Red Hat Software Suite 7.29

Red Hat Enterprise Linux Software Certification Policy Guide

For Use with Red Hat Enterprise Linux Software Certification Policy Guide

Last Updated: 2021-06-15

Red Hat Software Suite 7.29 Red Hat Enterprise Linux Software Certification Policy Guide

For Use with Red Hat Enterprise Linux Software Certification Policy Guide

Legal Notice

Abstract

This document describes the technical and operational certification requirements for Red Hat Partners who want to offer their own non-containerized software for use on systems and cloud environments running Red Hat Enterprise Linux (RHEL) 8. Last updated: Mar 22, 2021.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

CHAPTER 1. INTRODUCTION

1.1. AUDIENCE

Independent Software Vendors (ISV) who want to understand the requirements and obligations of certifying non-containerized software for use on Red Hat Enterprise Linux (RHEL) 8.

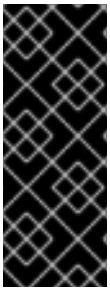
1.2. SOFTWARE CERTIFICATION PROCESS OVERVIEW

The software certification process includes three primary steps- 1) Certification on-boarding, 2) Certification testing, and 3) Publishing a Red Hat Ecosystem Catalog certified listing.

Red Hat Enterprise Linux Software Certification Workflow Guide **must be followed** as it covers the step by step process of the following high level procedure summary.

High level procedure summary

1. **Certification on-boarding**
    a. Partner joins the Red Hat Connect for Technology Partner Program.
    b. Partner accesses the Red Hat Enterprise Linux Zone.
    c. Partner adds a product to be certified.
    d. Partner joins TSANet.org joint support program.
2. **Certification testing**
    a. Partner creates a certification project.
    b. Partner completes the certification checklist and the application profile.
        i. Partner confirms the membership in TSANet.org.
        ii. Partner provides evidence that the product is a commercially supported General Available (GA) release.
    c. Partner downloads the certification test suite.
    d. Partner executes the certification test suite.
    e. Partner submits the certification test suite results.
    f. Red Hat reviews, rules and provides feedback on the test suite results.
3. **Publishing a Red Hat Ecosystem Catalog certified listing**
    a. Red Hat will authorize the listing once the certification is completed.



IMPORTANT

The Red Hat Enterprise Linux software certification does not conduct any explicit testing of the Partner's product, in how it functions or performs outside of its impact on the Red Hat Enterprise Linux (RHEL) platform on which it was installed and executed.

Any and all aspects of the certification candidate product's quality assurance remains the Partner's sole responsibility.

Additional resources

- Red Hat Enterprise Linux Application Workflow Guide
- Red Hat Partner Connect
- Red Hat Enterprise Linux Zone
- TSANet
- Red Hat Ecosystem Catalog

CHAPTER 2. CREATING VALUE FOR OUR JOINT CUSTOMERS

The certification process includes a series of tests that provide your Red Hat customers an assurance that they will have a consistent experience when your application is deployed across different Red Hat Enterprise Linux (RHEL) 8 environments and footprints.

Partners are expected to have entered into certifications in good faith and for the interest of our joint customers. Customers will also have the confidence that their deployments are jointly supported by Red Hat and your organization ensuring the customer's experience comes with the highest level of support.

CHAPTER 3. CERTIFICATION LIFECYCLE

A Red Hat Enterprise Linux software certification covers a range of Red Hat Enterprise Linux (RHEL) 8 minor versions and RHEL application minor versions on a single architecture and is expected to be maintained once certified to ensure the continued success of our joint customers.

3.1. RED HAT CERTIFICATION TEST SUITE LIFE CYCLE AND POLICY UPDATE

Red Hat supports previous versions of the Red Hat Certification test suite and workflow for a maximum period of 90 days from the release date of the current version.

At the end of the 90 days period, test logs and results generated using the previous versions are automatically rejected and partners are expected to regenerate the test logs and results using the latest tooling and workflow.

The latest version of the certification tooling and workflow is available via the Red Hat Software Download Center.

Additional resources

- Red Hat Certification test suite download link

3.2. RED HAT ENTERPRISE LINUX 8 VERSIONS

A Red Hat Enterprise Linux (RHEL) 8 software certification is granted on a specific RHEL 8 minor version and is valid for each subsequent minor release of RHEL 8 when the compatibility guidelines are followed.

The compatibility guidelines are documented in the Red Hat Enterprise Linux 8: Application Compatibility Guide. Red Hat recommends Partners to retest their application with each new minor versions of RHEL 8.

Additional resources

- Red Hat Enterprise Linux 8: Application Compatibility Guide

3.3. VENDOR'S PRODUCT VERSIONS

A Red Hat Enterprise Linux (RHEL) 8 software certification is awarded for a given major release of the application. Minor releases of the software are expected to be retested for any regressions that would negatively impact the certification but are not required to be re-certified.

Partners are encouraged to provide customers a matrix of supported and tested application minor releases to RHEL 8 minor releases for clarity.

A new certification is required for major versions of the application. Partners are expected to recertify new major versions of their application either as a new version of the existing product or as a new product entry. It is the partner's responsibility to decide which releases of their product are major versus which releases are minor.

Additional resources

- Red Hat Enterprise Linux 8: Application Compatibility Guide

3.4. ARCHITECTURE

A Red Hat Enterprise Linux (RHEL) 8 software certification is architecture specific and does not carry over to any other architecture. Partners are required to certify on each architecture of RHEL 8 that their application supports.

3.4.1. Supported RHEL version and architecture

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

RHEL version	Architecture	Hypervisor
RHEL 8	• x86_64	• KVM • VMWare • HyperV • RHEV
	• ppc64le • s390x • aarch64	

3.5. CATALOG ENTRIES

A Red Hat Enterprise Linux (RHEL) 8 software certification is expected to remain listed in the catalog until the end of Red Hat service and support for RHEL 8. However, Red Hat reserves the right to remove a catalog entry.

CHAPTER 4. TEST ENVIRONMENT POLICIES

A proper test environment supports execution of your software on a supported platform running Red Hat Enterprise Linux (RHEL) 8. Red Hat recommends the platform should already be certified for RHEL 8 to avoid discovering problems with uncertified platforms and unsupported hardware. Certified platforms can be found in the Red Hat Ecosystem Catalog.

The platform may be any of the four supported footprints - bare metal, virtual machine, private cloud, or public cloud. It is recommended to follow the platform providers procedures for deploying RHEL 8 to avoid platform issues and ensure a successful certification.

Additional resources

- Red Hat Enterprise Linux Application Workflow Guide

4.1. RED HAT CERTIFICATION TESTS OVERVIEW

The Red Hat Enterprise software certification includes three primary tests - selfcheck, supportable, and system report with a series of subtests and checks. A certification may 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.

Partners are recommended to review the output of all tests, perform appropriate actions, and re-run the test as appropriate.

CHAPTER 5. TESTING REQUIREMENTS

The testing requirements include execution of the **redhat-certification-software** test suite, including all of the tests described in the following sections. The execution of the test suite happens in a single sequential session orchestrated by the **redhat-certification** application. The test execution is to be conducted while the software to be certified is running or the results will be rejected.

This test run provides a certification test result in a single file, which is provided to Red Hat. The file includes results for the following tests:

- rhcert/self check,
- rpm validation tests,
- sosreport, and
- supportability tests.

Additional resources

- Red Hat Certification test suite download link

5.1. 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 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.

5.2. RPM TEST

The RPM test is also known as software/rpm. The test validates that a packaged rpm software under test adheres to Red Hat's best practices for RPM packaging. If the software product under test is packaged as an RPM the subsequent subtests will be executed.

It is not a requirement for Red Hat Enterprise Linux software certification to package as an RPM, nor that the packaged RPM subtests should undergo PASS results.

The software/rpm test includes the following subtests:

5.2.1. RPM provenance

The RPM provenance subtest verifies if RPM packaged software under test and its RPM packaged dependencies have identifiable provenance in accordance with Red Hat's best practices for RPM packaging.

Success Criteria

- Non Red Hat packages are identified as the software product under test or dependencies of the software product under test.

- Files are tracked within the packages

Additional resources

- Packaging and Distributing Software

5.2.2. RPM version handling

The RPM version handling subtest verifies if the RPM packaged software product under test and it's RPM packaged dependencies are versioned in accordance with Red Hat's best practices for RPM packaging.

Success Criteria

- Packages and changes to packages are versioned

5.2.3. RPM dependency tracking

The RPM dependency tracking subtest verifies if the RPM packaged software product under test and its dependencies are tracked with validity in accordance with Red Hat's best practices for RPM dependency tracking.

- Success Criteria*
- All dependencies are validly tracked.

5.3. SUPPORTABILITY

The Supportability tests, also known as **software/supportable**, ensures that the Red Hat Enterprise Linux (RHEL) remains supportable by Red Hat with the software to be certified installed and running.

The software/supportable tests include the following subtests:

5.3.1. Log versions

The Log versions subtest verifies the version of Red Hat Enterprise Linux (RHEL) installed on the image.

5.3.2. Kernel

The Kernel subtest confirms the kernel that the image is running is from Red Hat, is appropriate and supports the RHEL version that is 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.

The 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 RHEL 8.
- The running kernel is not tainted.

Additional resources

- Red Hat Enterprise Linux Life Cycle
- Red Hat Enterprise Linux Kernel Versions
- Why is the kernel "tainted" and how are the taint values deciphered?

5.3.3. 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. The kernel module subtest also ensures the kernel modules do not identify as a Technology Preview and does not identify as having triggered a slow path in the kernel.

Success Criteria

- The kernel modules are from Red Hat and supported.

5.3.4. Third-party kernel modules

The use of third-party 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 third party kernel modules are required certification aims to establish a mutual understanding of and the ability to convey ownership and responsibility of support as to facilitate resolution of customer issues. Red Hat reserves the right to deny a certification whenever third-party kernel modules are required. Third-party kernel modules, if required, are subject to additional verification included but not limited to the following:

Success Criteria

- Partner must ensure that they perform the following tasks:
  - 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 your ownership and support to the module
  - Declare that module will not interfere with the Red Hat Enterprise Linux kernel or **userland** functionality
  - Declare that module is not a hardware driver
- Third-party kernel module must:
  - Show the module name, size, and dependencies in the **lsmod** command output
  - Show the module name, filename, license, and description in the **modinfo** command output, aligned with the partner documentation

- Show that the module is signed and supported by you in the **modinfo** output
- 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 and provides a mechanism to validate both the in-memory and on-disk kernel module
  If delivered and packaged in an RPM, then ensure that the RPM:
  - Meets the standard RHEL 8 RPM certification requirements
  - Shows a description that clearly defines the ownership and support of the included modules is the vendor's responsibility in **rpm -qi** output
  - Shows the supported Red Hat kernel range for the kernel modules in **rpm -q --requires** output

5.3.5. Hardware Health

The Hardware Health subtest checks the system's health by testing if the hardware is supported, meets the requirements, and has any known hardware vulnerabilities. The subtest does the following:

- Checks that the Red Hat Enterprise Linux (RHEL) kernel does not identify hardware as unsupported. When the kernel identifies unsupported hardware, it will display an unsupported hardware message in the system logs and/or trigger an unsupported kernel taint. This subtest prevents customers from possible production risks which may arise from running Red Hat products on unsupported configurations and environments.
  In hypervisor, partitioning, cloud instances, and other virtual machine situations, the kernel may trigger an unsupported hardware message or taint based on the hardware data presented to RHEL by the virtual machine (VM).

- Checks that the system under test (SUT) meets the minimum hardware requirements[1] as follows:
  - RHEL 8: Minimum system RAM should be 1.5GB, per CPU logical core count[2]
  - RHEL 7: Minimum system RAM should be 1GB, per CPU logical core count[3]

- Checks if the kernel has reported any known hardware vulnerabilities, if those vulnerabilities have mitigations and if those mitigations have resolved the vulnerability. Many mitigations are automatic to ensure that customers do not need to take active steps to resolve vulnerabilities. In some cases this is not possible; where most of these remaining cases require changes to the configuration of the system BIOS/firmware which may not be modifiable by customers in all situations.

- Confirms the system does not have any offline CPUs.

- Confirms if Simultaneous Multithreading (SMT) is available, enabled, and active in the system.

Failing any of these tests will result in a WARN from the test suite and should be verified by the partner to have correct and intended behavior.

Success Criteria:

- The kernel does not have the UNSUPPORTEDHARDWARE taint bit set.

- The kernel does not report an unsupported hardware system message.
- The kernel should not report any vulnerabilities with mitigations as vulnerable.
- The kernel does not report the logic core to installed memory ratio as out of range.
- The kernel does not report CPUs in an offline state.

5.3.6. Hypervisor/Partitioning

The Hypervisor/Partitioning subtest confirms that the host architecture of the test environment is supported by Red Hat Enterprise Linux (RHEL) 8.

Success Criteria

- The PASS scenarios of hypervisor/partitioning on Baremetal for RHEL 8 is x86_64, ppc64le, s390x and aarch64.
- The PASS scenarios of hypervisor/partitioning is x86_64 on, RHEL KVM, VMware, RHEV, QEMU, and HyperV.

5.3.7. 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 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 or ext formatted partition.

5.3.8. Installed Red Hat rpms

The Installed Red Hat rpms confirms that RPM packages installed on the system from Red Hat are from the Red Hat Enterprise Linux (RHEL) 8 baseOS and application stream (AppStream) modules, and are not modified.

Non-Red Hat packages may be installed if they are necessary to enable the application, where they are documented, and if they DO NOT modify or conflict with Red Hat packages/software. Red Hat performs a detailed review after the test results are submitted to Red Hat to confirm success or failure when non Red Hat packages are installed.

Success Criteria

- The installed Red Hat rpm packages are from RHEL 8.
- The installed Red Hat rpm packages are not modified.
- The installed non-Red Hat rpm packages are the application or are necessary to enable the application and are documented for joint customers as such.
- 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

- Red Hat support policies on third-party software

5.3.9. Software repositories

Software repositories confirms that relevant Red Hat repositories are configured and GPG keys are imported on the environment under test to avoid potential significant risks from customers being unable to upgrade their Red Hat Enterprise Linux (RHEL) 8 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.

Non-Red Hat repositories may be configured if they are necessary to enable the application but they must be properly described and approved.

Success Criteria

- RHEL 8 repositories - BaseOS and AppStream must be enabled
- GPG keys for RHEL 8 repositories are already imported in the environment
- The valid repositories are Red Hat Update Infrastructure, Red Hat Satellite, and Red Hat Content Delivery Network
- Configured non-Red Hat repositories are described and required for the proper operation or installation of the application to be certified
- Configured non-Red Hat repositories are required for the proper operation of the public cloud when testing is conducted on a Red Hat certified public cloud

Additional resources

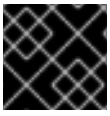
- Production Support Scope Coverage

5.3.10. Trusted containers

The trusted containers test verifies that any containers installed on the environment under test are known and provided by Red Hat Enterprise Linux (RHEL) 8. It is expected that customers maintain their ability to utilize containers on RHEL 8 in the presence of certified applications. You will be required to clarify the presence of any non RHEL 8 containers.

Success Criteria

- The RHEL 8 container tool set is installed and operational
- Any containers present in the environment are supplied as part of a RHEL 8 subscription
- The default RHEL 8 container registry **registry.redhat.io** is enabled



IMPORTANT

This program only certifies non-containerized applications for RHEL 8.

Additional resources

- Information on container tool set in RHEL8

5.3.11. Insights

Red Hat Insights gives customers the ability to predict and prevent problems before they occur through ongoing, in-depth analysis of their infrastructure. It is expected that customers maintainer their ability to utilize Red Hat Insights in the presence of certified applications. The Insights subtest verifies the insights-client rpm is installed and operational.

Success Criteria

- The insights-client package is installed and operational.

Additional Resources

- Red Hat Insights

5.3.12. RPM freshness

RPM freshness confirms that all important and critical security errata released against Red Hat packages are installed. Red Hat encourages partners to update their test environments whenever an errata is released. This test prompts partners to clarify, displays a status (REVIEW) status, and will require detailed review at Red Hat to confirm success or failure if important and critical security errata packages are not installed.

Success Criteria

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

Additional resources

- Red Hat security ratings

5.3.13. SELinux enforcing

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 (RHEL). SELinux policy is administratively-defined and enforced system-wide. SELinux reduces vulnerability to privilege escalation attacks and limits the damage made during configuration. If a process becomes compromised, the attacker only has access to the normal functions of that process and the files that process has been configured to have access to.

Success Criteria

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

Additional resources

- RHEL 8 SELinux

5.3.14. Software modules

Red Hat Enterprise Linux (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.

5.4. SYSTEM REPORT (SOSREPORT)

The sosreport test, also known as **software/sosreport**, captures a 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 environment under test and captures a basic sosreport.

Success Criteria

- A basic sosreport can be captured on the environment under test.

Additional resources

- sosreport article

---

[1] Minimum required memory

[2] For more information about hardware support available in RHEL 7 but removed from RHEL 8, see chapter Hardware Enablement in the *Considerations in Adopting Red Hat Enterprise Linux 8* document.

[3] For more information about hardware support available in RHEL 6 but removed from RHEL 7, see chapter Changes to Packages, Functionality, and Support in the *RHEL 7 Migration Planning Guide* document.