Leapp explained

Leapp is the supported tool used to perform in-place system upgrades from one major version of Red Hat® Enterprise Linux® to another. With Leapp, you can upgrade with confidence and benefit from the new features of Red Hat Enterprise Linux without having to reinstall your systems.

Why should I upgrade?

Read "Top reasons to upgrade to Red Hat Enterprise Linux Checklist"

Upgrading helps ensure that business continuity is maintained as customers benefit from using supported products which have the latest enhancements, fixes, and patches, along with the new features which accompany a new major version of Red Hat Enterprise Linux.

Performance improvements in Red Hat Enterprise Linux lower your total cost of ownership, influence productivity, and ensure that you are maximizing your technology investment.

Red Hat Enterprise Linux operates on a predictable 3-year major release cycle and your subscription is valid for any currently supported version of Red Hat Enterprise Linux. This gives you access to the latest emerging technology, which you can take advantage of as new versions become available. Each major version of Red Hat Enterprise Linux is supported for 10 years and is split into 2 support phases.

The 1st phase, which is 5 years after general availability (GA), is full support. New features are added, new hardware is supported, issues and bugs are fixed. For the second 5-years, the release enters maintenance support, which continues the publication of Critical and Important rated security errata and selected other features or bug-fix enhancements. After the 10-year normal lifecycle has concluded, customers may purchase a Red Hat Extended Life Cycle Support Add-On, which will allow an additional 2 years of support including "Critical and Important" security errata. Visit Red Hat Enterprise Linux life cycle page for details.

Customers benefit from several new features by upgrading to Red Hat Enterprise Linux, which include:

- Updated software provided by application streams provides newer language runtimes, databases, and other applications throughout the full support phase of a Red Hat Enterprise Linux major release.
- Red Hat Enterprise Linux container tools, like Podman, Buildah, and Skopeo that support the building, deployment, and management of containers.
- Kernel live patching (kpatch) which allows you to patch the kernel for select important and critical common vulnerabilities and exposures (CVEs) without rebooting.
- Performance observability tools using eBPF-based tools to gain insight into aspects of system performance.

- Flatpak support to run applications which are typically used for desktop applications.
- Cgroup2 that provides streamlined capabilities to regulate the resources consumed by processes.

There are a number of automation and management enhancements, including an improved web console interface for smoother administration.

Automation enhancements include:

- New system roles for Red Hat Enterprise Linux, powered by Red Hat Ansible® Automation Platform, to automate management at scale.
- Red Hat Lightspeed (formerly Red Hat Insights), which is contained in every Red Hat Enterprise Linux subscription, proactively scans for vulnerabilities, role omissions, and other predefined criteria.

For those focused on getting the most out of your hardware, it is worth noting that Red Hat Enterprise Linux generally 9 outperforms Red Hat Enterprise Linux 7 and 8. A few changes which facilitate this include:

- New disk elevators for the kernel.
- New tuned performance profiles.

What is Leapp and why should I use it?

Visit upgrading Red Hat Enterprise Linux 6 to 8 for product information.

Upgrading your servers could be challenging, but Red Hat Enterprise Linux ships with Leapp as the supported upgrade management tool, which delivers a single path to upgrading to the next major version of Red Hat Enterprise Linux. Leapp lets users keep the original subscription (attached to the system), system configurations, custom repositories, and third-party applications.

Leapp is included with Red Hat Enterprise Linux 7, 8, 9, and 10, allowing you to upgrade from one major version to the next. You can use Ansible Automation Platform to perform back-to-back conversions moving from Red Hat Enterprise Linx 7 to 10 in a single downtime event.

Red Hat Enterprise Linux 6 users need to upgrade to Red Hat Enterprise Linux 7 (using other tooling) before upgrading to Red Hat Enterprise Linux 8 or 9 using Leapp.

The table below lists the benefits of upgrading your server with Leapp.

In-place upgrade with Leapp	Reinstallation
Preserves configuration	Configuration data needs to be backed up and restarted
Machines retain existing subscription data	Machines have to be subscribed using subscription-manager
Positively influences productivity through automation	Additional time and cost

How does it work?

Understanding how Leapp works will improve your ability to perform a successful upgrade. Using Leapp is a two-phase process which consists of an upgradability analysis and the actual upgrade. Post-upgrade reboots are required, and it is important that this is accounted for when planning your upgrade.

For a single host using Leapp, the upgradability analysis is based on upgrade considerations, which are downloaded as metadata from *cloud.redhat.com*.

For hosts connected to Red Hat Satellite, the metadata needs to be distributed by Satellite to the servers using Leapp. The upgradability analysis can then be performed at scale using the Leapp plugin for Red Hat Satellite.

The upgradability analysis generates a report which may contain items for you to resolve before the upgrade is performed.

Leapp uses several Python programs as part of a workflow. These Python programs are called actors and can make changes to your system.

Read "Using Red Hat Satellite to upgrade with Leapp"

An example of an actor is **CheckOSRelease** which will check if the current Red Hat Enterprise Linux minor version is supported. If not, it will inhibit the upgrade process.

If you have an upgrade consideration which is not being addressed by the existing set of actors, you can write your own custom actor to remediate, inhibit, or inform you of these considerations. Your actor can then be incorporated into the Leapp workflow.

Leapp is integrated with Red Hat Lightspeed to scan your registered population to determine which machines are eligible for an upgrade.

Upgrading with Leapp can be executed via the command line or Red Hat Satellite.

Limitations

Before proceeding with upgrading your server, you need to understand a few notable limitations of using Leapp:

- It can only be used to upgrade from one major version of Red Hat Enterprise Linux to the following major version.
- Leapp will not work if your system uses disk encryption for the root filesystem.
- VDO devices must be converted to being managed by LVM.
- Network-based multipath or network storage mounts like iSCSI or network file system (NFS) cannot be used for a system partition.
- On-demand instances in public cloud which use the Red Hat Update Infrastructure (this is different then Red Hat Subscription Manager) are not eligible for being upgraded using Leapp.

I'm ready to upgrade—where do I start?

Let's see what an upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8 would look like. An upgrade from Red Hat Enterprise Linux 8 to Red Hat Enterprise Linux 9 would follow a similar workflow. Ensure that you have updated your system to Red Hat Enterprise Linux 7.9 using **yum update:**

```
[root@leapp7to8 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.9 (Maipo)
```

The **leapp** package needs to be installed. Ensure that your machine is subscribed to the Red Hat CDN or to your Satellite server, with the Red Hat Enterprise Linux 7 Extras channel enabled. This may be verified using the command:

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-7-server-extras-rpms
Repo Name: Red Hat Enterprise Linux 7 Server - Extras (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/7Server/$basearch/extras/os
Enabled:   1


Repo ID:   rhel-7-server-rpms
Repo Name: Red Hat Enterprise Linux 7 Server (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/$releasever/$basearch/os
Enabled:   1
```

If the rhel-7-server-extras-rpms repository is not enabled, you can enable it using:

```
[root@leapp7to8 ~]# subscription-manager repos --enable
rhel-7-server-extras-rpms
```

Leapp can now be installed on Red Hat Enterprise Linux 7 using:

```
[root@leapp7to8 ~]# yum install -y leapp
```

If you are upgrading from Red Hat Enterprise Linux 8 to Red Hat Enterprise Linux 9, review the following steps to install the leapp in-place upgrade utility. Red Hat Enterprise Linux 8 servers may need to be updated before upgrading to Red Hat Enterprise Linux 9. Consult Supported in-place upgrade paths for Red Hat Enterprise Linux for additional details.

```
[root@leapp8to9 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.6 (Ootpa)
```

The **leapp** and **leapp-upgrade-el8toel9** packages need to be installed and both packages are available in the **rhel-8-for-x86_64-appstream-rpms** repository. Install them using:

```
[root@leapp8to9 ~]# yum install -y leapp leapp-upgrade-el8toel9
```

If you previously performed an in-place upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8, remove the **/root/tmp_leapp_py3** directory if it is present on your system:

```
[root@leapp8to9 ~]# rm -rf /root/tmp_leapp_py3
```

Once you have the leapp in-place upgrade package(s) installed for your Red Hat Enterprise Linux release, your server needs to be analyzed with **leapp preupgrade** before you perform the upgrade to identify potential problems. Your system remains unmodified and it creates important files which will plot your upgrade path.

```
[root@leappXtoY ~]# leapp preupgrade
```

After running the preupgrade command, you are likely to see output similar to the below:

```
…
 output omitted
…


============================================================
                    UPGRADE INHIBITED
============================================================
```

```
Upgrade has been inhibited due to the following problems:
    1. Inhibitor: Use of NFS detected. Upgrade can't proceed
Consult the pre-upgrade report for details and possible remediation.

============================================================
                    UPGRADE INHIBITED
============================================================

Debug output written to /var/log/leapp/leapp-preupgrade.log

============================================================
                           REPORT
============================================================

A report has been generated at /var/log/leapp/leapp-report.json
A report has been generated at /var/log/leapp/leapp-report.txt

============================================================
                       END OF REPORT
============================================================

Answerfile has been generated at /var/log/leapp/answerfile
```

Noteworthy files:

/var/log/leapp/leapp-report.txt	Readable and understandable information about the leapp upgrade report
/var/log/leapp/leapp-report.json	The JSON formatted equivalent
/var/log/leapp/leapp-preupgrade.log	The debug output of the leapp preupgrade command
/var/log/leapp/answerfile	Answers to the questions the leapp upgrade command asks

The upgradability analysis report is stored in **/var/log/leapp/leapp-report.txt** and may have important considerations for you to take action on before you perform the upgrade. These considerations may require input from you which can be handled by following the instructions inside the report.

Addressing the Leapp preupgrade considerations

There may be several action items for you to address in the Leapp preupgrade report in /var/log/leapp/leapp-report.txt. An ***inhibitor*** is a blocking item which you will need to address in order to proceed with the upgrade. If inhibitors are not resolved, a leapp upgrade will not be performed on the system.

The ***risk factor*** describes the effect of an upgrade consideration using the following keys:

High	Very likely to result in a deteriorated state
Medium	Could affect both the system and applications
Low	Should not affect the system but could have an effect on applications
Info	Informational with no expected effect to neither the system nor applications

The ***title*** identifies an element of the Leapp preupgrade report and the summary provides you with more information.

The ***summary*** provides a short description of the issue detected that may need to be addressed.

A ***remediation*** is an actionable solution to a reported problem. Common remediation types include:

- editing a configuration file.
- running a command which changes the way your system behaves.
- remediation via the Leapp answerfile.
- remediation affecting modularity software from the Red Hat Enterprise Linux 7 Software Collections Library, such as Python, PHP, Node.js, PostgreSQL, etc.
- temporarily unmounting NFS exports.

Examples of upgrade considerations for high and medium risk factors are showcased in this section and structured to include:

- The message reported in the Leapp report–in the example snippet.
- The software subsystem affected.
- An explanation of what the reported item means.
- Action you should take.
- The consequences of not addressing the reported actionable item.

Your systems may exhibit different considerations dependent on the version of Red Hat Enterprise Linux you are upgrading to and your configuration.

Example 1: A high risk inhibitor requiring temporary changes to your system

This is an example of a high rated inhibitor issue reported by the preassessment report. If this issue is not corrected, a leapp upgrade run on this system will present an error and not upgrade the system. Besides the message itself, we will review how to resolve this issue on the system.

```
Risk Factor: high (inhibitor)
Title: Use of NFS detected. Upgrade can’t proceed
Summary: NFS is currently not supported by the inplace upgrade.
We have found NFS usage at the following locations:
- One or more NFS entries in /etc/fstab
- Currently mounted NFS shares

Remediation: [hint] Disable NFS temporarily for the upgrade if possible.
Key: 9881b25faceeeaa7a6478bcdac29afd7f6baaaed
```

What if I don’t take care of this note?

It is an inhibitor and will prevent the upgrade from proceeding until the appropriate action is taken. The risk factor is high because changes are expected to be made to the local server only and not NFS shares.

What subsystem is affected?

NFS mounts.

What does it mean?

NFS mounts cannot be used during the upgrade process and must be unmounted and disabled until the upgrade has finished.

What must I do?

Edit /etc/fstab to temporarily comment out NFS shares and unmount currently mounted NFS shares. Temporarily stop and disable autofs.service. The NFS entries and autofs.service can be re-enabled once the upgrade concludes.

```
[root@leapp8to9 ~]# systemctl disable –now autofs.service
```

Example 2: A high risk inhibitor requiring changes to an existing configuration file

This is largely applicable to upgrading from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8.

```
Risk Factor: high (inhibitor)

Title: Possible problems with remote login using root account

Summary: OpenSSH configuration file does not explicitly state the option
PermitRootLogin in sshd_config file, which will default in Red Hat
Enterprise Linux8 to “prohibit-password”.

Remediation: [hint] If you depend on remote root logins using passwords,
consider setting up a different user for remote administration or adding
“PermitRootLogin yes” to sshd_config.

Key: 3d21e8cc9e1c09dc60429de7716165787e99515f
```

What if I don’t take care of this note?

It is an inhibitor and will prevent the upgrade from proceeding but it is worth noting that the risk factor is high and incorrectly addressing this item could prevent you from remotely logging into your server using secure shell (SSH).

What subsystem is affected?

The ssh server (sshd.service).

What does it mean?

This snippet tells you that there is a high impact change between the way that the SSH server works between Red Hat Enterprise Linux 7 and Red Hat Enterprise Linux 8. Password authentication is disallowed for the root user in Red Hat Enterprise Linux 8 by default. In Red Hat Enterprise Linux 7, the implied default value for PermitRootLogin is yes, but in Red Hat Enterprise Linux 8, the implied default value is prohibit-password.

An implied configuration directive appears as a comment inside /etc/ssh/sshd_config, but it is not a comment. It appears to inform you of the directive’s default values.

What must I do?

Ensure that you are able to login as another user—either with a password or without.

You must explicitly set a value for PermitRootLogin inside /etc/ssh/sshd_config. The value could be yes to allow the root user to login via ssh or no to prevent this. What matters is that the directive is explicitly set.

Linux man pages are wonderful sources of additional information. Use the command **man sshd_config** and search for the string *PermitRootLogin* to learn more about this configuration directive.

Example 3: A high risk inhibitor requiring the use of the leapp answerfile

This specific issue is largely applicable to upgrading from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8. The unique element of this example is that it requires remediation using the leapp answerfile, a file in which data can be automatedly passed to the leapp utility.

```
Risk Factor: high (inhibitor)

Title: Missing required answers in the answer file

Summary: One or more sections in answerfile are missing user choices:
remove_pam_pkcs11_module_check.confirm

For more information consult https://leapp.readthedocs.io/en/latest/
dialogs.html

Remediation: [hint] Please register user choices with leapp answer cli
command or by manually editing the answerfile.

[command] leapp answer --section remove_pam_pkcs11_module_check.
confirm=True

Key: d35f6c6b1b1fa6924ef442e3670d90fa92f0d54b
```

What if I don't take care of this note?

It is an inhibitor and will prevent the upgrade from proceeding until you authorize the removal of the pam_pkcs11 module. The risk factor is high because you may have the *requisite or required* control values associated with the pam_pkcs11 module in your PAM configuration, and the removal of this module in Red Hat Enterprise Linux8 could lock you out of your system.

This upgrade item may **only** be resolved by using the Leapp answer file.

What subsystem is affected?

Authentication (pam).

What does it mean?

This snippet tells you that the pam_pkcs11 module is removed from Red Hat Enterprise Linux8 and its functionality is now provided by sssd.

What must I do?

Edit /var/log/leapp/answerfile as follows:

```
[remove_pam_pkcs11_module_check]

confirm = True
```

Or run the following command to edit the answerfile /var/log/leapp/answerfile:

```
leapp answer --section
remove_pam_pkcs11_module_check.confirm=true
```

You must also verify that there are other ways for you to authenticate which do not rely on the pam_pkcs11 module.

This can be verified by running **grep pam_pkcs11 /etc/pam.d/***

Visit managing software from an application stream for the hands-on lab

Example 4: A high risk, non-inhibiting consideration which effects Python programs post-upgrade

This example largely applies to machines upgrading from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8. Unlike earlier examples, it is not an inhibitor, meaning the leapp upgrade tool will perform an upgrade even if this detected issue is not resolved. Knowing whether or not this issue is required to be resolved would be determined by the system administrator. Knowing whether or not this machine uses Python2 based applications and whether those applications are compatible with Python3 provided by the upgraded operating system also would be determined by the system administrator.

```
Risk Factor: high

Title: Difference in Python versions and support in Red Hat Enterprise
Linux 8

Summary: In Red Hat Enterprise Linux 8, there is no ‘python’
command. Python 3 (backward incompatible) is the primary Python
version and Python 2 is available with limited support and
limited set of packages. Read more here: https://access.redhat.
com/documentation/en-us/red_hat_enterprise_linux/8/html-single/
configuring_basic_system_settings/#using-python3

Remediation: [hint] Please run “alternatives --set python /usr/bin/
python3” after upgrade

Key: 0c98585b1d8d252eb540bf61560094f3495351f5
```

What if I don’t take care of this note?

This is not an inhibitor and ignoring the remediation will not prevent the leapp upgrade command proceeding. The risk factor is high because the unversioned python command (/usr/bin/python) is not available by default in Red Hat Enterprise Linux 8. Running the python interpreter directly (e.g. from a terminal) or indirectly (another process runs the command for you) will fail.

What subsystem is affected?

Python and applications which depend on the unversioned /usr/bin/python command.

What does it mean?

While Python 2 is deprecated in favor of Python 3, it may still be installed using application streams. The application streams repository offers several Python modules which you can install in parallel on your server. You should always specify the version of Python either installing it, invoking it, or interacting with it. The unversioned Python command is not available by default, but it may still be configured should you wish.

What must I do?

You could run the following command to ensure that /usr/bin/python3 is used as the default version of python:

```
alternatives --set python /usr/bin/python3
```

Any applications which explicitly require Python 2 need to reference /usr/bin/python2 or you could set the default version of Python to Python 2 by using the following command:

```
alternatives --set python /usr/bin/python2
```

Example 5: A medium risk, non-inhibiting consideration

This example is largely applicable to upgrading from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8

```
Risk Factor: medium

Title: chrony using default configuration

Summary: default chrony configuration in Red Hat Enterprise Linux8 uses
leapsectz directive, which cannot be used with leap smearing NTP servers,
and uses a single pool directive instead of four server directives

Key: c4222ebd18730a76f6bc7b3b66df898b106e6554
```

What if I don't take care of this note?

This is not an inhibitor and will not prevent the leapp upgrade from proceeding. The risk factor is medium because Network Time Protocol (NTP) clients who are configured to get their time from multiple servers, which do not implement the same leap smear or do not all implement a leap smear, will get different times from different servers during the leap smear. This may cause NTP clients to stop updating their clocks or randomly jump between servers.

What subsystem is affected?

Time synchronization using chrony.

What does it mean?

Chrony implements time synchronization using NTP. In Red Hat Enterprise Linux8, the pool directive is used by default to reference a pool of NTP servers with the same capabilities. Using several server directives which reference NTP servers with different capabilities could cause degraded time synchronization.

What must I do?

From /etc/chrony.conf, remove any *leapsectz* and *leapfile* directives and use the pool directive instead of the server directive inside /etc/chrony.conf. This will ensure that NTP servers of the same capabilities are used.

Should you wish to synchronize your system time with explicitly defined servers, ensure that all servers have the same capabilities.

Read "Top reasons to upgrade to Red Hat Enterprise Linux Checklist"

I'm ready to upgrade!

After you have addressed issues identified in the preupgrade report, it is recommended to rerun the **leapp preupgrade** command and revisit the report file to ensure that there are no omissions, which would prevent a successful upgrade.

Once your system is ready to be upgraded, run either command: **leapp upgrade** or **leapp upgrade --reboot**

Visit what is BOOM and how to install it?

For more about managing system upgrades with snapshots

The **leapp upgrade** command queues the upgrade process and completion requires several reboots. It is important that this is planned for. Before the first boot, you are able to continue using your current version of Red Hat Enterprise Linux.

The **leapp upgrade reboot** command reboots the server automatically.

First boot: The bootloader automatically initializes a special upgrade environment using the menu entry **Red Hat Enterprise Linux-Upgrade-Initramfs**. It is within this upgrade environment that your server will be upgraded. A backup is required should you wish to revert the upgrade and continue using the previous major version of Red Hat Enterprise Linux.

Second boot: SELinux labels will be restored and your server will reboot once more.

Third boot: You can validate your upgrade and enjoy your new Red Hat Enterprise Linux experience.

Validate the version of Red Hat Enterprise Linux currently being used:

```
[root@leapp7to8 ~]# rpm -q redhat-release
redhat-release-8.6-0.1.el8.x86_64
```

```
[root@leapp8to9 ~]# rpm -q redhat-release
redhat-release-9.0-2.17.el9.x86_64
```

If you are upgrading from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8, you may expect to see a repository called *rhel-8-server-rpms*, but Red Hat Enterprise Linux8 features 2 repositories: *rhel-8-for-x86_64-baseos-rpms* which provides the core set of underlying OS functionality and *rhel-8-for-x86_64-appstream-rpms* which includes additional user space applications, runtime languages, and databases in support of varied workloads and use cases. This may be verified as follows:

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-8-for-x86_64-appstream-rpms
```

```
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/x86_64/
appstream/os
Enabled:   1


Repo ID:   rhel-8-for-x86_64-baseos-rpms
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/x86_64/baseos/os
Enabled:   1
```

Once your system has been upgraded and rebooted, you should revisit **/var/log/leapp/leapp-report.txt** that now has your post-upgrade report, which could have additional action items for you to complete.

Do you have any tips for me?

Before you begin, you may want to consider the following recommendations.

sosreport

Consider generating a sosreport so we can provide you with support should you need it.

1. Use **yum install sos** to ensure the sos package is installed.
2. Generate the report using the **sosreport** command.
3. Copy the generated tar archive from **/var/tmp/** to a safe location should you require Red Hat Support.

Make sure you have a backup

In the event of unforeseen circumstances that lead to your system being inoperable or your data inaccessible, the ability to recover timely and resume operations is of paramount importance. Data backups facilitate the recovery process, and you should have already been performing them. But it should be emphasized that you need to backup your data before using Leapp to upgrade your servers.

Use your current tools to implement a backup strategy.

- Identify the data which is pertinent to your server being operable.
- Backup your data to a secure location outside of the server being upgraded.
- Test your backup to ensure that the data was successfully backed up.
- Ensure that you are able to restore data from your backup.
- Validate your disaster recovery plan to ensure that you are sufficiently prepared for the potential loss of your server.

Use Red Hat Lightspeed

Red Hat Lightspeed can be used to determine your upgrade eligibility.

Take advantage of Red Hat Satellite Server

Red Hat Satellite Server can take advantage of the Leapp plugin to scan and upgrade eligible systems at scale.

Use the web console

Consider using the web console to facilitate the upgrade process, as it presents the preupgrade report in an easy-to-read format.

You need to ensure that you have the cockpit and cockpit-leapp packages installed using **yum install cockpit cockpit-leapp**.

Then use **systemctl enable --now cockpit.socket** to activate the cockpit socket.

Add the web console port to your firewall using **firewall-cmd --add-port 9090/tcp** and then make certain the rule is added to the permanent firewall configuration using **firewall-cmd --add-port 9090/tcp --permanent**.

Now login to the web console at *https://your_server_name:9090*

Satellite repository requirements

If you are using the Satellite Server for managing packages, make sure you have the following repositories available:

- rhel-7-server-rpms
- rhel-7-server-extras-rpms
- rhel-8-for-x86_64-baseos-rpms
- rhel-8-for-x86_64-appstream-rpms

yum versionlock

If you have used the yum versionlock command to lock packages to a specific version, clear them with **yum versionlock clear**.