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: 2021-06-02
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
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

MAKING OPEN SOURCE MORE INCLUSIVE .................................................. 3

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION .......................... 4

CHAPTER 1. PLANNING AN UPGRADE .................................................. 5

CHAPTER 2. PREPARING A RHEL 7 SYSTEM FOR THE UPGRADE .............. 7

CHAPTER 3. REVIEWING THE PRE-UPGRADE REPORT ............................ 12
  3.1. ASSESSING UPGRADABILITY FROM THE COMMAND LINE .............. 12
  3.2. ASSESSING UPGRADABILITY AND APPLYING AUTOMATED REMEDIATIONS THROUGH THE WEB CONSOLE .......................... 13

CHAPTER 4. PERFORMING THE UPGRADE FROM RHEL 7 TO RHEL 8 ........... 18

CHAPTER 5. VERIFYING THE POST-UPGRADE STATE OF THE RHEL 8 SYSTEM ............................................................................. 20

CHAPTER 6. PERFORMING POST-UPGRADE TASKS .................................. 21

CHAPTER 7. APPLYING SECURITY POLICIES ......................................... 22
  7.1. CHANGING SELINUX MODE TO ENFORCING ................................. 22
  7.2. SETTING SYSTEM-WIDE CRYPTOGRAPHIC POLICIES ................... 23
  7.3. REMEDIATING THE SYSTEM TO A SECURITY BASELINE ............... 23

CHAPTER 8. TROUBLESHOOTING ......................................................... 25
  8.1. TROUBLESHOOTING RESOURCES .............................................. 25
  8.2. TROUBLESHOOTING TIPS ......................................................... 25
  8.3. KNOWN ISSUES ........................................................................ 27
  8.4. OBTAINING SUPPORT ............................................................. 29

CHAPTER 9. RELATED INFORMATION .................................................... 31

APPENDIX A. RHEL 7 REPOSITORIES ................................................... 32
Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
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 upgrade 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 7.9 on the 64-bit Intel, IBM POWER 8 (little endian), and 64-bit IBM Z architectures
    - RHEL 7.6 on architectures that require kernel version 4.14: IBM POWER 9 (little endian) or 64-bit IBM Z (Structure A)
    - RHEL 7.7 when on SAP HANA on the 64-bit Intel architecture
    See Supported in-place upgrade paths for Red Hat Enterprise Linux for more information.
  - Minimum hardware requirements for RHEL 8 met
  - Access to up-to-date RHEL 7.9 and RHEL 8.4 content provided; see Preparing a RHEL 7 system for the upgrade, step 1 for details.

- **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 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.

- **Satellite** - If you manage your hosts through Satellite, you can upgrade multiple hosts simultaneously from RHEL 7 to RHEL 8 using the Satellite web UI. For more information, see Upgrading Hosts from RHEL 7 to RHEL 8.
- **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.

- **Public Clouds** - The in-place upgrade is supported for on-demand instances on Amazon Web Services (AWS) and Microsoft Azure, using [Red Hat Update Infrastructure (RHUI)](#).

- **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 the remaining Public Clouds (Huawei Cloud, Alibaba Cloud, Google Cloud) that use Red Hat Update Infrastructure but not Red Hat Subscription Manager (RHSM) for a RHEL subscription.

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, navigate 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.
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 [Planning an upgrade](#).

**Procedure**

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

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

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

b. 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 6.8.

c. All required repositories are enabled and synchronized with the latest updates and published on Satellite. 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 or x86_64 7.9
   - 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 8.4
   - Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
     rhel-8-for-x86_64-baseos-rpms
     x86_64 8.4

   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 6.8.

d. The content host belongs to one of the following:

   - A Content View containing the above RHEL 7 and RHEL 8 repositories.
   - The Default Organization View Content View and the Library life cycle environment.
     For more information, see the Managing Content Views chapter in the Content Management Guide for the particular version of Red Hat Satellite, for example, for version 6.8.

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

   # subscription-manager list --installed
   +---------------------------------------------------------------+
   | Installed Product Status                                      |
   +---------------------------------------------------------------+
You should see Server in the product name and Subscribed as the status.

3. 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:

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

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

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

   **NOTE**

   You can also have the Optional or Supplementary repositories enabled; see their list in 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:

   ```bash
   # 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:

   ```bash
   # 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`:

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

   If the locale is different, follow instructions in [How to change system locale on RHEL7?](#).

8. 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-config-manager --enable rhui-rhel-7-server-rhui-extras-rpms
# yum -y install rhui-azure-rhel7 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.

9. If you manage containers in Docker, recreate those containers with the appropriate container images 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?

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

# yum update

11. Reboot the system:

# reboot

12. Install the Leapp utility:

# yum install leapp leapp-repository

   Note that currently you need version 0.12.1 or later of the leapp package and version 0.14.0 or later of the leapp-repository package.

13. Ensure you have access to the latest version of additional required data files (RPM package changes, RPM repository mapping, unsupported drivers, and unsupported PCIs).
   a. If you are using RHSM for the upgrade, the system has access to cloud.redhat.com, and you have not downloaded an earlier version of the required data files, no further action is required from you. The data files are automatically downloaded from cloud.redhat.com. This also applies to developer subscriptions.
   b. Download the data files 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-data14.tar.gz archive or later. This is necessary for a successful upgrade in the following scenarios:
      i. You are upgrading on a public cloud using RHUI. If you do not have a Red Hat subscription or Red Hat Customer Portal account, create a no-cost RHEL developer subscription so that you can access the Knowledgebase article and download required
data packages. For more information, see How do I get a no-cost Red Hat Enterprise Linux Developer Subscription or renew it?

ii. Your system does not have internet access.

iii. You are using RHSM for the upgrade and you previously downloaded an older version of the required data files but did not perform the upgrade, for example to create automated scripts. You can also delete your older version of the data files to initiate the automatic download of the latest file version.

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

15. 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.

16. 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.

17. 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.

18. If you are upgrading with Red Hat Subscription Manager and have disabled the subscription-manager plug-in in yum or yum4, re-enable the plug-in. For more information, see Enabling, configuring, and disabling yum plug-ins.

To determine whether the subscription-manager plug-in is enabled in yum, run the following command:

```
# yum 2>&1 | head
```

Review the generated list of Loaded plugins and determine whether subscription-manager is included.
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.

In certain configurations, Leapp generates true/false questions to determine how to proceed. All questions are stored in `/var/log/leapp/answerfile` and in the pre-upgrade report in the Missing required answers in the answer file message. Leapp inhibits the upgrade if you do not provide answers to all the questions.

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.

NOTE

You can process the pre-upgrade report 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.

3.1. ASSESSING UPGRADABILITY FROM THE COMMAND LINE

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

Prerequisites

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

Procedure

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

   ```bash
   # 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 or using RHUI, add the --no-rhsm option.

2. Provide answers to each question required by Leapp by either of the following methods:
   a. Execute the leapp answer command, specifying the question you are responding to and your confirmed answer.

```
# leapp answer --section question_section.confirm=answer
```

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

```
# leapp answer --section remove_pam_krb5_module_check.confirm=True
```

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; see Leapp answerfile.

1. 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

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

Prerequisites

- The steps listed in 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 configured in the /etc/sudoers file. 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 or using RHUI, 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
  - Info - informational with no expected impact to the system or 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**

<table>
<thead>
<tr>
<th>Title</th>
<th>Packages not signed by Red Hat found in the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>26.08.2019 15:23:57</td>
</tr>
<tr>
<td>Risk factor</td>
<td>High</td>
</tr>
</tbody>
</table>

**Summary**

The following packages have not been signed by Red Hat and may be removed in the upgrade process: - leapp - leapp-deps - leapp-repository - leapp-repository-deps - leapp-repository-sos-plugin - python2-leapp - snactor

**Links**

- Information about package signatures

**Remediations**

<table>
<thead>
<tr>
<th>Run Remediation</th>
<th>Add to Remediation Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command: yum remove leapp leapp-deps leapp-repository</td>
<td></td>
</tr>
</tbody>
</table>

**Related resources**

- leapp
- leapp-deps
- leapp-repository

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
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. Review and answer questions required by Leapp in the web console. Each unanswered question appears as a Missing required answers in the answer file title in the Upgrade Report. Select a title to answer the question:
   a. To confirm the default True answer, select Add to Remediation Plan to execute the remediation later or Run Remediation to execute the remediation immediately.
   b. To select the non-default answer instead, perform either of the following:
      i. Execute the leapp answer command, specifying the question you are responding to and your confirmed answer.

# leapp answer --section question_section.confirm=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_krb5_module_check.confirm=False
```

ii. 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`; see Leapp answerfile example.

**Figure 3.4. Missing unanswered Leapp question**

9. 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 3.5. Remediation plan**

**Remediation Plan**

Execute Remediation Plan

<table>
<thead>
<tr>
<th>Remediation-ID</th>
<th>Status Code</th>
<th>Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>30499418b8169f1a59646cd5910642258411e4cac6e148e4d89195fb046416c</td>
<td>(scheduled)</td>
<td>(scheduled)</td>
</tr>
</tbody>
</table>

10. 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

11. 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

Upgrade to RHEL 8 using the Leapp utility.

Prerequisites

- The steps listed in Preparing a RHEL 7 system 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
```

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 or using RHUI, add the `--no-rhsm` option.

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 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 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. Complete post-upgrade tasks as described in Performing post-upgrade tasks. Especially, re-evaluate and re-apply your security policies.
CHAPTER 5. VERIFYING THE POST-UPGRADE STATE OF THE RHEL 8 SYSTEM

This procedure lists verification steps 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 8.4 (Ootpa)
  ```

- Check the OS kernel version:

  ```
  # uname -r
  4.18.0-304.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: 8.4 |
    | Arch: x86_64 |
    | Status: Subscribed |
    +-----------------------------------------+
    ```

  - Verify that the release version is set to 8.4 immediately after the upgrade:

    ```
    # subscription-manager release
    Release: 8.4
    ```

- 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. PERFORMING POST-UPGRADE TASKS

This procedure lists major tasks 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.

- The status of the in-place upgrade has been verified 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 remaining RHEL 7 packages.
   a. Locate remaining RHEL 7 packages:
      ```
      # rpm -aq | grep -v -e '[.]+el8' -e '^gpg-pubkey-' -e '^libmodulemd1-' -e 'katello-ca-consumer'
      ```
   b. Determine the old kernel version:
      ```
      # cd /lib/modules && ls -d *.el7*
      ```
   c. Remove weak modules from the old 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
      ```
   d. Remove the old kernel from the bootloader entry:
      ```
      # /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
      ```

2. If you upgraded using RHUI on AWS or Microsoft Azure and your software certification is not available on a later minor release version, lock your system to a minor release version supported by your certification.
   ```
   # echo '8.x' > /etc/yum-vars/releasever
   ```

3. Re-evaluate and re-apply your security policies. Especially, change the SELinux mode to enforcing. For details, see Applying security policies.
CHAPTER 7. 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.

7.1. 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:

   ```bash
   # 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:

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

3. Configure the SELINUX=enforcing option:

   ```bash
   # 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:

   ```bash
   # reboot
   ```

Verification

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

- Troubleshooting problems related to SELinux
- Changing SELinux states and modes

### 7.2. 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:

```bash
$ 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:

```bash
# 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 policy modifiers and Creating and setting a custom system-wide cryptographic policy sections.

### 7.3. 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:

   ```bash
   # 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:

   ```bash
   # reboot
   ```

Verification

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

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

Additional resources

- Scanning the system for security compliance and vulnerabilities
- `scap-security-guide(8)` man page
- `oscap(8)` man pages
CHAPTER 8. TROUBLESHOOTING

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

8.1. 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.

8.2. 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 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 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?
Red Hat Enterprise Linux 8 Upgrading from RHEL 7 to RHEL 8

- 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 8.1. 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.

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:

```bash
# 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.

### 8.3. KNOWN ISSUES

The following are Known Issues you may encounter when upgrading from RHEL 7 to RHEL 8.

- 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/remove_d_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)

- If a name of a third-party package (not signed by Red Hat) installed on your system is the same as of a package provided by Red Hat, the in-place upgrade fails. To work around this problem, choose 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

- During an in-place upgrade, the docker package is removed without a warning. If you use containers in RHEL, migrate to Podman prior to upgrading to RHEL 8. For instructions, 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?. (BZ#1858711)

- Due to 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 an IdM environment from RHEL 7 to RHEL 8 is possible because both versions of RHEL prefer stronger AES encryption types by default:

<table>
<thead>
<tr>
<th>Version of IdM</th>
<th>Default encryption types</th>
<th>Additional supported encryption types</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 7 Identity Management (IdM)</td>
<td>AES-128, AES-256</td>
<td>3DES</td>
</tr>
<tr>
<td>RHEL 8</td>
<td>AES-256</td>
<td></td>
</tr>
</tbody>
</table>

Due to 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 an 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  
eaes128-cts | camellia256-cts  
camellia128-cts  
des3-hmac  
arcfour-hmac
RHEL 8 | aes256-cts  
eaes128-cts | aes256-sha2  
eaes128-sha2  
camellia256-cts  
camellia128-cts  
arcfour-hmac [a]

[a] RC4 encryption has been deprecated and disabled by default in RHEL 8, as it is considered less secure than the newer AES-128 and AES-256 encryption types. For more information on 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 on re-keying Kerberos principals to use stronger encryption types, see [Retiring DES from MIT Kerberos Documentation](#).

- The in-place upgrade fails on systems with Software Redundant Array of Independent Disks (RAID). (BZ#1957192)
- Systems with a disabled GRUB bootloader 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 bootloader entry as described in [Chapter 6: Performing post-upgrade tasks](#). (BZ#1955099)

### 8.4. OBTAINING SUPPORT

You can 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:

  ```bash
  # 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 9. RELATED INFORMATION

You can refer to the following instructional materials:

- Red Hat Enterprise Linux technology capabilities and limits
- Considerations in adopting RHEL 8
- Customizing your Red Hat Enterprise Linux in-place upgrade
- Automating your Red Hat Enterprise Linux pre-upgrade report workflow
- Upgrading from RHEL 6 to RHEL 7
- Upgrading from RHEL 6 to RHEL 8
- How to convert from CentOS or Oracle Linux to RHEL
- 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
APPENDIX A. RHEL 7 REPOSITORIES

Before the upgrade, ensure you have appropriate repositories enabled as described in step 3 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:

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Repository</th>
<th>Repository ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit Intel</td>
<td>Base</td>
<td>rhel-7-server-rpms</td>
</tr>
<tr>
<td></td>
<td>Extras</td>
<td>rhel-7-server-extras-rpms</td>
</tr>
<tr>
<td>IBM POWER8 (little endian)</td>
<td>Base</td>
<td>rhel-7-for-power-le-rpms</td>
</tr>
<tr>
<td></td>
<td>Extras</td>
<td>rhel-7-for-power-le-extras-rpms</td>
</tr>
<tr>
<td>IBM POWER9 (little endian)</td>
<td>Base</td>
<td>rhel-7-for-power-9-rpms</td>
</tr>
<tr>
<td></td>
<td>Extras</td>
<td>rhel-7-for-power-9-extras-rpms</td>
</tr>
<tr>
<td>IBM Z</td>
<td>Base</td>
<td>rhel-7-for-system-z-rpms</td>
</tr>
<tr>
<td></td>
<td>Extras</td>
<td>rhel-7-for-system-z-extras-rpms</td>
</tr>
<tr>
<td>IBM Z (Structure A)</td>
<td>Base</td>
<td>rhel-7-for-system-z-a-rpms</td>
</tr>
<tr>
<td></td>
<td>Extras</td>
<td>rhel-7-for-system-z-a-extras-rpms</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Repository</th>
<th>Repository ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit Intel</td>
<td>Optional</td>
<td>rhel-7-server-optional-rpms</td>
</tr>
<tr>
<td></td>
<td>Supplementary</td>
<td>rhel-7-server-supplementary-rpms</td>
</tr>
<tr>
<td>IBM POWER8 (little endian)</td>
<td>Optional</td>
<td>rhel-7-for-power-le-optional-rpms</td>
</tr>
<tr>
<td></td>
<td>Supplementary</td>
<td>rhel-7-for-power-le-supplementary-rpms</td>
</tr>
<tr>
<td>IBM POWER9 (little endian)</td>
<td>Optional</td>
<td>rhel-7-for-power-9-optional-rpms</td>
</tr>
<tr>
<td></td>
<td>Supplementary</td>
<td>rhel-7-for-power-9-supplementary-rpms</td>
</tr>
<tr>
<td>Architecture</td>
<td>Repository</td>
<td>Repository ID</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>IBM Z</td>
<td>Optional</td>
<td>rhel-7-for-system-z-optional-rpms</td>
</tr>
<tr>
<td></td>
<td>Supplementary</td>
<td>rhel-7-for-system-z-supplementary-rpms</td>
</tr>
<tr>
<td>IBM Z (Structure A)</td>
<td>Optional</td>
<td>rhel-7-for-system-z-a-optional-rpms</td>
</tr>
<tr>
<td></td>
<td>Supplementary</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**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.