



# **Red Hat Enterprise Linux 7 Note di rilascio per la versione 7.1**

---

Note di rilascio per Red Hat Enterprise Linux 7

Red Hat Customer Content  
Services



# Red Hat Enterprise Linux 7 Note di rilascio per la versione 7.1

---

## Note di rilascio per Red Hat Enterprise Linux 7

Red Hat Customer Content Services

## Nota Legale

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.

## Sommario

Le Note di rilascio documentano le funzioni e i miglioramenti più importanti implementati nella release di Red Hat Enterprise Linux 7.1, insieme alle problematiche conosciute nella release 7.1. Per maggiori informazioni sulle differenze tra Red Hat Enterprise Linux 6 e 7, consultare la Migration Planning Guide. Riconoscimenti Red Hat Global Support Services desidera ringraziare Sterling Alexander e Michael Everette per il loro preziosissimo contributo durante i test di Red Hat Enterprise Linux 7.

# Indice

<b>Prefazione</b> .....	<b>4</b>
<b>Parte I. caratteristiche di</b> .....	<b>5</b>
<b>Capitolo 1. Architetture</b> .....	<b>6</b>
1.1. Red Hat Enterprise Linux for POWER, Little Endian	6
<b>Capitolo 2. Hardware Enablement</b> .....	<b>7</b>
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
<b>Capitolo 3. Installazione e avvio</b> .....	<b>8</b>
3.1. Programma di installazione	8
3.2. Boot loader	12
<b>Capitolo 4. Storage</b> .....	<b>13</b>
Cache LVM	13
Gestione array di archiviazione con libStorageMgmt API	13
Supporto per LSI Syncro	13
LVM Application Programming Interface	14
Supporto DIF/DIX	14
Output e controllo errore della sintassi del device-mapper-multipath migliorati	14
<b>Capitolo 5. File Systems</b> .....	<b>15</b>
Supporto per il file system Btrfs	15
OverlayFS	15
Supporto di Parallel NFS	15
<b>Capitolo 6. Kernel</b> .....	<b>16</b>
Supporto per i dispositivi a blocchi Ceph	16
Aggiornamenti simultanei Flash MCL	16
Patch del kernel dinamico	16
Crashkernel con più di una 1 CPU	16
Target dm-era	16
Driver del kernel Cisco VIC	16
Miglioramento gestione entropia in hwrng	16
Miglioramento prestazioni Load-Balancing dello Scheduler	17
newidle Balance migliorato nello scheduler	17
HugeTLB supporta l'allocazione di pagine 1GB Huge per-nodo	17
Nuovo meccanismo di locking basato su MCS	17
Dimensione Stack del processo aumentata da 8KB a 16KB	17
Funzionalità uprobe e uretprobe abilitate in perf e systemtap	17
Controllo consistenza dati End-To-End	17
DRBG su sistemi a 32-Bit	17
Supporto per dimensioni crashkernel molto grandi	17
<b>Capitolo 7. Virtualizzazione</b> .....	<b>18</b>
Aumentato il numero massimo di vCPU in KVM	18
Supporto 5th Generation Intel Core New Instructions in QEMU, KVM e libvirt API	18
Supporto USB 3.0 per guest KVM	18
Compressione per il comando dump-guest-memory	18
Open Virtual Machine Firmware	18
Migliorate le prestazioni di rete su Hyper-V	18

hypervcopyd in hyperv-daemons	18
Nuove funzioni in libguestfs	18
Flight Recorder Tracing	19
RDMA-based Migration of Live Guests	19
<b>Capitolo 8. Clustering</b> .....	<b>20</b>
Dynamic Token Timeout per Corosync	20
Miglioramenti del Corosync Tie Breaker	20
Miglioramenti al Red Hat High Availability	20
<b>Capitolo 9. Compiler e strumenti</b> .....	<b>21</b>
Supporto hot-patching per Linux sui binari System z	21
Miglioramenti Performance Application Programming Interface	21
OProfile	21
OpenJDK8	21
sosreport sostituisce snap	21
Supporto GDB per Little-Endian 64-bit PowerPC	21
Miglioramento di Tuna	22
<b>Capitolo 10. Networking</b> .....	<b>23</b>
Trusted Network Connect	23
Funzione SR-IOV nel driver qlcnic	23
Berkeley Packet Filter	23
Stabilità migliorata dell'orologio	23
Pacchetti libnetfilter_queue	23
Miglioramenti collaborazione	23
Driver Intel QuickAssist Technology	23
Supporto LinuxPTP timemaster per il failover tra PTP e NTP	24
initscripts di rete	24
TCP Delayed ACK	24
NetworkManager	24
Spazi nomi di rete e VTI	24
Storage per la configurazione alternativa del plug-in MemberOf	24
<b>Capitolo 11. Linux Containers</b> .....	<b>25</b>
11.1. Components of docker Formatted Containers	25
11.2. Advantages of Using Containers	26
11.3. Confronto con le macchine virtuali	27
11.4. Using Containers on Red Hat Enterprise Linux 7.1	27
11.5. Containers Using the libvirt-lxc Tooling Have Been Deprecated	27
<b>Capitolo 12. Autenticazione ed interoperabilità</b> .....	<b>29</b>
Manual Backup and Restore Functionality	29
Supporto per la migrazione da WinSync a Trust	29
One-Time Password Authentication	29
Integrazione SSSD per il Common Internet File System	29
Strumento di gestione del Certificate Authority	29
Migliorata la granularità per il controllo d'accesso	29
Accesso al dominio limitato per utenti non privilegiati	29
Configurazione del provider dei dati automatica	30
Utilizzo provider sudo AD e LDAP	30
32-bit Version of krb5-server and krb5-server-ldap Deprecated	30
<b>Capitolo 13. Sicurezza</b> .....	<b>31</b>
SCAP Security Guide	31

---

Politica di SELinux	31
Nuove funzioni in OpenSSH	31
Nuove funzioni in Libreswan	31
Nuove funzioni in TNC	32
Nuove funzioni in GnuTLS	32
<b>Capitolo 14. Desktop</b>	<b>34</b>
Supporto per le immagini Quad-buffered OpenGL Stereo	34
Provider di account online	34
<b>Capitolo 15. Supporto e gestione</b>	<b>35</b>
ABRT Authorized Micro-Reporting	35
<b>Capitolo 16. Red Hat Software Collection</b>	<b>36</b>
<b>Capitolo 17. Red Hat Enterprise Linux for Real Time</b>	<b>37</b>
<b>Parte II. Driver del dispositivo</b>	<b>38</b>
<b>Capitolo 18. Aggiornamenti driver di archiviazione</b>	<b>39</b>
<b>Capitolo 19. Aggiornamenti driver di rete</b>	<b>40</b>
<b>Capitolo 20. Aggiornamenti driver grafici</b>	<b>41</b>
<b>Parte III. Known Issues</b>	<b>42</b>
<b>Capitolo 21. Installation and Booting</b>	<b>43</b>
<b>Capitolo 22. Networking</b>	<b>44</b>
<b>Capitolo 23. Authentication and Interoperability</b>	<b>45</b>
<b>Capitolo 24. Desktop</b>	<b>46</b>
<b>Appendice A. Diario delle Revisioni</b>	<b>47</b>

## Prefazione

Le versioni minori di Red Hat Enterprise Linux rappresentano una raccolta di miglioramenti, security errata e correzioni. Le *Note di rilascio di Red Hat Enterprise Linux 7.1* documentano le modifiche più importanti fatte al sistema operativo di Red Hat Enterprise Linux 7 ed alle applicazioni relative per questa release minore. Le *Note di rilascio di Red Hat Enterprise Linux 7.1* documentano altresì le problematiche conosciute in Red Hat Enterprise Linux 7.1.



### Importante

Le *Note di rilascio di Red Hat Enterprise Linux 7.1*, disponibili online [qui](#), devono essere considerate versioni definitive e aggiornate. Per gli utenti che desiderano formulare domande su questa release, consultare le *Note di rilascio* online per le rispettive versioni di Red Hat Enterprise Linux.



### Nota

Per una descrizione degli errori conosciuti consultare [la versione inglese delle Note di rilascio di Red Hat Enterprise Linux 7.1](#).

Per maggiori informazioni sul ciclo di vita di Red Hat Enterprise Linux consultare <https://access.redhat.com/support/policy/updates/errata/>.



## Parte I. caratteristiche di

Questa sezione descrive le nuove funzionalità e i miglioramenti più importanti introdotti con il Red Hat Enterprise Linux 7.1.

## Capitolo 1. Architetture

Red Hat Enterprise Linux 7.1 è disponibile come kit singolo sulle seguenti architetture <sup>[1]</sup>

- ✦ 64-bit AMD
- ✦ 64-bit Intel
- ✦ IBM POWER7 e POWER8 (big endian)
- ✦ IBM POWER8 (little endian) <sup>[2]</sup>
- ✦ IBM System z <sup>[3]</sup>

Con questa release Red Hat propone miglioramenti al server, ai sistemi e all'esperienza generale della open source di Red Hat.

### 1.1. Red Hat Enterprise Linux for POWER, Little Endian

Red Hat Enterprise Linux 7.1 introduce il supporto little endian sui server IBM Power Systems utilizzando processori IBM POWER8. In precedenza con Red Hat Enterprise Linux 7 era disponibile solo la variante big endian per IBM Power Systems. Il supporto per little endian sui server basati su POWER8, migliora l'intercambiabilità delle applicazioni tra sistemi a 64-bit di Intel (**x86\_64**) e IBM Power Systems.

- ✦ In modalità little endian sono disponibili alcuni dispositivi separati per l'installazione di Red Hat Enterprise Linux su server IBM Power Systems. Questi dispositivi sono disponibili dalla sezione Download del Portale clienti di Red Hat.
- ✦ Con Red Hat Enterprise Linux for POWER, little endian sono supportati solo server basati su processori IBM POWER8.
- ✦ Attualmente Red Hat Enterprise Linux for POWER, little endian è solo supportato come guest KVM in **Red Hat Enterprise Virtualization for Power**. L'installazione su hardware bare metal non è attualmente supportata.
- ✦ Il **GRUB2** boot loader viene usato sul dispositivo di installazione per l'avvio di rete. La [Installation Guide](#) è stata aggiornata con le informazioni su come impostare un server per l'avvio di rete per client IBM Power Systems che utilizzano **GRUB2**.
- ✦ Tutti i pacchetti software per IBM Power Systems sono disponibili per entrambe le varianti little endian e big endian di Red Hat Enterprise Linux for POWER.
- ✦ Con i pacchetti compilati per Red Hat Enterprise Linux for POWER, little endian utilizza il codice per l'architettura **ppc64le** - per esempio, *gcc-4.8.3-9.ael7b.ppc64le.rpm*.

---

[1] Da notare che l'installazione di Red Hat Enterprise Linux 7.1 è supportata solo su hardware a 64-bit. Red Hat Enterprise Linux 7.1 è in grado di eseguire sistemi operativi a 32-bit, incluse le versioni precedenti di Red Hat Enterprise Linux, come macchine virtuali.

[2] Red Hat Enterprise Linux 7.1 (little endian) è attualmente supportato solo come guest KVM con gli hypervisor **Red Hat Enterprise Virtualization for Power** e **PowerVM**.

[3] Nota bene, Red Hat Enterprise Linux 7.1 supporta hardware IBM zEnterprise 196 o versioni più recenti; i sistemi IBM System z10 non sono più supportati e non potranno essere usati per l'avvio di avviare Red Hat Enterprise Linux 7.1.

## Capitolo 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.

## Capitolo 3. Installazione e avvio

### 3.1. Programma di installazione

L'installer di Red Hat Enterprise Linux, **Anaconda**, è stato aggiornato e ora è possibile avere un miglior processo d'installazione per Red Hat Enterprise Linux 7.1.

#### Interfaccia

- » L'interfaccia grafica dell'installer ora presenta una schermata aggiuntiva che permette di configurare il meccanismo di crash dumping del kernel **Kdump** durante l'installazione. In precedenza la configurazione veniva eseguita dopo l'installazione utilizzando **firstboot**, il quale non era accessibile senza una interfaccia grafica. Ora è possibile configurare **Kdump** come parte del processo d'installazione sui sistemi senza un ambiente grafico. La nuova schermata è disponibile dal menu principale dell'installer (**Sommario installazione**).



**Figura 3.1.** La nuova schermata di Kdump

- » La schermata di partizionamento manuale è stata modificata in modo da migliorare l'esperienza dell'utente. Alcuni controlli sono stati spostati in altre posizioni.

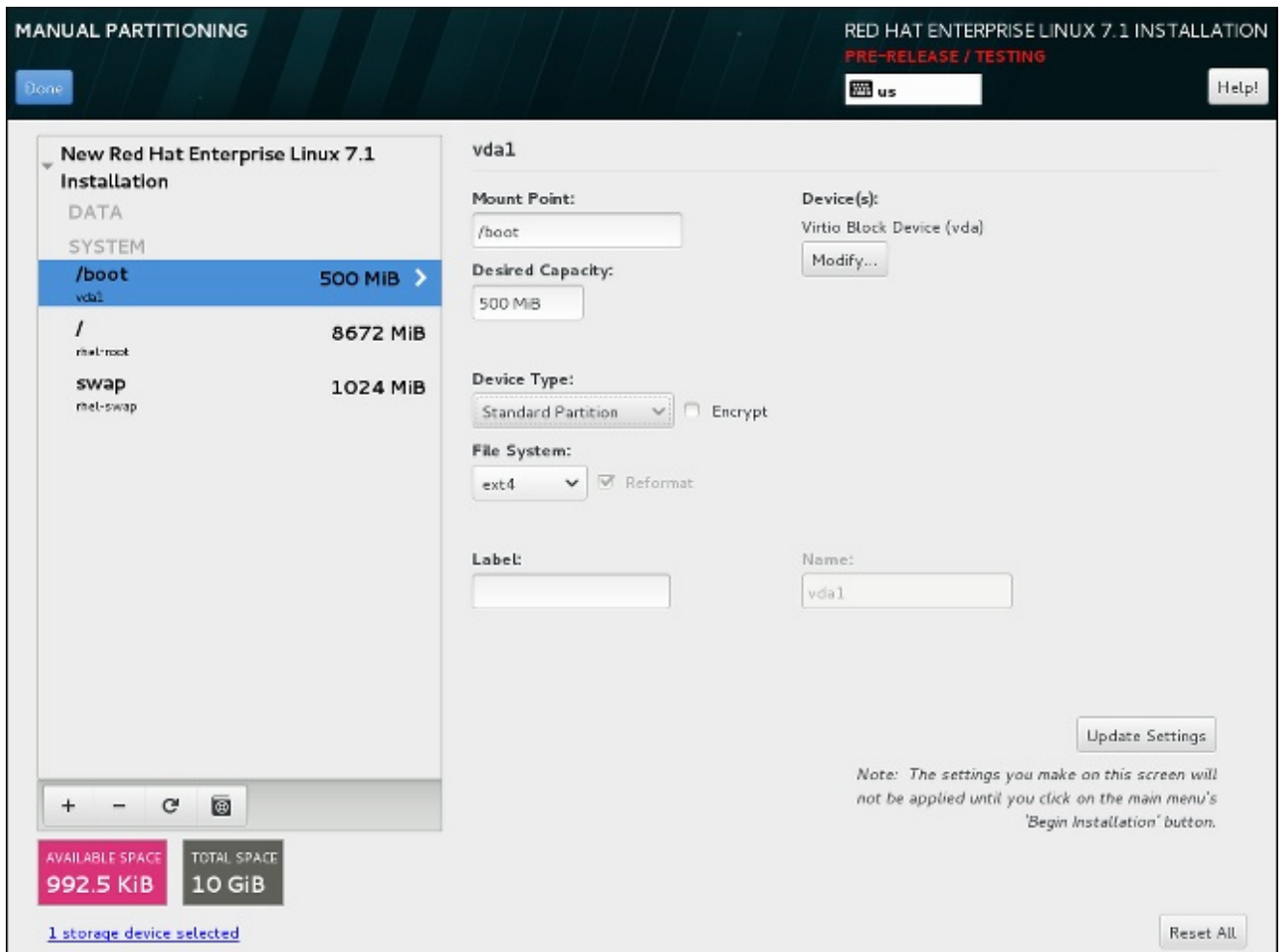


Figura 3.2. La nuova schermata per il Partizionamento manuale

- È ora possibile configurare un bridge di rete nella schermata **Rete & Hostname** dell'installer. Per fare questo selezionare **+** nella parte bassa dell'elenco, selezionare **Bridge** dal menu e configurare il bridge nel dialogo **Modifica connessione del bridge**. Questo dialogo è reso disponibile tramite **NetworkManager** ed è completamente documentato nella *Red Hat Enterprise Linux 7.1 Networking Guide*.

Sono state aggiunte nuove opzioni Kickstart per la configurazione del bridge. Consultare le informazioni di seguito riportate.

- L'installer non utilizza più console multiple per la visualizzazione dei log, tutti i log sono disponibili in **tmux** tramite la console virtuale 1 (**tty1**). Per consultare i log durante l'installazione, premere **Ctrl+Alt+F1** per selezionare **tmux**, e successivamente utilizzare **Ctrl+b X** per selezionare le finestre desiderate (sostituire **X** con il numero di una finestra desiderata come riportato nella parte bassa della schermata).

Per selezionare l'interfaccia grafica premere **Ctrl+Alt+F6**.

- L'interfaccia a linea di comando per **Anaconda** include ora le informazioni d'aiuto. Per visualizzarle usare **anaconda -h** su un sistema con il pacchetto *anaconda* installato. L'interfaccia a linea di comando permette all'utente di eseguire l'installer su un sistema installato, utile per le installazioni dell'immagine del disco.

## Opzioni e comandi di kickstart

- ✦ Il comando **logvol** presenta una nuova opzione: **--profile=**. Utilizzare questa opzione per specificare il nome del profilo di configurazione da usare con thin logical volume. Se usato, il nome verrà incluso nei metadati per il volume logico.

Per impostazione predefinita i profili disponibili sono **default** e **thin-performance**, e vengono definiti nella directory **/etc/lvm/profile**. Consultare la pagina man **lvm(8)** per informazioni aggiuntive.

- ✦ 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.

- ✦ L'opzione **--autoscreenshot** del comando **autostep** è stato corretto, ora è in grado di salvare uno screenshot di ogni schermata nella directory **/tmp/anaconda-screenshots**. Dopo il completamento dell'installazione gli screenshot verranno spostati in **/root/anaconda-screenshots**.
- ✦ Il comando **liveimg** ora supporta una installazione dai file tar e dalle immagini del disco. Il tar archive deve contenere il file system root del dispositivo d'installazione, e il nome del file deve terminare con **.tar**, **.tbz**, **.tgz**, **.txz**, **.tar.bz2**, **.tar.gz** o **.tar.xz**.
- ✦ Sono state aggiunte diverse opzioni al comando **network** per la configurazione dei bridge di rete. Queste opzioni sono:

- **--bridgeslaves=**: quando si utilizza questa opzione verrà creato un bridge di rete con il nome del dispositivo specificato con l'opzione **--device=**. I dispositivi definiti nell'opzione **--bridgeslaves=** verranno aggiunti al bridge. Per esempio:

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

- **--bridgeopts=**: Un elenco opzionale di parametri separati da virgole per l'interfaccia del bridge. I valori possibili sono **stp**, **priority**, **forward-delay**, **hello-time**, **max-age** e **ageing-time**. Per informazioni sui parametri consultare le pagine man di **nm-settings(5)**.
- ✦ Il comando **autopart** ha una nuova opzione, **--fstype**. Questa opzione permette di modificare il tipo di file system predefinito (**xfs**) quando si utilizza il partizionamento automatico in un file Kickstart.
- ✦ Several new features were added to Kickstart for better container support. These features include:
  - **repo --install**: Questa nuova opzione salva la configurazione del repository sul sistema installato all'interno della directory **/etc/yum.repos.d/**. Se questa opzione non viene utilizzata, il repository configurato in un file Kickstart risulterà disponibile solo durante il processo d'installazione e non sul sistema installato.
  - **bootloader --disabled**: Questa opzione impedirà l'installazione del boot loader.
  - **%packages --nocore**: Una nuova opzione per la sezione **%packages** di un file Kickstart la quale impedisce al sistema di installare il gruppo di pacchetti **@core**. Questa impostazione installa un sistema minimo per un utilizzo dei container.

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](#).

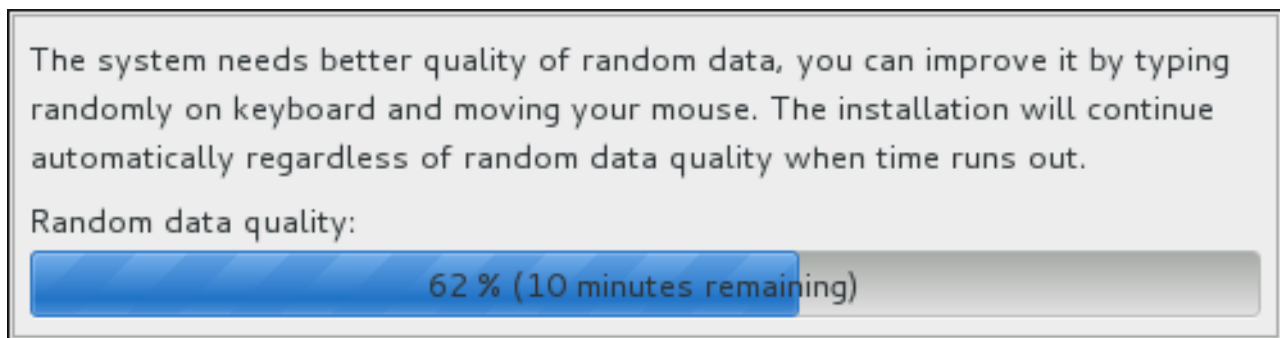


Figura 3.3. Gathering Entropy for Encryption

### Aiuto interno nell'installer grafico

In ogni schermata dell'interfaccia grafica dell'installer, e nell'utilità **Initial Setup**, è ora disponibile il pulsante **Aiuto** nell'angolo in alto sulla destra. La selezione di questo pulsante permetterà la visualizzazione della sezione relativa alla [Installation Guide](#) per la schermata corrente che utilizza il browser **Yelp**.

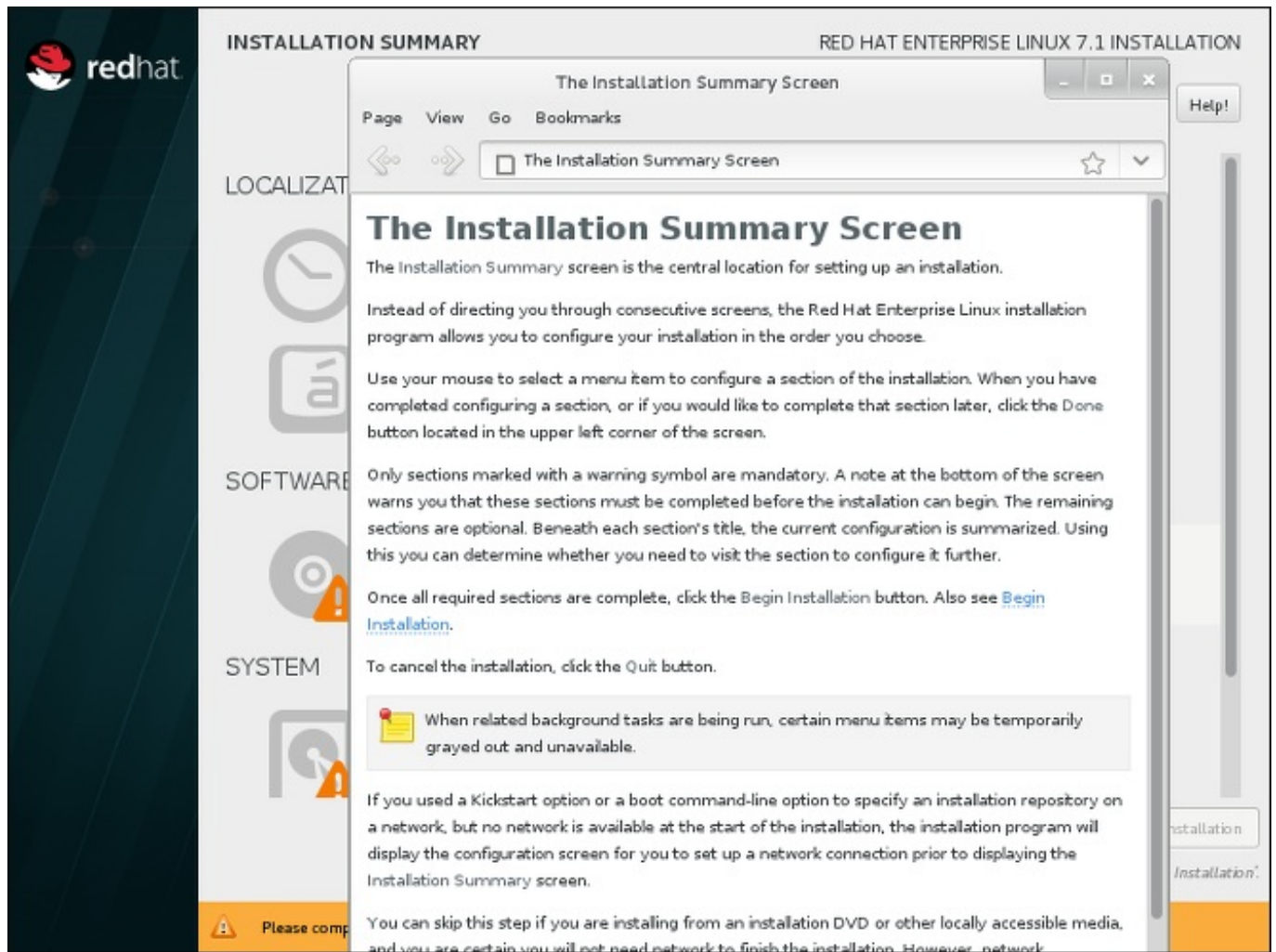


Figura 3.4. Anaconda built-in help

## 3.2. Boot loader

Il dispositivo d'installazione per IBM Power Systems utilizza ora il boot loader **GRUB2** al posto di **yaboot**. Per la variante big endian di Red Hat Enterprise Linux per POWER, viene preferito **GRUB2** anche se è possibile utilizzare ancora **yaboot**. La nuova variante di little endian ha bisogno di **GRUB2** per l'avvio.

L' [Installation Guide](#) è stata aggiornata con le informazioni necessarie all'impostazione di un server per l'avvio di rete per IBM Power Systems con **GRUB2**.



## Capitolo 4. Storage

### Cache 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.

Di seguito sono riportate le restrizioni sull'utilizzo di cache logical volume (LV):

- La cache LV deve essere un dispositivo di livello superiore, non può essere usata come thin-pool LV, immagine di un RAID LV o qualsiasi altro tipo di LV secondario.
- The cache LV sub-LVs (the origin LV, metadata LV, and data LV) can only be of linear, stripe, or RAID type.
- Le proprietà di una cache LV non possono essere modificate dopo la creazione. Per la modifica delle proprietà, rimuovere la cache e ricrearla con le proprietà desiderate.

### Gestione array di archiviazione con libStorageMgmt API

Con Red Hat Enterprise Linux 7.1 è supportata la gestione di array di archiviazione con **libStorageMgmt**, una API indipendente per l'array di archiviazione. L'API disponibile è stabile e uniforme e permette agli sviluppatori di gestire in modo programmatico diversi array, usufruendo altresì delle caratteristiche di accelerazione hardware fornite. Gli amministratori di sistemi possono utilizzare **libStorageMgmt** per configurare manualmente lo storage e automatizzare i compiti di gestione con il Command Line Interface incluso. Da ricordare che il plug-in **Targetd** non è completamente supportato e rimane una Anteprima di tecnologia.

- Filtro NetApp (ontap 7-Mode)
- Nexenta (solo nstor 3.1.x)
- SMI-S, per i seguenti rivenditori:
  - HP 3PAR
    - OS versione 3.2.1 o più recente
  - EMC VMAX e VNX
    - Solutions Enabler V7.6.2.48 o versione più recente
    - SMI-S Provider V4.6.2.18 hotfix kit o versione più recente
  - Provider HDS VSP Array non-embedded
    - Hitachi Command Suite v8.0 o versione più recente

Per maggiori informazioni su **libStorageMgmt** consultare il [capitolo rilevante nella Storage Administration Guide](#).

### Supporto per LSI Syncro

Red Hat Enterprise Linux 7.1 include il codice nel driver **megaraid\_sas** per abilitare gli adattatori LSI Syncro CS high-availability direct-attached storage (HA-DAS). Mentre il driver **megaraid\_sas** è completamente supportato per adattatori precedenti abilitati, l'uso di questi driver per Syncro CS è disponibile come Anteprima di Tecnologia. Il supporto per questo adattatore verrà fornito direttamente da LSI, l'integratore del sistema, o dal rivenditore. Incoraggiamo gli utenti che implementano Syncro CS su Red Hat Enterprise Linux 7.1, di inviare il proprio feedback a Red Hat e LSI. Per maggiori informazioni sulle soluzioni LSI Syncro CS, consultare <http://www.lsi.com/products/shared-das/pages/default.aspx>.

## LVM Application Programming Interface

Red Hat Enterprise Linux 7.1 introduce la nuova LVM application programming interface (API) come Anteprima di Tecnologia. Questa API viene usata per interrogare e controllare alcuni aspetti di LVM.

Per maggiori informazioni consultare il file d'intestazione **lvm2app.h**.

## Supporto DIF/DIX

DIF/DIX è una nuova caratteristica per lo SCSI Standard ed è una Anteprima di Tecnologia in Red Hat Enterprise Linux 7.1. DIF/DIX aumenta la dimensione del blocco del disco 512-byte da 512 a 520 byte, e aggiunge un Data Integrity Field (DIF). Il DIF archivia un valore checksum per il blocco dati calcolato dall'Host Bus Adapter (HBA) in presenza di un processo di scrittura. Il dispositivo di archiviazione conferma il valore del checksum in ricezione, archiviando sia i dati che il checksum. In presenza di una operazione di lettura, il checksum può essere verificato dal dispositivo di archiviazione e dall'HBA in ricezione.

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

## Output e controllo errore della sintassi del device-mapper-multipath migliorati

**device-mapper-multipath** è stato migliorato per la verifica più efficace del file **multipath.conf**. Ne risulta che se **multipath.conf** presenta una riga che non può essere analizzata, **device-mapper-multipath** riporta l'errore ignorando la riga, evitando così una analisi incorretta.

Sono state aggiunte anche le seguenti espressioni wildcard per il comando **multipathd show paths format**:

- %N e %n rispettivamente per l'host e i nomi del Fibre Channel World Wide Node target.
- %R e %r rispettivamente per l'host e i nomi del Fibre Channel World Wide Port target.

Ora è più semplice associare i multipath con host Fibre Channel specifici, target e rispettive porte, permettendo una gestione più efficiente della configurazione dello storage.

## Capitolo 5. File Systems

### Supporto per il file system Btrfs

Il file system **Btrfs** (B-Tree) è supportato come Anteprema di tecnologia in Red Hat Enterprise Linux 7.1, esso offre funzionalità avanzate di gestione, affidabilità e scalabilità. Permette altresì agli utenti di creare istantanee e di avere una gestione del dispositivo integrato e processi di compressione.

### 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.

### Supporto di Parallel NFS

Il Parallel NFS (pNFS) è parte dello standard v4.1 di NFS il quale permette ai client di accedere ai dispositivi di archiviazione direttamente ed in parallelo. L'architettura di pNFS migliora la scalabilità e le prestazioni associate con i server NFS con diversi carichi di lavoro.

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 continua a lavorare insieme ai suoi partner e con i progetti della open source, per riconoscere nuovi tipi di layout pNFS e per fornire un supporto futuro ad un numero maggiore di layout.

Per maggiori informazioni su pNFS consultare <http://www.pnfs.com/>.

## Capitolo 6. Kernel

### Supporto per i dispositivi a blocchi Ceph

I moduli **libceph.ko** e **rbd.ko** sono stati aggiunti al kernel di Red Hat Enterprise Linux 7.1. I suddetti moduli permettono ad un host di Linux di riconoscere un dispositivo a blocchi Ceph come voce del dispositivo a disco regolare, da montare su una directory formattata con un file system standard, ad esempio **XFS** o **ext4**.

Da notare che il modulo CephFS, **ceph.ko**, non è attualmente supportato in Red Hat Enterprise Linux 7.1.

### Aggiornamenti simultanei Flash MCL

In Red Hat Enterprise Linux 7.1 i Microcode level upgrades (MCL) sono abilitati sulle architetture IBM System z, e possono essere applicati senza interessare le operazioni I/O sul supporto di memorizzazione flash e notificare agli utenti i cambiamenti sul livello del servizio hardware.

### Patch del kernel dinamico

Red Hat Enterprise Linux 7.1 introduce **kpatch**, una "utilità di patch del kernel" dinamico, come Anteprima di tecnologia. **kpatch** permette agli utenti di gestire una raccolta di patch del kernel binario utilizzabili per un patch dinamico del kernel senza il riavvio. Da notare che **kpatch** è supportato solo per architetture AMD64 e Intel 64.

### Crashkernel con più di una 1 CPU

Red Hat Enterprise Linux 7.1 permette l'avvio di crashkernel con più di una CPU. Questa funzione è supportata come Anteprima di Tecnologia.

### Target dm-era

Red Hat Enterprise Linux 7.1 introduce il target del device-mapper dm-era come Anteprima di Tecnologia. dm-era tiene traccia dei blocchi usati per la scrittura all'interno di un periodo di tempo definito dall'utente chiamato "era". Ogni istanza target "era", conserva l'era corrente come contatore ad incremento costante a 32-bit. Questo target permette ad un software di backup di sapere quale blocco è stato modificato dall'ultimo backup. Esso Permette altresì un annullamento parziale dei contenuti di una cache, per ripristinare la coerenza della cache dopo il ripristino ad una istantanea del rivenditore. Il target dm-era deve essere usato insieme con il target dm-cache.

### Driver del kernel Cisco VIC

Il driver del kernel Cisco VIC Infiniband è stato aggiunto al Red Hat Enterprise Linux 7.1 come Anteprima di tecnologia. Questo driver permette l'uso di semantiche simili al Remote Directory Memory Access (RDMA) su architetture Cisco proprietarie.

### Miglioramento gestione entropia in hwrng

In Red Hat Enterprise Linux 7.1 è stato migliorato il supporto di hardware RNG (hwrng) paravirtualizzato per i guest Linux tramite virtio-rng. In precedenza il demone **rngd** aveva la necessità di essere riavviato all'interno del guest, e direzionato nel pool dell'entropia del kernel. Con Red Hat Enterprise Linux 7.1, è stata rimossa la fase manuale. Un nuovo thread **khwrngd** è in grado di ottenere l'entropia dal dispositivo **virtio-rng**, se il livello di entropia del guest è inferiore a un valore specifico. La trasparenza di questo processo apporta benefici sulla sicurezza a tutti i guest di Red Hat Enterprise Linux, grazie alla disponibilità di hardware RNG

paravirtualizzato fornito dagli host KVM.

## Miglioramento prestazioni Load-Balancing dello Scheduler

In precedenza il load-balancing dello Scheduler veniva effettuato per tutte le CPU inattive. Con Red Hat Enterprise Linux 7.1 il load balancing "idle" per una CPU inattiva, viene eseguito solo quando la CPU stessa è stata programmata per il load balancing. Questo nuovo comportamento riduce il tasso di load balancing su CPU non inattive e di conseguenza la quantità non necessaria di lavoro svolto dallo scheduler, migliorando così le prestazioni.

## newidle Balance migliorato nello scheduler

È stato modificato il comportamento dello scheduler in modo da arrestare le ricerche di compiti nel **newidle** balance code, se in presenza di compiti eseguibili, migliorando così le prestazioni generali.

## HugeTLB supporta l'allocazione di pagine 1GB Huge per-nodo

Red Hat Enterprise Linux 7.1 permette ora di supportare l'allocazione di pagine molto grandi durante il runtime. In questo modo l'utente di **hugetlbfs** da 1GB è in grado di specificare il nodo Non-Uniform Memory Access (NUMA) al quale assegnare 1GB durante il runtime.

## Nuovo meccanismo di locking basato su MCS

Red Hat Enterprise Linux 7.1 introduce un nuovo meccanismo di locking, MCS lock. Questo nuovo meccanismo riduce sensibilmente l'overhead di **spinlock** nei sistemi molto grandi, aumentando così l'efficienza di **spinlocks** con Red Hat Enterprise Linux 7.1.

## Dimensione Stack del processo aumentata da 8KB a 16KB

Iniziando con Red Hat Enterprise Linux 7.1, la dimensione dello stack del processo del kernel è stata aumentata da 8KB a 16KB per assistere i processi molto grandi che utilizzano memoria sullo stack.

## Funzionalità uprobe e uretprobe abilitate in perf e systemtap

Con Red Hat Enterprise Linux 7.1, le funzionalità **uprobe** e **uretprobe** funzionano correttamente con il comando **perf** e lo script **systemtap**.

## Controllo consistenza dati End-To-End

Con Red Hat Enterprise Linux 7.1 è ora supportato il controllo della consistenza dei dati End-To-End. Così facendo è stata migliorata l'integrità dei dati impedendone la loro corruzione e/o perdita.

## DRBG su sistemi a 32-Bit

Con Red Hat Enterprise Linux 7.1, il deterministic random bit generator (DRBG) è stato aggiornato per poter operare su sistemi a 32-bit.

## Supporto per dimensioni crashkernel molto grandi

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.

## Capitolo 7. Virtualizzazione

### Aumentato il numero massimo di vCPU in KVM

Il numero massimo di virtual CPU (vCPU) supportate in un guest KVM è stato aumentato a 240. Questa impostazione aumenta la quantità di unità di processazione virtuali che un utente è in grado di assegnare al guest. Così facendo è possibile aumentare le prestazioni.

### Supporto 5th Generation Intel Core New Instructions in QEMU, KVM e libvirt API

In Red Hat Enterprise Linux 7.1 è stato aggiunto il supporto per i processori 5th Generation Intel Core all'hypervisor QEMU, KVM kernel code e **libvirt** API. Ciò permette ai guest KVM di usare le seguenti istruzioni e funzionalità: ADCX, ADOX, RDSFEED, PREFETCHW e supervisor mode access prevention (SMAP).

### Supporto USB 3.0 per guest KVM

Red Hat Enterprise Linux 7.1 introduce un supporto USB migliorato attraverso l'emulazione USB 3.0 hostadapter (xHCI) come Anteprema di tecnologia.

### Compressione per il comando dump-guest-memory

Con Red Hat Enterprise Linux 7.1 il comando **dump-guest-memory** supporta ora la compressione crash dump. Questa impostazione permette agli utenti non in grado di utilizzare **virsh dump**, di usare una quantità minore di spazio del disco fisso per operazioni crash dump del guest. Altresì, la memorizzazione di un crash dump compresso del guest richiederà una quantità di tempo minore rispetto alla stessa operazione con un crash dump non compresso.

### Open Virtual Machine Firmware

L'Open Virtual Machine Firmware (OVMF) è disponibile come Anteprema di tecnologia in Red Hat Enterprise Linux 7.1. OVMF è un ambiente per l'avvio sicuro UEFI per guest AMD64 e Intel 64.

### Migliorate le prestazioni di rete su Hyper-V

Sono ora supportate nuove funzionalità del driver di rete Hyper-V per il miglioramento delle prestazioni di rete. Per esempio, Receive-Side Scaling, Large Send Offload, Scatter/Gather I/O sono ora supportati; è stato altresì aumentato il throughput della rete.

### hypervcopyd in hyperv-daemons

Il demone **hypervcopyd** è stato aggiunto ai pacchetti *hyperv-daemons*. **hypervcopyd** è una implementazione della funzionalità del servizio di copiatura del file per i guest di Linux eseguiti su host Hyper-V 2012 R2. Ora un host sarà in grado di copiare un file (attraverso VMBUS) nel guest di Linux.

### Nuove funzioni in libguestfs

Red Hat Enterprise Linux 7.1 introduce un certo numero di nuove funzioni in **libguestfs**, un insieme di strumenti per l'accesso e la modifica delle immagini del disco di una macchina virtuale.

#### Nuovi strumenti

- ✦ **virt-builder** — un nuovo strumento per la compilazione delle immagini della macchina virtuale. Usare virt-builder per una creazione veloce e sicura di guest, e per la loro personalizzazione.
- ✦ **virt-customize** — un nuovo strumento per la personalizzazione delle immagini del disco della macchina virtuale. Usare virt-customize per installare pacchetti, modificare i file di configurazione eseguire gli script e impostare le password.
- ✦ **virt-diff** — un nuovo strumento per mostrare le differenze tra i file system di due macchine virtuali. Usare virt-diff per sapere quali sono i file modificati nelle istantanee.
- ✦ **virt-log** — un nuovo strumento per elencare i file di log dei guest. virt-log supporta una varietà di guest inclusi quelli tradizionali di Linux, Linux con journal e log di eventi di Windows.
- ✦ **virt-v2v** — un nuovo strumento per la conversione dei guest da un hypervisor esterno per l'esecuzione su KVM, gestito da libvirt, OpenStack, oVirt, Red Hat Enterprise Virtualization (RHEV) e altri target. Attualmente virt-v2v è in grado di convertire guest Red Hat Enterprise Linux e Windows in esecuzione su Xen e VMware ESX.

## Flight Recorder Tracing

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.

Per informazioni dettagliate su come configurare e utilizzare il flight recorder tracing consultare la [Virtualization Deployment and Administration Guide](#).

## 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.

## Capitolo 8. Clustering

### Dynamic Token Timeout per Corosync

È stata aggiunta l'opzione **token\_coefficient** al **Corosync Cluster Engine**. **token\_coefficient** viene usato solo quando si specifica la sezione **odelist** e sono presenti un minimo di tre nodi. In questa situazione il timeout del token è il seguente:

```
[token + (amount of nodes - 2)] * token_coefficient
```

Ciò permette una modifica del cluster senza cambiare manualmente il timeout ogni qualvolta viene aggiunto un nuovo nodo. Il valore predefinito è 650 millisecondi, ma può essere impostato su 0 per una sua rimozione.

Questa funzione permette a **Corosync** di gestire l'aggiunta e la rimozione dinamiche dei nodi.

### Miglioramenti del Corosync Tie Breaker

**auto\_tie\_breaker** di **Corosync** è stato migliorato, ora è possibile utilizzare le opzioni necessarie per processi di modifica e configurazione più flessibili dei nodi tie breaker. Gli utenti sono ora in grado di selezionare un elenco di nodi per garantire un quorum in presenza di una condizione cluster split, oppure se mantenere un quorum su un nodo con l'ID più basso o più alto.

### Miglioramenti al Red Hat High Availability

Grazie alla release di Red Hat Enterprise Linux 7.1, **Red Hat High Availability Add-On** supporta ora le seguenti funzionalità. Per informazioni aggiuntive consultare il manuale *High Availability Add-On Reference*.

- Il comando **pcs resource cleanup** è in grado ora di resettare lo stato e **failcount** per tutte le risorse.
- È possibile specificare un parametro **lifetime** per il comando **pcs resource move**, e indicare così il periodo di tempo per un vincolo delle risorse, permesso a questo comando.
- Usare il comando **pcs acl** per impostare i permessi degli utenti locali abilitandoli ad un accesso, di sola lettura o sola scrittura, alla configurazione del cluster tramite l'access control list (ACL).
- Il comando **pcs constraint** supporta ora la configurazione di opzioni specifiche oltre a quelle generali per le risorse.
- Il comando **pcs resource create** supporta il parametro **disabled** per indicare che la risorsa creata non sarà automaticamente avviata.
- Il comando **pcs cluster quorum unblock** impedisce al cluster di attendere tutti i nodi quando stabilisce un quorum.
- È possibile configurare l'ordine del gruppo di risorse con i parametri **before** e **after** del comando **pcs resource create**.
- È possibile eseguire il backup della configurazione del cluster usando un tarball e ripristinando i file di configurazione del cluster su tutti i nodi dal backup, con le opzioni **backup** e **restore** del comando **pcs config**.



## Capitolo 9. Compiler e strumenti

### Supporto hot-patching per Linux sui binari System z

GNU Compiler Collection (GCC) rende possibile il supporto per l'on-line patching dei codici multi-thread di Linux su binari System z. La selezione di funzioni specifiche per l'hot-patching viene abilitata utilizzando un "attributo della funzione", così facendo è possibile abilitare hot-patching per tutte le funzioni usando l'opzione della linea di comando **-mhotpatch**.

L'uso di hot-patching ha un impatto negativo sulle prestazioni e sulla dimensione del software. Per questo motivo è consigliato usare hot-patching solo per funzioni specifiche.

Su Red Hat Enterprise Linux 7.0, hot-patching sui binari System z per Linux era una Anteprima di tecnologia. Con la disponibilità di Red Hat Enterprise Linux 7.1 ora è completamente supportato.

### Miglioramenti Performance Application Programming Interface

Red Hat Enterprise Linux 7 include la **Performance Application Programming Interface** (PAPI). PAPI è una specifica per le interfacce multi-piattaforma per i contatori delle prestazioni hardware su microprocessori moderni. I suddetti contatori sono disponibili come un insieme di registratori in grado di contare gli eventi, i quali rappresentano il numero di segnali specifici relativi alla funzione di un processore. Il controllo di questi eventi può essere utilizzato in una varietà di modi durante il processo di ottimizzazione e analisi delle prestazioni.

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** è un profiler per i sistemi Linux. Il profiling viene eseguito in modo trasparente nel background, e i dati possono essere raccolti in ogni istante. Con Red Hat Enterprise Linux 7.1 **OProfile** è stato aggiornato per rendere disponibile il supporto alle seguenti famiglie di processori: Intel Atom Processor C2XXX, 5th Generation Intel Core Processors, IBM Power8, AppliedMicro X-Gene e ARM Cortex A57.

### OpenJDK8

Come Anteprima di tecnologia Red Hat Enterprise Linux 7.1 presenta i pacchetti *java-1.8.0-openjdk* con l'ultimissima versione di Open Java Development Kit (OpenJDK), OpenJDK8. Questi pacchetti forniscono una implementazione conforme di Java SE 8, e possono essere usati in parallelo con i pacchetti *java-1.7.0-openjdk* esistenti, ancora disponibili in Red Hat Enterprise Linux 7.1.

Java 8 rende disponibili numerosi miglioramenti, come ad esempio le espressioni Lambda, i metodi predefiniti, un nuovo insieme di API, JDBC 4.2 e il supporto hardware AES e altro ancora. Oltre ai miglioramenti sopra indicati, OpenJDK8 apporta numerosi aggiornamenti sulle prestazioni e altre correzioni.

### sosreport sostituisce snap

**snap** è stato rimosso dal pacchetto *powerpc-utils*, le sue funzionalità sono state integrate in **sosreport**.

### Supporto GDB per Little-Endian 64-bit PowerPC

Red Hat Enterprise Linux 7.1 implementa il supporto per l'architettura a 64-bit PowerPC little-endian in GNU Debugger (GDB).

## Miglioramento di Tuna

**Tuna** è uno strumento utilizzabile per il miglioramento dei parametri dello scheduler come la politica, la priorità RT e l'affinità della CPU. Con Red Hat Enterprise Linux 7.1 la GUI di **Tuna** è stata migliorata per richiedere l'autorizzazione ai permessi root quando avviata, in questo modo l'utente non avrà la necessità di eseguire il desktop come utente root per invocare la GUI di **Tuna**. Per maggiori informazioni su **Tuna** consultare la [Tuna User Guide](#).

## Capitolo 10. Networking

### Trusted Network Connect

Red Hat Enterprise Linux 7.1 introduce il Trusted Network Connect come Anteprima di Tecnologia. Il Trusted Network Connect viene usato con soluzioni network access control (NAC), come ad esempio TLS, 802.1X, o IPsec, per integrare le informazioni relative al sistema (come ad esempio le impostazioni del sistema operativo, i pacchetti installati e altro, definiti come misure di integrità). Il Trusted Network Connect viene usato per verificare queste informazioni con le politiche di accesso alla rete, prima di permettere al sistema in questione di accedere alla rete.

### Funzione SR-IOV nel driver qlcnic

È stato aggiunto al driver **qlcnic** come Anteprima di Tecnologia il supporto per il Single Root I/O virtualization (SR-IOV). Il supporto per questa funzione verrà fornito direttamente da QLogic. Esortiamo gli utenti a fornire il loro feedback a QLogic e Red Hat. Altre funzioni presenti nel driver qlcnic sono ancora supportate.

### Berkeley Packet Filter

È stato aggiunto a Red Hat Enterprise Linux 7.1. il supporto per un Berkeley Packet Filter (BPF) based *traffic classifier*. BPF viene usato durante il filtro dei pacchetti per i socket, per sand-boxing in *secure computing mode* (seccomp), e con Netfilter. BPF una implementazione "just-in-time" per le architetture più importanti e presenta una sintassi ricca per la compilazione dei filtri.

### Stabilità migliorata dell'orologio

I risultati di alcuni test precedentemente eseguiti indicavano che disabilitando la capacità tickless del kernel si migliorava sensibilmente la stabilità dell'orologio del sistema. La modalità tickless può essere disabilitata aggiungendo **nohz=off** ai parametri per l'opzione d'avvio del kernel. Tuttavia l'implementazione di nuovi miglioramenti del kernel con la release di Red Hat Enterprise Linux 7.1, hanno apportato una maggiore stabilità dell'orologio del sistema, e la differenza in stabilità con o senza **nohz=off** dovrebbe essere minima per la maggior parte degli utenti. Ciò è molto utile per applicazioni per la sincronizzazione dell'ora con **PTP** e **NTP**.

### Pacchetti libnetfilter\_queue

È stato aggiunto a Red Hat Enterprise Linux 7.1 il pacchetto *libnetfilter\_queue*. **libnetfilter\_queue** è una libreria per lo spazio utente in grado di fornire una API ai pacchetti messi in coda dal filtro del kernel. Esso è in grado di abilitare la ricezione dei pacchetti messi in coda dal sottosistema **nfnetlink\_queue** del kernel, l'analisi dei pacchetti, la modifica delle intestazioni dei pacchetti e il reinserimento dei pacchetti modificati.

### Miglioramenti collaborazione

Il pacchetto *libteam* è stato aggiornato alla versione **1.14-1** in Red Hat Enterprise Linux 7.1. Sono ora disponibili diverse correzioni e miglioramenti, in particolare, **teamd** può essere rigenerato automaticamente da **systemd**, aumentandone notevolmente l'affidabilità.

### Driver Intel QuickAssist Technology

Il driver Intel QuickAssist Technology (QAT) è stato aggiunto al Red Hat Enterprise Linux 7.1, ed è in grado di abilitare l'hardware di QuickAssist il quale rende disponibile per il sistema, le capacità di crittografia per l'offload dell'hardware.

## Supporto LinuxPTP timemaster per il failover tra PTP e NTP

Il pacchetto *linuxptp* è stato aggiornato alla versione **1.4** in Red Hat Enterprise Linux 7.1. Sono ora disponibili diverse correzioni e miglioramenti, in particolare, supporto per il failover tra i domini **PTP** e i sorgenti **NTP** che utilizzano l'applicazione **timemaster**. In presenza di domini **PTP** multipli sulla rete, o per il ripristino di **NTP**, usare il programma **timemaster** per sincronizzare l'orologio del sistema su tutti i sorgenti dell'ora disponibili.

## initscripts di rete

È stato aggiunto il supporto per i nomi VLAN personalizzati in Red Hat Enterprise Linux 7.1. È stato migliorato il supporto per **IPv6** nei tunnel GRE: l'indirizzo interno ora è persistente durante i processi di riavvio.

## TCP Delayed ACK

In Red Hat Enterprise Linux 7.1 è stato aggiunto al pacchetto *iproute* il supporto per un TCP Delayed ACK configurabile. Usare il comando **ip route quickack** per poterlo abilitare.

## NetworkManager

È ora supportata l'opzione **larp\_rate** in Red Hat Enterprise Linux 7.1. **NetworkManager** è stato migliorato per facilitare la modifica dei nomi durante il processo di modifica dei nomi delle interfacce master con interfacce slave.

È stata aggiunta altresì un processo di priorità alla funzione auto-connect di **NetworkManager**. Se sono presenti più candidati per auto-connect, **NetworkManager** seleziona il collegamento con la priorità più alta. Se tutte le connessioni presenti hanno lo stesso valore, **NetworkManager** utilizza il comportamento predefinito e seleziona l'ultima connessione attiva.

## Spazi nomi di rete e VTI

È stato aggiunto al Red Hat Enterprise Linux 7.1 il supporto per il *virtual tunnel interface* (VTI) con spazio dei nomi di rete. Ciò permette il passaggio di traffico da un VTI ai diversi nomi di spazio quando i pacchetti sono incapsulati o de-incapsulati.

## Storage per la configurazione alternativa del plug-in MemberOf

La configurazione del plug-in **MemberOf** per la Directory Server 389 può essere ora archiviata in un suffisso mappato ad un database back-end. Questa impostazione permette alla configurazione del plug-in di **MemberOf** di essere replicata, facilitando così il mantenimento di una configurazione di **MemberOf** costante in un ambiente replicato da parte di un utente.

## Capitolo 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.

**Kubernetes** è disponibile tramite Red Hat e può essere utilizzato con i container. Per maggiori informazioni su Kubernetes consultare [Introduzione al Controllo dei container Docker con Kubernetes](#).

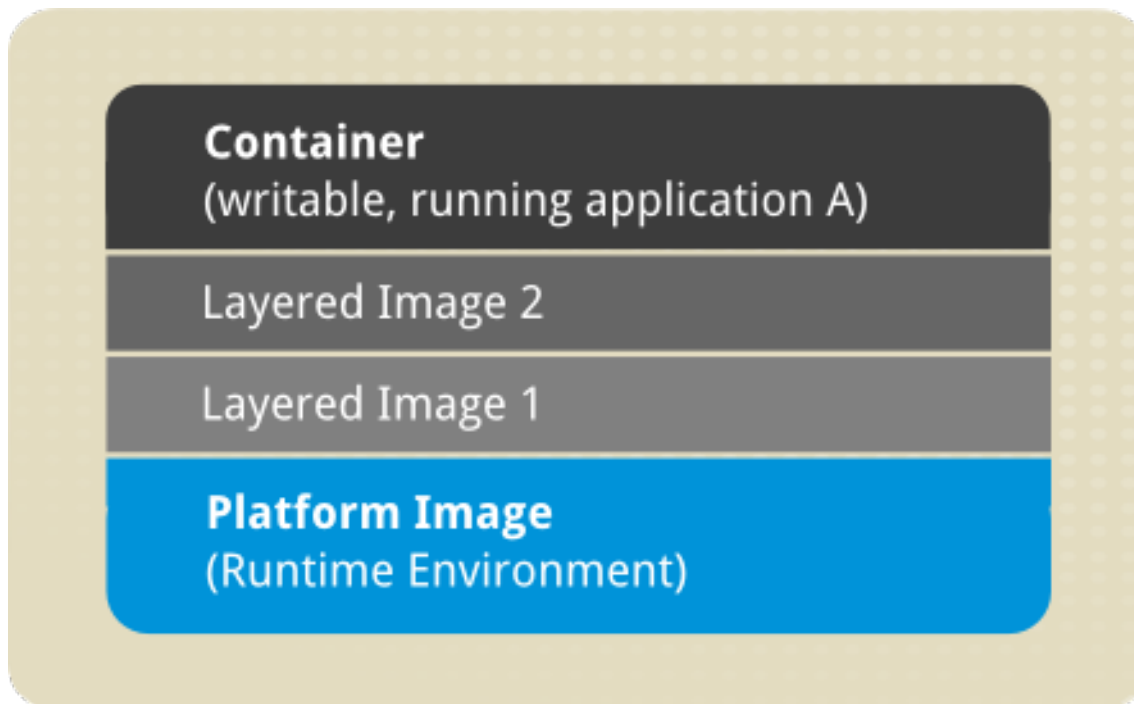
Linux containers are supported running on hosts with SELinux enabled. SELinux is not supported when the `/var/lib/docker` directory is located on a volume using the B-tree file system (Btrfs).

### 11.1. Components of docker Formatted Containers

The docker container format works with the following fundamental components:

- *Container* - un sandbox delle applicazioni. Ogni container si basa su una *immagine* che contiene i dati necessari per la configurazione. Al momento di lanciare un container da una immagine, un livello modificabile viene aggiunto sopra l'immagine. Ogni qualvolta che si esegue il commit di un container (tramite il comando **docker commit**), verrà aggiunto un nuovo livello per l'archiviazione delle modifiche.
- *Image* – una istantanea statica della configurazione del container. L'immagine è un livello "in sola lettura" che non potrà mai essere modificato, tutte le modifiche verranno eseguite nel livello più alto modificabile, e verranno archiviate solo tramite la creazione di una nuova immagine. Ogni immagine dipende da una o più immagini genitore.

- ✦ *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 [Figura 11.1, «Livelli immagine con formato Docker»](#).
- ✦ *Registro* – un repository di immagini. I registri sono repository pubblici o privati che contengono immagini disponibili per il download. Alcuni registri permettono agli utenti di caricare le immagini e renderle disponibili ad altri.
- ✦ *Dockerfile* – un file di configurazione con informazioni sulla compilazione per le immagini Docker. Dockerfiles forniscono un modo per automatizzare, riutilizzare e condividere le procedure di compilazione.



**Figura 11.1. Livelli immagine con formato 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:

- ✦ *Implementazione rapida delle applicazioni* – i container includono requisiti minimi di runtime delle applicazioni, riducendone la dimensione e velocizzando i tempi di una implementazione.
- ✦ *Portabilità su diverse macchine* – una applicazione in grado con tutte le sue dipendenze, di essere raggruppata in un container indipendente dalla versione host del kernel Linux, dalla distribuzione della piattaforma o modello di implementazione. Questo container può essere trasferito su una macchina diversa che esegue Docker, ed eseguito senza alcun problema di compatibilità.
- ✦ *Controllo versione e riutilizzo del componente* – è possibile tracciare versioni successive di un container, controllarne le differenze o ripristinare le versioni precedenti. I container riutilizzano i componenti dei livelli precedenti, semplificandoli notevolmente.
- ✦ *Condivisione* – è possibile riutilizzare un repository remoto per la condivisione del container con altri. Red Hat fornisce un registro per questo tipo di processo. È possibile altresì configurare un repository privato.

- *Footprint semplice e overhead minimo* – Le immagini Docker sono generalmente piccole, ciò ne facilita la disponibilità e riduce i tempi di implementazione di nuovi container di applicazioni.
- *Gestione semplificata* – Docker riduce gli sforzi e i rischi derivati dalle dipendenze delle applicazioni.

### 11.3. Confronto con le macchine virtuali

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.

- È possibile creare o eliminare facilmente i container. Le macchine virtuali invece hanno bisogno di installazioni complete e richiedono un numero maggiore di risorse informatiche per l'esecuzione.
- I container sono molto semplici, e per questo motivo è possibile eseguire simultaneamente più container di macchine virtuali su una macchina host.
- I container condividono le risorse in modo più efficiente. Le macchine virtuali sono isolate. Per questo motivo è possibile semplificare l'uso di versioni multiple di una applicazione in esecuzione nei container. Per esempio, i binari condivisi non sono duplicati sul sistema.
- È possibile migrare le macchine virtuali durante la loro esecuzione, tuttavia i container non possono essere migrati se prima non sono stati arrestati. Solo dopo il loro arresto sarà possibile spostarli tra le macchine host.

I container non devono essere usati in sostituzione alle macchine virtuali, è sempre necessario determinare lo scenario migliore per l'applicazione desiderata.

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 Using the libvirt-lxc Tooling Have Been Deprecated

The following libvirt-lxc packages are deprecated starting with Red Hat Enterprise Linux 7.1:

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

The Linux containers functionality is now focused on the docker command-line interface. Please note: libvirt-lxc may not be shipped in future releases of Red Hat Enterprise Linux (including Red Hat Enterprise Linux 7), and may be considered for formal removal in a future release of Red Hat Enterprise Linux 7.



## Capitolo 12. Autenticazione ed interoperabilità

### 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](#).

### Supporto per la migrazione da WinSync a Trust

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](#).

### Integrazione SSSD per il Common Internet File System

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](#).

### Strumento di gestione del Certificate Authority

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.

### Migliorata la granularità per il controllo d'accesso

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.

### Accesso al dominio limitato per utenti non privilegiati

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](#).

## Configurazione del provider dei dati automatica

Il comando **ipa-client-install** ora configura per impostazione predefinita **SSSD** come provider dei dati per il servizio sudo. È possibile disabilitare questo processo usando l'opzione **--no-sudo**. È stata aggiunta altresì una opzione **--nisdomain** per specificare il nome del dominio NIS per l'installazione del client Identity Management, e l'opzione **--no-nisdomain** per impedire l'impostazione del nome del dominio NIS. Se non utilizzate queste due opzioni verrà implementato il dominio IPA.

## Utilizzo provider sudo AD e LDAP

Il provider AD è un backend usato per la connessione con un server Active Directory. In Red Hat Enterprise Linux 7.1, l'utilizzo del provider sudo AD insieme con il provider LDAP è supportato come Antepima di tecnologia. Per abilitare il provider sudo AD, aggiungere le impostazioni **sudo\_provider=ad** nella sezione del dominio del file **sssd.conf**.

## 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**).

## Capitolo 13. Sicurezza

### SCAP Security Guide

Con Red Hat Enterprise Linux 7.1 è stato incluso il pacchetto *scap-security-guide* il quale fornisce le linee guida sulla sicurezza e i meccanismi di convalida associati. Le linee guida sono specificate nel *Security Content Automation Protocol* (SCAP), il quale rappresenta un catalogo sui consigli pratici. La **SCAP Security Guide** presenta i dati necessari per eseguire scansioni sulla conformità della sicurezza dei sistemi, in relazione a determinati requisiti di sicurezza di una politica; sono inclusi una descrizione scritta e un test automatizzato (probe). Automatizzando il test, la **SCAP Security Guide** fornisce un metodo affidabile e conveniente per la verifica della conformità dei sistemi.

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.

### Politica di SELinux

In Red Hat Enterprise Linux 7.1 la politica SELinux è stata modificata; i servizi sprovvisti di politica SELinux, che in precedenza erano in grado di essere eseguiti nel dominio **init\_t**, ora vengono eseguiti in un nuovo dominio **unconfined\_service\_t**. Consultare il capitolo [Processi non confinati](#) nella [SELinux User's and Administrator's Guide](#) di Red Hat Enterprise Linux 7.1.

### Nuove funzioni in OpenSSH

Il set **OpenSSH** è stato aggiornato alla versione 6.6.1p1 e ora sono disponibili nuove funzioni relative alla crittografia:

- Lo scambio di chiavi con elliptic-curve **Diffie-Hellman** in **Curve25519** di Daniel Bernstein è ora supportato. Questo metodo è quello predefinito previo supporto disponibile sia sul server che sul client.
- È stato aggiunto il supporto per l'utilizzo dello schema di firma elliptic-curve **Ed25519** come tipo di chiave pubblica. **Ed25519**, utilizzabile sia per gli utenti che per le chiavi dell'host, offre una maggiore sicurezza e migliori prestazioni rispetto a **ECDSA** e **DSA**.
- È stato aggiunto un nuovo formato di chiave-privata il quale utilizza la funzione **bcrypt** key-derivation (KDF). Per impostazione predefinita questo formato viene usato per le chiavi **Ed25519** ma può essere richiesto per altri tipi di chiavi.
- È stato aggiunto un nuovo cifrario per il trasporto **chacha20-poly1305@openssh.com**. Esso combina **ChaCha20** di Daniel Bernstein e il **Poly1305** message authentication code (MAC).

### Nuove funzioni in Libreswan

L'implementazione **Libreswan** di IPsec VPN è stata aggiornata alla versione 3.12, ora sono disponibili nuove funzioni e miglioramenti:

- Sono stati aggiunti nuovi tipi di cifrari
- **IKEv2** support has been improved.
- È stato aggiunto il supporto per la catena del certificato intermediario in **IKEv1** e **IKEv2**.
- È stata migliorata la gestione dei collegamenti.
- È stata migliorata l'interoperabilità con i sistemi OpenBSD, Cisco e Android.
- È stato migliorato il supporto per **systemd**.
- È stato aggiunto il supporto per **CERTREQ** e per le statistiche del traffico.

## Nuove funzioni in TNC

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.
- Il supporto per l'Attestation IMV è stato migliorato tramite l'implementazione di un nuovo elemento di lavoro TPMRA.
- È stato aggiunto il supporto per una REST API basata su JSON con SWID IMV.
- 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.
- Numerosi bug sono stati corretti nei protocolli esistenti **IF-TNCCS (PB-TNC, IF-M (PA-TNC))** e nella coppia **OS IMC/IMV**.

## Nuove funzioni in GnuTLS

L'implementazione **GnuTLS** dei protocolli **SSL**, **TLS** e **DTLS** è stata aggiornata alla versione 3.3.8, ora sono disponibili nuove funzioni e miglioramenti:

- È stato aggiunto il supporto per **DTLS 1.2**.
- È stato aggiunto il supporto per *Application Layer Protocol Negotiation* (ALPN).
- Sono state migliorate le prestazioni delle suite del cifrario elliptic-curve.
- Sono state aggiunte nuove suite del cifrario, **RSA-PSK** e **CAMELLIA-GCM**.
- È stato aggiunto il supporto nativo per lo standard *Trusted Platform Module* (TPM).
- È stato migliorato il supporto per le **PKCS#11** smart card e per gli *hardware security module* (HSM).

- ✦ Miglioramenti apportati per la conformità agli standard di sicurezza *FIPS 140 (Federal Information Processing Standards)*.

## Capitolo 14. Desktop

### Supporto per le immagini Quad-buffered OpenGL Stereo

**GNOME Shell** e **Mutter** ora sono in grado di permettere all'utente di utilizzare le immagini quad-buffered OpenGL stereo su hardware supportato. Per fare questo è necessario avere la versione 337 di NVIDIA Display Driver o una versione più recente.

### Provider di account online

Una nuova chiave **GSettings**, `org.gnome.online-accounts.whitelisted-providers`, è stata aggiunta su **GNOME Online Accounts** (resa disponibile tramite il pacchetto *gnome-online-accounts*). Questa chiave fornisce un elenco di provider per account online caricabili all'avvio. Specificando questa chiave gli amministratori di sistema possono abilitare provider specifici o disabilitarne altri.

## Capitolo 15. Supporto e gestione

### ABRT Authorized Micro-Reporting

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.

Consultare il Portale clienti [per maggiori informazioni su questa funzionalità](#).

## Capitolo 16. Red Hat Software Collection

Red Hat Software Collection è un insieme di contenuti di Red Hat in grado di fornire un set di linguaggi di programmazione dinamici, server del database e pacchetti relativi, installabili e utilizzabili su tutte le release supportate di Red Hat Enterprise Linux 6 e Red Hat Enterprise Linux 7 su architetture AMD64 e Intel 64.

Linguaggi dinamici, server del database e altri strumenti distribuiti con Red Hat Software Collection, non sostituiscono gli strumenti predefiniti disponibili con Red Hat Enterprise Linux, e non devono essere preferiti ai suddetti strumenti.

Red Hat Software Collection utilizza un meccanismo alternativo per il packaging basato sull'utilità **sc1**, e fornisce un insieme parallelo di pacchetti. Questo insieme permette l'uso di versioni alternative su Red Hat Enterprise Linux. Utilizzando **sc1** gli utenti possono scegliere in qualsiasi momento la versione del pacchetto da eseguire.



### Importante

Red Hat Software Collection ha un ciclo di vita e termini di supporto più breve rispetto a Red Hat Enterprise Linux. Per maggiori informazioni consultare il [Ciclo di vita di Red Hat Software Collection](#).

Red Hat Developer Toolset fa ora parte di Red Hat Software Collection ed è incluso come raccolta software separata. Red Hat Developer Toolset è stato creato per gli sviluppatori che utilizzano una piattaforma Red Hat Enterprise Linux, e fornisce le versioni correnti di GNU Compiler Collection, GNU Debugger, piattaforma di sviluppo Eclipse, debugging e gli strumenti per il controllo delle prestazioni.

Consultare la [Documentazione di Red Hat Software Collection](#) per informazioni sui componenti inclusi nell'insieme, per i requisiti del sistema, per le problematiche conosciute, per l'utilizzo e per le specifiche degli Insiemi software.

Consultare la [Documentazione su Red Hat Developer Toolset](#) per maggiori informazioni sui componenti inclusi in questo insieme software, per l'installazione, utilizzo, problematiche conosciute e altro ancora.



## Capitolo 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](#).

## Parte II. Driver del dispositivo

Questo capitolo fornisce un elenco completo di tutti i driver del dispositivo aggiornati in Red Hat Enterprise Linux 7.1.

## Capitolo 18. Aggiornamenti driver di archiviazione

- ✦ Il driver **hpsa** è stato aggiornato alla versione 3.4.4-1-RH1.
- ✦ Il driver **qla2xxx** è stato aggiornato alla versione 8.07.00.08.07.1-k1.
- ✦ Il driver **qla4xxx** è stato aggiornato alla versione 5.04.00.04.07.01-k0.
- ✦ Il driver **qlcnic** è stato aggiornato alla versione 5.3.61.
- ✦ Il driver **netxen\_nic** è stato aggiornato alla versione 4.0.82.
- ✦ Il driver **qlge** è stato aggiornato alla versione 1.00.00.34.
- ✦ Il driver **bnx2fc** è stato aggiornato alla versione 2.4.2.
- ✦ Il driver **bnx2i** è stato aggiornato alla versione 2.7.10.1.
- ✦ Il driver **cnic** è stato aggiornato alla versione 2.5.20.
- ✦ Il driver **bnx2x** è stato aggiornato alla versione 1.710.51-0.
- ✦ Il driver **bnx2** è stato aggiornato alla versione 2.2.5.
- ✦ Il driver **megaraid\_sas** è stato aggiornato alla versione 06.805.06.01-rc1.
- ✦ Il driver **mpt2sas** è stato aggiornato alla versione 18.100.00.00.
- ✦ Il driver **ipr** è stato aggiornato alla versione 2.6.0.
- ✦ I pacchetti *kmod-lpfc* sono stati aggiunti a Red Hat Enterprise Linux 7, e permettono una maggiore stabilità quando si utilizzano i driver lpfc con gli adattatori Fibre Channel (FC) e Fibre Channel over Ethernet (FCoE). Il driver **lpfc** è stato aggiornato alla versione 0:10.2.8021.1.
- ✦ Il driver **be2iscsi** è stato aggiornato alla versione 10.4.74.0r.
- ✦ Il driver **nvme** è stato aggiornato alla versione 0.9.

## Capitolo 19. Aggiornamenti driver di rete

- Il driver **bna** è stato aggiornato alla versione 3.2.23.Or.
- Il driver **cxgb3** è stato aggiornato alla versione 1.1.5-ko.
- Il driver **cxgb3i** è stato aggiornato alla versione 2.0.0.
- Il driver **iw\_cxgb3** è stato aggiornato alla versione 1.1.
- Il driver **cxgb4** è stato aggiornato alla versione 2.0.0-ko.
- Il driver **cxgb4vf** è stato aggiornato alla versione 2.0.0-ko.
- Il driver **cxgb4i** è stato aggiornato alla versione 0.9.4.
- Il driver **iw\_cxgb4** è stato aggiornato alla versione 0.1.
- Il driver **e1000e** è stato aggiornato alla versione 2.3.2-k.
- Il driver **igb** è stato aggiornato alla versione 5.2.13-k.
- Il driver **igbvf** è stato aggiornato alla versione 2.0.2-k.
- Il driver **ixgbe** è stato aggiornato alla versione 3.19.1-k.
- Il driver **ixgbev** è stato aggiornato alla versione 2.12.1-k.
- Il driver **i40e** è stato aggiornato alla versione 1.0.11-k.
- Il driver **i40evf** è stato aggiornato alla versione 1.0.1.
- Il driver **e1000** è stato aggiornato alla versione 7.3.21-k8-NAPI.
- Il driver **m1x4\_en** è stato aggiornato alla versione 2.2-1.
- Il driver **m1x4\_ib** è stato aggiornato alla versione 2.2-1.
- Il driver **m1x5\_core** è stato aggiornato alla versione 2.2-1.
- Il driver **m1x5\_ib** è stato aggiornato alla versione 2.2-1.
- Il driver **ocrdma** è stato aggiornato alla versione 10.2.287.0u.
- Il driver **ib\_ipoib** è stato aggiornato alla versione 1.0.0.
- Il driver **ib\_qib** è stato aggiornato alla versione 1.11.
- Il driver **enic** è stato aggiornato alla versione 2.1.1.67.
- Il driver **be2net** è stato aggiornato alla versione 10.4r.
- Il driver **tg3** è stato aggiornato alla versione 3.137.
- Il driver **r8169** è stato aggiornato alla versione 2.3LK-NAPI.

## Capitolo 20. Aggiornamenti driver grafici

- ✦ Il driver **vmwgfx** è stato aggiornato alla versione 2.6.0.0.

## Parte III. Known Issues

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

## Capitolo 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.

## Capitolo 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.



## Capitolo 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
```

## Capitolo 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.

## Appendice A. Diario delle Revisioni

<b>Revisione 1.0-9.3</b>	<b>Wed Jan 28 2015</b>	<b>Francesco Valente</b>
Translation files synchronised with XML sources 1.0-9		
<b>Revisione 1.0-9</b>	<b>Wed Jan 14 2015</b>	<b>Milan Navrátil</b>
Versione delle Note di rilascio per Red Hat Enterprise Linux 7.1.		
<b>Revisione 1.0-8</b>	<b>Thu Dec 15 2014</b>	<b>Jiří Herrmann</b>
Versione Beta delle Note di rilascio per Red Hat Enterprise Linux 7.1.		