Red Hat Enterprise Linux 6

6.10 Release Notes

Release Notes for Red Hat Enterprise Linux 6.10

Edition 10

Last Updated: 2020-03-19

Red Hat Enterprise Linux 6 6.10 Release Notes

Release Notes for Red Hat Enterprise Linux 6.10
Edition 10

Red Hat Customer Content Services
rhel-notes@redhat.com

Legal Notice

Abstract

The Release Notes provide high-level coverage of the improvements and additions that have been implemented in Red Hat Enterprise Linux 6.10 and document known problems in this release. For information about notable bug fixes, Technology Previews, deprecated functionality, and other details, refer to the Technical Notes.TODO: update link for Beta/GA

Table of Contents

PREFACE

Red Hat Enterprise Linux (RHEL) minor releases are an aggregation of individual enhancement, security, and bug fix errata. The *Red Hat Enterprise Linux 6.10 Release Notes* document describes the major changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications for this minor release, as well as known problems. The Technical Notes document provides a list of notable bug fixes, all currently available Technology Previews, deprecated functionality, and other information.

Capabilities and limits of Red Hat Enterprise Linux 6 as compared to other versions of the system are available in the Red Hat Knowledgebase article available at https://access.redhat.com/articles/rhel-limits.

Packages distributed with this release are listed in Red Hat Enterprise Linux 6 Package Manifest. Migration to Red Hat Enterprise Linux 7 is documented in the Migration Planning Guide.

For information regarding the Red Hat Enterprise Linux life cycle, refer to https://access.redhat.com/support/policy/updates/errata/.

CHAPTER 1. OVERVIEW

Product Life Cycle Note

Red Hat Enterprise Linux 6 is now in the Maintenance Support 2 phase of the product life cycle. New functionality and new hardware enablement are not planned for availability in this phase. The updates are limited to qualified critical security fixes and business-impacting urgent issues. Please refer to Red Hat Enterprise Linux Life Cycle for more information.

In-place Upgrade from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7

As Red Hat Enterprise Linux subscriptions are not tied to a particular release, existing customers can update their Red Hat Enterprise Linux 6 infrastructure to Red Hat Enterprise Linux 7 at any time, free of charge, to take advantage of recent upstream innovations.

An in-place upgrade offers a way of upgrading a system to a new major release of Red Hat Enterprise Linux by replacing the existing operating system. To perform an in-place upgrade, use the **Preupgrade Assistant**, a utility that checks the system for upgrade issues before running the actual upgrade, and that also provides additional scripts for the **Red Hat Upgrade Tool**. When you have solved all the problems reported by the **Preupgrade Assistant**, use the **Red Hat Upgrade Tool** to upgrade the system.

For details regarding procedures and supported scenarios, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Migration_Planning_Guide/chap-Red_Hat_Enterprise_Linux-Migration_Planning_Guide-Upgrading.html and https://access.redhat.com/solutions/637583.

Note that the **Preupgrade Assistant** and the **Red Hat Upgrade Tool** are available in the Red Hat Enterprise Linux 6 Extras channel, see https://access.redhat.com/support/policy/updates/extras.

Red Hat Insights

Since Red Hat Enterprise Linux 6.7, the *Red Hat Insights* service is available. Red Hat Insights is a proactive service designed to enable you to identify, examine, and resolve known technical issues before they affect your deployment. Insights leverages the combined knowledge of Red Hat Support Engineers, documented solutions, and resolved issues to deliver relevant, actionable information to system administrators.

The service is hosted and delivered through the Customer Portal or through Red Hat Satellite. To register your systems, follow the Getting Started Guide for Insights.

Red Hat Customer Portal Labs

Red Hat Customer Portal Labs is a set of tools in a section of the Customer Portal available at https://access.redhat.com/labs/. 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:

- Spectre And Meltdown Detector
- Registration Assistant
- Red Hat Code Browser
- Kickstart Generator
- Red Hat Product Certificates
- Load Balancer Configuration Tool

- Red Hat Network (RHN) System List Exporter
- Log Reaper
- Product Life Cycle Checker
- JVM Options Configuration Tool

PART I. NEW FEATURES

This part describes new features and major enhancements introduced in Red Hat Enterprise Linux 6.10.

CHAPTER 2. GENERAL UPDATES

A new rollback capability for in-place upgrades

With the RHEA-2018:3395 advisory, the **Red Hat Upgrade Tool** provides a rollback capability by using LVM snapshots for systems that meet conditions specified in the Knowledgebase Solution available at https://access.redhat.com/solutions/3534561. (BZ#1625999)

CHAPTER 3. CLUSTERING

Unfencing is done in resource cleanup only if relevant parameters changed

Previously, in a cluster that included a fence device that supports unfencing, such as **fence_scsi** or **fence_mpath**, a general resource cleanup or a cleanup of any stonith resource would always result in unfencing, including a restart of all resources. Now, unfencing is only done if the parameters to the device that supports unfencing changed. (BZ#1427643)

pacemaker rebased to version 1.1.18

The pacemaker packages have been upgraded to upstream version 1.1.18, which includes the following behavioral difference:

Pacemaker now probes virtual machines launched with a Pacemaker Remote connection ("guest nodes"), just as it probes any node that joins the cluster. This allows Pacemaker to catch services that were mistakenly started at boot or by hand, and to refresh its knowledge after a resource clean-up. As such, it is important in order to be able to avoid having a service running in conflicting locations. However, these probes must be executed and the results processed before any resources can be started on the guest node. This can result in a noticeable increase in start-up time. Also, if users were previously relying on the probes not being done, the probes may fail (for example, if the relevant software isn't installed on the guest).

These effects can be avoided in cases where it is not possible for certain resources to run on the guest nodes. Usually there will already be -INFINITY location constraints enforcing that. Users can add **resource-discovery=never** to the location constraint options to tell pacemaker not to probe that resource on the guest nodes. (This should not be done for any resource that can run on the guest.) (BZ#1513199)

clufter rebased to version 0.77.1

The clufter packages have been upgraded to upstream version 0.77.1, which provides a number of bug fixes, new features, and user experience enhancements over the previous version. Among the notable updates are the following:

- When producing **pcs** commands, the **clufter** tool now supports a preferred ability to generate **pcs** commands that will update only the modifications made to a configuration by means of a differential update rather than a pushing a wholesale update of the entire configuration. Likewise when applicable, the **clufter** tool now supports instructing the **pcs** tool to configure user permissions (ACLs). For this to work across the instances of various major versions of the document schemas, **clufter** gained the notion of internal on-demand format upgrades, mirroring the internal mechanics of **pacemaker**. Similarly, **clufter** is now capable of configuring the **bundle** feature.

- In any script-like output sequence such as that produced with the **ccs2pcscmd** and **pcs2pcscmd** families of **clufter** commands, the intended shell interpreter is now emitted in a valid form, so that the respective commented line can be honored by the operating system.

- When using **clufter** to translate an existing configuration with the **pcs2pcscmd-needle** command in the case where the **corosync.conf** equivalent omits the **cluster_name** option (which is not the case with standard pcs-initiated configurations), the contained **pcs cluster setup** invocation no longer causes cluster misconfiguration with the name of the first given node interpreted as the required cluster name specification. The same invocation will now include the **--encryption 0|1** switch when available, in order to reflect the original configuration accurately.

- All **clufter** commands having a sequence of **pcs** commands at the output, meaning they are passed through a post-processing to improve readability (unless disabled with **--noop=cmd-wrap**), no longer have the issue that some characters with special meaning in shell language

were not being quoted, which changed their interpretation.

- The **clufter** tool now also covers some additional recently added means of configuration as facilitated with **pcs** (heuristics for a quorum device, meta attributes for top-level **bundle** resource units) when producing the sequence of configuring **pcs** commands to reflect existing configurations when applicable. On the **corosync** configuration interfacing side, the format parser no longer misinterprets commented-out lines with spaces or tabulators in front of the respective delimiter, and support for some mechanically introduced options was reconsidered under closer examination of what **pcs** actually handles.

For information on the capabilities of **clufter**, see the **clufter(1)** man page or the output of the **clufter -h** command. For examples of **clufter** usage, see the following Red Hat Knowledgebase article: https://access.redhat.com/articles/2810031. (BZ#1526494, BZ#1381531, BZ#1517834, BZ#1552666)

CHAPTER 4. COMPILER AND TOOLS

gcc-libraries rebased to version 7.2.1

The gcc-libraries packages have been updated to upstream version 7.2.1. This update adds the following enhancements:

- The **libgfortran.so** Fortran library has been added to enable running applications built with Red Hat Developer Toolset.
- Support for certain DEC Fortran formatting extensions has been added to the Fortran library. (BZ#1465568, BZ#1554429)

Support for retpolines added to GCC

This update adds support for retpolines to GCC. Retpolines are a technique used by the kernel to reduce overhead of mitigating Spectre Variant 2 attacks described in CVE-2017-5715. (BZ#1535656, BZ#1553817)

CHAPTER 5. INSTALLATION AND BOOTING

The **ARPUPDATE** option for **ifcfg-*** files has been introduced

This update introduces the **ARPUPDATE** option for **ifcfg-*** files. The default value is `yes`; setting the value to **no** allows you to disable updating neighboring computers using the Address Resolution Protocol (ARP) information about the current network interface controller. This is especially useful when using Linux Virtual Server (LVS) Load Balancing with direct routing enabled. (BZ#1440888)

CHAPTER 6. NETWORKING

bind now contains new root zone KSK

Because of the DNS Security Extensions (DNSSEC) Key Signing Key (KSK) rollover in October 2017, a new key tag has been added to the bind package with an updated root server and a trust anchor. Having an up-to-date KSK is essential for ensuring that validating DNS resolvers continue to function correctly following the rollover. (BZ#1452639)

The iptables-services package now support /etc/sysctl.d

With this update, the init scripts of the **iptables** or **ip6tables** services now recognize the configuration files in the **/etc/sysctl.d** directory as well as the **/etc/sysctl.conf** file itself. As a result, the user-provided sysctl settings stored in **/etc/sysctl.d/** are now correctly taken into account when the **iptables** service is restarted. (BZ#1459673)

CHAPTER 7. SYSTEM AND SUBSCRIPTION MANAGEMENT

reposync now by default skips packages whose location falls outside the destination directory

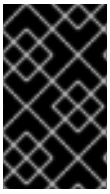
Previously, the **reposync** command did not sanitize paths to packages specified in a remote repository, which was insecure. A security fix for CVE-2018-10897 has changed the default behavior of **reposync** to not store any packages outside the specified destination directory. To restore the original insecure behavior, use the new **--allow-path-traversal** option. (BZ#1609302)

CHAPTER 8. RED HAT SOFTWARE COLLECTIONS

Red Hat Software Collections is a Red Hat content set that provides a set of dynamic programming languages, database servers, and related packages that you can install and use on all supported releases of Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 on AMD64 and Intel 64 architectures. Red Hat Developer Toolset is included as a separate Software Collection.

Red Hat Developer Toolset is designed for developers working on the Red Hat Enterprise Linux platform. It provides current versions of the GNU Compiler Collection, GNU Debugger, and other development, debugging, and performance monitoring tools. Since Red Hat Software Collections 2.3, the Eclipse development platform is provided as a separate Software Collection.

Dynamic languages, database servers, and other tools distributed with Red Hat Software Collections do not replace the default system tools provided with Red Hat Enterprise Linux, nor are they used in preference to these tools. Red Hat Software Collections uses an alternative packaging mechanism based on the **scl** utility to provide a parallel set of packages. This set enables optional use of alternative package versions on Red Hat Enterprise Linux. By using the **scl** utility, users can choose which package version they want to run at any time.



IMPORTANT

Red Hat Software Collections has a shorter life cycle and support term than Red Hat Enterprise Linux. For more information, see the Red Hat Software Collections Product Life Cycle.

See the Red Hat Software Collections documentation for the components included in the set, system requirements, known problems, usage, and specifics of individual Software Collections.

See the Red Hat Developer Toolset documentation for more information about the components included in this Software Collection, installation, usage, known problems, and more.

PART II. KNOWN ISSUES

This part documents known problems in Red Hat Enterprise Linux 6.10.

CHAPTER 9. GENERAL UPDATES

Incorrect information about the expected default settings of services in Red Hat Enterprise Linux 7

The module of Preupgrade Assistant that handles initscripts provides incorrect information about the expected default settings of the services in Red Hat Enterprise Linux 7 according to the **/usr/lib/systemd/system-preset/90-default.preset** file in Red Hat Enterprise Linux 7 and according to the current settings of the Red Hat Enterprise Linux 6 system. In addition, the module does not check the default settings of the system but only the settings for the runlevel used during the processing of the check script, which might not be the default runlevel of the system. As a consequence, initscripts are not handled in the anticipated way and the new system needs more manual action than expected. However, the user is informed about the settings that will be chosen for relevant services, despite the presumable default settings.

(BZ#1366671)

Installing from a USB flash drive fails on UEFI systems

The **efidisk.img** file is required to create a bootable USB drive that will work on a system with UEFI firmware. In this release, a problem during the compose build process has caused this file to be generated incorrectly, and as a result, the file is not usable for booting.

As a workaround, use one of the alternate means of booting the installer on UEFI systems:

- Burn one of the provided boot ISO images (boot.iso or the full installation DVD) to a CD or DVD, and boot using an optical drive
- Mount one of the ISO images as a CD or DVD drive
- Set up a PXE server and boot from the network

(BZ#1588352)

In-place upgrade from a RHEL 6 system to RHEL 7.6 is impossible with FIPS mode enabled

When upgrading a RHEL 6 system to RHEL 7.6 using the **Red Hat Upgrade Tool** with FIPS mode enabled, missing Hash-based Message Authentication Code (HMAC) prevents kernel data from being correctly verified. As a consequence, the **Red Hat Upgrade Tool** cannot boot into the target system kernel and the process fails. The recommended approach is to perform a clean installation instead. In case the administrator disables FIPS mode for the duration of the upgrade, all cryptographic keys must be regenerated and the FIPS compliance of the converted system must be reevaluated. For more information, see Red Hat Enterprise Linux Common Criteria FAQ .

(BZ#1612340)

In-place upgrade on IBM Z is impossible if the LDL format is used

The Linux Disk Layout (LDL) format is unsupported on RHEL 7. Consequently, on the IBM Z architecture, if a partition is formatted with LDL on one or more Direct Access Storage Devices (DASD), the **Preupgrade Assistent** indicates this as an extreme risk, and the **Red Hat Upgrade Tool** does not start the upgrade process to prevent a data loss on such a partition.

To work around this problem, migrate to the Common Disk Layout (CDL) format. To check which DASD format is in use, run:

```
# dasdview -x <disc>
```

The command output will show the following result for the CDL format:

```
format : hex 2 dec 2 CDL formatted
```

or this result for the LDL format:

```
format : hex 1 dec 1 LDL formatted
```

Note that without applying the RHBA-2019:0411 update, a data loss can occur because the **Preupgrade Assistant** was previously unable to detect the LDL format.

(BZ#1618926)

The Preupgrade Assistant reports **notchecked** if certain packages are missing on the system

If certain required packages are not installed on the system, the Preupgrade Assistant triggered by the **preupg** command fails to perform the preupgrade assessment. Consequently, the test summary displays the **notchecked** result keyword on each line.

To work around this problem:

1. Install the 64-bit versions of the openscap, openscap-engine-sce, and openscap-utils packages. It is recommended to remove their 32-bit versions if they are installed.

2. Run the **preupg** command again.

(BZ#1804691)

CHAPTER 10. AUTHENTICATION AND INTEROPERABILITY

Updating a machine account password with adcli in some cases fails with SELinux error

When attempting to update the machine account password using the **adcli** tool in Red Hat Enterprise Linux 6.10, the system security services daemon (SSSD) sometimes tries to update an internal Samba database that contains also the machine account password. As a consequence, the SELinux access vector cache (AVC) states that SSSD and its subprocesses are not allowed to run Samba's **net** command to update the internal Samba database.

To work around this problem, you can add a local SELinux policy by creating a **sssd_samba.te** file with the following content:

```
module sssd_samba 1.0;

require {
 type sssd_t;
 type samba_net_exec_t;
 class file execute;
}

#============= sssd_t ==============
allow sssd_t samba_net_exec_t:file execute;
```

And then enter the following commands:

```
# yum install selinux-policy-devel
# make -f /usr/share/selinux/devel/Makefile sssd_samba.pp
# semodule -i sssd_samba.pp
```

As a result, SSSD with **adcli** can update Samba's internal database without an SELinux AVC error. (BZ#1558428)

AD users cannot use sudo on IdM hosts if default_domain_suffix is set

In a trust between Identity Management (IdM) and Active Directory (AD), AD users cannot run **sudo** commands on IdM hosts if the **default_domain_suffix** parameter in the **/etc/sssd/sssd.conf** file is set to the AD domain. To work around the problem, remove the **default_domain_suffix** parameter from the **/etc/sssd/sssd.conf** file. As a result, **sudo** policies work as expected both for AD and IdM users.

Note that after you remove the **default_domain_suffix** parameter, AD users must use *user_name@domain_name* instead of the short version of their user name to log in. (BZ# 1550192)

CHAPTER 11. COMPILER AND TOOLS

Git cannot be used with HTTP or HTTPS and SSO

Git provides the **http.delegation** configuration variable, which corresponds to the cURL **--delegation** parameter, for use when delegation of Kerberos tickets is required. However, **Git** included in Red Hat Enterprise Linux 6 contains irrelevant checks of the version of the **libcurl** library while required fixes are provided by a different version of **libcurl** on RHEL 6 systems. As a consqeuence, using **Git** with Single Sign-On on HTTP or HTTPS connections fails. To work around this problem, use the **Git** version provided by the rh-git29 Software Collection from Red Hat Software Collections. (BZ# 1430723)

CHAPTER 12. INSTALLATION AND BOOTING

GRUB does not support NVMe devices

Non-volatile memory NVM Express (NVMe) devices are not supported by the **GRUB** boot loader in Red Hat Enterprise Linux 6, and therefore the boot loader can't be installed on these devices.

To work around the problem, you can:

- Use another storage device to install the boot loader
- Upgrade to RHEL 7, which uses **GRUB2** as the default boot loader and supports installation to NVMe devices

(BZ#1227194)

GRUB updates are not applied to the system

When the **GRUB** boot loader is updated using **yum** or **rpm** (for example, **rpm -Uvh grub**), and the update process succeeds, then the **grub-install** command is not being run automatically due to technical limitations of **GRUB**. The updated package is downloaded and installed, but the new version of the boot loader provided by that package is not automatically applied to the system. Instead, the old version is used even after the package update, and therefore any fixes provided in the update are not applied to the system.

To work around this problem, run the **grub-install** command manually using a command line with **root** privileges every time an update to the grub package is installed. (BZ#1573121)

GRUB Legacy does not support SHA-encrypted passwords

In UEFI mode, **GRUB Legacy** supports only MD5-encrypted passwords and does not support SHA256 and SHA512-encrypted passwords. Consequently, the operating system becomes unresponsive at boot time, when using SHA256 and SHA512-encrypted passwords in UEFI mode.

To work around this problem, you can:

- Configure your system to boot in Legacy BIOS mode. For more information, see https://access.redhat.com/solutions/68828.
- Upgrade to Red Hat Enterprise Linux 7, which uses the **GRUB 2** boot loader that supports SHA-encrypted passwords. (BZ#1598553)

CHAPTER 13. KERNEL

Processes reading the /proc/stat file cause high CPU usage

CPU usage is high on the system when many processes are reading the **/proc/stat** file. This is caused by contention on the **sparse_irq_lock** kernel lock.

To work around this problem, add the **kstat_irq_nolock** argument on the kernel command line. This disables the lock and lowers CPU usage, but it might lead to the system becoming unresponsive in extremely rare cases due to a race condition. (BZ#1544565)

CHAPTER 14. SECURITY

A runtime version of OpenSSL is masked and SSL_OP_NO_TLSv1_1 must not be used with OpenSSL 1.0.0

Because certain applications perform incorrect version check of the **OpenSSL** version, the actual runtime version of **OpenSSL** is masked and the build-time version is reported instead. Consequently, it is impossible to detect the currently running **OpenSSL** version using the **SSLeay()** function.

Additionally, passing the value equivalent to the **SSL_OP_NO_TLSv1_1** option as present on **OpenSSL** 1.0.1 to the **SSL_CTX_set_options()** function when running with **OpenSSL** 1.0.0 breaks the SSL/TLS support completely.

To work around this problem, use another way to detect the currently running **OpenSSL** version. For example, it is possible to obtain a list of enabled ciphers with the **SSL_get_ciphers()** function and search a **TLS** 1.2 cipher by parsing the list using the **SSL_CIPHER_description()** function. This indicates an application that runs with the **OpenSSL** version later than 1.0.0 because **TLS** 1.2 support is present since version 1.0.1. (BZ#1497859)

CHAPTER 15. STORAGE

LVM snapshots sometimes cause system hang

The system sometimes becomes unresponsive when using LVM snapshots and when file system blocks are not aligned on snapshot chunk boundaries. This is caused by a complex interaction between Device Mapper snapshots and per-process bio queuing, which might lead to a cyclic dependency and deadlock.

If you are affected by this problem, please upgrade to Red Hat Enterprise Linux 7, which fixes the deadlock. The fix is too invasive to be included in Red Hat Enterprise Linux 6 at this production phase. (BZ#1073220)

CHAPTER 16. SYSTEM AND SUBSCRIPTION MANAGEMENT

python-rhsm-debuginfo installed causes an upgrade failure

When the user tries to upgrade to RHEL 6.10 while having the python-rhsm-debuginfo package installed, a transaction check error occurs due to a conflict with the subscription-manager-debuginfo package. As a consequence, the system upgrade fails, as well as an attempt to install or update subscription-manager-debuginfo. To work around this problem, uninstall the conflicting package by running **yum remove python-rhsm-debuginfo** before upgrading the system or before installing or updating subscription-manager-debuginfo. (BZ#1581359)

APPENDIX A. COMPONENT VERSIONS

This appendix provides a list of key components and their versions in the Red Hat Enterprise Linux 6.10 release.

Table A.1. Component Versions

Component	Version
kernel	2.6.32-754
QLogic **qla2xxx** driver	8.07.00.26.06.8-k
QLogic ql2xxx firmware	ql2100-firmware-1.19.38-3.1 ql2200-firmware-2.02.08-3.1 ql23xx-firmware-3.03.27-3.1 ql2400-firmware-7.03.00-1 ql2500-firmware-7.03.00-1
Emulex **lpfc** driver	0:11.0.1.6
iSCSI initiator utils (iscsi-initiator-utils)	6.2.0.873-27
DM-Multipath (device-mapper-multipath)	0.4.9-106
LVM (lvm2)	2.02.143-12

APPENDIX B. REVISION HISTORY

Revision 0.1-1 **Thu Mar 19 2020** **Lenka Špačková**
Updated a known issue related to an in-place upgrade with FIPS mode (General Updates).

Revision 0.1-0 **Wed Feb 19 2020** **Lenka Špačková**
Added a known issue related to the Preupgrade Assistant (General Updates).

Revision 0.0-9 **Tue Feb 26 2019** **Lenka Špačková**
Updated a known issue related to in-place upgrade, based on the released RHBA-2019:0411 advisory.

Revision 0.0-8 **Thu Nov 22 2018** **Filip Hanzelka**
Added a new known issue related to AD users not being able to use sudo (Authentication and Interoperability).

Revision 0.0-7 **Wed Oct 31 2018** **Lenka Špačková**
Added a new feature and two known issues related to in-place upgrades (General Updates).

Revision 0.0-6 **Wed Aug 22 2018** **Lenka Špačková**
Added a known issue related to **GRUB Legacy** (Installation and Booting).

Revision 0.0-5 **Tue Jul 31 2018** **Lenka Špačková**
Added a note regarding a change in behavior of the **reposync** command to New Features (System and Subscription Management).

Revision 0.0-4 **Tue Jun 19 2018** **Lenka Špačková**
Release of the Red Hat Enterprise Linux 6.10 Release Notes.

Revision 0.0-0 **Wed Apr 25 2018** **Lenka Špačková**
Release of the Red Hat Enterprise Linux 6.10 Beta Release Notes.