Red Hat Software Certification 2024

Red Hat Enterprise Linux Software Certification Policy Guide

For Use with Red Hat Enterprise Linux Software Certification

Last Updated: 2024-06-24

Red Hat Software Certification 2024 Red Hat Enterprise Linux Software Certification Policy Guide

For Use with Red Hat Enterprise Linux Software Certification

Legal Notice

Abstract

The Red Hat Enterprise Linux Software Policy Guide describes the technical and operational requirements to certify third-party products on systems and cloud environments running Red Hat Enterprise Linux (RHEL) 8 and 9. Version 9.0 and 8.80 updated May 28, 2024.

Table of Contents

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 THE RED HAT ENTERPRISE LINUX SOFTWARE CERTIFICATION

The Red Hat Enterprise Linux Software Certification Policy Guide describes the policy overview to certify third-party vendor products running on Red Hat Enterprise Linux (RHEL) 8 and 9.

This guide is intended for partners who want to offer their products for use with RHEL in a jointly supported customer environment. A strong working knowledge of RHEL is required.

1.1. CERTIFICATION PREREQUISITES

To start your certification journey, you must:

- Join the Red Hat Partner Connect program.
- Accept the standard Partner Agreements along with the terms and conditions specific to containerized software.
- Enter basic information about your company and the products you need to certify. Common information includes a product overview and links to supporting collateral such as product documentation, datasheets, or other relevant resources.
- Support RHEL as a platform for the product being certified and establish a support relationship with Red Hat. You can do this through the multi-vendor support network of TSANet, or through a custom support agreement.

Additional resources

- General Program Guide for Partners.

1.2. TEST SUITE LIFECYCLE

Use the latest version of the test suit to certify your products.

After the release of a new test suite version, Red Hat accepts test results generated with the earlier version of the suite for a period of 90 days. During this period, the Red Hat certification team may require you to run the tests with the latest version of the suite if they consider that it is more suitable for your certification project.

Additional resources

- Red Hat Certification test suite download link

1.3. RED HAT ENTERPRISE LINUX VERSIONS AND ARCHITECTURE

A Red Hat Enterprise Linux software certification is architecture-specific and does not carry over to any other architecture. You must certify your product on each version and architecture of RHEL that it supports.

The following table shows the RHEL versions, processor architectures, and hypervisor software that can you can combine in a certification:

RHEL version	Architecture	Hypervisor
• RHEL 8 • RHEL 9	• x86_64	• Kernel-based Virtual Machine (KVM) • VMWare • HyperV • Red Hat Virtualization (RHV)
	• ppc64le • s390x • aarch64	

Red Hat grants RHEL software certifications on specific RHEL 8 or RHEL 9 minor versions. The certification is valid for subsequent minor releases of RHEL if you follow the compatibility guidelines documented in the Red Hat Enterprise Linux: Application Compatibility Guide.

Red Hat recommends partners to retest their products with each new minor version of RHEL.

Additional resources

- Red Hat Enterprise Linux 8: Application Compatibility Guide
- Red Hat Enterprise Linux 9: Application Compatibility Guide

1.4. PARTNER'S PRODUCT VERSIONS

Red Hat grants RHEL software certifications to specific major releases of your product. You should run the certification tests on minor releases of the product to avoid functional regressions, but you do not need to certify the product again.

You must certify subsequent major releases of the product either as a new version of the existing product or as a new product entry.

It is your responsibility to decide which releases of their product are major and which releases are minor.

Additional resources

- Red Hat Enterprise Linux 8: Application Compatibility Guide
- Red Hat Enterprise Linux 9: Application Compatibility Guide

1.5. PACKAGING FORMAT

Products targeted for certification can use any packaging format provided it does not alter the RHEL platform in a way that impacts its support. Red Hat recommends that you use packaging formats compatible with the platform's native tools, such as containers and RPMs.

Any components packaged as containers must follow the requirements established in Container image requirements.

1.6. CATALOG ENTRIES

Red Hat expects that a RHEL software certification remains listed in the catalog until the end of support life for the certified RHEL version. However, Red Hat reserves the right to remove a catalog entry.

1.7. DISTRIBUTION OF CERTIFIED CONTAINER IMAGES

The Red Hat Container Certification program offers the following options for the distribution of certified container images:

- **Red Hat Container Registry**. Managed by Red Hat at no cost to partners. This option requires compliance with U.S. export control laws. For more information, see the Export compliance guide.
- **Non-Red Hat Container Registry**. For example, your own registry, or any public registry such as *Quay.io* and *Docker.io*.

CHAPTER 2. CONTAINER IMAGE REQUIREMENTS

Products packaged as containers must comply with the following requirements to ensure that container images are:

- Covered as part of the end-user Red Hat Enterprise Linux support subscription.
- Scanned to avoid introducing known security vulnerabilities in customer environments.

Additional resources

- Red Hat Container Support Policy

2.1. PLATFORM REQUIREMENTS

Requirement	Justification
Containers must be able to run by using Podman.	Allows the administrator to run and manage their containers by using an OCI-compatible, RHEL-integrated command. The **podman** command supports options similar to those found in the **docker** command.
Containers must be able to be started and stopped by using a Systemd unit file.	Allows an administrator to automatically start, stop, and check the status of their containers by using a standard RHEL command.

2.2. IMAGE CONTENT REQUIREMENTS

Requirement	Justification
Container images must declare a non-root user unless their functionality requires privileged access. To certify container images requiring *root* access, you must: - Include the requirement in the product documentation. - Indicate that the container requires privileged host-level access in the certification project settings. This setting is subject to Red Hat review. Test name: *RunAsNonRoot*	Ensures that containers do not run as the root user unless required. Images running as the root user can pose a security risk.

Requirement	Justification
Container images must use a Universal Base Image (UBI) provided by Red Hat. The version of the UBI base image must be supported on the RHEL version undergoing certification. For more information, see the Red Hat Enterpise Linux Container Compatibility Matrix. You can add additional RHEL packages to the UBI images, except for kernel packages. Test name: *BasedOnUbi*	Ensures that application runtime dependencies, such as operating system components and libraries, are covered under the customer's subscription.
Container images must not change content provided by Red Hat packages or layers except for files that both you or the customers can change, such as configuration files. Test name: *HasModifiedFiles*	Ensures that Red Hat does not deny support on the basis of unauthorized changes to Red Hat components.
Container images must contain a "licenses" directory. Use this directory to add files containing software terms and conditions for your product and any open source software included in the image. Test name: *HasLicense*	Ensures that customers are aware of the terms and conditions applicable to the software included in the image.
Uncompressed container images must have less than 40 layers. Test name: *LayerCountAcceptable*	Ensures that images run appropriately on containers. Too many layers could degrade the performance.
Container images must not include RHEL kernel packages. Test name: *HasNoProhibitedPackages*	Ensures compliance with RHEL redistribution rules for partners.
Container images must not contain Red hat components with identified important or critical vulnerabilities. Test name: *N/A*. The Red Hat Certification Service conducts this scan.	Ensures that customers are not exposed to known vulnerabilities.

Additional resources

- Red Hat Container Support Policy
- UBI FAQ's and licensing information
- UBI images, repositories, and package details

2.3. IMAGE METADATA REQUIREMENTS

Requirement	Justification
Container images must include the following labels: • **name**: Image Name • **vendor**: Company name • **version**: Version of the image • **release**: A number used to identify the specific build for this image • **summary**: A short overview of the application or component in this image • **description**: A long description of the application or component in this image Test name: *HasRequiredLabel*	Ensures that customers can obtain information about the image provider and the content of the images in a consistent way.
Container images must include a unique tag that is descriptive of the certified image. Red Hat recommends appending the image version and its build date or released date to the unique tag. Floating tags, such as **latest** although not adequate for certification, can be added to the image in addition to the descriptive tag. Test name: *HasUniqueTag*	Ensures that images can be uniquely identified.

Additional resources

- For more information about container images and Red Hat support, see Red Hat Container Support Policy.
- For more information about Red Hat base images, see Red Hat Enterprise Linux documentation .

2.4. IMAGE MAINTENANCE REQUIREMENTS

Partners are responsible for monitoring the health status of their certified containers. When an image rebuild is required because of new functionality or a security update, submit the updated container image for recertification and publication.

Partners must keep the application components up-to-date and rebuild their container images periodically.

CHAPTER 3. TEST ENVIRONMENT

The test environment is the platform where you run both the product undergoing certification and the certification tests. It must comply with the following requirements:

Requirement	Justification
Red Hat Enterprise Linux (RHEL) must be installed on a certified platform (hardware, hypervisor, or cloud instance).	Ensures that the underlying physical or virtual platform does not introduce issues that might impact testing.
The test environment must not make any modifications to RHEL kernel and user packages beyond those identified as acceptable configuration changes in the RHEL documentation. Any non-Red Hat kernel modules are subject to further inspection.	Changes to Red Hat components might impact supportability for our customers.
RHEL must not contain components with critical or important vulnerabilities.	Ensures that the product undergoing certification is compatible with the security updates that customers are expected to install in their environments.
SELinux must be enabled and running in enforcing mode.	Ensures that the product undergoing certification is compatible with the recommended security settings.
Red Hat Insights must be installed and running.	Ensures compatibility with the platform's solution for proactive risk management.

APPENDIX A. TESTS

The Red Hat Enterprise Linux software certification includes several tests and subtests described in the following sections. A certification might exit with one of the following statuses:

- **Pass**: All the subtests have passed and no further action is required.
- **Fail**: A critical subtest or check has not succeeded and requires a change before a certification can be achieved.
- **Review**: Additional detailed review is required by Red Hat to determine the status.
- **Warn**: One or more subtests did not follow best practices and require further action. However, the certification will succeed.
  Red Hat recommends that you review the output of all tests, perform appropriate actions, and re-run the test as appropriate.

The Red Hat Certification application plans the tests sequentially and writes a single log file each time you run the tests. Submit the log file to Red Hat for new certifications and recertifications.

For more information about the certification tool and how to run the tests, see the Red Hat Software Certification Workflow Guide.

Additional resources

- Red Hat Certification test suite download link

A.1. SELF CHECK TEST

The **self check** test verifies 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 installed certification software packages are supportable.

Success criteria

- The test environment includes all the packages required in the certification process and the packages have not been modified.

A.2. RPM TEST

The **RPM test** checks whether RPM-packaged products undergoing certification adhere to Red Hat's best practices for RPM packaging. This test is mandatory for products packaged as RPMs only.

The test includes the following subtests:

A.2.1. RPM provenance subtest

The **RPM provenance** subtest checks whether the origin of the RPM-packaged product undergoing certification and its dependencies can be tracked in accordance with Red Hat's best practices for RPM packaging.

Success criteria

- Non-Red Hat packages are identified as belonging to the product undergoing certification, or its dependencies.
- Files are tracked within the packages.

Additional resources

- Packaging and Distributing Software (RHEL 8)
- Packaging and Distributing Software (RHEL 9)

A.2.2. RPM version handling subtest

The **RPM version handling** subtest checks whether the RPM-packaged product undergoing certification and its dependencies are versioned in accordance with Red Hat's best practices for RPM packaging.

Success criteria

- Packages and changes to packages are versioned.

A.2.3. RPM dependency tracking subtest

The **RPM dependency tracking** subtest checks whether the RPM-packaged product undergoing certification and its dependencies are tracked in accordance with Red Hat's best practices for RPM dependency tracking.

Success criteria

- All dependencies are tracked.

A.3. SUPPORTABILITY TEST

The **supportability** test ensures that Red Hat can support Red Hat Enterprise Linux (RHEL) with the product undergoing certification as installed and running.

The software/supportable tests include the following subtests:

A.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.

A.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?

A.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?

A.3.4. Third-party kernel modules subtest

The **third-party kernel** subtest checks whether non-Red Hat kernel packages are running.

The use of partner kernel modules has the potential to introduce risks to the Red Hat kernel that may not be fully ascertained during certification. As a result, when partner kernel modules are required, the certification process aims to ensure that the stack remains supportable, and the partner's responsibilities are clearly delineated.

Red Hat reserves the right to deny a certification whenever partner kernel modules are required. Partner kernel modules are subject to additional verification, including (but not limited to) the following:

Success criteria

- Partners must:
  - Agree that you understand and will act according to the policies defined in Red Hat's production scope of coverage.
  - Agree that you understand and will act according to the policies defined in Red Hat's third party support policy.
  - Provide Red Hat the documentation of kernel modules written for joint customers.

    - Provide Red Hat the contact information of your application support team and kernel engineering support team
    - Declare that you own and support the module.
    - Declare that module will not interfere with the RHEL kernel or userland functionality.
    - Declare that module is not a hardware driver.
- Partner kernel modules must:
    - Show the module name, size, and dependencies in the output of the **lsmod** command.
    - Show the module name, filename, license, and description in the output of the **modinfo** command, aligned with the partner documentation.
    - Show that the partner signs and supports the module in the output of the **modinfo** command.
    - Be precompiled **ko** or **ko.xz kmods**.
    - Be loaded after the final **pivot_root**.
    - Be delivered and packaged in an RPM or other format that is signed by the partner. It must also provide a mechanism to validate both the in-memory and on-disk kernel module.
- If delivered and packaged as an RPM, partner kernel modules must:
    - Meet the standard RHEL RPM certification requirements.
    - Show that the package's vendor is responsible for its support in the output of the **rpm -qi** command.
    - Show the supported Red Hat kernel range for the kernel modules in the output of the **rpm -q --requires** command.

A.3.5. 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 RHEL kernel does not identify hardware as unsupported. When the kernel identifies unsupported hardware, it displays a message similar to "unsupported hardware" in the system logs and triggers an unsupported kernel taint. This subtest mitigates the risk of 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.
- Checks that the host under test meets the minimum hardware requirements:
    - RHEL 8 and RHEL 9: Minimum system RAM must be 1.5GB by CPU logical core count.
- Checks if the kernel has reported any known hardware vulnerabilities.
- Confirms that no CPUs are offline in the system.
- Confirms if simultaneous multithreading is available, enabled, and active in the system.

Failing any of these tests will result in a warning from the test suite. Check the warnings to ensure the product is working as intended.

Success criteria

- The kernel does not have the UNSUPPORTEDHARDWARE taint bit set.
- The kernel does not report an unsupported hardware system message.
- The kernel does not report any vulnerabilities.
- 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 7 but removed from RHEL 8
- Hardware support available in RHEL 8 but removed from RHEL 9

A.3.6. Hypervisor/Partitioning subtest

The **hypervisor/partitioning** subtest verifies that the architecture of the host under test is supported by RHEL.

Success criteria

- The pass scenarios on bare-metal systems are: x86_64, ppc64le, s390x, and aarch64.
- The pass scenarios on hypervisor or partitioning environments are: RHEL KVM, VMware, RHEV, QEMU, and HyperV.

A.3.7. Filesystem layout subtest

The **filesystem layout** subtest verifies that the size of the root filesystem and the size and type of the boot filesystem 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 updates.

Success criteria

- RHEL 8 and RHEL 9:
  - The root file system is 10GB or larger.
  - The boot file system is 1GB or larger, and on an **xfs** or **ext** formatted partition.

A.3.8. 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

A.3.9. Software repositories subtest

The **software repositories** subtest verifies that relevant Red Hat repositories are configured, and that GPG keys are imported on the host under test.

Red Hat provides software packages and content in the Red Hat official software repositories. These repositories are signed with GPG keys to ensure authenticity of the distributed files. Software provided in these repositories is fully supported and reliable for customer production environments.

You might configure Non-Red Hat repositories if they are necessary, but they must be properly documented and approved.

Success criteria

- You enabled the BaseOS and AppStream RHEL repositories.
- You imported the GPG keys for the RHEL repositories.
- The relevant Red Hat repositories are: Red Hat Update Infrastructure, Red Hat Satellite, and Red Hat Content Delivery Network.
- You documented the non-Red Hat repositories required by the product undergoing certification, or by the certified Red Hat public cloud where you are running the tests.

NOTE

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

Additional resources

- Production Support Scope of Coverage

A.3.10. Trusted containers subtest

The **trusted containers** subtest verifies that the RHEL container tool set is installed, and that any containers installed on the host under test are either provided by Red Hat or are part of the product undergoing certification.

Success criteria

- The RHEL container tool set is installed and operational.
- Any containers present in the environment are supplied as part of a RHEL subscription or have been verified as part of the product certification.
- The default RHEL container registry, **registry.redhat.io**, is enabled.

Additional resources

- Building, running, and managing containers (RHEL 8)
- Building, running, and managing containers (RHEL 9)

A.3.11. Insights subtest

The **insights** subtest verifies that the insights-client package is installed and operational.

Red Hat Insights lets customers predict and prevent problems before they occur through ongoing, in-depth analysis of their infrastructure. Red Hat recommends customers to use Red Hat Insights in their own environments.

Success criteria

- The **insights-client** package is installed and operational.

Additional resources

- Red Hat Insights

A.3.12. RPM freshness subtest

The **RPM freshness** subtest checks whether all important and critical security updates released against Red Hat packages are installed, and displays a review status for those packages that need updating. Red Hat will review the results of this test if important or critical updates are not installed.

Red Hat encourages partners to update their test environments whenever a security update is released.

Success criteria

- All important and critical security updates released for Red Hat packages are installed.

Additional resources

- Red Hat security ratings

A.3.13. SELinux enforcing subtest

The **Security-Enhanced Linux (SELinux) enforcing** subtest confirms that SELinux is enabled and running in enforcing mode on the host under test.

Success criteria

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

Additional resources

- Using SELinux (RHEL 8)
- Using SELinux (RHEL 9)

A.3.14. Software modules subtest

The **software modules** subtest validates modules available on RHEL systems. The RHEL modularity feature is a collection of packages available on the system.

Success criteria

- The subtest fails if non-Red Hat software modules are installed.

A.4. FINGERPRINTING TEST

The **fingerprinting** test captures the digital fingerprint of the product undergoing certification.

By using the output of the **ps** and **systemd** commands, the test detects services and processes related to the product undergoing certification and any non-Red Hat applications installed on the test system. Then, the test prompts you about the services and processes it has found.

Red Hat will use the test results to investigate customer-reported problems and redirect them to the appropriate teams.

Success criteria

- The product undergoing certification is installed and running on the host under test.

A.5. CONTAINER TEST

The **container** test verifies that the container undergoing certification can be started and then stopped by using Podman and Systemd. This test is mandatory for containerized products only.

The test includes the following subtests:

A.5.1. Podman subtest

The **podman** subtest checks whether the container can be started and then stopped by using Podman.

The subtest performs the following actions:

- Displays a list of the containers running on the test system.
- Prompts you to identify the container undergoing certification.
- Starts and then stops the container by using the **podman** command.

Success criteria

Containers must start and stop successfully by using the **podman** command.

A.5.2. Systemd subtest

The **systemd** subtest checks whether the container can be controlled with Systemd and automatically restarted after a container failure.

The subtest performs the following actions:

- Prompts you to confirm whether a Systemd unit file for the container exists.
  If the file exists, enter its location. The test will use this file to start and stop the container.

  If the file does not exist, the test can generate one in **/etc/systemd/system**. Ensure that the container is running before letting the test create the file.
- Stops the container if it is running.
- Checks that the container can be controlled by **systemd**.
- Verifies that the container is set to restart on failure.
- Stops the container using the **podman kill** command to simulate failure.
- Verifies that the container automatically restarts.

Success criteria

- Containers must start successfully during all the tests.

Additional resources

- Generating a Systemd unit file using Podman (RHEL 8)
- Generating a Systemd unit file using Podman (RHEL 9)

A.6. SOSREPORT TEST

The **sosreport** test ensures that the sosreport tool works as expected on the test environment and captures a basic system report test.

The sosreport tool collects configuration and diagnostic information that Red Hat can use to assist customers in troubleshooting issues.

Success criteria

- A basic **sosreport** can be collected on the host under test.

Additional resources

- What is an sosreport and how to create one in Red Hat Enterprise Linux?