vRealize Suite Lifecycle Manager 2.0 Installation, Upgrade, and Management

VMware vRealize Suite Lifecycle Manager 2018

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

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.

- Deploy the vRealize Suite Lifecycle Manager Appliance

  Deploy the vRealize Suite Lifecycle Manager appliance to begin using vRealize Suite Lifecycle Manager.

- 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.

- Check for and Install vRealize Suite Lifecycle Manager Updates and Upgrades from a Repository

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

- Install Upgrades to vRealize Suite Lifecycle Manager from an ISO File

  You can upgrade vRealize Suite Lifecycle Manager using an upgrade ISO file.

- Configuring vRealize Suite Lifecycle Manager Common Settings

  You can modify settings for vRealize Suite Lifecycle Manager, such as passwords, SSH settings, and configuration drift interval.

- Configure Product Binaries

  Select a Product Binary to use for each vRealize Suite product.

- User Management with VMware Identity Manager

  You can add an existing VMware Identity Manager or deploy new VMware Identity Manager through vRealize Suite Lifecycle Manager.

- Register with My VMware

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

- vRealize Suite Lifecycle Manager Logs

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

- Generate Certificate

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

- 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 LCM appliance.

- Configure Log Insight Agent

  vRealize Suite Lifecycle Manager 1.3 supports Log Insight agent. You can configure to analyze them to understand the performance of the appliance. You can configure vRealize Log Insight Linux agents in the vRealize Suite Lifecycle Manager virtual appliance.

- 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 are not used by the vRealize Suite Lifecycle Manager appliance itself, they are also used as input to vRealize Suite product deployment schema.

- Add a Data Center to vRealize Suite Lifecycle Manager

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

- Assign a User Role in vCenter Server

  Create a user role in the vSphere Web 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.

- 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.

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.

- 2 vCPUs if content lifecycle management is disabled.
- 4 vCPUs, if content lifecycle management is enabled.
- 16 GB memory
- 127 GB storage

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	7.5.0 and 7.6.0
vRealize Business for Cloud	7.5.0 and 7.6.0
vRealize Operations Manager	7.0.0 and 7.5.0
vRealize Log Insight	4.7.0, 4.7.1 and 4.8.0
VMware Identity Manager	2.9.2, 3.2.0, 3.2.0.1, and 3.3.0
vRealize Network Insight	3.9.0 and 4.0

For more information about vRealize Suite, see vRealize Suite Overview. You can onboard a supported vRealize product version which 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 and 7.6.0
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 and 7.5.0
vRealize Log Insight	4.5.1, 4.6.0, 4.6.1, 4.7.0, 4.7.1, and 4.8.0

Product	Supported Versions
VMware Identity Manager	2.9.2, 3.2.0, 3.2.0.1, and 3.3.0
vRealize Network Insight	3.7.0, 3.8.0, 3.9.0 and 4.0

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 Upstream Ports and Endpoint Services

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://simservice.vmware.com
Patch and policy refresh repository	443	https://vrealize-updates.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		

Table 1-2. Requires Ports for Product and Integration Communications

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

Table 1-2. Requires Ports for Product and Integration Communications (Continued)

Product or Integration	TCP Port Number
vRealize Log Insight Appliances	443, 9543, 16520, 22
Identity Manager Appliances	8443, 443
vRealize Orchestrator Appliances	8281
vCenter Server Instances	443
ESXi Host Instances	443
Content Management Host (GitLab)	443

Note To upgrade suite products, port 4443 should be open. For more information on ports, see *vRealize Suite Lifecycle Manager 1.x Security Hardening Guide*.

Deploy the vRealize Suite Lifecycle Manager Appliance

Deploy the vRealize Suite Lifecycle Manager appliance to begin using vRealize Suite Lifecycle Manager.

To create the appliance, you use the vSphere Client to download and deploy a partially configured virtual machine from a template.

Prerequisites

- Log in to the vSphere Client with an account that has permission to deploy OVF templates to the inventory.
- Download vRealize Suite Lifecycle Manager .ovf or .ova file from My VMware to a location accessible to the vSphere Client.

Procedure

1. Select the vSphere **Deploy OVF Template**.
2. Enter the path to the vRealize Suite Lifecycle Manager appliance `.ovf` or `.ova` file.
3. Read and accept the end-user license agreement.
4. Enter an appliance name and inventory location.

   Always deploy vRSLCM appliance with unique name and do not include non-alphanumeric characters such as underscores (_) in the names.
5. Select the host and cluster in which the appliance will reside.
6. Review the template details.
7. Select the resource pool in which the appliance will reside.
8. Select a deployment configuration.

   Note Enable this feature if you want to use content management, where the VA is deployed with 4 CPUs.

Typically, there is an option to include or exclude content management. You can select a configuration and mention the change in the number of CPU that is required.

9 Select the storage that will host the appliance.

10 Select **Thick** as the disk format.

Format does not affect appliance disk size. If an appliance needs more space for data, increase disk size by using vSphere after deploying.

11 From the drop-down menu, select a Destination Network.

12 Complete the appliance properties.

a For **Hostname**, enter the appliance Fully Qualified Domain Name (FQDN).

b (Optional) Enter the certificate properties.

c In Network Properties, when using static IP addresses, enter the values for gateway, Netmask, and DNS servers. You must also enter the IP address, FQDN, and domain for the appliance itself.

Note vRealize Suite Lifecycle Manager does not verify the revocation status of the SSL certificates. You must verify the status manually before accepting the certificate.

13 Depending on your deployment, vCenter Server, and DNS configuration, select one of the following ways of finishing deployment and powering up the appliance.

- If you deployed to vSphere, and **Power on after deployment** is available on the Ready to Complete page, take the following steps.
  a Select **Power on after deployment** and click **Finish**.
  b After the file finishes deploying into vCenter Server, click **Close**.
  c Wait for the virtual machine to start, which might take up to 5 minutes.
- If you deployed to vSphere, and **Power on after deployment** is not available on the Ready to Complete page, take the following steps.
  a After the file finishes deploying into vCenter Server, click **Close**.
  b Power on the vRealize Suite Lifecycle Manager appliance.
  c Wait for the virtual machine to start, which might take up to 5 minutes.
  d Verify that the vRealize Suite Lifecycle Manager appliance is deployed by pinging its FQDN. If you cannot ping the appliance, restart the virtual machine.
  e Wait for the virtual machine to start, which might take up to 5 minutes.

14 Verify that the vRealize Suite Lifecycle Manager appliance is deployed by pinging its FQDN.

Log in to vRealize Suite Lifecycle Manager using a supported Web browser. See Log In to vRealize Suite Lifecycle Manager and System Requirements.

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. See 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/vrlcm`

   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@localhost`

3. Enter the default administrator password.

   `vmware`

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 and SSH settings and configuration drift interval. See Configuring vRealize Suite Lifecycle Manager Common Settings.

Check for and Install vRealize Suite Lifecycle Manager Updates and Upgrades from a Repository

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

Upgrade is supported from vRealize Suite Lifecycle Manager 1.0 and later versions. You can also upgrade vRealize Suite Lifecycle Manager by using an ISO file to install the upgrade. See Install Upgrades to vRealize Suite Lifecycle Manager from an ISO File.

Note If you are upgrading from vRealize Suite Lifecycle Manager 1.2, then see information in KB article 56511 before proceeding with 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 in-progress tasks.

Procedure

1. Click **Settings** and click the **Update** tab.

   vRealize Suite Lifecycle Manager displays the name, version number, and vendor of the current vRealize Suite Lifecycle Manager appliance.
2. (Optional), to install patch, under **System Information**, click **Install Patch**.
3. To check for online patches, click **Check Patches Online**.
4. To upload downloaded patches, click **Upload** and click **Next**.
5. (Optional), review the summary and click **Install**.
6. Select the repository for vRealize Suite Lifecycle Manager updates.

Option	Description
Default	Use the default VMware repository for vRealize Suite Lifecycle Manager updates. To use this option, the vRealize Suite Lifecycle Manager virtual appliance must have access to My VMware.
Repository 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 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. For more information, see Install Upgrades to vRealize Suite Lifecycle Manager from an ISO File.

7. Click **CHECK UPDATES**.

   After a few minutes, vRealize Suite Lifecycle Manager displays a message indicating whether there are updates available.
8. Select the upgrades to install, and click **INSTALL UPGRADES**.
9. After a few minutes, refresh the vRealize Suite Lifecycle Manager UI and click **Settings** > **Update**.

   On 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.

   If the **Reboot** button is not visible, wait a few minutes and repeat this step.

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.

Install Upgrades to vRealize Suite Lifecycle Manager from an ISO File

You can upgrade vRealize Suite Lifecycle Manager using an upgrade ISO file.

You can also upgrade vRealize Suite Lifecycle Manager from My VMware or a private repository. See Check for and Install vRealize Suite Lifecycle Manager Updates from a Repository.

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 servers and restarts the vRealize Suite Lifecycle Manager virtual appliance, which might corrupt in-progress tasks.

Procedure

1. Mount the upgrade ISO file on the vRealize Suite Lifecycle Manager virtual appliance's CD ROM drive.
2. For vRealize Suite Lifecycle Manager 1.0 upgrade, use SSH to connect to the vRealize Suite Lifecycle Manager virtual appliance.
3. For upgrade from vRealize Suite Lifecycle Manager 1.1 or later, on the UI go to **Home > Settings**, select **CD-ROM** on the Update vRealize Suite Lifecycle Manager page.
4. Click **Check Updates**.

   After an update is detected, click **Install Updates** for completing the installation.
5. If you are upgrading from **vRealize Lifecycle manager 1.1** or later, skip next steps and go to step 10.

6 Edit `provider-runtime.xml` by running `vi /opt/vmware/var/lib/vami/update/provider/provider-runtime.xml`.

```
<? xml version="1.0" encoding="UTF-8"?>
<service>
   <properties>
      <property name="localRepositoryAddress" value="cdrom://" />
      <property name="localRepositoryPasswordFormat" value="base64" />
   </properties>
</service>
```

7 Save and close the file.

8 Verify that a new version is available by running the command `/opt/vmware/bin/vamicli update --check`.

This should return a message similar to the following:

```
Checking for available updates, this process can take a few minutes....
Available Updates -
    x.x.x.x Build yyyyy
```

9 When upgrading from vRealize Suite Lifecycle Manager 1.0, if a 1.3 update is available, run the command `/opt/vmware/bin/vamicli update --install latest -- accepteula` to trigger the upgrade.

The upgrade process restarts the vRealize Suite Lifecycle Manager virtual appliance, which might cause your SSH session to expire.

10 After a few minutes, log in to the vRealize Suite Lifecycle Manager web UI and click **Settings** > **Update**.

If the update is finished, vRealize Suite Lifecycle Manager displays the message `Upgrade Completed Successfully`. If you do not see this message, wait a few minutes and repeat this step.

Configuring vRealize Suite Lifecycle Manager Common Settings

You can modify settings for vRealize Suite Lifecycle Manager, such as passwords, SSH settings, and configuration drift interval.

The first time you view the common configuration page, you must provide data for all available settings to save any settings.

- Change vRealize Suite Lifecycle Manager Passwords

  You can change the default administrator password and set passwords for root, and SSH users.

- Extend Storage

  You can extend the storage space for vRealize Suite Lifecycle Manager.

- Change the Configuration Drift Interval

  Set the interval of time vRealize Suite Lifecycle Manager uses to collect data for configuration drift reports.

- Restart the vRealize Suite Lifecycle Manager Server

  You can restart the vRealize Suite Lifecycle Manager server immediately or schedule weekly server restarts.

- Enable or Disable SSH on vRealize Suite Lifecycle Manager

  You can enable SSH for troubleshooting purposes.

- Join or Leave the VMware Customer Experience Program

  You can join or leave the VMware Customer Experience Program at any time.

Change vRealize Suite Lifecycle Manager Passwords

You can change the default administrator password and set passwords for root, and SSH users.

Procedure

1 Click **Settings** and click the **System Settings** tab.

2 Type new passwords for root, administrator, and SSH users.

  vRealize Suite Lifecycle Manager enforces the following password requirements:

  - Between 8 and 16 characters long
  - At least one uppercase character
  - At least one lowercase character
  - At least one numerical digit
  - At least one special character limited to !@#$%^&*"

3 Click **SAVE**.

  You can update passwords for the products installed in an environment. The new policy is applicable not only for vRealize Suite Lifecycle Manager, but for passwords of the deployed products.

What to do next

If you changed the administrator password, vRealize Suite Lifecycle Manager logs you out and displays the log in page. Log in with the new administrator password to continue using vRealize Suite Lifecycle Manager.

Extend Storage

You can extend the storage space for vRealize Suite Lifecycle Manager.

Prerequisites

Verify that there is enough disk space where you are installing vRealize Suite Lifecycle Manager.

Procedure

1. To extend storage, click **EXTEND STORAGE**.
2. Enter the vCenter Host Name, User Name and Password for the first time.
3. Use the drop-down menu to add the storage.
4. Click **Extend**.

   If vRealize Suite Lifecycle Manager VA has a snapshot existing in vCenter, then the extend storage request for vRealize Suite Lifecycle Manager VA fails. Delete all the snapshots and then extend Storage for LCM.

   After you add the storage, the progress bar increases and displays the storage percentage.

Change the Configuration Drift Interval

Set the interval of time vRealize Suite Lifecycle Manager uses to collect data for configuration drift reports.

Procedure

1. Click **Settings** and click the **System Settings** tab.
2. Enter the Configuration Drift interval in hours.
3. Click **SAVE**.

Restart the vRealize Suite Lifecycle Manager Server

You can restart the vRealize Suite Lifecycle Manager server immediately or schedule weekly server restarts.

Procedure

1. Click **Settings** and click the **System Settings** tab.
2. To restart the server immediately, click **RESTART SERVER**.
3. To schedule a weekly server restart, select **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 Click **Settings** and click the **System Settings** tab.

2 Select **SSH Enabled** to enable SSH connections or deselect it to disable SSH connections.

3 Click **SAVE**.

Join or Leave the VMware Customer Experience Program

You can join or leave the VMware Customer Experience Program at any time.

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.

Procedure

1 Click **Settings** and click the **System Settings** tab.

2 Select **Join the VMware Customer Experience Improvement Program** to join CEIP or deselect the option to leave CEIP.

3 Click **Update**.

Configure Product Binaries

Select a Product Binary to use for each vRealize Suite product.

You can download binaries outside of LCM and make them available on a NFS path.

Prerequisites

To use an 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 Click **Settings** and click the **Product Binaries** tab.

2 Click **Add Product Binaries**.

3 Select the location type.

Select either **Local** or **NFS** to map to a downloaded product binary with products dependent on the product binary location, or select **My VMware Downloads** to map to product binary downloaded from My VMware.

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. For more information, see KB article 56362. 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`.

4 To provide Windows ISO, select the location type as **Windows ISO** and enter the **Windows ISO Mapping Details**.

5 Enter the location of the Product Binary to use in the **Base Location** text box, and click **Discover**.

6 Select the Product Binary file from the **Product Binary** list.

Note By default all the My VMware downloads from within 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.

7 Click **Add**.

8 With vRealize Suite Lifecycle Manager 2.0 and later, you can also view the list of **ISO Binaries** and **Patches** available for Products.

9 Click **Upload**, to upload the downloaded Patch files.

10 Click **Online Patches**.

The patches are listed under the patch list, to use these patches, you must download them.

User Management with VMware Identity Manager

You can add an existing VMware Identity Manager or deploy new VMware Identity Manager through vRealize Suite Lifecycle Manager.

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

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

In vRSLCM, you can provide a suite administrator (in AD Settings) at the time of configuring vIDM with vRSLCM. vRealize Suite products deployed after this configuration can be accessed with the suite administrator credentials with one time authentication.

Note When vIDM is used with vRSLCM, 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.

Deployment of an identity manager through vRLSCM is through a single node with an Internal PostgreSQL database embedded in the appliance and does not support an external database like Microsoft SQL. vRSLCM does not perform cluster-based installations of VMware Identity Manager.

Prerequisites

Verify that you have an existing VMware Identity Manager version 2.9.2, 3.2.0, 3.2.0.1, 3.3.0 as vRealize Suite Lifecycle Manager supports only these versions.

Procedure

1 Click **Settings** and navigate to **User Management > Authentication Source**.

2 You can either select **Add an Existing Identity Manager** or **Install a New Identity Manager**.

   a If you want to add an existing identity manager then, enter the **Host Name**, **User Name**, **Password** and click **Add**.

   b To replace certificate, click **Replace Certificate**.

   c If you do not want to use the identity manager, then click **Unregister**. If you unregister, the associated roles and active directories from vRealize Suite Lifecycle Manager are also deleted. Therefore, read the warning message and then click **Delete**.

   When you register an existing identity manager to update, a duplicate catalog entry is created.

   Note VMware Identity Manager 3.2 or later does not automatically sync users under a corresponding group that are synced through group DN unless they are manually synced or entitled to an application. For more information, see KB article 55737 and KB article 55727.

3 Click **Upgrade** and select the required **Repository Type**.

Option	Description
VMware Repository	You can provide a online source.
Repository URL	You can provide an upgrade link.
vRSLCM Repository	You can upload a upgraded file and map them locally in vRSLCM.

4 Select the version to which you want to upgrade the identity manager.

5 Enter the **SSH Password**, **vIDM Root Password** and click **Next**.

6 Click **Run Precheck** and click **Upgrade**.

7 If you have selected to install a new existing identity manager.

   a Select an existing data center or click **+** to add a data center.

   b Select **Identity Manager version** from the drop-down menu.

   c Click **Install**.

8 Under **Access Control**, after configuring VMware Identity Manager, click **Add User/Group** to add existing Active Directory users and assign roles to manage vRealize Suite Lifecycle Manager.

9 To remove an existing user from the list of users, click **Remove User**.

With 1.3 onwards, when you remove a user, it means that you are removing the role mapping for that selected user. Therefore, the user is not available from the vRealize Suite Lifecycle Manager access control.

After vRealize Suite Lifecycle Manager is registered to the identity manager, vRealize Suite Lifecycle Manager is visible in the VMware Identity Manager app catalog. You should have at least one role attached to that user.

What to do next

You can view the installation progress for a new VMware Identity Manager on the **Requests** tab. When the request shows a status as **COMPLETED**, vRealize Suite Lifecycle Manager is registered to VMware Identity Manager.

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 2018 or vCloud Suite 2017 or 2018 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. The vRealize Suite Lifecycle Manager 2.0 contains the product support pack for vRealize Network Insight 4.6.2 and 4.7.1. For more information, see KB article 60237. Download the support pack from the *VMware Solution Marketplace*.

Procedure

1 Click **Settings** and navigate to **Product Support > My VMware**.

2 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 Enable or Disable Proxy Settings.

Enable or Disable 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) as well as Proxy with AD configuration, are supported by vRealize Suite Lifecycle Manager as of now.

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. Click **Settings** and click the **My VMware** tab.

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

2. 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.

3. If you are enabling proxy, enter the server, port, user name, and password for the proxy server.
4. Click **Submit**.

vRealize Suite Lifecycle Manager Logs

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

Starting with vRealize Suite Lifecycle Manager 1.3 and later, vRealize Suite Lifecycle Manager logs are written in `vrlcm-server.log` and `vrlcm-xserver.log`. For an upgraded scenario, the older logs of `catalina.out` and `console.log` are zipped and is available as part of support bundle.

Configure vRealize Suite Lifecycle Manager Logging

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 to keep.

Procedure

1. Click **Settings** and click the **Logs** tab.
2. In the **Select Log Level** drop-down menu, select the level of information vRealize Suite Lifecycle Manager collects in its log files.

3 In the **Select Log File Count** drop-down menu, select the number of log files for vRealize Suite Lifecycle Manager to keep.

vRealize Suite Lifecycle Manager starts a new log file when the previous file reaches more than 25 MB. vRealize Suite Lifecycle Manager keeps the most recent log files and deletes any older log files over the number specified.

Note For more information on downloading log files, see Download vRealize Suite Lifecycle Manager Logs.

4 Click **Update Log Level**.

Download vRealize Suite Lifecycle Manager Logs

Download vRealize Suite Lifecycle Manager logs to help troubleshoot any problems you encounter.

Procedure

1 Click **Settings** and click the **Logs** tab.

2 Click **Trigger Download Logs**.

Note After you trigger the download logs, you can go to request page to monitor the log download status. For vRealize Suite Lifecycle Manager 1.3, the relevant logs for LCM appliance are found in the following locations:

- `/var/log/vlcm/vrlcm-server.log`: Holds the engine logs
- `/var/log/vlcm/vrlcm-xserver.log`: Holds the log for the xenon layer

What to do next

View download progress on the Requests page. When the download is complete, vRealize Suite Lifecycle Manager displays a link to the downloaded logs.

Generate Certificate

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

Note After an upgrade from vRealize Suite Lifecycle Manager 1.3 to 2.0, if a certificate is generated in the older version of vRealize Suite Lifecycle Manager then such certificates are not available in the latest version under the Certificates tab. However, you can add the older certificate during a scale out by click **Add**. This populates the older certificate data from the environment's Infrastructure properties.

Prerequisites

- Certificates that are less than 15 days cannot be imported.
- To manage the certificate for an imported environment, add the certificate in the LCM and perform the replace certificate operation in the product through LCM.

Procedure

1 To add a certificate, navigate to **Certificate Management > Add Certificate**.

2 You can either select Generate Certificate or Import Certificate.

Option	Description
Generate Certificate	a Enter the required fields. See Step 3 for the field descriptions. b Enter the **FQDN** or **IP Address**.
Import Certificate	a Enter a valid certificate name. b In the Passphrase field, type <Cert-Password>. c Click **Choose File** and browse to the saved PEM file. d When you upload a PEM file, the private key details are populated automatically. e When you upload a PEM file, the certificate details are populated automatically.

3 To generate a CSR, click **GENERATE CSR**.

Enter the required details.

Fields	Description
Certificate Name	Enter a valid certificate name.
Common Name	Enter a common name to identify the certificate.
Organization	Enter the Organization name.
Organizational Unit	Enter the Organization Unit.
Country Code	Enter a country code which should in two characters only.
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.

4 Click **Generate**.

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. You can use the CSR option to sign the certificate authority to make it as a trusted certificate after you download the PEM file.

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

6 While you are creating an environment, you can toggle the **Provide Product Specific Certificate** to add certificate under the **Certificate** tab.

Note You can also view the associated components that are available for a vRealize Automation instance.

Enabling the Product Specific Certificate allows you to specify the certificates at the product level but not at the environment level.

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

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 LCM appliance.

You can record SNMP configurations, that are relevant to vRNI. 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 vRNI 4.0 and later, a new brick size is introduced in vRSLCM, 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.

To edit a configuration:

1 Click **Settings** and navigate to **Servers and Protocols > SNMP Configurations**.

2 Click **Add Configuration**.

3 To select the **SNMP Version**, select **2C** or **3**.

4 Enter the **Username** and **Context Name**.

5 Enter a valid **Community String**, and **Context Name**.

6 Enter the **Authentication Type**, **Password**, and **Privacy Type**.

7 Click **Add**.

Configure Log Insight Agent

vRealize Suite Lifecycle Manager 1.3 supports Log Insight agent. You can configure to analyze them to understand the performance of the appliance. You can configure vRealize Log Insight Linux agents in the vRealize Suite Lifecycle Manager virtual appliance.

You can configure vRealize Suite Lifecycle Manager appliance to forward `cfapi` or system logs and events to the vRealize Log Insight instance. All `cfapi` or `syslog` information can then be viewed and analyzed from the vRealize Log Insight Web interface.

Prerequisites

vRealize Log Insight agent comes pre-installed on the vRealize Suite Lifecycle Manager virtual appliance.

Procedure

1 Log into the vRealize Suite Lifecycle Manager virtual appliance.

   a Open a Web browser and go to https://vRSLCMIP/vrlcm and login with your user credentials.

   b From the **Home** page, click **Settings > Log Agent Configuration**.

   c Update the following parameters in the LCM UI section and save your changes.

```
[server]
hostname=vrli-cluster-01.sfo01.rainpole.local
proto=cfapi
port=9000
```

   Or

```
hostname=vRealize Log Insight hostname
proto=syslog
port=514
```

   Note Edit the `liagent.ini` file on the first vRealize Suite Lifecycle Manager virtual appliance if the user wants to change the protocol. Restart the Log Insight agent by running the following command: `/etc/init.d/liagentd restart`

2 Configure the Linux Agent Group on the Log Insight server.

   a Open a Web browser and go to `https://vRealize Log Insight hostname/IP`.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

   c Click the configuration drop-down menu icon and select **Administration**.

   d Under **Management**, click **Agents**.

   e From the drop-down menu on the top, select vRealize Suite Lifecycle Manager - Linux from the **Available Templates** section.

   f Click **Copy Template**.

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 are not used by the vRealize Suite Lifecycle Manager appliance itself, they are also used as input to vRealize Suite product deployment schema.

Prerequisites

Verify that the NTP servers are functioning.

Procedure

1. From vRealize Suite Lifecycle Manager, click **Settings** and select **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**.
5. To edit, click the edit icon on the list of NTP servers.

   Note You cannot edit the FQDN/ IP Address, you can only edit the name of the NTP server.

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 vrslcm_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 typing **Logout**.

Add a Data Center to vRealize Suite Lifecycle Manager

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

Procedure

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

   You can see all the datacenters along with its products that are associated with them. You can also click on the product icons that will direct 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 any INITIATED, IN PROGRESS or COMPLETED request for an environment, then you cannot delete a datacenter. If it has a FAILED request, or request related to vCenter, such requests will get archived.

What to do next

Add a vCenter to the data center. See Add a vCenter to a Data Center.

Assign a User Role in vCenter Server

Create a user role in the vSphere Web 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.

Procedure

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

2 On the home page of vSphere Web Client, click **Roles** under Administration.

3 Create a role for all system interactions between vRealize Suite Lifecycle Manager and vCenter Server.

4 On the **Roles** page, click the **Create role action** icon.

5 Clone **Read-only** and provide a name to the role.

6 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	■ Datastore ■ Select All privileges ■ Host.Local ■ Operations- Add Host to vCenter ■ Operations - Create Virtual Machine ■ Operations - Delete Virtual Machine ■ Operations - Reconfigure Virtual Machine ■ Network ■ Assign Network ■ Resource ■ Assign vApp to Resource Pool ■ Assign Virtual Machine to Resource Pool ■ vApp ■ Select All privileges ■ Virtual Machines ■ Select All privileges ■ Content Library ■ 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.

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

8 Select **Global Permissions** under the Administration and click **Manage**.

9 To add permissions, click the plus sign.

10 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 **Data Centers**.
2. On the **Data Centers** page, click **Manage Datacenters**.
   a. Click **+ Add vCenter**.
   b. Enter the **Name** in the form of a fully qualified domain name.
   c. Type the location and click **Add**.
3. On the **Data centers** page, select **Manage vCenter Servers** tab.
   a. Select a newly added or an existing datacenter from the drop-down menu.
4. Enter the **User Name** and **Password** for the vCenter server.

   Either an administrator or a user with administrator role can use vCenter 6.7.
5. 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.
6. To import vCenter Servers, select Data Center location from the drop-down menu, 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.

Creating an Environment

2

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	7.5 and 7.6
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	7.0.0 and 7.5.0
vRealize Log Insight	4.7.0, 4.7.1 and 4.8.0
vRealize Network Insight	3.9.0 and 4.0.0

For more information on installing vRSLCM and installing vRealize Suite Products, see:

- Chapter 1 Installing and Configuring vRealize Suite Lifecycle Manager
- Install suite products

This chapter includes the following topics:

- Create a New Private Cloud Environment Using the Installation Wizard
- Import an Existing Environment using Installation Wizard
- Create a New 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. See Add a vCenter Server to a vRealize Suite Lifecycle Manager Data Center.

- 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
- 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. Configure Environment Settings for a New Private Cloud

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

2. Select the vRealize Suite Products to Install

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

3. Configure Licensing and Accept License Agreement

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

4. Configure Infrastructure Details

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

5. Configure Certificate Details

   To create an environment you can use the existing certificate.

6. Configure Network Details

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

7 Configure Product Details

With this page, you can view the list of products that were selected initially in the create environment page.

8 Configure Private Cloud Environment Details

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

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 Confirm Environment and Installation Settings

Verify that the environment and installation settings are accurate.

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 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 Select the environment type.

Option	Description
Production	Production
Test	For testing new developments
Stage	To stage changes before releasing them to production
Development	For active development

Environment type has no bearing on the configurations or product functioning at the moment.

4 In **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.

5 Enter an **Administrator Email** for vRealize Suite Lifecycle Manager.

This is applicable forvRealize Log Insight email alerts.

6 Enter a **Default password for all products** to set a common password for all vRealize Suite products in the environment.

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.

7 (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.

8 Click **Next**.

Select the vRealize Suite Products to Install

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 or solution.

Option	Description
Products	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 and existing installation of the product. For each new install, select the product **Version** and **Size** to deploy.
Solutions	Select a use case-based solution for the environment, and vRealize Suite Lifecycle Manager installs the vRealize Suite products and product versions best suited to that use case. You can mouse-over the product icons to see which products and product versions are included in each solution. vRealize Suite Lifecycle Manager offers the following environment solutions: ■ **IT Automating IT** - Enable automation and simplification of workload provisioning tasks of production-ready infrastructure and applications across multi-cloud environments. For details, see VMware Validated Design for IT Automating IT. ■ **Micro-Segmentation** - Enable distribution of firewall and isolation policies to create better network security built inside the data center. For details, see VMware Validated Design for Micro Segmentation. ■ **Intelligent Operations** - Enable proactive identification and remediation of performance, capacity, and configuration issues of the infrastructure. For details, see VMware Validated Design for Intelligent Operations.

2 Click **Next**.

Configure Licensing and Accept License Agreement

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 Select the license key from the drop-down menu or manually enter license key for **Suite License Key** and click **Next**.

3 Select the license key from the drop-down menu after registering with MyVMware account.

The drop-down lists the license keys that are generated from MyVMware. While deploying products from vRealize Suite Lifecycle Manager 2.0, you should not use vRealize Suite Standard license if vRealize Automation 7.5 and vRealize Business for Cloud 7.5 is included in the deployment.

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 the required **Cluster**, **DataStore**, and **Disk Format**.

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. When 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 might not be able to 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 Infrastructure-related issues are detected and can be corrected before triggering the deployment.

3 Select the required Time sync mode:

Option	Description
Use Time Server (NTP)	When you select the NTP Server option, you have to select the assigned time server from the NTP list. If a 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.

4 After you have added NTP servers, you can click **Select Servers** to add an NTP at an Infrastructure level.

5 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.

6 Click **Finish**.

7 To configure the **Network** details, click **Next**.

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**, toggle to provide **Product Specific Certificate**.

When you disable the Product-Specific Certificate, you can specify the certificates at the environment level. When you toggle the option, the product certificate is then visible under the Product Properties for the product instance.

2 Select the **Certificate** from the drop-down menu.

3 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.
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.

4 Click **Generate**.

5 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>.
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.

6 Click **Import**.

7 Click **Next**.

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 vRSLCM. This is applicable for starting from vRSLCM 1.0 and above.
- Verify that you have Domain Name mapped for the IP addresses used for deployed.

Procedure

1. Under the **Network Details** page, enter the **Default Gateway** address.
2. Enter the **Domain Name**, **Domain Search Path** and **Domain Name Servers**.
3. Enter the **Netmask** IP address.
4. Click **Next**.

Configure Product Details

With this page, you can view the list of products that were selected initially in the create environment page.

Procedure

- Under the **Product Details** page, if you have selected all the products for a new installation.

Product	Function
vRealize Automation	a Select the **Monitor with vROps** checkbox to monitor health of vRealize Automation. b Select the **Workload Placement and Reclamation** checkbox to manage the workload using load balancer and reclaim unused resources from the resource pool. **Note** This option is mainly used for cross product integration and is only applicable for vRealize Operations Manager and vRealize Automation. This option is only available for a new installation where in vRealize Operations Manager monitors health of vRealize Automation. Interproduct configuration is not supported for an existing environment. Only new vRealize Automation installation will have the inter product configuration support. During the new installation of vRealize Automation, vRealize Operations Manager must be present, irrespective of vRealize Operations Manager deployment, which includes create, import environment and organic growth. If vRealize Operations Manager is not present at the time of installation then the user has to perform integration outside of LCM. Cross product integration for vRealize Automation with vRealize Operations Manager is not applicable for import of vRealize Automation. And is only applicable in case of new installation of vRealize Automation. Also, option to perform Cross Product Configuration should come for vRealize Automation only in 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. c Enter the **Windows Username**, and **Password**. d Select the **Applicable Time Sync mode**. e Select the **Time Server (NTP)**. For more information, see Configure NTP Servers. f If you want to configure cluster virtual IPs, then select the **Yes** or **No** options. If you select yes, the load balancer is connected to the individual product and then configure the **vRA Appliance**, **IaaS Web**, and **IaaS Manager** manually. g As a cloud admin, you can configure a template, click **Yes**, and from the **Configure Windows box**, select the required windows template and its associated spec. When you select **Yes**, the Window box section appears. If no is selected, then vRSLCM will not deploy new Windows VMs for IaaS components. **Note** For more information on configuring IaaS components, see Deploy Windows VMs for vRealize Automation Installation.
vRealize Business for Cloud	a Under **Product Properties** section, enter the **VM Name**, **Hostname**, and **IP Address**.

Product	Function
vRealize Log Insight	a Select the node size from the drop-down menu. b Under **Integrated Load Balance Configuration**, if you select the **Configure Cluster Virtual IPs**, enter the **FQDN** and **Virtual IP Address**. c To add more node, click **ADD NODE**. d Select the **Applicable Time Sync Mode**. e Under components, enter the **vRLI** master node details.
vRealize Operations Manager	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 master node details.
vRealize Network Insight	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.

Deploy Windows VMs for vRealize Automation Installation

With vRealize Suite Lifecycle Manager 2.0, 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 vRSLCM installation wizard. Click **Yes**, and from the **Configure Windows box** under **Product properties**, select the required windows template and its associated spec.

   When you select **Yes**, the Window box section appears. If you select no, then vRSLCM will not deploy new Windows VMs for IaaS components.
5. To **Configure Cluster Virtual IPs**, select the **Yes** or **No** options.

   If you select yes, then the load balancer is connected to the individual product and then configure the **vRA Appliance**, **IaaS Web,** and **IaaS Manager** manually.

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 vRSLCM. 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.

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 the database software should 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 vRA deployment request from LCM.

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, LCM does not deploy IaaS database machine. LCM 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 place 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 LCM (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.

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 LCM 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 2.0.
- 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 LCM 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 work-around, 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 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 Generate Certificate.

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, then 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 vRSLCM, 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 of the Management Site 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.

   ```
   service vami-lighttp restart
   ```

5. Run the following command to restart the haproxy service.

   ```
   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.

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 withVMware Identity Manager and so on.

Procedure

1 Click the **vRealize Automation** check box to configure installation details for vRealize Automation.

   a 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 **Add** 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 tovRealize 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 by using the form `dbhost,SQL_port_number\SQLinstance`. If the database instance is a new one and default instance is expected, then provide hostname of the DB VM only. If you specify a port number or named instance, use `FQDN,Port\Instance format`. If the database already exists and no changes needed then from advanced properties, you can provide the database name. For more information, see Microsoft SQL server.

   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.

   There are three types of deployments in vRealize Automation which includes small, medium, and large.

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 **Add** 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 **Add** to add additional 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) To add an additional component, click **Add** 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 **Advanced Settings**, 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) To add an additional component, click **Add** 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**.

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 New Private Cloud Environment Using a Configuration File. Modify the exported configuration file as required before using it create another private cloud. The Private and master 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 you are asked to enter the **Infrastructure**, **Network** and **Certificate** details, as a new Install of product requires those details. 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**.

Create a New Private Cloud Environment Using a Configuration File

You can create a private cloud environment using a product configuration file.

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. See Add a vCenter Server to a vRealize Suite Lifecycle Manager Data Center.
- In the configuration file, change `encoded:true` to `encoded:false`, and ensure that all passwords in the configuration file appear in plain text.

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 Select the environment type.

Option	Description
Production	Production
Test	For testing new developments
Stage	To stage changes before releasing them to production
Development	For active development

   Environment type has no bearing on the configurations or product functioning at the moment.

4 In **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.

5 Enter an **Administrator Email** for vRealize Suite Lifecycle Manager.

   This is applicable forvRealize Log Insight email alerts.

6 Enter a **Default password for all products** to set a common password for all vRealize Suite products in the environment.

   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.

7 (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.

8 Click **Use Configuration file** toggle feature.

9 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 sample JSON file, see KB article 2151908.

Note If the JSON file contains encrypted passwords, then you have to convert them to plain text and set the paramater `encoded` to false in the JSON file.

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

3

You can manage data centers, vCenters, and vRealize Suite products in your private cloud environments.

This chapter includes the following topics:

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 the ellipsis (...) for the environment, and select **Add Data Source**.

3 You can select the required vCenter, NSX and related Switches.

4 **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**. For more information on adding SNMP configuration, see Data Source Using SNMP Configurations for vRealize Network Insight. **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 2.0, 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 **Data Source > Bulk Import**.

After import of product for a scale-out, you need to add certificate. To manage certificate, the same certificate needs to be added from the Settings tab. For more information on adding components, see Add a Component to an Existing Private Cloud Environment.

2 Select CSV or JSON format to import the data sources in a defined report format.

3 Click **Choose File** and 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**.

Add a Component to an Existing Private Cloud Environment

You can add components to your product to configure a multi node setup to form a cluster.

Prerequisites

Verify that there is a node available and is configured.

Procedure

1 On the environment card, select a product, click the vertical ellipses, and select **Add Component**.

For an imported environment, manually enter the fields for the selected product.

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 fields are auto-populated. If the environment is imported, you have to manually enter the fields.

5 Click **Next**.

6 Select the **Applicable Time Sync Mode** and under the components section, select the node.

The Advanced settings provides more information on configuring the selected node in a cluster. For an imported environment in 2.0 where a product needs to be scaled out, ensure that the provided certificate is master-node certificate, as the pre-check matches for the master node certificate. For environments from older vRSLCM 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 fields.

The fields in this section varies for different products.

Product Name	Components
vRealize Automation	■ vra-server-secondary ■ iaas-web ■ iaas-manager-passive ■ iaas-dem-orchestrator ■ iaas-dem-worker ■ proxy-agent-vsphere
vRealize Operations Manager	■ Data ■ Remote Collector
vRealize Business for Cloud	VRB-Collector
vRealize Log Insight	VRLI-Worker
vRealize Network Insight	■ vRNI-Platform ■ vRNI-Collector

8 Enter the required fields and click **Next**, and run **Precheck**.

9 Read the summary and click **Submit**.

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 New 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.

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.

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 LCM 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**.

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.

- Upgrade a vRealize Suite Product

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

- Configuration Drift

  Configuration drift shows the changes in product configuration over time and allows you to revert a product to an earlier configuration state.

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.

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.

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.

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, 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.

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 LCM) 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 LCM virtual appliance.
vRealize Suite Lifecycle Repository	When you select this option, you can select the upgrade path available after mapping the binaries through LCM.

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**.

Configuration Drift

Configuration drift shows the changes in product configuration over time and allows you to revert a product to an earlier configuration state.

- Save a Product Baseline

  Save a product baseline to capture a product's configuration parameters at a given time.

- View a Configuration Drift Report

  View a configuration drift report to view the changes in a product's current configuration compared to the product's configuration drift baseline.

- Revert a Product to a Previous Configuration

  You can revert a product's configuration to a previous state if you discover problems with the product's current configuration.

- Export a Configuration Drift Baseline

  Export a configuration drift baseline to use a product's baseline as the configuration drift baseline for other deployments of the product.

- Import a Configuration Drift Baseline

  Import a configuration drift baseline to have vRealize Suite Lifecycle Manager use an imported baseline to generate configuration drift reports for this product.

- Replace Certificate for vRealize Suite Lifecycle Manager Products

  You can replace your existing certificates for products within the vRealize Suite Lifecycle Manager.

Save a Product Baseline

Save a product baseline to capture a product's configuration parameters at a given time.

vRealize Suite Lifecycle Manager uses the product baseline to generate configuration drift reports that show how the current product configuration differs from the baseline configuration.

Procedure

1 Click **Manage Environments**.

2 Click **DETAILS** for the environment the product to upgrade is part of.

3 Click the ellipses (...) icon next to the name of the product and select **Save Baseline**.

vRealize Suite Lifecycle Manager saves the current product configuration as the product baseline. You can save a new product baseline at any time.

View a Configuration Drift Report

View a configuration drift report to view the changes in a product's current configuration compared to the product's configuration drift baseline.

Prerequisites

Verify that the product has a saved baseline for vRealize Suite Lifecycle Manager to measure current product configurations against. See Save a Product Baseline.

Procedure

1 Click **Manage Environments**.

2 Click **DETAILS** for the environment.

3 Click the ellipses (...) icon next to the name of the product and select **Show Report**.

4 Select an instance on the **Drift TimeLine** to view the configuration drift report for the date and time listed for the instance.

5 Toggle **Show Drifted Parameter**.

6 Select the view for the drift report.

- Configuration Parameter
- Base Configuration
- Selected Configuration
- Comparison Status

7 To edit, click **EDIT TO REMEDIATE**.

Revert a Product to a Previous Configuration

You can revert a product's configuration to a previous state if you discover problems with the product's current configuration.

Prerequisites

You must have a saved configuration drift baseline for the product to revert it to a previous state. See Save a Product Baseline.

Procedure

1 Click **Manage Environments**.

2 Click **DETAILS** for the environment the product to upgrade is part of.

3 Click the ellipses (...) icon next to the name of the product and select **Show Report**.

4 Select an instance on the **Drift TimeLine** to view the configuration drift report for the date and time listed for the instance.

5 Toggle **Show Drifted Parameters** and verify that you have a stable configuration available to revert to.

6 Click **Remediate**.

7 Click the date and time under **Remediation Baseline** to change the date and time to use as the product baseline to revert to.

By default, the remediation baseline is set to the saved configuration drift baseline.

8 Verify that the configuration values listed in the remediation baseline are the values you want to revert to, and click **Save**.

What to do next

Check the **Recent Reports** page and check the **Remediation Report** to verify the remediation completed without errors.

Save a new product baseline. See Save a Product Baseline.

Export a Configuration Drift Baseline

Export a configuration drift baseline to use a product's baseline as the configuration drift baseline for other deployments of the product.

Procedure

1 Click **Manage Environments**.

2 Click **DETAILS** for the environment the product to upgrade is part of.

3 Click the ellipses (...) icon next to the name of the product and select **Export Baseline**.

4 Click **Save File** and click **OK**.

The product's configuration drift baseline file is downloaded to your browser's default download location.

What to do next

Import the downloaded configuration drift baseline file to other deployments of the product. See Import a Configuration Drift Baseline.

Import a Configuration Drift Baseline

Import a configuration drift baseline to have vRealize Suite Lifecycle Manager use an imported baseline to generate configuration drift reports for this product.

By default, the configuration drift baseline for a product is the product configuration at the time of deployment.

Note When an existing vRealize Automation environment is imported into vRealize Suite Lifecycle Manager and the primary and secondary virtual appliance root passwords differ, virtual machine-related configurations like certificates, network details, and file-based configurations are not collected from all virtual appliances as part of the baseline creation. Only the master or primary node virtual machine configurations will be collected during baseline creation.

Prerequisites

Export a configuration drift baseline from another deployment of this product. See Export a Configuration Drift Baseline.

Procedure

1 Click **Manage Environments**.

2 Click **DETAILS** for the environment the product to upgrade is part of.

3 Click the ellipses (...) icon next to the name of the product to and select **Import Baseline**.

4 Click **Browse**, navigate to the configuration drift baseline file to import, and click **OK**.

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 vRSLCM VAMI/VA certificate, see VMware Validate Design.

Prerequisites

Verify that a product has an existing certificate.

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**, select a **Product or a Component** level certificate for an vRealize Automation from the drop-down menu and click **Next**.

With vRealize Suite Lifecycle Manager 2.1, you can now select both product level and component level certificates for a vRealize Automation instance.

4 Select a certificate and review the certificate summary, and click **Next**.

5 To validate the certificate information, click **RUN PRECHECK** and click **Finish**.

The replace certificate is supported from the following product versions:

- vRealize Automation - 7.5.0
- vRealize Business for Cloud - 7.5.0
- vRealize Operations Manager - 7.0.0
- vRealize Log Insight - 4.7.0
- vRealize Network Insight 3.9.0

6 Go to the **Requests** page to see the status of this request.

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

Verify that you have a private cloud environment that contains VMware vRealize Operations Manager. For information on adding to an existing environment, see Add a Product to an Existing Cloud Environment. For information on creating an environment, see Creating a Private Cloud 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. Configure vRealize Operations Manager with the VMware SDDC Management Health Solution Management Pack. See VMware SDDC Management Health Solution microsite on the VMware Solution Exchange.
2. Configure adapter instances for vRealize Log Insight, vRealize Business for Cloud, and vRealize Automation in vRealize Operations Manager.

   For information on configuring adapters in vRealize Operations Manager, see the following topics:

   - Configuring vRealize Log Insight with vRealize Operations Manager
   - Configure the vRealize Business for Cloud Adapter
   - Configuring vRealize Automation
3. If you have an instance of vRealize Automation in your environment, install End Point Operations Management agents on all nodes on vRealize Automation applications and on any new node added to the vRealize Automation cluster later.

   See End Point Operations Management Agent Installation and Deployment .

vRealize Suite Lifecycle Manager displays the health status of the vRealize Suite management stack as provided by VMware SDDC Management Health Solution Management Pack.

vRealize Suite Lifecycle Manager retrieves health status information from one instance of vRealize Operations Manager in a given private cloud environment. The health displayed applies only to the vRealize Suite products configured in the target vRealize Operations Manager instance within the private cloud environment. Do not configure additional vRealize Suite products from other private cloud environments in the same instance of vRealize Operations Manager.

What to do next

View the health status of vRealize Suite in vRealize Suite Lifecycle Manager. See Health Status in vRealize Suite Lifecycle 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: ■ 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 monitory 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. See My VMware Settings.

Procedure

1 Click **Marketplace**.

2 Click the **Refresh Content from Marketplace** button.

You can also click the **Sync Content**, if you are syncing marketplace for the first time.

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 1.3 supports vRealize Automation 7.4, 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. It is recommended to extend the storage from the system settings page, if multiple OVAs are downloaded and to avoid disk storage alert.

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.

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 **Download** 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 **Download** 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 vRA, 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**.

The content is deleted from vRealize Suite Lifecycle Manager and no longer appears under downloaded content on the **Marketplace** page.

Content Lifecycle Management

4

Content lifecycle management in vRealize Suite Lifecycle Manager provides a way for release managers and content developers to manage software-defined data center (SDDC) content, including capturing, testing, and release to various environments, and source control capabilities through GitLab integration. Content Developers are not allowed to set Release policy on end-points only Release Managers can set policies.

You can use content lifecycle management to dispense with the time-consuming and error-prone manual processes required to manage software-defined content. Supported content includes entities from

- vRealize Automation 7.2 and later
- vRealize Orchestrator 7.x and later
- VMware vSphere 6.0 and later.
- vRealize Operations Manager 6.6.1+ and later.
- Source Control server: All latest versions of Gitlab Community Edition and Enterprise Edition.

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.
- vRealize Orchestrator is embedded on the appliance to run only content workflows.
- Updated vRealize Code Stream Pipeline services.

If there are dependencies between captured content packages, you can use content management life cycle to link them together while still having independent version control for each content package. 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 stale. vRealize Automation allows 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-ComponentProfiles in vRealize Suite Lifecycle Manager to a target end-point if the corresponding value set already exists on the end-point.

vRealize Suite Lifecycle Manager content lifecycle management supports native integration with GitLab (both CE or EE), including capabilities such as auto merge and performing a code review. You can provide an access token against your GitLab user profile so that content that has been captured can be checked in, checked out, and released. With vRealize Suite Lifecycle Manager 1.2, you now have the provision to toggle the usage of Content Lifecycle on your UI under the **Features** tab. To access the Content Lifecycle Management, navigate to **Settings > Features**. By default, when content lifecycle management is enabled in LCM UI, SSH service will be enabled and you cannot disable it.

Using public API available for update settings including SSH connection, you can disable the SSH, even if the Content Lifecycle Management is enabled in vRSLCM UI, but Content Lifecycle Management will stop functioning. So SSH connection should not be disabled using available Public API, if content management feature is enabled in LCM UI.

- 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 use a source control access. With this privilege, a release manager can be selecting the GitLab type and entering the git lab 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 source control server to the system.

- Working with Content Settings

  You can define a content release and manage source control access while you configure extensibility of your content release.

- Working with Content Pipelines

  Content pipeline services allow the custom release flow of content to be applied, there are various pre-pipelines or post pipelines that are set up to run that are configured in the Content Settings page. Each pipeline can be run either in the background (asynchronous call) or the whole release flow can stop until the pipeline has completed (synchronous). With Lifecycle Manager 2.1, you cannot create of new pipeline.

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 monitor health of your environment.
- 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. Under **Content Management**, click **Endpoints**.
2. Click **NEW ENDPOINT**.

3 Select **Orchestration**.

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 vRO Package provided as input.

4 Click **Next**.

5 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.

vRO–Server–FQDN`:Port`

d Enter a user name and password to use to access this content endpoint.

6 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.

7 Select **vRO Package**.

The vRealize Orchestrator package can be captured from an endpoint and is associated with the content endpoint. Selection of a vRO package is a post deployment capability that imports the package once any other can has been deployed allowing localized or regional settings to be maintained.

- 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 2.1, 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.

8 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.
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.

9 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 Under **Content Management**, click **Endpoints**.

2 Click **NEW ENDPOINT**.

3 Select **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 cam 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.

e Enter a tenant name, user name, and password to use to access this content endpoint.

f Select a vRealize Orchestrator endpoint to associate with this endpoint from the **vRO Server Endpoint** drop-down menu.

When selecting a user account for exporting or importing content into vRSLCM, 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 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. Under **Content Management**, click **Endpoints**.
2. Click **NEW ENDPOINT**.
3. Select **Source Control**.
4. Select the configured **Bitbucket server**, **cloud**, or **Gitlab**.
5. Enter the information for the Source Control content endpoint.
   a. In the **Name** field, 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 Bitbucket cloud, enter *repository_name*

   Note In bitbucket cloud, you can only create a repository and use the repository name. The source control endpoint with a repository needs to be initialized with any file. Gitlab and bitbucket 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 bitbucket 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.

Procedure

1. Under **Content Management**, click **Endpoints**.
2. Click **NEW ENDPOINT**.
3. Select **vCenter**.

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 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 monitor health of your environment.

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. Under **Content Management**, click **Endpoints**.
2. Click **NEW ENDPOINT**.
3. Select **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 a 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 a SSH User in vRealize Operations Manager

You can create a vRealize Operations Manager end-point in vRSLCM Content Management end-point.

1 When you are selecting a Root as a SSH user from the content endpoint, create a user on vRealize Operations Manager appliance. The user must have SSH access and belong to user groups root and wheel with a valid home directory.

2 Log into the vRealize Operations Manager appliance as root user and create user on the vRealize Operations Manager appliance using below command. For example, `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 - `passwd sshuser`.

6 Enabled password less sudo capabilities for the user

```
Run command visudo

sshuser ALL = NOPASSWD: /usr/lib/vmware-vcopssuite/python/bin/python /usr/lib/vmware-
vcops/tools/opscli/ops-cli.py *
sshuser ALL = NOPASSWD: /bin/rm –rf /tmp/*
sshuser ALL = NOPASSWD: /bin/mv /tmp/*
```

Note OPS-CLI is used for most of the vRealize Operations Manager contents to export or import as part of content capture or release in vRealize Suite Lifecycle Manager. Therefore, SSH credentials are required to execute those commands.

Delete a Content Endpoint

You can delete an existing content endpoint.

Procedure

1 Under **Content Management**, click **Endpoints**.

You have to manually delete the endpoint manually.

2 Click the vertical ellipses to the left of the endpoint, and select **Delete**.

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. Under **Content Management**, click **Endpoints**.
2. 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.

- Add Content

  You can add content from an existing content endpoint.
- 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 a 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 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 2.0 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.

Add Content

You can add content from an existing content endpoint.

Prerequisites

Verify that you have added a content endpoint.

Procedure

1. Under **Content Management**, click **Content**.
2. Click **ADD CONTENT**.

   Note A content can be added either with the Add Content button or with an inline capture, if a version has already been captured.

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 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.
   c. Select the content type and content to capture.

d 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.

e Enter the **vRO Package Name** or select from the drop-down menu. Any spaces in the name are replaced with an _ underscore character and do not add any external URL to a vRO package name.

The vRealize Orchestrator package only exist the Content Repository, which can be checked into source control. Once the package is created, you can deploy it to your content endpoint to further work with it. If the vRealize Orchestrator package is not captured before from a given content endpoint, 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 vRO content, including individual workflows in the content files, appears in the vRO package that is created.

f If the content is ready for production, select **Mark this version as production ready**.

g Enter a description for this content version in the **Comments** field.

h 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 deploy is run in the background every 20 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 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.

7 Click **SUBMIT**.

Working with Captured Content

You can capture a new version of an existing content package.

Procedure

1 Under **Content Management**, click **Content**.

2 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 production ready	Release Manager Developer	You can view the test endpoints that have the Test policy set.
Content version is NOT marked 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 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. Currently this is not supported in vRealize Suite Lifecycle Manager 1.2.

Content Types Available for Products

The content packages available for each endpoint are displayed in the following tables.

Content Types

Table 4-1. vSphere Content Endpoint

Type	Value	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 4-2. vRealize Automation Content Endpoint

Type	Value	Description
Automation- CompositeBlueprint	vRealize Automation version 7.0+	Captures a vRealize Automation composite blueprint to deploy virtual machines managed by vRealize Automation.
Automation- Componentprofile	vRealize Automation version 7.0+	Captures a vRealize Automation component profile .
Automation- PropertyDefinition	vRealize Automation version 7.0+	Captures a vRealize Automation property definition for specifying custom properties.
Automation-PropertyGroup	vRealize Automation version 7.0+	Captures a vRealize Automation property group to group custom properties.
Automation-ResourceAction	vRealize Automation version 7.0+	Captures a vRealize Automation resource actions.
Automation-Software	vRealize Automation version 7.0+	Captures vRealize Automation software component settings that govern how middleware or applications are installed, configured, and uninstalled.
Automation-Subscription	vRealize Automation version 7.0+	Captures vRealize Automation subscription events that are triggered using the event broker. Captures the configured event and dependent workflows.
Automation-XaaSBlueprint	vRealize Automation version 7.0+	Captures vRealize Automation XaaS blueprints.

Table 4-3. vRealize Operations Manager Content Endpoint

Type	Value	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, vIews, 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 4-4. vRealize Orchestrator Content Endpoint

Type	Value	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 a 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 on 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. Under **Content Management**, click **Content**.
2. Click the name of the content package to test.
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

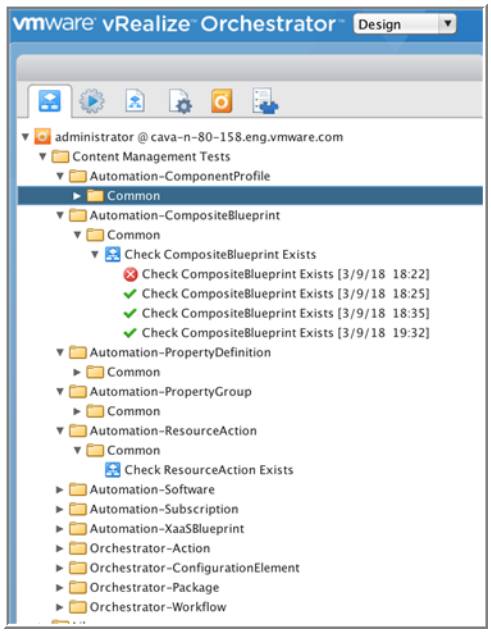
- Test endpoint

The server is a staging environment in which you can deploy the contents and run unit tests against the deployed contents to the environment.

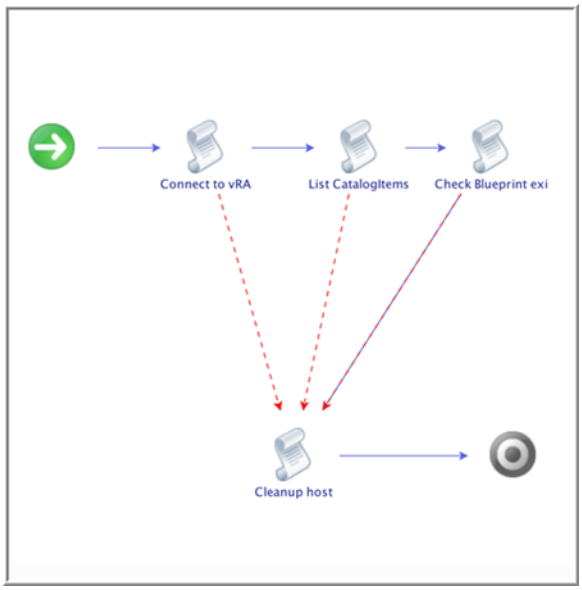
Unit Test Server

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

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 branch endpoint to provide source control for content.

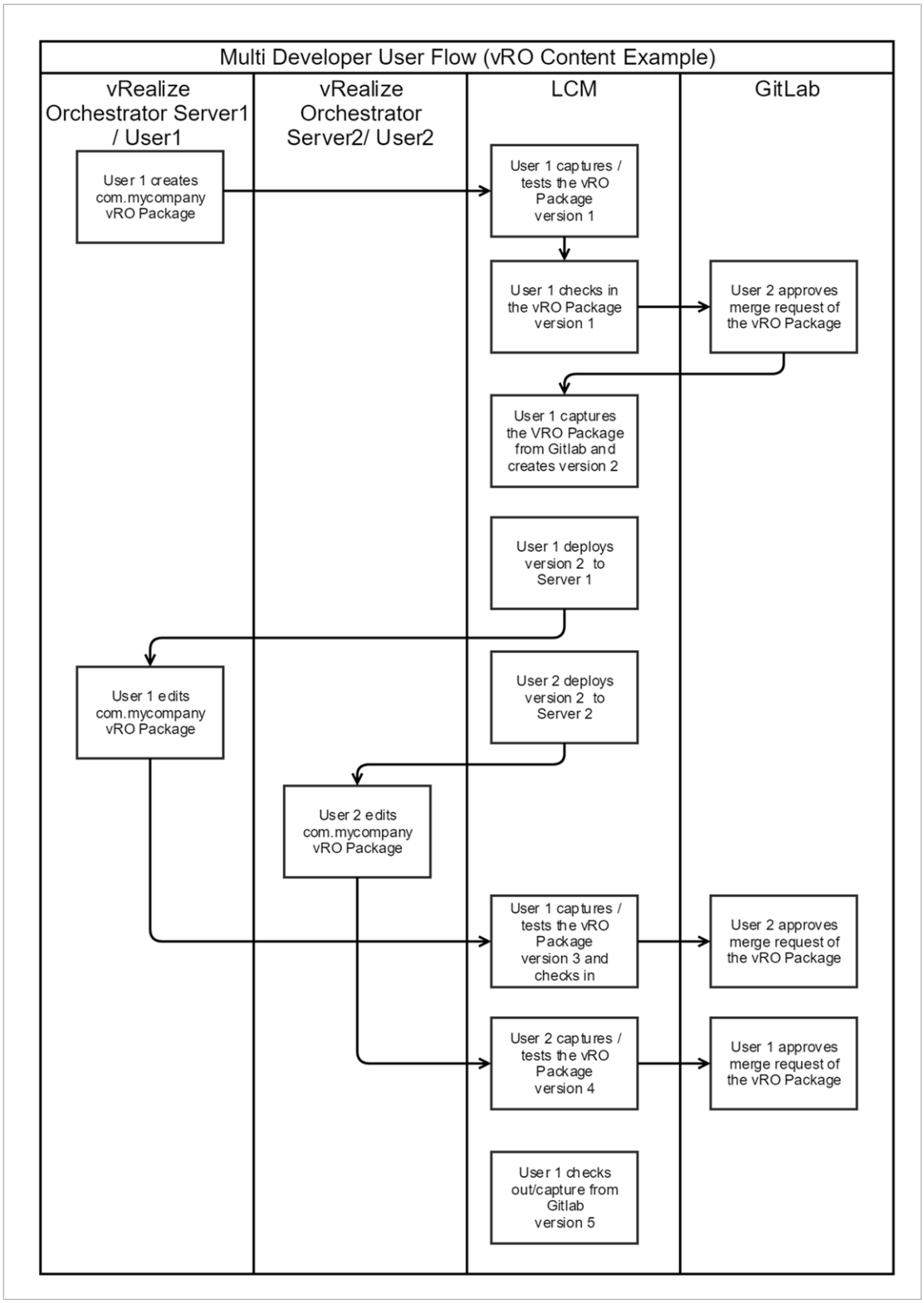
You can store content in both the vRealize Suite Lifecycle Manager version-controlled repository and a GitLab branch. This allows developers to work together to check in and check out content, and to code review changes prior to deploying to test or production environments.

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 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.
- 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.



Check In Content to a Source Control Endpoint

You can check in 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. Under **Content Management**, click **Content**.
2. Click the name of the content package to test.
3. Click the three vertical dots to the right of the version to check in, and select **Checkin**.
4. Select a content endpoint to check the content package in to.
5. Select **Include all dependencies** to include all dependencies associated with the content package in the check-in.

6 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 already exists in 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 the to view the vRO package in which it needs to be merged. With vRSLCM 2.1 patch, you have the following new features added when you check in an Orchestrator package:

- The ability to 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.
- New capability to release subset of contents from an Orchestrator-package while deploying to an endpoint.
- As part of dependency management, you have an option to remove dependency from a content version.

For a vRealize Automation content check out, you can merge directly on GitLab. You can check out without dependency or check out with dependancy, where you can perform the following:

- You need to 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 source control, you need to perform the following operation to resolve the dependency hierarchy correctly.
- Check-out the uber package and deploy to the endpoint.
- Check-out the vRealize Automation content with dependency and deploy to the endpoint.

If 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 Under **Content Management**, click **Content**.

2 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**.

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 Under **Content Management**, click **Content**.

2 Click the name of the content package to test.

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 2.0 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 left pane, select **Content Management > Content Item**.

2 Expand the **Filter Applied** tree.

3 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. ■ 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.

4 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.

5 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**. 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.

6 To deploy the content to a release endpoint, follow the wizard.

7 Click **Actions** and select **Checkin**.

Note With Lifecycle Manager 2.1, 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.

8 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**.

9 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.

10 In a content pipeline, a new multi release pipeline is initiated, where it is queued and released when the system is available to process them.

For each type of content, a separate multi release pipeline is started. All contents are grouped and are imported for performance. For example, all automation blueprints and any dependencies are downloaded from the LCM repository and released in one flow. The Pre and Post pipeline stubs support is available for the multi_release_pipeline.

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 Under **Content Management**, click **Content**.

2 Click the name of the content package to test.

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.

Access Source Control

Only a release manager can use a source control access. With this privilege, a release manager can be selecting the GitLab type and entering the git lab 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 LCM 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 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.

Prerequisites

- Verify that you have a GitLab instance (GitLab Community Edition/Enterprise Editions version 10.5.6+) and is supported for this version of vRealize Suite Lifecycle Manager.
- Log in to GitLab and generate an access token for your user with all scopes enabled. Copy and save this one-time token from GitLab.
- Log in to GitLab and verify you have group, project and branch created in GitLab before adding it as a source control endpoint.

Procedure

1. Under **Content Management**, click **Content Settings**.
2. On the **Source Control Access** tab, click **ADD SOURCE CONTROL SERVER**.
3. Select the **Source Control Type**.

   Note With Lifecycle Manager 2.1, you can now select Bitbucket Server or Bitbucket Cloud.

4 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 needs to be specified in `<GroupName>/<ProjectName>` form. Whenever multiple developers are working on the bitbucket repository then the performance is slow in the bitbucket enterprise version. Therefore, you can use at least 4vCPU machine of bitbucket.

5 Click the pencil icon for the source control server.

6 Enter your GitLab access token in the **ACCESS KEY** field, and click **SUBMIT**.

   An access token is a unique identity for a user to perform check-in or check-out to track the GitLab API. To create a access token for Gitlab, access the gitlab.eng.vmware.com and create a token name. For Bitbucket Server and Cloud, browse to bitbucket.org.com 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 Under **Content Management**, click **Content Settings**.

2 On the **Source Control Access** tab, click the trash icon for the source control server endpoint to delete.

3 Click **OK**.

Working with Content Settings

You can define a content release and manage source control access while you configure extensibility of your content release.

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
- Post-Capture
- Pre-Test
- Post-Test

- Pre-Release
- Post-Release

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 will have templates from LCM 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 `lib.json` file. This will be available when you create a publisher in Step 1.
Authentication Disabled	Disabled
Library content	■ 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). vRSLCM 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 B, first this requires a custom pipeline/workflow to be implemented. If this rule is to be bypassed, for example, for Release Mangers 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

Content pipeline services allow the custom release flow of content to be applied, there are various pre-pipelines or post pipelines that are set up to run that are configured in the Content Settings page. Each pipeline can be run either in the background (asynchronous call) or the whole release flow can stop until the pipeline has completed (synchronous). With Lifecycle Manager 2.1, you cannot create of new pipeline.

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.

Once you have selected 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.

Table 4-5. Task Types in Content Pipelines

Task Type	Description
Invoke Rest API	■ Run a `GET/POST/PUT/PATCH/DELETE HTTP` request against a given URL. ■ Custom Http header can be added. ${input.myHeader} where myHeader is an input for the pipeline. ■ Once the task has completed, you then have access to various properties: `status/responseBody/responseCode/responseHeaders` and you can access them with the $ character. For example, $.{Stage.task.status} ■ Custom Http header can be added: ${input.myHeader} where myHeader is an input for the pipeline. ■ Once the task has completed, you then have access to various properties: `status/responseBody/responseCode/responseHeaders` and you can access them with the $ character. For example, $.{Stage.task.status}
Poll Rest API	■ Run a GET HTTP request against a given URL that has a timeout and interval. The exit criteria assert a success or failure and you specify a dotted notation to a JSON field. ■ Custom Http header can be added. For example, ${input.myHeader} where myHeader is an input for the pipeline. ■ Once the task has completed, you then have access to various properties: `status/responseBody/responseCode/responseHeaders` and you can access them with the $ character. $.{Stage.task.status}
Pipeline	To create a pipeline, click **New Pipeline** and provide required inputs, for example, raise a ticket with helpdesk or email a custom notification. Using the Pipeline task you can chain pipelines together and created a catalog of content.

Table 4-5. Task Types in Content Pipelines (Continued)

Task Type	Description
Script	Run a bash or PowerShell script against a given host.
vRealize Orchestrator External	Run a vRealize Orchestrator Workflow against an external vRO Appliance. To configure vRealize Orchestrator 1 Edit on the LCM appliance `opt/vmware/vlcm/blackstone/configuration/vrcs-config/endpoints/system-vro.json and edit the pipeline-vro entry` and provide correct values for the `URL/username` and password to the remote vRO instance. `"name": "pipeline-vro", "description": "Pipeline VRO Server used by Content Lifecycle Management Services", "type": "vrcs.vco:VCOServer", "properties": {"url": "https://@LOCALHOST@:8281", "username": "@VRO_USER@","password": "@VRO_PASSWORD@","ignoreCertificateCheck": "yes" }, "tags": [], "tenantLinks": ["/tenants/default/groups/default","/tenants/default"]` 2 Restart LCM Xenon Server: `systemctl restart vlcm-xserver` 3 Against a given workflow, provide a global custom tag called vRCS_CUSTOM as the key and value. 4 To associate a vRO tag to a workflow, run the`/Library/Tagging/Tag` workflow. These workflows appear in the Pipeline Services.

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 11 content pipelines can run at a time. Some parameters are empty in Lifecycle Manager 2.1 on pipelines stubs. If you still want to use the pipelines, then you can click the package version link. And you can also perform similar operation using pre and post-test stubs.

Request Status

5

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.

With vRealize Suite Lifecycle Manager 2.0, you can now export **All Requests** or **Filtered Requests** by clicking the **Export** button. Click **Download Report** to download the Audit Report on to your local machine. Under the **Request** tab, the **Request User ID** is set to **Unknown** for the following categories.

- Requests migrated from an earlier vRealize Suite Lifecycle Manager version to 2.0.
- Requests which have been created by the system for internal processing purposes.
- Whenever a request type, ScheduledMarketplace_Sync is triggered with User ID.

Note The last two exported files on the system are available and can be downloaded from the location `'/data/lcm-audit'`. This is required, as the download link from the UI allows you to download only the last audit file at this point in time.

You can now audit all the available environment-related operations, data center, marketplace operations, and settings. You can also monitor the role-user assignment changes from vRealize Suite Lifecycle Manager.

Notifications in vRealize Suite Lifecycle Manager

6

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.

Patching for Products through vRealize Suite Lifecycle Manager 7

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

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.

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. Navigate to **Settings > Product Support** and click **Patch Binaries**.
2. To add a patch, navigate to **Settings > System Administration**, and click **Update > Install Patch**.
3. To upload patches, click **Upload Patches** and select a patch file.
4. To check if there are patches available on the internet, click**Online Patches**.
5. 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.
6. Click **Next**.
7. **Review and Install** the available patch and click **Finish**.

   The patch install request progress can be tracked under **Requests**.
8. To view the history of patches, click **Patch > History**.

9 To view patches history from Environment Card, click **View Patch History**

The vRealize Log Insight product patch history has no content even when the vRLI patches are applied successfully. This is caused due to the minor version bump 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 vRLI 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.

Backup and Restore

8

Backup and restore your vRealize Suite Lifecycle Manager system for any event of corruption, data loss or appliance failure.

To backup and restore vRealize Suite components, see the Backup and Restore section in the vRealize Suite Information Center.

This chapter includes the following topics:

- Backup vRealize Suite Lifecycle Manager using VMware vSphere Data Protection
- Restore vRealize Suite Lifecycle Manager Using vSphere Data Protection

Backup vRealize Suite Lifecycle Manager using VMware vSphere Data Protection

This section provides guidance on the use of a vSphere Storage APIs - Data Protection (VADP) solution for performing backup and restore of vRealize Suite Lifecycle Manager. You can back up vRealize Suite Lifecycle Manager by using vSphere Data Protection by creating a backup schedule and retention policies. You are not required to delete any snapshots, however, be aware that vSphere Data Protection deletes all existing snapshots at the time of backup.

Prerequisites

- Verify that vRealize Suite Lifecycle Manager VM is powered on and accessible while the backup is taking place.
- Deploy and configure the vSphere Data Protection appliance. For more information on vSphere Data protection, see *vSphere Data Protection Administration Guide*.

Procedure

1. In the left pane of the VMware vSphere Web Client, select **vSphere Data Protection**.
2. Select the pre-configured vSphere Data Protection appliance and click **Connect**.
3. On the **Getting Started** tab, select **Create Backup Job**.
4. Select the **Guest Images** and click **Next**.
5. Select the **Full Images** and click **Next**.

6 Under the **Inventory Tree**, select vRealize Suite Lifecycle Manager VM to back up, and click **Next**.

7 Set a schedule for the backup job, and click **Next**.

8 Specify a retention policy for the backup job, and click **Next**.

9 Enter a name for the backup job, and click **Next**.

10 Review the summary information for the backup job and click **Finish**.

11 The newly created backup job is listed under the **Backup** tab. The backup runs automatically according to the schedule you configured.

12 (Optional) To run the backup job manually at a later time.

   a On the **Backup** tab, select the **Backup Job**.

   b Click **Backup Now**, and select **Backup all Sources**.

13 (Optional)On the **Reports** tab, select **Job Details** to verify that the backup job was completed.

Restore vRealize Suite Lifecycle Manager Using vSphere Data Protection

You can restore the backed up data for vRealize Suite Lifecycle Manager by using vSphere Data Protection.

Prerequisites

- Deploy and configure the vSphere Data Protection appliance. See the *vSphere Data Protection Administration Guide* for more information.
- Access the vSphere Web Client to log in as an administrator to the vCenter Server instance that manages your environment.
- In the Web Client verify that the virtual machines have the latest VMware Tools installed.

Procedure

1 In the left pane of the vSphere Web Client, select **vSphere Data Protection**.

2 Select the pre-configured **vSphere Data Protection** appliance, and click **Connect**.

3 Click the **Restore** tab.

4 Select the vRealize Suite Lifecycle Manager virtual machine listed.

   All performed backups for this virtual machine are displayed.

5 Select the backup from which you want to restore components.

6 Double-click the backup job, and select the components that you want to restore.

7 Click **Restore** to start the **Restore backup** wizard.

8 On the **Select Backup** page, verify that the backup is correct and click **Next**.

9 On the **Set Restore Options** page, select the **Restore** to original location, and click **Next**.

If you deselect the Restore to original location check box, you can select a different destination for the restore. You might have to specify options such as the host name, network, datastore, and folder.

10 On the **Ready to complete** page, review the summary information for the restore request, and click **Finish**.

11 To verify that the restore operation is successful, power on the virtual machine and check that all vRealize Suite Lifecycle Manager services are running.

Troubleshooting vRealize Suite Lifecycle Manager

9

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 vRLI Clustering and vIDM Registration

  Environment deployment fails during the `Adding vIDM user as vRLI Super Admin` task while running`vRLI Clustering and vIDM Registration`

- Wrong IP details during vRealize Suite Lifecycle Manager Deployment

  You can follow the steps in this section if you have given an incorrect IP address or if you want to upgrade an existing IP address during vRealize Suite Lifecycle Manager.

- Debug vRealize Orchestrator Workflow

  You can encounter errors while working with vRealize Orchestrator workflows.

- Binary Mappings Are Not Populated

  Even if the requests for each product binary are marked as completed, the binary mappings are not populated.

- Fix Errors Using Log Files

  vRealize Suite Lifecycle Manager log files are present under the following locations for trouble shooting any issues.

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 vRLI Clustering and vIDM Registration

Environment deployment fails during the `Adding vIDM user as vRLI Super Admin` task while running`vRLI Clustering and vIDM Registration`

Problem

Even upon retry, 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.

Wrong IP details during vRealize Suite Lifecycle Manager Deployment

You can follow the steps in this section if you have given an incorrect IP address or if you want to upgrade an existing IP address during vRealize Suite Lifecycle Manager.

Problem

Cause

If you have given an Incorrect IP address given 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`

Debug vRealize Orchestrator Workflow

You can encounter errors while working with vRealize Orchestrator workflows.

Problem

To open ports for vRealize Orchestrator workflows.

Solution

1. Enter the following `sed –i '$a\iptables –I INPUT –m state ––state NEW –m tcp –p tcp ––dport 8281 –j ACCEPT' /etc/systemd/scripts/iptables`
2. `sed –i '$a\iptables –I OUTPUT –m state ––state NEW –m tcp –p tcp ––dport 8281 –j ACCEPT' /etc/systemd/scripts/iptables`
3. `sed –i '$a\iptables –I FORWARD –m state ––state NEW –m tcp –p tcp ––dport 8281 –j ACCEPT' /etc/systemd/scripts/iptables`
4. `systemctl restart iptables`

   The default credentials to login in vcoadmin/vcoadmin when the port 8281 is open.

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.

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`.