



Red Hat Hardware Certification 2024

Red Hat OpenStack Platform Hardware Bare Metal Certification Policy Guide

For Use with Red Hat OpenShift Container Platform 4 and Red Hat OpenStack Platform 17

Red Hat Hardware Certification 2024 Red Hat OpenStack Platform Hardware Bare Metal Certification Policy Guide

For Use with Red Hat OpenShift Container Platform 4 and Red Hat OpenStack Platform 17

Legal Notice

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

The Red Hat OpenStack Platform Hardware (Bare Metal) Certification Policy Guide covers the procedural, technical and policy requirements for achieving a Red Hat Hardware Certification. Version 8.78 updated April 16, 2024.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	4
CHAPTER 1. INTRODUCTION TO RED HAT OPENSTACK AND RED HAT OPENSIFT CONTAINER PLATFORM BARE METAL HARDWARE CERTIFICATION POLICIES	5
1.1. AUDIENCE	5
1.2. CREATING VALUE FOR OUR JOINT CUSTOMERS	5
CHAPTER 2. PREREQUISITES	6
2.1. PARTNER ELIGIBILITY CRITERIA	6
2.2. CERTIFICATION TARGETS	6
2.2.1. Server	6
2.2.2. Red Hat Cloud Platform Products	6
2.2.3. Baseboard management controllers (BMC)	7
2.2.4. Bare Metal Drivers	8
CHAPTER 3. OVERVIEW OF BARE METAL CERTIFICATION	9
3.1. PUBLICATION IN THE CATALOG	9
3.2. RED HAT PRODUCT RELEASES	9
3.3. CERTIFICATION DURATION	9
3.4. RECERTIFICATION WORKFLOW	9
CHAPTER 4. CERTIFICATION TESTING	10
4.1. PREREQUISITES FOR CERTIFICATION TESTING	10
4.2. CERTIFICATION WORKFLOW	10
4.3. CERTIFICATION REQUIREMENTS	12
CHAPTER 5. LEVERAGING CERTIFICATION	14
CHAPTER 6. PASS-THROUGH CERTIFICATION	15
CHAPTER 7. SUPPLEMENTAL CERTIFICATION	16
CHAPTER 8. RED HAT OPENSTACK PLATFORM BARE METAL HARDWARE CERTIFICATION	17
CHAPTER 9. IPI CERTIFICATION TESTS	18
9.1. SELF CHECK TEST	18
9.2. SUPPORTABLE TEST	18
9.2.1. Kernel subtest	18
9.2.2. Kernel modules subtest	19
9.2.3. Hardware Health subtest	19
9.2.4. Installed RPMs subtest	20
9.2.5. System report subtest	20
9.2.6. SELinux subtest	21
9.3. DIRECTOR_UNDERCLOUD TEST	21
9.4. BARE METAL TEST	21
9.4.1. Bare Metal InstackStackrc validation	22
9.4.2. Bare Metal driver validation	22
9.4.3. Bare Metal undercloud validation	22
9.4.4. Bare Metal enrolling test	22
9.4.5. Bare Metal inspecting test	23
9.4.6. Bare Metal deploying test	23
9.4.7. Bare Metal redeploying test	23
CHAPTER 10. RED HAT OPENSIFT CONTAINER PLATFORM BARE METAL HARDWARE CERTIFICATION

	24
CHAPTER 11. IPI CERTIFICATION TESTS	25
11.1. SELF CHECK TEST	25
11.2. IPI TEST	25
11.2.1. Check and update power state subtest	25
CHAPTER 12. ASSISTED INSTALLER CERTIFICATION TESTS	26
12.1. SELF CHECK TEST	26
12.2. ASSISTED INSTALLER TEST	26
12.3. SOSREPORT TEST	26
12.4. CLUSTER INSPECTION TEST	27

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 AND RED HAT OPENSIFT CONTAINER PLATFORM BARE METAL HARDWARE CERTIFICATION POLICIES

The Red Hat OpenStack Platform and Red Hat OpenShift Container Platform bare-metal hardware certification policy guide is intended for hardware vendors who want to certify their bare-metal servers with Red Hat.

The RHOSP bare-metal certification tests installer-provisioner infrastructure (IPI) functionality, which ensures that your servers can be automatically orchestrated without manual intervention.

The RHOCP bare-metal certification is divided in the following components:

- The IPI component, which ensures that your servers can be automatically orchestrated without manual intervention.
- The Assisted installer component, which ensures that customers can install your servers with the assisted installer for RHOCP.

You can certify your servers for the IPI component in both platforms and also for both components of the RHOCP bare-metal certification if the servers meet the requirements.

1.1. AUDIENCE

This guide is intended for Partners who offer their own infrastructure hardware like system servers, or management controllers for use with Red Hat OpenStack Platform or Red Hat OpenShift Container Platform in a supported customer environment.

1.2. CREATING VALUE FOR OUR JOINT CUSTOMERS

Red Hat OpenStack Platform and Red Hat OpenShift Container Platform bare metal hardware certifications create value for customers, because the systems can be managed and automatically deployed and redeployed with Red Hat OpenStack bare metal hardware or Red Hat OpenShift Container Platform bare metal hardware, without manual intervention.

The certification process, through a series of tests, validates that a certified solution meets the requirements of an enterprise cloud, and is jointly supported by Red Hat and your organization.

The Red Hat OpenStack Platform and Red Hat OpenShift Container Platform bare metal hardware certification program policies includes multiple tests each with a series of subtests and checks, which are explained in the document.

CHAPTER 2. PREREQUISITES

A strong working knowledge of Red Hat Enterprise Linux and Red Hat OpenStack or Red Hat OpenShift Platform is required. A [Red Hat Certified Engineer](#) and a [Red Hat OpenStack Platform Certified Engineer](#) or [Red Hat Certified Specialist in OpenShift Administration](#) accreditation is preferred and suggested before participating.

2.1. PARTNER ELIGIBILITY CRITERIA

You must meet the following requirements before applying for a bare-metal certification:

- You are part of the [Red Hat Hardware Certification program](#).
- You are in a support relationship with Red Hat by means of the TSANet network or a custom support agreement.

2.2. CERTIFICATION TARGETS

The certification targets provide details and requirements about the components and products relevant to the certification.

Specific information for each of the certification components is provided when applicable.

2.2.1. Server

IPI component certification

- The server must have earned the following certifications:
 - Red Hat Enterprise Linux System
 - Red Hat OpenStack Platform Compute Node OR Red Hat OpenShift Container Platform, depending on the platform that you are certifying.
Each certification is keyed to the respective Cloud Platform product version and its associated ironic revision. You can certify your server for either RHOSP or RHOCP, or for both if your hardware is compatible with the ironic drivers for that platform.
- The server must have a baseboard management controller (BMC) installed.

Assisted installer component certification

- The server must have earned the following certifications:
 - Red Hat Enterprise Linux System
 - Red Hat OpenShift Container Platform
- The server must be bare-metal. VMs are not supported.

2.2.2. Red Hat Cloud Platform Products

IPI component certification

You can certify BMC and bare-metal servers for the following versions of Red Hat products:

- Red Hat OpenStack Platform 17.1
- Red Hat OpenShift Container Platform 4.12, 4.13, 4.14, or 4.15

Table 2.1. Supported RHOCP version and architecture for IPI

RHOCP version	Architecture
RHOCP 4.12	<ul style="list-style-type: none"> ○ 64-bit AMD and Intel ○ 64-bit ARM
RHOCP 4.13-4.x	<ul style="list-style-type: none"> ○ 64-bit AMD and Intel ○ 64-bit ARM

Assisted Installer component certification

You can certify bare-metal servers for the following versions of Red Hat products:

- Red Hat OpenShift Container Platform 4.13, 4.14, or 4.15 and RHEL 9.2 or 9.4

Table 2.2. Supported RHOCP version and architecture for AI

RHOCP version	Architecture
RHOCP 4.13-4.x	<ul style="list-style-type: none"> ○ 64-bit AMD and Intel ○ 64-bit IBM Z ○ 64-bit ARM ○ Little endian IBM Power systems

Additional resources

- [Supported RHOCP versions and their corresponding RHEL versions](#)

2.2.3. Baseboard management controllers (BMC)

IPI component certification

A BMC is a specialized microcontroller embedded or installed on the motherboard of a server which administers the interface between systems management software and physical hardware platforms. The bare metal service in the Red Hat Platforms provisions systems for use in a cluster by utilizing the BMC in a server, to control power, network booting, and automating the deployment of a node as well as terminating those nodes when they become unnecessary.

BMC can be certified as a component for use in [leveraging](#), across server systems where the same BMC can be utilized in multiple systems. Similar to leveraging components in the Red Hat Hardware Certification programs, having tested the interaction between the BMC and the Red Hat software,

Red Hat is leveraging the partner's internal quality analysis testing, to provide a more efficient certification process without introducing risk to customer environments. So, partners utilizing leveraging in bare metal certifications with their BMCs and server systems are recommended to conduct their own testing with the specific server system, the specific BMC, and the specific Red Hat Cloud Platform product to validate the specific combination. But you need not submit individual certification results to Red Hat for every combination.

2.2.4. Bare Metal Drivers

IPI component certification

BMCs must use supported ironic drivers provided in the corresponding Red Hat Cloud Platform product. You cannot certify a BMC that requires an ironic driver that is not included in the Red Hat product.

- [Red Hat OpenStack Platform Bare Metal Drivers](#)
- [Red Hat OpenShift Deploying on Bare Metal](#)

CHAPTER 3. OVERVIEW OF BARE METAL CERTIFICATION

The bare-metal certification overview provides details about product publication in the catalog, product release, certification duration, and recertification.

3.1. PUBLICATION IN THE CATALOG

When you certify your server for bare metal on Red Hat OpenStack Platform, it is published in the Red Hat Ecosystem Catalog as **Bare Metal**. The Bare Metal Management feature also appears as a certified component of your server.

When you certify your server for bare metal on Red Hat OpenShift Container Platform, the following features might appear as certified component of your server depending on the certification tests the server passed:

- **Installer Provisioned Infrastructure**
- **Assisted Installer Service**

Names may differ corresponding to the language of the products.

3.2. RED HAT PRODUCT RELEASES

You may have access to, and are encouraged to test with, pre released Red Hat software. You may begin your engagement with the Red Hat Certification team before Red Hat software is generally available (GA) to customers, to expedite the certification process for your product. However, official certification testing must be conducted on the generally available (GA) releases of Red Hat OpenStack Platform bare metal hardware or Red Hat OpenShift Container Platform bare metal hardware.

3.3. CERTIFICATION DURATION

Certifications are valid starting with the specific major and minor releases of Red Hat OpenStack Platform or Red Hat OpenShift Container Platform software as tested and listed in the Red Hat Ecosystem Catalog. They continue to be valid through the last minor release of the major release. This allows customers to count on certifications from the moment they are listed until the end of the lifecycle of the products.

3.4. RECERTIFICATION WORKFLOW

You do not need to recertify after a new major or minor release of RHOCP or RHOSP if you have not made changes to your product. However, it is your responsibility to certify your product again any time you make significant changes to it.

Red Hat recommends that you run the certification tests on your product periodically to ensure its quality, functionality, and performance with the supported versions of RHOCP or RHOSP.

To recertify your product, open a supplemental certification.

CHAPTER 4. CERTIFICATION TESTING

The certification testing educates Partners about the prerequisites for testing, understanding the certification process, and its requirements.

4.1. PREREQUISITES FOR CERTIFICATION TESTING

IPI component certification

- The corresponding RHEL server certification is successfully completed and posted.
- The corresponding Red Hat OpenStack Platform Compute Node certification or Red Hat OpenShift Container Platform certification is successfully completed and posted.
- The corresponding bare-metal driver is on the Supported Drivers List for the corresponding Red Hat OpenStack Platform or Red Hat OpenShift Container Platform release.

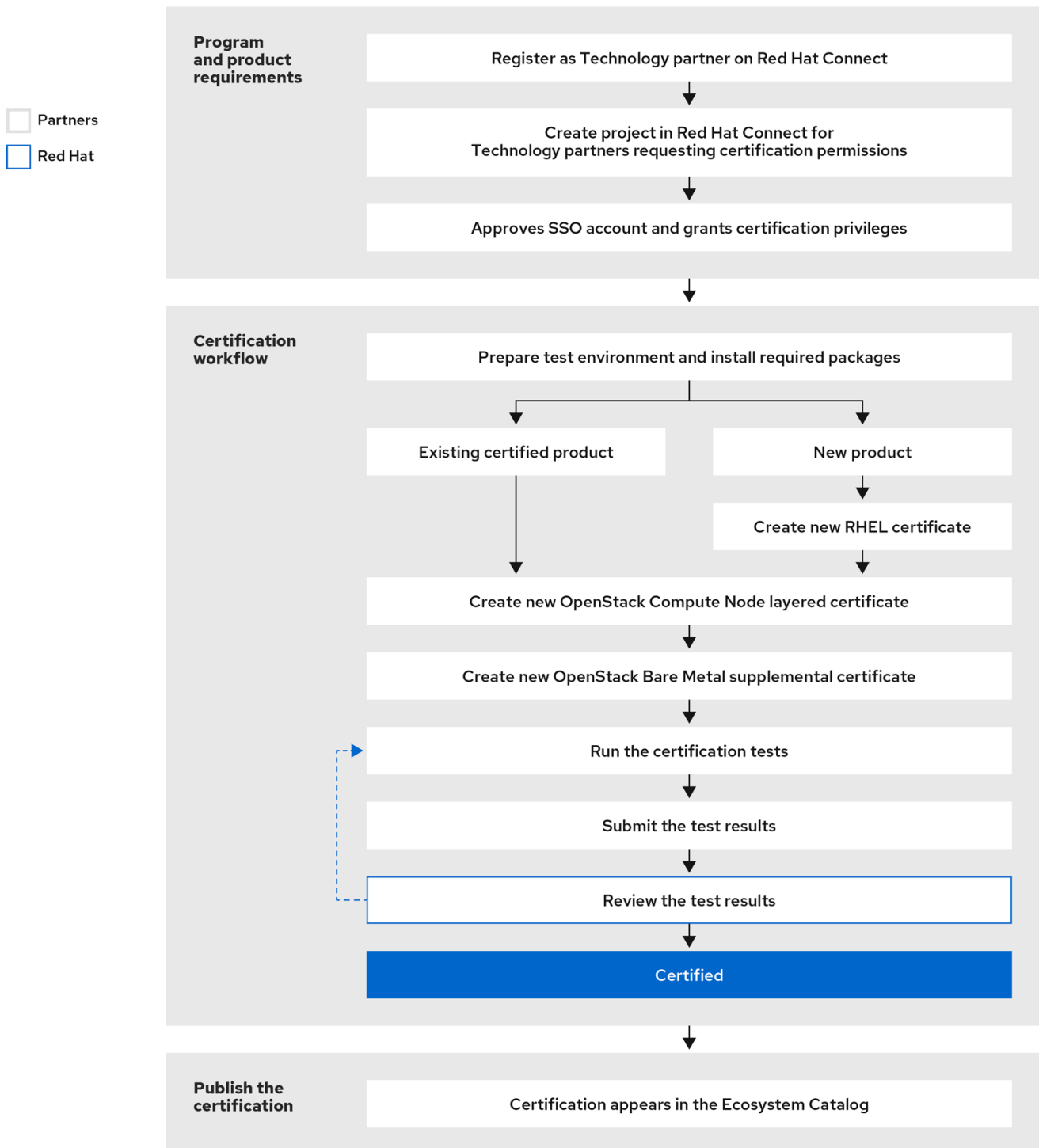
Assisted installer component certification

- The corresponding RHEL server certification is successfully completed and posted.
- The corresponding Red Hat OpenStack Platform Compute Node certification or Red Hat OpenShift Container Platform certification is successfully completed and posted.

4.2. CERTIFICATION WORKFLOW

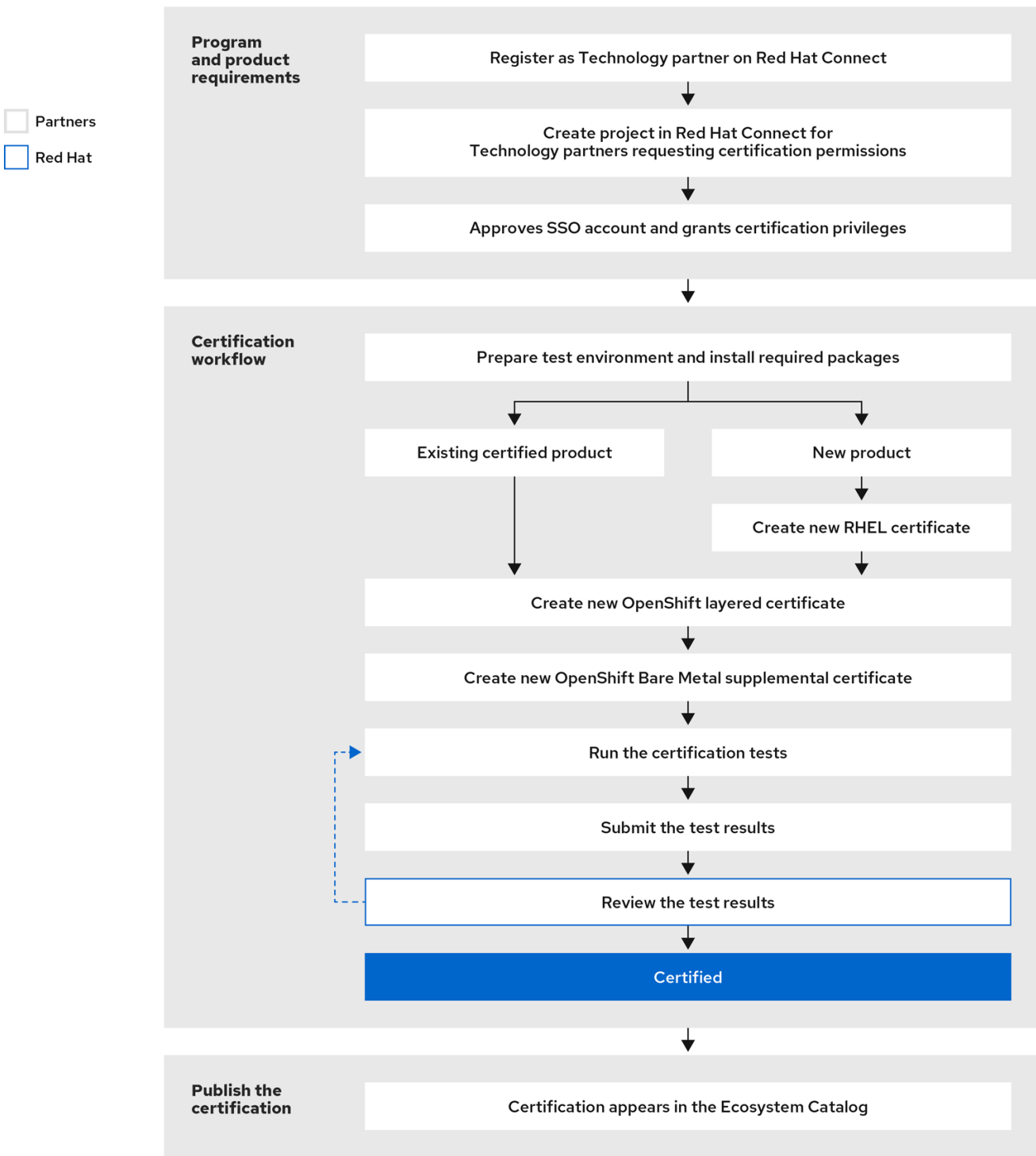
The Red Hat Bare Metal Hardware certification process includes the following requirements and steps:

Figure 4.1. Red Hat OpenStack Platform Bare Metal Hardware Certification Process



305_OpenStack_0523

Figure 4.2. Red Hat OpenShift Container Platform Bare Metal Hardware Certification Process



305_OpenStack_0523

4.3. CERTIFICATION REQUIREMENTS

Ensure you follow the respective Red Hat OpenStack bare metal hardware or Red Hat OpenShift Container Platform bare metal hardware Workflow Guides. Additional details for the certification requirements include:

- The Host Under Test (HUT) must already be RHEL certified. Hence the tests must run on a previously certified server, and all of the tests prescribed in the test plan must be executed in a single run.

- If you have a failed test, take the corrective action and retest **all of the tests in a single run**. Open a support case if necessary for guidance.

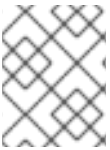
CHAPTER 5. LEVERAGING CERTIFICATION

Leveraging allows you to request credit for previously conducted successful certification testing. This is possible when a family of server systems utilizes a similar or substantially similar BMC.

Leveraging is based on your own internal qualification testing of the specific BMC on the specific individual system. You need to confirm that nuanced variations presented in the combination are not material, and the solution requesting leveraging is the same as demonstrated in a previous Red Hat certification.

Where applicable leveraging can reduce the overall amount of official testing required to achieve certification.

You can request leveraging for required testing when the solution contains a previously certified BMC with the same firmware branch and the same or fewer features.



NOTE

It is your responsibility to verify that any differences in BMC-to-server interaction do not affect the certification.

CHAPTER 6. PASS-THROUGH CERTIFICATION

A Pass-Through Certification refers to the ability of a third party system or component to be granted certification for hardware previously certified by the original hardware manufacturer. Pass-Through can reduce the overall amount of testing that is required to be performed and submitted to Red Hat to achieve certification for the third-party hardware.

System manufacturers can extend a certification granted to their own systems to another vendor's system where the original vendor:

- Has permission from the third party,
- Has the mechanics to ensure the third party does not alter the hardware in such a way that it would no longer be considered a subset of the original model certified by Red Hat, and
- Extends their responsibilities of support and representative hardware to include situations involving the third party hardware (refer to sections 1.2 and 1.3 of the Hardware Certification Agreement).

The third party cannot then extend their Pass-Through Certification to another vendor.

While both vendors are required to be members of the Red Hat Hardware Certification Program, only the original vendor may request Pass-Through Certifications. Vendors may also utilize the Pass-Through process where the same vendor has multiple names for the same hardware.

CHAPTER 7. SUPPLEMENTAL CERTIFICATION

Open supplemental certifications in the following scenarios:

First time certification

The Bare Metal supplemental certification may be automatically created for you during a different certification process. For example, when you applied for the Red Hat Enterprise Linux System certification.

If it was not automatically created for you, or if you need to apply for the certification at a later date, open a new supplemental certification on top of the Red Hat OpenStack Compute Node or the Red Hat OpenShift Platform certifications.

Recertification

Open a supplemental certification to update an existing RHOSP or RHOCP bare-metal certification. You may want to recertify your product, for example, to certify the same system on different versions of a Red Hat platform, or because your product has received a significant update.

It is your responsibility to open these certifications and notify Red Hat of material changes to your product.

CHAPTER 8. RED HAT OPENSTACK PLATFORM BARE METAL HARDWARE CERTIFICATION



NOTE

This chapter is applicable only for Red Hat OpenStack Platform bare metal hardware certification.

CHAPTER 9. IPI CERTIFICATION TESTS

The certification includes self-check, supportable, director_undercloud and bare metal tests.

9.1. SELF CHECK TEST

The **self_check** test confirms that all the software packages required in the certification process are installed and that they have not been altered. This ensures that the test environment is ready for certification.

The certification packages must not be modified for certification testing or for any other purpose.

Success Criteria

The test environment includes all the packages required in the certification process and the packages have not been modified.

9.2. SUPPORTABLE TEST

The supportable test, also known as **baremetal/supportable**, ensure that the test environment is compliant with Red Hat's support policy. The test confirms that the test node (an OpenStack deployment under test) consists only of components supported by Red Hat (Red Hat OpenStack Platform, Red Hat Enterprise Linux).

An OpenStack deployment under test refers to the node where the plugin or application under test is installed.

Supportability tests must be run on both the control node and the compute node.

This test is required for all OpenStack software certifications.

Compute Node Considerations:

- If your kernel is not updated, ensure that you update the kernel test section to verify that the compute uses the GA kernel to prevent review exit. Review will need to account for the status of RHEL certification.
- Driver Update Programs (DUPs) are acceptable on the compute node but will cause the test to exit review. Review needs to confirm the DUP that aligns with the one used in the corresponding RHEL certification.

The **baremetal/supportable** tests include the following subtests:

9.2.1. Kernel subtest

The **kernel** subtest checks the kernel module running on the test environment. The version of the kernel can be either the original General Availability (GA) version or any subsequent kernel update released for the RHEL major and minor releases.

The kernel subtest also ensures that the kernel is not tainted when running in the environment.

Success criteria

- The running kernel is a Red Hat kernel.

- The running kernel is released by Red Hat for use with the RHEL version.
- The running kernel is not tainted.
- The running kernel has not been modified.

Additional resources

- [Red Hat Enterprise Linux Life Cycle](#)
- [Red Hat Enterprise Linux Release Dates](#)
- [Why is the kernel "tainted" and how are the taint values deciphered?](#)

9.2.2. Kernel modules subtest

The **kernel modules** subtest verifies that loaded kernel modules are released by Red Hat, either as part of the kernel's package or added through a Red Hat Driver Update. The kernel module subtest also ensures that kernel modules do not identify as Technology Preview.

Success criteria

- The kernel modules are released by Red Hat and supported.

Additional resources

- [What does a "Technology Preview" feature mean?](#)

9.2.3. Hardware Health subtest

The Hardware Health subtest checks the system's health by testing if the hardware is supported, meets the requirements, and has any known hardware vulnerabilities. The subtest does the following:

- Checks that the Red Hat Enterprise Linux (RHEL) kernel does not identify hardware as unsupported. When the kernel identifies unsupported hardware, it will display an unsupported hardware message in the system logs and/or trigger an unsupported kernel taint. This subtest prevents customers from possible production risks which may arise from running Red Hat products on unsupported configurations and environments.
In hypervisor, partitioning, cloud instances, and other virtual machine situations, the kernel may trigger an unsupported hardware message or taint based on the hardware data presented to RHEL by the virtual machine (VM).
- Checks that the Host Under Test (HUT) meets the minimum hardware requirements.
 - RHEL 8 and 9: Minimum system RAM should be 1.5GB, per CPU logical core count.
 - RHEL 7: Minimum system RAM should be 1GB, per CPU logical core count.
- Checks if the kernel has reported any known hardware vulnerabilities, if those vulnerabilities have mitigations and if those mitigations have resolved the vulnerability. Many mitigations are automatic to ensure that customers do not need to take active steps to resolve vulnerabilities. In some cases this is not possible; where most of these remaining cases require changes to the configuration of the system BIOS/firmware which may not be modifiable by customers in all situations.
- Confirms the system does not have any offline CPUs.

- Confirms if Simultaneous Multithreading (SMT) is available, enabled, and active in the system.

Failing any of these tests will result in a WARN from the test suite and should be verified by the partner to have correct and intended behavior.

Success criteria

- The kernel does not have the UNSUPPORTEDHARDWARE taint bit set.
- The kernel does not report an unsupported hardware system message.
- The kernel should not report any vulnerabilities with mitigations as vulnerable.
- The kernel does not report the logic core to installed memory ratio as out of range.
- The kernel does not report CPUs in an offline state.

Additional resources

- [Minimum required memory](#)
- [Hardware support available in RHEL 8 but removed from RHEL 9](#) .
- [Hardware support available in RHEL 7 but removed from RHEL 8](#) .
- [Hardware support available in RHEL 6 but removed from RHEL 7](#) .

9.2.4. Installed RPMs subtest

The **installed RPMs** subtest verifies that RPM packages installed on the system are released by Red Hat and not modified. Modified packages may introduce risks and impact the supportability of the customer's environment. You might install non-Red Hat packages if necessary, but you must add them to your product's documentation, and they must not modify or conflict with any Red Hat packages.

Red Hat will review the output of this test if you install non-Red Hat packages.

Success criteria

- The installed Red Hat RPMs are not modified.
- The installed non-Red Hat RPMs are necessary and documented.
- The installed non-Red Hat RPMs do not conflict with Red Hat RPMs or software.

Additional resources

- [Production Support Scope of Coverage](#)

9.2.5. System report subtest

Red Hat uses a tool called **sos** to collect configuration and diagnostics information from a RHEL system. The **sos** tool assists customers in troubleshooting a RHEL system and following the recommended practices.

The System Report subtest ensures that the sos tool functions as expected on the image or system and captures a basic sosreport.

Success Criteria

The RHCERT tool captures a basic sosreport on the OpenStack deployment under test.

Additional resources

- For more information about sosreport, see [What is an sosreport and how to create one in Red Hat Enterprise Linux?](#)

9.2.6. SELinux subtest

Confirms that SELinux is running in **enforcing mode** on the OpenStack deployment-under test.



NOTE

Security-Enhanced Linux (SELinux) adds Mandatory Access Control (MAC) to the Linux kernel, and is enabled by default in Red Hat Enterprise Linux.

SELinux policy is administratively-defined, enforced system-wide, and is not set at user discretion, reducing vulnerability to privilege escalation attacks helping limit the damage made by configuration mistakes. If a process becomes compromised, the attacker only has access to the normal functions of that process, and the files that the process has been configured to.

Success Criteria

SELinux is configured and running in enforcing mode on the OpenStack deployment under test.

Additional resources

- For more information on SELinux in RHEL, see [SELinux Users and Administrators Guide](#).

9.3. DIRECTOR_UNDERCLOUD TEST

The Director_undercloud test, also known as **openstack/director**, ensures that the **deployment-under-test** is originally installed using Red Hat OpenStack Platform Director. This test is required for all OpenStack software certifications.

Red Hat OpenStack Platform Director is the supported toolset for installing and managing a Red Hat OpenStack Platform environment in production. It helps in easy installation of a lean and robust OpenStack cloud. It is specifically targeted for enterprise cloud environments where updates, upgrades, and infrastructure control are critical for underlying OpenStack operations.

Success Criteria

The deployment under test is originally installed using Red Hat OpenStack Platform Director.

Additional resources

- For more information on installing Red Hat OpenStack Platform Director, see [Director Installation and Usage Guide](#).

9.4. BARE METAL TEST

The following sub-tests comprise the bare metal test. The tests perform enrolling, inspection and deployments to validate the bare metal node.

9.4.1. Bare Metal InstackStackrc validation

Validates the **instackenv.json** and **stackrc** files.

Success Criteria

- Checks if the **instackenv.json** and **stackrc** files exist in the specified location and validate the content of **instackenv.json** file, and
- Requires validation check if the file is a valid json file and the specified BMC IPs are reachable.

9.4.2. Bare Metal driver validation

Compares the drivers configured on the HUT with the drivers supported by Red Hat. If a driver mismatch occurs the subtest generates a *Review* state and exits. The drivers supported by Red Hat are part of the test suite

Success Criteria

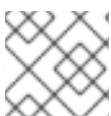
- The specified driver should match with the driver in **instackenv.json** file, and
- If the drivers do not match the test will exit with a *Review* state. In this scenario, the Red Hat certification team will manually check the **instackenv.json** file and the specified driver to validate if the drivers are supported drivers.

9.4.3. Bare Metal undercloud validation

Checks if tests are running from the undercloud node. If the tests are not running from this node, the test fails and you need to rerun the test.

Success Criteria

Testing undercloud artifacts to check if the test ran from the undercloud node.



NOTE

The undercloud node is the valid node.

9.4.4. Bare Metal enrolling test

Checks if the bare metal driver is successfully able to enroll the hardware node using the BMC IP. The enrollment process requires driver to communicate properly with BMC IP. The BMC changes the **Power state** and **Provisioning state** of the enrolled nodes to **off** and **available**.

The test also checks if the stack overcloud exists and if the nodes are already added. It deletes the stack and nodes if they exist, and then tries to enroll nodes based on the **instackenv.json** file. The test is failed if any of the stages fail.

Success Criteria

Enrolled nodes are expected to be in **Power** and **Provisioning** state.

9.4.5. Bare Metal inspecting test

Once the operator sets the required **driver_info** fields, BareMetalInspectingTest allows **Bare Metal** service to discover required node properties.

Success Criteria

Node properties should be correctly populated so that BMC can gather hardware details based on the instructions provided by the driver.

9.4.6. Bare Metal deploying test

Once the inspection is completed successfully, the Bare Metal Deploying Test will try to **nova boot** two virtual machines by creating and assigning a custom flavor to the nodes. This helps to check if BMCs can provide instances with the required boot images, and then try to boot up the instances.

Success Criteria

Start of VMs' with **Active** status attached to them.

9.4.7. Bare Metal redeploying test

Tries to redeploy nova instances.

Success Criteria

All the stages covered previously should pass in the redeploy too. The test enrolls and inspects the hardware instances, deploys the instances based on the enroll and inspect stages.

CHAPTER 10. RED HAT OPENSIFT CONTAINER PLATFORM BARE METAL HARDWARE CERTIFICATION



NOTE

This chapter is applicable only for Red Hat OpenShift Container Platform bare metal hardware certification.

CHAPTER 11. IPI CERTIFICATION TESTS

The IPI test validates whether the Host Under Test (HUT) can be controlled, accessed, deployed, and rebooted remotely by using the Red Hat OpenShift Container Platform ironic service and the HUT's baremetal management controller (BMC).

The test runs in a container accessible by the node that is running the ironic service.

The following RHEL and RHOCP combinations are supported:

- RHEL 9.2 or 9.4 with RHOCP 4.13, 4.14, or 4.15
- RHEL 8 with RHOCP 4.12

The test plan consists of the following tests:

11.1. SELF CHECK TEST

The **self_check** test confirms that all the software packages required in the certification process are installed and that they have not been altered. This ensures that the test environment is ready for certification.

The certification packages must not be modified for certification testing or for any other purpose.

Success Criteria

The test environment includes all the packages required in the certification process and the packages have not been modified.

11.2. IPI TEST

The **IPI** test automates power management of the server from the OpenShift console through the ironic service to the BMC.

The test runs the following subtest:

11.2.1. Check and update power state subtest

The **check_update_power_state** subtest first checks if the HUT is powered on, and then restarts the HUT.

The subtest monitors the status of the HUT node every 15 seconds, for a maximum of 15 minutes.

Success Criteria

- The HUT restarts successfully in less than 15 minutes.

CHAPTER 12. ASSISTED INSTALLER CERTIFICATION TESTS

The assisted installer tests ensure that the HUT can be installed successfully by using the assisted installer for Red Hat OpenShift Container Platform.

The tests verify single-node clusters only. If you want to certify multiple bare-metal servers, you must install each of them as a single-node cluster.

The following RHEL and RHOCP combinations are supported:

- RHEL 9.2 or 9.4 with RHOCP 4.13, 4.14, or 4.15

The test plan consists on the following tests:

12.1. SELF CHECK TEST

The **self_check** test confirms that all the software packages required in the certification process are installed and that they have not been altered. This ensures that the test environment is ready for certification.

The certification packages must not be modified for certification testing or for any other purpose.

Success Criteria

The test environment includes all the packages required in the certification process and the packages have not been modified.

12.2. ASSISTED INSTALLER TEST

The **assisted_installer** test queries the assisted installer APIs to collect basic information about the assisted installer and the HUT cluster.

Before you run the test, generate an OpenShift Manager API token and export it as the value of the **OFFLINE_TOKEN** variable. For example:

```
# export OFFLINE_TOKEN=<value_of_your_token>
```

The test will prompt for the cluster ID if unable to determine it.

Success Criteria

The test connects to the assisted installer APIs and collects the information successfully.

12.3. SOSREPORT TEST

The **Sosreport test** connects to the HUT cluster and collects information about the cluster's hardware and configuration.

The **sos_reports/manifest.json** file contains details about node hostnames and the commands run by this test.

Success Criteria

The test correctly collects the information from the Single node OpenShift (SNO) cluster's master node.

12.4. CLUSTER INSPECTION TEST

The cluster inspection test invokes the Cloud-native Network Function (CNF) test. It is a backlog test and is available only in the preview mode.

Additional resources

- For more information about assisted installer tests, see [Running the assisted installer tests](#).