



Red Hat Enterprise Linux 7 Note di rilascio 7.2

Note di rilascio per Red Hat Enterprise Linux 7.2

Red Hat Customer Content
Services

Red Hat Enterprise Linux 7 Note di rilascio 7.2

Note di rilascio per Red Hat Enterprise Linux 7.2

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 forniscono informazioni dettagliate sui miglioramenti e sulle nuove implementazioni presenti in Red Hat Enterprise Linux 7.2, e documentano le problematiche conosciute in questa release. Per informazioni più approfondite su tutte le modifiche a Red Hat Enterprise Linux relative all'aggiornamento 7.2, consultare le Note tecniche.

Indice

| | |
|--|-----------|
| Prefazione | 6 |
| Capitolo 1. Architetture | 7 |
| Parte I. Nuove funzioni | 8 |
| Capitolo 2. Autenticazione | 9 |
| ca-certificate aggiornato alla versione 2.4 | 9 |
| Supporto per rapporti fidati unidirezionali | 9 |
| openldap aggiornato alla versione 2.4.40 | 9 |
| Autenticazione cache in SSSD | 9 |
| SSSD abilita una mappatura UID e GID su client individuali | 9 |
| SSSD è ora in grado di negare l'accesso SSH agli account bloccati | 9 |
| L'utilità sudo è ora in grado di verificare il checksum del comando | 10 |
| Supporto delle smart card SSSD | 10 |
| Supporto profili multipli del certificato | 10 |
| Password Vault | 10 |
| Supporto DNSSEC con l'Identity Management | 10 |
| Proxy HTTPS di Kerberos con Identity Management | 11 |
| Aggiornamento nel background delle voci memorizzate in cache | 11 |
| Memorizzazione in cache di operazioni inittgroups | 11 |
| Negoziazione autenticazione semplificata con mod_auth_gssapi | 11 |
| Capacità di gestione del ciclo di vita dell'utente | 11 |
| Supporto SCEP in certmonger | 11 |
| Nuovi pacchetti: epsilon | 11 |
| NSS aumenta i valori minimi accettati delle chiavi | 12 |
| nss e nss-util aggiornati alla versione 3.19.1 | 12 |
| I moduli Apache per IdM sono ora completamente supportati | 12 |
| Capitolo 3. Clustering | 13 |
| systemd e pacemaker ora seguono correttamente il processo di spegnimento del sistema | 13 |
| I comandi pcs resource move e pcs resource ban ora mostrano un messaggio d'avvertimento per chiarirne il comportamento | 13 |
| Nuovo comando per spostare una risorsa del Pacemaker sul nodo preferito | 13 |
| Supporto per il comando clufter per la trasformazione e l'analisi dei formati di configurazione del cluster | 13 |
| Capitolo 4. Compiler e strumenti | 14 |
| tail --follow ora funziona correttamente su file con Veritas Clustered file system (VXFS) | 14 |
| Il comando dd ora è in grado di mostrare lo stato del processo di trasferimento | 14 |
| Tempi d'attesa migliorati in libcurl | 14 |
| La libreria libcurl implementa ora operazioni handshake SSL senza alcun blocco | 14 |
| GDB su IBM Power System non genera più alcun errore quando accede alla tabella dei simboli | 14 |
| nscd aggiornato per un caricamento automatico dei dati per la configurazione | 14 |
| La funzione della libreria dlopen non si arresta più inaspettatamente in presenza di chiamate ricorsive. | 14 |
| operf è in grado ora di riconoscere gli identificatori di huge page statiche | 15 |
| Il comando rsync -X ora funziona correttamente | 15 |
| Gli eseguibili Subversion vengono ora compilati con dati RELRO completi | 15 |
| L'estensione del thread in TCL ora funziona correttamente | 15 |
| Capitolo 5. Desktop | 16 |
| GNOME 3.14 | 16 |
| Il pacchetto ibus-gtk2 aggiorna ora il file immodules.cache | 16 |
| Capitolo 6. File System | 18 |

| | |
|--|-----------|
| gfs2-utils aggiornato alla versione 3.1.8 | 18 |
| GFS2 impedisce agli utenti di superare i propri quota | 18 |
| XFS aggiornato alla versione 4.1 | 18 |
| Aggiornamento ext4 e jbd2 | 18 |
| cifs aggiornato alla versione 3.17 | 18 |
| Capitolo 7. Aggiornamenti generali | 19 |
| lftp ora gestisce correttamente 302 redirection | 19 |
| Più informazioni per la diagnosi e modifica del nome per il plug-in di sosreport | 19 |
| Capitolo 8. Installazione e avvio | 20 |
| È possibile correggere l'impostazione di rete in initrd se si fornisce una configurazione di rete in Kickstart | 20 |
| Anaconda ora supporta la creazione dei volumi logici in cache | 20 |
| Elenco del menu d'avvio di GRUB migliorato | 20 |
| Anaconda ripristina ora correttamente le azioni del disco al variare della selezione del disco stesso | 20 |
| Rilevamento migliorato dei nomi per il device-mapper | 20 |
| Corretto il processo di gestione di PReP Boot durante il partizionamento | 20 |
| Partizioni EFI su dispositivi RAID1 | 21 |
| L'installazione in modalità testo non si arresta più inaspettatamente durante la configurazione di rete | 21 |
| Le schermate della modalità di ripristino su IBM System z, sono ora visualizzate correttamente | 21 |
| Componente aggiuntivo OpenSCAP in Anaconda | 21 |
| Non si verifica più il time out di Anaconda durante l'attesa per un file Kickstart su un CD o DVD | 22 |
| Capitolo 9. Kernel | 23 |
| I parametri del kernel, SHMMAX e SHMALL, sono stati reimpostati su valori predefiniti. | 23 |
| le transparent huge pages non causano più la corruzione della memoria | 23 |
| Aggiornamento SCSI LIO | 23 |
| makedumpfile supporta ora il nuovo formato di sadump fino a 16 TB di memoria fisica | 23 |
| La rimozione o l'aggiornamento del kernel non mostra più alcun messaggio d'avviso | 23 |
| Nuovo pacchetto: libevdev | 23 |
| Tuned è ora in grado di essere eseguito in modalità no-daemon | 23 |
| Nuovo pacchetto: tuned-profiles-realtime | 24 |
| Programmazione Multiqueue I/O con blk-mq | 24 |
| Ora è più semplice interpretare i messaggi d'errore SCSI | 24 |
| Driver e sottosistema libATA aggiornati | 24 |
| Aggiornati FCoE e DCB | 25 |
| perf aggiornato alla versione 4.1 | 25 |
| Supporto per TPM 2.0 | 25 |
| Turbostat fornisce ora un output corretto | 25 |
| Supporto per il processore Xeon v5 di Intel | 25 |
| zswap utilizza l'API zpool | 25 |
| La lunghezza del file /proc/pid/cmdline è ora illimitata | 25 |
| Ora è disponibile il supporto per dma_rmb e dma_wmb | 25 |
| Capitolo 10. Networking | 27 |
| SNMP segue correttamente le direttive di clientaddr attraverso IPv6 | 27 |
| tcpdump supporta -J, -j, e --time-stamp-precision | 27 |
| Aggiornamento TCP/IP | 27 |
| Capitolo 11. Servizi e Server | 28 |
| La direttiva ErrorPolicy è ora valida | 28 |
| Per impostazione predefinita CUPS ora disabilita la cifratura SSLv3 | 28 |
| Cups ora permette l'uso del trattino basso nei nomi della stampante | 28 |
| Le dipendenze non necessarie sono state rimosse dal pacchetto tftp-server | 28 |

| | |
|---|-----------|
| Il file <code>/etc/sysconfig/conman</code> deprecato è stato rimosso | 28 |
| Capitolo 12. Storage | 29 |
| Nuove opzioni <code>delay_watch_checks</code> e <code>delay_wait_checks</code> nel file <code>multipath.conf</code> | 29 |
| Nuova opzione <code>config_dir</code> nel file <code>multipath.conf</code> | 29 |
| Aggiornamento DM | 29 |
| Nuovo comando <code>dmstats</code> per visualizzare e gestire le statistiche I/O delle regioni definite dall'utente dei dispositivi che utilizzano il driver del <code>device-mapper</code> | 29 |
| Supporto per DIX su hardware specificato | 29 |
| Cache LVM | 30 |
| Nuova politica della cache LVM/DM | 30 |
| LVM <code>systemID</code> | 30 |
| Capitolo 13. Gestione delle sottoscrizioni e sistemi | 31 |
| PowerTOP ora rispetta i nomi dei file definiti dall'utente | 31 |
| Modificati i comandi <code>yum-config-manager</code> | 31 |
| Nuovo plug-in <code>search-disabled-repos</code> per <code>yum</code> | 31 |
| Capitolo 14. Virtualizzazione | 32 |
| I bus root PCI supplementari sono ora supportati usando i dispositivi <code>bridge PCI expander</code> | 32 |
| <code>qemu-kvm</code> supporta gli eventi per il tracciamento dell'arresto della macchina virtuale | 32 |
| Intel MPX esposto <code>guest</code> | 32 |
| Estrazione <code>dump</code> della memoria del <code>guest</code> dal <code>qemu-kvm core</code> | 32 |
| <code>virt-v2v</code> è completamente supportato | 32 |
| Virtualizzazione su sistemi IBM Power | 32 |
| Supporto <code>VirtIO-1</code> | 32 |
| Supporto <code>Hyper-V TRIM</code> | 32 |
| Capitolo 15. Red Hat Software Collection | 34 |
| Parte II. Anteprima di tecnologia | 35 |
| Capitolo 16. Autenticazione | 36 |
| Utilizzo provider <code>sudo AD</code> e <code>LDAP</code> | 36 |
| Capitolo 17. File System | 37 |
| <code>OverlayFS</code> | 37 |
| Supporto per i client <code>NFSv4</code> con una disposizione del file <code>flexible</code> | 37 |
| <code>NFS over RDMA</code> | 37 |
| Filesystem <code>Btrfs</code> | 37 |
| Capitolo 18. Abilitazione hardware | 39 |
| Supporto schede <code>OSA-Express5s</code> in <code>qethcoat</code> | 39 |
| Strumentazione di runtime per IBM System z | 39 |
| Adattatori <code>LSI Syncro CS HA-DAS</code> | 39 |
| Capitolo 19. Kernel | 40 |
| Supporto CPU multiple in <code>kdump</code> su sistemi Intel 64 e AMD64 | 40 |
| Strumento <code>criu</code> | 40 |
| Spazio nome utente | 40 |
| <code>LPAR Watchdog</code> per IBM System z | 40 |
| Aggiornamenti del kernel automatici con <code>kpatch</code> | 40 |
| <code>i40evf</code> gestisce operazioni di reset molto grandi | 40 |
| Capitolo 20. Networking | 41 |
| Aggiornato il driver Intel ethernet server adapter <code>X710/XL710</code> | 41 |
| Output <code>ethtool</code> accurato | 41 |

| | |
|---|-----------|
| Driver Cisco usNIC | 41 |
| Driver kernel Cisco VIC | 41 |
| Trusted Network Connect | 41 |
| Funzione SR-IOV nel driver qlcnic | 41 |
| Capitolo 21. Storage | 42 |
| Programmazione Multi-queue I/O per SCSI | 42 |
| Infrastruttura di blocco LVM migliorata | 42 |
| Plug-in Targetd dell'API libStorageMgmt | 42 |
| DIF/DIX | 42 |
| dm-era device-mapper target | 42 |
| Capitolo 22. Virtualizzazione | 43 |
| Virtualizzazione nidificata | 43 |
| Lo strumento virt-p2v | 43 |
| Supporto USB 3.0 per guest KVM | 43 |
| Parte III. Driver del dispositivo | 44 |
| Capitolo 23. Aggiornamenti driver di archiviazione | 45 |
| Capitolo 24. Aggiornamenti driver di rete | 46 |
| Capitolo 25. Aggiornati i driver grafici e quelli generici | 47 |
| Parte IV. Problematiche conosciute | 48 |
| Capitolo 26. Compiler e Tool | 49 |
| Bug multipli durante l'avvio da uno SAN usando FCoE | 49 |
| Valgrind non è in grado di eseguire programmi compilati utilizzando una versione precedente di Open MPI | 49 |
| Capitolo 27. Desktop | 50 |
| Dipendenze incomplete del pacchetto pygobject3 impediscono l'aggiornamento dal Red Hat Enterprise Linux 7.1 | 50 |
| Capitolo 28. Aggiornamenti generali | 51 |
| I nuovi nomi dei dispositivi possono causare una interruzione della connessione di rete | 51 |
| Capitolo 29. Installazione e avvio | 52 |
| L'installazione in modalità testo non si arresta più inaspettatamente durante la configurazione di rete | 52 |
| Possibile messaggio d'errore di NetworkManager durante l'installazione | 52 |
| L'installazione di Atomic Host offre cryptsetup anche se non è disponibile. | 52 |
| L'installer può solo aggiungere uno storage avanzato durante il primo inserimento dello spoke di storage. | 52 |
| Capitolo 30. Kernel | 53 |
| Impossibile modificare la dimensione di alcuni filesystem ext4 | 53 |
| Perdita di connessione ripetuta con target iSCSI abilitati-iSER. | 53 |
| Il comando I/O invoca SCSI mid-layer fino a quando il sistema viene arrestato | 53 |
| Il certificato della chiave pubblica di Red Hat Beta deve essere caricato manualmente | 53 |
| Capitolo 31. Networking | 54 |
| Politica di timeout non abilitata con il kernel di Red Hat Enterprise Linux 7.2 | 54 |
| Capitolo 32. Gestione delle sottoscrizioni e sistemi | 55 |
| Registrazione incompleta in presenza di un errore | 55 |
| Pulsante Indietro (Back) inattivo nel componente aggiuntivo di Subscription Manager per l'utilità Initial Setup | 55 |

| | |
|--|-----------|
| Capitolo 33. Virtualizzazione | 56 |
| Navigazione GRUB 2 problematica con KVM | 56 |
| Il ridimensionamento dei dischi GUID Partition Table (GPT) sui guest Hyper-V, causa la generazione di alcuni errori della tabella. | 56 |
| Appendice A. Versione dei componenti | 57 |
| Appendice B. Diario delle Revisioni | 58 |

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 7.2* documentano le modifiche più importanti fatte al sistema operativo di Red Hat Enterprise Linux 6 e alle applicazioni relative per questa release minore, insieme ad un elenco completo delle problematiche conosciute e di tutte le Anteprime di tecnologia presenti.

Le funzionalità e i limiti di Red Hat Enterprise Linux 7 confrontati con altre versioni del sistema, sono disponibili nell'articolo della Knowledge Base su <https://access.redhat.com/articles/rhel-limits>.

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

Capitolo 1. Architetture

Red Hat Enterprise Linux 7.2 è disponibile come kit singolo sulle seguenti architetture: [1]

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

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

[1] Da notare che l'installazione di Red Hat Enterprise Linux 7.2 è supportata solo su hardware a 64-bit. Red Hat Enterprise Linux 7.2 può essere eseguito su sistemi operativi a 32-bit, incluse le versioni precedenti di Red Hat Enterprise Linux, come macchine virtuali.

[2] Red Hat Enterprise Linux 7.2 (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 7.2 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 7.2.

Parte I. Nuove funzioni

Questa sezione descrive nuove le funzioni e i miglioamenti più importanti introdotti in Red Hat Enterprise Linux 7.2.

Capitolo 2. Autenticazione

ca-certificates aggiornato alla versione 2.4

Il pacchetto `ca-certificates` è stato aggiornato alla versione upstream 2.4, ora sono disponibili alcune correzioni e miglioramenti rispetto alla versione precedente. In particolare `ca-certificates` presenta ora le seguenti modifiche:

In passato Mozilla rimuoveva il rapporto di fiducia con numerosi certificati CA preesistenti contenenti chiavi RSA a 1024-bit. Questa versione del pacchetto `ca-certificates` modifica l'elenco di Mozilla in modo da mantenere un rapporto fidato, per impostazione predefinita, con i suddetti certificati. Queste modifiche sono state apportate per garantire una compatibilità con implementazioni PKI esistenti e con software basati su OpenSSL o GnuTLS.

Il pacchetto `ca-certificates` include ora il comando **ca-legacy**, utilizzabile per disabilitare le modifiche di compatibilità precedentemente indicate. Consultare la pagina `man ca-legacy(8)` per maggiori informazioni su come utilizzare questo comando.

È consigliato agli utenti che desiderano disabilitare queste modifiche di consultare l'articolo del Knowledgebase 1413643, il quale fornisce le informazioni sulle suddette modifiche insieme alle possibili conseguenze se disabilitate.

Da notare che l'utilizzo del CA store unificato è necessario per utilizzare il comando **ca-legacy**. Consultare la pagina `man update-ca-trust(8)` su come abilitare un CA store unificato.

Supporto per rapporti fidati unidirezionali

L'Identity Management permette ora all'utente di configurare un rapporto fidato unidirezionale tramite l'esecuzione di **ipa trust-add**.

openldap aggiornato alla versione 2.4.40

I pacchetti `openldap` sono stati aggiornati alla versione upstream 2.4.40, questa versione fornisce un certo numero di correzioni e miglioramenti rispetto alla versione precedente. In particolare, le regole per la corrispondenza ORDERING sono state aggiunte alle descrizioni del tipo di attributo **ppolicy**. Tra i bug corretti: Il server non viene più terminato inaspettatamente durante la processazione dei record SRV, sono state aggiunte le informazioni **objectClass** mancanti, permettendo così all'utente di modificare una configurazione front-end seguendo gli standard previsti.

Autenticazione cache in SSSD

È ora disponibile con SSSD in modalità online l'autenticazione con la cache senza un tentativo di ricollegamento. L'autenticazione diretta ripetuta con il server di rete può causare una latenza ecceziva aumentando sensibilmente il tempo necessario per un processo di login.

SSSD abilita una mappatura UID e GID su client individuali

È ora possibile mappare gli utenti con UID e GID differenti su client Red Hat Enterprise Linux specifici attraverso una configurazione del client utilizzando SSSD. Questa impostazione può risolvere le problematiche causate da una duplicazione UID e GID.

SSSD è ora in grado di negare l'accesso SSH agli account bloccati

Quando SSSD utilizzava OpenLDAP come database di autenticazione gli utenti erano in grado di eseguire

una autenticazione nel sistema utilizzando una chiave SSH anche quando l'account utente risultava bloccato. Il parametro `ldap_access_order` accetta ora il valore `ppolicy`, il quale può negare l'accesso SSH all'utente in presenza di una situazione simile. Per maggiori informazioni sull'utilizzo di `ppolicy` consultare la descrizione di `ldap_access_order` disponibile nella pagina man di `sssd-ldap(5)`.

L'utilità sudo è ora in grado di verificare il checksum del comando

La configurazione dell'utilità sudo è in grado di archiviare il checksum di un comando o script abilitato. All'esecuzione dello script o del comando, il checksum viene confrontato con il valore archiviato per verificare la presenza di eventuali modifiche. Se il comando, o il binario, è stato modificato sudo non esegue il comando o registra un messaggio d'avvertimento. Questa funzione devolve correttamente le attività per la risoluzione dei problemi e le responsabilità in presenza di un errore.

Supporto delle smart card SSSD

SSSD supporta ora le smart card per l'autenticazione locale. Con questa funzione l'utente può eseguire una smart card per la registrazione sul sistema usando una console grafica o basata sul testo, insieme ai servizi locali come ad esempio sudo. L'utente posiziona la smart card nel lettore fornendo il nome utente e il relativo PIN al momento del login. Se il certificato della smart card è stato verificato correttamente, l'utente verrà autenticato.

Attualmente SSSD non permette all'utente di ottenere il ticket di Kerberos usando una smart card. A tale proposito l'utente dovrà utilizzare l'utilità kinit per la sua autenticazione.

Supporto profili multipli del certificato

Identity Management ora supporta i profili multipli per l'emissione di certificati del server e altri al posto di un profilo del certificato per un singolo server. I profili vengono archiviati nel Sistema del certificato.

Password Vault

È stata aggiunta all'Identity Management una nuova funzione che permette un'archiviazione centralizzata e sicura delle informazioni private degli utenti, come ad esempio password e chiavi. Password Vault aggiunge un livello ulteriore al sottosistema Public Key Infrastructure (PKI) Key Recovery Authority (KRA).

Supporto DNSSEC con l'Identity Management

I server dell'Identity Management con DNS integrato supportano ora le DNS Security Extensions (DNSSEC), un insieme di estensioni per DNS per il miglioramento della sicurezza del protocollo DNS. Le zone DNS presenti con i server dell'Identity Management possono essere firmate automaticamente utilizzando DNSSEC. Le chiavi crittografiche vengono generate e ruotate automaticamente.

È consigliato agli utenti che desiderano utilizzare questo livello di sicurezza offerto da DNSSEC, di consultare i documenti di seguito elencati:

DNSSEC Operational Practices, Version 2: <http://tools.ietf.org/html/rfc6781#section-2>

Secure Domain Name System (DNS) Deployment Guide: <http://dx.doi.org/10.6028/NIST.SP.800-81-2>

Da notare che i server dell'Identity Management con DNS integrato utilizzano DNSSEC per convalidare le risposte DNS ricevute da altri server DNS. Ciò potrebbe interessare negativamente la disponibilità delle zone DNS non configurate in base al tipo di nomi consigliati descritti in Red Hat Enterprise Linux Networking Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices

Proxy HTTPS di Kerberos con Identity Management

Una funzione Key Distribution Center (KDC), utilizzabile con Microsoft Kerberos KDC Proxy Protocol (MS-KKDCP), è ora disponibile nella Identity Management e permette ai clienti di accedere ai servizi **kpasswd** e KDC utilizzando HTTPS. Gli amministratori di sistema possono ora esporre il proxy ai margini della propria rete utilizzando un proxy HTTPS inverso, senza impostare e gestire un'applicazione apposita.

Aggiornamento nel background delle voci memorizzate in cache

SSSD permette alle voci memorizzate in cache di essere aggiornate fuori banda nel background. In precedenza quando la validità delle voci in cache scadeva, SSSD le recuperava dal server remoto e le archiviava nel database, questa operazione poteva richiedere un periodo di tempo molto esteso. Con questo aggiornamento le voci possono essere ritornate in modo istantaneo poiché il backend le mantiene sempre aggiornate. Questa impostazione causa un carico più elevato sul server poiché SSSD scarica periodicamente le voci.

Memorizzazione in cache di operazioni `initgroups`

La cache di memoria rapida SSSD supporta ora le operazioni **initgroups** le quali migliorano la velocità di processazione `initgroups` e le prestazioni di alcune applicazioni, per esempio GlusterFS e **slapi-nis**.

Negoziante autenticazione semplificata con `mod_auth_gssapi`

L'Identity Management utilizza ora il modulo **mod_auth_gssapi**, il quale utilizza le chiamate GSSAPI per le chiamate di Kerberos dirette usate dal modulo **mod_auth_kerb**.

Capacità di gestione del ciclo di vita dell'utente

La gestione del ciclo di vita dell'utente conferisce all'amministratore un maggior controllo sull'attivazione o disattivazione degli account. Gli amministratori possono ora eseguire il provisioning di nuovi account utente aggiungendoli in una area di stage senza attivarli, oppure attivarli o disattivarli in modo da renderli completamente operativi, o disattivarli senza rimuoverli completamente dal database.

Le capacità di gestione del ciclo di vita dell'utente rendono disponibili benefici importanti per le implementazioni IdM molto grandi. È possibile aggiungere gli utenti nell'area di stage direttamente da un client LDAP standard usando operazioni LDAP dirette. In precedenza IdM supportava solo la gestione degli utenti con strumenti a linea di comando IdM, o tramite l'IdM web UI.

Supporto SCEP in `certmonger`

È stato aggiornato il servizio **certmonger** per il supporto del Simple Certificate Enrollment Protocol (SCEP). È ora possibile emettere un nuovo certificato e rinnovare, o sostituire, quelli esistenti attraverso SCEP.

Nuovi pacchetti: `ipsilon`

I pacchetti *ipsilon* rendono disponibile il servizio per il provider dell'identità Ipsilon per il single sign-on (SSO) federato. Ipsilon vincola i provider per l'autenticazione e le applicazioni, o utilità, abilitando così un SSO. Esso include un server e le utilità per la configurazione dei provider dei servizi basati su Apache.

L'autenticazione utente per il SSO disponibile con Ipsilon viene eseguita tramite un sistema Identity Management separato, come ad esempio un server Identity Management. Ipsilon comunica con varie applicazioni e utilità attraverso protocolli federati, SAML o OpenID.

NSS aumenta i valori minimi accettati delle chiavi

La libreria Network Security Services (NSS) in Red Hat Enterprise Linux 7.2 non accetta più valori più piccoli di 768 bit per i parametri usati nello scambio delle chiavi Diffie-Hellman (DH), o certificati RSA e DSA con una dimensione delle chiavi minore di 1023 bit. L'aumento dei valori minimi accettati impedisce il verificarsi di attacchi alla sicurezza simili a Logjam (CVE-2015-4000) e FREAK (CVE-2015-0204).

Il tentativo di collegamento ad un server utilizzando chiavi più deboli rispetto ai nuovi valori minimi fallirà, anche se in passato era possibile stabilire una connessione su versioni precedenti di Red Hat Enterprise Linux.

nss e nss-util aggiornati alla versione 3.19.1

I pacchetti *nss* e *nss-util* sono stati aggiornati alla versione upstream 3.19.1. Ora sono disponibili un certo numero di correzioni e miglioramenti rispetto alla versione precedente. In particolare è ora possibile eseguire un aggiornamento a Mozilla Firefox 38 Extended Support Release. Questo aggiornamento impedisce il verificarsi di attacchi Logjam CVE-2015-4000.

I moduli Apache per IdM sono ora completamente supportati

I seguenti moduli Apache per l'Identity Management (IdM), aggiunti come Anteprima di tecnologia in Red Hat Enterprise Linux 7.1, sono ora completamente supportati: **mod_authnz_pam**, **mod_lookup_identity** e **mod_intercept_form_submit**. I moduli Apache sono utilizzabili ora da applicazioni esterne per una migliore interazione con IdM.

Capitolo 3. Clustering

systemd e pacemaker ora seguono correttamente il processo di spegnimento del sistema

In precedenza systemd e pacemaker non seguivano correttamente il processo di spegnimento del sistema causando l'arresto non corretto delle risorse di pacemaker. Con questo aggiornamento pacemaker viene arrestato correttamente prima di dbus e altri servizi systemd avviati da pacemaker. Questo processo permette l'arresto corretto di pacemaker e delle risorse da esso gestite.

I comandi `pcs resource move` e `pcs resource ban` ora mostrano un messaggio d'avvertimento per chiarirne il comportamento

`pcs resource move` e i comandi `pcs resource ban` creano un vincolo di posizione che impedisce l'esecuzione delle risorse sul nodo corrente fino alla rimozione del vincolo stesso, o alla scadenza del ciclo di vita del vincolo. In precedenza questo tipo di comportamento non era molto chiaro agli utenti. I suddetti comandi ora mostrano un messaggio d'avvertimento che ne chiarisce il comportamento. Altresì, sono stati semplificati sia la documentazione dei comandi che le schermate d'aiuto per una più facile comprensione.

Nuovo comando per spostare una risorsa del Pacemaker sul nodo preferito

Dopo aver riposizionato una risorsa di Pacemaker, a causa di un failover o per scelta di un amministratore, la risorsa non si riposiziona necessariamente sul suo nodo originale anche quando le circostanze che hanno causato il failover sono state corrette. A tal proposito è ora possibile utilizzare il comando `pcs resource relocate run` per riposizionare una risorsa sul nodo desiderato in base allo stato corrente del cluster, alle limitazioni, alla posizione delle risorse e altre impostazioni. È possibile usare altresì il comando `pcs resource relocate show` per visualizzare le risorse migrate. Per informazioni su questi comandi consultare la High Availability Add-On Reference.

Supporto per il comando `clufte` per la trasformazione e l'analisi dei formati di configurazione del cluster

Il comando `clufte` rende disponibile uno strumento per la trasformazione e l'analisi dei formati di configurazione del cluster. `clufte` può essere utilizzato durante la migrazione da una configurazione dello stack più vecchia ad una più nuova, in grado di sfruttare le potenzialità di Pacemaker. Per informazioni sulle capacità del comando `clufte` consultare la pagina man o l'output del comando `clufte -h`.

Capitolo 4. Compiler e strumenti

tail --follow ora funziona correttamente su file con Veritas Clustered file system (VXFS)

Veritas Clustered file system (VXFS) è un file system remoto, e per filesystem remoti, **tail** non può utilizzare 'inotify' per la modalità '--follow'. Il filesystem clusterizzato di Veritas è stato aggiunto all'elenco di filesystem remoti per i quali viene utilizzata la modalità di polling al posto di 'inotify'. **tail --follow** ora funziona correttamente anche quando utilizzati su file con VXFS.

Il comando dd ora è in grado di mostrare lo stato del processo di trasferimento

Il comando **dd**, usato per copiare i file per byte, ora è in grado di fornire l'opzione 'status=progress' per la visualizzazione dello stato di un processo di trasferimento. Ciò è particolarmente utile per il trasferimento di file molto grandi poichè permette all'utente di prevedere il tempo restante e rilevarne potenziali problemi.

Tempi d'attesa migliorati in libcurl

libcurl utilizzava un ritardo di blocco molto lungo non necessario per le azioni senza descrittori del file attivo, anche per operazioni molto piccole. Per tale motivo alcune azioni, come ad esempio la risoluzione del nome dell'host utilizzando **/etc/hosts**, richiedevano un periodo di tempo esteso. Il codice di blocco in **libcurl** è stato modificato, ora il ritardo iniziale è più corto e aumenta gradualmente fino alla presenza di un evento. Operazioni **libcurl** veloci vengono completate più rapidamente.

La libreria libcurl implementa ora operazioni handshake SSL senza alcun blocco

In precedenza **libcurl** non implementava operazioni handshake SSL senza blocco, questa impostazione influiva negativamente sulle prestazioni delle applicazioni in base a **libcurl** multi API. Per correggere questo problema è stata implementata una operazione handshake SSL senza alcun blocco in **libcurl**, e **libcurl** multi API ora ritorna immediatamente il controllo all'applicazione ogni qualvolta non è in grado di leggere o scrivere i dati da o per il socket di rete sottostante.

GDB su IBM Power System non genera più alcun errore quando accede alla tabella dei simboli

In precedenza su sistemi IBM Power a 64-bit GDB rimuoveva erroneamente una variabile importante che conteneva la tabella dei simboli per il binario usato per il debugging. Questo comportamento causava un errore di segmentazione quando GDB cercava di accedere la tabella in questione. A tale scopo la variabile è stata resa persistente, e GDB può ora accedere alle informazioni necessarie durante la sessione di debugging, senza leggere l'area non valida della memoria.

nscd aggiornato per un caricamento automatico dei dati per la configurazione

L'aggiornamento del Name Server Caching Daemon (nscd) aggiunge un sistema di monitoraggio basato su inotify e un monitoraggio di backup basato su stat per i file di configurazione nscd, in questo modo nscd ora rileva correttamente le modifiche alla propria configurazione, ricaricando i dati. Ciò impedisce a nscd di ritornare dati obsoleti.

La funzione della libreria dlopen non si arresta più inaspettatamente in presenza di chiamate ricorsive.

In precedenza, un difetto in **dlopen** causava l'arresto inaspettato delle chiamate ricorsive per questa funzione, o una interruzione con una asserzione della libreria. È possibile eseguire chiamate ricorsive se una implementazione **malloc** dell'utente invoca **dlopen**.

Ora l'implementazione risulta essere conforme e le chiamate ricorsive non si arrestano inaspettatamente o interrotte con una asserzione.

operf è in grado ora di riconoscere gli identificatori di huge page statiche

In precedenza durante il profiling del codice Java just-in-time (JIT) con pagine molto grandi statiche, il comando **operf** di OProfile registrava un numero elevato d'esempi di eventi sulla memoria anonima (in `anon_hugepage`), al posto di usare il metodo Java appropriato. Con questo aggiornamento **operf** riconosce gli identificatori di pagine grandi statiche e mappa correttamente gli esempi sui metodi Java se si utilizzano le suddette pagine.

Il comando **rsync -X** ora funziona correttamente

In precedenza **rsync** modificava la proprietà del file dopo, e non prima, l'impostazione degli attributi di sicurezza. Di conseguenza non erano disponibili gli attributi di sicurezza sul target e **rsync -X** non veniva eseguito correttamente in presenza di determinate circostanze. Con questo aggiornamento l'ordine delle operazioni è stato modificato e **rsync** ora modifica la proprietà prima di impostare gli attributi di sicurezza. Così facendo gli attributi di sicurezza sono presenti come previsto nella situazione appena descritta.

Gli eseguibili Subversion vengono ora compilati con dati RELRO completi

Gli eseguibili disponibili con il pacchetto *subversion* sono ora compilati con read-only relocation data (RELRO) completi, e proteggono contro alcuni attacchi alla memoria. Così facendo sarà più difficile attaccare Subversion in presenza di possibili vulnerabilità future.

L'estensione del thread in TCL ora funziona correttamente

In precedenza il supporto per il threading nel Tool Command Language (TCL) non veniva implementato in maniera ottimale. Se la chiamata `fork()` veniva utilizzata con una estensione del thread abilitata nell'interprete TCL, il processo poteva risultare inattivo. Per questo motivo l'interprete TCL e l'applicazione TK erano disponibili con una estensione del thread non abilitata. A causa di questa impostazione le applicazioni di Terze Parti che dipendevano dal TK o TCL in thread non funzionavano correttamente. Per correggere questo problema è stato reso disponibile un patch. Ora per impostazione predefinita è stata abilitata l'estensione del thread sia su TCL che su TK.

Capitolo 5. Desktop

GNOME 3.14

GNOME Desktop è stato aggiornato alla versione 3.14 upstream, e include nuove funzioni e miglioramenti. In particolare:

Sono state aggiunte un certo numero di funzioni al protocollo **Wayland**, esse includono la configurazione della tastiera, il supporto per uno schermo tattile, supporto per operazioni trascina e rilascia, menu scelta rapida funzionali, suggerimenti e caselle combinate, supporto per un display ad alta risoluzione e ridimensionamento e spostamento della finestra.

Con i touchscreen è ora possibile eseguire **Gesti Multitouch** per la navigazione del sistema o per le applicazioni desiderate. I gesti sono utilizzabili per aprire la Panoramica delle attività, per consultare la visuale delle applicazioni e l'area di notifica. Essi possono essere utilizzati anche per cambiare applicazioni e aree di lavoro.

GNOME 3.14 rende disponibile un supporto migliorato per gli Wi-Fi hotspot. Durante il collegamento ad un portale Wi-Fi che richiede una autenticazione, GNOME ora mostra automaticamente la pagina di login come parte del processo di connessione.

Screen Sharing (VNC), **Media Sharing (DLNA)** e **File Sharing (WebDAV)** personale ora sono in grado di memorizzare la rete sulla quale l'utente desidera attivarli. Le Impostazione possono altresì fornire l'abilità di controllare le reti sulle quali eseguire la condivisione. Questa funzione impedisce la condivisione pubblica di servizi e contenuti.

Se si utilizzano monitor multipli, GNOME 3.14 ripristina ora le schermate nella loro posizione originale quando i monitor vengono scollegati e ricollegati.

Applicazione di GNOME per macchine virtuali e remote, **Boxes** introduce le istantanee. Altresì, **Boxes** fornisce ora un download automatico, l'esecuzione di riquadri multipli in finestre separate, e miglioramenti all'interfaccia utente, incluso un miglior comportamento in modalità schermo intero e nelle anteprime.

GTK+ 3.14 presenta un certo numero di correzioni e miglioramenti, come ad esempio il caricamento automatico dei menu dalle risorse, il supporto per selezioni multiple in **GtkListBox**, l'associazione delle proprietà nei file **GtkBuilder**, il supporto per il disegno al di fuori di una allocazione del widget (`gtk_widget_set_clip()`), nuove transizioni in **GtkStack**, ed il salvataggio e caricamento dei file con **GtkSourceView**. Altresì, **GTK+** rende disponibile ora il supporto per il riconoscimento dei gesti. Con 3.14, la maggior parte dei gesti più comuni sono disponibili con le applicazioni GTK+, come ad esempio tocca, trascina, scorri, ruota e avvicina le dita (pinch). È possibile altresì aggiungere ulteriori gesti alle applicazioni GTK+ esistenti usando **GtkGesture**.

Glib 3.14 fornisce ora un supporto per le nuove Specifiche per le associazioni delle applicazioni MIME, il supporto SHA-512 in GHmac, il supporto per le implementazioni nei file del desktop e il supporto unicode 7.0.

Il browser di documentazione **Help** di GNOME è stato aggiornato. Ora risulta essere più conforme ad altre applicazioni GNOME 3, utilizza una barra per le intestazioni, ha una funzione di ricerca integrata e una interfaccia per i segnalibri.

GNOME Shell Extension, **Looking Glass Inspector**, presenta ora un certo numero di funzioni per sviluppatori: ora è possibile mostrare tutti i metodi, le classi, ecc. in uno spazio dei nomi tra le ispezioni, espansione cronologia per il controllo degli oggetti, o la copiatura dei risultati "Looking Glass" come stringhe, e il passaggio di eventi su `gnome-shell`.

Il pacchetto `ibus-gtk2` aggiorna ora il file `immodules.cache`

In precedenza lo script **update-gtk-immodules** andava alla ricerca di una directory non più esistente **/etc/gtk-2.0/\$host**. Di conseguenza lo script post-installazione del pacchetto *ibus-gtk2* falliva, uscendo senza creare o aggiornare la cache. Lo script post-installazione è stato modificato per sostituire **update-gtk-immodules** con **gtk-query-immodules-2.0-BITS**, risolvendo così questo problema.

Capitolo 6. File System

gfs2-utils aggiornato alla versione 3.1.8

Il pacchetto *gfs2-utils* è stato aggiornato alla versione 3.1.8, ora sono disponibili correzioni importanti e un certo numero di miglioramenti:

- * Migliorate le prestazioni di **fsck.gfs2**, **mkfs.gfs2**, e **gfs2_edit**.
- * Controllo migliorato da parte di **fsck.gfs2** sui journal, jindex, inode del sistema e valori 'goal' dell'inode.
- * Le utilità **gfs2_jadd** e **gfs2_grow** sono ora programmi separati e non collegamenti simbolici per **mkfs.gfs2**.
- * Migliorata la suite di test e relative documentazioni.
- * Il pacchetto non dipende più da Perl.

GFS2 impedisce agli utenti di superare i propri quota

In precedenza GFS2 eseguiva il controllo delle violazioni dopo il completamento delle operazioni, così facendo gli utenti o gruppi potevano superare i limiti dei quota a loro assegnati. Questo comportamento è stato corretto, ora GFS2 è in grado di prevedere il numero di blocchi assegnabili da una operazione, e controlla se la loro assegnazione supera i quota previsti. Le operazioni che risultano in una violazione non verranno eseguite, così facendo gli utenti e i gruppi non potranno superare i limiti di quota a loro assegnati.

XFS aggiornato alla versione 4.1

XFS è stato aggiornato alla versione 4.1 dell'upstream e include piccole correzioni, refactoring, modifiche di alcuni meccanismi interni, ad esempio login, pcpu accounting e un nuovo blocco mmap. Oltre ad alcune modifiche importanti questo aggiornamento amplia il tipo di utilizzo della funzione rename() aggiungendo cross-rename (una variante simmetrica di rename()) e la gestione whiteout.

Aggiornamento ext4 e jbd2

I dispositivi ext4 e jbd2 sono stati aggiornati all'ultimissima versione dell'upstream. Ora sono disponibili le correzioni e i miglioramenti rispetto alla versione precedente.

cifs aggiornato alla versione 3.17

Il modulo CIFS è stato aggiornato alla versione 3.17 dell'upstream e rende disponibile piccole correzioni e nuove funzioni per il Server Message Block 2 e 3 (SMB2 and SMB3).

Capitolo 7. Aggiornamenti generali

Iftp ora gestisce correttamente 302 redirection

Iftp è stato aggiornato, ora è in grado di gestire 302 redirection quando in esecuzione in modalità mirror. In precedenza Iftp eseguiva l'arresto con un errore.

Più informazioni per la diagnosi e modifica del nome per il plug-in di sosreport

sosreport è stato migliorato, ora è in grado di ottenere le informazioni relative al processo da varie applicazioni, incluso ptp, lastlog e ethtool. In questa modifica il plug-in **startup** è stato rinominato in **services** per migliorare la comunicazione delle proprie funzioni.

Capitolo 8. Installazione e avvio

È possibile correggere l'impostazione di rete in `initrd` se si fornisce una configurazione di rete in Kickstart

In precedenza l'installer non era in grado d'impostare o riconfigurare le interfacce di rete in `initrd` se le suddette interfacce erano definite nei file kickstart. Ciò poteva causare il fallimento dell'installazione e l'introduzione di una modalità di emergenza, se l'accesso alla rete era richiesto da altri comandi nel file Kickstart.

Ora questo problema è stato risolto, Anaconda è in grado di gestire correttamente la configurazione di rete dai file Kickstart in `initrd` nelle fasi iniziali del processo d'avvio.

Anaconda ora supporta la creazione dei volumi logici in cache

L'installer supporta ora la creazione dei volumi logici LVM in cache e l'installazione del sistema sui volumi.

Attualmente questo approccio è supportato solo con Kickstart. Per creare un volume logico in cache usare le nuove opzioni `--cachepvs=`, `--cachesize=` e `--cachemode=` del comando `logvol` di Kickstart.

Per informazioni dettagliate su queste nuove opzioni consultare la Red Hat Enterprise Linux 7 Installation Guide.

Elenco del menu d'avvio di GRUB migliorato

In precedenza un problema relativo al dispositivo di selezione usato dal comando `grub2-mkconfig`, poteva causare la generazione del file di configurazione `grub.cfg` con i kernel disponibili ordinati in modo incorretto.

GRUB2 ora utilizza il pacchetto `rpmdevtools` per ordinare i kernel disponibili, ora il file di configurazione viene generato correttamente con la versione del kernel più recente elencato nella parte più alta.

Anaconda ripristina ora correttamente le azioni del disco al variare della selezione del disco stesso

In precedenza Anaconda e Blivet non ripristinavano correttamente le azioni programmate sul disco al variare della selezione del disco stesso, causando vari tipi di problemi. Con questo aggiornamento Anaconda è stato corretto, ora è possibile avere una istantanea della configurazione dello storage originale, utilizzabile al variare della selezione del disco ripristinando così tutte le azioni programmate.

Rilevamento migliorato dei nomi per il device-mapper

Nella versione precedente di Red Hat Enterprise Linux 7 l'installer si arrestava inaspettatamente durante il processo d'installazione sui dischi contenenti volumi logici LVM, e i metadati per questi volumi erano ancora presenti. L'installer non era in grado di riconoscere i nomi del `device-mapper` corretti e il processo di creazione di nuovi volumi logici LVM falliva.

Il metodo usato per ottenere i nomi del `device-mapper` è stato aggiornato. L'installazione sui dischi contenenti metadati LVM esistenti ora è più affidabile.

Corretto il processo di gestione di PReP Boot durante il partizionamento

Su sistemi IBM Power in alcune circostanze la partizione **PreP Boot** poteva essere impostata su una dimensione non valida durante il partizionamento personalizzato. In questa condizione, e se si rimuoveva qualsiasi partizione, l'installer si arrestava inaspettatamente.

Ora vengono implementati alcuni controlli in *anaconda* per assicurare che la partizione abbia sempre una dimensione corretta, la gamma accettata è tra **4096 KiB** e **10 MiB**. Non è altresì più necessario modificare il formanto della partizione **PreP Boot** per modificare la dimensione.

Partizioni EFI su dispositivi RAID1

Le partizioni EFI possono ora essere create su dispositivi RAID1, ciò permette di eseguire il ripristino del sistema se un disco d'avvio fallisce. Tuttavia se **Boot####** o **BootOrder**, e il volume di ESP scoperto dal firmware, risultano essere corrotti ma continuano a ad essere riportati come ESP validi, l'ordine d'avvio non verrà compilato automaticamente. In queste situazioni sarà possibile avviare manualmente il sistema utilizzando il secondo disco.

L'installazione in modalità testo non si arresta più inaspettatamente durante la configurazione di rete

In precedenza nella schermata di Configurazione di rete con l'installer in modalità di testo interattiva, l'uso dello spazio durante l'inserimento dei server dei nomi causava un arresto inaspettato dell'installer.

Anaconda ora gestisce correttamente gli spazi presenti nelle definizioni del server dei nomi in modalità testo, e l'installer non si arresterà più inaspettatamente se lo spazio viene usato per separare gli indirizzi.

Le schermate della modalità di ripristino su IBM System z, sono ora visualizzate correttamente

In precedenza, la seconda e terza schermata in modalità di ripristino sui server IBM System z venivano visualizzate incorrettamente poiché parte della schermata era incompleta. La modalità di ripristino su questa architettura è stata migliorata, ora tutte le schermate vengono visualizzate correttamente.

Componente aggiuntivo OpenSCAP in Anaconda

È ora possibile applicare il contenuto Security Content Automation Protocol (SCAP) durante il processo d'installazione. Questo nuovo componente rende disponibile un metodo semplice e affidabile per configurare una politica di sicurezza, senza dover utilizzare gli script personalizzati.

Questo componente fornisce una nuova sezione di kickstart ("`%addon org_fedora_oscaps`") e una nuova schermata nell'interfaccia utente grafica durante una installazione interattiva. Esse sono documentate nella Red Hat Enterprise Linux 7 Installation Guide.

L'uso di una politica di sicurezza durante l'installazione comporterà l'esecuzione di alcune modifiche durante e immediatamente dopo l'installazione a seconda della politica abilitata. Selezionando un profilo verrà aggiunto il pacchetto *openscap-scanner* (uno strumento d'analisi della conformità di OpenSCAP) alla selezione dei pacchetti, e verrà eseguita una scansione iniziale dopo l'installazione. I risultati di questa scansione saranno archiviati in `/root/openscap_data`.

Tramite il pacchetto *scap-security-guide* saranno resi disponibili sul supporto d'installazione diversi profili. Se necessario, sarà possibile caricare altri contenuti come flusso dati, archivio o pacchetto RPM da un server HTTP, HTTPS o FTP.

Ricordiamo che la politica di sicurezza non viene necessariamente applicata su tutti i sistemi. Usare questo componente solo quando una politica specifica deve essere implementata a causa di direttive governative o aziendali, in caso contrario lasciare il componente aggiuntivo con uno stato predefinito, così facendo non verrà implementata alcuna politica.

Non si verifica più il time out di Anaconda durante l'attesa per un file Kickstart su un CD o DVD

Se in passato Anaconda veniva configurato per caricare un file kickstart da un supporto ottico usando il comando `inst.ks=cdrom:/ks.cfg`, e se il sistema veniva avviato da un CD o DVD, l'installer attendeva per un breve periodo di tempo fino a quando l'utente non cambiava disco. Per impostazione predefinita questo periodo era molto breve - solo 30 secondi. Dopo il suddetto periodo veniva utilizzata la modalità di ripristino.

Ora Anaconda è stato modificato, durante il periodo d'attesa entro il quale l'utente doveva fornire un file Kickstart su un CD o DVD, Anaconda non incorrerà più in un time out. Se vengono utilizzate le opzioni d'avvio `inst.ks=cdrom`, e il file Kickstart non è stato rilevato, Anaconda mostrerà un prompt e attenderà fino a quando l'utente non sarà in grado di fornire un file o eseguirà un riavvio.

Capitolo 9. Kernel

I parametri del kernel, SHMMAX e SHMALL, sono stati reimpostati su valori predefiniti.

In precedenza i valori di `kernel.shmmax` e `kernel.shmall`, impostati nel file `/usr/lib/sysctl.d/00-system.conf`, erano troppo bassi. A causa di questa impostazione alcune applicazioni, ad esempio SAP, non erano in grado di operare correttamente. Gli override non corretti sono stati rimossi, al loro posto vengono utilizzati i valori predefiniti del kernel.

Le transparent huge pages non causano più la corruzione della memoria

Le Transparent huge pages non venivano sincronizzate correttamente durante le operazioni di lettura e scrittura, ne risultava una corruzione della memoria quando le transparent huge pages venivano abilitate. A tale scopo sono state aggiunte alcune barriere per la gestione delle transparent huge page le quali non permettono più alcuna corruzione della memoria.

Aggiornamento SCSI LIO

Il target del kernel SCSI, LIO, è stato aggiornato da Linux-4.0.stable. L'aggiornamento apporta numerose correzioni, in particolare per iSER, ma include anche il supporto per i comandi XCOPY, WRITE SAME e ATS; ed il supporto per l'integrità dei dati DIF.

makedumpfile supporta ora il nuovo formato di sadump fino a 16 TB di memoria fisica

Il comando `makedumpfile` supporta ora il nuovo formato di `sadump` con uno spazio di memoria fisica maggiore di 16 TB. Questo nuovo formato permette agli utenti di `makedumpfile` di leggere i file dump con una dimensione maggiore a 16 TB, generati da `sadump` su alcuni nuovi modelli di server.

La rimozione o l'aggiornamento del kernel non mostra più alcun messaggio d'avviso

Lo script `weak-modules`, usato da `kmod` per gestire i link simbolici del modulo compatibile con kABI, rimuoveva `/lib/modules/<version>/weak-updates` durante la rimozione dei file associati con un kernel. La directory apparteneva al pacchetto `kernel`, e la sua rimozione causava un livello di inconsistenza tra il file system e lo stato previsto da `rpm`. Questo comportamento causava un messaggio d'avvertimento ogni qualvolta un kernel veniva aggiornato o rimosso.

Questo script è stato aggiornato, ora verranno rimossi solo i contenuti della directory `weak-updates` senza toccare la directory stessa. Così facendo non saranno più visualizzati i messaggi d'avvertimento.

Nuovo pacchetto: libevdev

`libevdev` è una libreria semplice per l'interfaccia del dispositivo degli eventi d'input del kernel di Linux. Questa libreria fornisce una interfaccia sicura per l'interrogazione delle capacità del dispositivo e degli eventi dei processi. Questa libreria è una dipendenza per le versioni correnti di `xorg-x11-drv-evdev` e `xorg-x11-drv-synaptics`.

Tuned è ora in grado di essere eseguito in modalità no-daemon

In precedenza Tuned poteva essere eseguito solo come demone. Questa impostazione diminuiva le prestazioni di sistemi più piccoli a causa del footprint della memoria del demone Tuned. Con questo aggiornamento la modalità no-daemon (one shot), la quale non richiede alcuna memoria residente, è stata aggiunta a Tuned. La modalità no-daemon è disabilitata per impostazione predefinita poichè gran parte della funzionalità di Tuned non è disponibile in questa modalità.

Nuovo pacchetto: tuned-profiles-rttime

È stato aggiunto un nuovo pacchetto *tuned-profiles-rttime* a Red Hat Enterprise Linux Server e Red Hat Enterprise Linux per Real Time. Nel suo interno è disponibile un profilo realtime usato dall'utilità **tuned** per isolare la CPU e ottimizzare IRQ. Se attivato, questo profilo è in grado di consultare una sezione variabile, la quale specifica le CPU da isolare, modificando altresì la posizione di tutti i thread che potevano essere spostati dalle suddette CPU.

Programmazione Multiqueue I/O con blk-mq

Red Hat Enterprise Linux 7.2 rende disponibile un nuovo meccanismo per la programmazione I/O per code multiple di dispositivi a blocco, conosciuto come blk-mq. Il suo utilizzo permette di migliorare le prestazioni tramite la mappatura delle richieste I/O su code software o hardware multiple da parte di alcuni driver del dispositivo. Riducendo la contesa del blocco presente quando thread multipli eseguono un I/O per un dispositivo, sarà possibile migliorare le prestazioni. I dispositivi più recenti, come ad esempio Non-Volatile Memory Express (NVMe), sono in grado di sfruttare al massimo i vantaggi offerti da questa funzione, a causa del supporto nativo per code e per trasmissioni hardware multiple, e delle caratteristiche di rendimento a bassa latenza. I miglioramenti delle prestazioni dipendono dal carico di lavoro e dal tipo di hardware.

È attualmente implementata, e abilitata per impostazione predefinita, la funzione blk-mq nei seguenti driver: virtio-blk, mtip32xx, nvme e rbd.

La funzione scsi-mq permette ai driver del dispositivo Small Computer System Interface (SCSI) di utilizzare l'infrastruttura blk-mq. scsi-mq è disponibile come Anteprema di tecnologia in Red Hat Enterprise Linux 7.2. Per abilitare scsi-mq specificare **scsi_mod.use_blk_mq=y** nella linea di comando del kernel. Il valore predefinito è **n** (disabilitato).

Il target multipath del device mapper (DM), il quale utilizza le richieste basate su DM, può essere configurato per l'infrastruttura di blk-mq se l'opzione **dm_mod.use_blk_mq=y** è stata specificata. Il valore predefinito è **n** (disabled).

Se i dispositivi SCSI sottostanti utilizzano blk-mq può essere utile impostare **dm_mod.use_blk_mq=y**, così facendo è possibile ridurre l'overhead del blocco a livello del DM.

Per determinare se DM multipath utilizzi blk-mq su un sistema eseguire cat sul file **/sys/block/dm-X/dm/use_blk_mq**, dove **dm-X** viene sostituito dal dispositivo DM multipath relativo. Questo è un file di sola lettura e riflette il valore globale in **/sys/module/dm_mod/parameters/use_blk_mq** al momento della creazione del dispositivo DM multipath.

Ora è più semplice interpretare i messaggi d'errore SCSI

In precedenza le modifiche apportate sul kernel che riguardavano la funzione printk() generavano messaggi d'errore Small Computer System Interface (SCSI) su linee multiple. Ne conseguiva che in presenza di errori multipli su diversi dispositivi, era estremamente complesso interpretare correttamente i messaggi d'errore. Questo aggiornamento modifica il codice di registrazione degli errori SCSI, e permette di utilizzare l'opzione dev_printk() la quale associa ogni messaggio con il dispositivo che ha generato l'errore.

Driver e sottosistema libATA aggiornati

Questo aggiornamento fornisce un certo numero di correzioni e miglioramenti dei driver e del sottosistema libATA

Aggiornati FCoE e DCB

I componenti Fibre Channel over Ethernet (FCoE) e Data Center Bridging (DCB) sono stati aggiornati all'ultimissima versione upstream. Ora sono disponibili diverse correzioni e miglioramenti rispetto alle versioni precedenti.

perf aggiornato alla versione 4.1

I pacchetti perf sono stati aggiornati alla versione 4.1 dell'upstream. Sono ora disponibili un certo numero di miglioramenti e correzioni relative alle prestazioni e alla stabilità rispetto alla versione precedente. In particolare, questo aggiornamento rende disponibile le funzioni Intel Cache QoS Monitoring e AMD IBS Ops, e fornisce un supporto per Intel Xeon v4, per i moduli kernel compressi, per gli eventi parametrizzati e la possibilità di specificare la lunghezza dei punti d'interruzione. Sono state aggiunte altresì un certo numero di opzioni allo strumento perf, come ad esempio `--system-wide`, `top -z`, `top -w`, `trace --filter-pids` e `trace --event`.

Supporto per TPM 2.0

Questo aggiornamento aggiunge un supporto a livello-driver per i dispositivi Trusted Platform Module (TPM) conformi alla versione 2.0.

Turbostat fornisce ora un output corretto

In precedenza turbostat era in grado di rilevare la presenza del supporto del dispositivo MSR attraverso la lettura del file `/dev/cpu/0/msr` per `cpu0`, al posto di `cpu`. Ne risultava che disabilitando una CPU causava la rimozione delle CPU dall'output di turbostat. Questo bug è stato corretto, ora l'esecuzione del comando `turbostat ls` ritorna un output conforme.

Supporto per il processore Xeon v5 di Intel

Con questo aggiornamento è stato introdotto su turbostat il supporto al processore Xeon v5 di Intel

zswap utilizza l'API zpool

In precedenza zswap utilizzava zbud, un pool di archiviazione in grado di archiviare pagine compresse con un rapporto di 2:1 (quando complete). Questo aggiornamento introduce l'API zpool per mezzo della quale è possibile accedere ai pool zbud o zsmalloc: zsmalloc archivia le pagine compresse con una densità potenzialmente più elevata, ne consegue così una richiesta maggiore di memoria per pagine altamente comprimibili. Con questo aggiornamento zsmalloc è stato promosso ai driver `/mm`, ora zpool funziona come previsto.

La lunghezza del file `/proc/pid/cmdline` è ora illimitata

Il limite della lunghezza del file `/proc/pid/cmdline` per il comando `ps` era precedentemente impostato nel kernel su 4096 caratteri. Con questo aggiornamento la lunghezza di `/proc/pid/cmdline` è illimitata. Questa impostazione è utile per l'ascolto dei processi con argomenti della linea di comando molto lunghi.

Ora è disponibile il supporto per `dma_rmb` e `dma_wmb`

Questo aggiornamento introduce due nuove primitive per la sincronizzazione dei processi di scrittura e lettura

della memoria coerente, `dma_wmb()` e `dma_rmb()`. Questa funzione sarà disponibile per un uso appropriato nei driver.

Capitolo 10. Networking

SNMP segue correttamente le direttive di `clientaddr` attraverso IPv6

In precedenza l'opzione `clientaddr` in `snmp.conf` interessava solo i messaggi in uscita inviati attraverso IPv4. Con questa release i messaggi IPv6 in uscita vengono inviati correttamente dall'interfaccia specificata da `clientaddr`.

tcpdump supporta `-J`, `-j`, e `--time-stamp-precision`

Come kernel, glibc e libpcap dispongono ora di API per ottenere i timestamp con risoluzioni in nanosecondi, tcpdump è stato aggiornato per sfruttare questa funzionalità. Gli utenti sono ora in grado di richiedere i sorgenti dei timestamp disponibili (`-J`), impostare un sorgente specifico del timestamp (`-j`) e richiedere timestamp con risoluzioni specifiche (`--time-stamp-precision`).

Aggiornamento TCP/IP

TCP/IP stack è stato aggiornato alla versione 3.18 dell'upstream. Ora sono disponibili le correzioni e i miglioramenti rispetto alla versione precedente. In particolare, questo aggiornamento corregge l'estensione d'apertura rapida TCP; ora la suddetta estensione funziona correttamente con IPv6. È disponibile altresì un supporto per un autocorking TCP opzionale e l'implementazione di Data Center TCP (DCTCP).

Capitolo 11. Servizi e Server

La direttiva `ErrorPolicy` è ora valida

In precedenza la direttiva `ErrorPolicy` non era valida, per questo motivo era possibile utilizzare una politica d'errore non desiderata senza alcun preavviso. Ora la direttiva è stata convalidata al momento dell'avvio, e il valore predefinito verrà ripristinato se quello configurato non è corretto. Con questo aggiornamento potrà essere usata solo la politica desiderata, in caso contrario verrà generato un messaggio d'avvertimento.

Per impostazione predefinita `CUPS` ora disabilita la cifratura `SSLv3`

In precedenza non era possibile disabilitare la cifratura `SSLv3` nello scheduler `CUPS`, lasciandolo così vulnerabile agli attacchi nei confronti di `SSLv3`. Per risolvere questo problema è stato esteso l'uso di `cupsd.conf SSLOptions` in modo da includere due nuove opzioni, `AllowRC4` e `AllowSSL3`, ognuna delle quali abilita la funzione named in `cupsd`. Le nuove opzioni sono supportate nel file `/etc/cups/client.conf`. Per `cupsd`, per impostazione predefinita sia `RC4` che `SSL3` sono disabilitati.

`Cups` ora permette l'uso del trattino basso nei nomi della stampante

Il servizio `cups` permette ora agli utenti di includere il trattino basso (`_`) nei nomi della stampante locale.

Le dipendenze non necessarie sono state rimosse dal pacchetto `tftp-server`

In passato, per impostazione predefinita, veniva installato un pacchetto aggiuntivo durante l'installazione di `tftp-server`. Con questo aggiornamento la dipendenza del pacchetto superfluo è stata rimossa. Così facendo il pacchetto non necessario non verrà più installato per impostazione predefinita durante l'installazione di `tftp-server`.

Il file `/etc/sysconfig/conman` deprecato è stato rimosso

Prima di introdurre il `systemd` manager era possibile configurare in `/etc/sysconfig/conman` svariati limiti per il servizio. Dopo la migrazione a `systemd`, `/etc/sysconfig/conman` non viene più usato e quindi è stato rimosso. Per impostare i limiti e altri parametri del demone, come ad esempio `LimitCPU=`, `LimitDATA=`, o `LimitCORE=`, modificare `conman.service`. Per maggiori informazioni consultare la pagina man di `systemd.exec(5)`. Altresì, è stata aggiunta una nuova variabile `LimitNOFILE=10000`, sul file `systemd.service`. Per impostazione predefinita questa variabile è stata decommentata. Dopo aver eseguito qualsiasi modifica nella configurazione di `systemd`, eseguire `systemctl daemon-reload` per la loro implementazione.

Capitolo 12. Storage

Nuove opzioni `delay_watch_checks` e `delay_wait_checks` nel file `multipath.conf`

Se un percorso non è affidabile - se il collegamento si interrompe spesso - `multipathd` cercherà di usare quel percorso. Il timeout usato da `multipathd` per considerare il percorso non più accessibile è 300 secondi. Un periodo di tempo considerevole che può indicare erroneamente che `multipathd` è entrato in sospensione.

Per correggere questo errore sono state aggiunte due nuove opzioni di configurazione: `delay_watch_checks` e `delay_wait_checks`. Impostare `delay_watch_checks` sul numero di cicli che `multipathd` deve utilizzare per controllare il percorso dopo uno stato online. Se il percorso fallisce entro il valore assegnato, `multipathd` non lo utilizzerà, affidandosi a `delay_wait_checks` per indicare il numero di cicli da passare prima che il percorso venga preso in considerazione (valido). Questa impostazione impedisce l'uso di percorsi non validi appena gli stessi risultano essere online.

Nuova opzione `config_dir` nel file `multipath.conf`

Gli utenti non erano in grado di suddividere la propria configurazione tra `/etc/multipath.conf` e altri file di configurazione. Ciò impediva loro di impostare un file di configurazione principale per tutte le macchine, e mantenere le informazioni sulla configurazione specifiche alle macchine, in file di configurazione separati per ogni macchina.

Per risolvere questo problema è stata aggiunta una opzione `config_dir` nel file `multipath.conf`. A tale scopo è richiesto agli utenti di modificare l'opzione `config_dir` con una stringa vuota o un fully qualified directory path name. Se impostata su qualsiasi altro valore diverso da una stringa vuota, `multipath` leggerà tutti i file `.conf` in ordine alfabetico. Successivamente verranno applicate le configurazioni esatte come se le stesse fossero state aggiunte a `/etc/multipath.conf`. Se questa modifica non viene apportata, `config_dir` eseguirà un default su `/etc/multipath/conf.d`.

Aggiornamento DM

Device Mapper (DM) è stato aggiornato alla versione upstream 4.0 e fornisce ora una serie di correzioni e miglioramenti rispetto alla versione precedente, incluso un aggiornamento importante delle prestazioni di cifratura del DM e un aggiornamento per il supporto di Multi-Queue Block I/O Queueing Mechanism (blk-mq).

Nuovo comando `dmstats` per visualizzare e gestire le statistiche I/O delle regioni definite dall'utente dei dispositivi che utilizzano il driver del device-mapper

Il comando `dmstats` fornisce un supporto dello spazio utente per le statistiche I/O del device-mapper. Ciò consente all'utente di creare, gestire e riportare i contatori I/O, le metriche e i dati di istogramma della latenza, per regioni arbitrarie dei dispositivi del device-mapper. I campi delle statistiche sono disponibili nei rapporti `dmsetup`, il comando `dmstats` aggiunge alcune nuove modalità di riporto specializzate utilizzabili con le informazioni relative alle statistiche. Per informazioni sul comando `dmstats`, consultare la pagina man di `dmstats(8)`.

Supporto per DIX su hardware specificato

In Red Hat Enterprise Linux 7.2, SCSI T10 DIX è completamente supportato per i seguenti array di storage e HBA e non sulle LUN usate per eseguire l'avvio da un ambiente SAN. T10 DIX è supportato in RHEL 7 solo su hardware nativo e non se eseguito su guest virtualizzati.

* EMULEX LPe16000/LPe16002

* QLOGIC QLE2670/QLE2672

- * FUJITSU ETERNUS DX100 S3
- * FUJITSU ETERNUS DX200 S3
- * FUJITSU ETERNUS DX500 S3
- * FUJITSU ETERNUS DX600 S3
- * FUJITSU ETERNUS DX8100 S3
- * FUJITSU ETERNUS DX8700 S3
- * FUJITSU ETERNUS DX8900 S3
- * FUJITSU ETERNUS DX200F
- * FUJITSU ETERNUS DX60 S3

Il supporto per DIX rimane una Anteprima di tecnologia per array di archiviazione e HBA.

T10 DIX ha bisogno di un database, o di altro software, in grado di generare e verificare i checksum su blocchi a disco. Nessun filesystem di Linux attualmente supportato possiede questa capacità.

Cache LVM

La cache in LVM è completamente supportata con l'introduzione di Red Hat Enterprise Linux 7.1. Questa funzione permette agli utenti di creare volumi logici con un dispositivo piccolo ma veloce, il quale si comporta come una cache per dispositivi più grandi e lenti. Consultare la pagina man di `lvmcache(7)` per informazioni su come creare i volumi logici della cache.

Di seguito sono riportate le restrizioni sull'utilizzo dei volumi logici della cache (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.

* cache LV sub-LV (le LV d'origine, le LV dei metadati e le LV dei dati) possono essere solo lineari, segmentate o RAID.

* 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.

Nuova politica della cache LVM/DM

Scritta una nuova politica dm-cache `smq` per ridurre il consumo di memoria e migliorare le prestazioni nella maggior parte delle situazioni. Questa è ora la politica predefinita per nuovi volumi logici della cache LVM. Gli utenti che preferiscono usare la politica `mq` precedente, possono farlo utilizzando l'argomento `–cachepolicy` durante la creazione del volume logico della cache.

LVM systemID

Ora i gruppi di volumi LVM possono avere un proprietario. Il proprietario è il system ID di un host. Solo l'host con un system ID dato può utilizzare il VG. Questa impostazione è idonea per i gruppi di volumi che risiedono sui dispositivi condivisi, visibili agli host multipli, i quali potrebbero non essere protetti da un uso simultaneo di host multipli. I gruppi di volumi LVM sui dispositivi condivisi con un system ID, sono posseduti solo da un host e protetti nei confronti di altri host.

Capitolo 13. Gestione delle sottoscrizioni e sistemi

PowerTOP ora rispetta i nomi dei file definiti dall'utente

In precedenza i nomi dei file PowerTOP venivano generati in modo non chiaro e non documentato. Con questo aggiornamento l'implementazione è stata migliorata, ora i nomi dei file generati rispettano i nomi richiesti dall'utente. Ciò viene applicato sia nei riporti HTML che in quelli CSV.

Modificati i comandi `yum-config-manager`

In precedenza l'esecuzione del comando `yum-config-manager --disable` disabilitava tutti i repository configurati, al contrario `yum-config-manager --enable` non ne abilitava alcuno. Questo tipo di comportamento è stato corretto. I comandi `--disable` e `--enable` ora hanno bisogno di `*` all'interno della sintassi; `yum-config-manager --enable *` è in grado di abilitare i repository. L'esecuzione del comando senza l'aggiunta di `*` genererà un messaggio il quale indicherà all'utente di eseguire `yum-config-manager --disable *` o `yum-config-manager --enable *`, per abilitare o disabilitare i repository.

Nuovo plug-in `search-disabled-repos` per yum

Il plug-in `search-disabled-repos` di yum è stato aggiunto ai pacchetti del `subscription-manager`. Questo plug-in permette agli utenti di completare le operazioni di yum che falliscono a causa della dipendenza del repository sorgente per un repository disabilitato. Se `search-disabled-repos` è installato nel modo appena descritto, yum visualizza le informazioni per abilitare temporaneamente i repository disabilitati, andando alla ricerca delle dipendenze mancanti. Dopo aver eseguito le modifiche necessarie al file `/etc/yum/pluginconf.d/search-disabled-repos.conf`, sarà possibile ripristinare l'operazione yum utilizzando i repository disabilitati come se fossero repository abilitati.

Capitolo 14. Virtualizzazione

I bus root PCI supplementari sono ora supportati usando i dispositivi bridge PCI expander

Diversamente dai bridge PCI-PCI, un bus presente su un bridge PCI expander può essere associato con un nodo NUMA, permettendo così al sistema operativo del guest di riconoscere la vicinanza di un dispositivo ad una RAM o CPU. Con questo aggiornamento i dispositivi assegnati possono essere associati al nodo NUMA corrispondente, migliorando così le prestazioni.

qemu-kvm supporta gli eventi per il tracciamento dell'arresto della macchina virtuale

È stato aggiunto il supporto per gli eventi qemu-kvm durante il processo di spegnimento del sistema della macchina virtuale. L'utente ora potrà ottenere informazioni dettagliate sulle richieste di arresto del sistema guest emesse dal comando `virsh shutdown`, o da `virt-manager`. Questo aggiornamento fornisce all'utente maggiori capacità per isolare e risolvere i problemi del guest KVM durante il processo di spegnimento.

Intel MPX esposto guest

Ora qemu-kvm permette alla funzione Memory Protection Extensions (MPX) di Intel di essere esposta al guest. Sui sistemi host Intel 64 che supportano MPX, l'utente potrà utilizzare un insieme di estensioni che forniscono un supporto hardware per protezioni associate sui riferimenti del puntatore.

Estrazione dump della memoria del guest dal qemu-kvm core

Lo script `dump-guest-memory.py` è stato introdotto in QEMU. Il suddetto script permette un'analisi del dump della memoria del guest da un qemu-kvm core, nel caso in cui il kernel del guest fallisce. Per maggiori informazioni consultare il testo d'aiuto usando il comando `help dump-guest-memory`.

virt-v2v è completamente supportato

Con Red Hat Enterprise Linux 7.2 lo strumento `virt-v2v` è completamente supportato. Questo strumento converte le macchine virtuali in esecuzione su hypervisor esterni per un loro utilizzo su KVM. Attualmente `virt-v2v` può convertire i guest Red Hat Enterprise Linux e Windows in esecuzione su Red Hat Enterprise Linux 5 Xen e VMware vCenter.

Virtualizzazione su sistemi IBM Power

Red Hat Enterprise Linux with KVM è supportato su sistemi AMD64 e Intel 64, ma non su sistemi IBM Power. Red Hat attualmente fornisce una soluzione basata su POWER8 con Red Hat Enterprise Virtualization per sistemi IBM Power.

Per maggiori informazioni sul supporto delle versioni e sulle procedure d'installazione consultare l'articolo della Knowledge Base: <https://access.redhat.com/articles/1247773>

Supporto VirtIO-1

I driver Virtio sono stati aggiornati al Kernel 4.1 per il supporto del dispositivo VirtIO 1.0

Supporto Hyper-V TRIM

Ora è possibile usare il Thin Provisioned Hyper-V virtual hard disk (VHDX). Questo aggiornamento permette di avere un supporto per la riduzione dei file VHDX sottostanti delle macchine virtuali Microsoft Hyper-V, alla dimensione effettiva utilizzata.

Capitolo 15. 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 database e altri tool distribuiti con Red Hat Software Collection non sono intesi come sostituti dei tool del sistema predefinito con Red Hat Enterprise Linux, e non vengono utilizzati come tool preferiti. Red Hat Software Collection utilizza un meccanismo alternativo basato sull'utilità **sc1**, per fornire un insieme parallelo di pacchetti. Questo set permette di utilizzare versioni alternative sul Red Hat Enterprise Linux. Utilizzando **sc1** gli utenti sono in grado di scegliere la versione del pacchetto desiderata.

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.



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](#).

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.

Parte II. Anteprima di tecnologia

Questa sezione fornisce un sommario sulle Anteprime di tecnologia introdotte o aggiornate in Red Hat Enterprise Linux 7.2.

Per maggiori informazioni sulle Anteprime di tecnologia di Red Hat consultare <https://access.redhat.com/support/offerings/techpreview/>.

Capitolo 16. Autenticazione

Utilizzo provider sudo AD e LDAP

Il provider Active Directory (AD) è un backend usato per la connessione con un server Active Directory. Con Red Hat Enterprise Linux 7.2, l'utilizzo del provider sudo AD insieme con il provider LDAP è supportato come Antepima di tecnologia. Per abilitare il provider sudo AD, aggiungere **sudo_provider=ad** nella sezione [domain] del file **sssd.conf**.

Capitolo 17. File System

OverlayFS

OverlayFS è un tipo di file system d'unione che permette di sovrapporre (**overl**ay) i diversi filesystem. Le modifiche vengono registrate sul filesystem superiore mentre quello inferiore resta inalterato. Così facendo è possibile per utenti multipli condividere una immagine del file-system, come ad esempio un container o un DVD-ROM, dove l'immagine di base è su un dispositivo di sola lettura. Consultare la documentazione del file del kernel `/filesystems/overlayfs.txt` per ulteriori informazioni.

OverlayFS resta una Anteprima di tecnologia in Red Hat Enterprise Linux 7.2. Per questo motivo verrà visualizzato un messaggio d'avvertimento se si attiva questa funzione.

È disponibile un supporto completo per OverlayFS se utilizzato in presenza delle seguenti limitazioni:

- * OverlayFS è supportato solo se utilizzato come driver Docker grafico. Il suo utilizzo è supportato solo per un contenuto COW del container, non per storage persistenti. Per il supporto, posizionare lo storage persistente su volumi non-OverlayFS. È possibile usare solo la configurazione del Docker predefinita; e cioè, un livello di overlay, uno di lowerdir, ed entrambi i livelli, superiore e inferiore, sono presenti sullo stesso file system.
- * Solo XFS è attualmente supportato per un suo utilizzo come livello inferiore del file system.
- * Sulla macchina virtuale SELinux deve essere abilitato e in modalità enforcing, ma deve essere disabilitato durante la separazione del container; e cioè, `/etc/sysconfig/docker` non deve contenere `--selinux-enabled`. Il supporto SELinux per OverlayFS è in fase di sviluppo e si prevede una sua implementazione con release future.
- * Il comportamento dello spazio utente e di OverlayFS kernel ABI non è considerato stabile e potrà subire modifiche in futuro.

Da notare che OverlayFS fornisce un insieme limitato di standard POSIX. Eseguire il test dell'applicazione prima di implementarla con OverlayFS.

Attualmente sono presenti con Red Hat Enterprise Linux 7.2 alcuni problemi associati a OverlayFS. Per informazioni consultare **Non-standard behavior** in `Documentation/filesystems/overlayfs.txt`.

Supporto per i client NFSv4 con una disposizione del file flexible

Red Hat Enterprise Linux 7.2 rende disponibile un supporto per la disposizione del file flexible su client NFSv4. Questa tecnologia permette l'uso di funzioni avanzate come la mobilità dei file senza interruzione e il mirroring del client, migliorando così l'uso nei database, virtualizzazione e in presenza di dati molto grandi.

Consultare <https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/> per informazioni dettagliate sulla disposizione del file flessibile NFS.

NFS over RDMA

Il servizio NFSoverRDMA è disponibile come Anteprima di tecnologia per Red Hat Enterprise Linux 7.2. Ciò rende il modulo `svcrdma` disponibile a utenti che desiderano usare il Remote Direct Memory Access (RDMA) con il server NFS di Red Hat Enterprise Linux 7.

Filesystem Btrfs

Il file system Btrfs (B-Tree) è supportato come Anteprima di tecnologia in Red Hat Enterprise Linux 7.2, 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.

Capitolo 18. Abilitazione hardware

Supporto schede OSA-Express5s in qethqoat

È stato aggiunto al tool qethqoat il supporto per le schede OSA-Express5s, parte del pacchetto s390utils. Questo miglioramento estende le capacità di servizio della rete e le impostazioni per le schede OSA-Express5s, ed è incluso come Anteprima di tecnologia con Red Hat Enterprise Linux 7.2 su IBM System z.

Strumentazione di runtime per IBM System z

Il supporto per la funzione di strumentazione del runtime è disponibile come Anteprima di tecnologia in Red Hat Enterprise Linux 7.2 su IBM System z. La strumentazione di runtime permette un'analisi avanzata e l'esecuzione di un certo numero di applicazioni spazio-utente, disponibili con il sistema IBM zEnterprise EC12.

Adattatori LSI Syncro CS HA-DAS

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 precedentemente 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 7.2, 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>.

Capitolo 19. Kernel

Supporto CPU multiple in kdump su sistemi Intel 64 e AMD64

Sui sistemi AMD64 e Intel 64, il meccanismo di kernel crash dump **kdump** può essere avviato con più di una CPU abilitata. Così facendo è possibile risolvere alcuni problemi presenti su sistemi con una dimensione di memoria molto grande, dove a causa di output e input elevati durante il processo di creazione di un kernel crash dump, Linux potrà non essere in grado di assegnare le interruzioni per i dispositivi con una sola CPU abilitata ("maxcpus=1" o **nr_cpus=1**).

Per avere CPU multiple in un crash kernel, inserire **nr_cpus=X** (dove **X** è il numero di processori) e **disable_cpu_apicid=0** nella linea di comando del kernel.

Strumento criu

Red Hat Enterprise Linux 7.2 introduce **criu** come Anteprima di tecnologia. Questo strumento implementa **Checkpoint/Restore in User-space**, utilizzabile per arrestare una applicazione in esecuzione e archivarla come insieme di file. Successivamente sarà possibile ripristinare l'uso dell'applicazione.

criu dipende dai **Protocol Buffers**, un meccanismo di estensione con linguaggio e piattaforma neutrali per la serializzazione di dati strutturati. I pacchetti *protobuf* e *protobuf-c*, i quali forniscono questa dipendenza, sono stati aggiunti a Red Hat Enterprise Linux 7.2 come Anteprima di tecnologia.

Spazio nome utente

Questa funzione fornisce un livello di sicurezza aggiuntivo per i server in esecuzione su container di Linux, tramite l'implementazione di un migliore isolamento tra l'host e i container. Gli amministratori di un container non saranno più in grado di eseguire operazioni amministrative sull'host, aumentandone così la sicurezza.

LPAR Watchdog per IBM System z

Un driver watchdog migliorato per IBM System z è ora disponibile come Anteprima di tecnologia. Il suddetto driver supporta le Linux logical partitions (LPAR) e i guest di Linux in z/VM hypervisor, fornisce altresì capacità di dump e riavvio automatici se un sistema Linux è inattivo

Aggiornamenti del kernel automatici con kpatch

L'utilità kpatch permette agli utenti di gestire un insieme di patch del kernel binario utilizzabili per una loro implementazione dinamica nei confronti del kernel, senza dover eseguire il riavvio. kpatch è supportato come Anteprima di tecnologia e solo per architetture AMD64 e Intel 64.

i40evf gestisce operazioni di reset molto grandi

Il tipo di reset più comune presente con una Virtual Function (VF) è una Physical Function (PF) la quale provoca un reset VF per ogni VF. Tuttavia per operazioni più grandi come ad esempio i reset dei Core o EMP, in precedenza durante il ripristino del dispositivo, la VF non otteneva lo stesso VSI, per questo motivo VF non era in grado di eseguire il reset poiché richiedeva le risorse dal VSI originale. Come Anteprima di tecnologia questo aggiornamento aggiunge uno stato supplementare alla macchina dello stato della coda amministrativa. Così facendo il driver è in grado di richiedere le informazioni sulla sicurezza durante l'esecuzione. Durante operazioni di reset questa operazione viene definita nel campo `aq_required`, e le informazioni relative alla configurazione possono essere recuperate prima di riattivare il driver.

Capitolo 20. Networking

Aggiornato il driver Intel ethernet server adapter X710/XL710

I driver i40e e i40evf sono stati aggiornati alla versione 1.3.4-k. I suddetti driver sono inclusi come Anteprima di tecnologia in Red Hat Enterprise Linux 7.2.

Output ethtool accurato

Le capacità d'interrogazione di rete dell'utilità ethtool sono state migliorate nell'Anteprima di tecnologia per Red Hat Enterprise Linux 7.2 su IBM System z. Se utilizzate un hardware compatibile con le suddette interrogazioni, ethtool fornisce opzioni di monitoraggio migliorate e visualizza con più accuratezza i valori e le impostazioni della scheda di rete.

Driver Cisco usNIC

I server Cisco Unified Communication Manager (UCM) dispongono di una funzione opzionale in grado di fornire un Cisco proprietary User Space Network Interface Controller (usNIC) che permette di eseguire operazioni simili al Remote Direct Memory Access (RDMA), con applicazioni per lo spazio utente. Il driver libusnic_verbs, supportato come Anteprima di tecnologia, rende possibile l'uso di dispositivi usNIC tramite una programmazione InfiniBand RDMA standard basata sull'API Verbs.

Driver kernel Cisco VIC

Il driver del kernel Cisco VIC Infiniband, supportato come Anteprima di tecnologia, permette l'uso di semantiche simili al Remote Directory Memory Access (RDMA) su architetture Cisco proprietarie.

Trusted Network Connect

Trusted Network Connect, supportato come Anteprima di Tecnologia, 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.

Capitolo 21. Storage

Programmazione Multi-queue I/O per SCSI

Red Hat Enterprise Linux 7.2 include un nuovo meccanismo di programmazione multiple-queue I/O per dispositivi a blocchi conosciuti come blk-mq. Il pacchetto `scsi-mq` permette al sottosistema Small Computer System Interface (SCSI) di utilizzare questo nuovo meccanismo. Questa funzione risulta essere una Anteprima di tecnologia e non è abilitata per impostazione predefinita. Per poterla abilitare aggiungere `scsi_mod.use_blk_mq=Y` alla riga di comando del kernel.

Infrastruttura di blocco LVM migliorata

`lvmlockd` è l'infrastruttura di blocco di prossima generazione per LVM. Essa permette a LVM di gestire in modo sicuro uno storage condiviso da host multipli, utilizzando gestori del blocco `dlm` o `sanlock`. `sanlock` permette a `lvmlockd` di coordinare gli host attraverso un blocco basato sullo storage, senza dover utilizzare una infrastruttura cluster completa. Per maggiori informazioni consultare la pagina man di `lvmlockd(8)`.

Plug-in Targetd dell'API libStorageMgmt

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 l'interfaccia a linea di comando inclusa.

Da ricordare che il plug-in Targetd non è completamente supportato e rimane una Anteprima di tecnologia.

DIF/DIX

DIF/DIX è una caratteristica nuova per lo standard SCSI, è completamente supportata con Red Hat Enterprise Linux 7.2 per HBA e gli array di storage specificati nel capitolo Funzioni, ma resta ancora una Anteprima di tecnologia per tutti gli altri HBA e array di storage.

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 di 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.

dm-era device-mapper target

Red Hat Enterprise Linux 7.1 introduce il dm-era device-mapper target 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.

Capitolo 22. Virtualizzazione

Virtualizzazione nidificata

Come Anteprima di tecnologia Red Hat Enterprise Linux 7.2 offre una funzione di virtualizzazione nidificata. Questa nuova implementazione permette di utilizzare i guest KVM-QEMU come host, permettendo così all'utente di creare guest all'interno di guest.

Lo strumento virt-p2v

Red Hat Enterprise Linux 7.2 rende disponibile virt-p2v come Anteprima di tecnologia. Virt-p2v (fisico a virtuale) è un CD-ROM, ISO o immagine PXE che l'utente può avviare su una macchina fisica, e converte la macchina fisica in una virtuale in grado di essere eseguita su KVM.

Supporto USB 3.0 per guest KVM

L'emulazione USB 3.0 host adapter (xHCI) per guest KVM è ancora una Anteprima di tecnologia in Red Hat Enterprise Linux 7.2.

Parte III. Driver del dispositivo

Questo capitolo fornisce un elenco completo di tutti i driver del dispositivo aggiornati in Red Hat Enterprise Linux 7.2.

Capitolo 23. Aggiornamenti driver di archiviazione

- ✦ Il driver hpsa è stato aggiornato alla versione 3.4.4-1-RH4.
- ✦ Aggiornato il driver qla2xxx alla versione 8.07.00.18.07.2-k.
- ✦ Il driver lpfc è stato aggiornato alla versione 10.7.0.1.
- ✦ Aggiornato il driver megaraid_sas alla versione 06.807.10.00.
- ✦ Aggiornato il driver fnic alla versione 1.6.0.17
- ✦ Aggiornato il driver mpt2sas alla versione 20.100.00.00.
- ✦ Aggiornato il driver mpt3sas alla versione 9.100.00.00.
- ✦ Aggiornato il driver Emulex be2iscsi alla versione 10.6.0.0r.
- ✦ Aggiornato il driver aacraid alla versione 1.2.
- ✦ Aggiornato il driver bnx2i alla versione 2.7.10.1.
- ✦ Aggiornato il driver bnx2fc alla versione 2.4.2.

Capitolo 24. Aggiornamenti driver di rete

- Aggiornato il driver tg3 alla versione 3.137.
- Il driver e1000 è stato aggiornato alla versione 7.3.21-k8-NAPI, ora è disponibile il supporto per il ritardo di aggiornamento txtd quando si utilizza la variabile booleana xmit_more.
- Aggiornato il driver e1000e alla versione 2.3.2-k.
- Aggiornato il driver igb alla versione 5.2.15-k.
- Aggiornato il driver igbvf alla versione 2.0.2-k.
- Aggiornato il driver ixgbevfv alla versione 2.12.1-k.
- Aggiornato il driver ixgbe alla versione 4.0.1-k.
- Il firmware ed il driver bna sono stati aggiornati alla versione 3.2.23.0r.
- Aggiornato il driver bnx2 alla versione 2.4.2.
- Aggiornato il driver CNIC alla versione 2.5.21.
- Aggiornato il driver bnx2x alla versione 1.710.51-0, ora è disponibile il supporto qllogic NPAR per gli adattatori qllogic-nx2.
- Aggiornato il driver be2net alla versione 10.6.0.2.
- Il driver bna è stato aggiornato alla versione 3.2.23.0r.
- Aggiornato il driver qlcnic alla versione 5.3.62.
- Il driver qlge è stato aggiornato alla versione 1.00.00.34, la nuova versione corregge una condizione di corsa critica tra la registrazione e l'annullamento della registrazione di una New API (NAPI). Questo comportamento causava un arresto inaspettato del sistema se l'utente modificava determinati parametri mentre la Network Interface Card (NIC) era impostata su "down".
- Aggiornato il driver r8169 alla versione 2.3LK-NAPI.
- I driver i40e e i40evf sono stati aggiornati alla versione 1.3.4-k.
- Aggiornato il driver netxen_nic alla versione 4.0.82.
- Aggiornato il driver sfc all'ultimissima versione upstream.
- Questo aggiornamento rende disponibile il driver fm10k con una versione 0.15.2-k.
- Questo aggiornamento rende disponibile il supporto VTI6 include le capacità netns.
- Aggiornato il driver bonding alla versione 3.7.1.
- Aggiornato il driver iwlwifi all'ultimissima versione upstream.
- Aggiornato il driver vxlan alla versione 0.1.

Capitolo 25. Aggiornati i driver grafici e quelli generici

- Il driver HDA è stato aggiornato all'ultimissima versione upstream per poter utilizzare il nuovo metodo jack kctl.
- Aggiornato il driver HPI alla versione 4.14.
- Il driver Realtek HD-audio codec è stato aggiornato e ora include gli ultimissimi codici init EAPD.
- Il driver IPMI è stato aggiornato e ora sostituisce timespec con timespec64.
- Aggiornato il driver i915 in modo da includere una nuova versione del driver delle estensioni video ACPI in Red Hat Enterprise Linux 7.2.
- Aggiornato il driver ACPI Fan alla versione 0.25.
- Aggiornato il driver NVM-Express alla versione 3.19.
- Aggiornato il driver rtsx alla versione 4.0 per il supporto dei chip rtl8402, rts524A, rts525A.
- Aggiornato il driver del dispositivo Generic WorkQueue Engine all'ultimissima versione upstream.
- Aggiornato il driver PCI alla versione 3.16.
- Il modulo del kernel EDAC è stato aggiornato e rende ora disponibile il supporto per i processori Xeon v4 di Intel
- Aggiornato il driver pstate, ora è disponibile il supporto dei processori 6th Generation Intel Core.
- Aggiornato il driver intel_idle, ora è disponibile il supporto dei processori 6th Generation Intel Core.

Parte IV. Problematiche conosciute

Questa sezione documenta le problematiche conosciute presenti in Red Hat Enterprise Linux 7.2.

Capitolo 26. Compiler e Tool

Bug multipli durante l'avvio da uno SAN usando FCoE

Si sono verificati bug multipli a causa dell'implementazione corrente durante l'avvio da uno Storage Area Network (SAN) utilizzando Fibre Channel over Ethernet (FCoE). Red Hat desidera risolvere questi errori tramite una versione futura di Red Hat Enterprise Linux 7. Per un elenco di bug interessati, e per la loro risoluzione (se disponibile), contattare un rappresentante del supporto di Red Hat.

Valgrind non è in grado di eseguire programmi compilati utilizzando una versione precedente di Open MPI

Red Hat Enterprise Linux 7.2 supporta solo Open MPI application binary interface (ABI) con versione 1.10, la quale è incompatibile con la versione 1.6 di Open MPI ABI. Ne consegue che i programmi compilati usando versioni precedenti di Open MPI, non possono essere eseguiti con Valgrind disponibile con Red Hat Enterprise Linux 7.2. Per risolvere questo problema usare la versione presente con il Red Hat Developer Toolset per programmi associati con Open MPI versione 1.6.

Capitolo 27. Desktop

Dipendenze incomplete del pacchetto `pygobject3` impediscono l'aggiornamento dal Red Hat Enterprise Linux 7.1

In Red Hat Enterprise Linux 7.2 il pacchetto `pygobject3-devel.i686` a 32-bit è stato rimosso e sostituito con una versione multilib. Se siete in possesso di una versione a 32-bit del pacchetto installato su un sistema Red Hat Enterprise Linux 7.1, allora potrete visualizzare un errore `yum` durante l'aggiornamento a Red Hat Enterprise Linux 7.2.

Per risolvere questo problema usare `yum remove pygobject3-devel.i686` come utente `root` per rimuovere la versione a 32-bit del pacchetto prima di aggiornare il sistema.

Capitolo 28. Aggiornamenti generali

I nuovi nomi dei dispositivi possono causare una interruzione della connessione di rete

In precedenza l'assegnazione di nomi stabili per l'interfaccia di rete dei dispositivi virtio era una operazione impossibile da eseguire, poichè l'ordine di enumerazione dei dispositivi era imprevedibile. Con questa correzione è presente solo un dispositivo PCI genitore per virtio bus, così facendo i dispositivi di rete virtio ora possono avere dei nomi persistenti nelle macchine virtuali (come riportato in <http://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>).

Da notare che dopo l'aggiornamento di systemd e il riavvio della macchina virtuale, la quale in precedenza presentava i nomi dell'interfaccia di uno spazio dei nomi del kernel (eth0, eth1,...), i nuovi nomi del dispositivo vengono assegnati al riavvio successivo. Questo comportamento può causare l'interruzione della connessione di rete per una macchina virtuale.

Capitolo 29. Installazione e avvio

L'installazione in modalità testo non si arresta più inaspettatamente durante la configurazione di rete

In precedenza nella schermata di Configurazione di rete con l'installer in modalità di testo interattiva, l'uso dello spazio durante l'inserimento dei server dei nomi causava un arresto inaspettato dell'installer.

Anaconda ora gestisce correttamente gli spazi presenti nelle definizioni del server dei nomi in modalità testo, e l'installer non si arresterà più inaspettatamente se lo spazio viene usato per separare gli indirizzi.

Possibile messaggio d'errore di NetworkManager durante l'installazione

Durante l'installazione è possibile visualizzare il seguente messaggio d'errore:

```
ERR NetworkManager: <error> [devices/nm-device.c:2590] activation_source_schedule(): (eth0): activation stage already scheduled
```

Per questo bug nessuna soluzione è attualmente disponibile.

L'installazione di Atomic Host offre cryptsetup anche se non è disponibile.

Durante l'installazione di Red Hat Enterprise Linux 7 Atomic Host, l'installer offre l'opzione di cifrare il partizionamento usando **cryptsetup** nella schermata di Partizionamento manuale, in modo simile al processo offerto durante l'installazione di Red Hat Enterprise Linux 7.2.

Tuttavia le partizioni cifrate non sono supportate sull'Atomic Host. Se cifrate qualsiasi partizione durante l'installazione, non sarete in grado di sbloccarle in un secondo momento.

Per risolvere questo problema non cifrate le partizioni o i volumi logici durante l'installazione di Red Hat Enterprise Linux Atomic Host, anche se l'installer presenta questa opzione.

L'installer può solo aggiungere uno storage avanzato durante il primo inserimento dello spoke di storage.

Durante una installazione interattiva usando l'interfaccia grafica di Anaconda, l'aggiunta dello storage avanzato (iSCSI, zFCP, FCoE) alla selezione del disco non funziona correttamente se in precedenza è stato inserito lo spoke di storage. Per risolvere questo problema assicuratevi che la rete, se necessario, sia attiva, successivamente inserire lo spoke di storage e tutti i dispositivi di storage avanzati.

Capitolo 30. Kernel

Impossibile modificare la dimensione di alcuni filesystem ext4

A causa di un bug nel codice ext4, attualmente non è possibile modificare la dimensione dei filesystem ext4 con dimensione del blocco di 1 kilobyte e più piccoli di 32 megabyte.

Perdita di connessione ripetuta con target iSCSI abilitati-iSER.

Quando si utilizza il server come target iSCSI abilitato-iSER si verificano numerose perdite di connessione. In questa situazione il target non risponde e il kernel risulta inattivo. Per risolvere questo problema minimizzare le perdite del collegamento iSER o ripristinare la modalità iSCSI non-iSER.

Il comando I/O invoca SCSI mid-layer fino a quando il sistema viene arrestato

Quando un array di storage ritorna uno stato CHECK CONDITION, e i dati di rilevamento non sono validi, il codice Small Computer Systems Interface (SCSI) mid-layer cercherà di eseguire nuovamente l'operazione I/O. Se le operazioni I/O seguenti ricevono lo stesso risultato, SCSI proverà ad eseguire questa operazione all'infinito. Per questo bug non è attualmente disponibile alcuna soluzione.

Il certificato della chiave pubblica di Red Hat Beta deve essere caricato manualmente

L'amministratore di sistema potrà utilizzare il meccanismo machine owner key (MOK) per caricare il certificato della chiave pubblica di Red Hat Beta, necessario per autenticare il kernel incluso nella release di Red Hat Enterprise Linux Beta. La registrazione della chiave pubblica di Red Hat Certificate Authority (CA) Beta si effettua solo una volta per qualsiasi sistema usato per eseguire Red Hat Enterprise Linux 7.2 Beta con UEFI Secure Boot abilitata.

1. Disabilitare UEFI Secure Boot e installare Red Hat Enterprise Linux 7.2 Beta.
2. Installare il pacchetto kernel-doc se non è stato già installato. Questo pacchetto rende disponibile un file del certificato che contiene la chiave di Red Hat CA public Beta nel file: `/usr/share/doc/kernel-keys/<kernel-ver>/kernel-signing-ca.cer`, dove `<kernel-ver>` è la stringa della versione del kernel senza il suffisso dell'architettura della piattaforma, per esempio, `3.10.0-314.el7`.
3. Richiedere manualmente la registrazione della chiave pubblica all'elenco della Machine Owner Key (MOK) sul sistema che utilizza l'utilità `mokutil`. Eseguire il seguente comando come utente root:

```
mokutil --import /usr/share/doc/kernel-keys/<kernel-ver>/kernel-signing-ca.cer
```

Per eseguire la richiesta di registrazione sarà necessario fornire una password.

4. All'avvio successivo del sistema sarà richiesto all'utente di completare la registrazione della richiesta MOK. Continuare con il processo e fornire la password usata per `mokutil` durante la fase 3.
5. Dopo il completamento della registrazione MOK il sistema verrà resettato e riavviato. È possibile riabilitare UEFI Secure Boot durante il riavvio oppure durante i processi d'avvio del sistema successivi.

Capitolo 31. Networking

Politica di timeout non abilitata con il kernel di Red Hat Enterprise Linux 7.2

Il comando `nfct timeout` non è supportato in Red Hat Enterprise Linux 7.2. Per ovviare a questa limitazione usare i valori di timeout globali disponibili su `/proc/sys/net/netfilter/nf_conntrack_*_timeout_*` per impostarne uno.

Capitolo 32. Gestione delle sottoscrizioni e sistemi

Registrazione incompleta in presenza di un errore

Durante la registrazione di un sistema utilizzando una GUI di Subscription Manager se il processo fallisce, la finestra principale non potrà essere chiusa quando l'utente seleziona **OK** nella finestra di dialogo dell'errore. In questo modo la finestra di registrazione principale veniva lasciata aperta e il processo non poteva essere completato con successo. Questo problema si verifica per esempio quando un utente fornisce credenziali non valide o se utilizza auto-attach per la registrazione. Per risolvere questo problema selezionare il pulsante **Cancella** nella finestra di registrazione principale se in presenza di un errore.

Pulsante **Indietro (Back)** inattivo nel componente aggiuntivo di Subscription Manager per l'utilità Initial Setup

Il pulsante **Indietro (Back)** del primo pannello del componente iniziale di Subscription Manager per l'utilità Initial Setup non funziona. Per correggere questo problema selezionare **Fatto (Done)** nella parte alta di Initial Setup e uscire dal processo di registrazione.

Capitolo 33. Virtualizzazione

Navigazione GRUB 2 problematica con KVM

Durante l'uso di una console seriale con KVM, se l'utente preme e mantiene premuto un tasto freccetta per un periodo di tempo esteso durante la navigazione del menu di GRUB 2, si avrà un comportamento irregolare. Per risolvere questo problema è consigliato non premere il tasto freccetta per un periodo di tempo esteso.

Il ridimensionamento dei dischi GUID Partition Table (GPT) sui guest Hyper-V, causa la generazione di alcuni errori della tabella.

Il manager Hyper-V supporta il ridimensionamento di un disco partizionato con GPT su un guest in presenza di spazio disponibile dopo l'ultima partizione. Così facendo l'utente sarà in grado di eliminare l'ultima sezione del disco non utilizzata. Tuttavia questa operazione rimuoverà l'intestazione GPT secondaria la quale può generare i messaggi d'errore quando il guest esamina la tabella di partizioni (per esempio con `parted(8)`). Questo rappresenta una limitazione di Hyper-V.

Per risolvere questo problema ripristinare manualmente l'intestazione GPT secondaria con il comando `e` di `gdisk(8)`, dopo aver ridimensionato il disco. Questo comportamento si verifica anche durante l'uso dell'opzione `Expand` di Hyper-V, ma può essere corretto solo con `parted(8)`.

Appendice A. Versione dei componenti

La suddetta appendice rappresenta un elenco di componenti e delle relative versioni nella release Red Hat Enterprise Linux 7.2

Tabella A.1. Versione dei componenti

| Componente | Versione |
|------------------------------|---|
| Kernel | 3.10.0-306.0.1 |
| Driver qla2xxx QLogic | 8.07.00.08.07.1-k1 |
| Driver QLogic qla4xxx | 5.04.00.04.07.01-k0 |
| Driver lpfc Emulex | 10.2.8021.1 |
| iSCSI initiator utils | <i>iscsi-initiator-utils-6.2.0.873-32</i> |
| DM-Multipath | <i>device-mapper-multipath-0.4.9-82</i> |
| LVM | <i>lvm2-2.02.128-1</i> |

Appendice B. Diario delle Revisioni

| | | |
|---|------------------------|--------------------------|
| Revisione 0.0-1.16.2 | Thu Oct 29 2015 | Francesco Valente |
| Translation Completed | | |
| Revisione 0.0-1.16.1 | Thu Oct 29 2015 | Francesco Valente |
| I file della traduzione sono sincronizzati con con le versioni 0.0-1.16 dei sorgenti XML | | |
| Revisione 0.0-1.16 | Mon Oct 12 2015 | Lenka Špačková |
| Aggiunte nuove funzioni e problematiche conosciute | | |
| Revisione 0.0-1.16 | Mon Oct 12 2015 | Lenka Špačková |
| Added several new features and known issues. | | |
| Revisione 0.0-1.15 | Thu Oct 8 2015 | Lenka Špačková |
| Aggiornate le problematiche conosciute e aggiunti nuovi elementi a questo capitolo. Aggiunte altre architetture e aggiornate le Anteprime di tecnologia. | | |
| Revisione 0.0-1.15 | Thu Oct 8 2015 | Lenka Špačková |
| Restructured Known Issues and added several items to this chapter. Added Architectures, updated Technology Previews. | | |
| Revisione 0.0-1.14 | Thu Oct 1 2015 | Lenka Špačková |
| Driver del dispositivo aggiornati, aggiunti diversi problemi conosciuti. | | |
| Revisione 0.0-1.14 | Thu Oct 1 2015 | Lenka Špačková |
| Updated Device Drivers, added several known issues. | | |
| Revisione 0.0-1.13 | Wed Sep 16 2015 | Lenka Špačková |
| Aggiunte diverse descrizioni delle funzioni e problemi conosciuti. | | |
| Revisione 0.0-1.13 | Wed Sep 16 2015 | Lenka Špačková |
| Added multiple feature descriptions and known issues. | | |
| Revisione 0.0-1.10 | Wed Sep 09 2015 | Laura Bailey |
| Aggiunti gli aggiornamenti del driver per 7.2 Beta. | | |
| Revisione 0.0-1.10 | Wed Sep 09 2015 | Laura Bailey |
| Added driver updates for 7.2 Beta. | | |
| Revisione 0.0-1.9 | Wed Sep 09 2015 | Laura Bailey |
| Aggiunte alcune problematiche conosciute relative all'Anteprima di tecnologia OverlayFS | | |
| Revisione 0.0-1.9 | Wed Sep 09 2015 | Laura Bailey |
| Added known issues related to OverlayFS Technology Preview. | | |
| Revisione 0.0-1.8 | Mon Sep 07 2015 | Laura Bailey |
| Modifica delle Note di rilascio per l'implementazione dei benefici, nuove funzioni, modifiche sui parametri de kernel, problemi conosciuti, aggiornamenti dei driver e Anteprime di tecnologia. | | |
| Revisione 0.0-1.8 | Mon Sep 07 2015 | Laura Bailey |

Rewriting release notes to be based on features and benefits document, kernel parameter changes, known issues, driver updates, and technology previews.

| | | |
|--------------------------|------------------------|---------------------|
| Revisione 0.0-1.7 | Fri Sep 04 2015 | Laura Bailey |
|--------------------------|------------------------|---------------------|

Aggiunti alle Note di rilascio gli elementi relativi all'Anteprima di tecnologia

| | | |
|--------------------------|------------------------|---------------------|
| Revisione 0.0-1.7 | Fri Sep 04 2015 | Laura Bailey |
|--------------------------|------------------------|---------------------|

Added technology preview items to release notes.

| | | |
|--------------------------|------------------------|---------------------|
| Revisione 0.0-1.4 | Mon Aug 31 2015 | Laura Bailey |
|--------------------------|------------------------|---------------------|

Versione Beta delle Note di rilascio per Red Hat Enterprise Linux 7.2.

| | | |
|--------------------------|------------------------|---------------------|
| Revisione 0.0-1.4 | Mon Aug 31 2015 | Laura Bailey |
|--------------------------|------------------------|---------------------|

Release of the Red Hat Enterprise Linux 7.2 Beta Release Notes.