Red Hat OpenStack Certification 7.27

Red Hat OpenStack Platform Hardware Bare Metal Certification Policy Guide

For Use with Red Hat OpenStack 16

Last Updated: 2021-04-23

Red Hat OpenStack Certification 7.27 Red Hat OpenStack Platform Hardware Bare Metal Certification Policy Guide

For Use with Red Hat OpenStack 16

Legal Notice

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: Mar 22, 2021.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

CHAPTER 1. INTRODUCTION

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.

1.1. AUDIENCE

This guide describes the technical certification requirement 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 a value for customer 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

The following list summarizes the prerequisites that Partners must meet to attain Red Hat OpenStack Hardware Platform 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 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. UNDERSTANDING THE 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

Partners may have access to, and are encouraged to test with, pre released Red Hat software. They may begin their engagement with the Red Hat OpenStack Certification team before Red Hat software is generally available (GA) to customers, to expedite the certification process for their 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

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 the Partner's 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.

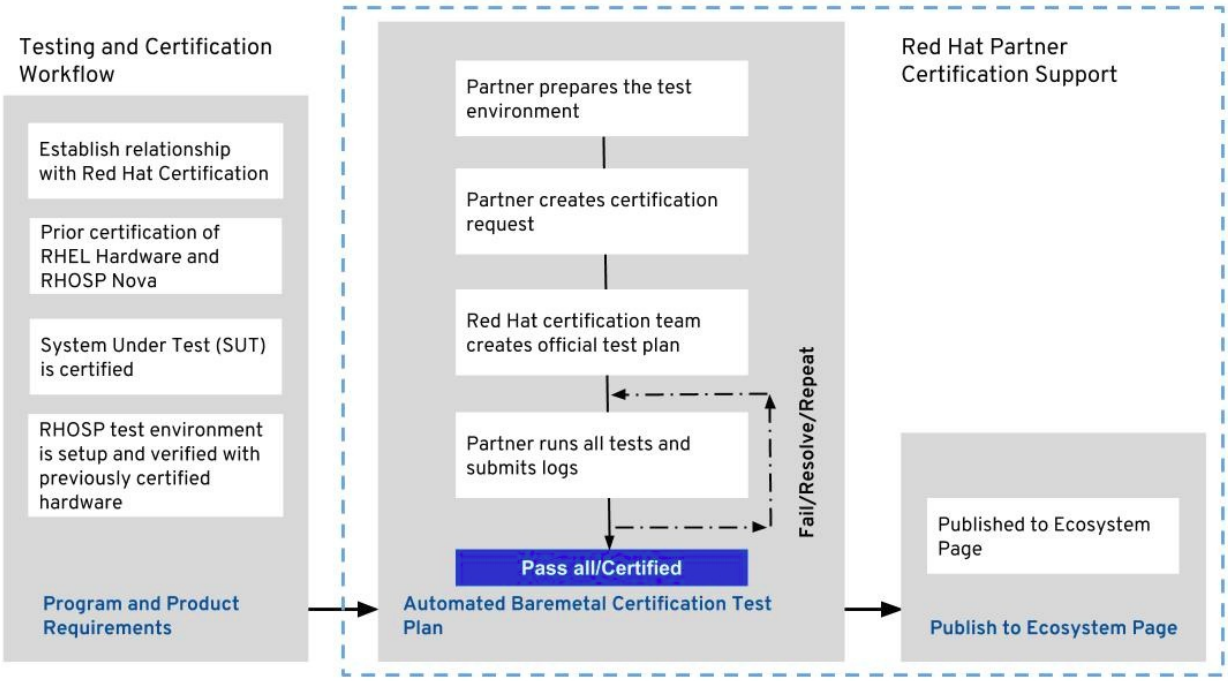
4.1. PREREQUISTES FOR CERTIFICATION TESTING

Complete the following requirements before you begin the 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. UNDERSTANDING THE CERTIFICATION PROCESS

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



4.3. CERTIFICATION REQUIREMENTS

Partners are expected to follow the Red Hat OpenStack Hardware Workflow Guide. However, additional details for the certification requirements include:

- The system under test (SUT) must already be certified; therefore,
- 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 allow Partners 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 the Partner performing their own internal qualification testing of the specific BMC on the specific individual system. It requires the partner to confirm that nuanced variations presented in the combination are not material, and the solution requesting leveraging is same as demonstrated in a previous Red Hat certification.

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

Partners may 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 the partner's 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.

Pass-Through is based on the original Partner 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

A Supplemental certification is utilized for recertifying. It is required when either the Partner 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 (e.g. 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

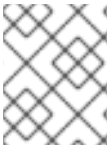
It is the responsibility of the partner to open these certifications and notify Red Hat of material changes to the product that was certified.

CHAPTER 8. TYPES OF CERTIFICATION TESTS

The certification includes self-check, supportable, director_undercloud and bare metal tests. The following sections explains about the test and their sub-test along with the success criteria that is to be an expected outcome.

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 **openstack/supportable**, ensure that the test environment is compliant with Red Hat's support policy. This test is required for all OpenStack software certifications. 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/application-under-test is installed.

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

Compute Node Considerations:

- Update the kernel test section to clarify that the compute node needs to use the GA kernel, or it will exit review. Review will need to account for how did the RHEL cert go.
- 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 **openstack/supportable** tests include the following subtests:

8.2.1. Kernel

Verifies that the kernel utilized by Red Hat Enterprise Linux and included in the deployment-under-test is from Red Hat, is appropriate and supported for the version of Red Hat Enterprise Linux included in the OpenStack deployment-under-test, and has not been modified.

The kernel version may be the original General Availability (GA) version or any subsequent kernel errata released by Red Hat for the Red Hat Enterprise Linux minor release.

NOTE

For more information on Red Hat Enterprise Linux Life Cycle and Kernel Versions, refer to the Red Hat Enterprise Linux Life Cycle and Red Hat Enterprise Linux Release Dates .

The kernel subtest also ensures that the kernel is not tainted when running in the environment. For more information about kernel tainting, refer to Why is the kernel "tainted" and how are the taint values deciphered?.

Success Criteria:

- The running kernel is a Red Hat kernel, and is released by Red Hat for use with the RHEL version, and
- The running kernel is not tainted

8.2.2. Kernel Modules

Confirms that the loaded kernel modules are from Red Hat, either from the running kernel's package or from a Red Hat Driver Update (see Where can I download Driver Update Program (DUP) disks).

The kernel module subtest also ensures the kernel modules do not identify as Technology Preview when running in the environment (see What does a "Technology Preview" feature mean).

Success Criteria:

The kernel modules are from and supported by Red Hat.

8.2.3. Hardware Health

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[1] as follows:
  - RHEL 8: Minimum system RAM should be 1.5GB, per CPU logical core count[2]
  - RHEL 7: Minimum system RAM should be 1GB, per CPU logical core count[3]
- 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.

8.2.4. Installed RPMs

Confirms that RPM packages installed on the system are from Red Hat and are not modified. This prevents potential significant risks to customer environments and ensures that customers make use of a supported environment.

NOTE

Non-Red Hat packages may not be installed in the OpenStack deployment-under-test.

Success Criteria:

- The installed Red Hat provided RPM packages are from Red Hat product(s) available in the offering, and
- The installed Red Hat RPM packages are not modified.

8.2.5. System Report

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

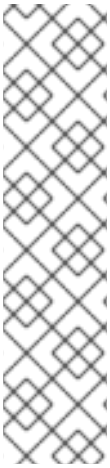
The System Report subtest ensures that the sos tool functions as expected on the image or system and captures a basic sosreport. For more information about sosreport, refer to https://access.redhat.com/solutions/3592.

Success Criteria:

A basic sosreport can be captured on the OpenStack deployment-under-test.

8.2.6. SELinux

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.

For more information on SELinux in RHEL, refer to the SELinux Users and Administrators Guide.

Success Criteria:

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

8.3. DIRECTOR_UNDERCLOUD

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.

For more information on installing Red Hat OpenStack Platform Director, refer the Director Installation and Usage Guide.

Success Criteria:

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

8.4. BARE METAL TEST

The following sub-tests comprise the bare metal test.

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 bare metal driver is successfully able to enroll the hardware node using the BMC IP. The enrollment process involves 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, IronicInspectingTest 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 (VMs') by assigning a custom flavor to the nodes. This helps to check if BMCs can provide VMs' 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 will try to enroll and inspect the hardware instances, and will deploy the instances based on the enroll and inspect stages.

Revised on 2021-04-23 06:42:19 UTC

---

[1] Minimum required memory

[2] For more information about hardware support available in RHEL 7 but removed from RHEL 8, see chapter Hardware Enablement in the *Considerations in Adopting Red Hat Enterprise Linux 8* document.

[3] For more information about hardware support available in RHEL 6 but removed from RHEL 7, see chapter Changes to Packages, Functionality, and Support in the *RHEL 7 Migration Planning Guide* document.