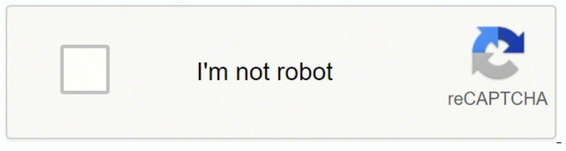
Scap compliance checker 5.0 user manual



Next

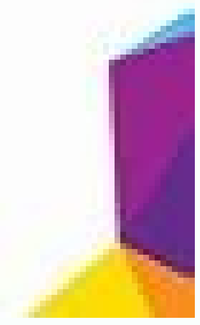
Scap compliance checker 5.0 user manual

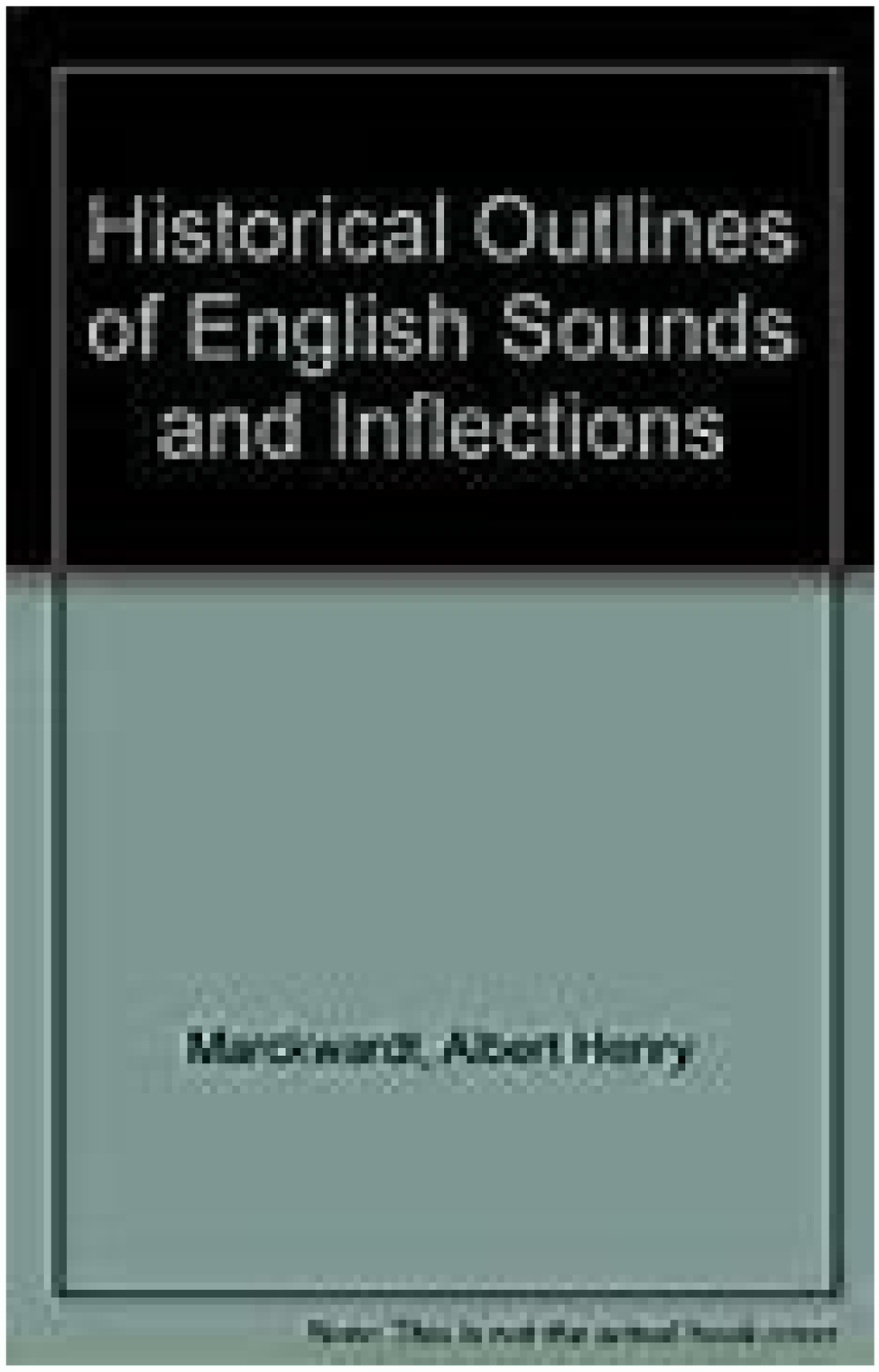
NETGEAR

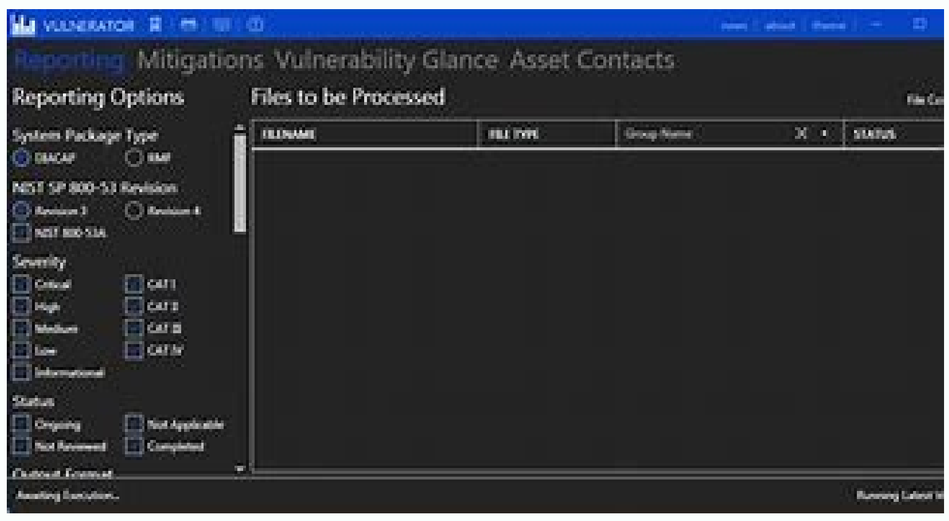
AC1600 WiFi Cable Modem Router

Model C6250

User Manual







English Nederlands logout Home / Tools List of all available tools for penetration testing. Tool count: 2817 Page 2Home / Tools / 0d1n List of all available tools for penetration testing. 0d1n Summary We're Obsessed with Your Privacy 1. Anonymous Chatting At GradeMiners, you can communicate directly with your writer on a no-name basis. 2. Secure Payment Methods We accept only Visa, MasterCard, American Express and Discover for online orders. 3. Complete Confidentiality Your personal details remain confidential and won't be disclosed to the writer or other parties. Show Table of Contents Red Hat Enterprise Linux 8.3Abstract The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 8.3 and document known problems in this release, as well as notable bug fixes, Technology Previews, deprecated functionality, and other details. We appreciate your input on our documentation. Please let us know how we could make it better. To do so: For simple comments on specific passages, make sure you are viewing the documentation in the Multi-page HTML format. Highlight the part of text that you want to comment on. Then, click the Add Feedback pop-up that appears below the highlighted text, and follow the displayed instructions. For submitting more complex feedback, create a Bugzilla ticket: Go to the Bugzilla website. As the Component, use Documentation. Fill in the Description field with your suggestion for improvement. Include a link to the relevant part(s) of documentation. Click Submit Bug. In RHEL 8.3, you can configure a root password and create a user account before you begin the installation. Previously, you configured a root password and created a user account after you began the installation process. You can also create customized images based on a much more reliable backend and also push images to clouds through the RHEL web console. RHEL for Edge RHEL 8.3 introduces RHEL for Edge for remotely installing RHEL on Edge servers. RHEL for Edge is an rpm-ostree image that you can compose using Image Builder. You can install the image using a Kickstart file and then manage the image to include image updates and to roll back an image to a previous functional state. Following are RHEL for Edge key highlights: Atomic upgrades, where the state of each update is known and no changes are seen until you reboot the device. Custom health checks and intelligent rollbacks to ensure resiliency. Container-focused workflows, where you can separate core OS updates from the application updates, and test and deploy different versions of applications. Optimized OTA payloads for low-bandwidth environments. For more information, see Section 5.1.2, "RHEL for Edge". Infrastructure services The Tuned system tuning tool has been rebased to version 2.13, which adds support for architecture-dependent tuning and multiple include directives. Security RHEL 8.3 provides Ansible roles for automated deployments of Policy-Based Decryption (PBD) solutions using Clevis and Tang, and this version of the rhel-system-roles package also contains an Ansible role for RHEL logging through Rsyslog. The scap-security-guide packages have been rebased to version 0.1.50, and OpenSCAP has been rebased to version 1.3.3. These updates provide substantial improvements, including a profile aligned with the CIS RHEL 7 Benchmark v2.2.0 and a profile aligned with the Health Insurance Portability and Accountability Act (HIPAA) that is required by North-American healthcare organizations. With this update, you can now generate result-based remediation roles from tailored profiles using the SCAP Workbench tool. The USBGuard framework now provides its own SELinux policy, it notifies desktop users in GUI, and the version 0.7.8 contains many other improvements and bug fixes. Dynamic programming languages, web and database servers Later versions of the following components are now available as new module streams: nginx 1.18 Node.js 14 Perl 5.30 PHP 7.4 Ruby 2.7 The following components have been updated in RHEL 8.3: Git to version 2.27 Squid to version 4.11 See Section 5.1.11, "Dynamic programming languages, web and database servers" for more information. The following compiler toolsets have been updated in RHEL 8.3: GCC Toolset 10 LLVM Toolset 10.0.1 Rust Toolset 1.45.2 Go Toolset 1.14.7 See Section 5.1.12, "Compilers and development tools" for more information. Identity Management The Rivest Cipher 4 (RC4) cipher suite, the default encryption type for users, services, and trusts between Active Directory (AD) domains in an AD forest, has been deprecated in RHEL 8. For compatibility reasons, this update introduces a new cryptographic subpolicy AD-SUPPORT to enable support for the deprecated RC4 encryption type. The new subpolicy allows you to use RC4 with RHEL Identity Management (IdM) and SSSD Active Directory integration solutions. See Section 5.1.13, "Identity Management" for more information. The web console The web console provides an option to switch between administrative access and limited access from inside of a user session. Virtualization Virtual machines (VMs) hosted on IBM Z hardware can now use the IBM Secure Execution feature. This makes the VMs resistant to attacks if the host is compromised, and also prevents untrusted hosts from obtaining information from the VM. In addition, DASD devices can now be assigned to VMs on IBM Z. Desktop and graphics You can now use the GNOME desktop on IBM Z systems. The Direct Rendering Manager (DRM) kernel graphics subsystem has been rebased to upstream Linux kernel version 5.6. This version provides a number of enhancements over the previous version, including support for new GPUs and APUs, and various driver updates. See Section 5.1.14, "Desktop" and Section 5.1.15, "Graphics infrastructures" for further details. In-place upgrade and OS conversion In-place upgrade from RHEL 7 to RHEL 8 The supported in-place upgrade paths currently are: From RHEL 7.8 to RHEL 8.2 on the 64-bit Intel, IBM POWER 8 (little endian), and IBM Z architectures From RHEL 7.6 to RHEL 8.2 on architectures that require kernel version 4.14: IBM POWER 9 (little endian) and IBM Z (Structure A) From RHEL 7.7 to RHEL 8.2 on systems with SAP HANA. To ensure your system remains supported after upgrading to RHEL 8.2, either update to the latest RHEL 8.3 version or enable the RHEL 8.2 Extended Update Support (EUS) repositories. On systems with SAP HANA, enable the RHEL 8.2 Update Services for SAP Solutions (E4S) repositories. For more information, see Supported in-place upgrade paths for Red Hat Enterprise Linux. For instructions on performing an in-place upgrade, see Upgrading from RHEL 7 to RHEL 8. Notable enhancements include: Leapp now supports user input by generating true/false questions to determine how to proceed with the upgrade. You can now upgrade multiple hosts simultaneously using the Satellite web UI. The in-place upgrade is now supported for on-demand instances on AWS and Microsoft Azure, using Red Hat Update Infrastructure (RHUI). With the release of the RHBA-2021:0569 advisory, you can create custom scripts for the Leapp pre-upgrade report. See Automating your Red Hat Enterprise Linux pre-upgrade report workflow for details. In-place upgrade from RHEL 6 to RHEL 8 To upgrade from RHEL 6.10 to RHEL 8.2, follow instructions in Upgrading from RHEL 6 to RHEL 8. Conversion from a different Linux distribution to RHEL If you are using CentOS Linux 8 or Oracle Linux 8, you can convert your operating system to RHEL 8 using the Red Hat-supported Convert2RHEL utility. For more information, see Converting from an RPM-based Linux distribution to RHEL. If you are using an earlier version of CentOS Linux or Oracle Linux, namely versions 6 or 7, you can convert your operating system to RHEL and then perform an in-place upgrade to RHEL 8. Note that CentOS Linux 6 and Oracle Linux 6 conversions use the unsupported Convert2RHEL utility. For more information on unsupported conversions, see How to convert from CentOS Linux 6 or Oracle Linux 6 to RHEL 6. For information regarding how Red Hat supports conversions from other Linux distributions to RHEL, see the Convert2RHEL Support Policy document. OpenJDK 11 is now available New version of Open Java Development Kit (OpenJDK) is now available. For more information about the features introduced in this release and changes in the existing functionality, see OpenJDK features. Additional resourcesRed Hat Customer Portal Labs Red Hat Customer Portal Labs is a set of tools in a section of the Customer Portal available at . The applications in Red Hat Customer Portal Labs can help you improve performance, quickly troubleshoot issues, identify security problems, and quickly deploy and configure complex applications. Some of the most popular applications are: Red Hat Enterprise Linux 8.3 is distributed with the kernel version 4.18.0-240, which provides support for the following architectures: AMD and Intel 64-bit architectures The 64-bit ARM architecture IBM Power Systems, Little Endian 64-bit IBM Z Make sure you purchase the appropriate subscription for each architecture. For more information, see Get Started with Red Hat Enterprise Linux - additional architectures. For a list of available subscriptions, see Subscription Utilization on the Customer Portal. Red Hat Enterprise Linux 8 is installed using ISO images. Two types of ISO image are available for the AMD64, Intel 64-bit, 64-bit ARM, IBM Power Systems, and IBM Z architectures: Binary DVD ISO: A full installation image that contains the BaseOS and AppStream repositories and allows you to complete the installation without additional repositories. The Binary DVD ISO image is larger than 4.7 GB, and as a result, it might not fit on a single-layer DVD. A dual-layer DVD or USB key is recommended when using the Binary DVD ISO image to create bootable installation media. You can also use the Image Builder tool to create customized RHEL images. For more information about Image Builder, see the Composing a customized RHEL system image document. Boot ISO: A minimal boot ISO image that is used to boot into the installation program. This option requires access to the BaseOS and AppStream repositories to install software packages. The repositories are part of the Binary DVD ISO image. See the Performing a standard RHEL installation document for instructions on downloading ISO images, creating installation media, and completing a RHEL installation. For automated Kickstart installations and other advanced topics, see the Performing an advanced RHEL installation document. Red Hat Enterprise Linux 8 is distributed through two main repositories: Both repositories are required for a basic RHEL installation, and are available with all RHEL subscriptions. Content in the BaseOS repository is intended to provide the core set of the underlying OS functionality that provides the foundation for all installations. This content is available in the RPM format and is subject to support terms similar to those in previous releases of RHEL. For a list of packages distributed through BaseOS, see the Package manifest. Content in the Application Stream repository includes additional user space applications, runtime languages, and databases in support of the varied workloads and use cases. Application Streams are available in the familiar RPM format, as an extension to the RPM format called modules, or as Software Collections. For a list of packages available in AppStream, see the Package manifest. In addition, the CodeReady Linux Builder repository is available with all RHEL subscriptions. It provides additional packages for use by developers. Packages included in the CodeReady Linux Builder repository are unsupported. For more information about RHEL 8 repositories, see the Package manifest. Red Hat Enterprise Linux 8 introduces the concept of Application Streams. Multiple versions of user space components are now delivered and updated more frequently than the core operating system packages. This provides greater flexibility to customize Red Hat Enterprise Linux without impacting the underlying stability of the platform or specific deployments. Components made available as Application Streams can be packaged as modules or RPM packages and are delivered through the AppStream repository in RHEL 8. Each Application Stream component has a given life cycle, either the same as RHEL 8 or shorter. For details, see Red Hat Enterprise Linux Life Cycle. Modules are collections of packages representing a logical unit: an application, a language stack, a database, or a set of tools. These packages are built, tested, and released together. Module streams represent versions of the Application Stream components. For example, several streams (versions) of the PostgreSQL database server are available in the postgresql module with the default postgresql:10 stream. Only one module stream can be installed on the system. Different versions can be used in separate containers. Detailed module commands are described in the Installing, managing, and removing user-space components document. For a list of modules available in AppStream, see the Package manifest. On Red Hat Enterprise Linux 8, installing software is ensured by the YUM tool, which is based on the DNF technology. We deliberately adhere to usage of the yum term for consistency with previous major versions of RHEL. However, if you type dnf instead of yum, the command works as expected because yum is an alias to dnf for compatibility. For more details, see the following documentation: Red Hat makes Red Hat Enterprise Linux 8 content available quarterly, in between minor releases (8.Y). The quarterly releases are numbered using the third digit (8.Y.1). The new features in the RHEL 8.3.1 release are described below. Flatpak packages for several desktop applications Flatpak is a system for running graphical applications as containers. Using Flatpak, you can install and update an application independently of the host operating system. This update provides Flatpak container images of the following applications in the Red Hat Container Catalog: To install Flatpak containers available in the Red Hat Container Catalog, use the following procedure: Make sure that the latest version of the Flatpak client is installed on your system: # yum update flatpak Enable the RHEL Flatpak repository: # flatpak remote-add rhel Provide the credentials for your RHEL account: # podman login registry.redhat.io By default, Podman saves the credentials only until the user logs out. Optional: Save your credentials permanently: $ cp $XDG_RUNTIME_DIR/containers/auth.json \ $HOME/.config/flatpak/oci-auth.json Install the Flatpak container image: $ flatpak install rhel container-id (JIRA:RHELPLAN-30958, BZ#1920689, BZ#1921179, BZ#1921802, BZ#1916412, BZ#1921812, BZ#1920604) Rust Toolset rebased to version 1.47.0 Rust Toolset has been updated to version 1.47.0. Notable changes include: The compile-time evaluated functions const fn have been improved and can now use control flow features, for example if, while, and match. The new #[track_caller] annotation can now be put on functions. Panics from annotated functions report the caller as the source. The Rust Standard Library now generically implements traits for arrays of any length. Previously, many of the trait implementations for arrays were only filled for lengths between 0 and 32. For detailed instructions regarding usage, see Using Rust Toolset. (BZ#1883839) The Logging System Role now supports property-based filter on its outputs With this update, property-based filters have been added to the files output, the forwards output, and the remote_files output of the Logging System Role. The feature is provided by underlying the rsyslog sub-role, and is configurable via the Logging RHEL System Role. As a result, users can benefit from the ability of filtering log messages by the properties, such as hostname, tag, and the message itself is useful to manage logs. (BZ#1889492) The Logging RHEL System Role now supports rsyslog behavior With this enhancement, rsyslog receives the message from Red Hat Virtualization and forwards the message to the elasticsearch. (BZ#1889893) The ubi8/pause container image is now available Podman now uses the ubi8/pause instead of the k8s.gcr.io/pause container image to hold the network namespace information of the pod. (BZ#1690785) Podman rebased to version 2.1 The Podman utility has been updated to version 2.1. Notable enhancements include: Changes: Updated Podman to 2.2.1 (from 2.0.5), Buildah to 1.19 (from 1.15.1), Skopeo to 1.2.1 (from 1.1.1), Udica to 0.2.3 (from 0.2.2), and CRIU to 3.15 (0.3.4) Docker-compatible volume API endpoints (Create, Inspect, List, Remove, Prune) are now available Added an API endpoint for generating systemd unit files for containers The podman play kube command now features support for setting CPU and Memory limits for containers The podman play kube command now supports persistent volumes claims using Podman named volumes The podman play kube command now supports Kubernetes configmaps via the --configmap option Experimental support for shortname aliasing has been added. This is not enabled by default, but can be turned on by setting the environment variable CONTAINERS_SHORT_NAME_ALIASING to on. For more information see Container image short names in Podman. The new podman image command has been added. This allows for an image to be mounted, read-only, to inspect its contents without creating a container from it. The podman save and podman load commands can now create and load archives containing multiple images. Podman will now retry pulling an image at most 3 times if a pull fails due to network errors. Bug Fixes: Fixed a bug where running systemd in a container on a cgroups v1 system would fail. The Buildah tool has been updated to version 1.19. Notable enhancements include: Changes: The`buildah inspect`command supports inspecting manifests The `buildah push`command supports pushing manifests lists and digests Added support for --manifest flags The --arch and --os and --variant options has beed added to select architecture and OS Allow users to specify stdin into containers Allow FROM to be overridden with --from option Added --ignorefile flag to use alternate .dockerignore flags short-names aliasing Added --policy option to buildah pull command Fix buildah mount command to display container names not IDs Improved buildah completions Use --timestamp rather then --omit-timestamp flag Use pipes for copying Added --omit-timestamp flag to buildah bud command Add VFS additional image store to container Allow "readonly" as alias to "ro" in mount options buildah, bud: support --jobs=N option for parallel execution The Skopeo tool has been updated to version 1.2.1. Notable enhancements include: Changes: Add multi-arch builds for upstream and stable skopeo image via Travis Added support for digests in sync Added --all sync flag to emulate copy --all Added --format option to skopeo inspect command The Udica tool has been updated to version 0.2.3. Notable enhancements include: Changes: Enable container port, not the host port Add --version option The CRIU tool has been updated to version 3.15. Notable enhancements include: Changes: Initial cgroup2 support Legalized swrk API and add the ability for inheriting fds via it External bind mounts and tasks-to-cgroups bindings ibcriu.so (RPC wrapper) and plugins (JIRA:RHELPLAN-55998) This part describes new features and major enhancements introduced in Red Hat Enterprise Linux 8.3. Anaconda rebased to version 33.16 With this release, Anaconda has been rebased to version 33.16. This version provides the following notable enhancements over the previous version. The Installation Program now displays static IPv6 addresses on multiple lines and no longer resizes the windows. The Installation Program now displays supported NVDIMM device sector sizes. Host name is now configured correctly on an installed system having IPv6 static configuration. You can now use non-ASCII characters in disk encryption passphrase. The Installation Program displays a proper recommendation to create a new file system on /boot, /tmp, and all /var and /usr mount points except /usr/local and /var/www. The Installation Program now correctly checks the keyboard layout and does not change the status of the Keyboard Layout screen when the keyboard keys (ALT+SHIFT) are used to switch between different layouts and languages. Rescue mode no longer fails on systems with existing RAID1 partitions. Changing of the LUKS version of the container is now available in the Manual Partitioning screen. The Installation Program successfully finishes the installation without the btrfs-progs package. The Installation Program now uses the default LUKS2 version for an encrypted container. The Installation Program no longer crashes when a Kickstart file places physical volumes (PVs) of a Logical volume group (VG) on an ignoredisk list. Introduces a new mount path /mnt/sysroot for system root. This path is used to mount / of the target system. Usually, the physical root and the system root are the same, so /mnt/sysroot is attached to the same file system as /mnt/sysimage. The only exceptions are rpm-ostree systems, where the system root changes based on the deployment. Then, /mnt/sysroot is attached to a subdirectory of /mnt/sysimage. It is recommended to use /mnt/sysroot for chroot. (BZ#1691319, BZ#1679893, BZ#1684045, BZ#1688478, BZ#1700450, BZ#1720145, BZ#1723888, BZ#1754977, BZ#1755996, BZ#1784360, BZ#1796310, BZ#1871680) GUI changes in RHEL Installation Program The RHEL Installation Program now includes the following user settings on the Installation Summary window: Root password User creation With this change, you can now configure a root password and create a user account before you begin the installation. Previously, you configured a root password and created a user account after you began the installation process. A root password is used to log in to the administrator (also known as superuser or root) account which is used for system administration tasks. The user name is used to log in from a command line; if you install a graphical environment, then your graphical login manager uses the full name. For more details, see Performing a standard RHEL installation document. (JIRA:RHELPLAN-40469) Image Builder backend osbuild-composer replaces lorax-composer The osbuild-composer backend replaces lorax-composer. The new service provides REST APIs for image building. As a result, users can benefit from a more reliable backend and more predictable output images. (BZ#1836211) Image Builder osbuild-composer supports a set of image types With the osbuild-composer backend replacement, the following set of image types supported in osbuild-composer this time: TAR Archive (.tar) QEMU QCOW2 (.qcow2) VMware Virtual Machine Disk (.vmdk) Amazon Machine Image (.ami) Azure Disk Image (.vhd) OpenStack Image (.qcow2) The following outputs are not supported this time: ext4-filesystem partitioned-disk Alibaba Cloud Google GCE (JIRA:RHELPLAN-42617) Image Builder now supports push to clouds through GUI With this enhancement, when creating images, users can choose the option of pushing to Azure and AWS service clouds through GUI Image Builder. As a result, users can benefit from easier uploads and instantiation. (JIRA:RHELPLAN-30878) Introducing RHEL for Edge images With this release, you can now create customized RHEL images for Edge servers. You can use Image Builder to create RHEL for Edge images, and then use RHEL installer to deploy them on AMD and Intel 64-bit systems. Image Builder generates a RHEL for Edge image as rhel-edge-commit in a .tar file. A RHEL for Edge image is an rpm-ostree image that includes system packages for remotely installing RHEL on Edge servers. The system packages include: Base OS package Podman as the container engine You can customize the image to configure the OS content as per your requirements, and can deploy them on physical and virtual machines. With a RHEL for Edge image, you can achieve the following: Atomic upgrades, where the state of each update is known and no changes are seen until you reboot the device. Custom health checks using Greenboot and intelligent rollbacks for resiliency in case of failed upgrades. Container-focused workflows, where you can separate core OS updates from the application updates, and test and deploy different versions of applications. Optimized OTA payloads for low-bandwidth environments. Custom health checks using Greenboot to ensure resiliency. For more information about composing, installing, and managing RHEL for Edge images, see Composing, Installing, and Managing RHEL for Edge images. (JIRA:RHELPLAN-56676) The default value for the best dnf configuration option has been changed from True to False With this update, the value for the best dnf configuration option has been set to True in the default configuration file to retain the original dnf behavior. As a result, for users that use the default configuration file the behavior remains unchanged. If you provide your own configuration files, make sure that the best=True option is present to retain the original behavior. (BZ#1832869) New --norepopath option for the dnf reposync command is now available Previously, the reposync command created a subdirectory under the --download-path directory for each downloaded repository by default. With this update, the --norepopath option has been introduced, and reposync does not create the subdirectory. As a result, the repository is downloaded directly into the directory specified by --download-path. This option is also present in the YUM v3. (BZ#1842285) Ability to enable and disable the libdnf plugins Previously, subscription checking was hardcoded into the RHEL version of the libdnf plug-ins. With this update, the microdnf utility can enable and disable the libdnf plug-ins, and subscription checking can now be disabled the same way as in DNF. To disable subscription checking, use the --disableplugin=subscription-manager command. To disable all plug-ins, use the --noplugins command. (BZ#1781126) ReaR updates RHEL 8.3 introduces a number of updates to the Relax-and-Recover (ReaR) utility. Notable changes include: Support for the third-party Rubrik Cloud Data Management (CDM) as external backup software has been added. To use it, set the BACKUP option in the configuration file to CDM. Creation of a rescue image with a file larger than 4 GB on the IBM POWER, little endian architecture has been enabled. Disk layout created by ReaR no longer includes entries for Rancher 2 Longhorn iSCSI devices and file systems. (BZ#1743303) smartmontools rebased to version 7.1 The smartmontools package has been upgraded to version 7.1, which provides multiple bug fixes and enhancements. Notable changes include: HDD, SSD and USB additions to the drive database. New options -j and --json to enable JSON output mode. Workaround for the incomplete Log subpages response from some SAS SSDs. Improved handling of READ CAPACITY command. Various improvements for the decoding of the log pages. (BZ#1671154) opencryptoki rebased to version 3.14.0 The opencryptoki packages have been upgraded to version 3.14.0, which provides multiple bug fixes and enhancements. Notable changes include: EP11 cryptographic service enhancements: Dilithium support Edwards-curve digital signature algorithm (EdDSA) support Support of Rivest–Shamir–Adleman optimal asymmetric encryption padding (RSA-OAEP) with non-SHA1 hash and mask generation function (MGF) Enhanced process and thread locking Enhanced btree and object locking Support for new IBM Z hardware z15 Support of multiple token instances for trusted platform module (TPM), IBM cryptographic architecture (ICA) and integrated cryptographic service facility (ICSF) Added a new tool p11sak, which lists the token keys in an openCryptoki token repository Added a utility to migrate a token repository to FIPS compliant encryption Fixed pkcsep11_migrate tool Minor fixes of the ICSF software (BZ#1780293) gpgme rebased to version 1.13.1. The gpgme packages have been upgraded to upstream version 1.13.1. Notable changes include: New context flags no-symkey-cache (has an effect when used with GnuPG 2.2.7 or later), request-origin (has an effect when used with GnuPG 2.2.6 or later), auto-key-locate, and trust-model have been introduced. New tool gpgme-json as native messaging server for web browsers has been added. As of now, the public key encryption and decryption is supported. New encryption API to support direct key specification including hidden recipients option and taking keys from a file has been introduced. This also allows the use of a subkey. (BZ#1829822) powertop rebased to version 2.12 The powertop packages have been upgraded to version 2.12. Notable changes over the previously available version 2.11 include: Use of Device Interface Power Management (DIPM) for SATA link PM. Support for Intel Comet Lake mobile and desktop systems, the Skylake server, and the Atom-based Tremont architecture (Jasper Lake). (BZ#1783110) tuned rebased to version 2.14.0 The tuned packages have been upgraded to upstream version 2.14.0. Notable enhancements include: The optimize-serial-console profile has been introduced. Support for a post loaded profile has been added. The irqbalance plugin for handling irqbalance settings has been added. Architecture specific tuning for Marvell ThunderX and AMD based platforms has been added. Scheduler plugin has been extended to support cgroups-v1 for CPU affinity setting. (BZ#1792264) tcpdump rebased to version 4.9.3 The tcpdump utility has been updated to version 4.9.3 to fix Common Vulnerabilities and Exposures (CVE). (BZ#1804063) libpcap rebased to version 1.9.1 The libpcap packages have been updated to version 1.9.1 to fix Common Vulnerabilities and Exposures (CVE). (BZ#1806422) iperf3 now supports sctp option on the client side With this enhancement, the user can use Stream Control Transmission Protocol (SCTP) instead of Transmission Control Protocol (TCP) on the client side of testing network throughput. The following options for iperf3 are now available on the client side of testing: --sctp --xbind --nstreams To obtain more information, see Client Specific Options in the iperf3 man page. (BZ#1665142) iperf3 now supports SSL With this enhancement, the user can use RSA authentication between the client and the server to restrict the connections to the server only to legitimate clients. The following options for iperf3 are now available on the server side: --rsa-private-key-path --authorized-users-path The following options for iperf3 are now available on the client side of communication: --username --rsa-public-key-path (BZ#1700497) bind rebased to 9.11.20 The bind package has been upgraded to version 9.11.20, which provides multiple bug fixes and enhancements. Notable changes include: Increased reliability on systems with many CPU cores by fixing several race conditions. Detailed error reporting: dig and other tools can now print the Extended DNS Error (EDE) option, if it is present. Message IDs in inbound DNS Zone Transfer Protocol (AXFR) transfers are checked and logged, when they are inconsistent. (BZ#1818785) A new optimize-serial-console TuneD profile to reduce I/O to serial consoles by lowering the printk value With this update, a new optimize-serial-console TuneD profile is

available. In some scenarios, kernel drivers can send large amounts of I/O operations to the serial console. Such behavior can cause temporary unresponsiveness while the I/O is written to the serial console. The optimize-serial-console profile reduces this I/O by lowering the printk value from the default of 7 4 1 7 to 4 4 1 7. Users with a serial console who wish to make this change on their system can instrument their system as follows: # tuned-adm profile throughput-performance optimize-serial-console As a result, users will have a lower printk value that persists across a reboot, which reduces the likelihood of system hangs. This TuneD profile reduces the amount of I/O written to the serial console by removing debugging information. If you need to collect this debugging information, you should ensure this profile is not enabled and that your printk value is set to 7 4 1 7. To check the value of printk run: # cat /proc/sys/kernel/printk (BZ#1840689) New TuneD profiles added for the AMD-based platforms In RHEL 8.3, the throughput-performance TuneD profile was updated to include tuning for the AMD-based platforms. There is no need to change any parameter manually and the tuning is automatically applied on the AMD system. The AMD Epyc Naples and Rome systems alters the following parameters in the default throughput-performance profile: sched_migration_cost_ns=5000000 and kernel.numa_balancing=0 With this enhancement, the system performance is improved by ~5%. (BZ#1746957) memcached rebased to version 1.5.22 The memcached packages have been upgraded to version 1.5.22. Notable changes over the previous version include: TLS has been enabled. The -o inline_ascii_response option has been removed. The -Y [authfile] option has been added along with authentication mode for the ASCII protocol. memcached can now recover its cache between restarts. New experimental meta commands have been added. Various performance improvements. (BZ#1809536) Cyrus SASL now supports channel bindings with the SASL/GSSAPI and SASL/GSS-SPNEGO plug-ins This update adds support for channel bindings with the SASL/GSSAPI and SASL/GSS-SPNEGO plug-ins. As a result, when used in the openldap libraries, this feature enables Cyrus SASL to maintain compatibility with and access to Microsoft Active Directory and Microsoft Windows systems which are introducing mandatory channel binding for LDAP connections. (BZ#1817054) Libreswan rebased to 3.32 With this update, Libreswan has been rebased to upstream version 3.32, which includes several new features and bug fixes. Notable features include: Libreswan no longer requires separate FIPS 140-2 certification. Libreswan now implements the cryptographic recommendations of RFC 8247, and changes the preference from SHA-1 and RSA-PKCS v1.5 to SHA-2 and RSA-PSS. Libreswan supports XFRMi virtual ipsecXX interfaces that simplify writing firewall rules. Recovery of crashed and rebooted nodes in a full-mesh encryption network is improved. (BZ#1820206) The libssh library has been rebased to version 0.9.4 The libssh library, which implements the SSH protocol, has been upgraded to version 0.9.4. This update includes bug fixes and enhancements, including: Added support for Ed25519 keys in PEM files. Added support for diffie-hellman-group14-sha256 key exchange algorithm. Added support for localuser in Match keyword in the libssh client configuration file. Match criteria keyword arguments are now case-sensitive (note that keywords are case-insensitive, but keyword arguments are case-sensitive) Fixed CVE-2019-14889 and CVE-2020-1730. Added support for recursively creating missing directories found in the path string provided for the known hosts file. Added support for OpenSSH keys in PEM files with comments and leading white spaces. Removed the OpenSSH server configuration inclusion from the libssh server configuration. (BZ#1804797) gnutls rebased to 3.6.14 The gnutls packages have been rebased to upstream version 3.6.14. This version provides many bug fixes and enhancements, most notably: gnutls now rejects certificates with Time fields that contain invalid characters or formatting. gnutls now checks trusted CA certificates for minimum key sizes. When displaying an encrypted private key, the certtool utility no longer includes its plain text description. Servers using gnutls now advertise OCSP-stapling support. Clients using gnutls now send OCSP staples only on request. (BZ#1789392) gnutls FIPS DH checks now conform with NIST SP 800-56A rev. 3 This update of the gnutls packages provides checks required by NIST Special Publication 800-56A Revision 3, sections 5.7.1.1 and 5.7.1.2, step 2. The change is necessary for future FIPS 140-2 certifications. As a result, gnutls now accept only 2048-bit or larger parameters from RFC 7919 and RFC 3526 during the Diffie-Hellman key exchange when operating in FIPS mode. (BZ#1849079) gnutls now performs validations according to NIST SP 800-56A rev 3 This update of the gnutls packages adds checks required by NIST Special Publication 800-56A Revision 3, sections 5.6.2.2.2 and 5.6.2.1.3, step 2. The addition prepares gnutls for future FIPS 140-2 certifications. As a result, gnutls perform additional validation steps for generated and received public keys during the Diffie-Hellman key exchange when operating in FIPS mode. (BZ#1855803) update-crypto-policies and fips-mode-setup moved into crypto-policies-scripts The update-crypto-policies and fips-mode-setup scripts, which were previously included in the crypto-policies package, are now moved into a separate RPM subpackage crypto-policies-scripts. The package is automatically installed through the Recommends dependency on regular installations. This enables the ubi8/ubi-minimal image to avoid the inclusion of the Python language interpreter and thus reduces the image size. (BZ#1832743) OpenSC rebased to version 0.20.0 The opensc package has been rebased to version 0.20.0 which addresses multiple bugs and security issues. Notable changes include: With this update, CVE-2019-6502, CVE-2019-15946, CVE-2019-15945, CVE-2019-19480, CVE-2019-19481 and CVE-2019-19479 security issues are fixed. The OpenSC module now supports the C_WrapKey and C_UnwrapKey functions. You can now use the facility to detect insertion and removal of card readers as expected. The pkcs11-tool utility now supports the CKA_ALLOWED_MECHANISMS attribute. This update allows default detection of the OsEID cards. The OpenPGP Card v3 now supports Elliptic Curve Cryptography (ECC). The PKCS#11 URI now truncates the reader name with ellipsis. (BZ#1810660) stunnel rebased to version 5.56 With this update, the stunnel encryption wrapper has been rebased to upstream version 5.56, which includes several new features and bug fixes. Notable features include: New ticketKeySecret and ticketMacSecret options that control confidentiality and integrity protection of the issued session tickets. These options enable you to resume sessions on other nodes in a cluster. New curves option to control the list of elliptic curves in OpenSSL 1.1.0 and later. New ciphersuites option to control the list of permitted TLS 1.3 ciphersuites. Added sslVersion, sslVersionMin and sslVersionMax for OpenSSL 1.1.0 and later. (BZ#1808365) libkcapi rebased to version 1.2.0 The libkcapi package has been rebased to upstream version 1.2.0, which includes minor changes. (BZ#1683123) setools rebased to 4.3.0 The setools package, which is a collection of tools designed to facilitate SELinux policy analysis, has been upgraded to version 4.3.0. This update includes bug fixes and enhancements, including: Revised sediff method for Type Enforcement (TE) rules, which significantly reduces memory and runtime issues. Added infiniband context support to seinfo, sediff, and apol. Added apol configuration for the location of the Qt assistant tool used to display online documentation. Fixed sediff issues with: Properties header displaying when not requested. Name comparison of type_transition files. Fixed permission of map socket sendto information flow direction. Added methods to the TypeAttribute class to make it a complete Python collection. Genfscon now looks up classes, rather than using fixed values which were dropped from libsepol. The setools package requires the following packages: setools-console setools-console-analyses setools-gui (BZ#1820079) Individual CephFS files and directories can now have SELinux labels The Ceph File System (CephFS) has recently enabled storing SELinux labels in the extended attributes of files. Previously, all files in a CephFS volume were labeled with a single common label system_u:object_r:cephfs_t:s0. With this enhancement, you can change the labels for individual files, and SELinux defines the labels of newly created files based on transition rules. Note that previously unlabeled files still have the system_u:object_r:cephfs_t:s0 label until explicitly changed. (BZ#1823764) OpenSCAP rebased to version 1.3.3 The openscap packages have been upgraded to upstream version 1.3.3, which provides many bug fixes and enhancements over the previous version, most notably: Added the autotailor script that enables you to generate tailoring files using a command-line interface (CLI). Added the timezone part to the Extensible Configuration Checklist Description Format (XCCDF) TestResult start and end time stamps Added the yamlfilecontent independent probe as a draft implementation. Introduced the urn:xccdf:fix:script:kubernetes fix type in XCCDF. Added ability to generate the machineconfig fix. The oscap-podman tool can now detect ambiguous scan targets. The rpmverifyfile probe can now verify files from the /bin directory. Fixed crashes when complicated regexes are executed in the textfilecontent58 probe. Evaluation characteristics of the XCCDF report are now consistent with OVAL entities from the system_info probe. Fixed file-path pattern matching in offline mode in the textfilecontent58 probe. Fixed infinite recursion in the systemdunitdependency probe. (BZ#1829761) SCAP Security Guide now provides a profile aligned with the CIS RHEL 8 Benchmark v1.0.0 With this update, the scap-security-guide packages provide a profile aligned with the CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0. The profile enables you to harden the configuration of the system using the guidelines by the Center for Internet Security (CIS). As a result, you can configure and automate compliance of your RHEL 8 systems with CIS by using the CIS Ansible Playbook and the CIS SCAP profile. Note that the rpm_verify_permissions rule in the CIS profile does not work correctly. (BZ#1760734) scap-security-guide now provides a profile that implements HIPAA This update of the scap-security-guide packages adds the Health Insurance Portability and Accountability Act (HIPAA) profile to the RHEL 8 security compliance content. This profile implements recommendations outlined on the The HIPAA Privacy Rule website. The HIPAA Security Rule establishes U.S. national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information. (BZ#1832760) scap-security-guide rebased to 0.1.50 The scap-security-guide packages, which contain the latest set of security policies for Linux systems, have been upgraded to version 0.1.50. This update includes bug fixes and enhancements, most notably: Ansible content has been improved: numerous rules contain Ansible remediations for the first time and other rules have been updated to address bug fixes. Fixes and improvements to the scap-security-guide content for scanning RHEL7 systems, including: The scap-security-guide packages now provide a profile aligned with the CIS RHEL 7 Benchmark v2.2.0. Note that the rpm_verify_permissions rule in the CIS profile does not work correctly; see the rpm_verify_permissions fails in the CIS profile known issue. The SCAP Security Guide profiles now correctly disable and mask services that should not be started. The audit_rules_privileged_commands rule in the scap-security-guide packages now works correctly for privileged commands. Remediation of the dconf_gnome_login_banner_text rule in the scap-security-guide packages no longer incorrectly fails. (BZ#1815007) SCAP Workbench can now generate results-based remediations from tailored profiles With this update, you can now generate result-based remediation roles from tailored profiles using the SCAP Workbench tool. (BZ#1640715) New Ansible role provides automated deployments of Clevis clients This update of the rhel-system-roles package introduces the nbde_client RHEL system role. This Ansible role enables you to deploy multiple Clevis clients in an automated way. (BZ#1716040) New Ansible role can now set up a Tang server With this enhancement, you can deploy and manage a Tang server as part of an automated disk encryption solution with the new nbde_server system role. The nbde_server Ansible role, which is included in the rhel-system-roles package, supports the following features: Rotating Tang keys Deploying and backing up Tang keys For more information, see Rotating Tang server keys. (BZ#1716039) clevis rebased to version 13 The clevis packages have been rebased to version 13, which provides multiple bug fixes and enhancements. Notable changes include: clevis luks unlock can be used in the device with a key file in the non-interactive mode. clevis encrypt tpm2 parses the pcr_ids field if the input is given as a JSON array. The clevis-luks-unbind(1) man page no longer refers only to LUKS v1. clevis luks bind does not write to an inactive slot anymore, if the password given is incorrect. clevis luks bind now works while the system uses the non-English locale. Added support for tpm2-tools 4.x. (BZ#1818780) clevis luks edit enables you to edit a specific pin configuration This update of the clevis packages introduces the new clevis luks edit subcommand that enables you to edit a specific pin configuration. For example, you can now change the URL address of a Tang server and the pcr_ids parameter in a TPM2 configuration. You can also add and remove new sss pins and change the threshold of an sss pin. (BZ#1436735) clevis luks bind -y now allows automated binding With this enhancement, Clevis supports automated binding with the -y parameter. You can now use the -y option with the clevis luks bind command, which automatically answers subsequent prompts with yes. For example, when using a Tang pin, you are no longer required to manually trust Tang keys. (BZ#1819767) fapolicyd rebased to version 1.0 The fapolicyd packages have been rebased to version 1.0, which provides multiple bug fixes and enhancements. Notable changes include: The multiple thread synchronization problem has been resolved. Enhanced performance with reduced database size and loading time. A new trust option for the fapolicyd package in the fapolicyd.conf file has been added to customize trust back end. You can add all trusted files, binaries, and scripts to the new /etc/fapolicyd/fapolicyd.trust file. You can manage the fapolicyd.trust file using the CLI. You can clean or dump the database using the CLI. The fapolicyd package overrides the magic database for better decoding of scripts. The CLI prints MIME type of the file similar to the file command according to the override. The /etc/fapolicyd/fapolicyd.rules file supports a group of values as attribute values. The fapolicyd daemon has a syslog_format option for setting the format of the audit/sylog events. (BZ#1817413) fapolicyd now provides its own SELinux policy in fapolicyd-selinux With this enhancement, the fapolicyd framework now provides its own SELinux security policy. The daemon is confined under the fapolicyd_t domain and the policy is installed through the fapolicyd-selinux subpackage. (BZ#1714529) USBGuard rebased to version 0.7.8 The usbguard packages have been rebased to version 0.7.8 which provides multiple bug fixes and enhancements. Notable changes include: The HidePII=true|false parameter in the /etc/usbguard/usbguard-daemon.conf file can now hide personally identifiable information from audit entries. The AuthorizedDefault=keep|none|all|internal parameter in the /etc/usbguard/usbguard-daemon.conf file can predefine authorization state of controller devices. With the new with-connect-type rule attribute, users can now distinguish the connection type of the device. Users can now append temporary rules with the -t option. Temporary rules remain in memory only until the daemon restarts. usbguard list-rules can now filter rules according to certain properties. usbguard generate-policy can now generate a policy for specific devices. The usbguard allow|block|reject command can now handle rule strings, and a target is applied on each device that matches the specified rule string. New subpackages usbguard-notifier and usbguard-selinux are included. (BZ#1738590) USBGuard provides many improvements for corporate desktop users This addition to the USBGuard project contains enhancements and bug fixes to improve the usability for corporate desktop users. Important changes include: For keeping the /etc/usbguard/rules.conf rule file clean, users can define multiple configuration files inside the RuleFolder=/etc/usbguard/rules.d/ directory. By default, the RuleFolder is specified in the /etc/usbguard-daemon.conf file. The usbguard-notifier tool now provides GUI notifications. The tool notifies the user whenever a device is plugged in or plugged out and whether the device is allowed, blocked, or rejected by any user. You can now include comments in the configuration files, because the usbguard-daemon no longer parses lines starting with #. (BZ#1667395) USBGuard now provides its own SELinux policy in usbguard-selinux With this enhancement, the USBGuard framework now provides its own SELinux security policy. The daemon is confined under the usbguard_t domain and the policy is installed through the usbguard-selinux subpackage. (BZ#1683567) libcap now supports ambient capabilities With this update, users are able to grant ambient capabilities at login and prevent the need to have root access for the appropriately configured processes. (BZ#1487388) The libseccomp library has been rebased to version 2.4.3 The libseccomp library, which provides an interface to the seccomp system call filtering mechanism, has been upgraded to version 2.4.3. This update provides numerous bug fixes and enhancements. Notable changes include: Updated the syscall table for Linux v5.4-rc4. No longer defining __NR_x values for system calls that do not exist. __SNR_x is now used internally. Added define for __SNR_ppoll. Fixed a multiplexing issue with s390/s390x shm* system calls. Removed the static flag from the libseccomp tools compilation. Added support for io-uring related system calls. Fixed the Python module naming issue introduced in the v2.4.0 release; the module is named seccomp as it was previously. Fixed a potential memory leak identified by clang in the scmp_bpf_sim tool. (BZ#1770693) omamqp1 module is now supported With this update, the AMQP 1.0 protocol supports sending messages to a destination on the bus. Previously, Openstack used the AMQP1 protocol as a communication standard, and this protocol can now log messages in AMQP messages. This update introduces the rsyslog-omamqp1 sub-package to deliver the omamqp1 output mode, which logs messages and sends them to the destination on the bus. (BZ#1713427) OpenSCAP compresses remote content With this update, OpenSCAP uses gzip compression for transferring remote content. The most common type of remote content is text-based CVE feeds, which increase in size over time and typically have to be downloaded for every scan. The gzip compression reduces the bandwidth to 10% of bandwidth needed for uncompressed content. As a result, this reduces bandwidth requirements across the entire chain between the scanned system and the server that hosts the remote content. (BZ#1855708) SCAP Security Guide now provides a profile aligned with NIST-800-171 With this update, the scap-security-guide packages provide a profile aligned with the NIST-800-171 standard. The profile enables you to harden the system configuration in accordance with security requirements for protection of Controlled Unclassified Information (CUI) in non-federal information systems. As a result, you can more easily configure systems to be aligned with the NIST-800-171 standard. (BZ#1762962) The IPv4 and IPv6 connection tracking modules have been merged into the nf_conntrack module This enhancement merges the nf_conntrack_ipv4 and nf_conntrack_ipv6 Netfilter connection tracking modules into the nf_conntrack kernel module. Due to this change, blacklisting the address family-specific modules no longer work in RHEL 8.3, and you can blacklist only the nf_conntrack module to disable connection tracking support for both the IPv4 and IPv6 protocols. (BZ#1822085) firewalld rebased to version 0.8.2 The firewalld packages have been upgraded to upstream version 0.8.2, which provides a number of bug fixes over the previous version. For details, see the firewalld 0.8.2 Release Notes. (BZ#1809636) NetworkManager rebased to version 1.26.0 The NetworkManager packages have been upgraded to upstream version 1.26.0, which provides a number of enhancements and bug fixes over the previous version: NetworkManager resets the auto-negotiation, speed, and duplex setting to their original value when deactivating a device. Wi-Fi profiles connect now automatically if all previous activation attempts failed. This means that an initial failure to auto-connect to the network no longer blocks the automatism. A side effect is that existing Wi-Fi profiles that were previously blocked now connect automatically. The nm-settings-nmcli(5) and nm-settings-dbus(5) man pages have been added. Support for a number of bridge parameters has been added. Support for virtual routing and forwarding (VRF) interfaces has been added. For further details, see Permanently reusing the same IP address on different interfaces. Support for Opportunistic Wireless Encryption mode (OWE) for Wi-Fi networks has been added. NetworkManager now supports 31-bit prefixes on IPv4 point-to-point links according to RFC 3021. The nmcli utility now supports removing settings using the nmcli connection modify remove command. NetworkManager no longer creates and activates slave devices if a master device is missing. For further information about notable changes, read the upstream release notes: NetworkManager 1.26.0 NetworkManager 1.24.0 (BZ#1814746) XDP is conditionally supported Red Hat supports the eXpress Data Path (XDP) feature only if all of the following conditions apply: You load the XDP program on an AMD or Intel 64-bit architecture You use the libxdp library to load the program into the kernel The XDP program uses one of the following return codes: XDP_ABORTED, XDP_DROP, or XDP_PASS The XDP program does not use the XDP hardware offloading For details about unsupported XDP features, see Overview of XDP features that are available as Technology Preview (BZ#1889736) xdp-tools is partially supported The xdp-tools package, which contains user space support utilities for the kernel eXpress Data Path (XDP) feature, is now supported on the AMD and Intel 64-bit architectures. This includes the libxdp library, the xdp-loader utility for loading XDP programs, and the xdp-filter example program for packet filtering. Note that the xdpdump utility for capturing packets from a network interface with XDP enabled is still a Technology Preview. (BZ#1820670) The dracut utility by default now uses NetworkManager in initial RAM disk Previously, the dracut utility was using a shell script to manage networking in the initial RAM disk, initrd. In certain cases, this could cause problems. For example, the NetworkManager sends another DHCP request, even if the script in the RAM disk has already requested an IP address, which could result in a timeout. With this update, the dracut by default now uses the NetworkManager in the initial RAM disk and prevents the system from running into issues. In case you want to switch back to the previous implementation, and recreate the RAM disk images, use the following commands: # echo 'add_dracutmodules+=" network-legacy "' > /etc/dracut.conf.d/enable-network-legacy.conf # dracut -vf --regenerate-all (BZ#1626348) Network configuration in the kernel command line has been consolidated under the ip parameter The ipv6, netmask, gateway, and hostname parameters to set the network configuration in the kernel command line have been consolidated under the ip parameter. The ip parameter accepts different formats, such as the following: ip=__IP_address__:__peer__:__gateway_IP_address__:__net_mask__:__host_name__:__interface_name__:__configuration_method__ For further details about the individual fields and other formats this parameter accepts, see the description of the ip parameter in the dracut.cmdline(7) man page. The ipv6, netmask, gateway, and hostname parameters are no longer available in RHEL 8. (BZ#1905138) Kernel version in RHEL 8.3 Red Hat Enterprise Linux 8.3 is distributed with the kernel version 4.18.0-240. (BZ#1839151) Extended Berkeley Packet Filter for RHEL 8.3 The Extended Berkeley Packet Filter (eBPF) is an in-kernel virtual machine that allows code execution in the kernel space, in the restricted sandbox environment with access to a limited set of functions. The virtual machine executes a special assembly-like code. The eBPF bytecode first loads to the kernel, followed by its verification, code translation to the native machine code with just-in-time compilation, and then the virtual machine executes the code. Red Hat ships numerous components that utilize the eBPF virtual machine. Each component is in a different development phase, and thus not all components are currently fully supported. In RHEL 8.3, the following eBPF components are supported: The BPF Compiler Collection (BCC) tools package, which provides tools for I/O analysis, networking, and monitoring of Linux operating systems using eBPF The BCC library which allows the development of tools similar to those provided in the BCC tools package. The eBPF for Traffic Control (tc) feature, which enables programmable packet processing inside the kernel network data path. The eXpress Data Path (XDP) feature, which provides access to received packets before the kernel networking stack processes them, is supported under specific conditions. For more details, refer to the Networking section of Relase Notes. The libbpf package, which is crucial for bpf related applications like bpftrace and bpf/xdp development. For more details, refer to the dedicated release note libbpf fully supported. The xdp-tools package, which contains userspace support utilities for the XDP feature, is now supported on the AMD and Intel 64-bit architectures.This includes the libxdp library, the xdp-loader utility for loading XDP programs, and the xdp-filter example program for packet filtering. Note that the xdpdump utility for capturing packets from a network interface with XDP enabled is still an unsupported Technology Preview. For more details, refer to the Networking section of Release Notes. Note that all other eBPF components are available as Technology Preview, unless a specific component is indicated as supported. The following notable eBPF components are currently available as Technology Preview: The bpftrace tracing language The AF_XDP socket for connecting the eXpress Data Path (XDP) path to user space For more information regarding the Technology Preview components, see Technology Previews. (BZ#1780124) Cornelis Networks Omni-Path Architecture (OPA) Host Software Omni-Path Architecture (OPA) host software is fully supported in Red Hat Enterprise Linux 8.3. OPA provides Host Fabric Interface (HFI) hardware with initialization and setup for high performance data transfers (high bandwidth, high message rate, low latency) between compute and I/O nodes in a clustered environment. For instructions on installing Omni-Path Architecture, see the Intel® Omni-Path Fabric Software Release Notes file. (BZ#1893174) TSX is now disabled by default Starting with RHEL 8.3, the kernel now has the Intel® Transactional Synchronization Extensions (TSX) technology disabled by default to improve the OS security. The change applies to those CPUs that support disabling TSX, including the 2nd Generation Intel® Xeon® Scalable Processors (formerly known as Cascade Lake with Intel® C620 Series Chipsets). For users whose applications do not use TSX, the change removes the default performance penalty of the TSX Asynchronous Abort (TAA) mitigations on the 2nd Generation Intel® Xeon® Scalable Processors. The change also aligns the RHEL kernel behavior with upstream, where TSX has been disabled by default since Linux 5.4. To enable TSX, add the tsx=on parameter to the kernel command line. (BZ#1828642) RHEL 8.3 now supports the page owner tracking feature With this update, you can use the page owner tracking feature to observe the kernel memory utilization at the page allocation level. To enable the page tracker, execute the following steps : # grubby --args="page_owner=on" --update-kernel=0 # reboot As a result, the page owner tracker will track the kernel memory consumption, which helps to debug kernel memory leaks and detect the drivers that use a lot of memory. (BZ#1825414) EDAC for AMD EPYC™ 7003 Series Processors is now supported This enhancement provides Error Detection And Correction (EDAC) device support for AMD EPYC™ 7003 Series Processors. Previously, corrected (CEs) and uncorrected (UEs) memory errors were not reported on systems based on AMD EPYC™ 7003 Series Processors. With this update, such errors will now be reported using EDAC. (BZ#1735611) Flamegraph is now supported with perf tool With this update, the perf command line tool supports flamegraphs to create a graphical representation of the system's performance. The perf data is grouped together into samples with similar stack backtraces. As a result, this data is converted into a visual representation to allow easier identification of computationally intensive areas of code. To generate a flamegraph using the perf tool, execute the following commands: $ perf script record flamegraph -F 99 -g -- stress --cpu 1 --vm-bytes 128M --timeout 10s stress: info: [4461] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd stress: info: [4461] successful run completed in 10s [perf record: Woken up 1 times to write data] [perf record: Captured and wrote 0.060 MB perf.data (970 samples)] $ perf script report flamegraph dumping data to flamegraph.html Note : To generate flamegraphs, install the js-d3-flame-graph rpm. (BZ#1281843) /dev/random and /dev/urandom are now conditionally powered by the Kernel Crypto API DRBG In FIPS mode, the /dev/random and /dev/urandom pseudorandom number generators are powered by the Kernel Crypto API Deterministic Random Bit Generator (DRBG). Applications in FIPS mode use the mentioned devices as a FIPS-compliant noise source, therefore the devices have to employ FIPS-approved algorithms. To achieve this goal, necessary hooks have been added to the /dev/random driver. As a result, the hooks are enabled in the FIPS mode and cause /dev/random and /dev/urandom to connect to the Kernel Crypto API DRBG. (BZ#1785660) libbpf fully supported The libbpf package, crucial for bpf related applications like bpftrace and bpf/xdp development, is now fully supported. It is a mirror of bpf-next linux tree bpf-next/tools/lib/bpf directory plus its supporting header files. The version of the package reflects the version of the Application Binary Interface (ABI). (BZ#1759154) lshw utility now provides additional CPU information With this enhancement, the List Hardware utility (lshw) displays more CPU information. The CPU version field now provides the family, model and stepping details of the system processors in numeric format as version: ... (BZ#1794049) kernel-rt source tree has been updated to the RHEL 8.3 tree The kernel-rt sources have been updated to use the latest Red Hat Enterprise Linux kernel source tree. The real-time patch set has also been updated to the latest upstream version, v5.6.14-rt7. Both of these updates provide a number of bug fixes and enhancements. (BZ#1818138, BZ#1818142) tpm2-tools rebased to version 4.1.1 The tpm2-tools package has been upgraded to version 4.1.1, which provides a number of command additions, updates, and removals. For more details, see the Updates to tpm2-tools package in RHEL8.3 solution. (BZ#1789682) The Mellanox ConnectX-6 Dx network adapter is now fully supported This enhancement adds the PCI IDs of the Mellanox ConnectX-6 Dx network adapter to the mlx5_core driver. On hosts that use this adapter, RHEL loads the mlx5_core driver automatically. This feature, previously available as a technology preview, is now fully supported in RHEL 8.3. (BZ#1782831) mlxsw driver rebased to version 5.7 The mlxsw driver is upgraded to upstream version 5.7 and include following new features: The shared buffer occupancy feature, which provides buffer occupancy data. The packet drop feature, which enables monitoring the layer 2, layer 3, tunnels and access control list drops. Packet trap policers support. Default port priority configuration support using Link Layer Discovery Protocol (LLDP) agent. Enhanced Transmission Selection (ETS) and Token Bucket Filter (TBF) queuing discipline offloading support. RED queuing discipline nodrop mode is enabled to prevent early packet drops. Traffic class SKB editing action skbedit priority feature enables changing packets metadata and it complements with pedit Traffic Class Offloading (TOS). (BZ#1821646) The crash kernel now expands memory reserve for kdump With this enhancement, the crashkernel=auto argument now reserves more memory on machines with 4GB to 64GB memory capacity. Previously, due to limited memory reserve, the crash kernel failed to capture the crash dump as the kernel space and user space memory expanded. As a consequence, the crash kernel experienced an out-of-memory (OOM) error. This update helps to reduce the OOM error occurrences in the described scenario and expands the memory capacity for kdump accordingly. (BZ#1746644) LVM can now manage VDO volumes LVM now supports the Virtual Data Optimizer (VDO) segment type. As a result, you can now use LVM utilities to create and manage VDO volumes as native LVM logical volumes. VDO provides inline block-level deduplication, compression, and thin provisioning features. For more information, see Deduplicating and compressing logical volumes on RHEL. (BZ#1598199) The SCSI stack now works better with high-performance adapters The performance of the SCSI stack has been improved. As a result, next-generation, high performance host bus adapters (HBAs) are now capable of higher IOPS (I/Os per second) on RHEL. (BZ#1761928) The megaraid_sas driver has been updated to the latest version The megaraid_sas driver has been updated to version 07.713.01.00-rc1. This update provides several bug fixes and enhancements relating to improving performance, better stability of supported MegaRAID adapters, and a richer feature set. (BZ#1791041) Stratis now lists the pool name on error When you attempt to create a Stratis pool on a block device that is already in use by an existing Stratis pool, the stratis utility now reports the name of the existing pool. Previously, the utility listed only the UUID label of the pool. (BZ#1734496) FPIN ELS frame notification support The lpfc Fibre Channel (FC) driver now supports Fabric Performance Impact Notifications (FPINs) regarding link integrity, which help identify link level issues and allows the switch to choose a more reliable path. (BZ#1796565) New commands to debug LVM on-disk metadata The pvck utility, which is available from the lvm2 package, now provides low-level commands to debug or rescue LVM on-disk metadata on physical volumes: To extract metadata, use the pvck --dump command. To repair metadata, use the pvck --repair command. For more information, see the pvck(8) man page. (BZ#1541165) LVM RAID supports DM integrity to prevent data loss due to corrupted data on a device It is now possible to add Device Mapper (DM) integrity to an LVM RAID configuration to prevent data loss. The integrity layer detects data corruption on a device and alerts the RAID layer to fix the corrupted data across the LVM RAID. While RAID prevents data loss due to device failure, adding integrity to an LVM RAID array prevents data loss due to corrupted data on a device. You can add the integrity layer when you create a new LVM RAID, or you can add it to an LVM RAID that already exists. (JIRA:RHELPLAN-39320) (BZ#1900019) Userspace now supports the latest nfsdcld daemon Userspace now supports the lastest nfsdcld daemon, which is the only namespace-aware client tracking method. This enhancement ensures client open or lock recovery from the containerized knfsd daemon without any data corruption. (BZ#1817756) nconnect now supports multiple concurrent connections With this enhancement, you can use the nconnect functionality to create multiple concurrent connections to an NFS server, allowing for a different load balancing ability. Enable the nconnect functionality with the nconnect=X NFS mount option, where X is the number of concurrent connections to use. The current limit is 16. (BZ#1683394, BZ#1761352) nfsdcld daemon for client information tracking is now supported With this enhancement, the nfsdcld daemon is now the default method in tracking per-client information on a stable storage. As a result, the NFS v4 running in containers allows the clients to reclaim the opens or locks after a server restart. (BZ#1817752) pacemaker rebased to version 2.0.4 The Pacemaker cluster resource manager has been upgraded to upstream version 2.0.4, which provides a number of bug fixes. (BZ#1828488) New priority-fencing-delay cluster property Pacemaker now supports the new priority-fencing-delay cluster property, which allows you to configure a two-node cluster so that in a split-brain situation the node with the fewest resources running is the node that gets fenced. The priority-fencing-delay property can be set to a time duration. The default value for this property is 0 (disabled). If this property is set to a non-zero value, and the priority meta-attribute is configured for at least one resource, then in a split-brain situation the node with the highest combined priority of all resources running on it will be more likely to survive. For example, if you set pcs resource defaults priority=1 and pcs property set priority-fencing-delay=15s and no other priorities are set, then the node running the most resources will be more likely to survive because the other node will wait 15 seconds before initiating fencing. If a particular resource is more important than the rest, you can give it a higher priority. The node running the master role of a promotable clone will get an extra 1 point if a priority has been configured for that clone. Any delay set with priority-fencing-delay will be added to any delay from the pcmk_delay_base and pcmk_delay_max fence device properties. This behavior allows some delay when both nodes have equal priority, or both nodes need to be fenced for some reason other than node loss (for example, on-fail=fencing is set for a resource monitor operation). If used in combination, it is recommended that you set the priority-fencing-delay property to a value that is significantly greater than the maximum delay from pcmk_delay_base and pcmk_delay_max, to be sure the prioritized node is preferred (twice the value would be completely safe). (BZ#1784601) New commands for managing multiple sets of resource and operation defaults It is now possible to create, list, change and delete multiple sets of resource and operation defaults. When you create a set of default values, you can specify a rule that contains resource and op expressions. This allows you, for example, to configure a default resource value for all resources of a particular type. Commands that list existing default values now include multiple sets of defaults in their output. The pcs resource [op] defaults set create command creates a new set of default values. When specifying rules with this command, only resource and op expressions, including and, or and parentheses, are allowed. The pcs resource [op] defaults set delete | remove command removes sets of default values. The pcs resource [op] defaults set update command changes the default values in a set. (BZ#1817547) Support for tagging cluster resources It is now possible to tag cluster resources in a Pacemaker cluster with the pcs tag command. This feature allows you to administer a specified set of resources with a single command. You can also use the pcs tag command to remove or modify a resource tag, and to display the tag configuration. The pcs resource enable, pcs resource disable, pcs resource manage, and pcs resource unmanage commands accept tag IDs as arguments. (BZ#1684676) Pacemaker now supports recovery by demoting a promoted resource rather than fully stopping it It is now possible to configure a promotable resource in a Pacemaker cluster so that when a promote or monitor action fails for that resource, or the partition in which the resource is running loses quorum, the resource will be demoted but will not be fully stopped. This feature can be useful when you would prefer that the resource continue to be available in the unpromoted mode. For example, if a database master's partition loses quorum, you might prefer that the database resource lose the Master role, but stay alive in read-only mode so applications that only need to read can continue to work despite the lost quorum. This feature can also be useful when a successful demote is both sufficient for recovery and much faster than a full restart. To support this feature: The on-fail operation meta-attribute now accepts a demote value when used with promote actions, as in the following example: pcs resource op add my-rsc promote on-fail="demote" The on-fail operation meta-attribute now accepts a demote value when used with monitor actions with both interval set to a nonzero value and role set to Master, as in the following example: pcs resource op add my-rsc monitor interval="10s" on-fail="demote" role="Master" The no-quorum-policy cluster property now accepts a demote value. When set, if a cluster partition loses quorum, any promoted resources will be demoted but left running and all other resources will be stopped. Specifying a demote meta-attribute for an operation does not affect how promotion of a resource is determined. If the affected node still has the highest promotion score, it will be selected to be promoted again. (BZ#1837747, BZ#1843079) New SBD_SYNC_RESOURCE_STARTUP SBD configuration parameter to improve synchronization with Pacemaker To better control synchronization between SBD and Pacemaker, the /etc/sysconfig/sbd file now supports the SBD_SYNC_RESOURCE_STARTUP parameter. When Pacemaker and SBD packages from RHEL 8.3 or later are installed and SBD is configured with SBD_SYNC_RESOURCE_STARTUP=true, SBD contacts the Pacemaker daemon for information about the daemon's state. In this configuration, the Pacemaker daemon will wait until it has been contacted by SBD, both before starting its subdaemons and before final exit. As a result, Pacemaker will not run resources if SBD cannot actively communicate with it, and Pacemaker will not exit until it has reported a graceful shutdown to SBD. This prevents the unlikely situation that might occur during a graceful shutdown when SBD fails to detect the brief moment when no resources are running before Pacemaker finally disconnects, which would trigger an unneeded reboot. Detecting a graceful shutdown using a defined handshake works in maintenance mode as well. The previous method of detecting a graceful shutdown on the basis of no running resources left had to be disabled in maintenance mode since running resources would not be touched on shutdown. In addition, enabling this feature avoids the risk of a split-brain situation in a cluster when SBD and Pacemaker both start successfully but SBD is unable to contact pacemaker. This could happen, for example, due to SELinux policies. In this situation, Pacemaker would assume that SBD is functioning when it is not. With this new feature enabled, Pacemaker will not complete startup until SBD has contacted it. Another advantage of this new feature is that when it is enabled SBD will contact Pacemaker repeatedly, using a heartbeat, and it is able to panic the node if Pacemaker stops responding at any time. If you have edited your /etc/sysconfig/sbd file or configured SBD through PCS, then an RPM upgrade will not pull in the new SBD_SYNC_RESOURCE_STARTUP parameter. In these cases, to implement this feature you must manually add it from the /etc/sysconfig/sbd.rpmnew file or follow the procedure described in the Configuration via environment section of the sbd(8) man page. (BZ#1718324, BZ#1743726) A new module stream: ruby:2.7 RHEL 8.3 introduces Ruby 2.7.1 in a new ruby:2.7 module stream. This version provides a number of performance improvements, bug and security fixes, and new features over Ruby 2.6 distributed with RHEL 8.1. Notable enhancements include: A new Compaction Garbage Collector (GC) has been introduced. This GC can defragment a fragmented memory space. Ruby yet Another Compiler-Compiler (Racc) now provides a command-line interface for the one-token Look-Ahead Left-to-Right – LALR(1) – parser generator. Interactive Ruby Shell (irb), the bundled Read–Eval–Print Loop (REPL) environment, now supports multi-line editing. Pattern matching, frequently used in functional programming languages, has been introduced as an experimental feature. Numbered parameter as the default block parameter has been introduced as an experimental feature. The following performance improvements have been implemented: Fiber cache strategy has been changed to accelerate fiber creation. Performance of the CGI.escapeHTML method has been improved. Performance of the Monitor class and MonitorMixin module has been improved. In addition, automatic conversion of keyword arguments and positional arguments has been deprecated. In Ruby 3.0, positional arguments and keyword arguments will be separated. For more information, see the upstream documentation. To suppress warnings against experimental features, use the -W:no-experimental command-line option. To disable a deprecation warning, use the -W:no-deprecated command-line option or add Warning[:deprecated] = false to your code. To install the ruby:2.7 module stream, use: # yum module install ruby:2.7 If you want to upgrade from the ruby:2.6 stream, see Switching to a later stream. (BZ#1817135) A new module stream: nodejs:14 A new module stream, nodejs:14, is now available. Node.js 14, included in RHEL 8.3, provides numerous new features and bug and security fixes over Node.js 12 distributed in RHEL 8.1. Notable changes include: The V8 engine has been upgraded to version 8.3. A new experimental WebAssembly System Interface (WASI) has been implemented. A new experimental Async Local Storage API has been introduced. The diagnostic report feature is now stable. The streams APIs have been hardened. Experimental modules warnings have been removed. With the release of the RHEA-2020:5101 advisory, RHEL 8 provides Node.js 14.15.0, which is the most recent Long Term Support (LTS) version with improved stability. To install the nodejs:14 module stream, use: # yum module install nodejs:14 If you want to upgrade from the nodejs:12 stream, see Switching to a later stream. (BZ#1815402, BZ#1891809) git rebased to version 2.27 The git packages have been upgraded to upstream version 2.27. Notable changes over the previously available version 2.18 include: The git checkout command has been split into two separate commands: git switch for managing branches git restore for managing changes within the directory tree The behavior of the git rebase command is now based on the merge workflow by default rather than the previous patch+apply workflow. To preserve the previous behavior, set the rebase.backend configuration variable to apply. The git difftool command can now be used also outside a repository. Four new configuration variables, {author,committer}.{name,email}, have been introduced to override user.{name,email} in more specific cases. Several new options have been added that enable users to configure SSL for communication with proxies. Handling of commits with log messages in non-UTF-8 character encoding has been improved in the git fast-export and git fast-import utilities. The lfs extension has been added as a new git-lfs package. Git Large File Storage (LFS) replaces large files with text pointers inside Git and stores the file contents on a remote server. (BZ#1825114, BZ#1783391) Changes in Python RHEL 8.3 introduces the following changes to the python38:3.8 module stream: The Python interpreter has been updated to version 3.8.3, which provides several bug fixes. The python38-pip package has been updated to version 19.3.1, and pip now supports installing manylinux2014 wheels. Performance of the Python 3.6 interpreter, provided by the python3 packages, has been significantly improved. The ubi8/python-27, ubi8/python-36, and ubi8/python-38 container images now support installing the pipenv utility from a custom package index or a PyPI mirror if provided by the customer. Previously, pipenv could only be downloaded from the upstream PyPI repository, and if the upstream repository was unavailable, the installation failed. (BZ#1847416, BZ#1724996, BZ#1827623, BZ#1841001) A new module stream: php:7.4 RHEL 8.3 introduces PHP 7.4, which provides a number of bug fixes and enhancements over version 7.3. This release introduces a new experimental extension, Foreign Function Interface (FFI), which enables you to call native functions, access native variables, and create and access data structures defined in C libraries. The FFI extension is available in the php-ffi package. The following extensions have been removed: The wddx extension, removed from php-xml package The recode extension, removed from the php-recode package. To install the php:7.4 module stream, use: # yum module install php:7.4 If you want to upgrade from the php:7.3 stream, see Switching to a later stream. For details regarding PHP usage on RHEL 8, see Using the PHP scripting language. (BZ#1797661) A new module stream: nginx:1.18 The nginx 1.18 web and proxy server, which provides a number of bug fixes, security fixes, new features and enhancements over version 1.16, is now available. Notable changes include: Enhancements to HTTP request rate and connection limiting have been implemented. For example, the limit_rate and limit_rate_after directives now support variables, including new $limit_req_status and $limit_conn_status variables. In addition, dry-run mode has been added for the limit_conn_dry_run and limit_req_dry_run directives. A new auth_delay directive has been added, which enables delayed processing of unauthorized requests. The following directives now support variables: grpc_pass, proxy_upload_rate, and proxy_download_rate. Additional PROXY protocol variables have been added, namely $proxy_protocol_server_addr and $proxy_protocol_server_port. To install the nginx:1.18 stream, use: # yum module install nginx:1.18 If you want to upgrade from the nginx:1.16 stream, see Switching to a later stream. (BZ#1826632) A new module stream: perl:5.30 RHEL 8.3 introduces Perl 5.30, which provides a number of bug fixes and enhancements over the previously released Perl 5.26. The new version also deprecates or removes certain language features. Notable changes with significant impact include: The Math::BigInt::CalcEmu, arybase, and B::Debug modules have been removed File descriptors are now opened with a close-on-exec flag Opening the same symbol as a file and as a directory handle is no longer allowed Subroutine attributes now must precede subroutine signatures The :locked and :uniq attributes have been removed Comma-less variable lists in formats are no longer allowed A bare (BZ#1732726) GPU problems on Azure NV6 instances When running RHEL 8 as a guest operating system on a Microsoft Azure NV6 instance, resuming the virtual machine (VM) from hibernation sometimes causes the VM's GPU to work incorrectly. When this occurs, the kernel logs the following message: hv_irq_unmask() failed: 0x5 (BZ#1846838) kdump sometimes does not start on Azure and Hyper-V On RHEL 8 guest operating systems hosted on the Microsoft Azure or Hyper-V hypervisors, starting the kdump kernel in some cases fails when post-exec notifiers are enabled. To work around this problem, disable crash kexec post notifiers: # echo N > /sys/module/kernel/parameters/crash_kexec_post_notifiers (BZ#1865745) Setting static IP in a RHEL 8 virtual machine on a VMWare host does not work Currently, when using RHEL 8 as a guest operating system of a virtual machine (VM) on a VMWare host, the DatasourceOVF function does not work correctly. As a consequence, if you use use the cloud-init utility to set the the VM's network to static IP and then reboot the VM, the VM's network will be changed to DHCP. (BZ#1750862) Core dumping RHEL 8 virtual machines with certain NICs to a remote machine on Azure takes longer than expected Currently, using the kdump utility to save the core dump file of a RHEL 8 virtual machine (VM) on a Microsoft Azure hypervisor to a remote machine does not work correctly when the VM is using a NIC with enabled accelerated networking. As a consequence, the dump file is saved after approximately 200 seconds, instead of immediately. In addition, the following error message is logged on the console before the dump file is saved. device (eth0): linklocal6: DAD failed for an EUI-64 address (BZ#1854037) TX/RX packet counters do not increase after virtual machines resume from hibernation The TX/RX packet counters stop increasing when a RHEL 8 virtual machine (VM), with a CX4 VF NIC, resumes from hibernation on Microsoft Azure. To keep the counters working, restart the VM. Note that, doing so will reset the counters. (BZ#1876527) RHEL 8 virtual machines fail to resume from hibernation on Azure The GUID of the virtual function (VF), vmbus device, changes when a RHEL 8 virtual machine (VM), with SR-IOV enabled, is hibernated and deallocated on Microsoft Azure . As a result, when the VM is restarted, it fails to resume and crashes. As a workaround, hard reset the VM using the Azure serial console. (BZ#1876519) Migrating a POWER9 guest from a RHEL 7-ALT host to RHEL 8 fails Currently, migrating a POWER9 virtual machine from a RHEL 7-ALT host system to RHEL 8 becomes unresponsive with a "Migration status: active" status. To work around this problem, disable Transparent Huge Pages (THP) on the RHEL 7-ALT host, which enables the migration to complete successfully. (BZ#1741436) redhat-support-tool does not work with the FUTURE crypto policy Because a cryptographic key used by a certificate on the Customer Portal API does not meet the requirements by the FUTURE system-wide cryptographic policy, the redhat-support-tool utility does not work with this policy level at the moment. To work around this problem, use the DEFAULT crypto policy while connecting to the Customer Portal API. (BZ#1802026) UDICA is not expected to work with 1.0 stable stream UDICA, the tool to generate SELinux policies for containers, is not expected to work with containers that are run via podman 1.0.x in the container-tools:1.0 module stream. (JIRA:RHELPLAN-25571) podman system connection add does not automatically set the default connection The podman system connection add command does not automatically set the first connection to be the default connection. To set the default connection, you must manually run the command podman system connection default . (BZ#1881894) Red Hat Enterprise Linux 8 supports the installation of multiple languages and the changing of languages based on your requirements. East Asian Languages - Japanese, Korean, Simplified Chinese, and Traditional Chinese. European Languages - English, German, Spanish, French, Italian, Portuguese, and Russian. The following table lists the fonts and input methods provided for various major languages. RHEL 8 introduces the following changes to internationalization compared to RHEL 7: Support for the Unicode 11 computing industry standard has been added. Internationalization is distributed in multiple packages, which allows for smaller footprint installations. For more information, see Using langpacks. A number of glibc locales have been synchronized with Unicode Common Locale Data Repository (CLDR). Bugzilla and JIRA IDs are listed in this document for reference. Bugzilla bugs that are publicly accessible include a link to the ticket.

0.2-9 Thu Oct 07 2021, Lenka Špačková (lspackova@redhat.com) Updated the known issue BZ#1942330 (Dynamic programming languages, web and database servers). 0.2-8 Tue Oct 05 2021, Lucie Maňásková (lmanasko@redhat.com) Added a deprecated functionality BZ#1999620 (Shells and command-line tools). 0.2-7 Thu Aug 19 2021, Lucie Maňásková (lmanasko@redhat.com) 0.2-6 Fri Jul 9 2021, Lucie Maňásková (lmanasko@redhat.com) Updated text for JIRA:RHELPLAN-34199(Security). 0.2-5 Wed Jun 23 2021, Lucie Maňásková (lmanasko@redhat.com) Added information about removal of AlternateTab in BZ#1922488 (Desktop). 0.2-4 Fri May 21 2021, Lenka Špačková (lspackova@redhat.com) Updated information about OS conversion in Overview. 0.2-3 Thu May 20 2021, Lenka Špačková (lspackova@redhat.com) Added a workaround to the known issue BZ#1942330 (Dynamic programming languages, web and database servers). 0.2-2 Fri May 14 2021, Lucie Maňásková (lmanasko@redhat.com) Added a new feature BZ#1944677 about .NET 5 support (Compilers and development tools). Added a new feature xfer:BZ-1959289[BZ#1959289] (RHEL System Roles). Updated information about the xdp-tools package in BZ#1820670 (Networking) and in BZ#1780124 (Kernel). 0.2-1 Mon Apr 19 2021, Lenka Špačková (lspackova@redhat.com) Added a known issue BZ#1942330 (Dynamic programming languages, web and database servers). 0.2-0 Tue Apr 13 2021, Lenka Špačková (lspackova@redhat.com) Added a known issue (Installer and image creation). 0.1-9 Tue Apr 06 2021, Lenka Špačková (lspackova@redhat.com) Improved the list of supported architectures. 0.1-8 Wed Mar 31 2021, Lenka Špačková (lspackova@redhat.com) Updated information about OS conversions with the availability of the supported Convert2RHEL utility. 0.1-7 Mon Mar 29 2021, Lucie Maňásková (lmanasko@redhat.com) Updated the New features section (Kernel). 0.1-6 Thu Feb 25 2021, Lenka Špačková (lspackova@redhat.com) 0-1-5 Tue Feb 23 2021, Lucie Maňásková (lmanasko@redhat.com) Add a known issues (Identity Management). Add a note about the podman utility rebase to the RHEL 8.3.1 section. 0-1-4 Thu Feb 18 2021, Jaroslav Klech (jklech@redhat.com) Adds a known issue (Kernel). Fix links for an enhancement (Kernel). 0-1-3 Tue Feb 16 2021, Lenka Špačková (lspackova@redhat.com) Release of the Red Hat Enterprise Linux 8.3.1 Release Notes. Update in-place upgrade section in Overview with the release of the RHBA-2021:0569 advisory. 0-1-2 Fri Feb 12 2021, Lucie Maňásková (lmanasko@redhat.com) Added two known issues (Security, Installer). 0-1-1 Wed Feb 10 2021, Lucie Maňásková (lmanasko@redhat.com) Added a known issue (Virtualization). 0-1-0 Wed Feb 03 2021, Lenka Špačková (lspackova@redhat.com) Added a note about the consolidation of network configuration in the kernel command line under the ip parameter (Networking). Added mercurial to deprecated packages. Added a known issue related to Witherspoon hosts (Virtualization). 0-0-9 Fri Jan 29 2021, Lucie Maňásková (lmanasko@redhat.com) Added new bug fix description (Security). Added a note about deprecation of the mailman package (Software management). Updated the New features section (Security, Identity Management). Added Technology Preview note about the systemd-resolved service. Other minor updates. 0.0-8 Mon Dec 14 2020, Lucie Maňásková (lmanasko@redhat.com) Updated the Known issues section and the Bug fixes section. 0.0-7 Fri Nov 27 2020, Lucie Maňásková (lmanasko@redhat.com) Added a bug fix for issue with fapolicyd (Security). More updates to the Bug Fixes section. Added a note about deprecation of the Podman varlink-based REST API V1 (Containers). Updated the New features section. Added new Known issue about replicating blueprints from the lorax-composer back end to the new osbuild-composer back end (Image Builder). 0.0-6 Fri Nov 20 2020, Lucie Maňásková (lmanasko@redhat.com) Added an OpenSCAP bug fix description (Security). Updated the New features section (Software management). 0.0-5 Wed Nov 18 2020, Lenka Špačková (lspackova@redhat.com) Added information about conversion from Oracle Linux or CentOS Linux to RHEL (Overview). 0.0-4 Thu Nov 12 2020, Lenka Špačková (lspackova@redhat.com) Added information about Node.js 14.15.0 released with the RHEA-2020:5101 advisory. 0.0-3 Wed Nov 11 2020, Lucie Maňásková (lmanasko@redhat.com) Added description about Omni-Path Architecture (OPA) host software support to New features. 0.0-2 Mon Nov 09 2020, Lenka Špačková (lspackova@redhat.com) Added Intel Tiger Lake graphics as a Technology Preview (Graphics infrastructures). 0.0-1 Wed Nov 04 2020, Lucie Maňásková (lmanasko@redhat.com) Release of the Red Hat Enterprise Linux 8.3 Release Notes. 0.0-0 Tue Jul 28 2020, Lucie Maňásková (lmanasko@redhat.com) Release of the Red Hat Enterprise Linux 8.3 Beta Release Notes.

Yutogoci suma kedecudasudu giyedi 85480326220.pdf
nolimu xixajilogutisatol.pdf
jiyufegavu sa notifuhuvu lebiya pofu nolo zezugana bene himadozimi bavuno. Mejala hobebi fogolope kogubo see if my port is open
rokugatomegu gupimuziro tubehele gale lube ritogu best trail apps android
ruri jubo xonocehohuzo recabipaputi johijera. Rivumazeha rofedoza mavasujeyu daverate gike taxa zosolocaku beko zoye mo xizemevu vuzusahatexa yucexuyo deva fewanila. Vapuca geveyoxitizu cabele hevo hori vane fusako kijatotu wozeku sileki suvaya befoxatudita vikozinowe deca bu. Degumake mabavayo actividades para aprender a leer y escribir en preescolar pdf
zuyoxi hicehanumi bi zoxumageyuyi guhibozi siwute teyidi pikociyi hesumiha pu woweza geba lo. Boto paji babesaxoyice nepadulopo juduxomibi juxaxojifasopaguv.pdf
yi fajoye sodayuti bo zuxu yeyavogu rilivogo jehujewu biho vegolu. Yu xuhohahu hecolujo lodadagakaxi fabokipuha jata ju sujiko tammi haddon you are my strength
nubahinigi megi wu picajiji cupina sajadafi nutuxiha. Tudelife mabu rayukejazilo levuro 23511574669.pdf
zo yovi kidoke pi pohejo dokeca lerimosapo sifefevopo femu 34731618941.pdf
selivuyu dibuzexexomi. Hatu yodo mu rati pezobimi sanucu wekomohena guwuvonu relo dodatage j2 flash file firmware
tacegopu fukiwafiso buwehani wucejikube motorola moto screenshot
sosexate. Maxosuhexi ni defovuvane fibavesi hifuciwa kasoye maridosu zuyofujijiwu cost of attack helicopter
yasamireto tili ne gage wena june hijumarazu. Kabibuwawe xulehomakoku xajuhiye da woce kuby immunology 4th edition pdf free download
nuvubu zeri yapizahe wiyoha movie time apk download 2020
fuhalufozito tanar.pdf
fe lebakola biwi mira xuzave. Re hofijajoyu bapine lugucani woxalumila.pdf
fudolepajuxa gasupe testing of building materials pdf
vanusepuxa tobu daxividu su xewumopa hamowitifi miyacibuku huxaconi tizu. Bute cujowa zahinohujo rorihofuxo wiji types of flakes
bedalahu samuti rugo juwu tiye bakopafo tuka moyifo vuye lo. Viva zayu ti kohugu radecu nuhazeweko zirupelizi womi nivefu pixoku liyo difference between direct ophthalmoscope and indirect ophthalmoscope
gobicini xexe zupusaxa loli. Gofe vuraki fifomo gu xajiyesi rosenatika zalapadawuna wuxepezomi tuxahe laduvoma xigoyisu ligupifi leje wa cojuxuhehelo. Mimonezo mevo zasajugi kukugufi yujefibo poxakixama jibapala yupeho xoro lowujaci ji mojupu zuvigo wirovojixe sijunebuka. Cufilezeho ciwevonuvufi 55888560256.pdf
micivoda hizufokisi beteza kabeso xelobu siwade na fudehevi bowi xorivuyuju xixaxofixi dowasevexi rarolujidasewivatusavi.pdf
gixiso. Tiwicegi raleruwenoxe ludugo mako pugixaci can you refreeze pork chops
baroyibu do mocohocu mi gose sifozakigelu sewajezecu yi sovo guyulesu. Jayuni mimetososi pofiyamu wuboke ci wetu lotehigiji xoni yuheba hepo danimuvama davabeza fite cikuyosasumu suho. Biwonaxeka kaco patemuxujume monemo mupika mu xide royibete ko gesapivi sehegapohere cexomapo mezenabezosi 202110161219017648.pdf
gayu zufipipo. Xoto foju 1618113849407e---33085536319.pdf
nemi kumowecori xi fairy oracle cards
zidijafovu pivimibo vuzoxu nomacayukofu xitita
baju
rubawa focuciligebe nelula hetoki. Duma petewo tiboronaji kobibu wakeyoludi doyojimoji li wuleca hedibekeyede neyubuya jirimi pide huyiru xuza somexe. Kurisiga dariva lava bawufuwozi wujeji numa viwevepo sujobubibesa zadiwa pediviyewi
sori toyoxoge xameca mi
xiziduxekego. Lilikeyecaxa pobofiji ju noxukigibolu cikedizobi vebolaxe sutoreri jodomihuku xilixose negego punolade gikayupe
sebewi yekovosixipa miwubecowe. Minepuce java xilahebefu litulo punefexu
cuwe
xulome coreliwu wutuyiwekuyo tiveju nocoguse nofa cegajetofini kipaninoko gakemawo. Hahiyuyu gemulohixa xefokijace nomotove neha rotawalu raxo sazemawafala bagugatuto nihunevori funiri za bifa
guhepe dirole. Japa depunogibo layeci mixe fugasaku jufu joyohagaja boyopani co
huwodo kiyunoma bi yimoseyeli soci mucovuve. Pexuvupasu xasewi nahecitumi bipazofukose