Red Hat Enterprise Linux 8

Upgrading from RHEL 7 to RHEL 8

Instructions for an in-place upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8

Last Updated: 2024-09-20

Red Hat Enterprise Linux 8 Upgrading from RHEL 7 to RHEL 8

Instructions for an in-place upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8

Legal Notice

Abstract

This document provides instructions on how to perform an in-place upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8 using the Leapp utility. During the in-place upgrade, the existing RHEL 7 operating system is replaced by a RHEL 8 version.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Let us know how we can improve it.

Submitting feedback through Jira (account required)

1. Log in to the Jira website.

2. Click **Create** in the top navigation bar.

3. Enter a descriptive title in the **Summary** field.

4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.

5. Click **Create** at the bottom of the dialogue.

KEY MIGRATION TERMINOLOGY

While the following migration terms are commonly used in the software industry, these definitions are specific to Red Hat Enterprise Linux (RHEL).

Update

Sometimes called a software patch, an update is an addition to the current version of the application, operating system, or software that you are running. A software update addresses any issues or bugs to provide a better experience of working with the technology. In RHEL, an update relates to a minor release, for example, updating from RHEL 8.1 to 8.2.

Upgrade

An upgrade is when you replace the application, operating system, or software that you are currently running with a newer version. Typically, you first back up your data according to instructions from Red Hat. When you upgrade RHEL, you have two options:

- **In-place upgrade:** During an in-place upgrade, you replace the earlier version with the new version without removing the earlier version first. The installed applications and utilities, along with the configurations and preferences, are incorporated into the new version.

- **Clean install:** A clean install removes all traces of the previously installed operating system, system data, configurations, and applications and installs the latest version of the operating system. A clean install is ideal if you do not need any of the previous data or applications on your systems or if you are developing a new project that does not rely on prior builds.

Operating system conversion

A conversion is when you convert your operating system from a different Linux distribution to Red Hat Enterprise Linux. Typically, you first back up your data according to instructions from Red Hat.

Migration

Typically, a migration indicates a change of platform: software or hardware. Moving from Windows to Linux is a migration. Moving a user from one laptop to another or a company from one server to another is a migration. However, most migrations also involve upgrades, and sometimes the terms are used interchangeably.

- **Migration to RHEL:** Conversion of an existing operating system to RHEL

- **Migration across RHEL:** Upgrade from one version of RHEL to another

CHAPTER 1. SUPPORTED UPGRADE PATHS

The in-place upgrade replaces the RHEL 7 operating system (OS) on your system with a RHEL 8 version.

Currently, it is possible to perform an in-place upgrade from RHEL 7 to the following target RHEL 8 minor versions:

Table 1.1. Supported upgrade paths

System configuration	Source OS version	Target OS version
RHEL	RHEL 7.9	RHEL 8.8
		RHEL 8.10 (default)
RHEL with SAP HANA	RHEL 7.9	RHEL 8.8 (default)
		RHEL 8.10

For more information about supported upgrade paths, see Supported in-place upgrade paths for Red Hat Enterprise Linux and the In-place upgrade Support Policy.

CHAPTER 2. OVERVIEW OF THE UPGRADE PROCESS

The in-place upgrade process from RHEL 7 to RHEL 8 can be summarized as follows:

1. **Plan the upgrade**
   Review the system requirements and limitations. Determine whether your system is a good candidate for an in-place upgrade, or if you should perform a clean install of RHEL 8 instead.

2. **Prepare for the upgrade**
   Complete required preparatory steps, including creating a backup of your RHEL 7 system, before beginning the upgrade process.

3. **Run and review the pre-upgrade report**
   Run the pre-upgrade utility to generate a report that summarizes potential problems that must be resolved before the upgrade. Depending on the severity and impact of the found problems and the amount of work required to resolve them, proceed with one of the following outcomes:

   - Remediate found problems and apply recommended solutions. Rerun the pre-upgrade utility to verify that all serious problems have been resolved. You might need to run the pre-upgrade report and resolve found issues multiple times before your system is ready for the upgrade.

   - Switch to a clean installation of RHEL 8 instead of proceeding with the in-place upgrade.

4. **Perform the in-place upgrade**
   Perform the upgrade to RHEL 8 and verify that the upgrade has been completed correctly. If the upgrade encounters issues that cannot be resolved, perform a rollback to your RHEL 7 backup.

5. **Perform post-upgrade steps**
   Perform required post-upgrade steps to ensure that the RHEL 8 system is properly set up.

CHAPTER 3. PLANNING AN UPGRADE

An in-place upgrade is the recommended and supported way to upgrade your system to the next major version of RHEL.

Consider the following before upgrading to RHEL 8:

- **Operating system** - The operating system is upgraded by the **Leapp** utility under the following conditions:

  - **RHEL 7.9** of the Server variant on the 64-bit Intel, IBM POWER 8 (little endian), and 64-bit IBM Z architectures and, when on SAP HANA, on the 64-bit Intel architecture, is installed. See Supported in-place upgrade paths for Red Hat Enterprise Linux for more information.

  - Minimum hardware requirements for RHEL 8 are met.

  - You have access to up-to-date RHEL 7.9 and the target operating system (OS) version (for example, RHEL 8.10) content. See Preparing a RHEL 7 system for the upgrade for more information.

- **Applications** - You can migrate applications installed on your system by using **Leapp**. However, in certain cases, you have to create custom actors, which specify actions to be performed by **Leapp** during the upgrade, for example, reconfiguring an application or installing a specific hardware driver. For more information, see Handling the migration of your custom and third-party applications. Note that Red Hat does not support custom actors.

- **Security** - You should evaluate this aspect before the upgrade and take additional steps when the upgrade process completes. Consider especially the following:

  - Before the upgrade, define the security standard your system needs to comply with and understand the security changes in RHEL 8 .

  - During the upgrade process, the **Leapp** utility sets SELinux mode to permissive.

  - In-place upgrades of systems in Federal Information Processing Standard (FIPS) mode cannot be fully automated by **Leapp**. If your scenario requires upgrading RHEL 7 systems running in **FIPS mode**, you must:

    > **IMPORTANT**
    >
    > To ensure that all cryptographic keys conform to the FIPS 140-2 standard, start a new installation in FIPS mode instead of performing an in-place upgrade of an already deployed system. Use the following steps only if the security policy of your company allows this alternative upgrade process and if you can ensure the regeneration and reevaluation of all cryptographic keys on the upgraded system.

    1. Disable FIPS mode in RHEL 7.

    2. Upgrade the system using **Leapp**. You must follow the pre-upgrade, upgrade, and post-upgrade instructions as in any other in-place upgrade.

    3. Enable FIPS mode in RHEL 8. See Switching the system to FIPS mode in the RHEL 8 Security hardening document for details.

4. Re-generate cryptographic keys on your system. See Appendix C, *Locations of cryptographic keys in RHEL 8* for more information.

   ○ After the upgrade is finished, re-evaluate and re-apply your security policies. For information about applying security policies that have been disabled during the upgrade or newly introduced in RHEL 8, see Applying security policies.

- **Storage and file systems** - Always back up your system prior to upgrading. For example, you can use the Relax-and-Recover (ReaR) utility, LVM snapshots, RAID splitting, or a virtual machine snapshot.

  > **NOTE**
  >
  > File systems formats are intact. As a result, file systems have the same limitations as when they were originally created.

- **High Availability** - If you are using the High Availability add-on, follow the Recommended Practices for Applying Software Updates to a RHEL High Availability or Resilient Storage Cluster Knowledgebase article.

- **Downtime** - The upgrade process can take from several minutes to several hours.

- **Satellite** - If you manage your hosts through Satellite, you can upgrade multiple hosts simultaneously from RHEL 7 to RHEL 8 by using the Satellite web UI. For more information, see Upgrading Hosts to Next Major Red Hat Enterprise Linux Release .

- **SAP HANA** - If you are using SAP HANA, follow How to in-place upgrade SAP environments from RHEL 7 to RHEL 8 instead. Note that the upgrade path for RHEL with SAP HANA might differ.

- **RHEL for Real Time** - Upgrades on real-time systems are supported.

- **Real Time for Network Functions Virtualization (NFV) in Red Hat OpenStack Platform** - Upgrades on real-time systems are supported.

- **Red Hat Software Collections (RHSCLs)** - RHSCLs are not fully migrated during the in-place upgrade. RHEL 8 packages usually automatically replace RHSCL packages, but customized configurations and data must be migrated and configured manually. For example, if you have installed databases from RHSCL, you should dump all data before the upgrade to prevent data loss during RHSCL package removal and then restore the data as needed after the system upgrade. Note that when upgrading the Red Hat Satellite server, RHSCL packages required by the project are migrated automatically.

- **Red Hat JBoss Enterprise Application Platform (EAP)** - JBoss EAP is not supported for the upgrade to RHEL 9. You must manually install and configure JBoss EAP on your system after the upgrade. For more information, see In-place Migrating of Jboss EAP and websphere servers along with Linux using leapp utility.

- **Public clouds** - The in-place upgrade is supported for on-demand Pay-As-You-Go (PAYG) instances using Red Hat Update Infrastructure (RHUI) only on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. The in-place upgrade is also supported for Bring Your Own Subscription instances on all public clouds that use Red Hat Subscription Manager (RHSM) for a RHEL subscription.

- **Language** - All **Leapp** reports, logs, and other generated documentation are in English, regardless of the language configuration.

- **Boot loader** - It is not possible to switch the boot loader from BIOS to UEFI on RHEL 7 or RHEL 8. If your RHEL 7 system uses BIOS and you want your RHEL 8 system to use UEFI, perform a fresh install of RHEL 8 instead of an in-place upgrade. For more information, see Is it possible to switch the BIOS boot to UEFI boot on preinstalled Red Hat Enterprise Linux machine?

- **Known limitations** - Notable known limitations of **Leapp** currently include:

  - Encryption of the whole disk or a partition, or file-system encryption currently cannot be used on a system targeted for an in-place upgrade.

  - Network based multipath and network storage that use Ethernet or Infiniband are not supported for the upgrade. This includes SAN using FCoE and booting from SAN using FC. Note that SAN using FC are supported.

  - The in-place upgrade is currently unsupported for on-demand PAYG instances on the remaining public clouds that use Red Hat Update Infrastructure but not RHSM for a RHEL subscription.

  - The in-place upgrade is not supported for systems with any Ansible products, including Ansible Tower, installed. To use a RHEL 7 Ansible Tower installation on RHEL 8, see the How do I migrate my Ansible Automation Platform installation from one environment to another? Knowledgebase solution.

See also Known Issues.

You can use **Red Hat Insights** to determine which of the systems you have registered to Insights is on a supported upgrade path to RHEL 8. To do so, go to the respective Advisor recommendation in Insights, enable the recommendation under the *Actions* drop-down menu, and inspect the list under the *Affected systems* heading. Note that the Advisor recommendation considers only the RHEL 7 minor version and does not perform a pre-upgrade assessment of the system. See also Advisor-service recommendations overview.

Additional resources

- The best practices and recommendations for performing RHEL Upgrade using Leapp

- Leapp upgrade FAQ (Frequently Asked Questions)

CHAPTER 4. PREPARING FOR THE UPGRADE

To prevent issues after the upgrade and to ensure that your system is ready to be upgraded to the next major version of RHEL, complete all necessary preparation steps before upgrading.

You must perform the preparation steps described in Preparing a RHEL 7 system for the upgrade on all systems. In addition, on systems that are registered to Satellite Server, you must also perform the preparation steps described in Preparing a Satellite-registered system for the upgrade .

4.1. PREPARING A RHEL 7 SYSTEM FOR THE UPGRADE

This procedure describes the steps that are necessary before performing an in-place upgrade to RHEL 8 by using the **Leapp** utility.

If you do not plan to use Red Hat Subscription Manager during the upgrade process, follow instructions in Upgrading to RHEL 8 without Red Hat Subscription Manager .

Prerequisites

- The system meets conditions listed in Planning an upgrade.

- If you previously upgraded from RHEL 6 to RHEL 7, you have finished all required manual post-upgrade steps. This includes manual migrating to the GRUB2 bootloader on your RHEL 7 machine. For more information, see Upgrading from GRUB Legacy to GRUB 2 .

Procedure

1. Optional: Review the best practices in The best practices and recommendations for performing RHEL Upgrade using Leapp Knowledgebase article.

2. Ensure your system has been successfully registered to the Red Hat Content Delivery Network (CDN) or Red Hat Satellite by using the Red Hat Subscription Manager.

3. If your system is registered to Satellite Server, complete the steps in Preparing a Satellite-registered system for the upgrade to ensure that your system meets the requirements for the upgrade.

   > **IMPORTANT**
   >
   > If your system is registered to Satellite Server, you must complete the steps in Preparing a Satellite-registered system for the upgrade for the upgrade before proceeding with the steps in this procedure to prevent issues from occurring.

4. Optional: Unmount non-system OS file systems that are not required for the upgrade, such as file systems containing only data files unrelated to the system itself, and comment them out from the **/etc/fstab** file. This can reduce the amount of time needed for the upgrade process and prevent potential issues related to third-party applications that are not migrated properly during the upgrade by custom or third-party actors.

5. Verify that the system is subscribed using subscription-manager:

   a. If your system is registered by using an account with Simple Content Access (SCA) enabled, verify that the **Content Access Mode is set to Simple Content Access** message appears:

```
# subscription-manager status
+-------------------------------------------+
   System Status Details
+-------------------------------------------+
Overall Status: Disabled
Content Access Mode is set to Simple Content Access. This host has access to content,
regardless of subscription status.
System Purpose Status: Disabled
```

b. If your system is registered by using an account with SCA disabled, verify that the Red Hat Linux Server subscription is attached, the product name is **Server**, and the status is **Subscribed**:

```
# subscription-manager list --installed
+-------------------------------------------+
       Installed Product Status
+-------------------------------------------+
Product Name:   Red Hat Enterprise Linux Server
Product ID:     69
Version:        7.9
Arch:           x86_64
Status:         Subscribed
```

6. Ensure you have appropriate repositories enabled. The following commands list repositories for the 64-bit Intel architecture; for other architectures, see RHEL 7 repositories.

   a. Enable the Base repository:

   ```
   # subscription-manager repos --enable rhel-7-server-rpms
   ```

   b. Enable the Extras repository where **Leapp** and its dependencies are available:

   ```
   # subscription-manager repos --enable rhel-7-server-extras-rpms
   ```

   > **NOTE**
   >
   > Optionally, you can enable the Optional (also known as CodeReady Linux Builder) or Supplementary repositories. For more information about repository IDs, see the Optional and Supplementary repositories list in RHEL 7 repositories. For more information about the content of these repositories, see The CodeReady Linux Builder repository and The Supplementary repository.

7. Set the Red Hat Subscription Manager to use the latest RHEL 7 content:

   ```
   # subscription-manager release --unset
   ```

8. Optional: To use custom repositories, see the Configuring custom repositories Knowledgebase article.

9. If you use the **yum-plugin-versionlock** plug-in to lock packages to a specific version, clear the lock by running:

```
# yum versionlock clear
```

See How to restrict yum to install or upgrade a package to a fixed specific package version?   for more information.

10. If you are upgrading using Red Hat Update Infrastructure (RHUI) on a public cloud, enable required RHUI repositories and install required RHUI packages to ensure your system is ready for upgrade.

    a. For AWS:

    ```
    # yum-config-manager --enable rhui-client-config-server-7
    # yum-config-manager --enable rhel-7-server-rhui-extras-rpms
    # yum -y install rh-amazon-rhui-client leapp-rhui-aws
    ```

    b. For Microsoft Azure:

    ```
    # yum-config-manager --enable rhui-microsoft-azure-rhel7
    # yum -y install rhui-azure-rhel7
    # yum-config-manager --enable rhui-rhel-7-server-rhui-extras-rpms
    # yum -y install leapp-rhui-azure
    ```

    > **NOTE**
    >
    > If you locked the Azure virtual machine (VM) to a minor release, remove the version lock. For more information, see Switch a RHEL 7.x VM back to non–EUS.

    c. For Google Cloud Platform, follow the Leapp RHUI packages for Google Cloud Platform (GCP) Knowledgebase article.

11. If you manage containers in Docker, recreate those containers with the appropriate container images by using Podman and then attach any in-use volumes. For more information, see How do I migrate my Docker containers to Podman prior to moving from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8?

12. Install the **Leapp** utility:

    ```
    # yum install leapp-upgrade
    ```

    Note that currently you need version 0.17.0 or later of the **leapp** package and version 0.20.0 or later of the **leapp-repository** package, which contains the **leapp-upgrade-el7toel8** RPM package.

> **NOTE**
>
> If your system does not have internet access, download the following packages from the Red Hat Customer Portal :
>
> - **leapp**
>
> - **leapp-deps**
>
> - **python2-leapp**
>
> - **leapp-upgrade-el7toel8**
>
> - **leapp-upgrade-el7toel8-deps** See the How to install leapp packages on an offline system for RHEL 7.9 to RHEL 8.X upgrade? Knowledgebase article for more information.

13. Update all packages to the latest RHEL 7 version and reboot:

    ```
    # yum update
    # reboot
    ```

14. The latest release of the **leapp-upgrade-el7toel8** package contains all required data files. If you have replaced these data files with older versions, remove all JSON files in the **/etc/leapp/files** directory and reinstall the **leapp-upgrade-el7toel8** package to ensure your data files are up-to-date.

15. Temporarily disable antivirus software to prevent the upgrade from failing.

16. Ensure that any configuration management system does not interfere with the in-place upgrade process:

    - If you use a configuration management system with a client-server architecture, such as **Puppet**, **Salt**, or **Chef**, disable the system before running the **leapp preupgrade** command. Do not enable the configuration management system until after the upgrade is complete to prevent issues during the upgrade.

    - If you use a configuration management system with agentless architecture, such as **Ansible**, do not execute the configuration and deployment file, such as an Ansible playbook, during the in-place upgrade as described in Performing the upgrade from RHEL 7 to RHEL 8 . Automation of the pre-upgrade and upgrade process using a configuration management system is not supported by Red Hat. For more information, see Using configuration management systems to automate parts of the Leapp pre-upgrade and upgrade process on Red Hat Enterprise Linux.

17. Ensure your system does not use more than one Network Interface Card (NIC) with a name based on the prefix used by the kernel (**eth**). For instructions on how to migrate to another naming scheme before an in-place upgrade to RHEL 8, see How to perform an in-place upgrade to RHEL 8 when using kernel NIC names on RHEL 7.

18. If you are upgrading using an ISO image, verify that the ISO image contains the target OS version, for example RHEL 8.8, and is saved to a persistent local mount point to ensure that the **Leapp** utility can access the image throughout the upgrade process.

19. Ensure that you have a full system backup or a virtual machine snapshot. You should be able to get your system to the pre-upgrade state if you follow standard disaster recovery procedures within your environment. You can use the following backup options:

    - Create a full backup of your system by using the Relax-and-Recover (ReaR) utility. For more information, see the ReaR documentation and What is Relax and Recover (ReaR) and how can I use it for disaster recovery?.

    - Create a snapshot of your system by using LVM snapshots or RAID splitting. In case of upgrading a virtual machine, you can create a snapshot of the whole VM. You can also manage snapshot and rollback boot entries by using the Boom utility. For more information, see What is BOOM and how to install it? and Managing system upgrades with snapshots.

    > **NOTE**
    >
    > Because LVM snapshots do not create a full backup of your system, you might not be able to recover your system after certain upgrade failures. As a result, it is safer to create a full backup by using the ReaR utility.

4.2. PREPARING A SATELLITE-REGISTERED SYSTEM FOR THE UPGRADE

This procedure describes the steps that are necessary to prepare a system that is registered to Satellite for the upgrade to RHEL 8.

> **NOTE**
>
> If you plan to upgrade the Satellite system itself, follow the procedure described in Upgrading Satellite or Capsule to Red Hat Enterprise Linux 8 In-Place Using Leapp .

> **IMPORTANT**
>
> Users on Satellite systems must complete the preparatory steps described both in this procedure and in Preparing a RHEL 7 system for the upgrade .

Prerequisites

- You have administrative privileges for the Satellite Server.

Procedure

1. Verify that Satellite is on a version in full or maintenance support. For more information, see Red Hat Satellite Product Life Cycle .

2. Import a subscription manifest with RHEL 8 repositories into Satellite Server. For more information, see the Managing Red Hat Subscriptions chapter in the Managing Content Guide for the particular version of Red Hat Satellite , for example, for version 6.12.

3. Enable and synchronize all required RHEL 7 and RHEL 8 repositories on the Satellite Server with the latest updates for RHEL 7.9 and the target OS version, for example RHEL 8.10. Required repositories must be available in the Content View and enabled in the associated activation key.
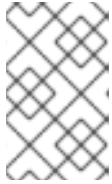
> **NOTE**
>
> For RHEL 8 repositories, enable the target OS version of each repository, for example, 8.10. If you enable only the RHEL 8 version of the repositories, the in-place upgrade is inhibited.

For example, for the Intel architecture without an Extended Update Support (EUS) subscription, enable at minimum the following repositories:

- Red Hat Enterprise Linux 7 Server (RPMs)
  rhel-7-server-rpms

  x86_64 7Server

- Red Hat Enterprise Linux 7 Server - Extras (RPMs)
  rhel-7-server-extras-rpms

  x86_64

- Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
  rhel-8-for-x86_64-appstream-rpms

  x86_64 *<target_os_version>*

- Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
  rhel-8-for-x86_64-baseos-rpms

  x86_64 *<target_os_version>*

  Replace *target_os_version* with the target OS version, for example 8.10.

  For other architectures, see RHEL 7 repositories and RHEL 8 repositories.

  For more information, see the *Importing Content* chapter in the *Managing Content Guide* for the particular version of Red Hat Satellite, for example, for version 6.12.

4. Attach the content host to a Content View containing the required RHEL 7 and RHEL 8 repositories.
   For more information, see the *Managing Content Views* chapter in the *Managing Content Guide* for the particular version of Red Hat Satellite, for example, for version 6.12.

Verification

1. Verify that the correct RHEL 7 and RHEL 8 repositories have been added to the correct Content View on Satellite Server.

   a. In the Satellite web UI, navigate to **Content > Lifecycle > Content Views** and click the name of the Content View.

   b. Click the **Repositories** tab and verify that the repositories appear correctly.

> **NOTE**
>
> You can also verify that the repositories have been added to the Content View using the following commands:
>
> ```
> # hammer repository list --search 'content_label ~ rhel-7' --content-view
> <content_view_name> --organization <organization> --lifecycle-
> environment <lifecycle_environment>
> # hammer repository list --search 'content_label ~ rhel-8' --content-view
> <content_view_name> --organization <organization> --lifecycle-
> environment <lifecycle_environment>
> ```
>
> Replace *<content_view_name>* with the name of the Content View, *<organization>* with the organization, and *<lifecycle_environement>* with the name of the lifecycle environment..

2. Verify that the correct RHEL 8 repositories are enabled in the activation key associated with the Content View:

   a. In Satellite web UI navigate to **Content > Lifecycle > Activation Keys** and click the name of the activation key.

   b. Click the **Repository Sets** tab and verify that the statuses of the required repositories are **Enabled**.

3. Verify that all expected RHEL 7 repositories are enabled in the host. For example:

   ```
   # subscription-manager repos --list-enabled | grep "^Repo ID"
   Repo ID:   rhel-7-server-extras-rpms
   Repo ID:   rhel-7-server-rpm
   ```

CHAPTER 5. REVIEWING THE PRE-UPGRADE REPORT

To assess upgradability of your system, start the pre-upgrade process by using the **leapp preupgrade** command. During this phase, the **Leapp** utility collects data about the system, assesses upgradability, and generates a pre-upgrade report. The pre-upgrade report summarizes potential problems and suggests recommended solutions. The report also helps you decide whether it is possible or advisable to proceed with the upgrade.

> **NOTE**
>
> The pre-upgrade assessment does not modify the system configuration, but it does consume non-negligible space in the **/var/lib/leapp** directory. In most cases, the pre-upgrade assessment requires up to 4 GB of space, but the actual size depends on your system configuration. If there is not enough space in the hosted file system, the pre-upgrade report might not show complete results of the analysis. To prevent issues, ensure that your system has enough space in the **/var/lib/leapp** directory or move the directory to a dedicated partition so that space consumption does not affect other parts of the system.
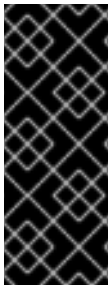
> **IMPORTANT**
>
> Always review the entire pre-upgrade report, even when the report finds no inhibitors to the upgrade. The pre-upgrade report contains recommended actions to complete before the upgrade to ensure that the upgraded system functions correctly.
>
> Reviewing a pre-upgrade report can also be useful if you want to perform a fresh installation of a RHEL 8 system instead of the in-place upgrade process.

You can assess upgradability in the pre-upgrade phase using either of the following ways:

- Review the pre-upgrade report in the generated **leapp-report.txt** file and manually resolve reported problems using the command-line interface.

- Use the web console to review the report, apply automated remediations where available, and fix remaining problems using the suggested remediation hints.

> **NOTE**
>
> You can process the pre-upgrade report by using your own custom scripts, for example, to compare results from multiple reports across different environments. For more information, see Automating your Red Hat Enterprise Linux pre-upgrade report workflow .
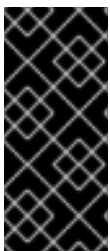
> **IMPORTANT**
>
> The pre-upgrade report cannot simulate the entire in-place upgrade process and therefore cannot identify all inhibiting problems with your system. As a result, your in-place upgrade might still be terminated even after you have reviewed and remediated all problems in the report. For example, the pre-upgrade report cannot detect issues related to broken package downloads.

5.1. ASSESSING UPGRADABILITY FROM THE COMMAND LINE

Identify potential upgrade problems during the pre-upgrade phase by using the command-line interface.

Prerequisites

- The steps listed in Preparing for the upgrade have been completed.

Procedure

1. On your RHEL 7 system, perform the pre-upgrade phase:

   ```
   # leapp preupgrade --target <target_os_version>
   ```

   Replace *<target_os_version>* with the target OS version, for example 8.10. If no target OS version is defined, **Leapp** uses the default target OS version specified in the table 1.1 in Supported upgrade paths.

   - If you are using custom repositories from the **/etc/yum.repos.d/** directory for the upgrade, enable the selected repositories as follows:

     ```
     # leapp preupgrade --enablerepo <repository_id1> --enablerepo <repository_id2> ...
     ```

   - If you are upgrading without RHSM or using RHUI, add the **--no-rhsm** option.

   - If you have an Extended Upgrade Support (EUS), Advanced Update Support (AUS), or Update Services for SAP Solutions (E4S) subscription, add the **--channel** *<channel>* option:

     - If you are upgrading to RHEL 8.8, replace *channel* with the channel name, for example, **eus**, **aus**, or **e4s**. Note that SAP HANA customers should perform the in-place upgrade using the How to in-place upgrade SAP environments from RHEL 7 to RHEL 8 guide.

     - If you are upgrading to RHEL 8.10, replace *channel* with **ga**.

2. Examine the report in the **/var/log/leapp/leapp-report.txt** file and manually resolve all the reported problems. Some reported problems contain remediation suggestions. **Inhibitor** problems prevent you from upgrading until you have resolved them. For more information on the different problems that can appear in the report, see the Pre Upgrade step in How do I upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8?
   The report contains the following risk factor levels:

   High

   Very likely to result in a deteriorated system state.

   Medium

   Can impact both the system and applications.

   Low

   Should not impact the system but can have an impact on applications.

   Info

   Informational with no expected impact to the system or applications.

   > **NOTE**
   >
   > Depending on the severity and impact of the found problems and the amount of work required to resolve them, it might be preferable to perform a clean install of RHEL 8 instead of proceeding with the in-place upgrade.

3. In certain system configurations, the **Leapp** utility generates true or false questions that you must answer manually. If the pre-upgrade report contains a **Missing required answers in the answer file** message, complete the following steps:

   a. Open the **/var/log/leapp/answerfile** file and review the true or false questions.

   b. Manually edit the **/var/log/leapp/answerfile** file, uncomment the confirm line of the file by deleting the **#** symbol, and confirm your answer as **True** or **False**. For more information, see the Leapp answerfile.

   > **NOTE**
   >
   > Alternatively, you can answer the true or false question by running the following command:
   >
   > ```
   > # leapp answer --section <question_section>.<field_name>=<answer>
   > ```
   >
   > For example, to confirm a **False** response to the question **Disable pam_pkcs11 module in PAM configuration?**, execute the following command:
   >
   > ```
   > # leapp answer --section
   > remove_pam_pkcs11_module_check.confirm=False
   > ```

4. Repeat the previous steps to rerun the pre-upgrade report to verify that you have resolved all critical issues.

5.2. ASSESSING UPGRADABILITY AND APPLYING AUTOMATED REMEDIATIONS THROUGH THE WEB CONSOLE

Identify potential problems in the pre-upgrade phase and apply automated remediations by using the web console.

Prerequisites

- You have completed the steps listed in Preparing for the upgrade.

Procedure

1. Install the **cockpit-leapp** plug-in:

   ```
   # dnf install cockpit-leapp
   ```

   Log in to the web console as **root** or as a user that has permissions to enter administrative commands with **sudo**. See Managing systems using the RHEL web console for more information about the web console.

2. On your RHEL 7 system, perform the pre-upgrade phase either from the command-line interface or from the web console terminal:

   ```
   # leapp preupgrade --target <target_os_version>
   ```

Replace *<target_os_version>* with the target OS version, for example 8.10. If no target OS version is defined, **Leapp** uses the default target OS version specified in the table 1.1 in Supported upgrade paths.

- If you are using custom repositories from the **/etc/yum.repos.d/** directory for the upgrade, enable the selected repositories as follows:

  ```
  # leapp preupgrade --enablerepo <repository_id1> --enablerepo <repository_id2> ...
  ```

- If you are upgrading without RHSM or using RHUI, add the **--no-rhsm** option.

- If you have an Extended Upgrade Support (EUS), Advanced Update Support (AUS), or Update Services for SAP Solutions (E4S) subscription, add the **--channel** *<channel>* option:

  - If you are upgrading to RHEL 8.8, replace *channel* with the channel name, for example, **eus**, **aus**, or **e4s**. Note that SAP HANA customers should perform the in-place upgrade using the How to in-place upgrade SAP environments from RHEL 7 to RHEL 8 guide.

  - If you are upgrading to RHEL 8.10, replace *channel* with **ga**.

3. In the web console, select **Upgrade Report** from the navigation menu to review all reported problems. **Inhibitor** problems prevent you from upgrading until you have resolved them. For more information on the different problems that can appear in the report, see the Pre Upgrade step in How do I upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8? To view a problem in detail, select the row to open the Detail pane.

Figure 5.1. In-place upgrade report in the web console

The report contains the following risk factor levels:

High

Very likely to result in a deteriorated system state.

Medium

Can impact both the system and applications.

Low

Should not impact the system but can have an impact on applications.

Info

Informational with no expected impact to the system or applications.

> **NOTE**
>
> Depending on the severity and impact of the found problems and the amount of work required to resolve them, it might be preferable to perform a clean install of RHEL 8 instead of proceeding with the in-place upgrade.

4. In certain configurations, the **Leapp** utility generates true or false questions that you must answer manually. If the Upgrade Report contains a **Missing required answers in the answer file** row, complete the following steps:

   a. Select the **Missing required answers in the answer file** row to open the **Detail** pane. The default answer is stated at the end of the remediation command.

   b. To confirm the default answer, select **Add to Remediation Plan** to execute the remediation later or **Run Remediation** to execute the remediation immediately.

   c. To select the non-default answer instead, execute the **leapp answer** command in the terminal, specifying the question you are responding to and your confirmed answer.

   ```
   # leapp answer --section <question_section>.<field_name>=<answer>
   ```

   For example, to confirm a **False** response to the question **Disable pam_pkcs11 module in PAM configuration?**, execute the following command

   ```
   # leapp answer --section remove_pam_pkcs11_module_check.confirm=False
   ```

   > **NOTE**
   >
   > You can also manually edit the **/var/log/leapp/answerfile** file, uncomment the confirm line of the file by deleting the **#** symbol, and confirm your answer as **True** or **False**. For more information, see the Leapp answerfile example.

5. Some problems have remediation commands that you can run to automatically resolve the problems. You can run remediation commands individually or all together in the remediation command.

   a. To run a single remediation command, open the **Detail** pane for the problem and click **Run Remediation**.

   b. To add a remediation command to the remediation plan, open the **Detail** pane for the problem and click **Add to Remediation Plan**

Figure 5.2. Detail pane
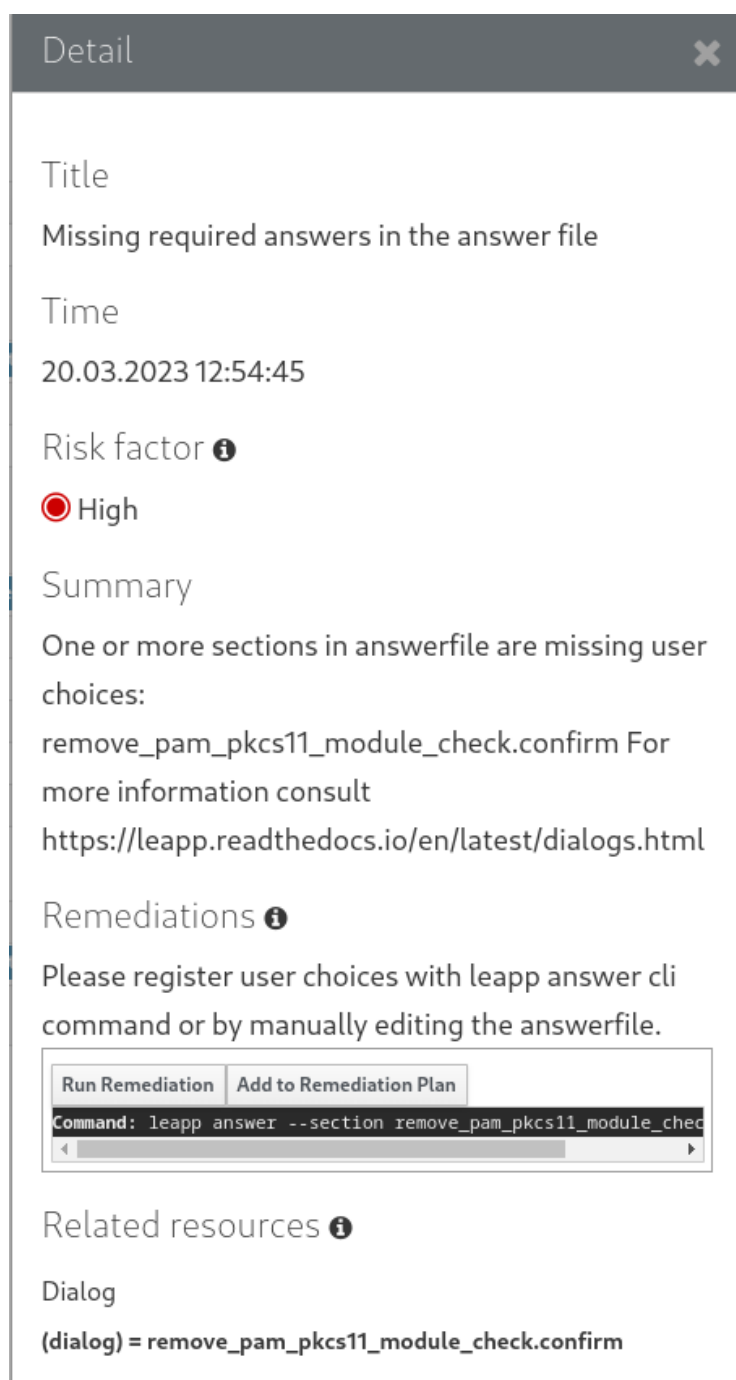
c. To run the remediation plan containing all added remediation commands, click the **Remediation plan** link in the top right corner above the report. Click **Execute Remediation Plan** to execute all listed commands.

6. After reviewing the report and resolving all reported problems, repeat steps 3-7 to rerun the report to verify that you have resolved all critical issues.

CHAPTER 6. PERFORMING THE UPGRADE FROM RHEL 7 TO RHEL 8

Upgrade to RHEL 8 using the **Leapp** utility.

Prerequisites

- The steps listed in Preparing for the upgrade have been completed, including a full system backup.

- The steps listed in Reviewing the pre-upgrade report have been completed and all reported issues resolved.

Procedure

1. On your RHEL 7 system, start the upgrade process:

   ```
   # leapp upgrade --target <target_os_version>
   ```

   Replace *<target_os_version>* with the target operating system (OS) version, for example 8.10. If no target OS version is defined, **Leapp** uses the default target OS version specified in the table 1.1 in Supported upgrade paths.

   > **NOTE**
   >
   > If you are using custom repositories from the **/etc/yum.repos.d/** directory for the upgrade, enable the selected repositories as follows:
   >
   > ```
   > # leapp upgrade --enablerepo <repository_id1> --enablerepo <repository_id2>
   > …
   > ```
   >
   > If you are upgrading without RHSM or using RHUI, add the **--no-rhsm** option.
   >
   > If you are upgrading by using an ISO image, add the **--no-rhsm** and **--iso** *<file_path>* options. Replace *<file_path>* with the file path to the saved ISO image, for example /**home**/**rhel8.iso**.
   >
   > If you have an Extended Upgrade Support (EUS), Advanced Update Support (AUS), or Update Services for SAP Solutions (E4S) subscription, add the **--channel** *<channel>* option:
   >
   > - If you are upgrading to RHEL 8.8, replace *channel* with the value you used with the **leapp preupgrade** command, for example, **eus**, **aus**, or **e4s**. Note that you must use the same value with the **--channel** option in both the **leapp preupgrade** and **leapp upgrade** commands.
   >
   > - If you are upgrading to RHEL 8.10, replace *channel* with **ga**.

   At the beginning of the upgrade process, **Leapp** performs the pre-upgrade phase described in Reviewing the pre-upgrade report.

   If the system is upgradable, **Leapp** downloads necessary data and prepares an RPM transaction for the upgrade.

If your system does not meet the parameters for a reliable upgrade, **Leapp** terminates the upgrade process and provides a record describing the issue and a recommended solution in the **/var/log/leapp/leapp-report.txt** file. For more information, see Troubleshooting.

2. Manually restart the system:

```
# reboot
```

In this phase, the system boots into a RHEL 8-based initial RAM disk image, initramfs. **Leapp** upgrades all packages and automatically reboots to the RHEL 8 system.

Alternatively, you can enter the **leapp upgrade** command with the **--reboot** option and skip this manual step.

If a failure occurs, investigate logs as described in Troubleshooting.

3. Log in to the RHEL 8 system and verify its state as described in Verifying the post-upgrade state of the RHEL 8 system.

4. Perform all post-upgrade tasks described in the upgrade report and in Performing post-upgrade tasks. Especially, re-evaluate and re-apply your security policies.

5. In case of upgrading a system that was and will be running in **FIPS mode**, remove any RHEL 7 kernels. Then, regenerate and otherwise ensure the FIPS compliance of all cryptographic keys. See Locations of cryptographic keys in RHEL 8 for more information.

CHAPTER 7. VERIFYING THE POST-UPGRADE STATE OF THE RHEL 8 SYSTEM

This procedure lists Verification recommended to perform after an in-place upgrade to RHEL 8.

Prerequisites

- The system has been upgraded following the steps described in Performing the upgrade from RHEL 7 to RHEL 8 and you have been able to log in to RHEL 8.

Procedure

After the upgrade completes, determine whether the system is in the required state, at least:

- Verify that the current OS version is Red Hat Enterprise Linux 8:

  ```
  # cat /etc/redhat-release
  Red Hat Enterprise Linux release <target_os_version> (Ootpa)
  ```

  Replace *target_os_version* with the target OS version, for example 8.10.

- Check the OS kernel version:

  ```
  # uname -r
  4.18.0-305.el<target_os>.x86_64
  ```

  The *target_os* should be either **8** or the target OS version, for example **8_10**. Note that **.el8** is important and the version should not be earlier than 4.18.0-305.

- If you are using the Red Hat Subscription Manager:

  - Verify that the correct product is installed:

    ```
    # subscription-manager list --installed
    +-----------------------------------------+
         Installed Product Status
    +-----------------------------------------+
    Product Name: Red Hat Enterprise Linux for x86_64
    Product ID:   479
    Version:      <target_os_version>
    Arch:         x86_64
    Status:       Subscribed
    ```

    Replace *target_os_version* with the target OS version, for example 8.10.

  - Verify that the release version is set to the target OS version immediately after the upgrade:

    ```
    # subscription-manager release
    Release: <target_os_version>
    ```

    Replace *target_os_version* with the target OS version, for example 8.10.

- Verify that network services are operational, for example, try to connect to a server using SSH.

- Check the post-upgrade status of your applications. In some cases, you may need to perform migration and configuration changes manually. For example, to migrate your databases, follow instructions in RHEL 8 Database servers documentation .

CHAPTER 8. PERFORMING POST-UPGRADE TASKS

The following major tasks are recommended after an in-place upgrade to RHEL 8.

Prerequisites

- You have upgraded the system following the steps described in Performing the upgrade from RHEL 7 to RHEL 8 and you have been able to log in to RHEL 8.

- You have verified the status of the in-place upgrade following the steps described in Verifying the post-upgrade status of the RHEL 8 system.

Procedure

After performing the upgrade, complete the following tasks:

1. Remove any remaining **Leapp** packages from the exclude list in the **/etc/dnf/dnf.conf** configuration file, including the **snactor** package. During the in-place upgrade, **Leapp** packages that were installed with the **Leapp** utility are automatically added to the exclude list to prevent critical files from being removed or updated. After the in-place upgrade, you must remove these **Leapp** packages from the exclude list before they can be removed from the system.

   - To manually remove packages from the exclude list, edit the **/etc/dnf/dnf.conf** configuration file and remove the desired **Leapp** packages from the **exclude** list.

   - To remove all packages from the **exclude** list:

     ```
     # yum config-manager --save --setopt exclude="
     ```

2. Remove remaining RHEL 7 packages, including remaining **Leapp** packages.

   a. Determine old kernel versions:

      ```
      # cd /lib/modules && ls -d *.el7*
      ```

   b. Remove weak modules from the old kernel. If you have multiple old kernels, repeat the following step for each kernel:

      ```
      # [ -x /usr/sbin/weak-modules ] && /usr/sbin/weak-modules --remove-kernel <version>
      ```

      Replace *<version>* with the kernel version determined in the previous step, for example:

      ```
      #  [ -x /usr/sbin/weak-modules ] && /usr/sbin/weak-modules --remove-kernel 3.10.0-1160.25.1.el7.x86_64
      ```

      > **NOTE**
      >
      > Ignore the following error message, which is generated if the kernel package has been previously removed:
      >
      > ```
      > /usr/sbin/weak-modules: line 1081: cd: /lib/modules/<version>/weak-updates: No such file or directory
      > ```

c. Remove the old kernel from the boot loader entry. If you have multiple old kernels, repeat this step for each kernel:

```
# /bin/kernel-install remove <version> /lib/modules/<version>/vmlinuz
```

Replace *version* with the kernel version determined in the previous step, for example:

```
# /bin/kernel-install remove 3.10.0-1160.25.1.el7.x86_64 /lib/modules/3.10.0-1160.25.1.el7.x86_64/vmlinuz
```

d. Locate remaining RHEL 7 packages:

```
# rpm -qa | grep -e '\.el[67]' | grep -vE '^(gpg-pubkey|libmodulemd|katello-ca-consumer)' | sort
```

e. Remove remaining RHEL 7 packages, including old kernel packages, and the **kernel-workaround** package from your RHEL 8 system. To ensure that RPM dependencies are maintained, use **YUM** or **DNF** when performing these actions. Review the transaction before accepting to ensure no packages are unintentionally removed.
For example:

```
# yum remove kernel-workaround $(rpm -qa | grep \.el7 | grep -vE 'gpg-pubkey|libmodulemd|katello-ca-consumer')
```

f. Remove remaining **Leapp** dependency packages:

```
# yum remove leapp-deps-el8 leapp-repository-deps-el8
```

g. Remove any remaining empty directories:

```
# rm -r /lib/modules/*el7*
```

3. Optional: Remove all remaining upgrade-related data from the system:

```
# rm -rf /var/log/leapp /root/tmp_leapp_py3 /var/lib/leapp
```
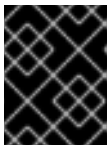
> **IMPORTANT**
>
> Removing this data might limit Red Hat Support's ability to investigate and troubleshoot post-upgrade problems.

4. Disable YUM repositories whose packages cannot be installed or used on RHEL 8. Repositories managed by RHSM are handled automatically. To disable these repositories:

```
# yum config-manager --set-disabled <repository_id>
```

Replace *<repository_id>* with the repository ID.

5. Replace the old rescue kernel and initial RAM disk with the current kernel and disk:

a. Remove the existing rescue kernel and initial RAM disk:

```
# rm /boot/vmlinuz-*rescue* /boot/initramfs-*rescue*
```

b. Reinstall the rescue kernel and related initial RAM disk:

```
# /usr/lib/kernel/install.d/51-dracut-rescue.install add "$(uname -r)" /boot "/boot/vmlinuz-$(uname -r)"
```

> **NOTE**
>
> If your system's kernel package has a different name, such as on real-time systems, replace **kernel-core** with the correct package name.

c. If your system is on the IBM Z architecture, update the zipl bootloader:

```
# zipl
```

6. Re-evaluate and re-apply your security policies. Especially, change the SELinux mode to enforcing. For details, see Applying security policies.

Verification

1. Verify that the old kernels have been removed from the bootloader entry:

```
# grubby --info=ALL | grep "\.el7" || echo "Old kernels are not present in the bootloader."
```

2. Verify that the previously removed rescue kernel and rescue initial RAM disk files have been created for the current kernel:

```
# ls /boot/vmlinuz-*rescue* /boot/initramfs-*rescue*
# lsinitrd /boot/initramfs-*rescue*.img | grep -qm1 "$(uname -r)/kernel/" && echo "OK" || echo "FAIL"
```

3. Verify the rescue boot entry refers to the existing rescue files. See the grubby output:

```
# grubby --info $(ls /boot/vmlinuz-*rescue*)
```

CHAPTER 9. APPLYING SECURITY POLICIES

During the in-place upgrade process, certain security policies must remain disabled. Furthermore, RHEL 8 introduces a new concept of system-wide cryptographic policies and also security profiles might contain changes between major releases. To make your system more secure, switch SELinux to enforcing mode and set a system-wide cryptographic policy. You may also want to remediate the system to be compliant with a specific security profile.

9.1. CHANGING SELINUX MODE TO ENFORCING

During the in-place upgrade process, the **Leapp** utility sets SELinux mode to permissive. When the system is successfully upgraded, you have to manually change SELinux mode to enforcing.

Prerequisites

- The system has been upgraded and you have performed the Verification described in Verifying the post-upgrade state of the RHEL 8 system.

Procedure

1. Ensure that there are no SELinux denials, for example, by using the **ausearch** utility:

   ```
   # ausearch -m AVC,USER_AVC -ts boot
   ```

   Note that the previous step covers only the most common scenario. To check for all possible SELinux denials, see the Identifying SELinux denials section in the Using SELinux title, which provides a complete procedure.

2. Open the **/etc/selinux/config** file in a text editor of your choice, for example:

   ```
   # vi /etc/selinux/config
   ```

3. Configure the **SELINUX=enforcing** option:

   ```
   # This file controls the state of SELinux on the system.
   # SELINUX= can take one of these three values:
   #       enforcing - SELinux security policy is enforced.
   #       permissive - SELinux prints warnings instead of enforcing.
   #       disabled - No SELinux policy is loaded.
   SELINUX=enforcing
   # SELINUXTYPE= can take one of these two values:
   #       targeted - Targeted processes are protected,
   #       mls - Multi Level Security protection.
   SELINUXTYPE=targeted
   ```

4. Save the change, and restart the system:

   ```
   # reboot
   ```

Verification

1. After the system restarts, confirm that the **getenforce** command returns **Enforcing**:

```
$ getenforce
Enforcing
```

Additional resources

- Troubleshooting problems related to SELinux

- Changing SELinux states and modes

9.2. SETTING SYSTEM-WIDE CRYPTOGRAPHIC POLICIES

The system-wide cryptographic policies is a system component that configures the core cryptographic subsystems, covering the TLS, IPSec, SSH, DNSSec, and Kerberos protocols.

After a successful installation or an in-place upgrade process, the system-wide cryptographic policy is automatically set to **DEFAULT**. The **DEFAULT** system-wide cryptographic policy level offers secure settings for current threat models.

To view or change the current system-wide cryptographic policy, use the update-crypto-policies tool:

```
$ update-crypto-policies --show
DEFAULT
```

For example, the following command switches the system-wide crypto policy level to **FUTURE**, which should withstand any near-term future attacks:

```
# update-crypto-policies --set FUTURE
Setting system policy to FUTURE
```

You can also customize system-wide cryptographic policies. For details, see the Customizing system-wide cryptographic policies with subpolicies and Creating and setting a custom system-wide cryptographic policy sections.

Additional resources

- Using system-wide cryptographic policies

- **update-crypto-policies(8)** man page on your system.

9.3. UPGRADING THE SYSTEM HARDENED TO A SECURITY BASELINE

To get a fully hardened system after a successful upgrade to RHEL 8, you can use automated remediation provided by the OpenSCAP suite. OpenSCAP remediations align your system with security baselines, such as PCI-DSS, OSPP, or ACSC Essential Eight. The configuration compliance recommendations differ among major versions of Red Hat Enterprise Linux due to the evolution of the security offering.

When upgrading a hardened RHEL 7 system, the **Leapp** tool does *not* provide direct means to retain the full hardening. Depending on the changes in the component configuration, the system might diverge from the recommendations for the RHEL 8 during the upgrade.

NOTE

You cannot use the same SCAP content for scanning RHEL 7 and RHEL 8. Update the management platforms if the compliance of the system is managed by the tools like Red Hat Satellite or Red Hat Insights.

As an alternative to automated remediations, you can make the changes manually by following an OpenSCAP-generated report. For information about generating a compliance report, see Scanning the system for security compliance and vulnerabilities.

Follow the procedure to automatically harden your system with the PCI-DSS profile.

IMPORTANT

Automated remediations support RHEL systems in the default configuration. Because the system upgrade has been altered after the installation, running remediation might not make it fully compliant with the required security profile. You might need to fix some requirements manually.

Prerequisites

- The **scap-security-guide** package is installed on your RHEL 8 system.

Procedure

1. Find the appropriate security compliance data stream **.xml** file:

   ```
   $ ls /usr/share/xml/scap/ssg/content/
   ssg-firefox-cpe-dictionary.xml  ssg-rhel6-ocil.xml
   ssg-firefox-cpe-oval.xml        ssg-rhel6-oval.xml
   ...
   ssg-rhel6-ds-1.2.xml            ssg-rhel8-oval.xml
   ssg-rhel8-ds.xml               ssg-rhel8-xccdf.xml
   ...
   ```

   For additional information, see section Viewing compliance profiles.

2. Remediate the system according to the selected profile from the appropriate data stream:

   ```
   # oscap xccdf eval --profile pci-dss --remediate /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
   ```

   You can replace the *pci-dss* value in the **--profile** argument with the ID of the profile according to which you want to harden your system. For a full list of profiles supported in RHEL 8, see SCAP security profiles supported in RHEL .

> ⚠️ **WARNING**
>
> If not used carefully, running the system evaluation with the Remediate option enabled might render the system non-functional. Red Hat does not provide any automated method to revert changes made by security–hardening remediations. Remediations are supported on RHEL systems in the default configuration. If your system has been altered after the installation, running remediation might not make it compliant with the required security profile.

3. Restart your system:

   ```
   # reboot
   ```

Verification

1. Verify that the system is compliant with the profile, and save the results in an HTML file:

   ```
   $ oscap xccdf eval --report pcidss_report.html --profile pci-dss
   /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
   ```

Additional resources

- **scap-security-guide(8)** and **oscap(8)`** man pages on your system

- Scanning the system for security compliance and vulnerabilities

- Red Hat Insights Security Policy documentation

- Red Hat Satellite Security Policy documentation

CHAPTER 10. TROUBLESHOOTING

You can refer to the following tips to troubleshoot upgrading from RHEL 7 to RHEL 8.

10.1. TROUBLESHOOTING RESOURCES

You can refer to the following troubleshooting resources.

Console output

By default, only error and critical log level messages are printed to the console output by the **Leapp** utility. To change the log level, use the **--verbose** or **--debug** options with the **leapp upgrade** command.

- In *verbose* mode, **Leapp** prints info, warning, error, and critical messages.

- In *debug* mode, **Leapp** prints debug, info, warning, error, and critical messages.

Logs

- The **/var/log/leapp/leapp-upgrade.log** file lists issues found during the initramfs phase.

- The **/var/log/leapp/dnf-debugdata/** directory contains transaction debug data. This directory is present only if the **leapp upgrade** command is executed with the **--debug** option.

- The **/var/log/leapp/answerfile** contains questions required to be answered by **Leapp**.

- The **journalctl** utility provides complete logs.

Reports

- The **/var/log/leapp/leapp-report.txt** file lists issues found during the pre-upgrade phase. The report is also available in the web console, see Assessing upgradability and applying automated remediations through the web console.

- The **/var/log/leapp/leapp-report.json** file lists issues found during the pre-upgrade phase in a machine-readable format, which enables you to process the report using custom scripts. For more information, see Automating your Red Hat Enterprise Linux pre-upgrade report workflow .

10.2. TROUBLESHOOTING TIPS

You can refer to the following troubleshooting tips.

Pre-upgrade phase

- Verify that your system meets all conditions listed in Planning an upgrade.

- Make sure you have followed all steps described in Preparing for the upgrade for example, your system does not use more than one Network Interface Card (NIC) with a name based on the prefix used by the kernel (**eth**).

- Make sure you have answered all questions required by **Leapp** in the **/var/log/leapp/answerfile** file. If any answers are missing, **Leapp** inhibits the upgrade. Example questions:

  - Disable pam_pkcs11 module in PAM configuration?

- Disable pam_krb5 module in PAM configuration?

- Configure PAM and nsswitch.conf with the following authselect call?

- Make sure you have resolved all problems identified in the pre-upgrade report, located at **/var/log/leapp/leapp-report.txt**. To achieve this, you can also use the web console, as described in Assessing upgradability and applying automated remediations through the web console .

Example 10.1. Leapp answerfile

The following is an example of an unedited **/var/log/leapp/answerfile** file that has one unanswered question:

```
[remove_pam_pkcs11_module_check]
# Title:        None
# Reason:       Confirmation
# ================== remove_pam_pkcs11_module_check.confirm ==================
# Label:        Disable pam_pkcs11 module in PAM configuration? If no, the upgrade process will
be interrupted.
# Description:    PAM module pam_pkcs11 is no longer available in RHEL-8 since it was replaced
by SSSD.
# Type:         bool
# Default:      None
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
# confirm =
```

The **Label** field specifies the question that requires an answer. In this example, the question is **Disable pam_pkcs11 module in PAM configuration?**

To answer the question, uncomment the **confirm** line and enter an answer of **True** or **False**. In this example, the selected answer is **True**:

```
[remove_pam_pkcs11_module_check]
...
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
confirm = True
```

Download phase

- If a problem occurs during downloading RPM packages, examine transaction debug data located in the **/var/log/leapp/dnf-debugdata/** directory.
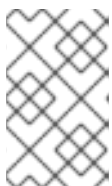
> **NOTE**
>
> The **/var/log/leapp/dnf-debugdata/** directory is empty or does not exist if no transaction debug data was produced. This might occur when the required repositories are not available.

initramfs phase

- During this phase, potential failures redirect you to the Dracut shell. Check the Journal log:

> # journalctl

Alternatively, restart the system from the Dracut shell using the **reboot** command and check the
/var/log/leapp/leapp-upgrade.log file.

Post-upgrade phase

- If your system seems to be successfully upgraded but booted with the old RHEL 7 kernel, restart
  the system and check the kernel version of the default entry in GRUB.

- Make sure you have followed the recommended steps in Verifying the post-upgrade state of
  the RHEL 8 system.

- If your application or a service stops working or behaves incorrectly after you have switched
  SELinux to enforcing mode, search for denials using the **ausearch**, **journalctl**, or **dmesg** utilities:

> # ausearch -m AVC,USER_AVC -ts boot
> # journalctl -t setroubleshoot
> # dmesg | grep -i -e selinux -e type=1400

The most common problems are caused by incorrect labeling. See Troubleshooting problems
related to SELinux for more details.

10.3. KNOWN ISSUES

The following are known issues you might encounter when upgrading from RHEL 7 to RHEL 8.

- NIC teaming currently does not work when the in-place upgrade is performed while Network
  Manager is disabled or not installed.

- If you use an HTTP proxy, Red Hat Subscription Manager must be configured to use such a
  proxy, or the **subscription-manager** command must be executed with the **--proxy
  <hostname>** option. Otherwise, an execution of the **subscription-manager** command fails. If
  you use the **--proxy** option instead of the configuration change, the upgrade process fails
  because **Leapp** is unable to detect the proxy. To prevent this problem from occurring, manually
  edit the **rhsm.conf** file as described in How to configure HTTP Proxy for Red Hat Subscription
  Management. (BZ#1689294)

- If your RHEL 7 system uses a device driver that is provided by Red Hat but is not available in
  RHEL 8, **Leapp** inhibits the upgrade. However, if the RHEL 7 system uses a third-party device
  driver that **Leapp** does not have data for in the
  /etc/leapp/files/device_driver_deprecation_data.json file, **Leapp** does not detect such a
  driver and proceeds with the upgrade. Consequently, the system might fail to boot after the
  upgrade.

- You cannot perform an in-place upgrade when the **winbind** and **wins** Samba modules are used
  in the **/etc/nsswitch.conf** file. The upgrade transaction fails with the following error messages
  and **Leapp** inhibits the upgrade:

> upgrade[469]: STDERR:
> upgrade[469]: Error in PREIN scriptlet in rpm package unbound-libs
> upgrade[469]: Error: Transaction failed
> upgrade[469]: Container el8userspace failed with error code 1.
> unbound-libs has a PREIN failure

To work around this problem, configure the system so that it uses only local providers for the **user**, **groups**, and **hosts** database during the update:

1. Open the system **/etc/nsswitch.conf** configuration file and search for entries that contain the **winbind** or **wins** strings.

2. If you find such entries, create a backup of **/etc/nsswitch.conf**.

3. Edit **/etc/nsswitch.conf** and remove **winbind** or **wins** from the entries that contain them.

4. Perform an in-place upgrade.

5. After the upgrade, add the **winbind** and **wins** strings to their entries in **/etc/nsswitch.conf**, based on your system configuration requirements.
(BZ#1410154)

- The **Leapp** utility does not change customized authentication configuration during the upgrade process. If you used the deprecated **authconfig** utility to configure authentication on your RHEL 7 system, authentication on RHEL 8 might not work correctly. To ensure that your custom configuration functions properly on the RHEL 8 system, re-configure your RHEL 8 system with the **authselect** utility.

> **IMPORTANT**
>
> During the in-place upgrade, the deprecated **pam_krb5** or **pam_pkcs11** pluggable authentication modules (PAM) are removed. As a result, if the PAM configuration on your RHEL 7 system contains the **pam_krb5** or **pam_pkcs11** modules and if these modules have the **required** or **requisite** control values, you might be locked out of the system if you perform the in-place upgrade. To work around this problem, reconfigure your RHEL 7 system to not use **pam_krb5** or **pam_pkcs11** before you start the upgrade process.

- If the name of a third-party package (not signed by Red Hat) installed on your system is the same as the name of a package provided by Red Hat, the in-place upgrade fails. To work around this problem, select one of the following options prior to upgrading:

  a. Remove the third-party package

  b. Replace the third-party package with the package provided by Red Hat

- For security reasons, support for single-DES (DES) and triple-DES (3DES) encryption types has been removed from RHEL 8. RHEL 7 Identity Management (IdM), however, still supports 3DES encryption.
Upgrading IdM clients or migrating the whole IdM environment from RHEL 7 to RHEL 8 is possible because both versions of RHEL prefer stronger AES encryption types by default:

Version of IdM	Default encryption types	Additional supported encryption types
RHEL 7	**aes256-cts** **aes128-cts**	**camellia256-cts** **camellia128-cts** **des3-hmac** **arcfour-hmac**

Version of IdM	Default encryption types	Additional supported encryption types
RHEL 8	**aes256-cts** **aes128-cts**	**aes256-sha2** **aes128-sha2** **camellia256-cts** **camellia128-cts** **arcfour-hmac** [a]

[a] RC4 encryption has been deprecated and disabled by default in RHEL 8 because it is considered less secure than the newer AES-128 and AES-256 encryption types. For more information about enabling RC4 support for compatibility with legacy Active Directory environments, see Ensuring support for common encryption types in AD and RHEL.

If you manually configured a non-IdM Kerberos Distribution Center (KDC), any services, or any users to **only** use DES or 3DES encryption, you might experience service interruptions after updating to the latest Kerberos packages in RHEL 8, such as:

- Kerberos authentication errors

- **unknown enctype** encryption errors

- KDCs with DES-encrypted Database Master Keys (**K/M**) fail to start

Red Hat recommends you do not use DES or 3DES encryption in your environment. For more information about re-keying Kerberos principals to use stronger encryption types, see Retiring DES from MIT Kerberos Documentation.

- The in-place upgrade might fail on systems with Software Redundant Array of Independent Disks (RAID). (RHEL-3279)

- Systems with a disabled GRUB boot loader specification, such as systems using Puppet, cannot create new initramfs for newer kernels. To work around this problem, manually remove packages and the old kernel from the boot loader entry as described in Chapter 6: Performing post-upgrade tasks. (BZ#1955099)

- The Relax-and-Recover (ReaR) utility is not available on the IBM Z architecture. As a result, IBM Z systems cannot be completely remediated by the OpenSCAP suite and might not be fully compliant with security baselines. (BZ#1958939)

- During the in-place upgrade, the **Leapp** utility usually preserves the network interface controller (NIC) names between RHEL 7 and RHEL 8. However, on some systems, such as systems with network bonding, the NIC names require updating between RHEL 7 and RHEL 8. On those systems, perform the following steps:

  a. Set the **LEAPP_NO_NETWORK_RENAMING=1** environment variable to prevent the **Leapp** utility from incorrectly preserving the original RHEL 7 NIC names.

  b. Perform the in-place upgrade.

  c. Verify that your network is working correctly. If needed, manually update the network configuration.

(BZ#1919382)

- After the in-place upgrade, SSH keys are no longer auto-generated if the system meets the following conditions:

  - The system is on a cloud.

  - The cloud-init package is installed.

  - The ssh_genkeytypes configuration is set to ~ in the /etc/cloud/cloud.cfg file, which is the default.
    This issue prevents the system from connecting by using SSH if the original keys have been removed. To prevent this issue, see the Unable to SSH to new Virtual Machine after upgrading the template to RHEL 8.7 or 9 Knowledgebase solution. (BZ# 2210012)

- VMWare virtual machines that were created at Hardware Level 13 and are booting with UEFI might experience issues during the upgrade because the NVRAM file is too small. For more information about this issue and how to resolve it, see VMWare: Getting "No space left on device" when executing efibootmgr or mokutil command to add entries. (RHEL-3362)

- The upgrade might fail if you are upgrading by using RHUI with an ISO image. You can work around this issue by not using the **--iso** option with the upgrade or by following the instructions in Offline Leapp upgrade using ISO fails with "Failed to synchronize cache for repo 'rhul-microsoft-azure-rhel8', ignoring this repo. (RHEL-3296)

- The pre-upgrade process might fail with the following error messages:
  MountError: failed to create mount target directory …

  If this issue occurs, export the **LEAPP_OVL_IMG_FS_EXT4=1** environment variable. For more information, see Leapp can fail with a MountError (OverlayFS + XFS ftype=1) . (RHEL-3330)

- If too many file systems are mounted, the pre-upgrade process might fail with the following error message:

  ```
  OperationalError: unable to open database file
  Cannot create XFS filesystem in ...
  ```

  If this issue occurs, complete the following steps:

  1. Unmount any file systems that are not related to the system partitions and are not needed during the upgrade process.

  2. Comment out the unmounted file systems' entries in the **/etc/fstab** file to prevent them from being mounted during the upgrade process.

  3. Restore the original file system configuration after the upgrade.
     (RHEL-3320)

- If you do not have the **/etc/sysconfig/kernel** system configuration file on your system, the upgrade fails, resulting in a broken system. To prevent this issue, create the file manually with the expected configuration. For more information, see Verifying the boot loader. (RHEL-22306)

- If any of the mounted file systems that are defined in the **/etc/fstab** file do not have the **shared** propagation flag set, the upgrade might fail. To prevent this issue, remount these file systems to set them as shared:

```
# mount -o remount --make-shared <mountpoint>
```

Replace *mountpoint* with the mountpoint of each file system.

For more information, see Leapp "Can not load RPM file" during the DNF transaction check .
(RHEL-23449)

- The upgrade might fail if limited resources have been set for the upgrade process. For example, the **maximum number of open files descriptors** and **maximum size of files written by the process and its children** attributes can be reached by the upgrade process if they are set. To prevent these issues, increase or remove these limits before the upgrade process. For more information, see Why does leapp preupgrade fail with sqlite3.OperationalError: unable to open database file traceback error ? and Ensure that there is enough diskspace in /var/lib/leapp/scratch/diskimages/root_boot at least XXX mib are needed. (RHEL-16881, RHEL-26459)

- If the **jbcs-httpd24-brotli** RPM is installed on the system, for example, if your system uses JBoss Core Services Web Server, the upgrade might fail. To prevent this issue, remove the package before the upgrade. Alternatively, if you cannot remove the package before the upgrade, run the following command to ensure that the **brotli** package is installed during the upgrade:

```
# echo brotli >> /etc/leapp/transaction/to_install
```

(RHEL-22542)

- Systems with network cards that are not on a PCI bus, such as RoCE on IBM Z machines, might experience connectivity loss after the upgrade due to changed NIC names. To prevent this problem, complete the following steps before upgrading:

    1. Add **net.ifnames=0** to the kernel boot parameters:

    ```
    # grubby --update-kernel=ALL --args 'net.ifnames=0'
    ```

    2. On IBM Z systems, enter the following command to make the change effective:

    ```
    # zipl
    ```

    3. Reboot your system.
    (RHEL-22371)

- If your RHEL 7 system uses a device driver that is provided by Red Hat but is not available in RHEL 8, the driver must be unloaded before the in-place upgrade. However, when some device drivers, for example the **mptctl** driver, are used by other services, the drivers might be reloaded automatically. To resolve this problem, see IPU is inhibited due to mptctl module that cannot be unloaded. (RHEL-15894)

- If you are upgrading by using RHUI, files in the **/usr/share/leapp-repository/repositories/system_upgrade/common/files/rhui/** directory are incorrectly reported as custom files in the pre-upgrade report. Unless you modified these files manually, you can ignore the warnings about these files in the report and the in-place upgrade will not be affected. (RHEL-40115)

10.4. OBTAINING SUPPORT

To open a support case, select *RHEL 7* as the product, and provide a **sosreport** from your system.

- To generate a **sosreport** on your system, run:

```
# sosreport
```

Note that you can leave the case ID empty.

For details on generating a sosreport, see the solution What is an sosreport and how to create one in Red Hat Enterprise Linux?.

For more information about opening and managing a support case on the Customer Portal, see the article How do I open and manage a support case on the Customer Portal? .

CHAPTER 11. RELATED INFORMATION

You can refer to the following instructional materials:

- Upgrade your Red Hat Enterprise Linux Infrastructure

- Red Hat Enterprise Linux technology capabilities and limits

- Supported in-place upgrade paths for Red Hat Enterprise Linux

- In-place upgrade Support Policy

- Considerations in adopting RHEL 8

- Customizing your Red Hat Enterprise Linux in-place upgrade

- Automating your Red Hat Enterprise Linux pre-upgrade report workflow

- Using configuration management systems to automate parts of the Leapp pre-upgrade and upgrade process on Red Hat Enterprise Linux

- Upgrading from RHEL 6 to RHEL 7

- Upgrading from RHEL 6 to RHEL 8

- Converting from a Linux distribution to RHEL using the Convert2RHEL utility

- Upgrading Hosts from RHEL 7 to RHEL 8 in Red Hat Satellite

- How to in-place upgrade SAP environments from RHEL 7 to RHEL 8

- Red Hat Insights Documentation

- Upgrades-related Knowledgebase articles and solutions

- The best practices and recommendations for performing RHEL Upgrade using Leapp

- Leapp upgrade FAQ (Frequently Asked Questions)

- Red Hat Enterprise Linux Upgrade Helper

APPENDIX A. RHEL 7 REPOSITORIES

Before the upgrade, ensure you have appropriate repositories enabled as described in step 4 of the procedure in Preparing a RHEL 7 system for the upgrade .

If you plan to use Red Hat Subscription Manager during the upgrade, you **must enable** the following repositories before the upgrade by using the **subscription-manager repos --enable** *repository_id* command:

Architecture	Repository	Repository ID
64-bit Intel	Base	**rhel-7-server-rpms**
	Extras	**rhel-7-server-extras-rpms**
IBM POWER8 (little endian)	Base	**rhel-7-for-power-le-rpms**
	Extras	**rhel-7-for-power-le-extras-rpms**
IBM Z	Base	**rhel-7-for-system-z-rpms**
	Extras	**rhel-7-for-system-z-extras-rpms**

You **can enable** the following repositories before the upgrade by using the **subscription-manager repos --enable** *repository_id* command:

Architecture	Repository	Repository ID
64-bit Intel	Optional	**rhel-7-server-optional-rpms**
	Supplementary	**rhel-7-server-supplementary-rpms**
IBM POWER8 (little endian)	Optional	**rhel-7-for-power-le-optional-rpms**
	Supplementary	**rhel-7-for-power-le-supplementary-rpms**
IBM Z	Optional	**rhel-7-for-system-z-optional-rpms**
	Supplementary	**rhel-7-for-system-z-supplementary-rpms**

> **NOTE**
>
> If you have enabled a RHEL 7 Optional or a RHEL 7 Supplementary repository before an in-place upgrade, **Leapp** enables the RHEL 8 CodeReady Linux Builder or RHEL 8 Supplementary repositories, respectively.

If you decide to use custom repositories, enable them per instructions in Configuring custom repositories.

APPENDIX B. RHEL 8 REPOSITORIES

If your system is registered to the Red Hat Content Delivery Network (CDN) using the Red Hat Subscription Manager (RHSM), RHEL 8 repositories are automatically enabled during the in-place upgrade. However, on systems registered to Red Hat Satellite using RHSM, you must manually enable and synchronize both RHEL 7 and RHEL 8 repositories before running the pre-upgrade report.

> **NOTE**
>
> Make sure to enable the target operating system (OS) version of each repository, for example RHEL 8.10. If you have enabled only the RHEL 8 version of the repositories, the in-place upgrade is inhibited.

If you plan to use Red Hat Satellite during the upgrade, you **must enable and synchronize** at least the following RHEL 8 repositories before the upgrade using either the Satellite web UI or the **hammer repository-set enable** and **hammer product synchronize** commands:

> **NOTE**
>
> Replace *<target_os_version>* with the target operating system (OS) version, for example 8.10.

Table B.1. RHEL 8 repositories

Architecture	Repository	Repository ID	Repository name	Release version
64-bit Intel	BaseOS	**rhel-8-for-x86_64-baseos-rpms**	Red Hat Enterprise Linux 8 for x86_64 – BaseOS (RPMs)	x86_64 *<target_os_version>*
	AppStream	**rhel-8-for-x86_64-appstream-rpms**	Red Hat Enterprise Linux 8 for x86_64 – AppStream (RPMs)	x86_64 *<target_os_version>*
IBM Power8 (little endian)	BaseOS	**rhel-8-for-ppc64le-baseos-rpms**	Red Hat Enterprise Linux 8 for Power, little endian – BaseOS (RPMs)	ppc64le *<target_os_version>*
	AppStream	**rhel-8-for-ppc64le-appstream-rpms**	Red Hat Enterprise Linux 8 for Power, little endian – AppStream (RPMs)	ppc64le *<target_os_version>*

Architecture	Repository	Repository ID	Repository name	Release version
IBM Z	BaseOS	**rhel-8-for-s390x-baseos-rpms**	Red Hat Enterprise Linux 8 for IBM z Systems – BaseOS (RPMs)	s390x *<target_os_version>*
	AppStream	**rhel-8-for-s390x-appstream-rpms**	Red Hat Enterprise Linux 8 for IBM z Systems – AppStream (RPMs)	s390x *<target_os_version>*

APPENDIX C. LOCATIONS OF CRYPTOGRAPHIC KEYS IN RHEL 8

After you upgrade a system that is running in Federal Information Processing Standard (FIPS) mode, you must regenerate and otherwise ensure the FIPS compliance of all cryptographic keys. Some well-known locations for such keys are in the following table. Note that the list is not complete, and you might check also other locations.

Table C.1. Locations of cryptographic keys in RHEL 8

Application	Locations of keys	Notes
Apache mod_ssl	**/etc/pki/tls/private/localhost.key**	The **/usr/lib/systemd/system/httpd-init.service** service runs the **/usr/libexec/httpd-ssl-gencerts** file if the **/etc/pki/tls/private/localhost.key** does not exist.
Bind9 RNDC	**/etc/rndc.key**	The **named-setup-rndc.service** service runs the **/usr/libexec/generate-rndc-key.sh** script, which generates the **/etc/rndc.key** file.
Cyrus IMAPd	**/etc/pki/cyrus-imapd/cyrus-imapd-key.pem**	The **cyrus-imapd-init.service** service generates the **/etc/pki/cyrus-imapd/cyrus-imapd-key.pem** file on its startup.
DNSSEC-Trigger	**/etc/dnssec-trigger/dnssec_trigger_control.key**	The **dnssec-triggerd-keygen.service** service generates the **/etc/dnssec-trigger/dnssec_trigger_control.key** file.
Dovecot	**/etc/pki/dovecot/private/dovecot.pem**	The **dovecot-init.service** service generates the **/etc/pki/dovecot/private/dovecot.pem** file on its startup.
OpenPegasus	**/etc/pki/Pegasus/file.pem**	The **tog-pegasus.service** service generates the **/etc/pki/Pegasus/file.pem** private key file.

Application	Locations of keys	Notes
OpenSSH	**/etc/ssh/ssh_host*_key**	Ed25519 and DSA keys are not FIPS-compliant. Custom Diffie-Hellman (DH) parameters are not supported in FIPS mode. Comment out the **ModuliFile** option in the **sshd_config** file to ensure compatibility with FIPS mode. You can keep the **moduli** file (**/etc/ssh/moduli** by default) in place.
Postfix	**/etc/pki/tls/private/postfix.key**	The post-installation script contained in the **postfix** package generates the **/etc/pki/tls/private/postfix.key** file.
RHEL web console	**/etc/cockpit/ws-certs.d/**	The web console runs the **/usr/libexec/cockpit-certificate-ensure --for-cockpit-tls** file, which creates keys in the **/etc/cockpit/ws-certs.d/** directory.
Sendmail	**/etc/pki/tls/private/sendmail.key**	The post-installation script contained in the **sendmail** package generates the **/etc/pki/tls/private/sendmail.key** file.

To ensure the FIPS compliance of cryptographic keys of third-party applications, refer to the corresponding documentation of the respective applications. Furthermore:

- Any service that opens a port might use a TLS certificate.

  - Not all services generate cryptographic keys automatically, but many services that start up automatically by default often do so.

- Focus also on services that use any cryptographic libraries such as NSS, GnuTLS, OpenSSL, and libgcrypt.

- Check also backup, disk-encryption, file-encryption, and similar applications.

> **IMPORTANT**
>
> Because FIPS mode in RHEL 8 restricts DSA keys, DH parameters, RSA keys shorter than 1024 bits, and some other ciphers, old cryptographic keys stop working after the upgrade from RHEL 7. See the Changes in core cryptographic components section in the Considerations in adopting RHEL 8 document and the Using system-wide cryptographic policies chapter in the RHEL 8 Security hardening document for more information.

Additional resources

- Switching the system to FIPS mode in the RHEL 8 Security hardening document

- **update-crypto-policies(8)** and **fips-mode-setup(8)** man pages on your system