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

## PART I. MAKING OPEN SOURCE MORE INCLUSIVE

### CHAPTER 1. INTRODUCTION TO RED HAT OPENSTACK HARDWARE (BARE METAL) CERTIFICATION POLICIES

1.1. AUDIENCE

1.2. CREATING VALUE FOR OUR JOINT CUSTOMERS

### CHAPTER 2. PREREQUISITES

2.1. PARTNER ELIGIBILITY CRITERIA

2.2. BASEBOARD MANAGEMENT CONTROLLERS (BMC)

2.3. SERVER

### CHAPTER 3. OVERVIEW OF BARE METAL CERTIFICATION LIFE CYCLE

3.1. RED HAT PRODUCT RELEASES

3.2. CERTIFICATION DURATION

3.3. RECERTIFICATION WORKFLOW

### CHAPTER 4. CERTIFICATION TESTING

4.1. PREREQUISITES FOR CERTIFICATION TESTING

4.2. CERTIFICATION WORKFLOW

4.3. CERTIFICATION REQUIREMENTS

### CHAPTER 5. LEVERAGING CERTIFICATION

### CHAPTER 6. PASS-THROUGH CERTIFICATION

### CHAPTER 7. SUPPLEMENTAL CERTIFICATION

### CHAPTER 8. TYPES OF CERTIFICATION TESTS

8.1. SELF_CHECK TEST

8.2. SUPPORTABLE TEST

8.2.1. Kernel subtest

8.2.2. Kernel modules subtest

8.2.3. Hardware Health subtest

8.2.4. Installed RPMs subtest

8.2.5. System report subtest

8.2.6. SELinux subtest

8.3. DIRECTOR_UNDERCLOUD TEST

8.4. BARE METAL TEST

8.4.1. Bare Metal InstackStackrc validation

8.4.2. Bare Metal driver validation

8.4.3. Bare Metal undercloud validation

8.4.4. Bare Metal enrolling test

8.4.5. Bare Metal inspecting test

8.4.6. Bare Metal deploying test

8.4.7. Bare Metal redeploying test
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 HARDWARE (BARE METAL) CERTIFICATION POLICIES

The Red Hat OpenStack Hardware (Bare Metal) Certification Policy Guide is intended for hardware vendors who want to certify their system hardware with Red Hat. Red Hat OpenStack Platform Hardware Certification creates value for customers as the system can be managed and automatically deployed and redeployed with Red Hat OpenStack Platform, without manual intervention.

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 in a supported customer environment.

1.2. CREATING VALUE FOR OUR JOINT CUSTOMERS

Red Hat OpenStack Platform Hardware Certification creates value for customers as the system can be managed and automatically deployed and redeployed with Red Hat OpenStack Platform, 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 Hardware Certification program policy 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 Platform is required. A Red Hat Certified Engineer and a Red Hat OpenStack Platform Certified Engineer accreditation is preferred and suggested before participating.

2.1. PARTNER ELIGIBILITY CRITERIA

Before you begin, make sure you meet the eligibility criteria for certification.

- Join the Red Hat Hardware Certification program
- A valid Red Hat Enterprise Linux hardware certification and a Red Hat OpenStack Platform Nova hardware certification, and
- A support relationship with Red Hat. This can be fulfilled through the multi-vendor support network of TSANet, or through a custom support agreement

2.2. BASEBOARD MANAGEMENT CONTROLLERS (BMC)

BMC is a specialized microcontroller embedded on the motherboard of a server and manages the interface between system management software and hardware platform. The bare metal service provisions the system by utilizing BMC in a server, to control both power and network booting automating the deployment of node in openstack as well as terminating those nodes when they become unnecessary.

2.3. SERVER

A server is required to have the corresponding Red Hat Enterprise Linux and Red Hat OpenStack Platform Compute (Nova) certifications. A server must also contain a BMC that has a supported bare metal driver to be eligible for certification testing.
CHAPTER 3. OVERVIEW OF BARE METAL CERTIFICATION LIFE CYCLE

The bare metal certification life cycle consists of the product release, certification duration, and recertification.

3.1. 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 OpenStack 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) Red Hat OpenStack Platform software packages.

3.2. CERTIFICATION DURATION

Certifications are valid for a specific major release of Red Hat OpenStack Platform. Customers count on certifications from the moment they are listed until the end of the lifecycle of the products, so certifications are valid for the same period.

3.3. RECERTIFICATION WORKFLOW

Certification on a new, major release of Red Hat OpenStack Platform is considered a New Certification.

Typically, recertification during a major release of Red Hat OpenStack Platform is not required; however, it is your responsibility to recertify if there are changes to a partner’s product that would degrade or invalidate the previous certification.

The recertification process may utilize a Supplemental Certification. Red Hat encourages Partners to perform retest during the lifecycle of their product, including minor changes, to ensure that customers can expect a consistent level of quality and performance, despite minor changes. This may be conducted utilizing the partners own testing or with sandbox testing provided in Red Hat 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

- The corresponding RHEL server certification is successfully completed and posted.
- The corresponding Red Hat OpenStack Platform Compute (Nova) certification is successfully completed and posted.
- The corresponding Bare Metal driver is on the Supported Drivers List for the corresponding Red Hat OpenStack Platform release.

4.2. CERTIFICATION WORKFLOW

The Red Hat OpenStack Platform Hardware certification process includes the following requirements and steps:

4.3. CERTIFICATION REQUIREMENTS

Ensure that you follow the Red Hat OpenStack Hardware Workflow Guide. Additional details for the certification requirements include:

- The system under test (SUT) must already be 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 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.
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.

Pass-Through is based on your understanding and controlling the nuanced variations of the hardware of the third-party. Partner’s confirm to Red Hat that the hardware of the third party is the same as demonstrated previously in the original certification.

System manufacturers can extend a certification granted to their 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 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

For recertification, use a supplemental certification. It is required when either your product or Red Hat product in the solution has been updated, which affects the current certification, but where a new certification catalog entry is not desired. For example, a firmware update that adds a feature.

Supplemental testing is required when the Partner has upgraded part of an existing product, be it the system or the BMC, that affects the combination.

NOTE

It is your responsibility to open these certifications and notify Red Hat of material changes to the product that was certified.
CHAPTER 8. TYPES OF CERTIFICATION TESTS

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

8.1. SELF_CHECK TEST

The Red Hat Certification Self Check test also known as rhcert/self_check 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 the certification process and that all the certification software packages are supportable.

NOTE

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.

8.2. 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:

8.2.1. Kernel subtest

The Kernel subtest confirms the kernel that the image is running is from Red Hat, is appropriate and supported for the version of RHEL undergoing certification, and has not been modified. The kernel version may be the original General Availability (GA) version or any subsequent kernel errata released for the RHEL major and minor release.
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.

**Additional resources**

- For more information on Red Hat Enterprise Linux Life Cycle and Kernel Versions, see [Red Hat Enterprise Linux Life Cycle](#).
- [Red Hat Enterprise Linux Release Dates](#).
- For more information about kernel tainting, see link:[Why is the kernel “tainted” and how are the taint values deciphered?](#).

**8.2.2. Kernel modules subtest**

The Kernel Modules subtest confirms the loaded kernel modules are from Red Hat, either from the running kernel’s package or a Red Hat Driver Update. The kernel module subtest also ensures the kernel modules do not identify as Technology Preview when running in the environment.

**Success criteria**

The kernel modules are from Red Hat and supported.

**Additional resources**

- For more information about Technology Preview, see [What does a “Technology Preview” feature mean?](#).

**8.2.3. 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 system under test (SUT) meets the minimum hardware requirements.
  - RHEL 8: 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
- For more information about hardware support available in RHEL 7 but removed from RHEL 8, see Hardware Enablement.
- For more information about hardware support available in RHEL 6 but removed from RHEL 7, see Changes to Packages, Functionality, and Support.

### 8.2.4. Installed RPMs subtest

Confirms that RPM packages installed on the system are from Red Hat and not modified, potentially enabling customers to avoid the significant risks arising from unexpected software/packages, further ensuring that customers are starting with a supportable environment.

Non-Red Hat packages may be installed if they are necessary to enable the cloud environment, but they are acceptable where they are documented and if they DO NOT modify or conflict with Red Hat packages/software. This subtest will require detailed review at Red Hat to confirm success or failure if non Red Hat packages are installed.

### Success criteria

- The installed Red Hat provided RPM packages are from Red Hat products available in the offering.
- The installed Red Hat RPM packages are not modified.
- The installed Non-Red Hat RPM packages are necessary to enable the cloud environment and are documented.
- The installed Non Red Hat RPM packages do not conflict with Red Hat provided packages/software available in Red Hat products included in the offering.

**Additional resources**
- For more information on Red Hat support policies on third-party software, see [Production Support Scope of Coverage](#).

### 8.2.5. 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?](#).

### 8.2.6. 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](#).

### 8.3. 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](#).

### 8.4. 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.

#### 8.4.1. 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.

#### 8.4.2. Bare Metal driver validation

Compares the drivers configured on the SUT 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.

#### 8.4.3. 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.

8.4.4. 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.

8.4.5. 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.

8.4.6. 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.

8.4.7. 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.