prerequisites

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

See Intelligent Operations Solution Path.

Procedure

1 Login to vRealize Suite Lifecycle Manager

   a Open a Web browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	*vrlcm_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
Environment Name	VVD-Intelligent-Ops-JSON
Administrator Email	administrator@vsphere.local
Default Password	*default_admin_password*
Customer Experience Improvement Program	Selected

5 On the **Product Config JSON** section, copy and paste the sample JSON file below.

Note You are responsible for providing license key and certificate and key information.

6 Click **Create Environment**.

Example: Example JSON File for Intelligent Operations

```
{
  "requestId": null,
  "environmentId": "f3c8969d4a574e75558e64e985228",
  "infrastructure": {
    "sourceLink": "f3c8969d4a574e75558e64e985228",
    "properties": {
      "bindPassword": "",
      "dataCenterName": "sfo01-m01dc",
      "vcHostname": "sfo01m01vc01.sfo01.rainpole.local",
      "environmentId": "f3c8969d4a574e75558e64e985228",
      "masterVidmAdminUserName": "",
      "netmask": "255.255.255.0",
      "environmentName": "VVD-IntelligentOperation",
      "clusterName": "sfo01-m01dc#sfo01-m01-mgmt01",
      "enableTelemetry": "true",
      "dnsServers": "172.16.11.4,172.16.11.5",
      "diskFormat": "Thin",
      "baseDN": "",
      "vcPassword": "vsphere_admin_password",
      "defaultPassword": "vsphere_admin_password",
      "adminEmail": "admin@rainpole.local",
      "adName": "",
      "certificateChain":
                                  "-----BEGIN CERTIFICATE-----
                           CERTIFICATE CHAIN CONTENTS HERE
          -----END CERTIFICATE-----\n
          -----BEGIN CERTIFICATE-----
          CERTIFICATE CONTENTS HERE
          -----END CERTIFICATE-----",
      "masterKeyPassphrase": "",
      "datastoreName": "sfo01-m01-vsan01",
      "masterVidmAdminPassword": "",
      "masterVidmEnabled": "",
      "uberAdmin": "",
      "license": "xxxx-xxxx-xxxx-xxxx-xxxx",
      "privateKey": "-----BEGIN RSA PRIVATE KEY-----
                    RSA PRIVATE KEY HERE
                    -----END RSA PRIVATE KEY-----",
      "bindDN": "",
      "vmNetwork": "distributed switch that ends with Mgmt-xRegion01-VXLAN",
      "masterPrivateKey": "",
      "masterVidmHostName": "",
      "groupDN": "",
      "masterVidmCloudAdminGroup": "",
      "vcUsername": "administrator@vsphere.local",
```

```
      "domain": "rainpole.local",
      "acceptEULA": true,
      "keyPassphrase": "Certificate_Passphrase",
      "gateway": "192.168.11.1",
      "searchpath": "rainpole.local,sfo01.rainpole.local",
      "masterCertificateChain": ""
    }
  },
  "encoded": true,
  "products": [
    {
      "sourceLink": null,
      "id": "vrops",
      "version": "6.6.1",
      "clusterVIP": [],
      "properties": {
        "ntpServerIP": "ntp.sfo01.rainpole.local"
      },
      "nodes": [
        {
          "type": "master",
          "sourceLink": "",
          "properties": {
            "name": "vrops01svr01a.rainpole.local",
            "ipAddress": "192.168.11.31",
            "hostname": "vrops01svr01a.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "",
            "netmask": "",
            "diskFormat": "",
            "ntpServer": "",
            "dns": "",
            "timeZone": "",
            "license": "",
            "domain": "",
            "gateway": "",
            "deployOption": "",
            "extendedStorage": "sfo01-m01-vsan01",
            "searchpath": "",
            "masterVidmEnabled": "",
            "masterVidmHostName": "",
            "masterVidmSourceName": "",
            "masterVidmTenant": "",
            "masterVidmAdminUserName": "",
            "masterVidmAdminPassword": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "replica",
          "sourceLink": "",
          "properties": {
```

```
            "name": "vrops01svr01b.rainpole.local",
            "ipAddress": "192.168.11.32",
            "hostname": "vrops01svr01b.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "",
            "netmask": "",
            "diskFormat": "",
            "dns": "",
            "timeZone": "",
            "domain": "",
            "gateway": "",
            "deployOption": "",
            "extendedStorage": "sfo01-m01-vsan01",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "data",
          "sourceLink": "",
          "properties": {
            "name": "vrops01svr01c.rainpole.local",
            "ipAddress": "192.168.11.33",
            "hostname": "vrops01svr01c.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "",
            "netmask": "",
            "diskFormat": "",
            "dns": "",
            "timeZone": "",
            "domain": "",
            "gateway": "",
            "deployOption": "",
            "extendedStorage": "sfo01-m01-vsan01",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "remotecollector",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vropsc01a.sfo01.rainpole.local",
            "ipAddress": "192.168.31.31",
            "hostname": "sfo01vropsc01a.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
```

```
            "netmask": "",
            "diskFormat": "",
            "ntpServer": "",
            "dns": "",
            "timeZone": "",
            "domain": "sfo01.rainpole.local",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "extendedStorage": "",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "remotecollector",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vropsc01b.sfo01.rainpole.local",
            "ipAddress": "192.168.31.32",
            "hostname": "sfo01vropsc01b.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "diskFormat": "",
            "ntpServer": "",
            "dns": "",
            "timeZone": "",
            "domain": "sfo01.rainpole.local",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "extendedStorage": "",
            "searchpath": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        }
      ]
    },
    {
      "sourceLink": null,
      "id": "vrli",
      "version": "4.5.0",
      "clusterVIP": [],
      "properties": {
        "vrliClusterVips": "192.168.31.10#sfo01vrli01.sfo01.rainpole.local"
      },
      "nodes": [
        {
          "type": "vrli-master",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01a.sfo01.rainpole.local",
```

```
            "ipAddress": "192.168.31.11",
            "hostname": "sfo01vrli01a.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "vrliAdminEmail": "",
            "netmask": "",
            "vrliAdminUser": "",
            "diskFormat": "",
            "vrliLicenseKey": "",
            "dns": "",
            "domain": "sfo01.rainpole.local",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "masterVidmEnabled": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "vrli-worker",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01b.sfo01.rainpole.local",
            "ipAddress": "192.168.31.12",
            "hostname": "sfo01vrli01b.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "dns": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "domain": "sfo01.rainpole.local",
            "diskFormat": "",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "vrli-worker",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01c.sfo01.rainpole.local",
            "ipAddress": "192.168.31.13",
            "hostname": "sfo01vrli01c.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "dns": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
```

```
            "netmask": "",
            "domain": "sfo01.rainpole.local",
            "diskFormat": "",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        }
      ]
    }
  ]
}
```

Import a JSON File to Deploy the Micro-Segmentation Use Case

9

You can deploy the products that are required by the Micro-Segmentation use case by importing a JSON file file in vRealize Suite Lifecycle Manager.

Prerequisites

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

See Micro-Segmentation Solution Path.

Procedure

1 Login to vRealize Suite Lifecycle Manager

   a Open a Web browser and go to **`https://sfo01m01vrlcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	*vrlcm_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
Environment Name	VVD-Micro-segmentation-JSON
Administrator Email	administrator@vsphere.local
Default Password	*default_admin_password*
Customer Experience Improvement Program	Selected

5 On the **Product Config JSON** section, copy and paste the sample JSON file below.

6 Click **Create Environment**.

Example: Micro-Segmentation Example JSON File

```
{
  "requestId": null,
  "environmentId": "f3c8969d4a574e75558e64e985228",
  "infrastructure": {
    "sourceLink": "f3c8969d4a574e75558e64e985228",
    "properties": {
      "bindPassword": "",
      "dataCenterName": "sfo01-m01dc",
      "vcHostname": "sfo01m01vc01.sfo01.rainpole.local",
      "environmentId": "f3c8969d4a574e75558e64e985228",
      "masterVidmAdminUserName": "",
      "netmask": "255.255.255.0",
      "environmentName": "VVD-Mseg",
      "clusterName": "sfo01-m01dc#sfo01-m01-mgmt01",
      "enableTelemetry": "true",
      "dnsServers": "172.16.11.4,172.16.11.5",
      "diskFormat": "Thin",
      "baseDN": "",
      "vcPassword": "vsphere_admin_password",
      "defaultPassword": "vsphere_admin_password",
      "adminEmail": "admin@rainpole.local",
      "adName": "",
      "certificateChain":
                                  "-----BEGIN CERTIFICATE-----
                           CERTIFICATE CHAIN CONTENTS HERE
          -----END CERTIFICATE-----\n
          -----BEGIN CERTIFICATE-----
          CERTIFICATE CONTENTS HERE
          -----END CERTIFICATE-----",
      "masterKeyPassphrase": "",
      "datastoreName": "sfo01-m01-vsan01",
      "masterVidmAdminPassword": "",
      "masterVidmEnabled": "",
      "uberAdmin": "",
      "license": "xxxx-xxxx-xxxx-xxxx-xxxx",
     "privateKey": "-----BEGIN RSA PRIVATE KEY-----
                    RSA PRIVATE KEY HERE
                    -----END RSA PRIVATE KEY-----",
      "bindDN": "",
      "vmNetwork": "distributed switch that ends with Mgmt-xRegion01-VXLAN",
      "masterPrivateKey": "",
      "masterVidmHostName": "",
      "groupDN": "",
      "masterVidmCloudAdminGroup": "",
      "vcUsername": "administrator@vsphere.local",
      "domain": "rainpole.local",
      "acceptEULA": true,
      "keyPassphrase": "Certificate_Passphrase",
      "gateway": "192.168.11.1",
      "searchpath": "rainpole.local,sfo01.rainpole.local",
      "masterCertificateChain": ""
```

```
    }
  },
  "encoded": true,
  "products": [
    {
      "sourceLink": null,
      "id": "vrli",
      "version": "4.5.0",
      "clusterVIP": [],
      "properties": {
        "vrliClusterVips": "192.168.31.10#sfo01vrli01.sfo01.rainpole.local"
      },
      "nodes": [
        {
          "type": "vrli-master",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01a.sfo01.rainpole.local",
            "ipAddress": "192.168.31.11",
            "hostname": "sfo01vrli01a.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "vrliAdminEmail": "",
            "netmask": "",
            "vrliAdminUser": "",
            "diskFormat": "",
            "vrliLicenseKey": "",
            "dns": "",
            "domain": "sfo01.rainpole.local",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "masterVidmEnabled": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "vrli-worker",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01b.sfo01.rainpole.local",
            "ipAddress": "192.168.31.12",
            "hostname": "sfo01vrli01b.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "dns": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "domain": "sfo01.rainpole.local",
            "diskFormat": "",
            "searchpath": "",
```

```
            "gateway": "192.168.31.1",
            "deployOption": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        },
        {
          "type": "vrli-worker",
          "sourceLink": "",
          "properties": {
            "name": "sfo01vrli01c.sfo01.rainpole.local",
            "ipAddress": "192.168.31.13",
            "hostname": "sfo01vrli01c.sfo01.rainpole.local",
            "cluster": "sfo01-m01dc#sfo01-m01-mgmt01",
            "dns": "",
            "vCenterHost": "sfo01m01vc01.sfo01.rainpole.local",
            "storage": "",
            "network": "distributed switch that ends with Mgmt-RegionA01-VXLAN",
            "netmask": "",
            "domain": "sfo01.rainpole.local",
            "diskFormat": "",
            "searchpath": "",
            "gateway": "192.168.31.1",
            "deployOption": "",
            "userName": "administrator@vsphere.local",
            "password": "vsphere_admin_password"
          }
        }
      ]
    }
  ]
}
```

Post-Deployment Tasks for vRealize Suite Lifecycle Manager Use Cases

10

After you deploy a use case with vRealize Suite Lifecycle Manager, you have to perform post-deployment tasks on some of the products that vRealize Suite Lifecycle Manager installs.

Which post-deployment tasks you perform depends on the use case you deployed. See Chapter 1 vRealize Suite Lifecycle Manager Solution Paths for details.

This chapter includes the following topics:

Post-Deployment Tasks for vRealize Automation

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

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

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

Set Up NTP on the vRealize Automation Appliance

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

Procedure

1 Log in to the first vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480/`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

2 On the **VMware vRealize Appliance** page, click the **Admin** tab.

3 On the **Admin** tab, click **Time Settings**.

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

Setting	Value
Time Server	ntp.sfo01.rainpole.local

5 Click **Save Settings**.

6 Repeat the above steps for the second vRealize Automation appliance, **`https://vra01svr01b.rainpole.local:5480/`**

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

vRealize Automation Default Tenant Configuration

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

Create a Local Tenant Administrator

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

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

Procedure

1 Log in to the vRealize Automation portal.

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

   b Log in using the following credentials.

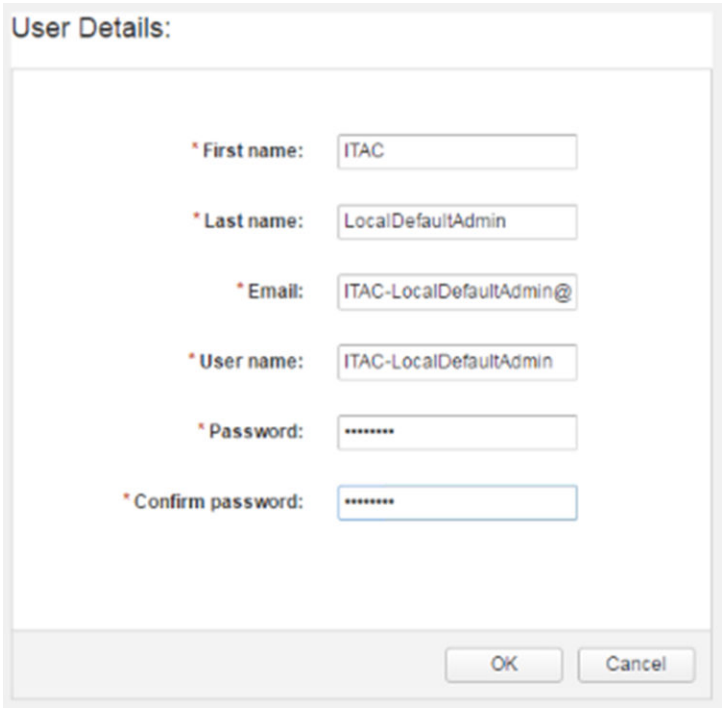
Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 On the `Tenants` page, click the default tenant **vsphere.local** to edit its settings.

3 Click the **Local users** tab and click **New** to add a local user to the default tenant.

4 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	ITAC
Last name	LocalDefaultAdmin
Email	ITAC-LocalDefaultAdmin@vsphere.local
User name	ITAC-LocalDefaultAdmin
Password	*itac-localdefaultadmin_password*
Confirm password	*itac-localdefaultadmin_password*

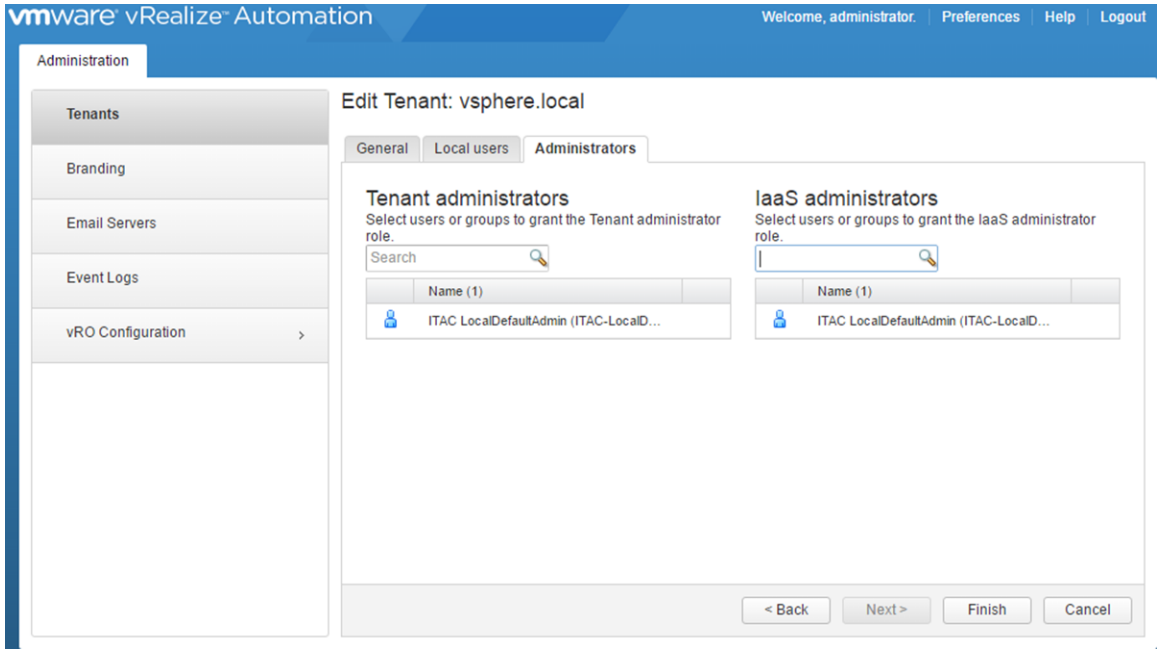


5 On the **Administrators** tab, specify tenant and infrastructure administrators.

a In the **Tenant administrators** search text box, enter **`ITAC-LocalDefaultAdmin`** and press Enter.

b In the **IaaS administrators** search text box, enter **`ITAC-LocalDefaultAdmin`** and press Enter.

c Click **Finish**.



6 Log out from the vRealize Automation portal.

Join Connectors to an Active Directory Domain

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

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

Procedure

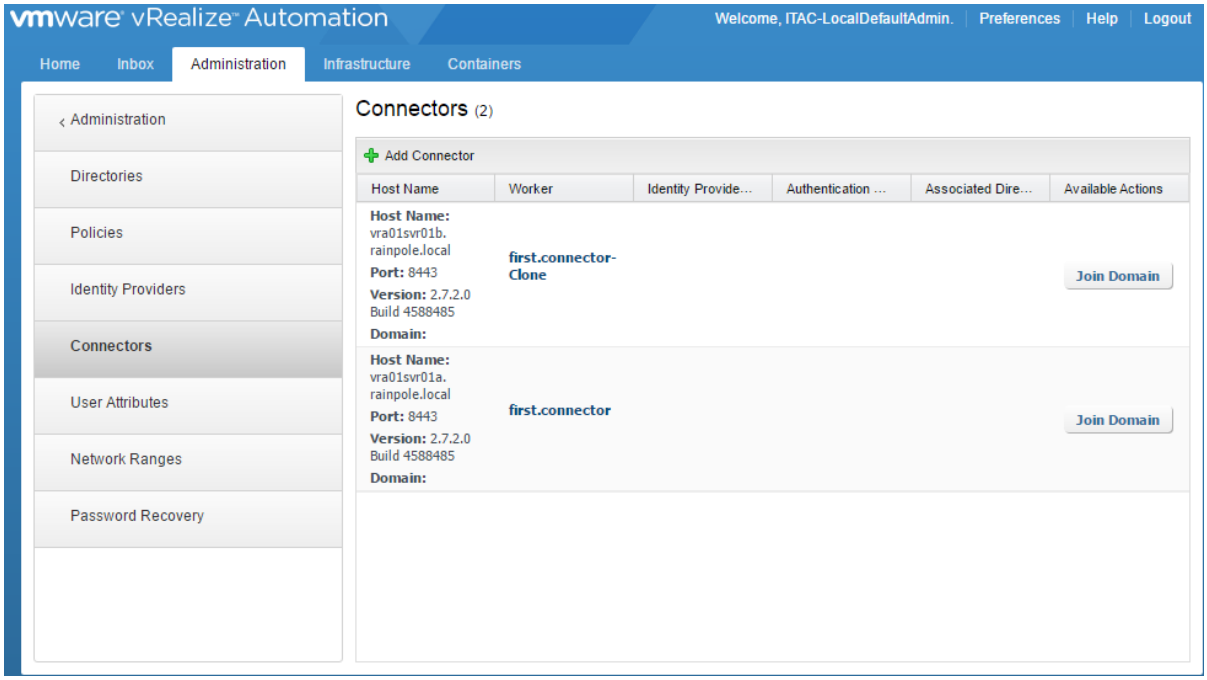
1 Log in to the vRealize Automation portal.

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

b Log in using the following credentials.

Setting	Value
User name	ITAC-LocalDefaultAdmin
Password	*itac-localdefaultadmin_password*

2 Navigate to **Administration > Directories Management > Connectors**.



3 For the **first.connector**, click **Join Domain**, specify the following settings and click **Join Domain**.

Setting	Value
Domain	Custom Domain
	rainpole.local
Domain User	administrator
Domain Password	*domain_admin_password*

4 For the **first-connector-Clone**, click **Join Domain**, specify the following settings and click **Join Domain**.

Setting	Value
Domain	Custom Domain
	rainpole.local
Domain User	administrator
Domain Password	*domain_admin_password*

5 Log out from the vRealize Automation portal.

vRealize Automation Tenant Creation

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

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

Create the Rainpole Tenant

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

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

Procedure

1 Log in to the vRealize Automation portal.

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

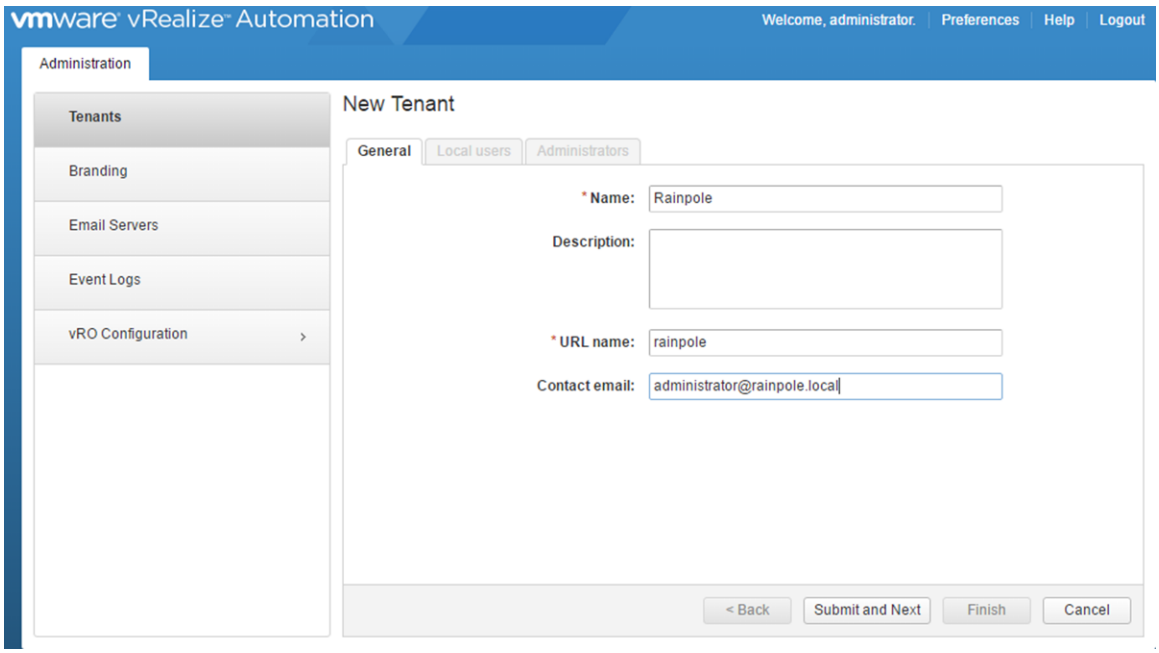
   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 On the **Tenants** page, click **New** to configure a new tenant.

3 On the **General** tab, enter the following settings for the Rainpole tenant, and click **Submit and Next**.

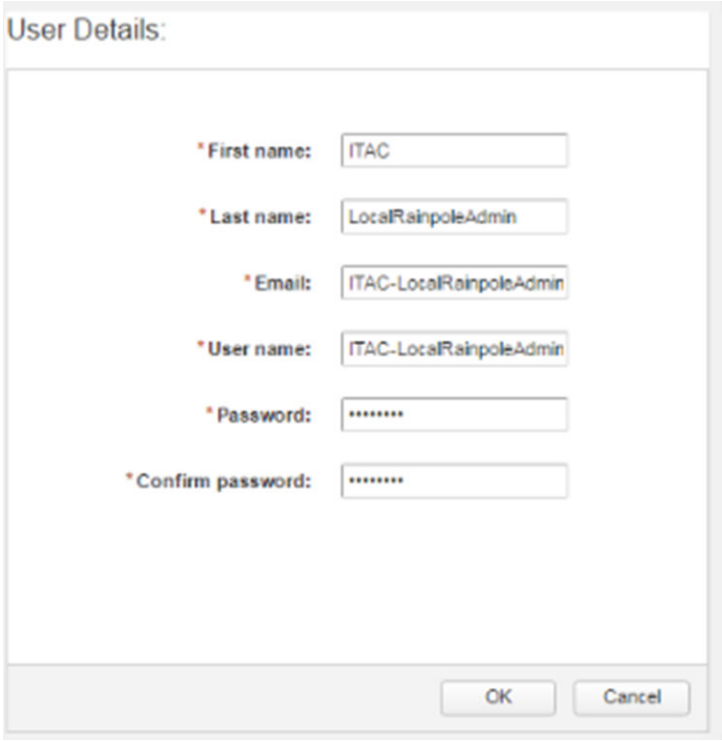
Setting	Value
Name	Rainpole
URL Name	rainpole
Contact email	administrator@rainpole.local



4 On the **Local Users** tab, click **New** to add a local user for the tenant.

5 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	ITAC
Last name	LocalRainpoleAdmin
Email	ITAC-LocalRainpoleAdmin@rainpole.local
User name	ITAC-LocalRainpoleAdmin
Password	*itac-localrainpoleadmin_password*
Confirm password	*itac-localrainpoleadmin_password*

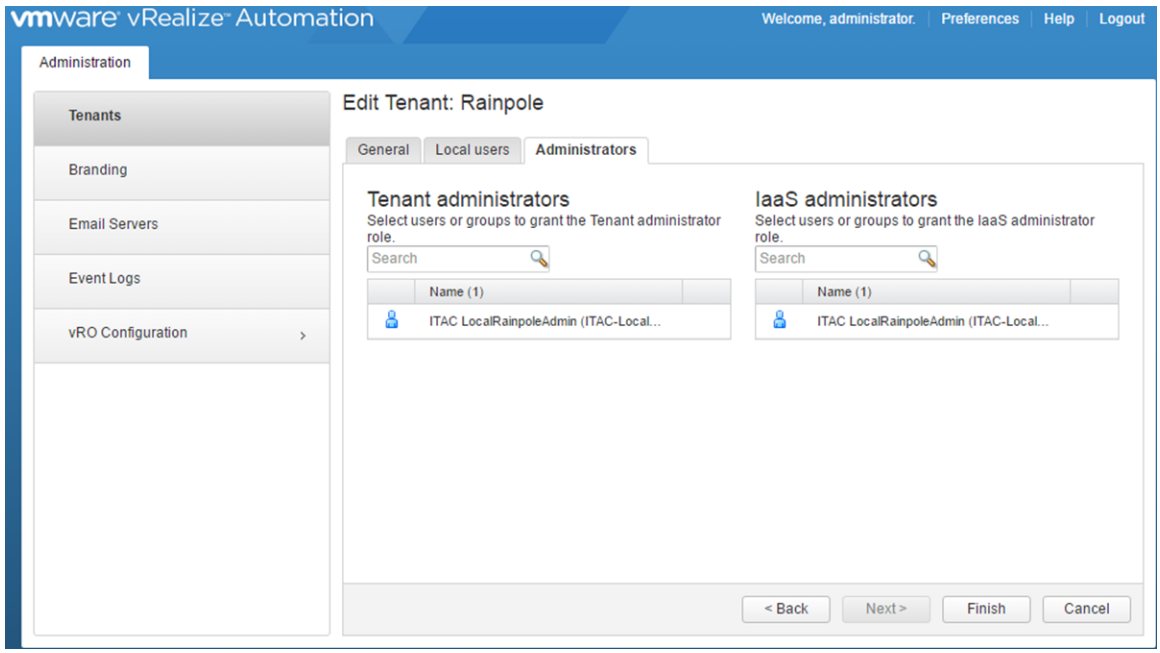


6 On the **Administrators** tab, specify tenant and infrastructure administrators.

a Enter `ITAC-LocalRainpoleAdmin` in the **Tenant administrators** search text box and press **Enter**.

b Enter `ITAC-LocalRainpoleAdmin` in the **IaaS administrators** search text box and press **Enter**.

c Click **Finish**.



7 Log out of vRealize Automation portal.

Configure Identity Management for the vRealize Automation Tenant

vRealize Automation uses VMware Identity Manager to authenticate users. You have to associate each tenant with at least one directory. Active Directory user information for selected groups and users is then synchronized with the directory for the tenant.

You can add more directories if necessary. Perform the procedure by using the ITAC-LocalRainpoleAdmin that you configured.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

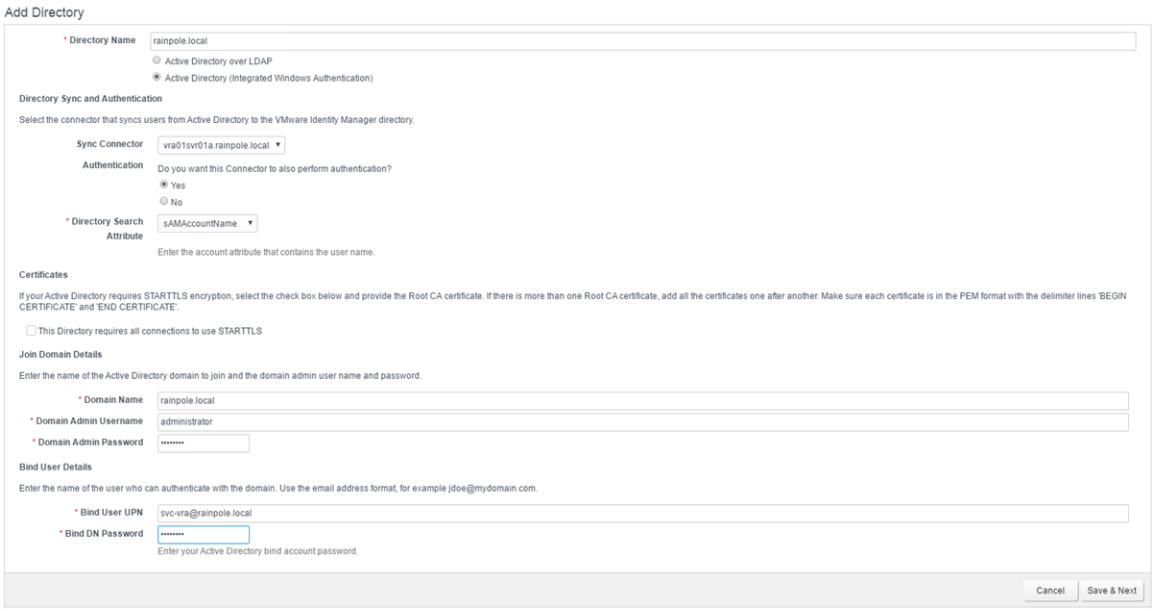
b Log in using the following credentials.

Setting	Value
User name	ITAC-LocalRainpoleAdmin
Password	*itac-localrainpoleadmin_password*

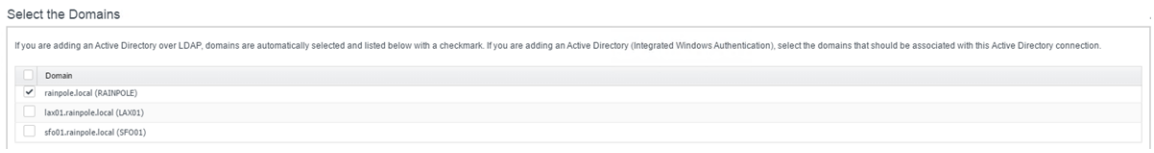
2 Navigate to **Administration > Directories Management > Directories**.

3 Click **Add Directory**, select **Add Active Directory over LDAP/IWA**, specify the following settings, and click **Save & Next**.

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



4 On the **Select the Domains** page, select **rainpole.local (RAINPOLE)** and click **Next**.



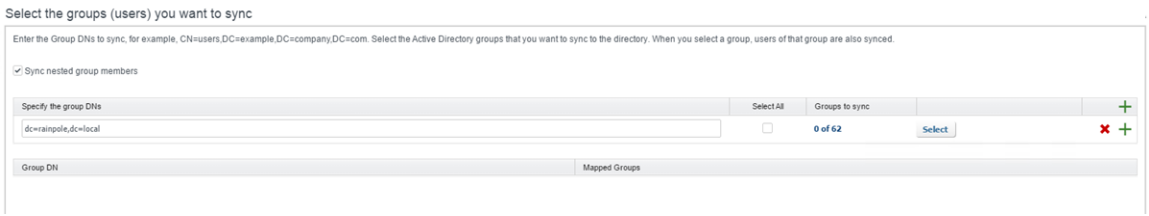
5 On the **Map User Attributes** page, click **Next**.

6 On the **Select the groups (users) you want to sync** page, enter the group DNs to sync.

a Click the **Add** icon to add the distinguished name to the search criteria.

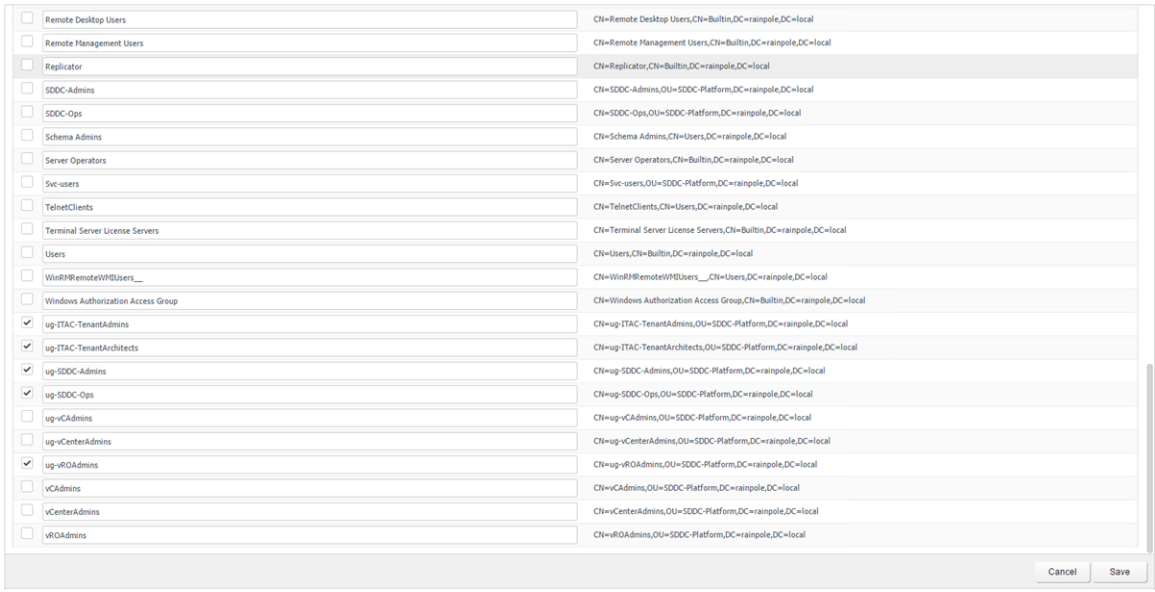
b In the **Specify the group DNs** text box, enter **`dc=rainpole,dc=local`** and click **Find Groups**.

c After the **Groups to sync** value updates, click **Select**.

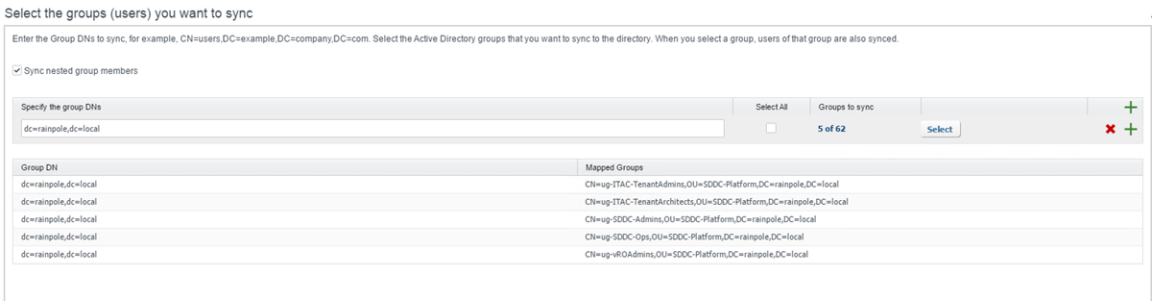


d Select the following groups and click **Save**.

- ug-ITAC-TenantAdmins
- ug-ITAC-TenantArchitects
- ug-SDDC-Admins
- ug-SDDC-Ops
- ug-vROAdmins



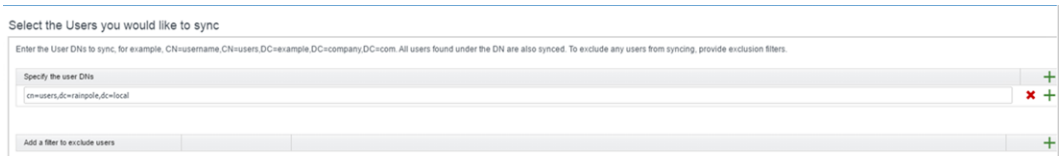
e Click **Save** and then click **Next**.



7 On the **Select the Users you would like to sync** page, enter the user DNs to sync.

   a Click the **Add** icon to add the distinguished name to the search criteria.

   b In the **Specify the user DNs** text box, enter **`cn=users,dc=rainpole,dc=local`**, click the **Add** icon on the same row, and click **Save**.



8 On the **Review** page, click **Sync Directory**.

Configure Directories Management for High Availability

Each vRealize Automation appliance includes a connector that supports user authentication. One connector is typically configured to perform directory synchronization. To support high availability, you configure a second connector.

The second connector points to your second vRealize Automation appliance. That second connector connects to the same Identity Provider and, through VMware Identity Manager, points to the same Active Directory instance. With this configuration, if one appliance fails, the other can take over management of user authentication.

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

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

   b Log in using the following credentials.

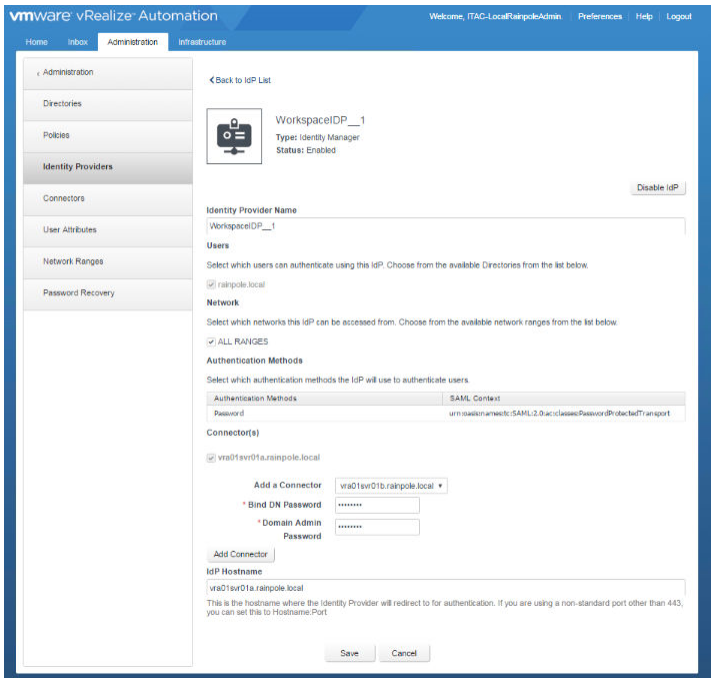
Setting	Value
User name	ITAC-LocalRainpoleAdmin
Password	*itac-localrainpoleadmin_password*

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

3 Click **WorkspaceIDP_1** to edit its settings.

4 Under **Connector(s)**, specify the following settings and click **Add Connector**.

Setting	Value
Add a Connector	vra01svr01b.rainpole.local
Bind DN Password	*svc-vra_password*
Domain Admin Password	*domain_admin_password*



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

Assign Tenant Administrative Roles to Active Directory Users

After you associate a tenant directory with an Active Directory domain for each tenant, you can administer the tenant user groups. In this task, you assign domain user groups for the Rainpole tenant and for infrastructure administrators.

Procedure

1 Log in to the vRealize Automation portal.

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

b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

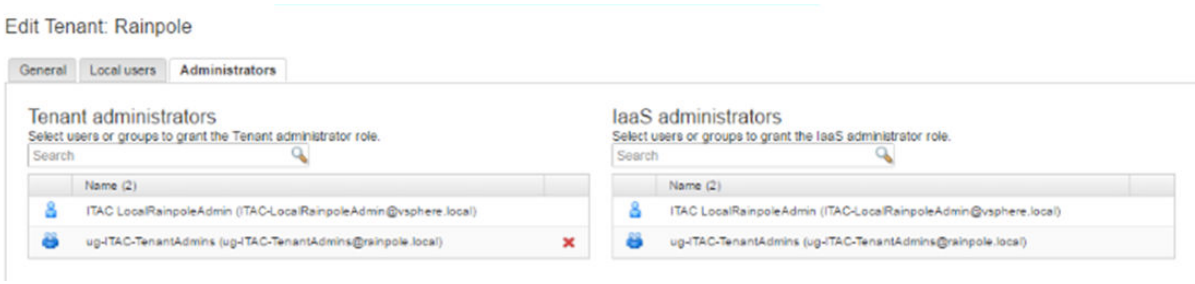
2 On the **Tenants** page, click the Rainpole tenant to edit its settings.

3 Click the **Administrators** tab to assign domain user groups for tenant and infrastructure administrators.

   a Enter **`ug-ITAC-TenantAdmins`** in the **Tenant administrators** search text box and press **Enter**.

   b Enter **`ug-ITAC-TenantAdmins`** in the **IaaS administrators** search text box and press **Enter**.

   c Click **Finish**.



Brand the Tenant Login Pages

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

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

Procedure

1 Log in to the vRealize Automation portal.

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

   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

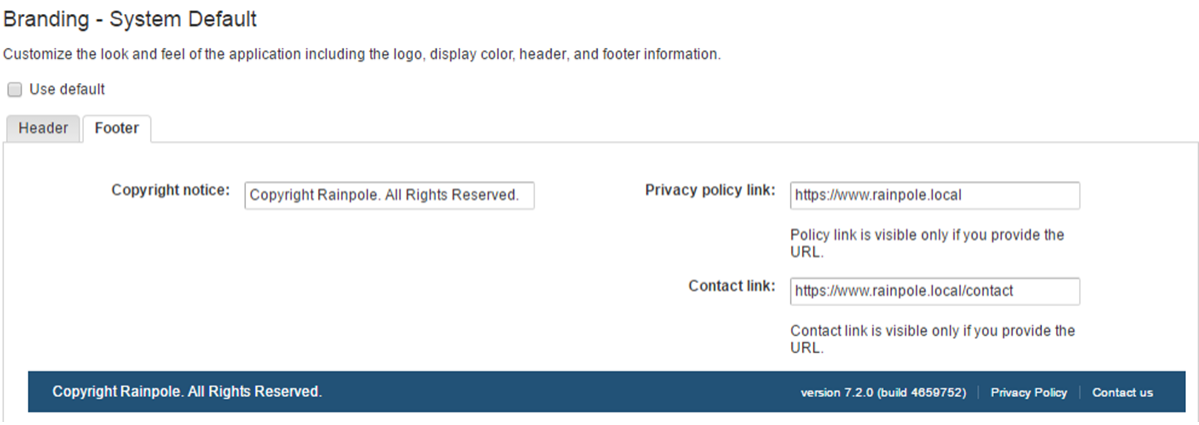
2 Navigate to **Administration > Branding** and deselect the **Use default** check box.

3 On the **Header** tab specify the following settings for the header branding.

Setting	Value
Company Name	Rainpole
Product Name	Infrastructure Service Portal
Background hex color	*3989C7*
Text hex color	*FFFFFF*

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

Setting	Value
Copyright notice	Copyright Rainpole. All Rights Reserved.
Privacy policy link	https://www.rainpole.local
Contact link	https://www.rainpole.local/contact



Configure the Default Email Servers

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

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

Procedure

1 Log in to the vRealize Automation portal.

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

   b Log in using the following credentials.

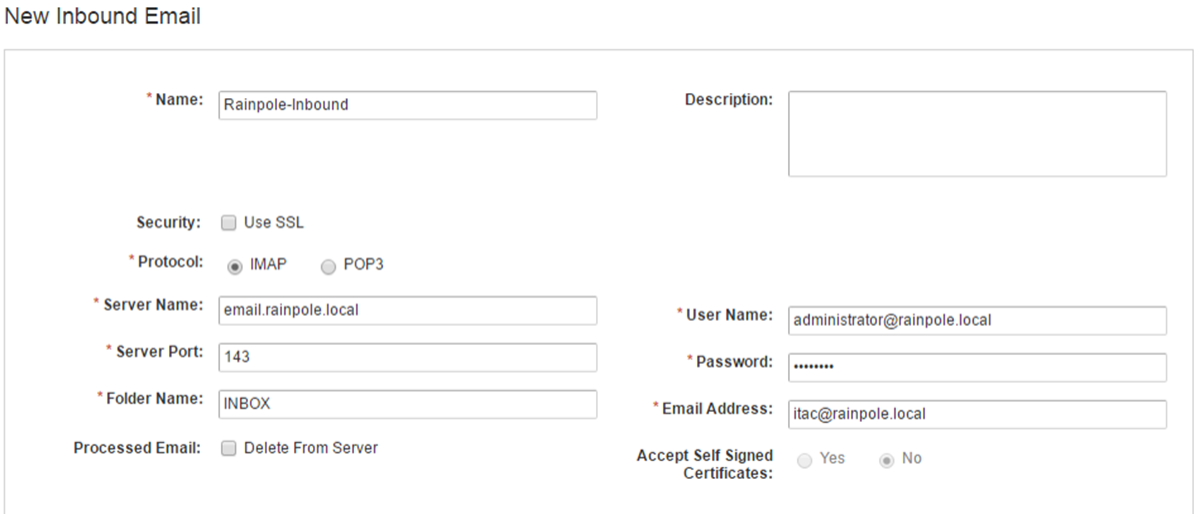
Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 Navigate to **Administration > Email Servers** and click **New**.

3 In the **New Email Server** dialog box, select **Email - Inbound** and click **OK**.

4 On the **New Inbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

Setting	Value
Name	Rainpole-Inbound
Security	Deselected
Protocol	IMAP
Server Name	email.rainpole.local
Server Port	143
Folder Name	INBOX
Processed Email	Deselected
User Name	administrator@rainpole.local
Password	*vra_administrator_password*
Email Address	itac@rainpole.local



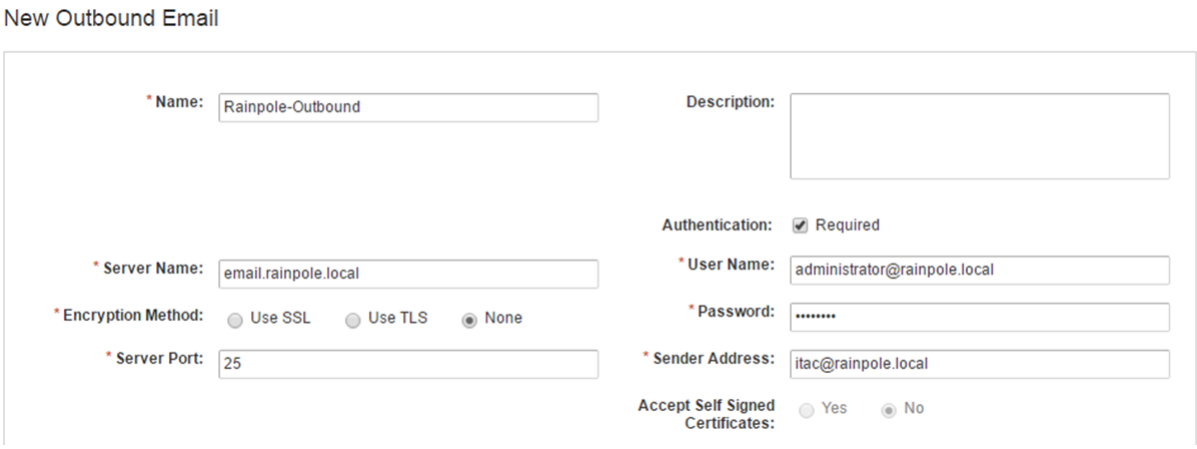
5 On the **Email Servers** page, click **New** to configure the outbound server settings.

6 In the **New Email Server** dialog box, select **Email - Outbound** and click **OK**.

7 On the **New Outbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

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

Setting	Value
Password	*vra_administrator_password*
Sender Address	itac@rainpole.local



8 Log out of vRealize Automation portal.

Embedded vRealize Orchestrator Configuration

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

vRealize Orchestrator consists of three layers:

- An orchestration platform that provides the common features required for an orchestration tool.
- A plug-in architecture to integrate control of subsystems.
- A library of workflows.

vRealize Orchestrator is an open platform that can be extended with new plug-ins and libraries, and can be integrated into larger architectures through a REST API.

Configure the Embedded vRealize Orchestrator Virtual Appliances

You configure two vRealize Automation virtual appliances to create a highly available embedded vRealize Orchestrator cluster.

Perform this procedure twice to configure two appliances using the values in the following table.

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

Procedure

1 Log in to the vRealize Automation appliance:

a SSH to vRealize Automation Appliance vra01svr01a.rainpole.local using the following credentials.

Setting	Value
User name	root
Password	*hostA_root_password*

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

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

4 Repeat the procedure to configure the vRealize Orchestrator virtual appliance for Host B vra01svr01b.rainpole.local.

Configure Authentication Provider for vRealize Orchestrator

Configure vRealize Orchestrator to utilize the vRealize Automation customer tenant (rainpole) for authentication.

Procedure

1 Log in to the vRealize Orchestrator Control Center.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local:8283/vco-controlcenter`**.

b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vsphere_admin_password*

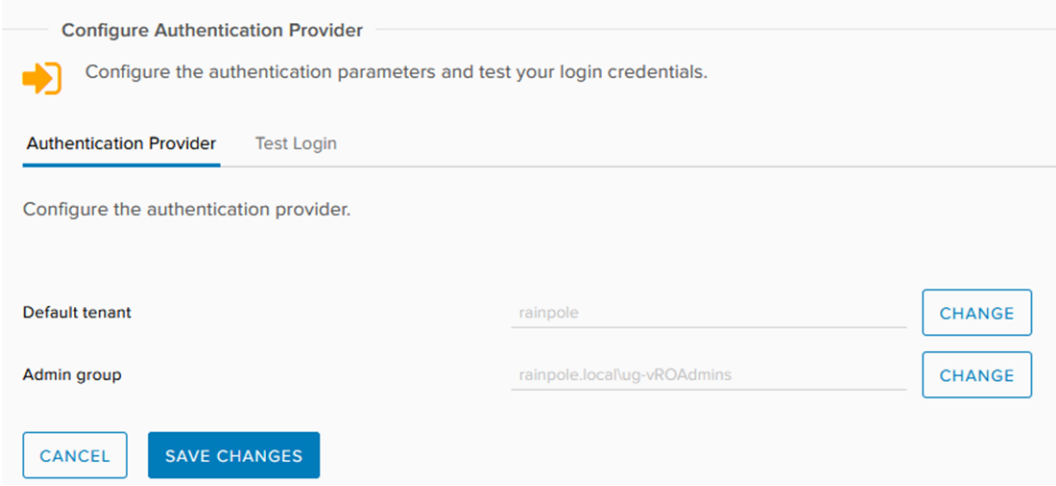
2 Configure vRealize Automation as a vRealize Orchestrator authentication provider.

a On the **Home** page, under **Manage**, click **Configure Authentication Provider**.

b In the **Default Tenant** text box, click the **Change** button, enter **rainpole**, and click **Apply**.

c In the **Admin group** text box, enter **ug-vRO** and click **Search**.

d From the drop-down menu, select **rainpole.local\ug-vROAdmins** and click **Save Changes**.



At this point, you will be automatically logged out of the control center.

3 Verify that you can log in as **svc-vra**.

a Open a Web browser and go to **https://vra01svr01.rainpole.local:8283/vco-controlcenter**.

b Log in using the following credentials.

Setting	Value
User name	svc-vra
Password	*svc-vra_password*

4 Log out of the control center.

5 SSH into both vRealize Automation appliances and run the following commands to restart the vRealize Orchestrator services.

a service vco-server restart

b service vco-configurator restart

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

Note The log in process may be delayed while the vRealize Orchestrator services restart.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local:8283/vco-controlcenter`**.

b Log in using the following credentials.

Setting	Value
User name	svc-vra
Password	*svc-vra_password*

Validate the Configuration

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

Procedure

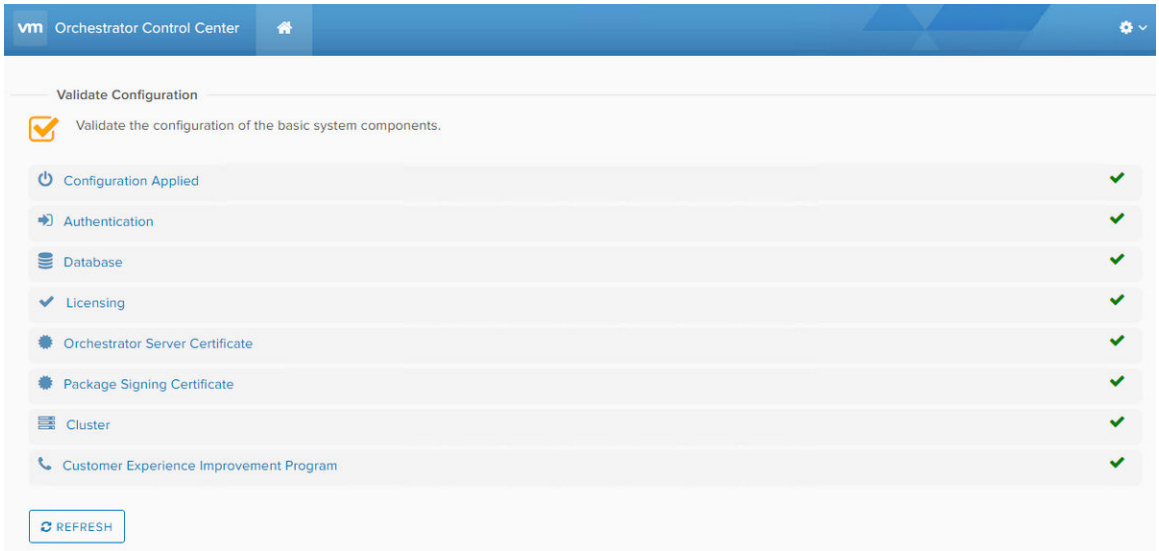
1 Log in to the Embedded vRealize Orchestrator Control Center.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local:8283/vco-controlcenter`**.

b Log in using the following credentials.

Setting	Value
User name	svc-vra
Password	*svc-vra_password*

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



Add Compute vCenter Server Instance to Embedded vRealize Orchestrator

To allow communication, you add vCenter Server instances to Embedded vRealize Orchestrator. You add each vCenter Server instance that contributes resources to vRealize Automation and uses vRealize Orchestrator workflows.

Procedure

1 Download and Install the vRealize Orchestrator Client.

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

   b Click **vRealize Orchestrator Client**.

   c On the **VMware vRealize Orchestrator Login** page, log in to the Embedded vRealize Orchestrator by using the following host name and credentials.

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

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

3 Right-click the **Add a vCenter Server instance** workflow and click **Start Workflow**.

   a On the **Set the vCenter Server Instance** page, configure the following settings and click **Next**.

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

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

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

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

   The vCenter Server instance that you added will be visible in the inventory.

Integrate vRealize Orchestrator with vRealize Automation

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

Configure Embedded vRealize Orchestrator Server

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

Procedure

1 Log in to the vRealize Automation portal.

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

   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 Click **Administration > vRO Configuration > Server Configuration**.

3 Select the **Use the default Orchestrator server** radio button and click **Test Connection**.

4 When the `Successfully connected to the Orchestrator server` message appears, click **OK** to complete the configuration.

Create a vRealize Orchestrator Endpoint

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

Procedure

1 Log in to the Rainpole Infrastructure Service Portal.

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

   b From the **Select your domain** drop-down menu select **Rainpole.local** and click **Next**

   c Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	rainpole.local

2 Create a new endpoint for vRealize Orchestrator.

a Select **Infrastructure > Endpoints > Endpoints**.

b Click **New > Orchestration > vRealize Orchestrator**, enter the following values, and click **OK**.

Setting	Value
Name	vra01svr01.rainpole.local
Address	https://vra01svr01.rainpole.local/vco
User name	svc-vra@rainpole.local
Password	*svc-vra_password*
Priority	1

3 Start the data collection for the newly created endpoint.

a Select the vRealize Orchestrator endpoint in the Endpoints list and click **Actions > Data Collection**.

b Click **Start** to begin the vRealize Orchestrator data collection process.

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

Add a vRealize Automation Host to vRealize Orchestrator

You add the vRealize Automation host to vRealize Orchestrator so you can call vRealize Automation Plugin workflows, you configure the vRealize Automation host in vRealize Orchestrator.

Procedure

1 Log in to the vRealize Orchestrator Client.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vco`**.

b Click **Start Orchestrator Client**.

c On the VMware vRealize Orchestrator login page, log in to vRealize Orchestrator using the following hostname and credentials.

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

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

3 Right-click the **Add a vRA host using component registry** workflow and click **Start Workflow**.

a On the **Common parameters** page, configure the following settings, and click **Submit**.

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

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

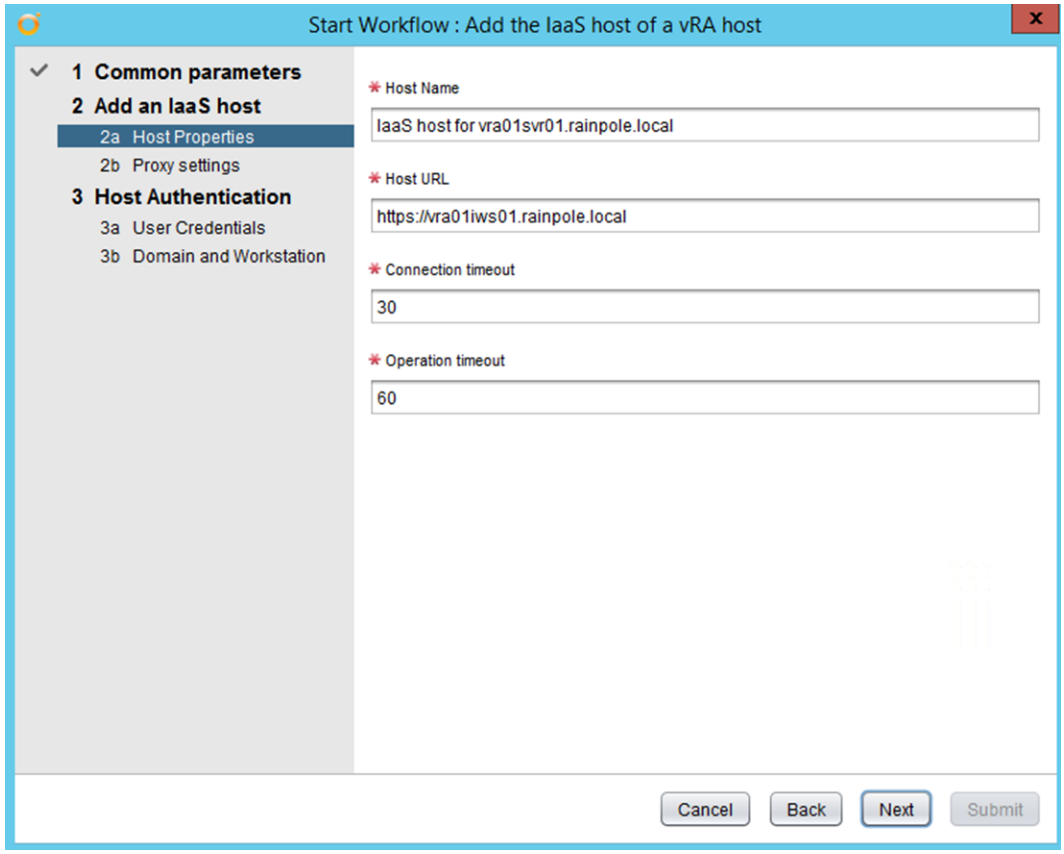
The vRealize Automation Server instance that you just added is visible in the inventory.

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

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

a On the **Common parameters** page, click the search icon labelled **Not set**. Select **vra01svr01.rainpole.local [https://vra01svr01.rainpole.local] [rainpole]** for **vCAC host** and click **Next**.

b On the **Add an IaaS host** page, keep the default settings for **Host Properties** and click **Next**.

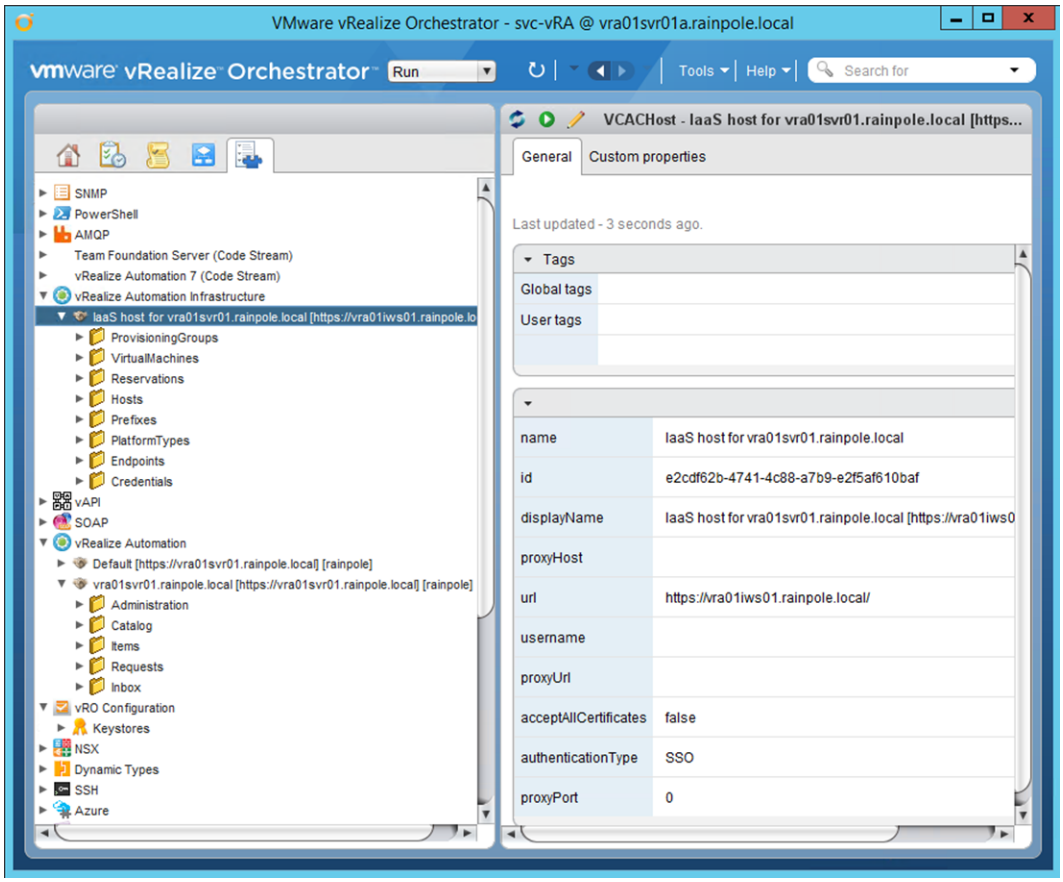


c On the **Add an IaaS host** page, keep the default settings for the **Proxy Settings** and click **Next**.

d On the **Host Authentication** page, select **SSO** for **Host's authentication type**, and click **Submit**.

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

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



vRealize Business Post-Deployment Tasks

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

vRealize Suite Lifecycle Manager can deploy vRealize Business for you but you have to perform some post-deployment tasks.

The following values are different in a vRealize Suite Lifecycle Manager deployment for sfo01vrbc01.sfo01.rainpole.local. No impact results.

VVD Recommended Value	2 GB RAM virtual appliance
Lifecycle Manager Deployed Value	8 GB RAM virtual appliance

Configure NTP for vRealize Business

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

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

Host	VAMI URL
Server	https://vrb01svr01.rainpole.local:5480
Data Collector	https://sfo01vrbc01.sfo01.rainpole.local:5480

Procedure

1 Log in to the vRealize Business Server appliance management console.

   a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Configure the appliance to use a time server.

   a Click the **Administration** tab and click **Time Settings**.

   b On the **Time Settings** page, enter the following settings and click **Save Settings**.

Setting	Value
Time Sync. Mode	Use Time Server
Time Server #1	ntp.sfo01.rainpole.local
Time Server #2	ntp.lax01.rainpole.local

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

Register the vRealize Business Data Collector with the Server

After you integrate vRealize Business with vRealize Automation, you connect the two vRealize Business appliances.

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

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

Procedure

1 Log in to the vRealize Automation Rainpole portal.

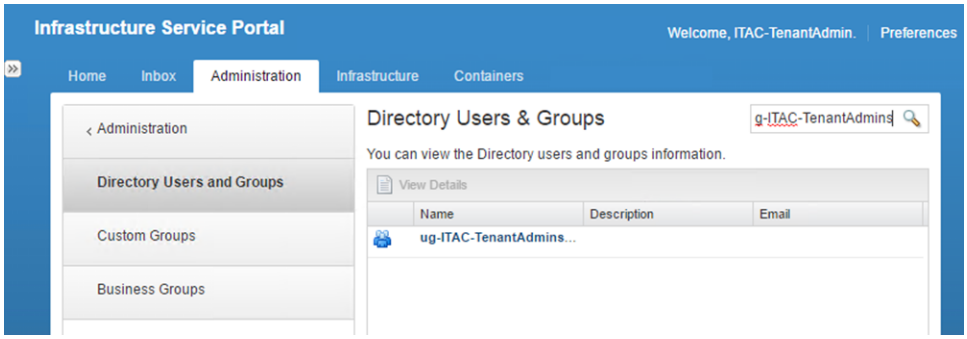
   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

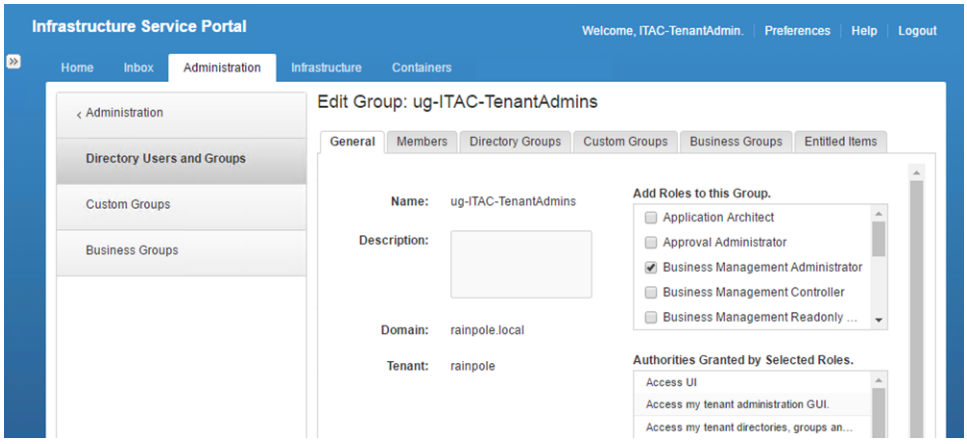
2 Navigate to **Administration > Users & Groups > Directory Users and Groups**.

3 In the search text box, enter **`ug-ITAC-TenantAdmins`**.



4 Click the **ug-ITAC-TenantAdmins** group to edit its settings.

5 On the **Edit Group** page, in the **Add Roles to this Group** list, select the **Business Management Administrator** role to add the role and click **Finish**.



6 Close your browser, and log in again by using the same credentials.

7 Assign a license to the vRealize Business solution.

a Click the **Business Management** tab.

b Under **License**, enter your serial number for vRealize Business and click **Save**.

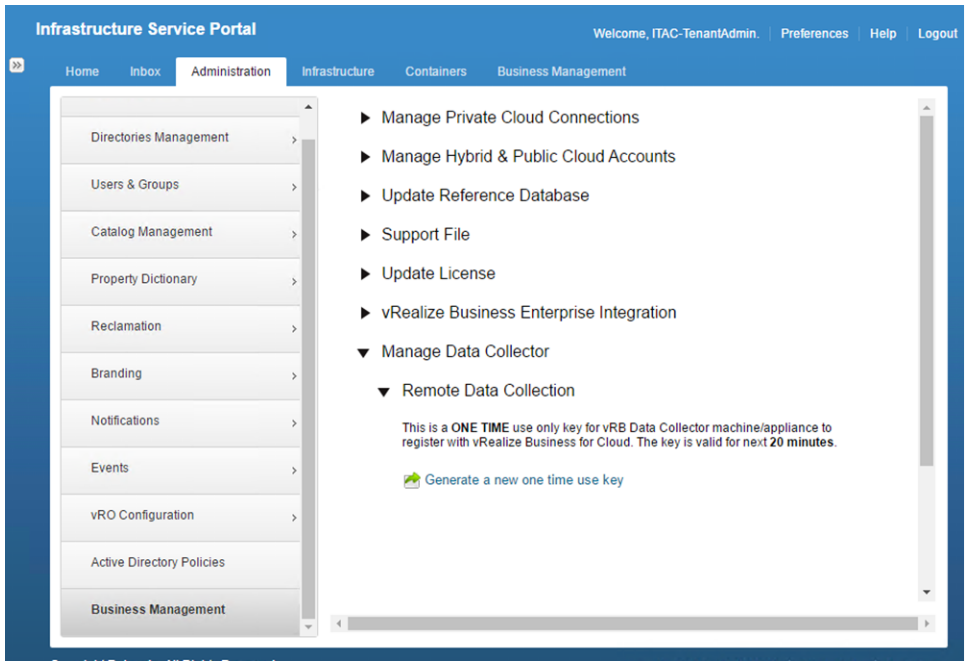
8 Generate a one-time use key for connecting the two vRealize Business appliances.

a Navigate to **Administration > Business Management**.

b Expand the **Manage Data Collector > Remote Data Collection** section.

c Click **Generate a new one time use key**.

d Save the one time use key as you need it at a later stage in the implementation sequence.



9 Log in to the vRealize Business Data Collector console.

a Open a Web browser and go to **`https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

10 Register the Data Collector with the vRealize Business Server.

a Expand the **Registration with the vRealize Business Server** section.

b Enter the following values and click **Register**.

Setting	Value
Enter the vRB Server Url	https://vrb01svr01.rainpole.local
Enter the One Time Key	*one_time_use_key*

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

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

The vRealize Business appliances are now connected.

Connect vRealize Business with the Compute vCenter Server

vRealize Business requires communication with the Compute vCenter Server to collect data from the entire cluster. You use the vRealize Business Data Collector console to connect these two components.

Procedure

1 Log in to the vRealize Business Data Collector console.

a Open a Web browser and go to **`https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

2 Click **Manage Private Cloud Connections**, select **vCenter Server**, and click **Add**.

3 In the **Add vCenter Server Connection** dialog box, enter the following settings and click **Save**.

Setting	Value
Name	sfo01w01vc01.sfo01.rainpole.local
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
Username	svc-vra@rainpole.local
Password	*svc_vra_password*

4 In the **SSL Certificate warning** dialog box, click **Install**.

5 In the **Success** dialog box, click **OK**.

Other vRealize Automation Suite Post-Deployment Tasks

After you deploy and configure the vRealize Automation suite of products, you create anti-affinity rules to enable HA protection for both services, enable health monitors to check the health status of individual servers, and remove the snapshots created during the vRealize Automation installation.

Create Anti-Affinity Rules for vRealize Automation and vRealize Orchestrator Virtual Machines

A VM-Host anti-affinity (or affinity) rule specifies a relationship between a group of virtual machines and a group of hosts. Anti-affinity rules force specified virtual machines to remain apart during failover actions, and are a requirement for high availability. We create rules to ensure that the vRealize Automation and vRealize Orchestrator instances remain on separate hosts.

Table 10-1. Anti-affinity Rules for the vRealize Automation Components

Name	Type	Members
anti-affinity-rule-vra-svr	Separate Virtual Machines	vra01svr01a.rainpole.local, vra01svr01b.rainpole.local
anti-affinity-rule-vra-iws	Separate Virtual Machines	vra01iws01a.rainpole.local, vra01iws01b.rainpole.local
anti-affinity-rule-vra-ims	Separate Virtual Machines	vra01ims01a.rainpole.local, vra01ims01b.rainpole.local
anti-affinity-rule-vra-dem	Separate Virtual Machines	vra01dem01a.rainpole.local, vra01dem01b.rainpole.local
anti-affinity-rule-vra-ias	Separate Virtual Machines	sfo01ias01a.sfo01.rainpole.local, sfo01ias01b.sfo01.rainpole.local

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** page, click **Hosts and Clusters**.

3 Under **sfo01m01vc01.sfo01.rainpole.local**, click **sfo01-m01dc**, and click **sfo01-m01-mgmt01**.

4 Click the **Configure** tab, and under **Configuration**, select **VM/Host Rules**.

5 Under **VM/Host Rules**, click **Add** to create a virtual machine anti-affinity rule.

6 In the **Create VM/Host Rule** dialog box, specify the first rule for the vRealize Automation virtual appliances.

   a In the **Name** text box, enter **`anti-affinity-rule-vra-svr`**.

   b Select the **Enable rule** check box.

c Select **Separate Virtual Machines** from the **Type** drop-down menu.

d Click **Add**, select the **vra01svr01a.rainpole.local** and **vra01svr01b.rainpole.local** virtual machines, click **OK**, and click **OK**.

7 Repeat the procedure to configure the remaining anti-affinity rules.

Create VM Groups to Define the Startup Order of vRealize Automation VMs

VM Groups allow you to define the startup order of virtual machines. The startup order you define ensures that vSphere HA powers on virtual machines in the correct order.

Procedure

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

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 In the **Navigator**, select **Host and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Create a VM Group for the vRealize Automation IaaS Database.

a Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

b On the **Configure** page, click **VM/Host Groups**.

c On the **VM/Host Groups** page, click the **Add** button.

d In the **Create VM/Host Group** dialog, enter **`vRealize Automation IaaS Database`** in the **Name** field, select **VM Group** from the **Type** drop down, and click the **Add** button.

e In the **Add VM/Host Group Member** dialog, select **vra01mssql01.rainpole.local** and click **OK**.

f Click **OK** to save the VM/Host Group.

4 Repeat step 3 to create the following VM/Host Groups.

VM/Host Group Name	VM/Host Group Member
vRealize Automation Virtual Appliances	vra01svr01a.rainpole.local vra01svr01b.rainpole.local
vRealize Automation IaaS Web Servers	vra01iws01a.rainpole.local vra01iws01b.rainpole.local
vRealize Automation IaaS Managers	vra01ims01a.rainpole.local vra01ims01b.rainpole.local

VM/Host Group Name	VM/Host Group Member
vRealize Automation IaaS DEM Workers	vra01dem01a.rainpole.local vra01dem01b.rainpole.local
vRealize Automation IaaS Proxy Agents	sfo01ias01a.sfo01.rainpole.local sfo01ias01b.sfo01.rainpole.local
vRealize Business Servers	vrb01svr01.rainpole.local
vRealize Business Remote Collectors	sfo01vrbc01.sfo01.rainpole.local

5 Create a rule to power on the vRealize Automation Database before the vRealize Automation Virtual Appliances.

a Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

b On the **Configure** page, click **VM/Host Rules**.

c On the **VM/Host Rules** page, click the **Add** button.

d In the **Create VM/Host Rule** dialog, enter **`SDDC Cloud Management Platform 01`** in the **Name** field, ensure that the **Enable Rule** check box is selected, select **Virtual Machines to Virtual Machines** from the **Type** drop down.

e Select **vRealize Automation IaaS Database** for the **First restart VMs in VM group** drop down list.

f Select **vRealize Automation Virtual Appliances** for the **Then restart VMs in VM group** drop down list

g Click **OK** to save the rule.

6 Repeat step 5 to create the following VM/Host Rules to ensure the correct restart order for your Cloud Management Platform.

VM/Host Rule Name	First restart VMs in VM group	Then restart VMs in VM group
SDDC Cloud Management Platform 02	vRealize Automation Virtual Appliances	vRealize Automation IaaS Web Servers
SDDC Cloud Management Platform 03	vRealize Automation IaaS Web Servers	vRealize Automation IaaS Managers
SDDC Cloud Management Platform 04	vRealize Automation IaaS Managers	vRealize Automation IaaS DEM Workers
SDDC Cloud Management Platform 05	vRealize Automation IaaS Managers	vRealize Automation IaaS Proxy Agents
SDDC Cloud Management Platform 06	vRealize Automation IaaS Managers	vRealize Business Servers
SDDC Cloud Management Platform 07	vRealize Business Servers	vRealize Business Remote Collectors

Enable Load Balancer Health Monitoring

You did not enable load balancer health monitoring for the sfo01m01lb01 load balancer to complete configuration of vRealize Automation first. You can now enable health monitoring for the load balancer.

Perform this procedure multiple times to configure the health monitor and to enable the second member for the server pools as described in the following table.

Pool Name	Monitor	Enable Pool Member
vra-svr-443	vra-svr-443-monitor	vra01svr01b
vra-iws-443	vra-iws-443-monitor	vra01iws01b
vra-ims-443	vra-ims-443-monitor	vra01ims01b
vra-svr-8444	vra-svr-443-monitor	-
vra-vro-8283	vra-vro-8283-monitor	vra01svr01b

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 In the **Navigator**, click **Networking & Security**, and select **NSX Edges**.

3 Select **172.16.11.65** from the **NSX Manager** drop-down menu, and double-click **sfo01m01lb01** to edit its settings.

4 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

5 From the pools table, select the **vra-svr-443** server pool, and click **Edit** icon.

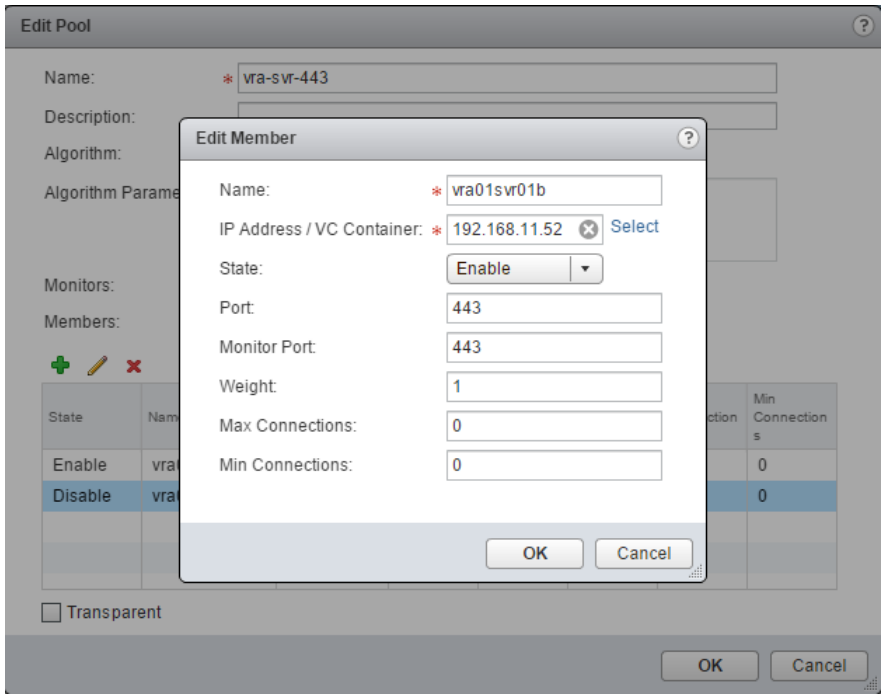
6 In the **Edit Pool** dialog box, configure the monitor, and enable the member that is not enabled.

   a From the **Monitors** drop-down menu, select **vra-svr-443-monitor**.

   b From the **Members** table, select **vra01svr01b** and click **Edit** icon.

c In the **Edit Member** dialog box, from the **State:** drop-down menu, select **Enable** and click **OK**.

d Click **OK** to close the **Edit Pool** dialog box.



7 Repeat the procedure to configure the health monitor and enable the second member for the remaining server pools.

8 Click **Show Pool Statistics** and make sure all the server pools **Status** show as **UP**.

Clean Up the vRealize Automation VM Snapshots

You made snapshots of each vRealize virtual machine during the vRealize Automation installation process. After you successfully complete the installation, you can delete these snapshots.

Repeat this procedure to remove all of the vRealize Automation virtual machine snapshots you created during the implementation. The virtual machine names and their respective folders are listed in the following table.

Virtual Machines	vCenter Folder
vra01svr01a.rainpole.local	sfo01-m01fd-vra
vra01svr01b.rainpole.local	sfo01-m01fd-vra
vra01mssql01.rainpole.local	sfo01-m01fd-vra
vra01iws01a.rainpole.local	sfo01-m01fd-vra
vra01iws01b.rainpole.local	sfo01-m01fd-vra
vra01ims01a.rainpole.local	sfo01-m01fd-vra
vra01ims01b.rainpole.local	sfo01-m01fd-vra
vra01dem01a.rainpole.local	sfo01-m01fd-vra

Virtual Machines	vCenter Folder
vra01dem01b.rainpole.local	sfo01-m01fd-vra
sfo01ias01a.sfo01.rainpole.local	sfo01-m01fd-vraias
sfo01ias01b.sfo01.rainpole.local	sfo01-m01fd-vraias

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** page, click **VMs and Templates**.

3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** folder.

4 Right-click the **vra01dem01a.rainpole.local** VM and select **Snapshots > Manage Snapshots**.

5 Select the **Prior to vRA IaaS Component Installation** snapshot and click **Delete** icon.

6 Repeat this procedure to remove all of the remaining vRealize Automation virtual machine snapshots.

Content Library Configuration

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

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

Configure a Content Library in the First Compute vCenter Server Instance

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

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

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** page, click **Content Libraries** and click the **Create a new content library** icon.

   The **New Content Library** wizard opens.

3 On the **Name** page, specify the following settings and click **Next**.

Setting	Value
Name	SFO01-ContentLib01
vCenter Server	sfo01w01vc01.sfo01.rainpole.local

4 On the **Configure content library** page, specify the following settings, and click **Next**.

Setting	Value
Local content library	Selected
Publish externally	Selected
Enable authentication	Selected
Password	*SFO01-ContentLib01_password*
Confirm password	*SFO01-ContentLib01_password*

5 On the **Add storage** page, click the **Select a datastore** radio button, select the **sfo01-w01-lib01** datastore to store the content library, and click **Next**.

6 On the **Ready to complete** page, click **Finish**.

Import the Virtual Machine Template OVF Files

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

You repeat this procedure three times to import the virtual machine templates listed in Table 10-2.

Table 10-2. VM Templates to Import

VM Template Name	Description
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

Prerequisites

Verify that you have prepared the OVF templates, as specified in the *Virtual Machine Template Specifications* section.

Procedure

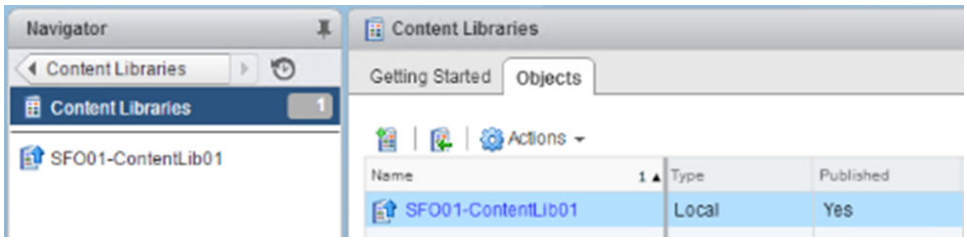
1 Log in to vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** page, click **Content Libraries** and click the **Objects** tab.



3 Right-click the content library **SFO01-ContentLib01** and select **Import Item**.

4 In the **Import Library Item** dialog box, specify the settings for the first template and click **OK**.

Setting	Value
Source file	redhat6-enterprise-64.ovf
Item name	redhat6-enterprise-64
Notes	Red Hat Enterprise Server 6 (64-bit)

5 Repeat the procedure to import the remaining virtual machine templates.

Post-Deployment Tasks for vRealize Operations Manager

After deployment with vRealize Suite Lifecycle Manager, you perform some additional tasks.

The following table summarizes the differences between a manual deployment following the VMware Validated Design instructions, and an automated deployment with vRealize Suite Lifecycle Manager. These parameter differences have no performance impact.

Analytics Node of vRealize Operations Manager	VMware Validate Design Recommended Value	Lifecycle Manager Deployed Value	Impact
vrops01svr01a	Increase hard disk 2 size from 250GB to 1TB	Hard disk 2 size remains 250GB and Add additional hard disk of size 1TB	None
vrops01svr01b	Increase hard disk 2 size from 250GB to 1TB	Hard disk 2 size remains 250GB and Add additional hard disk of size 1TB	None
vrops01svr01c	Increase hard disk 2 size from 250GB to 1TB	Hard disk 2 size remains 250GB and Add additional hard disk of size 1TB	None

Move Nodes of the Analytics Cluster and Remote Collector to VM Folders

Use the vSphere Web Client to move nodes of the Analytics cluster and virtual appliances of the remote collector group to VM folders for easier management.

vRealize Suite Lifecycle Manager deploys:

- Three analytics VMs: master, master replica, and data.
- Two remote collector virtual appliances: 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 Folder **sfo01-m01fd-vrops** and **sfo01-m01fd-vropsrc**.
5. Move the analytics VMs.
   a. Select the virtual machines **vrops01svr01a**, **vrops01svr01b** and **vrops01svr01c**.
   b. Right click and select Move to VM folder **sfo01-m01fd-vrops**.

6 Move the remote collector VMs.

   a Select the virtual machines **sfo01vropsc01a** and **sfo01vropsc01b**.

   b Right click and select Move to VM folder **sfo01-m01fd-vropsrc**.

Configure DRS Anti-Affinity Rules for vRealize Operations Manager

You have to protect the vRealize Operations Manager virtual machines from a host-level failure. Configure vSphere DRS to run both the VMs of the analytics cluster and the VMs 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 cluster 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 From the Home menu, select **Hosts and Clusters**.

3 Navigate to the sfo01m01vc01.sfo01.rainpole.local vCenter Server object, and under the sfo01-m01dc data center object select the **sfo01-m01-mgmt01** cluster.

4 Click the **Configure** tab.

5 Under the **Configuration** group of settings, select **VM/Host Rules**.

6 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

Setting	Value for the Analytics Nodes	Value for the Remote Collectors
Type	Separate Virtual Machines	Separate Virtual Machines
Members	■ vrops01svr01a ■ vrops01svr01b ■ vrops01svr01c	■ sfo01vropsc01a ■ sfo01vropsc01b

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	*vrops_admin_password*

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)** to indicate that no key is required and click **Next**.

5 (Optional) On the **Customer Experience Improvement Program** page, select **Join the VMware Customer Experience Impovement Program** to send technical information for product improvement, and click **Next**.

6 On the **Ready to Complete** page, click **Finish**.

Group Remote Collector Nodes

After you start vRealize Operations Manager and proceed with evalution mode, join the remote collectors in a group. Grouping results in adapter resiliency if a 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	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Management** and click **Collector Groups**.

4 Click **Add**.

5 In the **Add New Collector Group** dialog box, configure the following settings, and click **Save**.

Setting	Value
Name	sfo01-remote-collectors
Description	Remote collector group for sfo01
sfo01vropsc01a	Selected
sfo01vropsc01b	Selected

The sfo01-remote-collectors group appears on the **Collector Groups** page under the **Administration** view of the user interface.

Add an Active Directory Authentication Source

Connect vRealize Operations Manager to the Active Directory domain of the SDDC for central user management and access control.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Access** and click **Authentication Sources**.

4 On the **Authentication Sources** page, click **Add**.

5 In the **Add Source for User and Group Import** dialog box, enter the settings for the rainpole.local and sfo01.rainpole.local Active Directories, and click **OK**.

Active Directory Settings	rainpole.local Value	sfo01.rainpole.local Value
Source Display Name	RAINPOLE.LOCAL	SFO01.RAINPOLE.LOCAL
Source Type	Active Directory	Active Directory
Integration Mode	Basic	Basic
Domain/Subdomain	RAINPOLE.LOCAL	SFO01.RAINPOLE.LOCAL
Use SSL/TLS	Deselected	Deselected
User Name	svc-vrops@rainpole.local	svc-vrops@rainpole.local
Password	*svc-vrops_password*	*svc-vrops_password*
Settings under the **Details** 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 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 Directory domains are added to vRealize Operations Manager.

Configure User Access in vSphere for Integration with vRealize Operations Manager

Configure operations service accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the Management vCenter Server and Compute vCenter Server.

You associate the `svc-vrops-xxx` 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.

Procedure

1 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 and vSAN health in vRealize Operations Manager.

2 Configure User Privileges in vSphere for Integration with vRealize Operations Manager

Assign global permissions to the operations service accounts in order to access monitoring data from the Management vCenter Server and Compute vCenter Server with vRealize Operations Manager.

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 and vSAN health 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 **Administration > Roles**.

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	■ **Host.CIM.CIM interaction** ■ **Host.Configuration.Storage partition configuration** ■ **Profile-driven storage.Profile-driven storage view** ■ **Storage views.View**

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

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

Configure User Privileges in vSphere for Integration with vRealize Operations Manager

Assign global permissions to the operations service accounts in order to access monitoring data from the Management vCenter Server and Compute vCenter Server with vRealize Operations Manager.

- The svc-vrops-vsphere and svc-vrops-nsx users have read-only access on all objects in vCenter Server.
- The svc-vrops-mpsd user has rights that are required for access to vCenter Server storage devices in vRealize Operations.

- The svc-vrops-vsan user has rights that are required for access to vCenter Server storage devices in vRealize Operations.

In this procedure, you assign global permissions to these service accounts by assigning them the following roles.

User	Role
svc-vrops-vsphere@rainpole.local	Read-only
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** in the **Access Control** area.
4. Click **Add permission** on the **Manage** tab.
5. In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
6. In the **Select Users/Groups** dialog box, select the first user
   a. From the **Domain** drop-down menu, select **rainpole.local**
   b. In the filter box type `svc-vrops` and press **Enter**.
   c. From the list of users and groups, select **svc-vrops-vsphere**, click **Add**, and click **OK**.
7. Select a role.
   a. In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Read-only**.
   b. Ensure that **Propogate to children** is selected and click **OK**.

8 Repeat the steps to assign global permissions to the other service accounts.

User	Role
svc-vrops-vsphere@rainpole.local	Read-only
svc-vrops-nsx@rainpole.local	Read-only
svc-vrops-mpsd@rainpole.local	MPSD Metrics User
svc-vrops-vsan@rainpole.local	MPSD Metrics User

Add vCenter Adapter Instances to vRealize Operations Manager

After you deploy the analytics cluster and the remote collector nodes of vRealize Operations Manager and start vRealize Operations Manager, pair a vCenter Adapter instance with the Management vCenter Server and another adapter instance with the Compute vCenter Server.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 From the solution table on the **Solutions** page, select the **VMware vSphere** solution, and click the **Configure** icon at the top.

The **Manage Solution - VMware vSphere** dialog box appears.

5 Under **Instance Settings**, enter the settings for connection to vCenter Server.

a If you already have added another vCenter Adapter, click the **Add** icon on the left side to add an 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 instances, and click **OK**.

vCenter Server Credentials Attribute	Value
Credential name	■ vCenter Adapter Credentials - sfo01m01vc01 ■ vCenter Adapter Credentials - sfo01w01vc01
User Name	svc-vrops-vsphere@rainpole.local
Password	*svc-vrops-vsphere-password*

d Leave **Enable Actions** set to **Enable** so that vCenter Adapter can run actions on objects in the 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 Define the goals for vSphere monitoring.

a Click **Define Monitoring Goals**.

b In the **Define Monitoring Goals** dialog box, under **Enable vSphere Hardening Guide Alerts?**, select **Yes**, leave the default configuration for the other options, and click **Save**.

c Click **OK** in the **Success** dialog box.

7 Click **Save Settings**.

8 In the **Info** dialog box, click **OK**.

9 Repeat for the Compute vCenter Server.

10 In the **Manage Solution - VMware vSphere** dialog box, click **Close.**

11 On the **Solutions** page, select **VMware vSphere** from the solution table to view the collection state and collection status of the adapters.

   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 Adapters displays `Collecting`, and the **Collection Status** column displays `Data receiving`.

Connect vRealize Operations Manager to the NSX Managers

Install and configure the vRealize Operations Management Pack for NSX for vSphere. The management pack enables monitoring the NSX networking services deployed in each vSphere cluster and viewing 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 for better visibility into logical connectivity. Information about physical host and network device relationships in this view also helps in isolating problems in the logical or physical network.

Procedure

1 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 solution entry and adapters to vRealize Operations Manager.

2 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 Management NSX Manager and Compute NSX Manager in vRealize Operations Manager.

3 Add NSX-vSphere Adapter Instances to vRealize Operations Manager

   After you install the management pack, configure NSX-vSphere Adapters: one adapter for the management cluster and one adapter for the shared edge and compute cluster.

4 Add Network Devices Adapter to vRealize Operations Manager

   Configure a Network Devices Adapter to monitor the switches and routers in your environment and to view related alerts, metrics and object capacity.

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 solution entry and adapters 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 Management NSX Manager and Compute 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 for Management Cluster	Value for Compute Cluster
User name	admin	admin
Password	*mgmtnsx_admin_password*	*compnsx_admin_password*

2 Create the local service account svc-vrops-nsx on the NSX Manager instances.

a Run the following command to switch to Privileged mode of the 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 Give the svc-vrops-nsx user access privileges to NSX Manager from the vSphere Web Client.

```
user svc-vrops-nsx privilege web-interface
```

f Exit Configuration mode.

```
exit
```

g Commit these updates to the NSX Manager.

```
copy running-config startup-config
```

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 In a Chrome Web browser, start 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 for Management Cluster	Value for Compute Cluster
Type	Basic Auth	Basic Auth
User name	admin	admin
Password	*mgmtnsx_admin_password*	*compnsx_admin_password*

f On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Value	Application/xml

g In the **Body** tab, select **raw**, 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.

Add NSX-vSphere Adapter Instances to vRealize Operations Manager

After you install the management pack, configure NSX-vSphere Adapters: one adapter for the management cluster and one adapter for the shared edge and compute cluster.

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 connecting to the NSX Manager for the management cluster or to the NSX Manager for the shared edge and compute cluster.

   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**.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Credential name	NSX Adapter Credentials - sfo01m01nsx01	NSX Adapter Credentials - sfo01w01nsx01
NSX Manager User Name	svc-vrops-nsx	svc-vrops-nsx
NSX Manager Password	*svc-vrops-nsx_password*	*svc-vrops-nsx_password*
vCenter User Name	svc-vrops-nsx@rainpole.local	svc-vrops-nsx@rainpole.local
vCenter Password	*svc-vrops-nsx-password*	*svc-vrops-nsx-password*

d Click **Test Connection** to validate the connection to the NSX Manager instance.

The NSX Manager certificate appears.

e In the **Review and Accept Certificate** dialog box, verify the certificate information and click **Accept**.

f Click **OK** in the **Info** dialog.

g Expand the **Advanced Settings** section of settings.

h From the **Collectors/Groups** drop-down menu, select the **sfo01-remote-collectors** remote collector group.

i Click **Save Settings**.

j Click **OK** in the **Info** dialog box that appears.

k Repeat the steps to create an NSX-vSphere Adapter for the other NSX Manager.

7 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The NSX-vSphere Adapters appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapters 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 to view related alerts, metrics and object capacity.

The Network Devices Adapter collects data across all vCenter Server instances that you monitor by using vRealize Operations Manager. In a multi-region environment, you use a single adapter instance to access data for all regions.

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 **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). For SNMPv3 devices, provide SNMPv3 credentials in addition to the settings for SNMPv1 and SNMPv2.

   c Click **Test Connection** to verify the settings, and if the test is successful click the **OK** button.

d Expand the **Advanced Settings** section of settings, and verify that the **Collectors/Groups** option is set to **Default collector group**.

e Click **Save Settings**.

f Click **OK** in the **Info** dialog box that appears.

7 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The Network Devices Adapter appears on the **Solutions** page of the vRealize Operations Manager user interface. The adapter is collecting data about the network devices in all regions of the SDDC.
The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Connect vRealize Operations Manager to vRealize Automation

Install and configure the vRealize Operations Manager Management Pack for vRealize Automation to monitor the health and capacity risk of your cloud infrastructure in the context of the tenant's business groups.

Note You perform this task only for the IT Automating IT use case.

Procedure

1 Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager

To support collecting statistics about the tenant workloads, you assign the permissions that are required. You assign permissions to the svc-vrops-vra operations service account so that account can access monitoring data from vRealize Automation in vRealize Operations Manager. The svc-vrops-vra user has rights that are required for access to vRealize Automation in vRealize Operations Manager.

2 Add vRealize Automation Adapter to vRealize Operations Manager

To support collecting statistics about the tenant workloads, you configure a vRealize Automation adapter that collects monitoring data from vRealize Automation.

3 Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation

Configure read-only privileges for the svc-vra-vrops@rainpole.local service account on vRealize Operations Manager. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads.

4 Add vRealize Operations Manager as a Metrics Provider in vRealize Automation

Integrate vRealize Automation with vRealize Operations Manager to pull metrics for reclamation of tenant workloads.

Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager

To support collecting statistics about the tenant workloads, you assign the permissions that are required. You assign permissions to the svc-vrops-vra operations service account so that account can access monitoring data from vRealize Automation in vRealize Operations Manager. The svc-vrops-vra user has rights that are required for access to vRealize Automation in vRealize Operations Manager.

Procedure

1 Log in to the vRealize Automation portal.

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

   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*
Domain	vsphere.local

2 On the **Tenants** tab, click the **Rainpole** tenant.

3 Click the **Administrators** tab to assign tenant administrator and IaaS administrator roles to the svc-vrops-vra service account.

   a Enter **`svc-vrops-vra`** in the **Tenant administrators** search text box, click the **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** in the search result list to assign the role to the account.

   b Enter **`svc-vrops-vra`** in the **IaaS administrators** search text box, click the **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** in the search results list to assign the role to the account.

   c Click **Finish**.

4 Log out of the vRealize Automation Default tenant portal.

5 Log in to the vRealize Automation Rainpole portal.

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

   b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

6 Navigate to **Administration > Users & Groups > Directory Users and Groups** to assign the software architect role to the svc-vrops-vra service account.

   a Enter **`svc-vrops-vra`** in the search box, click the **Search** icon and click the **svc-vrops-vra (svc-vrops-vra@rainpole.local)** user.

   The setting of the svc-vrops-vra account appear.

   b On the **General** tab, select **Infrastructure Architect** and **Software Architect** under **Add roles to this User**, and click **Finish**.

7 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign the fabric administrator role to the svc-vrops-vra service account.

   a On the **Fabric Groups** page, click **SFO Fabric Group**.

   b On **Edit Fabric Group** page, enter **`svc-vrops-vra`** in the **Fabric administrators** search text box and click the **Search** icon.

   c Click **svc-vrops-vra@rainpole.local** in the search results list to assign the fabric administrator role to the account, and click **OK**.

Add vRealize Automation Adapter to vRealize Operations Manager

To support collecting statistics about the tenant workloads, you configure a vRealize Automation adapter that collects monitoring data from vRealize Automation.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 From the solution table on the **Solutions** page, select **VMware vRealize Automation** and click **Configure**.

   The Manage Solution - VMware vRealize Automation dialog box appears.

5 In the Manage Solution - VMware vRealize Automation dialog box, under **Instance Settings**, enter the settings for the connection to vRealize Automation.

a Enter the display name, description and FQDN of the vRealize Automation front-end portal, and turn data collection on for the Rainpole tenant.

Setting	Value
Display Name	vRealize Automation Adapter - vra01svr01 (Rainpole)
Description	vRealize Automation - Rainpole Tenant
vRealize Automation Appliance URL	https://vra01svr01.rainpole.local

b Click the **Add** icon next to the **Credential** text box, configure the credentials for connection to vRealize Automation, and click **OK**.

Credential	Value
Credential name	vRA Adapter Credentials - vra01svr01
SysAdmin Username	administrator@vsphere.local
SysAdmin Password	*vra_administrator_password*
SuperUser Username	svc-vrops-vra@rainpole.local
SuperUser Password	*svc_vrops_vra_password*

c Click **Test Connection** to validate the connection to vRealize Automation.

d In the **Review and Accept Certificate** dialog box, verify the vRealize Automation certificate information and click **Accept**.

e Click **OK** in the **Info** dialog box.

f Expand the **Advanced Settings** section, and verify the following configuration.

Advanced Setting	Value
Collectors/Groups	Default collector group
Tenants	rainpole
vRA Endpoint Monitoring	Enabled
Auto Discovery	true

g Click **Save Settings** and click **OK** in the **Info** box that appears.

6 In the **Manage Solution - VMware vRealize Automation** dialog box, click **Close**.

The **vRealize Automation Adapter** appears on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation

Configure read-only privileges for the svc-vra-vrops@rainpole.local service account on vRealize Operations Manager. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, expand **Access**, and click **Access Control**.

4 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.

5 On the **Import Users** page, import the svc-vra-vrops@rainpole.local service account.

   a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.

   b Select the **Basic** option for the search query.

   c In the **Search String** text box, enter **`svc-vra-vrops`** and click **Search**.

   The search results contain the svc-vra-vrops user account.

   d Select **svc-vra-vrops@rainpole.local** and click **Next**.

6 On the **Assign Groups and Permissions** page, to assign the `ReadOnly` role to the svc-vra-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings and click **Finish**.

Setting	Value
Select Role	ReadOnly
Assign this role to the user	Selected
Select Object	**vCenter Adapter > vCenter Adapter - sfo01w01vc01**

Add vRealize Operations Manager as a Metrics Provider in vRealize Automation

Integrate vRealize Automation with vRealize Operations Manager to pull metrics for reclamation of tenant workloads.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

   b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

2 Navigate to **Administration > Reclamation > Metrics Provider**.

3 On the **Metrics Provider** page, configure the vRealize Operations Manager settings.

   a Select **vRealize Operations Manager endpoint**.

   b Configure the following settings for vRealize Operations Manager.

Setting	Value
URL	https://vrops01svr01.rainpole.local/suite-api/
Username	svc-vra-vrops@rainpole.local
Password	*svc-vra-vrops_password*

   c Click **Test Connection**, verify that the test connection is successful, and click **Save**.

   d In the certificate warning message box, click **OK**.

   The `vSphere metrics provider updated successfully` message appears.

Connect vRealize Operations Manager with vRealize Business

Configure the vRealize Operations Manager Management Pack for vRealize Business to view your infrastructure performance, cost information, and also troubleshooting tips. You can connect vRealize Operations Manager to a single instance of vRealize Business for Cloud.

Note You perform this task only for the IT Automating IT use case.

Configure the vRealize Business Adapter in vRealize Operations

Configure a vRealize Business for Cloud adapter to collect monitoring data from vRealize Business for Cloud.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 From the solution table on the **Solutions** page, select the **VMware vRealize Business for Cloud** solution, and click **Configure**.

5 In the **Manage Solution - VMware vRealize Business for Cloud** dialog box, under **Instance Settings**, enter and verify the connection settings for vRealize Business for Cloud.

   a Enter the display name, description and FQDN of the vRealize Business for Cloud server.

Setting	Value for vRealize Business for Cloud Server
Display Name	vRealize Business Adapter - vrb01svr01
Description	vRealize Business for Cloud Server
vRealize Business for Cloud server	vrb01svr01.rainpole.local

   b Click **Test Connection** to validate the connection to the vRealize Business for Cloud Server instance.

   c Click **OK** in the **Info** dialog box.

   d Under **Settings**, expand **Advanced Settings**.

   e In the **Collectors/Groups** drop-down menu, make sure that the **Default collector group** is selected.

6 Click **Save Settings**.

7 Click **OK** in the **Info** dialog box.

8 In the **Manage Solution - VMware vRealize Business for Cloud** dialog box, click **Close**.

   The **vRBC Adapter** appears on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting`. The **Collection Status** is `Data receiving`.

Verify Connectivity to vRealize Business for Cloud

You can verify integration of VMware vRealize Business for Cloud with vRealize Operations Manager by removing a vCenter Server and then adding it again and observing the synchronization.

Procedure

1 Log in to the vRealize Business Data Collector console.

   a Open a Web browser and go to **`https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

2 Click **Manage Private Cloud Connections** and select **vCenter Server**.

3 Select the Compute vCenter Server `sfo01w01vc01.sfo01.rainpole.local` and click the **Delete** icon.

   The connection to Compute vCenter Server is removed.

4 Re-register the Compute vCenter Server with vRealize Business for Cloud.

   a Click **Add**.

   b In the **Add vCenter Server Connection** dialog box, enter the following settings and click **Save**.

Setting	Value
Name	sfo01w01vc01.sfo01.rainpole.local
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
Username	svc-vra@rainpole.local
Password	*svc_vra_password*

5 In the **SSL Certificate warning** dialog box, click **Install**.

6 In the **Success** dialog box, click **OK**.

Enable Storage Device Monitoring in vRealize Operations Manager

Install and configure the vRealize Operations Management Pack for Storage Devices to view the storage topology, and to monitor the capacity and problems on storage components.

Procedure

1 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.

2 Add Storage Devices Adapters in vRealize Operations Manager

   After you install the management pack, configure Storage Devices adapter to collect monitoring data about the storage devices in the SDDC.

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.

Add Storage Devices Adapters in vRealize Operations Manager

After you install the management pack, configure Storage Devices adapter to collect monitoring data about the storage devices 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 **Management Pack for Storage Devices** from the solution table and click **Configure**.

   The **Manage Solution - Management Pack for Storage Devices** dialog box appears.

5 Under **Instance Settings**, enter the settings for connection to the vCenter Server instances.

   a If you already have added another Storage Devices adapter, click the **Add** icon on the left side to add an adapter settings.

   b Enter the display name, description, and FQDN 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 instances, and click **OK.**

vCenter Server Credentials Attribute	Value
Credential name	■ Storage Devices Adapter Credentials - sfo01m01vc01 ■ Storage Devices Adapter Credentials - sfo01w01vc01
User Name	svc-vrops-mpsd@rainpole.local
Password	*svc-vrops-mpsd-password*

   d Click **Test Connection** to validate the connection to 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 adapters appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapters 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.

Procedure

1 Turn on the 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.

2 Add a vSAN Adapter in vRealize Operations Manager

You add a vSAN adapter to vRealize Operations Manager and configure the vSAN adapter to collect monitoring data about vSAN usage.

Turn on the 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 cluster's vSAN datastore.

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 Enable the vSAN Performance Service.

   a In the Navigator, expand the **sfo01-m01dc** data center object.

   b Click the **sfo01-m01-mgmt01** cluster object and click **Configure**.

   c Under **vSAN**, select **Health and Performance**.

   d Under settings, click **Edit** next to **Performance Service** , configure the following settings, and click **OK**.

Setting	Value
Turn ON vSAN performance service	Selected
Storage policy	vSAN Default Storage Policy

3 If you have a vSAN datastore configured in the shared edge and compute cluster sfo01-w01-comp01, repeat the procedure.

Add a vSAN Adapter in vRealize Operations Manager

You add a vSAN adapter to vRealize Operations Manager and configure the vSAN adapter to collect monitoring data about vSAN usage.

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 Management vCenter Server.

a If you already added another vSAN adapter, click the **Add** icon on the left side to add an adapter.

b Enter the settings for connection to the vCenter Server.

Setting	Value for the Management vCenter
Display Name	vSAN Adapter - sfo01m01vc01
Description	Management vCenter Server vSAN Adapter for sfo01
vCenter Server	sfo01m01vc01.sfo01.rainpole.local

c Click the **Add** icon next to the **Credential** text box, configure the credentials for connection to vCenter Server, and click **OK**.

Setting	Value for the Management vCenter
Credential name	vSAN Adapter Credentials - sfo01m01vc01
vCenter User Name	svc-vrops-vsan@rainpole.local
vCenter Password	*svc-vrops-vsan-password*

d Click **Test Connection** to validate the connection to 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** collector group.

i Click **Save Settings**.

j Click **OK** in the **Info** dialog box that appears.

6 If you have a vSAN datastore configured in the shared edge and compute cluster, repeat the steps for the Compute vCenter Server.

7 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 E-Mail Alerts for vRealize Operations Manager

You configure e-mail 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	*vrops_admin_password*

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	mailserver.rainpole.local
SMTP Port	25
Secure Connection Type	TLS
Sender Email Address	vrops@rainpole.com
Sender Name	vRealize Operations Admin

6 Click **Test** to verify the connection with the SMTP server and click **OK**.

7 Click **Save**.

Post-Deployment Tasks for vRealize Log Insight

After deploying vRealize Log Insight you perform some post-deployment tasks.

Procedure

1 Move Each Node in the vRealize Log Insight Cluster to a VM Folder

   Use the vSphere Web Client to move each vRealize Log Insight node to a single VM folder for easier 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 management cluster.

3 Configure the vRealize Log Insight Master Node

Configure the general properties of the vRealize Log Insight Master Node.

4 Join vRealize Log Insight to Active Directory

To use user roles 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

You can obtain the CA-signed vRealize Log Insight PEM certificate chain file that contains the own certificate, the signer certificate and the private key file by using the Cert-GenVVD tool. See the *Certificate Replacement* guide.

6 Connect vRealize Log Insight to the vSphere Environment

Set up your environment to collect 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. Launch in Context supports troubleshooting vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

8 Connect vRealize Log Insight to the NSX Instances

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

9 Connect vRealize Log Insight to vRealize Automation

Connect the vRealize Log to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight UI.

10 Install the Linux Content Pack and Configure the Virtual Appliance Agent Group for vRealize Log Insight

Install the content pack for VMware Linux to add the dashboards for viewing log information about the management virtual appliances in vRealize Log Insight.

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 Each Node in the vRealize Log Insight Cluster to a VM Folder

Use the vSphere Web Client to move each vRealize Log Insight node to a single VM folder for easier 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

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 Find the virtual machines **sfo01vrli01a**, **sfo01vrli01b** and **sfo01vrli01c** and move them to the VM folder **sfo01-m01fd-vrli**.

   If the VM folder doesn't exist, create the folder first.

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 management 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.

3 Under the **sfo01-m01dc** data center object select the **sfo01-m01-mgmt01** cluster.

4 On the **Configure** tab, select **VM/Host Rules**.

5 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

Rule Attribute	Value
Type	Separate Virtual Machines
Members	■ sfo01vrli01a ■ sfo01vrli01b ■ sfo01vrli01c

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	*vrli_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**.

Join vRealize Log Insight to Active Directory

To use user roles 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	*vrli_admin_password*

2 On the **Authentication** page, select the check box to enable the support for Active Directory and configure the Active Directory settings.

a Configure the Active Directory connection settings.

Setting	Value
Enable Active Directory support	Selected
Default Domain	rainpole.local
Domain Controller(s)	dc01rpl.rainpole.local
User Name	svc-vrli
Password	*svc_vrli_password*
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

You can obtain the CA-signed vRealize Log Insight PEM certificate chain file that contains the own certificate, the signer certificate and the private key file by using the Cert-GenVVD tool. See the *Certificate Replacement* guide.

The *Certificate Replacement* guide starts at http://pubs.vmware.com/vmware-validated-design-41/topic/com.vmware.vvd.sddc-certificate.doc/GUID-FA99EBD8-CE1C-405A-96C8-7B5EA9F79D23.html.

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 **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 icon 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 into 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

Set up your environment to collect log information about the ESXi and vCenter Server instances in the SDDC.

Procedure

1 Configure vSphere User Privileges for Integration with vRealize Log Insight

The svc-vrli service account is dedicated to collecting log information from vCenter Server and ESXi. Assign global permissions to the svc-vrli service account to collect log information from the vCenter Server instances and ESXi hosts with vRealize Log Insight.

2 Connect vRealize Log Insight to vSphere

After you configure the svc-vrli Active Directory user with the vSphere privileges that are required for retrieving log information, connect vRealize Log Insight to vSphere. You perform the task from the vRealize Log Insight user interface.

3 Configure vCenter Server to Forward Log Events to vRealize Log Insight

You can configure each vCenter Server and Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

4 Update the Host Profiles for the Management and Shared Edge and Compute Clusters with Syslog Settings

To have a consistent logging configuration across all ESXi hosts in the clusters, update the host profile in each cluster to accommodate the syslog settings for connection to vRealize Log Insight.

Configure vSphere User Privileges for Integration with vRealize Log Insight

The svc-vrli service account is dedicated to collecting log information from vCenter Server and ESXi. Assign global permissions to the svc-vrli service account to collect log information from the vCenter Server instances and ESXi hosts with 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, select **Administration**.

3 Under **Access Control**, click **Roles**.

4 Create a custom role for vRealize Log Insight.

   a Select **Read-only** and click the **Clone** 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.

   b 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	■ **Host.Configuration.Advanced settings** ■ **Host.Configuration.Change settings** ■ **Host.Configuration.Network configuration** ■ **Host.Configuration.Security profile and firewall**

   These 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@rainpole.local service account.

   a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Access Control > Global Permissions**.

   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** 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@rainpole.local user propagate to all vCenter Server instances.

Connect vRealize Log Insight to vSphere

After you configure the svc-vrli Active Directory user with the vSphere privileges that are required for retrieving log information, connect vRealize Log Insight to vSphere. You perform the task from 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	*vrli_admin_password*

2 Click the configuration icon and select **Administration**.

3 Under **Integration**, click **vSphere**.

4 In the **vCenter Servers** pane, enter the connection settings for the Management vCenter Server and for the Compute vCenter Server.

   a Enter the host name, user credentials, and collection options for the vCenter Server instances, and click **Test Connection**.

vCenter Server Option	Value
Hostname	■ sfo01m01vc01.sfo01.rainpole.local for Management vCenter Server ■ sfo01w01vc01.sfo01.rainpole.local for Compute vCenter Server
Username	svc-vrli@rainpole.local
Password	*svc-vrli_user_password*
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** and repeat the steps to add the settings for the second vCenter Server instance.

6 Click **Save**.

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

You can configure each vCenter Server and Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster. 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	*mgmtvc_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 vCenter Server Appliance and Platform Services Controller instances.

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	*vrli_admin_password*

c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** under **Content Pack Dashboards**.

d Verify that the vCenter Server nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

Update the Host Profiles for the Management and Shared Edge and Compute Clusters with Syslog Settings

To have a consistent logging configuration across all ESXi hosts in the clusters, update the host profile in each cluster to accommodate the syslog settings for connection to vRealize Log Insight.

Setting	Management Cluster	Shared Edge and Computer Cluster
vCenter Server URL	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client/	https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client/
Host Profiles	sfo01-m01hp-mgmt01	sfo01-w01hp-comp01
First ESXi host	sfo01m01esx01.sfo01.rainpole.local	sfo01w01esx01.sfo01.rainpole.local

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Update the host profile to the management cluster.

   a From the vSphere Web Client **Home** menu, select **Home**.

   b In the Navigator, click **Policies and Profiles** and click **Host Profiles**.

   c Right-click **sfo01-m01hp-mgmt01** and select **Copy Settings** from **Host**.

   d Select **sfo01m01esx01.sfo01.rainpole.local** and click **OK**.

3 Verify that the syslog host settings have been updated.

   a On the **Host Profiles** page in the **Navigator**, click **sfo01-m01hp-mgmt01** .

   b On the **Configure** tab, click **Settings**.

   c In **Filter** search box, type in **Syslog.global.logHost**.

   d Select **Syslog.global.logHost** from the list and verify that value of the option is `udp://sfo01vrli01.sfo01.rainpole.local:514`

4 Verify compliance for the hosts in the consolidated cluster.

   a From the vSphere Web Client **Home** menu, select **Hosts and Clusters**.

   b Click the **sfo01-m01-mgmt01** cluster, click the **Monitor** tab, and click **Profile Compliance**.

   c Click the **Check Compliance Now button**.

   d Verify all hosts are compliant with the attached profile.

5 Repeat the procedure with a host in the Shared Edge and Compute cluster.

Connect vRealize Log Insight to vRealize Operations Manager

Connect vRealize Log Insight to vRealize Operations Manager so that you can use the Launch in Context functionality between the two applications. Launch in Context supports troubleshooting vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

Note You do not perform this task for the Micro-Segmentation use case.

Procedure

1 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 on vRealize Operations Manager.

2 Enable the vRealize Log Insight Integration with vRealize Operations Manager

Connect vRealize Log Insight with vRealize Operations Manager to enable launching vRealize Log Insight from within vRealize Operations Manager and sending alerts to vRealize Operations Manager.

3 Connect vRealize Operations Manager to vRealize Log Insight

Configure a vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager. You can access unstructured log data about any object in your environment by using the Launch in Context functionality in vRealize Operations Manager.

4 Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight

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.

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 on 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 navigator bar, click **Administration.**

3 In 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, assign the `Administrator` role to the svc-vrli-vrops@rainpole.local service account:

   a Click the **Objects** tab.

   b 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 with vRealize Operations Manager to enable launching vRealize Log Insight from within vRealize Operations Manager and sending 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 validation the connection and click **Save**.

6 Click **OK** to close the dialog.

Connect vRealize Operations Manager to vRealize Log Insight

Configure a vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager. You can access unstructured log data about any object in your environment by using the Launch in Context functionality 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 vRelalize 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 for vRealize Log Insight
Display Name	Log Insight Adapter - sfo01vrli01
Description	vRealize Log Insight for sfo01
Log Insight server	sfo01vrli01.sfo01.rainpole.local

b Click **Test Connection** to validate the connection to vRealize Log Insight.

c Click **OK** in the **Info** box.

d Expand the **Advanced Settings** pane and select **sfo01-remote-collectors** from the **Collectors/Groups** drop-down menu.

e Click **Save Settings**.

f Click **OK** in the **Info** box.

6 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

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 SSH on each node of vRealize Operations Manager in vCenter Sverver

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 appliance 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
Hostname	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local
User name	root
Password	*vrops_root_password*

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 and uncomment the following parameters.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=sfo01vrli01.sfo01.rainpole.local
; Set protocol to use:
; cfapi – Log Insight REST API
; syslog – Syslog protocol
; If omitted the default value is cfapi
;
proto=cfapi
; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000
;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
ssl=no
; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30
```

d After the `[server]` section, add the following block on each vRealize Operations Manager node:

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"<vROPS Node Role Here>",
"vmw_vr_ops_nodename":"<Your vROPS Node Name Here>",
"vmw_vr_ops_hostname":"<Your vROPS Hostname Here>"}
```

Modify the following parameters for each node.

Parameter	Description	Location in liagent.ini
vmw_vr_ops_clusterrole	Role of the vRealize Operations Manager node	Set to **Master**, **Replica**, **Data** or **Remote Collector** according to the role of the node.
vmw_vr_ops_nodename	IP address or FQDN of the vRealize Operations Manager node	Replace each `<Your VROPS Node Name Here>` with the following names: ■ vrops01svr01a ■ vrops01svr01b ■ vrops01svr01c ■ sfo01vropsc01a ■ sfo01vropsc01b
vmw_vr_ops_hostname	Name of the vRealize Operations Manager node that is set during node initial configuration	Replace each `<Your VROPS Hostname Here>` with the following names: ■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local

Use the following as an example, on the master replica node you change the `[common|filelog]` section to add context to the logs that are sent to the vRealize Log Insight cluster:

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"Replica", "vmw_vr_ops_nodename":"vrops01svr01b",
"vmw_vr_ops_hostname":"vrops01svr01b.rainpole.local"}
```

e Press Esc and enter **`:wq!`** to save the file.

f Restart the Log Insight agent on node by running the following console command.

```
/etc/init.d/liagentd restart
```

g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

h 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 from 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 **`vRops6 – 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	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local

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 vRealize Log Insight Home page.

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.

Procedure

1 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.

2 Configure NSX Managers to Forward Log Events to vRealize Log Insight

Configure the NSX Manager for the management cluster and the NSX Manager for the compute and edge clusters to send audit logs and system events to vRealize Log Insight.

3 Configure the NSX Controllers to Forward Events to vRealize Log Insight

Configure the NSX Controller instances for the management cluster and shared compute and edge cluster 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 for Google Chrome.

4 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.

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	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration 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 Managers to Forward Log Events to vRealize Log Insight

Configure the NSX Manager for the management cluster and the NSX Manager for the compute and edge clusters to send audit logs and system events to vRealize Log Insight.

Procedure

1 On the Windows host that has access to the data center, log in to the NSX Manager Web interface.

a Open a Web browser and go to following URL.

NSX Manager	URL
NSX Manager for the management cluster	https://sfo01m01nsx01.sfo01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://sfo01w01nsx01.sfo01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

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 for the management cluster and shared compute and edge cluster 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 for Google Chrome.

Procedure

1 Log in to the Windows host that has access to your data center.

2 In a Chrome browser, start the Postman application and log in.

3 Specify the request headers for requests to the NSX Manager.

a On the **Authentication** tab, configure the following authorization settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	*sfo01m01nsx01_admin_password* *sfo01w01nsx01_admin_password*

The Authorization:Basic XXX header appears in the **Headers** pane.

b On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Value	application/xml

The Content-Type:application/xml header appears in the **Headers** pane.

4 Contact the 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	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller
NSX Manager for the shared edge and compute cluster	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller

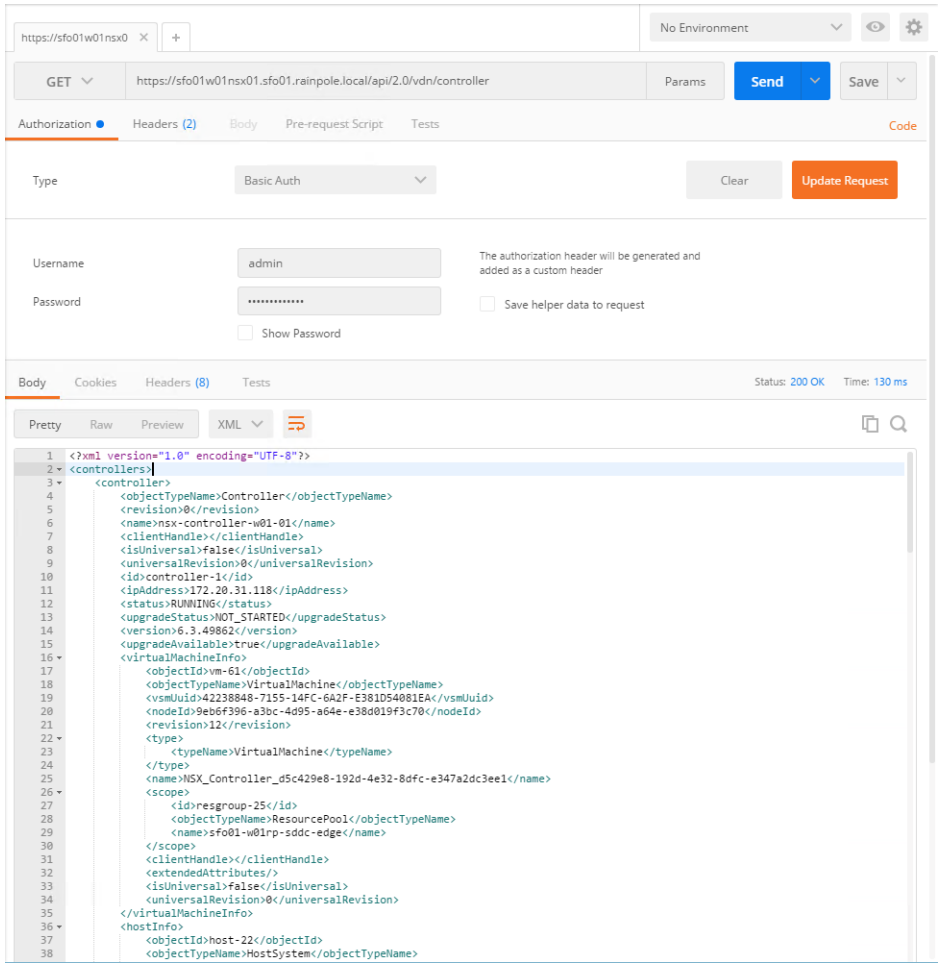
The Postman application sends a query to the NSX Manager about the installed NSX controllers.

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 image below.



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.

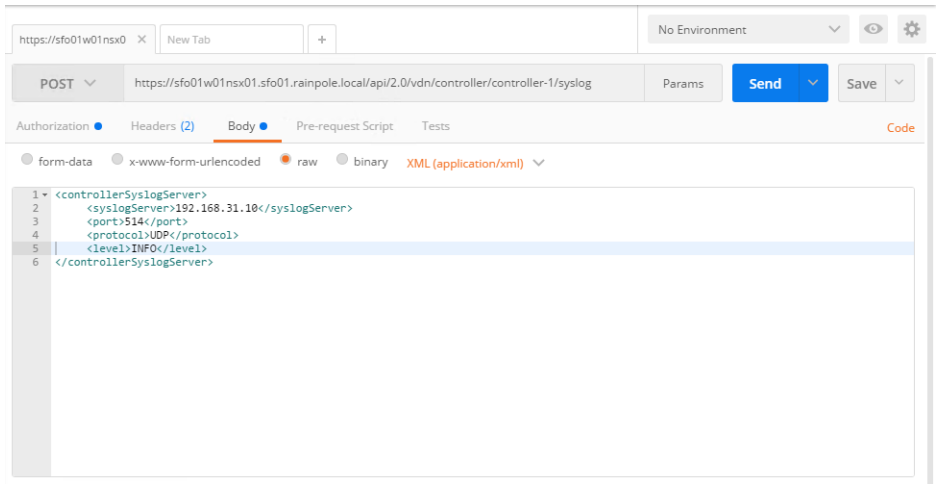
a In the request pane at the top, select **POST** from the drop-down menu that contains the HTTP request methods, and in the **URL** text box, enter the following URL. Replace *controller-ID* with the controller IDs you have written down.

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/**controller-1**/syslog
	NSX Controller 2	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
	NSX Controller 3	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-3**/syslog
NSX Manager for the shared edge and compute cluster	NSX Controller 1	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-1**/syslog
	NSX Controller 2	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
	NSX Controller 3	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-3**/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.

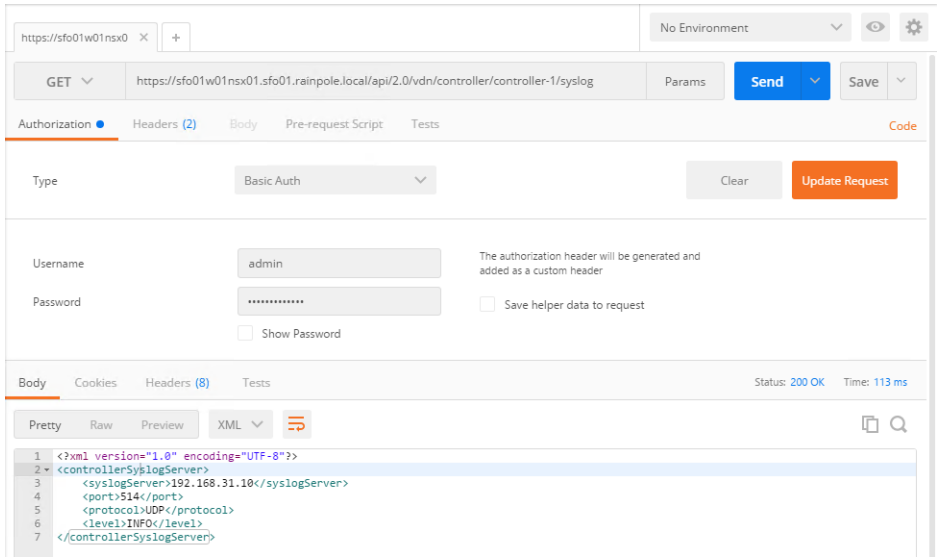
a In the **Request** pane, from the **Method** drop-down menu, select **GET**, in the **URL** text box, enter the controller-specific syslog URL from the previous step, and click the**SEND** button.

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, select **Networking & Security**.

3 From the **Networking & Security** menu on the left, 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
Management NSX Manager	172.16.11.65
Compute NSX Manager	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 of Management and Compute NSX Managers instances.

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 of Management and Compute NSX Manager instances.

The vRealize Log Insight user interface starts showing log data in the **NSX-vSphere-Overview** dashboard available under the VMware - NSX-vSphere group of content pack dashboards.

Connect vRealize Log Insight to vRealize Automation

Connect the vRealize Log to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight UI.

Note You perform this task only for the IT Automating IT use case.

Procedure

1 Install the vRealize Log Insight Content Packs for vRealize Automation and vRealize Orchestrator

Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information about the Cloud Management Platform in vRealize Log Insight.

2 Install and Configure vRealize Log Insight Windows Agents

Install the vRealize Log Insight agent on the Windows virtual machines for the Distributed Execution Manager, IaaS Manager Service, IaaS Web Server, IaaS SQL Server and the vSphere proxy agents. Configure Log Insight Windows Agents centrally from the vRealize Log Insight Web interface.

3 Configure vRealize Log Insight Linux Agents in the vRealize Automation Virtual Appliances

vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on each virtual appliance.

4 Configure the vRealize Log Insight Linux Agents on vRealize Business

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

5 Configure Embedded vRealize Orchestrator to Forward Log Events to vRealize Log Insight

You enable the vRealize Log Insight agent and configure the agent group for the embedded vRealize Orchestrator to start collecting log data in the vRealize Orchestrator dashboards.

Install the vRealize Log Insight Content Packs for vRealize Automation and vRealize Orchestrator

Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information about the Cloud Management Platform in vRealize Log Insight.

You install the following content packs:

- VMware - vRA 7
- VMware - Orchestrator 7.0.1+
- Microsoft - SQL Server

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Content Packs**.

3 Under Content Pack Marketplace, select **Marketplace**.

4 In the list of content packs, locate the **VMware - vRA 7** content pack and click its icon.

5 In the Install Content Pack dialog box, click **Install**.

6 Repeat the procedure to install the **VMware - Orchestrator** and **Microsoft - SQL Server** content packs.

After the installation is complete, the VMware - vRA, VMware - Orchestrator 7.0.1+ and Microsoft - SQL Server content packs appear in the **Installed Content Packs** list on the left.

Install and Configure vRealize Log Insight Windows Agents

Install the vRealize Log Insight agent on the Windows virtual machines for the Distributed Execution Manager, IaaS Manager Service, IaaS Web Server, IaaS SQL Server and the vSphere proxy agents. Configure Log Insight Windows Agents centrally from the vRealize Log Insight Web interface.

Procedure

1 Install the Log Insight Windows Agents on all the vRealize Automation Windows VMs.

a Open a Remote Desktop Protocol (RDP) connection to each of the following vRealize Automation virtual machines.

vRealize Automation Component	Host Name or VM Name
IaaS Web Server	vra01iws01a.rainpole.local
IaaS Web Server	vra01iws01b.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
IaaS DEM Worker	vra01dem01a.rainpole.local
IaaS DEM Worker	vra01dem01b.rainpole.local
vSphere Proxy Agent	sfo01ias01a.sfo01.rainpole.local
vSphere Proxy Agent	sfo01ias01b.sfo01.rainpole.local
Microsoft SQL Server	vra01mssql01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	Rainpole\svc-vra
Password	*svc-vra-user-password*

c Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`** .

d Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

e Click the configuration drop-down menu icon and select **Administration**.

f Under **Management**, click **Agents**.

g On the **Agents** page, click the **Download Log Insight Agent Version** link.

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

i Double-click the `.msi` file to run the installer.

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

k With the Log Insight host name **`sfo01vrli01.sfo01.rainpole.local`** shown in the **Host** text box, click **Install**.

l When the installation is complete, click **Finish**.

2 Configure the Log Insight Windows Agent Group for the vRealize Automation IaaS components from 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 at the top, select **vRealize Automation 7 - Windows** from the **Available Templates** section.

f Click **Copy Template.**

g In the **Copy Agent Group** dialog box, enter **`vRA7 – Windows Agent Group`** in the name text box and click **Copy.**

h In the agent filter fields, use the following selections.

Use ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	vra01iws01a.rainpole.local vra01iws01b.rainpole.local vra01ims01a.rainpole.local vra01ims01b.rainpole.local vra01dem01a.rainpole.local vra01dem01b.rainpole.local sfo01ias01a.sfo01.rainpole.local sfo01ias01b.sfo01.rainpole.local

i Click **Refresh** and verify that all the agents that are listed in the filter appear in the Agents list.

j Click **Save New Group** at the bottom of the page.

3 In the vRealize Log Insight Web user interface, configure the Log Insight Windows Agent Group for the Microsoft SQL Server component that is used by vRealize Automation.

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 at the top, select **Microsoft - SQL Server** from the **Available Templates** section.

f Click **Copy Template**.

g In the **Copy Agent Group** dialog box, enter **`vRA7 – Microsoft SQL Server Agent Group`** in the name text box and click **Copy.**

h In the agent filter fields, use the following selections.

Use ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	vra01mssql01.rainpole.local

i Under **Agent Configuration**, click **Edit**

j Locate `directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log` and change it to **`directory=C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Log`**

> **Note** In this VMware Validated Design, Microsoft SQL Server 2012 R2 has been installed in the default location on the Windows Server virtual machine.

k Click **Refresh** and verify that all the agents listed in the filter appear in the Agents list.

l Click **Save New Group** at the bottom of the page.

All VMware vRA 7 dashboards become available on the vRealize Log Insight Home page.

Configure vRealize Log Insight Linux Agents in the vRealize Automation Virtual Appliances

vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on each virtual appliance.

Procedure

1 Configure logging in the management interface of the vRealize Automation virtual appliance.

a Open a Web browser and log in to the following URL.

Setting	Value
URL	https://vra01svr01a.rainpole.local:5480
Username	root
Password	*vra_applianceA_root_password*

b On the **VRA Settings** tab, click the **Logs** tab.

c Scroll down to the **Log Insight Agent Configuration** section.

d Enter the following values and click **Save Settings**

Setting	Value
Host	sfo01vrli01.sfo01.rainpole.local
Port	9000
Protocol	CFAPI
SSL Enabled	Unchecked
Reconnect	30
Max Buffer Size	2000

e Verify these settings have been replicated to vRealize Automation appliance vra01svr01b.rainpole.local.

2 Configure the Linux Agent Group on the Log Insight server.

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 on the top, select **vRealize Automation 7 - Linux** from the **Available Templates** section.

f Click **Copy Template** at the bottom of the page.

g In the **Copy Agent Group** dialog box, enter **`vRA7 – Linux Agent Group`** in the name field and click **Copy**.

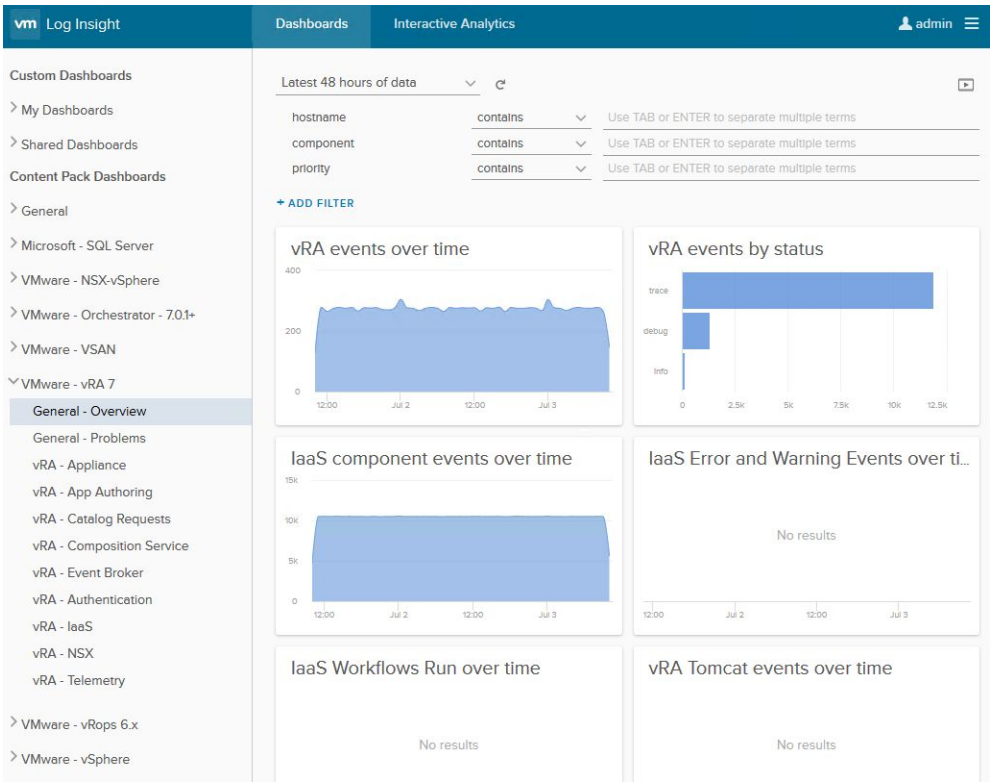
h In the agent filter fields, enter the following values pressing Enter after each host name.

Filter	Operator	Values
Hostname	matches	vra01svr01a.rainpole.local

i Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.

j Click **Save New Group** at the bottom of the page.

k Click the **Dashboard** tab and select the **VMware - vRA 7** dashboard from the navigator menu on the left.



All VMware vRA 7 dashboards become available on the vRealize Log Insight Home page.

Configure the vRealize Log Insight Linux Agents on vRealize Business

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

Procedure

1 Enable Secure Shell (SSH) on the vRealize Business appliances.

a Open a Web browser and go to the following URL.

vRealize Business Node	Virtual Appliance Management Interface URL
vRealize Business Server Appliance	https://vrb01svr01.rainpole.local:5480
vRealzie Business Data Collector	https://sfo01vrbc01.sfo01.rainpole.local:5480

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

The appliance management interface of the appliance opens.

c Click the **Administration** tab and click **Administration**.

d In the **Actions** pane, click **Toggle SSH setting**.

e Verify that the **SSH service status** is `Enabled`.

f Repeat the step for the second vRealize Business appliance.

2 Configure the vRealize Log Insight agent in on the vRealize Business appliances.

a Open an SSH connection to the vRealize Business appliance using the following settings.

Setting	Value
Hostname	■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local
User name	root
Password	*vrb_server_appliance_root_password*

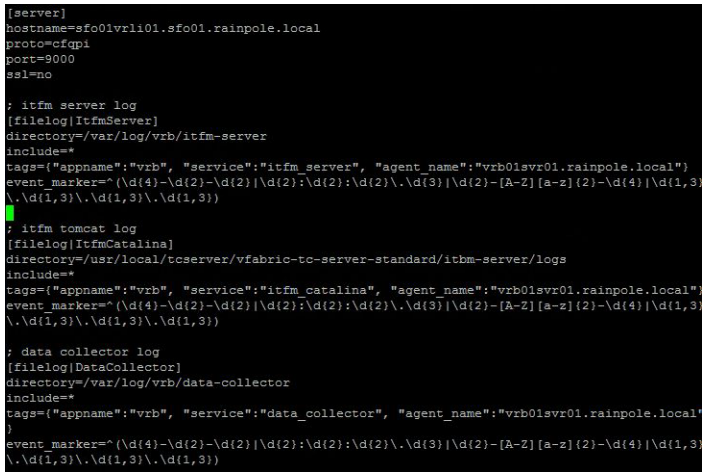
b Edit the `liagent.ini` file using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

c Add the following information under the `[server]` section.

```
[server]
hostname=sfo01vrli01.sfo01.rainpole.local
proto = cfapi
port = 9000
ssl = no
```

d Replace all instances of the `FQDN_localhost` parameter located after `agent_name` with **`vrb01svr01.rainpole.local`**.



e Press Esc and type `:wq!` to save the file.

f Start the Log Insight agent.

```
/etc/init.d/liagentd start
```

g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

h Turn on auto-run by default for the Log Insight agent.

```
chkconfig liagentd on
```

i Repeat the steps to configure the vRealize Business Data Collector at sfo01vrbc01.sfo01.rainpole.local.

3 Confirm that the Log Insight agents are working in the vRealize Log Insight Web 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 icon and select **Administration**.

d Under **Management**, click **Agents**.

e Verify that vrb01svr01.rainpole.local and sfo01vrbc01.sfo01.rainpole.local appear on the page.

Configure Embedded vRealize Orchestrator to Forward Log Events to vRealize Log Insight

You enable the vRealize Log Insight agent and configure the agent group for the embedded vRealize Orchestrator to start collecting log data in the vRealize Orchestrator dashboards.

Procedure

1 Log in 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	*vrli_admin_password*

2 Click the configuration drop-down menu icon and select **Administration**.

3 Under **Management**, click **Agents**.

4 From the drop-down menu at the top, select **vRealize Orchestrator 7.0.1** from the **All Agents** section and click **Copy Template**.

5 In the **Copy Agent Group** dialog box, enter **`vRO7 – Agent Group`** in the name text box and click **Copy**.

6 In the **agent filter** fields, enter the following values pressing Enter after each host name to determine which agents receive the configuration.

Filter	Operator	Values
Hostname	matches	■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local

7 Click **Refresh** and verify that in the **Agents** list vRealize Log Insight receives data from the two agents in the filter.

8 Click **Save New Group** at the bottom of the page.

9 Verify that the vRealize Log Insight server is receiving log events from the vRealize Orchestrator appliances.

   a Click on **Dashboards**, select **VMware - Orchestrator - 7.0.1+** from the **Navigator** menu on the left side.

   b Verify that the **Server nodes grouped by hostname** widget on the **Server overview** dashboard shows the two vRealize Orchestrator hosts.

Install the Linux Content Pack and Configure the Virtual Appliance Agent Group for vRealize Log Insight

Install the content pack for VMware Linux to add the dashboards for viewing log information about the management virtual appliances 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	*vrli_admin_password*

2 Install the content pack for VMware Linux.

   a In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Content Packs**.

   b Under **Content Pack Marketplace**, select **Marketplace**.

   c In the list of content packs, locate the **Linux** content pack and click its icon.

   d In the **Install Content Pack** dialog box, accept the License Agreement and click **Install**.

   e After the installation is complete, the **Linux** content pack appears in the **Installed Content Packs** list on the left.

3 Configure the Log Insight Linux agent group for the virtual appliances from the vRealize Log Insight user interface.

   a Click the configuration drop-down menu icon and select **Administration**.

   b Under **Management**, click **Agents**.

   c From the drop-down at the top, select **Linux** from the **Available Templates** section.

   d Click **Copy Template**.

   e In the **Copy Agent Group** dialog box, enter **`vAppliances – Agent Group`** in the **Name** text box and click **Copy**.

f In the agent filter fields, use the following selections.

Press Enter to separate the host name values.

Filter	Operator	Values
Hostname	matches	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local

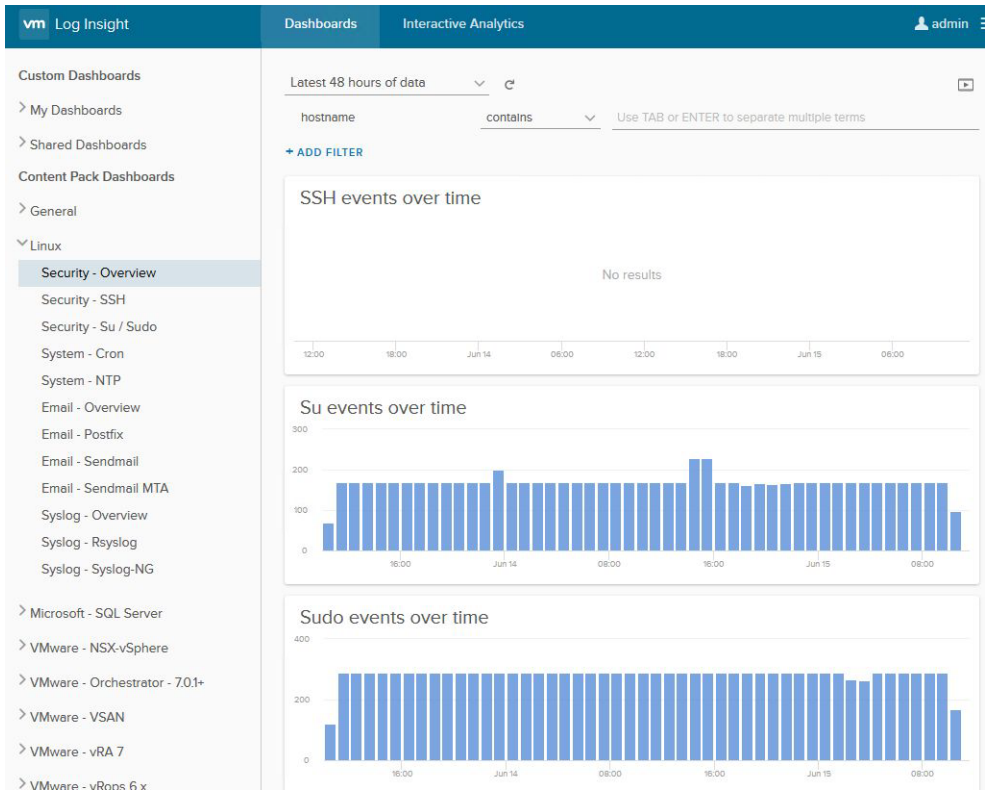
g Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.

h Click **Save New Group** at the bottom of the page.

4 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**.



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	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Administration**.

3 Configure retention threshold notification.

   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 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, in the **Alerts** pane, 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** to on.

   c In the **Archive Location** text box, enter the path to an NFS partition where logs will be archived.

   Use the form **`nfs://nfs-server-address/V2D_vRLI_MgmtA_400GB`**

   d Click **Test** next to the **Archive Location** text box to verify that the share is accessible.

   e Click **Save**.