Red Hat Certified Cloud and Service Provider Certification 1.0

Red Hat Certified Cloud and Service Provider Certification Policy Guide

For Use with Red Hat Certified Cloud and Service Provider 1.0

Last Updated: 2018-11-20

Red Hat Certified Cloud and Service Provider Certification 1.0 Red Hat Certified Cloud and Service Provider Certification Policy Guide

For Use with Red Hat Certified Cloud and Service Provider 1.0

Legal Notice

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.

Table of Contents

CHAPTER 1. INTRODUCTION

1.1. AUDIENCE

This document describes 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. USING CERTIFICATION TO 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. For more information on running the tests, refer to CCSP Certification User Guide.

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 action(s) but do not prevent a certification from succeeding. Partners are recommended to review the output of such tests and perform appropriate action(s) based on the information contained within the warnings.

1.3. TEST SUITE VERSIONS

Partners 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 partners 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 Workflow Guide.

CHAPTER 2. RED HAT CERTIFICATION SELF CHECK

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

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. SOSREPORT (SYSTEM REPORT)

The 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. For more information about sosreports, refer to https://access.redhat.com/solutions/3592

Success Criteria

A basic sosreport can be captured on the image.

NOTE

The SOSReport archives the output and can be used as a reference while debugging certification or any other system issues.

CHAPTER 3. SUPPORTABILITY

3.1. SUPPORTABILITY OVERVIEW

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:

3.2. KERNEL

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 + minor release. For more information on Red Hat Enterprise Linux Life Cycle and Kernel Versions, refer to 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.
- The running kernel is released by Red Hat for use with the RHEL version.
- The running kernel is not tainted.

3.3. KERNEL MODULES

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 (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 Red Hat and supported.

3.4. UNSUPPORTED HARDWARE

The Unsupported Hardware subtest confirms that the Red Hat kernel does not identify unsupported hardware. When the kernel identifies such hardware, it will either provide an unsupported hardware message in the system logs or trigger a kernel taint. This prevents customer production risks which arise from running Red Hat products on unsupported configurations and environments.

For a complete list of hardware certified for RHEL 6 and RHEL 7, see Red Hat Ecosystem Catalog.

Success Criteria:

The kernel does not identify unsupported hardware.

3.5. ARCHITECTURE

The Architecture 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 RHEL versions and corresponding architectures:

- RHEL 6: x86, x86_64, ppc, ppc64
- RHEL 7: x86_64, ppc, ppc64, ppc64le, and
- RHEL 8.0 Beta: x86_64, ppc64le

Success Criteria:

- The PASS scenarios of architecture/hypervisor 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 architecture/hypervisor for RHEL 7 and RHEL 8.0 Beta 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

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

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.

For more information on Red Hat support policies on third-party software, refer to https://access.redhat.com/support/offerings/production/soc.

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 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.

3.8. SOFTWARE REPOSITORIES

Confirms 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 authenticity of the distributed files. Software provided as part of these repositories is fully supported and reliable for customer production environments. For more information, refer to Production Support Scope of Coverage.

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 but they 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
- RHEL 8.0 Beta 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

3.9. SOFTWARE CONTAINERS

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

Success Criteria:

All the containers should be supplied by Red Hat

CHAPTER 4. IMAGE CONFIGURATION

4.1. IMAGE CONFIGURATION OVERVIEW

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:**

4.2. 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.

4.3. NETWORK CONFIGURATION

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 Beta, firewalld with nftables or iptables**
- **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.

4.4. 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.

For more information about runlevels in RHEL 6, 7, and 8.0 Beta see:

- RHEL 6 Deployment Guide: 12.1. Configuring the Default Runlevel
- RHEL 7 Systems Administrator's Guide: Working with systemd Targets
- RHEL 8.0 Beta Configuring and Maintaining: Working with systemd targets

Success Criteria:

The current runlevel is 3, 4, or 5.

4.5. 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.

For more information on gaining the required privileges, see:

- RHEL 6 Deployment Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/chap-Deployment_Guide-Gaining_Privileges.html
- RHEL 7 Deployment Guide: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/system_administrators_guide/#chap-Gaining_Privileges
- RHEL 8.0 Beta Configuring Basic System Settings: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8-beta/html-single/configuring_basic_system_settings/#managing-users-group-gui_managing-users-groups-permissions

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.

4.6. 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. SECURITY PRACTICES

5.1. SECURITY PRACTICES OVERVIEW

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:

5.2. PASSWORD CONFIGURATION

This test checks the hashing algorithm that depends on certificates or SHA-512 algorithm for RHEL 6, 7, and 8.0 Beta. For RHEL 6, and 7 the profile uses `authconfig` utility whereas for RHEL 8.0 Beta 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 8.0 Beta**
- **The test fails for RHEL 8.0 Beta if either of the services NIS, SSSD, or winbind are not configured**

5.3. 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 partners 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. For more information on Red Hat security ratings, refer to https://access.redhat.com/security/updates/classification.

Success Criteria:

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

5.4. SELINUX ENFORCING

Security-Enhanced Linux (SELinux) Enforcing subtest confirms that SELinux is enabled and running in enforcing mode on the image or is running in permissive mode. It is always recommended to run Enforcing mode on RHEL 6, 7, or 8.0 Beta

NOTE

If SELinux is running in Permissive mode, Partners will receive a Warning notification: "Run SELinux in Enforcing Mode."

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.

For more information on SELinux in RHEL, see:

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

Success Criteria:

SELinux is configured and running in enforcing mode (preferred) or permissive mode on the image.

CHAPTER 6. FINDING MORE INFORMATION

6.1. REFERENCES

For more information on Red Hat Certified Cloud and Service Provider Program or Red Hat Certified Cloud and Service Provider Certification, refer the following documents/pages.

- **Red Hat Connect for Business Partners**
- **Red Hat Certified Cloud and Service Provider Certification Policy Guide**
- **Red Hat Certified Cloud and Service Provider Certification Workflow Guide**