Oracle Linux 10

Release Notes for Oracle Linux 10

G14593-08
August 2025

Oracle Linux 10 Release Notes for Oracle Linux 10,

G14593-08

Contents

3 Deprecated Features

4 Removed Features

Preface

Oracle Linux 10: Release Notes for Oracle Linux 10 provides information about the new features and known issues in the Oracle Linux 10 release. The information applies to both x86_64 and 64-bit Arm (aarch64) architectures. This document might be updated after it is released.

1

About Oracle Linux 10

The current Oracle Linux 10 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 OS adaptable to different types of deployment such as on-premises installations, hybrid deployments that combine on-premises and cloud installations, and full cloud deployment.

> **Important**
>
> Upgrading from an Oracle Linux Developer Preview release to its later official version is not supported. If you're running the Developer Preview version, you must reinstall the official Oracle Linux release upon its general availability.

System Requirements and Limitations

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

Available Architectures

The release is available for installation on the following platforms:

- Intel® 64-bit (x86_64) (x86-64-v3)
- AMD 64-bit (x86_64) (x86-64-v3)
- 64-bit Arm (aarch64) (Arm v8.0-A)

  The Arm platform runs only with Unbreakable Enterprise Kernel Release (UEK).

Shipped Kernels

For the x86_64 platform, Oracle Linux 10 ships with the following default kernel packages:

- **`kernel-uek-6.12.0-100.28.2`** (Unbreakable Enterprise Kernel 8 Update 1 (UEK 8U1))

  For new installations, the UEK kernel is automatically enabled and installed. It also becomes the default kernel on first boot.
- **`kernel-6.12.0-55.9.1.0.1`** (Red Hat Compatible Kernel (RHCK))

For the aarch64 platform, Oracle Linux ships with the UEK kernel only.

The Oracle Linux release is tested as a bundle, as shipped on the installation media image. When installed from the installation media image, the kernel's version included in the image is the minimum version that's supported. Downgrading kernel packages isn't 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 added 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 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 the application vendor.

The kernel ABI for a UEK release remains unchanged in all later 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's independent of the kernel version that underlies the OS. Existing applications in user space continue to run unmodified on UEK R8 with no required recertifications for Oracle Linux certified applications.

Obtaining Installation Images

The following installation images for the current Oracle Linux 10 release are available:

- Full ISO of Oracle Linux for typical on-premises installations
- Boot ISO of Oracle Linux for network installations
- Boot ISO of the official UEK release for installing on hardware which 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 Linux yum server at https://yum.oracle.com/oracle-linux-downloads.html

  For more information managing and updating software on Oracle Linux systems, see Oracle Linux: Managing Software on Oracle Linux.
- Oracle Software Delivery Cloud at https://edelivery.oracle.com

To prepare a downloaded image for installing Oracle Linux, see Oracle Linux 10: Installing Oracle Linux.

> **Note**
>
> Aside from installation ISO images, 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're 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.

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

Preparing Installation Media

Before you can use an ISO image to install Oracle Linux, you must first store it on bootable installation media, such as the following:

- USB Flash Drive
- DVD or CD

USB Flash Drive

You can install Oracle Linux by using a boot image on portable devices such as a USB flash drive or an SD card, if the system's firmware can boot from those devices.

To create a bootable drive, use the `dd` or `xorriso-dd-target` command. Or, use a separate third-party utility to write the ISO image to a drive. See, for example, Create USB Installation Media for Oracle Linux with Fedora Media Writer.

> **Caution**
>
> This procedure destroys any existing data on the drive. Ensure that you specify the correct device name for the USB drive on the system.

1. Insert a USB flash drive into an Oracle Linux system.
2. Use the `xorriso-dd-target` command to list available block devices and to identify likely candidate devices for use.

   ```
   xorriso-dd-target -with_sudo -list_all
   ```

   The command presents a password prompt as it uses sudo to access all devices on the system. Output similar to the following is displayed:

   ```
   sda : YES : usb+ has_vfat+ : SanDisk Cruzer Switch
   nvme0n1 : NO  : not_usb- has_vfat+ has_xfs- has_crypto_LUKS- has_swap- :
   PM9A1 NVMe Samsung 512GB
   ```

The command identifies removable block devices with disposable content. In the example output, the command identified a USB device at `/dev/sda`, that could be used to write an ISO image.

3. Ensure that any file systems on the device are unmounted.

   For example, to unmount the first partition on `/dev/sda`:

   ```
   sudo umount /dev/sda1
   ```

4. Write the contents of the ISO image file to the USB device.

   Do one of the following to write the ISO image file to the USB device:

   - Use the `dd` command directly:

     ```
     sudo dd if=./full_image.iso of=/dev/sda bs=512k
     ```

   - Use the `xorriso-dd-target` command to guide you through this process:

     ```
     xorriso-dd-target -with_sudo -plug_test -DO_WRITE -image_file ./
     full_image.iso
     ```

     The command guides you through testing for appropriate devices and finally prompts you to select and approve writing to the device. Example output follows:

     ```
     sudo /bin/lsblk seems ok.

     Caused by option -plug_test: Attempt to find the desired device
     by watching it appear after being plugged in.

     Step 1:
     Please make sure that the desired target device is plugged _out_ now.
     If it is currently plugged in, make sure to unmount all its fileystems
     and then unplug it.
     Press the Enter key when ready.

     Found and noted as _not_ desired:  nvme0n1

     Step 2:
     Please plug in the desired target device and then press the Enter key.

     Waiting up to 10 seconds for a new device to be listed .... found: sda
     Now waiting 5 seconds to let it settle .........
     Found and noted as desired device:  sda

     sda : YES : usb+ has_vfat+ : SanDisk Cruzer Switch

     Step 3:
     Last chance to abort. Enter the word 'yes' to start REAL WRITING.
     yes
     Looking for mount points of sda:
     Performing:
       sudo /bin/dd if=/dev/zero of=/dev/'sda' bs=512 seek='30595071'
     count=1 status=none
     ```

```
  sudo /bin/dd if='OracleLinux.iso' of=/dev/'sda' bs=1M status=progress
oflag=dsync ; sync
```

The USB flash drive is now ready to be used to boot a system and start the installation.

DVD or CD

Because of storage limits, optical media such as CDs or DVDs might not have capacity to accommodate most installation ISO images. However they can be used to store the boot ISO image.

1. Insert an empty recordable CD or DVD into the CD or DVD writer device.
2. Open a terminal and use `cdrecord` to write the ISO file to the device.

   To write the downloaded ISO image file to a CD or DVD, use a command such as `cdrecord`, for example:

   ```
   sudo cdrecord -v -eject speed=16 dev=/dev/sr0 file_name.iso
   ```

   To display the device that corresponds to the CD or DVD writer, use the `cdrecord --devices` command.

The CD or DVD is now ready to be used to boot a system and start the installation.

Upgrading From Previous Oracle Linux Releases

You can upgrade an Oracle Linux 9 system to the Oracle Linux 10 release by using the `leapp` utility.

For step-by-step instructions and information about any known issues that might arise when upgrading the system, see Oracle Linux 10: Upgrading Systems With Leapp.

2

New Features and Changes

Unless indicated otherwise, the following new features, major enhancements, bug fixes, and other changes that are introduced in this release of Oracle Linux 10 apply to both the x86_64 and 64-bit Arm (aarch64) platforms.

Installation and Boot

The following features, enhancements, and changes related to installation and boot are introduced in this Oracle Linux 10 release.

Image Builder Disk Images Have Predictable Network Interface Names

The `net.ifnames=0` is removed from kernel arguments. All systems now use predictable network interface names. Disk images created with image builder also have predictable network interface names. For older versions, remove the kernel argument after the first boot and then reboot the system.

New Users Made Administrators by Default in the Installer

When you create a new user in the installer, they are given the `Add administrative privileges to this user account` privilege automatically. If you don't want the user to have these privileges, remove the option during setup.

NVMe Over Fabrics Devices Available in Installer

Add NVMe over Fabrics devices to Oracle Linux 10 installation. You can select these devices under the NVMe over Fabrics devices while adding disks on the Installation Destination screen.

Remote Desktop Protocol Replaces Virtual Network Computing

Remote desktop protocol (RDP) replaces virtual network computing (VNC) as the protocol for graphical remote access. It provides secure sessions with encrypted connections and enforced password length restrictions. `inst.vnc`, `inst.vncpassword`, and `inst.vncconnect` kernel boot options are replaced by `inst.rdp`, `inst.rdp.password`, and `inst.rdp.username`.

Enhanced Kickstart Provides Encrypted DNS Configuration

You can use the installer to add CA certificates in the Kickstart file using the `%certificate` section. This allows encrypted DNS to work immediately after installation by including certificates in Base64 format and importing them with the `--dir` and `--filename` options, helping meet Zero Trust requirements.

Disk Images Can Have Consistent Default Locale and Timezone

In earlier versions, Oracle Linux disk images had varying default locale and timezone settings. Now, all Oracle Linux disk images can use consistent defaults: the locale is set to C.UTF-8 and the timezone to UTC.

`grub2` Released at Version 2.12

The `grub2` package in Oracle Linux 10 is released at version 2.12.

The following notable features and changes are included:

- Dynamic GRUB runtime memory addition using firmware calls.
- GRUB 2 can be configured to output to a serial console, including those using PCI and MMIO UARTs.
- VLAN support.
- TPM driver fixes.
- File system fixes.
- CVE fixes.
- Debugging improvements.
- Tests improvements.
- Documentation improvements.

Operating System and Software Management

The following features, enhancements, and changes related to the OS and software management are introduced in this Oracle Linux 10 release.

`dnf-plugins-core` Released at Version 4.7.0

`dnf-plugins-core` is released at version 4.7.0 and includes the `python3-dnf-plugin-pre-transaction-actions` package that includes tooling to run a command when an RPM transaction is started. See the `dnf-pre-transaction-actions(8)` manual page for more information.

Filelists Metadata No Longer Downloaded

The filelists metadata provides details such as the names, paths, and permissions of all files installed by a package, and is used for more precise management of package contents, enabling features such as file-based dependencies and conflict detection between different versions of packages. However, because of its size and limited necessity in most DNF transactions, by default, filelists metadata is no longer downloaded when retrieving repository metadata.

Also, the filelists metadata isn't downloaded or updated from repositories when performing DNF transactions using `dnf` commands. However, filelists metadata can be automatically loaded if a `dnf` command specifically requires it or includes a file-related argument.

In cases where a package relies on a filepath dependency requiring filelists metadata, the transaction might fail with a dependency resolution error that includes a hint suggesting one of two possible solutions:

- Use `--skip-broken` to bypass uninstallable packages.
- Set `--setopt=optional_metadata_types=filelists` to load the optional filelists metadata.

To configure DNF to download filelist metadata by default, append the `filelists` value to the `optional_metadata_types` option within `/etc/dnf/dnf.conf`.

Consolidation of PGP Key Verification in DNF and RPM

RPM package signature verification is enhanced to use the `rpm-sequoia` library, instead of the custom PGP parser that was used before. Similarly, `librepo` which verifies PGP signatures on DNF repositories, is also updated to use the same `rpm-sequoia` library for a more consistent handling signature verification in both RPM and DNF tooling.

`createrepo_c` Package Added

The `createrepo_c` package is added as a C implementation of the `createrepo` tool used to generate and manage a common metadata repository for RPM packages compatible with tools such as yum and DNF. The C implementation includes the following features and enhancements:

- `zstd` is the default compression algorithm to provide smaller metadata and quicker decompression. `zstd` replaces `gz`, although `gz` compression is still available.
- Metadata in SQLite database format is no longer generated by default to improve performance and disk usage. Use the `--database` switch or the `sqliterepo_c` tool to create this metadata, if required.
- `group.xml` metadata is present only when compressed and has the group metadata type. The metadata is no longer presented when uncompressed.

Improved Package Upgrades With DNF and Related Tools

Use DNF with the `exclude_from_weak_autodetect` option to automatically detect unmet weak dependencies of installed packages and prevent the installation of packages that would satisfy those unmet dependencies. Previously, this option was disabled by default, resulting in the installation of all weak dependencies associated with a package during an upgrade, regardless of whether they were installed before. With this update, the `exclude_from_weak_autodetect` option is now enabled by default, ensuring that only newly recommended packages are installed when using DNF, PackageKit, or microdnf to perform an upgrade.

RPM Database Moved for Simplified System Snapshots

With this update, the RPM database is moved from the `/var/lib/rpm` directory to the `/usr/lib/sysimage/rpm` directory. Storing the database in `/usr` simplifies the creation and rollback of system snapshots because the contents of `/var` no longer must be considered. It also aligns with `rpm-ostree` based systems, such as Oracle Linux CoreOS, which already store the RPM database under the `/usr` directory.

Enhanced Control Over Stale Processes With the `--exclude-services` Flag

You can use the `dnf needs-restarting --services` to list systemd services that need restarting. With this update, a new `--exclude-services` flag is added to `dnf needs-restarting` to exclude systemd services from the list of stale processes.

Shells and Command Line Tools

The following features, enhancements, and changes related to shells and command line tools are introduced in this Oracle Linux 10 release.

`ksh` Released at Version 1.0.10 (93u+m)

The KornShell (ksh) version 1.0.10 (93u+m) includes the following changes:

- The alarm command is deprecated. Use the cron daemon instead for tasks that require running at fixed intervals.
- Subject to system limitations, ksh shell can now process 32767 simultaneous background jobs.
- A bug causing an incorrect default exit status for exit within a trap action is fixed.
- A bug causing a race condition occurring on some systems when running an external command with a redirection from a command substitution is fixed.
- Other bug fixes

Coreutils Updated for Better POSIX compliance

Some of the tooling included with `coreutils` is updated to be more POSIX compliant. Notably, the `uname` command might return 'unknown' when using the `-i` or `-p` options. These options have been marked as 'non-portable' for many years, because Linux doesn't store values for these operating system features. In previous releases, `uname` was patched to return the machine information returned for the POSIX compliant `-m` option when these options were used. In future, you should use uname `-m` where you might previously have used uname `-i` or uname `-p`.

Systemd Released at Version 257

The `systemd` package is released at version 257.

This version includes the following changes:

- The use of cgroup v1 (including legacy and hybrid hierarchies) is now obsolete. `systemd` now only uses cgroup v2, regardless of the kernel command line setting `systemd.legacy_systemd_cgroup_controller=yes`.
- System V service scripts is deprecated.

> **Note**
>
> To ensure compatibility with upcoming systemd versions, update the software to use native `systemd` unit files instead of legacy System V scripts.

ReaR Released at Version 2.9

The `ReaR` utility is released at version 2.9

Automatic `tmux` Session Startup at Boot Time for Specific Users

You can now use automatic tmux session startup for specific users during system boot. This enhancement is beneficial for systems that have the `KillUserProcesses=yes` parameter enabled, which terminates user processes when they log out. In such cases, if users aren't configured to linger (for example, their processes aren't allowed to continue running after logout), a `tmux` session can be automatically started at boot time to preserve their work. This feature ensures that users can resume their work from where they left off, even after a system restart.

Changes to `polkit-rules` Directory Visibility and Permissions

In the previous version, `polkit-123`, files in the `/usr/share/polkit-1/rules.d` directory had a default file mode, rather than inheriting it from the parent directory. Also, files in the `/etc/polkit-1/rules.d` directory were owned by `polkitd`.

This enhancement introduces the following changes:

- `/usr/share/polkit-1/rules.d`
  The default permission mask for files in this directory is changed from `700` (`polkitd:root`) to `755` (`root:root`), making them visible to all users.

  This change is justified because the files in this directory are endorsed by various packages and are accessible in the project's public repositories. The new file permission mask is also aligned with the Filesystem Hierarchy Standard (FHS).
- `/etc/polkit-1/rules.d`
  Files in this directory represent custom rules created by the system administrator. The default permission mask for files in this directory is changed to `0750` (`root:polkitd`) for increased security.

  The polkit daemon is in the `polkitd` group, which has read access to the files. This prevents unauthorized access to the polkit daemon from changing the rules or granting more privileges. The files are only visible to the root user or members of the `polkitd` group.

> **Note**
>
> Don't store custom `.rules` files in `/usr/share/polkit-1/rules.d`. Store or migrate custom rules to the `/etc/polkit-1/rules.d` directory for security reasons.

Compilers and Development Tools

The following features, enhancements, and changes related to compilers and development tools are introduced in this Oracle Linux 10 release.

GCC Released at Version 14.2

GNU Compiler Collection (GCC) is released at version 14.2.

For more information, see upstream GCC release notes.

GCC Released at 14 x86-64-v3 Default

GCC 14 defaults to the x86-64-v3 microarchitecture level for both AMD and Intel. This level enables certain capabilities by default, such as the AVX and AVX2 instruction sets and the fused multiply-add (FMA) instruction set.

`annobin` Released at Version 12.55

`annobin` is released at version 12.55.

`binutils` Released at Version 2.41

`binutils` is released at version 2.41.

Gnu `ld` linker `--section-ordering-file` option

Use `ld.bfd` with the `--section-ordering-file` option to group sections of code or data that can benefit from being in proximity to each other and to reduce cache misses.

Analyze use of code over time with profiling tools then improve code grouping in the executable image. This provides more control over the layout of programs in memory.

This option also enhances compatibility with the `gold` and `lld` linkers, which already provide this feature.

`glibc` Released at Version 2.39

GNU C Library, `glibc`, is released at version 2.39.

`glibc` AMD Zen 3 and 4 Optimizations

Optimized versions of `memcpy` and `memmove` used by AMD Zen 3 and Zen 4 processors when using `glibc`.

Previously, AMD Zen 3 and Zen 4 processors occasionally used the Enhanced Repeat Move String (ERMS) version of the `memcpy` and `memmove` library routines, regardless of the most best choice.

`glibc` Intel APX-enabled Dynamic Linking of Functions

The `glibc` dynamic linker preserves Advanced Performance Extensions (APX) related registers.

This resolves a previous issue where a dynamic linker trampoline might have been a source of incompatibilities for Intel APX applications. The previous workaround of using the `BIND_NOW` executable or use only the standard calling convention, is no longer necessary.

> **Note**
>
> More space is required beyond the top of the stack with this change. Consider adjusting or evaluating the stack limits if you have strict space limits.

GDB Released at Version 14.2

GNU Debugger (GDB) is released at version 14.2. See https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;a=blob_plain;f=gdb/NEWS;hb=gdb-14.2-release for more information.

For changes since the Oracle Linux 9 system version of GDB 10.2, see the release notes for the GDB 11.2 shipped in GCC Toolset 12 and the GDB 12.1 shipped in GCC Toolset 13.

`elfutils` Released at Version 0.192

`elfutils` is released at version 0.192.

SystemTap Released at Version 5.2

SystemTap tracing and probing tool is released at version 5.2.

See https://inbox.sourceware.org/systemtap/Zy640M7FbVZf-lwz@elastic.org/ for more information.

Valgrind Released at Version 3.24.0

The Valgrind suite is released at version 3.24.0.

Dyninst Version 12.3.0 Available

The Dyninst library in included at version 12.3.0. See https://github.com/dyninst/dyninst/releases/tag/v12.3.0 for more information.

`libabigail` Released at Version 2.6

The `libabigail` library is released at version 2.6.

LLVM Toolset Released at Version 19.1.7

The LLVM Toolset is released at version 19.1.7.

See https://discourse.llvm.org/t/llvm-19-1-7-released/84062 for more information.

LLVM Toolset is a rolling Application Stream and only the latest version is supported.

`llvm-doc` Package Update

The `llvm-doc` package now contains a reference to the upstream documentation.

Rust Toolset Released at Version 1.84

The Rust Toolset is now at version 1.84.

See https://blog.rust-lang.org/2025/01/30/Rust-1.84.1/ for more information.

Go Toolset Released at Version 1.23

The Go Toolset is released at version 1.23.

See https://tip.golang.org/doc/go1.23 for more information.

The Go Toolset is a rolling Application Stream and only the latest version is supported.

PCP Released at Version 6.3.2

PCP is released at version 6.3.2.

See https://github.com/performancecopilot/pcp/blob/main/CHANGELOG for more information.

Grafana-PCP Plugin Update

The `grafana-pcp` plugin is released at version 5.2.2.

Valkey Replaces Redis

The Valkey key-value store replaces Redis. Valkey is a high-performance, open-source, in-memory data structure store that's compatible with Redis. Valkey provides the same functionality as Redis, including support for strings, hashes, lists, sets, and more. It also includes additional features and improvements, such as improved performance and scalability.

The replacement of Redis with Valkey is transparent to most applications, and existing Redis configurations and data can be used with Valkey without modification.

Valkey is used by various Oracle Linux components, including Grafana, PCP, and the `grafana-pcp` plugin.

`zlib-ng-compat` Replaces `zlib`

The new `zlib-ng-compat` package provides a general-purpose lossless data compression library used by many different programs. This implementation provides various benefits over `zlib` distributed in Oracle Linux 9. For example, `zlib-ng-compat` can use hardware acceleration when available and enhances compression efficiency and performance. `zlib-ng-compat` is built in API and ABI compatible mode to ensure a smooth transition from `zlib`.

SWIG Released at Version 4.2.1

Simplified Wrapper and Interface Generator (SWIG) version 4.2.1 is now available in the CodeReady Linux Builder (CRB) repository.

OpenJDK Released at Version 21

OpenJDK version 21 is the default Java implementation for Oracle Linux 10. Use the `java-21-openjdk` packages, which provide the OpenJDK 21 Java Runtime Environment and the OpenJDK 21 Java Software Development Kit.

`debugedit` Version 5.1

Oracle Linux 10 includes `debugedit` version 5.1. For more information see https://sourceware.org/debugedit/.

`cmake` 3.30.5

Oracle Linux 10 includes `cmake` version 3.30.5.

See https://cmake.org/cmake/help/latest/release/3.30.html for more information.

.NET 9.0 and 8.0

Oracle Linux 10 includes .NET versions 9.0 and 8.0.

.NET is a general-purpose development platform that features automatic memory management and modern programming languages.

The .NET 9.0 release includes several new features and improvements, including:

- Improved performance and scalability
- New APIs and libraries for various tasks, such as networking and data access
- Improved support for various platforms and architectures

.NET 8.0 is a Long-Term Support (LTS) release, providing a stable and supported platform for applications.

To install .NET on Oracle Linux 10, you can use the `dnf` package manager.

For example, to install .NET 9.0, you can run the following command:

```
sudo dnf install dotnet9
```

For more information on .NET, see the upstream documentation.

Dynamic Programming Languages, Web and Database Servers

The following features, enhancements, and changes related to programming languages, web servers, and database servers are introduced in this Oracle Linux 10 release.

Python Released at Version 3.12

Oracle Linux 10 includes Python 3.12 as the default Python implementation. Python is distributed as a non-modular `python3` package in the BaseOS repository and is typically installed by default. Python 3.12 includes full life cycle support on Oracle Linux 10. Other versions of Python 3 with a shorter life cycle, available through the AppStream repository, are installable in parallel. `/usr/bin/python` and other Python-related commands, such as `pip`, are available in the unversioned form and point to the default Python 3.12 version. Notable enhancements compared to Python 3.11 include:

- A new type statement and type parameter syntax for generic classes and functions.
- Formatted string literal (f-strings) formalized in the grammar and can now be integrated into the parser directly.

- A unique per-interpreter global interpreter lock (GIL).
- You can now use the buffer protocol from Python code.
- To improve security, the built-in hashlib implementations of the SHA1, SHA3, SHA2-384, SHA2-512, and MD5 cryptographic algorithms are replaced with formally verified code from the HACL* project. The builtin implementations remain available as fallback if OpenSSL doesn't provide them.
- Dictionary, list, and set comprehensions in CPython are now inlined to increase the speed of a comprehension execution.
- CPython now works with the Linux perf profiler.
- CPython now provides stack overflow protection on supported platforms.
- Python 3.12 is compiled with GCC's -O3 optimization flag, which is used by default in upstream, for improved performance.

To install packages from the Python 3.12 stack, you can use the following commands:

```
# dnf install python3
# dnf install python3-pip
```

To run the interpreter, you can use the following commands:

```
$ python
$ python3
$ python3 -m pip --help
```

Perl Released at Version 5.40

Perl version 5.40, includes the following changes from the 5.32 version:

- Core enhancements:
  - Unicode 15.0 available.
  - -g command-line option, an alias for the umask option -0777.
  - The -M command-line option accepts a space.
  - builtin module now includes documentation for new always-present functions.
  - try/catch feature for exception handling.
  - Deprecation warnings now have specific subcategories to provide finer-grained control. Note that you can still disable all deprecation warnings in a single statement.
  - The @INC hooks are enhanced with the new $INC variable and INCDIR method.
  - Forbidden control flow out of the defer and finally modules is now detected at compile-time.
  - Using `(?{ … })` and `(??{ … })` in a pattern now disables various optimizations globally in that pattern.
  - The limit for the `REG_INF` regex engine quantifier is increased from 65,536 to 2,147,483,647.
  - The new regexp variable ${^LAST_SUCCESSFUL_PATTERN} allows access to the last successful pattern that matched in the current scope.
  - A new __CLASS__ keyword

  - Perl now provides the ^^ logical XOR operator.
- Incompatible changes:
  - A physically empty sort function now triggers a compile-time error.
  - The readline() function no longer clears the stream error and EOF flags.
  - INIT blocks no longer run after an exit() function inside a BEGIN block.
  - Calling the import method on an unknown package now produces a warning.
  - The return function no longer allows an indirect object.
  - Changes in errors and warnings can now cause failures in tests.
- Deprecations:
  - The use of the ' character as a package name separator is deprecated.
  - The switch feature and the smartmatch operator ~~ are deprecated.
  - Using the goto function to jump from an outer scope into an inner scope is deprecated.
- Internal Changes:
  - Multiple deprecated C functions have been removed.
  - Internal C API functions are now hidden with the __attribute__((hidden)) attribute on the platforms that support it. This means they're no longer callable from XS modules on those platforms.
- Modules:
  - The Term::Table and Test2::Suite modules have been added to Perl Core.
  - Most modules are updated.

For more information, see the `perl5340delta`, `perl5360delta`, `perl5380delta`, and `perldelta` man pages.

Ruby Released at Version 3.3.7

Ruby version 3.3.7 includes performance enhancements, fixes, and several new features, including:

- The new `Prism` parser provides an alternative to `Ripper`. See https://github.com/ruby/prism for more information.
- YJIT, the Ruby just-in-time (JIT) compiler is stable and is updated for performance improvements. Use this compiler in production.
- The `Regexp` matching algorithm includes security enhancements.
- The M:N thread scheduler is available.
- Use the `Lrama` LALR parser generator instead of `Bison`.
- The `Racc` gem is now a bundled gem.

Node.js Released at Version 22

`Node.js` version 22 includes the following changes from version 20:

- V8 JavaScript engine version 12.4.
- V8 Maglev compiler enabled by default on architectures where available. For example, the AMD/Intel 64-bit architectures and the 64-bit ARM architecture.

- Maglev improves performance for short-lived CLI programs.
- npm package manager version 10.8.1.
- `node --watch` mode now considered stable. In watch mode, changes in watched files cause the `Node.js` process to restart.
- The browser-compatible implementation of WebSocket is now considered stable and enabled by default. A WebSocket client to `Node.js` is therefore available without external dependencies.
- `Node.js` includes an experimental feature for execution of scripts from package.json. To use this feature, run the `node --run` <script-in-package.json> command.

MySQL Released at Version 8.4

MySQL version 8.4 includes the following notable changes since 8.0:

- `mysql_native_password` authentication plugin is deprecated and no longer enabled by default.
- User accounts or roles with the `BINLOG_ADMIN` privilege automatically receive the `TRANSACTION_GTID_TAG` privilege after upgrading to MySQL 8.4.
- The `mysql_upgrade_history` file is created or updated in the server's data directory when installing MySQL 8.4. The file is in JSON format and includes information about the version installed, date, and time of installation, and whether the release was part of a Long-Term Support (LTS series) or an Innovation series.
- The use of the `%` and _ characters as wildcards in database grants is deprecated. These characters are treated as literals. They're already treated as literals when the `partial_revokes` server system variable is set to ON.
- The treatment of the `%` character by the server as a synonym for `localhost` when checking privileges is deprecated.
- Use the `--tls-version` and `--admin-tls-version` server system variables. The deprecated `--ssl` and `--admin-ssl` server options and `have_ssl` and `have_openssl` server system variables are removed.
- Use the `authentication_policy` server system variable. The deprecated `default_authentication_plugin` system variable is removed.
- Use the `SET_ANY_DEFINER` privilege for definer object creation and the `ALLOW_NONEXISTENT_DEFINER` privileges for orphan object protection. The deprecated `SET_USER_ID` privilege is removed.
- The deprecated `mysql_upgrade` utility is removed.

For more information, see the MySQL documentation.

File Systems and Storage

The following features, enhancements, and changes related to file systems and storage are introduced in this Oracle Linux 10 release.

`cryptsetup` Released at Version 2.7

`cryptsetup` version 2.7 includes the following changes:

- `libcryptsetup` improved support for LUKS encrypted devices in the `kdump` enabled systems.
- Critical fixes for LUKS2 SED OPAL feature.
- known or already fixed issues with LUSK2 SED OPAL feature avoided.

Snapshot Manager

The Snapshot Manager, `snapm`, is a new software component designed to help manage system state snapshots when a system is using copy-on-write and thinly provisioned logical volume management (LVM2) volumes. You can use `snapm` to create snapshots of the system at a moment in time and to rollback to that system state based on the snapshot that you have taken.

See https://github.com/snapshotmanager/snapm for more information about this utility.

`device-mapper-multipath` Released at Version 0.9.9

The `device-mapper-multipath` package is released at version 0.9.9, providing various bug fixes and enhancements.

This update includes several notable changes and enhancements, including:

- The `multipathd.socket systemd` unit is no longer enabled by default. However, `multipathd` continues to run automatically on boot. If stopped, you must restart it manually or update the `multipathd.socket` systemd file to uncomment the line:

  ```
  # WantedBy=sockets.target
  ```

- `multipathd` runs as a real-time process with a moderate priority (10) by default. If unsuccessful, it continues to run as a normal process, but with an increased priority.
- The `systemctl reload multipathd.service` or `multipathd reconfigure` commands reload a device only if something has changed, instead of reloading every `multipath` device.
- A new `path_grouping_policy` called `group_by_tpg` is introduced to group paths by their alua target port group.
- Configuration settings `detect_pgpolicy` and `detect_pgpolicy_use_tpg` are introduced to control the path grouping policy.
  - `detect_pgpolicy` is a configuration setting that controls whether `multipath` automatically detects the path grouping policy for a device. If enabled, `multipath` sets the `path_grouping_policy` to `group_by_prio` or `group_by_tpg` based on the prioritizer used.
  - `detect_pgpolicy_use_tpg` is a configuration setting that controls whether `detect_pgpolicy` sets the `path_grouping_policy` to `group_by_tpg` when the prioritizer is `alua` or `sysfs`. If enabled, `detect_pgpolicy` sets the policy to `group_by_tpg`; otherwise, it sets the policy to `group_by_prio`.

`dm-vdo` Module for RHCK

The `dm-vdo` module is added to RHCK, replacing the `kmod-kvdo` module.

NVMe SED Available

The `nvme-cli` and `cryptsetup` commands can automate encryption management and drive unlocking for NVMe Self-Encrypting Drives (SED). NVMe SED is an Opal storage specification of hardware encryption technology that provides a secure way to protect data at rest by encrypting data stored on the drive.

To use NVMe SED options on an NVMe disk with `nvme-cli`, you can perform the following actions:

- Discover SED features on a SED Opal device. See the `nvme-sed-discover(1)` manual page.

  ```
  nvme sed discover /dev/nvme0n1
  ```

- Initialize a SED Opal device for locking. See the `nvme-sed-initialize(1)` manual page.

  ```
  nvme sed initialize /dev/nvme0n1
  ```

- Lock a SED Opal device. See the `nvme-sed-lock(1)` manual page.

  ```
  nvme sed lock /dev/nvme0n1
  ```

- Unlock a SED Opal device. See the `nvme-sed-unlock(1)` manual page.

  ```
  nvme sed unlock /dev/nvme0n1
  ```

- Change the locking password on a SED Opal device. See the `nvme-sed-password(1)` manual page.

  ```
  nvme sed password /dev/nvme0n1
  ```

- Revert a SED Opal device from it's locking state. See the `nvme-sed-revert(1)` manual page.

  ```
  nvme sed revert /dev/nvme0n1
  ```

These commands provide a flexible and secure way to manage NVMe SEDs, to automate encryption management and drive unlocking.

NFS with TLS Support

NFS with Transport Layer Security (TLS) is now fully supported on RHCK, enhancing NFS security by encrypting RPC traffic.

NFS with TLS is available in previous releases with UEK R7U3 and later. NFS with TLS continues to be support with UEK 8.

Atomic Write

Oracle Linux 10 introduces atomic write in RHCK, ensuring that write operations are atomic and preventing partial data writes or torn writes.

Atomic write is useful for applications that require high data consistency and reliability, such as databases. By ensuring that write operations are atomic, applications can optimize their performance and reduce the risk of data corruption or loss.

When atomic write is enabled, the file system, block layer, and drivers work together to ensure that write operations are run as a single, atomic unit.

To take advantage of atomic write, applications must use the `RWF_ATOMIC` flag when performing write operations by using various programming interfaces, such as the `write()` system call or higher-level libraries and frameworks.

High Availability and Clusters

The following features, enhancements, and changes related to high availability are introduced in this Oracle Linux 10 release.

Pacemaker Released at Version 2.1.8

Pacemaker is released at version 2.1.8.

`pcs status wait` Command Added

Pacemaker includes the `pcs status wait` command that ensures that Pacemaker completes any actions required by changes to the Cluster Information Base (CIB). It ensures that no further actions are required to make the actual cluster state match the requested cluster state.

`--output-format` Option Available for `pcs` Commands

The `--output-format` option is added to various pcs commands, to display output in different formats. The option accepts the following values:

- `text`: displays output in plain text,
- `cmd`: displays output as `pcs` commands to re-create the configuration,
- `json`: displays output in JSON format for machine parsing.

The `--output-format` option can be used with the `pcs tag` command to display configured tags. For example:

```
pcs tag --output-format cmd
```

HA Cluster Management Web UI

The standalone `pcsd` Web UI is replaced with a Cockpit web console add-on called the HA Cluster Management application. The HA Cluster Management application can be used to create and manage high-availability clusters using Pacemaker and Corosync from within the Cockpit web console. Features include graphical tools to perform tasks such as configuring cluster nodes, managing resources, and setting up fencing devices.

Documentation for the HA Cluster Management application is covered in Oracle Linux 10: Setting Up High Availability Clustering.

`pcs` Validation on Resource Creation and Update

By default, `pcs` instructs the resource agent to validate the parameters you enter when you create or update a cluster resource. For backward compatibility, if you enter an invalid parameter, a warning appears that doesn't prevent entering the invalid parameter. To prevent invalid parameter entry, specify the `--agent-validation` parameter.

`pcs` Confirmation Option For Destructive Actions

The `pcs` command includes a `--yes` option that confirms destructive actions, such as destroying a cluster or unblocking quorum. This update separates this functionality from the `--force` option, which is used to override validation errors.

`pcs` Command to Query the Status of Resources

You can use the `pcs status query resource` command to query various attributes of a single resource in a cluster, such as its existence, type, and state. The command returns plain text outputs for each of the resource attributes that you query.

Pacemaker Configuration Option to Leave a Panicked Node Shut Down

Set the `PCMK_panic_action` variable in the `/etc/sysconfig/pacemaker` configuration file to `off` or `sync-off` so that a node remains shut down after a panic condition instead of rebooting automatically.

Deleting Several Resources With a Single `pcs` Command

You can now specify several resources at the same time when using the `pcs resource delete`, `pcs resource remove`, `pcs stonith delete`, and `pcs stonith remove` commands, so that you don't have to run the command repeatedly for each resource that you want to remove.

For example, you can run:

```
pcs resource delete service2 service3
```

Creating Globally Unique Cluster Resource Clones

To configure a cluster resource clone to be globally unique, you can configure the clone option `clone-node-max > 1` when creating the clone of an existing resource or resource group. You also don't need to use the `globally-unique="true"` option when cloning resources or resource groups.

Updated Date Specification and Duration Options in Pacemaker Rules

Pacemaker rules are updated with new date specification and duration options. The following options are removed:

- `monthdays`, `moon`, `weekdays`, `weekyears`, and `yearsdays` from the `duration` options.
- `moon` and `yearsdays` from the `date-spec` options.

The following new options are available:

- The `duration` options are `seconds`, `minutes`, `hours`, `days`, `weeks`, `months`, and `years`.
- The `date-spec` options are `seconds`, `minutes`, `hours`, `monthdays`, `weekdays`, `yeardays`, `months`, `weeks`, `years`, and `weekyears`.

You can configure rules that incorporate these new `duration` and `date-spec` options in the following `pcs resource defaults` and `pcs resource op defaults` commands and their aliases, `pcs stonith defaults` and `pcs stonith op defaults`. The options also apply to the `pcs constraint location` command.

Infrastructure Services

The following features, enhancements, and changes related to infrastructure services are introduced in this Oracle Linux 10 release.

`cups-browsed` Daemon Not Configured by Default

The `cups-browsed` daemon no longer specifies a default service browsers in the `/etc/cups/cups-browsed.conf` file (`BrowseRemoteProtocols` is set to `none`). To enable `cups-browsed`, you must add the `BrowsePoll` directive that specifies to the server that the `cups-browsed` daemon polls for printers.

To search on `mDNS`, or `CUPS broadcast`, or both, set `BrowseRemoteProtocols dnssd cups` in the `/etc/cups/cups-browsed.conf` file.

`tuned-ppd` Available

The `tuned-ppd` package can be installed as a replacement drop-in for the `power-profiles-daemon` to use TuneD as a backend.

Note that `tuned-ppd` works with bare-metal systems and isn't intended for use on KVM guests.

Root GECOS Field Is Super User

The GECOS (comment) for the root user in the `/etc/passwd` file is `Super User` instead of `root`.

`dnsconfd` Added

The `dnsconfd` package is a local DNS cache configuration daemon that you can install to set up DNS caching, split DNS, DNS over TLS, and other DNS features.

Kea DHCP Server

Kea is a Dynamic Host Configuration Protocol (DHCP) server from Internet Systems Consortium (ISC) that includes fully functional DHCPv4, DHCPv6, and Dynamic DNS servers. It replaces the ISC DHCP server. The Kea DHCP server includes the following features:

- An extensible server solution with module hooks.
- Configurable through a REST API.
- Allows separation of data (leases) and execution environment.

Networking

The following features, enhancements, and changes related to networking are introduced in this Oracle Linux 10 release.

Enable Duplicate Address Detection for IPv4 in NetworkManager

The Duplicate Address Detection (DAD) is enabled ensuring that each IP address within a network is unique when configuring a new IP address. The NetworkManager `ipv4.dad-timeout` parameter is set to `200ms` by default. This parameter controls the duration for which the DAD check runs.

`xdp-tools` Released at Version 1.5.1

The `xdp-tools` package is released at version 1.5.1, which includes various enhancements and bug fixes.

`nftables` Released at Versions 1.1.1

The nftables framework includes changes from upstream versions 1.1.0 and 1.1.1, bringing several bug fixes and enhancements. This update introduces several notable changes, including JSON format for many devices and improved performance when listing tables.

The update also adds virtual local area network (VLAN) ID match and set support, encompassing the 802.1ad (Q-in-Q) standard. It also provides zero burst in byte rate limiter and egress for list hooks. Furthermore, the update addresses listing inconsistencies in the nft list hooks command.

For a comprehensive understanding of the changes and enhancements, see the upstream release notes for versions 1.1.0 and 1.1.1, available at https://www.netfilter.org/projects/nftables/files/changes-nftables-1.1.0.txt and https://www.netfilter.org/projects/nftables/files/changes-nftables-1.1.1.txt.

`iptables` Released at Version 1.8.11

The iptables framework is upgraded to version 1.8.11 providing several bug fixes and enhancements.

`firewalld` Released at Version 2.3.0

The `firewalld` service is released at version 2.3.0, introducing several enhancements. A notable addition is the `StrictForwardPorts` configuration option, which allows `firewalld` to be more restrictive about Destination NAT traffic when enabled. With this option set to `yes`, only explicitly enabled forward ports are allowed, blocking container-published ports.

The update also expands support for various services, including the Advanced Linux Sound Architecture (ALSA) sequencer (aseqnet) for client/server, Music Player Daemon (MPD), Radsec, and SlimeVR. For a comprehensive overview of the release updates, see the upstream repository at https://github.com/firewalld/firewalld/releases/tag/v2.3.0.

The Kernel Provides the `netkit` Network Device Type

The kernel is enhanced with the `netkit` network device type for high-performance networking in containers using Berkeley Packet Filter (BPF). This improvement is expected to boost the efficiency, scalability, and responsiveness of containerized applications that use a Container Network Interface (CNI) compatible with the netkit network device type, making it beneficial for cloud environments and high-throughput systems.

`nmstate` Includes the `require-id-on-certificate` Setting for Libreswan Configuration

The `nmstate` API now includes the `require-id-on-certificate` setting for Libreswan VPN configurations. This feature enables users to configure Subject Alternative Name (SAN) validation for IPsec connections, enhancing the security of VPN connections.

Automatic Reset for Problematic SR-IOV Virtual Functions in `i40e` Driver for RHCK

The Intel Network Adapter Driver for PCIe 40 Gigabit Ethernet, `i40e`, provided with RHCK, is enhanced to automatically reset problematic Single Root I/O Virtualization (SR-IOV) virtual functions (VFs) when a malicious driver detection (MDD) event is detected. This feature disables Tx/Rx queues or drops the offending packet until a VF driver reset occurs, thereby helping to prevent network disruptions caused by malfunctioning or malicious VFs.

The automatic reset is controlled by setting the `mdd-auto-reset-vf` option for the ethernet device, for example:

```
sudo ethtool --set-priv-flags eth0 *mdd-auto-reset-vf* on
```

Security

The following features, enhancements, and changes related to security are introduced in this Oracle Linux 10 release.

`keylime-agent-rust` Released at Version 0.2.7

`keylime-agent-rust` version 0.2.7 is a RUST based implementation of the Keylime agent. The Rust programming language focuses on safety, concurrency, and performance. The Keylime agent provides system integrity monitoring within the Keylime framework. This release includes the following improvements:

- Initial Device Identity (IDevID) and Initial Attestation Key (IAK) are available for device identity. This includes the following options:
  - `enable_iak_idevid`: (default: false) Enables the use of IDevID and IAK certificates to identify the device.
  - `iak_idevid_template`: (default: detect) Specifies the template that sets the algorithms to be used for IDevID and IAK (defined in TPM 2.0 Keys for Identity and Attestation, section 7.3.4). The detect keyword sets the template according to the algorithms used in the configured certificates.
  - `iak_idevid_name_alg`: (default: sha256) Specifies the digest algorithm used in IDevID and IAK. Used only if the iak_idevid_template option is not set as detect.

  - `iak_idevid_asymmetric_alg`: (default: rsa) Specifies the signing algorithm used in IDevID and IAK. Used only if the iak_idevid_template option is not set as detect.
  - `iak_cert`: (default: default) Specifies the path to the file that contains the X509 IAK certificate. The default path is /var/lib/keylime/iak-cert.crt.
  - `idevid_cert`: (default: default) Specifies the path to the file that contains the X509 IDevID certificate. The default path is /var/lib/keylime/idevid-cert.crt.
- Configurable IMA and measured boot event log locations are supported by using the new ima_ml_path and measuredboot_ml_path configuration options.
- Local DNS name, local IP, and configured contact IP are included as part of the Subject Alternative Name of the generated self-signed X509 certificate.
- IPv6 addresses with or without brackets are supported in the registrar_ip configuration option.
- Hexadecimal encoded values are supported in the tpm_ownerpassword configuration option.
- TLS 1.3 is enabled in connections to the agent.
- API modularity and multiversion support
- Enhanced configuration such as hostnames in addition to IP addresses and modular configurations.

Libreswan Released at Version 5.2

IKEv2 Enhancements

- Added PPK in INTERMEDIATE exchange and initial RFC 5723 IKE_SESSION_RESUME support. Fixed crash in ipsec rereadsecrets.
- Fixed race conditions in rekey requests and improved logging for IKE_AUTH and invalid payloads.
- Supported addresspool=v4/mask,v6/mask and subnet=SELECTOR,... with single Child SA. Fixed NATed endpoint updates and IKE_AUTH revival.

IKEv1 Changes

- Removed SOFTREMOTE_CLIENT_WORKAROUND, fixed reconnect and padding issues, updated ikepad= options.
- Added ah=sha2{256,512} and DH29, DH31 to proposals. Fixed Quick mode and ISAKMP deletion issues.
- Disabled by default (ikev1-policy=drop, RFC9395), limited cryptosuite, removed Labeled IPsec.
- Set default ESP/AH proposals, rejected invalid ESP proposals.

IPsec Interface

- Added support for FreeBSD, NetBSD, OpenBSD, and ipsec-interface-managed=no for namespaces.
- Fixed Linux IPsec Interface address handling and supported FreeBSD/OpenBSD interfaces.
- Added XFRM interface IP management with ref-counting, fixed IPcomp.

Linux Kernel Support

- Supported packet offload counters (kernel 6.7+), added IPTFS (RFC 9347), and adjusted SA settings for kernel 6.10+.
- Handled NLMSG_DONE for kernels > 6.9.0, fixed TCP connection hangs.
- Added HW packet offload support.

Security Fixes

- Fixed CVE-2024-3652.
- Fixed CVE-2024-2357.
- Fixed CVE-2023-38710, CVE-2023-38711, CVE-2023-38712 for IKEv1/IKEv2, and IPcomp crash.

Configuration and Utilities

- Fixed ipsec add performance with protoports.
- Improved ipsec.conf comment handling, added --narrowing options.
- Updated ipsec.conf.5, added encap-dscp=, interface-ip=, ppk-ids=, and experimental debug=. Deprecated ipsec auto and moved scripts to contrib/.

Building and Testing

- Fixed builds for OpenBSD 7.6, GCC 15/C23, and Alpine. Updated testing for OpenBSD 7.6, NetBSD 10.1, FreeBSD 14.2, Alpine 3.21.
- Removed libxz dependency, added Alpine/Debian/NetBSD/FreeBSD to nightly builds, improved install options.

For the full changelog, see https://download.libreswan.org/CHANGES.

Libreswan Improved Adding Connection Speed

Libreswan is updated to resolve a significant performance issue when adding a large number of connections defined in the ipsec.conf configuration file. In an example configuration where 1000 connection entries were specified, it took 30 minutes to complete processing of the configuration, because the full configuration file was parsed for each connection added and the resource intensive `getservbyname()` function was called each time.

The latest libreswan update optimizes performance by bypassing the `getservbyname()` function for numbered connections and delegating the validation of existing connections to the pluto daemon. This enhancement reduces the loading times associated with large configuration files with many defined connections.

OpenSSH Released at Version 9.9

Oracle Linux 10 now includes OpenSSH version 9.9, upgrading from version 8.7 in Oracle Linux 9. This brings many security and usability improvements. Key changes include:

- **Key and Agent Security:** New restrictions on forwarding and using keys with `ssh-agent`, enhancing security.
- **Improved FIDO Support:** Better handling of hardware keys, fewer unnecessary PIN prompts, and safeguards to avoid overwriting credentials.
- **New Features:**
  - `EnableEscapeCommandline` lets users access escape commands during sessions.
  - `ChannelTimeout` allows automatic closing of inactive SSH channels.

  - `ssh-keygen` now creates Ed25519 keys by default (RSA in FIPS mode).
- **Keystroke Obfuscation:** The SSH client can obscure keystroke timing to prevent side-channel attacks.
- **Removed/Updated Components:** DSA key support, `pam-ssh-agent`, and some tools are removed or moved.
- **Security Enhancements:**
  - `sshd` now blocks and penalizes problematic client addresses.
  - Splitting `sshd` into listener and session binaries for better security.
  - Improved compatibility with PKCS #11 and overall hardening.
- **Post-Quantum Cryptography (Preview):** Initial support for new cryptographic algorithms that resist quantum attacks.

These changes make SSH connections in Oracle Linux 10 more secure, easier to manage, and ready for future security challenges. For full technical details, see the `openssh-9.9p1/ChangeLog` file.

`libkcapi` Released at Version 1.5.0

`libkcapi` version 1.5.0 provides various improvements including:

- The sha* applications in `libkcapi` are removed and replaced with a single application called `kcapi-hasher`. Symlinks to `kcapi-hasher` with equivalent names as the original sha* applications are added into the `libexec` directory and symlinks to `sha*hmac` applications are added into `bin` directory.
- The `sha3sum` command, which prints checksums of files that use `sha3`, is added.
- The `kcapi_md_sha3_*` wrapper APIs are added.

`p11-kit` Released at Version 0.25.5

The `p11-kit` packages are provided in version 0.25.5 in Oracle Linux 10. This version provides enhancements and fixes over the previous version, most importantly, the following:

- Recursive attributes can be used with the p11-kit RPC protocol.
- A function to check runtime version of the library is added.
- Version information is no longer accessible through macros.
- With the new `--id` option, you can assign an ID to key pairs generated with the `generate-keypair` command or imported with the import-object command.
- With the new `--provider` option, you can specify a PKCS #11 module when using p11-kit commands.
- Fixed a bug in p11-kit where the EdDSA mechanism wasn't recognized in `generate-keypair`.
- p11-kit falls back to the `C_GetFunctionList` function when the `C_GetInterface` function isn't supported.

`setools` Released at Version 4.5.0

`setools` version 4.5.0 provides the following improvements:

- Graphical results for information flow analysis and domain transition analysis are added to the `apol`, `sedta`, and `seinfoflow` tools.
- Tooltips and detail popups in `apol` are added to help cross-referencing query and analyzing results along with context-sensitive help.

NSS Released at Version 3.101

The NSS cryptographic toolkit packages are released at version 3.101 to provide many bug fixes and enhancements, including an important fix to prevent RSA certificates with keys shorter than 2048 bits from working, in accordance with the system-wide cryptographic policy.

- PBMAC1 is now available (RFC 9579) for stronger password-based protection in **PKCS #12** files, enhancing security for key and certificate management.
- `libpkix` is now the default certificate validator, ensuring strict RFC 5280 compliance for X.509 certificate validation.
- RSA certificates with keys shorter than 2048 bits stopped working, aligning with system-wide cryptographic policies for stronger security.

`gnutls` Released at Version 3.8.9

The `gnutls` packages in version 3.8.9 includes various non backward compatible security-related changes such as the enhanced handling of Online Certificate Status Protocol (OCSP) responses.

Additionally, the validation process for OCSP responses is strengthened to check all records in an OCSP response until it finds a match for the server certificate, rather than only the first one. In FIPS mode, the minimum RSA key size required for verification to be considered approved is raised to 2048 bits, enhancing the security posture.

Other notable changes include:

- Certificate compression in TLS is available (RFC 8879).
- Optimal Asymmetric Encryption Padding scheme (RSA-OAEP) is available (RFC 8017).
- API for incremental calculation of SHAKE hashes of arbitrary length across multiple calls is added.
- RSA encryption and decryption with PKCS #1 v1.5 padding is deprecated and disallowed by default.
- In FIPS mode, `gnutls` now defaults to exporting PKCS #12 files with Password-Based Message Authentication Code 1 (PBMAC1) as defined in RFC 9579. If you need interoperability with systems running in FIPS mode, use PBMAC1 explicitly.

`clevis` Released at Version 21

`clevis` version 21 includes the following changes:

- The new subpackage called `clevis-pin-pkcs11`, provides the necessary PIN functionality for PKCS #11 devices. This allows users to securely unlock LUKS-encrypted volumes using a smart card, thereby enhancing the security of their encrypted data.
- Two new checks into the `clevis-udisks2` subpackage improve the reliability and functionality of Clevis. These checks are designed to ensure smoother operation and better error handling when working with LUKS-encrypted volumes in conjunction with udisks2.

- A critical issue that was causing "Address in use" errors is fixed. This enhancement ensures that users can rely on Clevis for secure and automated decryption of their encrypted volumes without interruptions.
- Increased security by fixing potential problems reported by static analyzer tools in the clevis luks command, udisks2 integration, and the Shamir's Secret Sharing (SSS) thresholding scheme.
- Password generation now uses the jose utility instead of pwmake. This ensures enough entropy for passwords generated during the Clevis binding step.

`jose` Released at Version 14

`jose` version 14 is a C-language implementation of the Javascript Object Signing and Encryption (JOSE) standards. It includes tools for handling various cryptographic operations such as signing, encryption, and verification for JSON Web Tokens (JWT), JSON Web Signatures (JWS), and JSON Web Encryption (JWE). Changes include the following:

- Improved bound checks for the len function for the oct JSON Web Key (JWK) Type in OpenSSL, as a fix to an error reported by the Static Application Security Testing (SAST) process.
- The protected JWE headers no longer contain zip.
- Avoids potential DoS attacks using high decompression chunks.

`openCryptoki` Released at Version 3.24.0

`openCryptoki` version 3.24.0 is an implementation of the PKCS#11 API, enabling applications to use cryptographic tokens for secure operations such as encryption, decryption, and key management. This version includes the following changes:

- RSA-OAEP encryption and decryption works with SHA-224, SHA-384, and SHA-512 hash functions.
- PKCS #11 v3.0 SHA-3 mechanisms are available, ensuring compliance with the latest industry standards.
- SHA-2 mechanisms and SHA-based key derivation mechanisms are available.
- Tokens can be protected with a token-specific user group.

SELinux Userspace Component Updated in Version 3.8

SELinux userspace components in version 3.8 includes the following updates and changes:

- New `audit2allow -C` option for the CIL output mode.
- The `sepolgen` utility is adjusted to parse `refpolicy` modules.
- The `semanage` utility can change records on `add`.
- The `semanage` utility no longer sorts local `fcontext` definitions.
- The `checkpolicy` program includes the CIDR notation for `nodecon` statements.
- The SELinux `sandbox` utility includes the Wayland display protocol.
- Several performance enhancements, including updates to the `selabel_lookup` call.
- The binary `file_contexts.bin` file format is changed in SELinux 3.8 for optimization. The file is part of the SELinux policy and contains mappings between file paths and their

associated SELinux contexts. You can re-create the file in the correct format by rebuilding the policy.

`polkit` Released at Version 125

`polkit` version 125 is a tool for controlling system-wide privileges allowing unprivileged processes to communicate with privileged ones in a controlled manner, enhancing security by centralizing policy decisions. Changes in this version include:

- `tmpfiles.d` file used to store configuration in the `/etc/polkit-1` directory.
- Adopting more granular `syslog-style` log levels.
- Improved logging control with the `LogControl` protocol.
- Improved control over log verbosity in logs and in the journal. This enhancement addresses the requirement to log every loaded `.rules` file for debug purposes, preventing the journal from being flooded with unnecessary information.
- Log-level control in the `polkit.service` unit. The `polkit.service` unit file contains a new parameter specified in the call of polkitd daemon called `--log-level=`<level>. By default this parameter is set to `--log-level=err`, logging only error messages. If the parameter `--log-level` is omitted, only critical messages are logged.
- Better handling of accidental or intentional removal of the `/etc/polkit-1/` directory

  or subdirectories. `polkit` can automatically re-create the required `/etc/polkit-1/` subdirectories upon the next boot, and no longer requires a full reinstall to restore missing configuration directories.

SCAP Security Guide Released at Version 0.1.76

The SCAP Security Guide (SSG) packages are released at version 0.1.76.

OpenSCAP Released at Version 1.4.1

The OpenSCAP packages are released at version 1.4.1. Notable features and changes include:

- The `oscap info` subcommand no longer prints SCAP source data stream component references.
- Fixed error when applying tailoring on DISA SCAP content caused by incorrect `xlink` namespace processing.
- Introduces the ability to generate kickstart files for unattended operating system installation by running:

  ```
  oscap xccdf generate fix --fix-type kickstart
  ```

See the OpenSCAP release notes for more information.

`libssh` Released at Version 0.11.1

The `libssh` SSH library is released at version 0.11.1, with new functionalities such as improved asynchronous SFTP IO, PKCS #11 provider for OpenSSL 3.0, testing for GSSAPI authentication, and proxy jump capabilities.

OpenSC Released at Version 0.26.1

The `opensc` packages are released at version 0.26.1. This update includes several security-related enhancements and bug fixes, notably addressing time side-channel leakage related to RSA PKCS #1 v1.5 padding removal after decryption. It also introduces unified OpenSSL logging, improving the overall logging consistency.

The pkcs11-tool utility now includes various cryptographic mechanisms, including HKDF, RSA OEAP encryption, AES GCM, and AES GMAC. Furthermore, several CVEs related to uninitialized memory problems are addressed, such as CVE-2024-45615, CVE-2024-45616, CVE-2024-45617, CVE-2024-45618, CVE-2024-45619, and CVE-2024-45620.

Other notable fixes in this update include resolving issues with allocations of aligned memory that were causing malfunctions in the Chromium web browser, and improving the reading of certificates in the TeleSec Chipcard Operating System (TCOS) card driver.

Rsyslog Released at Version 8.2412.0

The `rsyslog` packages is released at version 8.2412.0.

In this version, you can bind a ruleset to the `imjournal` module, allowing for early filtering and processing of log messages at the input stage. This optimization reduces the load on the main message queue, resulting in more efficient handling of large log volumes and minimizing resource usage.

`setroubleshoot` Released at Version 3.3.35

The setroubleshoot packages are released at version 3.3.35.

AppStream metadata is corrected to address previously broken data. The paths of used icons are updated to reflect recent changes to file paths.

Keylime Released at Version 7.12

The `Keylime` packages is released at version 7.12.

The new `keylime-policy` tool merges the management of Keylime runtime policies and measured boot policies, and also improves policy generation performance. The verifier and tenant components of Keylime no longer require payloads for the agent component, simplifying their operation.

`nettle` Library Released at Version 3.10.1

The `nettle` library package is released at version 3.10.1.

This update includes several key enhancements and changes:

- Performance improvements for certain cryptographic operations.
- The addition of DRBG-CTR-AES256, a new deterministic random-bit generator.
- The introduction of RSA-OAEP, an RSA encryption/decryption method that uses a new OAEP padding scheme.
- The inclusion of SHAKE-128, an arbitrary-length hash function from the SHA-3 family.
- A streaming API for SHAKE-128 and SHAKE-256.

- The removal of the MD5 assembly, which might result in a slight performance impact.

For more information, see the upstream information on https://git.lysator.liu.se/nettle/nettle/-/blob/master/NEWS?ref_type=heads.

OpenSSL `pkcs11-provider` Hardware Tokens

`pkcs11-provider` is an OpenSSL provider used with hardware tokens in applications such as `httpd`, `libssh`, `bind`, and other applications. It also includes asymmetric private keys stored in an HSM, smartcard, or other tokens with a PKCS #11 driver available. This provider replaces `openssl-pkcs11` engine

`pkcs11-provider` New Custom Configurations

The `pkcs11-provider` allows direct access to hardware tokens by using pkcs11 URIs from OpenSSL programs. Upon installation, the `pkcs11-provider` is automatically enabled and loads tokens detected by the `pcscd` daemon by using the `p11-kit` driver by default. Therefore, you can use tokens available to the system if you provide a key URI by using the pkcs11 URI specification to an application that supports that format by installing the package without the need to further change OpenSSL configuration. Uninstalling the package also removes the OpenSSL configuration snippet, which prevents errors when OpenSSL parses the configuration files.

`/var/run = /run` in SELinux Policy

The `/run = /var/run` file context equivalency is now `/var/run = /run` to match the actual file system state and to prevent some userspace tools from reporting an error. SELinux policy sources are updated with this change. If you have any custom modules that contain file specification for files in `/var/run`, change them to `/run`.

Stricter SSH Host Key Permissions

Host key permissions are now by default with the stricter `0600` permissions. `ssh-keysign` utility now uses SUID bit instead of the SGID bit. The `ssh_keys` group, that owned all SSH keys, is removed.

`pkeyutl` Encapsulation and Decapsulation

`pkeyutl` is a utility that includes operations such as signing, verifying, encrypting, decrypting, and deriving shared secrets using public key algorithms. This utility now includes encapsulation and decapsulation cryptographic operations. The new post-quantum cryptographic (PQC) algorithm ML-KEM (FIPS 203) permits only encapsulation and decapsulation operations, and you can now use algorithms such as RSASVE and ML-KEM through pkeyutl.

OpenSSL New `no-atexit` Option

The new `no-atexit` option in OpenSSL disables the automatic cleanup of OpenSSL resources using the `atexit()` handler when a program completes. Using this option might cause the valgrind debugging tool to report one-time memory leaks of the resources allocated on OpenSSL startup.

OpenSSL FIPS-Compliant PKCS #12 Files

OpenSSL can now create FIPS-compliant PKCS #12 files according to RFC 9579.

GnuTLS Certificate Compression

You can use GnuTLS to compresses client and server certificates based on the RFC 8879 standard with the zlib, brotli, or zstd compression algorithms. Both the client and server side must use the same library. Compression reduces the size of the certificate data transmitted.

DEFAULT Cryptographic Policy Includes New Scopes

`crypto-policies` includes the following new scopes in the DEFAULT system-wide cryptographic policy:

- `@pkcs12`
- `@pkcs12-legacy`
- `@smime`
- `@smime-legacy`

The selection of cryptographic algorithms used for PKCS #12 and S/MIME when network security services (NSS) is the underlying cryptographic library now follows system-wide cryptographic policies. Therefore, you can more easily select algorithms with higher granularity by using custom policies and subpolicies. The scopes use the following ciphers, hashes, and key exchanges:

```
cipher@pkcs12 = AES-256-CBC AES-128-CBC
cipher@pkcs12-import = 3DES-CBC+ RC2-CBC+
cipher@smime = AES-256-CBC AES-128-CBC 3DES-CBC
cipher@smime-import = RC2-CBC+
hash@{pkcs12,smime} = SHA2-256 SHA2-384 SHA2-512 SHA3-256 SHA3-384 SHA3-512 \
    SHA2-224 SHA3-224
hash@{pkcs12-import,smime} = SHA1+
key_exchange@smime = RSA DH ECDH
```

The LEGACY cryptographic policy uses a less strict selection of ciphers, hashes, and key exchanges than the DEFAULT policy, whereas the FUTURE policy is stricter. As a result, you can customize the algorithms used in NSS for importing and exporting PKCS #12 files and S/MIME encryption and decryption. NSS is currently the only cryptographic library linked to the newly offered scopes.

FIPS Mode OpenSSH Generates RSA Keys by Default

The `ssh-keygen` utility in OpenSSH by default generates ed25519 keys in non-FIPS mode and RSA keys in FIPS mode.

NSS FIPS-Compliant PKCS #12 Files

NSS can now create FIPS-compliant PKCS #12 files according to RFC 9579.

Password-based message authentication code 1 (PBMAC1) is now in PKCS #12 files to Network Security Services (NSS) as defined in RFC 9579. NSS can now read any .p12 file that

uses RFC 9579 and can generate RFC-9579-compliant message authentication codes (MAC) when requested by the user. For compatibility, NSS generates old MACs by default when not in FIPS mode. For more information on generating new MACs, see the pk12util(1) man page.

New SELinux Policy libvirt Services Rules

New SELinux types related to the libvirt services are added to the SELinux policy:

- `virt_dbus_t`
- `virt_hook_unconfined_t`
- `virt_qmf_t`
- `virtinterfaced_t`
- `virtnetworkd_t`
- `virtnodedevd_t`
- `virtnwfilterd_t`
- `virtproxyd_t`
- `virtqemud_t`
- `virtsecretd_t`
- `virtstoraged_t`
- `virtvboxd_t`
- `virtvzd_t`
- `virtxend_t`

SELinux Policy Confinement for More Services

The SELinux policy includes new rules to further confine certain `systemd` services. The services now confined include `iio-sensor-proxy`, `samba-bgqd`, `tlshd`, `gnome-remote-desktop`, and `pcm-sensor-server`.

With these changes, these services are no longer running with the `unconfined_service_t` SELinux label, which was in violation of the CIS Server Level 2 benchmark rule: *Ensure No Daemons are Unconfined by SELinux*. With the new confinement in place, these services can now run successfully in SELinux enforcing mode.

`dmesg` Hardening for Administrator Privileges

Administrator privileges are required to run the `dmesg` command. This update hardens the system against unrestricted access to sensitive information about the system. Use the `sudo` command to gain administrator privileges when running dmesg.

Flatpak Applications can now use Smart Card Functionality (opensc)

The `opensc` packages are now divided into the following subpackages: `opensc` and `opensc-libs` so that Flatpak applications can now use smart card functionality.

tpm2-openssl New Package

The new tpm2-openssl package includes a Trusted Platform Module (TPM) 2.0 provider for the OpenSSL TLS toolkit. You can now use cryptographic keys stored in a TPM 2.0 chip with the OpenSSL API, enhancing the integration of TPM 2.0 capabilities with OpenSSL-based applications.

Enhanced Audit Event Filtering and Forwarding

You can use the new audisp-filter plugin to suppress specific Audit events based on custom ausearch expressions, reducing unnecessary output to downstream plugins. By acting as an intermediary between Audit and other plugins, audisp-filter selectively filters out certain events and forwards only those that match the rules defined in its configuration file.

Use this capability for targeted filtering of Audit events with either allowlist or blocklist modes, where each plugin uses audisp-filter to specify its own configuration file containing matching rules. A common application of this feature is to exclude unnecessary or irrelevant Audit events, forwarding only significant ones to the syslog plugin for logging, thus making Audit logs more manageable.

Optimized SELinux Policy Packaging for EPEL

The SELinux policy modules that are only related to packages found in the Extra Packages for Enterprise Linux (EPEL) repository, and not associated with any Oracle Linux package, are moved from the selinux-policy package to a new package called selinux-policy-epel. This reorganization results in a more streamlined selinux-policy package, leading to improved performance in operations such as rebuilding and loading the SELinux policy.

Group Merging Added in authselect

To use the authselect utility for group merging, enable it in the authselect profiles. You no longer need to manually edit the nssswitch.conf file to enable group merging.

authselect Is a Required Component of PAM

The authselect-libs package is now mandatory and can't be removed, because it's a dependency of the pam package. authselect-libs now takes ownership of several key configuration files, including /etc/nsswitch.conf and various PAM configuration files in /etc/pam.d/, such as system-auth, password-auth, smartcard-auth, fingerprint-auth, and postlogin. These files were managed by other packages, including glibc and pam.

When upgrading from a previous Oracle Linux version:

- If an existing authselect configuration is detected, authselect apply-changes automatically updates it to the latest version.
- If no authselect configuration exists, no changes is made.
- On systems managed by authselect, non-authselect configurations is overwritten without prompting during the next authselect call.
- To maintain a custom configuration, create a custom authselect profile and manually update it to ensure it remains compatible with the system.

To stop using `authselect`, opt out by running the command:

```
# authselect opt-out
```

authselect Local Profile Replaces SSSD Files Provider

The `authselect` local profile replaces the SSSD files provider when handling local user management. The local profile replaces the previous minimal profile and becomes the default `authselect` profile for new installations instead of the SSSD profile.

The `authselect` utility automatically migrates existing configurations from minimal to local profile during an upgrade.

The `authselect` profile no longer includes `with-files-domain` and `with-files-access-provider` options. If you relied on these options, update the SSSD configuration to use `proxy provider` instead of `files provider`.

The sssd profile now includes the `--with-tlog` option, which enables session recording for users managed by SSSD.

New SSSD `exop_force` Option

With the `exop_force` option, you can force a password change in the following scenarios:

- When no grace logins remain on the LDAP server.
- The SSSD service attempts to change the password even if the LDAP server indicates that no remaining grace logins.

To use this feature, configure the following setting in the `sssd.conf` file:

- Set `ldap_pwmodify_mode = exop_force` in the `[domain/…]` section.

SSSD can Run With Reduced Privileges

To enhances system security, System Security Services Daemon (SSSD) can run with the `sssd` or `root` user through the systemd service configuration. The default is the `sssd` user. All root capabilities are dropped for the SSSD service except for a few privileged helper processes.

> **Note**
>
> Ensure that the `sssd.conf` configuration file is owned by the same user running the SSSD service, which is sssd by default. If the configuration file is created manually or with tools like Ansible, set the ownership to `sssd:sssd` with chown command if it was initially created by root.

KnownHostsCommand Added to SSSD

SSSD includes `KnownHostsCommand` in SSH configurations so that users can fetch host public keys from servers like FreeIPA or LDAP using the `sss_ssh_knownhosts` tool. This new tool replaces the older `sss_ssh_knownhostsproxy` tool. A message now indicates that `sss_ssh_knownhostsproxy` is obsolete.

Cockpit Web Console

The following features, enhancements, and changes related to the Cockpit web console are introduced in this Oracle Linux 10 release.

`cockpit-files` Package Added

The `cockpit-files` package is added to provide a File manager page in the Cockpit web console. With the File manager, you can browse files and directories, perform general file operations such as copying, moving, and renaming files, and you can upload files from the browser to the file system.

Containers

The following features, enhancements, and changes related to containers are introduced in this Oracle Linux 10 release.

Podman Released at Version 5.4

Podman is released at version 5.4. Podman component packages include:

- podman-5.4
- buildah-1.39
- crun-1.19
- skopeo-1.18

You can install any of these packages directly by using the `dnf install` command. For example, you can run:

```
sudo dnf install podman buildah crun skopeo
```

Buildah Artifact Manifests

`buildah manifest` subcommands support new options.

`buildah manifest add`

- `--artifact`
- `--artifact-type`
- `--artifact-config-type`
- `--artifact-layer-type`
- `--artifact-exclude-titles`
- `--subject`

`buildah manifest annotate`

- `--index`
- `--subject`

`buildah manifest create`

- `--annotation`

Disable Podman Healthcheck Events

You can disable the logging of Podman healthcheck events.

In the `containers.conf` configuration file, locate the new `healthcheck_events` option under the `[engine]` section, then set it to `healthcheck_events=false`.

Persistent Changes to Resources

When you run `podman update` to modify container configurations, those changes are now persistent. This capability applies to SQLite and BoltDB databases.

Default Settings for Podman Version 5.0

Podman version 5.0 now has the following default settings:

- `cgroups v2` is used instead of `cgroups v1`.
- The default network for rootless containers is now `pasta` instead of `slirp4netns`.

Handling Compatible Volumes

The `--compat-volumes` option is now available to provide compatibility with older container volumes. You can specify `--compat-volumes` with the following commands:

- `buildah build`
- `podman build`
- `podman farm build`

`podman pod inspect` Returns a JSON Array

Running `podman pod inspect` always returns a JSON array, even if the command inspects only a single pod.

Customizable Healthcheck Output in Podman

You can now customize the storage of healthcheck output for individual containers in Podman, enabling more detailed debugging information to be retained as needed, and controlling healthcheck output storage for specific containers to address concerns around data sensitivity and storage optimization. This enhancement is useful for troubleshooting sporadic healthcheck failures without impacting the live service. This is a significant improvement over the previous limitations, where healthcheck output was restricted to the five most recent runs, with a character limit of 500 per run, and could only be accessed through the `podman inspect` command.

Container Storage Configuration File Moved

The default containers storage configuration file is moved from `/etc/containers/storage.conf` to `/usr/share/containers/storage.conf`.

Support

The following features, enhancements, and changes related to support are introduced in this Oracle Linux 10 release.

`sos` is Updated

The `sos` package, that contains tools used to gather information from a system for debugging and diagnostic purposes, is updated.

Several new features are added:

- `sos report` is updated to provide a `--skip-cleaning-files` option to define a list of files that you don't want cleaned to obfuscate sensitive information. The option supports globs and wildcards.
- For better consistency across `sos` global options, the `--plugin-option` expects all plugin namespaces to use only hyphens instead of underscores.

3
Deprecated Features

This chapter lists features and functionalities that are deprecated in Oracle Linux 10. While these features might be included and operative in the release, support isn't guaranteed in future major releases. Thus, these features must not be used in new Oracle Linux 10 deployments.

Installation

The following installation related features and functionalities are deprecated in Oracle Linux 10.

Cockpit Composer

The `cockpit-composer` package is deprecated and will be removed in future major Oracle Linux releases. Use `cockpit-image-builder` instead.

SquashFS

The `squashfs` package is deprecated and will be removed in a future major Oracle Linux release. Consider using EROFS as an alternative solution.

Gdisk

`gdisk` is deprecated from the `boot.iso` image type. Other tools, such as `parted`, are available for handling GPT disks.

Module Kickstart Command

The module kickstart command is deprecated due to Anaconda's deprecated support for DNF modularity.

Inst.gpt Boot Option

The `inst.gpt` boot option is deprecated and will be removed in future releases. Use the `inst.disklabel` boot option instead.

Compilers and Development Tools

Utmp and Utmpx Interfaces

The `utmp` and `utmpx` interfaces provided by the `glibc` library are deprecated and will be removed in Oracle Linux 11.

Nodejs 18 Deprecation

The `nodejs-18` and `nodejs-18-minimal` container images are deprecated and will no longer receive feature updates. Use `nodejs-22` and `nodejs-22-minimal` instead.

Networking

The following network related features and functionalities are deprecated in Oracle Linux 10.

Ipset

Ipset is unmaintained and planned to be removed in a future major release. Use nftables sets functionality as an alternative.

Security

The following security related features and functionalities are deprecated in Oracle Linux 10.

ENGINE API in OpenSSL

The Engine API in OpenSSL is deprecated and will be removed in a future major release. No new applications should be built using the Engine API.

Crypto Policies

The `allow-rsa-pkcs1-encrypt` option is set to false for GnuTLS in all system-wide cryptographic policies (DEFAULT, FUTURE, and FIPS).

HMAC-SHA-1 in FIPS Mode

The HMAC-SHA-1 cryptographic algorithm is deprecated in FIPS mode and may be removed in a future release.

File Systems and Storage

The following features and functionalities related to file systems and storage are deprecated in Oracle Linux 10.

SquashFS

The `squashfs` package is deprecated and will be removed in a future major Oracle Linux release. Consider using EROFS as an alternative solution.

High Availability and Clusters

The following features and functionalities related to high availability and clusters are deprecated in Oracle Linux 10.

Deprecated High Availability Add-On Features

The following features have been deprecated in Oracle Linux 10 and will be removed in the next major release.

- Specifying rules as multiple arguments. Use a single string argument instead.
- Specifying score as a standalone value in `pcs constraint location add` and `pcs constraint colocation add`. Use `score=value` instead.

Other deprecations:

- The `--group`, `--after`, and `--before` options used with the `pcs resource create` command are deprecated in favor of `group`, `after`, and `before`. To start using the replacement flags, you can run the `pcs resource create` command with the `--future` option.

  See the `pcs(8)` manual page for more information.

Containers

The following features and functionalities related to container technologies are deprecated in Oracle Linux 10.

Runc Container Runtime

The `runc` container runtime is removed. The default container runtime is `crun`.

Tzdata Package

The `tzdata` package is no longer installed by default in the minimal container images.

Podman v5.0 Deprecations

The following features are deprecated in Podman v5.0:

- The system connections and farm information stored in the `containers.conf` file.
- The `slirp4netns` network mode.
- The `containernetworking-plugins` package.

Virtualization

The following virtualization related features and functionalities are deprecated in Oracle Linux 10.

Virt Manager

The Virtual Machine Manager application (`virt-manager`) is deprecated. The Cockpit web console is intended to become its replacement in a subsequent release.

Libvirtd

The monolithic `libvirt` daemon (`libvirtd`) is deprecated and will be removed in a future major release. Use the newly introduced modular `libvirt` daemons instead.

SecureBoot Image Verification

Performing SecureBoot image verification using SHA1-based signatures on UEFI (PE/COFF) executables is deprecated. Use signatures based on the SHA-2 algorithm or later instead.

Virtual Floppy Driver

The `isa-fdc` driver, which controls virtual floppy disk devices, is deprecated and will become unsupported in a future release.

Qcow2-v2 Image Format

The qcow2-v2 format for virtual disk images is deprecated and will become unsupported in a future major release. Use qcow2-v3 instead.

Deprecated Packages

The following packages are deprecated in Oracle Linux 10:

- `daxio`
- `gvvisor-tap-vsock-gvforwarder`
- `libpmem`
- `libpmem2`
- `libpmemblk`
- `libpmemlog`
- `libpmemobj`
- `libpmemobj-cpp`
- `libpmempool`
- `libslirp`
- `nvml`
- `pmempool`
- `pmreorder`
- `sdl2-compat`
- `wget`

4
Removed Features

This chapter lists features and functionalities that are removed in Oracle Linux 10 and which might have been available in previous Oracle Linux releases.

Installer and Image Creation

The following installation related features and functionalities are removed in Oracle Linux 10.

Authconfig Commands

The `auth` and `authconfig` Kickstart commands are removed. Use the `authselect` kickstart command instead.

Inst.xdriver and Inst.usefbx Options

The `inst.xdriver` and `inst.usefbx` boot options are removed.

Capturing Screenshots from the Anaconda GUI

Capturing screenshots from the Anaconda GUI with a global hot key is removed.

Removed Boot Options

The following boot options are removed: `inst.nompath`, `dmraid`, and `nodmraid`.

Automatic Bug Reporting System

The automatic bug reporting system from Anaconda is removed.

Timezone Kickstart Command Options

The following options of the `timezone` Kickstart command are removed: `--isUtc`, `--ntpservers`, and `--nontp`.

Logging Kickstart Command Parameter

The `--level` parameter of the logging kickstart command is removed.

Support for %anaconda Kickstart Command

The support for the `%anaconda` Kickstart command is removed.

Pwpolicy Kickstart Command

The `pwpolicy` Kickstart command is removed.

Support for Adding Additional Repositories from GUI

Support for adding additional repositories from the GUI is removed.

Support for LUKS Version Selection from Anaconda

Support for selecting the LUKS version from the Manual Installation screen is removed.

Initial-Setup Package

The `initial-setup` package is removed. Use `gnome-initial-setup` instead.

Anaconda Built-in Help

The built-in documentation from all Anaconda user interfaces is removed.

Teaming Options from the Network Kickstart Command

The `--teamslaves` and `--teamconfig` options used for configuring team devices in the `network` kickstart command are removed.

NVDIMM Reconfiguration Support during the Installation Process

Support for reconfiguring NVDIMM devices during the Kickstart and GUI installation is removed.

Options from %packages

The `--excludeWeakdeps` and `--instLangs` options used in the `%packages` section are removed.

Security

The following security related features and functionalities are deprecated in Oracle Linux 10.

Scap-Workbench

The `scap-workbench` package is removed.

Oscap-Anaconda-Addon

The `oscap-anaconda-addon` is removed.

DSA and SEED Algorithms

The DSA and SEED algorithms are removed from the Network Security Services (NSS) cryptographic library.

Fips-Mode-Setup

The `fips-mode-setup` command is removed.

/etc/system-fips

Support for indicating FIPS mode through the `/etc/system-fips` file is removed.

TLS HeartBeat

Support for the HeartBeat extension in TLS is removed.

SRP Authentication

Authentication that uses Secure Remote Password protocol (SRP) in TLS is removed.

Keylime HTTP

The Keylime components no longer support the HTTP protocol for revocation notification webhooks.

DEFAULT Cryptographic Policy

TLS ciphers that use the RSA key exchange are no longer accepted in the `DEFAULT` system-wide cryptographic policy.

Ca-Certificates Trust Store

The `/etc/pki/tls/certs` trust store is converted to a different format.

LEGACY Cryptographic Policy

The `LEGACY` system-wide cryptographic policy no longer allows creating or verifying signatures that use SHA-1 in TLS contexts.

Pam_Ssh_Agent_Auth

The `pam_ssh_agent_auth` package is removed.

OpenSSL SHA-1 in TLS

OpenSSL does not accept the SHA-1 algorithm at `SECLEVEL=2` in TLS.

Stunnel OpenSSL ENGINE API

The `stunnel` TLS offloading and load-balancing proxy no longer supports the previously deprecated OpenSSL ENGINE API.

OpenSSL Engines

OpenSSL Engines are removed from upstream.

Libsss_Simpleifp Subpackage

The `libsss_simpleifp` subpackage is removed.

SSSD Files Provider

The SSSD files provider is removed.

Ad-Allow-Remote-Domain-Local-Groups Option

The `ad_allow_remote_domain_local_groups` option is removed from SSSD.

Reconnection_Retries Option

The `reconnection_retries` option is removed from the `sssd.conf` file in SSSD.

Software Management

The following software management related features and functionalities are deprecated in Oracle Linux 10.

Libreport Library

Support for the `libreport` library is removed from DNF.

Dnf Debug Plug-in

The DNF `debug` plug-in is removed from the `dnf-plugins-core` package.

Numberless %patch Syntax

Using the `%patch` directive without a number specified as a shorthand for `%patch 0` is removed.

Infrastructure Services

The following infrastructure related features and functionalities are removed in Oracle Linux 10.

Removed Packages

The following packages are removed:

- `sendmail`
- `redis`
- `dhcp`

- `mod_security`
- `spamassassin`
- `xsane`

Rename of Gpsd

The `gpsd-minimal` package is renamed to `gpsd`.

ISC Kea DHCP Server Solution

The ISC Kea DHCP server solution is now available, replacing `ISC DHCP`.

Networking

The following networking related features and functionalities are removed in Oracle Linux 10.

ATM Encapsulation

Asynchronous Transfer Mode (ATM) encapsulation is removed.

Dhcp-Client Package

The `dhcp-client` package is removed.

Mlx4 Driver

The `mlx4` driver for the Mellanox ConnectX-3 network interface controller (NIC) is removed from RHCK.

Kernel

The following kernel related features and functionalities are removed in Oracle Linux 10.

Kexec_Load System Call

The `kexec_load` system call is removed.

Crash --log Dumpfile Option

The `crash --log dumpfile` option is deprecated.

File Systems and Storage

The following file systems and storage related features and functionalities are removed in Oracle Linux 10.

Support for NVMe Devices in lsscsi and sg3_utils

Support for Non-volatile Memory Express (NVMe) devices is removed from the `lsscsi` and `sg3_utils` packages.

VDO Sysfs Parameters

The Virtual Data Optimizer (VDO) `sysfs` parameters are removed.

Support for GFS2 File Systems

Support for GFS2 file systems is removed.

Support for Block Translation Table Driver

Support for the block translation table driver is removed.

Nvme_Core.Multipath Parameter

The `nvme_core.multipath` parameter is removed.

Md-Faulty and Md-Multipath Modules

The `md-faulty` and `md-multipath` MD RAID kernel modules are removed.

High Availability and Clusters

The following high availability and cluster related features and functionalities are removed in Oracle Linux 10.

pcsd Web UI

The `pcsd` Web UI is no longer available as a standalone user interface. Use the Cockpit web console instead.

Removed and Updated Pacemaker CIB Elements

The following configuration components of the Pacemaker CIB are removed or changed:

- The `validate-with` attribute of the `cib` element is set to `pacemaker-4.0`.
- The `stonith-action` cluster property is set to `off` if it was previously set to `poweroff`.
- Legacy promotable clone (master) resources are changed to standard promotable clones by changing the `master` xml element to the `clone` xml element and by setting the `promotable` meta attribute.
- Location constraints with more than one top-level rule are converted to separate location constraints for each top-level rule.

The following components are renamed:

- The `crmd-finalization-timeout` cluster property is renamed to `join-finalization-timeout`.
- The `crmd-integration-timeout` cluster property is renamed to `join-integration-timeout`.
- The `crmd-transition-delay` cluster property is renamed to `transition-delay`.

The following components are removed from the CIB:

- `nagios-class` and `upstart-class` resources.
- `bundle` resources based on an `rkt` container.
- The `restart-type` resource meta-attribute.
- The `can_fail` operation meta-attribute.
- The `role_after_failure` operation meta-attribute.
- `moon` attributes in `date_spec` elements of rules.
- The `remove-after-stop` cluster property.
- Ping nodes, which are changed to cluster member nodes with all resources banned and probes disabled.
- NVpairs without a value attribute.
- Duplicate NVpairs with a specific name within an NVset, for which only the first NVpair is kept.

Compilers and Development Tools

Linking against 32-bit Packages

Linking against 32-bit multilib packages is removed.

Perl(Mail::Sender) Module

The `perl(Mail::Sender)` module is removed.

Containers

The following container technology related features and functionalities are removed in Oracle Linux 10.

Runc Container Runtime

The `runc` container runtime is removed. The default container runtime is `crun`.

Cgroupv1

The `cgroupv1` control group mechanism is removed, use `cgroupv2` instead.

5
Known Issues

This chapter describes known issues that you may encounter when installing and using the Oracle Linux 10 software. Unless indicated otherwise, the issues apply to both x86_64 and aarch64 systems. Information that pertains only to a specific platform is also noted accordingly.

Installation Issues

The following are known installation issues for Oracle Linux 10.

RDP Install Error

When using RDP during an installation of Oracle Linux 10, the following error message might appear on the console or in the install logs:

```
*** BUG *** In pixman_region32_init_rect: Invalid rectangle passed
Set a breakpoint on '_pixman_log_error' to debug
```

The installation proceeds normally, and this error can be ignored.

(Bug 37644579)

Kernel Issues

The following kernel issues apply in Oracle Linux 10.

Console Font Loading Failure Messages During `systemd-vconsole-setup` With UEK 8

During system boot, when booting into UEK 8, the system might emit error messages while starting the `systemd-vconsole-setup` service:

```
systemd-vconsole-setup[1463]: setfont: ERROR kdfontop.c:183
put_font_kdfontop: Unable to load such font with such kernel version
systemd-vconsole-setup[1453]: /usr/bin/setfont failed with a "system error"
(EX_OSERR), ignoring.
systemd-vconsole-setup[1453]: Setting source virtual console failed, ignoring
remaining ones.
```

The issue results because the framebuffer console driver, `fbcon`, is set to use deferred takeover, which causes it to wait until a message is sent to the default boot console. The deferred takeover causes the `systemd-vconsole-setup` service to try to set the font on the default boot console which doesn't support this operation.

You can work around the issue by setting the `fbcon=nodefer` kernel command line option. For example, if UEK 8 is the default kernel, run:

```
sudo grubby --update-kernel=DEFAULT --args="fbcon=nodefer"
```

(Bug 37920190)

6

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 BaseOS by Oracle:

- `btrfs-progs`
- `dtrace`
- `iwl1000-firmware`
- `iwl100-firmware`
- `iwl105-firmware`
- `iwl135-firmware`
- `iwl2000-firmware`
- `iwl2030-firmware`
- `iwl3160-firmware`
- `iwl3945-firmware`
- `iwl4965-firmware`
- `iwl5000-firmware`
- `iwl5150-firmware`
- `iwl6000-firmware`
- `iwl6000g2a-firmware`
- `iwl6000g2b-firmware`
- `iwl6050-firmware`
- `iwl7260-firmware`
- `iwlax2xx-firmware`
- `kernel-uek`
- `kernel-uek-core`

- kernel-uek-debug
- kernel-uek-debug-core
- kernel-uek-debug-devel
- kernel-uek-debug-modules
- kernel-uek-debug-modules-core
- kernel-uek-debug-modules-extra
- kernel-uek-debug-modules-extra-netfilter
- kernel-uek-debug-modules-usb
- kernel-uek-debug-modules-wireless
- kernel-uek-devel
- kernel-uek-doc
- kernel-uek-modules
- kernel-uek-modules-core
- kernel-uek-modules-desktop
- kernel-uek-modules-extra
- kernel-uek-modules-extra-netfilter
- kernel-uek-modules-usb
- kernel-uek-modules-wireless
- libertas-sd8686-firmware
- libertas-sd8787-firmware
- libertas-usb8388-firmware
- libertas-usb8388-olpc-firmware
- linux-firmware-core
- liquidio-firmware
- ocfs2-tools
- oracle-backgrounds
- oracle-indexhtml
- oraclelinux-release
- oraclelinux-release-el10
- oracle-logos
- oracle-logos-httpd
- oracle-logos-ipa
- python3-dmidecode

Added Binary Packages for AppStream by Oracle

The following binary packages have been added to AppStream by Oracle:

- dnf-plugin-spacewalk

- dtrace-devel
- dtrace-testsuite
- libblockdev-btrfs
- NetworkManager-config-connectivity-oracle
- python3-dnf-plugin-spacewalk
- python3-dnf-plugin-ulninfo
- python3-hwdata
- python3-netifaces
- python3-pyOpenSSL
- python3-rhn-check
- python3-rhn-client-tools
- python3-rhnlib
- python3-rhn-setup
- python3-rhn-setup-gnome
- rhn-check
- rhn-client-tools
- rhnlib
- rhnsd
- rhn-setup
- rhn-setup-gnome

Added Binary Packages for CodeReady Linux Builder by Oracle

The following binary packages have been added to CodeReady Linux Builder by Oracle:

- oraclelinux-sb-certs

Modified BaseOS Binary Packages

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

- alternatives
- audispd-plugins
- audispd-plugins-zos
- audit
- audit-libs
- audit-rules
- autofs
- basesystem
- binutils
- binutils-gold

- biosdevname
- chkconfig
- chrony
- cockpit
- cockpit-bridge
- cockpit-doc
- cockpit-system
- cockpit-ws
- coreutils
- coreutils-common
- coreutils-single
- dnf
- dnf-automatic
- dnf-data
- dnf-plugins-core
- dracut
- dracut-config-generic
- dracut-config-rescue
- dracut-network
- dracut-squash
- dracut-tools
- efibootmgr
- efi-filesystem
- firewalld
- firewalld-filesystem
- glibc
- glibc-all-langpacks
- glibc-common
- glibc-gconv-extra
- 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-ckb
- 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-gbm
- 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-kv
- 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-mnw
- 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-rif
- 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-ssy
- glibc-langpack-st
- glibc-langpack-su
- glibc-langpack-sv
- glibc-langpack-sw
- glibc-langpack-syr
- 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-tok
- 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-zgh
- glibc-langpack-zh
- glibc-langpack-zu
- glibc-minimal-langpack
- grub2-common
- grub2-efi-aa64-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
- initscripts
- initscripts-rename-device
- initscripts-service
- ipset
- ipset-libs
- iptables-libs
- iscsi-initiator-utils
- iscsi-initiator-utils-iscsiuio
- iwl1000-firmware
- iwl100-firmware
- iwl105-firmware

- iwl135-firmware
- iwl2000-firmware
- iwl2030-firmware
- iwl3160-firmware
- iwl3945-firmware
- iwl4965-firmware
- iwl5000-firmware
- iwl5150-firmware
- iwl6000-firmware
- iwl6000g2a-firmware
- iwl6000g2b-firmware
- iwl6050-firmware
- iwl7260-firmware
- iwlax2xx-firmware
- kdump-utils
- kernel
- kernel-abi-stablelists
- kernel-core
- kernel-debug
- kernel-debug-core
- kernel-debug-modules
- kernel-debug-modules-core
- kernel-debug-modules-extra
- kernel-debug-uki-virt
- kernel-modules
- kernel-modules-core
- kernel-modules-extra
- kernel-tools
- kernel-tools-libs
- kernel-uki-virt
- kernel-uki-virt-addons
- kexec-tools
- kmod
- kmod-libs
- krb5-libs
- krb5-pkinit
- krb5-server

- krb5-server-ldap
- krb5-workstation
- libdnf
- libertas-sd8686-firmware
- libertas-sd8787-firmware
- libertas-usb8388-firmware
- libertas-usb8388-olpc-firmware
- libipa_hbac
- libkadm5
- libkcapi
- libkcapi-hasher
- libkcapi-hmaccalc
- libnfsidmap
- libnsl
- libsss_autofs
- libsss_certmap
- libsss_idmap
- libsss_nss_idmap
- libsss_sudo
- linux-firmware
- linux-firmware-core
- linux-firmware-whence
- liquidio-firmware
- makedumpfile
- mcelog
- mdadm
- microcode_ctl
- netconsole-service
- netronome-firmware
- NetworkManager
- NetworkManager-adsl
- NetworkManager-bluetooth
- NetworkManager-config-server
- NetworkManager-libnm
- NetworkManager-tui
- NetworkManager-wifi
- NetworkManager-wwan

- nfs-utils
- nvme-cli
- nvmetcli
- openssh
- openssh-clients
- openssh-keycat
- openssh-server
- openssl
- openssl-fips-provider
- openssl-fips-provider-so
- openssl-libs
- os-prober
- pcre2
- pcre2-syntax
- polkit
- polkit-libs
- python3-configshell
- python3-dnf
- python3-dnf-plugin-post-transaction-actions
- python3-dnf-plugin-pre-transaction-actions
- python3-dnf-plugins-core
- python3-dnf-plugin-versionlock
- python3-firewall
- python3-hawkey
- python3-libdnf
- python3-libipa_hbac
- python3-libsss_nss_idmap
- python3-sss
- python3-sssdconfig
- python3-sss-murmur
- readonly-root
- redhat-release
- selinux-policy
- selinux-policy-doc
- selinux-policy-mls
- selinux-policy-sandbox
- selinux-policy-targeted

- shim-x64
- sos
- sssd
- sssd-ad
- sssd-client
- sssd-common
- sssd-common-pac
- sssd-dbus
- sssd-ipa
- sssd-kcm
- sssd-krb5
- sssd-krb5-common
- sssd-ldap
- sssd-nfs-idmap
- sssd-passkey
- sssd-proxy
- sssd-tools
- sssd-winbind-idmap
- systemd
- systemd-container
- systemd-libs
- systemd-oomd
- systemd-pam
- systemd-resolved
- systemd-rpm-macros
- systemd-udev
- tuned
- tuned-profiles-cpu-partitioning
- vim-data
- vim-filesystem
- vim-minimal
- yum
- yum-utils

Modified Binary Packages for CodeReady Linux Builder by Oracle

The following binary packages to CodeReady Linux Builder by Oracle have been modified:

- 389-ds-base-bdb

- 389-ds-base-devel
- anaconda-widgets-devel
- bind-devel
- bind-doc
- crash-devel
- dotnet-sdk-8.0-source-built-artifacts
- dotnet-sdk-9.0-source-built-artifacts
- edk2-aarch64
- edk2-tools
- edk2-tools-doc
- gdm-devel
- gdm-pam-extensions-devel
- glibc-benchtests
- glibc-nss-devel
- glibc-static
- hivex-devel
- ipset-devel
- java-21-openjdk-demo-fastdebug
- java-21-openjdk-demo-slowdebug
- java-21-openjdk-devel-fastdebug
- java-21-openjdk-devel-slowdebug
- java-21-openjdk-fastdebug
- java-21-openjdk-headless-fastdebug
- java-21-openjdk-headless-slowdebug
- java-21-openjdk-jmods-fastdebug
- java-21-openjdk-jmods-slowdebug
- java-21-openjdk-slowdebug
- java-21-openjdk-src-fastdebug
- java-21-openjdk-src-slowdebug
- java-21-openjdk-static-libs-fastdebug
- java-21-openjdk-static-libs-slowdebug
- kernel-cross-headers
- kernel-tools-libs-devel
- kmod-devel
- libdnf-devel
- libguestfs-devel
- libguestfs-man-pages-ja

- libguestfs-man-pages-uk
- libnfsidmap-devel
- libperf
- librados-devel
- libradospp-devel
- librbd-devel
- libsss_nss_idmap-devel
- libudisks2-devel
- libvirt-daemon-plugin-sanlock
- libvirt-devel
- libvirt-docs
- NetworkManager-libnm-devel
- nginx-mod-devel
- nss_db
- nss_hesiod
- ocaml-hivex
- ocaml-hivex-devel
- ocaml-libguestfs
- ocaml-libguestfs-devel
- OpenIPMI-devel
- PackageKit-glib-devel
- pcp-testsuite
- pcre2-static
- pcre2-tools
- podman-tests
- postgresql-test-rpm-macros
- python3-hivex
- python3-ipatests
- python3-mpich
- ruby-hivex
- sanlock-devel
- tog-pegasus-devel
- virt-v2v-man-pages-ja
- virt-v2v-man-pages-uk
- wireshark-devel

Modified AppStream Binary Packages

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

- 389-ds-base
- 389-ds-base-libs
- 389-ds-base-snmp
- anaconda
- anaconda-core
- anaconda-dracut
- anaconda-gui
- anaconda-install-env-deps
- anaconda-install-img-deps
- anaconda-tui
- anaconda-widgets
- aspnetcore-runtime-8.0
- aspnetcore-runtime-9.0
- aspnetcore-runtime-dbg-8.0
- aspnetcore-runtime-dbg-9.0
- aspnetcore-targeting-pack-8.0
- aspnetcore-targeting-pack-9.0
- audit-libs-devel
- bind
- bind-chroot
- bind-dnssec-utils
- bind-libs
- bind-license
- bind-utils
- binutils-devel
- blivet-data
- boom-boot
- boom-boot-conf
- buildah
- buildah-tests
- cloud-init
- cockpit-image-builder
- cockpit-machines

- cockpit-packagekit
- cockpit-session-recording
- cockpit-storaged
- containers-common
- containers-common-extra
- crash
- ddiskit
- delve
- dnf-bootc
- dotnet-apphost-pack-8.0
- dotnet-apphost-pack-9.0
- dotnet-host
- dotnet-hostfxr-8.0
- dotnet-hostfxr-9.0
- dotnet-runtime-8.0
- dotnet-runtime-9.0
- dotnet-runtime-dbg-8.0
- dotnet-runtime-dbg-9.0
- dotnet-sdk-8.0
- dotnet-sdk-9.0
- dotnet-sdk-aot-9.0
- dotnet-sdk-dbg-8.0
- dotnet-sdk-dbg-9.0
- dotnet-targeting-pack-8.0
- dotnet-targeting-pack-9.0
- dotnet-templates-8.0
- dotnet-templates-9.0
- dracut-caps
- dracut-live
- edk2-ovmf
- efi-srpm-macros
- fapolicyd
- fapolicyd-selinux
- firefox
- firewall-applet
- firewall-config
- gdb

- gdb-doc
- gdb-gdbserver
- gdb-headless
- gdb-minimal
- gdm
- glibc-devel
- glibc-doc
- glibc-locale-source
- glibc-utils
- gnome-shell-extension-background-logo
- gnome-tour
- gnome-user-docs
- gpsd
- gpsd-clients
- hivex
- hivex-libs
- httpd
- httpd-core
- httpd-devel
- httpd-filesystem
- httpd-manual
- httpd-tools
- ignition
- ignition-edge
- ignition-validate
- ipa-client
- ipa-client-common
- ipa-client-encrypted-dns
- ipa-client-epn
- ipa-client-samba
- ipa-common
- ipa-selinux
- ipa-selinux-luna
- ipa-selinux-nfast
- ipa-server
- ipa-server-common
- ipa-server-dns

- ipa-server-encrypted-dns
- ipa-server-trust-ad
- ipset-service
- iptables-devel
- iptables-nft
- iptables-nft-services
- iptables-utils
- java-21-openjdk
- java-21-openjdk-demo
- java-21-openjdk-devel
- java-21-openjdk-headless
- java-21-openjdk-javadoc
- java-21-openjdk-javadoc-zip
- java-21-openjdk-jmods
- java-21-openjdk-src
- java-21-openjdk-static-libs
- kernel-debug-devel
- kernel-debug-devel-matched
- kernel-devel
- kernel-devel-matched
- kernel-doc
- kernel-headers
- kernel-rpm-macros
- kernel-srpm-macros
- krb5-devel
- ksh
- libblockdev
- libblockdev-btrfs
- libblockdev-crypto
- libblockdev-dm
- libblockdev-fs
- libblockdev-loop
- libblockdev-lvm
- libblockdev-lvm-dbus
- libblockdev-mdraid
- libblockdev-mpath
- libblockdev-nvdimm

- libblockdev-nvme
- libblockdev-part
- libblockdev-plugins-all
- libblockdev-smart
- libblockdev-smartmontools
- libblockdev-swap
- libblockdev-tools
- libblockdev-utils
- libguestfs
- libguestfs-appliance
- libguestfs-bash-completion
- libguestfs-inspect-icons
- libguestfs-rescue
- libguestfs-rsync
- libguestfs-xfs
- librados2
- librbd1
- libreswan
- libudisks2
- libvirt
- libvirt-client
- libvirt-client-qemu
- libvirt-daemon
- libvirt-daemon-common
- libvirt-daemon-config-network
- libvirt-daemon-config-nwfilter
- libvirt-daemon-driver-interface
- libvirt-daemon-driver-network
- libvirt-daemon-driver-nodedev
- libvirt-daemon-driver-nwfilter
- libvirt-daemon-driver-qemu
- libvirt-daemon-driver-secret
- libvirt-daemon-driver-storage
- libvirt-daemon-driver-storage-core
- libvirt-daemon-driver-storage-disk
- libvirt-daemon-driver-storage-iscsi
- libvirt-daemon-driver-storage-logical

- libvirt-daemon-driver-storage-mpath
- libvirt-daemon-driver-storage-rbd
- libvirt-daemon-driver-storage-scsi
- libvirt-daemon-kvm
- libvirt-daemon-lock
- libvirt-daemon-log
- libvirt-daemon-plugin-lockd
- libvirt-daemon-proxy
- libvirt-libs
- libvirt-nss
- libvirt-ssh-proxy
- lorax
- lorax-docs
- lorax-lmc-novirt
- lorax-lmc-virt
- lorax-templates-generic
- lorax-templates-rhel
- mecab-ipadic
- mecab-ipadic-EUCJP
- mod_ldap
- mod_lua
- mod_proxy_html
- mod_session
- mod_ssl
- mpich
- mpich-autoload
- mpich-devel
- mpich-doc
- net-snmp
- net-snmp-agent-libs
- net-snmp-devel
- net-snmp-libs
- net-snmp-perl
- net-snmp-perl-module
- net-snmp-utils
- netstandard-targeting-pack-2.1
- NetworkManager-cloud-setup

- NetworkManager-config-connectivity-oracle
- NetworkManager-ovs
- NetworkManager-ppp
- nfs-utils-coreos
- nfsv4-client-utils
- nginx
- nginx-all-modules
- nginx-core
- nginx-filesystem
- nginx-mod-http-image-filter
- nginx-mod-http-perl
- nginx-mod-http-xslt-filter
- nginx-mod-mail
- nginx-mod-stream
- ntsysv
- OpenIPMI
- OpenIPMI-lanserv
- OpenIPMI-libs
- openscap
- openscap-engine-sce
- openscap-scanner
- openscap-utils
- openssh-askpass
- openssh-keysign
- openssl-devel
- openssl-perl
- open-vm-tools
- open-vm-tools-desktop
- open-vm-tools-salt-minion
- open-vm-tools-sdmp
- open-vm-tools-test
- osbuild
- osbuild-composer
- osbuild-composer-core
- osbuild-composer-worker
- osbuild-depsolve-dnf
- osbuild-luks2

- osbuild-lvm2
- osbuild-ostree
- osbuild-selinux
- osinfo-db
- pacemaker-cluster-libs
- pacemaker-libs
- pacemaker-schemas
- PackageKit
- PackageKit-command-not-found
- PackageKit-glib
- PackageKit-gstreamer-plugin
- PackageKit-gtk3-module
- passt
- passt-selinux
- pcp
- pcp-conf
- pcp-devel
- pcp-doc
- pcp-export-pcp2elasticsearch
- pcp-export-pcp2graphite
- pcp-export-pcp2influxdb
- pcp-export-pcp2json
- pcp-export-pcp2openmetrics
- pcp-export-pcp2spark
- pcp-export-pcp2xml
- pcp-export-pcp2zabbix
- pcp-export-zabbix-agent
- pcp-geolocate
- pcp-gui
- pcp-import-collectl2pcp
- pcp-import-ganglia2pcp
- pcp-import-iostat2pcp
- pcp-import-mrtg2pcp
- pcp-import-sar2pcp
- pcp-libs
- pcp-libs-devel
- pcp-pmda-activemq

- pcp-pmda-amdgpu
- pcp-pmda-apache
- pcp-pmda-bash
- pcp-pmda-bcc
- pcp-pmda-bind2
- pcp-pmda-bonding
- pcp-pmda-bpf
- pcp-pmda-bpftrace
- pcp-pmda-cifs
- pcp-pmda-cisco
- pcp-pmda-dbping
- pcp-pmda-denki
- pcp-pmda-dm
- pcp-pmda-docker
- pcp-pmda-ds389
- pcp-pmda-ds389log
- pcp-pmda-elasticsearch
- pcp-pmda-farm
- pcp-pmda-gluster
- pcp-pmda-gpfs
- pcp-pmda-gpsd
- pcp-pmda-hacluster
- pcp-pmda-haproxy
- pcp-pmda-infiniband
- pcp-pmda-json
- pcp-pmda-libvirt
- pcp-pmda-lio
- pcp-pmda-lmsensors
- pcp-pmda-logger
- pcp-pmda-lustre
- pcp-pmda-lustrecomm
- pcp-pmda-mailq
- pcp-pmda-memcache
- pcp-pmda-mic
- pcp-pmda-mongodb
- pcp-pmda-mounts
- pcp-pmda-mssql

- pcp-pmda-mysql
- pcp-pmda-named
- pcp-pmda-netcheck
- pcp-pmda-netfilter
- pcp-pmda-news
- pcp-pmda-nfsclient
- pcp-pmda-nginx
- pcp-pmda-nvidia-gpu
- pcp-pmda-openmetrics
- pcp-pmda-openvswitch
- pcp-pmda-oracle
- pcp-pmda-pdns
- pcp-pmda-perfevent
- pcp-pmda-podman
- pcp-pmda-postfix
- pcp-pmda-postgresql
- pcp-pmda-rabbitmq
- pcp-pmda-redis
- pcp-pmda-resctrl
- pcp-pmda-roomtemp
- pcp-pmda-rsyslog
- pcp-pmda-samba
- pcp-pmda-sendmail
- pcp-pmda-shping
- pcp-pmda-slurm
- pcp-pmda-smart
- pcp-pmda-snmp
- pcp-pmda-sockets
- pcp-pmda-statsd
- pcp-pmda-summary
- pcp-pmda-systemd
- pcp-pmda-trace
- pcp-pmda-unbound
- pcp-pmda-weblog
- pcp-pmda-zimbra
- pcp-pmda-zswap
- pcp-selinux

- pcp-system-tools
- pcp-zeroconf
- pcre2-devel
- pcre2-utf16
- pcre2-utf32
- perf
- perl-hivex
- perl-PCP-LogImport
- perl-PCP-LogSummary
- perl-PCP-MMV
- perl-PCP-PMDA
- perl-Sys-Guestfs
- perl-XML-Parser
- pesign
- plymouth
- plymouth-core-libs
- plymouth-devel
- plymouth-graphics-libs
- plymouth-plugin-fade-throbber
- plymouth-plugin-label
- plymouth-plugin-script
- plymouth-plugin-space-flares
- plymouth-plugin-two-step
- plymouth-scripts
- plymouth-system-theme
- plymouth-theme-fade-in
- plymouth-theme-script
- plymouth-theme-solar
- plymouth-theme-spinfinity
- plymouth-theme-spinner
- podman
- podman-docker
- podman-remote
- polkit-devel
- polkit-docs
- postgresql
- postgresql-contrib

- postgresql-docs
- postgresql-plperl
- postgresql-plpython3
- postgresql-pltcl
- postgresql-private-devel
- postgresql-private-libs
- postgresql-server
- postgresql-server-devel
- postgresql-static
- postgresql-test
- postgresql-upgrade
- postgresql-upgrade-devel
- pykickstart
- python3-audit
- python3-blivet
- python3-blockdev
- python3-boom
- python3-dnf-plugin-leaves
- python3-dnf-plugin-modulesync
- python3-dnf-plugin-show-leaves
- python3-gpsd
- python3-ipaclient
- python3-ipalib
- python3-ipaserver
- python3-iscsi-initiator-utils
- python3-kickstart
- python3-lib389
- python3-libguestfs
- python3-net-snmp
- python3-osbuild
- python3-pcp
- python3-perf
- python3-rtslib
- python3-virt-firmware
- rear
- redhat-rpm-config
- rhel-system-roles

- rpmdevtools
- rtla
- rv
- sanlock
- sanlock-lib
- scap-security-guide
- scap-security-guide-doc
- selinux-policy-devel
- setroubleshoot
- setroubleshoot-plugins
- setroubleshoot-server
- slapi-nis
- sssd-idp
- system-config-printer-libs
- system-config-printer-udev
- systemd-boot-unsigned
- systemd-devel
- systemd-journal-remote
- systemd-ukify
- systemtap
- systemtap-client
- systemtap-devel
- systemtap-exporter
- systemtap-initscript
- systemtap-runtime
- systemtap-runtime-java
- systemtap-runtime-python3
- systemtap-runtime-virtguest
- systemtap-runtime-virthost
- systemtap-sdt-devel
- systemtap-sdt-dtrace
- systemtap-server
- target-restore
- thunderbird
- tog-pegasus
- tog-pegasus-libs
- tuned-gtk

- tuned-ppd
- tuned-profiles-atomic
- tuned-profiles-mssql
- tuned-profiles-oracle
- tuned-profiles-postgresql
- tuned-profiles-spectrumscale
- tuned-utils
- udisks2
- udisks2-iscsi
- udisks2-lsm
- udisks2-lvm2
- uki-direct
- vim-common
- vim-enhanced
- vim-X11
- virt-p2v
- virt-top
- virt-v2v
- virt-v2v-bash-completion
- WALinuxAgent
- WALinuxAgent-udev
- wireshark
- wireshark-cli
- xxd

Removed BaseOS Binary Packages

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

- amd-ucode-firmware
- atheros-firmware
- brcmfmac-firmware
- cirrus-audio-firmware
- dvb-firmware
- intel-audio-firmware
- intel-vsc-firmware
- iwlegacy-firmware
- iwlwifi-dvm-firmware
- iwlwifi-mvm-firmware

- kpatch
- kpatch-dnf
- libdnf-plugin-subscription-manager
- libertas-firmware
- mlxsw_spectrum-firmware
- mrvlprestera-firmware
- mt7xxx-firmware
- nxpwireless-firmware
- python3-cloud-what
- python3-subscription-manager-rhsm
- qcom-firmware
- realtek-firmware
- redhat-release-eula
- rhsm-icons
- subscription-manager
- subscription-manager-cockpit
- subscription-manager-plugin-ostree
- subscription-manager-rhsm-certificates
- tiwilink-firmware

Removed AppStream Binary Packages

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

- amd-gpu-firmware
- ansible-collection-microsoft-sql
- command-line-assistant
- command-line-assistant-selinux
- fence-agents-aliyun
- fence-agents-azure-arm
- fence-agents-gce
- fence-agents-openstack
- insights-client
- insights-client-ros
- intel-gpu-firmware
- NetworkManager-config-connectivity-redhat
- nvidia-gpu-firmware
- opentelemetry-collector
- realtime-tests

- redhat-backgrounds
- redhat-cloud-client-configuration
- redhat-cloud-client-configuration-cdn
- redhat-indexhtml
- redhat-logos
- redhat-logos-httpd
- redhat-logos-ipa
- rhc
- rhc-worker-playbook
- s390utils
- s390utils-se-data
- toolbox
- virtio-win
- virt-who

Removed CodeReady Linux Builder Binary Packages

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

- redhat-sb-certs
- toolbox-tests

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:

- btrfs-progs
- dtrace
- kernel-uek
- ocfs2-tools
- oracle-indexhtml
- oraclelinux-release
- oraclelinux-release-el10
- oracle-logos
- python-dmidecode

Added Source Packages for AppStream by Oracle

The following source packages have been added to AppStream by Oracle:

- dnf-plugin-spacewalk
- dtrace
- pyOpenSSL
- python3-dnf-plugin-ulninfo
- python-hwdata
- python-netifaces
- rhn-client-tools
- rhnlib
- rhnsd

Modified BaseOS Source Packages

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

- audit
- autofs
- basesystem
- binutils
- biosdevname
- chkconfig
- chrony
- cockpit
- coreutils
- dnf
- dnf-plugins-core
- dracut
- efibootmgr
- efi-rpm-macros
- firewalld
- glibc
- grub2
- grubby
- initscripts
- ipset
- iptables

- iscsi-initiator-utils
- kdump-utils
- kernel
- kexec-tools
- kmod
- krb5
- libdnf
- libkcapi
- linux-firmware
- makedumpfile
- mcelog
- mdadm
- microcode_ctl
- NetworkManager
- nfs-utils
- nvme-cli
- nvmetcli
- openssh
- openssl
- openssl-fips-provider
- os-prober
- pcre2
- polkit
- python-configshell
- redhat-release
- selinux-policy
- shim
- sos
- sssd
- systemd
- tuned
- vim

Modified AppStream Source Packages

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

- 389-ds-base
- anaconda

- audit
- bind
- binutils
- boom-boot
- buildah
- ceph
- chkconfig
- cloud-init
- cockpit
- cockpit-image-builder
- cockpit-machines
- cockpit-session-recording
- containers-common
- crash
- ddiskit
- delve
- dnf
- dnf-plugins-core
- dotnet8.0
- dotnet9.0
- dracut
- edk2
- efi-rpm-macros
- fapolicyd
- firefox
- firewalld
- gdb
- gdm
- glibc
- gnome-shell-extension-background-logo
- gnome-tour
- gnome-user-docs
- gpsd
- hivex
- httpd
- ignition
- ipa

- ipset
- iptables
- iscsi-initiator-utils
- java-21-openjdk
- kernel
- kernel-srpm-macros
- krb5
- ksh
- libblockdev
- libguestfs
- libreswan
- libvirt
- lorax
- lorax-templates-rhel
- mecab-ipadic
- mpich
- net-snmp
- NetworkManager
- nfs-utils
- nginx
- OpenIPMI
- openscap
- openssh
- openssl
- open-vm-tools
- osbuild
- osbuild-composer
- osinfo-db
- pacemaker
- PackageKit
- passt
- pcp
- pcre2
- perl-XML-Parser
- pesign
- plymouth
- podman

- polkit
- postgresql16
- pykickstart
- python-blivet
- python-rtslib
- python-virt-firmware
- rear
- redhat-rpm-config
- rhel-system-roles
- rpmdevtools
- sanlock
- scap-security-guide
- selinux-policy
- setroubleshoot
- setroubleshoot-plugins
- slapi-nis
- sssd
- system-config-printer
- systemd
- systemtap
- thunderbird
- tog-pegasus
- tuned
- udisks2
- vim
- virt-p2v
- virt-top
- virt-v2v
- WALinuxAgent
- wireshark

Removed BaseOS Source Packages

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

- kpatch
- subscription-manager
- subscription-manager-cockpit
- subscription-manager-rhsm-certificates

Removed AppStream Source Packages

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

- `ansible-collection-microsoft-sql`
- `command-line-assistant`
- `insights-client`
- `opentelemetry-collector`
- `realtime-tests`
- `redhat-cloud-client-configuration`
- `redhat-indexhtml`
- `redhat-logos`
- `rhc`
- `rhc-worker-playbook`
- `s390utils`
- `toolbox`
- `virtio-win`
- `virt-who`