Red Hat Certified Cloud and Service Provider Certification 2024

Red Hat Certified Cloud and Service Provider Certification for Red Hat Enterprise Linux for SAP Images Policy Guide

For Red Hat Enterprise Linux for SAP with HA and Update Services Cloud Images

Last Updated: 2024-03-08

Red Hat Certified Cloud and Service Provider Certification 2024 Red Hat Certified Cloud and Service Provider Certification for Red Hat Enterprise Linux for SAP Images Policy Guide

For Red Hat Enterprise Linux for SAP with HA and Update Services Cloud Images

Legal Notice

Abstract

This document describes the technical and operational certification requirements for CCSP Partners who want to offer RHEL for SAP with HA and Update Services. Version 8.75 updated February 14, 2024.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE 3

CHAPTER 1. INTRODUCTION TO RED HAT CERTIFIED CLOUD AND SERVICE PROVIDER CERTIFICATION FOR RED HAT ENTERPRISE LINUX FOR SAP IMAGES POLICIES 4
1.1. AUDIENCE 4
1.2. CREATE VALUE FOR OUR JOINT CUSTOMERS 4
1.3. ADDITIONAL RESOURCES 4

CHAPTER 2. TEST SUITE VERSIONS 5

CHAPTER 3. RED HAT CERTIFICATION SELF CHECK (RHCERT/SELFCHECK) 6

CHAPTER 4. OVERVIEW OF RED HAT CERTIFICATION TESTS 7
4.1. SYSTEM REPORT 7
4.2. SUPPORTABILITY 8
4.2.1. Log versions subtest 8
4.2.2. Kernel subtest 8
4.2.3. Kernel modules subtest 8
4.2.4. Hardware Health subtest 9
4.2.5. Hypervisor/Partitioning subtest 10
4.2.6. Filesystem Layout 10
4.2.7. Installed RPMs subtest 10
4.2.8. Software repositories 11
4.2.9. Package groups 13
4.2.10. Containers 13
4.2.11. Software modules 13
4.3. OVERVIEW OF IMAGE CONFIGURATION TEST 14
4.3.1. Default system logging 14
4.3.2. Network configuration subtest 14
4.3.3. Default OS Runlevel 15
4.3.4. System Services 15
4.3.5. Subscription services 16
4.3.6. Linux kernel parameters 16
4.3.7. Process resource limits 17
4.3.8. systemd-tmpfiles 17
4.3.9. SAP RPM Dependencies 17
4.3.10. System Roles 18
4.4. OVERVIEW OF SECURITY PRACTICES 18
4.4.1. Password configuration test 18
4.4.2. RPM freshness 19
4.4.3. SELinux 19

MAKING OPEN SOURCE MORE INCLUSIVE

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

CHAPTER 1. INTRODUCTION TO RED HAT CERTIFIED CLOUD AND SERVICE PROVIDER CERTIFICATION FOR RED HAT ENTERPRISE LINUX FOR SAP IMAGES POLICIES

1.1. AUDIENCE

Use this guide to understand the technical and operational certification requirements for CCSP Partners who want to offer Red Hat Enterprise Linux (RHEL) for SAP with High Availability and Update Services in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or a managed service offerings.

1.2. CREATE VALUE FOR OUR JOINT CUSTOMERS

As a Certified Cloud and Service Provider (CCSP), you are required to certify images that you publish in a catalog. The RHEL for SAP with High Availability and Update Services image certification process includes a series of tests that provide your Red Hat customers an assurance that they will have a consistent experience across cloud providers.

You 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 and good security practices.

1.3. ADDITIONAL RESOURCES

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

CHAPTER 2. TEST SUITE VERSIONS

You must install the latest version of the certification tooling and use the latest workflow for the certification process. After a new version of the certification tooling is released, Red Hat supports the previous tooling and workflow for a period of 90 days post the release.

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

The latest version of the certification tooling and workflow is available (by default) via Red Hat Subscription Management and documented in the CCSP Workflow Guide.

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

Table 2.1. Supported RHEL version and architecture

RHEL version	Architecture
RHEL 9	• 64-bit AMD and Intel • 64-bit IBM Z • 64-bit ARM • Little endian IBM Power systems
RHEL 8	• 64-bit AMD and Intel • 64-bit IBM Z • 64-bit ARM • Little endian IBM Power systems
RHEL 7	• 64-bit AMD and Intel • Little endian IBM Power systems

CHAPTER 3. 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.

Success criteria

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

CHAPTER 4. OVERVIEW OF RED HAT CERTIFICATION TESTS

The cloud certification test suite **redhat-certification-cloud-sap** includes four image tests:

- sosreport
- supportable
- configuration, and
- security

Each image tests consists of a series of subtests and checks. For more information on running the tests, see CCSP Certification Workflow Guide.

Logs from a singular run with all four of the image tests and the **rhcert/selfcheck** must be submitted to Red Hat for credit in all new certifications as well as recertifications.

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.

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

4.1. SYSTEM REPORT

The System report (sosreport) test, also known as **cloud-sap/sosreport**, captures the basic sosreport.

Red Hat provides and utilizes an essential tool called **sos** to collect the configuration and diagnostic information from a RHEL environmen to assist customers. SOS is pivotal in troubleshooting and verifying recommended practices. The system report subtest ensures that the sos tool functions as expected and necessary on the image. During this test a basic sosreport is created and captured.

Success criteria

A basic sosreport can be captured on the image.

NOTE

This SOSReport archives can also assist with debugging issues during the certification process.

Additional resources

- For more information about sos reports, see What is an sosreport and how to create one in Red Hat Enterprise Linux?

4.2. SUPPORTABILITY

The Supportability tests, also known as **cloud-sap/supportable**, checks if the image is run in a Red Hat supportable environment and includes at least a minimal install of RHEL. Additionally, the test checks if the image consists of Red Hat kernel and user space software, and has support for Red Hat updates and fixes.

The test includes the following subtests.

4.2.1. 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.

4.2.2. 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?

4.2.3. 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?

4.2.4. Hardware Health subtest

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

- Checks that the Red Hat Enterprise Linux (RHEL) kernel does not identify hardware as unsupported. When the kernel identifies unsupported hardware, it will display an unsupported hardware message in the system logs and/or trigger an unsupported kernel taint. This subtest prevents customers from possible production risks which may arise from running Red Hat products on unsupported configurations and environments.
  In hypervisor, partitioning, cloud instances, and other virtual machine situations, the kernel may trigger an unsupported hardware message or taint based on the hardware data presented to RHEL by the virtual machine (VM).
- Checks that the Host Under Test (HUT) meets the minimum hardware requirements.
  - RHEL 8 and 9: Minimum system RAM should be 1.5GB, per CPU logical core count.
  - RHEL 7: Minimum system RAM should be 1GB, per CPU logical core count.
- Checks if the kernel has reported any known hardware vulnerabilities, if those vulnerabilities have mitigations and if those mitigations have resolved the vulnerability. Many mitigations are automatic to ensure that customers do not need to take active steps to resolve vulnerabilities. In some cases this is not possible; where most of these remaining cases require changes to the configuration of the system BIOS/firmware which may not be modifiable by customers in all situations.
- Confirms the system does not have any offline CPUs.
- Confirms if Simultaneous Multithreading (SMT) is available, enabled, and active in the system.

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

Success criteria

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

Additional resources

- Minimum required memory
- Hardware support available in RHEL 8 but removed from RHEL 9 .
- Hardware support available in RHEL 7 but removed from RHEL 8 .

- Hardware support available in RHEL 6 but removed from RHEL 7 .

4.2.5. Hypervisor/Partitioning subtest

The Hypervisor/Partitioning subtest confirms that the host architecture and hardware partitioning in the RHEL image is supported by RHEL, the CCSP program, and the kernel. Currently, the CCSP image certification is supported for the following existing and upcoming RHEL versions and corresponding architectures:

- **RHEL 8 and 9**: x86_64, ppc64le, IBM Z
- **RHEL 7**: x86_64, ppc, ppc64, ppc64le

Success criteria

- The PASS scenarios for RHEL 8 and 9 are x86_64 on RHEL KVM, Nutanix, VMware, and HyperV. It also includes ppc64le on BareMetal, PowerVM, and RHV for Power.
- The PASS scenarios for RHEL 7 are x86_64 on RHEL KVM, Nutanix, VMware, and HyperV. It also includes ppc and ppc64 on PowerVM and ppc64le on BareMetal, PowerVM, and RHV for Power.

4.2.6. Filesystem Layout

The Filesystem Layout confirms that the filesystem type and the minimum partition size of the 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 and 9**: The root file system is 10 GB in size or larger. The boot file system is a 1GB xfs partition.
- **RHEL 7**: The root file system is a 10 GB ext4 or xfs partition, or larger.

4.2.7. 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

4.2.8. Software repositories

Software repositories confirm that relevant Red Hat repositories are configured, and GPG keys are already imported to avoid potentially significant risks from unsupported content.

Red Hat provides core software packages and 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 use in customer production environments.

Repositories published but not supported by Red Hat, such as EPEL or the RHEL Supplementary and Optional, and non-Red Hat repositories can be configured if they are necessary to enable the cloud environment and are properly documented and approved by Red Hat.

Success criteria

- Supported Red Hat repositories are configured.
- GPG keys for Red Hat repositories are imported in the image.
- Valid repositories are Red Hat Update Infrastructure or Red Hat Satellite:

  TIP

  Red Hat Update Infrastructure and Red Hat Satellite use the same repositories with different naming conventions:

  - Red Hat Satellite: *repository-name-rpms*
  - Red Hat Infrastructure: *repository-name-rhui-rpms*

  The following repositories are shown in the Red Hat Satellite naming convention:

  - **RHEL 9 for SAP with HA and US Repos**(E4S support)
    - rhel-9-for-x86_64-baseos-e4s-rpms
    - rhel-9-for-x86_64-appstream-e4s-rpms
    - rhel-9-for-x86_64-sap-solutions-e4s-rpms
    - rhel-9-for-x86_64-sap-netweaver-e4s-rpms
    - rhel-9-for-x86_64-highavailability-e4s-rpms
  - **RHEL 9 for SAP Applications Repos**(Microsoft Azure only, EUS support)
    - rhel-9-for-x86_64-baseos-eus-rpms
    - rhel-9-for-x86_64-appstream-eus-rpms
    - rhel-9-for-x86_64-sap-netweaver-eus-rpms
  - **RHEL 8 Repos** (E4S support)
    - rhel-8-for-x86_64-baseos-e4s-rpms

        - rhel-8-for-x86_64-appstream-e4s-rpms
        - rhel-8-for-x86_64-sap-solutions-e4s-rpms
        - rhel-8-for-x86_64-sap-netweaver-e4s-rpms
        - rhel-8-for-x86_64-highavailability-e4s-rpms
    - **RHEL 8 for SAP with HA and US Repos**(Microsoft Azure only, E4S support)
        - rhel-8-for-x86_64-baseos-e4s-rpms
        - rhel-8-for-x86_64-appstream-e4s-rpms
        - rhel-8-for-x86_64-sap-solutions-e4s-rpms
        - rhel-8-for-x86_64-sap-netweaver-e4s-rpms
        - rhel-8-for-x86_64-highavailability-e4s-rpms
    - **RHEL 8 for SAP Applications Repos**(Microsoft Azure only, EUS support)
        - rhel-8-for-x86_64-baseos-eus-rpms
        - rhel-8-for-x86_64-appstream-eus-rpms
        - rhel-8-for-x86_64-sap-netweaver-eus-rpms
    - **RHEL 7.5 Repos** (EUS support)
        - rhel-7-server-eus-rpms
        - rhel-sap-hana-for-rhel-7-server-eus-rpms
        - rhel-sap-for-rhel-7-server-eus-rpms
        - rhel-ha-for-rhel-7-server-eus-rpms
    - **RHEL 7.4, 7.6, 7.7 Repos** (E4S support)
        - rhel-7-server-e4s-rpms
        - rhel-sap-hana-for-rhel-7-server-e4s-rpms
        - rhel-sap-for-rhel-7-server-e4s-rpms
        - rhel-ha-for-rhel-7-server-e4s-rpms
    - **RHEL 7.9 Repos** (Check the Red Hat Enterprise Linux Life Cycle)
        - rhel-7-server-rpms
        - rhel-sap-hana-for-rhel-7-server-rpms
        - rhel-ha-for-rhel-7-server-rpms
        - rhel-sap-for-rhel-7-server-rpms
- Red Hat repositories configured on the image match the image content.

- Non-Red Hat repositories, if required, for proper operation of the cloud are configured and described.

NOTE

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

Additional resources

- For more information about Red Hat Enterprise Linux support dates, see Red Hat Enterprise Linux Life Cycle.
- For more information about what Red Hat supports, see Production Support Scope of Coverage.

4.2.9. Package groups

The Package groups test verifies that the base package groups of the RHEL cloud image are provided by Red Hat and that the correct minimum package groups are configured properly.

Success criteria

All package groups are recognized as RHEL package groups

4.2.10. Containers

RHEL supports customers who intend to adopt and use containers in the hybrid cloud.

The **software/container** test verifies:

- If the Red Hat container tools are installed. If they are not installed and are not part of the minimal RHEL installation, the test will confirm that the tool can be installed from the RHEL registry and can download and execute containers.
- If the containers on the RHEL cloud image are either provided by Red Hat or are Red Hat certified Partner containers. If you need to use any other container for your cloud operation, you must mention them in your documentation.

Success criteria

- All installed containers are either provided or certified by Red Hat.
- The **podman** tool is either already installed or can be installed during the test run. Installation is supported on RHEL 8 and 9 image.
- The **podman** tool can download and run a sample Red Hat container.
- The **registry.redhat.io** registry is either already enabled or enabled after podman is installed on the RHEL image.

4.2.11. Software modules

The RHEL modularity feature is a collection of packages available on the system. The software modules test validates modules available on a RHEL 8 or RHEL 9 system.

Success criteria

- The test fails if there are non-Red Hat software modules.

4.3. OVERVIEW OF IMAGE CONFIGURATION TEST

The Image Configuration tests, also known as **cloud-sap/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-sap/configuration** test includes the following subtests.

4.3.1. Default system logging

Confirms the default system logging service (syslog) is configured to store the logs in the **/var/log/** directory of the image to allow quick issue resolution when needed.

Success criteria

Basic system logging is stored in **/var/log/** directory on the image.

4.3.2. Network configuration subtest

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.

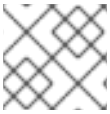
Success criteria

- Depending on the RHEL version, ensure that the following services are enabled and running:

RHEL version	Services
RHEL 9	**firewalld** or **nftables**
RHEL 8.3 and later	**firewalld** or **nftables**

RHEL version	Services
RHEL 8 to 8.2	**firewalld** and **nftables** or **firewalld** and **iptables**
RHEL 7	**firewalld**

- 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.

4.3.3. Default OS Runlevel

Confirms that the current system runlevel is 3, 4, or 5. This subtest ensures that the image is operating in the desired mode/state with all the required system services (for example networking) running.

Success criteria

The current runlevel is 3, 4, or 5.

Additional resources

For more information about runlevels, see:

- **RHEL 9**: Working with systemd targets.
- **RHEL 8**: Working with systemd targets.
- **RHEL 7**: Working with systemd targets.

4.3.4. System Services

The system services confirms the root user can start and stop services on the system. This ensures that your customers who have system administration privileges can access/work with applications and services on the system and perform all the tasks which require administrative access in a seamless manner. The system services also ensures that there is no gap between the configured and actual state of the installed system services.

Success criteria

- The root user can start and stop system services provided by the Red Hat product.
- The chronyd service is started and enabled and functional
- The uuidd service is started and enabled

- For all the installed system services, the service status should match to the configured status. For instance, if the service is enabled then it should be in running state.

Additional resources

For more information about gaining the required privileges, see:

- **RHEL 9**: Managing sudo access.
- **RHEL 8**: Managing sudo access.
- **RHEL 7**: Gaining privileges.

4.3.5. Subscription services

Confirms that the required Red Hat subscriptions are configured, available and working on the image and that the update mechanism is Red Hat Satellite or RHUI. This ensures that customers are able to obtain access to the packages and updates they need to support their applications through standard Red Hat package update or delivery mechanisms.

Success criteria

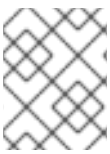
The image is configured and able to download, install, and upgrade a package from Red Hat Satellite or the RHUI subscription management services.

4.3.6. Linux kernel parameters

Confirms that the Linux kernel parameters are updated to appropriate configurations.

Success criteria

- Config file **/etc/sysctl.d/sap.conf** exists with the following:
  - RHEL 9:
    - vm.max_map_count = 2147483647
    - kernel.pid_max = 4194304
  - RHEL 8:
    - vm.max_map_count = 2147483647
    - kernel.pid_max = 4194304
  - RHEL 7:
    - vm.max_map_count = 2000000
    - kernel.sem = 1250 256000 100 1024



NOTE

The **vm.max_map_count** value for RHEL 7 is the minimum, higher values are also acceptable.

4.3.7. Process resource limits

Confirms that the system resource limiting is updated to appropriate configurations.

Success criteria

- Config file **/etc/security/limits.d/99-sap.conf** exists with the following:
  - @sapsys hard nofile 65536
  - @sapsys soft nofile 65536
  - @dba hard nofile 65536
  - @dba soft nofile 65536
  - @sapsys hard nproc unlimited
  - @sapsys soft nproc unlimited
  - @dba hard nproc unlimited
  - @dba soft nproc unlimited

4.3.8. systemd-tmpfiles

Confirms that the systemd-tmpfiles is updated to appropriate configurations.

Success criteria

- Config file **/etc/tmpfiles.d/sap.conf** exists with the following:
  - # systemd.tmpfiles exclude file for SAP
  - # SAP software stores some important files in /tmp which should not be deleted automatically.
  - # This file has been created using role sap-preconfigure in RHEL System Roles for SAP.
  - # Do not change this file as it might be overwritten when running role sap-preconfigure again.
  - # Exclude SAP socket and lock files
  - x /tmp/.sap*
  - # Exclude HANA lock file
  - x /tmp/.hdb*lock
  - # Exclude TREX lock file
  - x /tmp/.trex*lock

4.3.9. SAP RPM Dependencies

Confirms that the required RPM package dependencies for SAP are installed.

Success criteria

- The following packages are installed:
  - uuidd
  - libnsl
  - tcsh
  - psmisc
  - nfs-utils
  - Bind-utils
- RHEL 8.0:
  - setup-2.12.2-2.el8_0.1 (or later)
- RHEL 8.1:
  - setup-2.12.2-2.el8_1.1 (or later)

4.3.10. System Roles

Checks the availability of the RHEL System Roles for SAP and Ansible RPM packages. Also, the test runs an Ansible playbook to confirm system assertion role compliance.

Success criteria

- The latest version of the following RPMs is installed:
  - ansible-core
  - rhel-system-roles-sap
- The HUT has at least two Ansible roles configured.
- The test runs the Ansible playbook successfully.

4.4. OVERVIEW OF SECURITY PRACTICES

The Security Practices tests also known as **cloud-sap/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-sap/security** test includes the following subtests:

4.4.1. Password configuration test

The **password configuration** test checks that login authentication services are enabled on the HUT, and that the services are using the SHA512 encryption algorithm. The test ensures that the image uses the standard SHA512 encryption and decryption algorithm for optimal security.

For RHEL 7, the profile uses the **authconfig** utility. For RHEL 8 and 9, it uses the **authselect** utility.

Success criteria

- The SHA-512 encryption algorithm is enabled for system authentication.
- The test fails for RHEL 8 and RHEL 9 if the NIS, SSSD, or winbind services are not configured because these services support the SHA-512 algorithm.

4.4.2. RPM freshness

Confirms that all important and critical security errata released against Red Hat packages that are included in the image are installed. Red Hat encourages you to update and recertify their images whenever an errata is released. This test displays status (REVIEW) at runtime as it requires review at Red Hat to confirm success or failure.

Success criteria

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

Additional resources

- For more information on Red Hat security ratings, refer to Understanding Red Hat security ratings.

4.4.3. SELinux

Security-Enhanced Linux (SELinux) subtest confirms that SELinux is enabled and running in permissive or enforcing mode on the image.

SELinux adds Mandatory Access Control (MAC) to the Linux kernel, and is enabled by default in Red Hat Enterprise Linux. SELinux policy is administratively-defined, enforced system-wide, and is not set at user discretion. It reduces vulnerability to privilege escalation attacks and limits the damage made during the configuration. If a process becomes compromised, the attacker only has access to the normal functions of that process, and to files the process has been configured to have access to.

Success criteria

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

Additional resources

For more information about SELinux, see:

- **RHEL 9**: Using SElinux.
- **RHEL 8**: Using SElinux.
- **RHEL 7**: SELinux Users and Administrators Guide .