

vRealize Suite Lifecycle Manager 8.2 Installation, Upgrade, and Management

VMware vRealize Suite Lifecycle Manager 8.2

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

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

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

Copyright © 2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

vRealize Suite Lifecycle Manager Installation, Upgrade, and Management 8

1 Installing and Configuring vRealize Suite Lifecycle Manager 9

System Requirements	11
vRealize Suite Lifecycle Manager Ports	12
Downloading vRealize Easy Installer	14
Access vRealize Easy Installer	14
Installing vRealize Suite Lifecycle Manager with vRealize Easy Installer	17
Install and Configure Products	18
Log In to vRealize Suite Lifecycle Manager	19
Migrating 2.x Version to vRealize Suite Lifecycle Manager 8.x	20
Install VMware Identity Manager	22
Catalog Applications for vRealize Suite Products	23
Install and Configure vRealize Automation 8.2 Using Easy Installer	24
Assign a User Role in vCenter Server	25
Add a vCenter Server to a vRealize Suite Lifecycle Manager Data Center	27
Remove vCenter Server from vRealize Suite Lifecycle Manager Data Center	28
Configuring vRealize Suite Lifecycle Manager Settings	28
Authentication Provider in vRealize Suite Lifecycle Manager	29
Configure Your System	29
Working with Product Support	34
Configure Product Binaries	34
Patching for Products through vRealize Suite Lifecycle Manager	35
Configure Your Patched Product Binaries	37
Register with My VMware	37
Servers and Protocols	39
Configure NTP Servers	39
Configure DNS Servers	40
Data Source Using SNMP Configurations for vRealize Network Insight	40
Identity and Tenant Management With VMware Identity Manager	41
Manage Your Directory in Identity Management	42
Configuring User Attribute Definition	43
Assign User Roles with User Management	43
Add Active Directory Over LDAP	44
Add Active Directory with Integrated Windows Authentication	47
Tenant Management in vRealize Suite Lifecycle Manager	49
Using Tenant Migration	63
Configure Certificate Within Locker	66

Configure License Within Locker	68
Managing vRealize Cloud Licenses in Locker	69
Configure Your Password Within Locker	70
Password Management Within Locker	70
Add a Data Center to vRealize Suite Lifecycle Manager	71
Creating Roles for Specific Access	72
Assign Roles for Certificate Operations	72
Replace Certificate for vRealize Suite Lifecycle Manager	73
Federal Information Processing Standard 140-2 Support	74
Enable or Disable FIPS Mode Compliance in vRealize Suite Lifecycle Manager	74
vRealize Suite Lifecycle Manager on VMware Cloud on AWS Environment	75

2 Upgrading Your Product 76

Upgrade vRealize Suite Lifecycle Manager 8.x	76
Support for Additional Product Versions	78
Upgrade VMware Identity Manager	78
Migrating Windows Connector	79
Upgrade vRealize Automation 8.x with vRealize Suite Lifecycle Manager	80
Upgrade Functionality of vRealize Automation	82
Upgrade a vRealize Suite Product	84
Upgrade Existing Products Using Pre-Upgrade Checker	85
Update vRealize Operations Manager	87
Update vRealize Automation 7.x	88
Update vRealize Network Insight	89
Update vRealize Log Insight	90
Update vRealize Business for Cloud	90

3 Creating an Environment 92

Create a New Private Cloud Environment Using the Installation Wizard	93
Install VMware Identity Manager in vRealize Suite Lifecycle Manager	96
Configure Environment Settings for a New Private Cloud	96
Install vRealize Suite Products	97
Accept EULA and License Selection	97
Configure Certificate Details	98
Configure Infrastructure Details	99
Configure Network Details	101
Configure Product Details	102
Configure vRealize Suite Products for Installation	111
Validate Private Cloud Environment Details	115
Confirm Environment and Installation Settings	119
Import an Existing Environment using Installation Wizard	119

Import VMware Identity Manager Environment	120
Import vRealize Business for Cloud Environment	121
Import vRealize Automation Environment	121
Import vRealize Network Insight Environment	123
Import vRealize Operations Manager Environment	124
Import vRealize Log Insight Environment	124
Create a Private Cloud Environment Using a Configuration File	125

4 Managing Private Cloud Environments 127

Day 2 Operations for Global Environment in vRealize Suite Lifecycle Manager	127
Re-Size Hardware Resources for VMware Identity Manager	129
Day 2 Operations with Other Products In vRealize Suite Lifecycle Manager	129
Reconfigure Internal Pods and Service Subnets	131
Accessing Lifecycle Operations	131
Lifecycle Manager with a Dashboard	131
Add a Product to an Existing Private Cloud Environment	132
Add a Data Source to an Existing Private Cloud Environment	132
Data Operations Supported by vRealize Network Insight	132
Import Data sources in vRealize Suite Lifecycle Manager	133
Manage a Data Source in an Existing Private Cloud Environment	133
Update Bulk Passwords for Data Source	134
Scale-Out VMware Identity Manager	135
Scheduled Health Check	136
Scale-Out Tenant Enabled VMware Identity Manager	137
Scale-Out Windows Connector	137
Scale-Out vRealize Suite Products	138
Scale-Out Tenant Enabled vRealize Automation	139
Scale-Up vRealize Suite Products	140
Export a Private Cloud Environment Configuration File	141
Download Private Cloud Product Logs	142
Delete an Environment	142
Managing vRealize Suite Products in a Private Cloud	143
Create a Product Snapshot	144
Inventory Sync in vRealize Suite Lifecycle Manager	145
Product References	145
Change your Password for vRealize Products	146
Delete a Product from an Environment	147
Replace License for any Product	148
Configure Health Monitoring for the vRealize Suite Management Stack	149
Health Status in vRealize Suite Lifecycle Manager	150
View the SDDC Health Overview Dashboard in VMware vRealize Operations Manager	151

Enable or Disable Health Check for Products in vRealize Suite Lifecycle Manager	151
Adding and Managing Content from Marketplace	152
Getting Started with Marketplace	152
Find and Download Content from Marketplace	152
View and Upgrade Downloaded Marketplace Content	153
Install a Downloaded Marketplace Content	154
Delete Content Downloaded from the Marketplace	155
5 Managing Content Lifecycle in vRealize Suite Lifecycle Manager	156
Working with Content Endpoints	158
Add a vRealize Orchestrator Content Endpoint	159
Add a vRealize Automation Content Endpoint	161
Add a Source Control Endpoint	162
Add a vCenter Server Content Endpoint	163
Add a vRealize Operations Manager Endpoint	165
Delete a Content Endpoint	166
Edit a Content Endpoint	166
Managing Content	167
Add Content	168
Delete Multiple Content	170
Working with Captured Content	171
Content Actions	171
Content Types Available for Products	171
Searching Content	175
Test Content	175
Source Control with vRealize Suite Lifecycle Manager Content Lifecycle Management	178
Deploy a Content Package	184
Multi Release of Content Package	185
Delete a Content Package	186
Content Issues You might Encounter	187
Access Source Control	187
Managing Source Control Server Endpoints	187
Add a Source Control Server Endpoint	188
Delete a Source Control Server Endpoint	189
Working with Content Settings	189
Working with Content Pipelines	190
Content Pipeline Settings	192
6 Request Status	195
7 Notifications in vRealize Suite Lifecycle Manager	196

8 Troubleshooting vRealize Suite Lifecycle Manager 197

- Unexpectedly Large vRealize Operations Manager Virtual Machine Fails to Power On Due to Resource Limitations 198
- Environment Deployment Fails During vRealize Log Insight Clustering and VMware Identity Manager Registration 199
- Change in DNS Server 199
- Wrong IP Details During vRealize Suite Lifecycle Manager Deployment 200
- Binary Mappings Are Not Populated 200
- Content Capture Fails with Secure Field 201
- Fix Errors Using Log Files 201
- Blueprint Capture Fails 201
- Component Profile Deployment Fails 202
- Update vRealize Suite Lifecycle Manager Hostname 202
- Resource Not Found in Directory Management 203
- Inventory Sync Fails with an Error Message 203
- Import or Inventory Sync of vRealize Suite Product Fails 204
- VMware Identity Manager Postgres Cluster Outage Due to Loss of Delegate IP 204
- Importing vRealize Automation into vRealize Suite Lifecycle Manager Fails 205

vRealize Suite Lifecycle Manager Installation, Upgrade, and Management

vRealize Suite Lifecycle Manager Installation and Management provides instructions for installing VMware vRealize Suite Lifecycle Manager and using vRealize Suite Lifecycle Manager to install and manage products in the vRealize Suite.

Intended Audience

This information is intended for anyone who wants to use vRealize Suite Lifecycle Manager to deploy and manage the vRealize Suite of products to monitor and manage a software-defined data center (SDDC). The information is written for experienced virtual machine administrators who are familiar with enterprise management applications and data center operations.

Installing and Configuring vRealize Suite Lifecycle Manager

1

vRealize Suite Lifecycle Manager provides a single installation and management platform for most of the products in the vRealize Suite.

- [System Requirements](#)

Systems that run vRealize Suite Lifecycle Manager must meet specific hardware and operating system requirements.

- [Downloading vRealize Easy Installer](#)

To deploy standalone vRealize Automation, download the executable file from the My VMware download page.

- [Installing vRealize Suite Lifecycle Manager with vRealize Easy Installer](#)

You can install vRealize Suite Lifecycle Manager using vRealize Easy Installer.

- [Install and Configure Products](#)

You can deploy and configure vRealize Suite Lifecycle Manager using the Easy Installer when a deployment is completed.

- [Log In to vRealize Suite Lifecycle Manager](#)

Log in to the vRealize Suite Lifecycle Manager UI to create and manage cloud environments with vRealize Suite Lifecycle Manager.

- [Migrating 2.x Version to vRealize Suite Lifecycle Manager 8.x](#)

You can migrate the earlier versions of Lifecycle Manager to the latest versions.

- [Install VMware Identity Manager](#)

You can install a new instance of VMware Identity Manager or import an existing instance when you are configuring the vRealize Easy Installer.

- [Install and Configure vRealize Automation 8.2 Using Easy Installer](#)

The vRealize Easy Installer provides you with a functionality to install vRealize Automation 8.2 with minimum steps.

- [Assign a User Role in vCenter Server](#)

Create a user role in the vSphere Client with privileges that are required for vRealize Suite Lifecycle Manager. The same role can be assigned to the user who can add a vCenter Server in vRealize Suite Lifecycle Manager.

- [Configuring vRealize Suite Lifecycle Manager Settings](#)

You can access the Lifecycle Operations from the My Service dashboard. You can modify the settings for vRealize Suite Lifecycle Manager, such as passwords, and SSH settings in Lifecycle Operations.

- [Working with Product Support](#)

After configuring your vRealize Suite Lifecycle Manager system information, you can check and apply updates or patches that are available in your existing environment.

- [Servers and Protocols](#)

You can provide more information on configuring your appliance by defining the required servers and protocols.

- [Identity and Tenant Management With VMware Identity Manager](#)

In User or Identity Management, you can map users present in VMware Identity Manager to roles available in vRealize Suite Lifecycle Manager. Configuring VMware Identity Manager is a mandatory process before you install any suite products. If you have not installed when installing vRealize Suite Lifecycle Manager, you will still be prompted to configure and then proceed.

- [Configure Certificate Within Locker](#)

You can generate a new certificate for products that are deployed in vRealize Suite Lifecycle Manager.

- [Configure License Within Locker](#)

Locker is an application like Lifecycle Manager which helps to manage the Certificate, Passwords, and Licenses from single pane. You can configure licenses at the locker level.

- [Configure Your Password Within Locker](#)

Locker in vRealize Suite Lifecycle Manager 8.0 stores all the passwords that are used across the vRealize Suite Lifecycle Manager. Add the passwords for adding vCenter Server, product deployments, products import, My VMware, and Product Password Update. You can configure a password at the locker level and are retrieved from the UI.

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

You can add a data center to vRealize Suite Lifecycle Manager to back up your private cloud environments.

- [Creating Roles for Specific Access](#)

In vRealize Suite Lifecycle Manager, you can delegate the certificate replacement operations to any users in a consistent manner across VMware suite products.

- [Replace Certificate for vRealize Suite Lifecycle Manager](#)

If you use the custom certificate for vRealize Suite Lifecycle Manager instead of default self-signed certificate, you replace the vRealize Suite Lifecycle Manager certificate.

■ [Federal Information Processing Standard 140-2 Support](#)

VMware vRealize Suite Lifecycle Manager 8.2 supports Federal Information Processing Standard (FIPS) 140-2. FIPS 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules.

■ [vRealize Suite Lifecycle Manager on VMware Cloud on AWS Environment](#)

Starting with 8.2, vRealize Suite Lifecycle Manager supports VMware Cloud (VMC) on AWS environment. VMC on AWS is an integrated private cloud offering developed by VMware and Amazon Web Services (AWS). vRealize Suite Lifecycle Manager 8.2 supports M11 and M12 versions of VMC.

System Requirements

Systems that run vRealize Suite Lifecycle Manager must meet specific hardware and operating system requirements.

Minimum Software Requirements

Verify that the system where you run vRealize Suite Lifecycle Manager meets the following minimum software requirements.

- vCenter Server 6.0
- ESXi version 6.0

Minimum Hardware Requirements

Verify that the system where you run vRealize Suite Lifecycle Manager meets the following minimum software requirements.

- 6 GB memory
- 78 GB storage - Thick Provision

Supported vRealize Products for Greenfield Installation and Upgrade

vRealize Suite Lifecycle Manager supports the following vRealize products and product versions.

Product	Supported Versions
vRealize Automation	8.1 and 8.2
vRealize Business for Cloud	7.5.0 and 7.6.0
vRealize Operations Manager	8.1.1, and 8.2
vRealize Log Insight	8.1.1 and 8.2
VMware Identity Manager	3.3.2 (3.3.1 for import only)
vRealize Network Insight	5.2.0, 5.3.0, and 6.0.0 Install the vRealize Suite Lifecycle Manager product support pack 1 for vRealize Network Insight 6.0.0 by downloading the .pspk file. For more information, see VMware vRealize Suite Lifecycle Manager 8.2.0 Release Notes .

For more information about vRealize Suite, see [vRealize Suite Overview](#). You can onboard a supported vRealize product version that supports import in vRealize Suite Lifecycle Manager, and then can upgrade the same to a supported product versions by vRealize Suite Lifecycle Manager.

Supported vRealize Versions for Imported Products in vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager supports the following vRealize products and product versions.

Product	Supported Versions
vRealize Automation	7.2, 7.3.0, 7.3.1, 7.4, 7.5.0, 7.6.0, 8.0.0, 8.0.1, 8.1.0, and 8.2.0
vRealize Business for Cloud	7.2, 7.3.0, 7.3.1, 7.4, 7.5.0, and 7.6.0
vRealize Operations Manager	6.3, 6.4, 6.5.0, 6.6.0, 6.6.1, 6.7.0, 7.0.0, 7.5.0, 8.0.0, 8.0.1, 8.1.0, 8.1.1, and 8.2.0
vRealize Log Insight	4.5.1, 4.6.0, 4.6.1, 4.7.0, 4.7.1, 4.8.0, 8.0.0, 8.1.0, 8.1.1, and 8.2.0
VMware Identity Manager	New installation of vRealize Automation 8.2 supports only 3.3.2 (brown field). Only Lifecycle Manager migrated setups support older version.
vRealize Network Insight	4.0, 4.1, 4.1.1, 4.2.0, 5.0, 5.1.0, 5.2.0, 5.3.0, and 6.0.0 Install the vRealize Suite Lifecycle Manager product support pack 1 for vRealize Network Insight 6.0.0 by downloading the .pspk file. For more information, see VMware vRealize Suite Lifecycle Manager 8.2.0 Release Notes .

For the product interoperability, see [Interoperability Matrix](#). For more information about vRealize Suite, see [vRealize Suite Overview](#).

Supported Browser

- Google Chrome
- Internet Explorer
- Mozilla Firefox

vRealize Suite Lifecycle Manager Ports

This section provides a list of ports used by vRealize Suite Lifecycle Manager for product and integration communication.

Table 1-1. Required Ports and Endpoints for Integration and Communication with VMware Services in Cloud

Service	TCP Port	URL
My VMware	443	https://apigw.vmware.com
Solutions Exchange	443	https://marketplace.vmware.com
Updates	443	https://vapp-updates.vmware.com
Compatibility	443	https://simsservice.vmware.com

Table 1-1. Required Ports and Endpoints for Integration and Communication with VMware Services in Cloud (continued)

Service	TCP Port	URL
Patch and policy refresh repository	443	https://vrealize-updates.vmware.com
VMware Cloud	443	https://console.cloud.vmware.com
VMware Cloud API	443	https://api.mgmt.cloud.vmware.com
Subscriptions API	443	https://vconnect.vmware.com

My VMware API Host Names	Market Place API Host Names	Market Place API Host URLs
apigw.vmware.com	marketplace.vmware.com	https://marketplace.vmware.com/service/api/
download2.vmware.com download3.vmware.com	drd6c1w7be.execute-api.us-west-1.amazonaws.com (* .amazonaws.com)	https://drd6c1w7be.execute-api.us-west-1.amazonaws.com/prod/api
*.akamaiedge.net		

Note

- vRealize Suite Lifecycle Manager always initiates the communication to retrieve or to send data to the VMware services in Cloud. You can configure your network to permit outbound traffic and block inbound traffic to the specified port without impacting the vRealize Suite Lifecycle Manager features that integrate with the VMware services in Cloud.
- Ensure that any downloads or API host URLs that are redirected from Market Place are allowed.

Table 1-2. Required Ports for Integration and Communication with VMware Products On-Premise

Product or Integration	TCP Port Number
vRealize Automation Appliance	5480, 443, 22
vRealize Automation IaaS Server Nodes	443
vRealize Automation Proxy	443
vRealize Business for Cloud Server/Collector Appliances	5480, 443, 22
vRealize Operations Manager Analytics Cluster Appliances	443, 22
vRealize Operations Manager Remote Collector Appliances	443, 22
vRealize Log Insight Appliances	443, 9543, 16520, 22
vRealize Network Insight	443, 22
Identity Manager Appliances	8443, 443, 9999, 9898, 9000, 9694 (Use these for a cluster)

Table 1-2. Required Ports for Integration and Communication with VMware Products On-Premise (continued)

Product or Integration	TCP Port Number
vRealize Orchestrator Appliances	<ul style="list-style-type: none"> ■ 8281 - vRealize Orchestrator 7.x version only. ■ 443 - Starting with vRealize Orchestrator 8.x.
vCenter Server Instances	443
ESXi Host Instances	443
Content Management Host (GitLab)	443

Note For vRealize Suite Lifecycle Manager 8.x and later, ICMP protocol must be enabled between vRealize Suite Lifecycle Manager and products that are being managed.

Note For more information on ports, see *vRealize Suite Lifecycle Manager 8.x Security Hardening Guide* and [VMware Ports and Protocol](#) tool.

Downloading vRealize Easy Installer

To deploy standalone vRealize Automation, download the executable file from the My VMware download page.

Access vRealize Easy Installer

You can access vRealize Easy Installer after you download the executable file from My VMware download page.

Prerequisites

Verify that you have downloaded the ISO file.

Procedure

- 1 After you download the file, mount the `vra-lcm-installer.iso` file.
- 2 Browse to the folder `vrlcm-ui-installer` inside the CD-ROM.
- 3 The folder contains three sub-folder for three operating systems. Based on your operating system, browse to the corresponding operating system folder inside `vrlcm-ui-installer` folder.

4 Click the installer file in the folder.

Operating System	File Path
Windows	lcm-installer\vr lcm-ui-installer\win32
Linux	a Login to Linux VM. b Run <code>apt-get install p7zip-full</code> . c Run <code>7z x vra-lcm-installer.iso</code> . d Run <code>chmod +x vr lcm-ui-installer/lin64/installer</code> e Run <code>apt install libnss3</code> (required only if libnss3 component is not installed.) f Run <code>vr lcm-ui-installer/lin64/installer</code> .
Mac	vr lcm-ui-installer/mac/Installer

The vRealize Easy Installer UI is specific to the operating system. Ensure that you are using the valid UI folder path to launch the installer.

Install and Configure vRealize Identity Manager

You can install a new instance of vRealize Identity Manager or import an existing instance when you are configuring the vRealize Easy Installer.

If you want to customize your vRealize Identity Manager configuration, which can include deployment of vRealize Identity Manager in a standard or a cluster mode, customized mode of Network, storage, you can skip the installation of vRealize Identity Manager. If you have skipped, you are still prompted to configure the vRealize Identity Manager on the vRealize Suite Lifecycle Manager UI. With vRealize Easy Installer you either import an existing vRealize Identity Manager into vRealize Suite Lifecycle Manager or a new instance of vRealize Identity Manager can be deployed. For more information on Hardware re-sizing for vRealize Identity Manager, see [Re-sizing Hardware](#).

Prerequisites

Verify that you have a static IP address before you begin your configuration.

Procedure

- 1 To install a new instance, select **Install new vIDM**.
- 2 Enter the required text boxes under **Virtual Machine Name**, **IP Address**, **Hostname**, and **Default Configuration Admin**.

Note The vRealize Easy Installer creates the Default Configuration Admin user as a local user in vRealize Identity Manager and the same user is used to integrate products with vRealize Identity Manager.

3 To import an existing instance, select **Import Existing vIDM**.

- a Enter the **Hostname, Admin Password, System Admin Password, SSH User Password, Root Password, Default Configuration Admin, and Default Configuration Password**.
- b Select the **Sync group members to the Directory when user want to sync group member** while adding a group for the global configuration of vRealize Identity Manager.

With vRealize Easy Installer 8.2	vRealize Identity Manager supported version	Description
New installation of vRealize Suite Lifecycle Manager	3.3.2 only	
Import vRealize Suite Lifecycle Manager	3.3.1 and 3.3.2	
Deploy vRealize Automation	3.3.2	Note If you import vRealize Identity Manager 3.3.1 and install vRealize Automation 8.2, the installation fails.

Note vRealize Identity Manager will be supported if the scenarios are one of the following:

- Single or cluster instance with embedded Postgres database.
- vRealize Identity Manager 3.3.1 and 3.3.2 with the given deployment type.

Note vRealize Identity Manager will not be supported if the scenarios are one of the following:

- Single or cluster instance having external Database (Postgres/MSSQL and so on).
- Single or cluster instance with additional connectors (Windows and external connectors) other than the embedded ones.
- Earlier versions of vRealize Identity Manager. (3.3.0 and earlier version)

Note If the older version of vRealize Suite Lifecycle Manager does not have vRealize Identity Manager, it can either be installed or imported. vRealize Identity Manager Lifecycle and extended day-2 functionalities are not supported from the vRealize Suite Lifecycle Manager if the imported vRealize Identity Manager not in supported form factor:

Upgrade support from an older vRealize Identity Manager version (3.3.0 and earlier) to the latest is only available if it is a single instance or a node vRealize Identity Manager with embedded postgres database.

Else you can upgrade outside vRealize Suite Lifecycle Manager . Once upgraded, it can any time be reimported by triggering Inventory Sync in vRealize Suite Lifecycle Manager .

4 Click **Next**.

If you cannot deploy vRealize Suite Lifecycle Manager vRealize Identity Manager or vRealize Automation in VMC vCenter Server using vRealize Easy Installer, then use the vCenter Server that has an administrator privilege to deploy products.

Installing vRealize Suite Lifecycle Manager with vRealize Easy Installer

You can install vRealize Suite Lifecycle Manager using vRealize Easy Installer.

Watch the vRealize Suite Lifecycle Manager Installation of with Easy Installer video:



(Installation of vRealize Suite Lifecycle with Easy Installer)

Prerequisites

You must meet these prerequisites before you can install vRealize Suite Lifecycle Manager:

- Ensure you have a vCenter Server set up and access to the credentials.
- Ensure you have the network configuration details for vRealize Automation
- Ensure you know the Lifecycle VA deployment details

Procedure

- 1 Click **Install** on the **vRealize Easy Installer** window.
- 2 Click **Next** after reading the introduction.
- 3 Accept the License Agreement and click **Next**. Read the **Customer Experience Improvement Program** and select the checkbox to join the program.
- 4 To specify vCenter Server details, enter these details on the Appliance Deployment Target tab.
 - a Enter the **vCenter Server Hostname**.
 - b Enter the **HTTPs Port** number.
 - c Enter the **vCenter Server Username**, and **Password**.
- 5 Click **Next** and you are prompted with a Certificate Warning, click **Accept** to proceed.
- 6 You must specify a location to deploy virtual appliances.
 - a Expand the vCenter Server tree.
 - b Expand to any data center and map your deployment to a specific VM folder.
- 7 Specify a resource cluster on the Select a Compute Resource tab.
 - a Expand the data center tree to an appropriate resource location and click **Next**.
- 8 On the Select a Storage Location tab, select a datastore to store your deployment and click **Next**.
- 9 On the Network Configuration and Password Configuration tabs, set up your **Network** and **Password configuration** by entering the required fields, and clicking **Next**.
 - a For a vRealize Suite Lifecycle Manager VM, enter the **NTP Server** for the appliance and click **Next**.

The network configurations provided for all products are a one time entry for your configuration settings. The password provided is also common for all products and you need not enter the password again while you are installing the products.

Password should have minimum one upper case, one lower case, one number and one special character. Special characters can be !@#\$\$%^&*(). Colon(:) is not supported in the password for vRealize Automation 8.0 and 8.0.1.

- 10 Set up vRealize Suite Lifecycle Manager configuration settings,
 - a Enter a **Virtual Machine Name**, **IP Address**, and **Hostname**.
 - b Provide configuration information. Enter the **Data Center Name**, **vCenter Name** and **Increase the Disk Space** fields.
 - c Enable or disable the **FIPS Mode Compliance**, as required.
 - d Click **Next**.

What to do next

You can now start installing vRealize Identity Manager.

Install and Configure Products

You can deploy and configure vRealize Suite Lifecycle Manager using the Easy Installer when a deployment is completed.

Lifecycle Manager can be installed and configured using the Easy Installer. You can refer to the *Installing vRealize Automation using Easy Installer*.

Prerequisites

- Verify if a vCenter Server is available for deploying Lifecycle Manager and products.
- A static IPv4 with accurate FQDN is used for a Lifecycle Manager deployment.
- To prevent unwanted internal ports outside after vRealize Suite Lifecycle Manager Virtual appliance reboot, login to vRealize Suite Lifecycle Manager Virtual appliance through SSH and run the command `rm -rf /etc/bootstrap/everyboot.d/10-start-services`, after deploying vRealize Suite Lifecycle Manager Virtual appliance from the easy installer.

Procedure

- 1 Deploy Lifecycle Manager using Easy Installer.

Note By default, you can find:

- default_datacenter (datacenter name provided in the Easy Installer)
 - default_vCenter (vCenter Name provided in Easy Installer)
 - DNS servers and NTP servers
 - Data Disk Extended (Disk size provided in Easy Installer)
 - globalenvironment. (VMware Identity Manager - Based on product selection)
 - vRealize Automation environment (Based on product selection)
 - VMware Identity Manager and vRealize Automation passwords in the locker
 - Source mapping for vRealize Automation and VMware Identity Manager
-

- 2 To deploy a new product, after you log in to vRealize Suite Lifecycle Manager, click **Lifecycle Operations** on the **Dashboard - My Services**.
- 3 Click **Datacenter** and navigate to **ADD DATACENTER**.
- 4 Add a **vCenter Server** to the Data Center.
- 5 Create a valid certificate in the vRealize Suite Lifecycle Manager **Locker**.
- 6 Add the required license keys for future use in vRealize Suite Lifecycle Manager Locker.
- 7 Extend the Lifecycle Manager appliance disk space to accommodate product binaries and other necessary components to be used in future.
- 8 (Optional) Configure the proxy settings in Lifecycle Manager for an internal network connectivity.

Log In to vRealize Suite Lifecycle Manager

Log in to the vRealize Suite Lifecycle Manager UI to create and manage cloud environments with vRealize Suite Lifecycle Manager.

Prerequisites

Deploy the vRealize Suite Lifecycle Manager appliance.

Procedure

- 1 Use a supported Web browser (Chrome, IE or Mozilla FireFox) to connect to your vRealize Suite Lifecycle Manager appliance by using the appliance's IP address or host name.

https://IP address/vr1cm

Note You can also access vRealize Suite Lifecycle Manager using the URL **https://IP address**. The URL **http://IP address** does not successfully redirect to vRealize Suite Lifecycle Manager.

- 2 Enter the administrator user name.

admin@local

- 3 Enter the default administrator password.

Admin password will be the default password given in the Easy installer while deploying vRealize Suite Lifecycle Manager.

- 4 Click **Log In**.

What to do next

If you are logging in to vRealize Suite Lifecycle Manager for the first time, set the vRealize Suite Lifecycle Manager **root** password. If you want to reset the password, go to **Settings** tab to make the change.

Configure a new administrator password and other vRealize Suite Lifecycle Manager settings, such as SSH settings.

Migrating 2.x Version to vRealize Suite Lifecycle Manager 8.x

You can migrate the earlier versions of Lifecycle Manager to the latest versions.

You can migrate vRealize Suite Lifecycle Manager 2.1 to 8.x or later. The migration also requires inputs, such as legacy vRealize Suite Lifecycle Manager hostname, user name, password, and SSH password. For more information, watch the Migration of vRealize Suite Lifecycle Manager with Easy Installer video:



(Migration of vRealize Suite Lifecycle Manager with Easy Installer)

Prerequisites

- Verify that you have vRealize Suite Lifecycle Manager 2.1 version or later.
- Legacy vRealize Suite Lifecycle Manager must have SSH enabled for the root user.

Procedure

- 1 From the **Easy Installer** wizard, click **Migrate**.
- 2 Enter the vCenter details where the new vRealize Suite Lifecycle Manager 8.x is installed.

- 3 Select the data center in the **vCenter Server, Compute Resource, and Storage**.
- 4 Enter the network configuration details.
- 5 In the **Password configuration**, enter the password which can be set to the vRealize Suite Lifecycle Manager root and admin password.
- 6 If you want to deploy Identity Manager, then enter the password for **admin**, **sshuser**, and **root credential**.
- 7 Enter the vRealize Suite Lifecycle Manager 8.x **VMname**, **Hostname**, and the **IP details**.
- 8 Enter the legacy vRealize Suite Lifecycle Manager **Hostname**, **Username**, and **Password**.
- 9 Select **New Identity Manager Installation** or **Import Existing Identity Manager**.

If you have selected to install New Identity Manager, then it is deployed in the same vCenter Server mentioned in step 2. If you import an existing Identity manager, verify that the identity manager is already registered in the vRealize Suite Lifecycle Manager legacy VM and identity manager SSH is enabled for the root user.

Note A new installation of vRealize Suite Lifecycle Manager 8.x supports only VMware Identity Manager 3.3.4. The earlier versions of VMware Identity Manager will be supported only for an existing vRealize Suite Lifecycle Manager instance that is being migrated to vRealize Suite Lifecycle Manager 8.x and later. Upgrade support from earlier VMware Identity Manager version to the latest is only available if they conform to the vRealize Suite Lifecycle Manager supported criteria. Any earlier versions of vRealize Suite Lifecycle Manager 8.x allows only single instance of VMware Identity Manager to be deployed with the embedded connector and embedded postgresql database. Upgrade of VMware Identity Manager within vRealize Suite Lifecycle Manager 8.x to the latest versions will be supported if it conforms to the mentioned criteria. Else the upgrade has to be performed outside vRealize Suite Lifecycle Manager. After you upgrade, it can any time be reimported by triggering Inventory Sync in vRealize Suite Lifecycle Manager 8.x.

- 10 Click **Submit**.
- 11 When the migration is successful, click the vRealize Suite Lifecycle Manager URL or the migration request to view the progress by logging in with `admin@local` with the password given in step 5.
- 12 All the environments with data centers, vCenter Servers, Settings (such as NTP, DNS, and so on), content endpoints that are managed by older Lifecycle Manager are migrated and the environments are imported to the latest version.

Results

As part of migration, create a global environment based on installation or import when you import legacy vRealize Suite Lifecycle Manager VMware Identity Manager to vRealize Suite Lifecycle Manager 8.x. If there is a failure in the global environment, it can be due to the missing ssh user password in the legacy vRealize Suite Lifecycle Manager. Enter the SSH password details by selecting the correct password on retry and submit the changes to create a global environment. Once a global environment is created, you can resume the migration operation.

With migration you can create environments, settings, certificate and so on. You can check the status of migration on the Request status.

Note If you import an existing VMware Identity Manager and if the admin password is different from the SSH user for the VMware Identity Manager, then the global environment request fails. In this case, add the SSH password in the locker app manually and retry the request with this password.

Install VMware Identity Manager

You can install a new instance of VMware Identity Manager or import an existing instance when you are configuring the vRealize Easy Installer.

Note

- Without installing or importing a VMware Identity Manager, you cannot access any other environment from vRealize Suite Lifecycle Manager.
 - If you are installing vRealize Automation, ensure that you deploy VMware Identity Manager with the recommended size for vRealize Automation.
 - Refer to the [Easy Installer documentation](#) for the software and hardware requirements to deploy VMware Identity Manager.
-

Prerequisites

- Verify that you have a static IP address and Active Directory details before you begin your configuration.
- Verify that an external load balancer is installed with a valid certificate and the requirements are met. For more information, see [vRealize Automation Load Balancing](#).

Procedure

- 1 To install a new instance, select the **Install vIDM**.
 - a Enter the required text boxes under **Virtual Machine Name**, **IP Address**, **Hostname**, and **Default Configuration Admin**.

- 2 To import an existing instance, select **Import Existing vIDM**.
 - a Enter the **Hostname**, **Admin Password**, **System Admin Password**, **SSH User Password**, **Root Password**, **Default Configuration Admin**, and **Default Configuration Admin Password**.

Note This is a local user that you create on the default tenant in VMware Identity Manager and provide the admin access in the default tenant. The same user is used for all product integration with VMware Identity Manager and the admin role is assigned in the corresponding product. For example, when vRealize Automation 8.x is getting registered with VMware Identity Manager, this default configuration user is made the organization admin and is given with appropriate roles. Once vRealize Automation 8.x is deployed, the configuration user is the initial user to log in with. With other products when they are integrated with VMware Identity Manager, the same user is assigned an admin role in the product. More of SSO use-case where the default configuration admin has access to all deployed products.

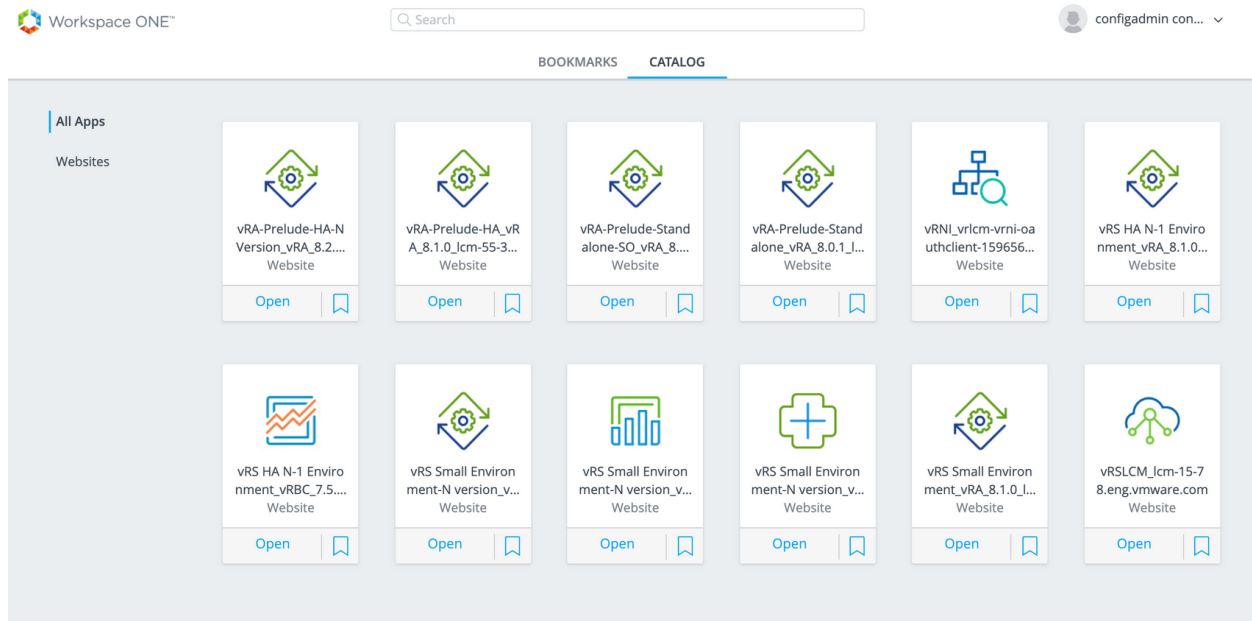
- 3 Click **Next**.

Catalog Applications for vRealize Suite Products

You can deploy a catalog application to access vRealize Suite products that are managed in VMware Workspace ONE Access (formerly called VMware Identity Manager).

When you install vRealize Suite products in VMware vRealize Suite Lifecycle Manager, integrate the desired product with VMware Identity Manager (optional) to create a catalog application in the VMware Workspace ONE Access. With a single sign-on to VMware Workspace ONE Access, view the list of catalogs that are created for the vRealize Suite products. You can choose to open any product from the catalog with the catalog single sign-on feature.

The vRealize Suite products that support the use of catalog applications are vRealize Automation, vRealize Log Insight, vRealize Network Insight, vRealize Operations Manager, vRealize Business for Cloud, and vRealize Suite Lifecycle Manager.



Note

- When installing a single node vRealize Automation 8.x, the catalog application directs you to the vRealize Automation primary host name.
- When installing a clustered vRealize Automation 8.x, the catalog application directs you to the vRealize Automation Load Balancer host name.
- When scaling out a single node vRealize Automation 8.x to a clustered setup, the catalog application directs you to the newly added vRealize Automation Load Balancer host name.

Install and Configure vRealize Automation 8.2 Using Easy Installer

The vRealize Easy Installer provides you with a functionality to install vRealize Automation 8.2 with minimum steps.

The installer provides you with minimal or a clustered deployment options before you start your vRealize Automation configuration. Manual installation of vRealize Automation through OVA or ISO is not supported.

Note The master node is now referred to as the primary node. The master replica node is now referred to as the primary replica node.

Prerequisites

- Verify that you have the primary vRealize Automation credentials before installing vRealize Automation. vRealize Automation 8.2 requires an external VMware Identity Manager 3.3.2 or later.

- Verify that an external load balancer is installed and the requirements are met. For more information, see [vRealize Automation Load Balancing](#).

Procedure

- 1 Enter the vRealize Automation **Environment Name**.
- 2 Under vRealize Automation license, enter the License Key.
- 3 After configuring your VMware Identity Manager settings, you can opt to install vRealize Automation.
- 4 For a standard deployment with a primary node, enter the **Virtual Machine Name**, **IP Address**, and **FQDN Hostname** of vRealize Automation. Skip to Step 6.
- 5 For a cluster deployment with three nodes, enter the **Load Balancer IP address** and **Hostname**.
- 6 For a cluster deployment, create a primary node by using step 4 as a guideline.
- 7 For a cluster deployment, create secondary nodes, enter the required text boxes, and proceed.
- 8 Under Advanced Configuration for vRealize Automation, you can either choose the **Use Default option** to enable the default values for internal pods and services configuration in CIDR format, or use the **Use Custom** option to enter the values for K8S Cluster IP Range and K8S Service IP Range in CIDR format.
- 9 Click **Next**.
- 10 Read the Summary page with the entered data and click **Submit**.

After submitting your details, the installer takes about 30 minutes to install the Lifecycle Manager, copy binaries and then start the installation process. You can enable the multi-tenancy for vRealize Automation, refer to [Tenant Management in vRealize Suite Lifecycle Manager](#).

Assign a User Role in vCenter Server

Create a user role in the vSphere Client with privileges that are required for vRealize Suite Lifecycle Manager. The same role can be assigned to the user who can add a vCenter Server in vRealize Suite Lifecycle Manager.

Prerequisites

Verify that you have administrative privileges to add a role to a user or a user group. You must have administrative privileges to use vCenter Server.

If you are using vCenter deployed on VMC SDDC, then you must use the available CloudAdmin role. For more information on VMC on vCenter, refer to the [VMware Cloud on AWS](#) documentation. When you deploy a VMC on vCenter, you can use the default CloudAdmin role. To learn more about cloud administrator privileges, refer to [CloudAdmin Privileges](#) documentation.

Procedure

- 1 Log in to vCenter Server by using the vSphere Client.
- 2 On the home page of vSphere Client, click **Roles** under Administration.
- 3 Create a role for all system interactions between vRealize Suite Lifecycle Manager and vCenter Server.
- 4 Clone **Read-only** and provide a name to the role.
- 5 In the **Create Role** dialog box, configure the role using the following configuration settings, and click **Next**.

Setting	Value
Role Name	vRealize Suite Lifecycle Manager
Privilege	<ul style="list-style-type: none"> ■ Datastore <ul style="list-style-type: none"> ■ You can select All privileges. ■ Host.Local <ul style="list-style-type: none"> ■ Operations- Add Host to vCenter ■ Operations - Create Virtual Machine ■ Operations - Delete Virtual Machine ■ Operations - Reconfigure Virtual Machine ■ Inventory - Modify - Cluster ■ Network <ul style="list-style-type: none"> ■ Assign Network ■ Resource <ul style="list-style-type: none"> ■ Assign vApp to Resource Pool ■ Assign Virtual Machine to Resource Pool ■ vApp <ul style="list-style-type: none"> ■ You can select All privileges. ■ Virtual Machines <ul style="list-style-type: none"> ■ You can select All privileges. ■ Content Library <ul style="list-style-type: none"> ■ You can select All privileges.

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

Note You should have permissions to create a content library. Content library uses a datastore to store all templates, so you require permission to access, read, and write on the same datastore. Therefore, all privileges under datastore and content library are needed.

- 6 Provide a name to the new role and click **Finish**.

- 7 Select **Global Permissions** under the Administration and click **Manage**.
- 8 To add permissions, click the plus sign.
- 9 Select the user and role that you have created, and click **OK**.

Add a vCenter Server to a vRealize Suite Lifecycle Manager Data Center

Add a vCenter Server to a Data Center before using that vCenter Server to create a private cloud environment.

Prerequisites

Ensure that you have the vCenter Server fully qualified domain name, user name, and password.

Procedure

- 1 On the left pane, click **Datacenters**.
- 2 To add a vcenter, on the **Datacenters** page, click **+ Add vCenter**.
- 3 Enter the **vCenter Name** and **vCenter FQDN**.
- 4 Click **Select vCenter Credentials**.
 - a You can either search for an existing vCenter credentials or add new credentials using the + sign .
 - b Click the + sign on the right corner to assign a password for the selected vCenter credential.
 - c Enter the Password details and click **Add**.
- 5 Enter the **vCenter User Name** for the vCenter server.
You should have the required vCenter privileges.
- 6 Select the **vCenter Type**.
 - Management: All VMware SDDC Suite products are managed by this vCenter type.
 - Workload: All the payload or business related VMs are managed by this vCenter type.
 - Consolidated Management and Workload: Is a vCenter type, where both VMware SDDC Suite products and payload VMs are managed together.

vCenter Type selection is currently used only for classification; the setting has no associated product functionality.
- 7 Click **Validate** and **Save** the changes.
- 8 To import vCenter Servers, click **Import**.
 - a Select the .CSV file and click **Import**. You can upload only one file at a time for a bulk import of VCs in a selected datacenter.
 - b Click **Submit**.

What to do next

Go to the **Requests** page to see the status of this request. When the status is **Completed**, you can use this vCenter Server to create environments. For more information on vCenter user privileges, see [Assign a User Role in vCenter Server](#)

Remove vCenter Server from vRealize Suite Lifecycle Manager Data Center

You can delete a vCenter server from vRealize Suite Lifecycle Manager Data Center that is not used by the environment.

Prerequisites

Ensure that the vCenter does not have a reference, such as a fully qualified domain name or a user name associated with an environment. If vCenter is associated with an environment, the delete option is disabled for the vCenter.

Procedure

- 1 On the Data Center page, select the vCenter, and click **Delete vCenter**.
- 2 Click **Delete** to remove the selected vCenter.

Configuring vRealize Suite Lifecycle Manager Settings

You can access the Lifecycle Operations from the My Service dashboard. You can modify the settings for vRealize Suite Lifecycle Manager, such as passwords, and SSH settings in Lifecycle Operations.

The first time you view the settings page, you must provide data for all available settings to save any settings. Only a user admin has access to the System Admin Applications. The system administration contains the applications:

- System Details
- Logs
- System Patches
- Product Support Pack
- System Upgrade
- Time Settings
- Change Password
- Proxy
- Servers and Accounts
- Change Certificate

- Authentication Provider
- [Authentication Provider in vRealize Suite Lifecycle Manager](#)
Starting with vRealize Suite Lifecycle Manager 8.2, you can view the authentication provider details under the **Settings** tab.
- [Configure Your System](#)
Configure your system after installing the vRealize Suite Lifecycle Manager appliance.

Authentication Provider in vRealize Suite Lifecycle Manager

Starting with vRealize Suite Lifecycle Manager 8.2, you can view the authentication provider details under the **Settings** tab.

The Authentication Provider Information section displays the type of the existing authentication provider, the authentication provider endpoint, the registered FQDN of the application, client ID, and the name of the catalog application.

The Authentication Provider Action section offers syncing and re-registering capabilities. When you change or update the host name or FQDN of vRealize Suite Lifecycle Manager, the authentication provider must sync with the host name. The **Sync** button ensures that the current host name or FQDN of vRealize Suite Lifecycle Manager is synced with VMware Identity Manager. After syncing, you can verify the target URL and the redirect URI in the **Catalog** tab of VMware Identity Manager.

The **RE-REGISTER** button allows re-registering of vRealize Suite Lifecycle Manager with VMware Identity Manager by creating new OAuth clients and catalog applications. The re-registering occurs when VMware Identity Manager is present in `globalenvironment` of vRealize Suite Lifecycle Manager.

When upgrading vRealize Suite Lifecycle Manager 8.1 and earlier releases, the catalog application ID for updating the existing catalog application is not saved, so a duplicate catalog application is created. The new hostname and catalog application ID is saved in the inventory which is used for the subsequent operations.

Configure Your System

Configure your system after installing the vRealize Suite Lifecycle Manager appliance.

Procedure

- 1 In the My Services dashboard, click **Lifecycle Operations**, and then click **Settings**.
- 2 To extend the disk space for vRealize Suite Lifecycle Manager, navigate to **System Details**, click **Extend Storage**.
 - a Enter the **vCenter Host Name**, **User Name**, and **Password** for the first time.
 - b Enter the Disk Size in GB and click **Extend**.

You cannot edit the Network Information fields.

- 3 To reboot the server, click **Reboot System**.
 - a To schedule a weekly server restart, toggle the **Schedule a restart** and select the day of the week, and time for the weekly restart.
- 4 Click **Save**.

Enable or Disable SSH on vRealize Suite Lifecycle Manager

You can enable SSH for troubleshooting purposes.

As a best practice, disable SSH in a production environment, and activate it only to troubleshoot problems that you cannot resolve by other means. Leave it enabled only while needed for a specific purpose and in accordance with your organization's security policies. If content management is enabled, then SSH is enabled automatically and it cannot be disabled. Force disablement of SSH causes failure of Content Lifecycle Management functionality.

Procedure

- 1 From the vRealize Suite Lifecycle Manager dashboard, click Lifecycle Operations and click **Settings**.
- 2 Click **System Details**, under Network Information, enter the **Host Name**, **IP Address**, **IP Address Type**, **Netmask** and **Gateway** fields.
- 3 Enter the **Preferred DNS** and **Alternate DNS address**.

Note SSH is enabled by default.

- 4 Click **SAVE**.

Work with vRealize Suite Lifecycle Manager Logs

You can configure the vRealize Suite Lifecycle Manager log files and download log files for troubleshooting purposes.

Starting with vRealize Suite Lifecycle Manager 8.0.0 and later, vRealize Suite Lifecycle Manager logs are entered in `vmware_vrlcm.log` and `/blackstone-spring.log`.

Generate Log Bundle in vRealize Suite Lifecycle Manager

You can configure the level of information vRealize Suite Lifecycle Manager collects in log files and the number of log files for vRealize Suite Lifecycle Manager.

In the vRealize Suite Lifecycle Manager user interface, perform the following steps.

- 1 Select **Lifecycle Operations**, and then select **Settings**, and navigate to **System Administration > Logs**.
- 2 To create a vRealize Suite Lifecycle Manager log bundle, click **GENERATE LOG BUNDLE**.
- 3 To download logs, click **DOWNLOAD THE LOGS**.

In the command line interface, perform the following steps.

- 1 Connect Secure Shell (SSH) to vRealize Suite Lifecycle Manager VA using root credentials.
- 2 Create a vRealize Suite Lifecycle Manager log bundle directory using the command `mkdir -p /data/lcm-logbundle`.
- 3 Generate a vRealize Suite Lifecycle Manager log bundle directory using the command `/var/lib/vlcm-common/vlcm-support -w /data/lcm-logbundle`.
- 4 Download `/data/lcm-logbundle/<file-name>` with secure copy.

Configure Log Insight Agent

vRealize Suite Lifecycle Manager 8.0.0 and later supports vRealize Log Insight for log analysis. The content pack in vRealize Log Insight for vRealize Suite Lifecycle Manager is supported with version 8.0.1(Patch 1) and later. vRealize Log Insight agent is pre-installed on the vRealize Suite Lifecycle Manager virtual appliance. You can configure the vRealize Suite Lifecycle Manager appliance to forward `cfapi` or system logs, and events to the vRealize Log Insight instance. To use the vRealize Suite Lifecycle Manager content pack dashboards and widgets, the configuration should be done on `cfapi` only.

Prerequisites

Verify that you already have the vRealize Log Insight server details before you set the properties of the Log Insight agent.

Procedure

- 1 Log in to the vRealize Suite Lifecycle Manager virtual appliance.
 - a Open a Web browser and go to *https://vRSLCMIP/vrlcm* and log in with your user credentials.
 - b Click to Lifecycle Operations and from the **Home** page, click **Settings > Logs > Logs Insight Agent Configuration**.
 - c Update the following parameters in the vRealize Suite Lifecycle Manager UI section and save your changes.

```
[server]
hostname= vRealize Log Insight hostname proto=cfapi port=9000 SSL=no
```

When vRealize Log Insight Server is not configured to accept an SSL connection, enabling SSL for Log Insight Agents in vRealize Suite Lifecycle Manager is optional.

Or

```
hostname=vRealize Log Insight hostname proto=cfapi port=9543 SSL=yes
```

When vRealize Log Insight Server is configured to accept an SSL connection, Log Insight Agents must be configured to use the SSL connection in vRealize Suite Lifecycle Manager.

Or

```
hostname=vRealize Log Insight hostname proto=syslog port=514
SSL Server Certificates
```

Set the rules for how the Log Insight client handles the validation of the Log Insight server certificate. Certificates received by the Log Insight agent are stored locally on the agent host machine.

```
Accept Any
Accept Any Trusted
Common Name: (Self-signed server certificate is accepted if its Common Name matches
this value)
Certificates acceptance rules:
```

Note Log Insight agents that receive a new self-signed certificate with the same public key as the existing locally stored self-signed certificate will accept the new certificate. For instance, a self-signed certificate may be regenerated with an existing private key but with a new expiration date.

If the Agent has a locally stored self-signed certificate and receives a valid CA-signed certificate, the Agent silently accepts the CA-signed certificate.

Agents that have a CA-signed certificate will reject self-signed certificates. The agent accepts self-signed certificates only when it initially connects to the Log Insight server.

If an agent with a locally stored CA-signed certificate receives a valid certificate signed by another trusted CA, it is rejected by default. You can select Accept Any Trusted to accept the certificate.

Reconnection Time: 30 min (Time in minutes to force reconnection to the server. This option mitigates the imbalances caused by long-lived TCP connections).

Max Buffer Size: 200 (Max local storage usage limit(data+logs) in MBs. Valid range: 100-2000 MB. Default: 200 MB).

2 Configure the Linux Agent Group on the Log Insight Administration UI .

- a Open a Web browser and go to *https://vRealize Log Insight hostname/IP*.
- b Log in with the credentials - **Setting Value User name** as admin and **Password** as `vrli_admin_password`.
- c Click the configuration drop-down menu icon and select **Administration**.

Note The content pack is not pre-installed in vRealize Log Insight. You must install the pack by downloading it from the marketplace and then configure the agents.

- d Under **Management**, click **Agents**.
- e From the drop-down menu on the top, select **vRealize Lifecycle Management 8.0.1** from the **Available Templates** section.
- f Click **Copy Template**.
- g After copying the template provide vRealize Suite Lifecycle Manager Ipv4 or FQDN, and save the configuration.
- h Once the configuration is complete, the vRealize Suite Lifecycle Manager events or logs start to flow into vRealize Log Insight and the relevant widgets displays the data.

Setting your vRealize Suite Lifecycle Manager Time

You can configure time settings and add NTP server or use a host time for vRealize Suite Lifecycle Manager.

- 1 To change the time settings, navigate to My services dashboard, click **Lifecycle Operations** and click **Settings**.

- 2 Click **Time Settings**.
- 3 For Applicable Time Sync Mode, select **Use Time Server (NTP)** or **Use Host Time**.
 - a To add a server, click **Add New Server** and enter the name, and FQDN address of the server.
 - b To edit, click the edit icon on the list of NTP servers. You cannot edit the FQDN/ IP Address, you can only edit the name of the NTP server.

For more information on adding NTP server, see [Configure NTP Servers](#).

Working with Product Support

After configuring your vRealize Suite Lifecycle Manager system information, you can check and apply updates or patches that are available in your existing environment.

Configure Product Binaries

You can select a Product Binary to use each vRealize Suite product.

You can download binaries outside of Lifecycle Manager and make them available on the NFS path.

Prerequisites

To use a Product Binary downloaded from My VMware, verify that you have registered with My VMware and registered My VMware services with vRealize Suite Lifecycle Manager. See [Register with My VMware](#).

Procedure

- 1 From the My services, navigate to Lifecycle Operations.
- 2 Click **Settings** and navigate to **Binary Mapping > Product Binaries**.
- 3 Click **Add Binaries**.
- 4 Select the Location type.
 - Local - You can map the binaries to the vRealize Suite Lifecycle Manager locally downloaded copy.
 - NFS - You can map to a downloaded product binary with products dependent on the product binary location.
 - My VMware Downloads - You can map to product binary downloaded from My VMware.

- Windows ISO - You can map ISO binary which is required for Windows deployment from Lifecycle Manager.

Note The automatic product OVA mappings are mapped based on the check sum of the binary files. When you select all the OVA files in the NFS share and try to map the product binaries, then it takes long time to map and the data disk might fill faster. NFS represents the local where the OVA files are copied in the NFS shared drive, user should provide the NFS location in the format, NFS-IP:<nfs hostname/ip>:<folder path>/x/y/z. For example, 10.11.12.134:/path/to/folder.

- 5 Enter the location of the Product Binary to use in the **Base Location** text box, and click **Discover**.
- 6 To provide Windows ISO, select the location type as **Windows ISO** and enter the **Windows ISO Mapping Details**.
- 7 Select the Product Binary file from the **Product Binary** list.

Note By default, all the My VMware downloads from vRealize Suite are automatically mapped with no user intervention. If you have already downloaded the product binaries using vRealize Suite My VMware integration but the mapping does not exist in the list under Product Binary then you can select My VMware Downloads option under Add Product Binaries window. To manually copy the OVA files from the vRealize Suite virtual appliance, you can select **Local** option from the Add Product Binaries window and provide the location that is residing within vRealize Suite appliance itself. For either of the scenarios, when you click **Discover**, the relevant binaries is listed in the table within the window.

- 8 Click **Add**.
- 9 With vRealize Suite Lifecycle Manager 2.0 and later, you can also view the list of **Patches** available for Products.
 - a Click **Check Patches Online**.
 - b To upload patches, click **UPLOAD**.

Note You can now delete the unsupported product binaries which are not in use. To delete the binaries, click **Delete Unsupported Binaries**, select the binaries, and then click **Delete All**.

Patching for Products through vRealize Suite Lifecycle Manager

You can search and download available patches for supported products within vRealize Suite Lifecycle Manager.

You can perform following actions using patches from the notifications icon:

- You can view product deployments that have the patches.
- You can view patch logs.

- You can view patch application status.

Note Starting with vRealize Suite Lifecycle Manager 8.2, if you select vRealize Automation 8.x for patching, a precheck option is available for validation.

Install a Patch for Products Through vRealize Suite Lifecycle Manager

You can view and click the related patch from the Notification service. You are then directed to the environment page where you can view a detailed set of information pertaining to all the patches.

Procedure

- 1 Click Lifecycle Operations, navigate to **Settings > Binary Mappings**.
- 2 Click **Patch Binaries**.
- 3 To map a patch offline, download the patch from [My VMware](#) portal and place it in the data folder in vRealize Suite Lifecycle Manager appliance, and then map the offline patch using the local folder option in vRealize Suite Lifecycle Manager UI.
- 4 To check if there are patches available on the internet, click **CHECK PATCHES ONLINE**.
- 5 Trigger the patch install from the product card in the environment page.
- 6 Select the patch from the list of downloaded patches.

The patches must be downloaded from the Product Binaries page. Only the downloaded patches are listed here.

- 7 Click **Next**.
- 8 **Review and Install** the available patch and click **Finish**.
The patch install request progress can be tracked under **Requests**.
- 9 To view the history of patches, click **Patches > History**.
- 10 To view patch history from Environment Card, click **Patch History**

The vRealize Log Insight product patch history has no content even when the vRealize Log Insight patches are applied successfully. This is caused due to the minor version of vRealize Log Insight after the patch is installed. For example, if patch 1 is applied for vRealize Log Insight 4.6.0, then the vRealize Log Insight version is changed to vRealize Log Insight 4.6.1, and the product card is updated to 4.6.1 and no patch history is visible. Installing patch on vRealize Suite Lifecycle Manager is only supported from the following versions of products.

- vRealize Automation 7.5 and later.
- vRealize Operations Manager 7.0 and later.
- vRealize Business for Cloud 7.5 and later.
- vRealize Log Insight 4.7 and later.
- vRealize Network Insight 3.9 and later.

Configure Your Patched Product Binaries

With 8.1 patch, you can now download and map the OVA bundle that are available for a product that is already patched. This operation is useful when you want to scale out a patched environment.

Prerequisites

Ensure the OVA bundle corresponding to the patched product is downloaded from My VMware Portal to vRealize Suite Lifecycle Manager appliance and is placed in the data folder. For example: `/data/patchovabundles/`. For more information on downloading the OVA bundles, click [My VMware](#) portal. You can also see the detailed procedure at [KB 79105](#).

Procedure

1 Click Lifecycle Operations and navigate to **Settings > Binary Mappings**.

2 Click **Patched Product Binaries**.

3 To download patches, click the link provided on the UI.

You are directed to My VMware page where you can download the required patch or a OVA bundle.

4 Click **ADD PATCHED BINARY**.

a Enter the **Source Location** and click **Discover**.

Source location is the directory path in the vRealize Suite Lifecycle Manager appliance where the OVA bundle files are retrieved.

b Select the required OVA bundle from the list and click **ADD**.

5 To delete a product patch, click the Delete icon on the selected patch.

Register with My VMware

You can register with My VMware to access licenses, download product binaries and consume Marketplace content.

Enter your My VMware user name and password to enable vRealize Suite Lifecycle Manager to download product Binary through My VMware. You can also enter using the proxy server under My VMware Settings. Configuring My VMware Settings is optional if you do not have internet connectivity.

Prerequisites

Verify the account details being entered has the following entitlements.

- vRealize Suite 2017 or later or vCloud Suite 2017 or later entitlement with download and view license permissions to download vRealize Suite products.
- vRealize Network Insight or NSX Data Center Enterprise Plus entitlement with download and view license permissions to download vRealize Network Insight.

The configured My VMware user must have permissions to download and view licenses. Download the support pack from the *VMware Solution Marketplace*.

Procedure

- 1 Navigate to **Servers and Accounts**, click **My VMware**.
- 2 Click **ADD MY VMWARE ACCOUNT**.
- 3 Enter your My VMware user name and password, and click **Submit**.

After registration, you can download all the required binaries.

Note To download Product Binary, click the download arrow under **Actions** for the Product Binary to download. If your network requires proxy settings to access external Websites, you can provide those details in the Configure Proxy section. For more information on configuring proxy settings, see [Configure Your Proxy Settings](#).

Configure Your Proxy Settings

If you are using a proxy server in your network, you must configure the proxy server in vRealize Suite Lifecycle Manager.

Normal Proxy (with or without Credential) and Proxy with AD configuration, are supported by vRealize Suite Lifecycle Manager.

Prerequisites

You must have installed and configured a proxy server in your network before using it in vRealize Suite Lifecycle Manager and the proxy server IP should have a host name that is resolvable from vRealize Suite Lifecycle Manager appliance console.

Note If the proxy server does not have a resolvable host name then the procedure to add proxy fails.

Procedure

- 1 Navigate to Lifecycle Operations and click **Settings**.
- 2 Click **Proxy**.
- 3 Toggle **Configure Proxy** to use a proxy server for vRealize Suite Lifecycle Manager, or deselect it to remove an existing proxy server.

vRealize Suite Lifecycle Manager does not save proxy server settings when you disable proxy.

- 4 If you are enabling proxy, enter the **Server**, **Port**, **User name**, and **Credential**.
- 5 Click **Save**.

If vRealize Suite Lifecycle Manager is already configured to use a proxy server, those proxy details are displayed.

Servers and Protocols

You can provide more information on configuring your appliance by defining the required servers and protocols.

Configure NTP Servers

Add the NTP servers in vRealize Suite Lifecycle Manager so that they can be referred while deploying vRealize Suite products. The NTP servers added in vRealize Suite Lifecycle Manager can be used to set for the system that is with vRealize Suite Lifecycle Manager. The NTP servers can also be used as input to vRealize Suite product deployment schema.

Prerequisites

Verify that the NTP servers are functioning.

Procedure

- 1 On the Lifecycle Operations dashboard and navigate to **Settings > NTP Servers**.
- 2 To add an NTP server, click **Add NTP Server**.
- 3 Enter a valid **Name** and **FQDN/ IP Address** of the NTP server.
- 4 Click **ADD**.

Note Starting with vRealize Suite Lifecycle Manager 8.2, NTP servers can be set for vRealize Automation 8.2 and later.

Configure NTP Settings Post Deployment

vRealize Suite Lifecycle Manager currently does not allow you to configure NTP settings for the virtual appliance during the OVA deployment. This section covers information on accurate time synchronization with the infrastructure and the suite products it deploys and manages.

Prerequisites

Verify that the SSH service on the vRealize Suite Lifecycle Manager appliance is enabled.

Procedure

- 1 Log in to vRealize Suite Lifecycle Manager by using the Secure Shell (SSH) client.
 - a Open an SSH connection to the FQDN or IP address of the virtual appliance.
 - b Log in using following credentials, with **Setting** as value, **User Name** as root and **Password** as vrs lcm_root_password.
- 2 Configure the NTP source for the virtual appliance.
 - a Open the `/etc/systemd/timesyncd.conf` file to edit, such as `vi`.
 - b Remove the comment for the NTP configuration, add the NTP settings, and save the changes. For example, `NTP=ntp.sfo01.rainpole.local ntp.lax01.rainpole.local`

- 3 Enable the `systemd-timesyncd` service and verify the status.
 - a Run the `timedatectl set-ntp true` command to enable the network time synchronization.
 - b Run the `systemctl restart systemd-timesyncd` to enable the NTP synchronization
 - c Run the `timedatectl status` to verify the status of the service.
- 4 Logout of the session by entering **Logout**.

Configure DNS Servers

Configure your DNS servers for configuring vRealize Suite Lifecycle Manager appliance to resolve Host names and IPs from the domain name server.

Prerequisites

Verify that you have an existing DNS servers.

Procedure

- 1 On the My Services dashboard, click **Lifecycle Operations**.
- 2 Click **Settings** and navigate to **Servers and Protocols > DNS**.
- 3 Click **Add DNS Server**
- 4 Enter a **DNS Server Name** and **IP Address** .
- 5 Click **Add**.

Data Source Using SNMP Configurations for vRealize Network Insight

The vRealize Suite Lifecycle Manager 1.3 supports vRealize Network Insight. vRealize Network Insight consists of data sources and are recognized by the vRealize Suite Lifecycle Manager appliance.

You can record SNMP configurations, that are relevant to vRealize Network Insight. Click **Add Configuration** to add SNMP for both 2c and 3 SNMP type. The configured SNMP is then used while you are adding vRealize Network Insight data source for Routers and Switches.

Note From vRealize Network Insight 4.0 and later, a new brick size is introduced in vRealize Suite Lifecycle Manager, extra large for both platform and collector node. When you have three nodes in a clustered environment, the brick size should be extra large. All platform nodes in a clustered environment should be of same brick size either large or extra large. But you cannot have both large and extra large in the same cluster.

If a clustered environment is deployed with large brick size and if you want to add one more platform nodes, then you have to manually increase the CPU and the RAM size from vCenter server. You can then import the environment and scale out with an extra large brick size.

Add SNMP Configuration

You can add the SNMP configuration.

Procedure

- 1 Navigate to **Lifecycle Operations** dashboard and navigate to **Settings > SNMP**.
- 2 Click **Add Configuration**.
- 3 To select the **SNMP Version**, select **v2C** or **v3**.
 - a If you have selected v3, enter the **Username** and **Context Name**.
 - b When you select the Authentication type, you are then prompted to enter to the **Auth Password** and **Privacy Type**.
- 4 Click **Add**.

Identity and Tenant Management With VMware Identity Manager

In User or Identity Management, you can map users present in VMware Identity Manager to roles available in vRealize Suite Lifecycle Manager. Configuring VMware Identity Manager is a mandatory process before you install any suite products. If you have not installed when installing vRealize Suite Lifecycle Manager, you will still be prompted to configure and then proceed.

Deployment of an identity manager through vRealize Suite Lifecycle Manager is either through a single node or a cluster with an Internal PostgreSQL database embedded in the appliance and does not support an external database like Microsoft SQL. vRealize Suite Lifecycle Manager supports scale-out of the VMware Identity Manager. For more information, see [Scale-Out VMware Identity Manager](#).

After you deploy a global environment successfully, under Identity and Tenant Management Service you can view.

- Directory Management
- User Management
- Tenant Management

Following are the available roles.

- LCM Cloud Admin
- Content Developer
- Content Release Manager
- Certificate Administrator

Even though the vRealize Suite Lifecycle Manager Cloud Admin has access to the Lifecycle Operations service, only a few services in Settings tab like **NTP Server Setting**, **SNMP**, **DNS**, **My VMware**, and **Binary Mapping** are accessed. Only **LCM Admin**, the `admin@local` has the privilege to access all the settings in the Lifecycle Operations service. The default `admin@local` user is the only application admin who can access the **User Management** service, where **Directory Management** and **Identity Management** are handled.

Note With migration from earlier versions of vRealize Suite Lifecycle Manager to vRealize Suite Lifecycle Manager 8.2, the LCM Admin and LCM Cloud Admin roles are converged into LCM Cloud Admin. So all users who were part of LCM Admin in the previous versions of vRealize Suite Lifecycle Manager will now become LCM Cloud Admin in vRealize Suite Lifecycle Manager 8.2.

Adding VMware Identity Manager is an optional step and by configuring VMware Identity Manager with single sign-on across vRealize Suite Lifecycle Manager and products can be achieved.

Note When VMware Identity Manager is used with vRealize Suite Lifecycle Manager, only **Active Directory over LDAP** and **Active Directory with IWA** are used to sync users and groups to the VMware Identity Manager service. Active Directory over LDAP and Active Directory with IWA are the only supported directory integration.

Manage Your Directory in Identity Management

With Directory Management, you can integrate your enterprise directory with VMware Identity Manager to sync users and groups to the VMware Identity Manager service. Starting from vRealize Suite Lifecycle Manager 8.0, you can create, read, update, and delete directories on VMware Identity Manager. Any updates made in the directory configuration from vRealize Suite Lifecycle Manager 8.0, the same are reflected in the VMware Identity Manager.

Options available under the directory management.

- **Directories** - You can create and manage Active Directories on vRealize Suite Lifecycle Manager. You can create one or more directories and sync them with their enterprise directories. With view directory, you can check sync logs and sync alerts apart from showing basic directory metadata. The directory edit allows an update for the mapped attributes, user, and group DNs. You can delete a directory configuration from vRealize Suite Lifecycle Manager.
- **User Attribute Definitions** - The user attributes lists the default user attributes that sync in the directory and you can add other attributes that you can map to Active Directory attributes.

Note Directory Management is managed by the default vRealize Suite Lifecycle Manager admin user - `admin@local`. Directory Management will be available in vRealize Suite Lifecycle Manager 8.0 only if the VMware Identity Manager version available in the global environment is higher than or equal 3.3.0.

Supported Directories

- Active Directory over LDAP - If you plan to connect to a single Active Directory domain environment, create this directory type
- Active Directory, Integrated Windows Authentication - Create this directory type if you plan to connect to a multi-domain or multi-forest Active Directory environment.
- Secure LDAP

To configure your enterprise directory, you perform the following tasks.

- Create a directory of the same type as your enterprise directory and specify the connection details.
- Map the VMware Identity Manager attributes to attributes used in your Active Directory or LDAP directory.
- Specify the users and groups to sync.
- Sync users and groups.

After you integrate your enterprise directory and perform the initial sync, you can update the configuration and resync at any time.

Configuring User Attribute Definition

When you set up the directory to sync with Active Directory, specify the user attributes. Before setting up the directory, you can specify which default attributes are required and if needed, additional attributes can be added to map the Active Directory attributes.

Changing the default attributes from a required to non-required and marking an attribute to be required can be done only if there are no directories created. Once the directories are created and synced, they cannot be changed. You can mark the required and non-required attributes before adding any directory in the directories page. When you add new custom attributes after the directories are created, to map them you have to edit the directory and update the directory attribute mapping. The change will be effective when the directory gets synced to Active Directory next time.

Assign User Roles with User Management

You can map a user role against users and groups present in VMware Identity Manager. On the User Management page, the user or a group can be selected and a mapping can be edited. You can delete a role mapping, if necessary. If a group is assigned a role, and if you are a part of the group, and you log in to vRealize Suite Lifecycle Manager, you can take the same roles that that group. If you have individual mapping, then it can be consolidation of user role and the roles assigned towards the group.

Prerequisites

Verify if you have any of the user groups for vRealize Suite Lifecycle Manager.

Role	Role Description	Add User/ Groups URL
LCM Cloud Admin	Cloud administrator for vRealize Suite Lifecycle Manager	ug-vrslcm-admins@rainpole.local
Content Release Manager	Content Release Manager	ug-vrslcm-content-admins@rainpole.local
Content Developer	Content Developer	ug-vrslcm-content-developers@rainpole.local
Certificate Administrator	Developer for performing certificate operations	ug-vrslcm-certificate-admins@rainpole.local

Procedure

- 1 Click **Identity and Tenant Management** on the My Services dashboard.
- 2 On the left side, navigate and click **User Management**.
- 3 To add a user or a group, click **+ADD USER/GROUP**.
- 4 To select a user from the populated list in the table, enter an existing user or a group and click **Next**.

If a user or a group already has a mapping, then a warning appears and you are then asked to edit the role mapping rather create again.
- 5 Select a role for the newly created user and click **Next**.
- 6 Read the summary and click **Submit**.

Add Active Directory Over LDAP

You can create this directory type when you plan to connect to a single Active Directory domain environment. For the Active Directory over an LDAP directory type, the connector binds to the Active Directory using a simple bind authentication.

Prerequisites

- List the Active Directory groups and users to sync from Active Directory.
- Verify that you have specified the required default attributes and add additional attributes on the User Attributes definition.
- Verify that you have the required user credentials to add a directory.

Procedure

- 1 Click **Identity and Tenant Management** on the My Services dashboard.
- 2 Navigate to Directory Management tab, click **Directories**.
- 3 Click **Add Directory**, and select **Add Active Directory Over LDAP**.

4 On the **Directory Detail** tab:

Fields	Description
Directory Information	Enter a valid Directory Name.
Directory Sync and Authentication	<p>Select the connector to sync with Active Directory. Connector is a VMware Identity Manager service component that synchronizes users and group data between Active Directory and VMware Identity Manager service.</p> <p>When used as an identity provider, it also authenticates users. Each VMware Identity Manager appliance node contains a default connector component.</p> <p>When required a dedicated connector can also be deployed through a global environment scale-out.</p>
Authentication Enabled	<p>If you want the connector to perform authentication, select Yes.</p> <p>You can indicate whether the selected connector also performs authentication. If you are using a third-party identity provider to authenticate users, click No.</p>
Directory Search Attribute	Select an account attribute from the drop-down menu that contains a user name.
Server Location	<p>Select Directory supports DNS Service Location check box.</p> <ul style="list-style-type: none"> ■ If your Active Directory requires access over SSL/TLS, select the Directory requires all connections to use STARTTLS or SSL check box in the Certificates section, and copy and paste the domain controllers intermediate (if used) and Root CA certificates into the SSL Certificate text box. Enter the intermediate CA certificate first, then the Root CA certificate. Ensure that each certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, enter all the Intermediate-Root CA certificate chains, one after another. If your Active Directory requires access over SSL/TLS and you do not provide the certificates, you cannot create the directory. ■ If you do not want to use DNS Service Location, verify that the Directory supports DNS Service Location check box is not selected and enter the Active Directory server host name and port number.

Fields	Description
Certificates	If your Active Directory requires access over SSL/TLS, select the Directory requires all connections to use SSL check box in the Certificates section and copy and paste the domain controller's Intermediate (if used) and Root CA certificate into the SSL Certificate text box. Enter the Intermediate CA certificate first, then the Root CA certificate. Ensure that the certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If your Active Directory requires access over SSL/TLS and you do not provide the certificate, you cannot create the directory.
Bind User Details	<ul style="list-style-type: none"> ■ Base DN - Enter the DN to start account searches. For example, OU=myUnit,DC=myCorp, DC=com. The Base DN is used for authentication. Only users under the Base DN can authenticate. Ensure that the group DNs and user DNs that you specify later for sync are under this Base DN. ■ Bind User DN - Enter the account details. For example, CN=binduser,OU=myUnit,DC=myCorp, DC=com. Use a Bind user account with a non-expiring password. ■ Bind Password: Click Test Connection to verify that the directory can connect to your Active Directory.

5 Click **Create and Next**.

For Active Directory over LDAP, the domains are listed with a check mark.

6 On the **Domain Selection Detail** tab, select the domain and click **Next**.

7 To map the directory attribute to the Active Directory, on the **Map Attribute** tab, select the required attribute and click **Save and Next**.

8 On the **Group Selection** tab, to sync from Active Directory to the VMware Identity Manager directory specify the Group DN details and click **Next**.

You can also select all the active directory groups that are already available in the list to sync to the directory.

- a To select groups, click **Add Group Distinguished Name**, and specify one or more group DNs. Select the groups under them. Specify group DNs that are under the Base DN that you entered in the "Base DN" text box in the Add Directory page. If a group DN is outside the Base DN, users from that DN will be synced but will not be able to log in.
- b Click **Find Groups**. The **Actions** column lists the number of groups found in the DN. To select all the groups in the DN, click **Select All**, or click the number and select the specific groups to sync. When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.
- c Select the **Sync Nested Group Members** option.

9 On the **User Selection** tab, enter the User DN details and click **Next**.

Suite administrators is a user name in the Active Directory who acts as an Admin user for the deployed suite products, Logs, and AD table.

10 Select the **Sync Nested Group Members** option and enter the **Suite Administrators**.

When this option is enabled, all the users that belong directly to the group you select and all the users that belong to the nested groups under it are synced when the group is entitled. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Identity Manager directory, these users will be members of the parent group that you selected for sync. If the “Sync nested group members” option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

- 11** Click **Save and Next**. In **User Selection** page, click **Add User** and specify the users DNs to sync. Specify user DNs that are under the Base DN that you entered in the Base DN text box in the Add Directory page. If a user DN is outside the Base DN, users from that DN will be synced but will not be able to log in. Click **Save and Next**.
- 12** Review the **Dry Run Check** tab, read the summary, click **Sync and Complete** to start the sync to the directory. The connection to Active Directory will be established, and users and group names are synced from the Active Directory to the VMware Identity Manager directory.
- 13** Click **Submit**.
- 14** To edit, click the **Edit** icon on the specific active directory in the list of active directories. Any information added is appended to the configuration on VMware Identity Manager. However, any removal through editing only removes the configuration from the vRealize Suite Lifecycle Manager inventory and not from the VMware Identity Manager.
- 15** To delete, click the **Delete** icon on the specific active directory in the list of active directories. The delete action deletes the active directory only from the vRealize Suite Lifecycle Manager inventory and not from VMware Identity Manager.

Add Active Directory with Integrated Windows Authentication

You can create this directory type when you plan to connect to a multi-domain Active Directory environment. The connector binds to Active Directory using Integrated Windows Authentication.

Prerequisites

Verify that you have the required user credentials to add a directory.

Procedure

- 1** Click **Identity and Tenant Management** on the My Services dashboard.
- 2** Navigate to Directory Management tab, click **Directories**.
- 3** Click **+Add Directory** and click **Add Active Directory Over IWA**.

4 On the **Directory Detail** tab:

Fields	Description
Directory Information	Enter a valid Directory Name.
Directory Sync and Authentication	Select the connector to sync with Active Directory. Connector is a VMware Identity Manager service component that synchronizes users and group data between Active Directory and VMware Identity Manager service. It authenticates users. Each VMware Identity Manager appliance node contains a default connector component. If necessary, a dedicated connector can also be deployed through a global environment scale-out.
Authentication Enabled	You can indicate whether the selected connector also performs authentication. If you are using a third-party identity provider to authenticate users, click No .
Directory Search Attribute	Select a search attribute from the drop-down menu.
Certificates	<ul style="list-style-type: none"> ■ If your Active Directory requires access over SSL/TLS, select the Directory requires all connections to use STARTTLS check box in the Certificates section, and copy and paste the domain controllers Intermediate (if used) and Root CA certificates into the SSL Certificate text box. Enter the Intermediate CA certificate first, then the Root CA certificate. Ensure that each certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, enter all the Intermediate-Root CA certificate chains, one after the other. If your Active Directory requires access over SSL/TLS and you do not provide the certificates, you cannot create the directory.
Join Domain Details	Enter the Domain Name, Domain Admin user name, and Domain Password.
Bind User Details	<ul style="list-style-type: none"> ■ Enter the Bind Username and Bind Password of the bind user who has permission to query users and groups for the required domains. Enter the user name as <code>sAMAccountName@domain</code>, where domain is the fully qualified domain name. Using a Bind user account with a non-expiring password.

5 Click **Create and Next**.

You can select the domains that should be associated with the Active Directory connection.

6 On the **Domain Selection Detail** tab, select the domain and click **Submit and Next**.

The Active Directory with IWA populates the list of domains and you can select or edit the domains as required.

7 To verify that the VMware Identity Manager directory attribute names are mapped to the correct Active Directory attributes, on the **Map Attribute** tab, select the required attribute and click **Submit and Next**.

- 8 On the **Group Selection** tab, specify the Group DN details and click **Next**.

To select groups, click **Add Group Distinguished Name**, and specify one or more group DNs and select the groups under them. Specify group DNs that are under the Base DN that you entered in the Base DN text box in the Add Directory section. If a group DN is outside the Base DN, users from that DN will be synced but you cannot log in.

When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.

- a Select the **Sync Nested Group Members** option.

- 9 On the **User Selection** tab, enter the User DN details and click **Next**.

Note When this option is enabled, all the users that belong directly to the group you select and all the users that belong to nested groups under it are synced when the group is entitled. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Identity Manager directory, these users are members of the parent group that you selected for sync. If the **Sync nested group members** option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

Suite administrators is a user name in the Active Directory who acts as an Admin user for the deployed suite products, Logs, and AD table.

- 10 On the **Dry Run Check** tab, read the Summary.
- 11 Click **Sync and Complete** to start the sync to the directory. The connection to Active Directory will be established and users and group names are synced from the Active Directory to the VMware Identity Manager directory.
- 12 Click **Submit**.
- 13 To edit, click the **Edit** icon on the specific active directory in the list of active directories. Any information added, gets appended to the configuration on VMware Identity Manager. However, if remove through editing you can only remove the configuration from the vRealize Suite Lifecycle Manager inventory and not from the VMware Identity Manager.
- 14 To delete, click the **Delete** icon on the specific active directory in the list of active directories. You can delete the active directory only from vRealize Suite Lifecycle Manager inventory and not from VMware Identity Manager.

Tenant Management in vRealize Suite Lifecycle Manager

Starting from 8.1, vRealize Suite Lifecycle Manager supports creating and managing of tenants. Tenants are created in VMware Identity Manager and are associated with products that are tenant-aware. So, apart from managing directories on top of VMware Identity Manager, tenants are also managed. Tenancy support is only available from VMware Identity Manager 3.3.2. The previously called User Management is now renamed to Identity and Tenant Management.

Multi-Tenancy Overview

This section describes the key concepts and terminologies required to be understood before starting with multi-tenancy.

Get Familiar with the Tenant Management Terms

Note The master tenant is now referred to as primary tenant.

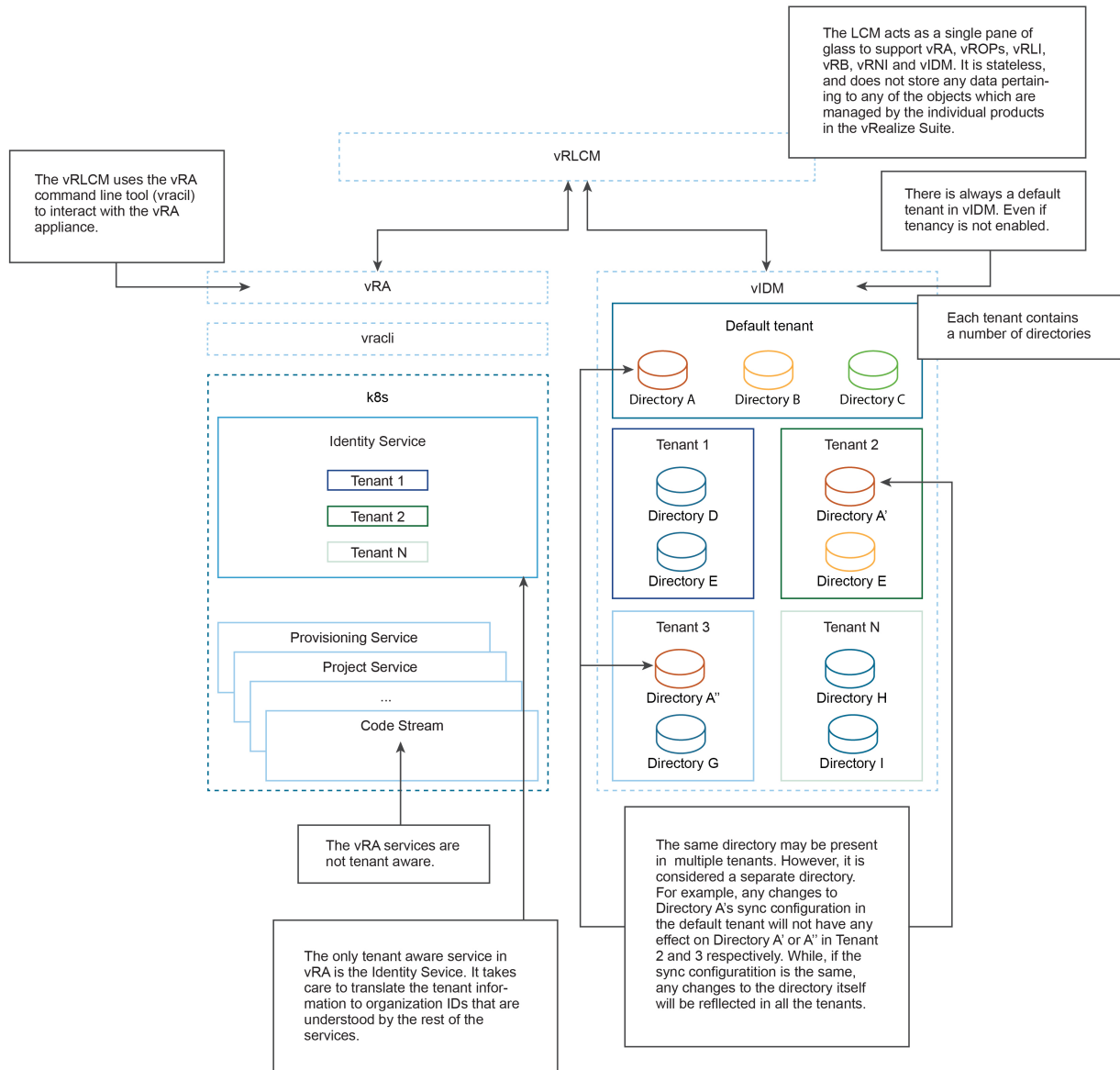
- **Tenant** - It is the highest level in an organizational structure in VMware Identity Manager. All objects like directories, users, groups, third party IDPs are maintained individually for each tenant. Each tenant is isolated from the rest of the tenants and they do not share any resource with each other.
- **Primary Tenant** - There is always at least one tenant (primary, default or base) present in the VMware Identity Manager which is called as primary tenant.

For vRealize Automation 7.x users, this is the 'vsphere.local' that was present out of the box in a vRealize Automation 7.x deployments. The primary tenant in vRealize Automation 7.x was by default bootstrapped with 'vsphere.local' as its name. But this does not happen in a standalone deployment of VMware Identity Manager. The primary tenant name is formed based on the first VMware Identity Manager node that gets deployed and bootstrapped. For example, if 'idm1.vmwlab.local' is the first VMware Identity Manager node that gets deployed, then when you bootstrap VMware Identity Manager, primary tenant is created with name 'idm1'. Nodes further getting scaled-out like 'idm2.vmwlab.local' and 'idm3.vmwlab.local' does not effect. The primary tenant name is formed only once and remains the same in a single or clustered instance.

- **Primary Tenant Alias** - You cannot create sub tenants in VMware Identity Manager under the primary tenant until a few configurations are set and enabled. Setting an alias name for the primary tenant is one such important configuration. An alias must be created on the primary tenant and the primary tenant should always be accessed through the primary tenant alias FQDN on a single node or a clustered instance.
- **Provider Admin** - An admin who owns the management infrastructure, that includes VMware Identity Manager, vRealize Automation and other products. The admin creates and manages all the tenants and associates products with tenants. The vRealize Suite Lifecycle Manager admin user, 'admin@local' is the only provider admin and is authorized to perform tenant management functionalities.
- **Tenant Admin** - An admin with the highest level of administrative permission in each VMware Identity Manager tenant. This permission can be assigned to both local VMware Identity Manager users and Active Directory users present within the VMware Identity Manager tenant.
- **Tenant Aware Products** - Products that support multi-tenancy and maintains proper isolation with each logical tenant instance are tenant aware products. They have one to one mapping with VMware Identity Manager tenants. As of vRealize Suite Lifecycle Manager 8.1 release, only vRealize Automation 8.1 is tenant aware.

- vRealize Automation Organization and Organization Owner - In vRealize Automation 8.x, organization is the top-level construct and it maps 1:1 with VMware Identity Manager tenant. Organization Owner has administrative permission in the vRealize Automation Organization or tenant. While adding tenants and associating vRealize Automation with the newly added tenant, the VMware Identity Manager tenant admin becomes the organization owner for the new tenant. For more information on adding tenants, see [Adding Tenants](#).
- Directory - Directories are second level of objects in VMware Identity Manager. It represents an external identity store or provider like Active Directory (AD) or an OpenLDAP server. There are multiple variants of directory supported in VMware Identity Manager. You can add Active Directory Over LDAP and Active Directory with IWA in the Directory Management section.
- Directory Synchronization - While adding directories, configuration options are provided to filter and synchronize the required users and groups from the Identity Store or provider to the VMware Identity Manager database. Only after a successful sync, you can integrate the users and groups with VMware Identity Manager.
- Directories in tenant - Each tenant can contain several directories. The same directory configuration can be present in multiple tenants, however, it is considered a separate directory. For example: You have added Directory A in primary tenant with some directory configurations (User DNs, Group DNs, Sync configurations). And you have two sub-tenants named Tenant-1 and Tenant-2. The same directory configurations of directory A can be used on to add directories A1 and A2 on each of the sub-tenants respectively, so that the same set of users and groups are synced in sub-tenants - Tenant-1 and Tenant-2. After adding, any changes to the sync configurations of directory A in primary tenant will not affect directories A1 and A2 and its synced users and groups in Tenant-1 and Tenant-2. All three directories and its configurations are independent of each other. All three directories are affected only if the external identity store or provider changes. For example, if users or groups are getting removed directly from the Identity provider then it influences all three directories in all three tenants.

Figure 1-1. Multi-Tenancy Model



Multi-Tenancy Model

This section describes multi-tenancy model explaining how tenants can be accessed through tenant FQDNs and the importance of enabling multi-tenancy along with the certificate, and DNS requirements.

Enabling Multi-Tenancy

The master tenant is now referred to as primary tenant. Even though on day-0, the out-of-the-box VMware Identity Manager includes a primary tenant already available, this is kept at a minimal configuration and further creation of tenants below the primary tenant is not possible. A sequence of configurations and API calls are to be performed on the VMware Identity Manager to enable multi-tenancy. There must be an alias name created for the primary tenant when you enable multi-tenancy. For more information on enabling multi-tenancy, see [Enable Multi-Tenancy](#).

For example, a VMware Identity Manager with FQDN 'idm1.vmwlab.local' can already have a primary tenant with name 'idm1'. Before enabling multi-tenancy, it is mandatory to create an alias for the primary. For example, 'master-tenant' set and use the same alias name everywhere the primary tenant is referred.

Tenant FQDNs

By default, tenants created on VMware Identity Manager are accessed through tenant URLs which are nothing but FQDNs mapped to the VMware Identity Manager server. Every tenant has its own tenant FQDN. For example, on a single node VMware Identity Manager with hostname `idm1.vmwlab.local`, with the primary tenant name (idm1) and primary tenant alias (master-tenant), the primary tenant should be accessed through its FQDN `master-tenant.vmwlab.local`. If a new tenant (tenant1) is created, then it must be accessed only through `tenant1.vmwlab.local`.

Since every tenant requires a dedicated FQDN, creating tenants on VMware Identity Manager mandatorily requires a A-type DNS record mapping the tenant FQDN to the VMware Identity Manager server IP address. For a clustered VMware Identity Manager deployment, every tenant FQDN must be having an A-type record mapping to the VMware Identity Manager load balancer IP address.

The same model applies to vRealize Automation as well. When vRealize Automation is associated with a tenant, the vRealize Automation tenant must be accessed by vRealize Automation tenant FQDNs. For example, VMware Identity Manager with FQDN `idm1.vmwlab.local` having a tenant 'tenant1' accessible through `tenant1.vmwlab.local` and vRealize Automation 8.1

`vra1.vmwlab.local` integrated with this VMware Identity Manager and associated with 'tenant1'. As mentioned, vRealize Automation tenant and VMware Identity Manager tenant maps 1:1, so the primary tenant vRealize Automation can still be accessed by `vra1.vmwlab.local` and 'tenant 1' vRealize Automation must be accessed by `tenant1.vra1.vmwlab.local`.

Note There is a difference between VMware Identity Manager and vRealize Automation tenant FQDNs. For a VMware Identity Manager instance, the tenant FQDN format is tenant name (tenant1) followed by the VMware Identity Manager domain name (vmwlab.local). For example, `tenant1.vmwlab.local`. Since it is tenant name followed by domain, it remains the same even for clustered VMware Identity Manager. For a vRealize Automation, the vRealize Automation tenant FQDN format is tenant name (tenant1) followed the vRealize Automation server FQDN (`vra1.vmwlab.local`) For example, `tenant1.vra1.vmwlab.local`. For a clustered vRealize Automation behind a load-balancer `vra-lb.vmwlab.local`, tenant 1 must be accessed through `tenant1.vra-lb.vmwlab.local`.

Similar to VMware Identity Manager, even vRealize Automation tenant FQDNs require DNS mapping. But for a vRealize Automation it should be CNAME type record mapping the vRealize Automation tenant FQDNs to the vRealize Automation server FQDN. For a clustered vRealize Automation deployment, all vRealize Automation tenant FQDNs must be having a CNAME type DNS record pointing to the vRealize Automation load balancer FQDN.

Apart from having DNS mappings as a mandatory pre-requisite, certificates are also mandatory for tenancy to work. Both VMware Identity Manager, vRealize Automation servers and its load balancers depending on the deployment architecture should have their corresponding certificates holding all the required tenant FQDNs.

Tenant FQDNs on a single node setup

- VMware Identity Manager Node: `idm1.vmwlab.local`
- vRealize Automation Node: `vra1.vmwlab.local`
- Primary tenant alias name: `master-tenant`
- Tenants: `tenant-1`, `tenant-2`

Tenant Names	VMware Identity Manager Tenant FQDNs	vRealize Automation Tenant FQDNs
<code>master-tenant</code>	<code>https://master-tenant.vmwlab.local</code>	<code>https://vra1.vmwlab.local</code>
<code>tenant-1</code>	<code>https://tenant-1.vmwlab.local</code>	<code>https://tenant-1.vra1.vmwlab.local</code>
<code>tenant-2</code>	<code>https://tenant-2.vmwlab.local</code>	<code>https://tenant-2.vra1.vmwlab.local</code>

Tenant FQDNs on a clustered setup

- VMware Identity Manager Load balancer: `idm-lb.vmwlab.local`
- VMware Identity Manager Nodes: `idm1.vmwlab.local`, `idm2.vmwlab.local`, `idm3.vmwlab.local`

vRealize Automation Load balancer: `vra-lb.vmwlab.local`

vRealize Automation Nodes: `vra1.vmwlab.local`, `vra2.vmwlab.local`,
`vra3.vmwlab.local`

Primary tenant alias name: **master-tenant**

Tenants: tenant-1, tenant-2

Tenant Names	VMware Identity Manager Tenant FQDNs	vRealize Automation Tenant FQDNs
master-tenant	<i><code>https://master-tenant.vmwlab.local</code></i>	<i><code>https://vra-lb.vmwlab.local</code></i>
tenant-1	<i><code>https://tenant-1.vmwlab.local</code></i>	<i><code>https://tenant-1.vra-lb.vmwlab.local</code></i>
tenant-2	<i><code>https://tenant-2.vmwlab.local</code></i>	<i><code>https://tenant-2.vra-lb.vmwlab.local</code></i>

Note After you enable multi-tenancy, VMware Identity Manager should only be accessed through its tenant FQDNs. The old FQDNs and hostnames (`idm1.vmwlab.local`, `idm2.vmwlab.local`, `idm3.vmwlab.local` & `idm-lb.vmwlab.local`) becomes invalid.

Mandatory Certificate Requirements

Depending on the deployment type of VMware Identity Manager and vRealize Automation, their corresponding server certificates should have all the tenant FQDNs present within itself. Since each tenant forms its own tenant FQDN (both VMware Identity Manager tenant FQDN and vRealize Automation tenant FQDN), every created tenant requires its tenant FQDN to be added as part of both VMware Identity Manager and vRealize Automation certificates. Enabling multi-tenancy on VMware Identity Manager also requires VMware Identity Manager certificates updated as the primary tenant gets a new alias name and primary tenant FQDN undergoes a change.

Note

- When you change the certificates on VMware Identity Manager to enable multi-tenancy or creating tenants, this brings down the service and leads to a downtime. If VMware Identity Manager certificate is changed, then it goes for a service downtime. The products or services integrated with VMware Identity Manager for their authentication purpose cannot use VMware Identity Manager auth log-in during the downtime. Also, changing VMware Identity Manager certificate requires retrust on all product or services which again lead to a downtime for the products.
 - For every new tenant that is created and associated with vRealize Automation, even vRealize Automation certificates must be changed and this causes service downtime for vRealize Automation.
 - To avoid service down-times on vRealize Automation, VMware Identity Manager and other products or services integrated with VMware Identity Manager, it is generally recommended to have wild-card certificates. For a new tenant, any change made in the VMware Identity Manager certificate or vRealize Automation certificate, can create a downtime in vRealize Automation.
 - If wild-card certificates are not used, then specific SAN entries are to be created for each tenant FQDN on all required certificates.
 - The vRealize Suite Lifecycle Manager locker service helps in managing certificates on the VMware Identity Manager and vRealize Automation server nodes. With vRealize Suite Lifecycle Manager, when you replace VMware Identity Manager certificate, the retrust of VMware Identity Manager certificate on all products is performed automatically.
 - Products or services external to vRealize Suite Lifecycle Manager is handled manually. Locker service does not handle updating load balancer certificates. They are to be done by the user manually. Whenever load-balancer certificates are changed, the same had to be re-trusted on the products.
 - For VMware Identity Manager, the VMware Identity Manager Certificate update or replace operation in vRealize Suite Lifecycle Manager internally makes sure the VMware Identity Manager load balancer certificate is re-trusted before updating the VMware Identity Manager server certificates. So, it is recommended to first change the VMware Identity Manager load balancer certificate manually and then do a VMware Identity Manager certificate to update or replace through vRealize Suite Lifecycle Manager locker service.
 - For a vRealize Automation 8.x, when SSL is terminated at vRealize Automation load balancer and load balancer certificate is changed manually, then make sure to click 'Re-trust Load Balancer' under the vRealize Automation 8.x product card to re-trust the load-balancer certificate in vRealize Automation. For more details, see [Day 2 Operations with Other Products In vRealize Suite Lifecycle Manager](#).
-

Mandatory DNS Requirements

For a single node VMware Identity Manager, you require A-type DNS records highlighting the tenant FQDNs to the VMware Identity Manager server IP address. And for a clustered VMware Identity Manager, A-type DNS records are required pointing the tenant FQDNs to the VMware Identity Manager load-balancer IP address.

For vRealize Automation, for a single node, CNAME type DNS records are required pointing vRealize Automation tenant FQDNs to the vRealize Automation server FQDN. And for a clustered vRealize Automation, CNAME type DNS records pointing vRealize Automation tenant FQDNs to the vRealize Automation load-balancer FQDN.

Requirements for multi-tenancy

Figure 1-2. Single node VMware Identity Manager and vRealize Automation

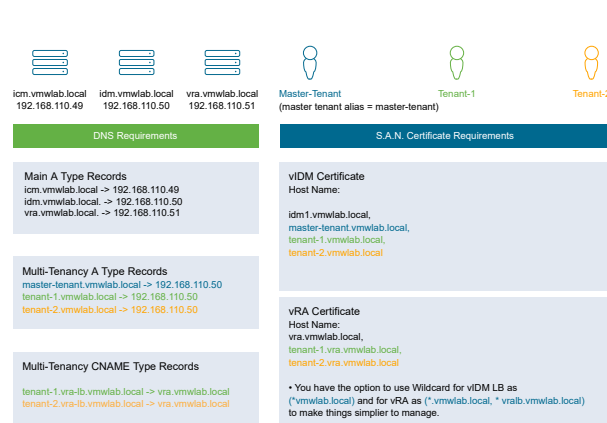


Figure 1-3. Both VMware Identity Manager and vRealize Automation Cluster

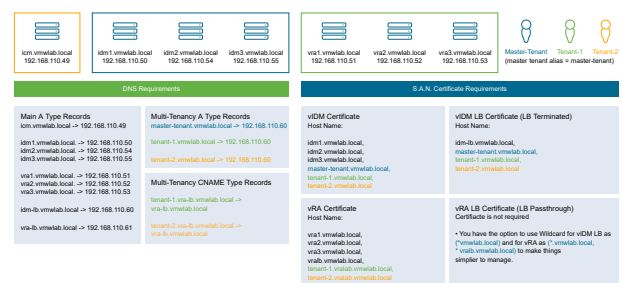


Figure 1-4. vIDM Single and vRA Clustered

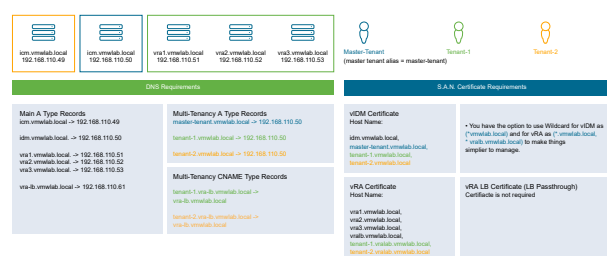
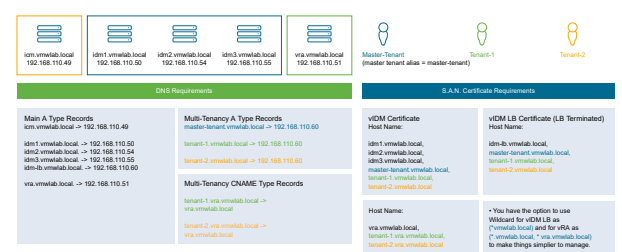


Figure 1-5. VMware Identity Cluster and vRealize Automation Single



Enable Multi-Tenancy

Multi-tenancy feature is not enabled out-of-the-box. You can opt-in for enabling multi-tenancy.

Prerequisites

- The VMware Identity Manager global environment version should be 3.3.2 or later.

- Verify if the inventories are synchronized for all the environments in vRealize Suite Lifecycle Manager and all environments and products are up to date. This is to discover all the VMware Identity Manager-product integrations required for VMware Identity Manager re-register.
- Verify if the VMware Identity Manager global environment certificate is managed through the vRealize Suite Lifecycle Manager Locker service.
- Ensure to take a snapshot of VMware Identity Manager. It is recommended, since enabling multi-tenancy transforms VMware Identity Manager to be accessed through tenant FQDNs and existing VMware Identity Manager URLs will not be accessible.
- For a clustered VMware Identity Manager, verify VMware Identity Manager cluster health status is green by triggering cluster health. For more information, [Day 2 Operations with Other Products In vRealize Suite Lifecycle Manager](#)
- Verify the VMware Identity Manager certificate is updated with the primary tenant alias FQDN. Also ensure that the A-type DNS record is added mapping the primary tenant alias FQDN. For more information about Mandatory Certificate and DNS requirements, see [Multi-Tenancy Model](#).

Procedure

- 1 Click **Identity and Tenant Management** and navigate to **Tenant Management**.
- 2 Read the Opt-in message and click **Enable Tenancy**.
- 3 Enter the primary tenant Alias name.

Ensure such a hostname or FQDN does not already exist. While enabling multi-tenancy, this FQDN is assigned to the primary tenant.

Ensure all products currently integrated with global environment VMware Identity Manager are already listed and selected for re-registration against the new primary tenant alias FQDN in the 'Product Re-registration' table. For more information on Product References, see [Product References](#).

- 4 Click **Submit**, after you validate the entries.

After you enable multi-tenancy on the VMware Identity Manager, it can only be accessed through its tenant FQDNs, and at this point as the primary tenant is the only available tenant, primary tenant alias FQDN is the only endpoint through which VMware Identity Manager can be accessed. Once the vRealize Suite Lifecycle Manager enable multi-tenancy request is completed, create tenants from the **Tenant Management** tab.

Tenant Management

This section describes all the tenant management functionalities available for vRealize Suite Lifecycle Manager.

While you are managing your tenants, you can add, delete, search and manage your tenants also.

Add Tenants

Add Tenant allows you to add tenants to VMware Identity Manager along with creating a tenant admin and optionally add directories to the created tenant and associate tenant-aware products to the newly created tenant.

When you add a tenant, the workflow also contains a pre-check step which validates all the given inputs and selected environments to make sure tenant creation and product associations work seamlessly.

Prerequisites

- Verify that you have DNS configured in both vRealize Automation and VMware Identity Manager. To access a tenant, the DNS server must be configured correctly before starting the vRealize Suite Lifecycle Manager flow 'Add Tenant' flow.
- Ensure that the A-type DNS record is added for the new tenant FQDN. For a multi-SAN environment, ensure that VMware Identity Manager certificate is updated with the new tenant FQDN that is to be created. For more details, see [Multi-Tenancy Model](#). For all the vRealize Automation instances that are to be associated with the new tenant ensure that the CNAME type DNS records are added and certificate requirements are met.
- For all the vRealize Automation instances that are to be associated with the new tenant ensure that the CNAME type DNS records are added and certificate requirements are entered.

Procedure

- 1 On the My Services dashboard, click **Identity and Tenant Management**.
- 2 Navigate to Tenant Management, click **ADD TENANT**.
- 3 Enter a tenant name and under the Administrator Details, enter **Username, First Name, Last name, Email ID**, and **Password** of the Tenant Admin.
- 4 Click **Next**.
- 5 (Optional) On the Directory Details tab, choose the directories from primary tenant that are to be migrated to the new tenant being created.

You can find the existing directory names listed in the directory column.

- 6 You can select any directories and click **Next**.
 - a Opt-in for migrate directories lists all the existing directories from the primary tenant. Only AD Over LDAP and AD with IWA directories is listed.
 - b To migrate, select the directories.
 - c Enter the passwords that are required for validation
 - d Click **Validate**. Once validation is successful, click **Save and Next**.

- 7 Select the products that should be associated with the new tenant. For vRealize Suite Lifecycle Manager 8.1 and later releases, vRealize Automation 8.1 and later releases can be listed.

Note Verify that you have considered the recommendation given for both certificate and DNS.

- 8 Click **Save** and **Next**.
- 9 Click **Run a Precheck** to validate the tenant details and certificate details.
 - Tenant Name validation Check – To validate the entered tenant name matches criteria.
 - Tenant Name Existence Check – To validate a tenant already exists.
 - VMware Identity Manager Tenant FQDN Reachability and Resolvability Check
 - VMware Identity Manager Tenant FQDN Certificate Check
 - vRealize Automation Tenant FQDN Reachability and Resolvability Check
 - vRealize Automation Tenant FQDN Certificate Check
 - a If the validations are not successful and if you want to make some changes, and resume the tenant creation operation, click **Save and Exit**. The same wizard can be opened anytime to re-run the precheck to complete and proceed.
 - b If the pre-check validations are green, click **Save and Next**. A summary of the whole selection appears.
- 10 Click **Next** and **Create Tenant** changes after reading the summary.

You can view the tenant creation under the **Request Details** page. Both VMware Identity Manager and vRealize Automation tenants can be accessed through its tenant FQDNs. For more information, see [Tenant Management in vRealize Suite Lifecycle Manager](#). You can log in to both VMware Identity Manager tenant FQDN and vRealize Automation tenant FQDN with the tenant admin credentials. The VMware Identity Manager tenant admin is also made the organization owner in new tenant vRealize Automation.

Delete a Tenant

Delete tenant operation deletes the tenant from VMware Identity Manager including the resources created under that tenant. As of vRealize Suite Lifecycle Manager 8.1, delete tenant option is only available for a tenant if there are no product associations.

Managing Tenants on Day 2

This section describes the Day 2 operations of a tenant. All operations that are available in the 'Add Tenant' wizard are available as an individual day-2 operation.

Manage Tenant Admins

When tenants are first created, only one local VMware Identity Manager user is created and that user is given tenant admin permissions. You can add and manage tenants admin at later stage when required.

Manage Tenant Admins - Add Tenant Admins

This option is used to add a new local user in VMware Identity Manager and assign tenant admin permission to that user.

- 1 Navigate to **Identity and Tenant Management** service and click **Tenant Management**.
- 2 To add an admin, select the tenant.
- 3 Click **ADD TENANT ADMIN**. The create tenant admin page loads
- 4 Enter the details for the new tenant admin and click **Create Tenant Admin**.

After you submit, a request is created that can be tracked for completion and user is listed in the tenant admin list.

Manage Tenant Admins - Search and Assign

This option is used when there are users already present in the VMware Identity Manager under the concerned tenant and requires tenant admin permission. The search can find both local VMware Identity Manager users and Active Directory Users that are synced in the concerned tenant. Multiple users can be searched and assigned with tenant admin permission. To search users.

- 1 Navigate to **Identity and Tenant Management** service and click **Tenant Management**.
- 2 To add an admin, select the tenant.
- 3 Click **SEARCH AND ASSIGN**.
- 4 When all the users are selected, click **Assign Tenant Admin**.

After you submit, a request is created that can be tracked for completion and user is listed in the tenant admin list

Associate Products

When the tenants are created, as a day-2 operation at any point, you can associate more products. For vRealize Suite Lifecycle Manager 8.1 and later releases, only vRealize Automation 8.1 and later releases can be associated. Product Associations lists the current products that are associated with the tenant. To add more association, click **Add Product Association**. Select the product and check the recommendations given. For vRealize Automation 8.x, ensure that the Certificate and DNS requirements are entered. Select the tenant admins from the list available. The tenant admin is made the organization owner for the new tenant vRealize Automation. Run pre-check to validate your entries and click **Submit**. Once the request completes, the associated product is listed under the **Product Association** list.

Migrate Directories

Migrate directories day-2 is similar to the **Add Tenant** wizard. The directories tab inside the tenant view lists the current directories that are present in the tenant.

Note These directories are read-only. vRealize Suite Lifecycle Manager does not allow complete directory management for subtenant directories. Directory management is only available for directories present in the primary tenant.

When you click **Add Directories**, all the directories from the primary tenant are retrieved. Select directories that are to be migrated, validate them, and then submit.

Using Tenant Migration

Tenant Migration is introduced to migrate tenants and specific tenant data for VMware Identity Manager (now renamed as VMware Workspace ONE Access) using vRealize Suite Lifecycle Manager.

Tenant Migration is supported for vRealize Suite Lifecycle Manager 8.2 Patch 1 and later releases. It involves close coordination between VMware Identity Manager, vRealize Suite Lifecycle Manager, and vRealize Automation.

vRealize Suite Lifecycle Manager migrates the following data of VMware Identity Manager for vRealize Automation 7 environment to Global Environment of VMware Identity Manager version 3.3.3 and later releases:

- Tenants
- Directories
- Custom groups
- Roles and rule set
- User attributes
- Access policies
- Network ranges
- Third-party IDP configurations

Migrating VMware Identity Manager

Using vRealize Suite Lifecycle Manager, you can migrate VMware Identity Manager.

Prerequisites

- The SMTP information of the source tenant must be configured on the Global Environment of VMware Identity Manager. This information is required to receive email instructions to reset the password for all local users. Prior to tenant migration, all local users in the source tenant must have valid email IDs.
- For migration, you must enable remote connection from the Global Environment of VMware Identity Manager to the vRealize Automation 7.x database. Refer to [KB 81219](#) for more information on enabling remote connection.
- Ensure that you have DNS configured in vRealize Automation and VMware Identity Manager.
- Ensure that the source vRealize Automation 7.x environment is in a healthy state and directories are synced before tenant migration.

Procedure

- 1 On the My Services dashboard of vRealize Suite Lifecycle Manager, click **Identity and Tenant Management**.
- 2 Select **Tenant Management**, and then click **Tenant Migrations**.
- 3 Read the information on VMware Identity Manager Tenant Migration and vRealize Automation Tenant Mapping, and then click **Continue**.
- 4 On the Environment Selection tab, select the **Source Environment** and **Target Environment**.

Based on your source and the target environment selection, you can view a tabular representation of the available tenants on the source vRealize Automation. You can also view the status of the migrated or merged tenants on the vRealize Automation 8 environment.

- 5 Click **Next**.
- 6 On the Tenant Migration Workflow page, you can view the workflow of Tenant Migration and Tenant Merge, and understand the correlation between the two operations.

vRealize Suite Lifecycle Manager also creates 7.x endpoint when adding a new tenant on vRealize Automation 8 environment. In Tenant Merge, the directories and tenants are already created on the source vRealize Automation 8 environment. vRealize Suite Lifecycle Manager creates the 7.x endpoint to the existing tenants on vRealize Automation 8 environment, so that you can migrate the business groups, infrastructure, and other specific tenants on vRealize Automation.

- 7 Click **SAVE AND NEXT** and read the list of manual steps which must be performed to proceed with the migration. Select the check box to confirm that you have read and verified the prerequisites and limitations.
- 8 To specify the Tenant Migration Workflow, enter these details on the Tenant Details tab.

- a Select the **Source Tenant**.

The source tenants listed are not the migrated or merged tenants.

- b Enter the **Tenant Name**.

- c Under Target Tenant administrator details, enter the **Target Tenant Username, First Name, Last Name**, valid **Email ID**, and **Password**.

Note To migrate a directory is a one-time operation, select all the directories which must be migrated. If the required directories are not selected during migration, you have to perform this operation manually.

- d Click **SAVE AND NEXT**.

- 9 To specify a directory that must be migrated from the source vRealize Automation 7 version to vRealize Automation 8 version tenant, select one of these directories on the Directory Migration tab.

- System Directory: Connector selection and password creation are not required.

- JIT directory: Connector selection and password creation are not required.
- Active Directory over LDAP: Select a Windows or Linux target Connector and enter the Bind Password.
- OpenLDAP: Select a Windows or Linux target Connector and enter the Bind Password.
- Active Directory with IWA: You can only select a Windows target Connector for the VMware Identity Manager 3.3.3 version. Enter the **Bind Password** and **Domain Admin Password** that is required for migration.

Note To migrate a directory is a one-time operation, select all the directories which must be migrated. If the required directories are not selected during migration, you have to perform this operation manually.

- 10 Click **Validate**. After a successful validation, click **SAVE AND NEXT**.
- 11 Click **Run Precheck** to validate the tenant details and certificate details. Click **SAVE AND NEXT**.
- 12 On the Summary Step tab, you can view the summary of your selections.
- 13 Click **SUBMIT** if your validations are successful.

If the validations are not successful and you want to make changes, and then resume the tenant migration operation, click **SAVE AND EXIT**. The same wizard can be opened anytime to rerun the precheck to proceed.

You can view the tenant migration details under the Request Details page. Both VMware Identity Manager and vRealize Automation tenants can be accessed through its tenant FQDNs.

Merging Tenants

In the Tenant Merge operation, the directories and tenants are already created on the target vRealize Automation 8 environment.

vRealize Suite Lifecycle Manager creates the vRealize Automation 7.x endpoints to the existing tenants on vRealize Automation 8 environment. You can migrate the business groups, infrastructure, and other specific tenants on vRealize Automation.

Prerequisites

- vRealize Automation 8.1 did not require you to accept a source certificate during migration assessment. To merge or manage the tenant using vRealize Suite Lifecycle Manager, you can delete the manually added source environment from vRealize Automation.
- Ensure that the VMware Identity Manager specific data is migrated to the target data in the Global Environment.

Procedure

- 1 On the My Services dashboard of vRealize Suite Lifecycle Manager, click **Identity and Tenant Management**.

- 2 Select **Tenant Management**, and then click **Tenant Migrations**.
- 3 Read the information on VMware Identity Manager Tenant Migration and vRealize Automation Tenant Mapping, and then click **Continue**.
- 4 On the Environment Selection tab, select the **Source Environment** and **Target Environment**.
Based on your source and the target environment selection, you can view a tabular representation of the available tenants on the source vRealize Automation. You can also view the status of the migrated or merged tenants on vRealize Automation 8 environment.
- 5 Click **Next** and on the Tenant Migration Workflow page, you can view the workflow of Tenant Migration and Tenant Merge.
- 6 On the Merge Details tab, you can select one or multiple tenant mappings for vRealize Automation 7.x and merge it with the same or different destination tenants for vRealize Automation 8.x.
If you cannot view the target tenant, perform an inventory sync, or perform a product association for the tenant.
- 7 Click **Next** and you can view the summary of your selections on the Summary Step tab.
- 8 Click **SUBMIT** if your validations are successful.

Note If the validations are not successful and you want to make changes, and then resume the tenant merge operation, click **SAVE AND EXIT**. The same wizard can be opened anytime to rerun the precheck to proceed.

Configure Certificate Within Locker

You can generate a new certificate for products that are deployed in vRealize Suite Lifecycle Manager.

Prerequisites

- Certificates that are about to expire in less than 15 days cannot be imported.
- To manage the certificate for an imported environment, add the certificate in the vRealize Suite Lifecycle Manager and perform inventory sync so that the certificate is mapped to the imported environment, after which replace certificate and scale-out wizards will be aware of the existing certificate.

Procedure

- 1 To add a certificate, navigate to **Lifecycle Manager > Locker**.

2 You can either select Generate Certificate or Import Certificate.

Option	Description
Generate	<ol style="list-style-type: none"> Enter the required text boxes. Select the length of the Key. Enter the valid Server Domain/Hostname. You can also include the Wildcard certificate. For example, you can enter *.sql.local. Enter the FQDN or IP Address. Click Generate.
Import Certificate	<ol style="list-style-type: none"> Enter a valid certificate name. In the Passphrase text box, type <Cert-Password> (if applicable). Click Browse File and browse to the saved PEM file. When you upload a PEM file, the private key and certificate chain details are populated automatically. Enter the private key and certificate chain details manually. Click Import. <p>The requirements for PEM file are:</p> <ul style="list-style-type: none"> ■ Both certificate chain and key must be in the same file. ■ The PEM file that are imported can have 2048 bits key or 4096 bits key. ■ If the PEM file certificate is encrypted then the passphrase must be provided while importing the certificate into vRealize Suite Lifecycle Manager.
Generate CSR	<ol style="list-style-type: none"> Enter the required text boxes. Select the length of the key. Enter a valid domain name. You can also include the Wildcard certificate. For example, you can enter *.sql.local. Enter the IP address in which you are assigning the certificate. <p>Note Generate CSR downloads a PEM file. This file can be taken to the certificate authority for signing and can be made as a trusted certificate. The pem file downloaded will have the private key and certificate request chain. You must be cautious and share only the CSR part of the pem file but not the key for the certificate signing.</p>

3 Click **Generate**.

4 You can click the certificate from the inventory to view the details and its associated environments with their products.

5 To download or replace the certificate, click the vertical ellipses on the certificate.

Results

vRealize Suite Lifecycle Manager generates a new certificate for the specific domain provided by the user.

Configure License Within Locker

Locker is an application like Lifecycle Manager which helps to manage the Certificate, Passwords, and Licenses from single pane. You can configure licenses at the locker level.

Prerequisites

Verify that a license is already available.

Procedure

- 1 Navigate to the **Lifecycle Operations** dashboard, click **Locker**.
- 2 On the left, click the **License** icon.
- 3 To add a license, click **ADD**.
- 4 Enter the alias in the **License Alias** text box.
- 5 Enter the **License Key** and click **Validate**.
- 6 After you validate the accuracy of the license, click **Add**.
- 7 To replace an existing license, click any license from the license table.
 - a Click the vertical ellipses and click **Replace**.
 - b Read the current license summary and click **Next**.
 - c Select an environment from the references table and click **Next**.
 - d Select a license from the drop-down menu and click **Finish**.
- 8 To delete a license, click the vertical ellipses and click **Delete**.
 - a If the Lifecycle Manager is having one or more My VMware accounts configured, then the corresponding license keys are automatically synced. To sync licenses from My VMware account, click REFRESH. However, if you have manually added the same license key to the locker then the corresponding entry from My VMware account cannot be captured.
 - b When any product is imported into vRealize Suite Lifecycle Manager, the license keys present in the product is also captured and stored in the Locker under Licenses. If the same license key is already present, then it cannot be imported.
 - c License keys can be applied to products managed by vRealize Suite Lifecycle Manager from **Home > Environments** under Lifecycle Operations. Select a product from any Lifecycle Operations managed environment, click the horizontal ellipses on the product name and select **Add License**, and follow the steps.
 - d If any product is associated to a license in vRealize Suite Lifecycle Manager then the license entry cannot be deleted from the locker.
 - e vRealize Suite Lifecycle Manager does not restrict applying multiple licenses to any product, however, the product behavior does allow to set only one license key as active at anytime.

- f License deletion from vRealize Suite Lifecycle Manager locker does not remove the license key from the product itself.

Managing vRealize Cloud Licenses in Locker

Starting with vRealize Suite Lifecycle Manager 8.2, the Locker application helps you to manage vRealize Cloud licenses for your vRealize Cloud Subscription and collect your daily data usage for the associated products and cloud services.

When you purchase vRealize Cloud Subscription, you receive access to vRealize Cloud Subscription Manager, which is a new complimentary utility service. With vRealize Cloud Subscription Manager, you can add endpoints and monitor the data usage for your vRealize Cloud Subscription services. You must create vRealize Cloud licenses at the locker level in vRealize Suite Lifecycle Manager, and then connect these licenses to vRealize Cloud Subscription Manager to monitor your cloud data usage. For more information on vRealize Cloud Subscription Manager, refer to the [vRealize Cloud Subscription Manager documentation](#).

Prerequisites

Verify if you have registered with My VMware to access licenses.

Procedure

- 1 If you do not have My VMware account, navigate to the Lifecycle Operations dashboard, and then click **Settings**.
- 2 Click **My VMware** and add a vRealize Cloud account.
- 3 After your My VMware accounts are configured, then the corresponding license keys are synced.
- 4 From the Lifecycle Operations dashboard, click **Locker**.
- 5 Click the **License** icon.
- 6 The vRealize Cloud licenses are created under My VMware account and are displayed as **vRealizeFlex** license type in the Licenses table.
- 7 To sync licenses from My VMware account, click **Retrieve Licenses**.
- 8 To connect a license to vRealize Cloud Subscription, select a license which is displayed in the License table, and then right-click the vertical ellipses.
 - a Click **Connect License**.
 - b Under API Token, generate an API token from your user account for vRealize Cloud Subscription, and then click **Next**.
 - c Under Match License Key, the vRealize Cloud Subscription Manager finds a correct match for the provided API token, and lists out the organization details.
 - d Under Report Frequency, you will receive a confirmation that you are connected to vRealize Cloud Subscription Manager, and your data usage is reported to vRealize Cloud Subscription Manager twice a day.

- e Click **Finish**.
- 9 To disconnect a license in vRealize Suite Lifecycle Manager, right-click the vertical ellipses, and then click **Disconnect License**.
- 10 To trigger the license usage for a product, select a license from the License table, and then right-click the vertical ellipses.
 - a Click **Sync Usage**.
 - b You can download the usage sync report to view the data usage for the products.
- 11 To view the data consumption report, select a license, and then right-click the vertical ellipses.
 - a Click **Generate Report**.
 - b To view a graphical representation of the report, click **GENERATE** in the Generate Report page.
 - c To download the report for a maximum period of 120 days, click **DOWNLOAD**.
- 12 To track your data usage for a product, right-click the vertical ellipses for a selected license, and then click **Import Allocation**. The Import Allocation is a unique license metadata file which helps you to view the details of data usage for an associated product in the License Details page.

Configure Your Password Within Locker

Locker in vRealize Suite Lifecycle Manager 8.0 stores all the passwords that are used across the vRealize Suite Lifecycle Manager. Add the passwords for adding vCenter Server, product deployments, products import, My VMware, and Product Password Update. You can configure a password at the locker level and are retrieved from the UI.

Procedure

- 1 Navigate to Lifecycle Operations, on My Services dashboard, click **Locker**.
- 2 On the left panel, click the key icon.
- 3 To add a Password, click **ADD**.
- 4 Enter the **Password Alias** and **Password**.
- 5 To confirm, re-enter the Password and enter **Password Description**, and a valid **User Name**.

Note The user name text box is mandatory for adding the vCenter server into vRealize Suite Lifecycle Manager.

- 6 Click **Add**.

Password Management Within Locker

Starting with vRealize Suite Lifecycle Manager 8.2, you can manage passwords that are stored at the Locker level for vCenter servers, products, and My VMware.

You can add a new password on the Passwords page under Locker. Click **Add** and enter the alias and password details to add a new password.

For the existing passwords on the Passwords page, click the ellipsis (...), and then select one of the following options:

Functionality	Description
View Password	You can view the selected password in plain text if you are an Admin user, after you authenticate the vRealize Suite Lifecycle Manager SSH root password. The view password is not available for the VMware Identity Manager users.
Copy ID	You can copy the password ID and reuse the password. For example, when exporting JSON for product deployment, you can copy and reuse the existing password ID.
Edit Password	You can edit a password that does not have a reference to an existing password. For example, if you use a password in an environment, such as vCenter server or MyVMware, the edit password option for that password is disabled.
Delete Password	You can delete a password that is no longer used and does not have any references. For example, if you use a password in an environment, such as vCenter server or MyVMware, the delete password option for that password is disabled.

If you select an existing password, you can view the password details and the references for the selected password. The **Details** tab displays the password identifier, username, password description, password creation and last updated dates for the selected password. The **References** tab displays the references for environments at the product and node level, vCenter passwords in data centers, and other passwords that are used in the **Settings** tab.

You can also update a password for products, nodes, MyVMware, proxy, and vCenter servers. To update the password, click the vertical ellipsis (⋮) for the selected password.

Note

- When you update a password that is managed by vRealize Suite Lifecycle Manager, such as products, nodes, or root user, the password is updated on the Passwords page and the vRealize Suite Lifecycle Manager inventory.
- When you update a password for vCenter, MyVMware, proxy, or VMware Identity Manager configuration administrators, the password is updated only in the vRealize Suite Lifecycle Manager inventory.

Add a Data Center to vRealize Suite Lifecycle Manager

You can add a data center to vRealize Suite Lifecycle Manager to back up your private cloud environments.

Procedure

- 1 On the left pane, click **Data Centers** and click **Manage Data Centers**.

You can see all the data centers with its products that are associated with them. You can also click the product icons that directs you to the view details page of that particular product.

- 2 Click **+ Add Data Center**.
- 3 Enter the **Data Center Name** and provide a **Location** even if the location is not available in the drop-down menu.
- 4 Click **ADD**.
- 5 To delete a datacenter, select the delete icon.

Note If there is any INITIATED, IN PROGRESS or COMPLETED requests for an environment, then you cannot delete a data center. If it has a FAILED request, or request related to vCenter, such requests are archived.

What to do next

Add a vCenter to the data center. See [Add a vCenter to a Data Center](#).

Creating Roles for Specific Access

In vRealize Suite Lifecycle Manager, you can delegate the certificate replacement operations to any users in a consistent manner across VMware suite products.

With this accessibility, you can also allow non-admin users to perform actions like replace the certificate.

Assign Roles for Certificate Operations

With this section, you can create a certificate admin who is a user or a group with a specific role assigned. These users or group of users can have certain privileges to access the certificate for any vRealize Product.

Prerequisites

- Verify that there are users or group of users available and such users should not have any prior roles mapped.

Procedure

- 1 On the Lifecycle Operations, click **User Management**.
- 2 Navigate to User Management, click **ADD USER/GROUP**.
- 3 Enter a user or a group name and the user list is auto-populated.

If a user already has a role mapped from the selected user, then select another user.

- 4 Click **Next**.

- 5 Select the **Certificate Administrator** role and click **Next**.
- 6 Click **Submit**.
- 7 Log out from vRealize Suite Lifecycle Manager and log in as VMware Identity Manager user to access the services as an assigned admin.

Change Certificate for vRealize Suite Lifecycle Manager

As an vRealize Suite Lifecycle Manager admin, you can change your certificate for your vRealize Suite Lifecycle Manager instance.

Prerequisites

Verify that you have an existing vRealize Suite Lifecycle Manager certificate available.

Procedure

- 1 On the My Services dashboard, click Lifecycle Operations.
- 2 Navigate to Settings and click **Change Certificate**.
You can view the certificate details that are used by the vRealize Suite Lifecycle Manager.
- 3 To replace the certificate, click **REPLACE CERTIFICATE**.
 - a Read the summary of the current certificate and click **Next**.
 - b Select a certificate from the drop-down menu and click **Next**.
 - c Click **Run Precheck** to validate your certificate details and click **Finish**.
- 4 After you click Finish, you can view the progress of the certificate changing on the **Request Details** page.

Replace Certificate for vRealize Suite Lifecycle Manager

If you use the custom certificate for vRealize Suite Lifecycle Manager instead of default self-signed certificate, you replace the vRealize Suite Lifecycle Manager certificate.

Prerequisites

- A X509 PEM base-64 encoded certificate and private key. Make sure the private key is not encrypted.
- A machine with an SSH access to vRealize Suite Lifecycle Manager, and software such as PuTTY and an SCP software such as WinSCP installed on it.

Procedure

- 1 Rename the certificate to server.crt and private key to server.key.
- 2 Open a Secure Shell connection vRealize Suite Lifecycle Manager appliance as root user.

- 3 Copy the certificate files `server.crt` and `server.key` to the `/opt/vmware/vlcm/cert` folder. You can use an SCP software like WinSCP on Windows. Make sure to backup the original files before copying.
- 4 After copying the certificates, restart the vRealize Suite Lifecycle Manager proxy services to update the appliance certificate.
 - a Restart the system services by executing the following command in the SSH session:
`systemctl restart nginx.`
 - b Check the status of the system services by executing the following command in the SSH session: `systemctl status nginx.`
- 5 After restarting the services, verify that the certificate is updated on the appliance, open a browser and go to `https://<lcm-server-host>`.
- 6 Verify that you see the new certificate in the browser.

Federal Information Processing Standard 140-2 Support

VMware vRealize Suite Lifecycle Manager 8.2 supports Federal Information Processing Standard (FIPS) 140-2. FIPS 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules.

FIPS Compliance is a new and secured opt-in mode adhering to the Enterprise Readiness Initiatives (ERI) in VMware vRealize Suite Lifecycle Manager. To learn more about support for FIPS 140-2 in VMware products, see [FIPS Security Policies and Certifications](#).

Enable or Disable FIPS Mode Compliance in vRealize Suite Lifecycle Manager

You can enable FIPS Mode Compliance using Easy Installer during vRealize Suite Lifecycle Manager installation or by selecting the option as a Day-2 operation in the Settings page. To know more about FIPS Mode Compliance using Easy Installer, see *vRealize Automation documentation*.

Procedure

- 1 From My Service dashboard, select Lifecycle Operations, and then select the Settings page.
- 2 Under System Administration, click **System Details**.
- 3 Enable or disable the FIPS Mode Compliance check box, as required. Click **Update**. vRealize Suite Lifecycle Manager restarts when you enable or disable FIPS Mode Compliance.

Note When you enable FIPS Mode Compliance, vRealize Suite Lifecycle Manager 8.2 does not upgrade to the next version. You must disable the FIPS Mode Compliance, and upgrade vRealize Suite Lifecycle Manager 8.2, and then re-enable FIPS Mode Compliance.

vRealize Suite Lifecycle Manager on VMware Cloud on AWS Environment

Starting with 8.2, vRealize Suite Lifecycle Manager supports VMware Cloud (VMC) on AWS environment. VMC on AWS is an integrated private cloud offering developed by VMware and Amazon Web Services (AWS). vRealize Suite Lifecycle Manager 8.2 supports M11 and M12 versions of VMC.

You can install vRealize Suite Lifecycle Manager on a VMC environment using Easy Installer. For more information, refer to the [Easy Installer](#) documentation. Configure a virtual machine on the vCenter of a VMC software-defined data center (SDDC) to launch the Easy Installer. To create cloud SDDC using VMC on AWS and to connect SDDC to the data center of your product, refer to the [Getting Started with VMware Cloud on AWS](#) documentation. After you have successfully deployed vRealize Suite Lifecycle Manager on VMC, you can also install other VMware vRealize Suite products, such as VMware Identity Manager and vRealize Automation on the VMC environment to perform the Day 2 operations.

On a VMC environment, you must add the SDDC vCenter as an endpoint only. Adding any vCenter external to the SDDC is not recommended. When you deploy a VMC vCenter, ensure that you have cloud administrator privileges. To learn more about cloud administrator privileges, refer to [CloudAdmin Privileges](#) documentation.

Upgrading Your Product

2

This topic describes how to upgrade your vRealize Suite products and vRealize Suite Lifecycle Manager when you are having an older version.

When you want to upgrade from an older version of vRealize Suite Lifecycle Manager to 8.2, you have three steps.

- Upgrade of vRealize Suite Lifecycle Manager
- Upgrade of VMware Identity Manager
- Upgrade of vRealize Automation 8.x

When you want to upgrade your individual products after installing vRealize Suite Lifecycle Manager 8.x or earlier versions.

- All products supported by vRealize Suite Lifecycle Manager.

This chapter includes the following topics:

- [Upgrade vRealize Suite Lifecycle Manager 8.x](#)
- [Upgrade VMware Identity Manager](#)
- [Upgrade vRealize Automation 8.x with vRealize Suite Lifecycle Manager](#)
- [Upgrade a vRealize Suite Product](#)

Upgrade vRealize Suite Lifecycle Manager 8.x

You can check for and install updates to the vRealize Suite Lifecycle Manager appliance.

Upgrade is supported from vRealize Suite Lifecycle Manager 8.0 and later versions. You can also upgrade vRealize Suite Lifecycle Manager by using an ISO file to install the upgrade. Latencies have been validated with 350 ms with a bandwidth of 1.5 MB for a vRealize Suite small suite deployment and upgrade.

Prerequisites

- Verify that you meet the system requirements. See [System Requirements](#).
- Take a snapshot of the vRealize Suite Lifecycle Manager virtual appliance. If you encounter any problems during upgrade, you can revert to this snapshot.

- Verify that no critical tasks are currently in progress in vRealize Suite Lifecycle Manager. The upgrade process stops and starts vRealize Suite Lifecycle Manager services and reboots the vRealize Suite Lifecycle Manager virtual appliance, which might corrupt tasks that are in progress.

Procedure

- 1 From the My services dashboard, click **Lifecycle Operations** and click **Settings**.
- 2 Click **System Upgrade**.

vRealize Suite Lifecycle Manager displays the name, version number, and vendor of the current vRealize Suite Lifecycle Manager appliance.

- 3 Select the repository type for vRealize Suite Lifecycle Manager updates.

Option	Description
Check Online	You can check if the upgrades are available online. To use this option, the vRealize Suite Lifecycle Manager virtual appliance must have access to vapp-updates.vmware.com.
URL	Enter your repository URL for updates. To use this option, extract the ISO containing the upgrade files to a private repository. Do not use a private repository that requires authentication for a file access.
CD-ROM	You can update the vRealize Suite Lifecycle Manager Appliance from an ISO file that the appliance reads from the virtual CD-ROM drive.

- 4 Click **CHECK FOR UPGRADE**.

After few minutes, vRealize Suite Lifecycle Manager displays a message indicating whether there are updates available.

- 5 Select the upgrades to install, and click **INSTALL UPGRADES**.
 - a When vRealize Suite Lifecycle Manager is not connected to the internet, you can download the "vRealize Suite Lifecycle Manager Update Repository Archive" binary from My VMware Portal.
 - b The downloaded ISO should be attached to vRealize Suite Lifecycle Manager VM's virtual CD-ROM drive. To do this, you can either upload the ISO in a content library of the vCenter server hosting vRealize Suite Lifecycle Manager or you can upload in a datastore that the vRealize Suite Lifecycle Manager VM can access. After uploading, you must attach the ISO to the vRealize Suite Lifecycle Manager VM's CD-ROM device by editing the VM's hardware configuration from the vCenter inventory. From vRealize Suite Lifecycle Manager UI, select CD-ROM based upgrade option and proceed.
- 6 After a few minutes, login to the vRealize Suite Lifecycle Manager UI and check for the upgrade successful message in the **Settings > System Upgrade**.

On an upgrade completion, vRealize Suite Lifecycle Manager displays the message upgrade completion message. If you do not see this message, wait for a few minutes and refresh the UI.

Support for Additional Product Versions

This section covers information about enabling applicable product versions for the vRealize Suite products while you are updating the LCM appliance. You can add additional Policy support and enhance the new product versions and add patches to vRealize Suite Lifecycle Manager as and when applicable.

With the check version feature, you can check the latest available product versions even without web connectivity. The table with the versions of the product of each vRealize Suite is pre-populated wherein the data is fetched from the VMware source.

If the selected upgraded product version does not work, then navigate to the downloaded product file with a file extension `.pspak`. Upload the file and validate the same using Chrome or Internet Explorer.

Upgrade VMware Identity Manager

Upgrade support from earlier versions of VMware Identity Manager to the latest is only available if they conform to vRealize Suite Lifecycle Manager supported form-factor. Otherwise, the upgrade has to be performed outside vRealize Suite Lifecycle Manager. After upgrade, it can anytime be reimported by triggering Inventory Sync in vRealize Suite Lifecycle Manager. For more information, see *Installing vRealize Automation with Easy Installer*.

Note

- To know more about VMware Identity Manager version 3.3.2 that is available for upgrade, see [VMware Identity Manager release notes](#).
 - VMware Identity Manager version 3.3.3 is backward compatible with Windows connectors of previous versions.
-

Prerequisites

- Verify that you have taken a snapshot of VMware Identity Manager nodes.
- Verify that you have your product binaries mapped. For more information, see [Configure Product Binaries](#).
- For a clustered VMware Identity Manager upgrade, ensure to disable all the stand-by nodes in the load-balancer so that the traffic is not routed to the stand-by nodes and enable them back once the upgrade is completed.

Procedure

- 1 On the Lifecycle Operations page, click **Manage Environment**.
- 2 Navigate to the **Global Environment** instance.
- 3 Click **View Details > Upgrade**.

- 4 Under the Product details section, you can select the following repository type.

Option	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in the Lifecycle virtual appliance.
vRealize Suite Lifecycle Repository	When you select this option, you can enter the upgrade path available after mapping the binaries through LCM. Note For VMware Identity Manager version 3.3.3, the only option available is vRealize Suite Lifecycle Repository . The other options, Repository URL and VMware Repository are not available.
VMware Repository	Select this option and select the version. The upgrade is performed using the online source.

- 5 Click and run the pre-check.

- 6 Click **Submit**.

Migrating Windows Connector

In Connector migration, the Windows connector for VMware Identity Manager is installed on a Windows box, by providing the configuration file which is generated from an external or embedded Linux connector. This is supported for vRealize Suite Lifecycle Manager 8.2 Patch 1 and later releases.

After the external or embedded Linux connector is migrated, the Integrated Windows Authentication (IWA) and LDAP directories on the Linux connector are migrated to Windows. In VMware Identity Manager version 3.3.2 and earlier releases, the active directories were supported on both external and embedded Linux connectors and external Windows connectors. Starting with VMware Identity Manager version 3.3.3, IWA active directories are supported only on external Windows connectors.

Prerequisites

Ensure that you adhere to the following requirements.

- The supported JRE version is between 8 update 181 to 8 update 251.
- The supported .NET framework version is 4.6.0.
- The supported Windows Server versions are 2012 R2, 2016, and 2019.
- A unique Windows system is required for the migration and it must be connected to a domain server.

Procedure

- 1 On the Lifecycle Operations page, click Manage Environment.
- 2 Navigate to the Global Environment instance.
- 3 Click **View Details > Upgrade**.

- 4 Select the check box and proceed to Upgrade.
- 5 In the Select Version tab, select the **Repository Type**, **Product Version**, and the **Repository URL**.
- 6 To specify the connector migration, enter the Target Windows Connector details in the Migrate Linux Connector to Windows Connection section.

Note The Source Connector details for Embedded Connector Type are populated from VMware Identity Manager. You must enter only the Linux Connector SSH passwords for the External Connector Type.

- a Enter the target **Windows FQDN** and **Windows Domain User**.
 - b Select the **Windows Domain Password**.
 - c Select the **Windows VM Center**.
- 7 Click and then **RUN PREHECK**.
If the validations are not successful and you want to make changes, and then resume the upgrade VMware Identity Manager operation, click **SAVE AND EXIT**.
- 8 If the validations are successful, click **Next**.
- 9 In the Upgrade Summary page, you can verify the details, and then click **Submit**.

Upgrade vRealize Automation 8.x with vRealize Suite Lifecycle Manager

You can upgrade vRealize Automation in vRealize Suite Lifecycle Manager.

Prerequisites

- Ensure that you have upgraded the earlier versions of vRealize Suite Lifecycle Manager to the latest. For more information on upgrading your vRealize Suite Lifecycle Manager, see [Upgrade vRealize Suite Lifecycle Manager 8.x](#).
- Ensure that you have upgraded the earlier version of VMware Identity Manager to 3.3.2. For more information on VMware Identity Manager upgrade, see [Upgrade VMware Identity Manager](#).
- Verify that you have already installed vRealize Automation 8.0, 8.0.1, or 8.1.
- Perform the binary mapping of the vRealize Automation upgrade ISO from Local, myvmware or NFS share. For more information on binary mapping, see [Configure Product Binaries](#).

- Increase the CPU, memory, and storage as per the system requirements of vRealize Automation 8.2. For more information, see the Hardware Requirements of [vRealize Automation 8.2 Reference Architecture](#).

Note When upgrading vRealize Automation in VMware Cloud Foundation environment, verify if your memory or RAM requirement is the latest target version.

Procedure

- 1 On the Lifecycle Operations page, click **Manage Environments**.
- 2 Navigate to a vRealize Automation instance.
- 3 Click **View Details** and click **Upgrade**.

A pop-up menu is appears to alert you to perform an inventory sync.

- 4 Click **Trigger Inventory Sync** of the product before you upgrade.

Note At times, there can be a drift or a change in the environment outside of Lifecycle Manager and for Lifecycle Manager to be aware of the current state of the system, the inventory requires to be up-to-date.

- a If the product inventory is already synced and up-to-date, then click **Proceed Upgrade**.
- 5 After the inventory is synced, select the vRealize Automation version to 8.2.
 - 6 To select the **Repository Type**, you can either select **vRealize Suite LCM Repository**, only if you have mapped the ISO Binary map, or you can select the **Repository URL** with a private upgrade Repository URL.
 - 7 If you selected the Repository URL, enter the unauthenticated URL, and then click **Next**.
 - 8 Click **Pre-Check**.

Pre-check validates the following criteria:

- If the source vRealize Automation versions are one of 8.0.0 or 8.0.1, ensure follow the steps given in the KB article [78325](#) before you upgrade to restore expired root accounts.
- SSH enabled - Verifies that SSH for the root user is enabled.
- Version check - Verifies if the target version selected for upgrade is compatible with the current vRealize Automation version.
- Disk space on root, data, and services log partition - Verifies if the required amount of free disk space is available in the root, data, and services log partition.
- CPU and Memory Check - Verifies if the required amount say 12 CPU and 40 GB Memory resources available in each vRealize Automation nodes before upgrade.

- vCenter property existence check - Verifies if the vCenter details are present as part of each node in the Lifecycle Manager inventory. Since a snapshot is taken during the upgrade process, it is important to have the right vCenter details within the Lifecycle Manager inventory.
- vRealize Automation VMs managed object reference ID retrieval check - Verifies if the managed object reference ID of the VM can be retrieved from the details available in the Lifecycle Manager inventory. This is required as you perform snapshot-related operations on the VMs, finding the VM using the same.

9 Click **Next** and **Submit**.

You can navigate to the Request Details page to view the progress of the upgrade status. You can enable the multi-tenancy for vRealize Automation, refer to [Tenant Management in vRealize Suite Lifecycle Manager](#).

Upgrade Functionality of vRealize Automation

There are three stages in the upgrade process of vRealize Automation within vRealize Suite Lifecycle Manager.

Stages of Upgrade	Description
Upgrade Preparation	The preparation phase verifies that the system is healthy and shuts down services to make sure that all data is persisted.
Snapshot of all the VMs for an automatic recovery	Snapshots are taken for faster recovery of failures. vRealize Suite Lifecycle Manager then shuts down the VMs, takes a snapshot, turns power on, and continues to the next phase.
Upgrade Execution.	Run the upgrade.

At certain unexpected or failure scenarios, the vRealize Suite Lifecycle Manager upgrade workflow gives user decision points to either finish the upgrade successfully or revert to the stage before upgrade.

- The upgrade process starts with a status check task that verifies the current state of the VA. If the system already has an upgrade request due to a previous upgrade attempt, then vRealize Suite Lifecycle Manager provides you with an option to clean the older states and start a new upgrade. You can see the status task failing with a retry parameter similar to 'cancelAndStartAfresh'. Setting this retry parameter to true cleans up older states and retriggers the upgrade again.
- If unexpected failures occur during the prepare phase, you can either cancel the whole upgrade process and start new. If a failure cannot be corrected or if the unexpected failure is fixed manually, you can proceed to the next phase in the upgrade workflow. The status selects done after the prepare failure provide you with two retry parameters that help you

decide which option to select. If you set 'cancelAndStartAfresh' to 'true', the upgrade process is cancelled and returns the system to the state before the upgrade. If you set 'proceedNext' to 'true', the vRealize Suite Lifecycle Manager upgrade workflow proceeds to the next state with an assumption that you fixed the prepare issue outside.

- The upgrade workflow consists of VM level operations like reverting or deleting a snapshot and VM Shutdown, power ON, and so on. If there was a failure, these operations include a **Skip** option which can be used if the RETRY option in the vRealize Suite Lifecycle Manager does not help and when you manually perform the same operation directly on the vCenter Server.
- The final phase of the upgrade can be successful or success with warnings or a fatal state.
 - Success with warnings indicates that the upgrade has completed successfully, but a minor error is detected. You can check the errors and rectify them. You can set the 'succeedUpgradeRequest' retry parameter to 'true' which will succeed and complete the vRealize Suite Lifecycle Manager upgrade workflow.
 - If there is an fatal error, you can decide if you want to revert the snapshot and retry the upgrade or cancel the whole upgrade process. You can revert and delete the snapshot, cancel the current upgrade request, and move the system to a state before the upgrade started.
 - For a fatal error, you can see the status task after the upgrade failure with retry parameters similar to 'revertSnapshotNRetryUpgrade' and 'cancelUpgradeNRevertBack'. If you set 'revertSnapshotNRetryUpgrade' to 'true', then it can revert the snapshot and retry the upgrade again.

- If you set 'cancelUpgradeNRevertBack' to 'true', you can cancel the upgrade process, which can revert and delete the snapshot and cancel the current upgrade request and move the system to a state before the upgrade started.

Note

- The vRealize Suite Lifecycle Manager upgrade workflow does not support removing the snapshots if there was a successful upgrade. You hold the snapshots or remove it manually from the vCenter Server, if necessary.
 - If you Cancel the upgrade process after a failure post prepare or upgrade phase, the vRealize Suite Lifecycle Manager workflow post cleaning up the upgrade request in vRealize Automation ends up in an canceled state. This indicates that the upgrade workflow from vRealize Suite Lifecycle Manager stopped. In such situations, retrigger an upgrade from the product actions under **Manager Environment** page.
 - You can enable the multi-tenancy for vRealize Automation, refer to [Tenant Management in vRealize Suite Lifecycle Manager](#).
 - If the vRealize Automation upgrade fails, you must cancel upgrade or revert a snapshot, and then retry to upgrade through vRealize Suite Lifecycle Manager. If you revert the snapshot manually in a vCenter Server, vRealize Automation goes into an inconsistent state.
 - For vRealize Automation, if you cancel upgrade or revert a snapshot, and then retry to upgrade, ensure that you create a support bundle that contains the log files for any future analysis and reference.
-

Upgrade a vRealize Suite Product

You can use vRealize Suite Lifecycle Manager to upgrade vRealize Suite product installations.

When a deployment request is saved in vRealize Suite Lifecycle Manager 1.1 and the same request is resumed after upgrading vRealize Suite Lifecycle Manager to 1.2, vRealize Automation 7.3 products details page items does not load. For more information, see KB article [56369](#). When a vRealize Suite Lifecycle Manager upgrade is triggered, the screen stays at Maintenance mode and **Home** page never comes up. After an upgrade, there can be some errors in the content from the marketplace. The content might contain few request that prevents the service to start. vRealize Suite Lifecycle Manager UI displays a maintenance mode message and the Home page is not displayed. In this scenario, restart the xenon server. If the issue still persists, delete the error request and restart xenon. To upgrade to vRealize Automation 8.x, see [Upgrade vRealize Automation 8.x with vRealize Suite Lifecycle Manager](#) .

Prerequisites

Verify that the vRealize Suite product to upgrade is part of a vRealize Suite Lifecycle Manager private cloud environment, and take a snapshot of the product that you can revert to in the event that something goes wrong with the upgrade. See [Create a Product Snapshot](#).

If you are upgrading vRealize Automation 7.x, ensure that the following additional prerequisites are met:

- The vRealize Automation management agent and all IaaS Windows nodes are running.
- The second member in the vRealize Automation load balancer is disabled.

If you are upgrading vRealize Automation 8.x, ensure that the following additional prerequisites are met:

- vRealize Suite Lifecycle Manager should be upgraded to latest.
- VMware Identity Manager should be upgraded to 3.3.2.
- The vRealize Automation services should be running.

Procedure

- 1 Click **Manage Environments**.
- 2 Click **VIEW DETAILS** for the environment the product to upgrade is part of.
- 3 Click the ellipses (...) icon next to the name of the product to upgrade and select **Upgrade** from the drop-down menu.
- 4 Choose a product version to upgrade to.
- 5 If you are upgrading vRealize Automation or vRealize Business for Cloud, choose whether to upgrade from the **Default** repository, the **vRealize Suite Lifecycle Manager Repository**, or a manually-entered **Repository URL**.
- 6 If you are upgrading vRealize Log Insight or vRealize Operations Manager, choose whether to upgrade from the **vRealize Suite Lifecycle Manager Repository**, or a manually-entered **Repository URL**.
- 7 Click **Upgrade**.

If you have upgraded a vRealize Suite product outside of vRealize Suite Lifecycle Manager, then vRealize Suite Lifecycle Manager will not reflect the latest product version or the latest data of the upgraded product. At such instances you have to delete the vRealize Suite product (the product which is already upgraded to the newer version outside vRealize Suite Lifecycle Manager) from vRealize Suite Lifecycle Manager only, and then re-import the same product again so that vRealize Suite Lifecycle Manager will fetch the latest state of the given product along with its newer version.

What to do next

You can view the progress of the upgrade on the **Requests** tab.

Upgrade Existing Products Using Pre-Upgrade Checker

You can trigger a pre-validation check from the product UI before upgrading an existing product within an environment. You can evaluate product upgrades and allow upgrade operation later. You can also validate the product compatibility matrix should be validated.

For more information on upgrade vRealize Suite products, see [Upgrade a vRealize Suite Product](#).

Prerequisites

Verify that you already have an existing vRealize Suite product in your environment.

Procedure

- 1 Right click the vertical ellipses of an existing vRealize Suite product and select an upgrade.

The compatibility matrix information is loaded with new, compatible and incompatible versions with product that needs to be upgraded.

- 2 Under the Product details section, you can select the following repository type.

Option	Description
VMware Repository	When you select this option, the latest versions of the vRealize Suite products are displayed in the Compatibility Matrix table. You can see this option only on vRealize Automation and vRealize Business for Cloud. Although, the compatibility matrix information is populated at the Suite product level, there can be a possibility for that latest versions might not be available at vRealize Suite Lifecycle Manager. However, with the Check Available Version , you can get only the latest version number with the associated build number.
Repository URL	When you select this option, you can manually add the local upgrade file location in vRealize Suite Lifecycle Manager virtual appliance.
vRealize Suite Lifecycle Repository	When you select this option, you can select the upgrade path available after mapping the binaries through vRealize Suite Lifecycle Manager.

Note Only vRealize Operations Manager upgrade consists of the **Run Assessment** feature. The run assessment checks for the vRealize Operations Manager upgrade readiness. It is not mandatory for the Run assessment to be passed, you can still go ahead with the upgrade. The compatibility matrix information is populated as per the selected version of the vRealize Operations Manager under the Product Version drop-down menu.

- 3 Click **Next** and click **Run Pre-check**.

Once the precheck validation is completed, you can then download the report to view the checks and validation status.

Note If you want to run the Precheck again after evaluating the discrepancies, you can select the **Re-Run Pre Check**. Pre-Check can also be performed using on **Submit** toggle button.

- 4 Click **Next** and click **Submit**.

- 5 If an vRealize Automation IaaS components upgrade fails

- a Revert all the Infrastructure components back to the snapshot "post-upgrade VA snapshot".
- b Revert the MS SQL database back to the pre-upgraded state.

- c Click **Retry** from vRealize Suite Lifecycle Manager and set **Upgrade Iaas Using Cli** to **True**.
- d Click **Submit**.

Update vRealize Operations Manager

You can trigger a pre-validation check from the product UI before upgrading vRealize Operations Manager within an environment. You can evaluate vRealize Operations Manager upgrades and allow upgrade operation later. You can also validate the product compatibility matrix must be validated.

Prerequisites

Verify that there is an older or an existing version of vRealize Operations Manager instance in the Manage Environments.

Procedure

- 1 Right click the vertical ellipses of an existing vRealize Operations Manager product and select an **Upgrade**.

The compatibility matrix information is loaded with new, compatible, and incompatible versions with product that must be upgraded.

- 2 Under the Product details section, you can select the following repository type.

Option	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in a Lifecycle virtual appliance.
vRealize Suite Lifecycle Repository	When you select this option, you can enter the upgrade path available after mapping the binaries through LCM.

- 3 Click **Next**.

- 4 To run the file format and **Version support from LCM**, click **RUN PRECHECK**.

Once the precheck validation is finished, you can then download the report to view the checks and validation status.

Note When you upgrade vRealize Operations Manager instance, you have two options.

- Run PreCheck: You must run to upgrade vRealize Operations Manager.
- Run Assessment Tool: You can use this option to run a vRealize Operations Manager APUAT tool.

The binary for vRealize Operations Manager APUAT tool is bundled with vRealize Suite Lifecycle Manager build, and once vRealize Suite Lifecycle Manager gets deployed it is present in vRealize Suite Lifecycle Manager VA location: `/data/lcmcontents/`, by default.

Note If you want to run the Precheck again after evaluating the discrepancies, you can select the **Re-Run Pre Check**. Pre-Check can also be performed using on **Submit** toggle button.

If the OS Admin Password for vRealize Operations Manager expires, vRealize Operations Manager upgrade Precheck fails while check-in even if the admin account is locked or not. You can change the admin password for the vRealize Operations Manager within vRealize Suite Lifecycle Manager UI, and then click Precheck for vRealize Operations Manager again. You can also change the vRealize Operations Manager admin password outside vRealize Suite Lifecycle Manager directly in vRealize Operations Manager, then run an inventory sync for the selected vRealize Operations Manager instance in the vRealize Suite Lifecycle Manager UI. Click **Run upgrade Precheck** for vRealize Operations Manager again.

Update vRealize Automation 7.x

You can trigger a pre-validation check from the product UI before upgrading vRealize Automation within an environment. You can evaluate vRealize Automation upgrades and allow upgrade operation later. You can also validate the product compatibility matrix should be validated.

Prerequisites

Verify that there is an older or an existing version of vRealize Automation instance in the Manage Environments.

Procedure

- 1 Right click the vertical ellipses of an existing vRealize Automation product and select an **Upgrade**.

The compatibility matrix information is loaded with new, compatible and incompatible versions with product that needs to be upgraded.

- 2 Select the **IAAS Snapshot After VA Upgrade** checkbox.

If an IaaS component fails after vRealize Automation then you can revert to the post upgrade VA snapshot.

- 3 Under the Product details section, you can select the following repository type.

Option	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in Lifecycle virtual appliance.
VMware Repository	When you select this option, the latest versions of the vRealize Suite products are displayed in the Compatibility Matrix table. You can see this option only on vRealize Automation. Although, the compatibility matrix information is populated at the Suite product level, there can be a possibility for that latest versions might not be available at vRealize Suite Lifecycle Manager. However, with the Check Available Version , you can get only the latest version number with the associated build number.
vRealize Suite Lifecycle Repository	When you select this option, you can select the upgrade path available after mapping the binaries through LCM.

- 4 Click **RUN PRECHECK** to execute.

Once the precheck validation is completed, you can then download the report to view the checks and validation status.

Note If you want to run the Precheck again after evaluating the discrepancies, you can select the **Re-Run Pre Check**. Pre-Check can also be performed using on **Submit** toggle button.

- 5 Click **Next** and read the summary before you click **Submit**.

Update vRealize Network Insight

You can trigger a pre-validation check from the product UI before upgrading vRealize Network Insight within an environment. You can evaluate vRealize Network Insight upgrades and allow upgrade operation later. You can also validate the product compatibility matrix should be validated.

Procedure

- 1 Right click the vertical ellipses of an existing vRealize Network Insight product and select an **Upgrade**.

The compatibility matrix information is loaded with new, compatible and incompatible versions with product that needs to be upgraded.

- 2 Under the Product details section, you can select the following repository type.

Option	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in Lifecycle virtual appliance.
vRealize Suite Lifecycle Repository	When you select this option, you can enter the upgrade path available after mapping the binaries through LCM.

- 3 Click **Next**.

- Click **RUN PRECHECK** to execute the File format and **Version support from LCM**.

Once the precheck validation is completed, you can then download the report to view the checks and validation status.

Note If you want to run the Precheck again after evaluating the discrepancies, you can select the **Re-Run Pre Check**. Pre-Check can also be performed using on **Submit** toggle button.

Update vRealize Log Insight

You can trigger a pre-validation check from the product UI before upgrading vRealize Log Insight within an environment. You can evaluate vRealize Log Insight upgrades and allow upgrade operation later. You can also validate the product compatibility matrix should be validated.

Prerequisites

Verify that there is an older or an existing version of vRealize Log Insight instance in the Manage Environments.

Procedure

- Right click the vertical ellipses of an existing vRealize Log Insight product and select an **Upgrade**.

The compatibility matrix information is loaded with new, compatible and incompatible versions with product that needs to be upgraded.

- Under the Product details section, you can select the following repository type.

Option	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in Lifecycle virtual appliance.
vRealize Suite Lifecycle Repository	When you select this option, you can select the upgrade path available after mapping the binaries through LCM.

- Click **Next**.
- Click **RUN PRECHECK**.

Once the precheck validation is completed, you can then download the report to view the checks and validation status.

Note If you want to run the Precheck again after evaluating the discrepancies, you can select the **Re-Run Pre Check**. Pre-Check can also be performed using on **Submit** toggle button.

Update vRealize Business for Cloud

You can trigger a pre-validation check from the product UI before upgrading vRealize Business for Cloud within an environment.

Procedure

- 1 Right click the vertical ellipses of an existing vRealize Business for Cloud product and select an **Upgrade**.

The compatibility matrix information is loaded with new, compatible, and incompatible versions with product that must be upgraded.

- 2 Under the Product details section, you can select the following repository type.

Option	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in Lifecycle virtual appliance.
vRealize Suite Lifecycle Repository	When you select this option, you can enter the upgrade path available after mapping the binaries through Lifecycle Manager.

- 3 Click **Next**.
- 4 Click **RUN PRECHECK** to run the file format and **Version support from LCM**.

Once the precheck validation is completed, you can then download the report to view the checks and validation status.

Note If you want to run the Precheck again after evaluating the discrepancies, you can select the **Re-Run Pre Check**. Pre-Check can also be performed using on **Submit** toggle button.

Creating an Environment

3

You can create an environment and install vRealize Suite products.

You can use vRealize Suite Lifecycle Manager to install the following vRealize Suite products and versions.

Product Name	Versions
vRealize Automation	8.1.0 and 8.2.0
vRealize Orchestrator	All versions embedded with supported vRealize Automation versions are supported.
vRealize Business for Cloud	7.5.0 and 7.6.0
vRealize Operations Manager	8.1.1 and 8.2.0
vRealize Log Insight	8.1.1 and 8.2.0
vRealize Network Insight	5.2.0, 5.3.0, and 6.0.0 Install the vRealize Suite Lifecycle Manager product support pack 1 for vRealize Network Insight 6.0.0 by downloading the .pspk file. For more information, see VMware vRealize Suite Lifecycle Manager 8.2.0 Release Notes .
VMware Identity Manager	3.3.2

For more information on installing vRealize Suite Lifecycle Manager and installing vRealize Suite products, see:

- [Chapter 1 Installing and Configuring vRealize Suite Lifecycle Manager](#)
- [Configure vRealize Suite Products for Installation](#)

The latency has been validated with 350 ms with a bandwidth of 1.5 MB/s for vRealize Suite small suite deployment and upgrade.

This chapter includes the following topics:

- [Create a New Private Cloud Environment Using the Installation Wizard](#)
- [Confirm Environment and Installation Settings](#)
- [Import an Existing Environment using Installation Wizard](#)
- [Create a Private Cloud Environment Using a Configuration File](#)

Create a New Private Cloud Environment Using the Installation Wizard

You can use the installation wizard to create a private cloud environment and install vRealize Suite products.

Prerequisites

- Configure Product Binaries for the products to install. See [Configure Product Binaries](#).
- Ensure that you have added a vCenter server to the data center with valid credentials and the request is complete.
- Generate a single SAN certificate with host names for each product to install from the Certificate tab in the UI.
- Verify that your system meets the hardware and software requirements for each of the vRealize Suite products you want to install. See the following product documentation for system requirements.
 - [vRealize Automation documentation](#)
 - [vRealize Business for Cloud documentation](#)
 - [vRealize Operations Manager documentation](#)
 - [vRealize Log Insight documentation](#)
- vRealize Automation SaltStack Config (formerly known as Salt Stack Enterprise) offers two setup options:
 - vRealize Automation SaltStack Config vRA-Integrated: This setup is introduced as a part of vRealize Automation 8.3.0. SaltStack Config (SSC) is a single node setup, which does not support multiple node setup or vertical scale up options. Prior to installing SaltStack Config vRA-Integrated, ensure that the supported version of vRealize Automation is installed. After vRealize Automation is installed, if multiple tenancy is not enabled, the SaltStack instance associates with the base tenant of vRealize Automation. When multi-tenancy is enabled in vRealize Automation, SaltStack Config vRA-Integrated associates with the newly added tenants, and then proceeds with the installation. When vRealize Automation is imported, the SaltStack Config vRA-Integrated instances which are associated with vRealize Automation are also imported.
 - vRealize Automation SaltStack Config Standalone: This setup has no dependency on vRealize Automation. You can install vRealize Automation SaltStack Config Standalone with a dedicated vRealize Automation Standard Plus license.
- If you are installing vRealize Automation, you must meet the following additional prerequisites.
 - Configure the vRealize Automation load balancer. See [vRealize Automation Load Balancing](#).

- Disable the second member of each pool in the vRealize Automation load balancer. You can re-enable these members after installation is complete.
- The cloud administrator has added all IaaS nodes and the Windows database server to the domain.
- The Windows database server and IaaS meet all vRealize Automation prerequisites. See [IaaS Windows Servers](#).

Add the domain user as part of **User Rights Assignment** under **Local Security Policies** for **Log on as a Service** and **Log on as a batch job**.

- The domain user has added the SQL server to the domain.
- Add the domain user as part of the SQL DB user Logins list with the `sysadmin` privilege.
- Install latest JRE (Java 1.8 or later) and create a `JAVA_HOME` environment variable on all Windows nodes.
- Install Microsoft .NET Framework 3.5.
- Install Microsoft .NET Framework 4.5.2 or later.

- A copy of .NET is available from any vRealize Automation appliance: <https://vrealize-automation-appliance-fqdn:5480/installer/>

If you use Internet Explorer for the download, verify that Enhanced Security Configuration is disabled. Navigate to `res://iesetup.dll/SoftAdmin.htm` on the Windows server.

- Set **User Access Control** settings to **Never Notify** on both Windows and database server virtual machines.
- Take a snapshot of the database machine and all Windows IaaS machines after configuration and before triggering the deployment in vRealize Suite Lifecycle Manager.
- Configure one NSX Edge as Active and one as Passive for the Windows machine. For detailed information on how to configure the NSX Load Balancer, see [Load Balancing the Cloud Management Platform in Region A](#).
- On all of the windows IaaS machines used in vRealize Automation deployment, log in to windows machine at least once as a domain user. If you do not login at least once to the IaaS machines, then the following error appears:

```
Private key is invalid: Error occurred while decoding private key. The computer must
be trusted for delegation
and the current user must be configured to allow delegation.
```

- Ensure that the IaaS nodes do not have any vRealize Automation components already installed. Follow the steps in the KB article [58871](#) to uninstall any vRealize Automation components in the IaaS node.

- Update the registry key on both Windows and database server virtual machines.
 - 1 Use the default PowerShell and run the following command as administrator on all Windows and database server virtual machines: `Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value "0"`
 - 2 Reboot the Windows virtual machine.
- Verify that the TLS 1.0 and 1.1 values are not present in the IaaS Windows machine registry path `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`.
- Alternatively, vRealize Automation install precheck provides a script, which can be executed in all Windows and database server to perform the above operations.
- If you are importing an existing vRealize Operations Manager installation, set a root password for that installation.

Procedure

1 [Install VMware Identity Manager in vRealize Suite Lifecycle Manager](#)

Before you create an environment in the vRealize Suite Lifecycle Manager, you must install VMware Identity Manager to create a global environment.

2 [Configure Environment Settings for a New Private Cloud](#)

Configure environment settings, such as name, password, and data center for a private cloud environment.

3 [Install vRealize Suite Products](#)

Select which vRealize Suite products to install in the private cloud environment.

4 [Accept EULA and License Selection](#)

Accept the VMware end-user license agreement and enter the license key.

5 [Configure Certificate Details](#)

To create an environment you can use the existing certificate.

6 [Configure Infrastructure Details](#)

You can configure the infrastructure details when you create an environment.

7 [Configure Network Details](#)

You can configure an environment by establishing a network connection within an environment.

8 [Configure Product Details](#)

You can view and configure the products that were selected environment creation.

9 Configure vRealize Suite Products for Installation

Configure the product details for each vRealize Suite product that you are installing in the private cloud environment.

10 Validate Private Cloud Environment Details

Configure vCenter server, cluster, network, datastore, and certificate details for a new private cloud environment.

Install VMware Identity Manager in vRealize Suite Lifecycle Manager

Before you create an environment in the vRealize Suite Lifecycle Manager, you must install VMware Identity Manager to create a global environment.

If you do not have an VMware Identity Manager instance, then you are automatically directed to install on the vRealize Suite Lifecycle Manager UI.

Procedure

- 1 Navigate to **My Services** dashboard, and click **Lifecycle Operations**.
 - 2 Click **Create Environment**, and enter the environment details.
 - a The environment name remains as global environment by default.
 - b Add the Password details.
-
- Note** If there is no password listed, then navigate to Locker to add a password.
-
- c Select the **Datacenter** name and click **Next**.
 - 3 Click **Next** and select the **New Install** option to install VMware Identity Manager.
 - 4 Select the required supported version for VMware Identity Manager and click **Next**.

Results

For more information on configuring VMware Identity Manager, see sections under [Install vRealize Suite Products](#).

Configure Environment Settings for a New Private Cloud

Configure environment settings, such as name, password, and data center for a private cloud environment.

Procedure

- 1 Log in to vRealize Suite Lifecycle Manager as an administrator and click **Create Environment**.
- 2 In the **Environment Name**, enter a descriptive name for the new private cloud environment.
This name must be unique among environments on this instance of vRealize Suite Lifecycle Manager.

- 3 Enter a **Default Admin Password** and confirm the Password.

The default password must be a minimum of eight characters.

Note The default password is not applied to vRealize Business for Cloud application password if vRealize Business for Cloud is deployed in a standalone mode. In standalone mode, vRealize Business for Cloud application credentials remain as admin/admin. To integrate vRealize Business for Cloud with vRealize Automation, add vRealize Automation to the private cloud environment before or at the same time you add vRealize Business for Cloud.

- 4 From **Data Center**, select an existing data center for this environment, or click + to add a data center to vRealize Suite Lifecycle Manager.

For information on adding a data center, see [Add a Data Center to vRealize Suite Lifecycle Manager](#).

- 5 (Optional) Select **Join the VMware Customer Experience Program** to join CEIP for this environment.

This product participates in the VMware Customer Experience Program (CEIP). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

- 6 Click **Next**.

Install vRealize Suite Products

Select which vRealize Suite products to install in the private cloud environment.

Prerequisites

Verify that you have a data center and environment credentials already created.

Procedure

- 1 Select whether to install vRealize Suite products by product.
 - a Select which individual vRealize Suite products to add to the private cloud environment and whether to do a new install of each product or import an existing installation of the product. For each new install, select the product **Version** and **Size** to deploy.
- 2 Click **Next**.

Note Starting with 8.2, vRealize Lifecycle Manager enables continuous availability (CA) for vRealize Operations Manager. For more information, see [Continuous Availability for vRealize Operations Manager](#).

Accept EULA and License Selection

Accept the VMware end-user license agreement and enter the license key.

Procedure

- 1 Read the end-user license agreement, select **I agree to the terms and conditions**, and click **Next**.
- 2 Under the license section,
 - a To select the license keys from the locker, click **Select** to open the list of licenses which are applicable to the selected products and versions. If not, select all the keys available from the listing.
 - b Click **Add**, to add a new license key to the locker from within the installation flow.
 - c Click **Validate** to validate the license. If multiple license keys are available for a product then this action will suggest to choose one per product selected for the deployment.

You can now view the applicable license keys in the table. The next step will not be enabled until all the products deployed are having appropriate license selected for them.

Note Valid standalone product licenses or vRealize Suite licenses or a combination of both is allowed for product deployment in vRealize Suite Lifecycle Manager. License validation does not check the functionality allowed by the licenses themselves. Therefore, select the license key considering the combination of products being deployed and their inter connectivity.

Configure Certificate Details

To create an environment you can use the existing certificate.

Prerequisites

Verify that the imported or created certificate has all the IP addresses and domain or host names added.

Procedure

- 1 Under the **Certificate Details**, select the **Certificate** from the drop-down menu.

If you want to provide certificate details at product level, you can specify the certificate at the product properties of each product. The action can override the certificates that are selected at the infrastructure level.

- 2 To create a certificate, click the plus sign.

In the **Add Certificate** window, enter the required details.

Fields	Description
Certificate Name	Enter a valid certificate name.
Common Name	To identify the certificate, enter a common name.
Organization	Enter the Organization name.
Organizational Unit	Enter the Organization Unit.
Country Code	Enter a country code which must be in two characters only.

Fields	Description
Locality	Enter your locality.
State	Enter the State.
Key Length	Select the length of the key. You can select 2048 or 4096 bits.
Domain Name	Enter a valid domain name.
IP Address	Enter the IP address in which you are assigning the certificate.

3 Click **Generate**.

4 To import an existing certificate, select **Import Certificate** option.

Fields	Description
Certificate Name	Enter a valid certificate name.
Select File	1 Click Choose File . 2 Browse to the saved PEM file.
Passphrase	Enter the Passphrase field, type <Cert- Password> (if applicable).
Enter Private Key	When you upload a PEM file, the private key details are populated automatically.
Enter Certificate Chain	When you upload a PEM file, the certificate details are populated automatically.

5 Click **Import**.

6 Click **Next**.

Configure Infrastructure Details

You can configure the infrastructure details when you create an environment.

Prerequisites

If the selected data center does not have a vCenter Server associated with it, then you must add a vCenter Server.

Procedure

1 Select a vCenter Server from the drop-down menu.

Note There should be at least one vCenter Server associated with a data center.

2 Select a **Cluster**.

3 When you click **Select a Folder**, all the folders that are associated in the vCenter Server are listed.

If the folders are not displayed, then refresh the vCenter data collection from the vRealize Suite Lifecycle Manager settings page.

- 4 To deploy your VM, click **Select a Resource Pool**.

All the resource pools that are associated with the selected cluster are listed.

Note You can select a resource pool to deploy your VM. Both folder and resource pool selection are optional. If you do not specify any resource pool, the VM is deployed in the root default resource pool of the selected cluster. If you do not specify the folder details for both vCenter Server and resource pool, the deployment of the VM is saved in the root default VM folder of the data center inside the vCenter .

- 5 Select the required **Network**, **DataStore**, and **Disk Disk Mode**.

Note vRealize Operations Manager deployment fails when you provide incorrect infrastructure details such as wrong DNS or gateway details without running a pre-check while you create an environment flow. If the deployment fails, you might not see the correct cause of deployment failure using the error or code message that appears in vRealize Suite Lifecycle Manager UI, and you cannot proceed further with that deployment. As a result, you might have to delete the Environment card from vRealize Suite Lifecycle Manager with all the products or nodes that were deployed as part of that environment. You can run Pre-check so that the Infrastructure-related issues are detected and can be corrected before triggering the deployment.

- 6 With Lifecycle Manager 8.0, to integrate with VMware Identity Manager, select **Integrate with Identity Manager** toggle button.

Note The default configuration admin given while installing VMware Identity Manager (global environment) will be made the admin for the product as well while integrating with VMware Identity Manager.

VMware Identity Manager acts as an identity provider and manages SSO for the vRealize Suite products and vRealize Suite Lifecycle Manager when integrated with vRealize Suite Lifecycle Manager. SSO provides a single set of credentials to access all vRealize Suite applications and vRealize Suite Lifecycle Manager. With SSO, you are only required to log in once, and then you can seamlessly access all vRealize Suite applications.

- 7 Select the **Use Content Library** to use OVF's hosted on vCenter's Content Library, if there is a network latency from vRealize Suite Lifecycle Manager to vCenter server

Copying OVF and VMDK files for deployment from vRealize Suite Lifecycle Manager to vCenter Server might take more time and lead to a deployment failure if there is a Network latency from vRealize Suite Lifecycle Manager to target vCenter Server. Content Libraries in vCenter can be used to host OVF's and the same can be used from vRealize Suite Lifecycle Manager to deploy products. You can perform the steps before you trigger a vCenter Inventory Sync in vRealize Suite Lifecycle Manager:

- To create a content library, see [Create Library](#).
- To import a content library, see [Import Library](#).

vRealize Suite Lifecycle Manager supports deployment only from Publisher or Local Content Libraries.

- 8 To configure the **Binary Mapping**, click **Next**.

Configure Binary Mapping Details

To create an environment, select one or more binaries for the products.

Ensure to map the correct library items for the respective products. If none are selected for a product then a default binary from vRealize Suite Lifecycle Manager will be used to deploy that product.

Procedure

- 1 Click **+SELECT CONTENT LIBRARY ITEMS** to add a content library item.
- 2 You can either search for a library item or open the content library tree to select one.

Note You can add multiple content library and associate suite products as per your requirement.

- 3 Click **Select**.
- 4 Select a **Product** corresponding to the selected content library item.

Note vRealize Suite Lifecycle Manager validates the OVF package in the specified content library item corresponding to the selected product.

- 5 Click **Next**.

Note Content Library item for a particular node, if it needs to be deployed into a different vCenter server, it can be selected in Advanced Settings.

Results

After submitting your binaries maps, click next to configure your network settings.

Configure Network Details

You can configure an environment by establishing a network connection within an environment.

Prerequisites

- Static IP address set is required for any product deployment from vRealize Suite Lifecycle Manager. This is applicable for starting from vRealize Suite Lifecycle Manager 1.0 and above.
- Verify that you have Domain Name mapped for the IP addresses used for deployed.

Procedure

- 1 Under the **Network** page, enter the **Default Gateway** address.
- 2 Enter the **Netmask** IP address.

- 3 Enter the **Domain Name** and **Domain Search Path**.
- 4 The DNS Servers are automatically listed, if they aren't then click **Add New Server** or **Edit Server Selection**.
- 5 Select the required Time sync mode:

Option	Description
Use Time Server (NTP)	When you select the NTP Server, you have to select the assigned time server from the NTP list. If an NTP server is not added, then to add one, click Global Settings . You are then directed to the Settings page to add an NTP server. For more information, see Configure NTP Servers .
Use Host Time	When you select the Host time, then the environment proceeds with the system time.

- 6 After you have added NTP servers, you can click **Select Servers** to add an NTP at an Infrastructure level.
- 7 Select the NTP servers from the list and you can reorder the NTP servers based on the precedence by clicking the arrows.

When you select a vRealize Suite product, you can configure using these Time servers for the selected component.

Configure Product Details

You can view and configure the products that were selected environment creation.

Procedure

- ◆ Under the **Product Details**, select the products for a new installation.

Product	Function
vRealize Automation	<p>a To monitor health of vRealize Automation, select the Monitor with vROps check box.</p> <p>b To manage the workload using load balancer and reclaim unused resources from the resource pool, select the Workload Placement and Reclamation check box.</p> <hr/> <p>Note This is only available for a new installation where in vRealize Operations Manager monitors health of vRealize Automation. Inter-product configuration is not supported for an existing environment.</p> <p>If vRealize Operations Manager is not present, then you can integrate the products outside of LCM.</p> <p>Cross-product integration for vRealize Automation with vRealize Operations Manager is not applicable for an import of vRealize Automation. And is only applicable if there is a new installation of vRealize Automation.</p> <p>You can also perform a cross product configuration where vRealize Automation is the only case where vRealize Operations Manager is already part of an environment or vRealize Automation is getting deployed along with Import or New Install of vRealize Operations Manager.</p> <hr/> <p>Note You can perform a cross product integration only when vRealize Operations Manager is already deployed in an environment where you can newly install vRealize Automation. You can also select vRealize Operations Manager Import or New install along with a new installation of vRealize Automation.</p> <hr/> <p>Note Starting with 8.2, when you newly install vRealize Automation, you can select the Configure internal pods and service subsets checkbox, and then enter the values for K8 Cluster IP Range and K8 Service IP Range.</p> <hr/> <p>Note In the 8.3 release, Federal Information Processing Standard 140-2 Support (FIPS) is supported for vRealize Automation.</p> <hr/> <p>c Select the Product Certificate from the drop-down menu.</p> <p>d (Optional) Select ON or OFF to enable or disable the FIPS Compliance Mode.</p> <p>e Select the Applicable Time Sync mode.</p> <p>f Select the Time Server (NTP). For more information, see Configure NTP Servers.</p> <p>g If you want to configure cluster virtual IPs, then select the Yes or No options.</p>

Product	Function
	<p>h (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for the deployed VM's.</p> <p>Note For more information on database creation, see Create a New Private Cloud Environment Using the Installation Wizard.</p>
vRealize Automation Salt Stack Config	<p>a Under Product Properties, select the Tenant ID from the drop-down menu.</p> <p>b Under Components, enter the VM name, FQDN and Virtual IP Address.</p> <p>Note You can only perform a single node Salt Stack Config installation at a time. For vRealize Automation deployment along with Salt Stack Config, the tenant ID is selected by default. Any additional Salt Stack Config deployment can be performed based on the tenant as organic growth.</p>
vRealize Business for Cloud	<p>a Under Product Properties section, enter the VM Name, Hostname, and IP Address.</p>
vRealize Log Insight	<p>Note In the 8.3 release, Federal Information Processing Standard 140-2 Support (FIPS) is supported for vRealize Log Insight. It is also supported as a Day-2 operation.</p> <p>a Select the node size from the drop-down menu.</p> <p>b (Optional) Select ON or OFF to enable or disable the FIPS Compliance Mode.</p> <p>c Under Integrated Load Balance Configuration, if you select the Configure Cluster Virtual IPs, enter the FQDN and Virtual IP Address.</p> <p>d To add more node, click ADD NODE.</p> <p>e Select the Applicable Time Sync Mode.</p> <p>f Under components, enter the vRLI primary node details.</p> <p>g (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for the deployed VM's.</p> <p>h (Optional) Click Add Components to configure additional settings.</p> <p>i Enter the required fields.</p>

Product	Function
vRealize Operations Manager	<p>Note In the 8.3 release, Federal Information Processing Standard 140-2 Support (FIPS) is supported for vRealize Log Insight. It is also supported as a Day-2 operation.</p> <ol style="list-style-type: none"> Under Product Properties, select the Disable TLS version from the drop-down menu. (Optional) Select ON or OFF to enable or disable the FIPS Compliance Mode. Select the Certificate from the drop-down menu. (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for the deployed VMs. Add the Product Password. (Optional) Click Integrate with Identity Manager check box. Select the Applicable Time Sync Mode. For Continuous Availability (CA) based deployment, under Components, enter the Infrastructure and Network details for Witness Domain. For Continuous Availability (CA) based deployment, enter the Infrastructure and Network details for Fault Domain 1 and Fault Domain 2. If you want to add additional data nodes for a cluster, click the Add Components tab. <p>Note If you select Use Global Configuration, the field data is populated based on the information provided in the Infrastructure tab. You can select this option for Witness Domain, Fault Domain 1, or Fault Domain 2. Ensure that each domain is in different physical location so that if one fault domain fails, nodes from the other fault domain remains active.</p>

Product	Function
vRealize Network Insight	<ul style="list-style-type: none"> a Under the Product Properties, select the node size from the drop-down menu. b Select the Applicable Time Sync Mode. c Under components, enter the vrni platform and vrni collector details. d (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for the deployed VM's.
VMware Identity Manager	<ul style="list-style-type: none"> a Under the Product Properties, select the certificate from drop-down menu. b Select the Admin Password from the locker. c Set Default Configuration Admin Username. This will be created as local user in VMware Identity Manager and is used for vRealize Suite Product Integration. d Select the password for Default Configuration Admin user. e Check Sync Group Members. When enabled, members of the groups are synced from the Active Directory. When this is disabled, group names are synced to the directory, but members of the group are not synced. f For a cluster deployment, under Cluster Virtual IP enter Cluster VIP FQDN, this is used to load balance the application. g For a cluster deployment, enter Database IP used internally for proxying to the postgres master (primary). <p>Note This is not same as the one used to load-balance the application and the IP address should be free, and available.</p> <ul style="list-style-type: none"> h Under Components, enter the VMware Identity Manager single or Cluster Node details.

Deploy Windows VMs for vRealize Automation Installation

With vRealize Suite Lifecycle Manager 2.0 onwards, you can install or deploy IaaS windows of a vRealize Automation deployment without having to provision it before trying to create an environment with vRealize Automation in vRealize Suite Lifecycle Manager.

The pre-check run ensures the system requirements are met, while the Windows OS template (one or more for specific IaaS component) itself is provided by any user.

- You can deploy IaaS components with a minimum number of steps.
- IaaS component deployments are part of vRealize Automation deployment.
- Pre-validations on the IaaS components should try to fix the issues wherever possible and when an issue is automatically handled you can fix from the UI.

Procedure

- 1 Enter the **Windows Username**, and **Password**.
- 2 Select the **Applicable Time Sync mode**.
- 3 Select the **Time Server (NTP)**. For more information, see [Configure NTP Servers](#).

- 4 As cloud admin you can deploy Windows VMs that are required for vRealize Automation installation, using vRealize Suite Lifecycle Manager installation wizard. Click **Yes** on the **Configure Windows box** under **Product properties** to deploy windows VMS with vRealize Automation.

When you select **Yes**, the Window box appears under the **Components** section. If you select no, then vRealize Suite Lifecycle Manager will not deploy new Windows VMs for IaaS components.

Windows VMs can be selectively deployed for specific components too. Select the option to deploy Windows VMs under product properties and enter False on the **Configure Windows for IAAS** field under the advanced property of the component for which Windows VM deployment is not desired.

If any component needs to be deployed with a specific template and customization spec, then select the option to deploy Windows VMs under the product properties. Provide the template and spec and access the advanced property of the component and provide details under the section **Windows IAAS Deployment**. For example:

- a Configure Windows for IAAS: true
- b Use ISO: false
- c Windows Template Name : mytemplate
- d ISO File Name
- e Use Customization Spec: true
- f Template Customization Specification: mycustomspec

where 'mytemplate', 'mycustomspec' already exists in the vCenter where the component is being deployed.

- 5 To **Configure Cluster Virtual IPs**, select the **Yes** or **No** options.

If you select yes, then appropriate load balancer details for **vRA Appliance**, **IaaS Web**, and **IaaS Manager** should be provided.

Note vRealize Suite Lifecycle Manager does not create the load balancers. Appropriate load balancers should be pre-created and only their details should be entered in vRealize Suite Lifecycle Manager during deployment.

- 6 For deploying IaaS VMs, you can either select **ISO** or **Template**.

When you select ISO, map a valid windows ISO image along with a correct license key in vRealize Suite Lifecycle Manager. For more information on ISO mapping, see [ISO Mapping in vRealize Suite Lifecycle Manager](#).

Note When you select **Template** as an option for IaaS, you are asked to select a template from a pre-populated list. The templates in the list are collected from the vCenter specified at the in **Infrastructure Details** section. For more details on usage of templates, see [Templates and Custom Specification in vCenter Server](#). During data collection in Lifecycle manager, you can collect all the templates on the ESXi host in the cluster to which you have access. Templates residing on the other hosts or cluster levels are not collected.

- 7 For a customization specification, select **Existing Spec** or **User Input**. An existing spec provides an option to select a spec from the vCenter Server. For a user input, enter the fields manually. The entries for user input are not saved but will be applied for the current deployment of vRealize Automation.
- 8 Enter the details required for each of the Components. For each components advanced property can be accessed to override details provided in the **Windows Box** section.
- 9 Click **Next** to continue to **PreCheck Details** section.

Before proceeding with precheck, see [Best Practices](#).

ISO Mapping in vRealize Suite Lifecycle Manager

Using ISO image you need to map or register the ISO image to deploy any VM from vRealize Suite Lifecycle Manager.

Prerequisites

ISO image should be imported in vRealize Suite Lifecycle Manager appliance under a sub-directory of `/data`. If the storage space is low, then extend the storage from the Settings page.

Procedure

- 1 Navigate to **Home > Settings Product Binaries**.
- 2 Click **ADD BINARIES** button and select **Windows ISO** from the **Add Product Binaries** dialogue box.
- 3 Provide the absolute path for the ISO image location against the field **Base Location** and click **DISCOVER**.
- 4 Under the **Windows ISO Mapping Details** section, select the ISO image name that are pre-populated after a successful discovery from base location.

Note Only a single ISO image can be selected at a time for mapping and one image cannot be mapped more than once, even if the subsequent details provided are different per attempt.

- 5 Select the OS version from the pre-populated list.

- 6 Enter a valid license key. Enter a valid password for the Administrator login to the VMS deployed using this ISO.
- 7 The image name is auto-populated and cannot be edited. Only the image names which are applicable for a vRealize Automation installation are available.

The image name is generated as per the [article](#).

- 8 Click **SUBMIT** to initiate the mapping process.

Templates and Custom Specification in vCenter Server

To deploy IaaS VM using templates, you need to ensure certain pre-requisites are met. vRealize Suite Lifecycle Manager uses existing VM templates and customization spec for IaaS deployment.

Things to remember

- Templates should be local to vCenter Server where the IaaS VMs are installed. Templates present in the content library are not considered for an IaaS installation. Only the templates that are present in the vCenter inventory are considered by vRealize Suite Lifecycle Manager.
- The template should have all the necessary configurations that include policies, firewall settings and so on. Also, the process does not configure policies, firewall rules, Antivirus, or any other software pre bundled in the VM template or ISO. As a workaround, configure the appropriate services in the template to have them functional after first boot of the deployed VMs. Once the VALIDATE & DEPLOY reports run, you can access the console of the deployed VM and configure the required policies in the respective VM as per requirement.
- The template should have VMware tools installed and the version should not be less than that present in the ESXi hosts present in the vCenter clusters considered for an IaaS installation.
- For a template used for a deployment of IaaS database VM, appropriate version of the database software should be installed and respective services should be enabled.
- User can select an existing Customization Specification present in the vCenter for an IaaS deployment. The custom-spec should be provided with correct details with valid settings for the selected network and domain. For example, if an IaaS VM is expected to obtain static IP residing on a vLAN with ID 'X' then the custom specification must have the gateway, subnet mask and DNS servers for 'X' in the custom-spec.

Note If the database is installed with a custom port, then the template for the DB should have the port and corresponding instance configured before an IaaS installation. Alternate way is to deploy the database VM using template and configure the port, and instance before submitting the vRealize Automation deployment request from vRealize Suite Lifecycle Manager.

Installation of IaaS VMs Using ISO

If vRealize Automation is deployed on a development or test environment then IaaS VMs can be deployed using valid windows ISO image. For ISO based deployments, vRealize Suite Lifecycle Manager does not deploy IaaS database machine. vRealize Suite Lifecycle Manager UI will not restrict but the submitted request will always discard the deployment of DB.

Requirements for Installation

- For an IaaS VM deployment with ISO Images from vRealize Suite Lifecycle Manager, vCenter version should be 6.5 or later.
- The vCenter Server where IaaS VMs are deployed, should be registered with vRealize Suite Lifecycle Manager, and the user credential used for the registration should have administrative capability for vCenter content libraries.
- VMware Tools ISO should be available in each of the ESXi (at the location `/vmimages / tools- isoimages`) which belongs to the cluster where IaaS VMs are to be deployed.
- The network configurations, including load-balancers should be in vCenter Server for consumption of the deployed VMs. vRealize Suite Lifecycle Manager cannot perform any network configuration in vCenter Server for an IaaS VM deployment.

Points to Remember

- IaaS deployment from vRealize Suite Lifecycle Manager (using ISO) uploads the ISO to a vCenter content library named - `LCM-LOCAL-ISO-LIB`. This content library is created automatically by vRealize Suite Lifecycle Manager.
- Once **VALIDATE & DEPLOY** is clicked in vRealize Suite Lifecycle Manager UI, the ISO images selected for the IaaS installation are uploaded to the content library mentioned. The uploaded ISO image name is same as that found in the entry under the column ISO Binary in the table ISO Binaries under Product Binaries. vRealize Suite Lifecycle Manager uploads ISO binary by this name in the vCenter content library mentioned earlier. If for a given ISO, an entry with the same name exists, then the upload task is ignored.
- The templates and ISO images used for an IaaS deployment, should be valid and working. Also, the Windows license keys used for ISO mapping, vCenter Customization Specification and other relevant places should be valid. Corrupt or wrong template or ISO leads to failure for the overall IaaS deployment task in vRealize Suite Lifecycle Manager.
- IaaS installation from vRealize Suite Lifecycle Manager using ISO supports a default locale as per the ISO image. User-specific input is not supported.
- When vRealize Suite Lifecycle Manager uploads the ISO deployment to a vCenter content library named - `LCM-LOCAL-ISO-LIB`, after an ISO is mapped in Lifecycle Manager, note the entry under the column ISO Binary in the ISO Binaries table. If Lifecycle Manager uploads ISO binary by the same name in the vCenter content library mentioned earlier then such uploads are ignored.

Delete the ISO file manually from content library `LCM-LOCAL-ISO-LIB`.

Best Practices

You can follow the listed practices when you are installing IaaS VMs using vRealize Suite Lifecycle Manager.

Windows Template

- Windows update, if pre-configured in the templates used for a IaaS deployment, can lead to failure. Turn off the Windows update in the templates or create the template after performing recent most applicable update of the OS.
- Have unique names for the templates in a vCenter inventory. If for a given vCenter, there are templates that do not have a unique name, then it is difficult to identify the correct one from vRealize Suite Lifecycle Manager installation UI.

Windows ISO Image

- You can use the ISO-based deployments of IaaS for development and test environments.
- If an ISO-based IaaS deployment is used, then IaaS database VM should be pre-deployed. Deployment of database VM using ISO is not supported in vRealize Suite Lifecycle Manager.
- If an existing customization specification is being used for an IaaS deployment, then ensure that all the inputs for the custom spec are consistent and correct. Also, ensure that a valid NIC configuration with subnet details is present in the customization specification details.
- IaaS installation from vRealize Suite Lifecycle Manager does not support use of **Run Once Commands** in a customization specification. Also, the process does not configure policies, firewall rules, Antivirus, or any other software pre-bundled in the VM template or ISO. As a workaround, configure the appropriate services in the template to have them functional after first start of the deployed VMs. After you validate and deploy reports successfully, you can access the console of the deployed VMs and configure the required policies in the respective VM as per requirement.

Configure vRealize Suite Products for Installation

Configure the product details for each vRealize Suite product that you are installing in the private cloud environment.

Configuration tabs appear only for the products you selected to install. You can access advanced properties if you want to update the advanced configurations like adding different vCenter, enabling or disabling the registration with VMware Identity Manager and so on.

Procedure

- 1 Click the **vRealize Automation** check box to configure installation details for vRealize Automation.
 - a If you select 7.x, enter the user name and password for the Windows Server vRealize Automation uses.
The Windows user must have administrator rights.
 - b Enter the fully qualified domain name in the form and the IP address for the vRealize Automation appliance.

For more information about the vRealize Automation appliance, see the [vRealize Automation Appliance](#) and KB article [55706](#).

- c Enter the names in the form of fully qualified domain names and IP addresses for the Infrastructure as a Service (IaaS) Web and Management servers.

For more information about IaaS, see [Infrastructure as a Service](#).

- d (Optional) To add an additional component, click the plus sign to **Add components** and select the type of component to add.
- e Enter the host name in the form of a fully qualified domain name and IP address for each component.

Windows machines that host the Model Manager Web service, Manager Service, and Microsoft SQL Server database must be able to resolve each other by Windows Internet Name Service (WINS) name. To authenticate vRealize Automation through an external VMware Identity Manager, you can either click the vRealize Automation application icon in the VMware Identity Manager catalog or manually logging in to vRealize Automation through the tenant URL. If the authentication fails, then the following error is displayed: `Identity Manager encountered an error. Contact your admin and provide information displayed below.`

- f If the database instance is an existing one or it is on a non-default port, include the port number in an instance specification from the **Advanced Properties**. If the database instance is a new one and default instance is expected, then provide hostname of the DB VM only. If the database already exists and no changes needed then from the **Advanced Properties**, you can provide the database name.

Note The Microsoft SQL default port number is 1443. During the installation of vRealize Automation, the first Web node task might fail after the vRealize Automation management agent is installed. This is caused by either a database installation failure or a connection timeout.

- g If you select 8.x, enter the fully qualified domain name in the form and the IP address for the vRealize Automation appliance.
- h Enter the host name in the form of a fully qualified domain name and IP address for each component.

For vRealize Automation 7.x, there are three types of deployments which includes small, medium, and large. For vRealize Automation 8.x includes Standard and Cluster.

- 2 Click the **vRealize Business for Cloud** check box to configure installation details for vRealize Business for Cloud.
 - a Select the **Currency** to use from the drop-down menu.
 - b (Optional) To add an additional component, click the plus sign to **Add components** and select the type of component to add.
 - c Enter the host name in the form of a fully qualified domain name and the IP address for each component.

If vRealize Automation is not present in the environment and is not getting deployed along with vRealize Business for Cloud, then specify the **Deploy Standalone vRealize Business for Cloud** property to true in **Advanced Properties**. If VMware Identity Manager is present in vRealize Suite Lifecycle Manager, then vRealize Business for Cloud will be registered with vIDM automatically.

There is only one deployment type with the Standard node cluster in vRealize Business for Cloud.

- 3 Click the **vRealize Operations** check box to configure installation details for vRealize Operations Manager.
 - a Enter the NTP server address.
 - b (Optional) Click the plus sign to **Add components** and then select the type of component.
 - c Enter the host name in the form of a fully qualified domain name and the IP address for each component.
 - d Select the **Node Count** or **Node Size** for **vRealize Operations** deployment. **vRealize Operations** recommends that the number of analytic nodes available for a selection, depends on the selected node size.

The default type of deployment for vRealize Operations Manager is a node size and node count.

- 4 Click the **vRealize Log Insight** check box to configure installation details for vRealize Log Insight.
 - a (Optional) Click the plus sign to **Add components** and select the type of component to add.
 - b Enter the host name in the form of a fully qualified domain name and the IP address for each component.
 - c If you are adding cluster virtual IPS, optionally enter load balancer settings.
 - d Click **Components + icon**, to add and enable any of the configuration during the deployment.

The deployment type available for vRealize Log Insight is Standalone and Cluster.

- 5 Click the **vRealize Network Insight** check box to configure installation details for vRealize Network Insight.
 - a (Optional) Click the plus sign to **Add components** and select the type of component to add.
 - b Select the License key if registered in My VMware or enter the License key manually.
 - c Enter the Infrastructure details and select the NTP servers.

- d Enter the Network and Certificate details.
- e Under the Product Details, click **Add** component to add a vRealize Network Insight platform or a collector. This option is dependant on what type of vRealize Network Insight you are selecting initially. If you have selected a cluster of vRealize Network Insight, then you can have two platforms and one collector by default.

The deployment type available for vRealize Network Insight is Standard and Cluster.

6 Click **Next**.

Points to remember while Configuring vRealize Automation

You might encounter a few issues while performing vRealize Automation 8.0 scale-out, deployment, replace certificate, and import brownfield.

- When the vRealize Automation 8.x replace certificate fails intermittently at initialize cluster after replacing the certificate, retry the failed vRealize Automation 8.0 replace certificate.
- vRealize Automation 8.0 HA replace certificate fails at the initial cluster after replacing the certificate, when SAN certificate has additional hostnames. At this instance, replace the vRealize Automation HA certificate with SAN certificate which has the required hostnames like vRealize Automation Load Balancer hostname and three vRealize Automation hostnames.
- When vRealize Automation 8.0 scale out fails at initialize cluster due to liquibase locks then click the retry option in the failed vRealize Automation 8.0 scale out request to retry the initialize cluster step.
- Verify if the SAN certificate is used instead of wild card certificate for vRealize Automation 8.0 deployment.
- Verify to provide all four hostname including 3 vRealize Automation nodes hostname and vRealize Automation Load Balancer hostname in the SAN certificate when the custom certificate is used.

Continuous Availability for vRealize Operations Manager

Continuous availability (CA) for vRealize Operations Manager prevents loss of data during a node failure and ensures availability of vRealize Operations during a physical location failure.

Note The master node is now referred to as the primary node. The master replica node is now referred to as the primary replica node.

CA segregates the vRealize Operations Manager cluster into two fault domains, stretching across vSphere clusters, and protects the analytics cluster against the loss of an entire fault domain. The two fault domains are **Fault Domain 1** and **Fault Domain 2**. By default, the primary node and the replica node are assigned to **Fault Domain 1** and **Fault Domain 2**. If **Fault Domain 1** fails, the functionality is not disrupted as the other pair node ensures that the incident results in no data loss.

The **Witness Node** is the third network domain that exists independently and identifies network partitioning across the two fault domains. If network connectivity between the two fault domains is lost, the cluster goes into a split-brain situation, which is detected by the **Witness Node**. Immediately, one of the fault domains goes offline to avoid data inconsistency problems.

Note A minimum of three pairs of nodes are required to enable CA. You can add a maximum of 16 data nodes, including the primary and replica nodes.

Enable Continuous Availability for vRealize Operations Manager

You can now enable continuous availability (CA) for vRealize Operations Manager.

Prerequisites

Verify that you have a data center and environment credentials already created.

Procedure

- 1 Under **Select Product**, select **vRealize Operations Manager**, and then select **New Install**.
- 2 Select the **Version** from the drop-down menu.
- 3 Select **CA** as the **Availability** option.
- 4 Select the **Deployment Type** from the drop-down menu, and based on the selection of the **Deployment Type**, select the number of nodes from the **Node Count** drop-down menu.

Note For more information about the sizing guidelines for vRealize Operations Continuous Availability, see [KB article 78495](#).

Validate Private Cloud Environment Details

Configure vCenter server, cluster, network, datastore, and certificate details for a new private cloud environment.

Procedure

- 1 Enter the details of the vCenter server where you are installing the vRealize Suite and the names of the cluster, network, and datastore to use for this environment.

The vCenter server name must be in the form of a fully qualified domain name.

- 2 Select the disk file format, and click **Next**.

Option	Description
Thin	Use for evaluation and testing.
Thick	Use for production environments.

- 3 Enter the default gateway, domain, domain search path, DNS server, and netmask details for the environment, and click **Next**.

- 4 Enter the key passphrase and private key.
- 5 Enter certificate chain for the SAN certificate to import or select the **Generated Certificate** option, and click **Next**.

For information on generating a SAN certificate, see [Configure Certificate Within Locker](#).

- 6 Enter the product details for each of the vRealize Suite products that you have selected to install by providing its Windows hostname and IP Address.
- 7 Click the **PRE-CHECK** to run and validate the properties for each of the vRealize Suite products.

Note If the Pre-Check fails, you are required to check the recommendations and fix the issues of the selected product and run the pre-check again.

- 8 Read the Summary and click **Submit**.

Pre-Check Validation

Based on the pre-check validation you can change your input anytime in the previous steps and run the pre-validation check again.

How does Pre-Check Validation Work?

When you click the **Run Pre-Check** button, a report is generated indicating whether the pre-validation is in PASS or FAIL state. Therefore, based on the report you can modify your inputs given in the previous steps and click the **RE - RUN PRE CHECK** button. The report contains the following information:

- Status of the Check
- Check Name
- Component/Resource against which the current check is run.
- Result description about the check execution
- Recommendation, if there is FAILURE or WARNING

The report also generates color coded status:

- GREEN SYMBOL - PASSED
- RED SYMBOL - FAILED
- YELLOW SYMBOL - WARNING
- GREEN FIXED SYMBOL - REMEDIATED & FIXED

You cannot go further unless the pre-validation run is successfully complete. The pre-validation request progress can be tracked in the **Request** tab through a request that gets created with a name `VALIDATE_CREATE_ENVIRONMENT`. Once the pre-validation is run and the **NEXT** button is enabled, you can **SUBMIT** the request for deployment. When you are submitting, you can skip the pre-validation. By default, this flag is enabled. This verifies pre-validations are anyway run before deployment is triggered. If you want to skip this, then you can deselect the flag and then click submit. Pre-validations check does not run again before the deployment begins.

If you click **Submit** with the pre-validation flag enabled, a request by name `VALIDATE_AND_CREATE_ENVIRONMENT` is created. If you click **SUBMIT** only by deselecting the pre-validation flag, a request by name `CREATE_ENVIRONMENT` is created. You can track the progress of pre-validation requests in the Request tab that vRealize Suite Lifecycle Manager provides Out of the box. Before you run a pre-check on vRealize Automation, verify all the IaaS component VMs are communicating with Lifecycle Manager appliance. After you enable pre-check and submit the create environment, if the pre-check fails then user can resume the wizard from the Request page with a request state as `PRE_VALIDATION_FAILED`. From the report, if the failure is due to the wrong IaaS credential then rerunning pre-check on updating the windows password in the Product details page still results in the wrong IaaS credential. To fix this, update the Windows password in the product details page at each node level and rerun the Pre-Check.

If the `VALIDATE_AND_CREATE_ENVIRONMENT` request fails with a status `PRE-VALIDATION-FAILED`, then you can validate your inputs by clicking the icon under the action tab. This directs you to the wizard where you can modify your inputs and run **PRE CHECK** or click **SUBMIT** for deployment. Once the deployment is complete, you can see the last run pre-validation report. This option is available from the environment page in the **Manage Environments** page. You can also view the last run report under **View Last Pre Check Result** under **Environment**.

Note Pre-Check in LCM does not take extended storage into account. This means if the extended storage option is used to deploy vRealize Operations Manager nodes using vRealize Suite Lifecycle Manager, then the precheck might succeed but the actual deployment can still fail due to insufficient disk space. For more information, see KB article [56365](#).

Only **Automate checks** is automated to run a manual pre-requisite for vRealize Suite in vRealize Suite Lifecycle Manager 1.2. You can **DOWNLOAD SCRIPT** and run on all the windows machine. The zip contains a Readme file, which explains how to run the script. This step is mandatory if you have selected vRealize Automation as one of the products during an environment creation.

vRealize Suite Lifecycle Manager Agent

The vRealize Suite Lifecycle Manager agent is used for running pre-validations on the IaaS windows servers even before any of the vRealize Automation components are installed. The vRealize Suite Lifecycle Manager agent runs as a windows service. It registers the windows server as an identified node with the vRealize Suite Lifecycle Manager appliance. Every windows server is registered as a node in vRealize Suite Lifecycle Manager.

When the user initiates pre-validation, the LCM agent gets deployed and bootstrapped on all the windows servers along with some configuration metadata. The agent binaries are kept at a default folder `C:\Program Files (x86)\VMware\LCMAgent\` in the windows machine.

Once the agent binaries are pushed a service is started with a name vRealize Suite Lifecycle Manager Agent Service pointing to the binaries which ultimately starts the agent. The agent works pull-based, where it polls in vRealize Suite Lifecycle Manager appliance to see if there are any commands tagged for the current node to be executed. After receiving a command, the agent updates back the command on every status change and finally updates the result after completion. The agent service is stopped after a complete pre-validation.

Uninstall vRealize Suite Lifecycle Manager agent

As every Windows server used for pre-check is registered uniquely, to use the same server on a different instance of the vRealize Suite Lifecycle Manager appliance, the agent has to be un-installed. To see steps to uninstall, see [KB 58871](#).

Replace the Certificate for vRealize Automation

You can replace the SSL certificate of the management site service if your certificate expires or if you are using a self-signed certificate and your company security policy requires you to use its SSL certificates. You secure the management site service on port 5480.

Prerequisites

- New certificates must be in PEM format and the private key cannot be encrypted. By default, the vRealize Automation appliance management site SSL certificate and private key are stored in a PEM file located at `/opt/vmware/etc/lighttpd/server.pem`.

Procedure

- 1 Log in by using the appliance console or SSH.
- 2 Back up your current certificate file.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 Copy the new certificate to your appliance by replacing the content of the file `/opt/vmware/etc/lighttpd/server.pem` with the new certificate information.
- 4 Run the following command to restart the lighttpd server.
- 5 Run the following command to restart the haproxy service.

```
service vami-lighttpd restart
```

```
service haproxy restart
```

- 6 Log in to the management console and validate that the certificate is replaced. You might need to restart your browser.

Note By default, vRealize Log Insight installs a self-signed SSL certificate on the virtual appliance. vRealize Suite Lifecycle Manager generates custom certificates for products during environment creation, but custom certificate generation fails for vRealize Log Insight. For more information, see KB article [55705](#).

Confirm Environment and Installation Settings

Verify that the environment and installation settings are accurate.

Procedure

- 1 Verify that the listed environment and installation settings are accurate.
- 2 (Optional) Click **Back** or click the relevant page in the navigation pane to change any settings.
- 3 (Optional) Click **Export** to export a configuration file with all the product and user data for this private cloud.

You can use the exported configuration file to create a private cloud. See [Create a Private Cloud Environment Using a Configuration File](#). Modify the exported configuration file as required before using it create another private cloud. The Private and primary key is not included in the exported config file while deploying an exported file. You need to manually insert those keys.

Update/modify the exported configuration file as required before using it create another private cloud.

- 4 Click **Finish**.

vRealize Suite Lifecycle Manager creates the private cloud environment and begins installing the selected vRealize Suite products in the background.

What to do next

To monitor product installation progress, click **Home**. Installation progress appears under **Recent Requests**.

Import an Existing Environment using Installation Wizard

You can use the installation wizard to import an existing private cloud environment for a vRealize Suite product.

Prerequisites

- Verify that you have an existing vRealize Suite instance.
- Verify that you have an existing datacenter.

- Verify that you have created or imported a certificate.

Note Certificate is not required for importing an existing environment, however, it is required when you select both import and new install in one flow while creating an environment.

Procedure

- 1 Log in to vRealize Suite Lifecycle Manager as an LCM Admin or LCM Cloud Admin and click **Create Environment**.
- 2 After entering the environment data fields, under each of the required vRealize Suite product, select **Import** and click the required vRealize Suite product checkbox on the top of the suite product name.
- 3 Click **Next**.
- 4 In the launched Install wizard, under **Products Details** page, update the details and select all the vCenters where all product components are installed.

If you select a combination of import and install for two or more products while creating an environment, then enter the details as a new Install of product. If you are opting for an organic growth by adding another product after creating an Environment with **New Install** or combination of **Import** and **New Install**, then the details in Install wizard is already pre-populated. You can go ahead and click **Next**. If you are opting for an organic growth by adding another product after creating an Environment with **Import** only, then the details in Install Wizard are not be pre-populated. As you have never provided those details while creating the environment.

After you import a product for a scale out, you need to add a certificate. To manage a certificate you need to add the certificate from the settings tab and then import during scale out.

- 5 Read the summary and click **Submit**.

Import VMware Identity Manager Environment

You can import an instance of VMware Identity Manager into vRealize Suite Lifecycle Manager.

Procedure

- 1 After creating an environment on the Create Environment page, on the products card, select VMware Identity Manager check box.
- 2 Select **Import** and click **Next**.
- 3 Enter a valid FQDN address. To import a clustered VMware Identity Manager use load balancer host name.
- 4 To import Tenancy Enabled VMware Identity Manager, enter the **Default Tenant Alias Host Name**.
- 5 The System Admin, Admin, SSH User, and Root passwords are listed automatically.

- 6 Enter the **Default Configuration Admin Username**.
- 7 (Optional) Select the **Sync Group Members** check box and vCenter Server list.
- 8 Click **Next** and read the summary.
- 9 Click **Submit**.

Import vRealize Business for Cloud Environment

You can import an instance of vRealize Business for Cloud into vRealize Suite Lifecycle Manager.

Prerequisites

Verify that you have the required IP credentials.

Procedure

- 1 After creating an environment on the **Create Environment**, on the products card, select vRealize Business for Cloud check box.
- 2 Select **Import** and click **Next**.
- 3 Enter the vRealize Business for Cloud **FQDN** and select **Root Password** from the existing locker entries. If the password does not exist in the locker, then you can create entries in the locker. Click **Add Password** from the top-right corner of the window.
- 4 Select the valid authentication type for the vRealize Business for Cloud instance.
 - a If an authentication type is Standalone, then proceed to select a valid vCenter Server.
 - b If an authentication type is VMware Identity Manager, then provide the identity manager **FQDN**, admin **User Name** and select the admin **User Password**.
 - c If an authentication type is vRealize Automation, then provide relevant details for the **vRA Cafe FQDN**, **vRA Cafe SSO Admin User name**, and select **vRA Cafe SSO Password** from the list of the pre-populated passwords.
- 5 Select a valid vCenter Server from the list. If the vRealize Business for Cloud instance has collector nodes spread across multiple vCenters, then all those vCenters should be selected, else the import operation fails.
- 6 Click **Next** and read the summary.
- 7 Click **Submit** to import.

Import vRealize Automation Environment

You can import an existing instance of vRealize Automation.

For creating a global environment, you will still be prompted to install VMware Identity Manager if you have skipped this step when you initially installed vRealize Suite Lifecycle Manager. To install VMware Identity Manager, see [Install VMware Identity Manager in vRealize Suite Lifecycle Manager](#). To import the vRealize Automation 8.0 brownfield environment, verify that the VMware Identity Manager present in vRealize Suite Lifecycle Manager is same as the VMware Identity Manager registered with vRealize Automation. Ensure to use the same configuration admin user for both VMware Identity Manager and vRealize Automation in vRealize Suite Lifecycle Manager.

Prerequisites

Verify that you have the required IP credentials.

Procedure

- 1 After creating an environment on the Create Environment page, on the products card, select vRealize Automation check box.
- 2 Click **Import** and click **Next**.
- 3 Under Products Details, enter the required fields to configure the vRealize Automation properties, select the **Import** version.
- 4 If you have selected 8.x
 - a Provide the Primary node Hostname.
 - b Select **Primary Node root Password**.

Note If each node has different passwords then the import request fails. You can provide the correct password in the retry of each failed request.

- c Select the **vCenter Server** where product nodes are residing. For more information on configuring vRealize Automation, see [Points to remember while Configuring vRealize Automation](#).
- 5 If you have selected 7.x
 - a Select a vCenter Server instance under vCenter Server.
 - b Click **Next** and read the summary.

When importing vRealize Automation, you have to enter specific details regarding the vRealize Automation and application. Default Tenant Administrator Password is one such input. The default tenant is set to `vsphere.local` and it is non-editable, you might find it blocked if in case the `vsphere.local` tenant is not configured in your vRealize Automation setup. The cause for this is mainly because you may have opted against configuring out of the box sample content during installation. You must enter the password for the system administrator against the field **Default Tenant Administrator Password** and then proceed with the import.

- 6 Click **Submit**.

Import vRealize Network Insight Environment

You can import an existing environment of vRealize Network Insight.

Prerequisites

Verify that there is an instance of vRealize Network Insight along with its user credentials available.

Procedure

- 1 After creating an **Create Environment** page, on the products card, select the vRealize Network Insight check box.

- 2 Click **Import** and click **Next**.

- 3 On the Product Details page, enter the **vRNI Admin user name**.

All authorization token and csrf tokens are generated using admin user name and password.

- 4 Enter the **Console Password** and **Support Password**.

With console user and support user credentials, you can run vRealize Network Insight specific commands and debug your environment.

Note Support password of all nodes must be same. Although, import of vRNI can be successful but future operations like upgrade precheck, upgrade, password update, clustering fails. You have to change the support password of all nodes to one single password. Similarly, console passwords of all nodes must be same. However, console and support password can be same across all nodes. If each node has different passwords then the import request fails. You can provide the correct password in the retry of each failed request.

- 5 Enter the **vRNI Admin Password** and **Platform IP** address.
- 6 Select the vCenter Server Instance from the drop-down menu and click **Next**.
- 7 Review the Request Summary and click **Submit**.

Example: Example for Console and Support Password

In a 2 Node cluster

- Platform: support password=VMware1! consoleuser password=Test@123
- Collector: support password=VMware1! consoleuser password=Test@123

In a 3 Node cluster with 1 collector

- Platform1: support password=VMware1! consoleuser password=Test@123
- Platform2: support password=VMware1! consoleuser password=Test@123
- Platform3: support password=VMware1! consoleuser password=Test@123
- Collector: support password=VMware1! consoleuser password=Test@123

Import vRealize Operations Manager Environment

You can import an instance of vRealize Operations Manager into vRealize Suite Lifecycle Manager.

Prerequisites

Verify that you have the required IP credentials.

Procedure

- 1 After creating an environment on the Create Environment page, on the products card, select vRealize Operations Manager check box.
- 2 Select **Import** and click **Next**.
- 3 Enter the vRealize Operations Manager, **Master Node IP Address**, **Root**, and **Admin Password**.

Note The admin password should be for a local user only, not a user with administrator permissions.

Note If each node has different passwords then the import request fails. You can provide the correct password in the retry of each failed request.

Note The master node is now referred to as the primary node.

- 4 Select a vCenter Server instance under **vCenter Servers**.
- 5 Click **Next** and read the summary.
- 6 Click **Submit** to import.

Note If you are importing an existing vRealize Operations Manager installation, then SSH should be enabled for all the vRealize Operations Manager nodes and set root passwords in all nodes.

Import vRealize Log Insight Environment

You can import an instance of vRealize Log Insight into vRealize Suite Lifecycle Manager.

Prerequisites

Verify that you have the required IP credentials.

Procedure

- 1 After creating an environment on the **Create Environment** page, on the products card, select vRealize Log Insight check box.
- 2 Select **Import** and click **Next**.

- 3 Enter the vRealize Log Insight **Master Node FQDN**, **Root**, and **Admin Password**.

Note The admin password should be for a local user only, not a user with administrator permissions.

Note If each node has different passwords then the import request fails. You can provide the correct password in the retry of each failed request.

Note The master node is now referred to as the primary node.

- 4 Select a vCenter Server instance under **vCenter Servers**.
- 5 Click **Next** and read the summary.
- 6 Click **Submit** to import.

Create a Private Cloud Environment Using a Configuration File

You can create a private cloud environment using a product configuration file.

Know more about [Private Cloud](#), before you configure your environment.

When you are creating an environment using a JSON spec, if the Locker ID for the passwords is used, you must make sure to use respective locker ID from the current vRealize Suite Lifecycle Manager. Navigate to **Locker > Passwords** and copy the Password ID, and use in the spec. There is no action required for a plain text password.

While using JSON spec, ensure to update all the parameters under each node's advanced settings as required. If you do not update, then it takes the original values from the JSON spec.

Prerequisites

- Configure OVA settings for the products to install. See [Configure Product Binaries](#).
- Ensure that you have added a vCenter to the data center with valid credentials and the request has completed.

Procedure

- 1 Log in to vRealize Suite Lifecycle Manager as administrator and click **Create Environment**.
- 2 From **Data Center**, select an existing data center for this environment, or click **+** to add a data center to vRealize Suite Lifecycle Manager.

For information on adding a data center, see [Add a Data Center to vRealize Suite Lifecycle Manager](#).

- 3 (Optional) Select **Join the VMware Customer Experience Program** to join CEIP for this environment.

This product participates in the VMware Customer Experience Program (CEIP). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

- 4 Click the **Use Configuration file** toggle feature.
- 5 Paste the text of the product configuration JSON file into the **Product Config JSON** text box, and click **Next**.

You can download the configuration file from the summary page to create a JSON file for the product or the solution with the latest inputs that were provided while configuring the environment.

The create installation wizard is launched and the JSON data is populated. You can validate the data before you click submit. For more information on getting a sample JSON file, see KB article [75255](#).

What to do next

To monitor product installation progress, click the **Home** button. vRealize Suite Lifecycle Manager displays installation progress for the environment under **Recent Requests** and on the **Requests** tab.

Managing Private Cloud Environments

4

You can manage data centers, vCenters Servers, and vRealize Suite products in your private cloud environments.

This chapter includes the following topics:

- Day 2 Operations for Global Environment in vRealize Suite Lifecycle Manager
- Day 2 Operations with Other Products In vRealize Suite Lifecycle Manager
- Accessing Lifecycle Operations
- Lifecycle Manager with a Dashboard
- Add a Product to an Existing Private Cloud Environment
- Add a Data Source to an Existing Private Cloud Environment
- Manage a Data Source in an Existing Private Cloud Environment
- Update Bulk Passwords for Data Source
- Scale-Out VMware Identity Manager
- Scale-Out vRealize Suite Products
- Scale-Up vRealize Suite Products
- Export a Private Cloud Environment Configuration File
- Download Private Cloud Product Logs
- Delete an Environment
- Managing vRealize Suite Products in a Private Cloud
- Configure Health Monitoring for the vRealize Suite Management Stack
- Adding and Managing Content from Marketplace

Day 2 Operations for Global Environment in vRealize Suite Lifecycle Manager

A global environment is created after an installation or a migration of vRealize Suite Lifecycle Manager. A global environment displays the VMware Identity Manager instance and also shows the version. When you click the **View Details** on a created environment, you can view the

lists of primary, secondary, and connector information of the VMware Identity Manager that is used in the vRealize Suite Lifecycle Manager. You can view the product properties for each the VMware Identity Manager cluster. To view the list of inter-product configurations, click the **Product References**.

After upgrading to 8.1, all products currently integrated with global environment VMware Identity Manager will be shown in this list. Starting from vRealize Suite Lifecycle Manager 8.1, the global environment VMware Identity Manager **View Details** page contains the day-2 operations:

- **Trigger Cluster Health** - Triggers instant health check on the VMware Identity Manager cluster nodes and provides a notification on vRealize Suite Lifecycle Manager UI.

Based on the health status of the cluster nodes, 'vIDM vPostgres Cluster Health' notification is either marked CRITICAL or OK. For the notification to be precise, verify that VMware Identity Manager can communicate to all the VMware Identity Manager nodes in the cluster and the global environment VMware Identity Manager inventory is up-to-date in vRealize Suite Lifecycle Manager.

The health check includes postgres service status check, pgpool service (responsible for automatic failover) status check and Delegate IP (database load balancer IP) availability check apart from basic the VMware Identity Manager service availability checks.

If status is marked CRITICAL, to troubleshoot, a link to the KB article [75080](#) is provided. This health check also runs every hour as a scheduled job at the backend and latest health statuses are updated in the 'vIDM vPostgres Cluster Health' notification.

If VMware Identity Manager is clustered through vRealize Suite Lifecycle Manager, then the Power ON option can also be used to remediate the critical cluster health.

- **Power ON** - Turns up the VMware Identity Manager nodes and ensures all the required services are bootstrapped. For a clustered instance (vRealize Suite Lifecycle Manager clustered VMware Identity Manager), this operation fixes any inconsistency in the cluster. For example, fixing the Delegate IP (database load balancer IP), correcting any replication delays in the secondary nodes . If VMware Identity Manager is clustered through vRealize Suite Lifecycle Manager, then use this option for any use case which involves powering on the cluster like snapshot revert, reboot, power on .
- **Power OFF** - Brings down all the VMware Identity Manager services by shutting them down and also brings down the services that are responsible for an automatic failover, and its related components in a clustered deployment. This option is provided for both single node and clustered node VMware Identity Manager.

If VMware Identity Manager is clustered through vRealize Suite Lifecycle Manager, then it is always recommended to use this option for a scenario which involves bringing down the cluster, such as reboot and shut down. Creating VMware Identity Manager snapshot through vRealize Suite Lifecycle Manager stores the snapshot after bringing down the VMware Identity Manager services gracefully.

Note A change in VMware Identity Manager certificate requires retrust of VMware Identity Manager certificate on all products or services currently integrated with it. While updating certificate, you can select all currently referenced products to opt in for retrust. For more information on product references, see [Product References](#). To know more about the hardware requirements depending on the number of users in the directory, see [System and Network Configurations Requirements](#).

Re-Size Hardware Resources for VMware Identity Manager

This topic describes how to re-size the hardware required for VMware Identity Manager when it is deployed through vRealize Suite Lifecycle Manager.

Procedure

- 1 On the Global Environment VMware Identity Manager, click the ellipses and click **Cluster Health**.

After the cluster health collection is complete, the health status is displayed in the vRealize Suite Lifecycle Manager under the notification lists on the top right of the UI.

Note If the status is red, to remediate click **Power ON** or see the KB article [75080](#).

- 2 To shut down the nodes with the VMware Identity Manager instance, click **Power Off**.
- 3 In the vCenter Server, navigate to **Edit** settings of VMware Identity Manager appliances and increase the resources like CPU, RAM, and Storage as recommended.
- 4 To power on the VMware Identity Manager, click **Power On**.

Results

For more information on hardware requirements for VMware Identity Manager when integrated with vRealize Automation, see the hardware requirements in the [vRealize Automation 8.1 Reference Architecture](#). To know more about the hardware requirements depending on the number of users in the directory, see [System and Network Configurations Requirements](#).

Day 2 Operations with Other Products In vRealize Suite Lifecycle Manager

You can now perform the Day 2 operations within vRealize Suite Lifecycle Manager.

Day 2 Operations for all products (Non VMware Identity Manager)

Starting from vRealize Suite Lifecycle Manager 8.1, all products under environments consists of the following:

- **Re-Trust With Identity Manager** - Whenever VMware Identity Manager certificate changes there is a need for all products/services currently integrated with VMware Identity Manager to retrust the VMware Identity Manager certificate. Even though starting from vRealize Suite Lifecycle Manager 8.1, when replacing or changing VMware Identity Manager certificate all products integrated with VMware Identity Manager that are linked in Product References are opted-in for an automatic retrust. This button can be used anytime when you want to retrust VMware Identity Manager certificate on the product explicitly.

Note This option is only applicable if a product is integrated with global environment VMware Identity Manager and shows up in the Product References table under global environment VMware Identity Manager.

- **Re-Register With Identity Manager** - When products integrate with VMware Identity Manager, it gets registered against a VMware Identity Manager endpoint which in general is with the FQDN of VMware Identity Manager. Whenever VMware Identity Manager FQDN changes, there is a need for products or services currently integrated with VMware Identity Manager to re-register with the new VMware Identity Manager FQDN.

Day 2 Operations for vRealize Automation Clustered Deployment

If the vRealize Automation load-balancer is configured such that SSL is terminated at the load-balancer, then for any change of certificate in the load balancer must be retrusted in vRealize Automation. Starting from vRealize Suite Lifecycle Manager 8.1, a clustered deployment of vRealize Automation 8.x, you can click **Re-trust Load Balancer** which retrusts the load balancer certificate in vRealize Automation.

Note This operation primarily checks vRealize Suite Lifecycle Manager inventory of the clustered vRealize Automation 8.x before performing the retrust. From vRealize Suite Lifecycle Manager 8.1 onwards, the inventory data for clustered vRealize Automation 8.x will have a parameter - `vra-va-SSL terminated at load-balancer` under the **Cluster VIP** section of product properties. The parameter decides whether the SSL is terminated at the vRealize Automation load balancer or not. For all green text box vRealize Automation 8.x deployments, this option is provided as an input to be filled by the user and for an existing brown field deployment, the value for the parameter is automatically computed.

Note Starting with vRealize Suite Lifecycle Manager 8.2, start up and shutdown operations are also available for vRealize Automation, which helps to gracefully start and shut down the vRealize Automation services.

Reconfigure Internal Pods and Service Subnets

Starting with 8.2, you can modify the IP range that is used internally by vRealize Automation services.

Prerequisites

Verify that a product has existing internal IP range values. For information on K8 service and cluster IP range, see [Install and Configure vRealize Automation 8.2 Using Easy Installer](#) .

Procedure

- 1 From the Environment page, select a product card, and then click the vertical ellipses.
- 2 Select **Reconfigure Internal Pods and Service Subnets**.
- 3 Enter internal IP range values for **K8 Cluster IP Range** and **K8 Service IP Range**.
- 4 Click **Next**.
- 5 To validate the IP range information, click **RUN PRECHECK** , and click **Finish**.

Accessing Lifecycle Operations

To start using Lifecycle Manager, access Lifecycle Operations on the Dashboard.

Lifecycle Manager with a Dashboard

The vRealize Suite Lifecycle Manager 8.0 includes a new dashboard which acts as a single pane of glass comprising of all the functionality as applications.

The dashboard consists of the applications:

Lifecycle Operations

Use this application on the dashboard to access the vRealize Suite Lifecycle Manager to manage the Day 0 to Day N operations of the vRealize Suite Products, including vRealize Network Insight.

Locker

Use this application to manage certificates, and licenses. You can create and import certificate including CSR. You can also validate the certificates before applying or replacing the certificates.

Identity and Tenant Management

You can manage active directories and tenants, and assign roles to users or groups.

Marketplace

Use the vRealize Suite Lifecycle Manager to add and manage content from Marketplace.

Content Management

You can use this application to access the Content lifecycle in vRealize Suite Lifecycle Manager to manage software-defined data center (SDDC) content, including capturing, testing, and release to various environments, and source control capabilities through GitLab or bit bucket integration. With Lifecycle Manager 8.0, you can capture multiple contents from a source control and check in those contents to another source-control or even a different branch.

Add a Product to an Existing Private Cloud Environment

If you want to change your environment, you can add a product to an existing environment.

Organic growth allows you to import an existing vRealize Suite product to an existing environment or to trigger a fresh deployment of the product to add to an existing environment.

An environment can contain only one instance of each supported vRealize Suite product.

Prerequisites

Have an existing private cloud environment in vRealize Suite Lifecycle Manager that does not already contain all of the supported vRealize Suite products.

Procedure

- 1 Click **Manage Environments**.
- 2 Click the ellipsis (...) for the environment, and select **Add Products** to perform organic growth.
- 3 Select the products to add and enter the necessary configuration information.

Add a Data Source to an Existing Private Cloud Environment

You can add a data source to your environment to collect network information.

Prerequisites

Have an existing vRealize Network Insight instance in vRealize Suite Lifecycle Manager.

Procedure

- 1 Click **Manage Environments**.
- 2 Click **View Details of Environments** where you must add the data source.
- 3 Click the ellipsis (...) for vRealize Network Insight, and select **Add Data Source**.
- 4 Enter the required details and click **Submit Request**.

Data Operations Supported by vRealize Network Insight

You can add all types of data sources that are supported by vRealize Network Insight.

Data Source	Description
VMware vCenter	You can enter the vCenter related information in the provided fields along with the proxy details.
VMware NSX Manager	You can enter the NSX Manager related information in the provided fields along with the proxy details.
Routers and Switches	You can enter the SNMP configuration details in the provided fields by clicking the Advanced Settings .
Note You can add similar data sources to the vRealize Network Insight that are specific to its respective products or functionalities.	

Import Data sources in vRealize Suite Lifecycle Manager

You can import data sources in bulk into vRealize Network Insight through vRealize Suite Lifecycle Manager. This feature is helpful when the same SNMP or other configurations have to be used for multiple switches. The common configurations along with other variable parameters such as IP address need to be imported in vRealize Suite Lifecycle Manager and provisioned into vRealize Network Insight. With vRealize Suite Lifecycle Manager 8.2, you can import data sources along with an import of a vRealize Network Insight instance.

Prerequisites

Verify that you have an existing vRealize Network Insight instance.

Procedure

- 1 From a vRealize Network Insight environment card, right click on the vertical ellipses and select **Add Data Sources > Bulk**.
- 2 Select CSV or JSON format to import the data sources in a defined report format.
- 3 Click **SELECT File** , and then select the JSON file, and click **Next**.
- 4 Click **Submit Request**.
To view the request status, view them on the Request page.
- 5 To update the CSV file in the required format, click **Download Template**.

Manage a Data Source in an Existing Private Cloud Environment

Starting with vRealize Suite Lifecycle Manager 8.2, you can edit or delete a data source in your environment.

Prerequisites

Verify that you have created a vRealize Network Insight data source in vRealize Suite Lifecycle Manager.

Procedure

- 1 In the vRealize Suite Lifecycle Manager 8.2 dashboard, click **Manage Environments**.
- 2 In the Environments page, select the vRealize Network Insight product card, and then click **View Details**.
- 3 Click **EDIT DATA SOURCE** or **DELETE DATA SOURCE**, as applicable.
 - a If you click **DELETE DATA SOURCE**, the selected data source is deleted.

Note If a data source is referenced in any other data source of vRealize Suite Lifecycle Manager, you cannot delete the referenced data source.

- b If you click **EDIT DATA SOURCE**, you can edit the Collector (Proxy) VM, data source username, data source password, and the data source nickname.

Note By default, the data source IP address/FQDN is disabled.

- 4 Click **SUBMIT**.

Update Bulk Passwords for Data Source

You can now perform a bulk password update for data source passwords.

Prerequisites

Verify if you have already created vRealize Network Insight data source passwords in vRealize Suite Lifecycle Manager.

Procedure

- 1 Under Environments, select the data sources you want to update.
- 2 Select vRealize Network Insight product card, and click the vertical ellipses for the environment, and then click **Change Data Sources Password**.
- 3 Under Select Data Sources, select the data sources that you want to update, and then click **Next**.
- 4 Under Update Credentials, click **New Password** to change the existing password, and then click **Next**.

Note If you select multiple data sources to update passwords, the new password applies to all the selected data sources.

- 5 Under Precheck details, click **RUN PRECHECK** to validate the new passwords, and then click **Next**.
- 6 Under Summary, you can verify the changes for the data sources.

7 Click **Finish**.

Note When you perform a bulk password update and one or more passwords fail to update, the request is marked complete, but you will receive a warning message for the passwords which are not updated. Click the data source details for information, and then retry updating the bulk passwords.

Scale-Out VMware Identity Manager

You can increase the HA option in VMware Identity Manager by having one or three nodes to manage VMware Identity Manager.

- Ensure to take snapshots of VMware Identity Manager nodes before you perform scale-out operations. VMware Identity Manager cluster is always three node including an existing node.
- Verify that there is a certificate already added in the locker and also perform the replace certificate on the standalone VMware Identity Manager node. The certificate should also have SAN entries of all the three nodes or wild-card certificate. For information on replacing certificate, see [Replace Certificate for vRealize Suite Lifecycle Manager Products](#).

Note If you apply [KB 87185](#) patch on a single node appliance, and then perform scale-out to cluster operations, follow KB 87185 to apply the patch on the scaled out nodes.

Prerequisites

For a VMware Identity Manager cluster and replace certificate actions, ensure to take a snapshot of the VMware Identity Manager nodes.

Procedure

- 1 Navigate to **Environments**, on the environment page, click **Add Component**.
- 2 Enter the **Infrastructure** details and click **Next**.
- 3 Enter the **Network** details and click **Next**.

Verify that the primary node and the additional components use the same default gateway and they are connected with each other.

- 4 On the Product Properties, the certificate details are auto-populated.
- 5 On the Components tab, click **Secondary** for the scale-out.

Enter the load balancer FQDN and a database cluster IP. The Database IP should be different from the VMware Identity Manager load balancer IP and it should have a DNS entry. For more information on load balance, see [vRealize Automation Load Balancing](#).

- 6 Enter the load balancer Host name.

- 7 Enter a delegate IP address.

Note The delegate IP address is used internally as a proxy to postgres master (primary) and it should be free or an available IP address. This is not same as the one used to load-balance the application.

Note You can add two components of type secondary and provide FQDN, and IP address. It is recommended for a VMware Identity Manager cluster to contain of three nodes behind a load balancer.

- 8 Click and run the pre-check.

- 9 Click **Submit**.

Note It is very important to reboot the appliance, otherwise the scale-out procedure fails with `unable to find root certificate` error. The errors occurs because of an existing product issue after you replace the certificates to reboot the appliance.

Scheduled Health Check

Once VMware Identity Manager is clustered through, a scheduled health check is registered. This scheduled check runs every hour and might pop-up a notification on the overall postgres cluster health status.

There are various checks that are important from a postgres cluster perspective that requires attention.

- 1 VMware Identity Manager nodes reachability from vRealize Suite Lifecycle Manager.
- 2 DelegateIP assignment to any of the cluster nodes.
- 3 Postgres primary node existence.
- 4 Postgres nodes having replication delay.
- 5 Postgres nodes being marked as down in the cluster.
- 6 Pgpool primary node existence.
- 7 Pgpool running on all nodes.

All the above checks are captured and appropriate description messages are displayed in the notification that pops-ups with a message like `vIDM postgres cluster health status is critical`. For more information on the steps, see the KB article [75080](#).

If all the checks are validated, vRealize Suite Lifecycle Manager gives a notification with a message as `vIDM postgres cluster health status is ok` that provides a healthy cluster status. On a Day-2 operation, you can also click the Trigger Cluster Health on the Global Environment for VMware Identity Manager in addition to scheduling the health check on an hourly basis. For more information on trigger cluster health, see [Day 2 Operations for Global Environment in vRealize Suite Lifecycle Manager](#).

Scale-Out Tenant Enabled VMware Identity Manager

A tenant enabled VMware Identity Manager can only be accessed through tenant FQDNs scaling-out a tenant enabled VMware Identity Manager from a single node to a three node cluster behind a load balancer requires changes to its DNS and certificate requirements.

All the VMware Identity Manager tenant FQDNs must now point to the load balancer IP address instead of VMware Identity Manager a single node IP address. And VMware Identity Manager load balancer certificate must hold all the tenant FQDNs. For more information on Mandatory Certificates and DNS Requirements, see [Multi-Tenancy Model](#).

The same recommendations are provided to you as a manual pre-requisite to select before scaling-out global environment VMware Identity Manager from vRealize Suite Lifecycle Manager UI. For more information on Tenant FQDNs, see [Multi-Tenancy Model](#).

Scale-Out Windows Connector

You can opt for scaling out a Windows connector.

Prerequisites

Follow these prerequisites for a Windows system in which the connector will be installed.

- The supported JRE version is between 8 update 181 to 8 update 251.
- The supported .NET framework version is 4.6.0.
- The supported Windows Server versions are 2012 R2, 2016, and 2019.
- A unique Windows system is required for the migration and it must be connected to a domain server.

Procedure

- 1 Navigate to **Environments** on the environment page, and then click **Add Components**.
- 2 Enter the **Infrastructure** details and then click **Next**.
- 3 Enter the **Network** details and then click **Next**.

Verify that the primary node and the additional components use the same default gateway and they are connected with each other.

- 4 On the Product Properties, the certificate details are auto-populated.
- 5 On the Components tab, select **Windows Connector**.
 - a Enter the **Windows VM Name**.
 - b Enter **FQDN**.
 - c Enter a user-defined Windows **Connector Name**, and then select the **Connector Admin Password**.
 - d Enter the **Domain Admin** details.

- 6 Click and run the pre-check.
- 7 Click **Submit**.

Scale-Out vRealize Suite Products

You can add components to your product to configure a multi node setup to form a cluster.

Prerequisites

vRealize Suite Lifecycle Manager does not allow you to add a component of a product until the certificate mapping for that product is created in the locker. When you replace the vRealize Automation certificate using the new certificate added to locker, the new certificate contains additional host entries for new components which should be added as part of scale-out. After you import or create a certificate in the locker, apply this certificate in the product, only then the additional components will be visible in the product.

To map the certificate for the product in the locker, import the product certificate in the locker and trigger the inventory sync for that product. This creates a reference for that product with the certificate in the locker. This is applicable for an import scenario.

Verify that the certificate is replaced in the product where the certificate contains all the product components host names including the Load Balancer host name and a new additional component host names that are added is also specified. For more information on replacing certificates, see [Replace Certificate for vRealize Suite Lifecycle Manager Products](#). For more information on load balance, see [vRealize Automation Load Balancing](#).

Procedure

- 1 On the environment card, select a product, click the vertical ellipses, and select **Add Component**.

For an imported environment, manually enter the text boxes for the selected product.

Note At times, scaling out patched products from vRealize Suite Lifecycle Manager might fail. This is because joining the cluster fails due to version mismatch in the product appliances. You can download and use the OVA corresponding to the patch. When you click Add Component, a warning message appears indicating whether the OVA required to scale out the patched product is available or not in the vRealize Suite Lifecycle Manager. The required OVA bundle can be downloaded from My VMware Portal into the vRealize Suite Lifecycle Manager appliance and mapped. You can download and map the patched product binaries. For more information on how to download the patch product binaries, see [Configure Your Patched Product Binaries](#).

- 2 Under the **Infra** details, select the required **vCenter Server**, **Cluster**, **Network**, **Datastore**, and **Disk Format** from the drop-down menus.
- 3 Select the **Applicable Time Sync** mode and click **Next**.

- 4 Under the **Network** details, if the environment is a newly created, then the text boxes are auto-populated. If the environment is imported, you have to manually enter the text boxes.

- 5 Click **Next**.

- 6 Select the **Applicable Time Sync Mode** and under the components section, select the node.

The advanced setting provides more information on configuring the selected node in a cluster. For an imported environment in 2.0 where a product is scaled out, ensure that the provided certificate is primary-node certificate, as the pre-check matches the primary node certificate. For environments from older vRealize Suite Lifecycle Manager versions, you can add the older certificate during a scale-out by clicking **Add** button. This populates the older certificate data from the environment's Infrastructure properties.

- 7 Under **Component > Product properties**, select the required text boxes.

The field in this section varies for different products.

Product Name	Components
vRealize Automation 7.x	<ul style="list-style-type: none"> ■ vra-server-secondary ■ iaas-web ■ iaas-manager-passive ■ iaas-dem-orchestrator ■ iaas-dem-worker ■ proxy-agent-vsphere
vRealize Automation 8.x	secondary
vRealize Operations Manager	<ul style="list-style-type: none"> ■ Data ■ Remote Collector
vRealize Business for Cloud	VRB-Collector
vRealize Log Insight	VRLI-Worker
vRealize Network Insight	<ul style="list-style-type: none"> ■ vRNI-Platform ■ vRNI-Collector

- 8 Enter the required text boxes and click **Next**, and run **Precheck**.

- 9 Read the summary and click **Submit**.

Scale-Out Tenant Enabled vRealize Automation

Tenant enabled vRealize Automation can only be accessed through vRealize Automation tenant FQDNs, scaling-out a tenant enabled vRealize Automation from a single node to a three node cluster behind a load-balancer requires changes to its DNS and certificate requirements.

For more information on Tenant FQDNs, see [Multi-Tenancy Model](#). After you scaled-out, vRealize Automation tenants must be accessed through load-balancer tenant FQDNs and DNS, and certificates changes are to be made accordingly. The same recommendations are shown to the user as a manual pre-requisite to be taken care before scaling-out vRealize Automation 8.x from vRealize Suite Lifecycle Manager UI.

Scale-Up vRealize Suite Products

Vertical Scale Up is introduced to increase the RAM, disk capacity, or vCPUs in the nodes of a cluster. The nodes of a cluster are grouped and each group consists of nodes of equal sizes. A product can have a single group or multiple groups, and if the node sizes vary across the different groups, you can scale up to standardize the node sizes.

Day 2 operations include the Vertical Scale Up operation to manage environments and avoid any performance degradation. Vertical Scale Up is supported for vRealize Log Insight, vRealize Automation, vRealize Operations, vRealize Network Insight, and VMware Identity Manager. You can increase the storage capacity for a product by scaling up the current size and adding a disk with the required capacity.

Prerequisites

Verify that you have an existing private cloud environment in vRealize Suite Lifecycle Manager that contains supported vRealize Suite products.

Procedure

- 1 From the vRealize Suite Lifecycle Manager dashboard, click **Manage Environments**.
- 2 Click **View Details** for a vRealize Suite product.
- 3 Click the ellipsis (...) for the product level operation, and then select **Vertical Scale Up**.
- 4 In the **Proceed to Vertical Scale Up** pop-up window, click **Trigger Inventory Sync**.
- 5 Click **Proceed** when the inventory sync is complete.
- 6 Select the **Node Type**, and then click **Next**.
- 7 Under **Vertical Scale-Up Details**, select **Scale Up Size** from the drop-down menu. You can select the **Additional Disk Size** (optional).
- 8 Under Advanced Settings, select the appropriate datastore for the nodes from the drop-down menus, and then click **Next**.
- 9 Click **RUN PRECHECK**.

Note If the validation is successful, a successful validation message appears. If you see an error message, follow the instructions provided in the **Recommendations** tab, and then click **RE-RUN PRECHECK**.

10 When the validation succeeds, click **Submit** to view the details of your request.

Note

- For VMware Identity Manager (vIDM), the default vIDM deployment option and vRealize Automation specified size of 8 CPU and 16 GB memory are supported. To increase the storage capacity from the additional disk space provided to vIDM 3.3.2, 70% can be assigned to `/db` and 30% to `/var`. To increase the storage capacity from the additional disk space provided to vIDM 3.3.3, 70% can be assigned to `/db` and 30% to `/opt`.
 - The `requiredCpuCount` and `requiredMemory` parameters are the overall CPU and memory parameters that are available for a node.
 - For vRealize Suite products, you provide the extra disk size to increase the capacity. The `requiredCapacity` parameter adds an extra disk to the available capacity.
 - For vRealize Automation, you select the required disk for expansion and choose how much to expand the existing disk.
 - If you are installing vRealize Automation, ensure that you deploy vIDM with the suggested size for vRealize Automation.
-

Export a Private Cloud Environment Configuration File

You can export a private cloud environment configuration file to reuse a deployment's configuration for future environment deployments.

If any data source is added in vRealize Network Insight environment, exporting of config file of this environment will have data source details. The config file can be used to create new vRealize Network Insight environment and data sources will be added automatically.

Procedure

- 1 Click **Manage Environments**.
- 2 Click the ellipsis (...) for the environment, and select **Export Configuration**.
- 3 Select the configuration file type to export from **Simple** or **Advance**, based on your requirement
- 4 Click **Save File** and click **OK**.

Earlier, the export configuration file feature was available at the LCM environment level. Starting with vRealize Suite Lifecycle Manager 1.3, you can export the configuration file at the product level also for the selected product.

The configuration file is downloaded to your browser's default download location.

What to do next

Use the configuration file to create new private cloud environments. See [Create a Private Cloud Environment Using a Configuration File](#).

Download Private Cloud Product Logs

You can download product log file bundles to share with VMware support.

Procedure

- 1 Click **Manage Environments**.
- 2 Click the ellipsis (...) for the environment, and select **Download Logs**.

Note When you click download logs on the Manage Environments page in vRealize Suite Lifecycle Manager, the link to download the support bundle does not appear. For more information, see KB article [55744](#).

Results

Downloaded logs are stored `/data/support-bundle` inside vRealize Suite LCM appliance.

Delete an Environment

You can delete an existing environment from vRealize Suite Lifecycle Manager.

In vRealize Suite Lifecycle Manager 1.1 onwards, you can delete the environment and not individual products. You cannot select a specific product within an environment to delete.

You can delete both successful and failed environment deployments. You can delete environments that are failed to deploy. From vRealize Suite Lifecycle Manager 1.2 onwards, you can delete an initiated environment as well.

Note You can rename an existing environment that is in progress or failed deployment state in vRealize Suite Lifecycle Manager. Select any product card under Environments, click the vertical ellipses for the chosen product, and select Rename Environment to edit the environment. However, you cannot rename the environment for globalenvironment.

Procedure

- 1 Click **Manage Environments** to delete a successfully installed environment, or delete a failed environment deployment listed under **Recent Requests** in Home page.
- 2 Click the three dots in the upper right corner of the environment tile, and select **Delete Environment**.
- 3 (Optional) Select **Delete related virtual machines from vCenter** to delete all virtual machines associated with this environment from vCenter server.

If you do not select this option, all virtual machines associated with this environment remain in vCenter after the environment is deleted from vRealize Suite Lifecycle Manager.

- 4 (Optional) Select **Delete related Windows machines** to delete Windows machines associated with vRealize Automation this environment.

This option is available only if you choose to delete all related virtual machines from vCenter. Ensure to confirm this action before you proceed.

- 5 Select **Delete related virtual machines from vCenter** to delete virtual machines associated with the environment.

This option is available only if you have virtual machine associated with an environment in vCenter server. If selected, then virtual machines associated to the environment is also deleted from the vCenter server. If it is not selected, then only the record of this environment is deleted from the vRealize Suite Lifecycle Manager inventory.

- 6 Click **DELETE**.

- 7 If you chose to delete virtual machines associate with the environment, verify that the list of virtual machines to delete is correct, and click **CONFIRM DELETE**.

IaaS virtual machine names do not appear in this list.

Note If the delete operation fails, an option is enabled in the environment card "Delete environment from vRealize Suite Lifecycle Manager". This action deletes the environment from vRealize Suite Lifecycle Manager and you can delete the VMs manually from the vCenter server. For brownfield import, if you fail to add a vCenter list, then delete environment confirmation dialog box does not show the VM list in that particular vCenter and you have to clean them up manually. For an organic growth, the environment card from the recent activity home page is not deleted or dimmed.

- 8 Click **CLOSE**.

Results

The environment is removed from vRealize Suite Lifecycle Manager.

What to do next

You can view the progress of the delete operation on the **Requests** page.

Managing vRealize Suite Products in a Private Cloud

You can use VMware vRealize Suite Lifecycle Manager to upgrade and patch vRealize Suite products and to download product logs.

- [Create a Product Snapshot](#)

Create a snapshot of a product to save product state at a particular point in time.

- [Inventory Sync in vRealize Suite Lifecycle Manager](#)

If you have updated any configuration outside of vRealize Suite Lifecycle Manager, then the products managed from vRealize Suite Lifecycle Manager will be out of sync. To update the configuration, you have to trigger inventory to sync.

- [Product References](#)

Starting from vRealize Suite Lifecycle Manager 8.1, product details has a new vertical tab named **Product References** listing all inter-product integrations. For example: If product A is integrated with product B or the other way, the **View Details** page of both product A and B has an entry in **Product References** table, pointing reference to each other.

- [Change your Password for vRealize Products](#)

You can change the password for the installed vRealize products. There are different types of password change options available on the Product Details page.

- [Delete a Product from an Environment](#)

You can delete a product instance from a Lifecycle Manager environment.

- [Replace License for any Product](#)

You can configure and replace license changes to vRealize Automation through the vRealize Suite Lifecycle Manager UI where you can access the product details on the environment card.

Create a Product Snapshot

Create a snapshot of a product to save product state at a particular point in time.

This procedure does not apply to snapshots of vRealize Automation database virtual machines. Snapshots of vRealize Automation database virtual machines must be taken manually rather than through vRealize Suite Lifecycle Manager.

Procedure

- 1 Click **Manage Environments**.
- 2 Click **VIEW DETAILS**.
- 3 Click the ellipses icon next to the name of the product to snapshot and select **Create Snapshot**.

Note Day 2 operations that depend on vCenter Server, such as creating a snapshot, might fail if the guest tools are not running or if the IP address/Hostname is not visible in vCenter Server. vRealize Operations Manager setup is not accessible after reverting the snapshot of vRealize Operations Manager as the vRealize Operations Manager cluster can be inconsistent state. For more information, see KB article [56560](#).

Results

vRealize Suite Lifecycle Manager saves state and configuration details for the product's virtual appliance. For more information, see KB article [56361](#).

What to do next

After you take a product snapshot, you can revert the product virtual appliance to the state of the snapshot.

Inventory Sync in vRealize Suite Lifecycle Manager

If you have updated any configuration outside of vRealize Suite Lifecycle Manager, then the products managed from vRealize Suite Lifecycle Manager will be out of sync. To update the configuration, you have to trigger inventory to sync.

If the product upgraded outside or if there is any failure in vRealize Automation or vRealize Operations Manager, inventory sync updates the correct primary node in vRealize Suite Lifecycle Manager.

If any components of products are added or deleted outside of vRealize Suite Lifecycle Manager, inventory sync is used to update them. If a product password changed outside can be updated in vRealize Suite Lifecycle Manager by syncing it with the inventory, but the request eventually fails. However, you can provide the right password when you retry.

To change the root password of vRealize Operations Manager, then you have to create a root password in the Locker and use the same to replace the vRealize Operations Manager root password through vRealize Suite Lifecycle Manager. You need not change the root password in the vRealize Operations Manager.

Also, if you modify the password directly in the application, for example, vRealize Operations Manager then you should run the inventory sync of the product in vRealize Suite Lifecycle Manager so that the modified passwords are synchronized with vRealize Suite Lifecycle Manager again. This action prompts you to provide the modified passwords during an inventory sync.

You can sync your inventories for each product and for all the products across all environments.

- Instead of navigating into each product to synchronize your inventories, you can click the horizontal ellipses on the product card and click **Trigger Inventory Sync**.
- If there are multiple environments and there are multiple products within an environment, you can click the **Trigger Inventory Sync** on the Environment page. This triggers the inventory sync on all the products in all environments.
- You can click the **View Details** of the product and then click the **Trigger Inventory Sync**. This would trigger the inventory sync for the required product alone.

Product References

Starting from vRealize Suite Lifecycle Manager 8.1, product details has a new vertical tab named **Product References** listing all inter-product integrations. For example: If product A is integrated with product B or the other way, the **View Details** page of both product A and B has an entry in **Product References** table, pointing reference to each other.

For vRealize Suite Lifecycle Manager, the table only shows VMware Identity Manager Authentication Provider references. If a product, for example vRealize Automation is integrated with global environment VMware Identity Manager and is using it as an authentication provider, then both vRealize Automation and the global environment VMware Identity Manager will have a reference linking each other in their **View Details > Product References** table.

The Product Reference entries are created when you create an environment and during an Inventory Sync. If the expected product does not show up in the VMware Identity Manager global environment Product Reference table, then validate if the Inventory Sync for the related product is selected and is completed successfully.

In-case of global environment VMware Identity Manager, the Product References are used while performing following day-2 operations:

- Certificate update or replace operation. A change in VMware Identity Manager certificate requires re-trust of VMware Identity Manager certificate on all products or services currently integrated with it. While updating certificate, you are provided with an option to select all currently referenced products to opt-in for re-trust.
- Enabling tenancy. Once tenancy is enabled, VMware Identity Manager can be accessed only through tenant FQDNs. All the existing products or services currently integrated with VMware Identity Manager must go for a re-register of VMware Identity Manager against its primary tenant alias FQDN. While enabling tenancy, you are provided an option to choose all the currently referenced products to opt-in for re-register.

With Manage Environments feature in the vRealize Suite Lifecycle Manager UI, a complete inventory about each product is listed.

The Product References once found are later used in day-2 operations to ensure a life-cycle operation performed on one product does not break the current integration with other product that is linked and referenced.

Change your Password for vRealize Products

You can change the password for the installed vRealize products. There are different types of password change options available on the Product Details page.

To change the password, on the product card environment, click **View Details > Change Password**.

The following table shows the different password change option available on the product details page.

Type of Password Change	vRealize Product Name
Admin Password Change	■ vRealize Automation
	■ vRealize Operations Manager
	■ vRealize Network Insight
	■ vRealize Log Insight
	■ VMware Identity Manager
Root Password Change	■ vRealize Automation
	■ vRealize Operations Manager
	■ vRealize Business for Cloud
	■ vRealize Log Insight
	■ VMware Identity Manager
Support Password Change	■ vRealize Network Insight

Type of Password Change	vRealize Product Name
Console User Password Change	■ vRealize Network Insight
SSH User Password Change	VMware Identity Manager

Delete a Product from an Environment

You can delete a product instance from a Lifecycle Manager environment.

You can delete a product deployment from a vCenter Server. The Lifecycle Manager can delete Product Integration in a given environment for the selected product, if it is done within Lifecycle Manager while deploying products.

In case of an environment where products are imported, Lifecycle Manager does not gather information about an existing product integration within products. Therefore, you can manually remove the product integration while deleting products.

Prerequisites

Verify that there is a product existing in an environment.

Procedure

- 1 From the Environment home page, select any product instance and right-click on the vertical ellipses.
- 2 Click **Delete Product**.

Note When there are products that are internally integrated within a product, then verify the integrations before deleting the product. However, Lifecycle Manager cannot remove the external integrations in the products.

- 3 To delete all associated VMs from vCenter Server for the selected product, select the **Delete associated VMs** check box.
- 4 If you want to delete windows machines, then select **Delete associated Windows Machines** check box and click **Delete**.

Before you delete associated VMs from the vCenter Server on the **Delete Product** window, review the list of VMs and then click **Confirm Delete**.

Results

The selected suite product and its associated VMs from an environment are deleted.

Replace Certificate for vRealize Suite Lifecycle Manager Products

You can replace your existing certificates for products within the vRealize Suite Lifecycle Manager.

For replacing a vRealize Suite Lifecycle Manager VAMI/VA certificate, see [Replace Certificate for vRealize Suite Lifecycle Manager](#). For re-trust of Identity Manager, see [Day 2 Operations with Other Products In vRealize Suite Lifecycle Manager](#).

Prerequisites

Verify that a product has an existing certificate. You can either create or import a certificate in the locker. For information on creating certificates, see [Configure Certificate Within Locker](#).

Procedure

- 1 From the Environment page, select a product card and click on the vertical ellipses.
- 2 Click **Replace Certificate**.
- 3 From the **Current Certificate**, click **Next**.
- 4 Select a Certificate from the drop-down menu and click **Next**.
- 5 Select a certificate and review the certificate summary, and click **Next**.
- 6 To replace a VMware Identity Manager certificate, you must re-trust the products that are already configured. Select the product instance here and click **Next**.

By default, all the products are listed under the Re-Trust Product Certificate wizard.

- 7 (Optional) Enable the **Opt-in for Snapshot** checkbox.

Note This options enables you to take snapshots for products which do not have certificate rollback built-in. You can use this option to revert the snapshot in case of a failure to replace a certificate. And this is only applicable for vRealize Business for Cloud, VMware Identity Manager, and vRealize Network Insight.

If the replace certificate request has failed and you have selected to take a snapshot, then you can set the revertToSnapshot flag to true and then submit the failed request to rollback the operaton.

- 8 To validate the certificate information, click **RUN PRECHECK** and click **Finish**.
- 9 Click **Accept** and **Submit**.

Replace License for any Product

You can configure and replace license changes to vRealize Automation through the vRealize Suite Lifecycle Manager UI where you can access the product details on the environment card.

Prerequisites

Verify that you have the vRealize Automation instance in vRealize Suite Lifecycle Manager.

Procedure

- 1 Log in to vRealize Suite Lifecycle Manager UI.
- 2 Add License in the locker and browse to the Environment tab.

Note For information on adding license, see [Configure License Within Locker](#).

- 3 Click **View Details** on the product environment tab.

- 4 Select the **Add License** from product options (...) icon.
- 5 Click **Next** and select the required License added to Locker.
- 6 Click **Finish** to replace the License of the product.

The replace License request can be tracked in the vRealize Suite Lifecycle Manager Requests tab.

What to do next

For more information on configuring the license, see [Configure License Within Locker](#).

Configure Health Monitoring for the vRealize Suite Management Stack

When vRealize Operations Manager is part of your environment, you can retrieve and display the health status of vRealize Suite products in vRealize Suite Lifecycle Manager.

Health status information in vRealize Suite Lifecycle Manager is available only for vRealize Suite Lifecycle Manager supported products: vRealize Automation, vRealize Operations Manager, vRealize Log Insight, and vRealize Business for Cloud.

Prerequisites

If you want the health status to appear in your environment card, ensure that VMware vRealize Operations Manager is present in the same environment card along with the other vRealize Suite products. For information on adding to an existing environment, see [Add a Product to an Existing Private Cloud Environment](#). For information on creating an environment, see [Chapter 3 Creating an Environment](#).

- [Health Status in vRealize Suite Lifecycle Manager](#)
vRealize Suite Lifecycle Manager displays private cloud environment health for the environment as a whole and at the individual product level.
- [View the SDDC Health Overview Dashboard in VMware vRealize Operations Manager](#)
With vRealize Suite Lifecycle Manager, you can view detailed health status in vRealize Operations Manager.
- [Enable or Disable Health Check for Products in vRealize Suite Lifecycle Manager](#)

Procedure

- 1 Install the SDDC Management Pack in vRealize Operations Manager. You can install the SDDC Management Pack from Marketplace in vRealize Suite Lifecycle Manager or outside of vRealize Suite Lifecycle Manager.
- 2 Configure adapter instances for vRealize Log Insight, vRealize Business for Cloud, and vRealize Automation in vRealize Operations Manager.

- 3 Verify if vRealize Operations Manager SDDC Health Overview dashboard displays the health status for vRealize Operations Manager and other vRealize Suite products.
- 4 After the health status displays in the SDDC Health Overview dashboard, vRealize Suite Lifecycle Manager runs the scheduled health status.

Note

- If you have an instance of vRealize Automation 7.x in your environment, you can install End Point Operations Management agent 7.x on all nodes on vRealize Automation applications and on any new node added to the vRealize Automation cluster later.
 - This is not required for vRealize Operations Manager using VMware SDDC Management Pack 8.x.
-

Results

vRealize Suite Lifecycle Manager displays the health status of SDDC Management Pack, and retrieves the health status information from one instance of vRealize Operations Manager in a given private cloud environment. The health status applies only to the vRealize Suite products configured in the target vRealize Operations Manager instance within the private cloud environment. You must not configure additional vRealize Suite products from other private cloud environments in the same instance of vRealize Operations Manager.

Health Status in vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager displays private cloud environment health for the environment as a whole and at the individual product level.

Health Status By Color

To enable or disable health at environment level, click the vertical ellipses in the environment card. The following table presents a color-coded guide to help you determine the health status of your private cloud environment.

Color	Status
Gray	A gray status indicates one of the following scenarios: <ul style="list-style-type: none">■ vRealize Operations Manager is not part of your private cloud environment.■ vRealize Operations Manager is not configured with VMware SDDC Management Health Solution Management Pack.■ An error occurred while determining private cloud environment health.■ Health information is not yet available.
Green	vRealize Operations Manager is reporting health as Green, as per its policies, for all configured products.
Yellow	vRealize Operations Manager is reporting health as Yellow, as per its policies, for at least one configured product.
Red	vRealize Operations Manager is reporting health as Orange or Red, as per its policies, for at least one configured product.

Health status in vRealize Suite Lifecycle Manager continues to display these colors, even when you only partially configure vRealize Suite products in vRealize Operations Manager. vRealize Suite Lifecycle Manager does not attempt to determine health status of vRealize Suite products that are not configured in the private cloud environment.

View the SDDC Health Overview Dashboard in VMware vRealize Operations Manager

With vRealize Suite Lifecycle Manager, you can view detailed health status in vRealize Operations Manager.

Prerequisites

Verify that you have a valid VMware vRealize Operations Manager credentials or have VMware Identity Manager configured.

Note For SDDC management pack 4.0, there is no requirement of installing End point agents for vRealize Automation 7.4 and IaaS node.

Procedure

- 1 In vRealize Suite Lifecycle Manager, click the health status for the private cloud environment to open the SDDC Health Overview Dashboard for the environment in VMware vRealize Operations Manager.
- 2 In vRealize Suite Lifecycle Manager, click the health status for an individual product to open the summary page for that product in VMware vRealize Operations Manager. For more information, see the *VMware Marketplace*.

Enable or Disable Health Check for Products in vRealize Suite Lifecycle Manager

You can enable the health check option to check the health of an existing environment. You can use this option on a scenario when you want to evaluate vRealize Suite Lifecycle Manager environment with vRealize Operations Management Suite is installed along with SDDC MP. This health check is only available on the vRealize Operations Manager instance with a SDDC Management pack to monitor the health of the entire system.

This option first checks whether there is an environment to run at first place. Once the health checks run, it checks if there is a SDDC management health solution available and then verifies the last status of the health solution. A health check runs periodically at a scheduled interval. When you want to avoid resource usage in development environments or production environments, you might want to disable a health check.

Once the health check is disabled, the environment health is not evaluated anymore. A message is displayed on the environment card, suggesting the user to enable health check to monitor the health of environment. When a health check has run, you can see the current status of the environment. If the status is ok and the data is fetched, then you can view a message on the card as Health OK.

Adding and Managing Content from Marketplace

You can use vRealize Suite Lifecycle Manager to add and manage content from Marketplace.

Marketplace contains content plugins for vRealize Orchestrator, including vRealize Automation blueprints and OVAs, vRealize Operations Manager management packs, and vRealize Log Insight content packs, that you can download and deploy in your vRealize Suite environments.

Getting Started with Marketplace

Provide My VMware credentials and sync Marketplace metadata to begin using Marketplace in vRealize Suite Lifecycle Manager.

Prerequisites

- Verify that the vRealize Suite Lifecycle Manager virtual appliance is connected to the Internet.
- Verify that you have entered your My VMware credentials in vRealize Suite Lifecycle Manager.

Procedure

- 1 On the My Services dashboard, click **Marketplace**.
- 2 If you do not have My VMware details configured, then, click the **myvmware** link.
 - a On the Settings page of **My VMware**, click **ADD MY VMWARE ACCOUNT**
 - b Enter the **User name** and select the **Password**.
 - c Click **Validate** and **Add**.

- 3 Click the **Refresh Content from Marketplace** button.

You can also click the **Sync Content**, if you are syncing marketplace for the first time.

Results

After a few minutes, available content appears on the **Marketplace** tab.

What to do next

Search for and download content from Marketplace. See [Find and Download Content from Marketplace](#).

Find and Download Content from Marketplace

You can use vRealize Suite Lifecycle Manager to search for and download content from Marketplace.

vRealize Suite Lifecycle Manager 8.1 supports vRealize Automation 7.6, OVA installation. Each OVA are in GBs in Marketplace. If you want to download more OVAs from Marketplace then increase the data folder size to avoid the Disk Full alert. OVAs in Marketplace have large file size. If multiple OVAs are downloaded and to avoid disk storage alert, extend the storage from the system settings page.

Prerequisites

Verify that you have performed an initial Marketplace sync to load Marketplace content. See [Getting Started with Marketplace](#).

Procedure

- 1 Click **VMware Marketplace** and click the **All** tab.
vRealize Suite Lifecycle Manager displays all content available for vRealize Suite in Marketplace.
- 2 (Optional) To filter the list of available content by search terms, enter search terms into the **Search** text box.
- 3 (Optional) To filter the list of available content by product, publisher, or technology, click **Filter** and select the appropriate filters.
- 4 Click **View Details** for to learn more about the downloadable content, including what products and version the content is compatible with, user ratings for the content, and a list of related content.
- 5 Click **Download** to download the content to vRealize Suite Lifecycle Manager.

Results

Downloaded content appears on the **Download** tab of the **Marketplace** page.

What to do next

Install the content you downloaded. See [Install Downloaded Marketplace Content](#).

View and Upgrade Downloaded Marketplace Content

You can view details about content previously downloaded from Marketplace, including version number and last updated date.

Procedure

- 1 Click **Marketplace** and click the **Available** tab.
vRealize Suite Lifecycle Manager displays all content downloaded to vRealize Suite Lifecycle Manager from Marketplace.

- 2 If there is an update available for content, you can download a newer version of the content.

- a Mouseover the notification icon in the upper left corner of the content tile to verify that there is an available update.

If there are no notifications for the content, the notification icon does not appear.

If there is a newer version of the content available, vRealize Suite Lifecycle Manager displays the message `New version updates are available for the app`.

- b Click the three dots on the upper right corner of the content tile, and select **Upgrade**.
- c To download, select a version, and click **Continue**.

If you are upgrading a vRealize Automation blueprint, vRealize Orchestrator plugin, or vRealize Log Insight content pack, or upgrading a VMware vRealize Operations Manager management pack with a newer version, the previous content is overwritten with upgraded content. If you attempt to update a VMware vRealize Operations Manager management pack with the same version that is already installed, the update fails.

- 3 Click **View Details** to view information about the content, including related content and the date the content was last modified.

Install a Downloaded Marketplace Content

You can install content downloaded from Marketplace.

Prerequisites

- Download the content to install from Marketplace. See [Find and Download Content from Marketplace](#).
- Verify that the environment which you are installing have the entitlement matching the entitlement which the content supports.

Procedure

- 1 Click **Marketplace** and click the **Available** tab.

vRealize Suite Lifecycle Manager displays all content that has been downloaded to vRealize Suite Lifecycle Manager from Marketplace.

- 2 Click the three dots in the upper right corner of the tile for the content to install, and click **Install**.

- 3 Select the data center and environment to install the content, if you are installing a blueprint or OVA in an vRealize Automation, and click **Next**.

vRealize Automation and vRealize Operations Management Suite contents are tagged with license entitlements.

- 4 After selecting a data center and environment, select the tenant in which the content needs to be installed and click **Submit**.

What to do next

You can track installation progress on the **Requests** page.

Delete Content Downloaded from the Marketplace

You can delete content that you downloaded from Marketplace. However, this does not remove the content from the environments in which it is installed through vRealize Suite Lifecycle Manager.

Procedure

- 1 Click **Marketplace** and click the **Download** tab.
- 2 Click the vertical dots in the upper right corner of the tile for to delete and click **Delete**.
- 3 Click **Yes**.

Results

The content is deleted from vRealize Suite Lifecycle Manager and no longer appears under downloaded content on the **Marketplace** page.

Managing Content Lifecycle in vRealize Suite Lifecycle Manager

5

Content lifecycle management in vRealize Suite Lifecycle Manager provides a way for release managers and content developers to manage software-defined data center (SDDC). It includes content capturing, testing, and release to various environments, and source control capabilities through different source control endpoints that include GitHub, GitLab, and Bitbucket. Content developers are not allowed to set a Release policy on end-points, only Release Managers can set policies.

Migration of contents or versions is not supported from an older instance to vRealize Suite Lifecycle Manager. The latest content version can be either source control or deploy to an endpoint before moving to vRealize Suite Lifecycle Manager . So that the same content can be re-captured from the endpoint in the new instance.

Migration of endpoints and content settings are captured supported:

- All the endpoints are migrated along with source control user tokens.
- Tags associated with the endpoints are migrated to new instance.
- Pipeline stub configurations are migrated.

Note vRealize Suite Lifecycle Manager cloud admin can only perform the content management operation. When the cloud admin user gets an additional role of release manager or content developer, the cloud admin can only view the content management app inside the vRealize Suite Lifecycle Manager. But the cloud admin does not have permission to view other applications. Whereas a Release manager and a content developer user can view the content management app. As a workaround, you can perform all the cloud admin operations using cloud admin role only and do not provide additional permission or role mapping.

You can use the content lifecycle management to dispense with the time-consuming and error-prone manual processes required to manage the software-defined content. Supported content includes entities from:

Product Name	Supported Version
vRealize Automation	7.2 and later
vRealize Orchestrator	7.x and later
VMware vSphere	6.0 and later

Product Name	Supported Version
vRealize Operations Manager	6.6.1+ and later
Source Control servers	<ul style="list-style-type: none"> ■ GitHub Enterprise Server: 2.20.15, 2.19.21, and 2.21.6 (GitHub Cloud is not supported) ■ GitLab: 12.2.12 (Enterprise Edition), 12.7, and 12.8 ■ Bitbucket Server 6.10 and 7.0 ■ Bitbucket Cloud: Version 2.0

Content lifecycle management in vRealize Suite Lifecycle Manager is similar to content lifecycle management with the vRealize Code Stream Management Pack for DevOps, with the following differences.

- Content lifecycle management is deployed as part of vRealize Suite Lifecycle Manager on a single appliance. It has a new user interface and is tightly integrated with vRealize Suite Lifecycle Manager core services.
- Updated Pipeline services: Advanced capability to manage content to work with source control to support a multi-developer use case.

If there are dependencies between captured content packages, all the dependencies are captured as first class objects in vRealize Suite Lifecycle Manager. Each content version shows all its dependencies associated with it. For example, if a vRealize Automation Composite Blueprint has a dependency on Property-Definition, there are two items in the content catalog, one for each content package. With independent version control for each content package, you can edit, capture, and release dependencies independently so that the content is never old. vRealize Automation allows you to define multiple named value sets within the Size and Image component profile types. You can add one or more of the value sets to machine components in a blueprint. We cannot deploy or release Automation-Component Profiles in vRealize Suite Lifecycle Manager to a target end point if the corresponding value set already exists on the end point.

- [Working with Content Endpoints](#)

A content endpoint is an infrastructure endpoint in the software-defined data center (SDDC), such as an instance of vRealize Automation, that is targeted for the capture, test, and release of managed content.

- [Managing Content](#)

Content is a collection of files that contains definitions that represent software defined services.

- [Access Source Control](#)

Only a release manager can add a source control access, where in the source control can be GitLab or Bitbucket. With this privilege, a release manager can select the GitLab type, Bitbucket and enter the gitLab server name. You can supply multiple server names and then use the git lab personal access token and assign it to the source control server.

- [Managing Source Control Server Endpoints](#)

Before you can check in or check out content, a vRealize Suite Lifecycle Manager must add a GitLab or Bitbucket source control server to the system.

- [Working with Content Settings](#)

You can add source control server endpoint, vCenter publisher, pipeline extensibility and developer restrictions in Content Settings.

- [Content Pipeline Settings](#)

Starting with vRealize Suite Lifecycle Manager 8.0, there are only Content Pipelines and Capture pipeline are supported. In the Content Pipelines section, under the Pipelines tab, the status of the last 24 pipeline executions can be seen in the Content_Pipeline card. Each of the content pipeline executions when selected, shows the associated Capture pipelines, if any, in the Capture pipeline card. The execution representations, the colored dot in the pipeline card, can be selected to view a detailed breakdown of the various stages of the selected execution. The Content pipeline execution can contain a maximum of nine stages in the order of execution. However, the actual execution has the stages which are relevant to the execution.

Working with Content Endpoints

A content endpoint is an infrastructure endpoint in the software-defined data center (SDDC), such as an instance of vRealize Automation, that is targeted for the capture, test, and release of managed content.

You add a content endpoint to an environment to capture, test, deploy or check-in software-defined content in the form of a content package. A content package is a file that contains definitions for software-defined services, such as blueprints, templates, workflows, and so on. Each content endpoint can support more than one type of content package. For example, a vRealize Automation content endpoint can support both composite blueprints and software.

You use content endpoints to perform the following actions:

- Capture one or more content packages.
- Test one or more content packages in a staging environment.
- Release one or more tested content packages to a production environment.

- [Add a vRealize Orchestrator Content Endpoint](#)

A vRealize Orchestrator endpoint is required to create vRealize Automation endpoints and to capture content.

- [Add a vRealize Automation Content Endpoint](#)

To capture, test, deploy, or check-in a content package, add a content endpoint to an environment.

- [Add a Source Control Endpoint](#)

A source control endpoint represents a project (repository) and a source control server.

- [Add a vCenter Server Content Endpoint](#)

Add a content endpoint to an environment to capture, test, deploy, or check-in a content package.

- [Add a vRealize Operations Manager Endpoint](#)

Add a vRealize Operations Manager content endpoint to capture, test, deploy, or check-in a content package.

- [Delete a Content Endpoint](#)

You can delete an existing content endpoint.

- [Edit a Content Endpoint](#)

You can edit the settings of an existing content endpoint.

Add a vRealize Orchestrator Content Endpoint

A vRealize Orchestrator endpoint is required to create vRealize Automation endpoints and to capture content.

Prerequisites

If you are using this vRealize Orchestrator endpoint for unit testing, verify that the vRealize Orchestrator instance has been configured as a unit test server.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**.
- 3 Click **vRealize Orchestrator**.

For an Orchestrator content, you can capture workflows, configuration elements, and actions individually or in a folder where they reside.

Note If a folder is captured, a temporary content name starting with [FOLDER] is displayed. You can start a Content Pipeline to capture all content, this is then added to the vRealize Orchestrator Package provided as input.

- 4 Enter the information for the vRealize Orchestrator content endpoint.

- a In the **Name** text box, enter a unique name for the endpoint.
- b In the **Tags** text box, enter tags associated with the endpoint.

Using tags allow you to deploy content to multiple endpoints at the same time. When you deploy content, you can select a tag instead of individual content endpoint names, and the content deploys to all endpoints that have that tag.

To add multiple tags, press **Enter** after you enter each tag.

- c In the **Sever FQDN/IP** field, enter the fully qualified server name, IP address, or host name for the content endpoint server.

If the vRealize Orchestrator instance is not embedded in vRealize Automation, include the port number in the server FQDN/IP. Typically the port number is 8281. The port number 8281 is required for vRealize Orchestrator 7.x versions. For vRealize Orchestrator 8.x and above, the port is not required.

vRO-Server-FQDN:Port

- d Enter a user name and password to use to access this content endpoint.

5 Press TEST CONNECTION to test the connection to the content endpoint.

If the connection test fails, verify that the information you entered for the content endpoint is correct and try again.

6 Select vRO Package.

The vRealize Orchestrator package can be captured from an endpoint and is associated with the content endpoint. Mark the version as Production ready. Selection of a vRO package is a post deployment capability that imports the package once any other content has been deployed allowing maintained localized or regional settings.

- Ignore modules when listing content: A comma-separated list of vRealize Orchestrator Actions or modules that are excluded when listing from an endpoint to reduce the number. With Lifecycle Manager 8.0, any module or folder with or without any dependencies can be excluded while capturing or listing the content. However, for Orchestrator-package these modules or folders are not ignored. Lifecycle manager validates the content dependencies available in the source endpoint while capturing with dependencies. This depends on the policy specified on the endpoints.
- Ignore Workflows in these folders: A comma-separated list of vRealize Orchestrator Workflow folders that are excluded when listing from an endpoint to reduce the number.
- A vRO package name cannot contain special characters and can cause issues when you capture, release or check-in a content. If you have a vRO package name with a space in between the name, then the space is converted to an underscore (_) during a capture and fails during a test and deploy.

7 Select the appropriate policies for the content endpoint, and click Next.

Policy	Description
Mark as a source content endpoint to capture content	Allows you to capture content from this endpoint and mark them as a source content.
Allow Unit tests to run on this content endpoint	Allows content to be tested on this endpoint and acts as a unit test server where vRealize Orchestrator workflows test content is placed.

Policy	Description
Mark as Production content endpoint	Allows you to deploy content to production.
Source Control Enabled	Allows you to enable if you plan to check in or check out content to or from the vRO endpoint. Enabling source control is a best practice when working with multiple users or vRealize Orchestrator Endpoints in which the same content is worked on. This policy prevents non source-controlled versions be deployed to this endpoint, so that all git commit codes are maintained against this server.

8 Verify that the content endpoint details are correct, and click **Submit**.

Add a vRealize Automation Content Endpoint

To capture, test, deploy, or check-in a content package, add a content endpoint to an environment.

Prerequisites

Verify that you have added at least one vRealize Automation endpoint.

Note If the vRealize Orchestrator is embedded, then there is no need of a separate instance of vRealize Orchestrator endpoint. vRealize Orchestrator endpoint creation is needed only if you are using an external vRealize Orchestrator endpoint for vRealize Automation.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**
- 3 Click **Automation**.
- 4 Enter the information for the vRealize Automation content endpoint.
 - a In the **Name** field, enter a unique name for the endpoint.
This can be a server name or any name.
 - b Select the product version of the endpoint from the **Endpoint Version** drop-down menu.
 - c In the **Tags** field, enter tags associated with the endpoint.
With tags, you can deploy content to multiple endpoints at the same time. When you deploy content, you can select a tag instead of individual content endpoint names, and the content deploys to all endpoints that have that tag.
To add multiple tags, press **Enter** after you enter each tag.

- d In the **Sever FQDN/IP** field, enter the fully qualified server name, IP address, or host name for the content endpoint server.

While adding an endpoint for a particular tenant, tenant based FQDN has to be used as a server. However, for a system based domain, user FQDN without a tenant should be used.

IP addresses are not supported while adding vRealize Automation 8.x endpoints.

- e Enter a tenant name, user name, and password to use to access this content endpoint.
- f Select an external or embedded vRealize Orchestrator endpoint to associate from the **vRO Server Endpoint** drop-down menu.

When selecting a user account for exporting or importing content into vRealize Suite Lifecycle Manager, ensure that the account has ALL Roles selected. The **Secure Export Consumer** role allows LCM to export passwords which can be imported into alternate vRA endpoints.

- 5 Press **TEST CONNECTION** to test the connection to the content endpoint.

If the connection test fails, verify that the information you entered for the content endpoint is correct and try again.

- 6 Click **Next**.
- 7 Select the appropriate policies for the content endpoint, and click **Next**.

Policy	Description
Allow capturing content packages from this endpoint	Allows you to capture content from this endpoint.
Allow testing content packages on this endpoint	Allows content to be tested on this endpoint and acts as a unit test server where vRealize Orchestrator a workflows test content.
Allow releasing content packages to this endpoint	Allows you to deploy content to production.

- 8 Verify that the content endpoint details are correct, and click **Submit**.

Add a Source Control Endpoint

A source control endpoint represents a project (repository) and a source control server.

You can have any number of source control repositories and branches added to vRealize Suite Lifecycle Manager. Adding a source control branch allows you to check in and check out the SDDC content.

Prerequisites

- Verify that a vRealize Suite Lifecycle Manager administrator has added a system source control server under Content Settings.
- Verify that a developer has entered the GitLab access token to the source control server so that they can check-in and check out content.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**
- 3 Click **Source Control**.
- 4 Select the configured **Source Control Server** (Bitbucket Server, Bitbucket cloud, GitLab, or GitHub).
- 5 Enter the information for the Source Control content endpoint.
 - a In the **Name** text box, enter a unique name for the endpoint.
 - b Enter a **Tag** name.
 - c Enter the **Branch** and **Repository Name** to use for the content endpoint in the following format: For GitLab, enter *group_name/repository_name*, Bitbucket server, enter *project_name/repository_name* and for a Bitbucket cloud, enter *repository_name*

Note In bit bucket cloud, you can only create a repository and use the repository name. The source control endpoint with a repository must be initialized with any file. GitLab and bit bucket cloud already have a provision to add the file but the bit bucket server does not. With Lifecycle Manager 2.1, cluster and elastic search instance for multi developer story is not supported for bit bucket server.

- 6 Click **Test Connection** and click **Next**.
- 7 Select the appropriate policies for this content endpoint, and click **Next**.

Policy	Description
Enable code review	Allows a manual review between developers. vRealize Suite Lifecycle Manager content lifecycle management creates a branch with the changes that require a code review. A code reviewer can accept or reject the merge request into the branch.

- 8 Verify that the content endpoint details are correct, and click **Submit**.

Add a vCenter Server Content Endpoint

Add a content endpoint to an environment to capture, test, deploy, or check-in a content package.

Prerequisites

Verify that you have added at least one vCenter endpoint in the **Content Settings > vSphere Template Repository** .

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**

3 Click vCenter Server.**4 Enter the information for the vCenter content endpoint.**

- a In the **Name** text box, enter a unique name for the endpoint.
- b In the **Tags** text box, enter tags associated with the endpoint.

Using tags allow you to deploy a content to multiple endpoints at the same time. When you deploy a content, you can select a tag instead of individual content endpoint names, and the content deploys to all endpoints that have that tag. To add multiple tags, press Enter after you enter each tag.

- 5** In the Server FQDN/IP text box, enter the fully qualified server name, IP address, or host name for the content endpoint server.
- 6** To access the endpoint, enter the **User name** and **Password**.
- 7** Click **Test Connection** and click **Next**.
- 8** Select the appropriate policies for the content endpoint, and click **Next**.

Policy	Description
Allow content to be captured from this endpoint	Allows you to capture content from this endpoint and mark them as a source content.
Allow unit tests to be run on this endpoint	Allows content to be tested on this endpoint and acts as a unit test server where a vCenter test content is placed.
Mark as Production Endpoint	Allows you to deploy content to production. When you select this check box to mark as a release endpoint, only then Enable vCenter Template support is enabled.
Source-controlled Content only	Allows deployment of content to an Endpoint that comes only from a Source Control branch. Where in the customization specification needed has to be code reviewed and checked in prior before releasing to vCenter Server. This setting is not used for vSphere templates as they are not checked in to the Source Control. The templates have versions in a vSphere Content Library.
Enable vCenter Template Support	When you enable this option, you are prompted with more fields. The vCenter details page stores information of where the template is deployed to, in each vCenter Server. During the release process, the templates are retrieved from the local Content Library and turned into a Virtual Machine Template.

9 Click Next and provide the vCenter sever details.**10 Click Next.****11 To import an existing data center, click Import LCM Data center.**

vCenter Server settings can be added to an LCM data center, once vCenter data collection is competed this endpoint is seen when importing from LCM and reduces the time to fill in the form as all the properties have been collected. Except the Virtual Machine folder path that is provides in the format /Templates/MyTemplates/ is not imported.

Once the endpoint is created, it validates if the configuration is correct. It can connect through API and that the configuration of the local subscriber details is setup to point to the publisher as defined in `Content Settings/vSphere Template Repository`. If there is a problem, then the endpoint is disabled and an error is displayed when you cover of the warning.

Add a vRealize Operations Manager Endpoint

Add a vRealize Operations Manager content endpoint to capture, test, deploy, or check-in a content package.

Prerequisites

- Verify that the SSH user account is configured.
- Verify all vRealize Operations Manager instances contain the same management packs installed and the required adapter instances configured.
- Dashboards that are configured to refer specific objects, for example, vCenter VM, Host or Datastore are not used on the release endpoint until they are manually edited to update the reference to a specific object.

Note Some content may not release between different versions of vRealize Operations Manager where a content from 6.6 to 6.7, some content types may fail.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**
- 3 Click **vRealize Operations**.
- 4 Enter the information for the vRealize Operations Manager content endpoint.
 - a In the **Name** field, enter a unique name for the endpoint.
 - b Enter a tag name so that endpoint can use them to test or capture.
 - c Enter the **Server FQDN/IP** address.
 - d Enter the **Username** and **Password**.
 - e Enter the **SSH Username** and **SSH Password**.
 - f Click **Test Connection** and once the connection is established, click **Next**. For more information on creating an SSH user on the vRealize Operations Manager instance, see [Create an SSH User in vRealize Operations Manager](#).
- 5 Under the **Policy Settings**, select the required options to capture, test, or mark as production.
- 6 Verify that the content endpoint details are correct, and click **Submit**.

Create an SSH User in vRealize Operations Manager

You can create a vRealize Operations Manager end-point in vRealize Suite Lifecycle Manager Content Management end-point.

- 1 When you are selecting a Root as an SSH user from the content endpoint, create a user on the vRealize Operations Manager appliance. The user must have a SSH access and belong to the user group root and with a valid home directory.
- 2 Log into the vRealize Operations Manager appliance as a root user and create user on the vRealize Operations Manager appliance using below command. `useradd sshuser`.
- 3 Configure user groups for the created user - `usermod -G root,wheel sshuser`
- 4 Configure the correct home directory for the user:

```
mkdir /home/sshuser"
"chown sshuser /home/sshuser"
```

- 5 Set the password to `passwd sshuser`.
- 6 Enable the password with sudo capabilities.

Run command visudo

```
sshuser ALL = NOPASSWD: /usr/lib/vmware-vcopssuite/python/bin/python /usr/lib/vmware-vcops/
tools/opsccli/ops-cli.py *
sshuser ALL = NOPASSWD: /bin/rm -rf /tmp/*
sshuser ALL = NOPASSWD: /bin/mv /tmp/*
```

Note Use OPS-CLI for most of the vRealize Operations Manager contents to export or import a content capture or release in vRealize Suite Lifecycle Manager.

Delete a Content Endpoint

You can delete an existing content endpoint.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Endpoints**, click the vertical ellipses to the left of the endpoint, and select **Delete**.
You have to manually delete the endpoint.
- 3 Click **OK**.

Edit a Content Endpoint

You can edit the settings of an existing content endpoint.

All content endpoint values can be edited apart from the name, which is used across various logs.

Note When vRealize Suite Lifecycle Manager deploys a vRA instance or a vRA instance is imported into vRealize Suite Lifecycle Manager, then content management services imports Content endpoints (per tenant) automatically through a data collection process. By default, all policies are disabled so you must edit the endpoint and assign appropriate content policies. Only certain set of users can edit a content endpoint, for more information on roles, see [Content Actions](#).

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Endpoints**, click the vertical ellipses to the left of the endpoint, and select **Edit**.
- 3 Edit the endpoint details you want to change, and click **Next**.
- 4 Edit the endpoint policy settings you want to change, and click **Next**.
- 5 Verify that the content endpoint details are correct, and click **Submit**.

Managing Content

Content is a collection of files that contains definitions that represent software defined services.

After you add a content endpoint to one or more environments, you can manage the software-defined content that each environment contains. You can use vRealize Suite Lifecycle Manager to perform the following operations on content:

- Capture content from an endpoint
- Deploy to test and run unit tests
- Check-in content
- Release content to production

For example, a YAML file for a vRealize Automation blueprint or an XML file for a vRealize Orchestrator workflow. Content is linked together so that when you capture a vRealize Automation blueprint, all dependencies are also displayed in the content catalog, and they can each have their own versions. vRealize Suite Lifecycle Manager displays dependency information within each content version. The / Characters cannot be used in the name for Topology or Text ResourceKind Metrics as the export fails.

vRealize Suite Lifecycle Manager does not support an Azure machine in content management for testing and releasing content. XaaS blueprint "Azure Machine" is shipped by default with vRealize Automation. However, transfer of XaaS blueprint between vRealize Automation environments is not supported.

- [Add Content](#)

You can add content from an existing content endpoint.

- [Delete Multiple Content](#)

With vRealize Suite Lifecycle Manager 8.0, you can delete multiple content items and content versions. The multi delete feature can delete all the versions related to the selected content item.

- [Working with Captured Content](#)

You can capture a new version of an existing content package.

- [Content Actions](#)

After you capture a content, you can perform and view the activity of a content.

- [Content Types Available for Products](#)

The content packages available for each endpoint are displayed in the following tables.

- [Searching Content](#)

You can search an existing content based on certain defined entries within the UI.

- [Test Content](#)

You can test content to ensure it is ready for release.

- [Source Control with vRealize Suite Lifecycle Manager Content Lifecycle Management](#)

vRealize Suite Lifecycle Manager content lifecycle management integrates natively into a defined GitLab and Bitbucket branch endpoint to provide source control for content.

- [Deploy a Content Package](#)

Deploy a content package when it is ready for a production environment.

- [Multi Release of Content Package](#)

vRealize Suite Lifecycle Manager 8.0 content management allows the bulk release of content spanning different types where vSphere, vRealize Operations Manager, and vRealize Automation are deployed in one request. It provides an advanced filter option on the content type that is established from a specific content endpoint.

- [Delete a Content Package](#)

You can delete a content package from all endpoints when you no longer need the content package.

- [Content Issues You might Encounter](#)

There can be content issues that you might encounter during any content operations.

Add Content

You can add content from an existing content endpoint.

Prerequisites

Verify that you have added a content endpoint.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.

- 2 Under **Content**, click **ADD CONTENT**.

If a version has already been captured, a content can be added either with the **Add Content** button or with an inline capture.

- 3 Select test or deploy the content package in addition to capturing it, and click **PROCEED**.

- 4 Enter the capture details for the content package.

- a From the **Select Capture Endpoint** drop-down menu, you can either select one or multiple content types to capture content.

- b Enter a tag name and select **Include all dependencies** to capture any dependencies associated with the content.

You can search for content by tag within the UI/API.

- c Enter the **vRO Package Name**. Any spaces in the name are replaced with an _ underscore character and a vRO package name.

The vRO Package Name is applicable only for vRealize Orchestrator or vRealize Automation content having some vRealize Orchestrator dependencies. The field is used for managing vRealize Orchestrator contents in an efficient way. If you provide any new name, then all the vRealize Orchestrator contents will be merged to one package. If you select an existing name from the drop-down menu, then a new version of the package will be created and merges all vRealize Orchestrator contents to the version. If there exists a package version already from that endpoint, the new version will have old contents in the previous version with new contents. This helps you to work incrementally on vRealize Orchestrator contents.

If the vRealize Orchestrator package is not captured prior from a given content endpoint, then a new version is created but the content might not be the same as the previous version. Deploy the added vRealize Orchestrator package to the vRealize Orchestrator content endpoint first to append the content. If you do not enter any package name, then the name of the vRealize Orchestrator package matches to the content that is captured with an added "-vro" as part of the name. All the discovered and captured vRealize Orchestrator content, including individual workflows in the content files, appears in the vRealize Orchestrator package that is created.

- d If the content is ready for production, select **Mark this version as production ready**.
- e Enter a description for this content version in the **Comments** field.
- f Click **Next**.

Note When you list the content for the first time for an endpoint, the UI retrieves the content from the endpoint. However, once you have captured then the content is cached and an auto refresh of content list runs in the background every 30 minutes. You can select the **Get latest content** option to retrieve the content in between this time.

5 Enter test details for the content endpoint.

This option appears only if you chose to test the content package.

- a Select one or more content endpoints to specify the environments to run tests on.
- b Select **Deploy Content** to deploy the content in the endpoint before running tests.
- c Select **Stop test deployment on first failure** to stop the test deployment when it encounters an error.
- d Select **Run unit tests** to run available unit tests on the content.
- e Select **Stop unit tests on first failure** to stop testing if any unit test fails.
- f Select a server to run unit tests on from the **Select a Unit Test Server** drop-down menu.
You must have a vRealize Orchestrator test package imported to use a unit test server.
- g Click **Next**.

6 Enter the check-in details for the content package.

This option appears only if you chose to check-in the content package.

- a Select one or more content endpoints from the **Select Release Endpoints** drop-down menu to specify the production environments where the system releases the content.

7 Click **SUBMIT**.

If you have selected a single content capture, then you can view a single content pipeline. If you have selected multiple content capture, then you can see the individual capture pipelines triggered for each of the content.

Delete Multiple Content

With vRealize Suite Lifecycle Manager 8.0, you can delete multiple content items and content versions. The multi delete feature can delete all the versions related to the selected content item.

Prerequisites

Verify that you have a content item already available in the content list.

Procedure

- 1 On the My Services dashboard, click **Content Management**.
- 2 Under Content, select the content item on the check box.
- 3 Click **Actions** and select **Delete**.

When you delete the content item, the associated content versions are also deleted. If there is more than one content item, then you can select all and click delete. You can perform the multi-delete operation for upto 15 content items.

Working with Captured Content

You can capture a new version of an existing content package.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Content**, click the name of the content package to capture and click **CAPTURE**.
- 3 From the **Select Capture Endpoint** drop-down menu, select the content endpoint to capture from.
- 4 Select **Include all dependencies** to capture any dependencies associated with the content.
- 5 If the content is ready for production, select **Mark this version as production ready**.
- 6 Enter a description for this content version in the **Comments** field, and click **CAPTURE**.

Content Actions

After you capture a content, you can perform and view the activity of a content.

Deploying a Content

Content Settings	Role	Expected Behavior
Content version is production ready	Release Manager	You can view only production endpoints.
Content version is production ready	Developer	You can test endpoints that have the Test policy set, and it cannot include the Production policy.
Content version is NOT marked as production ready	Release Manager Developer	You can view the test endpoints that have the Test policy set.
Content version is NOT marked as SourceControlled	Release Manager Developer	You can view the content endpoints that do not have the Source Control policy set on the content endpoint.
Content version is marked as SourceControlled	Release Manager Developer	All the content endpoints are displayed based on other conditions in this table.

Managing Tags

Tags can be managed at a given version to navigate content within the UI. These tags can be useful as a grouping mechanism when future capability of releasing all content by tag is supported.

Content Types Available for Products

The content packages available for each endpoint are displayed in the following tables.

Content Types

Table 5-1. vSphere Content Endpoint

Content Type	Product Support Versions	Description
vSphere-CustomSpecification	vSphere vCenter 6.0+	Captures guest operating system settings saved in a specification that you can apply when cloning virtual machines or deploying from templates.
vSphere-Template	vSphere vCenter 6.0 +	Captures template to deploy virtual machines in the vCenter Server inventory.

Table 5-2. vRealize Automation Content Endpoint

Content Type	vRealize Suite Lifecycle Manager Supported Versions	Other Product Support Versions	Description
Automation-CompositeBlueprint	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.x	Captures a vRealize Automation composite blueprint to deploy virtual machines managed by vRealize Automation.
Cloud Template (vRealize Automation 8.2 release. For vRealize Automation 8.1 and earlier releases, the content type was known as Automation-CompositeBlueprint.)	vRealize Suite Lifecycle Manager 8.1 and later versions.	vRealize Automation version 8.x	Captures a vRealize Automation composite blueprint to deploy virtual machines managed by vRealize Automation.
Automation-Componentprofile	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.x	Captures a vRealize Automation component profile.
Automation-PropertyDefinition	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.x	Captures a vRealize Automation property definition for specifying custom properties.
Policy Definition (vRealize Automation 8.0 and later releases. Prior to vRealize Automation 8.0 release, the content type was known as Automation-PropertyDefinition)	vRealize Suite Lifecycle Manager 8.1 and later versions.	vRealize Automation version 8.x	Captures a vRealize Automation property definition for specifying custom properties.
Automation-PropertyGroup	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.x	Captures a vRealize Automation property group to group custom properties.
Automation-ResourceAction	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.x	Captures a vRealize Automation resource action.

Table 5-2. vRealize Automation Content Endpoint (continued)

Content Type	vRealize Suite Lifecycle Manager Supported Versions	Other Product Support Versions	Description
Automation-ResourceAction	vRealize Suite Lifecycle Manager 8.2 and later versions.	vRealize Automation version 8.x	Captures a vRealize Automation resource action.
Automation-Software	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.x	Captures vRealize Automation software component settings that govern how middleware or applications are installed, configured, and uninstalled.
Automation-Subscription	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.x	Captures vRealize Automation subscription events that are triggered using the event broker. Captures the configured event and dependent workflows.
Automation-Subscription	vRealize Suite Lifecycle Manager 8.1 and later versions.	vRealize Automation version 8.x	Captures vRealize Automation subscription events that are triggered using the event broker. Captures the configured event and dependent workflows.
Automation-XaaSBlueprint	vRealize Suite Lifecycle Manager 8.1 and later versions.	vRealize Automation version 8.x	Captures vRealize Automation XaaS blueprints.
Automation-CustomForm	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.4.x	Captures vRealize Automation Customer form.
Automation-CustomForm	vRealize Suite Lifecycle Manager 8.1 and later versions.	vRealize Automation version 8.x	Captures vRealize Automation Customer form.
Automation-ResourceType	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.2.x	Captures vRealize Automation Resource Types.
Custom Resource (In vRealize Suite Lifecycle Manager, the content type is known as Automation-Resource Type.)	vRealize Suite Lifecycle Manager 8.2 and later versions.	vRealize Automation version 8.x	Captures vRealize Automation Resource Type.
Automation-ResourceMap	vRealize Suite Lifecycle Manager 2.1 and later versions.	vRealize Automation version 7.2.x	Captures vRealize Automation Resource Maps.

Note The naming convention for vRealize Automation 8.x content type may change for the vRealize Suite Lifecycle Manager 8.3 release.

Table 5-3. vRealize Operations Manager Content Endpoint

Content Type	Product Support Versions	Description
Operations Alert	vRealize Operations Manager 6.6.1+	Captures vRealize Operations alerts containing symptom definitions and recommendations that are used to evaluate conditions and generate alerts.
Operations-Dashboard	vRealize Operations Manager 6.6.1+	Captures vRealize Operations alerts dashboard data used to determine the nature and timeframe of existing and potential issues.
Operations-Report	vRealize Operations Manager 6.6.1+	Captures vRealize Operations report templates
Operations-SuperMetric	vRealize Operations Manager 6.6.1+	Integrates vRealize Operations super metric data definition that is used to track combinations of metrics. After releasing Super Metrics, assigning the one or more object types and enabling the super metric in policies are still required. All vRealize Operations package types also support .Super Metrics, which means dashboards, alerts, vviews, and metric configurations automatically point to the correct super metric at the time of release.
Operations- TextWidgetContent	vRealize Operations Manager 6.6.1+	Reads text from a Web page or text file. You specify the URL of the Web page or the name of the text file when you configure the Text widget.
Operations- TopoWidgetConfig	vRealize Operations Manager 6.6.1+	Captures the structure of the topography around a specific resource, including parent and child resources.
Operations-View	vRealize Operations Manager 6.6.1+	Captures vRealize Operations views that help you to interpret metrics, properties, and policies of various monitored objects.
Operations-ResourceKindMetricConfig	vRealize Operations Manager 6.6.1+	Captures vRealize Operations metric configurations for particular adapter and object types so that the supported widgets are populated based on the configured metrics and selected object type.
Operations-Symptoms	vRealize Operations Manager 6.6.1+	Captures the operation symptoms.

Table 5-4. vRealize Orchestrator Content Endpoint

Content Type	Product Support Versions	Description
Orchestrator-Action	vRealize Orchestrator version 7.0+	Captures a vRealize Orchestrator action.
Orchestrator-ConfigurationElement	vRealize Orchestrator version 7.0+	Captures a vRealize Orchestrator configuration element.
Orchestrator-Package	vRealize Orchestrator version 7.0+	Captures a vRealize Orchestrator package.
Orchestrator-Workflow	vRealize Orchestrator version 7.0+	Captures a vRealize Orchestrator workflow.

Searching Content

You can search an existing content based on certain defined entries within the UI.

- Content dependencies and dependency files can be seen by clicking the version and looking at the DEPENDENCIES tab.
- By clicking each file, you can download it from the content repository within vRealize Suite Lifecycle Manager.

Test Content

You can test content to ensure it is ready for release.

Prerequisites

Verify that the content package has been added to vRealize Suite Lifecycle Manager.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Content**, click the name of the content package to capture.
- 3 Click the three horizontal dots to the right of the version to test, and select **Test**.
- 4 Select one or more content endpoints to specify the environments to run tests on.
- 5 Select **Deploy Content** to deploy the content in the endpoint before running tests.
- 6 Select **Stop test deployment on first failure** to stop the test deployment as soon as it encounters an error.
- 7 Select **Run unit tests** to run available unit tests on the content.
- 8 Select **Stop unit tests on first failure** to stop testing if any unit test fails.
- 9 Select **Include all dependencies** to include all dependencies associated with the content package in the tests.

- 10 Select **Release Latest Dependencies** to release the latest versions of the dependencies associated with the content package.
- 11 Select a server to run unit tests on from the **Select a Unit Test Server** drop-down menu, and click **PROCEED**.

Performing Unit Tests

When you create a content endpoint, you can select **supportTest** policy to enable the system to run unit tests after deploying a content to the test environment.

There are two servers here:

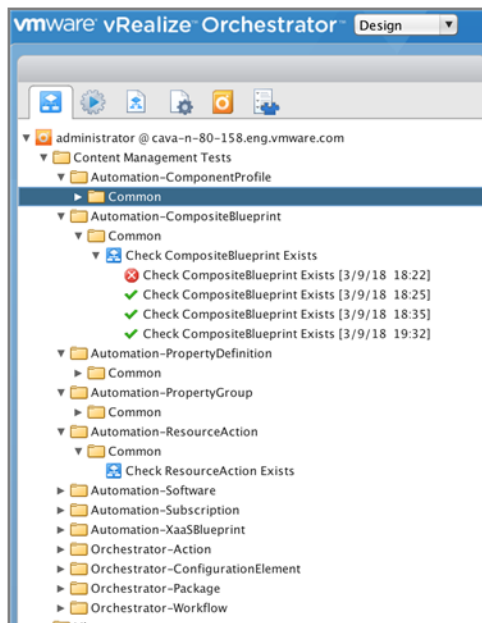
- Unit test server
- Test endpoint

The server is a staging environment in which you can deploy the contents and run unit tests against the deployed contents to the environment.

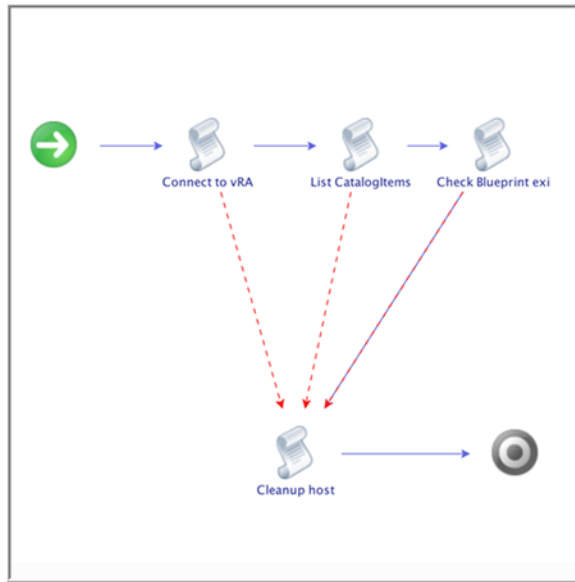
Unit Test Server

The test server is a vRO server, where you can run your unit tests against a deployed content in a test endpoint. Whenever you set an orchestrator endpoint as a test endpoint, it tests the vRealize Orchestrator package and is deployed automatically to this endpoint allowing unit or integration tests. There are some basic tests already present in the package and you can extend the tests in the unit test server as well.

Menu options for Unit Test Server



Sample Unit Test Flow



Common Tests

All tests under the PackageType Common folder are run.

If you go to the unit test server (vRO), under the **Content Management Tests**, you can view separate folders for all content types. For each content type folder, there is a **common** folder present where you see all the common workflows that are run for a given content type.

Package Specific Tests

Specific tests can be run per content name as well. For example, if an Automation-XaaSBlueprint content called "Add AD User" requests a unit test called "Add AD User - Test 1" can be created, which can connect to a given Content endpoint, and run the XaaS Blueprint and wait to see if it was successful. The format of tests is:

`<content name - test name>` and under the `<Content-Type>` folder.

Whenever you select the unit server while testing content, the new unit tests is also run based on the content type against the deployed content in a test endpoint.

The following lists the overall functionality of unit tests:

- Common unit tests workflows can be written under **common** folder per content type
- Unit test workflow for a given content can be written under `<Content Type>` and name the workflow as `<Content name> - <Tests name>`.
- If there is a test failure, then the test displays an error from a workflow.
- Checks the available inputs to test a workflow

Sample Workflows

You can refer to the existing unit workflows available in their vRealize Orchestrator (policy set to test). Navigate to a common folder in vRealize Orchestrator, **Workflows > Content Management Tests > Content Type > Common**.

Input properties available for a unit test workflow that is provided by the platform.

Property Name	Description
version	Version of content being tested.
testEndpointLink	The content endpoint link within the repository.
tenant	The tenant being connected to.
packageVersionLink	The version link to the repository.
packageType	Type of Content. Automation-CompositeBlueprint.
packageName	Content Name
packageId	Content Unique Identifier in the repository.
endpointUser	The username of the endpoint being tested against.
endpointServer	The server name of the endpoint being tested against.
endpointPassword	The password (SecureString) of the endpoint being tested against.

Source Control with vRealize Suite Lifecycle Manager Content Lifecycle Management

vRealize Suite Lifecycle Manager content lifecycle management integrates natively into a defined GitLab and Bitbucket branch endpoint to provide source control for content.

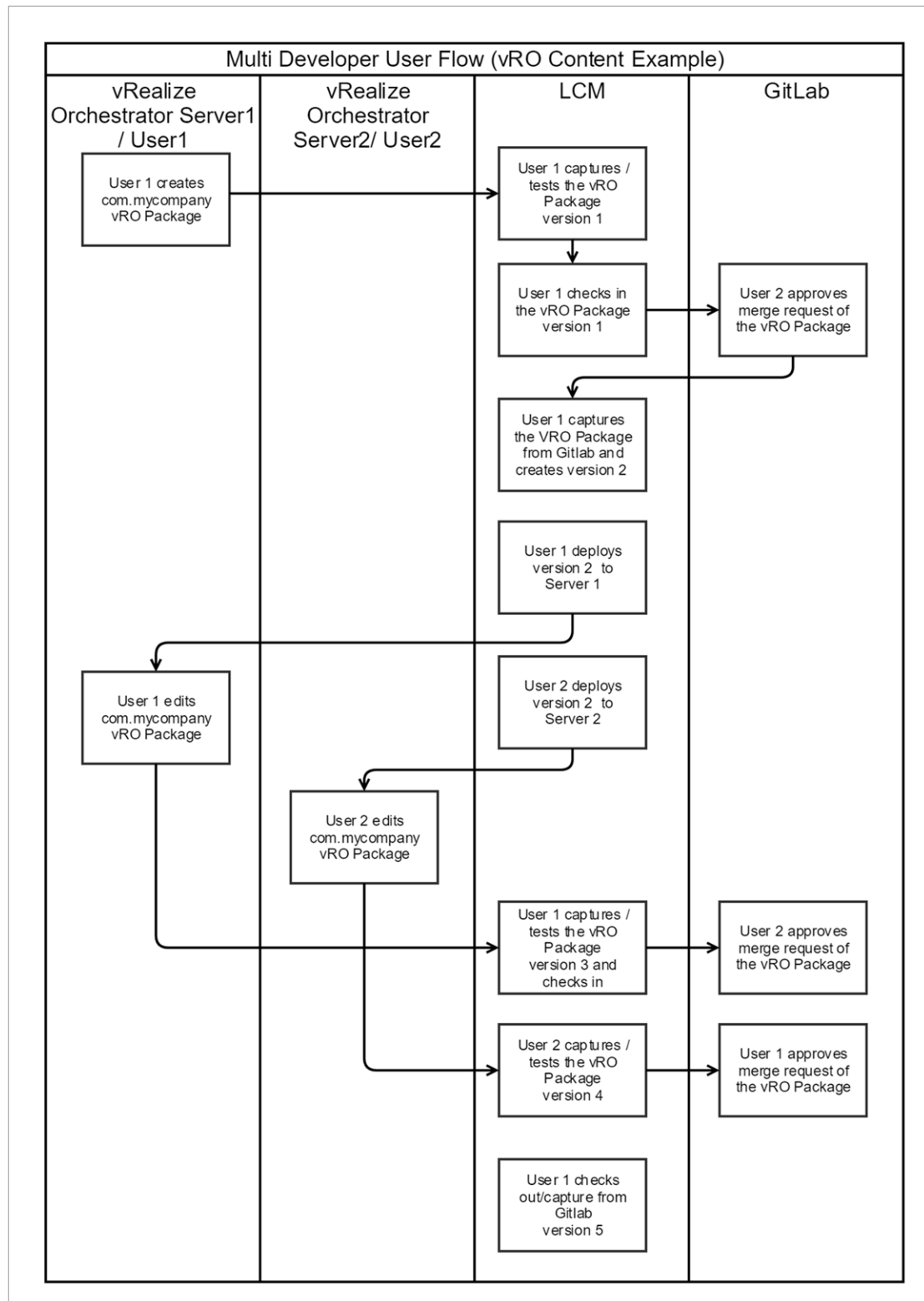
You can store content in both the vRealize Suite Lifecycle Manager version-controlled repository and a GitLab or Bitbucket branch. This allows developers to work together to check in and check out content, and to code review changes prior to deploying to test or production environments.

vRealize Suite Lifecycle Manager stores all source control commit hashes for the purpose of check in, so the correct state of content is known. This enables multi-developer support, which reduces the risk of overwriting content and reduces the number of merge conflicts that can occur.

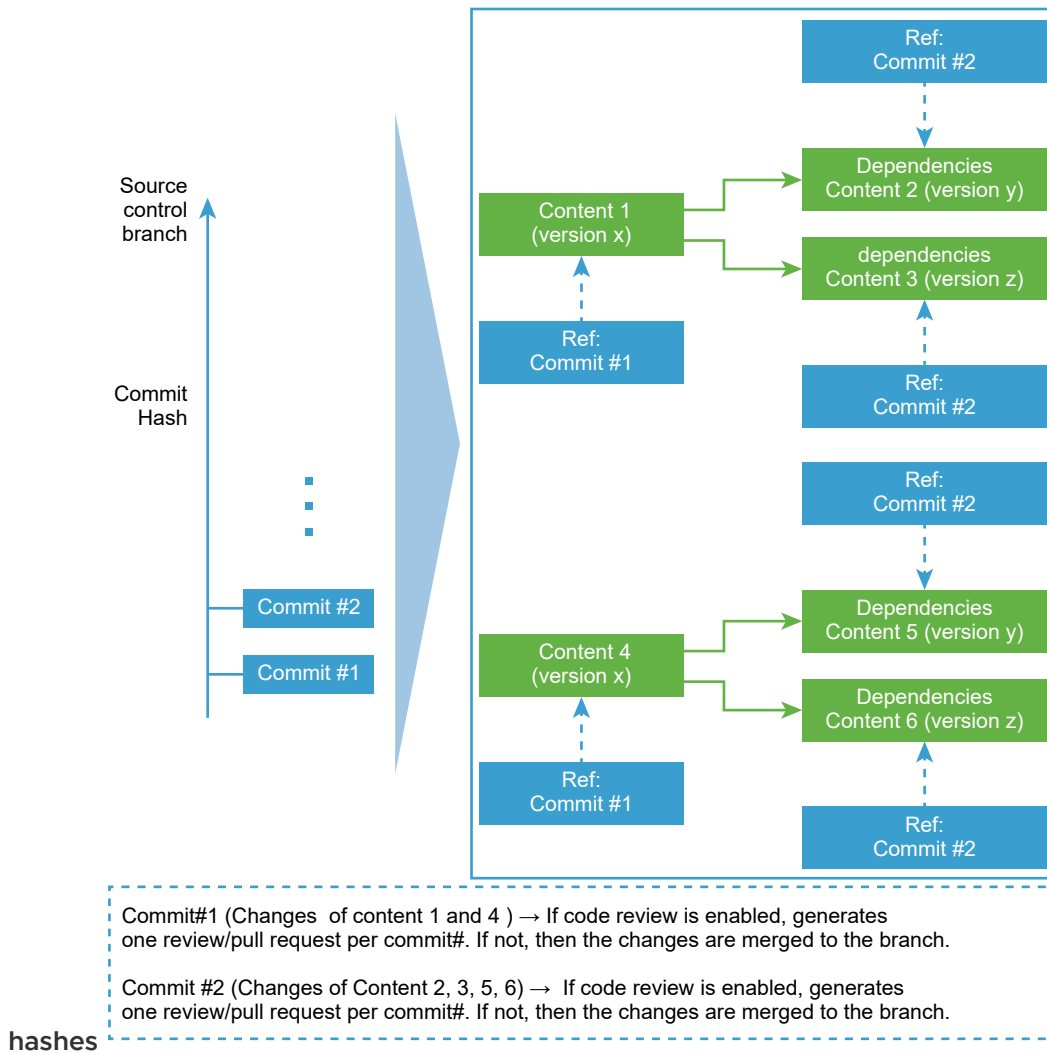
To use source control in vRealize Suite Lifecycle Manager, you must meet the following prerequisites:

- Verify that you have a GitLab or Bitbucket server. If you do not have an existing GitLab server, you can use the Gitlab-CE free docker container.
- Verify that at least one vRealize Suite Lifecycle Manager user has access to GitLab or Bitbucket.
- Create a branch in GitLab and apply the necessary permissions in GitLab for other developers to check in and check out content to the branch.
- The GitLab user must create an access token in GitLab and store the token against the GitLab instance under vRealize Suite Lifecycle Manager **Content Settings**.

It is a best practice when each time the content is checked in to source control, and new version should be checked out and deployed to a content endpoint. This saves the latest changes from other developers (effective rebase of the content) and also communicates to the vRealize Suite Lifecycle Manager content services which GIT Commit Hash is deployed to which content per endpoint. However, when you are capturing content from GitLab server, the checkout works if you are using the GitLab version 11.6.5 or earlier. The checkout fails if you are using GitLab version higher than 11.6.5.



Contents referring to multiple commit



Check in Content to a Source Control Endpoint

You can check-in the previously captured content to a source control endpoint.

Prerequisites

Verify that you have added a source control endpoint to vRealize Suite Lifecycle Manager. See [Source Control with vRealize Suite Lifecycle Manager Content Lifecycle Management](#) for source control requirements.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Content**, click the name of the content package to capture.
- 3 Click the name of the content package to test.
- 4 Click the three vertical dots to the right of the version to check in, and select **Checkin**.

- 5 Select a content endpoint to check the content package in to.
- 6 Select **Include all dependencies** to include all dependencies associated with the content package in the check-in.
- 7 Add a descriptive comment in the **Comment** field, and click **CHECK IN**.

Note Adding a check-in comment is mandatory.

When checking in a vRO package, there is an optional capability to merge with an existing vRO package that exists in the source control. This ensures that all files that are captured are checked into the path of the selected package (ultimately merged). If you do not see the package, then **Select the Source Control Endpoint > Orchestrator-Package type**, refresh the cache and check- in to view the vRO package in which it needs to be merged. You have the following new features added when you check in an Orchestrator package:

- You can merge a custom orchestrator-package from an endpoint to an uber package version in LCM.
- The ability to merge a custom Orchestrator-package directly to an uber package in GitLab.
- You can release a subset of contents from an Orchestrator-package while deploying to an endpoint.
- As part of the dependency management, you can remove dependency from a content version.

For a vRealize Automation content check-in, you can merge directly on GitLab. You can check out without dependency or check out with dependency, where you can perform the following:

- You can remove the package dependency from the latest version. For example, if you have performed a vRealize Automation content check in with dependency and enabled the option to merge the dependent Orchestrator-Package to an uber package directly on GitLab. When you check-out the same Automation content with dependency from a source control.
-

Results

If a code review is disabled on the source control branch, the content is auto merged.

What to do next

If a code review is enabled on the source control branch, you or another code reviewer must check the content in to GitLab manually after the code review is complete. After you check the content into GitLab, capture the latest content version from the source control server in vRealize Suite Lifecycle Manager.

If you are continuing to develop on your content endpoint, capture the latest content version from source control and deploy it to your development content endpoint. This updates the content endpoint so that the content is in sync with the source control and subsequent check-ins are valid.

You can view the check in status in the **Activity Log**.

Check Out Content from a Source Control Endpoint

After a content is checked in to a source control endpoint, you can check out the content and deploy it to a content endpoint. When the content is checked out from Source Control, the content is marked with the Git Hash Code for reference.

Prerequisites

Verify that the content has been checked in to the source control endpoint. See [Check in Content to a Source Control Endpoint](#).

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Content**, click **ADD CONTENT**.

Note You can check out the content inline as well.

- 3 Choose whether to test or deploy the content package in addition to capturing it, and click **PROCEED**.
- 4 Enter the capture details for the content package.
 - a From the **Select Capture Endpoint** drop-down menu, select the source control endpoint to capture content from.
 - b Select **Get the latest content** to retrieve the latest content dependencies rather than the dependencies the content was initially captured with.
 - c Select the content type and content to capture.
 - d Select **Include all dependencies** to capture any dependencies associated with the content.
Dependencies are stored in vRealize Suite Lifecycle Manager, not the source control endpoint.
 - e If the content is ready for production, select **Mark this version as production ready**.
 - f Enter a description for this content version in the **Comments** field.
 - g Click **Next**.

- 5 Enter test details for the content endpoint.

This option appears only if you selected to test the content package.

- a Select one or more content endpoints to specify the environments to run tests on.
- b Select **Deploy Content** to deploy the content in the endpoint before running tests.
- c Select **Stop test deployment on first failure** to stop the test deployment as soon as it encounters an error.
- d Select **Run unit tests** to run available unit tests on the content.
- e Select **Stop unit tests on first failure** to stop testing if any unit test fails.

- f Select a server to run unit tests on from the **Select a Unit Test Server** drop-down menu.

You must have a vRealize Orchestrator test package imported to use a unit test server.

- g Click **Next**.

6 Enter deployment details for the content package.

This option appears only if you chose to test the content package.

- a Select one or more content endpoints from the **Select Release Endpoints** drop-down menu to specify the production environments where the system releases the content.
- b Select **Stop release deployment on first failure** to stop deployment as soon as the system encounters a failure.
- c Enter a comment that explains why the content is being released in the **Release Comment** field as writing comments are mandatory.

7 Click **SUBMIT**.

Results

vRealize Suite Lifecycle Manager captures the content from the source control endpoint and creates a new version of the content in the content catalog. This version is marked **SourceControl Enabled**, which tells vRealize Suite Lifecycle Manager the state of the content when deploying to a content endpoint so the content is checked in against the right point in time.

What to do next

If you are using source control and have multiple capture content endpoints, only deploy content from the content catalog is marked **SourceControl Enabled**. This communicates the state of the content when deploying to a content endpoint so the content is checked in against the right point in time.

Deploy a Content Package

Deploy a content package when it is ready for a production environment.

Prerequisites

- Verify that the production environment has been added as a content endpoint.
- Verify that the content is ready for a production environment.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Click **Content** and click the name of the content package to deploy.
- 3 Click **DEPLOY** for the version to deploy.
- 4 Select one or more content endpoints from the **Select Release Endpoints** drop-down menu to specify the production environments where the system releases the content.

- 5 Select **Stop release deployment on first failure** to stop a deployment as soon as the system encounters a failure.
- 6 Select **Include all dependencies** to deploy all dependencies associated with the content package.
- 7 Select **Release Latest Dependencies** to release the latest versions of the dependencies associated with the content package.
- 8 Enter a comment that explains why the content is being released in the **Release Comment** field, and click **PROCEED**.

Multi Release of Content Package

vRealize Suite Lifecycle Manager 8.0 content management allows the bulk release of content spanning different types where vSphere, vRealize Operations Manager, and vRealize Automation are deployed in one request. It provides an advanced filter option on the content type that is established from a specific content endpoint.

Multi contents are selected as part of a multi release request. Failure to deploy one of the selected contents, will not roll back deployed contents which are part of that request.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Content**, select **Content Item List**.
- 3 Expand the **Filter Applied** tree.
- 4 Under the Content Filter section, you can filter by a single tag or multiple tags, Type, Endpoint, and Policy to get to a subset of the content you want to view and deploy.

Filter Type	Description
Content Filters	This section lists the content filters. <ul style="list-style-type: none"> ■ Production Ready ■ Development Content ■ Tested ■ Source Controlled ■ Dependencies Captured
Content Types	This section lists the Content category based on the content type.
Content Endpoints	This section lists all the associated Content Endpoints.

- 5 After you select a content filter, you can add a tag and then click **Apply**.

A tag is associated when a content is created. A tag-based filter is useful when you want to search. However, you can still add the tag even after creating content. You can also manage bulk tags for all content and older versions.

- 6 To save your filters, click **Save**.

Developers can only view their filters and release managers can view all other RM filters. The saved filters can be edited or deleted.

After you set the content filters, the default content view changes to **Content Version List**. When you provide a filter, you can locate a specific version of the content, for example, Production Ready Content with a specific tag and of a specific set of content types. For example, display only vSphere templates, vRealize Operations Manager dashboards and vRealize Automation Blueprints.

- 7 To deploy the content to a release endpoint, follow the wizard.

- 8 Click **Actions** and select **Checkin**.

Note With Lifecycle Manager 8.0, you can now check-in multiple content after filtering and selecting contents. When you are performing a multi-capture, test and release, verify that all the capture is successful because if one of the content capture fails, the entire content pipeline is marked as failed. Based on multi-capture pipeline failure, you cannot move to the next step of testing and releasing a pipeline.

- 9 To check in multiple content.

- a Select an **Endpoint repository**.
- b if you want to capture all the dependencies, select **Include all Dependencies** and merge the vRO package, if required.
- c Click **Check-in**.

- 10 Select an appropriate endpoint to each type of content appears.

Note Orchestrator endpoints are assumed by their parent automation instance. If there are standalone Orchestrator endpoints configured, then you can also deploy them.

Delete a Content Package

You can delete a content package from all endpoints when you no longer need the content package.

This operation cannot be undone.

Prerequisites

- Verify that one or more content endpoints are added.
- Verify that the content package is present in the deployment.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Click **Content** and click the name of the content package to delete.

- 3 Click the three horizontal dots to the right of the version and select **Delete**.
- 4 Click **OK**.

For the changes to appear on the UI, refresh the page.

Content Issues You might Encounter

There can be content issues that you might encounter during any content operations.

- When transferring a customization spec between vCenter servers the password fields cannot be decrypted by the target. This causes deployments that depend on custom specs with passwords to fail. You can manually enter the correct value in the Administrator password field after customization spec is deployed by the Lifecycle Manager pipeline.
- When a symptom definition is setup with REGEX or NOT_REGEX, the import fails using the vRealize Operations Manager APIs with the following error. **Error releasing Operations-Symptom message= "Invalid request... #1 violations found.", "validationFailures": [{"failureMessage": "Message Event Condition field 'operator' must be either EQ or CONTAINS.** If a symptom uses REGEX, the content needs to be imported manually through Lifecycle Manager UI.
- Content release from different versions of vRealize Operations Manager may fail. For example, content from 6.6 to 6.7 some content types may fail.
- A pipeline execution with a large number of captures or check-ins may fail, if the number of executions is higher than that supported by the endpoint type. For example, bitbucket cloud can support 1000 accesses per hour to its repository.

Access Source Control

Only a release manager can add a source control access, where in the source control can be GitLab or Bitbucket. With this privilege, a release manager can select the GitLab type, Bitbucket and enter the gitLab server name. You can supply multiple server names and then use the git lab personal access token and assign it to the source control server.

By enabling access source control, you can add an endpoint for a source control. For information on adding a source control, see [Add a Source Control Server Endpoint](#). Release manager can add a source control server. But any developer logged-in to vRealize Suite Lifecycle Manager has to associate their token to the server to access the source control server.

Managing Source Control Server Endpoints

Before you can check in or check out content, a vRealize Suite Lifecycle Manager must add a GitLab or Bitbucket source control server to the system.

- [Add a Source Control Server Endpoint](#)

To add a source control server to the system, add a source control server endpoint.

■ Delete a Source Control Server Endpoint

You can delete a source control server endpoint that is no longer in use.

Add a Source Control Server Endpoint

To add a source control server to the system, add a source control server endpoint.

When you disable the file editor option then the bitbucket API (PUT/POST) does not work for an admin or a developer. Either do not include the below property (feature.file.editor) in the property files or if this is included then ensure that the property is set to true.

Location:

```
<base_directory>\Atlassian\ApplicationData\Bitbucket\shared\bitbucket.properties
```

Properties: feature.file.editor=true

Prerequisites

- Verify that you have a Bitbucket, GitHub or a GitLab instance that is supported for this version of vRealize Suite Lifecycle Manager. For more information on the supported versions of Bitbucket, GitHub, or GitLab, refer to [Content Lifecycle Management](#).
- Log in to GitHub, GitLab or Bitbucket, and generate an access token for your user with all scopes enabled. Copy and save this one-time token from GitHub, GitLab or Bitbucket.
- Log in to GitHub, GitLab or Bitbucket and verify you have group, project and branch created in GitHub, GitLab or Bitbucket before adding it as a source control endpoint.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Click **Content Settings**.
- 3 On the **Source Control Access** tab, click **ADD SOURCE CONTROL SERVER**.
- 4 Select the **Source Control Type**.

Note With vRealize Suite Lifecycle Manager 8.0, you can now select Bitbucket Server or Bitbucket Cloud.

- 5 Enter the IP address or fully qualified domain name of the server, and click **SUBMIT**.
vRealize Suite Lifecycle Manager uses https scheme for any Source Control APIs by default. If you have not enabled https on the GitLab instance, then specify http://<ip address>:<port> in the source control server under the content settings page to change the scheme. When you create source control endpoint, the repository must be specified in <GroupName>/<ProjectName> form. Whenever multiple developers are working on the bit bucket repository then the performance is slow in the bit bucket enterprise version. Therefore, you can use at least 4 vCPU machine of bit bucket.
- 6 Click the pencil icon for the source control server.

- 7 Enter your GitLab or Bitbucket server access token in the **ACCESS KEY** text box, and click **SUBMIT**.
 - a For a GitHub instance, you can either select to enter the credential of the Github instance by providing the user name and password or enter the access token.
 - b Click **SUBMIT**.

An access token is a unique identity for a user to perform check-in or check-out to track the GitLab or GitHub API. To create an access token for GitLab or GitHub, access the GitLab or GitHub Server URL. For example, gitlab.example.com or github.com. For Bitbucket Server and Cloud, browse to bitbucket.org and navigate to App Passwords to create a password with full permissions.

Delete a Source Control Server Endpoint

You can delete a source control server endpoint that is no longer in use.

Prerequisites

Verify that the source control server endpoint is not being used by any content endpoints.

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Click **Content Settings**.
- 3 On the **Source Control Access** tab, click the trash icon for the source control server endpoint to delete.
- 4 Click **OK**.

Working with Content Settings

You can add source control server endpoint, vCenter publisher, pipeline extensibility and developer restrictions in Content Settings.

Source Control Access

To add a source control endpoint, provide a server for that source control from GitLab. For more information, see [Add a Source Control Server Endpoint](#).

Note You can add multiple server names for a source control server endpoint and only GitLab source control is supported for this version.

vSphere Template Repository

Starting with vRealize Suite Lifecycle Manager 1.3 and later, you can capture content from vSphere vCenter Server, the vSphere Template Repository is a Content Library within a designated vCenter instance that will store all the templates that are captured in which they can be managed from LCM. A best practice is to have this vCenter instance close to where the templates would typically be captured, that is a development vCenter for template authoring. You can go back to Endpoints and select vCenter to add as your endpoint. For more information, see [Add a vCenter Server Content Endpoint](#). The model for the Content Library Configuration is the following:

- 1 Create the Content Library (Publisher): The vSphere Template Repository points to a Content Library that is set up for publishing. For more details on how to setup a publisher Content Library, see [vCenter Documentation](#).
- 2 Create Content Library Subscribers: Each vCenter server that opts for a template support requires a Content Library to be configured which will Subscribe to the Published Library configured in Step 1. The following settings are required:

Setting	Description
Automatic Synchronization	You can enable this setting for automatic synchronization of the template metadata.
Subscription URL	This URL contains details about the publishers <code>lib.json</code> file. This will be available when you create a publisher in Step 1.
Authentication Disabled	Disabled
Library content	<ul style="list-style-type: none"> ■ Download all library immediately - If you don't select this option then vCenter will download ALL virtual machine templates. ■ Download library content only when needed - Only the metadata is downloaded (not the disks). vRealize Suite Lifecycle Manager instructs on demand and as requested to download the associated disks

Developer Restrictions

Content tags are useful for a variety of reasons, to locate content within the UI, that is when you find all content with "BugFix-Task-1" tag or can be used for custom business logic during the release pipeline.

An example of this may be custom business logic implemented by a release manager - Don't Deploy Content to Endpoint B unless the Content has been deployed to Endpoint A, first this requires a custom pipeline/workflow to be implemented. If this rule is to be bypassed, for example, for Release Managers to push Content straight to Endpoint B then a tag could be applied to the content. This tag should only be added by a Release Manager and not a Developer.

Working with Content Pipelines

Pipeline stubs are used to support the pipeline extensibility use case in content-management. The pipeline process can be extended by adding a custom logic in pre or post stages of capture, test, or deploy. The custom logic can be created as a vRealize Orchestrator workflow, which can then

be mapped to a pre or post stub. Pre and Post stubs are executed before and after, respectively for a given stage.

The content pipeline supports the pre or post stubs:

- Pre-Capture
- Post-Capture
- Pre-Test
- Post-Test
- Pre-Release
- Post-Release

Each pipeline is made up of various **Stages**, each stage then can have various **Tasks**. Tasks can be either parallel or sequential based on your custom business logic.

Content pipeline runs pre-stub and post-stub based on run in the background flag. If it is enabled, then a call is not a synchronized call and the content pipeline does not wait for the status of the stub. Similarly, if it is disabled, then the call is a synchronized call and content pipeline does wait for the status of the stub. It takes more time as compared to a disabled background process.

Note At a time, only 15 content pipelines can run at a time. Some parameters are empty in Lifecycle Manager 8.0 on pipelines stubs. If you still want to use the pipelines, then use the `packageVersionLink` to retrieve the package version details like `packageName`, `packageType`, and so on. And you can also perform similar operation using pre and post-test stubs.

Configure Pipeline Stub

Pipeline stubs can be executed in a synchronous or an asynchronous manner. When running a stub in an asynchronous manner other pipeline stages are executed without waiting for the custom logic to complete. For instance, a Pre-Capture configured to run asynchronously executes in parallel with the Capture stage. However, a Post-Capture stage's execution is triggered only after the Capture stage is executed, but can be made to run in parallel with the next scheduled stage such as pre-test.

To associate a tag to a vRealize Orchestrator workflow, the global custom tag name of workflow and value can either be manually edited to include `vRSLCM_CUSTOM` or the `'/Library/Tagging/Tag'` workflow can also be used for the tagging. Migration of pre and post stubs are not supported.

Prerequisites

Ensure that all the Orchestrator endpoints whose workflows are to be used in the pre or post stubs are added in vRealize Suite Lifecycle Manager and that the workflows which are to be used in the stubs are tagged with `vRSLCM_CUSTOM` keyword.

Procedure

- 1 On the **Content Settings**, click the **Edit** pencil icon.

The **Configure Pipeline Stub** appears.

- 2 The **Name and Execute Pipeline** condition appears by default.
- 3 Select Run in background if the stub is to be executed in an asynchronous manner.
- 4 Select the **Orchestrator Endpoint** from the drop-down menu.
- 5 Select a **Orchestrator Workflow** and click **Submit**.

Only workflows that are tagged as vRSLCM_CUSTOM is shown in this list.

- 6 Select the **Input Param Configuration** and click **Submit**.

Map Your Proxy Setting

vRealize Suite Lifecycle Manager 8.1 has introduced Proxy for Source Control Management endpoints. The feature allows SCM endpoints to channel all REST calls through a proxy server which can be configured on the vRealize Suite Lifecycle Manager setting page and map the same to the content management. Proxy can be enabled for an SCM server, which automatically enables the proxy for all endpoints using that SCM server.

The Proxy Mapping tab displays the proxy status, and configuration details such as proxy server hostname and port.

Note You can use the proxy settings for the source control endpoints only.

You can enable the proxy for an SCM instance by selecting it from the list of servers and clicking **Update**. Once the proxy is enabled for any of the SCM servers the administrator cannot remove the proxy from the vRealize Suite Lifecycle Manager setting page. To remove the proxy, disable the proxy mapping for all SCM servers and then proceed with the removal of proxy from the vRealize Suite Lifecycle Manager setting page. You can disable proxy mapping for an SCM server by selecting it again and clicking **Update**. The administrator can confirm that the proxy is not used by any of the servers from the status of vRealize Suite Lifecycle Manager Proxy used by Content Management.

If you notice that the proxy is not enabled, then navigate to **Locker > Proxy**, and select the **Configure Proxy** check box. For more information, see [Configure Your Proxy Settings](#). Only a Release Manager and the administrator has the privileges to access the Proxy mapping in vRealize Suite Lifecycle Manager.

Content Pipeline Settings

Starting with vRealize Suite Lifecycle Manager 8.0, there are only Content Pipelines and Capture pipeline are supported. In the Content Pipelines section, under the Pipelines tab, the status of the last 24 pipeline executions can be seen in the Content_Pipeline card. Each of the content pipeline executions when selected, shows the associated Capture pipelines, if any, in the Capture

pipeline card. The execution representations, the colored dot in the pipeline card, can be selected to view a detailed breakdown of the various stages of the selected execution. The Content pipeline execution can contain a maximum of nine stages in the order of execution. However, the actual execution has the stages which are relevant to the execution.

Pipeline Stubs

The pipeline stubs display the status of each action whenever a content is captured. The content pipeline has the following status types whenever a content is run.

- Pre-Capture
- Capture
- Post- Capture
- Pre-Test
- Test
- Post-Test
- Pre-Deploy/Checkin
- Deploy/Check-in
- Post-Deploy/Check-In

In the last three stages, the term Check-in is used if the content is released to a source control endpoint such as Git or BitBucket else the term deploy is used. By default, the pre or post stages are disabled and should be configured before they can be used in an execution. The configuration and various modes of execution for pre or post stages, also called pre or post stubs, are covered under the configure pipeline stubs section. The capture pipeline will always have a single stage, that is Capture. The corresponding details of the pre or post capture can be viewed in the associated content pipeline, also referred as the parent pipeline.

The Executions tab lists all the content and capture pipeline executions. The list shows the status, time taken, executed by and time of the request for each of the executions. This list can be filtered by the type of pipeline and execution status.

Each pipeline consists up of various Stages, each stage then can have various Tasks. Tasks can be either parallel or sequential based on your custom business logic. After selecting an action that you want to perform on a content, a content capture can list various types of status related to such an action. Each of the content settings is related to the view displayed on the Content Pipeline page.

Note At a time by default, only 15 content pipelines can run and at most six simultaneous captures for each of vRealize Automation, vRealize Operations Manager, and vRealize Orchestrator source control content categories. For vSphere, only one capture is executed at a point in time.

Execute Pipeline Conditions:

- 1 **EXECUTE_ON_SUCCESS** - The stub is executed only if the corresponding stage executes successfully. For example, Post-Capture if configured to EXECUTE_ON_SUCCESS executes only if the Capture stage is executed successfully.
- 2 **EXECUTE_ON_FAILURE** - The stub is executed only if the corresponding stage execution fails. For example, Post-Capture if configured to EXECUTE_ON_FAILURE executes only if the Capture stage is execution fails.
- 3 **EXECUTE_ON_SUCCESS_AND_FAILURE** - The stub is executed irrespective of whether the corresponding stage execution passes or fails. For example, Post-Capture if configured to EXECUTE_ON_SUCCESS_AND_FAILURE executes in both cases, whether Capture stage execution passes or fails.

Inputs Parameters

The pre or post stubs support the mentioned list of parameters, the values of which can be passed to the respective vRealize Orchestrator workflow as inputs. The value of these inputs depends on the content (been captured/tested/deployed) of the pipeline execution for which the pre or post routines are executed. Currently, all the parameters are of the type 'String'. Therefore, the input parameters configured for the corresponding workflow in vRealize Orchestrator should be necessarily of type 'String'. A mismatch between the type of parameters results in an execution failure for the pipeline. For more information on configuration, see [Configure Pipeline Stub](#).

Post-Deploy-Pipeline	Pre-Deploy-Pipeline	Post-Test-Pipeline	Pre-Test-Pipeline	Post-Capture-Pipeline	Pre-Capture-Pipeline
■ contentName	■ contentName	■ contentEndpoint	■ contentName	■ contentName	■ contentName
■ contentEndpoint	■ contentEndpoint	■ ContentId	■ contentEndpoint	■ contentEndpoint	■ contentEndpoint
■ ContentId	■ ContentId	■ contentName	■ ContentId	■ ContentId	■ ContentId
■ contentType	■ contentType	■ contentType	■ contentType	■ contentType	■ contentType
■ ContentVersionID	■ ContentVersionID	■ ContentVersionID	■ ContentVersionID	■ ContentVersionID	■ ContentVersionID
■ requestid	■ requestid	■ requestid	■ requestid	■ requestid	■ requestid
■ requestnumber	■ requestnumber	■ requestnumber	■ requestnumber	■ requestnumber	■ requestnumber
■ status	■ requestedby	■ requestedby	■ requestedby	■ requestedby	■ requestedby
■ requestedby	■ useridentity	■ useridentity	■ useridentity	■ useridentity	■ useridentity
■ useridentity				■ status	

Request Status

6

The request page displays the overall status of a product and environment.

The request page displays information on various request types that run on an environment. The request type displays the status as In Progress, Completed or Failed.

Notifications in vRealize Suite Lifecycle Manager

7

With vRealize Suite Lifecycle Manager 2.0 and later, you can view the available updates for the products in the environment and overall health vRealize Suite Lifecycle Manager under notifications.

To view notifications, navigate to **Home Page** and click **Bell** icon.

The notification features provides the following information:

Updates for Products in Environment

- Availability of product upgrade offline using a product support pack.

- Online patch availability

Updates for vRealize Suite Lifecycle Manager

- vRealize Suite Lifecycle Manager online upgrade

- vRealize Suite Lifecycle Manager Online patch

- Product Support Pack updates

You can view the overall health notifications for vRealize Suite Lifecycle Manager products and environment. To list all the notifications, click on the **View List** icon on the right corner of the **Notification** window.

Note vRealize Suite Lifecycle Manager should be connected to internet to get notifications from online source.

Troubleshooting vRealize Suite Lifecycle Manager



vRealize Suite Lifecycle Manager troubleshooting topics provide solutions to problems you might experience installing and managing vRealize Suite with vRealize Suite Lifecycle Manager.

- [Unexpectedly Large vRealize Operations Manager Virtual Machine Fails to Power On Due to Resource Limitations](#)

Large vRealize Operations Manager virtual machines fails to power on due to resource limitations.

- [Environment Deployment Fails During vRealize Log Insight Clustering and VMware Identity Manager Registration](#)

Environment deployment fails during the Adding vIDM user as vRLI Super Admin task while running vRLI Clustering and vIDM Registration.

- [Change in DNS Server](#)

If there is a change in the DNS server, you can update the vRealize Suite Lifecycle Manager Appliance DNS Settings.

- [Wrong IP Details During vRealize Suite Lifecycle Manager Deployment](#)

If you have given an incorrect IP address or if you want to upgrade an existing IP address during vRealize Suite Lifecycle Manager deployment, follow the steps provided in this section.

- [Binary Mappings Are Not Populated](#)

Even if the requests for each product binary are marked as completed, the binary mappings are not populated.

- [Content Capture Fails with Secure Field](#)

A vRealize Automation content with a secure field corrupts the field on the target environment on successful deploy.

- [Fix Errors Using Log Files](#)

vRealize Suite Lifecycle Manager log files are present under the following locations for trouble shooting any issues.

- [Blueprint Capture Fails](#)

The captured blueprint fails after the property group is deleted.

- **Component Profile Deployment Fails**

When the component profiles are released to vRealize Automation, the values for the text boxes "Clone from" and "Clone from snapshot" are not assigned automatically.

- **Update vRealize Suite Lifecycle Manager Hostname**

If you provide an incorrect hostname or if you want to change the hostname of vRealize Suite Lifecycle Manager after deployment, follow the steps provided in this section.

- **Resource Not Found in Directory Management**

The system shows an error message in the Directory Management.

- **Inventory Sync Fails with an Error Message**

Inventory sync fails with an error message `Unable to import the vIDM, due to invalid system admin password. Retry after entering the correct system admin password.`

- **Import or Inventory Sync of vRealize Suite Product Fails**

The import or inventory sync of vRealize Suite product fails with an error message.

- **VMware Identity Manager Postgres Cluster Outage Due to Loss of Delegate IP**

Troubleshooting VMware Identity Manager postgres cluster outage deployed through vRealize Suite Lifecycle Manager.

- **Importing vRealize Automation in vRealize Suite Lifecycle Manager Fails**

When importing vRealize Automation in vRealize Suite Lifecycle Manager, the import fails with an error message.

Unexpectedly Large vRealize Operations Manager Virtual Machine Fails to Power On Due to Resource Limitations

Large vRealize Operations Manager virtual machines fails to power on due to resource limitations.

Problem

When you deploy vRealize Operations Manager in vRealize Suite Lifecycle Manager, by selecting node size as large and if you have budgeted resources for a different size virtual machine, the virtual machine might fail to power on due to resource limitations.

Cause

vRealize Operations Manager deployment size set in vRealize Suite Lifecycle Manager is based on the number of virtual machines, catalog items, concurrent provisions, and other workload metrics for your vRealize Operations Manager environment. Virtual machine size is unrelated to deployment size.

Solution

vRealize Operations Manager virtual machines deployed from vRealize Suite Lifecycle Manager have a large (16 vCPU and 48 GB RAM) virtual machine size, if deployed with large size, and require sufficient vCPU and RAM to power on successfully.

Environment Deployment Fails During vRealize Log Insight Clustering and VMware Identity Manager Registration

Environment deployment fails during the Adding vIDM user as vRLI Super Admin task while running vRLI Clustering and vIDM Registration.

Problem

Even after you multiple deployment operation, environment deployment fails during the Adding vIDM user as vRLI Super Admin task while running vRLI Clustering and vIDM Registration.

The following error message appears in the logs:

```
{"errorMessage":"Unable to retrieve information about this user from VMware Identity Manager.", "errorCode":"RBAC_USERS_ERROR", "errorDetails": {"errorCode":"com.vmware.loginsight.api.errors.rbac.invalid_vidm_user"}}
```

Solution

- 1 Add the VMware Identity Manager Suite Administrator user to vRealize Log Insight by using the vRealize Log Insight UI.
See [Create a New User Account in vRealize Log Insight](#).
- 2 Remove the VMware Identity Manager Suite Administrator user from vRealize Log Insight by using the vRealize Log Insight UI.
- 3 Retry the environment deployment in vRealize Suite Lifecycle Manager.

Change in DNS Server

If there is a change in the DNS server, you can update the vRealize Suite Lifecycle Manager Appliance DNS Settings.

Cause

When a DNS server provided during deployment gets changed, then follow these steps to update the DNS Settings of vRealize Suite Lifecycle Manager.

Solution

- 1 SSH to vRealize Suite Lifecycle Manager appliance using root user.

- 2 Update the DNS setting using the command:

```
/opt/vmware/share/vami/vami_set_dns
vami_set_dns [-d <domain>] [ -s <searchpath>] DNS_Server_1 [DNS_Server_2]
```

For example: `/opt/vmware/share/vami/vami_set_dns -d sqa.local -s sqa.local 10.1.1.25`

- 3 Close the vRealize Suite Lifecycle Manager virtual appliance.
- 4 Select the vRealize Suite Lifecycle Manager virtual appliance from vCenter, and then select **Configure**.
- 5 Enable vApp Options.
- 6 Under Properties, edit the following command:

```
vami.DNS.VMware_vRealize_Suite_Life_Cycle_Manager_Appliance
```

- 7 Power ON the vRealize Suite Lifecycle Manager virtual appliance.
- 8 Verify the new DNS entry by running the `resolvectl status`, and then verify the DNS server.

Wrong IP Details During vRealize Suite Lifecycle Manager Deployment

If you have given an incorrect IP address or if you want to upgrade an existing IP address during vRealize Suite Lifecycle Manager deployment, follow the steps provided in this section.

Cause

If you have given an incorrect IP address while deploying vRealize Suite Lifecycle Manager.

Solution

- 1 SSH to vRealize Suite Lifecycle Manager appliance using root user.
- 2 Update the IP address using the below command:

```
vami_set_network <interface> (STATICV4|STATICV4+DHCPV6|STATICV4+AUTOV6) <ipv4_addr>
<netmask> <gatewayv4> For example: /opt/vmware/share/vami/vami_set_network eth0
STATICV4 192.168.1.150 255.255.255.0 192.168.1.1
```

Binary Mappings Are Not Populated

Even if the requests for each product binary are marked as completed, the binary mappings are not populated.

Problem

When you navigate from **Home > Settings > Product Binaries**, the corresponding request is marked as COMPLETED in the **Requests** page but the binary mappings are not populated.

Cause

The checksum for the target product binary cannot be same as the one published by VMware.

Solution

- ◆ Ensure that the binaries are not corrupted or modified and their SHA256 checksum is the same as mentioned in MyVMware portal.

Content Capture Fails with Secure Field

A vRealize Automation content with a secure field corrupts the field on the target environment on successful deploy.

Cause

In vRealize Suite Lifecycle Manager 8.0, the secure field is captured as encrypted from the source environment and the value cannot be decrypted when deployed.

Solution

- ◆ After you successfully deploy, login to the target vRealize Automation and manually update the secure fields in the content.

Fix Errors Using Log Files

vRealize Suite Lifecycle Manager log files are present under the following locations for trouble shooting any issues.

Solution

- 1 For vRealize Suite Lifecycle Manager 1.1 or older version, service Layer logs are present in the location `/opt/vmware/vlcm/logs/` and the file format is `xenon.*.log`, the active log file is `xenon.0.log`. For vRealize Suite Lifecycle Manager 1.2 or later, this log is available at `/var/log/vlcm` and log file name is `vrlcm-xserver.log`
- 2 For vRealize Suite Lifecycle Manager 1.1 or earlier version, engine logs are present in the location `/var/log/vlcm/` and the current log filename is `catalina.out`. For vRealize Suite Lifecycle Manager 1.2 or later, this log is available at `/var/log/vlcm` and log file name is `vrlcm-server.log`

Note To upgrade from 1.0 or 1.1–1.3, the old LCM service layers log present at the location `/opt/vmware/vlcm/logs/` are in the name `console.log`, and the new service layer logs are in the file format `xenon.*.log`.

Blueprint Capture Fails

The captured blueprint fails after the property group is deleted.

Problem

When a composite blueprint of vRealize Automation have references to any properties like Property Definition or Property Groups, and if those properties are deleted from the vRealize Automation then the Blueprint has to be updated in the vRealize Automation or else the capture in Lifecycle Manager fails.

Solution

- 1 Edit the Blueprint.
- 2 Click the **Setting** icon next to blueprint name at the top.
- 3 Click the **Properties** tab (select **custom properties** tab if any properties were added previously) and select **OK**.
- 4 Select each of the components in the blueprint and select the **Properties** tab. (select the **custom properties** tab if any properties were added previously).
- 5 Click **Save**.
- 6 Click **Finish**.

Component Profile Deployment Fails

When the component profiles are released to vRealize Automation, the values for the text boxes "Clone from" and "Clone from snapshot" are not assigned automatically.

Problem

When deploying an "Image Component Profile" the "Clone From" value of the component profile is stripped. The "Clone From" text boxes are empty on the target system.

Solution

- ◆ You can manually edit the component profile and the respective values from the drop-down menu.

Note When you capture and release a component profile of vRealize Automation using vRealize Suite Lifecycle Manager, the name of component profile should start with "ValueSet".

Update vRealize Suite Lifecycle Manager Hostname

If you provide an incorrect hostname or if you want to change the hostname of vRealize Suite Lifecycle Manager after deployment, follow the steps provided in this section.

Cause

If you want to update the hostname of vRealize Suite Lifecycle Manager.

Solution

- 1 Use the Secure Shell (SSH) to access vRealize Suite Lifecycle Manager appliance using the root user privileges.
- 2 Update the hostname using the following commands:


```
rm /opt/vmware/etc/vami/flags/vami_setnetwork
/opt/vmware/share/vami/vami_set_hostname new-hostname
```
- 3 Reboot the vRealize Suite Lifecycle Manager appliance.
- 4 Update the vRealize Suite Lifecycle Manager certificate under Settings in vRealize Suite Lifecycle Manager.

Resource Not Found in Directory Management

The system shows an error message in the Directory Management.

Problem

When you view or edit the directory in the Directory Management, the system cannot retrieve the required information from VMware Identity Manager and displays an error message.

Cause

The directory is partially created or the directory configuration is incomplete.

Solution

- 1 Log in to VMware Identity manager. Verify the directory configuration, and confirm if the directory is associated with a connector. Also, validate the bind password.
- 2 If the directory configuration is incomplete, you can configure it in VMware Identity Manager. You can also use vRealize Suite Lifecycle Manager to remove the directory using the delete functionality, provide correct configuration details, and then add back the directory.

Solution

Note Any role assigned to the directory user in vRealize Lifecycle Manager must be deleted and reassigned after the directory is added back.

This is supported in vRealize Suite Lifecycle Manager 8.2 Patch 1 and later releases.

Inventory Sync Fails with an Error Message

Inventory sync fails with an error message `Unable to import the vIDM, due to invalid system admin password. Retry after entering the correct system admin password.`

Cause

The inventory is not updated with correct system Admin password when the default password and Admin password provided during deployment are different.

Solution

During the deployment, ensure that you provide the same default password and the Admin password. You can also provide the correct system Admin password during the inventory sync request, and then proceed with the deployment.

Import or Inventory Sync of vRealize Suite Product Fails

The import or inventory sync of vRealize Suite product fails with an error message.

Cause

When the `keyUsage` does not have the `digitalSignature` attribute in the HTTPS certificate of target product, the import or inventory sync of the vRealize Suite product fails with an error message.

Solution

Perform the following steps:

- 1 Click the padlock icon in the address bar of a browser (Chrome, Edge, or Firefox), and then click **Certificate**.
- 2 Click **Details**, and then click **Key Usage**.
- 3 Verify if the `digitalSignature` attribute is present in the `keyUsage`. If the `digitalSignature` attribute is not present, replace the certificate on the target product with the certificate that has the `digitalSignature` attribute present in `keyUsage`.

VMware Identity Manager Postgres Cluster Outage Due to Loss of Delegate IP

Troubleshooting VMware Identity Manager postgres cluster outage deployed through vRealize Suite Lifecycle Manager.

Problem

VMware Identity Manager cluster health status displays as `CRITICAL` in vRealize Suite Lifecycle Manager Health Notification due to network loss in the VMware Identity Manager appliance.

Cause

Network loss on the postgres cluster primary node. For `/usr/local/bin/pcp_watchdog_info -p 9898 -h localhost -U pgpool` command, it would prompt for a password. If `/usr/local/etc/pgpool.pwd` file is present on the VMware Identity Manager node, that would contain the password. If the password is not available, use the default password `password`.

Command parameters help:

`-h` : The host against which the command is run is `localhost`.

`-p` : The port on which `pgpool` accepts connections is `9898`.

`-U` : The `pgpool` health check and replication delay check user is `pgpool`.

There must be an expected response.

```
3 YES <Host1>:9999 Linux <Host1> <Host1>
<Host1>:9999 Linux <Host1> <Host1> 9999 9000 4 MASTER
<Host2>:9999 Linux <Host2> <Host2> 9999 9000 7 STANDBY
<Host3>:9999 Linux <Host3> <Host3> 9999 9000 7 STANDBY
```

In the response, there needs to be a `MASTER` node and 2 `STANDBY` nodes present. If any of the node's status is `SHUTDOWN`, `DEAD` or the command execution is struck, follow the steps to resolve this issue.

Solution

- 1 Gracefully bring down the services on VMware Identity Manager nodes. Refer to KB [78815](#) for the required steps.
- 2 Power OFF the VMware Identity Manager appliances in vCenter.
- 3 Power ON the VMware Identity Manager nodes through vRealize Suite Lifecycle Manager.

Importing vRealize Automation in vRealize Suite Lifecycle Manager Fails

When importing vRealize Automation in vRealize Suite Lifecycle Manager, the import fails with an error message.

Problem

If the details of VMware Identity Manager fails to match with vRealize Automation, when importing vRealize Automation in vRealize Suite Lifecycle Manager, you may see the following error message.

Error Code: LCMVRAVACONFIG590026

vRealize Automation Import failed due to VMware Identity Manager details in vRealize Suite Lifecycle Manager not matching with the provided vRealize Automation. Please retry by providing vRealize Automation which has VMware Identity Manager details same as vRSCLM VMware Identity Manager details.

vRA vIDM details mismatch. vRA Import is supported only if vRSCLM vIDM is matched with vRA vIDM details.

Cause

The VMware Identity Manager imported into vRealize Suite Lifecycle Manager does not match the vRealize Automation host that was attempting to import.

Solution

- 1 Delete globalenvironment from vRealize Suite Lifecycle Manager. This action is supported in the UI from vRealize Suite Lifecycle Manager version 8.4.
- 2 Import VMware Identity Manager which is associated with the vRealize Automation host.
- 3 Create a new request to import vRealize Automation.