



Red Hat Certified Cloud and Service Provider Certification 8.67

Red Hat Certified Cloud and Service Provider Certification Policy Guide

For Use with Red Hat Certified Cloud and Service Provider 1.0

Red Hat Certified Cloud and Service Provider Certification 8.67 Red Hat Certified Cloud and Service Provider Certification Policy Guide

For Use with Red Hat Certified Cloud and Service Provider 1.0

Legal Notice

Copyright © 2023 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

This document describes the technical and operational certification requirements for CCSP partners who want to offer Infrastructure-as-a-Service (IaaS) based on Red Hat Enterprise Linux. Version 8.67 updated August 29, 2023.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
CHAPTER 1. INTRODUCTION TO RED HAT CERTIFIED CLOUD AND SERVICE PROVIDER CERTIFICATION POLICIES	4
1.1. AUDIENCE	4
1.2. CREATE VALUE FOR OUR JOINT CUSTOMERS	4
1.3. TEST SUITE VERSIONS	4
1.4. SUPPORTED RHEL VERSION AND ARCHITECTURE	4
1.5. UNDERSTAND PASSTHROUGH CERTIFICATIONS	5
CHAPTER 2. RED HAT CERTIFICATION SELF CHECK	6
2.1. RED HAT CERTIFICATION SELF CHECK (RHCERT/SELF CHECK) TEST	6
2.2. SYSTEM REPORT	6
CHAPTER 3. SUPPORTABILITY TESTS	7
3.1. LOG VERSIONS SUBTEST	7
3.2. KERNEL SUBTEST	7
3.3. KERNEL MODULES SUBTEST	7
3.4. HARDWARE HEALTH SUBTEST	8
3.5. HYPERVISOR/PARTITIONING SUBTEST	9
3.6. FILESYSTEM LAYOUT SUBTEST	9
3.7. INSTALLED RPMS SUBTEST	9
3.8. SOFTWARE REPOSITORIES SUBTEST	10
3.9. SOFTWARE CONTAINERS TEST	10
3.10. INSIGHTS SUBTEST	10
3.11. SOFTWARE MODULES TEST	11
CHAPTER 4. OVERVIEW OF IMAGE CONFIGURATION	12
4.1. DEFAULT SYSTEM LOGGING	12
4.2. NETWORK CONFIGURATION TEST	12
4.3. DEFAULT OS RUNLEVEL	13
4.4. SYSTEM SERVICES	13
4.5. SUBSCRIPTION SERVICES	14
CHAPTER 5. OVERVIEW OF SECURITY PRACTICES	15
5.1. PASSWORD CONFIGURATION TEST	15
5.2. RPM FRESHNESS	15
5.3. SELINUX ENFORCING SUBTEST	15

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 CERTIFIED CLOUD AND SERVICE PROVIDER CERTIFICATION POLICIES

1.1. AUDIENCE

Use this guide to understand the technical and operational certification requirements as implemented for CCSP partners who want to offer Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or a managed service based on Red Hat Enterprise Linux. The certification tools and methodologies cater to cloud application images built on Red Hat Enterprise Linux.

1.2. CREATE VALUE FOR OUR JOINT CUSTOMERS

As a Certified Cloud and Service Provider (CCSP), you are required to certify images that you publish in a catalog. The certification process includes a series of tests that provide your Red Hat customers assurance that they will have a consistent experience across cloud providers, that the customer's experience comes with the highest level of support, and that good security practices are available to the customers.

The cloud certification test suite (redhat-certification-cloud) includes three tests (supportable, configuration, security), each with a series of subtests and checks, which are explained below. Logs from a singular run with all three of the cloud tests and the test suite self check test (rhcert/selfcheck) must be submitted to Red Hat for new certifications and for recertifications.

Most of the cloud certification subtests provide an immediate return status (Pass/Fail); however, some subtests may require detailed review by Red Hat to confirm success. Such tests are marked with REVIEW status in the Red Hat Certification application.

Some tests may also identify a potential issue and return a WARN status. This status indicates that best practices have not been followed. Tests marked with the WARN status warrant attention or actions but do not prevent a certification from succeeding. Partners are recommended to review the output of such tests and perform appropriate actions based on the information contained within the warnings.

Additional resources

- For more information on running the tests, see [CCSP Certification Workflow Guide](#).

1.3. TEST SUITE VERSIONS

You must install the latest version of the certification tooling and use the latest workflow for the certification process. After a new version of the certification tooling is released, Red Hat supports the previous tooling and workflow for a period of 90 days post the release.

At the end of the 90 days period, test logs/results generated using the previous version(s) are automatically rejected and you are expected to regenerate the test logs/results using the latest tooling and workflow.

The latest version of the certification tooling and workflow is available (by default) via Red Hat Subscription Management and documented in the [CCSP Certification Workflow Guide](#).

1.4. SUPPORTED RHEL VERSION AND ARCHITECTURE

The certifications are supported on the following RHEL version and architecture.

RHEL version	Architecture
RHEL 9	<ul style="list-style-type: none"> ● 64-bit AMD and Intel ● 64-bit IBM Z ● 64-bit ARM ● Little endian IBM Power systems
RHEL 8	<ul style="list-style-type: none"> ● 64-bit AMD and Intel ● 64-bit IBM Z ● 64-bit ARM ● Little endian IBM Power systems
RHEL 7	<ul style="list-style-type: none"> ● 64-bit AMD and Intel ● Little endian IBM Power systems

For information about hypervisor support, see [Certified Guest Operating Systems in Red Hat OpenStack Platform, Red Hat Virtualization and OpenShift Virtualization](#).

1.5. UNDERSTAND PASSTHROUGH CERTIFICATIONS

A passthrough certification is used when the same image is provided as a copy of an existing certified cloud certification and is listed under a different image name.

You can create a passthrough regular or gold RHEL image from an originally certified regular or gold RHEL image.

The policy for submitting a passthrough image certification request requires you to:

- Ensure that the image is a duplicate of the original certified image except for the name which might be different.
- As with the original image certification, it is expected that a given running image does include a certain drift from the original static on-disk image file in the form of instance-type dependent configuration data.

CHAPTER 2. RED HAT CERTIFICATION SELF CHECK

2.1. RED HAT CERTIFICATION SELF CHECK (RHCERT/SELF CHECK) TEST

The Red Hat certification self check test also known as **rhcert/selfcheck** 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.

2.2. SYSTEM REPORT

The system report (sosreport) test, also known as **cloud/sosreport**, captures the basic sosreport.

Red Hat uses a tool called sos to collect the configuration and diagnostic information from a RHEL system, and to assist customers in troubleshooting their system and following recommended practices. The system report subtest ensures that the sos tool functions as expected on the image/system and captures a basic sosreport.

Success criteria

A basic sosreport can be captured on the image.

Additional resources

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

CHAPTER 3. SUPPORTABILITY TESTS

The Supportability tests, also known as **cloud/supportable**, ensure that the image is supportable by Red Hat. The test confirms that the image consists of Red Hat kernel and user space software, is run in a Red Hat supportable environment, and includes access to Red Hat updates and fixes.

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

3.1. LOG VERSIONS SUBTEST

The **log versions** subtest checks whether it can find the RHEL version and the kernel version that are installed on the host under test.

Success criteria

- The test successfully detects both the RHEL version and the kernel version.

3.2. 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?](#)

3.3. 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?](#)

3.4. 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 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](#) .

3.5. HYPERVISOR/PARTITIONING SUBTEST

The Hypervisor/Partitioning subtest confirms that the host architecture displayed in the RHEL image is supported by RHEL, the CCSP program, and the kernel. Currently, the CCSP image certification is supported for the following existing and upcoming RHEL versions and corresponding architectures:

- **RHEL 8 and 9:** x86_64, ppc64le, IBM Z
- **RHEL 7:** x86_64, ppc, ppc64, ppc64le

Success criteria

- The PASS scenarios for RHEL 8 and 9 are x86_64 on RHEL KVM, Nutanix, VMware, and HyperV. It also includes ppc64le on BareMetal, PowerVM, and RHV for Power.
- The PASS scenarios for RHEL 7 are x86_64 on RHEL KVM, Nutanix, VMware, and HyperV. It also includes ppc and ppc64 on PowerVM and ppc64le on BareMetal, PowerVM, and RHV for Power.

3.6. FILESYSTEM LAYOUT SUBTEST

The Filesystem Layout confirms that the type and minimum size of an image follow the guidelines for each RHEL release. This ensures that the image has a reasonable amount of space required to operate effectively, run applications, and install upgrades for customer use.

Success criteria

- **RHEL 8 and 9:** The root file system is 10 GB in size or larger. The boot file system is a 1GB xfs partition.
- **RHEL 7:** The root file system is a 10 GB ext4 or xfs partition, or larger.

3.7. 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](#)

3.8. SOFTWARE REPOSITORIES SUBTEST

Software repositories confirm that relevant Red Hat repositories are configured, and GPG keys are already imported on the image to avoid potential significant risks from unsupported content.

Red Hat provides core software packages/content in Red Hat official software repositories (included with attached subscriptions) which, are signed with GPG keys to ensure the authenticity of the distributed files. Software provided as part of these repositories is fully supported and reliable for customer production environments.

Repositories published but not supported by Red Hat, such as [EPEL](#) or the [RHEL Supplementary and Optional](#), and non-Red Hat repositories may be configured if they are necessary to enable the cloud environment. However, such repositories must be properly described and approved.

Success criteria

- Supported Red Hat repositories are configured.
- GPG keys for Red Hat repositories are already imported in the image.
- The valid repositories are Red Hat Update Infrastructure and Red Hat Satellite.
- RHEL 8 and AppStream repos must be enabled.
- Red Hat repositories configured on the image match the image content.
- Non-Red Hat repositories, if required, for proper operation of the cloud are configured and described.



NOTE

To verify Red Hat repositories, Partners must configure their base URL with either one of these keywords: *satellite*, *redhat.com*, or *rhui*.

Additional resources

- For more information, see [Production Support Scope of Coverage](#).

3.9. SOFTWARE CONTAINERS TEST

Software containers test verifies that containers on the RHEL cloud image are provided by Red Hat or Partners. It is expected that you can provide a reason if any non-RHT container exists.

Success criteria

- All the containers are supplied by Red Hat.
- The **podman** tool package is installed on the RHEL 8 and 9 image.
- The **registry.redhat.io** container registry is enabled on the RHEL image.

3.10. INSIGHTS SUBTEST

The Insights subtest verifies the **insights-client** rpm on RHEL 8 and 9.

Success criteria

- The **insights-client** rpm is installed on RHEL 8 and RHEL 9.

3.11. SOFTWARE MODULES TEST

The RHEL modularity feature is a collection of packages available on the system. The software modules test validates modules available on a RHEL 8 or RHEL 9 system.

Success criteria

The test fails if there are non-Red Hat software modules.

CHAPTER 4. OVERVIEW OF IMAGE CONFIGURATION

The Image Configuration tests, also known as **cloud/configuration**, confirm that the image is configured in accordance with Red Hat standards so that customers have a uniform and consistent experience across multiple cloud providers and images in an integrated environment.

The **cloud/configuration** test includes the following subtests:

4.1. DEFAULT SYSTEM LOGGING

Confirms the default system logging service (syslog) is configured to store the logs in the **/var/log/** directory of the image to allow quick issue resolution when needed.

Success criteria

Basic system logging is stored in **/var/log/** directory on the image.

4.2. NETWORK CONFIGURATION TEST

Network configuration confirms that the default firewall service (iptables) is running, port 22 is open with SSHD running, ports 80 and 443 are open or closed, and that all other ports are closed. This ensures that the image is protected from unauthorized access by default, with a known access configuration.

This also ensures that customers have SSH access to the image and are able to quickly deploy HTTP applications without additional configuration. The image may have other ports open if they are necessary for proper operation of the cloud infrastructure but such ports must be documented.

This test displays status (Pass) at runtime only if ports 22, 80 (optional), 443 (optional) are open on the image. If other ports are open, this test requests a description of the open ports for review at Red Hat to confirm success or failure.



NOTE

As part of the certification process, the Red Hat Certification application by default runs on port 8009. The Red Hat Certification application may also run on another open port during certification testing but it is recommended to open this port only during the testing and not as default in the configuration of an image.

Success criteria

- Depending on the RHEL version, ensure that the following services are enabled and running:

RHEL version	Services
RHEL 9	firewalld or nftables
RHEL 8.3 and later	firewalld or nftables
RHEL 8 to 8.2	firewalld and nftables or firewalld and iptables
RHEL 7	firewalld

- sshd is enabled and running on port 22 and is accessible
- Any other ports open are required for proper operation of the cloud infrastructure and are documented
- Red Hat Certification application is running on port 8009 (or another port as configured)
- All other ports are closed

**NOTE**

The httpd service is allowed but not required to be running on port 80 and/or port 443.

4.3. DEFAULT OS RUNLEVEL

Confirms that the current system runlevel is 3, 4, or 5. This subtest ensures that the image is operating in the desired mode/state with all the required system services (for example networking) running.

Success criteria

The current runlevel is 3, 4, or 5.

Additional resources

For more information about runlevels, see:

- **RHEL 9:** [Working with systemd targets.](#)
- **RHEL 8:** [Working with systemd targets.](#)
- **RHEL 7:** [Working with systemd targets.](#)

4.4. SYSTEM SERVICES

The system services confirms the root user can start and stop services on the system. This ensures that your customers who have system administration privileges can access/work with applications and services on the system and perform all the tasks which require administrative access in a seamless manner. The system services also ensures that there is no gap between the configured and actual state of the installed system services.

Success criteria

- The root user can start and stop system services provided by the Red Hat product.
- For all the installed system services, actual status should match to their configured status. For instance if the service is enabled then it should be in running state.

Additional resources

For more information about gaining the required privileges, see:

- **RHEL 9:** [Managing sudo access.](#)
- **RHEL 8:** [Managing sudo access.](#)

- **RHEL 7:** [Gaining privileges](#).

4.5. SUBSCRIPTION SERVICES

Confirms that the required Red Hat subscriptions are configured, available and working on the image and that the update mechanism is Red Hat Satellite or RHUI. This ensures that customers are able to obtain access to the packages and updates they need to support their applications through standard Red Hat package update or delivery mechanisms.

Success criteria

The image is configured and able to download, install, and upgrade a package from Red Hat Satellite or the RHUI subscription management services.

CHAPTER 5. OVERVIEW OF SECURITY PRACTICES

The Security Practices tests also known as **cloud/security** confirm that the image follows a minimum set of standard security practices. They also confirm (but do not require at this time) that the latest Red Hat security updates are installed.

The **cloud/security** test includes the following subtests:

5.1. PASSWORD CONFIGURATION TEST

The **password configuration** test checks that login authentication services are enabled on the HUT, and that the services are using the SHA512 encryption algorithm. The test ensures that the image uses the standard SHA512 encryption and decryption algorithm for optimal security.

For RHEL 7, the profile uses the **authconfig** utility. For RHEL 8 and 9, it uses the **authselect** utility.

Success criteria

- The SHA-512 encryption algorithm is enabled for system authentication.
- The test fails for RHEL 8 and RHEL 9 if the NIS, SSSD, or winbind services are not configured because these services support the SHA-512 algorithm.

5.2. RPM FRESHNESS

Confirms that all important and critical security errata released against Red Hat packages that are included in the image are installed. Red Hat encourages you to update and recertify their images whenever an errata is released. This test displays status (REVIEW) at runtime as it requires review at Red Hat to confirm success or failure.

Success criteria

All important and critical security errata released for installed Red Hat packages are current.

Additional resources

- For more information on Red Hat security ratings, refer to [Understanding Red Hat security ratings](#).

5.3. SELINUX ENFORCING SUBTEST

Security-Enhanced Linux (SELinux) Enforcing subtest confirms that SELinux is enabled and running in enforcing mode on the image.

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. It reduces vulnerability to privilege escalation attacks and limits the damage made during the configuration. If a process becomes compromised, the attacker only has access to the normal functions of that process, and to files the process has been configured to have access to.

Success criteria

SELinux is configured and running in enforcing mode on the image.

Additional resources

For more information about SELinux, see:

- **RHEL 9:** [Using SELinux](#).
- **RHEL 8:** [Using SELinux](#).
- **RHEL 7:** [SELinux Users and Administrators Guide](#).