



Red Hat OpenStack Certification 7.29

Red Hat OpenStack Application and VNF Policy Guide

For Use with Red Hat OpenStack 16

Red Hat OpenStack Certification 7.29 Red Hat OpenStack Application and VNF Policy Guide

For Use with Red Hat OpenStack 16

Legal Notice

Copyright © 2021 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

Red Hat OpenStack Application Policy Guide covers the requirements for achieving a Red Hat OpenStack Platform (RHOSP) application software certification. Last updated: Mar 22, 2021.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
CHAPTER 1. INTRODUCTION	4
1.1. AUDIENCE	4
1.2. CREATING VALUE FOR OUR CUSTOMERS	4
CHAPTER 2. RHOSP APPLICATION CERTIFICATION PREREQUISITES	5
CHAPTER 3. RHOSP APPLICATION TESTING REQUIREMENTS	6
CHAPTER 4. CERTIFICATION TESTS	7
4.1. SYSTEM REPORT OVERVIEW	7
4.2. SUPPORTABILITY TEST OVERVIEW	7
4.2.1. Kernel Subtest	7
4.2.2. Kernel Modules Subtest	8
4.2.3. Hardware Health	8
4.2.4. Installed RPMs Subtest	9
4.2.5. SELinux Subtest	9
4.3. DIRECTOR TEST	9
4.4. VNF TESTING CONFIGURATION REPORT TEST	10
CHAPTER 5. VNF CERTIFICATION LEVEL	12

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

This guide describes to our Red Hat Technology Partners the prerequisites and environmental testing requirements that are necessary to successfully complete and obtain a Red Hat OpenStack Platform (RHOSP) application certification.

This includes applications that depend on RHOSP API's, provide additional functionality in RHOSP cloud, such as a Virtual Network Function (VNF), Network Functions Virtualization (NFV), Management and Orchestration (MANO), and those applications which run on top of a RHOSP environment. It includes the applications that do not implement infrastructure software (plug-in or driver) for use with Red Hat OpenStack Platform in a supported customer environment.

1.1. AUDIENCE

Red Hat OpenStack application certification policy guide is intended for Partners who want to certify their system using an Openstack application like Virtual Network Function (VNF), Network Functions Virtualization (NFV), Management and Orchestration (MANO) and others.

1.2. CREATING VALUE FOR OUR CUSTOMERS

Red Hat OpenStack application certification creates a value for customer as it ensures that the certified application can be used with RHOSP in addition to making sure the underlying architecture is still supportable after installation of application. 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.

CHAPTER 2. RHOSP APPLICATION CERTIFICATION PREREQUISITES

The following list summarizes the prerequisites that the Partners need in order to meet OpenStack application certification requirements:

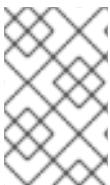
1. Companies must be Partners in [Red Hat Connect for Technology Partners](#). This program enables an ecosystem for commercial OpenStack deployments and includes numerous technology companies.
2. Partners must have a support relationship with Red Hat. This can be fulfilled through the multi-vendor support network of TSANet, or through a custom support agreement.
3. Partners must have a good working knowledge of RHOSP including installation and configuration of the product.



NOTE

To understand the product, you can use detailed product documentation on [Red Hat Customer Portal](#) or undertake the product training/certification on [Red Hat Training Page](#)

4. Partners must have a tested application on a supported RHOSP release.



NOTE

The RHOSP application certification does not verify if a Partner's application's intended behavior matches the application's actual behavior. This responsibility remain under the Partner's full control.

CHAPTER 3. RHOSP APPLICATION TESTING REQUIREMENTS

The RHOSP Application Testing Requirements will be required and provided by Red Hat to the Partner in a test plan for each certification. The following tests are explained in [Chapter 4, *Certification Tests*](#) of this guide:

- System Report Test
- Supportability Test
- Director Test
- VNF Configuration Testing Report Test (for VNF only)

Partners are expected to perform System Report, Supportability, and Director test for a regular RHOSP application. However, for VNF certification along with these three test Partners also need to perform the VNF Testing Configuration report test.

CHAPTER 4. CERTIFICATION TESTS

The Red Hat OpenStack application policy includes multiple tests each with a series of subtests and checks. Different certifications will require different tests. Following are the certification tests:

4.1. SYSTEM REPORT OVERVIEW

The System Report test, also known as **openstack/sosreport**, captures the basic sosreport. Red Hat uses a tool called sos to collect the configuration and diagnostics information from a Red Hat Enterprise Linux(RHEL) system, and to assist the customers in troubleshooting their system by following the recommended practices.

The system report subtest ensures that the sos tool functions as expected on the image/system and captures a basic sosreport. For more information about sosreport, see the [link](#)

Success Criteria

- A basic sosreport can be captured from the system under test, and
- The test status will be PASS if a valid rpm version captures and collects the openstack data

4.2. SUPPORTABILITY TEST OVERVIEW

The Supportability test, also known as **openstack/supportable**, ensures 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 RHOSP and RHEL that are supported by Red Hat or the Partner.



NOTE

An OpenStack deployment-under-test refers to the node where the plugin/application-under-test is installed and also the Undercloud Director node.

4.2.1. Kernel Subtest

The Kernel subtest verifies that the kernel utilized by RHEL and included in the deployment-under-test is from Red Hat. The subtest also verifies if the kernel is appropriate and supported for the version of RHEL 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 for the RHEL major + minor release.



NOTE

For more information on Red Hat Enterprise Linux Life Cycle and Kernel Versions, refer 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 Why is the kernel "tainted" and how are the taint values deciphered?

Success Criteria

The running kernel is a Red Hat released kernel which should not be tainted and can be used with the RHEL version.

4.2.2. 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. For information about Driver Update program see the article, [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. For information about Technology Preview see the article, [What does a "Technology Preview" feature mean?](#)

Success Criteria

The Kernel modules are from Red Hat and supported.

4.2.3. 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.

4.2.4. Installed RPMs Subtest

The installed RPMs subtest 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.

Non Red Hat packages may be installed if they are necessary to enable the cloud environment. But is expected that they are documented and 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.

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

Success Criteria

- The installed Red Hat provided RPM packages are from Red Hat product(s) 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 documented, and
- 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

4.2.5. SELinux Subtest

Security-Enhanced Linux (SELinux) adds Mandatory Access Control (MAC) to the Linux kernel, and is enabled by default in RHEL. The SELinux subtest confirms that SELinux is running in enforcing mode on the OpenStack deployment-under test.



NOTE

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

Success Criteria

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

4.3. DIRECTOR TEST

The Director 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 and is targeted specifically 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, see the [Director Installation and Usage Guide](#).

Success Criteria

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

4.4. VNF TESTING CONFIGURATION REPORT TEST

The VNF testing configuration report test is applicable only for VNF certification. In this test, a Partner selects the operating system on which the VNF is based; provides the link to a report, or uploads a VNF configuration testing report file. The VNF SME, reviews the report that describes the installation, configuration, and testing details that the Partner conducts.

The format of the required report is pre-defined and is at the Partner's discretion, however it will need to include the following information:

- Hardware configuration
 - Server make and model
 - CPU: make, model, speed, cores, HT
 - NIC make/model
 - Networking HW make/model
 - Storage make/model
 - Traffic Generator make/model
- Firmware configuration
 - Server firmware version
 - BMC firmware version
 - NIC firmware version
- System software configuration
 - Version and architecture of Red Hat Enterprise Linux used on the host
 - NUMA, Cores, Huge Pages config.
 - OpenStack Platform version
 - Third party OSP plug-ins used, with versions
 - Storage software used
 - Architectural / Topology Diagram
- VNF configuration

- VNF version
- vCPUs, Memory, storage used in testing
- Dataplane acceleration (ovs-dpdk, sr-ioV, etc.)
- Cores allocation - DPDK vs. application
- Bandwidth, IOPS, latency, etc. requirements
- Test cases performed:
 - Instantiation, termination, scale out/in, healing, HA, and others

[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.

CHAPTER 5. VNF CERTIFICATION LEVEL

Most certification do not have levels; instead a Partner solution is either certified or not. VNF however includes an additional certification level to address that these applications often include a VM that is not otherwise supportable by Red Hat. If a Partners performs a VNF certification following VNF certification levels will get generated:

- **Certified:** The Red Hat team generates a Certified level when the certificate is completed. The VNF test level will be Certified if the VNF image is based on the RHEL operating system during the VNF certification process. The following screenshot illustrates the Certified level:

Figure 5.1. VNF Certified Level

RED HAT CERTIFICATIONS

This product has been certified to run on the following Red Hat products and technologies:

Target Product	Level
Red Hat OpenStack Platform 10.0 Base: Red Hat Enterprise Linux (x86_64) 7.3-7.x	Certified
Red Hat OpenStack Platform 9.0 Base: Red Hat Enterprise Linux (x86_64) 7.2-7.x	Certified

- **Vendor Validated:** The Red Hat team generates a Vendor Validated level when the certificate is completed. The VNF test level will be Vendor Validated if the VNF image is based on a non-RHEL operating system during the VNF certification process. The following screenshot illustrates the Vendor Validated level:

Figure 5.2. VNF Vendor Validated Level

RED HAT CERTIFICATIONS

This product has been certified to run on the following Red Hat products and technologies:

Target Product	Level
Red Hat OpenStack Platform 10.0 Base: Red Hat Enterprise Linux (x86_64) 7.4-7.x	Vendor Validated