



Red Hat Enterprise Linux 7 Примечания к выпуску 7.1

Примечания к выпуску Red Hat Enterprise Linux 7

Red Hat отдел пользовательской
документации

Red Hat Enterprise Linux 7 Примечания к выпуску 7.1

Примечания к выпуску Red Hat Enterprise Linux 7

Red Hat отдел пользовательской документации

Юридическое уведомление

Copyright © 2015 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Аннотация

В этом документе обсуждаются основные особенности Red Hat Enterprise Linux 7.1. Подробное обсуждение обновления Red Hat Enterprise Linux 6 до версии 7 можно найти в руководстве по планированию миграции. Благодарности Отдел глобальной поддержки Red Hat отдельно благодарит Стерлинга Александра и Майкла Эверетта за их неоценимую помощь в тестировании Red Hat Enterprise Linux 7.

Содержание

| | |
|---|-----------|
| Предисловие | 4 |
| Часть I. Новые возможности | 5 |
| Глава 1. Архитектура | 6 |
| 1.1. Red Hat Enterprise Linux для POWER (с прямым порядком байтов) | 6 |
| Глава 2. Hardware Enablement | 7 |
| 2.1. Intel Broadwell Processor and Graphics Support | 7 |
| 2.2. Support for TCO Watchdog and I2C (SMBUS) on Intel Communications Chipset 89xx Series | 7 |
| 2.3. Intel Processor Microcode Update | 7 |
| Глава 3. Установка и загрузка | 8 |
| 3.1. Программа установки | 8 |
| 3.2. Загрузчик | 12 |
| Глава 4. Хранение данных | 13 |
| Кэш LVM | 13 |
| LibStorageMgmt API | 13 |
| LSI Syncro | 13 |
| LVM API | 14 |
| Поддержка DIF/DIX | 14 |
| Device-mapper-multipath | 14 |
| Глава 5. Файловые системы | 15 |
| Btrfs | 15 |
| OverlayFS | 15 |
| pNFS | 15 |
| Глава 6. Ядро | 16 |
| Поддержка блочных устройств Serp | 16 |
| Обновление микропрограмм | 16 |
| Динамические исправления | 16 |
| Загрузка аварийного ядра с несколькими процессорами | 16 |
| Dm-era | 16 |
| Cisco VIC | 16 |
| Hwrng | 16 |
| Распределение нагрузки | 16 |
| Newidle | 17 |
| HugeTLB и выделение страниц размером 1 ГБ | 17 |
| Блокирование MCS | 17 |
| Размер стека процессов увеличен до 16 КБ | 17 |
| Uprobe и uretprobe с perf и systemtap | 17 |
| Сквозная проверка согласованности данных | 17 |
| Генератор псевдослучайных чисел в 32-битных системах | 17 |
| Размер crashkernel в Kdump | 17 |
| Глава 7. Виртуализация | 18 |
| Число виртуальных процессоров в KVM | 18 |
| Поддержка Intel Core 5-го поколения | 18 |
| Поддержка USB 3.0 | 18 |
| Dump-guest-memory | 18 |
| OVMF | 18 |
| Hyper-V | 18 |

| | |
|--|-----------|
| Hypervfscoreyd в hyperv-daemons | 18 |
| Libguestfs | 18 |
| Анализ производительности qemu-kvm | 19 |
| RDMA-based Migration of Live Guests | 19 |
| Глава 8. Кластеризация | 20 |
| Token_coefficient в Corosync | 20 |
| Auto_tie_breaker в Corosync | 20 |
| Red Hat High Availability | 20 |
| Глава 9. Компилятор и инструменты | 21 |
| Внесение изменений в бинарные функции System z | 21 |
| PAPI | 21 |
| OProfile | 21 |
| OpenJDK8 | 21 |
| Sosreport и snap | 21 |
| GDB и PowerPC 64-бит с прямым порядком байтов | 21 |
| Tuna | 21 |
| Глава 10. Сетевые возможности | 23 |
| Trusted Network Connect | 23 |
| SR-IOV и qlcnic | 23 |
| Фильтр пакетов Berkeley | 23 |
| Стабильность работы часов | 23 |
| Libnetfilter_queue | 23 |
| Libteam | 23 |
| Intel QuickAssist | 23 |
| Timemaster в комбинации PTP с NTP | 23 |
| Сценарии инициализации сетевых подключений | 24 |
| Отсрочка ответов ACK в TCP | 24 |
| NetworkManager | 24 |
| VTI | 24 |
| Конфигурация MemberOf | 24 |
| Глава 11. Linux Containers | 25 |
| 11.1. Components of docker Formatted Containers | 25 |
| 11.2. Advantages of Using Containers | 26 |
| 11.3. Сравнение с виртуальными машинами | 27 |
| 11.4. Using Containers on Red Hat Enterprise Linux 7.1 | 27 |
| 11.5. Containers with the LXC Format Have Been Deprecated | 27 |
| Глава 12. Аутентификация и функциональная совместимость | 29 |
| Manual Backup and Restore Functionality | 29 |
| Переход от WinSync к отношениям доверия | 29 |
| One-Time Password Authentication | 29 |
| Интеграция SSSD с CIFS | 29 |
| ipa-casert-manage renew | 29 |
| Контроль доступа на сервере IDM | 29 |
| Ограничение доступа к доменам | 29 |
| Автоматическая конфигурация провайдера данных | 30 |
| Провайдеры AD и LDAP для sudo | 30 |
| 32-bit Version of krb5-server and krb5-server-ldap Deprecated | 30 |
| Глава 13. Безопасность | 31 |
| Scap-security-guide | 31 |

| | |
|---|-----------|
| SELinux | 31 |
| OpenSSH | 31 |
| Libreswan | 31 |
| Trusted Network Connect | 32 |
| GnuTLS | 32 |
| Глава 14. Рабочее окружение | 33 |
| Поддержка стереоизображений Quad Buffered OpenGL | 33 |
| Провайдеры сетевых учетных записей | 33 |
| Глава 15. Поддержка работоспособности | 34 |
| Микроотчеты ABRT | 34 |
| Глава 16. Программные коллекции | 35 |
| Глава 17. Red Hat Enterprise Linux for Real Time | 36 |
| Часть II. Драйверы | 37 |
| Глава 18. Драйверы устройств хранения | 38 |
| Глава 19. Сетевые драйверы | 39 |
| Глава 20. Графические драйверы | 40 |
| Часть III. Known Issues | 41 |
| Глава 21. Installation and Booting | 42 |
| Глава 22. Networking | 43 |
| Глава 23. Authentication and Interoperability | 44 |
| Глава 24. Desktop | 45 |
| Приложение А. История переиздания | 46 |

Предисловие

Дополнительные версии Red Hat Enterprise Linux объединяют новые функции, исправления ошибок и безопасности. Этот документ содержит описание основных изменений в Red Hat Enterprise Linux 7.1 и сопровождающих программах, а также список известных конфликтов.



Важно

Последнюю версию *примечаний* можно найти на [сайте Red Hat](#). За информацией о других версиях Red Hat Enterprise Linux обратитесь к соответствующей версии примечаний.



Примечание

Полный список конфликтов можно найти в английской версии [примечаний к выпуску Red Hat Enterprise Linux 7.1](#).

Информацию о жизненном цикле Red Hat Enterprise Linux можно найти на странице: <https://access.redhat.com/support/policy/updates/errata/>.

Часть I. Новые возможности

Далее обсуждаются новые функции Red Hat Enterprise Linux 7.1.

Глава 1. Архитектура

Red Hat Enterprise Linux 7.1 предлагается в виде одного комплекта для нескольких архитектур [1]:

- ✦ 64-бит AMD,
- ✦ 64-бит Intel,
- ✦ IBM POWER7 и POWER8 (с обратным порядком байтов),
- ✦ IBM POWER8 (с прямым порядком байтов) [2],
- ✦ IBM System z [3].

Этот выпуск объединяет множество усовершенствований для серверов и рабочих станций, а также в целом улучшает работу с открытым кодом Red Hat.

1.1. Red Hat Enterprise Linux для POWER (с прямым порядком байтов)

В Red Hat Enterprise Linux 7.1 добавлена поддержка режима прямого порядка байтов для серверов IBM Power Systems с процессорами IBM POWER8. Это облегчает процесс переноса приложений между 64-битными платформами Intel (**x86_64**) и IBM Power Systems.

- ✦ Для установки Red Hat Enterprise Linux на IBM Power Systems с прямым порядком байтов предлагается отдельный носитель. Его можно найти в секции загрузки на портале пользователей Red Hat.
- ✦ Red Hat Enterprise Linux для POWER с прямым порядком байтов поддерживается только на платформах с процессорной архитектурой IBM POWER8.
- ✦ В настоящее время Red Hat Enterprise Linux для POWER с прямым порядком байтов поддерживается только в качестве виртуального гостя KVM под управлением **Red Hat Enterprise Virtualization**. Установка в физической системе не поддерживается.
- ✦ Для локальной и сетевой загрузки программы установки используется **GRUB2**. В [руководстве по установке](#) рассказывается, как настроить загрузочный сервер для клиентов IBM Power Systems.
- ✦ Пакеты Red Hat Enterprise Linux для IBM Power Systems доступны в двух вариантах — с прямым и обратным порядком байтов.
- ✦ Red Hat Enterprise Linux для POWER с прямым порядком байтов использует пакеты **ppc64le** (например, `gcc-4.8.3-9.ael7b.ppc64le.rpm`).

[1] Установка Red Hat Enterprise Linux 7.1 официально поддерживается только на 64-битных платформах, но Red Hat Enterprise Linux 7.1 допускает создание виртуальных машин с 32-битными операционными системами, включая предыдущие версии Red Hat Enterprise Linux.

[2] Red Hat Enterprise Linux 7.1 (с прямым порядком байтов) в настоящее время поддерживается только в качестве гостя KVM под управлением гипервизоров **Red Hat Enterprise Virtualization для Power** и **PowerVM**.

[3] Red Hat Enterprise Linux 7.1 поддерживает IBM zEnterprise 196 и выше, в то время как мэйнфреймы IBM System z10 больше не поддерживаются и не смогут загрузить Red Hat Enterprise Linux 7.1.

Глава 2. Hardware Enablement

2.1. Intel Broadwell Processor and Graphics Support

Red Hat Enterprise Linux 7.1 adds support for all current 5th generation Intel processors (code name Broadwell). Support includes the CPUs themselves, integrated graphics in both 2D and 3D mode, and audio support (Broadwell High Definition Legacy Audio, HDMI Audio and DisplayPort Audio).

The **turbostat** tool (part of the *kernel-tools* package) has also been updated with support for the new processors.

2.2. Support for TCO Watchdog and I2C (SMBUS) on Intel Communications Chipset 89xx Series

Red Hat Enterprise Linux 7.1 adds support for TCO Watchdog and I2C (SMBUS) on the 89xx series Intel Communications Chipset (formerly Coletto Creek).

2.3. Intel Processor Microcode Update

CPU microcode for Intel processors in the *microcode_ctl* package has been updated from version **0x17** to version **0x1c** in Red Hat Enterprise Linux 7.1.

Глава 3. Установка и загрузка

3.1. Программа установки

Anaconda была доработана с целью оптимизации процесса установки Red Hat Enterprise Linux 7.1.

Интерфейс

- ✦ Графический процесс установки теперь включает этап настройки **Kdump**, который раньше настраивался в ходе выполнения **firstboot**. Как следствие, при отсутствии графического интерфейса настроить **Kdump** было невозможно. Окно **Kdump** можно открыть из главного меню установки.

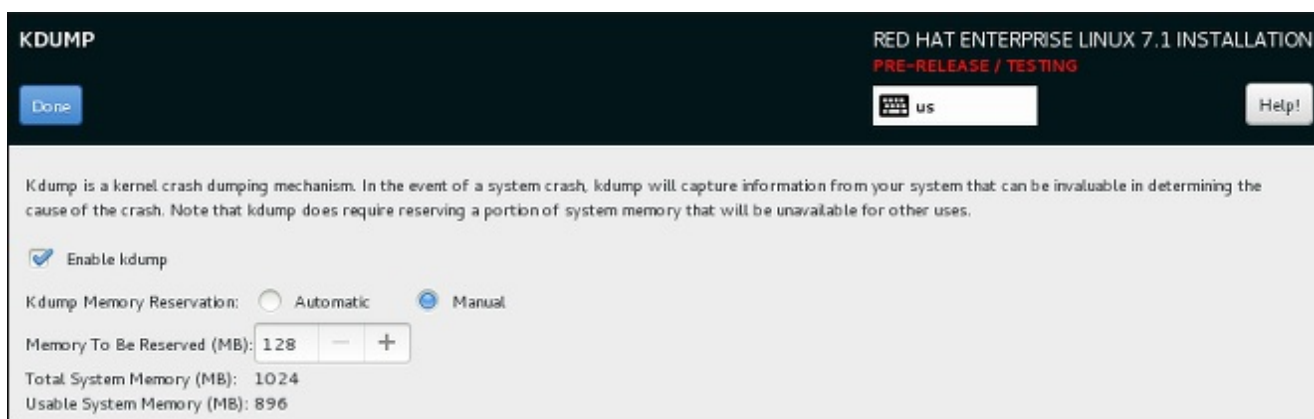


Рисунок 3.1. Окно kdump

- ✦ Окно разделов было доработано, поэтому порядок элементов несколько изменился.

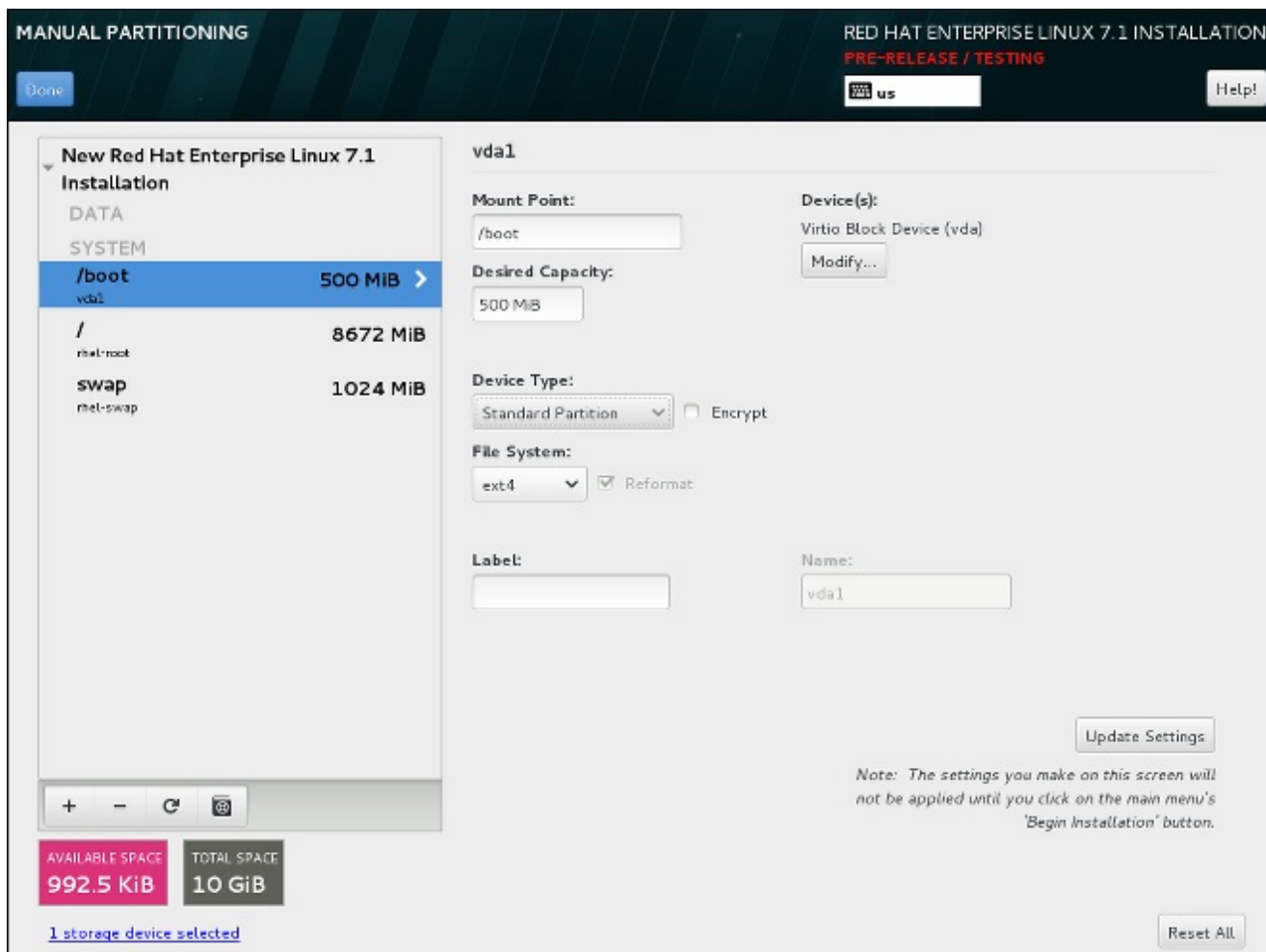


Рисунок 3.2. Окно создания разделов

- ❖ Сетевые мосты настраиваются в окне **Сеть и имя узла**. Нажмите кнопку со знаком **+** под списком интерфейсов, выберите **Мост** из выпадающего списка и в открывшемся диалоге введите необходимую информацию. Окно диалога предоставляется программой **NetworkManager** и подробно обсуждается в *сетевом руководстве Red Hat Enterprise Linux 7.1*.

Для конфигурации мостов были добавлены новые параметры кикстарта.

- ❖ Журналы установки теперь на панель **tmux** в **tty1**, не на разные консоли. Для перехода к **tmux** нажмите **Ctrl+Alt+F1**, а для переключения между окнами используйте комбинацию **Ctrl+b X** (где X — номер окна).

Чтобы вернуться к процессу установки, нажмите **Ctrl+Alt+F6**.

- ❖ Текстовая версия **Anaconda** теперь включает подробную справку. Чтобы ее открыть, выполните команду **anaconda -h**. В текстовом режиме **Anaconda** можно запустить в уже установленной системе, что часто используется для установки из дисковых образов.

Команды и параметры кикстарта

- ❖ Добавлен параметр **--profile=** команды **logvol**, с помощью которого можно определить профиль конфигурации динамических логических томов. Имя профиля будет также добавлено в метаданные тома.

По умолчанию будет создано два профиля (**default** и **thin-performance**), которые будут сохранены в `/etc/lvm/profile`. Подробную информацию можно найти на справочной странице **lvm(8)**.

- ✦ The behavior of the `--size=` and `--percent=` options of the **logvol** command has changed. Previously, the `--percent=` option was used together with `--grow` and `--size=` to specify how much a logical volume should expand after all statically-sized volumes have been created.

Starting with Red Hat Enterprise Linux 7.1, `--size=` and `--percent=` can not be used on the same **logvol** command.

- ✦ Аргумент `--autoscreenshot` команды **autostep** теперь работает как положено и сохраняет снимки экрана на каждом этапе установки в каталог `/tmp/anaconda-screenshots`. После завершения установки снимки будут перенесены в `/root/anaconda-screenshots`.
- ✦ **liveimg** теперь поддерживает установку из архивов `.tar`, `.tbz`, `.tgz`, `.txz`, `.tar.bz2`, `.tar.gz` и `.tar.xz`. Архив должен содержать корневую файловую систему установочного носителя.
- ✦ Для конфигурации мостов были добавлены новые параметры команды **network**:
 - `--bridgeslaves=`: определяет устройства, которые войдут в состав моста `--device=`.
Пример:

```
network --device=bridge0 --bridgeslaves=em1
```

- `--bridgeopts=`: список дополнительных параметров для подключаемого через мост интерфейса. Доступные параметры: **stp**, **priority**, **forward-delay**, **hello-time**, **max-age**, **ageing-time**. Их описание можно найти на справочной странице **nm-settings(5)**.
- ✦ Новый параметр `--fstype` команды **autopart** позволяет изменить тип файловой системы при автоматическом создании разделов (по умолчанию используется **xfs**).
- ✦ Several new features were added to Kickstart for better container support. These features include:
 - **repo** `--install` сохраняет конфигурацию репозитория в `/etc/yum.repos.d/`. Если не задан, используемые в процессе установки репозитории не сохраняются в установленной системе.
 - **bootloader** `--disabled` отменяет установку загрузчика.
 - `%packages` `--nocore` отменяет установку группы пакетов `@core`. Обычно используется для выполнения минимальной установки в контейнерах.

Please note that the described options are only useful when combined with containers, and using the options in a general-purpose installation could result in an unusable system.

Entropy Gathering for LUKS Encryption

- ✦ If you choose to encrypt one or more partitions or logical volumes during the installation (either during an interactive installation or in a Kickstart file), **Anaconda** will attempt to gather 256 bits of entropy (random data) to ensure the encryption is secure. The installation will continue after 256 bits of entropy are gathered or after 10 minutes. The attempt to gather entropy happens at the beginning of the actual installation phase when encrypted partitions or volumes are being created. A dialog window will open in the graphical interface, showing progress and remaining time.

The entropy gathering process can not be skipped or disabled. However, there are several ways to speed the process up:

- If you can access the system during the installation, you can supply additional entropy by pressing random keys on the keyboard and moving the mouse.
- If the system being installed is a virtual machine, you can attach a *virtio-rng* device (a virtual random number generator) as described in the [Red Hat Enterprise Linux 7.1 Virtualization Deployment and Administration Guide](#).

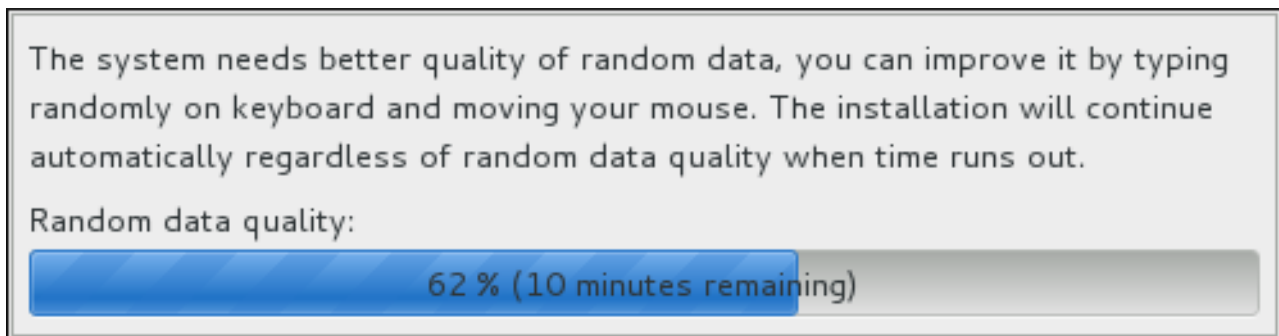


Рисунок 3.3. Gathering Entropy for Encryption

Встроенная справка в графическом режиме

В правом верхнем углу окна в графическом режиме установки доступна кнопка справки, которая откроет соответствующую секцию [руководства по установке](#) в окне **Yelp**.

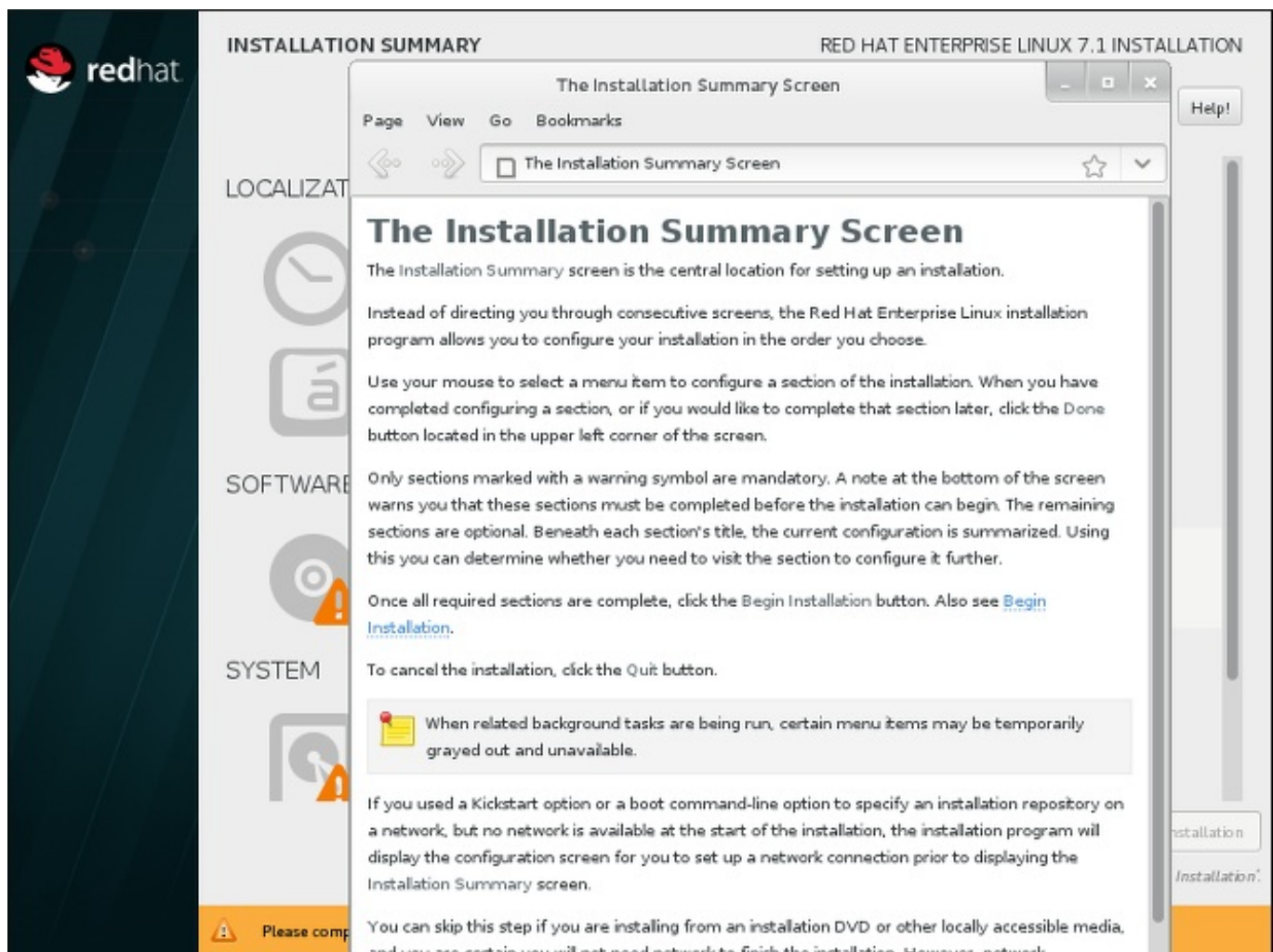


Рисунок 3.4. Anaconda built-in help

3.2. Загрузчик

Установочный носитель для IBM Power Systems теперь включает **GRUB2** вместо **yaboot**. Red Hat Enterprise Linux для POWER с прямым порядком байтов тоже требует **GRUB2**, в то время как комплект с обратным порядком байтов может использовать оба загрузчика, хотя **GRUB2** является более предпочтительным.

В [руководство по установке](#) добавлена информация о подготовке загрузочного сервера для загрузки IBM Power Systems при помощи **GRUB2**.

Глава 4. Хранение данных

Кэш LVM

As of Red Hat Enterprise Linux 7.1, LVM cache is fully supported. This feature allows users to create logical volumes with a small fast device performing as a cache to larger slower devices. Please refer to the **lvm(7)** manual page for information on creating cache logical volumes.

На подобное кэширование накладывается несколько ограничений:

- Том кэша должен располагаться на верхнем уровне устройства и не может использоваться как динамический том, образ RAID или любой другой подтип логических томов.
- The cache LV sub-LVs (the origin LV, metadata LV, and data LV) can only be of linear, stripe, or RAID type.
- После создания тома его параметры уже нельзя будет изменить. Чтобы это сделать, надо будет его удалить и создать заново с новыми параметрами.

LibStorageMgmt API

Red Hat Enterprise Linux 7.1 теперь официально поддерживает **libStorageMgmt** API, который позволяет программно управлять хранилищами разных производителей и эффективно использовать их функции аппаратного ускорения. **LibStorageMgmt** предоставляет команды для автоматизации задач управления хранилищем и необходимые функции для его ручной настройки. При этом поддержка модуля **Targetd** осталась на уровне экспериментальной.

- NetApp Filer (ontap 7-Mode);
- Nexenta (nstor 3.1.x);
- SMI-S:
 - HP ZPAR;
 - ОС 3.2.1 и выше;
 - EMC VMAX и VNX:
 - Solutions Enabler 7.6.2.48 и выше;
 - провайдер SMI-S 4.6.2.18 и выше;
 - внешний провайдер массива HDS VSP;
 - Hitachi Command Suite 8.0 и выше.

Подробную информацию о **libStorageMgmt** можно найти в [руководстве по управлению пространством данных](#).

LSI Syncro

Драйвер **megaraid_sas** теперь включает код активации адаптеров LSI Syncro CS HA-DAS (High-Availability Direct-Attached Storage). Несмотря на то что **megaraid_sas** полностью поддерживается в Red Hat Enterprise Linux 7.1, его поддержка для Syncro CS предлагается только в экспериментальном варианте, поэтому компании Red Hat и LSI продолжают принимать отзывы пользователей. За дальнейшей информацией обратитесь к <http://www.lsi.com/products/shared-das/pages/default.aspx>.

LVM API

Red Hat Enterprise Linux 7.1 предоставляет экспериментальный API для управления LVM.

Подробную информацию можно найти в `lvm2app.h`.

Поддержка DIF/DIX

Red Hat Enterprise Linux 7.1 предоставляет экспериментальные функции для обеспечения целостности данных на уровне стандарта SCSI. DIF/DIX увеличивает стандартный размер блока с 512 до 520 байт и добавляет поле целостности (DIF, Data Integrity Field). В этом поле хранится контрольная сумма блока данных, рассчитываемая HBA-адаптером в момент записи. Запоминающее устройство подтверждает сумму при получении и сохраняет ее вместе с данными. Во время чтения контрольная сумма будет проверяться устройством данных и HBA-адаптером.

For more information, refer to the section Block Devices with DIF/DIX Enabled in the [Storage Administration Guide](#).

Device-mapper-multipath

Если `device-mapper-multipath` обнаружил пустые строки во время проверки файла `multipath.conf`, они будут пропущены, а на экран будет выведено сообщение об ошибке.

В команде `multipathd show paths format` допускается использование подстановок:

- ✦ %N и %n для WWNN-идентификатора хоста и целевого узла Fibre Channel соответственно;
- ✦ %R и %r для WWPN-идентификатора хоста и целевого узла Fibre Channel соответственно.

Это значительно упрощает настройку многопутевых схем хостов Fibre Channel, целевых устройств и портов.

Глава 5. Файловые системы

Btrfs

Red Hat Enterprise Linux 7.1 включает пилотную версию файловой системы **Btrfs** (B-Tree) с усовершенствованными функциями управления, масштабирования и надежности. Btrfs поддерживает снимки файловой системы, возможности сжатия и интегрированного управления устройствами.

OverlayFS

The **OverlayFS** file system service allows the user to "overlay" one file system on top of another. Changes are recorded in the upper file system, while the lower file system becomes read-only. This can be useful because it allows multiple users to share a file system image, for example containers, or when the base image is on read-only media, for example a DVD-ROM.

On Red Hat Enterprise Linux 7.1, OverlayFS is supported as a Technology Preview. There are currently two restrictions:

- ✦ It is recommended to use **ext4** as the lower file system; the use of **xf**s and **gfs2** file systems is not supported.
- ✦ SELinux is not supported, and to use OverlayFS, it is required to disable enforcing mode.

pNFS

pNFS (Parallel NFS) является спецификацией стандарта NFS v4.1 для реализации параллельного доступа к данным на распределенных серверах NFS, что повышает производительность и облегчает их масштабирование.

pNFS defines three different storage protocols or layouts: files, objects, and blocks. The client supports the files layout, and with Red Hat Enterprise Linux 7.1, the blocks and object layouts are fully supported.

Red Hat при сотрудничестве с партнерами и другими открытыми проектами продолжает работу по стандартизации новых типов pNFS с целью обеспечения их полной поддержки.

За дальнейшей информацией обратитесь к <http://www.pnfs.com/>.

Глава 6. Ядро

Поддержка блочных устройств Ceph

Новые модули ядра **libceph.ko** и **rbd.ko** показывают блочные устройства Ceph как обычные устройства, которые могут быть смонтированы в каталог и отформатированы (например, как **XFS** или **ext4**).

Модуль **ceph.ko** больше не поддерживается.

Обновление микропрограмм

В Red Hat Enterprise Linux 7.1 на платформах IBM System z включены обновления на микропрограммном уровне. Их параллельная установка не приведет к снижению скорости операций ввода-вывода флэш-накопителя. Пользователь будет уведомлен о сделанных изменениях.

Динамические исправления

Добавлена экспериментальная поддержка **kpatch** на платформах AMD64 и Intel 64 для применения исправлений к ядру на лету без необходимости перезагрузки системы.

Загрузка аварийного ядра с несколькими процессорами

Red Hat Enterprise Linux 7.1 разрешает использование нескольких процессоров при загрузке аварийного ядра. Эта функциональность предоставляется на экспериментальном уровне.

Dm-era

Red Hat Enterprise Linux 7.1 поддерживает экспериментальный модуль **dm-era** для **device-mapper**, который обычно используется в комбинации с **dm-cache** и отслеживает изменения блоков за заданный промежуток времени. Отсчет времени ведет 32-разрядный счетчик. Программы резервного копирования могут использовать **dm-era** для контроля блоков, которые были изменены со времени последнего копирования. Также **dm-era** поможет частично освободить кэш в ходе отката к исходному снимку.

Cisco VIC

Добавлена экспериментальная поддержка драйвера ядра Cisco VIC Infiniband для реализации удаленного прямого доступа к памяти (RDMA, Remote Direct Memory Access) на платформах Cisco.

Hwrng

В Red Hat Enterprise Linux 7.1 было оптимизировано использование аппаратных генераторов случайных чисел (**hwrng**) виртуальными гостями Linux. Раньше в гостевой системе надо было запустить **rngd** и предоставить доступ к пулу энтропии ядра. Теперь этот шаг не требуется, а в случае снижения энтропии до заданного уровня **khwrngd** получит ее из **virtio-rng**. Прозрачность такого подхода помогает эффективно использовать преимущества аппаратных генераторов случайных чисел хоста KVM.

Распределение нагрузки

Раньше при балансировке нагрузки планировщик учитывал все бездействующие процессоры. В Red Hat Enterprise Linux 7.1 незанятый процессор будет задействован, только если достигнут порог простоя. Такой подход сокращает число лишних операций распределения нагрузки, тем самым повышая производительность планировщика.

Newidle

При отсутствии готовых к запуску задач планировщик прекратит их поиск в коде баланса **newidle**, что положительно скажется на производительности.

HugeTLB и выделение страниц размером 1 ГБ

Red Hat Enterprise Linux 7.1 поддерживает возможность выделения страниц памяти размером 1 ГБ во время работы системы. Помимо этого, пользователь сам сможет выбрать узел NUMA, на котором будет выделена страница.

Блокирование MCS

Новый механизм блокирования MCS значительно снижает накладные расходы **spinlock** в больших системах, что повышает эффективность блокировки.

Размер стека процессов увеличен до 16 КБ

С целью оптимизации работы больших процессов размер стека был увеличен с 8 КБ до 16 КБ.

Uprobe и uretprobe с perf и systemtap

Uprobe и **uretprobe** теперь правильно работают с **perf** и **systemtap**.

Сквозная проверка согласованности данных

Red Hat Enterprise Linux 7.1 поддерживает сквозную проверку согласованности данных на платформах IBM System z, что эффективно снижает риск их потери.

Генератор псевдослучайных чисел в 32-битных системах

Red Hat Enterprise Linux 7.1 допускает использование генератора псевдослучайных чисел в 32-битных системах.

Размер crashkernel в Kdump

The **Kdump** kernel crash dumping mechanism on systems with large memory, that is up to the Red Hat Enterprise Linux 7.1 maximum memory supported limit of 6TB, has become fully supported in Red Hat Enterprise Linux 7.1.

Глава 7. Виртуализация

Число виртуальных процессоров в KVM

Максимальное число виртуальных процессоров для гостей KVM увеличено до 240.

Поддержка Intel Core 5-го поколения

Гипервизор QEMU, код ядра KVM и **libvirt** API поддерживают процессоры Intel Core 5-го поколения. Это позволяет использовать инструкции ADCX, ADOX, RDSFEED, PREFETCHW и SMAP.

Поддержка USB 3.0

Добавлена экспериментальная поддержка эмуляции контроллера USB 3.0 (xHCI).

Dump-guest-memory

Dump-guest-memory теперь поддерживает сжатие дампа памяти. От этого особенно выиграют пользователи, которые по какой-либо причине не могут использовать **virsh dump**, экономя не только место, но и время, которое будет затрачено на запись дампа.

OVMF

В Red Hat Enterprise Linux 7.1 добавлена экспериментальная поддержка OVMF (Open Virtual Machine Firmware) — защищенной среды загрузки UEFI для гостей AMD64 и Intel 64.

Hyper-V

Драйвер Hyper-V оптимизирован с целью повышения производительности сети. Теперь он поддерживает функции RSS (Receive Side Scaling), LSO (Large Send Offload) и ввод-вывод с рассеиванием/сборкой.

Hypervfsd в hyperv-daemons

В комплект *hyperv-daemons* был добавлен **hypervfsd**, реализующий функциональность копирования файлов с хоста Hyper-V 2012 R2 в гостевую систему Linux по VMBUS.

Libguestfs

Библиотека **libguestfs** предлагает несколько новых инструментов для управления образами виртуальных машин.

Новые инструменты

- ✦ **virt-builder** — утилита для сборки образов виртуальных машин.
- ✦ **virt-customize** — утилита для модификации образов виртуальных машин (установки пакетов, редактирования файлов конфигурации, выполнения сценариев и изменения паролей).
- ✦ **virt-diff** — сравнение файловых систем двух виртуальных машин. Позволяет с легкостью определить файлы, которые изменились со времени создания снимка.
- ✦ **virt-log** — утилита просмотра журналов гостевых систем (в том числе Linux и Windows).

- ✦ **virt-v2v** — утилита для преобразования гостей, управляемых внешним гипервизором, с целью передачи управления KVM с libvirt, OpenStack, oVirt, Red Hat Enterprise Virtualization (RHEV) и др. В настоящее время virt-v2v может преобразовать гостевые системы Red Hat Enterprise Linux и Windows, работающие на Xen и VMware ESX.

Анализ производительности qemu-kvm

Support for flight recorder tracing has been introduced in Red Hat Enterprise Linux 7.1. Flight recorder tracing uses **SystemTap** to automatically capture qemu-kvm data as long as the guest machine is running. This provides an additional avenue for investigating qemu-kvm problems, more flexible than qemu-kvm core dumps.

Подробнее о мониторинге производительности рассказывается в [руководстве по внедрению и администрированию виртуализации](#).

RDMA-based Migration of Live Guests

The support for Remote Direct Memory Access (RDMA)-based migration has been added to **libvirt**. As a result, it is now possible to use the new **rdma://** migration URI to request migration over RDMA, which allows for significantly shorter live migration of large guests. Note that prior to using RDMA-based migration, RDMA has to be configured and **libvirt** has to be set up to use it.

Глава 8. Кластеризация

Token_coefficient в Corosync

Новый параметр **token_coefficient** для **Corosync Cluster Engine** используется только в том случае, если секция **odelist** определена и содержит как минимум 3 узла. Расчет времени ожидания производится по формуле:

$$[\text{токен} + (\text{число_узлов} - 2)] * \text{коэффициент}$$

Это позволяет наращивать кластер без необходимости ручной коррекции времени ожидания после добавления нового узла. По умолчанию интервал равен 650 миллисекундам. Нулевое значение отключит эту функцию.

Таким образом, **Corosync** с легкостью адаптируется к добавлению и удалению узлов.

Auto_tie_breaker в Corosync

Функциональность **auto_tie_breaker** была дополнена: теперь пользователь сможет сам выбрать набор узлов, который получит кворум при распаде кластера на равные части. По умолчанию будет выбрана часть, содержащая узел с наименьшим идентификатором.

Red Hat High Availability

Ниже перечислены основные изменения комплекта **Red Hat High Availability**.

- ✦ **pcs resource cleanup** теперь может сбрасывать значение **failcount** и статус всех ресурсов.
- ✦ С помощью параметра **lifetime** команды **pcs resource move** можно настроить срок действия ограничений, автоматически накладываемых на ресурсы при выполнении этой команды.
- ✦ Разрешения чтения и записи конфигурации кластера можно настроить при помощи команды **pcs acl**.
- ✦ **pcs constraint** позволяет настроить не только общие, но и индивидуальные параметры ограничений кластерных ресурсов.
- ✦ Параметр **disabled** команды **pcs resource create** запрещает автоматический запуск созданного ресурса.
- ✦ **pcs cluster quorum unblock** означает, что кластер не будет дожидаться установки кворума всеми узлами.
- ✦ Параметры **before** и **after** команды **pcs resource create** позволяют изменить порядок групп ресурсов.
- ✦ Параметры **backup** и **restore** команды **pcs config** отвечают за создание и восстановление архива файлов конфигурации кластера на всех узлах.

Глава 9. Компилятор и инструменты

Внесение изменений в бинарные функции System z

GCC (GNU Compiler Collection) теперь позволяет вносить исправления на лету в многопоточный код бинарных функций System z. Параметр командной строки **-mhotpatch** включает эту функциональность для всех функций, в то время как для конкретной функции это поведение можно контролировать с помощью атрибута `hotpatch`.

Так как применение исправлений в процессе работы отрицательно влияет на производительность, не рекомендуется использовать **-mhotpatch**, а разрешать это для отдельных функций по мере необходимости.

В Red Hat Enterprise Linux 7.1 эта функциональность поддерживается полностью.

PAPI

Red Hat Enterprise Linux 7 поддерживает PAPI (Performance Application Programming Interface) — кроссплатформенный интерфейс для анализа производительности современных микропроцессоров. Для отслеживания событий PAPI использует счетчики, представляющие собой наборы регистров, что широко применяется для анализа и оптимизации производительности.

In Red Hat Enterprise Linux 7.1 PAPI and the related **libpfm** libraries have been enhanced to provide support for IBM Power8, Applied Micro X-Gene, ARM Cortex A57, and ARM Cortex A53 processors. In addition, the events sets have been updated for Intel Haswell, Ivy Bridge, and Sandy Bridge processors.

OProfile

OProfile — средство профилирования систем Linux для сбора статистики в фоновом режиме. В Red Hat Enterprise Linux 7.1 вошла версия **OProfile**, совместимая с процессорами Intel Atom C2XXX, Intel Core 5-го поколения, IBM Power8, AppliedMicro X-Gene и ARM Cortex A57.

OpenJDK8

Red Hat Enterprise Linux 7.1 включает пакеты *java-1.8.0-openjdk* с последней версией открытой реализации Java SE 8 — OpenJDK 8. Эти пакеты могут устанавливаться параллельно с *java-1.7.0-openjdk*.

Java 8 предоставляет множество новых функций, в том числе новые стандартные методы, лямбда-выражения, Stream API, JDBC 4.2, аппаратную поддержку AES и др. Другие усовершенствования и исправления OpenJDK8 оптимизируют производительность при разработке и запуске программ Java.

Sosreport и snap

Функциональность устаревшей программы **snap** из пакета *powerpc-utils* была интегрирована в **sosreport**.

GDB и PowerPC 64-бит с прямым порядком байтов

GDB теперь поддерживает 64-битную архитектуру PowerPC с прямым порядком байтов (от младшего к старшему).

Tuna

При помощи утилиты **Tuna** можно корректировать регулируемые параметры планировщика, в том числе правила планирования, приоритет RT, привязку к процессорам и т.п. Улучшенный интерфейс **Tuna** теперь запрашивает авторизацию root при запуске — таким образом, не требуется запускать рабочий стол в режиме root, чтобы запустить **Tuna**. Подробное обсуждение можно найти в [руководстве пользователя Tuna](#).

Глава 10. Сетевые возможности

Trusted Network Connect

В Red Hat Enterprise Linux 7.1 добавлена экспериментальная поддержка стандарта TNC (Trusted Network Connect), используемого в комбинации с TLS, 802.1X и IPsec для защиты конечных узлов. TNC проверяет статистику системы (данные о конфигурации операционной системы, списки установленных пакетов и т.п.) и определяет уровень доступа к сети по результатам анализа.

SR-IOV и qlcnic

Драйвер **qlcnic** поддерживает экспериментальный вариант технологии SR-IOV (Single Root I/O Virtualization). Эта функциональность предоставляется на базе QLogic, поэтому отзывы и предложения следует отправлять Red Hat и QLogic. Остальные функции **qlcnic** поддерживаются полностью.

Фильтр пакетов Berkeley

В Red Hat Enterprise Linux 7.1 добавлена поддержка анализаторов трафика на базе BPF (Berkeley Packet Filter). BPF используется для фильтрации пакетов на уровне сокетов, а также в `sscmp` и `Netfilter`. Богатый синтаксис BPF предлагает широкие возможности по созданию фильтров.

Стабильность работы часов

Раньше отключение режима динамических прерываний могло улучшить работу системных часов (с помощью параметра ядра **nohz=off**). В ядре Red Hat Enterprise Linux 7.1 стабильность работы системных часов была существенно оптимизирована и **nohz=off** не имеет большого значения. Это особенно улучшает эффективность программ синхронизации времени, использующих **PTP** и **NTP**.

Libnetfilter_queue

Библиотека **libnetfilter_queue** предоставляет API для управления пакетами, которые были поставлены в очередь фильтром пакетов ядра. Функции включают извлечение пакетов из очереди подсистемы **nfnetlink_queue**, их анализ, изменение заголовков и вставку уже измененных пакетов.

Libteam

libteam обновлен до версии **1.14-1** и включает целый ряд исправлений и дополнений. Так, в частности, **systemd** теперь может автоматически запускать **teamd**, что в целом повышает производительность.

Intel QuickAssist

Добавлен драйвер Intel QAT (QuickAssist Technology) для поддержки оборудования QuickAssist, что позволяет интегрировать аппаратные функции ускорения в программный дизайн с целью повышения производительности.

Timemaster в комбинации PTP с NTP

Пакет *linuxptp* обновлен до версии **1.4**. Среди прочего, он поддерживает переход от синхронизации часов с доменами **PTP** к **NTP** при помощи **timemaster**. При наличии нескольких доменов **PTP** или при необходимости отката к **NTP**, **timemaster** выберет наиболее точный источник времени из доступных

вариантов.

Сценарии инициализации сетевых подключений

Red Hat Enterprise Linux 7.1 допускает использование произвольных имен VLAN. Поддержка **IPv6** в туннелях GRE улучшена: внутренний адрес после перезагрузки не меняется.

Отсрочка ответов ACK в TCP

lproute позволяет отсрочить отправку ACK, сгруппировав его с другими ответами ACK, тем самым сократив нагрузку. Эти функции контролируются командой **ip route quickack**.

NetworkManager

NetworkManager в Red Hat Enterprise Linux 7.1 поддерживает параметр **lACP_rate**. Также существенно упрощено переименование устройств при переименовании мастер-интерфейса и подчиненных интерфейсов.

Если при попытке автоматического подключения **NetworkManager** обнаружил несколько потенциальных вариантов, будет выбрано соединение с наиболее высоким приоритетом. Если все соединения имеют одинаковый приоритет, по умолчанию будет выбран наиболее активный канал.

VTI

В Red Hat Enterprise Linux 7.1 добавлена поддержка *интерфейсов виртуальных туннелей* (VTI, Virtual Tunnel Interface), что делает возможным прохождение трафика VTI в разных пространствах имен при инкапсуляции и извлечении пакетов.

Конфигурация MemberOf

Конфигурацию модуля **MemberOf** для 389 Directory Server теперь можно разместить не только в `cn=config`, но и в отдельной области в базе данных. Такое централизованное расположение облегчает копирование конфигурации **MemberOf** на мастер-серверы.

Глава 11. Linux Containers

The **Docker** project is an open-source project that automates the deployment of applications inside Linux Containers, and provides the capability to package an application with its runtime dependencies into a container. It provides a command-line tool for the life cycle management of image-based containers. Linux containers enable rapid application deployment, simpler testing, maintenance, and troubleshooting while improving security. Using Red Hat Enterprise Linux 7 with containers allows customers to increase staff efficiency, deploy third-party applications faster, enable a more agile development environment, and manage resources more tightly.

To quickly get up-and-running with docker formatted containers, refer to [Get Started with docker Formatted Containers](#).

Red Hat Enterprise Linux 7.1 ships with docker version 1.4.1, which includes a number of new features, security fixes, patches and changes. Highlights include:

- The ENV instruction in the Dockerfile now supports arguments in the form of ENV name=value name2=value2 ...
- An experimental overlayfs storage driver has been introduced.
- An update is included for CVE-2014-9356: Path traversal during processing of absolute symlinks. Absolute symlinks were not adequately checked for traversal which created a vulnerability via image extraction and/or volume mounts.
- An update is included for CVE-2014-9357: Escalation of privileges during decompression of LZMA (.xz) archives. Docker 1.3.2 added chroot for archive extraction. This created a vulnerability that could allow malicious images or builds to write files to the host system and escape containerization, leading to privilege escalation.
- An update is included for CVE-2014-9358: Path traversal and spoofing opportunities via image identifiers. Image IDs passed either via docker load or registry communications were not sufficiently validated. This created a vulnerability to path traversal attacks wherein malicious images or repository spoofing could lead to graph corruption and manipulation.

Red Hat provides platform container images for building applications on both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7.

Дополнительно предлагается приложение **Kubernetes** для одновременного управления группами контейнеров. Подробную информацию можно найти в документе [Управление контейнерами Docker с помощью Kubernetes](#).

Linux containers are supported running on hosts with SELinux enabled. SELinux is not supported when the `/var/lib/docker` directory is located on a volume using the B-tree file system (Btrfs).

11.1. Components of docker Formatted Containers

The docker container format works with the following fundamental components:

- *Контейнер* — изолированный экземпляр операционной системы на базе образа. При запуске контейнера из образа будет добавлен дополнительный слой образа. Сделанные в контейнере изменения можно сохранить в новый слой образа при помощи команды **docker commit**.
- *Образ* — статический снимок конфигурации контейнера, доступный только для чтения. Изменения будут применяться к образу на верхнем слое, после чего его можно будет сохранить в новый образ. Образ может быть связан с одним или несколькими родительскими образами.

- ✦ *Platform Container Image* – an image that has no parent. Platform container images define the runtime environment, packages, and utilities necessary for a containerized application to run. The platform image is read-only, so any changes are reflected in the copied images stacked on top of it. See an example of such stacking in [Рисунок 11.1, «Иерархия образов в Docker»](#).
- ✦ *Реестр* — полный комплект образов. Реестр может быть открытым или закрытым. В некоторые реестры можно добавлять образы, тем самым разрешая их загрузку другими пользователями.
- ✦ *Dockerfile* — файл конфигурации с командами сборки образов. С его помощью можно стандартизировать и автоматизировать процесс сборки.

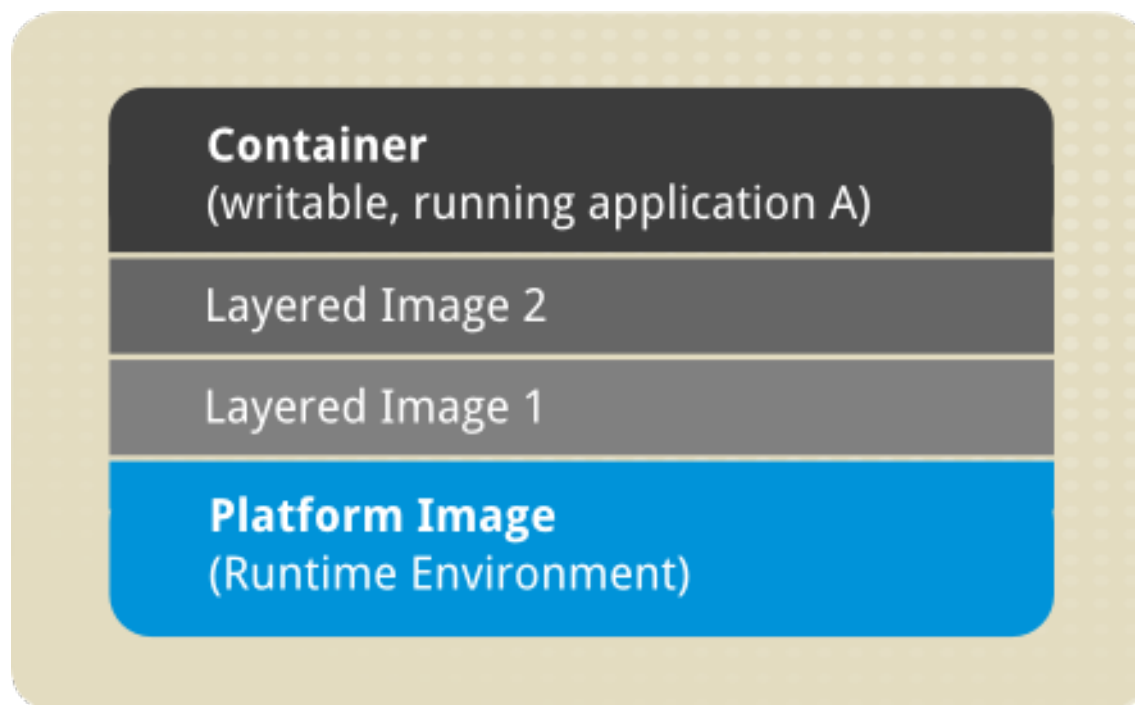


Рисунок 11.1. Иерархия образов в Docker

11.2. Advantages of Using Containers

The Docker project provides an API for container management, an image format, and the possibility to use a remote registry for sharing containers. This scheme benefits both developers and system administrators with advantages such as:

- ✦ *Быстрое развертывание приложений*: минимальные требования контейнеров к рабочему окружению позволяют поддерживать небольшой размер контейнера и быстро его развернуть.
- ✦ *Кроссплатформенность* : приложение и его зависимости могут быть упакованы в платформонезависимый контейнер и перенесены на другой компьютер с поддержкой Docker.
- ✦ *Контроль версий и многократное использование компонентов*: при необходимости можно выполнить откат к предыдущей версии контейнера или сравнить версии с целью определения различий. Новый контейнер создается на базе предыдущего с учетом различий — это и обеспечивает их легковесную структуру.
- ✦ *Совместный доступ*: чтобы поделиться контейнером с другими пользователями, поместите его в удаленный репозиторий — реестр. Реестры могут быть общедоступными и закрытыми.
- ✦ *Легковесная структура и минимальные издержки*: развертывание образов Docker происходит быстро, так как они не занимают много места.
- ✦ *Легкость обслуживания*: Docker существенно упрощает процесс разрешения зависимостей и

уменьшает риск их нарушения.

11.3. Сравнение с виртуальными машинами

Virtual machines represent an entire server with all of the associated software and maintenance concerns. Containers provide application isolation and can be configured with minimum run-time environments. In a container, the kernel and parts of the operating system infrastructure are shared. For the virtual machine, a full operating system must be included.

- Для создания виртуальной системы необходимо установить полную версию операционной системы, что существенно увеличивает нагрузку, в то время как создание и удаление контейнеров не требует значительных ресурсов.
- Контейнеры не занимают много места, поэтому на одном и том же хосте вы сможете разместить больше контейнеров чем виртуальных машин.
- Контейнеры используют системные ресурсы совместно, то есть выполнение разных экземпляров одного приложения в контейнерах не требует дублирования одних и тех же библиотек. В свою очередь, виртуальные машины полностью изолированы от других.
- Виртуальные машины можно переносить с одного хоста на другой, не прерывая работу, что невозможно для контейнеров — их надо будет остановить.

Прежде чем сделать выбор в пользу контейнеров или виртуальных машин, в каждом индивидуальном случае надо точно сформулировать свои требования и оценить последствия.

To quickly get up-and-running with docker formatted containers, refer to [Get Started with docker Formatted Containers](#).

More information about Linux Containers, the Docker project, subscriptions and support can be found in this [FAQ](#).

11.4. Using Containers on Red Hat Enterprise Linux 7.1

Packages containing **docker**, **kubernetes**, and registry software have been released as part of the Extras channel in Red Hat Enterprise Linux. Once the Extras channel has been enabled, the packages can be installed in the usual way. For more information on installing packages or enabling channels, see the [System Administrator's Guide](#).

Red Hat provides a registry of platform container images and Red Hat Atomic Container Images. This registry provides base images for building applications on both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 and pre-built solutions usable on Red Hat Enterprise Linux 7.1 with Docker. For more information about the registry and a list of available packages, see [Container Images](#).

11.5. Containers with the LXC Format Have Been Deprecated

The following LXC packages, which contain Linux resource containers, are deprecated starting with Red Hat Enterprise Linux 7.1:

- libvirt-daemon-driver-lxc
- libvirt-daemon-lxc
- libvirt-login-shell

The Linux container functionality is now focused on the docker management interface (docker command-line interface). Please note: It is possible that the listed LXC packages will not be shipped with future releases of Red Hat Enterprise Linux, as they may be considered for formal removal.

Глава 12. Аутентификация и функциональная совместимость

Manual Backup and Restore Functionality

This update introduces the **ipa-backup** and **ipa-restore** commands to Identity Management (IdM), which allow users to manually back up their IdM data and restore them in case of a hardware failure. For further information, see the [ipa-backup\(1\)](#) and [ipa-restore\(1\)](#) manual pages or the documentation in the [Linux Domain Identity, Authentication, and Policy Guide](#).

Переход от WinSync к отношениям доверия

This update implements the new **ID Views** mechanism of user configuration. It enables the migration of Identity Management users from a **WinSync** synchronization-based architecture used by **Active Directory** to an infrastructure based on Cross-Realm Trusts. For the details of **ID Views** and the migration procedure, see the documentation in the [Windows Integration Guide](#).

One-Time Password Authentication

One of the best ways to increase authentication security is to require two factor authentication (2FA). A very popular option is to use one-time passwords (OTP). This technique began in the proprietary space, but over time some open standards emerged (HOTP: RFC 4226, TOTP: RFC 6238). Identity Management in Red Hat Enterprise Linux 7.1 contains the first implementation of the standard OTP mechanism. For further details, see the documentation in the [System-Level Authentication Guide](#).

Интеграция SSSD с CIFS

A plug-in interface provided by **SSSD** has been added to configure the way in which the **cifs-utils** utility conducts the ID-mapping process. As a result, an **SSSD** client can now access a CIFS share with the same functionality as a client running the **Winbind** service. For further information, see the documentation in the [Windows Integration Guide](#).

ipa-cacert-manage renew

The **ipa-cacert-manage renew** command has been added to the Identity management (IdM) client, which makes it possible to renew the IdM Certification Authority (CA) file. This enables users to smoothly install and set up IdM using a certificate signed by an external CA. For details on this feature, see the [ipa-cacert-manage\(1\)](#) manual page.

Контроль доступа на сервере IDM

It is now possible to regulate read permissions of specific sections in the Identity Management (IdM) server UI. This allows IdM server administrators to limit the accessibility of privileged content only to chosen users. In addition, authenticated users of the IdM server no longer have read permissions to all of its contents by default. These changes improve the overall security of the IdM server data.

Ограничение доступа к доменам

The **domains=** option has been added to the **pam_sss** module, which overrides the **domains=** option in the **/etc/sss/sss.conf** file. In addition, this update adds the **pam_trusted_users** option, which allows the user to add a list of numerical UIDs or user names that are trusted by the **SSSD** daemon, and the **pam_public_domains** option and a list of domains accessible even for untrusted users. The mentioned

additions allow the configuration of systems, where regular users are allowed to access the specified applications, but do not have login rights on the system itself. For additional information on this feature, see the documentation in the [Linux Domain Identity, Authentication, and Policy Guide](#).

Автоматическая конфигурация провайдера данных

`ipa-client-install` по умолчанию использует **SSSD** в качестве провайдера данных для `sudo`. Это поведение можно отключить при помощи ключа `--no-sudo`. Новый параметр `--nisdomain` определяет имя домена NIS, которое будет использоваться при установке клиента IDM, а `--no-nisdomain` пропускает его настройку. Если ни один из этих параметров не указан, будет выбран домен IPA.

Провайдеры AD и LDAP для sudo

Провайдер AD обеспечивает подключение к серверу Active Directory. Red Hat Enterprise Linux 7.1 предлагает экспериментальную поддержку провайдера AD в комбинации с LDAP. Чтобы включить эту возможность, в `sssd.conf` добавьте `sudo_provider=ad` в секции домена.

32-bit Version of krb5-server and krb5-server-ldap Deprecated

The 32-bit version of **Kerberos 5 Server** is no longer distributed, and the following packages are deprecated starting with Red Hat Enterprise Linux 7.1: `krb5-server.i686`, `krb5-server.s390`, `krb5-server.ppc`, `krb5-server-ldap.i686`, `krb5-server-ldap.s390`, and `krb5-server-ldap.ppc`. There is no need to distribute the 32-bit version of `krb5-server` on Red Hat Enterprise Linux 7, which is supported only on the following architectures: AMD64 and Intel 64 systems (**x86_64**), 64-bit IBM Power Systems servers (**ppc64**), and IBM System z (**s390x**).

Глава 13. Безопасность

Scap-security-guide

Пакет *scap-security-guide* предоставляет рекомендации спецификации SCAP (Security Content Automation Protocol), стандартные профили, механизмы проверки и необходимые данные для проверки соответствия системы требованиям безопасности (текстовое описание и автоматический тест). Автоматический тест может выполняться регулярно, тем самым обеспечивая удобный и надежный метод проверки.

The Red Hat Enterprise Linux 7.1 version of the **SCAP Security Guide** includes the *Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)*, which can be used for compliance scans of Red Hat Enterprise Linux Server 7.1 cloud systems.

Also, the Red Hat Enterprise Linux 7.1 *scap-security-guide* package contains SCAP datastream content format files for Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7, so that remote compliance scanning of both of these products is possible.

The Red Hat Enterprise Linux 7.1 system administrator can use the **oscap** command line tool from the *openscap-scanner* package to verify that the system conforms to the provided guidelines. See the *scap-security-guide(8)* manual page for further information.

SELinux

В Red Hat Enterprise Linux 7.1 стратегия SELinux подверглась изменениям: сервисы, для которых не были определены правила, работавшие в домене `init_t`, теперь будут выполняться в домене `unconfined_service_t`. Подробно этот вопрос обсуждается в главе [Неограниченные процессы в руководстве SELinux](#).

OpenSSH

Комплект **OpenSSH** обновлен до версии 6.6.1p1.

- Добавлена поддержка обмена ключами в соответствии с алгоритмом **Диффи-Хеллмана** на эллиптических кривых **Curve25519**. Этот метод используется по умолчанию сервером и клиентом при условии, что они его поддерживают.
- Добавлена поддержка оптимизированного по быстродействию алгоритма **Ed25519** на эллиптических кривых, который может использоваться для расчета ключей как на стороне клиента, так и хоста, и обеспечивает более высокий уровень защиты по сравнению с **ECDSA** и **DSA**.
- Добавлен новый формат закрытого ключа на базе **bcrypt**. Ключи **Ed25519** используют этот формат по умолчанию.
- Новый шифр **chacha20-poly1305@openssh.com** объединяет поточный шифр **ChaCha20** и код аутентификации сообщений **Poly1305**.

Libreswan

Libreswan, открытая программная реализация VPN на базе IPsec, обновлена до версии 3.12.

- Добавлены новые шифры.
- **IKEv2** support has been improved.

- ✦ **IKEv1** и **IKEv2** поддерживают цепочки промежуточных сертификатов.
- ✦ Оптимизировано управление соединениями.
- ✦ Улучшена совместимость с OpenBSD, Cisco и Android.
- ✦ Усовершенствована поддержка **systemd**.
- ✦ Добавлена поддержка хэшированных запросов **CERTREQ** и статистики трафика.

Trusted Network Connect

The Trusted Network Connect (TNC) Architecture, provided by the *strongimcv* package, has been updated and is now based on **strongSwan 5.2.0**. The following new features and improvements have been added to the TNC:

- ✦ The **PT-EAP** transport protocol ([RFC 7171](#)) for Trusted Network Connect has been added.
- ✦ The Attestation *Integrity Measurement Collector* (IMC)/*Integrity Measurement Verifier* (IMV) pair now supports the IMA-NG measurement format.
- ✦ Аттестация IMV поддерживает TPMRA (TPM Remote Attestation).
- ✦ Добавлена поддержка REST API с SWID IMV на базе JSON.
- ✦ The SWID IMC can now extract all installed packages from the **dpkg**, **rpm**, or **pacman** package managers using the [swidGenerator](#), which generates SWID tags according to the new ISO/IEC 19770-2:2014 standard.
- ✦ The **libtls TLS 1.2** implementation as used by **EAP-(T)TLS** and other protocols has been extended by AEAD mode support, currently limited to **AES-GCM**.
- ✦ Improved (IMV) support for sharing access requestor ID, device ID, and product information of an access requestor via a common **imv_session** object.
- ✦ Исправлены ошибки в протоколах **IF-TNCCS (PB-TNC, IF-M (PA-TNC))** и в **OS IMC/IMV**.

GnuTLS

Свободная реализация **GnuTLS** для протоколов **SSL**, **TLS** и **DTLS** обновлена до версии 3.3.8.

- ✦ Добавлена поддержка **DTLS 1.2**.
- ✦ Добавлена поддержка расширения ALPN (*Application Layer Protocol Negotiation*).
- ✦ Оптимизирована работа комплектов шифрования, использующих алгоритмы на основе эллиптических кривых.
- ✦ Добавлены шифры **RSA-PSK** и **CAMELLIA-GCM**.
- ✦ Добавлена поддержка TPM (*Trusted Platform Module*).
- ✦ Добавлена поддержка смарт-карт **PKCS#11** и улучшена поддержка аппаратных модулей HSM (*Hardware Security Modules*).
- ✦ Улучшено соответствие требованиям федеральных стандартов **FIPS 140** (*Federal Information Processing Standards*).

Глава 14. Рабочее окружение

Поддержка стереоизображений Quad Buffered OpenGL

GNOME Shell и **Mutter** теперь допускают использование Quad Buffered OpenGL на поддерживаемом оборудовании. Для этого потребуется установить драйвер NVIDIA 337 и выше.

Провайдеры сетевых учетных записей

В *gnome-online-accounts* добавлен ключ **org.gnome.online-accounts.whitelisted-providers** для **GSettings**, определяющий список провайдеров сетевых учетных записей, которые должны быть включены во время запуска. Таким образом, администратор может контролировать добавление провайдеров.

Глава 15. Поддержка работоспособности

Микроотчеты ABRT

In Red Hat Enterprise Linux 7.1, the **Automatic Bug Reporting Tool (ABRT)** receives tighter integration with the Red Hat Customer Portal and is capable of directly sending micro-reports to the Portal. **ABRT** provides a utility, **abrt-auto-reporting**, to easily configure user's Portal credentials necessary to authorize micro-reports.

The integrated authorization allows **ABRT** to reply to a micro-report with a rich text which may include possible steps to fix the cause of the micro-report. For example, **ABRT** can suggest which packages are supposed to be upgraded or offer Knowledge base articles related to the issue.

Подробную информацию можно найти на [портале пользователей](#).

Глава 16. Программные коллекции

Комплект Red Hat Software Collections включает в свой состав ряд динамических языков программирования, серверов баз данных и относящихся к ним пакетов, которые можно установить в Red Hat Enterprise Linux 6 и Red Hat Enterprise Linux 7 на платформах AMD64 и Intel 64.

Red Hat Software Collections не ставит целью заменить стандартные системные инструменты Red Hat Enterprise Linux.

Механизм сборки пакетов в Red Hat Software Collections построен на базе **scl**, что позволяет выбрать конкретную версию интересующего пакета.



Важно

Цикл поддержки Red Hat Software Collections значительно короче Red Hat Enterprise Linux. Более подробно об этом рассказано на странице [Жизненный цикл Red Hat Software Collections](#).

Red Hat Developer Toolset теперь входит в состав Red Hat Software Collections в качестве отдельной коллекции. В его состав вошли компиляторы и отладчик GNU, платформа разработки Eclipse и другие инструменты разработки, отладки и контроля производительности.

Полный список программ в комплекте, а также обзор известных проблем и инструкции можно найти [здесь](#).

За подробной информацией обратитесь к [документации Red Hat Developer Toolset](#).

Глава 17. Red Hat Enterprise Linux for Real Time

Red Hat Enterprise Linux for Real Time is a new offering in Red Hat Enterprise Linux 7.1 comprised of a special kernel build and several user space utilities. With this kernel and appropriate system configuration, Red Hat Enterprise Linux for Real Time brings deterministic workloads, which allow users to rely on consistent response times and low and predictable latency. These capabilities are critical in strategic industries such as financial service marketplaces, telecommunications, or medical research.

For instructions on how to install Red Hat Enterprise Linux for Real Time, and how to set up and tune the system so that you can take full advantage of this offering, refer to the [Red Hat Enterprise Linux for Real Time 7 Installation Guide](#).

Часть II. Драйверы

В этой главе обсуждаются изменения драйверов в Red Hat Enterprise Linux 7.1.

Глава 18. Драйверы устройств хранения

- **hpsa** обновлен до версии 3.4.4-1-RH1.
- **qla2xxx** обновлен до версии 8.07.00.08.07.1-k1.
- **qla4xxx** обновлен до версии 5.04.00.04.07.01-k0.
- **qlcnic** обновлен до версии 5.3.61.
- **netxen_nic** обновлен до версии 4.0.82.
- **qlge** обновлен до версии 1.00.00.34.
- **bnx2fc** обновлен до версии 2.4.2.
- **bnx2i** обновлен до версии 2.7.10.1.
- **cnic** обновлен до версии 2.5.20.
- **bnx2x** обновлен до версии 1.710.51-0.
- **bnx2** обновлен до версии 2.2.5.
- **megaraid_sas** обновлен до версии 06.805.06.01-rc1.
- **mpt2sas** обновлен до версии 18.100.00.00.
- **ipr** обновлен до версии 2.6.0.
- В Red Hat Enterprise Linux 7 были включены пакеты *kmod-lpfc*, что обеспечило стабильность при использовании *lpfc* с адаптерами FC и FCoE. Драйвер **lpfc** обновлен до версии 0:10.2.8021.1.
- **be2iscsi** обновлен до версии 10.4.74.0r.
- **nvme** обновлен до версии 0.9.

Глава 19. Сетевые драйверы

- **bna** обновлен до версии 3.2.23.0r.
- **cxgb3** обновлен до версии 1.1.5-ko.
- **cxgb3i** обновлен до версии 2.0.0.
- **iw_cxgb3** обновлен до версии 1.1.
- **cxgb4** обновлен до версии 2.0.0-ko.
- **cxgb4vf** обновлен до версии 2.0.0-ko.
- **cxgb4i** обновлен до версии 0.9.4.
- **iw_cxgb4** обновлен до версии 0.1.
- **e1000e** обновлен до версии 2.3.2-k.
- **igb** обновлен до версии 5.2.13-k.
- **igbvf** обновлен до версии 2.0.2-k.
- **ixgbe** обновлен до версии 3.19.1-k.
- **ixgbev** обновлен до версии 2.12.1-k.
- **i40e** обновлен до версии 1.0.11-k.
- **i40evf** обновлен до версии 1.0.1.
- **e1000** обновлен до версии 7.3.21-k8-NAPI.
- **mlx4_en** обновлен до версии 2.2-1.
- **mlx4_ib** обновлен до версии 2.2-1.
- **mlx5_core** обновлен до версии 2.2-1.
- **mlx5_ib** обновлен до версии 2.2-1.
- **ocrdma** обновлен до версии 10.2.287.0u.
- **ib_ipoib** обновлен до версии 1.0.0.
- **ib_qib** обновлен до версии 1.11.
- **enic** обновлен до версии 2.1.1.67.
- **be2net** обновлен до версии 10.4r.
- **tg3** обновлен до версии 3.137.
- **r8169** обновлен до версии 2.3LK-NAPI.

Глава 20. Графические драйверы

- ✦ **vmwgfx** обновлен до версии 2.6.0.0.

Часть III. Known Issues

This part describes known issues in Red Hat Enterprise Linux 7.1.

Глава 21. Installation and Booting

anaconda component, BZ#1067868

Under certain circumstances, when installing the system from the boot DVD or ISO image, not all assigned IP addresses are shown in the network spoke once network connectivity is configured and enabled. To work around this problem, leave the network spoke and enter it again. After re-entering, all assigned addresses are shown correctly.

Глава 22. Networking

rsync component, [BZ#1082496](#)

The **rsync** utility cannot be run as a socket-activated service because the **rsyncd@.service** file is missing from the *rsync* package. Consequently, the **systemctl start rsyncd.socket** command does not work. However, running **rsync** as a daemon by executing the **systemctl start rsyncd.service** command works as expected.

Глава 23. Authentication and Interoperability

bind-dyndb-ldap component, BZ#[1139776](#)

The latest version of the **bind-dyndb-ldap** system plug-in offers significant improvements over the previous versions, but currently has some limitations. One of the limitations is missing support for the LDAP rename (MODRDN) operation. As a consequence, DNS records renamed in LDAP are not served correctly. To work around this problem, restart the **named** daemon to resynchronize data after each MODRDN operation. In an Identity Management (IdM) cluster, restart the **named** daemon on all IdM replicas.

ipa component, BZ#[1186352](#)

When you restore an Identity Management (IdM) server from backup and re-initialize the restored data to other replicas, the Schema Compatibility plug-in can still maintain a cache of the old data from before performing the restore and re-initialization. Consequently, the replicas might behave unexpectedly. For example, if you attempt to add a user that was originally added after performing the backup, and thus removed during the restore and re-initialization steps, the operation might fail with an error, because the Schema Compatibility cache contains a conflicting user entry. To work around this problem, restart the IdM replicas after re-initializing them from the master server. This clears the Schema Compatibility cache and ensures that the replicas behave as expected in the described situation.

ipa component, BZ#[1188195](#)

Both anonymous and authenticated users lose the default permission to read the **facsimiletelephonenumber** user attribute after upgrading to the Red Hat Enterprise Linux 7.1 version of Identity Management (IdM). To manually change the new default setting and make the attribute readable again, run the following command:

```
ipa permission-mod 'System: Read User Addressbook Attributes' --  
includedattrs facsimiletelephonenumber
```

Глава 24. Desktop

gobject-introspection component, BZ#[1076414](#)

The **gobject-introspection** library is not available in a 32-bit multilib package. Users who wish to compile 32-bit applications that rely on GObject introspection or libraries that use it, such as **GTK+** or **GLib**, should use the *mock* package to set up a build environment for their applications.

Приложение А. История переиздания

| | | |
|--|------------------------|-------------------------|
| Издание 1.0-9.5 | Thu Jan 29 2015 | Yuliya Poyarkova |
| Повторная публикация. | | |
| Издание 1.0-9.2 | Thu Jan 29 2015 | Yuliya Poyarkova |
| Перевод на русский язык. | | |
| Издание 1.0-9.1 | Thu Jan 29 2015 | Yuliya Poyarkova |
| Синхронизация с XML 1.0-9. | | |
| Издание 1.0-9 | Wed Jan 14 2015 | Milan Navrátil |
| Примечания к выпуску Red Hat Enterprise Linux 7.1 | | |
| Издание 1.0-8 | Thu Dec 15 2014 | Jiří Herrmann |
| Примечания к выпуску Red Hat Enterprise Linux 7.1 Beta | | |