Abstract

This document provides an overview of the certification workflow for Software Certification partners who want to offer their own applications, management applications or plug-in(driver) software for use with Red Hat OpenStack Platform in a jointly supported customer environment.

Last updated: June 28, 2021.
# Table of Contents

**PART I. MAKING OPEN SOURCE MORE INCLUSIVE** .......................................................... 3

**CHAPTER 1. INTRODUCTION TO RED HAT OPENSTACK CERTIFICATION POLICIES** .................. 4
  1.1. UNDERSTAND RED HAT CERTIFICATION .......................... 4
  1.2. CERTIFICATION WORKFLOW ....................................... 4
  1.3. GET HELP AND GIVE FEEDBACK .................................. 5
  1.4. ADDITIONAL RESOURCES ......................................... 6

**CHAPTER 2. CERTIFICATION PREREQUISITES** ......................................................... 7
  2.1. PROGRAM MEMBERSHIP ........................................... 7
  2.2. PRODUCT REQUIREMENT .......................................... 7

**CHAPTER 3. SETTING UP TEST ENVIRONMENT** ...................................................... 8
  3.1. PREREQUISITES ..................................................... 8
  3.2. PREPARING THE OPENSTACK DEPLOYMENT-UNDER-TEST ....... 9
    3.2.1. Installing software packages required on the OpenStack deployment-under-test or test client 9
  3.3. PREPARING THE TEST SERVER .................................. 10
  3.4. MANUALLY CONFIGURE THE TEST SERVER AND TEST CLIENT PROXY .......................... 12

**CHAPTER 4. CERTIFICATION AND RECERTIFICATION WORKFLOW** ................................. 13
  4.1. CREATING A NEW CERTIFICATION REQUEST ...................... 13
  4.2. RECERTIFICATION WORKFLOW .................................... 13

**CHAPTER 5. RECERTIFICATION OF CUSTOMIZED CONTAINER IMAGES FOR RED HAT OPENSTACK**
**PLATFORM 16 MINOR RELEASE** ................................................................. 15
  5.1. CREATING A NEW OPENSTACK PLUGIN PROJECT ................. 15
  5.2. ATTACHING THE NEWLY CREATED PROJECT TO THE EXISTING CERTIFIED PRODUCT 16
  5.3. FOLLOWING THE CONTAINER CERTIFICATION CHECKLIST .... 17
  5.4. DOCKERFILE REQUIREMENTS ................................... 17
  5.5. SETTING PROJECT DETAILS ...................................... 19
  5.6. BUILDING A CUSTOMIZED CONTAINER IMAGE WITH THE BUILD SERVICE 19
  5.7. UPLOADING A CUSTOMIZED CONTAINER IMAGE .................. 20
  5.8. CORRECTING FAILED SCANNED RESULT ......................... 21
  5.9. PUBLISHING A CONTAINER IMAGE ............................... 21

**CHAPTER 6. CERTIFICATION TESTS FOR OPENSTACK CERTIFICATION** ............................ 22
  6.1. RUNNING CERTIFICATION TESTS FOR PRODUCTS IMPLEMENTING OPENSTACK APIs ........ 22
  6.2. RUNNING OPENSTACK API/TEMPEST TESTS AND SUPPORTABILITY TESTS ................ 22
  6.3. RUNNING TEMPEST_CONFIG TEST .............................. 23
  6.4. RUNNING CERTIFICATION TESTS FOR PRODUCTS CONSUMING OPENSTACK API/S ........ 25
  6.5. RUNNING TRUSTED CONTAINER TEST ............................ 25
  6.6. RUNNING OPENSTACK DIRECTOR TEST AND SUPPORTABILITY TESTS ..................... 26
  6.7. RUNNING CERTIFICATION TESTS USING RED HAT CLI .......... 27
  6.8. ADDITIONAL RESOURCES ....................................... 28

**CHAPTER 7. VIEWING AND SUBMITTING TEST LOGS** ............................................... 29
  7.1. VIEWING AND SUBMITTING TEST LOGS USING WEB UI .......... 29
  7.2. VIEWING AND SUBMITTING THE TEST LOGS USING RED HAT CERTIFICATION CLI .......... 30

**CHAPTER 8. RERUNNING TESTS AND VIEWING CERTIFICATION** .................................... 31
PART I. MAKING OPEN SOURCE MORE INCLUSIVE
Red Hat is committed to replacing problematic language in our code and documentation. We are beginning with these four terms: master, slave, blacklist, and whitelist. Due to the enormity of this endeavor, these changes will be gradually implemented over upcoming releases. For more details on making our language more inclusive, see our CTO Chris Wright’s message.
CHAPTER 1. INTRODUCTION TO RED HAT OPENSTACK CERTIFICATION POLICIES

Use this guide to validate components that implement the OpenStack APIs for networking, block storage, and file share services with Red Hat OpenStack Platform. Also certify applications that rely on OpenStack services or APIs.

1.1. UNDERSTAND RED HAT CERTIFICATION

The Red Hat Certification Program ensures compatibility of Red Hat’s partner’s hardware and software products with Red Hat Enterprise Linux, Red Hat OpenStack Platform, Red Hat Gluster Storage, Red Hat Enterprise Linux for Real Time, and other Red Hat software products. The program has three main elements:

- **Test suite**: Tests for hardware or software undergoing certification.
- **Red Hat Certification Ecosystem**: Explore and find certified products including Hardware, Software, Cloud and service providers.
- **A joint support relationship**: between Red Hat and the vendor whose hardware or software is undergoing certification.

1.2. CERTIFICATION WORKFLOW

As a partner, it is important to understand the workflow, roles and responsibilities during a certification.

**Workflow of the certification program**

1. Create a certification request for a specific software or hardware component using redhat-certification.

2. Run the tests specified in the workflow guide and submit results using redhat-certification to Red Hat for analysis.

3. The certification team analyzes the test results and communicates any required retesting.

4. When all tests have favourable results, the certification is complete and the entry is made visible to the public on the external Red Hat Certification website at [Red Hat Certification Ecosystem](https://www.redhat.com/certification).

**Know your roles and responsibilities**

The following diagram represents the roles and responsibilities of Red Hat and Partners in the certification process.
1.3. GET HELP AND GIVE FEEDBACK

If you experience difficulty with a procedure described in this documentation, Open a Support Case in the Customer Portal.

The Customer Portal offers the following services and information:

- Search or browse through technical support articles and solutions pertaining to Red Hat products
- Submit a support case to Red Hat Global Support Services (GSS)
- Access product documentation

**NOTE**

Personal emails are not tracked as a support mechanism and do not include a Response Time or Service Level Agreement.

Questions During Certification

During the certification process, you may need to ask or reply to a question about topics which affect a specific certification. These questions and responses are recorded in the Additional Comments section of the Dialog Tab of the certification entry.
WARNING

It is not within the scope of the certification workflow to resolve product defects and/or compatibility issues identified during testing. These issues can block a certification and might require resolution before the certification can proceed. Resolving these issues should be accomplished through your Engineering Partner Manager or other engineering engagements.

We Need Feedback!

If you see a way to make this guide better, or if you think of a way to improve the certification workflow, or program, we would love to hear from you! Submit a bug in Bugzilla. Try to be as specific as possible; include the section number and some of the surrounding text.

1.4. ADDITIONAL RESOURCES

- To understand the requirements and policies for Red Hat OpenStack Certification, see Red Hat OpenStack Certification Policy Guide
CHAPTER 2. CERTIFICATION PREREQUISITES

As a partner, you must meet the following prerequisites for certification.

2.1. PROGRAM MEMBERSHIP

1. An active Vendor Single Sign On (SSO) account. The SSO credentials are used to access Red Hat products, certification toolset and other Red Hat assets.

2. A Product profile

3. Completed the Align, Build and Certify (ABC) Workflow on Red Hat Connect for Technology Partners

Additional Resources

- Have questions? Contact the Support team at connect@redhat.com.

2.2. PRODUCT REQUIREMENT

For policy related information, see Red Hat OpenStack Certification Policy Guide
CHAPTER 3. SETTING UP TEST ENVIRONMENT

The following diagram shows the certification packages that need to be installed on each host (color coded).

Figure 3.1. Test Environment Setup

You can launch the Red Hat Certification web user interface on a different host (test server) and use the web user Interface (UI) to run certification tests on an OpenStack deployment-under-test (test client). Using the Red Hat Certification web user interface you can:

- Generate requests for new certifications
- Submit logs
- Conduct discussions with the certification team

3.1. PREREQUISITES

- Red Hat Certification workflow implements a client server application.
● Setup a test server to run OpenStack Certification tests on the system-under-test/test client. This allows:
  ○ Testing of multiple test clients from a single test server
  ○ Quick validation and prevents resource constraints.

3.2. PREPARING THE OPENSTACK DEPLOYMENT-UNDER-TEST

For certifying OpenStack, you must prepare the OpenStack deployment-under-test.

**Prerequisites**

- Install OpenStack Platform
- Install plugin/driver or application that needs to be certified on an Overcloud node.
- Ensure you have a private (tenant) network and private subnet in the OpenStack deployment that is under test.

**Procedure**

1. Create an admin tenant owned router and add the private (tenant) subnet as one of that router’s interfaces in your OpenStack deployment.
2. Create an external (provider) network and a public subnet. Configure the external network as the above router’s gateway in your OpenStack deployment.
3. Run the command using the Keystone command-line client.
   
   $ openstack role create Member

3.2.1. Installing software packages required on the OpenStack deployment-under-test or test client

**NOTE**

The OpenStack deployment-under-test or test client refers to the node where the plugin/application-under-test is installed.

To understand the test environment, see Setting up test environment.

**IMPORTANT**

Complete the following steps on the node where the OpenStack plugin-under-test or application-under-test is installed.

**Procedure**

1. Register your host using Red Hat Subscription Management:
   
   # subscription-manager register
Use your RHN credentials for the registration.

2. Display the list of available subscriptions for your system:

```
# subscription-manager list --available
```

From the list of available subscriptions, search for the subscription which provides the **Red Hat Certification (for RHEL Server)** repository. Make a note of the subscription and its Pool ID.

**IMPORTANT**

The **Red Hat Certification (for RHEL Server)** repository provides the certification packages.

3. Attach the subscription which provides the **Red Hat Certification (for RHEL Server)** repository to your system:

```
# subscription-manager attach --pool=[pool_ID]
```

Replace `[pool_ID]` with the Pool ID of the subscription which provides the **Red Hat Certification (for RHEL Server)** repository.

It is mandatory to use the correct Pool ID with the `# subscription-manager attach --pool` command to attach the required subscription to the system.

**Verification**

To verify the list of subscriptions your system has currently attached, at any time, run the `# subscription-manager list --consumed` command. Ensure that the subscription which provides the Red Hat Certification (for RHEL Server) repository is attached to your system.

4. Subscribe to Red Hat Certification channel:

```
# subscription-manager repos --enable=cert-1-for-rhel-8-x86_64-rpms
```

5. To install the **redhat-certification-openstack** package. This automatically installs the required dependencies:

```
# yum install redhat-certification-openstack
```

6. To start the Red Hat Certification back-end server listener process:

```
# rhcertd start
```

**Result**

The OpenStack deployment-under-test (which refers to the node where the plugin or application-under-test is installed) is now prepared for certification testing.

### 3.3. PREPARING THE TEST SERVER

Install software packages required to ensure automatic installation of required dependencies via CDN.
Prerequisites

- Select a persistent RHEL 7 host that can act as a test server host with the ability to:
  - access Red Hat services including the certification channels
  - use the same network as the OpenStack deployment-under-test (test client).

Procedure

1. To register your host using Red Hat Subscription Management:

   # subscription-manager register

   Use your RHN credentials for the registration.

2. Display the list of available subscriptions for your system:

   # subscription-manager list --available

   From the list of available subscriptions, search for the subscription which provides the Red Hat Certification (for RHEL Server) repository. Make a note of the subscription and its Pool ID.

   **IMPORTANT**

   The Red Hat Certification (for RHEL Server) repository provides the certification packages.

3. Attach the subscription which provides the Red Hat Certification (for RHEL Server) repository to your system:

   # subscription-manager attach --pool=[pool_ID]

   Replace [pool_ID] with the Pool ID of the subscription which provides the Red Hat Certification (for RHEL Server) repository.

   It is mandatory to use the correct Pool ID with the # subscription-manager attach --pool command to attach the required subscription to the system.

   **Verification**

   To verify the list of subscriptions your system has currently attached, at any time, run the # subscription-manager list --consumed command. Ensure that the subscription which provides the Red Hat Certification (for RHEL Server) repository is attached to your system.

4. Subscribe to Red Hat Certification channel:

   #subscription-manager repos --enable=rhel-7-server-cert-rpms

5. To install the redhat-certification package on the host:

   # yum install redhat-certification

6. To start Apache, Red Hat Certification back-end server and the server listener process:
Result

The test server (RHEL 7.x host) is now prepared. The redhat-certification package provides Red Hat Certification web UI which can be used to run certification tests on the OpenStack deployment-under-test/test client.

3.4. MANUALLY CONFIGURE THE TEST SERVER AND TEST CLIENT PROXY

If your network utilizes a proxy, you may need to manually configure the test server and/or test client for the proxy:

Test Server: Update the /etc/rhcert.xml file.

- Syntax

```
<urls>
<proxy-url protocol="http">PROXY_SERVER:PROXY_PORT</proxy-url>
<proxy-url protocol="https">PROXY_SERVER:PROXY_PORT</proxy-url>
</urls>
```

- Example

```
<proxy-url protocol="http">http://rhcert-example.redhat.com:3148</proxy-url>
<proxy-url protocol="https">https://rhcert-example.redhat.com:3148</proxy-url>
```

To open port 80 and port 8009 on test server and test client, run the rhcert-cli register command.

Additional Resources

For more information about proxy settings, see How can we access to the Hardware Certification (rhcertd web interface) via proxy?
CHAPTER 4. CERTIFICATION AND RECERTIFICATION WORKFLOW

You must create a certification request for initial certification and recertification.

4.1. CREATING A NEW CERTIFICATION REQUEST

To create a new certification request, complete the following steps:

Procedure

1. In your test server, launch Red Hat Certification web user interface in a browser using the http://<machine-IP> link.

2. Type your Red Hat account credentials previously enabled for certification in the Username and Password fields. Click Login.

3. Click the Create Certification button. The New Certification webpage displays.

4. Choose the Partner, Make, and Name items from the drop-down list. The Make and Name value gets populated on selecting a Partner. Click Next.

5. Select the Certification, Platform, and Red Hat Product, and RHEL version from the drop-down list, and click Next.

6. Provide the following relevant information in the fields:
   a. In the Component field, select the component that you want to include for certification. The Install Guide field is a mandatory field.

   IMPORTANT
   
   The Director Integration guide can be a text, URL, or a file.

   b. In the Director Integration field, choose Yes or No.

   c. If the Director Integration is selected as Yes, select the type of Director Template, and provide the details in the Director Instructions field.

7. Click Next.

8. This will take you to Create Red Hat OpenStack Platform Certification web page. Select the protocols and features compatible with your plugin. Click Create.

9. A notification of the requested OpenStack certification gets displayed.

   NOTE

   The information which you provide in the Product Name and the Public Catalog URL fields is used by customers in locating the certified product entry (after a successful certification) on Red Hat OpenStack Certification Ecosystem Page.

4.2. RECERTIFICATION WORKFLOW
Understand the procedure and policies involved in recertifying Red Hat OpenStack.

**IMPORTANT**

It is mandatory to create a new certification request for recertification.

1. See [Creating a new certification](#).

2. Run the certification tests and proceed with the rest of the workflow as documented.

**Additional Resources**

- For more information about recertification requirements and policies, see [Red Hat OpenStack Certification Policy Guide](#).
CHAPTER 5. RECERTIFICATION OF CUSTOMIZED CONTAINER IMAGES FOR RED HAT OPENSTACK PLATFORM 16 MINOR RELEASE

Partners who provide their customized container images must recertify the container images for each minor release of the Red Hat OpenStack Platform. For example, if you have certified your plugin for 16.0 or 16.1 and provide a customized container image, you must recertify your container image for 16.2.

For each minor version of RHOSP, you must rebuild the customized container images via a separate OpenStack plugin project. Red Hat OpenStack minor releases are shipped with a different RHEL minor release. Ensure that your existing product is certified with RHOSP 16.

Additional resources

For more information on when a customized container image is required, see Red Hat OpenStack Certification - Red Hat Partner Connect General Guide.

5.1. CREATING A NEW OPENSTACK PLUGIN PROJECT

To rebuild the customized container images, you need to create a separate project. One project represents one partner image. If you have multiple images, you must create multiple projects.

Procedure

1. Log in to Red Hat Connect for Technology Partners and click Zones & Resources.

2. Select Red Hat OpenStack & NFV zone.

3. Click Certify to access the existing products and projects of your company.
4. Click **Add Project** to create a new project.

5. Set **Project Name**.
   - The project name is not visible outside the system.
   - For Red Hat OpenStack Platform (RHOSP), the project name must be defined in the following format: `[product][Major version].[Minor version]-[extended-base-container-image]-[your-plugin].`

6. Set **Release Category** to **Tech Preview**.

   **NOTE**
   You will not see the Generally Available option until you have completed API testing with Red Hat Certification.

7. Select **Red Hat Product** and **Red Hat Product Version** based on the base image that you want to modify with your plugin. For this release, select **Red Hat OpenStack Platform** and **16**.

8. Click **Submit** to create the new project.

**Result**
Red Hat assesses and confirms the certification of your project.

**5.2. ATTACHING THE NEWLY CREATED PROJECT TO THE EXISTING CERTIFIED PRODUCT**

You can attach the newly approved project with your existing corresponding certified product.

**Procedure**

1. On the **Red Hat Connect for Technology Partners** page, select **Product Certification**.
2. Click **Manage Products** and select the product your project must be associated with.

3. Select **Certification Projects**. A list of available projects displays, including the one created in **Creating a new OpenStack Plugin Project** section.

4. Select the check box beside the newly created project and click **Attach Project**.

5.3. FOLLOWING THE CONTAINER CERTIFICATION CHECKLIST

Certified containers must meet Red Hat standards for packaging, distribution, and maintenance. Containers certified by Red Hat have a high level of trust and supportability from container-capable platforms, including the Red Hat OpenStack Platform (RHOSP). To maintain this, you must keep your images up-to-date.

**Procedure**

1. On the **Red Hat Connect for Technology Partners** page, select **Product Certification**.

2. Click **Manage Projects** and select the project created in **Creating a new OpenStack Plugin Project** section.

3. Click **Overview**. The certification checklist displays.

4. Complete all sections of the checklist. If you need more information about an item, click the drop-down arrow on the left to view the item information and links to other resources.

The checklist includes the following items:

- **Submit your container for verification**
  Set up the build service and test your images using our inbound testing registry.

- **Complete export control questionnaire**
  Our legal team must ensure that export compliance standards have been met. Approval takes 2-3 weeks.

- **Accept the Red Hat OpenStack Appendix**
  Additional terms must be agreed to certify and publish your containerized application.

- **Provide details about your container**
  The details are displayed in the Ecosystem Catalog, along with the instructions on how to pull the container image.

- **Complete your company profile**
  Ensure that your company profile is ready to be published in the Catalog.

**Additional resources**

For more information on Export Compliances, see **Export Compliance**.

5.4. DOCKERFILE REQUIREMENTS

As a part of the image build process, the build service scans your built image to ensure that it complies with Red Hat standards. Use the following guidelines as a basis for the dockerfile to include with your project:
The base image must be a Red Hat image. Any images that use Ubuntu, Debian, and CentOS as a base do not pass the scanner.

You must configure the required labels:

- name
- maintainer
- vendor
- version
- release
- summary

You must include the software license as a text file within the image. Add the software license to the licenses directory at the root of your project.

You must configure a user that is not the root user.

The following dockerfile example demonstrates the required information for the scan:

```
FROM registry.redhat.io/rhosp-rhel8/openstack-cinder-volume
MAINTAINER VenderX Systems Engineering <maintainer@vendorX.com>

### Required Labels
LABEL name="rhosp-rhel8/openstack-cinder-volume-vendorx-plugin" \\ 
    maintainer="maintainer@vendorX.com" \\ 
    vendor="VendorX" \\ 
    version="3.7" \\ 
    release="1" \\ 
    summary="Red Hat OpenStack Platform 16.1 cinder-volume VendorX PluginY" \\ 
    description="Red Hat OpenStack Platform 16.1 cinder-volume VendorX PluginY"

USER root

### Adding package
### repo example
COPY vendorX.repo /etc/yum.repos.d/vendorX.repo

### Adding package with curl
RUN curl -L -o /verdorX-plugin.rpm http://vendorX.com/vendorX-plugin.rpm

### Adding local package
COPY verdorX-plugin.rpm /

# Enable a repo to install a package
RUN dnf clean all
RUN yum-config-manager --enable openstack-16.1-for-rhel-8-x86_64-rpms
RUN dnf install -y vendorX-plugin
RUN yum-config-manager --disable openstack-16.1-for-rhel-8-x86_64-rpms

# Add required license as text file in Licenses directory (GPL, MIT, APACHE, Partner End User Agreement, etc)
```
5.5. SETTING PROJECT DETAILS

You must set details for your project, including the namespace and registry for your container image.

Procedure

2. Click Manage Projects and select the project created in Creating a new OpenStack Plugin Project section.
3. Click Settings.
4. Ensure that your project name is in the correct format.
5. [Optional] Check Auto-Publish if you want to automatically publish containers that pass certification. Certified containers get published in the Red Hat Container Catalog.
6. To set the Container Registry Namespace, follow the online instructions.
   - The container registry namespace is the name of your company.
   - The final registry URL is registry.connect.redhat.com/namespace/repository:tag.
7. To set the Outbound Repository Name, follow the online instructions. The outbound repository name must be the same as the project name.
   - For Red Hat OpenStack Platform (RHOSP), the project name must be defined in the following format: [product][version]-[extended_base_container_image]-[your_plugin].
   - The final registry URL is registry.connect.redhat.com/namespace/repository:tag.
8. Add additional information about your project in the relevant fields:
   - Repository Description
     You can view the repository description on the container catalog repository overview page.
9. Click Submit.

5.6. BUILDING A CUSTOMIZED CONTAINER IMAGE WITH THE BUILD SERVICE

Use the Red Hat provided Build Service to build your customized container image.
Procedure

1. On the Red Hat Connect for Technology Partners page, select **Product Certification**.

2. Click **Manage Projects** and select the project created in **Creating a new OpenStack Plugin Project** section.

3. Click **Configure Build Service** to configure your build details.
   - Ensure that the **Red Hat Container Build** is set to **ON**.
   - Add your **Git Source URL** and optionally add your **Source Code SSH Key** if your git repository is protected. The URL can be HTML or SSH. SSH is required for protected git repositories.
   - [Optional] Add **Dockerfile Name** or leave blank if your Dockerfile name is **Dockerfile**.
   - [Optional] Add the **Context Directory** if the docker build context root is not the root of the git repository. Otherwise, leave this field blank.
   - Set the **Branch** in your git repository to base the container image on.
   - Click **Submit** to finalize the **Build Service** settings.

4. Click **Start Build**.

5. Add **Tag Name** and click **Submit**. It can take up to six minutes for the build to complete.
   - The tag name must be a version of your plugin.
   - The final reference URL is `registry.connect.redhat.com/namespace/repository:tag`.

6. Click **Refresh** to check that your build is complete. [Optional] Click the matching **Build ID** to view the build details and logs.

7. The build service builds and scans the image. It takes 10-15 minutes to complete. When the scan completes, click the corresponding link under **Certification test** to expand the scan results.

5.7. UPLOADING A CUSTOMIZED CONTAINER IMAGE

Upload your pre-built customized container image if you decide not to use the Red Hat provided Build Service.

Procedure

1. On the Red Hat Connect for Technology Partners page, select **Product Certification**.

2. Click **Manage Projects** and select the project created in **Creating a new OpenStack Plugin Project** section.

3. Select **Images**, click **Push Images Manually**.

4. Follow the instructions appearing on the screen to upload your customized container image.
5. Upon upload, the build service scans your customized container image. It takes 10-15 minutes to complete. When the scan completes, click the corresponding link under Certification test to expand the scan results.

5.8. CORRECTING FAILED SCANNED RESULT

The Scan Details page displays the results of the scan, including any failed items. If your image scan reports a FAILED status, use the following procedure to investigate how to correct the failure.

Procedure

2. Click Manage Projects and select the project created in Creating a new OpenStack Plugin Project section.
3. Select Images, click the corresponding Certification Test result to expand the scan results.
4. Expand the failed items to view more information about how to correct the issues.

NOTE

If you receive an Access Denied warning when you access the Policy Guide, please open a support case at Red Hat Technology Partner Success Desk with Category “Product Certification” and Product “Red Hat OpenStack Platform”.

5.9. PUBLISHING A CONTAINER IMAGE

After the container image passes the scan, you can publish the container image.

Procedure

2. Click Manage Projects and select the project created in Creating a new OpenStack Plugin Project section.
3. Select Images and expand the corresponding container image. Click the Publish link.
4. The Publish link changes to Unpublish. To unpublish a container, click the Unpublish link.

Additional Resources

After you publish the link, check the certification documentation to certify the plugin. Certification documentation links are available in Partner integration prerequisites.
CHAPTER 6. CERTIFICATION TESTS FOR OPENSTACK CERTIFICATION

Run certification tests on the OpenStack deployment-under-test based on the type of OpenStack application undergoing certification.

6.1. RUNNING CERTIFICATION TESTS FOR PRODUCTS IMPLEMENTING OPENSTACK APIs

If the OpenStack application undergoing certification implements OpenStack APIs, complete the following steps on the test server to run certification tests on the OpenStack deployment-under-test or test client.

**NOTE**
This category includes OpenStack plugins/drivers which implement OpenStack APIs for Networking, Block Storage, and File Share services.

Additional resources

- For more information about products implementing OpenStack APIs, see [Red Hat OpenStack Certification Policy Guide](#).

6.2. RUNNING OPENSTACK API/TEMPEST TESTS AND SUPPORTABILITY TESTS

Procedure

1. In your test server launch Red Hat certification web UI in a browser using the http://machine-ip link.
2. Specify Red Hat account credentials enabled for certification in the Username and Password fields. Click Login.
4. In the Register a System field, type the hostname or IP address of the Overcloud node where the plugin-under-test/driver-under-test is installed and then click Add.
5. Click the existing product entry from Red Hat Certification Home Page and then the relevant certification entry from the Certifications Page.

**Figure 6.1. Available Certification Test**

| 2838903 | Abbee cloud-19-oct-web2 |

[+ Product]
6. In the Testing Page, click **Select Test Systems**.

7. In the Select Host Page, the Partner decides which host will run the test from the selected roles. From the drop-down list, choose the role for a host as **controller** or **compute**.

8. Click **Test**

   **NOTE**
   The test generated for Controller node depends on the features that the Partner plugin supports. Tests for Compute node include supportable, sosreport, self_check, and director.

9. Click **Start Test Run** The mandatory tests will get executed, however, you can check or uncheck the optional tests. The test run executes at the same time for Controller and Compute nodes.

10. Click on the generated test results, this will take you to the Progress tab. Click on the **Submit Result**. The Red Hat certification team verifies the test results.

   **NOTE**
   Currently, multi-host testing does not support Sandboxing and CLI. Testing can be performed only through WebUI.

**Additional Resources**

- For more information about registering a system, see [Registering a System using Redhat-Certification](#).

### 6.3. RUNNING TEMPEST_CONFIG TEST

This test checks the generation of tempest_config based on the lab environment details.

**PROCEDURE**

If the system under test is subscribed to OpenStack product repositories the tempest will be installed. If the product repositories are not installed you will get a failure notification that the tempest cannot be installed.

Being an interactive test it asks for the following details:
• In the **keystone auth url** field, type the Keystone authentication URL that allows access to service endpoints.

**Figure 6.2. Keystone Authentication URL**

```
Testing:

Please input your keystone auth url (eg: http://your_openstack:5000/v2.0):

http://10.65.207.207:5000/v2.0

Submit
gerestart
```

• In the **OpenStack admin username** field, type the OpenStack username of a user with the admin role.

• In the **OpenStack admin password** field, type the corresponding OpenStack password of the user with the admin role.

• Modify the **Edit tempest.conf** field if required and then click **Submit**.

**Figure 6.3. Edit Tempest.conf**

```
Testing:

Edit tempest.conf

[DEFAULT]
dump = true
use_stderr = false
log_file = tempest.log

[auth]
tempest_roles = _member_

[compute]
image_ssh_user = cirros
flavor_ref = 25820baa-1f5b-4a35-a9f0-cb5e02e92fb5
flavor_ref_alt = 6165da6a-88a1-4cf2-92a8-8a6fc817ad9c
image_ref = f10dd792-db60-4bf6-b07e-2af3e304f681
image_ref_alt = 7335f807-8764-4cc8-af1b-21485f36476a
```

The tempest_config test automatically generates a tempest.conf file during run-time. If you need to alter this configuration, place a full tempest.conf into the /etc/redhat-certification-openstack directory that will override the automatic configuration. The configuration override
can assist in addressing tempest issues but it does not change the certification testing requirements to be satisfied by tempest.

**NOTE**

While it is not explicitly required that tempest automatically corrects configuration of the testing environment for your product it is suggested that you open a bug with the **upstream tempest project**, against the **RHOSP Tempest component**, or the **Red Hat Certification Component**. The RHOS Tempest component link can be used to file the downstream bugs on bugzilla. Incase of the tempest issue, in the **Component** field select **openstack-tempest** from the drop-down list. If there is a bug in the component you can select the related component like, openstack-neutron, openstack-cinder or openstack-manila. This process will help you to avoid the repeated correction of configuration.

### 6.4. RUNNING CERTIFICATION TESTS FOR PRODUCTS CONSUMING OPENSTACK APIs

#### Procedure

If the OpenStack application undergoing certification consume Openstack APIs, see **Red Hat OpenStack Certification Policy Guide**, and perform the steps documented in the **Preparing the test server** on the test server to run certification tests on the OpenStack deployment-under-test.

**NOTE**

This category includes products which generally facilitate an OpenStack deployment or complement the Cloud Infrastructure with additional functionalities such as configuration, scaling and management. OpenStack management applications, monitoring applications and OpenStack-enabled applications such as virtual network functions fall in this category.

### 6.5. RUNNING TRUSTED CONTAINER TEST

#### Procedure

1. Select the trusted container test.

   **Figure 6.4. Trusted Container test in web UI**

   ![Trusted Container test in web UI]

2. Click on the Run Selected button.

3. As this session is interactive, during execution it will prompt to provide the following information:
a. Reason for non Red Hat containers found on System-under-test
b. Select the checkboxes for the containers for which test needs to be performed.

6.6. RUNNING OPENSTACK DIRECTOR TEST AND SUPPORTABILITY TESTS

Procedure

1. On Red Hat Certification Home Page, click the Server settings tab.
   
   **Figure 6.5. Server Settings**
   
   ![](server-settings.png)

2. In the Register a System field, type the hostname or IP address of the Overcloud node where the application-under-test is installed and then click Add.

3. Click the existing product entry from Red Hat Certification Home Page and then click the relevant certification entry from the Certifications Page.

   **Figure 6.6. Available Certification Test**

<table>
<thead>
<tr>
<th>2838903</th>
<th>Abbee cloud-19-oct-web2</th>
</tr>
</thead>
</table>

The Progress Page opens and displays the certification tests available in the certification test suite and the progress of the previous runs (if any).

4. Click the Testing link to open the Testing Page.

5. In the Testing Page, click System.

6. In the Select Host Page, select the host/hostname of the Overcloud node where the application-under-test is configured and then click Test.

   The Testing Page opens and a certification test plan is created for the application-under-test.

   After the certification test plan run is complete and the test plan is ready, the status column displays a "Finished test run" status and a Continue Testing button.

   **Figure 6.7. Continue Testing**

   ![Continue Testing](continue-testing.png)
7. Click **Continue Testing**.

8. Select **interactive** next to the **openstack/supportable** checkbox and then click **Run Selected**.

**Figure 6.8. Run Supportable Tests**

<table>
<thead>
<tr>
<th>Run:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>rhcert/self_check</td>
<td></td>
</tr>
<tr>
<td>openstack/supportable</td>
<td></td>
</tr>
</tbody>
</table>

**Result**

Certification tests are run on the application-under-test. The status of the certification test run is displayed on the Testing Page under the relevant hostname.

**Figure 6.9. Test Run Status**

After the test run completes, the test logs from the **openstack/supportable** tests are stored in the same log file as for the **openstack/director** test on the test server. See [View and submit test logs using web UI](#) in the guide to submit the test logs.

### 6.7. RUNNING CERTIFICATION TESTS USING RED HAT CLI

**NOTE**

Tests to be run depends on the type of driver/plugin, and features implemented by the driver/plugin.

```
#rhcert-cli run --test supportable --test tempest_config --test cinder_volumes --test cinder_consistency_groups
```

The below tests are the mandatory tests for a plugin/driver for cinder that has volumes and consistency_group features implemented.

**Procedure**

1. To run the certification tests using Red Hat Certification CLI (rhcert-cli), execute the following commands on the **System Under Test (SUT)**:

```
#rhcert-cli clean
#rhcert-cli plan
#rhcert-cli run --test cinder_volumes
```
NOTE

Tests to be run depends on the type of driver/plugin, and features implemented by the driver/plugin.

#rhcert-cli run --test supportable --test tempest_config --test cinder_volumes --test cinder_consistency_groups

The above tests are the mandatory tests for a plugin/driver for cinder that has volumes and consistency_group features implemented.

All component-based tests in openstack are tagged, which means the following commands will run all the tests for cinder, manila or neutron, respectively:

```bash
# rhcert-cli run --tag cinder
# rhcert-cli run --tag manila
# rhcert-cli run --tag neutron
```

1. After the tests run, the test logs or results are automatically collected in a single .xml.gz file. To save the test logs or results, run the following command on the image-under-test.

```bash
# rhcert-cli save --server [hostname/IP address of LTS]
```

NOTE

In the above command LTS stands for Linux Test Server.

You can submit the test results or logs for validation without saving them on the image-under-test.

6.8. ADDITIONAL RESOURCES

- For more information about certification targets, see Red Hat OpenStack Certification Policy Guide.
CHAPTER 7. VIEWING AND SUBMITTING TEST LOGS

You can view and submit your test logs for review using the Red Hat certification web user interface (UI) or using the command line interface (CLI).

7.1. VIEWING AND SUBMITTING TEST LOGS USING WEB UI

The test runs generate two log files based on the type of product undergoing certification. The log files generated are as follows:

- For Products Implementing OpenStack APIs: A consolidated log file for OpenStack API/Tempest and the OpenStack Supportability tests
- For Products Consuming OpenStack APIs: A single log file for OpenStack Supportability tests

**IMPORTANT**

It is mandatory to submit the log files generated based on your product type to Red Hat Certification services for review.

**NOTE**

Test logs are also generated for every test type and may be viewed on Red Hat Certification application. However, it is mandatory to submit the consolidated log file for review using the procedure covered below.

Procedure

1. Launch Red Hat Certification web UI on the test server.
2. On Red Hat Certification Home Page, from the Products Table, click the name of the product/image-under-test.
3. From the Certification Page, click the relevant certification entry.
4. Click the Testing link to open the Testing Page.
5. In the Testing Page, click the results timestamp under the hostname of the Undercloud node on which you run the OpenStack Director test (openstack/director).
6. Results Timestamp Director

   ![Run timestamp](2016-10-30 04:07:30)

7. From the Actions list, select an appropriate action based on the following details:
8. Result Actions
To submit the test log file for review, select submit. To close the test log file, select close. The submit action is mandatory to submit the test log file for review.

To save the test log file on a different Red Hat Certification server, select save. The save action transfers the test log file (in .xml.gz format) to a remote server which has Red Hat Certification application installed. If you save the test log file on a different Red Hat Certification server, you must submit the log file from the same server.

To download the test log file (in .xml.gz format), select download.

To delete the test log file from the server, select delete.

9. In the Testing Page, click the results timestamp under the hostname of the Overcloud node on which you run OpenStack API/Tempest tests (if applicable) and OpenStack Supportability tests.

10. Results Timestamp Others

   2016-10-30 01:31:34

11. Repeat step 6 and submit the test logs generated from the OpenStack API/Tempest tests (if applicable) and OpenStack Supportability and Director tests for review.

7.2. VIEWING AND SUBMITTING THE TEST LOGS USING RED HAT CERTIFICATION CLI

Procedure

1. To submit the test logs using Red Hat Certification CLI, run the following command on the image-under-test.

   ```bash
   # rhcert-cli submit
   ```

   1. Specify your Red Hat account credentials previously enabled for certification in the Red Hat Catalog Username and Password. The Certification ID is generated when you successfully create a certification request. Type the ID of the certification request in the Certification ID dialog box.

   The # rhcert-cli submit command works only if the image has a network that can connect to the Red Hat services. The command submits the latest timestamped test logs on your host/image to Red Hat certification services for review. The test log file is reviewed by Red Hat certification services and Red Hat Review team. The certification results are displayed on Red Hat Certification web user interface.

   If the image-under-test does not have internet access, save the test logs on the image-under-test using the # rhcert-cli save --server [hostname/IP address of LTS] command.
CHAPTER 8. RERUNNING TESTS AND VIEWING CERTIFICATION

Red Hat Certification Services and the Review Team validates the test log file submitted after a certification test is run. The review team may get in touch with you using the Dialog tab on Red Hat Certification web user interface to confirm specific results and obtain more information.

Rerun certification tests

In some instances, there may be a need to rerun some tests. You can submit the logs from the rerun using the existing certification request.

View certification results

The final certification results are displayed on the Red Hat Certification web user interface. On successful certification, the certified product is listed on Red Hat OpenStack Certification Ecosystem Page.