Red Hat Certified Cloud and Service Provider Certification Policy Guide

For Use with Red Hat Certified Cloud and Service Provider 1.0
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. Last updated: June 28, 2021.
## Table of Contents

**PART I. 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** .................................................... 7
2.1. RED HAT CERTIFICATION SELF CHECK (RHCERT/SELFCHECK) TEST 7
2.2. SYSTEM REPORT 7

**CHAPTER 3. SUPPORTABILITY TESTS** ........................................................................ 8
3.1. LOG VERSIONS SUBTEST 8
3.2. KERNEL SUBTEST 8
3.3. KERNEL MODULES SUBTEST 8
3.4. HARDWARE HEALTH SUBTEST 9
3.5. HYPervisor/PARTITIONING SUBTEST 10
3.6. FILESYSTEM LAYOUT SUBTEST 10
3.7. INSTALLED RPMs SUBTEST 10
3.8. SOFTWARE REPOSITORIES SUBTEST 11
3.9. SOFTWARE CONTAINERS TEST 11
3.10. INSIGHTS SUBTEST 12
3.11. SOFTWARE MODULES TEST 12

**CHAPTER 4. OVERVIEW OF IMAGE CONFIGURATION** ................................................ 13
4.1. DEFAULT SYSTEM LOGGING 13
4.2. NETWORK CONFIGURATION TEST 13
4.3. DEFAULT OS RUNLEVEL 14
4.4. SYSTEM SERVICES 14
4.5. SUBSCRIPTION SERVICES 14

**CHAPTER 5. OVERVIEW OF SECURITY PRACTICES** ................................................... 16
5.1. PASSWORD CONFIGURATION TEST 16
5.2. RPM FRESHNESS 16
5.3. SELINUX ENFORCING SUBTEST 16
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 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.
<table>
<thead>
<tr>
<th>RHEL version</th>
<th>Architecture</th>
<th>Hypervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 8</td>
<td>x86_64</td>
<td>KVM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMWare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HyperV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RHEV</td>
</tr>
<tr>
<td></td>
<td>ppc64le</td>
<td></td>
</tr>
<tr>
<td></td>
<td>s390x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>aarch64</td>
<td></td>
</tr>
<tr>
<td>RHEL 7</td>
<td>x86_64</td>
<td>KVM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMWare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HyperV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RHEV</td>
</tr>
<tr>
<td></td>
<td>ppc64le</td>
<td></td>
</tr>
<tr>
<td>RHEL 6</td>
<td>x86_64</td>
<td>KVM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMWare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HyperV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RHEV</td>
</tr>
<tr>
<td></td>
<td>ppc64</td>
<td></td>
</tr>
</tbody>
</table>

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 pass-through RHEL images in any of the following ways:

- Create a pass-through gold image from an originally certified regular image
- Create a pass-through gold image from an originally certified gold image
• Create a pass-through regular image from an originally certified gold image

• Create a pass-through regular image from an originally certified regular image

The policy for submitting a pass-through 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/SELFCHECK) 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 verifies the version of Red Hat Enterprise Linux (RHEL) installed on the image.

3.2. 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?

3.3. 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?
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: 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.
  - RHEL 6: 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.
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 6: x86, x86_64, ppc, ppc64
- RHEL 7: x86_64, ppc, ppc64, ppc64le, and
- RHEL 8: x86_64, ppc64le, z/VM

Success criteria

- The PASS scenarios of hypervisor/partitioning for RHEL 6 is x86 (i386 packages with i686 kernel), and x86_64 on RHEL KVM, VMware, and HyperV. It also includes ppc and ppc64 on PowerVM
- The PASS scenarios of hypervisor/partitioning for RHEL 7 and RHEL 8 is x86_64 on RHEL KVM, VMware, and HyperV. It also includes ppc and ppc64 on PowerVM; ppc64le on BareMetal, PowerVM, and RHEV 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 6: The root file system for RHEL 6.x is 6GB or greater on an ext4 or ext3 formatted partition
- RHEL 7: The root file system for RHEL 7.x is 10GB or greater on an xfs or ext4 formatted partition
- RHEL 8: The root file system for RHEL 8.x is 10GB or greater, and the boot file system is 1GB or greater on an xfs formatted partition.

3.7. 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.

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 should be supplied by Red Hat.
- For RHEL 8 the container tool podman is a required package.
- Enable the required container registry registry.redhat.io.

3.10. INSIGHTS SUBTEST

The Insights subtest verifies the insights-client rpm for RHEL 8.

Success criteria

For RHEL 8 insights-client is a required package.

3.11. SOFTWARE MODULES TEST

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

- Ensure for the following RHEL versions subsequent services are enabled and running:
  - For RHEL 6 and RHEL 7, iptables and firewalld respectively
  - For RHEL 8.0-8.2, firewalld with nftables or iptables
  - For RHEL 8.3 and above, either firewalld or nftables
- ssdh 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 in RHEL 6, 7, and 8 versions see:

- RHEL 8 Configuring basic system settings: 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 on gaining the required privileges, see:
  - RHEL 6 Deployment Guide
  - RHEL 7 Deployment Guide
  - RHEL 8 Configuring Basic System Settings

### 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

This test checks the hashing algorithm that depends on certificates or SHA-512 algorithm for RHEL 6, 7, and 8 versions. For RHEL 6, and 7 versions the profile uses authconfig utility whereas for the RHEL 8 versions it uses authselect utility. The test ensures that the image follows standard encryption/decryption mechanisms for optimal security.

Success criteria

- Successful user authentication support certificates or SHA-512 algorithm for RHEL 6, 7, and 8 versions
- The test fails for RHEL 8 if either of the services NIS, SSSD, or winbind are not configured

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 on SELinux in RHEL, see:

- RHEL 6 Security Enhanced Linux
- RHEL 7 SELinux Users and Administrators Guide