Oracle Linux 8

Release Notes for Oracle Linux 8

F12584-14

September 2022

ORACLE®

Oracle Linux 8 Release Notes for Oracle Linux 8,

F12584-14

Copyright © 2019, 2022, Oracle and/or its affiliates.

Contents

3   Known Issues

Preface

Oracle Linux 8: Release Notes for Oracle Linux 8 provides information about the new features and known issues in the Oracle Linux 8 release. The information applies to both x86_64 and 64-bit Arm (aarch64) architectures. This document might be updated after it is released.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

For information about the accessibility of the Oracle Help Center, see the Oracle Accessibility Conformance Report at https://www.oracle.com/corporate/accessibility/templates/t2-11535.html.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees,

customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1
About Oracle Linux 8

The current Oracle Linux 8 release contains new features and enhancements that improve performance in different areas including automation and management, security and compliance, container management, and developer tools. These enhancements are especially designed to make the operating system adaptable to different types of deployment from strictly on-premises installations, hybrid deployments that combine on-premises and cloud installations, and full cloud deployment.

System Requirements and Limitations

To determine whether your hardware is supported on the current Oracle Linux 8 release, check the Hardware Certification List at https://linux.oracle.com/hardware-certifications. Note that hardware is listed as it becomes available and is validated.

Note that Oracle Linux 8 for the aarch64 platform is primarily engineered for use with Ampere™ eMAG™-based EVK platform and the Marvell ThunderX2® processor. Other hardware may be supported and added to the Hardware Certification List in future.

CPU, memory, disk and file system limits for all Oracle Linux releases are described in Oracle Linux: Limits.

Supported Architectures

The following architectures are supported in Oracle Linux 8:

- Intel `x86_64`
- AMD 64-bit

> **Note:**
>
> The 64-bit Arm (aarch64) platform can be installed as a developer preview release in Oracle Linux 8. See #unique_9.

Shipped Kernel

Oracle Linux 8 ships with the `kernel-4.18.0-80.el8` Red Hat Compatible Kernel (RHCK) kernel package.

The Oracle Linux release is tested as a bundle, as shipped on the installation media image. When installed from the installation media image, the minimum kernel version supported is the one that is included in the image. Downgrading kernel packages is not supported, unless recommended by Oracle Support.

About the Unbreakable Enterprise Kernel

The Unbreakable Enterprise Kernel (UEK) is a Linux kernel built by Oracle and supported through Oracle Linux support. UEK is tested on Arm (aarch64), Intel x86, and AMD x86 (x86_64) platforms. Each release contains additional features, bug fixes, and updated drivers to provide support for key functional requirements, improve performance, and optimize the kernel for use on Oracle products such as Oracle's Engineered Systems, Oracle Cloud Infrastructure, and large enterprise deployments for Oracle customers.

Typically, a UEK release contains changes to the kernel ABI relative to a previous UEK release. These changes require recompilation of third-party kernel modules on the system. To minimize impact on interoperability during releases, the Oracle Linux team works closely with third-party vendors regarding hardware and software that have dependencies on kernel modules. Thus, before installing the latest UEK release, verify its support status with your application vendor.

The kernel ABI for a UEK release remains unchanged in all subsequent updates to the initial release.

The kernel source code for UEK is available after the initial release through a public git source code repository at https://github.com/oracle/linux-uek.

For more information about UEK such as tutorials, notices, and release notes of different UEK versions, go to Unbreakable Enterprise Kernel documentation.

User Space Compatibility

Oracle Linux maintains user space compatibility with Red Hat Enterprise Linux (RHEL) that is independent of the kernel version that underlies the operating system. Existing applications in user space continue to run unmodified on UEK R6 and UEK R7, with no required recertifications for RHEL certified applications.

Obtaining Installation Images

The following installation images for the current Oracle Linux 8 release are available:

- Full ISO of Oracle Linux for typical on-premise installations
- Boot ISO of Oracle Linux for network installations
- Boot ISO of the supported UEK release for installing on hardware that is supported only on UEK
- Source DVDs

You can download these images from the following locations. Note that the images in these locations are for both the x86_64 and aarch64 platforms, unless indicated otherwise:

- Oracle Software Delivery Cloud at https://edelivery.oracle.com
- Oracle Linux yum server at https://yum.oracle.com/oracle-linux-downloads.html

> **✎ Note:**
>
> Oracle Linux 8 (aarch64) is available as a developer preview on Oracle Linux 8.0 and Oracle Linux 8.1. The developer preview images for Oracle Linux 8 for the 64-bit Arm (aarch64) platform are available at https://www.oracle.com/linux/downloads/linux-beta8-downloads.html.

To prepare a downloaded image for installing Oracle Linux, see Oracle Linux 8: Installing Oracle Linux.

For information about the available ISOs for the three most recent updates to the Oracle Linux releases, refer to https://yum.oracle.com/oracle-linux-isos.html.

For developers who are making use of the Raspberry Pi hardware platform, Oracle provides an unsupported developer release image, which includes the firmware that is required to boot this platform. For more information about making use of the Raspberry Pi hardware platform, see Install Oracle Linux on a Raspberry Pi.

> **✎ Note:**
>
> Aside from installation ISOs, you can also use Oracle Linux images to create compute instances on Oracle Cloud Infrastructure. For information about these images, see the release notes for the specific image that you are using on the *Oracle Cloud Infrastructure Documentation* page.
>
> To use Oracle Linux on Oracle Cloud Infrastructure, see https://docs.oracle.com/iaas/oracle-linux/home.htm.

Upgrading From Oracle Linux 7 to Oracle Linux 8

You can upgrade an Oracle Linux 7 system to the latest Oracle Linux 8 release by using the `leapp` utility. For step-by-step instructions, as well as information about any known issues that you might encounter when upgrading your system, see Oracle Linux 8: Performing System Upgrades With Leapp.

2

New Features and Changes

This chapter describes the new features, major enhancements, bug fixes, and other changes that are included in this release of Oracle Linux 8.

Oracle Linux 8 Software Distribution and Management

Oracle Linux 8 introduces the following software management features, enhancements, and changes.

Oracle Linux 8 Content Distribution Changes

The core operating system and associated packages for a typical Oracle Linux 8 server are distributed through Applications Streams. Application Streams contain all of the necessary system components and a range of applications that were previously distributed in Software Collections, as well as other products and programs.

About Oracle Linux 8 Repositories

The yum repositories on the Oracle Linux 8 ISO, which form the base repositories for an Oracle Linux 8 installation, are divided into two repositories: BaseOS and AppStream, both of which are available with all Oracle Linux subscriptions. These two repositories are required for the operating system to work. Additional packages may be provided in additional repositories, for example, the CodeReady Linux Builder repository.

The BaseOS repository includes the core set of packages that are required for Oracle Linux to function and includes packages that are required for all installation methods. The content of the BaseOS repository is available in RPM format. The same support terms that applied in previous releases apply to the Oracle Linux 8 release.

The AppStream repository includes packages that provide additional support for a variety of workloads, such as user-space applications, runtime languages, and databases. The AppStream repository includes content with various life cycles, which is available as traditional RPM packages and an extended format, referred to as *modules*.

The CodeReady Linux Builder repository provides the build packages that are required for developers and package maintainers to build traditionally compiled binaries that you might ship as packages with Oracle Linux. For example, this repository contains compilers, build tools, library sources, developer documentation, documentation build tools, and several other developer-related packages.

If you attempt to install packages from the `codeready_builder` yum repository or ULN channel, the system must also be subscribed to the `appstream` yum repository or ULN channel to avoid dependency issues. It is not sufficient for a system to only be subscribed to the `codeready_builder` yum repository or ULN channel and to `baseos_latest`.

For information about package changes in this release, see Package Changes from the Upstream Release.

About Application Streams

Oracle Linux 8 introduces the concept of Application Streams, where multiple versions of user-space components can be delivered and updated more frequently than the core operating system packages. Application Streams contain all of the necessary system components and a range of applications that were previously distributed in Software Collections, as well as other products and programs.

The content in the AppStream repository is available in two formats: RPM and modules, which are an extension of the RPM format. Traditional RPM packages are available for immediate installation. Traditional package management methods and installation are transparently supported for all content. Modules are similar to Software Collections, in that they provide a mechanism by which multiple, major versions of a component are made available for installation in the AppStream repository. Note that modules are easier than Software Collections to install and use. The appropriate combination of modules and streams is automatically used to enable the installation of packages that rely on modular features.

The AppStream repository contains the following components:

- **Modules**: Are a set of RPM packages that are grouped and installed together. Modules can contain several streams that consist of multiple versions of applications that can be installed. A module stream is enabled to provide system access to the RPM packages that are contained within that module stream.

  A typical module can contain the following different types of packages: packages with an application, packages with the application's specific dependency libraries, packages with documentation for the application, and packages with helper utilities

- **Module streams**: Contain a different version of packages and their dependencies. Modules can have multiple streams and each stream receives updates independently. Although modules can have multiple streams, only one of its streams can be enabled and provide its packages to enable the installation of the respective version of content. Typically, the stream with the latest version is selected as the default stream and will be used when operations do not specify a particular stream or a different stream is not enabled.

  > **Note:**
  >
  > Oracle recommends that you use the latest stream for any module that is installed, even though other streams may continue to receive limited support.

- **Module profiles**: List certain packages that are to be installed at the same time for a particular use case. Each module can have one or more profiles.

For more detailed information about modules, including examples, see the chapter on DNF in Oracle Linux: Managing Software on Oracle Linux.

DNF Support Added

Oracle Linux 8 supports a new version of the Yum tool that is based on the DNF technology. DNF, or *Dandified yum*, is a software package manager that installs, updates, and removes packages on RPM-based Linux distributions. Yum DNF (often

referred to simply as DNF) provides several advantages over the Yum v3 tool that was used in previous releases. Most notably, DNF provides support for modular content, as well as a strict and stable API for extensions and plugins.

Keep the following key points in mind when using DNF:

- DNF is compatible with Yum v3 when used from the command line or when editing or creating configuration files.

- You can use the `dnf` command and all of its options similarly to how you used the `yum` command in Oracle Linux 7 and previous releases.

- You can install Yum packages under the names that were previously used by using the `provides` command.

- To aid in the transition from Yum v3 to DNF, packages include compatibility symlinks to enable binaries, configuration files, and directories to be found in their usual locations.

- Because the Python API that is provided by Yum v3 and the Libdnf C API are likely to change during the Oracle Linux 8 life cycle, users are encouraged to migrate plugins and scripts to the new DNF Python API, as this API is stable and fully supported in Oracle Linux 8.

For a comparison of command-line, plugin, and utility differences between Yum v3 and DNF, see Comparing Yum Version 3 With DNF.

RPM Improvements

Oracle Linux 8 ships with version 4.14 of RPM. This version of RPM introduces many improvements over the previously supported RPM version 4.11.

With RPM version 4.14, you can install `debuginfo` packages in parallel. This version of RPM also provides support for several new features, including the following:

- Weak dependencies
- Rich or boolean dependencies
- Packaging of files that are greater than 4 GB
- File triggers

Other important changes include stricter spec-parser, simplified signature checking of output in non-verbose mode, as well as additions and deprecations in macros.

One significant change in this version of RPM is that it now validates the entire package contents before starting an installation. In Oracle Linux 7, RPM verified the payload contents of individual files during unpacking, which could be inefficient, especially if the payload was damaged.

Also, in the previous version of RPM, hashes on individual files were performed on uncompressed data, thus causing RPM to be susceptible to decompressor vulnerabilities. In Oracle Linux 8, the entire package is validated as a separate step prior to installation using the best available hash. In this release, packages are built by using a new `SHA-256` hash on the compressed payload. For signed packages, the payload hash is additionally protected by the signature; and, therefore, cannot be altered without breaking a signature and other hashes on the package header. Note that older packages use the `MD5` hash for the header and payload unless the hash has been disabled by configuration. In addition, you can use the `%_pkgverify_level` macro to enforce signature verification prior to installation or to disable the payload verification. You can also use the `%_pkgverify_flags` macro to limit the hashes and signatures that are allowed.

Installation, Boot, and Image Creation

Oracle Linux 8 introduces the following notable features and improvements to installing and booting a system, and creating images:

- **New kernel boot parameter added to the installer**

  A new kernel boot parameter, `inst.addrepo=name,url` , has been added to the installer. You can use this parameter to specify an additional repository during an installation. Note that the parameter has two mandatory values that must be provided: the name of the repository and a URL that points to that repository. Previously, you could only specify a base repository by setting kernel boot parameters.

- **LUKS2 disk encryption added to installer**

  By default, the Oracle Linux 8 installer uses the LUKS2 format. This change introduces several improvements such as extending the capabilities of the on-disk format and providing flexible ways to store metadata. During an installation with the installer, you can now select a LUKS version in the Custom Partitioning window. Or, you can specify these new command options in a kickstart profile by using the `autopart`, `logvol`, `part`, and `RAID` options.

- **Boom Boot Manager added**

  The Boom Boot Manager uses boot loaders that support the BootLoader Specification for boot entry configuration. Boom provides flexible boot configuration and simplifies the creation of new or modified boot entries. Boom includes a simple command-line interface (CLI) and an API that make the task of creating boot entries easier.

  Note that the Boom Boot Manager does not modify any existing boot loader configuration; it only inserts additional entries, thereby maintaining the existing configuration, as well as any distribution integration such as kernel installation and update scripts. This configuration continues to function as in previous releases.

- **Support for unified ISO added to the installer**

  In this release, the installer uses a unified ISO, which automatically loads the BaseOS and AppStream installation source repositories. The feature works for the first base repository that is loaded during an installation, but it does not work if you boot by using a different base repository and then attempt to change to the unified ISO. Doing so replaces the base repository; however, the AppStream repository is not replaced and continues to point to the original file.

- **Deprecated Kickstart commands and options**

  Several Kickstart commands and options that were available in previous releases are now deprecated. Most significantly, the `--interactive` option for the `ignoredisk` command is deprecated and should be removed from any existing kickstart configurations to prevent a fatal error during installation.

  Other deprecated commands and options include:

  - `auth`

  - `authconfig`

  - `device`

  - `deviceprobe`

- `dmraid`

- `install`

- `lilo`

- `lilocheck`

- `mouse`

- `multipath`

- `bootloader --upgrade`

- `ignoredisk --interactive`

- `partition --active`

- `reboot --kexec`

Red Hat Compatible Kernel

The following notable features, enhancements, and changes apply to the Red Hat Compatible Kernel (RHCK) that is shipped with Oracle Linux 8.

- **modinfo command updated to recognize and display the PKCS#7 module signature**

  The `modinfo` command has been updated to recognize and display signature information, such as signature key fingerprint, signer, and correct hash algorithm, for modules that are signed with CMS and PKCS#7 formatted signatures. Also, note that previous versions of the `modinfo` command incorrectly displayed these modules as signed with the MD4 hash and did not display the appropriate signature information, such as the signature key or the correct hash algorithm.

- **Some kernel modules have been moved to the `kernel-modules-extra` package**

  To increase security in Oracle Linux 8, a set of kernel modules have been moved to the `kernel-modules-extra` package, which means none of these modules are installed by default. As a consequence, non-root users cannot load these components, as they are also blocklisted by default. To use one of these kernel modules, as the `root` user, you must install the `kernel-modules-extra` package, then explicitly remove the module blocklist. As a result, non-root users will be able to load the software component automatically.

  To check whether a module was moved and is now included in the `kernel-modules-extra` package, you can run the following command:

  ```
  sudo dnf repoquery -l kernel-modules-extra
  ```

- **5-level paging added**

  T has been updated to include a new `P4d_t` software page table type. This change enables 5-level paging in Oracle Linux 8. This feature requires hardware support which may not be available on your processor type.

- **Memory management 5-level paging added**

  Memory bus limits have been extended to 57/52 bit of virtual/physical memory addressing, with 128 PiB of virtual address space and 4 PB of physical memory capacity. This extended address range allows the memory management feature in Oracle Linux 8 to enable 5-level paging, which is capable of handling an expanded address range.

The I/O memory management unit (IOMMU) code in the Linux kernel is also updated in this release to enable 5-level paging tables.

- **Support for Control Group v2 added**

  This release supports the Control Group v2 mechanism, which organizes processes hierarchically and distributes system resources along the hierarchy in a controlled and configurable manner. Unlike the previously supported version, Control Group v2 is a single hierarchy that categorizes processes based on the role of the process owner and eliminates issues with conflicting policies and multiple hierarchies.

  The Control Group v2 mechanism supports numerous controllers, including the following: CPU controller, memory controller, I/O controller, PID controller, and the RDMA controller. Note that the I/O controller, in conjunction with the memory controller, implements the control of page cache write-back IOs.

  > **Note:**
  >
  > Support for the `cpuset` Cgroup v2 controller is not currently available in Oracle Linux 8.

- **Capability for reporting eBPF-based programs and maps added to sosreport tool**

  In Oracle Linux 8, the `sosreport` tool includes the capability for reporting any loaded extended Berkeley Packet Filtering (eBPF) programs and maps.

- **bpftool added**

  Support for the `bpftool` tool has been added to the Linux kernel. This tool is used for inspection and the basic manipulation of programs and maps that are based on eBPF. The `bpftool` tool is part of the kernel source tree and is provided by the `bpftool` package, which is a subpackage of the `kernel` package.

- **Support for early kdump added**

  The `early kdump` feature enables the crash kernel and `initramfs` to load early so that it can capture `vmcore` information, including early crashes. Previously, the `kdump` service did not start soon enough to capture crash information (`vmcore`), especially for early kernel crashes. See the `/usr/share/doc/kexec-tools/early-kdump-howto.txt` file for more details.

Cockpit

Oracle Linux 8 includes the following features, enhancements, and changes for the Cockpit interface:

> **Note:**
>
> For security purposes, Cockpit usually requires that web browsers communicate with the application by using HTTPS. For more information about Cockpit usage requirements, including information about certificates and SSL and TLS versions, visit https://cockpit-project.org/guide/latest/https.html#https-certificates.

- **Cockpit packages available for installation by default**

  Cockpit packages are now included in the Oracle Linux default repositories and are available for immediate installation. For non-minimal installations, Cockpit is automatically installed. A system message that is displayed prior to login provides information about how to enable or access Cockpit.

  > **Note:**
  >
  > If your firewall is enabled, you might need to allow access for the ports that are used by cockpit. To explicitly enable the firewall ports for this service, run the following command:
  >
  > ```
  > sudo firewall-cmd --permanent --add-service=cockpit; firewall-cmd --reload
  > ```

- **Firewall section added to Cockpit Networking page**

  The new Firewall section on the Networking page provides support for enabling and disabling a firewall. You can also add, remove, and modify firewall rules in this section of the page.

- **Cockpit front page improved to display missing updates and subscriptions**

  If your Cockpit-managed system has outdated packages or a lapsed subscription, a warning is now displayed on the Cockpit front page of the system.

- **Cockpit compatibility with mobile browsers**

  In this release, you have the ability to navigate Cockpit menus and pages on several different mobile browsers. This change makes it possible to manage systems by using Cockpit from a mobile device.

- **Support for PBD rules added**

  You can now use the Cockpit interface to apply Policy-Based Decryption (PBD) rules to disks on managed systems. The use of the Clevis decryption client facilitates several security management functions in Cockpit, for example, the automatic unlocking of LUKS-encrypted disk partitions.

- **Support for managing virtual machines with Cockpit**

  The ability to add a Virtual Machine page to the Cockpit interface has been added. You can use this page to create and manage `libvirt`-based virtual machines.

Podman, Buildah, and Skopeo Container Tools Included

The `podman`, `buildah`, and `skopeo` container tools are provided in the Oracle Linux 8 release. These tools are compatible with the Open Container Initiative (OCI) and can be used

to manage the same Linux containers that are produced and managed by Docker and other compatible container engines. Because these tools are light-weight and primarily focused on a subset of features, you can run them minus the overhead of working with a daemon process.

- **Pod Manager (`podman`)**

  Oracle Linux 8 introduces the Pod Manager tool (`podman`), which is a daemonless container engine that you can use to develop, run, and manage compatible container images on Linux systems. The containers can be run as root or in rootless mode.

  The `podman` tool is built on the `libpod` library, which enables the management of containers and groups of containers, called *pods*.You can use `podman` to directly manage pods, container images, and containers on a single node, with commands such as `run`, `stop`, `start`, `ps`, `attach`, `exec`, and similar commands.

  The `podman` tool uses syntax that is similar to the `docker` command-line tool and is able to run images that are designed to run in a Docker environment. The `podman` syntax is often also simplified to make it easier to run common commands; for instance, the Docker command, `docker container ls --all`, is shortened to `podman ls --all`. Furthermore, `podman` introduces the `--latest` syntax, which can be used as shorthand for the most recently created container so that you do not have to repeatedly type the container name.

  Note that `podman` and related tools depend on cgroup v1 functionality, so this functionality should not be disabled.

  For more information about using `podman`, visit https://podman.io.

- **Buildah (`buildah`)**

  You use the `buildah` command to create container images from a working container, a Dockerfile, or from scratch. The resulting images are Open Container Initiative compliant, so they will work on any container runtime that meets the Open Container Initiative Runtime Specification, such as Docker and CRI-O.

  The `buildah` command includes several options that enable you to also do the following: inspect a container or image, mount and unmount a container, create a new container layer, and delete a container or image.

  Note that Buildah can operate without Docker or other container runtimes because it stores data separately and includes features that enable you to both build images, as well as run those images as containers. Note also that Buildah stores images in an area that is identified as `containers-storage` that is located in `/var/lib/containers`.

  The `buildah` command differs from the `docker` command in the following ways:

  - No container runtime (Docker, CRI-O, or other) is required to use Buildah because the `buildah` command bypasses the Docker daemon.

  - You can use the `buildah` command to build an image that is based on another container. You can also start with a scratch (empty) image.

  - Buildah tools are external. No build tools are included within the image itself, which means the size of the images that you build with Buildah are reduced. As a result, these smaller images require fewer resources to transport. Also, the images that you build with Buildah are more secure because you do not need to use tools like `gcc`, `make`, or `dnf` to build a container with the resulting image.

For more information about using Buildah, visit the GitHub Buildah page.

- **Skopeo (`skopeo`)**

  Skopeo is a client tool that you use to work with remote images registries to retrieve information, images, and signing content. You can use the `skopeo` command to copy container images to and from remote container registries. The tool also includes capability for signing and authenticating images remotely.

  The `skopeo` command includes several options that enable you to copy, inspect, delete, and sign images. For example, if you wanted to inspect a container image before you pull it to your system, you would use the `skopeo inspect` command. This command displays information about an image that resides in a remote container registry.

  For more information about using Skopeo, visit the GitHub Skopeo page.

Database

This release of Oracle Linux 8 ships with version 8.0 of the MySQL database software.

Desktop

In Oracle Linux 8, the GNOME desktop introduces the following features, enhancements, and changes:

- **GNOME Shell version updated to 3.27**

  This version of the GNOME Shell includes several improvements over the previous version, including the following:

  – New GNOME Boxes features

  – On-screen keyboard implemented

  – Extended device support that includes the integration of the Thunderbolt 3 interface

  – Improvements to GNOME software, `dconf-editor`, and the GNOME terminal

- **Wayland is the default display server**

  In Oracle Linux 8, both the GNOME session and GNOME Display Manager (GDM) use Wayland as the default display server. Wayland is a simpler replacement to the `X.org` server used in the previous major Oracle Linux release. Wayland, a protocol for a compositor, can be a stand-alone display server that is running on the Linux kernel's mode-setting and `evdev` input devices, an X application, or a Wayland client. The clients can be traditional applications, X servers (rootless or fullscreen), or other display servers.

  In addition, Wayland is easier to develop and maintain. Wayland provides the following other advantages over `X.org` server:

  – Stronger security

  – Improved multi-monitor handling

  – Improved user interface (UI) scaling

  – Direct control of window handling by the desktop

> **✎ Note:**
>
> Some Wayland features currently do not work as expected or are not available.

Note that the system also automatically falls back to `X.org` as the default display server when the following graphics drivers are in use:

– NVIDIA binary driver

– `cirrus` driver

– `mga` driver

– `aspeed` driver

You can disable Wayland manually as follows:

– To disable Wayland in GDM, set the `WaylandEnable=false` option in the `/etc/gdm/custom.conf` file.

– To disable Wayland in the GNOME desktop, select the legacy X11 option in the cogwheel menu that is located in the login screen after typing your login name.

• **Locating desktop packages in additional repositories not enabled by default**

In this release, additional repositories for desktop packages are not enabled by default and is indicated by the `enabled=0` line in the corresponding `.repo` file. If you attempt to install a package from one of these repositories with PackageKit, you will encounter an error indicating the application is not available. To make the package available, change the line in the respective `.repo` file with `enabled=1`.

• **GNOME Software utility replaces gnome-packagekit**

In Oracle Linux 8, the GNOME Software utility package (`gnome-software`) replaces the `gnome-packagekit` package used in previous releases. The GNOME Software utility enables you to install and update applications and `gnome-shell` extensions.

• **PackageKit updated to operate on RPM packages**

Support for operating on `rpm` packages has been added to `PackageKit`.

Developer Tools and Compilers

Oracle Linux 8 introduces numerous feature enhancements and changes to developer tools and compilers, including the following:

• **Boost C++ library updated to version 1.66**

This version of the Boost C++ library provides several enhancements and improvements over Boost version 1.53, which was used in Oracle Linux 7.

> **✎ Note:**
>
> Installing the `boost` package no longer installs the `Boost.Python` library as a dependency. To use the `Boost.Python` library, you must explicitly install the `boost-python3` or the `boost-python3-devel` packages.

- **GNU C library updated to version 2.28**

  Oracle Linux 8 provides the GNU C library version 2.28 (`glibc`), which includes security hardening features, performance improvements, Unicode version 11.0.0, and new developer features.

- **ltrace tool improved to display large structures correctly**

  Oracle Linux 8 includes an improved `ltrace` tool, which can now handle large structures and print them correctly.

- **New compat-libpthread_nonshared package added**

  Oracle Linux 8 provides the new `compat-libpthread-nonshared` package. This package enables applications that directly reference `/usr/lib64/libpthread_nonshared.a` to work properly.

- **Locale package distribution change**

  In Oracle Linux 8, languages and locales are distributed in multiple `glibc-langpack-CODE` packages. In previous releases, all locales and languages were distributed in a single package, `glibc-common`. Note also that in this release, not all locales are installed by default: just those that are selected during an installation are installed. Any additional locale packages that you require must be installed separately.

- **compat-libgfortran-48 package added**

  Oracle Linux 8 provides the new `compat-libgfortran-48` compatibility package. This package, which provides the `libgfortran.so.3` library, is provided for backwards compatibility with Oracle Linux 6 and Oracle Linux 7 applications that use the Fortran library,

- **Support for retpolines added to GCC**

  Oracle Linux 8 adds support for retpolines to the GNU Compiler Collection (GCC). A *retpoline* is a software construct that the kernel uses to reduce the overhead of mitigating Spectre Variant 2 attacks, as described in CVE-2017-5715.

- **CMake updated to version 3.11**

  The CMake build system version 3.11 is provided in the `cmake` package in Oracle Linux 8.

- **make tool updated to version 4.2.1**

  Oracle Linux 8 includes version 4.2.1 of the `make` build tool.

- **FIPS compliance for Go programs built with the Go Toolset**

  If a host system is configured in FIPS mode, the cryptographic library that is included in the Go Toolset uses the OpenSSL library version 1.1.0. Thus, any programs that are built with this version of the Go Toolset are FIPS-compliant.

  To specify that Go programs use only the uncertified, standard cryptographic routines. use the `-tags no_openssl` option of the Go compiler at build time.

- **SystemTap updated to version 4.0**

Oracle Linux 8 includes version 4.0 of the SystemTap instrumentation tool. This version of SystemTap includes several notable features and improvements over the previous version.

- **binutils updated to version 2.30**

  Oracle Linux 8 provides version 2.30 of the `binutils` package. Improvements include improved support for the new `s390x` architecture extensions, as well as improvements to assembler and linker support. Other significant changes in this version of `binutils` include the addition of new options for the `readelf`, `objdump`, and `nm` tools.

- **Performance Co-Pilot updated to version 4.1.3**

  This release includes version 4.1.3 of Performance Co-Pilot (pcp), which provides several improvements over the previous version of `pcp`.

- **Memory protection keys provided**

  In this release, hardware features that allow per-thread page protection flag changes are enabled. New `glibc` system call wrappers have been added for the following functions: `pkey_alloc()`, `pkey_free()`, and `pkey_mprotect()`. In addition, the `pkey_set()` and `pkey_get()` functions have been added. These functions allow access to per-thread protection flags.

- **Time zone data updated to new upstream default data format**

  Oracle Linux 8 includes a version of the `tzdata-2018e` package that works with the new default upstream data format and also includes negative DST (Daylight Saving Time) offsets.

- **elfutils updated to version 0.174**

  Oracle Linux 8 includes the `elfutils` version 0.174 . This version of `elfutils` provides several improvements over the previous version of the tool.

- **Valgrind updated to version 3.14**

  Oracle Linux 8 includes the Valgrind executable code analysis tool version 3.14. This version of Valgrind includes several feature enhancements and changes over the previous version of the tool.

- **GDB updated to version 8.2**

  Oracle Linux 8 includes the GDB debugger version 8.2. This version of the GDB debugger several improvements over the previous version.

- **GCC updated to version 8.2**

  In Oracle Linux 8, the GCC toolchain is based on the GCC 8.2 release series, which provides several changes and improvements over the previous version of GCC.

File Systems and Storage

Oracle Linux 8 introduces the following notable file systems and storage features, enhancements, and changes:

- **Btrfs file system removed in RHCK**

  The Btrfs file system is removed from RHCK in Oracle Linux 8. As such, you cannot create or mount Btrfs file systems when using this kernel. Also, no Btrfs

user-space packages are provided in this release. If you are using Btrfs, continue to use Oracle Linux 7.

- **OCFS2 file system support not available in RHCK**

  The OCFS2 file system is not supported on RHCK in Oracle Linux 8. If you need to use OCFS2, continue to run Oracle Linux 7.

- **NFSv3 over UDP support not available in Oracle Linux 8**

  In Oracle Linux 8, by default, the NFS server no longer opens or listens on a User Datagram Protocol (UDP) socket. Note that this change impacts NFS version 3 (NFSv3) only, as version 4 requires the Transmission Control Protocol (TCP).

- **DM Multipathing enhancements**

  Oracle Linux 8 introduces some noteworthy enhancements for the Device Mapper Multipathing (DM Multipathing) configuration, including the following:

  – New `overrides` section has been added to the `/etc/multipath.conf` file. You can enter a configuration value for all of your devices by using this section. The attributes that you set are then used by DM Multipathing for all of your devices, unless the values are overwritten by any attributes that are set in the `multipaths` section of the `/etc/multipath.conf` file for paths that contain the device. Note that this new functionality is a replacement for the `all_devs` parameter in the `devices` section of the configuration file, which is no longer supported.

  – Support for improved detection of marginal paths has been added to the `multipathd` service. This enhancement helps multipath devices avoid paths that are likely to fail repeatedly, thereby improving performance. For more details about this change, including information about the options in the `/etc/multipath.conf` file that control marginal paths behavior, see the `multipath.conf` man page.

- **SCSI Multiqueue driver support added**

  In Oracle Linux 8, block devices use multiqueue scheduling. This feature enhancement enables block layer performance to scale well with fast solid-state drives (SSDs) and multi-core systems.

  Also, the SCSI Multiqueue (`scsi-mq`) driver is enabled by default and the kernel boots with the `scsi_mod.use_blk_mq=Y` option. Note that a requirement of DM Multipathing is that the `scsi-mq` driver be active.

- **Stratis local storage manager introduced**

  Oracle Linux 8 includes the Stratis local storage management tool. Stratis enables you to perform complex storage tasks and manage your storage stack more easily by using a unified interface.

- **XFS support for shared COW data extents**

  The XFS file system now supports shared copy-on-write (COW) data extent functionality, whereby two or more files can share a common set of data blocks. This feature is similar to Copy on write (COW) functionality that is found in other file systems, where if either of the files that are sharing common blocks change, XFS breaks the link to those common blocks and then creates a new file.

  Shared COW extents are fast, space efficient, and transparent. User-space utilities can use COW extents for cloning, per-file snapshots, and out-of-band deduplication. Some kernel subsystems, such as Overlayfs and NFS, also use COW extents.

Shared COW data extents are currently disabled by default during the creation of an XFS file system, in the `xfsprogs 4.19.0-2.0.1.el8` package version. To create an XFS file system with this feature enabled, run the following command:

```
sudo mkfs.xfs -m crc=1,reflink=1 block-device
```

Future versions of `xfsprogs` are likely to enable this functionality by default.

- **Technology Preview: Clustered Bitmap on MD Raid**

  The `mdadm` command, used to manage MD Raid devices, includes the `--bitmap=clustered` option to store the bitmap for the array within a clustered environment. This feature is available as a technology preview and is unsupported on Oracle Linux 8.

Identity Management

Oracle Linux 8 introduces several major identity management features and enhancements, including a major change to how the packages that are necessary for installing an Identity Management (IdM) server and client are distributed. The following are details of this and other noteworthy identity management changes:

- **IdM packages now distributed as a module**

  Starting with Oracle Linux 8, the packages that are necessary to install an IdM (Identity Management) server and client are distributed as a module. The client stream is the default stream for the `idm` module. Note that you can download the packages that are necessary to install the client without enabling the stream.

  The IdM server *module stream* is called the `DL1` stream and it contains multiple profiles that correspond to the following different types of IdM servers: `server`, `dns`, `adtrust`, `client`, and `default`.

  To download the packages to a specific profile of the `DL1` stream, do the following:

  1. Enable the stream.

  2. Switch to using the RPMs that are delivered through the stream.

  3. Run the following command:

     ```
     sudo yum module install idm: DL1/profile-name
     ```

- **Directory Server enhancements**

  This release includes the following Directory Server enhancements:

  - **New password syntax checks:** This enhancement for Directory Server enables dictionary checks and allows or denies the use of character sequences and palindromes. The password policy syntax check employed by Directory Server enforces more secure passwords when it is enabled.

  - **Improved internal operations logging support:** Directory Server now logs the real connection and operation ID, thereby enabling you to trace the internal operation to the server or client operation that caused the operation. Previously, the server only logged the `Internal` connection keyword for internal operations. Also, the operation ID was always set to `-1`.

- **Enterprise Security Client uses the opensc library for token detection**

The Enterprise Security Client (ESC) now uses the `opensc` library for token detection instead of the `coolkey` library, which has been removed. This change causes applications to correctly detect supported tokens.

- **Certificate System supports log rotation**

  Certificate System now uses the `java.logging.util` framework, which supports log rotation. As a result of this change, you can now configure log rotation in the `/var/lib/pki/` *instance-name* `/conf/logging.properties` file, instead of using the previous logging framework method that did not support log rotation.

  See the documentation for the `java.util.logging` package for more details.

- **Local user and group resolution cached by SSSD and served through the nss_sss module**

  The resolution of local users and groups is faster in Oracle Linux 8. Note that the `root` user is never handled by the System Security Services Daemon (SSSD). As such, root resolution cannot be impacted by a potential bug in SSSD. Also, if SSSD is not running, the `nss_sss` module falls back to `nss_files`. Note that you do not have to configure SSSD because the files domain is automatically added.

- **KCM replaces KEYRING**

  In Oracle Linux 8, the default credential cache storage is the Kerberos Credential Manager (KCM), which is backed by the `sssd-kcm` daemon. This enhancement provides better support for containerized environments and is the basis for adding more features in subsequent releases. KCM overcomes the limitations of KEYRING, which is difficult to use in containerized environments because the feature does not use name-spacing and therefore cannot be used to view and manage quotas.

- **Support for administering identity management with Active Directory added**

  In this release, you can add a user ID override for an Active Directory (AD) user as a member of an Identity Management (IdM) group. This change enables the IdM LDAP server to apply access control rules to the AD user for the IdM group.

  In addition, an AD administrator can now fully administer idM without having two separate accounts. AD users can also use self-service features of the IdM user interface (UI), such as uploading SSH keys and changing personal data. However, note that some IdM features still might not be available to AD users.

- **Support for printing a HBAC rules report for an IdM domain by using sssctl added**

  In Oracle Linux 8, you can use the SSSD `sssctl` command to print an access control report for an IdM domain. This enhancement provides the ability, in certain environments (for regulatory reasons), to view the list of users and groups that can access a specific client system. Running the `sssctl access-report` *domain-name* command on an IdM client prints the parsed subset of the host-based access control (HBAC) rules in the IdM domain that applies to the client's system.

- **Support for session recording solution added**

  Oracle Linux 8 provides a session recording solution. The new `tlog` package and its associated Cockpit session player enable you to record and play back user terminal sessions. The recording can then be configured per-user or per user group by using the SSSD service. All terminal input and output is captured and stored in text-based format in a system journal. For security reasons, the input is inactive by default.

  You can also use the recording solution to audit user sessions on security-sensitive systems. You can review and analyze the recorded sessions in the event of a security

breach. In addition, you can configure session recording locally and then view the result from either the Cockpit web-based interface or by using the `tlog-play` command.

- **authselect command replaces authconfig command**

  In this release, the `authselect` command replaces the `authconfig` command. The `authselect` command simplifies user authentication configuration on Oracle Linux 8. The `authselect` command also provides a safer approach to Pluggable Authentication Modules (PAM) stack management.

  You can use the `authselect` command to configure the following authentication methods: passwords, certificates, smart cards, and fingerprints. However, note that you cannot use the `authselect` command to configure services that are required to join remote domains. For this type of configuration, use the `realmd` or `ipa-client-install` command.

Infrastructure Services

Oracle Linux 8 introduces the following infrastructure services features, enhancements, and changes:

- **GeoLite database packages replaced with Geolite2 Database packages**

  The `GeoIP` package and the legacy database that was provided for GeoLite databases in Oracle Linux 7 is no longer supported. In Oracle Linux 8, GeoLite2 databases are provided by multiple packages, including the following: the `libmaxminddb` package, which includes the library, and the `mmdblookup` command-line tool, which enables manual searching of addresses. Note that the `geoipupdate` binary from the legacy `GeoIP` package is now provided by the `geoipupdate` package. This package is capable of downloading both legacy databases and the new GeoLite2 databases.

Networking

This release of Oracle Linux 8 introduces the following features, enhancements, and improvements.

Replacement of iptables With nftables

In Oracle Linux 8, the default `iptables` network packet filtering framework been replaced with the `nftables` framework. As the designated successor to `iptables`, `ip6tables`, `arptables`, and `ebtables`, the `nftables` framework includes packet classification facilities and several improvements, which provide added convenience and improved performance over the previously used packet-filtering tools.

The `nftables` implementation provides the following improvements:

- Replacement of linear processing with lookup tables
- Single framework for both the IPv4 and IPv6 protocols
- More consistent and compact syntax
- Support for debugging and tracing in the ruleset with `nftrace`
- Netlink API for third-party applications

Note the following additional information about the `nftables` implementation:

- The `nftables` framework uses tables for storing chains, similarly to `iptables`. *Chains* contain individual rules for performing actions.

- The `nft` tool replaces all of the previously used packet-filtering framework tools.

- You can use the `libnftables` library for low-level interaction with the `nftables` Netlink API over the `libmnl` library.

- The `iptables`, `ip6tables`, `ebtables` and `arptables` tools are replaced by drop-in replacements that are `nftables`-based and use the same name.

  Although these tools behave identically to their legacy counterparts, internally, they use `nftables` with legacy `netfilter` kernel modules through a compatibility interface, as required.

  You can use the `nft list ruleset` command to observe the effect of the modules on the `nftables` ruleset. It is worth noting, however, that these tools add tables, chains, and rules to the `nftables` ruleset; and as such, some `nftables` ruleset operations, for example, the `nft flush ruleset` command, might affect rulesets that were installed by using legacy commands, as these were formerly separate.

  To determine which version of the tool is currently running, use the `iptables --version` command, as version information has been updated to include the back-end name. For example, if you are running Oracle Linux 8, you can run the `nftables`-based `iptables` tool as follows:

  ```
  iptables --version
  ```

  Running the previous command displays output similar to the following:

  ```
  iptables v1.8.2 (nf_tables)
  ```

  If the legacy version of the `iptables` tool is installed and you run the same command, the following output is displayed:

  ```
  iptables v1.8.0 (legacy)
  ```

Tools for Converting iptables Rules to the nftables Equivalents

Oracle Linux 8 provides the `iptables-translate` and `ip6tables-translate` commands for converting existing `iptables` and `ip6tables` rules to their `nftables` equivalents. In cases where extensions do not include translation support, the untranslated rule, prefixed by a hash sign (`#`), is printed by the conversion tools when you run the following command:

```
iptables-translate -A INPUT -j CHECKSUM --checksum-fill
```

The output is as follows:

```
nft # -A INPUT -j CHECKSUM --checksum-fill
```

You can use the utility to translate a dump of `iptables` rules in a single operation by running the following commands:

```
iptables-save > rules.iptables
iptables-restore-translate -f rules.iptables > rules.nft
nft -f rules.nft
```

firewalld Uses nftables by Default

In Oracle Linux 8, the `nftables` filtering subsystem is the default firewall backend for the `firewalld` daemon. If you want to change the back-end firewall, specify the `FirewallBackend` option in the `/etc/firewalld/firewalld.conf` file.

This feature change introduces the following notable differences in behavior when using `nftables`:

- The `iptables` rule executions always occur before `firewalld` rules.

- In `iptables`, `DROP` means a packet is never seen by `firewalld`, while `ACCEPT` means a packet is still subject to `firewalld` rules.

- The `firewalld` direct rules are still implemented through `iptables`, while other `firewalld` features use `nftables`.

- Direct rule execution occurs before `firewalld` generic acceptance of established connections.

IPVLAN Virtual Network Driver Added

The Oracle Linux 8 kernel supports IPVLAN virtual Network Interface Cards (NICs). This added support enables network connectivity for multiple containers by exposing a single MAC address to the local network. The enhancement makes it possible to enable network connectivity for multiple containers on a single host, thereby overcoming a possible limitation on the number of MAC addresses that are supported by the peer networking equipment.

Networking Stack Updated to Version 4.18

The networking stack in Oracle Linux 8 has been updated to version 4.18. This version of the networking stack includes several bug fixes and improvements over the previous version, including new offload features and the new `fq_codel` default transmit queue scheduling algorithm. Several additional changes were made, including improvements to the generic busy polling code, and improved scalability for the User Datagram Protocol (UDP), IPv6, routing code, as well as some transmit queue scheduling algorithms.

Removal of -ok Option From tc Command

In Oracle Linux 8, the `tc` command no longer supports the `-ok` option. One workaround is to implement code to communicate directly with the kernel through netlink. Another alternative for less time-critical applications is use a custom script to simulate `tc -batch` behavior by printing `OK` for each successful `tc` invocation.

SR-IOV Virtual Functions Added to NetworkManager

In this release, `NetworkManager` enables you to configure the number of virtual functions (VF) for interfaces that support single-root I/O virtualization (SR-IOV). `NetworkManager` also enables you to configure certain attributes of the VFs, including the MAC address, a VLAN, the spoof-checking setting, and allowed bitrates. All of the

properties that are related to SR-IOV are available in the `sriov` connection setting. See the `nm-settings(5)` man page for details.

TCP Updated to Version 4.18

Oracle Linux 8 provides version 4.18 of the Transmission Control Protocol (TCP). This version of TCP provides increased performance, as well as better scalability, and increased stability over previous versions.

Also new in this release, are the new TCP congestion algorithms, `BBR` and `NV`. These algorithms provide lower latency and better throughput than cubic in most situations.

wpa_supplicant Package Improvements

In this release, the `wpa_supplicant` package is built with `CONFIG_DEBUG_SYSLOG` enabled. This change provides the capability to read the `wpa_supplicant` log by using the `journalctl` utility rather than having to check the contents of the `/var/log/wpa_supplicant.log` file, as in previous releases.

Scripting and Dynamic Programming Languages

The following scripting and dynamic programming language changes are introduced in this release:

- **Python version 3.6 included**

  Oracle Linux 8 includes Python version 3.6. Note that this version of the Python package is not installed on your Oracle Linux 8 by default.

  The Python 2.7 package `python2` is also available for installation on your Oracle Linux 8 system; but, note that Python 2.7 is provided to facilitate a smoother transition to Python 3 and that its life cycle will be shorter than that of Python 3.

  > **✎ Note:**
  >
  > Developers may want to migrate former code that is written in Python 2 to Python 3. After the migration, the original Python 2 code becomes interpretable by the Python 3 interpreter, while also remaining interpretable for the Python 2 interpreter.

  The default `python` package, as well as the unversioned `/usr/bin/python` executable, is included in Oracle Linux 8. You should use either `python3` or `python2` directly. Or, alternatively, you can configure the unversioned `python` command by using the `alternatives` command.

- **PHP updated to version 7.2**

  Oracle Linux 8 includes PHP version 7.2, which includes several improvements over the previous version of PHP, including the following:

  - PHP now uses the FastCGI Process Manager (FPM) by default, which is safe for use with a threaded `httpd`.

- In this release, you no longer specify the `php_value` and `php-flag` variables in the `httpd` configuration files. Instead, set these variables in the pool configuration, `/etc/php-fpm.d/*.conf`.

- `PHP` script errors and warnings are now logged to `/var/log/php-fpm/www-error.log` instead of `/var/log/httpd/error.log`.

- Changing the PHP `max_execution_time` configuration variable requires that you also change the `httpd ProxyTimeout` setting so that the configurations match.

- The user who is running PHP scripts is now configured in the FPM pool configuration file, `/etc/php-fpm/d/www.conf`. Also, the `apache` user is the now the default.

- If you make configuration changes or install a new extension, you are now required to restart the `php-fpm` service for the changes to take effect.

- The following PHP extensions are removed in this release:

  * `aspell`

  * `memcache`

  * `mysql`

    The `mysqli` and `pdo_mysql` extensions are still provided by `php-mysqlnd` package.

  * `zip`

- **Ruby improvements**

  Oracle Linux 8 includes Ruby version 2.5, which provides several improvements over Ruby 2.0.0, including the following:

  - Symbols are now garbage collected.

  - Several `refinements` syntax improvements.

  - The `$SAFE=2` and `$SAFE=2` levels are obsoleted.

  - The consolidation of the Fixnum and Bignum classes into the Integer class.

  - Performance improvements, including optimization of the Hash class, improved access to instance variables, as well as performance improvements to the Mutex class.

  - The deprecation of some older APIs.

  - Updated bundled libraries, including the following: RubyGems, Rake, RDoc, Psych, Minitest, and test-unit.

  - The `mathn`, `DL`, `ext/tk`, and `XMLRPC` libraries that were previously distributed with Ruby are deprecated or no longer included.

  - The SemVer versioning scheme is now used for Ruby versioning.

- **Perl features and improvements**

  Oracle Linux 8 includes Perl version 5.26, which provides new features and improvements over the previous version of Perl. Note that in this version of Perl, some features are deprecated.

  Notable changes in this version of Perl include the following:

- Availability of Unicode 9.0.

- Addition of the `op-entry`, `loading-file`, and `loaded-file SystemTap` probes.

- Addition of the `Config::Perl::V` module to access `perl -V` data in a structured way.

  Addition of the `IO::Socket::IP` module to handle IPv4 and IPv6 sockets transparently.

- New `perl-App-cpanminus` package has been added. This package includes the `cpanm` utility, which enables you to get, extract, build, and install modules from the Comprehensive Perl Archive Network (CPAN) repository.

- Ability to use the copy-on-write mechanism when assigning scalars for improved performance.

- Hashes are now randomized by default. Also, the order in which keys and values are returned from a hash changes on each `perl` run. You can disable the randomization by setting the `PERL_PERTURB_KEYS` variable to `0`.

- The `perl` packaging is now aligned with upstream and also installs core modules. The `/usr/bin/perl` interpreter is provided by the `perl-interpreter` package, which is a change from previous releases, where the `perl` package included only a minimal interpreter and the `perl-core` package included both the interpreter and the core modules.

The following Perl features are deprecated or removed:

- The current directory (`.`) has been removed from the `@INC` module search path. This change was made for security reasons.

- The `do` statement returns a deprecation warning when it fails to load a file.

- The `do subroutine(LIST)` call is no longer supported and results in a syntax error.

- Unescaped literal `{` characters in regular expression patterns are not allowed.

- Removed lexical scope support for the `$_` variable.

- Cannot use the `defined` operator on an array or a hash, as it results in a fatal error.

- Importing functions from the `UNIVERSAL` module result in a fatal error.

- Removal of the `find2perl`, `s2p`, `a2p`, `c2ph`, and `pstruct` tools.

- Removal of the `${^ENCODING}` facility. In addition, the `encoding` pragma's default mode is no longer supported. To write source code using encoding other than UTF-8, use the encoding's `Filter` option.

Security

Oracle Linux 8 introduces the following security features, enhancements, and changes:

- **OpenSSH updated to version 7.8p1**

  The `openssh` packages have been upgraded to upstream version 7.8p1. This version of OpenSSH includes the following changes:

  - `UsePrivilegeSeparation=sandbox` option is now mandatory and cannot be disabled.

  - Minimal accepted `RSA` key size is set to 1024 bits.

  - Modulus size for Diffie-Hellman parameters has been changed to 2048 bits.

- – Default value of the `UseDNS` option has been changed to `no`.

  – `DSA` public key algorithms are disabled by default.

  – Semantics of the `ExposeAuthInfo` configuration option has changed.

  – The following features are removed in OpenSSH 7.8p1:

    * SSH version 1 protocol

    * `hmac-ripemd160` message authentication code

    * RC4 (`arcfour`), Blowfish, and CAST ciphers

- **LUKS2 replaces LUKS1**

  The LUKS version 2 (LUKS2) format replaces the legacy LUKS (LUKS1) format in this release. Also, the `dm-crypt` subsystem and the `cryptsetup` tool now use LUKS2 as the default format for encrypted volumes.

- **Replacement of nfsnobody user and group pair with nobody user and group pair**

  The `nobody` user and group pair, with the ID of 99, and the `nfsnobody` user and group pair, with the ID of 65534 (the default kernel overflow ID), have been merged into the `nobody` user and group pair. This change reduces confusion about the files that are owned by `nobody` and have nothing to do with NFS. The merged user and group pair use the 65534 ID. Note that the `nfsnobody` user and group pair are no longer created during a fresh installation.

- **GPG key length increased to 4096 bits**

  Oracle Linux 8 RPM packages are now signed with a new 4096-bit GNU Privacy Guard (GPG) key for greater security. Previously, the GPG key length was 2048 bits.

- **RSA-PSS available in OpenSC**

  Oracle Linux 8 provides the RSA-PSS cryptographic signature scheme for the `OpenSC` smart card driver. The new scheme enables a secure cryptographic algorithm, which is required for the TLS 1.3 support in the client software.

- **rsyslog updated to version 8.37.0**

  In Oracle Linux 8, the `rsyslog` packages have been upgraded to version 8.37.0. This version of `rsyslog` includes several bug fixes and improvements over previous versions.

- **New omkafka rsyslog module added**

  You can use the `omkafka` module in the Oracle Linux 8 release to enable Kafka centralized data storage scenarios. You can also use this module to forward logs to the Kafka infrastructure.

- **libssh implements SSH as a core cryptographic component**

  The `libssh` library, which implements the SSH protocol, is introduced as a core cryptographic component in Oracle Linux 8. Note that `libssh` does not comply with the system-wide cryptographic policy.

- **Consolidation of OpenSCAP API**

  In Oracle Linux 8, the OpenSCAP shared library API has been consolidated. As a result, 63 symbols are removed, 14 symbols are added, and 4 symbols have an updated signature.

The following symbols are removed in OpenSCAP 1.3.0:

– Symbols marked as deprecated in version 1.2.0

– SEAP protocol symbols

– Internal helper functions

– Unused library symbols

– Unimplemented symbols

- **PKCS #11 support for smart cards and HSMs is now consistent**

  In Oracle Linux 8, using smart cards and Hardware Security Modules (HSM) with the PKCS #11 cryptographic token interface is consistent, which means users and administrators can use the same syntax for all related tools in the system.

- **SELinux policy improvement to enable iscsiuio processes to work correctly**

  Oracle Linux 8 adds missing rules to the SELinux policy to enable `iscsiuio` processes to access `/dev/uio*` devices by using the `mmap` system call. Previously, SELinux policy restricted this access, which caused the connection to the discovery portal to fail.

- **System-wide cryptographic policies applied by default**

  In Oracle Linux 8, the `crypto-policies` component configures the core cryptographic subsystems and covers the TLS, IPSec, SSH, DNSSec, and Kerberos protocols. The component provides a small set of policies that can be selected by using the `update-crypto-policies` command.

  The `DEFAULT` system-wide cryptographic policy that provides secure settings for current threat models is also compatible with PCI-DSS requirements, as it allows the TLS 1.2 and 1.3 protocols, as well as the IKEv2 and SSH2 protocols. The RSA keys and Diffie-Hellman parameters are accepted, if they are larger than 2047 bits.

  See the `update-crypto-policies(8)` man page.

- **OSPP 4.2 added to SCAP Security Guide**

  The SCAP Security Guide includes a draft of the OSPP (Protection Profile for General Purpose Operating Systems) profile version 4.2 RHEL 8. This profile reflects the mandatory configuration controls that are identified in the NIAP Configuration Annex to the Protection Profile for General Purpose Operating Systems (Protection Profile Version 4.2). The SCAP Security Guide provides automated checks and scripts so that users can meet the requirements that are defined in the OSPP.

- **Improvements to the OpenSCAP command-line interface**

  The verbose mode is now available in all `oscap` modules and submodules. In addition, improvements have been made to the tool output.

  Several options are deprecated and have been removed, including the following:

  – The `--show` option in the `osccap xccdf generate report` command is completely removed.

  – The `--probe-root` option in the `oscap oval eval`. As a replacement, you can set the environment variable, `OSCAP_PROBE_ROOT`.

  – The `--sce-results` option in the `oscap xccdf eval` command is replaced by the `--check-engine-results` option.

- The `validate-xml` submodule validator has been dropped from the CPE, OVAL, and XCCDF modules. You can use `validate` submodules to validate SCAP content against XML schemas and XSD schematrons.

- The `oscap oval list-probes` command. Instead, use the `oscap` command with the `--version` option to display this information.

- > **Note:**
  >
  > OpenSCAP allows for evaluating all of the rules in a given XCCDF benchmark by using `--profile '(all)'`, regardless of the profile.

- **SELinux map permission code added**

  Oracle Linux 8 provides the SELinux `map` permission feature. This feature controls memory mapped access to files, directories, and sockets and enables SELinux policy to prevent direct memory access to various file system objects and also ensure that all such access is revalidated.

- **systemd No New Privileges added to SELinux**

  Oracle Linux 8 provides support for the `nnp_nosuid_transition` policy capability, which enables SELinux domain transitions under No New Privileges (NNP) or `nosuid`, if `nnp_nosuid_transition` is allowed between the old and new contexts. The `selinux-policy` packages now contain a policy for systemd services that use the NNP security feature.

  The following example shows the rule that defines how you would allow this capability for a service:

  ```
  allow source_domain
                    target_type:process2 { nnp_transition
  nosuid_transition };
  ```

  would be defined as follows for this service:

  ```
  allow init_t fprintd_t:process2 { nnp_transition nosuid_transition };
  ```

  Note that the distribution policy now also contains the m4 macro interface, which can be used in SELinux security policies for services that use the `init_nnp_daemon_domain()` function.

- **getrlimit permission in the process class added to SELinux**

  A new SELinux access control check, `process:getrlimit`, has been added to the `prlimit()` function. This change enables SELinux policy developers to control when one process attempts to read and then modify the resource limits of another process by using the `process:setrlimit` permission. Note that SELinux does not restrict a process from manipulating its own resource limits through `prlimit()`. See the `prlimit(2)` and `getrlimit(2)` man pages for details.

- **New SELinux booleans added**

  Oracle Linux 8 includes the following new SELinux booleans:

  - `colord_use_nfs`

  - `mysql_connect_http`

- – `pdns_can_network_connect_db`

- – `ssh_use_tcpd`

- – `sslh_can_bind_any_port`

- – `sslh_can_connect_any_port`

- – `virt_use_pcscd`

For more details, run the `semanage boolean -l` command.

- **TLS 1.3 in cryptographic libraries added**

  This release adds Transport Layer Security (TLS) 1.3, by default, in all major back-end cryptographic libraries. This change enables low latency across the operating system communications layer and enhances privacy and security for applications by taking advantage of new algorithms such as RSA-PSS or X25519.

- **OpenSCAP updated to version 1.3.0**

  In Oracle Linux 8, the OpenSCAP suite has been upgraded to version 1.3.0. This version of the OpenSCAP suite introduces many enhancements, including the consolidation of the API and the ABI, an enhanced command-line interface, and other notable improvements over the previous OpenSCAP version.

- **Replacement of audispd with auditd in Audit 3.0**

  In this release, the functionality of `audispd` has been moved to `auditd`. As a result, `audispd` configuration options are now part of `auditd.conf`, and the `plugins.d` directory is now under `/etc/audit`. You can check the current status of `auditd` and its plugins by running the `auditd state` command.

- **imfile module added to rsyslog**

  In Oracle Linux 8, the rsyslog `imfile` module has been enhanced for improved performance and the addition of more configuration options. This change enables you to use the module for more complicated file monitoring.

New systemd Behavior in Oracle Linux 8

In Oracle Linux 8, systemd uses a pager to enable the viewing of full status output in paginated format. You can use the `--no-pager --full` options when running the `systemctl` command to obtain the full output without using the pager. Or, you can set the `$PAGER` environment variable to specify the default pager program that should be used.

Note that when using a pager, the output is piped to a forked process that might not exit immediately. In this case, use the exit keys that are appropriate for the pager program, usually the `q` key or by pressing `Ctrl-c`.

Virtualization

Oracle Linux 8 introduces the following virtualization features, enhancements, and changes:

- **5-level paging added to KVM**

  In Oracle Linux 8, Kernel-based Virtual Machine (KVM) virtualization enables the 5-level paging feature for hardware that can support this feature. This enhancement significantly increases the physical and virtual address space that the host and guest systems can use.

- **UMIP added to KVM**

  Oracle Linux 8 includes the addition of the User Mode Instruction Prevention (UMIP) feature for KVM virtualization. This security enhancement assists in preventing user-space applications from accessing system-wide settings, resulting in a reduction in the potential vectors for privilege escalation attacks.

- **Additional information included in KVM guest crash reports**

  In this release, the crash information that KVM hypervisor generates if a guest terminates unexpectedly or becomes unresponsive includes additional information, which makes it easier to diagnose and fix problems when using KVM virtualization.

- **qemu-kvm updated to version 2.12**

  Oracle Linux 8 provides the `qemu-kvm` 2.12 package. This version of `qemu-kvm` includes numerous bug fixes and improvements over the previously supported 1.5.3 version.

- **NVIDIA vGPU compatible with the VNC console**

  As of Oracle Linux 8, you can use the VNC console to display the visual output of the guest when using the NVIDIA virtual GPU (vGPU) feature.

- **Virtualization for Ceph added**

  In this release, Ceph storage is supported by KVM virtualization on all CPU architectures that are supported by Oracle Linux.

- **Virtualization for Q35 machine type added**

  Oracle Linux 8 provides the Q35 machine type, which is a more modern PCI Express-based machine type. Feature changes include a wide variety of improvements and performance enhancements for virtual devices, which ensure that a wider range of modern devices are compatible with virtualization features. Note that any virtual machines (VMs) that you create in Oracle Linux 8 are set to use the Q35 machine type by default.

- **QEMU sandboxing added**

  In Oracle Linux 8, the QEMU emulator introduces sandboxing, which is enabled and configured by default. Sandboxing provides configurable limitations for the system calls that QEMU can perform, thereby making VMs more secure.

- **Mounting ephemeral disks on VMs running on Microsoft Azure works more reliably in Oracle Linux 8**

  An improvement has been made in Oracle Linux 8 to ensure that reconnecting an ephemeral disk on a VM that is running on the Microsoft Azure platform is handled correctly and does not fail if the disk was recently detached from the VM, which was the case in previous releases.

Web Services

In Oracle Linux 8, the following web service features, enhancements, and changes are introduced:

- **Apache Tomcat package is not available in Oracle Linux 8**

  The Apache Tomcat software package that was available in Oracle Linux 7 is no longer included in Oracle Linux 8.

- **Apache HTTP Server updated to version 2.4.35**

Oracle Linux 8 includes Apache HTTP Server version 2.4.35, which provides several improvements over the previous version of Apache.

This version of the Apache HTTP Server includes the following changes:

– **HTTP/2 available in Oracle Linux 8**

HTTP/2 has been added in this release and is provided by the `mod_http2` package. This package is included in the `httpd` module.

– **Automated TLS certificate provisioning**

Oracle Linux 8 includes automated TLS certificate provisioning and renewal by using the Automatic Certificate Management Environment (ACME) protocol through the `mod_md` package has been added. The `mod_md` package is used with certificate providers such as Let's Encrypt.

– **TLS certificate loading added**

The Apache HTTP Server now includes capability for loading TLS certificates and private keys from hardware security tokens directly from `PKCS#11` modules. Additionally, `mod_ssl` configuration can now use `PKCS#11` URLs to identify the TLS private key, and optionally, the TLS certificate in the `SSLCertificateKeyFile` and `SSLCertificateFile` directives.

– **Multi-processing module changed to high-performance multi-thread event model**

The multi-processing module (MPM) that the Apache HTTP Server configures by default has changed to a high-performance, multi-threaded `event` model. Previously, the multi-process forked model (also known as `prefork`) was used. Note that you must replace or remove any third-party modules that are not thread-safe. To change the MPM that is currently configured, edit the `/etc/httpd/conf.modules.d/00-mpm.conf` file by following the directions documented in the `httpd.service(8)` man page.

• **Availability of HTTP for nginx 1.14 web and proxy server**

The `nginx` 1.14 web and proxy server includes support for HTTP and other protocols by providing high currency performance with low-memory usage. Previously, `nginx` was only available as a Software Collection.

The `nginx` web server also provides support for loading TLS certificates and private keys from hardware security tokens, directly from `PKCS#11` modules. As a result, an `nginx` configuration can use `PKCS#11` URLs to identify the TLS private key in the `ssl_certificate_key` directive.

3
Known Issues

This chapter lists known issues in the current Oracle Linux 8 release. The list covers issues that might affect both x86 and aarch64 platforms. In the list, additional issues that are specific only to aarch64 platforms are labeled `aarch64 only:`.

Installation Issues

The following are known installation issues that are reported in Oracle Linux 8.

ULN registration wizard not displayed on first boot after an installation

On new installations of Oracle Linux 8, the ULN registration wizard that presents the options to register with ULN and to use Oracle Ksplice is not displayed on first boot.

As an alternative, you can register with ULN after the installation completes. For instructions, see https://linux.oracle.com/.

(Bug ID 29933974)

Syslog Error: Failed to insert module 'ip_tables': Operation not permitted

During an Oracle Linux 8 installation, the following message can be observed in the `/var/log/messages:systemd` log:

```
1]: Failed to insert module 'ip_tables': Operation not permitted
```

This error can be safely ignored, as the `ip_tables` kernel module subsequently and can be verified by running the following command:

```
grep IPTABLES /boot/config*
```

The following output indicates the module loaded successfully:

```
CONFIG_IP_NF_IPTABLES=m
CONFIG_IP6_NF_IPTABLES=m
```

You can also check that the module loaded successfully by running the following command:

```
modinfo ip_tables
```

The output of the previous command indicates the module loaded successfully:

```
filename:
/lib/modules/4.18.0-32.el8.x86_64/kernel/net/ipv4/netfilter/ip_tables.ko.xz
alias:          ipt_icmp
description:    IPv4 packet filter
author:         Netfilter Core Team <coreteam@netfilter.org>
license:        GPL
rhelversion:    8.0
srcversion:     3967C875058C2EE2475C9C2
depends:
```

```
retpoline:      Y
intree:         Y
name:           ip_tables
vermagic:       4.18.0-32.el8.x86_64 SMP mod_unload modversions
sig_id:         PKCS#7
signer:
sig_key:
sig_hashalgo:   md4
signature:      30:82:02:59:06:09:2A:86:48:86:F7:0D:01:07:02:A0:82:02:4A:30:
82:02:46:02:01:01:31:0D:30:0B:06:09:60:86:48:01:65:03:04:02:
01:30:0B:06:09:2A:86:48:86:F7:0D:01:07:01:31:82:02:23:30:82:
02:1F:02:01:01:30:7A:30:62:31:22:30:20:06:03:55:04:0A:0C:19:
4F:72:61:63:6C:65:20:41:6D:65:72:69:63:61:2C:20:49:6E:63:2E:
2C:63:3D:55:53:31:19:30:17:06:03:55:04:03:0C:10:4F:72:61:63:
.
.
.
```

(Bug ID 29500599)

Graphics controller requirements for an installation on an Oracle VM VirtualBox guest

To successfully install Oracle Linux 8 on an Oracle VM VirtualBox guest, where the graphical installation program is used and the default `Server with GUI` environment is selected, you must set the guest to use the VMSVGA graphics controller and configure the guest with at least 64MB of memory. Otherwise, the graphical display is unable to start correctly.

Beginning with Oracle VM VirtualBox 6.0, the VMSVGA graphics controller is the default controller for guests running Linux operating systems. This issue is more likely to appear if install Oracle Linux 8 on an existing guest that was created on an earlier Oracle VM VirtualBox release. To configure Oracle Linux 8 guests, Oracle recommends that you use Oracle VM VirtualBox 6.0 or later.

(Bug ID 30004543)

Installation on KVM guest by using iPXE and iSCSI boot results in incorrect IQN name

After installing Oracle Linux 8 on a KVM guest by using iPXE and iSCSI boot, the SCSI Qualified Name (IQN) in the `/etc/iscsi/initiatorname.iscsi` file is not correct.

Note that this incorrect configuration could impact `kdump` functionality.

The workaround for this issue is to manually modify the `/etc/iscsi/initiatorname.iscsi` file with the correct IQN after the installation completes.

(Bug ID 29536715)

Oracle Linux 8 does not recognize SAS controllers on older Oracle Sun hardware

The Oracle Linux 8 installer does not recognize some Serial Attached SCSI (SAS) controllers that are found in older Oracle Sun server models. If you attempt to install Oracle Linux 8 on these server models, the installer does not recognize the local disk and the installation fails. Examples of these server models include, but are not limited to, the following: Oracle Sun Fire X4170 M2 Server, Oracle Sun Fire X4170 M3 Server, Oracle Sun OVCA X3-2 Server, and the Oracle Sun X4-2 Server.

The following SAS controllers are removed from the `mpt2sas` driver in RHCK:

- SAS2004, PCI ID 0x1000:0x0070

- SAS2008, PCI ID 0x1000:0x0072

- SAS2108_1, PCI ID 0x1000:0x0074

- SAS2108_2, PCI ID 0x1000:0x0076

- SAS2108_3, PCI ID 0x1000:0x0077

- SAS2116_1, PCI ID 0x1000:0x0064

- SAS2116_2, PCI ID 0x1000:0x0065

- SSS6200, PCI ID 0x1000:0x007E

The following SAS controllers are removed from the `megaraid_sas` driver in RHCK:

- Dell PERC5, PCI ID 0x1028:0x15

- SAS1078R, PCI ID 0x1000:0x60

- SAS1078DE, PCI ID 0x1000:0x7C

- SAS1064R, PCI ID 0x1000:0x411

- VERDE_ZCR, PCI ID 0x1000:0x413

- SAS1078GEN2, PCI ID 0x1000:0x78

- SAS0079GEN2, PCI ID 0x1000:0x79

- SAS0073SKINNY, PCI ID 0x1000:0x73

- SAS0071SKINNY, PCI ID 0x1000:0x71

The workaround for this issue to use the Unbreakable Enterprise Kernel Release 6 (UEK R6) boot ISO, and then run UEK R6 with Oracle Linux 8, as these controllers are supported in the Unbreakable Enterprise Kernel release.

(Bug ID 29120478)

GPG key file location must be explicitly set when adding repositories

If you are using the `dnf config-manager --add-repo` command to add a repository, the command does not add the GPG key file location configuration for that repository. The result

is a package installation failure; as by default, `dnf` enables `gpgcheck`, but it requires the GPG key to be set or imported.

One workaround for this issue is to run the following command to ensure that the GPG key file location is set and imported:

```
sudo rpm --import "file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle"
```

Another workaround is to add/set the GPG key for all of the individual repository entries under `/etc/yum.repos.d`, for example:

```
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
```

(Bug ID 29535274)

File System Issues

The following are known file systems issues that have been encountered in this release of Oracle Linux 8.

ext4: File system corruption occurs when both quota and dioread_nolock options are enabled

An issue with `ext4` in Oracle Linux 8 results in file system corruption if unwritten extents are converted in IO completion so that they can be merged with siblings and both the `dioread_nolock` and `quota` options are enabled. This is a corner-case issue that exists in upstream code. A proposed patch is currently under review.

(Bug ID 29688421)

ext4: Frequent or repeated system shutdowns can cause file system corruption

If a system that is using the `ext4` file system is repeatedly or frequently shut down, the file system might become corrupted. This issue is difficult to replicate and is therefore considered to be a corner-case issue. The issue exists in the upstream code and proposed patches are currently under review.

(Bug ID 27547113)

XFS: Existence of many unlinked tmp files causes file system corruption

An issue has been identified with XFS in Oracle Linux 8, where many unlinked `tmp` files are created, which causes file system corruption and results in the inability to recover after a system crash. This issue, the cause of which is currently unknown, has been observed when running a stress test.

(Bug ID 29682399)

XFS: xfs_repair interprets a slash (/) character in extended attribute name as corruption

An issue exists in Oracle Linux 8 that causes the `xfs_repair` utility to interpret a slash (/) character in an extended attribute name as file system corruption. The issue exists in upstream code and a proposed patch is currently under review.

(Bug ID 29680752)

XFS: Incorrect mkfs parameters cause file system corruption

If you run the `mkfs` utility and set invalid extent hints, the file system is created, but it becomes corrupted and cannot be mounted. The following error is displayed:

```
[18143.814821] XFS (sdb1): Failed to read root inode 0x80, error 117
mount: /mnt: mount(2) system call failed: Structure needs cleaning.
```

(Bug ID 29602175)

Kernel Issues

The following are known kernel issues that have been encountered in this release of Oracle Linux 8.

KVM guests boot with "amd64_edac_mod: Unknown symbol" errors on AMD 64-bit platforms

The following errors might be displayed repeatedly when KVM guests are booting on 64-bit AMD hosts:

```
[   12.474069] amd64_edac_mod: Unknown symbol amd_register_ecc_decoder (err [ 120)
[   12.474083] amd64_edac_mod: Unknown symbol amd_report_gart_errors (err 0)
[   12.852250] amd64_edac_mod: Unknown symbol amd_unregister_ecc_decoder (err 0)
[   12.852297] amd64_edac_mod: Unknown symbol amd_register_ecc_decoder (err 0)
.
.
.
```

These errors occur because the module code for the kernel erroneously returns `-EEXIST` for modules that failed to load and are in the process of being removed from the module list. The `amd64_edac_mod` module will not be loaded in a VM. These errors can be ignored, as they do not impact functionality in any way.

This issue occurs on Oracle Linux 8 hosts that are running RHCK *only* and is not encountered on UEK R6 hosts.

(Bug ID 29853602)

Output of modinfo command does not show Retpoline support

A bug in the Oracle Linux 8 code causes Retropline support to not be displayed in the output of the `modinfo -F retpoline` command, even though the `CONFIG_RETPOLINE` flag is set to `Y`, for example:

```
sudo modinfo -F retpoline
/usr/lib/modules/4.18.0-80.el8.x86_64/kernel/sound/usb/usx2y/snd-usb-us122l.ko
.xz
```

The `CONFIG_RETPOLINE=Y` flag is still required to add and display Retpoline support. If the parameter is enabled, the kernel builds with a retpoline capable compiler.

To confirm that the `CONFIG_RETPOLINE` flag is enabled, search for the parameter in the kernel's `config-kernel` configuration file, for example:

```
cat /boot/config-5.4.17-2011.7.4.el8uek.x86_64 | grep RETPOLINE.
```

```
CONFIG_RETPOLINE=y
```

(Bug ID 29894295)

Kdump service fails to start on systems with Secure Boot enabled

In Oracle Linux 8, the Kdump service fails to start on systems that have Secure Boot enabled. This issue has been observed on both bare metal systems, as well as KVM guests. The following errors are reported by `syslog`:

```
Jun 24 03:12:18 vmx209-ps kdumpctl[930]: kexec_file_load failed: Required key
not available
Jun 24 03:12:18 vmx209-ps kdumpctl[930]: kexec: failed to load kdump kernel
Jun 24 03:12:18 vmx209-ps kdumpctl[930]: Starting kdump: [FAILED]
Jun 24 03:12:18 vmx209-ps systemd[1]: kdump.service: Failed with result
'exit-code'.
Jun 24 03:12:18 vmx209-ps systemd[1]: Failed to start Crash recovery kernel
arming.
```

If you want to use Kdump, the easiest workaround for this issue is to disable Secure Boot.

If you require Secure Boot and wish to continue to use Kdump, you can consider updating the UEFI key database for your system. The key database is used as a store for the key certificates issued by a vendor, so that signed EFI binaries can be validated when the system is operating in secure mode. To perform this update you may require physical access to the system to access the UEFI console and enroll the key there. You can use the Machine Owner Key (MOK) facility to update the UEFI Secure Boot key database and import the keys manually. The certificate keys that are used to sign each kernel are contained in the `shim` source packages that are used to verify the keys the kernels use.

> **⊕ Important:**
>
> Using the MOK utility with your system may depend on server firmware implementation and configuration. Check that your server supports this before attempting to manually update signature keys used for UEFI Secure Boot. If you are unsure, do not follow the instructions provided here.
>
> Adding certificates to the UEFI Secure Boot key database by using the MOK utility requires that you have physical access to the system so that you can complete the enrollment request at the UEFI console. If you do not have physical access to the system, do not follow the instructions that are provided here.

1. Certificates used to sign each kernel, built by Oracle, are contained in the `shim` source package. You can download this package using the `yumdownloader` command available in the `dnf-utils` package:

```
sudo dnf install -y dnf-utils
sudo mkdir /tmp/shim
cd /tmp/shim
sudo yumdownloader --source shim
```

2. Extract the source package to access the Extended Validation certificate that is included as a `secureboot.cer` file. Use the `rpm2cpio` command to extract the package:

```
sudo rpm2cpio ./shim*.rpm | cpio -idmv
```

3. Use the `mokutil` command to request that the certificate that you have extracted from the `shim` package is included in the MOK list:

```
sudo mokutil --import ./secureboot.cer
```

The command prompts you to enter and confirm a password for the MOK enrollment request. You can use any password for this purpose, but you should note the password that you use, as you are prompted for it again when the system reboots.

4. Reboot the system.

5. The pending MOK key enrollment request is detected, and you must complete the enrollment from the UEFI console. You are prompted for the password that you set when you imported the certificate. When you have entered the correct password, the certificate is added to the MOK list and is automatically propagated to the system key ring on this boot, as well as subsequent boots.

(Bug ID 29954639)

Kdump runs out of memory when attempting to mount /sysroot on FC disks that use the Logical Volume Manager

An issue in Oracle Linux 8 causes Kdump to run out of memory if you attempt to mount `/sysroot` on a Fibre Channel (FC) disk that uses LVM. This issue is due to a lack of memory when the `crashkernel` loads.

To resolve the issue, you can do one of the following:

- Override the `crashkernel=auto` boot option so that more memory is reserved for Kdump. For example, set the kernel boot parameter to `crashkernel=512M`.

- Set the Kdump destination to a network location (NFS or SSH).

(Bug ID 29840266)

aarch64 only: Kdump tools fail to create vmcore.dmesg.txt on X-Gene 3 and ThunderX2 platforms

The Kdump crash dump tools fail to create a `vmcore-dmesg.txt` file (which is created with the `vmcore` file) on the X-Gene 3 and ThunderX2 platforms. This failure to create the `vmcore-dmesg.txt` file might result in a segmentation fault similar to the following:

```
...
kdump: saving to /sysroot//var/crash/127.0.0.1-2018-05-22-12:34:45/
kdump: saving vmcore-dmesg.txt
/lib/kdump-lib-initramfs.sh: line 118:   459 Segmentation fault
$_dmesg_collector /proc/vmcore > ${_path}/vmcore-dmesg-incomplete.txt
kdump: saving vmcore-dmesg.txt failed
kdump: saving vmcore
Copying data                                : [100.0 %] \
eta: 0s
kdump: saving vmcore complete
```

You can retrieve the `dmesg` output manually by running `crash` against the `vmcore` and using the `dmesg` command when in the crash shell.

(Bug ID 29709556)

aarch64 only: netconsole kernel module does not work with some devices

In Oracle Linux 8, the `netconsole` kernel module does not work with the Mellanox ConnectX devices (`mlx4_core` and `mlx5_core` driver modules) and the QLogic FastLinQ devices (`qede` driver module).

(Bug IDs 29778572, 29692757, and 29691892)

aarch64 only: Kernel panic might occur during a kexec boot on X-Gene 3 platform

A kernel panic might occur sometimes during a `kexec` boot on the X-Gene 3 platform.

(Bug ID 29710047)

Networking Issues

The following are networking issues that might be encountered in this release of Oracle Linux 8.

tracepath6 does not parse destination IPv6 address correctly

Running the `tracepath6` command fails to parse the destination IPv6 address correctly. Consequently, the tool traces a route to the wrong host.

To work around this issue, use a tool with similar capabilities to the `tracepath6` command.

(Bug ID 29540588)

Failure to insert ip_tables module

The `ip_tables` module fails to insert with an 'Operation not permitted' error. This issue, which is currently under investigation, can occur if SELinux is in enforcing mode.

A workaround for this issue is to set SELinux to permissive mode, which you can do temporarily by running the `setenforce 0` command. Or, you can set SELinux to permissive mode permanently by editing the `/etc/selinux/config` file and then rebooting the system.

(Bug ID 29517166)

aarch64 only: mlx5_core driver fails on X-Gene 3 platform with MTU setting greater than 1500

Mellanox ConnectX-5 devices (the `mlx5_core` driver module) fail to work on the X-Gene 3 platform with an MTU setting that is greater than 1500.

(Bug ID 29692676)

Restarting firewalld service results in SSH connection timeout

Restarting the `firewalld` service leads to an SSH connection timeout on the terminal from which the service was started. Note that other SSH terminals remain connected.

(Bug ID 29478124)

/var/run/rhnsd.pid file not readable after starting Spacewalk daemon

Oracle Linux 8 systems fail to read PID from `/var/run/rhnsd.pid` after the Spacewalk daemon starts.

The following error is reported in the `/var/log/messages` log:

```
systemd: Failed to read PID from file /var/run/rhnsd.pid: Invalid argument
```

This error can be safely ignored.

(Bug ID 2953130)

Error: "mcelog service does not support this processor"

An error indicating that the `mcelog` service does not support the processor can appear in the system log on systems with AMD processors, such as some Oracle Server hardware. The message might be displayed as follows:

```
mcelog: ERROR: AMD Processor family
23: mcelog does not support this processor.  Please use the edac_mce_amd
module instead.
```

The `mcelog` daemon is a service that is used on x86_64 platforms to log and handle hardware error messaging. On AMD systems, the `edac_mce_amd` kernel module handles machine exception logging. Therefore, AMD systems do not require the `mcelog` daemon. This error should be downgraded to a warning.

(Bug ID 29501190)

Podman Issues

The following are known issues for the Podman container management tool in this release of Oracle Linux 8.

Executing podman attach --latest causes panic if no containers are available

If you execute `podman attach --latest` and no containers exist in your environment, a runtime error occurs:

```
panic: runtime error: index out of range
...
```

Note that this error no longer occurs as soon as there are containers in the environment. Running the command when there are no containers is meaningless.

(Bug ID 29882537)

Requirements for using the default podman detach key sequence

The default key sequence that you use to detach a container (`CTRL+P`, `CTRL+Q`) requires a console that can handle detachment (`pseudo-tty`), as well as an input channel for passing control signals (`stdin`). Otherwise, you cannot create a container, attach it with the `podman attach -l` command, and then quit or detach the container by using the default key sequence, as documented in the `podman-attach(1)` manual page.

To ensure that you can use the default `CTRL+P`, `CTRL+Q` key sequence to detach a container, use either of the following methods to create a container:

- Create a container in the background:

  ```
  podman run --rm -t -d container-registry.oracle.com/os/oraclelinux:7 top -b
  ```

  You can then use the `podman attach -l` command to attach the container and the `CTRL+P`, `CTRL+Q` key sequence to detach the container.

- Create a container interactively:

  ```
  podman run --rm -t -i container-registry.oracle.com/os/oraclelinux:7 top -b
  ```

  The interactive method creates the container and automatically attaches it. You can then use the `CTRL+P`, `CTRL+Q` key sequence to detach the container.

  For more information, see the `podman(1)` and `podman-attach(1)` manual pages.

(Bug ID 29882852)

Authentication error displayed when attempting to pull an image and not specifying its correct name

If you attempt to pull an image by running the `podman pull` *image-name* command, but you do not specify the correct or full name of the image, an authentication error occurs.

For example, the following error is displayed because `oracle:latest` was specified as the name of the image instead of `oraclelinux:latest`, which is the correct name for the image:

```
Trying to pull registry.redhat.io/oracle:latest...Failed
Trying to pull quay.io/oracle:latest...Failed
Trying to pull docker.io/oracle:latest...Failed
error pulling image "oracle:latest": unable to pull oracle:latest: 3 errors
occurred:

* Error determining manifest MIME type for
docker://registry.redhat.io/oracle:latest: unable to retrieve auth token:
invalid username/password
* Error determining manifest MIME type for docker://quay.io/oracle:latest:
Error reading manifest latest in quay.io/oracle: error parsing HTTP 404
response body: invalid character '<' looking for beginning of value:
"<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 3.2 Final//EN\">\n<title>404 Not
Found</title>\n<h1>Not Found</h1>\n<p>The requested URL was not found on the
server.  If you entered the URL manually please check your spelling and try
again.</p>\n"
* Error determining manifest MIME type for docker://oracle:latest: Error
reading manifest latest in docker.io/library/oracle: errors:
denied: requested access to the resource is denied
unauthorized: authentication required
```

To prevent this error from occurring, always specify the correct image name with the `podman pull` command.

(Bug ID 29894231)

Non-root user cannot export a running container as a tar archive when container is created by same non-root user

Although a non-root user can create a privileged running container, running the `podman export -o` *tar_name*`.tar` *container_name* command to export the container as a tar archive fails if it is run by the same non-root user.

If you have `root` access, the workaround for this issue is to create the privileged running container as the `root` user and also export it as the `root` user.

(Bug ID 29890374)

Oracle Container Registry unable to service requests to search catalog

Attempts to search for an image in the Oracle Container Registry by using the `podman search` command fail with an authorization error, even if you are logged into the registry:

```
ERRO[0001] error getting search results from v2 endpoint
"container-registry.oracle.com", status code 401 (Unauthorized)
...
```

ORACLE®

The issue is related to how Oracle Container Registry handles token requests for access to "/v2/_catalog". The `podman search` command only requests a token for ping-level access and not for catalog access.

There is currently no workaround for this issue.

(Bug ID 29942671)

SELinux: "Class bpf not defined in policy" and "Class xdp_socket not defined in policy" errors occur during a boot

Rebooting an Oracle Linux 8 system in either SELinux permissive mode or enforcing mode produces the following messages in the `/var/log/messages` file:

```
SELinux:  Class bpf not defined in policy.
SELinux:  Class xdp_socket not defined in policy.
SELinux: the above unknown classes and permissions will be allowed
```

These messages are displayed because no definitions currently exist for these classes in SELinux policy. Per the last line of the message, classes and permissions will be allowed by default; and therefore, the messages can be safely ignored.

(Bug ID 29502976)

4

Comparing Yum Version 3 With DNF

Oracle Linux 8 introduces a new version of the Yum tool, which is based on DNF technology. DNF provides several advantages over the Yum v3 tool. Most notably, DNF provides support for modular content and a more stable API. DNF is compatible with Yum v3 when used from the command line or when editing or creating configuration files, and you can use the `dnf` command and all of its options similarly to how you used the `yum` command in Oracle Linux 7. However, there are some differences between the two versions of the tool. This appendix describes many of those differences. For more information about DNF, see DNF Support Added.

For more detailed information about using DNF in Oracle Linux 8, see Oracle Linux: Managing Software on Oracle Linux

The following table compares Yum v3 features, commands, and options with the DNF tool that is introduced in Oracle Linux 8.

Yum v3 Feature, Command or Option	DNF Feature, Command or Option	Notable Differences
`--skip-broken` option	`--skip-broken` option Is an alias for the `--setopt=strict=0` option	**When used for installations:** Skips all packages (or those with broken dependencies that are passed to DNF) without raising an error or causing the operation to fail. You can use either option with DNF. You can also set this behavior as the default in the `dnf.conf` file. **When used for upgrades:** The semantics that were used to trigger the `yum` command with the `--skip-broken` option are set for `dnf update` as the default. Note that you do not need to use the `--skip-broken` option with the `dnf upgrade` command. Instead, use the `--best` option if you want to use only the latest version of packages in transactions.
`yum update` command	`dnf update` command	Command syntax change only. No differences with the behavior for `dnf update` and `yum update`.

Yum v3 Feature, Command or Option	DNF Feature, Command or Option	Notable Differences
`yum upgrade` command	`dnf upgrade` command	Aside from the syntatical difference, the behavior of `dnf upgrade` is the same as `yum upgrade`. Note that in Yum v3, `yum upgrade` is the same as `yum --obsoletes update`.
`clean_requirements_on_remove` option	`clean_requirements_on_remove` option	This option is enabled by default in DNF, which might cause confusion when comparing the `remove` operation results between the two Yum versions, as DNF removes more packages.
`resolvdep` command	Not supported Use the `dnf provides` command to determine which package provides a specific file.	The Yum v3 command is maintained for legacy purposes *only*.
`deplist` command	Not supported Use the `dnfrepoquery-- deplist` command to determine dependencies for a package.	The `yumdeplist` alias is provided for Yum v3 compatibility with the `dnf repoquery --deplist` command.
Excludes (and repository excludes)	Excludes (and repository excludes)	Yum v3 respects excludes during installations and upgrades; whereas, DNF respects all operations, including erasing and listing.
`includepkgs` option	`include` option	In DNF, the directive name for repository (and main) configuration has been renamed for better alignment with its DNF counterpart, `exclude`.
`skip_if_available` option	`skip_if_available` option	This option is enabled by default in DNF. Without this setting, and without explicitly setting `skip_if_unavailable=True` in the relevant repository `.ini` file, Yum immediately stops and reports a repository error.
`overwrite_groups` option	Not supported	This configuration option has been removed in DNF. Instead, when DNF identifies several groups with the same group ID, it merges the contents of the groups.

Yum v3 Feature, Command or Option	DNF Feature, Command or Option	Notable Differences
`mirrorlist_expire` option	Not supported	DNF uses `metadata_expire` for the expiring metadata, as well as the `mirrorlist` file.
"metalink" mention in the `mirrorlist` repository option.	Not supported	A fix has been applied in DNF to render the following information in the `yum.conf(5)` inapplicable: If the `mirrorlist` URL contains the word *metalink*, then the value of `mirrorlist` is copied to `metalink` (if `metalink` is not set).
`alwaysprompt` option	Not supported	This option has been removed from DNF to simplify configuration.
`group_package_types` option	Not supported	This option has been removed from DNF to simplify configuration.
`dnf history rollback` command	Not supported	This option has been removed from DNF to simplify configuration. Use the `dnfupgrade` command to upgrade all packages to their latest version.
`upgrade_requirements_on_install`	Behaves as though disabled.	Because DNF tolerates the use of other package managers, it is possible that not all changes that are made to RPMDB are stored in the history of transactions. Thus, DNF does not fail in this situation, which means the `force` option is no longer required.
`yum swap` command	`dnfshell` command This command performs a remove and install transaction. `dnf --allowerasing` command	Using the `dnf --allowerasing` command is the equivalent to using `yum swap A B`, where you want to replace `A` (providing `P`) with `B` (also providing `P`), which conflicts with `A`, without removing `C` (which requires `P`).
Dependency processing details displayed during the depsolving phase.	Not supported	In DNF, the `depsolver` considers all dependencies for update candidates, which would result in a quite lengthy output. Note that the Yum v3 output can also be confusing and lengthy, especially for large transactions.

Yum v3 Feature, Command or Option	DNF Feature, Command or Option	Notable Differences
`yum provides` command	`dnf provides` command	The behavior of the `dnf provides` command is more closely aligned to how it's documented; whereas, during the execution of the `yum provides` command, Yum applies certain, undocumented behavior. For example, if you run the `yum provides sandbox` command, Yum applies extra heuristics to interpret the `sandbox` portion of the command, then it sequentially prepends entries from the `PATH` environment variable to the command to determine if it matches a file that is provided by a package. DNF does not emulate this undocumented behavior.
`--enableplugins` option	Not supported	This option is not documented for DNF, as all plugins are enabled by default.
`throttle` and `bandwidth` options	`throttle` and `bandwidth` options	In DNF, for multiple downloads that run simultaneously, the total downloading speed is now throttled. This support was not available in the Yum v3 tool, as downloaders ran in different processes.
`installonlypkgs` option	`installonlypkgs`	DNF appends the list values from the `installonlypkgs` configuration option to DNF defaults. Yum v3 overwrites the defaults by option values.
`deltarpm_percentage` option	Not supported	The boolean `deltarpm` option controls whether delta RPM files are used. Yum DNF does not support the use of the `deltarpm_percentage` option. Instead, the tool chooses an optimal value of the DRPM/RPM ratio to decide whether using `deltarpm` is appropriate in a given situation.

Yum v3 Feature, Command or Option	DNF Feature, Command or Option	Notable Differences
`.srpm` files and non-existent package handling	`.srpm` files and non-existent package handling	DNF terminates early with an error if a command requesting an installing operation on a local `.srpm` file is executed. Yum v3 issues a warning and continues by installing the `tour` package. Note that Yum DNF will emit the same error for package specifications that do not match any available package.
Promoting a package to install to a package that obsoletes it.	Promoting a package to install to a package that obsoletes it.	DNF does not automatically replace a request to install a package (`A`) by installing another package (`B`) if package B would obsolete package(`A`. The Yum v3 behavior is to perform the action if the `obsoletes` configuration option is enabled. However, note that this behavior is not properly documented and can be harmful.
`--installroot` option	`--installroot` option	DNF provides more predictable behavior for this option and handles the path differently than the `--config` option, where this path is always related to the host system. Yum v3 combines this path with the `installroot` option. The `reposdir` option is also handled slightly differently in Yum DNF. For example, if one `reposdirs` path exists inside of `installroot`, then repositories are taken strictly from `installroot`. Whereas, Yum v3 tests each path from `reposdir` separately.
Prompts displayed after a transaction table	Prompts displayed after a transaction table	The prompts that are displayed after a transaction table are different in DNF than they are for Yum v3. DNF does not provide download functionality after displaying the transaction table. You are only prompted to continue with the transaction or not. If you want to download packages, use the `download` command.

Yum v3 Feature, Command or Option	DNF Feature, Command or Option	Notable Differences
`list` command	`list` command	The DNF behavior for this command is to list all packages from all repositories, which means there can be duplicate package names with different repository names listed. This change was made to enable users to choose a preferred repository.

There is no direct replacement for `yum-updateonboot` command in DNF. However, you can obtain a similar result by running the `dnfautomatic` command.

The following table compares Yum V3 plugins with DNF plugins.

Yum Version 3 Plugin	DNF Plugin	Package
`yum check`	`dnf repoquery -- unsatisfied`	`dnf`
`yum-langpacks`		`dnf-langpacks`
`yum-plugin-auto-update-debug-info`	Option in `debuginfo-install.conf`	`dnf-plugins-core`
`yum-plugin-copr`	`dnf copr`	`dnf-plugins-core`
`yum-plugin-fastestmirror`	`fastestmirror` option in `dnf.conf`	`dnf`
`yum-plugin-fs-snapshot`		`dnf-plugins-extras-snapper`
`yum-plugin-local`		`dnf-plugins-core`
`yum-plugin-merge-conf`		`dnf-plugins-extras-rpmconf`
`yum-plugin-priorities`	`priority` option in `dnf.conf`	`dnf`
`yum-plugin-remove-with-leaves`	`dnfautoremove`	`dnf`
`yum-plugin-show-leaves`		`dnf-plugins-core`
`yum-plugin-versionlock`		`dnf-plugins-core`
`yum-rhn-plugin`		`dnf-plugin-spacewalk`

The following table compares Yum v3 utilities with DNF plugins.

Yum Version 3 Utility	DNF Plugin	DNF Package
`debuginfo-install`	`dnf debuginfo-install`	`dnf-plugins-core`
`find-repos-of-install`	`dnf list installed`	`dnf`
`needs-restarting`	`dnf tracer`	`dnf-plugins-extras-tracer`
`package-cleanup`	`dnf list`, `dnf repoquery`	`dnf`, `dnf-plugins-core`
`repoclosure`	`dnf repoclosure`	`dnf-plugins-extras-repoclosure`
`repodiff`	`dnf repodiff`	`dnf-plugins-core`
`repo-graph`	`dnf repograph`	`dnf-plugins-extras-repograph`
`repomanage`	`dnf repomanage`	`dnf-plugins-extras-repomanage`
`repoquery`	`dnf repoquery`	`dnf`
`reposync`	`dnf reposync`	`dnf-plugins-core`
`repotrack`	`dnf download -resolve -alldeps`	`dnf-plugins-core`
`yum-builddep`	`dnf builddep`	`dnf-plugins-core`
`yum-config-manager`	`dnf config-manager`	`dnf-plugins-core`
`yum-debug-dump`	`dnf debug-dump`	`dnf-plugins-extras-debug`
`yum-debug-restore`	`dnf debug-restore`	`dnf-plugins-extras-debug`
`yumdownloader`	`dnf download`	`dnf-plugins-core`

The following table lists the Yum v3 `package-cleanup` command and its DNF replacement.

Yum Version 3 Command	DNF Command
`package-cleanup--dupes`	`dnfrepoquery--duplicates`
`package-cleanup--leaves`	`dnfrepoquery--unneeded`
`package-cleanup--orphans`	`dnfrepoquery--extras`
`package-cleanup--oldkernels`	`dnfrepoquery--installonly`
`package-cleanup--problems`	`dnfrepoquery--unsatisfied`
`package-cleanup--cleandupes`	`dnfremove--duplicates`
`package-cleanup--oldkernels`	`dnfremove--oldinstallonly`

5

Package Changes from the Upstream Release

The following sections list the changes to binary and source packages from the upstream release.

Changes to Binary Packages

This section contains information about the removed, modified, and new **binary** packages in this release. For information about the **source** package changes, see Changes to Source Packages.

Added Binary Packages for BaseOS by Oracle

The following binary packages have been added to the BaseOS by Oracle:

- `oraclelinux-release`
- `oracle-backgrounds`
- `oracle-logos`
- `oracle-logos-httpd`
- `oracle-logos-ipa`

Modified BaseOS Binary Packages

The following binary packages from the BaseOS upstream release have been modified:

- `audispd-plugins`
- `audispd-plugins-zos`
- `autofs`
- `autofs-debugsource`
- `binutils`
- `binutils-debugsource`
- `binutils-devel`
- `boom-boot`
- `boom-boot-conf`
- `boom-boot-grub2`
- `chrony`
- `chrony-debugsource`

- `cockpit`
- `cockpit-bridge`
- `cockpit-composer`
- `cockpit-debugsource`
- `cockpit-doc`
- `cockpit-system`
- `cockpit-ws`
- `coreutils`
- `coreutils-common`
- `coreutils-debugsource`
- `coreutils-single`
- `dbus`
- `dbus-common`
- `dbus-daemon`
- `dbus-debugsource`
- `dbus-devel`
- `dbus-libs`
- `dbus-tests`
- `dbus-tools`
- `dbus-x11`
- `dracut`
- `dracut-caps`
- `dracut-config-generic`
- `dracut-config-rescue`
- `dracut-debugsource`
- `dracut-live`
- `dracut-network`
- `dracut-squash`
- `dracut-tools`
- `efibootmgr`
- `efibootmgr-debugsource`
- `efi-filesystem`
- `elfutils`
- `elfutils-debugsource`
- `elfutils-default-yama-scope`

- `elfutils-devel`
- `elfutils-devel-static`
- `elfutils-libelf`
- `elfutils-libelf-devel`
- `elfutils-libelf-devel-static`
- `elfutils-libs`
- `fuse`
- `fuse3`
- `fuse3-devel`
- `fuse3-libs`
- `fuse-common`
- `fuse-debugsource`
- `fuse-devel`
- `fuse-libs`
- `fwupdate`
- `fwupdate-debugsource`
- `fwupdate-devel`
- `fwupdate-efi`
- `fwupdate-libs`
- `glibc`
- `glibc-all-langpacks`
- `glibc-benchtests`
- `glibc-common`
- `glibc-devel`
- `glibc-headers`
- `glibc-langpack-aa`
- `glibc-langpack-af`
- `glibc-langpack-agr`
- `glibc-langpack-ak`
- `glibc-langpack-am`
- `glibc-langpack-an`
- `glibc-langpack-anp`
- `glibc-langpack-ar`
- `glibc-langpack-as`
- `glibc-langpack-ast`

- `glibc-langpack-ayc`
- `glibc-langpack-az`
- `glibc-langpack-be`
- `glibc-langpack-bem`
- `glibc-langpack-ber`
- `glibc-langpack-bg`
- `glibc-langpack-bhb`
- `glibc-langpack-bho`
- `glibc-langpack-bi`
- `glibc-langpack-bn`
- `glibc-langpack-bo`
- `glibc-langpack-br`
- `glibc-langpack-brx`
- `glibc-langpack-bs`
- `glibc-langpack-byn`
- `glibc-langpack-ca`
- `glibc-langpack-ce`
- `glibc-langpack-chr`
- `glibc-langpack-cmn`
- `glibc-langpack-crh`
- `glibc-langpack-cs`
- `glibc-langpack-csb`
- `glibc-langpack-cv`
- `glibc-langpack-cy`
- `glibc-langpack-da`
- `glibc-langpack-de`
- `glibc-langpack-doi`
- `glibc-langpack-dsb`
- `glibc-langpack-dv`
- `glibc-langpack-dz`
- `glibc-langpack-el`
- `glibc-langpack-en`
- `glibc-langpack-eo`
- `glibc-langpack-es`
- `glibc-langpack-et`

- `glibc-langpack-eu`
- `glibc-langpack-fa`
- `glibc-langpack-ff`
- `glibc-langpack-fi`
- `glibc-langpack-fil`
- `glibc-langpack-fo`
- `glibc-langpack-fr`
- `glibc-langpack-fur`
- `glibc-langpack-fy`
- `glibc-langpack-ga`
- `glibc-langpack-gd`
- `glibc-langpack-gez`
- `glibc-langpack-gl`
- `glibc-langpack-gu`
- `glibc-langpack-gv`
- `glibc-langpack-ha`
- `glibc-langpack-hak`
- `glibc-langpack-he`
- `glibc-langpack-hi`
- `glibc-langpack-hif`
- `glibc-langpack-hne`
- `glibc-langpack-hr`
- `glibc-langpack-hsb`
- `glibc-langpack-ht`
- `glibc-langpack-hu`
- `glibc-langpack-hy`
- `glibc-langpack-ia`
- `glibc-langpack-id`
- `glibc-langpack-ig`
- `glibc-langpack-ik`
- `glibc-langpack-is`
- `glibc-langpack-it`
- `glibc-langpack-iu`
- `glibc-langpack-ja`
- `glibc-langpack-ka`

- `glibc-langpack-kab`
- `glibc-langpack-kk`
- `glibc-langpack-kl`
- `glibc-langpack-km`
- `glibc-langpack-kn`
- `glibc-langpack-ko`
- `glibc-langpack-kok`
- `glibc-langpack-ks`
- `glibc-langpack-ku`
- `glibc-langpack-kw`
- `glibc-langpack-ky`
- `glibc-langpack-lb`
- `glibc-langpack-lg`
- `glibc-langpack-li`
- `glibc-langpack-lij`
- `glibc-langpack-ln`
- `glibc-langpack-lo`
- `glibc-langpack-lt`
- `glibc-langpack-lv`
- `glibc-langpack-lzh`
- `glibc-langpack-mag`
- `glibc-langpack-mai`
- `glibc-langpack-mfe`
- `glibc-langpack-mg`
- `glibc-langpack-mhr`
- `glibc-langpack-mi`
- `glibc-langpack-miq`
- `glibc-langpack-mjw`
- `glibc-langpack-mk`
- `glibc-langpack-ml`
- `glibc-langpack-mn`
- `glibc-langpack-mni`
- `glibc-langpack-mr`
- `glibc-langpack-ms`
- `glibc-langpack-mt`

- `glibc-langpack-my`
- `glibc-langpack-nan`
- `glibc-langpack-nb`
- `glibc-langpack-nds`
- `glibc-langpack-ne`
- `glibc-langpack-nhn`
- `glibc-langpack-niu`
- `glibc-langpack-nl`
- `glibc-langpack-nn`
- `glibc-langpack-nr`
- `glibc-langpack-nso`
- `glibc-langpack-oc`
- `glibc-langpack-om`
- `glibc-langpack-or`
- `glibc-langpack-os`
- `glibc-langpack-pa`
- `glibc-langpack-pap`
- `glibc-langpack-pl`
- `glibc-langpack-ps`
- `glibc-langpack-pt`
- `glibc-langpack-quz`
- `glibc-langpack-raj`
- `glibc-langpack-ro`
- `glibc-langpack-ru`
- `glibc-langpack-rw`
- `glibc-langpack-sa`
- `glibc-langpack-sah`
- `glibc-langpack-sat`
- `glibc-langpack-sc`
- `glibc-langpack-sd`
- `glibc-langpack-se`
- `glibc-langpack-sgs`
- `glibc-langpack-shn`
- `glibc-langpack-shs`
- `glibc-langpack-si`

- `glibc-langpack-sid`
- `glibc-langpack-sk`
- `glibc-langpack-sl`
- `glibc-langpack-sm`
- `glibc-langpack-so`
- `glibc-langpack-sq`
- `glibc-langpack-sr`
- `glibc-langpack-ss`
- `glibc-langpack-st`
- `glibc-langpack-sv`
- `glibc-langpack-sw`
- `glibc-langpack-szl`
- `glibc-langpack-ta`
- `glibc-langpack-tcy`
- `glibc-langpack-te`
- `glibc-langpack-tg`
- `glibc-langpack-th`
- `glibc-langpack-the`
- `glibc-langpack-ti`
- `glibc-langpack-tig`
- `glibc-langpack-tk`
- `glibc-langpack-tl`
- `glibc-langpack-tn`
- `glibc-langpack-to`
- `glibc-langpack-tpi`
- `glibc-langpack-tr`
- `glibc-langpack-ts`
- `glibc-langpack-tt`
- `glibc-langpack-ug`
- `glibc-langpack-uk`
- `glibc-langpack-unm`
- `glibc-langpack-ur`
- `glibc-langpack-uz`
- `glibc-langpack-ve`
- `glibc-langpack-vi`

- `glibc-langpack-wa`
- `glibc-langpack-wae`
- `glibc-langpack-wal`
- `glibc-langpack-wo`
- `glibc-langpack-xh`
- `glibc-langpack-yi`
- `glibc-langpack-yo`
- `glibc-langpack-yue`
- `glibc-langpack-yuw`
- `glibc-langpack-zh`
- `glibc-langpack-zu`
- `glibc-locale-source`
- `glibc-minimal-langpack`
- `glibc-nss-devel`
- `glibc-static`
- `glibc-utils`
- `grub2-common`
- `grub2-efi-ia32`
- `grub2-efi-ia32-cdboot`
- `grub2-efi-ia32-modules`
- `grub2-efi-x64`
- `grub2-efi-x64-cdboot`
- `grub2-efi-x64-modules`
- `grub2-pc`
- `grub2-pc-modules`
- `grub2-tools`
- `grub2-tools-efi`
- `grub2-tools-extra`
- `grub2-tools-minimal`
- `grubby`
- `grubby-debugsource`
- `grubby-deprecated`
- `iscsi-initiator-utils`
- `iscsi-initiator-utils-debugsource`
- `iscsi-initiator-utils-devel`

- `iscsi-initiator-utils-iscsiuio`
- `kernel-rpm-macros`
- `kexec-tools`
- `kexec-tools-debugsource`
- `kmod`
- `kmod-debugsource`
- `kmod-devel`
- `kmod-kvdo`
- `kmod-kvdo-debugsource`
- `kmod-libs`
- `ksc`
- `libasan`
- `libasan-static`
- `libatomic`
- `libatomic-static`
- `libdnf`
- `libdnf-debugsource`
- `libdnf-devel`
- `libgcc`
- `libgfortran`
- `libgfortran-static`
- `libgomp`
- `libgomp-offload-nvptx`
- `libitm`
- `libitm-devel`
- `libitm-static`
- `libkcapi`
- `libkcapi-debugsource`
- `libkcapi-devel`
- `libkcapi-doc`
- `libkcapi-hmaccalc`
- `libkcapi-static`
- `libkcapi-tests`
- `libkcapi-tools`
- `libnsl`

- `libquadmath`

- `libquadmath-devel`

- `libquadmath-static`

- `libreport-filesystem`

- `libstdc++`

- `libstdc++-devel`

- `libstdc++-docs`

- `libstdc++-static`

- `libtsan`

- `libtsan-static`

- `libubsan`

- `libubsan-static`

- `libxml2`

- `libxml2-debugsource`

- `libxml2-devel`

- `libxml2-static`

- `libxslt`

- `libxslt-debugsource`

- `libxslt-devel`

- `mdadm`

- `mdadm-debugsource`

- `mozjs52`

- `mozjs52-debugsource`

- `mozjs52-devel`

- `nscd`

- `nss_db`

- `opa-address-resolution`

- `opa-basic-tools`

- `opa-fastfabric`

- `opa-fm`

- `opa-fm-debugsource`

- `opa-libopamgt`

- `opa-libopamgt-devel`

- `OpenIPMI`

- `OpenIPMI-debugsource`

- OpenIPMI-devel
- OpenIPMI-lanserv
- OpenIPMI-libs
- OpenIPMI-perl
- openssl
- openssl-debugsource
- openssl-devel
- openssl-libs
- openssl-perl
- openssl-static
- os-prober
- os-prober-debugsource
- parted
- parted-debugsource
- parted-devel
- platform-python
- platform-python-debug
- platform-python-devel
- policycoreutils
- policycoreutils-dbus
- policycoreutils-debugsource
- policycoreutils-devel
- policycoreutils-gui
- policycoreutils-newrole
- policycoreutils-python-utils
- policycoreutils-restorecond
- policycoreutils-sandbox
- polkit
- polkit-debugsource
- polkit-devel
- polkit-docs
- polkit-libs
- python3-boom
- python3-configshell
- python3-hawkey

- `python3-iscsi-initiator-utils`
- `python3-libdnf`
- `python3-libs`
- `python3-libxml2`
- `python3-openipmi`
- `python3-policycoreutils`
- `python3-rtslib`
- `python3-syspurpose`
- `python3-test`
- `redhat-indexhtml`
- `redhat-release`
- `rpm-ostree`
- `rpm-ostree-debugsource`
- `rpm-ostree-devel`
- `rpm-ostree-libs`
- `sanlock-lib`
- `selinux-policy`
- `selinux-policy-devel`
- `selinux-policy-doc`
- `selinux-policy-minimum`
- `selinux-policy-mls`
- `selinux-policy-sandbox`
- `selinux-policy-targeted`
- `sos`
- `sos-audit`
- `stunnel`
- `target-restore`
- `tuned`
- `tuned-profiles-atomic`
- `tuned-profiles-compat`
- `tuned-profiles-cpu-partitioning`
- `tuned-profiles-mssql`
- `tuned-profiles-oracle`
- `xfsprogs`
- `xfsprogs-debugsource`

ORACLE

- `xfsprogs-devel`

5-14

Modified AppStream Binary Packages

The following binary packages from the AppStream upstream release have been modified:

- `abrt`
- `abrt-addon-ccpp`
- `abrt-addon-coredump-helper`
- `abrt-addon-kerneloops`
- `abrt-addon-pstoreoops`
- `abrt-addon-upload-watch`
- `abrt-addon-vmcore`
- `abrt-addon-xorg`
- `abrt-atomic`
- `abrt-cli`
- `abrt-cli-ng`
- `abrt-console-notification`
- `abrt-dbus`
- `abrt-debugsource`
- `abrt-desktop`
- `abrt-devel`
- `abrt-gui`
- `abrt-gui-devel`
- `abrt-gui-libs`
- `abrt-libs`
- `abrt-plugin-machine-id`
- `abrt-plugin-sosreport`
- `abrt-retrace-client`
- `abrt-tui`
- `anaconda`
- `anaconda-core`
- `anaconda-debugsource`
- `anaconda-dracut`
- `anaconda-gui`
- `anaconda-install-env-deps`
- `anaconda-tui`

- `anaconda-user-help`
- `anaconda-widgets`
- `anaconda-widgets-devel`
- `autocorr-af`
- `autocorr-bg`
- `autocorr-ca`
- `autocorr-cs`
- `autocorr-da`
- `autocorr-de`
- `autocorr-en`
- `autocorr-es`
- `autocorr-fa`
- `autocorr-fi`
- `autocorr-fr`
- `autocorr-ga`
- `autocorr-hr`
- `autocorr-hu`
- `autocorr-is`
- `autocorr-it`
- `autocorr-ja`
- `autocorr-ko`
- `autocorr-lb`
- `autocorr-lt`
- `autocorr-mn`
- `autocorr-nl`
- `autocorr-pl`
- `autocorr-pt`
- `autocorr-ro`
- `autocorr-ru`
- `autocorr-sk`
- `autocorr-sl`
- `autocorr-sr`
- `autocorr-sv`
- `autocorr-tr`
- `autocorr-vi`

ORACLE

- autocorr-zh
- binutils-devel
- blivet-data
- buildah
- buildah-debuginfo
- buildah-debugsource
- clang
- clang-analyzer
- clang-debuginfo
- clang-debugsource
- clang-devel
- clang-libs
- clang-libs-debuginfo
- clang-tools-extra
- clang-tools-extra-debuginfo
- cloud-init
- cockpit-composer
- compat-libgfortran
- compat-libpthread-nonshared
- compat-openssl10
- compat-openssl10-debugsource
- composer-cli
- containernetworking-plugins
- containernetworking-plugins-debuginfo
- containernetworking-plugins-debugsource
- containers-common
- cpp
- cups-filters
- cups-filters-debugsource
- cups-filters-devel
- cups-filters-libs
- daxio
- dbus-devel
- dbus-x11
- efi-srpm-macros

- firefox

- firefox-debugsource

- gcc

- gcc-c++

- gcc-debugsource

- gcc-gdb-plugin

- gcc-gfortran

- gcc-offload-nvptx

- gcc-plugin-devel

- git-clang-format

- glibc-utils

- httpd

- httpd-debuginfo

- httpd-debugsource

- httpd-devel

- httpd-filesystem

- httpd-manual

- httpd-tools

- httpd-tools-debuginfo

- initial-setup

- initial-setup-gui

- ipa-client

- ipa-client-common

- ipa-client-debuginfo

- ipa-common

- ipa-python-compat

- ipa-server

- ipa-server-common

- ipa-server-debuginfo

- ipa-server-dns

- ipa-server-trust-ad

- ipa-server-trust-ad-debuginfo

- java

- kernel-rpm-macros

- ksh

- ksh-debugsource
- libguestfs
- libguestfs-bash-completion
- libguestfs-benchmarking
- libguestfs-benchmarking-debuginfo
- libguestfs-debuginfo
- libguestfs-debugsource
- libguestfs-devel
- libguestfs-gfs2
- libguestfs-gobject
- libguestfs-gobject-debuginfo
- libguestfs-gobject-devel
- libguestfs-inspect-icons
- libguestfs-java
- libguestfs-java-debuginfo
- libguestfs-java-devel
- libguestfs-javadoc
- libguestfs-man-pages-ja
- libguestfs-man-pages-uk
- libguestfs-rescue
- libguestfs-rsync
- libguestfs-tools
- libguestfs-tools-c
- libguestfs-tools-c-debuginfo
- libguestfs-xfs
- libitm-devel
- libpmem
- libpmemblk
- libpmemblk-debug
- libpmemblk-devel
- libpmem-debug
- libpmem-devel
- libpmemlog
- libpmemlog-debug
- libpmemlog-devel

- `libpmemobj`
- `libpmemobj-debug`
- `libpmemobj-devel`
- `libpmempool`
- `libpmempool-debug`
- `libpmempool-devel`
- `libquadmath-devel`
- `libreoffice-base`
- `libreoffice-calc`
- `libreoffice-core`
- `libreoffice-data`
- `libreoffice-draw`
- `libreoffice-emailmerge`
- `libreoffice-filters`
- `libreoffice-graphicfilter`
- `libreoffice-gtk2`
- `libreoffice-gtk3`
- `libreoffice-help-ar`
- `libreoffice-help-bg`
- `libreoffice-help-bn`
- `libreoffice-help-ca`
- `libreoffice-help-cs`
- `libreoffice-help-da`
- `libreoffice-help-de`
- `libreoffice-help-dz`
- `libreoffice-help-el`
- `libreoffice-help-en`
- `libreoffice-help-es`
- `libreoffice-help-et`
- `libreoffice-help-eu`
- `libreoffice-help-fi`
- `libreoffice-help-fr`
- `libreoffice-help-gl`
- `libreoffice-help-gu`
- `libreoffice-help-he`

- `libreoffice-help-hi`
- `libreoffice-help-hr`
- `libreoffice-help-hu`
- `libreoffice-help-id`
- `libreoffice-help-it`
- `libreoffice-help-ja`
- `libreoffice-help-ko`
- `libreoffice-help-lt`
- `libreoffice-help-lv`
- `libreoffice-help-nb`
- `libreoffice-help-nl`
- `libreoffice-help-nn`
- `libreoffice-help-pl`
- `libreoffice-help-pt-BR`
- `libreoffice-help-pt-PT`
- `libreoffice-help-ro`
- `libreoffice-help-ru`
- `libreoffice-help-si`
- `libreoffice-help-sk`
- `libreoffice-help-sl`
- `libreoffice-help-sv`
- `libreoffice-help-ta`
- `libreoffice-help-tr`
- `libreoffice-help-uk`
- `libreoffice-help-zh-Hans`
- `libreoffice-help-zh-Hant`
- `libreoffice-impress`
- `libreofficekit`
- `libreofficekit-devel`
- `libreoffice-langpack-af`
- `libreoffice-langpack-ar`
- `libreoffice-langpack-as`
- `libreoffice-langpack-bg`
- `libreoffice-langpack-bn`
- `libreoffice-langpack-br`

- `libreoffice-langpack-ca`
- `libreoffice-langpack-cs`
- `libreoffice-langpack-cy`
- `libreoffice-langpack-da`
- `libreoffice-langpack-de`
- `libreoffice-langpack-dz`
- `libreoffice-langpack-el`
- `libreoffice-langpack-en`
- `libreoffice-langpack-es`
- `libreoffice-langpack-et`
- `libreoffice-langpack-eu`
- `libreoffice-langpack-fa`
- `libreoffice-langpack-fi`
- `libreoffice-langpack-fr`
- `libreoffice-langpack-ga`
- `libreoffice-langpack-gl`
- `libreoffice-langpack-gu`
- `libreoffice-langpack-he`
- `libreoffice-langpack-hi`
- `libreoffice-langpack-hr`
- `libreoffice-langpack-hu`
- `libreoffice-langpack-id`
- `libreoffice-langpack-it`
- `libreoffice-langpack-ja`
- `libreoffice-langpack-kk`
- `libreoffice-langpack-kn`
- `libreoffice-langpack-ko`
- `libreoffice-langpack-lt`
- `libreoffice-langpack-lv`
- `libreoffice-langpack-mai`
- `libreoffice-langpack-ml`
- `libreoffice-langpack-mr`
- `libreoffice-langpack-nb`
- `libreoffice-langpack-nl`
- `libreoffice-langpack-nn`

- `libreoffice-langpack-nr`
- `libreoffice-langpack-nso`
- `libreoffice-langpack-or`
- `libreoffice-langpack-pa`
- `libreoffice-langpack-pl`
- `libreoffice-langpack-pt-BR`
- `libreoffice-langpack-pt-PT`
- `libreoffice-langpack-ro`
- `libreoffice-langpack-ru`
- `libreoffice-langpack-si`
- `libreoffice-langpack-sk`
- `libreoffice-langpack-sl`
- `libreoffice-langpack-sr`
- `libreoffice-langpack-ss`
- `libreoffice-langpack-st`
- `libreoffice-langpack-sv`
- `libreoffice-langpack-ta`
- `libreoffice-langpack-te`
- `libreoffice-langpack-th`
- `libreoffice-langpack-tn`
- `libreoffice-langpack-tr`
- `libreoffice-langpack-ts`
- `libreoffice-langpack-uk`
- `libreoffice-langpack-ve`
- `libreoffice-langpack-xh`
- `libreoffice-langpack-zh-Hans`
- `libreoffice-langpack-zh-Hant`
- `libreoffice-langpack-zu`
- `libreoffice-math`
- `libreoffice-ogltrans`
- `libreoffice-opensymbol-fonts`
- `libreoffice-pdfimport`
- `libreoffice-pyuno`
- `libreoffice-ure`
- `libreoffice-ure-common`

- `libreoffice-wiki-publisher`
- `libreoffice-writer`
- `libreoffice-x11`
- `libreoffice-xsltfilter`
- `libreport`
- `libreport-anaconda`
- `libreport-centos`
- `libreport-cli`
- `libreport-compat`
- `libreport-debugsource`
- `libreport-devel`
- `libreport-filesystem`
- `libreport-gtk`
- `libreport-gtk-devel`
- `libreport-newt`
- `libreport-plugin-bugzilla`
- `libreport-plugin-kerneloops`
- `libreport-plugin-logger`
- `libreport-plugin-mailx`
- `libreport-plugin-mantisbt`
- `libreport-plugin-reportuploader`
- `libreport-plugin-systemd-journal`
- `libreport-plugin-ureport`
- `libreport-web`
- `libreport-web-devel`
- `libreswan`
- `libreswan-debugsource`
- `librpmem`
- `librpmem-debug`
- `librpmem-devel`
- `librsvg2`
- `librsvg2-debugsource`
- `librsvg2-devel`
- `librsvg2-tools`
- `libsrtp`

- `libsrtp-debugsource`
- `libsrtp-devel`
- `libstdc++-devel`
- `libstdc++-docs`
- `libvirt`
- `libvirt-admin`
- `libvirt-admin-debuginfo`
- `libvirt-bash-completion`
- `libvirt-client`
- `libvirt-client-debuginfo`
- `libvirt-daemon`
- `libvirt-daemon-config-network`
- `libvirt-daemon-config-nwfilter`
- `libvirt-daemon-debuginfo`
- `libvirt-daemon-driver-interface`
- `libvirt-daemon-driver-interface-debuginfo`
- `libvirt-daemon-driver-network`
- `libvirt-daemon-driver-network-debuginfo`
- `libvirt-daemon-driver-nodedev`
- `libvirt-daemon-driver-nodedev-debuginfo`
- `libvirt-daemon-driver-nwfilter`
- `libvirt-daemon-driver-nwfilter-debuginfo`
- `libvirt-daemon-driver-qemu`
- `libvirt-daemon-driver-qemu-debuginfo`
- `libvirt-daemon-driver-secret`
- `libvirt-daemon-driver-secret-debuginfo`
- `libvirt-daemon-driver-storage`
- `libvirt-daemon-driver-storage-core`
- `libvirt-daemon-driver-storage-core-debuginfo`
- `libvirt-daemon-driver-storage-disk`
- `libvirt-daemon-driver-storage-disk-debuginfo`
- `libvirt-daemon-driver-storage-iscsi`
- `libvirt-daemon-driver-storage-iscsi-debuginfo`
- `libvirt-daemon-driver-storage-logical`
- `libvirt-daemon-driver-storage-logical-debuginfo`

- `libvirt-daemon-driver-storage-mpath`
- `libvirt-daemon-driver-storage-mpath-debuginfo`
- `libvirt-daemon-driver-storage-rbd`
- `libvirt-daemon-driver-storage-rbd-debuginfo`
- `libvirt-daemon-driver-storage-scsi`
- `libvirt-daemon-driver-storage-scsi-debuginfo`
- `libvirt-daemon-kvm`
- `libvirt-debuginfo`
- `libvirt-debugsource`
- `libvirt-devel`
- `libvirt-docs`
- `libvirt-libs`
- `libvirt-libs-debuginfo`
- `libvirt-lock-sanlock`
- `libvirt-lock-sanlock-debuginfo`
- `libvirt-nss`
- `libvirt-nss-debuginfo`
- `libvmem`
- `libvmem-debug`
- `libvmem-devel`
- `libvmmalloc`
- `libvmmalloc-debug`
- `libvmmalloc-devel`
- `libxml2-devel`
- `libxslt-devel`
- `llvm-toolset`
- `lorax`
- `lorax-composer`
- `lorax-lmc-novirt`
- `lorax-lmc-virt`
- `lorax-templates-generic`
- `lorax-templates-rhel`
- `lua-guestfs`
- `lua-guestfs-debuginfo`
- `mecab-ipadic`

- mecab-ipadic-EUCJP
- mod_ldap
- mod_ldap-debuginfo
- mod_md
- mod_md-debuginfo
- mod_proxy_html
- mod_proxy_html-debuginfo
- mod_session
- mod_session-debuginfo
- mod_ssl
- mod_ssl-debuginfo
- nginx
- nginx-all-modules
- nginx-debuginfo
- nginx-debugsource
- nginx-filesystem
- nginx-mod-http-image-filter
- nginx-mod-http-image-filter-debuginfo
- nginx-mod-http-perl
- nginx-mod-http-perl-debuginfo
- nginx-mod-http-xslt-filter
- nginx-mod-http-xslt-filter-debuginfo
- nginx-mod-mail
- nginx-mod-mail-debuginfo
- nginx-mod-stream
- nginx-mod-stream-debuginfo
- npm
- nss-softokn
- nss-softokn-debugsource
- nss-softokn-devel
- nss-softokn-freebl
- nss-softokn-freebl-devel
- openscap
- openscap-containers
- openscap-debugsource

- openscap-devel
- openscap-engine-sce
- openscap-engine-sce-devel
- openscap-python3
- openscap-scanner
- openscap-utils
- open-vm-tools
- open-vm-tools-debugsource
- open-vm-tools-desktop
- open-vm-tools-devel
- open-vm-tools-test
- osinfo-db
- PackageKit
- PackageKit-command-not-found
- PackageKit-cron
- PackageKit-debugsource
- PackageKit-glib
- PackageKit-glib-devel
- PackageKit-gstreamer-plugin
- PackageKit-gtk3-module
- perl-Sys-Guestfs
- perl-Sys-Guestfs-debuginfo
- perl-XML-Parser
- perl-XML-Parser-debugsource
- pesign
- pesign-debugsource
- platform-python
- platform-python-debug
- platform-python-devel
- plymouth
- plymouth-core-libs
- plymouth-debugsource
- plymouth-devel
- plymouth-graphics-libs
- plymouth-plugin-fade-throbber

- `plymouth-plugin-label`
- `plymouth-plugin-script`
- `plymouth-plugin-space-flares`
- `plymouth-plugin-throbgress`
- `plymouth-plugin-two-step`
- `plymouth-scripts`
- `plymouth-system-theme`
- `plymouth-theme-charge`
- `plymouth-theme-fade-in`
- `plymouth-theme-script`
- `plymouth-theme-solar`
- `plymouth-theme-spinfinity`
- `plymouth-theme-spinner`
- `pmempool`
- `podman`
- `podman-debuginfo`
- `podman-debugsource`
- `podman-docker`
- `policycoreutils-gui`
- `policycoreutils-sandbox`
- `pykickstart`
- `python2`
- `python2-daemon`
- `python2-debug`
- `python2-debuginfo`
- `python2-debugsource`
- `python2-devel`
- `python2-libs`
- `python2-test`
- `python2-tkinter`
- `python2-tools`
- `python3-abrt`
- `python3-abrt-addon`
- `python3-abrt-container-addon`
- `python3-abrt-doc`

- `python3-blivet`
- `python3-idle`
- `python3-ipaclient`
- `python3-ipalib`
- `python3-ipaserver`
- `python3-kickstart`
- `python3-libguestfs`
- `python3-libguestfs-debuginfo`
- `python3-libreport`
- `python3-rhnlib`
- `python3-spacewalk-backend-libs`
- `python3-test`
- `python3-tkinter`
- `rear`
- `redhat-lsb`
- `redhat-lsb-core`
- `redhat-lsb-cxx`
- `redhat-lsb-debugsource`
- `redhat-lsb-desktop`
- `redhat-lsb-languages`
- `redhat-lsb-printing`
- `redhat-lsb-submod-multimedia`
- `redhat-lsb-submod-security`
- `redhat-lsb-supplemental`
- `redhat-lsb-trialuse`
- `redhat-rpm-config`
- `rhn-custom-info`
- `rhnlib`
- `rhnsd`
- `rhnsd-debuginfo`
- `rhnsd-debugsource`
- `rpmdevtools`
- `rpmemd`
- `rpm-ostree`
- `rpm-ostree-debugsource`

ORACLE®

- rpm-ostree-devel
- rpm-ostree-libs
- ruby-libguestfs
- ruby-libguestfs-debuginfo
- runc
- runc-debuginfo
- runc-debugsource
- sanlk-reset
- sanlock
- sanlock-debugsource
- sanlock-devel
- sanlock-lib
- scap-security-guide
- scap-security-guide-doc
- scap-workbench
- scap-workbench-debugsource
- setroubleshoot
- setroubleshoot-debugsource
- setroubleshoot-legacy
- setroubleshoot-plugins
- setroubleshoot-server
- skopeo
- skopeo-debuginfo
- skopeo-debugsource
- thunderbird
- thunderbird-debugsource
- tog-pegasus
- tog-pegasus-debugsource
- tog-pegasus-devel
- tog-pegasus-libs
- tog-pegasus-test
- tuned-gtk
- tuned-utils
- tuned-utils-systemtap
- virt-dib

- `virt-dib-debuginfo`

- `virt-install`

- `virt-manager`

- `virt-manager-common`

- `virt-p2v-maker`

- `virt-v2v`

- `virt-v2v-debuginfo`

- `wget`

- `xsane`

- `xsane-common`

- `xsane-debugsource`

- `xsane-gimp`

Removed BaseOS Binary Packages

The following binary packages from the BaseOS upstream release have been removed:

- `atlas-z10`

- `atlas-z10-devel`

- `atlas-z196`

- `atlas-z196-devel`

- `dnf-plugin-subscription-manager`

- `grub2-ppc64le`

- `grub2-ppc64le-modules`

- `kernel-zfcpdump`

- `kernel-zfcpdump-core`

- `kernel-zfcpdump-devel`

- `kernel-zfcpdump-modules`

- `kernel-zfcpdump-modules-extra`

- `kpatch`

- `libcxl`

- `libica`

- `libica-devel`

- `libocxl`

- `librtas`

- `librtas-devel`

- `libservicelog`

- `libservicelog-devel`
- `libvpd`
- `libzfcphbaapi`
- `libzfcphbaapi-docs`
- `lsvpd`
- `opal-firmware`
- `opal-prd`
- `opal-utils`
- `opencryptoki-ccatok`
- `opencryptoki-ep11tok`
- `opencryptoki-icatok`
- `openssl-ibmca`
- `powerpc-utils`
- `powerpc-utils-core`
- `ppc64-diag`
- `python3-subscription-manager-rhsm`
- `python3-syspurpose`
- `qclib`
- `qclib-devel`
- `redhat-logos`
- `redhat-logos-httpd`
- `s390utils-base`
- `servicelog`
- `shim-aa64`
- `subscription-manager`
- `subscription-manager-cockpit`
- `subscription-manager-plugin-container`
- `subscription-manager-plugin-ostree`
- `subscription-manager-rhsm-certificates`
- `tss2`

Removed AppStream Binary Packages

The following binary packages from the AppStream upstream release have been removed:

- `edk2-aarch64`
- `fence-agents-lpar`

- `fence-agents-zvm`

- `insights-client`

- `libblockdev-s390`

- `libreport-plugin-rhtsupport`

- `libreport-rhel`

- `libreport-rhel-anaconda-bugzilla`

- `libreport-rhel-bugzilla`

- `redhat-logos-ipa`

- `redhat-support-lib-python`

- `redhat-support-tool`

- `s390utils`

- `s390utils-cmsfs`

- `s390utils-cmsfs-fuse`

- `s390utils-cpacfstatsd`

- `s390utils-cpuplugd`

- `s390utils-hmcdrvfs`

- `s390utils-iucvterm`

- `s390utils-mon_statd`

- `s390utils-osasnmpd`

- `s390utils-zdsfs`

- `s390utils-ziomon`

- `SLOF`

- `subscription-manager-initial-setup-addon`

- `subscription-manager-migration`

- `subscription-manager-migration-data`

- `virt-who`

Removed CodeReady Linux Builder Binary Packages

The following binary packages from the CodeReady Linux Builder upstream release have been removed:

- `clucene-contribs-lib`

- `exiv2`

- `exiv2-libs`

- `json-glib-devel`

- `libcxl-devel`

- `libdnet`

- `libdv`
- `libdwarf`
- `libetonyek`
- `libgexiv2`
- `libgpod`
- `libgsf`
- `libimobiledevice`
- `liblangtag`
- `liblangtag-data`
- `libmad`
- `libmspack`
- `libocxl-devel`
- `libocxl-docs`
- `libodfgen`
- `libpeas-gtk`
- `libplist`
- `libquvi`
- `libquvi-scripts`
- `LibRaw-devel`
- `libreoffice-gtk2`
- `libreoffice-x11`
- `libusbmuxd`
- `libvisio`
- `libvncserver`
- `libwps`
- `libxkbcommon-x11`
- `lttng-ust`
- `lua-expat`
- `lua-json`
- `lua-lpeg`
- `lua-socket`
- `opencl-filesystem`
- `python3-qt5`
- `s390utils-devel`
- `tss2-devel`

Changes to Source Packages

This section contains information about the removed, modified, and new **source** packages in this release. For information about the **binary** package changes, see Changes to Binary Packages.

Added Source Packages for BaseOS by Oracle

The following source packages have been added to the BaseOS by Oracle:

- `oraclelinux-release`
- `oracle-logos`

Modified BaseOS Source Packages

The following source packages from the BaseOS upstream release have been modified:

- `autofs`
- `binutils`
- `boom-boot`
- `chrony`
- `cockpit`
- `coreutils`
- `dbus`
- `dracut`
- `efibootmgr`
- `fuse`
- `fwupdate`
- `glibc`
- `grubby`
- `iscsi-initiator-utils`
- `kernel`
- `kexec-tools`
- `kmod`
- `kmod-kvdo`
- `ksc`
- `libdnf`
- `libkcapi`
- `libxml2`
- `libxslt`

- `mdadm`

- `mozjs52`

- `opa-fm`

- `OpenIPMI`

- `openssl`

- `os-prober`

- `parted`

- `policycoreutils`

- `polkit`

- `python3-syspurpose`

- `redhat-indexhtml`

- `redhat-release`

- `selinux-policy`

- `sos`

- `stunnel`

- `systemd`

- `tuned`

- `xfsprogs`

Modified AppStream Source Packages

The following source packages from the AppStream upstream release have been modified:

- `abrt`

- `anaconda`

- `anaconda-user-help`

- `clang`

- `cloud-init`

- `compat-libgfortran-48`

- `cups-filters`

- `firefox`

- `gcc`

- `httpd`

- `initial-setup`

- `java-11-openjdk`

- `ksh`

- `libguestfs`

- `libreport`

- `libreswan`

- `libvirt`

- `lorax`

- `lorax-templates-rhel`

- `mecab-ipadic`

- `nginx`

- `openscap`

- `open-vm-tools`

- `osinfo-db`

- `PackageKit`

- `perl-XML-Parser`

- `pesign`

- `plymouth`

- `pykickstart`

- `python2`

- `python3-blivet`

- `rear`

- `redhat-lsb`

- `redhat-rpm-config`

- `rhn-client-tools`

- `rhn-custom-info`

- `rhnlib`

- `rhnsd`

- `rpmdevtools`

- `rpm-ostree`

- `sanlock`

- `scap-security-guide`

- `scap-workbench`

- `setroubleshoot`

- `setroubleshoot-plugins`

- `thunderbird`

- `tog-pegasus`

- `tuned`

- `virt-manager`

ORACLE®

- wget

- xsane

Removed BaseOS Source Packages

The following source packages from the BaseOS upstream release have been removed:

- kpatch

- libcxl

- libica

- libocxl

- librtas

- libservicelog

- libvpd

- libzfcphbaapi

- lsvpd

- opal-prd

- openssl-ibmca

- powerpc-utils

- ppc64-diag

- qclib

- redhat-logos

- servicelog

- subscription-manager

Removed AppStream Source Packages

The following source packages from the AppStream upstream release have been removed:

- insights-client

- redhat-support-lib-python

- redhat-support-tool

- s390utils

- SLOF

- subscription-manager-migration-data

- virt-who