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: 2020-06-01

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 input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:
  1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.
  2. Use your mouse cursor to highlight the part of text that you want to comment on.
  3. Click the **Add Feedback** pop-up that appears below the highlighted text.
  4. Follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
  1. Go to the Bugzilla website.
  2. As the Component, use **Documentation**.
  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
  4. Click **Submit Bug**.

CHAPTER 1. PLANNING AN UPGRADE

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

You should consider the following before upgrading to RHEL 8:

- **Operating system** - The operating system is upgraded by the **Leapp** utility under the following conditions:
  - The Server variant installed of the **latest available RHEL 7 version**, which currently is:
    - **RHEL 7.8** on the 64-bit Intel, IBM POWER 8 (little endian), and IBM Z architectures
    - **RHEL 7.6** on architectures that **require kernel version 4.14**: 64-bit ARM, IBM POWER 9 (little endian), or IBM Z (Structure A)
      See Supported in-place upgrade paths for Red Hat Enterprise Linux for more information.
  - Minimum hardware requirements for RHEL 8 met
  - Access to RHEL 8 content provided
- **Applications** - You can migrate applications installed on your system 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 custom actors are unsupported by Red Hat.
- **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 FIPS mode are not supported.
  - 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 Chapter 6, *Applying security policies*.
- **Storage and file systems**- You should 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.
- **Downtime** - The upgrade process can take from several minutes to several hours.
- **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.
  - No network-based multipath and no kind of network storage mount can be used as a system partition (for example, iSCSI, or NFS).

- The in-place upgrade is currently unsupported for on-demand instances on Public Clouds (Amazon EC2, Azure, Huawei Cloud, Alibaba Cloud, Google Cloud) that use Red Hat Update Infrastructure but not Red Hat Subscription Manager for a RHEL subscription.

See also Section 7.3, “Known issues” .

You can use **Red Hat Insights** to determine which of the systems you have registered to Insights can be upgraded to RHEL 8. To do so, navigate to the respective Insights rule and inspect the list under the *Affected systems* heading. Note that the Insights rule considers only the RHEL 7 minor version and does not perform a pre-upgrade assessment of the system.

CHAPTER 2. 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 using the **Leapp** utility.

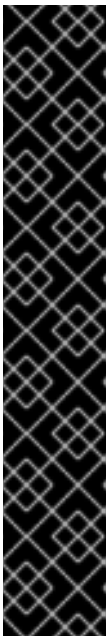
If you do not plan to use Red Hat Subscription Manager during the upgrade process, follow instructions in Upgrading to RHEL 8 without Red Hat Subscription Manager .

Prerequisites

- The system meets conditions listed in Chapter 1, *Planning an upgrade*.

Procedure

1. Ensure your system has been successfully registered to the Red Hat Content Delivery Network (CDN) or Red Hat Satellite 6.5 or later using the Red Hat Subscription Manager.



IMPORTANT

If your system is registered to Satellite Server, ensure that Satellite meets the following conditions:

a. Satellite has a subscription manifest with RHEL 8 repositories imported. For more information, see the *Managing Subscriptions* chapter in the *Content Management Guide* for the particular version of Red Hat Satellite, for example, for version 6.7.

b. The following repositories are enabled and synchronized on Satellite:

- Red Hat Enterprise Linux 8 for x86_64 - AppStream RPMs x86_64 **8.2**
- Red Hat Enterprise Linux 8 for x86_64 - BaseOS RPMs x86_64 **8.2**

For more information, see the *Importing Red Hat Content* chapter in the *Content Management Guide* for the particular version of Red Hat Satellite, for example, for version 6.7.

2. Verify that you have the Red Hat Enterprise Linux Server subscription attached:

```
# subscription-manager list --installed
+-------------------------------------------+
    Installed Product Status
+-------------------------------------------+
Product Name:   Red Hat Enterprise Linux Server
Product ID:     69
Version:        7.8
Arch:           x86_64
Status:         Subscribed
```

3. Ensure you have appropriate repositories enabled. The following commands list repositories for the 64-bit Intel architecture; for other architectures, see Appendix A, *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

You can also have the Optional or Supplementary repositories enabled; see their list in Appendix A, *RHEL 7 repositories*. In such a case, **Leapp** enables the RHEL 8 CodeReady Linux Builder or the RHEL 8 Supplementary repositories, respectively.

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

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

5. Optional: If you want to use custom repositories, configure them per instructions in Configuring custom repositories.

6. 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.

7. Ensure you have the system locale set to **en_US.UTF-8**:

```
$ cat /etc/locale.conf
```

If the locale is different, follow instructions in How to change system locale on RHEL7? .

8. Update all packages to the latest RHEL 7 version:

```
# yum update
```

9. Reboot the system:

```
# reboot
```

10. Install the **Leapp** utility:

```
# yum install leapp leapp-repository
```

Note that currently you need version 0.10.0-2 or later of both the **leapp** and **leapp-repository** packages.

11. Download additional required data files (RPM package changes and RPM repository mapping) attached to the Knowledgebase article Data required by the Leapp utility for an in-place upgrade from RHEL 7 to RHEL 8 and place them in the **/etc/leapp/files/** directory. This is

necessary for a successful upgrade. Note that currently you need data files from the **leapp-data7.tar.gz** archive or later.

12. If GRUB is installed outside of the default location, which is /**boot**, export the respective environment variable as follows:

```
# export LEAPP_GRUB_DEVICE="/path_to_device"
```

13. Ensure you have any configuration management (such as **Salt**, **Chef**, **Puppet**, **Ansible**) disabled or adequately reconfigured to not attempt to restore the original RHEL 7 system.

14. 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.

15. Ensure 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. For example, you can use 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?. Alternatively, you can use LVM snapshots, or RAID splitting. In case of upgrading a virtual machine, you can create a snapshot of the whole VM.

CHAPTER 3. REVIEWING THE PRE-UPGRADE REPORT

To assess upgradability of your system, start the pre-upgrade process by 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 is available both in the **/var/log/leapp/leapp-report.txt** file and in the web console. The report summarizes potential problems and proposes recommended solutions. The report also helps you decide whether it is possible or advisable to proceed with the upgrade.

You have two options when assessing upgradability in the pre-upgrade phase:

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

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

IMPORTANT

During the pre-upgrade phase, **Leapp** neither simulates the whole in-place upgrade process nor downloads all RPM packages.

Reviewing a pre-upgrade report is useful also if you decide or need to redeploy a RHEL 8 system without the in-place upgrade process.

3.1. ASSESSING UPGRADABILITY FROM THE COMMAND LINE

This procedure describes how to identify potential upgrade problems during the pre-upgrade phase using the command-line interface.

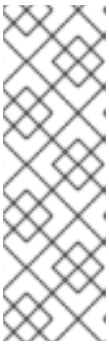
Prerequisites

- The steps listed in Chapter 2, *Preparing a RHEL 7 system for the upgrade* have been completed.

Procedure

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

```
# leapp preupgrade
```



NOTE

If you are going to use 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 going to upgrade without RHSM, add the **--no-rhsm** option.

2. Examine the report in the **/var/log/leapp/leapp-report.txt** file, and manually resolve all the reported problems before proceeding with the in-place upgrade.

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

This procedure describes how to identify potential problems in the pre-upgrade phase and how to apply automated remediations using the web console.

Prerequisites

- The steps listed in Chapter 2, *Preparing a RHEL 7 system for the upgrade* have been completed.

Procedure

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

```
# yum install cockpit-leapp
```

2. Navigate to the web console in your browser and log in as **root** or as a user with sufficient privileges. See Managing systems using the RHEL 7 web console for more information about the web console.

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

```
# leapp preupgrade
```

NOTE

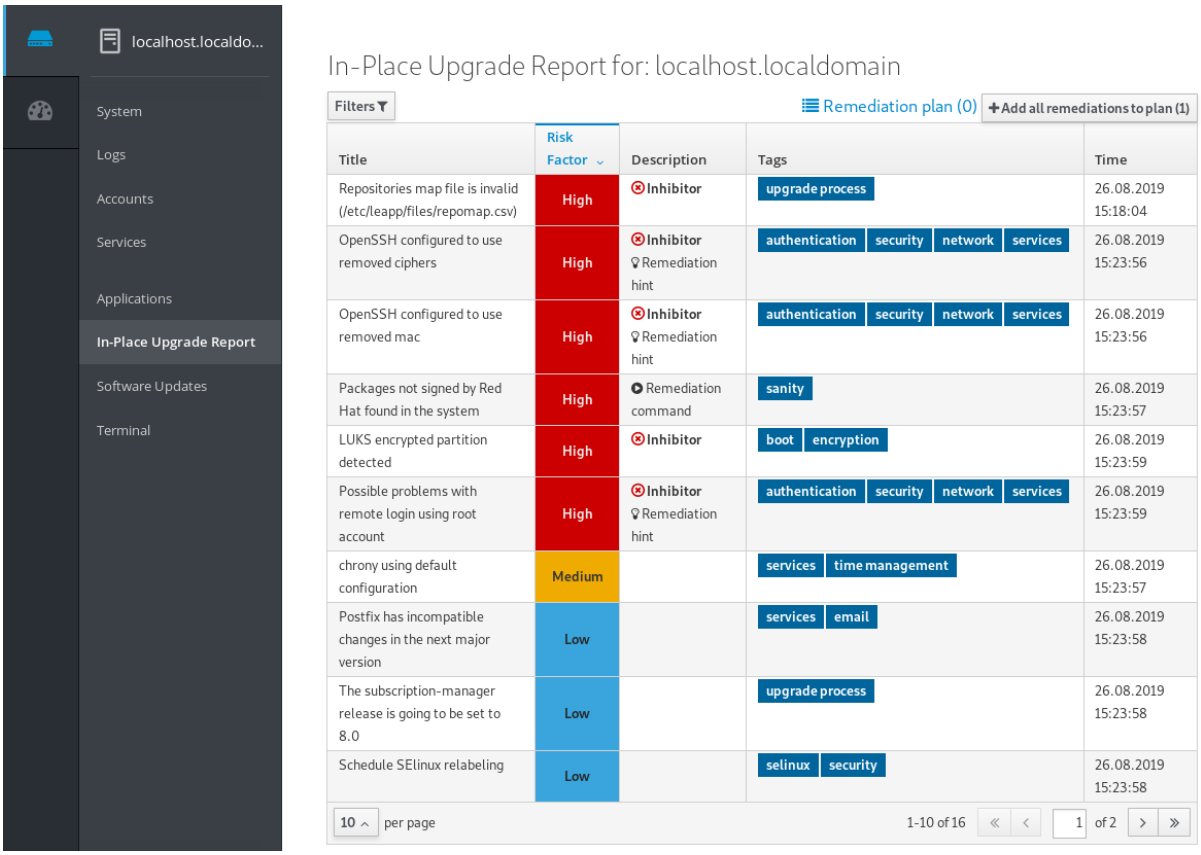
If you are going to use custom repositories from the **/etc/yum.repos.d/** directory for the upgrade, enable the selected repositories as follows:

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

If you are going to upgrade without RHSM, add the **--no-rhsm** option.

4. In the web console, select **In-place Upgrade Report** from the left menu.

Figure 3.1. In-place upgrade report in the web console

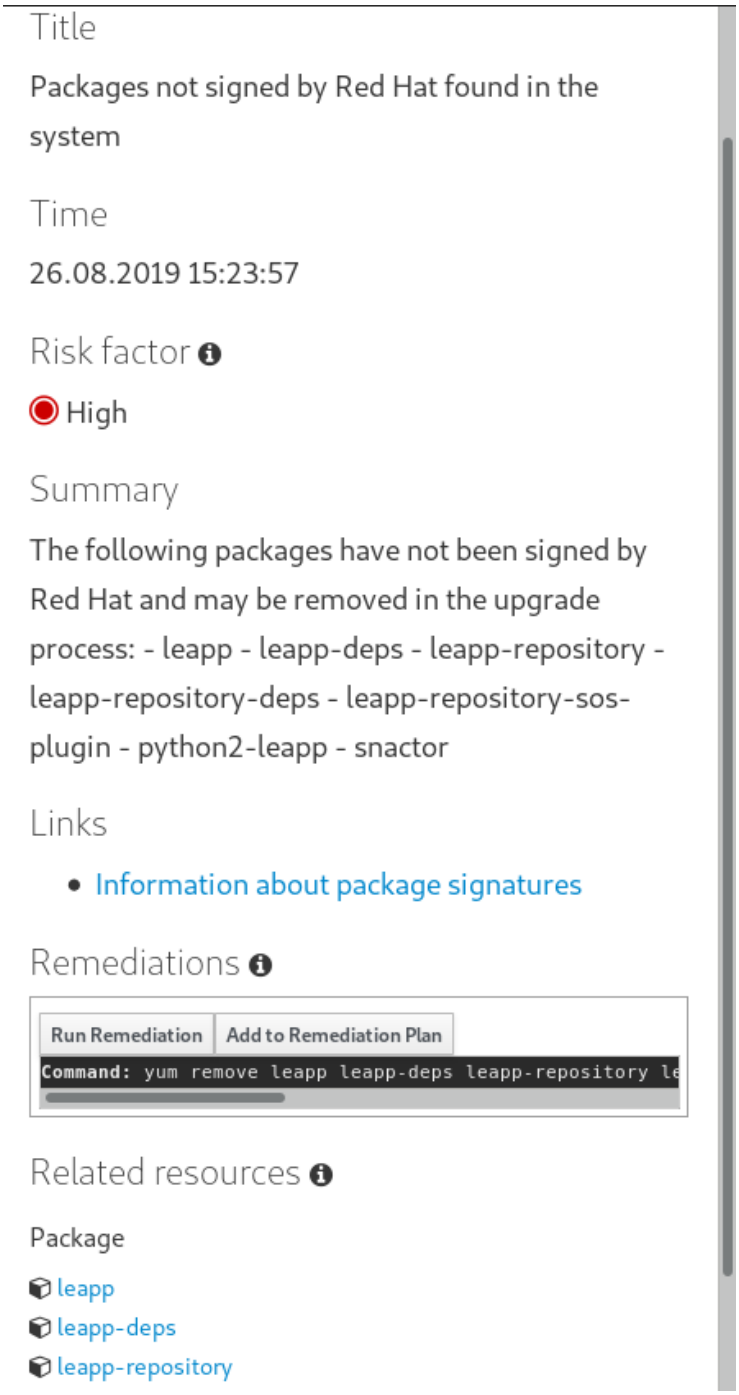


The report table provides an overview of the problems found, their risk assessment, and remediations (if available).

- Risk factor:
  - 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
- Inhibitor - will inhibit (hard stop) the upgrade process, otherwise the system could become unbootable, inaccessible, or dysfunctional
- Remediation - an actionable solution to a reported problem:
  - Remediation command - can be executed directly through the web console
  - Remediation hint - instructions on how to resolve the problem manually

5. Examine the content of the report. You can sort the table by clicking a header. To open a detail pane, click a selected row.

Figure 3.2. Detail pane

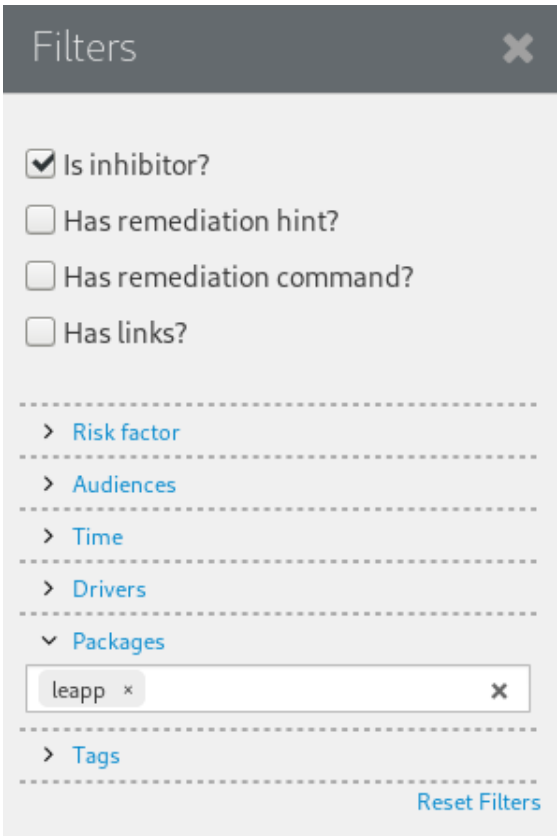


The detail pane displays the following additional information:

- Summary of the problem and links to Knowledgebase articles describing the problem in more detail
- Remediations - you can run or schedule an automated remediation (if available), and see its results when applied
- Affected system resources: packages, repositories, files (configuration, data), disks, volumes

6. Optionally filter the results. Click the **Filters** button in the top left corner above the report and apply a filter based on your preferences. Filter categories are applied in conjunction with one another.

Figure 3.3. Filters



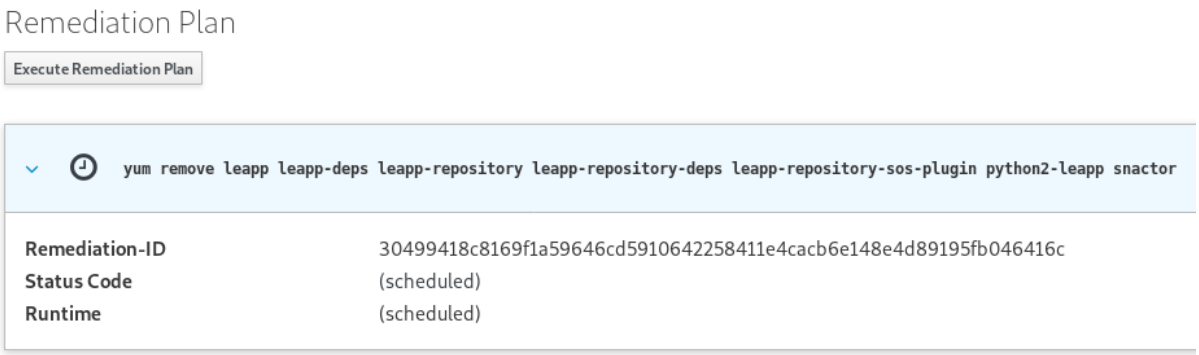
7. Select issues for which you want to apply an automated remediation. You have two options:

   a. Choose individual items by clicking the **Add to Remediation Plan** button in the detail pane. Alternatively, you can execute individual remediations directly by clicking **Run Remediation** in the detail pane.

   b. Select all items for which a remediation is available by clicking the **Add all remediations to plan** button in the top right corner above the report.

8. Open the remediation plan by clicking the **Remediation plan** link in the top right corner above the report. The remediation plan provides a list of all executed or scheduled remediations.

Figure 3.4. Remediation plan



9. Process all scheduled remediations by clicking **Execute Remediation Plan**. The following information is displayed for each remediation entry:

   - A unique ID of the remediation
   - Exit status of the command

- Elapsed time of the executed remediation
- Standard output
- Standard error

10. After executing selected remediations, generate the pre-upgrade report again by using the **leapp preupgrade** command, examine the new report, and take additional remediation steps if needed.

CHAPTER 4. PERFORMING THE UPGRADE FROM RHEL 7 TO RHEL 8

This procedure describes how to upgrade to RHEL 8 using the **Leapp** utility.

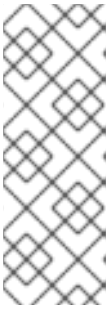
Prerequisites

- The steps listed in Chapter 2, *Preparing a RHEL 7 system for the upgrade* have been completed, including a full system backup.
- The steps listed in Chapter 3, *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
```



NOTE

If you are going to use 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 going to upgrade without RHSM, add the **--no-rhsm** option.

At the beginning of the upgrade process, **Leapp** performs the pre-upgrade phase described in Chapter 3, *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 Chapter 7, *Troubleshooting*.

2. Manually reboot 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 run the **leapp upgrade** command with the **--reboot** option and skip this manual step.

If a failure occurs, investigate logs as described in Chapter 7, *Troubleshooting*.

3. Log in to the RHEL 8 system and verify its state as described in Chapter 5, *Verifying the post-upgrade state of the RHEL 8 system*.

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

CHAPTER 5. VERIFYING THE POST-UPGRADE STATE OF THE RHEL 8 SYSTEM

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

Prerequisites

- The system has been upgraded following the steps described in Chapter 4, *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 8.2 (Ootpa)
```

- Check the OS kernel version:

```
# uname -r
4.18.0-193.el8.x86_64
```

  Note that **.el8** is important.

- 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:      8.2
Arch:         x86_64
Status:       Subscribed
```

  - Verify that the release version is correctly set to 8.2:

```
# subscription-manager release
Release: 8.2
```

    Note that when the release version is set to 8.2, you will be receiving **yum** updates only for this specific version of RHEL. If you want to unset the release version to be able to consume updates from the latest minor version of RHEL 8, use the following command:

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

- 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 6. 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. This section guides you when securing your upgraded RHEL systems.

6.1. 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 steps 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 steps

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

6.2. SETTING SYSTEM-WIDE CRYPTOGRAPHIC POLICIES

Crypto 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
```

RHEL 8.2 also introduces customization of system-wide cryptographic policies. For details, see the Customizing system-wide cryptographic policies with policy modifiers and Creating and setting a custom system-wide cryptographic policy sections.

Additional resources

- For more information , see the Using system-wide cryptographic policies and the **update-crypto-policies(8)** man page.

6.3. REMEDIATING THE SYSTEM TO A SECURITY BASELINE

The OpenSCAP suite provides remediations to make your system compliant with security baselines, such as PCI-DSS, OSPP, or ACSC E8. Use the steps in the following procedure for changing your system settings to conform with the PCI-DSS profile.

IMPORTANT

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.

Prerequisites

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

Procedure

1. Use the **oscap** command with the **--remediate** option:

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

   You can replace *pci-dss* in the previous example by a profile required by your scenario.

2. Restart your system:

```
# reboot
```

Verification steps

1. Evaluate the system of how it complies with the PCI-DSS profile, and save results to the *pcidss_report.html* file:

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

Additional resources

- For more information, see the Scanning the system for security compliance and vulnerabilities and the **scap-security-guide(8)** and **oscap(8)** man pages.

CHAPTER 7. TROUBLESHOOTING

This chapter lists troubleshooting resources and tips.

7.1. 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 **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 Section 3.2, “Assessing upgradability and applying automated remediations through the web console”.

7.2. TROUBLESHOOTING TIPS

Pre-upgrade phase

- Verify that your system meets all conditions listed in Chapter 1, *Planning an upgrade*.
- Make sure you have followed all steps described in Chapter 2, *Preparing a RHEL 7 system 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 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 Section 3.2, “Assessing upgradability and applying automated remediations through the web console”.

Download phase

- If a problem occurs during downloading RPM packages, examine transaction debug data located in the **/var/log/leapp/dnf-debugdata/** directory.

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 Chapter 5, *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.

7.3. KNOWN ISSUES

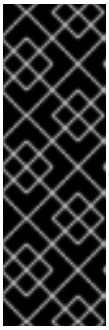
- Network teaming currently does not work when the in-place upgrade is performed while Network Manager is disabled or not installed.
- If you use an HTTP proxy, Red Hat Subscription Manager must be configured to use such a proxy, or the **subscription-manager** command must be executed with the **--proxy <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 is installed on an FCoE Logical Unit Number (LUN) and connected to a network card that uses the **bnx2fc** driver, the LUN is not detected in RHEL 8 after the upgrade. Consequently, the upgraded system fails to boot. (BZ#1718147)
- 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 is not included in the list of removed drivers (located at **/etc/leapp/repos.d/system_upgrade/el7toel8/actors/kernel/checkkerneldrivers/files/removed_drivers.txt**), **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 at the moment. 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 the respective 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. Consequently, 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, performing the in-place upgrade might result in locking you out of the system. To work around this problem, reconfigure your RHEL 7 system to not use **pam_krb5** or **pam_pkcs11** before you start the upgrade process.

- On IBM Z systems, **Leapp** always expects a DASD disk attached. Consequently, if the **/etc/dasd.conf** file does not exist, the in-place upgrade fails. To work around this problem, create an empty **dasd.conf** file by using the **touch > /etc/dasd.conf** command. (BZ#1783248)

7.4. OBTAINING SUPPORT

To open a support case, select *RHEL 8* 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 on 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 8. RELATED INFORMATION

- Red Hat Enterprise Linux technology capabilities and limits
- Considerations in adopting RHEL 8
- Customizing your Red Hat Enterprise Linux in-place upgrade
- How do I upgrade from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7?
- Upgrading from RHEL 6 to RHEL 8
- How to convert from CentOS or Oracle Linux to RHEL
- Red Hat Insights Documentation

APPENDIX A. RHEL 7 REPOSITORIES

Before the upgrade, ensure you have appropriate repositories enabled as described in step 3 of the procedure in Chapter 2, *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**
64-bit ARM	Base	**rhel-7-for-arm-64-rpms**
	Extras	**rhel-7-for-arm-64-extras-rpms**
IBM POWER8 (little endian)	Base	**rhel-7-for-power-le-rpms**
	Extras	**rhel-7-for-power-le-extras-rpms**
IBM POWER9 (little endian)	Base	**rhel-7-for-power-9-rpms**
	Extras	**rhel-7-for-power-9-extras-rpms**
IBM Z	Base	**rhel-7-for-system-z-rpms**
	Extras	**rhel-7-for-system-z-extras-rpms**
IBM Z (Structure A)	Base	**rhel-7-for-system-z-a-rpms**
	Extras	**rhel-7-for-system-z-a-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**
64-bit ARM	Optional	**rhel-7-for-arm-64-optional-rpms**
	Supplementary	N/A

Architecture	Repository	Repository ID
IBM POWER8 (little endian)	Optional	**rhel-7-for-power-le-optional-rpms**
	Supplementary	**rhel-7-for-power-le-supplementary-rpms**
IBM POWER9 (little endian)	Optional	**rhel-7-for-power-9-optional-rpms**
	Supplementary	**rhel-7-for-power-9-supplementary-rpms**
IBM Z	Optional	**rhel-7-for-system-z-optional-rpms**
	Supplementary	**rhel-7-for-system-z-supplementary-rpms**
IBM Z (Structure A)	Optional	**rhel-7-for-system-z-a-optional-rpms**
	Supplementary	N/A

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.