



# Red Hat Enterprise Linux 6

## Note di rilascio 6.4

Note di rilascio per Red Hat Enterprise Linux 6.4

Edizione 4



# Red Hat Enterprise Linux 6 Note di rilascio 6.4

---

Note di rilascio per Red Hat Enterprise Linux 6.4

Edizione 4

Landmann

[rlandmann@redhat.com](mailto:rlandmann@redhat.com)

## Nota Legale

Copyright © 2012 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). 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 forniscono informazioni dettagliate sui miglioramenti e sulle nuove funzioni implementate con Red Hat Enterprise Linux 6.4. Per una documentazione dettagliata su tutte le modifiche presenti in Red Hat Enterprise Linux consultate le Note tecniche.

# Indice

<b>PREFAZIONE</b> .....	<b>3</b>
<b>CAPITOLO 1. INSTALLAZIONE</b> .....	<b>4</b>
Supporto FCoE nel file di Kickstart	4
Installazione con VLAN	4
Configurazione del bonding	4
<b>CAPITOLO 2. KERNEL</b> .....	<b>5</b>
Fibre Channel Protocol: Controllo consistenza dati End-To-End	5
Supporto Flash Express per IBM System z	5
Modulo del kernel Open vSwitch	5
Confronto tra un sistema avviato ed un sistema "dumped"	5
Aggiornato il tool Perf	5
Supporto Uncore PMU	5
Ridotto l'overhead della memoria memcg	6
Compattazione e rivendicazione della memoria	6
Supporto per la Transactional Execution Facility e Runtime Instrumentation Facility	6
Modalità Fail-open	6
Completamente supportato il meccanismo kdump e kexec Kernel Dumping per IBM System z	6
Supporto TSC Deadline per KVM	6
Nomi del dispositivo persistenti	6
Nuovo pacchetto linuxptp	7
Documentazione per le Transparent Hugepages	7
Stato del supporto per i target dump	7
<b>CAPITOLO 3. DRIVER DEL DISPOSITIVO</b> .....	<b>8</b>
Driver di storage	8
Driver di rete	9
Driver vari	10
<b>CAPITOLO 4. NETWORKING</b> .....	<b>12</b>
HAProxy	12
<b>CAPITOLO 5. AUTENTICAZIONE ED INTEROPERABILITÀ</b> .....	<b>13</b>
Funzioni supportate di SSSD	13
Nuova tipologia di storage in cache SSSD	13
Aggiunta di domini fidati basati su AD ai gruppi esterni	13
Rinnovo-automatico dei Certificati del sottosistema per l'Identity Management	13
Configurazione automatica dei tool del client OpenLDAP sui client interessati alla Identity Management	13
PKCS#12 Supporto per python-nss	13
Ricerca persistente del DNS	14
Nuova operazione CLEANALLRUV	14
Aggiornate le librerie samba4	14
Funzionalità Cross Realm Kerberos Trust in Identity Management	15
Supporto schema Posix per il Directory Server 389	15
<b>CAPITOLO 6. SICUREZZA</b> .....	<b>17</b>
Trattamento autoritario delle corrispondenze nella ricerca di voci sudoers	17
Controlli aggiuntivi delle password per pam_cracklib	17
Opzione size per il tmpfs Polyinstantiation	17
Blocco di account inattivi	17
Nuove modalità operative per libica	17
Ottimizzazione e supporto per la libreria di compressione zlib per System z	18

Configurazione fallback del firewall	18
<b>CAPITOLO 7. ENTITLEMENT</b>	<b>19</b>
Aggiornamenti stringa	19
Test del collegamento Proxy	19
Sottoscrizione o rimozione delle sottoscrizioni con entitlement multipli	19
Supporto chiavi di attivazione nella GUI	19
Registrazione con server esterni	19
Modifiche sull'usabilità nella GUI	19
<b>CAPITOLO 8. VIRTUALIZZAZIONE</b>	<b>20</b>
8.1. KVM	20
virtio-SCSI	20
Supporto per il Core Processor di prossima generazione di Intel	20
Supporto per la CPU AMD Opteron 4xxx Series	20
Migrazione live dei guest utilizzando l'USB Forwarding via SPICE	20
Migrazione live dei guest utilizzando i dispositivi USB	20
QEMU Guest Agent aggiornato	20
Paravirtualized End-of-Interrupt Indication (PV-EOI)	21
Audio pass-through configurabile	21
8.2. HYPER-V	21
Inclusione di, e supporto installazione del guest per, i driver Microsoft Hyper-V	21
8.3. VMWARE ESX	22
Driver VMware PV	22
<b>CAPITOLO 9. CLUSTERING</b>	<b>23</b>
Supporto per il dispositivo di fencing IBM iPDU	23
Supporto per il dispositivo di fencing Eaton Network Power Controller	23
Nuovo pacchetto keepalived	23
Ripristino del Watchdog	23
Supporto per lo storage basato su VMDK	23
<b>CAPITOLO 10. STORAGE</b>	<b>24</b>
Parallel NFS completamente supportato	24
Supporto per la rimozione online XFS	24
Supporto LVM per Micron PCIe SSD	24
Supporto LVM per un RAID10 Mirror bidirezionale	24
Impostazione e gestione delle prenotazioni persistenti SCSI attraverso dispositivi Device Mapper	24
<b>CAPITOLO 11. COMPILATORE E TOOL</b>	<b>25</b>
Aggiornato SystemTap alla versione 1.8	25
Le utilità lscpu e hcpcu	25
<b>CAPITOLO 12. AGGIORNAMENTI GENERALI</b>	<b>26</b>
Aggiornati i pacchetti samba	26
Nuovo pacchetto SciPy	26
Supporto TLS v1.1 in NSS	26
Valgrind gdbserver Embedded	26
Nuovi pacchetti libjpeg-turbo	27
Nuovo pacchetto redhat-lsb-core	27
Utilità createrepo aggiornata	27
<b>APPENDICE A. CRONOLOGIA DI REVISIONE</b>	<b>28</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 6.4* documentano le modifiche più importanti fatte al sistema operativo di Red Hat Enterprise Linux 6 ed alle applicazioni relative per questa release minore. Informazioni dettagliate sulle modifiche (miglioramenti, problematiche conosciute e correzioni) di questa release sono disponibili nelle [Note tecniche](#). Le suddette note contengono anche un elenco completo di tutte le Anteprime di tecnologia disponibili insieme ai pacchetti necessari.



### IMPORTANTE

Le *Note di rilascio Red Hat Enterprise Linux 6.4*, disponibili online [qui](#), devono essere considerate versioni definitive ed aggiornate. Per gli utenti che desiderano formulare domande su questa release, consultare le *Release* e le *Note tecniche* online per le rispettive versioni di Red Hat Enterprise Linux.

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

## CAPITOLO 1. INSTALLAZIONE

### Supporto FCoE nel file di Kickstart

Se utilizzate il file kickstart per installare Red Hat Enterprise Linux 6.4, con la nuova opzione **fcoe** sarà possibile specificare i dispositivi Fibre Channel over Ethernet (FCoE) da attivare automaticamente in aggiunta ai dispositivi scoperti dai servizi Enhanced Disk Drive (EDD). Per maggiori informazioni consultare la sezione *Opzioni di Kickstart* nella *Red Hat Enterprise Linux 6 Installation Guide*.

### Installazione con VLAN

Con Red Hat Enterprise Linux 6.4 le opzioni **vlanid=** e **--vlanid=** permettono all'utente di impostare un LAN ID (802.1q tag) virtuale per un dispositivo di rete specificato. Specificando una di queste opzioni sarà possibile eseguire l'installazione del sistema attraverso un VLAN.

### Configurazione del bonding

È possibile ora configurare usando le opzioni **bond**, **--bondslaves** e **--bondopts** il bonding come parte del processo di installazione. Per maggiori informazioni sulla configurazione consultare le seguenti sezioni della *Red Hat Enterprise Linux 6 Installation Guide*: sezione *Opzioni Kickstart* ed il capitolo *Opzioni d'avvio*.



## CAPITOLO 2. KERNEL

### Fibre Channel Protocol: Controllo consistenza dati End-To-End

Con Red Hat Enterprise Linux 6.4 è stata migliorata l'integrità dei dati tra un adattatore host ed un server di storage per mezzo della implementazione di una parte specifica a zFCP dello standard migliorato T10 DIF SCSI per il controllo della consistenza dei dati End-To-End (E2E).

### Supporto Flash Express per IBM System z

Lo Storage-Class Memory (SCM) per IBM System z è una classe di dispositivi di storage per i dati in grado di unire le proprietà sia della memoria che dello storage. SCM per System z ora supporta la memoria Flash Express. È possibile accedere agli incrementi di SCM attraverso canali Extended Asynchronous Data Mover (EADM). Ogni incremento viene rappresentato da un dispositivo a blocchi. Questa funzione migliora le prestazioni relative all'accesso e alla velocità di paging per uno storage temporaneo, per esempio per il data warehouse.

### Modulo del kernel Open vSwitch

Red Hat Enterprise Linux 6.4 include il modulo del kernel, Open vSwitch, come attivatore per le offerte dei prodotti di Red Hat. Open vSwitch viene supportato solo con prodotti in possesso di utilità dello spazio utente. Senza le suddette utilità dello spazio utente necessarie, Open vSwitch non potrà essere usato né abilitato all'uso. Per maggiori informazioni consultare il seguente articolo del Knowledge Base article: <https://access.redhat.com/knowledge/articles/270223>.

### Confronto tra un sistema avviato ed un sistema "dumped"

Questa funzione permette di eseguire un confronto tra un sistema avviato ed un sistema "dumped". Così facendo sarà possibile analizzare efficacemente le modifiche introdotte a causa di una migrazione dell'immagine. Per identificare un guest verranno usati i dati **stsi** e **stfle**. Una nuova funzione, **lgr\_info\_log()**, esegue il confronto dei dati correnti (**lgr\_info\_cur**) con gli ultimi dati registrati (**lgr\_info\_last**).

### Aggiornato il tool Perf

Il tool **perf** è stato aggiornato alla versione 3.6-rc7, sono ora disponibili numerosi bug fix e miglioramenti. Di seguito viene riportato un elenco di miglioramenti più importanti:

- Aggiunto il supporto per gli eventi Kprobe.
- È stato aggiunto un nuovo motore della sintassi per la linea di comando degli eventi **perf** il quale permette l'uso di parentesi graffe (**{** e **}**) per la definizione di gruppi di eventi, ad esempio: **{cycles, cache-misses}**.
- Il browser **perf** è stato migliorato e permette ora la navigazione attraverso le istruzioni call e jump di ASM.
- Il tool **perf** è stato aggiornato e fornisce ora una visuale utilizzando la nuova opzione **--uid**. Quando usato **perf** mostra i compiti specifici di un utente.
- Il tool **perf** fornisce ora una gamma più vasta di test automatizzati.

### Supporto Uncore PMU

Il kernel di Red Hat Enterprise Linux 6.4 permette di avere un supporto Performance Monitoring Unit (PMU) "uncore" per il sottosistema di eventi perf per processori Intel Xeon Processor X55xx e Intel Xeon Processor X56xx. Il termine "uncore" si riferisce ai sottosistemi nel pacchetto del processore fisico condivisi da processori multipli principali, per esempio L3 cache. Con il supporto PMU uncore è possibile acquisire più facilmente i dati sulle prestazioni di un pacchetto.

È stato altresì abilitato l'analisi di eventi PMU per un debugging tramite perf.

## Ridotto l'overhead della memoria memcg

I gruppi di controllo della memoria conservano il proprio elenco Least Recently Used (LRU), per esempio, rivendicazione della memoria. Questo elenco era situato sopra l'elenco LRU per-zona globale. Con Red Hat Enterprise Linux 6.4 l'overhead della memoria di **memcg** è stato ridotto per mezzo di una disabilitazione dell'elenco LRU per-zona globale, convertendo gli utenti all'uso di elenchi cgroup per-memoria.

## Compattazione e rivendicazione della memoria

Il kernel di Red Hat Enterprise Linux 6.4 utilizza una compattazione e rivendicazione per le richieste di assegnazione più significative o in caso di problemi di memoria "memory pressure".

## Supporto per la Transactional Execution Facility e Runtime Instrumentation Facility

Il supporto per il Transactional-Execution Facility (disponibile con IBM zEnterprise EC12) nel kernel di Linux aiuta ad eliminare il software locking overhead in grado di impattare negativamente sulle prestazioni offrendo al tempo stesso una maggiore scalabilità ed un throughput delle transazioni più elevato. Il supporto per il Runtime Instrumentation Facility (disponibile con IBM zEnterprise EC12) fornisce un meccanismo avanzato di tracciamento del codice del programma per una migliore analisi ed una ottimizzazione del codice generato dal nuovo IBM JVM.

## Modalità Fail-open

Red Hat Enterprise Linux 6.4 rende disponibile il supporto per una nuova modalità fail-open se utilizzate un target NFQUEUE di netfilter. Questa modalità permette agli utenti di disabilitare momentaneamente il controllo dei pacchetti, mantenendo al tempo stesso il collegamento anche con livelli di traffico di rete elevati.

## Completamente supportato il meccanismo kdump e kexec Kernel Dumping per IBM System z

Con Red Hat Enterprise Linux 6.4 il meccanismo di dumping del kernel kdump/kexec è abilitato per i sistemi IBM System z come funzione completamente supportata, insieme al meccanismo di dumping dell'hypervisor e IBM System z stand-alone. Il limite auto-reserve viene impostato su 4 GB; per questo motivo il meccanismo kdump/kexec sarà abilitato su qualsiasi sistema IBM System z con più di 4 GB di memoria.

È necessaria una quantità di memoria sufficiente poichè per impostazione predefinita kdump riserva circa 128 MB. Ciò è molto importante quando si esegue un aggiornamento a Red Hat Enterprise Linux 6.4. È necessario inoltre avere spazio sufficiente su disco per l'archiviazione del dump in presenza di un crash del sistema.

È possibile configurare o disabilitare kdump attraverso **/etc/kdump.conf**, **system-config-kdump**, o **firstboot**.

## Supporto TSC Deadline per KVM

Il timer TSC deadline rappresenta una nuova modalità all'interno del timer Local APIC (LAPIC), esso è in grado di generare interruzioni del timer one-shot in base al TSC deadline e sostituisce l'attuale intervallo del clock APIC. In questo modo vengono fornite interruzioni più precise (meno di un 1 tic) favorendo così l'unità di pianificazione del sistema operativo. KVM ora espone questa funzione anche ai guest.

## Nomi del dispositivo persistenti

Questa funzione archivia la mappatura dei nomi dei dispositivi (per esempio, **sda**, **sdb** ed altri) ed i nomi del dispositivo persistenti (fornita da **udev** in **/dev/disk/by-\*/**) all'interno di messaggi del kernel. Così facendo un utente sarà in grado di identificare un dispositivo usando i messaggi del kernel. Il log **/dev/kmsg** del kernel, visualizzabile con il comando **dmesg**, mostra ora i messaggi per i link simbolici creati da **udev** per i dispositivi del kernel. Questi messaggi vengono visualizzati con il seguente formato:

```
udev-alias: <device_name> (<symbolic_link> <symbolic link> ...)
```

Qualsiasi analizzatore del log è in grado di mostrare questi messaggi, i quali vengono archiviati in `/var/log/messages` via **syslog**.

### Nuovo pacchetto linuxptp

Il pacchetto `linuxptp` disponibile con Red Hat Enterprise Linux 6.4 come Anteprima di tecnologia, è una implementazione del Precision Time Protocol (PTP) basato sullo standard IEEE 1588 di Linux. Esso fornisce una implementazione robusta dello standard e permette di utilizzare le Application Programming Interfaces (API) più moderne e rilevanti offerte dal kernel di Linux. Esso non è stato ideato per supportare API più vecchie ed altre piattaforme.

### Documentazione per le Transparent Hugepages

La documentazione per le transparent hugepages è stata aggiunta al seguente file:

```
/usr/share/doc/kernel-doc-<version>/Documentation/vm/transhuge.txt
```

### Stato del supporto per i target dump

Con Red Hat Enterprise Linux 6.4, il file `/usr/share/doc/kexec-tools-2.0.0/kexec-kdump-howto.txt` fornisce un elenco completo di target dump supportati, non supportati e sconosciuti nella sezione «Stato supporto target dump».

## CAPITOLO 3. DRIVER DEL DISPOSITIVO

### Driver di storage

- Il driver del dispositivo Direct Access Storage Devices (**DASD**) è stato aggiornato ed ora è in grado di rilevare gli errori di configurazione del percorso non rilevati dall'hardware o dal microcodice. Previo rilevamento, il driver del dispositivo non utilizzerà i percorsi interessati. Con questa funzione il driver del dispositivo DASD rileva i percorsi assegnati ad un canale secondario specifico, indicando però server di storage diversi.
- Il driver del dispositivo **zfcp** è stato aggiornato ed aggiunge ora strutture dati e una gestione degli errori per il supporto di una modalità migliorata della scheda per l'adattatore di System z Fibre Channel Protocol (FCP). In questa modalità l'adattatore passa i dati direttamente dalla memoria al SAN (instradamento dei dati) quando la memoria sulla scheda dell'adattatore è stata bloccata a causa di richieste I/O molto grandi e lente.
- Il driver **mtip32xx** è stato aggiornato e ora include il supporto per le ultimissime unità PCIe SSD.
- Il driver **lpfc** per gli adattatori Emulex Fibre Channel Host Bus è stato aggiornato alla versione 8.3.5.82.1p.
- Il driver **qla2xxx** per QLogic Fibre Channel HBAs è stato aggiornato alla versione 8.04.00.04.06.4-k e fornisce ora un supporto per 83XX Converged Network Adapter (CNA) di QLogic, un supporto 16 GBps FC per gli adattatori QLogic ad un nuovo Form Factor CNA per i server HP ProLiant.
- Il driver **qla4xxx** è stato aggiornato alla versione v5.03.00.00.06.04-k0 rendendo disponibile un supporto alle API **change\_queue\_depth**, corregge un certo numero di bug ed introduce vari miglioramenti.
- Il firmware **ql2400-firmware** per il QLogic 4Gbps fibre channel HBA è stato aggiornato alla versione 5.08.00.
- Il firmware **ql2500-firmware** per il QLogic 4Gbps fibre channel HBA è stato aggiornato alla versione 5.08.00.
- Il driver **ipr** per IBM Power Linux RAID SCSI HBA è stato aggiornato alla versione 2.5.4 ed aggiunge ora un supporto per gli adattatori SAS Power7 6Gb ed abilita la capacità SAS VRAID sui suddetti adattatori.
- Il driver **hpsa** è stato aggiornato alla versione 2.0.2-4-RH1 ed aggiunge ora il PCI-ID per la famiglia di controllori HP Smart Array Generation 8 .
- Il driver **bnx2i** per Broadcom NetXtreme II iSCSI è stato aggiornato alla versione 2.7.2.2 e ora presenta un supporto generale dell'hardware.

In Red Hat Enterprise Linux 6.4 il supporto per un avvio iSCSI e FCoE su dispositivi Broadcom è ora completamente supportato. Queste due funzioni sono rese disponibili dai driver Broadcom bnx2i e bnx2fc.

- **bnx2fc** per il Broadcom NetXtreme II 57712 è stato aggiornato alla versione 1.0.12.

In Red Hat Enterprise Linux 6.4 il supporto per un avvio iSCSI e FCoE su dispositivi Broadcom è ora completamente supportato. Queste due funzioni sono rese disponibili dai driver Broadcom bnx2i e bnx2fc.

- Il driver **mpt2sas** è stato aggiornato alla versione 13.101.00.00, ed aggiunge ora un supporto per la modalità segmenti-multipli per il driver Linux BSG.
- Il driver Brocade **bfa** Fibre Channel and FCoE è stato aggiornato alla versione 3.0.23.0 ed include ora il supporto per l'adattatore Brocade 1860 16Gbps Fibre Channel, un nuovo supporto hardware con server Dell PowerEdge 12th Generation ed un supporto **issue\_lip**. Il firmware **bfa** è stato aggiornato alla versione 3.0.3.1.
- Il driver **be2iscsi** per i dispositivi ServerEngines BladeEngine 2 Open iSCSI è stato aggiornato alla versione 4.4.58.0r per avere un supporto iSCSI netlink VLAN.
- Il driver **qib** per TrueScale HCA è stato aggiornato all'ultimissima versione ed ora presenta un:
  - Migliore riconoscimento NUMA
  - Congestion Control Agent (CCA) per fabric Performance Scale Messaging (PSM)
  - Dual Rail per fabric PSM
  - Miglioramenti delle prestazioni e correzioni
- I seguenti driver sono stati aggiornati in modo da includere le ultimissime funzioni e correzioni: **ahci**, **md/bitmap**, **raid0**, **raid1**, **raid10**, e **raid456**.

## Driver di rete

- Il driver **netxen\_nic** per il NetXen Multi port (1/10) Gigabit Network è stato aggiornato alla versione 4.0.80 ed aggiunge ora il supporto miniDIMM. Il firmware **netxen\_nic** è stato aggiornato alla versione 4.0.588.
- Il driver **bnx2x** è stato aggiornato alla versione 1.72.51-0 ed include il supporto per la famiglia di chip Broadcom 57800/57810/57811/57840, insieme ad alcune correzioni generali ed aggiornamenti del firmware per i chip Broadcom 57710/57711/57712. Questo aggiornamento include anche i seguenti miglioramenti:
  - Supporto per gli iSCSI offload e Data Center Bridging/Fibre Channel over Ethernet (DCB/FCOE) su chip Broadcom 57712/578xx. Il chip Broadcom 57840 viene supportato solo in una configurazione 4x10G e non supporta FCoE e iSCSI offload. Versioni future supporteranno configurazioni aggiuntive insieme a iSCSI offload e FCoE.
  - Supporto aggiuntivo livello fisico, incluso l'Energy Efficient Ethernet (EEE).
  - Miglioramenti iSCSI offload
  - Funzioni specifiche di OEM
- Il driver **be2net** per i dispositivi ServerEngines BladeEngine2 10Gbps è stato aggiornato alla versione 4.4.31.0r per aggiungere il supporto RDMA over Converged Ethernet (RoCE).

La funzionalità SR-IOV del driver Emulex **be2net** è ora completamente supportata con Red Hat Enterprise Linux 6.4. SR-IOV può essere eseguito su tutte le varianti Emulex e OEM di hardware basato su BE3, le quali hanno bisogno di software del driver **be2net**.

- Il driver **ixgbev** è stato aggiornato alla versione 2.6.0-k in modo da includere le ultimissime correzioni, miglioramenti e supporto hardware.
- Il driver **cxgb4** per i Chelsio Terminator4 10G Unified Wire Network Controller è stato

aggiornato per il supporto degli adattatori Chelsio T480-CR e T440-LP-CR.

- Aggiornato il driver **cxgb3** per la famiglia Chelsio T3 dei dispositivi di rete alla versione 1.1.5-ko.
- Il driver **ixgbe** per i dispositivi di rete Intel 10 Gigabit PCI Express è stato aggiornato alla versione 3.9.15-k in modo da includere il supporto per SR-IOV con Data Center Bridging (DCB) o Receive-Side Scaling (RSS), un supporto PTP come Anteprima di tecnologia, l'ultimissimo supporto hardware, miglioramenti e correzioni.
- Il driver **iw\_cxgb3** è stato aggiornato.
- Il driver **iw\_cxgb4** è stato aggiornato.
- Il driver **e1000e** per i dispositivi di rete Intel PRO/1000 è stato aggiornato ed aggiunge ora l'ultimissimo supporto hardware, alcune funzioni e rende disponibili un certo numero di correzioni.
- Il driver **enic** per i dispositivi ethernet Cisco 10G è stato aggiornato alla versione 2.1.1.39.
- Il driver **igbvf** (Intel Gigabit Virtual Function Network driver) è stato aggiornato all'ultimissima versione.
- Il driver **igb** per gli adattatori ethernet Gigabit di Intel è stato aggiornato alla versione 4.0.1, ora è disponibile l'ultimissimo supporto hardware. È stato aggiunto altresì un supporto PTP al driver **igb** come Anteprima di tecnologia.
- Il driver **tg3** per i dispositivi Broadcom Tigon3 Ethernet è stato aggiornato alla versione 3.124. Questo aggiornamento rende disponibile un nuovo supporto hardware. È stato altresì aggiunto un supporto PTP al driver **tg3** come Anteprima di tecnologia.
- Il driver **qlcnic** per gli adattatori HP NC-Series QLogic 10 Gigabit Server è stato aggiornato alla versione 5.0.29.
- Il driver Brocade **bnx** per il driver dei controllori ethernet Brocade 10Gb PCIe è stato aggiornato alla versione 3.0.23.0, è ora disponibile il supporto per i server Dell PowerEdge 12th Generation, altresì è possibile utilizzare cavi di tipo non-Brocade Twinax Copper. Il firmware **bnx** è stato aggiornato alla versione 3.0.3.1.
- Il driver Broadcom NetXtreme II **cnic** è stato aggiornato alla versione 2.5.13 ed include ora nuove funzioni, bug fix e supporto per nuove piattaforme OEM.

## Driver vari

- Il driver **intel\_idle** cpuidle per i processori Intel è stato aggiornato. Ora è disponibile il supporto per i processori Xeon E5-XXX V2 di Intel.
- Il driver **wacom** è stato aggiornato ed ora è disponibile il supporto per il CTL-460 Wacom Bamboo Pen, il Wacom Intuos5 Tablet ed il Wacom Cintiq 22HD Pen Display.
- Il driver audio ALSA HDA è stato aggiornato per abilitare o migliorare il supporto per nuovi hardware ed un certo numero di bug.
- Il driver **mlx4\_en** è stato aggiornato all'ultimissima versione upstream.
- Il driver **mlx4\_ib** è stato aggiornato all'ultimissima versione upstream.

- Il driver **mlx4\_core** è stato aggiornato all'ultimissima versione upstream.
- Aggiornato il driver del dispositivo **z90crypt**. È disponibile ora un supporto per la nuova scheda dell'adattatore Crypto Express 4 (CEX4).

## CAPITOLO 4. NETWORKING

### **HAProxy**

HAProxy è un servizio di bilanciamento del carico della rete ad elevate prestazioni di tipo stand-alone, Layer 7 per applicazioni basate su HTTP e TCP in grado di eseguire diversi compiti di programmazione in base al contesto delle richieste HTTP. Red Hat Enterprise Linux 6.4 introduce il pacchetto haproxy come Anteprima di tecnologia.



## CAPITOLO 5. AUTENTICAZIONE ED INTEROPERABILITÀ

### Funzioni supportate di SSSD

Un certo numero di funzioni introdotte con Red Hat Enterprise Linux 6.3 sono ora completamente supportate in Red Hat Enterprise Linux 6.4. Esse comprendono:

- supporto per una gestione centrale delle chiavi SSH
- Mappatura utente SELinux
- e supporto per la memorizzazione in cache per la mappa di automount.

### Nuova tipologia di storage in cache SSSD

La versione 1.10 di Kerberos rende disponibile un nuovo tipo di storage in cache, **DIR:**, che permette a Kerberos di mantenere simultaneamente i Ticket Granting Ticket (TGT) per Key Distribution Center (KDC) multipli ed eseguire una selezione automatica tra di essi durante una negoziazione con risorse conformi a kerberos. Con Red Hat Enterprise Linux 6.4, SSSD è stato migliorato ed ora permette di selezionare un cache **DIR:** per utenti registrati usando SSSD. Questa funzione è stata introdotta come Anteprima di tecnologia.

### Aggiunta di domini fidati basati su AD ai gruppi esterni

Con Red Hat Enterprise Linux 6.4 il comando **ipa group-add-member** permette di aggiungere i membri dei domini fidati basati sull'Active Directory ai gruppi contrassegnati come **esterni** alla Identity Management. È possibile specificare i suddetti membri in base al nome utilizzando domain- o la sintassi basata su UPN, per esempio **AD\UserName** o **AD\GroupName**, o **User@AD.Domain**. Se specificati con questo formato i membri vengono risolti usando il Global Catalog del dominio fidato basato sulla Active Directory per ottenere il valore del Security Identifier (SID).

Alternativamente è possibile specificare direttamente un valore per il SID. In questo caso il comando **ipa group-add-member** verificherà solo che la parte del dominio relativo al suddetto valore risulti essere uno dei domini fidati di Active Directory. Non verrà eseguito alcun tentativo di verifica della validità per il SID all'interno del dominio.

È consigliato utilizzare una sintassi per il nome del gruppo o dell'utente per specificare membri esterni al posto di fornire direttamente i rispettivi valori SID.

### Rinnovo-automatico dei Certificati del sottosistema per l'Identity Management

Il periodo di validità predefinito per un nuovo Certificate Authority è 10 anni. Il CA emette un numero di certificati per i propri sottosistemi ((OCSP, audit log, e altri). I certificati del sottosistema sono generalmente validi per 2 anni. Se i certificati scadono il CA non eseguirà alcun avvio o non sarà in grado di operare correttamente. Per questo motivo con Red Hat Enterprise Linux 6.4 i server di Identity Management sono in grado di rinnovare automaticamente i certificati dei sottosistemi. I certificati sono monitorati da **certmonger** il quale cercherà di rinnovare automaticamente i certificati prima della loro scadenza.

### Configurazione automatica dei tool del client OpenLDAP sui client interessati alla Identity Management

Con Red Hat Enterprise Linux 6.4, OpenLDAP viene configurato automaticamente con un LDAP URI predefinito, un DN di Base, ed un certificato TLS durante l'installazione del client per Identity Management. Ciò migliorerà l'esperienza dell'utente durante le ricerche LDAP per l'Identity Management Directory Server.

### PKCS#12 Supporto per python-nss

Il pacchetto **python-nss**, il quale fornisce le associazioni Python per il Network Security Services (NSS) e Netscape Portable Runtime (NSPR), è stato aggiornato ed ora rende disponibile il supporto PKCS #12.

## Ricerca persistente del DNS

Con Red Hat Enterprise Linux 6.4 LDAP include un supporto per le ricerche persistenti sia per le zone che per le informazioni sulle risorse relative. Questo tipo di ricerca permette al plugin **bind-dyndb-ldap** di essere informato immediatamente su tutte le modifiche avvenute in un database LDAP. Esso diminuisce altresì l'uso della larghezza di banda necessaria.

## Nuova operazione CLEANALLRUV

Elementi obsoleti in un Database Replica Update Vector (RUV) possono essere rimossi con una operazione **CLEANRUV**, la quale esegue una rimozione su un distributore singolo o master. Red Hat Enterprise Linux 6.4 rende disponibile una nuova operazione **CLEANALLRUV** la quale è in grado di rimuovere i dati RUV più vecchi, questa operazione può essere eseguita solo su un distributore/master singoli.

## Aggiornate le librerie samba4

Le librerie **samba4** (rese disponibili dal pacchetto samba4-libs) sono state aggiornate all'ultimissima versione, ciò apporta un miglioramento dell'interoperabilità con i domini dell'Active Directory (AD). SSSD utilizza ora la libreria **libndr-krb5pac** per analizzare il Privilege Attribute Certificate (PAC) emesso da un AD Key Distribution Center (KDC). Sono stati apportati altresì vari miglioramenti al Local Security Authority (LSA) ed ai servizi Net Logon, ed ora è possibile una verifica dei rapporti fidati di un sistema Windows. Per informazioni sulla introduzione della funzionalità Cross Realm Kerberos Trust, la quale dipende dai pacchetti samba4, consultare [sezione chiamata «Funzionalità Cross Realm Kerberos Trust in Identity Management»](#).



### AVVERTIMENTO

SE desiderate eseguire un avanzamento di versione da Red Hat Enterprise Linux 6.3 a Red Hat Enterprise Linux 6.4 ed usate Samba, assicuratevi di rimuovere il pacchetto samba4 in modo da evitare conflitti durante il processo di aggiornamento.

Poichè la funzionalità Cross Realm Kerberos Trust è considerata una Anteprima di tecnologia, determinati componenti **samba4** sono anch'essi considerati Antepreme di tecnologia. Per maggiori informazioni sui pacchetti Samba considerati Anteprima di tecnologia consultare [Tabella 5.1, «Supporto pacchetto Samba4»](#).

**Tabella 5.1. Supporto pacchetto Samba4**

Nome del pacchetto	Nuovo pacchetto in 6.4?	Stato supporto
samba4-libs	No	Anteprima di tecnologia ad eccezione della funzionalità prevista da OpenChange
samba4-pidl	No	Anteprima di tecnologia ad eccezione della funzionalità prevista da OpenChange
samba4	No	Anteprima di tecnologia
samba4-client	Si	Anteprima di tecnologia

Nome del pacchetto	Nuovo pacchetto in 6.4?	Stato supporto
samba4-common	Si	Anteprima di tecnologia
samba4-python	Si	Anteprima di tecnologia
samba4-winbind	Si	Anteprima di tecnologia
samba4-dc	Si	Anteprima di tecnologia
samba4-dc-libs	Si	Anteprima di tecnologia
samba4-swat	Si	Anteprima di tecnologia
samba4-test	Si	Anteprima di tecnologia
samba4-winbind-clients	Si	Anteprima di tecnologia
samba4-winbind-krb5-locator	Si	Anteprima di tecnologia

### Funzionalità Cross Realm Kerberos Trust in Identity Management

La funzionalità Cross Realm Kerberos Trust fornita dall'Identity Management è stata inclusa come Anteprima di tecnologia. Questa funzione permette di creare un rapporto di fiducia tra un Identity Management ed un dominio Active Directory. Ciò significa che gli utenti di un dominio AD sono in grado di accedere alle risorse e ai servizi di un dominio Identity Management, usando le proprie credenziali AD. Non sarà necessaria alcuna sincronizzazione dei dati tra i controllori del dominio AD e l'Identity Management; gli utenti dell'AD verranno sempre autenticati usando il controllore del dominio AD e non sarà necessaria alcuna sincronizzazione delle informazioni relative agli utenti.

Questa funzione è resa disponibile dal pacchetto `ipa-server-trust-ad`. Il pacchetto dipende da funzioni disponibili solo in **samba4**. Poiché i pacchetti `samba4-*` entrano in conflitto con i pacchetti `samba-*` corrispondenti, tutti i pacchetti `samba-*` devono essere rimossi prima di installare `ipa-server-trust-ad`.

Dopo l'installazione del pacchetto `ipa-server-trust-ad` eseguire il comando `ipa-adtrust-install` su tutti i server Identity Management e le repliche. Così facendo sarà possibile abilitare una gestione dei rapporti di fiducia da parte dell'Identity Management. Successivamente potrete instaurare un rapporto di fiducia utilizzando il comando `ipa trust-add` o la WebUI. Per maggiori informazioni consultare la sezione *Integrazione con l'Active Directory attraverso i Cross-Realm Kerberos Trust* disponibile nella *Identity Management Guide* su [https://access.redhat.com/knowledge/docs/Red\\_Hat\\_Enterprise\\_Linux/](https://access.redhat.com/knowledge/docs/Red_Hat_Enterprise_Linux/).

### Supporto schema Posix per il Directory Server 389

Windows Active Directory (AD) supporta lo schema POSIX (RFC 2307 e 2307bis) per le voci relative ai gruppi ed utenti. In numerosi casi AD viene usato come sorgente autorevole per dati di utenti e gruppi, incluso gli attributi POSIX. Con Red Hat Enterprise Linux 6.4, la Directory Server Windows Sync non ignora più i suddetti attributi. Gli utenti sono ora in grado di sincronizzare gli attributi POSIX con Windows Sync tra AD e 389 Directory Server.



## **NOTA**

Durante l'aggiunta al Directory Server di voci relative ai gruppi e utenti gli attributi POSIX non verranno sincronizzati con AD. Con l'aggiunta di nuove voci su AD verrà eseguita una sincronizzazione con il Directory Server, mentre una loro modifica renderà possibile una sincronizzazione in entrambe le modalità.

## CAPITOLO 6. SICUREZZA

### Trattamento autoritario delle corrispondenze nella ricerca di voci sudoers

L'utilità **sudo** è in grado di consultare il file `/etc/nsswitch.conf` per la presenza di voci sudoers ricercandole all'interno dei file o in LDAP. In precedenza in presenza di una corrispondenza nel primo database di voci sudoers, il processo di ricerca continuava in altri database (incluso file). Con Red Hat Enterprise Linux 6.4 è stata aggiunta una opzione al file `/etc/nsswitch.conf` che permette agli utenti di specificare un database sul quale è sufficiente la presenza di una sola corrispondenza. Tale procedura elimina la necessità di interrogare altri database; ciò migliora le prestazioni durante le ricerche di voci sudoers in ambienti molto grandi. Per impostazione predefinita questo comportamento non è abilitato e deve essere configurato aggiungendo la stringa `[SUCCESS=return]` dopo il database desiderato. Al rilevamento di una corrispondenza nel database che processa la stringa, nessun altro database verrà interrogato.

### Controlli aggiuntivi delle password per pam\_cracklib

Il modulo **pam\_cracklib** è stato aggiornato, è ora possibile avere nuovi controlli multipli sulla robustezza della password:

- Alcune politiche di autenticazione non permettono l'uso di password con sequenze continue lunghe, ad esempio "abcd" o "98765". Questo aggiornamento permette di introdurre la possibilità di limitare la lunghezza massima delle sequenze usando l'opzione **maxsequence**.
- Il modulo **pam\_cracklib** permette ora di controllare se una nuova password contiene parole presenti nel campo GECOS nelle voci del file `/etc/passwd`. Il campo GECOS viene usato per archiviare le informazioni aggiuntive relative all'utente, ad esempio il nome o il numero di telefono, utilizzabili da un aggressore nel tentativo di violare una password.
- Il modulo **pam\_cracklib** permette ora di specificare il numero massimo consentito di caratteri consecutivi della stessa classe (minuscole, maiuscole, caratteri e numeri speciali) in una password tramite l'opzione **maxrepeatclass**.
- Il modulo **pam\_cracklib** supporta ora l'opzione **enforce\_for\_root**, la quale impone l'uso di limitazioni sulla complessità delle nuove password per l'account root.

### Opzione size per il tmpfs Polyinstantiation

Su un sistema con montaggi multipli tmpfs è necessario limitare la dimensione per impedire l'uso di tutta la memoria del sistema. PAM è stato aggiornato e permette ora agli utenti di specificare la dimensione massima del montaggio del file system tmpfs, quando si utilizza tmpfs polyinstantiation tramite l'opzione **mntopts=size=<size>** nel file di configurazione `/etc/namespace.conf`.

### Blocco di account inattivi

Alcune politiche di autenticazione hanno bisogno di un supporto per il blocco di un account non utilizzato durante un periodo di tempo determinato. Red Hat Enterprise Linux 6.4 introduce una funzione aggiuntiva al modulo **pam\_lastlog** e permette ora agli utenti di bloccare gli account desiderati dopo un periodo specifico.

### Nuove modalità operative per libica

La libreria **libica**, che presenta un set di funzioni e utilità per l'accesso all'hardware IBM eServer Cryptographic Accelerator (ICA) su IBM System z, è stata modificata e permette ora l'uso di nuovi algoritmi per il supporto delle istruzioni Message Security Assist Extension 4 nel Central Processor Assist for Cryptographic Function (CPACF). Per DES e 3DES sono supportate le seguenti modalità operative:

- Cipher Block Chaining con Ciphertext Stealing (CBC-CS)

- Cipher-based Message Authentication Code (CMAC)

Per AES sono supportate le seguenti modalità operative:

- Cipher Block Chaining con Ciphertext Stealing (CBC-CS)
- Modalità contatore con Cipher Block Chaining Message Authentication Code (CCM)
- Galois/Counter (GCM)

L'accelerazione degli algoritmi complessi di cifratura migliora drammaticamente le prestazioni delle macchine IBM System z.

### **Ottimizzazione e supporto per la libreria di compressione `zlib` per System z**

La libreria `zlib`, libreria generale per la compressione dei dati, è stata aggiornata per migliorare le prestazioni di compressione su IBM System z.

### **Configurazione fallback del firewall**

I servizi `iptables` e `ip6tables` forniscono ora la possibilità di assegnare una configurazione di fallback del firewall se le configurazioni predefinite non possono essere applicate. Se fallisce l'applicazione delle regole firewall di `/etc/sysconfig/iptables`, verrà applicato, se disponibile, il file fallback. Il file fallback corrisponde a `/etc/sysconfig/iptables.fallback` e utilizza il formato del file `iptables-save` (lo stesso di `/etc/sysconfig/iptables`). Se l'uso del file fallback a sua volta fallisce, non vi sarà alcun fallback aggiuntivo. Per la creazione di questo file usare i tool di configurazione standard del firewall e rinominare, o copiare, il file sul file di fallback. Usare lo stesso processo per il servizio `ip6tables`, sostituendo solo «iptables» con «ip6tables».

## CAPITOLO 7. ENTITLEMENT

### Aggiornamenti stringa

Con Red Hat Enterprise Linux 6.4 sono state modificate numerose stringhe nel Gestore delle sottoscrizioni:

- *sottoscrizione* è stato modificato in *assegnazione*
- *sottoscrizione-automatica* è stato modificato in *assegnazione-automatica*
- *rimozione sottoscrizione* è stato modificato in *rimozione*
- *utenza* è stato modificato in *sistema o unità*

### Test del collegamento Proxy

Il dialogo di configurazione del proxy permette ora agli utenti di eseguire la prova di una connessione ad un proxy dopo l'inserimento di un valore.

### Sottoscrizione o rimozione delle sottoscrizioni con entitlement multipli

Il Gestore delle sottoscrizioni è ora in grado di eseguire una sottoscrizione (assegnazione) o una rimozione della sottoscrizione (rimozione) di entitlement multipli usando i rispettivi numeri seriali contemporaneamente.

### Supporto chiavi di attivazione nella GUI

L'interfaccia grafica del Gestore delle sottoscrizioni permette ora di registrare un sistema usando una *chiave di attivazione*. Le chiavi di attivazione permettono agli utenti di preconfigurare le sottoscrizioni per un sistema, prima di una sua registrazione.

### Registrazione con server esterni

Con il Gestore delle sottoscrizioni è ora disponibile il supporto per la selezione di un server remoto durante la registrazione di un sistema. L'interfaccia utente del Gestore delle sottoscrizioni fornisce ora una opzione per la selezione di un URL di un server per la registrazione, insieme ad una porta ed un prefisso. Durante la registrazione sulla linea di comando sarà possibile utilizzare `--serverurl` per specificare il server desiderato. Per maggiori informazioni su questa funzione consultare la sezione *Registrazione, Riregistrazione di un sistema* nella *Guida alla gestione delle sottoscrizioni*.

### Modifiche sull'usabilità nella GUI

La GUI del Gestore delle sottoscrizioni è stata migliorata in base ai suggerimenti degli utenti.

## CAPITOLO 8. VIRTUALIZZAZIONE

### 8.1. KVM

#### virtio-SCSI

Lo storage stack di KVM Virtualization è stato migliorato con l'aggiunta di capacità virtio-SCSI (una architettura storage per KVM basato sullo SCSI). Contrariamente a virtio-blk, virtio-SCSI permette di collegarsi direttamente alle SCSI LUN e migliorare significativamente la scalabilità. A differenza di virtio-blk, il quale è in grado di gestire circa 25 dispositivi ed esaurisce gli slot PCI, il vantaggio offerto da virtio-SCSI è quello di saper gestire centinaia di dispositivi.

Virtio-SCSI è in grado di ereditare il set di capacità del dispositivo di destinazione con la possibilità di:

- collegare un disco fisso virtuale o CD attraverso il controllore di virtio-scsi,
- passare attraverso un dispositivo SCSI fisico dall'host al guest tramite il dispositivo blocchi-scsi QEMU,
- permettere l'uso di centinaia di dispositivi per il guest; un miglioramento rispetto al limite di 25 dispositivi offerto da virtio-blk.

virtio-scsi è stato introdotto con Red Hat Enterprise Linux 6.3 come Anteprima di tecnologia ed ora è completamente supportato in Red Hat Enterprise Linux 6.4. I guest di Windows (ad eccezione di Windows XP) sono supportati con gli ultimissimi driver virtio-win.

#### Supporto per il Core Processor di prossima generazione di Intel

Red Hat Enterprise Linux 6.4 rende disponibile il supporto per il Core processor di prossima generazione di Intel su **qemu-kvm**, in questo modo i guest KVM saranno in grado di usare le nuove funzioni fornite da questo processore, le più importanti sono: Advanced Vector Extensions 2 (AVX2), Bit-Manipulation Instructions 1 (BMI1), Bit-Manipulation Instructions 2 (BMI2), Hardware Lock Elision (HLE), Restricted Transactional Memory (RTM), Process-Context Identifier (PCID), Invalidate Process-Context Identifier (INVPCID), Fused Multiply-Add (FMA), Big-Endian Move instruction (MOVBE), F Segment and G Segment BASE instruction (FSGSBASE), Supervisor Mode Execution Prevention (SMEP), Enhanced REP MOVSB/STOSB (ERMS).

#### Supporto per la CPU AMD Opteron 4xxx Series

Il processore AMD Opteron 4xxx series è ora completamente supportato da **qemu-kvm**. Ciò permette l'esposizione di nuove funzioni ai guest KVM, ad esempio: il set di istruzioni F16C, Trailing Bit Manipulation, funzioni Bit-Manipulation Instructions 1 (BMI1), ed il set di istruzioni Fused Multiply-Add (FMA).

#### Migrazione live dei guest utilizzando l'USB Forwarding via SPICE

Con Red Hat Enterprise Linux 6.4, KVM supporta la migrazione live dei guest utilizzando l'USB forwarding via SPICE, conservando il ridirezionamento del dispositivo USB esistente per tutti i dispositivi configurati.

#### Migrazione live dei guest utilizzando i dispositivi USB

Con Red Hat Enterprise Linux 6.4, KVM supporta la migrazione live dei guest con dispositivi USB. Vengono supportati i seguenti dispositivi: frasi d'accesso locali Enhanced Host Controller Interface (EHCI) e Universal Host Controller Interface (UHCI) e dispositivi emulati come i dispositivi di storage, mice, tastiere, hubs e altro.

#### QEMU Guest Agent aggiornato



Il QEMU guest agent (reso disponibile da `qemu-guest-agent`) è ora completamente supportato con Red Hat Enterprise Linux 6.4. È stato aggiornato alla aversione 1.1 ed include le seguenti correzioni e miglioramenti:

- I comandi **guest -suspend-disk** e **guest -suspend-ram** possono essere usati per la sospensione con la RAM o sul disco con un sistema Windows.
- È possibile usare il comando **guest -network-get-interfaces** per ottenere le informazioni sull'interfaccia di rete in Linux.
- Questo aggiornamento fornisce le correzioni ed i miglioramenti per il supporto della sospensione del file system.
- Questo aggiornamento include varie correzioni e piccoli miglioramenti.

### Paravirtualized End-of-Interrupt Indication (PV-EOI)

Gli host ed i guest che eseguono Red Hat Enterprise Linux 6.3 e versioni più vecchie, hanno bisogno di due uscite VM (selettori del contesto da una VM ad un Hypervisor) per ogni interruzione: una per inserire l'interruzione e l'altra per indicare la fine dell'interruzione stessa. Dopo aver aggiornato i sistemi host e guest a Red Hat Enterprise Linux 6.4, o versione più recente, essi potranno negoziare una funzione di tipo end-of-interrupt paravirtualizzata e usare solo un selettore per interruzione. Di conseguenza con l'uso di Red Hat Enterprise Linux 6.4 o di una versione più recente come host o guest, il numero di uscite viene ridotto a metà per carichi di lavoro con un numero di interruzioni elevato, ad esempio il traffico di rete in ingresso con un dispositivo di rete virtio. Ciò comporta una riduzione significativa dell'utilizzo della CPU dell'host per carichi di lavoro simili. Da notare che solo le interruzioni edge sono state migliorate: per esempio il networking e 1000 utilizza una tipologia diversa di interruzioni (level interrupt) per questo motivo non è stato migliorato.

### Audio pass-through configurabile

È possibile ora rilevare un dispositivo audio come **microfono** o **speaker** nel sistema guest (in aggiunta al rilevamento come **line-in** e **line-out**). I dispositivi audio ora possono operare correttamente nelle applicazioni guest che accettano determinati tipi di input per la registrazione della voce e audio.

## 8.2. HYPER-V

### Inclusione di, e supporto installazione del guest per, i driver Microsoft Hyper-V

L'installazione del guest Red Hat Enterprise Linux integrata ed il supporto per il dispositivo paravirtualizzato Hyper-V con Red Hat Enterprise Linux 6.4 su Microsoft Hyper-V permette agli utenti una esecuzione di Red Hat Enterprise Linux 6.4 come guest con gli hypervisor Microsoft Hyper-V. I seguenti driver Hyper-V ed il sorgente dell'orologio sono stati aggiunti al kernel presente con Red Hat Enterprise Linux 6.4:

- un driver di rete (**hv\_netvsc**)
- un driver di storage (**hv\_storvsc**)
- un driver del mouse conforme a HID (**hid\_hyperv**)
- un driver VMbus (**hv\_vmbus**)
- un driver util (**hv\_util**)
- un driver del disco IDE (**ata\_piix**)
- un sorgente dell'orologio (i386, AMD64/Intel 64: **hyperv\_clocksource**)

Red Hat Enterprise Linux 6.4 include anche il supporto per Hyper-V come sorgente dell'orologio ed un demone guest Hyper-V Key-Value Pair (KVP) (**hypervkvpd**) il quale è in grado di passare informazioni di base, come l'IP del guest, FQDN, il nome del sistema operativo ed il numero della release all'host attraverso VMbus.

## 8.3. VMWARE ESX

### Driver VMware PV

I driver paravirtualizzati VMware sono stati aggiornati e ora forniscono una esperienza nuova durante l'esecuzione di Red Hat Enterprise Linux 6.4 in VMware ESX. L'installer di anaconda è stato aggiornato ed ora elenca di driver durante il processo di installazione. Sono stati aggiornati i seguenti driver:

- un driver di rete (**vmxnet3**)
- un driver di storage (**vmw\_pvscsi**)
- un balloon driver della memoria (**vmware\_balloon**)
- un driver del mouse (**vmmouse\_drv**)
- un driver video (**vmware\_drv**)

## CAPITOLO 9. CLUSTERING

### Supporto per il dispositivo di fencing IBM iPDU

Red Hat Enterprise Linux 6.4 aggiunge il supporto per i dispositivi di fencing IBM iPDU. Per maggiori informazioni sui parametri relativi consultare l'appendice *Parametri del dispositivo di fencing* nella guida di Red Hat Enterprise Linux 6 *Cluster Administration*.

### Supporto per il dispositivo di fencing Eaton Network Power Controller

Red Hat Enterprise Linux 6.4 aggiunge il supporto per `fence_eaton_snmp`, il dispositivo di fencing per l'Eaton over SNMP network power switch. Per maggiori informazioni sui parametri relativi consultare l'appendice *Parametri del dispositivo di fencing* nella guida di Red Hat Enterprise Linux 6 *Cluster Administration*.

### Nuovo pacchetto keepalived

Red Hat Enterprise Linux 6.4 include il pacchetto keepalived come Anteprema di tecnologia. Il pacchetto keepalived fornisce funzioni semplice e robuste per il bilanciamento del carico e per le elevate prestazioni. Il framework per il bilanciamento del carico si affida al modulo Linux Virtual Server kernel e rende disponibile un bilanciamento del carico della rete a 4 livelli. Il demone `keepalived` implementa un set di controllori dello stato per i gruppi di server con un carico bilanciato in base allo stato. Il demone keepalived implementa anche un Virtual Router Redundancy Protocol (VRRP) e permette di avere così una elevata disponibilità tramite un processo di failover.

### Ripristino del Watchdog

`fence_sanlock` e `checkquorum.wdmd` sono stati inclusi in Red Hat Enterprise Linux 6.4 come Anteprema di tecnologia, essi rendono disponibile un nuovo meccanismo per il ripristino di un nodo tramite un dispositivo watchdog. I Tutorial su come abilitare questa Anteprema di tecnologia sono disponibili su <https://fedorahosted.org/cluster/wiki/HomePage>.

### Supporto per lo storage basato su VMDK

Red Hat Enterprise Linux 6.4 rende disponibile un supporto dei cluster che utilizzano una tecnologia dell'immagine del disco VMDK (Virtual Machine Disk) di VMware con l'opzione multi-writer. Ciò permette ad un utente di utilizzare uno storage basato su VMDK con l'opzione multi-writer per file system clusterizzati come ad esempio GFS2.

## CAPITOLO 10. STORAGE

### Parallel NFS completamente supportato

Il Parallel NFS (pNFS) è parte dello standard v4.1 di NFS il quale permette ai client di accedere ai dispositivi di storage direttamente ed in parallelo. L'architettura di pNFS aumenta la scalabilità e le prestazioni associate con i server NFS per diversi carichi di lavoro comuni. Con Red Hat Enterprise Linux 6.4 pNFS è supportato.

Il pNFS supporta 3 diversi protocolli di storage o layout: file, oggetti e blocchi. Il client NFS di Red Hat Enterprise Linux 6.4 supporta il protocollo di layout dei file.

Per abilitare questa nuova funzionalità usare una delle seguenti opzioni di montaggio da un server abilitato-pNFS: **-o minorversion=1 o -o v4.1**.

Quando il server è abilitato al pNFS il modulo del kernel **nfs\_layout\_nfsv41\_files** viene caricato automaticamente al primo processo di montaggio. Usare il seguente comando per verificare il caricamento effettivo del modulo:

```
~]$ lsmod | grep nfs_layout_nfsv41_files
```

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

### Supporto per la rimozione online XFS

L'operazione di rimozione online eseguita su un file system montato rimuove i blocchi non usati dal file system. Le operazioni di rimozione online sono ora supportate sui file system XFS. Per maggiori informazioni consultare la sezione *Rimozione blocchi non utilizzati* presente nella Red Hat Enterprise Linux 6 *Storage Administration Guide*.

### Supporto LVM per Micron PCIe SSD

Con Red Hat Enterprise Linux 6.4, LVM rende disponibile il supporto per i Micron PCIe Solid State Drives (SSDs) come dispositivi utilizzabili per la formazione di una parte del gruppo di volumi.

### Supporto LVM per un RAID10 Mirror bidirezionale

LVM è ora in grado di creare, rimuovere e modificare la dimensione di volumi logici RAID10. Per creare un volume logico RAID10, in modo simile ad altri tipi di RAID, specificare il tipo di segmento nel modo seguente:

```
~]# lvcreate --type raid10 -m 1 -i 2 -L 1G -n lv vg
```

Da notare che gli argomenti **-m** e **-i** si comportano in modo simile ad altri tipi di segmenti. E cioè **-i** rappresenta il numero totale di segmenti mentre **-m** è il numero di copie (aggiuntive) (quindi, **-m 1 -i 2** indica 2 segmenti su mirror bidirezionali).

### Impostazione e gestione delle prenotazioni persistenti SCSI attraverso dispositivi Device Mapper

In precedenza per impostare una prenotazione persistente su dispositivi multipath era necessario eseguire la sua impostazione su tutti i dispositivi del percorso. Se un dispositivo veniva aggiunto in un secondo momento, allora era necessario aggiungere manualmente le prenotazioni al percorso in questione. Red Hat Enterprise Linux 6.4 aggiunge ora la possibilità di impostare e gestire le prenotazioni persistenti SCSI attraverso i dispositivi del device mapper con il comando **mpathpersist**. Se aggiungete nuovi dispositivi sarà necessario impostare anche le prenotazioni persistenti.

## CAPITOLO 11. COMPILATORE E TOOL

### Aggiornato SystemTap alla versione 1.8

SystemTap è uno strumento di rilevamento e monitoraggio che permette agli utenti di studiare e monitorare le attività del sistema operativo (in particolare del kernel) in modo dettagliato. Esso fornisce informazioni simili all'output di strumenti come **netstat**, **ps**, **top**, e **iostat**; tuttavia SystemTap è stato creato per fornire un numero maggiore di opzioni d'analisi e di filtraggio per le informazioni raccolte.

Il pacchetto `systemtap` in Red Hat Enterprise Linux 6.4 è stato aggiornato alla versione 1.8 e fornisce ora un certo numero di correzioni e miglioramenti:

- La sintassi **@var** è ora una sintassi alternativa del linguaggio per l'accesso alle variabili DWARF nei gestori **uprobe** e **kprobe** (processo, kernel e modulo).
- SystemTap esegue la modifica delle variabili locali per evitare conflitti con le intestazioni C incluse nei tapset.
- Il server di compilazione di SystemTap ed il client supportano ora le reti IPv6.
- Il runtime di SystemTap (**staprun**) ora accetta una opzione per il timeout **-T** che permette di avere un numero minore di attivazioni "wake-up" per rilevare output con capacità di elaborazione bassa dagli script.
- Il driver del traduttore di script SystemTap (**stap**) fornisce ora le seguenti opzioni:

```
--rlimit-as=NUM
--rlimit-cpu=NUM
--rlimit-nproc=NUM
--rlimit-stack=NUM
--rlimit-fsize=NUM
```

- I moduli SystemTap sono più piccoli ed eseguono una compilazione più veloce. Per impostazione predefinita il `debuginfo` dei moduli è ora annullato.
- Corretto il Bug [CVE-2012-0875](#) (kernel panic durante la processazione di dati formati incorrettamente DWARF unwind).

### Le utilità **lscpu** e **chcpu**

L'utilità **lscpu**, la quale mostra informazioni dettagliate sulla disponibilità delle CPU, è stata aggiornata ed include ora numerose nuove funzioni. Altresì una nuova utilità, **chcpu**, è stata aggiunta e permette agli utenti di modificare lo stato della CPU (online/offline, standby/attiva, e altri stati), disabilitare e abilitare le CPU e configurare CPU specifiche.

Per maggiori informazioni sulle suddette utilità consultare le pagine man **lscpu(1)** e **chcpu(8)**.

## CAPITOLO 12. AGGIORNAMENTI GENERALI

### Aggiornati i pacchetti samba

Red Hat Enterprise Linux 6.4 include ora i pacchetti samba modificati i quali apportano numerose correzioni e miglioramenti, il più importante è la presenza del supporto per il protocollo SMB2. Il supporto SMB2 può essere abilitato con il seguente parametro nella sezione `[global]` del file `/etc/samba/smb.conf`:

```
max protocol = SMB2
```

Samba presenta ora il supporto per una cifratura AES in Kerberos. Il supporto AES era disponibile nei sistemi operativi Microsoft Windows con l'introduzione di Windows Vista e Windows Server 2008. Esso risulta essere il nuovo sistema di cifratura Kerberos predefinito con l'introduzione di Windows 7. Samba ora rende disponibili le chiavi AES in Kerberos nel keytab da esso controllato. Ciò significa che altri servizi interessati a kerberos che utilizzano il keytab di samba e sono eseguiti sulla stessa macchina possono utilizzare la cifratura AES. Per poter utilizzare le chiavi della sessione AES (e non solo il ticket granting tickets cifrato con AES), è necessario modificare manualmente l'account della macchina samba nel server LDAP dell'Active Directory. Per maggiori informazioni consultare il [Blog del Team di supporto per il Microsoft Open Specifications](#).



#### AVVERTIMENTO

I pacchetti samba aggiornati modificano il modo attraverso il quale viene configurata la mappatura dell'ID. Per questo motivo è consigliato modificare i file di configurazione Samba esistenti.

Da notare che alcuni file Trivial Database (TDB) sono stati aggiornati, il supporto per la stampa è stato modificato in modo da poter utilizzare l'attuale implementazione del registro. Ciò significa che tutti i file TDB vengono aggiornati durante l'avvio della nuova versione di `smbd`. Non sarà possibile implementare una versione più vecchia di Samba 3.x se non avete eseguito un backup dei file TDB.

Per maggiori informazioni sulle modifiche consultare le [Note di rilascio di Samba 3.6.0](#).

### Nuovo pacchetto SciPy

Red Hat Enterprise Linux 6.4 include un nuovo pacchetto scipy. Questo pacchetto fornisce il software necessario per operazioni matematiche, scienze e di engineering. Il pacchetto NumPy, creato per la manipolazione di array multi-dimensionali di informazioni arbitrarie molto grandi, è la libreria principale per SciPy. La libreria SciPy viene utilizzata insieme agli array NumPy e fornisce varie sequenze numeriche, per esempio sequenze per l'ottimizzazione e integrazioni numeriche.

### Supporto TLS v1.1 in NSS

Il pacchetto nss e nss-util sono stati aggiornati alla versione 3.14 e forniscono tra l'altro un supporto per il TLS versione 1.1. Altresì il pacchetto nspr è stato aggiornato alla versione 4.9.2. Per maggiori informazioni consultare le [Note di rilascio di NSS 3.14](#).

### Valgrind gdbserver Embedded

Il pacchetto `valgrind` è stato aggiornato alla versione 3.8.1. Questo aggiornamento presenta, oltre ad altri miglioramenti e correzioni, un **`gdbserver`** embedded. Per maggiori informazioni consultare il capitolo *Valgrind* e l'appendice *Modifiche in Valgrind 3.8.1* nella *Red Hat Developer Toolset 1.1 User Guide*.

### **Nuovi pacchetti libjpeg-turbo**

Red Hat Enterprise Linux 6.4 include un nuovo set di pacchetti: `libjpeg-turbo`. Questi pacchetti sostituiscono i pacchetti `libjpeg` tradizionali e forniscono le stesse funzionalità e API di `libjpeg` apportando migliori prestazioni.

### **Nuovo pacchetto redhat-lsb-core**

Quando installate il pacchetto `redhat-lsb` verranno visualizzate nel sistema un certo numero di dipendenze per soddisfare lo standard LSB. Red Hat Enterprise Linux 6.4 fornisce un nuovo pacchetto `redhat-lsb-core` il quale permette di avere un numero minimo di pacchetti necessari. Per questo motivo è consigliato l'installazione di `redhat-lsb-core`.

### **Utilità createrepo aggiornata**

L'utilità **`createrepo`** è stata aggiornata all'ultimissima versione e rende possibile supportare ora l'operazione di multitasking tramite l'opzione `--workers`.

## APPENDICE A. CRONOLOGIA DI REVISIONE

<b>Revisione 1.1-12.1.400</b> Rebuild with publican 4.0.0	<b>2013-10-31</b>	<b>Rüdiger Landmann</b>
<b>Revisione 1.1-12.2</b> updated	<b>Mon Jan 21 2013</b>	<b>Francesco Valente</b>
<b>Revisione 1.1-12.1</b> Translation files synchronised with XML sources 1.1-12	<b>Mon Jan 21 2013</b>	<b>Francesco Valente</b>
<b>Revisione 1.1-12</b> Versione delle Note di rilascio della Versione Beta di Red Hat Enterprise Linux 6.4.	<b>Wed Dec 4 2012</b>	<b>Martin Prpič</b>