Red Hat

Reference

Red Hat Software Certification

October 21, 2026

Contents

1 Reference 4

Test environment 4

Tests 4

Self check test 5

RPM test 5

RPM provenance subtest 5

RPM version handling subtest 6

RPM dependency tracking subtest 6

Supportability test 6

Log versions subtest 6

Kernel subtest 7

Kernel modules subtest 7

Third-party kernel modules subtest 7

Hardware Health subtest 9

Hypervisor/Partitioning subtest 10

Filesystem layout subtest 10

Installed RPMs subtest 10

Software repositories subtest 11

Trusted containers subtest 12

Insights subtest 12

RPM freshness subtest 12

SELinux enforcing subtest 13

Software modules subtest 13

Fingerprinting test 13

Container test 13

Podman subtest 14

Systemd subtest 14

Sosreport test 14

Configuring the system and running tests by using Cockpit 15

Reference

Setting up the Cockpit server 15

Adding system under test to Cockpit 16

Getting authorization on the Red Hat SSO network 17

Downloading test plans in Cockpit from Red Hat certification portal 17

Using the test plan to prepare the system under test for testing 18

Running the certification tests using Cockpit 19

Reviewing and downloading the results file of the executed test plan 19

Submitting the test results from Cockpit to the Red Hat Certification Portal 20

1 Reference

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.
RHEL can be installed using either package mode or image mode.	Ensures that the certification test environment reflects a deployment method supported by the partner application.

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.

REFERENCE

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.

Related information
Red Hat Certification test suite download link

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.

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:

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.

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.

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.

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:

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.

REFERENCE

Kernel subtest

The **kernel** subtest checks the kernel 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.

Related information
Red Hat Enterprise Linux Life Cycle
Red Hat Enterprise Linux Release Dates
Why is the kernel "tainted" and how are the taint values deciphered?

Kernel modules subtest

The **kernel modules** subtest verifies that all loaded kernel modules are released and supported by Red Hat as part of the kernel package or a Driver Update.

The kernel module subtest also ensures that kernel modules are not unmaintained and do not identify as Technology Preview.

Success criteria

All loaded kernel modules are released, and supported by Red Hat.

Related information
What does a "Technology Preview" feature mean?

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.

REFERENCE

Related information
Red Hat's production scope of coverage
Red Hat's third party support policy

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 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 later: 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.

Related information
Minimum required memory

Hypervisor/Partitioning subtest

The **hypervisor/partitioning** subtest verifies that the architecture of the host under test is supported by Red Hat Enterprise Linux (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.

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 Red Hat Enterprise Linux (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 version 8 and later:
  - The root file system is 10GB or larger.
  - The boot file system is 1GB or larger, and on an `xfs` or `ext` formatted partition.

Installed RPMs subtest

The installed RPM subtest verifies that RPM packages installed on the system are released by Red Hat and not modified. Modified packages may introduce risks and affect environment supportability.

You might install non-Red Hat packages if necessary, but you must add them to your product documentation, and they must not modify or conflict with any Red Hat packages.

Red Hat reviews 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. For example, you may develop custom packages to manage CPU affinity of interrupt requests (IRQs) for network interfaces. However, such packages might conflict with Red Hat's tuned package, which already provides similar functionality for performance tuning.

Related information
Production Support Scope of Coverage

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*.

Related information
Production Support Scope of Coverage

REFERENCE

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.

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.

Related information
Red Hat Insights

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.

Related information

REFERENCE

Red Hat security ratings

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.

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.

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.

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:

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.

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.

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.

Related information
[What is an sosreport and how to create one in Red Hat Enterprise Linux?]

Configuring the system and running tests by using Cockpit

To run the certification tests by using Cockpit you need to upload the test plan to the SUT first. After running the tests, download the results and review them.

NOTE:
Although it is not mandatory, Red Hat recommends you to configure and use Cockpit for the certification process. Configuring cockpit greatly helps you to manage and monitor the certification process on the SUT.

Setting up the Cockpit server

Cockpit is a RHEL tool that lets you change the configuration of your systems as well as monitor their resources from a user-friendly web-based interface.

Before you begin

- The Cockpit server has RHEL version 8 or later installed.
- You have installed the Cockpit plugin on your system.
- You have enabled the Cockpit service.

NOTE:
- You must set up Cockpit either on the SUT or a new system.
- Ensure that the Cockpit has access to SUT.

Procedure

1. Log in to the system where you installed Cockpit.
2. Install the Cockpit RPM provided by the Red Hat Certification team.

```
# dnf install redhat-certification-cockpit
```

By default, Cockpit runs on port 9090.

Related information
Introducing Cockpit
Cockpit

Adding system under test to Cockpit

To enable passwordless SSH communication, add the system under test to Cockpit. This configuration establishes a secure connection for running certification tests.

Before you begin

- You have the IP address or hostname of the SUT.

Procedure

1. Enter **http://*Cockpit_system_IP*:9090/** in your browser to launch the Cockpit web application.
2. Enter the username and password, and then click **Login**.
3. Click the down-arrow on the logged-in cockpit user name → **Add new host**.

   The dialog box displays.
4. In the **Host** field, enter the IP address or hostname of the system.
5. In the **User name** field, enter the name you want to assign to this system.
6. Optional: Select the predefined color or select a new color of your choice for the host added.
7. Click **Add**.
8. Click **Accept key and connect** to let Cockpit communicate with the SUT through passwordless SSH.
9. Enter the **Password**.
10. Select the **Authorize SSH Key** checkbox and click **Log in**.

Result

On the left panel, click **Tools** → **Red Hat Certification**. Verify that the SUT you just added displays below the Hosts section on the right.

Getting authorization on the Red Hat SSO network

To establish connectivity with Red Hat, authorize the Cockpit web application on the Red Hat Single Sign-On network.

Procedure

1. Enter **http://<Cockpit_system_IP>:9090/** in your browser's address bar to launch the Cockpit web application.
2. Enter the username and password, and then click **Login**.
3. Select **Tools** → **Red Hat Certification** in the left panel.
4. On the Cockpit homepage, click **Authorize**, to establish connectivity with the Red Hat system.

   The **Log in to your Red Hat account** page displays.
5. Enter your credentials and click **Next**.

   The **Grant access to rhcert-cwe** page displays.
6. Click **Grant access**.

   A confirmation message displays a successful device login. You are now connected to the Cockpit web application.

Downloading test plans in Cockpit from Red Hat certification portal

To view the components evaluated during a test run, download the Red Hat certification test plan in Cockpit. This prepares the system for verification.

For Non-authorized or limited access users:

- To download the test plan, see *Downloading the test plan from Red Hat Certification portal*.

For authorized users:

Procedure

1. Enter **http://<Cockpit_system_IP>:9090/** in your browser's address bar to launch the Cockpit web application.
2. Enter the username and password, and then click **Login**.
3. Select **Tools** → **Red Hat Certification** in the left panel.
4. Click the **Test Plans** tab.

A list of **Recent Certification Support Cases** appears.

5. Click **Download Test Plan**.

   A message displays confirming the successful addition of the test plan.

6. Locate the downloaded test plan.

   The downloaded test plan is listed under the **File Name** of the **Test Plan Files** section.

Using the test plan to prepare the system under test for testing

To prepare your system under test (SUT) for certification, you must provision the host. You can use the Cockpit web interface to install required packages, establish SSH communication, and upload your final test plan.

Before you begin

You have downloaded the test plan provided by Red Hat. For more details, see *Downloading test plans in Cockpit*.
Provisioning the system under test (SUT) includes the following operations:

- setting up passwordless SSH communication with cockpit
- installing the required packages on your system based on the certification type
- creating a final test plan to run, which is a list of common tests taken from both the test plan provided by Red Hat and tests generated on discovering the system requirements.

For instance, required software packages will be installed if the test plan is designed for certifying a software product.

Procedure

1. Enter `http://cockpit_system_ip:9090/` in your browser address bar to launch the Cockpit web application.
2. Enter the username and password, and then click **Login**.
3. Select **Tools** → **Red Hat Certification** in the left panel.
4. Click the **Hosts** tab, and then click the host under test on which you want to run the tests.
5. Click **Provision**.

   A dialog box appears.

   a. Click **Upload**, and then select the new test plan .xml file. Then, click **Next**.

      A successful upload message is displayed.

      Optionally, if you want to reuse the previously uploaded test plan, then select it again to reupload.

> **NOTE:**
> During the certification process, if you receive a redesigned test plan for the ongoing product certification, then you can upload it following the previous step. However, you must run `rhcert-clean all` in the Terminal tab before proceeding.

b. In the **Role** field, select **System under test** and click **Submit**.

By default, the file is uploaded to path: `/var/rhcert/plans/<testplanfile.xml>`

Running the certification tests using Cockpit

Run certification tests on a prepared system under test by using the Cockpit web application.

Before you begin

- You have prepared the system under test.

Procedure

1. Enter **http://*Cockpit_system_IP*:9090/** in your browser address bar to launch the Cockpit web application.
2. Enter the username and password, and click **Login**.
3. Select **Tools** → **Red Hat Certification** in the left panel.
4. Click the **Hosts** tab and click on the host on which you want to run the tests.
5. Click the **Terminal** tab and select **Run**.

   A list of recommended tests based on the test plan uploaded displays. The final test plan to run is a list of common tests taken from both the test plan provided by Red Hat and tests generated on discovering the system requirements.
6. When prompted, choose whether to run each test by typing `yes` or `no`.

   You can also run particular tests from the list by typing `select`.

Reviewing and downloading the results file of the executed test plan

Review and download the results file of your executed test plan by using the Cockpit web application.

Procedure

1. Enter **http://*Cockpit_system_IP*:9090/** in your browser address bar to launch the Cockpit web application.
2. Enter the username and password, and then click **Login**.
3. Select **Tools** → **Red Hat Certification** in the left panel.
4. Click the **Result Files** tab to view the test results generated.
    a. Optional: Click **Preview** to view the results of each test.
    b. Click **Download** beside the result files.

    By default, the result file is saved as `/var/rhcert/save/hostname-date-time.xml`.

Submitting the test results from Cockpit to the Red Hat Certification Portal

You can submit the test results from Cockpit by using the Red Hat Certification Portal.

Procedure

1. Enter `http://<Cockpit_system_IP>:9090/` in your browser's address bar to launch the Cockpit web application.
2. Enter the username and password, and then click **Login**.
3. Select **Tools** → **Red Hat Certification** in the left panel.
4. Click the **Result Files** tab and select the case number from the displayed list.
    a. For the authorized users click **Submit**.

    A message displays confirming the successful upload of the test result file.
    b. For non-authorized users see *Uploading the results file of the executed test plan to Red Hat Certification portal*.

The test result file of the executed test plan will be uploaded to the Red Hat Certification portal.