Red Hat Enterprise Linux 6

6.4 Versionshinweise

Versionshinweise für Red Hat Enterprise Linux 6.4

Ausgabe 4

Last Updated: 2017-10-24

Red Hat Enterprise Linux 6 6.4 Versionshinweise

Versionshinweise für Red Hat Enterprise Linux 6.4
Ausgabe 4

Landmann
rlandmann@redhat.com

Rechtlicher Hinweis

Zusammenfassung

Die Versionshinweise liefern einen allgemeinen Überblick über die Verbesserungen und Erweiterungen, die in Red Hat Enterprise Linux 6.4 implementiert wurden. Eine detaillierte Dokumentation aller Änderungen dieser Red Hat Enterprise Linux 6.4 Release steht in den Technischen Hinweisen zur Verfügung.

Inhaltsverzeichnis

VORWORT

Red Hat Enterprise Linux Nebenversionen (Minor Releases) sind eine Sammlung individueller Verbesserungen, Sicherheits-Errata und Bugfix-Errata. Die *Red Hat Enterprise Linux 6.4 Versionshinweise* dokumentieren die wesentlichen Änderungen, die für diese Nebenversion des Red Hat Enterprise Linux 6 Betriebssystems und der darin enthaltenen Applikationen implementiert wurden. Detailliertere Informationen über Änderungen in dieser Nebenversion (d.h. behobene Fehler, hinzugefügte Verbesserungen und gefundene, bekannte Probleme) stehen Ihnen in den Technischen Hinweisen zur Verfügung. Die Technischen Hinweise enthalten zudem eine vollständige Liste aller derzeit verfügbaren Technologievorschauen samt der Pakete, die diese bereitstellen.

WICHTIG

Die Online *Red Hat Enterprise Linux 6.4 Versionshinweise*, hier verfügbar, sollten als definitive, aktuellste Version betrachtet werden. Kunden mit Fragen bezüglich der Release wird empfohlen, die Online-Versionen der *Versionshinweise* und *Technischen Hinweise* für Ihre Red Hat Enterprise Linux Version zu Rate zu ziehen.

Sollten Sie Informationen über den Red Hat Enterprise Linux Lebenszyklus benötigen, werfen Sie bitte einen Blick auf https://access.redhat.com/support/policy/updates/errata/.

KAPITEL 1. INSTALLATION

FCoE-Unterstützung in Kickstart-Datei

Falls Sie zur Installation von Red Hat Enterprise Linux 6.4 eine Kickstart-Datei verwenden, können Sie mit der neuen ***fcoe***-Kickstart-Option spezifizieren, welche Fibre Channel over Ethernet (FCoE) Geräte aktiviert werden sollen zusätzlich zu jenen, die von Enhanced Disk Drive (EDD) Diensten entdeckt wurden. Weitere Informationen finden Sie im Abschnitt *Kickstart-Optionen* im Red Hat Enterprise Linux 6 *Installationshandbuch*.

Installation über VLAN

In Red Hat Enterprise Linux 6.4 ermöglichen Ihnen die **vlanid=** Boot-Option und die **--vlanid=** Kickstart-Option das Festlegen einer virtuellen LAN-ID (802.1q-Tag) für bestimmte Netzwerkgeräte. Indem Sie eine dieser beiden Optionen spezifizieren, können Systeminstallationen über ein VLAN durchgeführt werden.

Konfiguration von Bonding

Die **bond** Boot-Option und die **--bondslaves** und **--bondopts** Kickstart-Optionen können nun dazu verwendet werden, um Bonding als Teil des Installationsvorgangs zu konfigurieren. Weitere Informationen über die Konfiguration von Bonding finden Sie in den folgenden Abschnitten des Red Hat Enterprise Linux 6 *Installationshandbuchs*: Abschnitt *Kickstart-Optionen* und Kapitel *Boot-Optionen*.

KAPITEL 2. KERNEL

Fibre-Channel-Protokoll: End-To-End Datenkonsistenzprüfung

Die Datenintegrität zwischen einem Host-Adapter und einem Speicherserver wurde in Red Hat Enterprise Linux 6.4 verbessert, indem der zFCP-spezifische Teil des erweiterten T10 DIF SCSI Standards für End-To-End (E2E) Datenkonsistenzprüfung implementiert wurde.

Flash-Express-Unterstützung für IBM System z

Storage-Class Memory (SCM) für IBM System z ist eine Klasse von Speichergeräten, die Eigenschaften von Festplattenspeicher und Arbeitsspeicher kombiniert. SCM für System z unterstützt nun Flash-Express-Speicher. Über Extended Asynchronous Data Mover (EADM) Unterkanäle kann auf SCM-Inkremente zugegriffen werden. Jedes Inkrement wird durch ein Blockgerät dargestellt. Dieses Feature verbessert die Paging-Rate und Zugriffsperformanz für temporären Speicher, beispielsweise für Data-Warehousing.

Open vSwitch Kernel-Modul

Red Hat Enterprise Linux 6.4 enthält das Open vSwitch Kernel-Modul, um Red Hats weitere Produktangebote zu ermöglichen. Open vSwitch wird nur in Verbindung mit solchen Produkten unterstützt, die die zugehörigen User-Space-Tools enthalten. Bitte beachten Sie, dass ohne diese erforderlichen User-Space-Tools Open vSwitch nicht funktionieren kann und nicht zur Verwendung aktiviert weren kann. Weitere Informationen finden Sie in dem folgenden Artikel der Wissensdatenbank: https://access.redhat.com/knowledge/articles/270223.

Vergleich von gebootetem System mit Speicherauszug eines Systems

Dieses Feature ermöglicht Ihnen den Vergleich eines gebooteten Systems mit dem Speicherauszug eines Systems, um effizient Änderungen zu analysieren, die möglicherweise durch eine Image-Migration verursacht wurden. Um einen Gast zu identifizieren, werden **`stsi`**- und **`stfle`**-Daten verwendet. Eine neue Funktion **`lgr_info_log()`** vergleicht die aktuellen Daten (***`lgr_info_cur`***) mit den zuletzt aufgezeichneten Daten (***`lgr_info_last`***).

Perf-Tool aktualisiert

Das **perf**-Tool wurde auf die Upstream-Version 3.6-rc7 aktualisiert, die zahlreiche Fehlerbehebungen und Verbesserungen implementiert. Nachfolgend sehen Sie eine Liste der nennenswerten Verbesserungen:

- Unterstützung für Kprobe-Ereignisse wurde hinzugefügt.
- Eine neue **perf**-Ereignis-Befehlszeilensyntax-Engine wurde integriert, die es ermöglicht, geschweifte Klammern (**`{`** und **`}`**) zur Definition von Ereignisgruppen zu verwenden, zum Beispiel: **`{cycles,cache-misses}`**.
- Der **perf**-annotierte Browser wurde erweitert, um die Navigation per ASM-Aufrufen und -Sprüngen zu erlauben.
- Das **perf**-Tool wurde aktualisiert, um eine Ansicht pro Benutzer mit der neuen **`--uid`**-Befehlszeilenoption zu liefern. Mithilfe dieser Option kann **perf** Aufgaben nur für den angegebenen Benutzer anzeigen.
- Das **perf**-Tool bietet nun eine größere Vielzahl automatisierter Tests.

Unterstützung für Uncore PMU

Der in Red Hat Enterprise Linux 6.4 enthaltene Kernel fügt "uncore" Performance Monitoring Unit (PMU) Unterstützung zum perf-Ereignisuntersystem für die Intel Xeon-Prozessor X55xx und die Intel Xeon-Prozessor X56xx Prozessorfamilien hinzu. "uncore" bezieht sich auf Untersysteme im physischen

Prozessorpaket, die von mehreren Prozessorkernen, z.B. dem L3-Cache, gemeinsam verwendet werden. Mit uncore-PMU-Unterstützung können Performancedaten einfach auf Paketebene gesammelt werden.

PMU-Ereignisverarbeitung wurde ebenfalls aktiviert, um das Debugging via perf zu ermöglichen.

Verringerter `memcg`-Speicher-Overhead

Speicherkontrollgruppen pflegen ihre eigenen "Least Recently Used" (LRU) Listen, um beispielsweise Speicher wieder freizugeben. Diese Liste lag über der globalen LRU-Liste pro Zone. In Red Hat Enterprise Linux 6.4 wurde der Speicher-Overhead für **`memcg`** verringert, indem die globale LRU-Liste pro Zone deaktiviert wurde und deren Benutzer nun mit den cgroup-Listen pro Speicher arbeiten.

Speicherfreigabe und -verdichtung

Der in Red Hat Enterprise Linux 6.4 enthaltene Kernel verwendet Speicherfreigabe und -verdichtung für höherrangige Anforderungen oder unter hoher Speicherauslastung.

Unterstützung für die Transactional Execution Facility und Runtime Instrumentation Facility

Die Unterstützung für die Transactional-Execution Facility (verfügbar mit IBM zEnterprise EC12) im Linux-Kernel hilft dabei, Software-Locking-Overhead zu vermeiden, der sich auf die Leistung auswirken kann, und bietet verbesserte Skalierbarkeit und Parallelismus für höheren Transaktionsdurchsatz. Unterstützung für die Runtime Instrumentation Facility (verfügbar mit IBM zEnterprise EC12) bietet einen verbesserten Mechanismus zum Profilieren von Programmcode für verbesserte Analyse und Optimierung von Code, der von der neuen IBM JVM generiert wurde.

Fail-Open-Modus

Red Hat Enterprise Linux 6.4 implementiert Unterstützung für einen neuen Fail-Open-Modus bei der Verwendung von Netfilters NFQUEUE-Ziel. Dieser Modus ermöglicht es Benutzern, vorübergehend die Untersuchung von Paketen zu deaktivieren und so die Verbindungsfähigkeit unter hoher Netzwerkauslastung aufrechtzuerhalten.

kdump und kexec Kernel-Dumping-Mechanismus für IBM System z vollständig unterstützt

In Red Hat Enterprise Linux 6.4 wurde der kdump/kexec Kernel-Dumping-Mechanismus für IBM System z Systeme als vollständig unterstütztes Feature aktiviert, zusätzlich zu den IBM System z Stand-Alone und Hypervisor Dumping-Mechanismen. Die Auto-Reserve-Schwelle ist auf 4 GB festgelegt; somit ist auf einem IBM System z System mit mehr als 4 GB Speicher der kdump/kexec-Mechanismus aktiviert.

Es muss ausreichender Speicher verfügbar sein, da kdump standardmäßig etwa 128 MB reserviert. Dies ist insbesondere dann wichtig, wenn ein Upgrade auf Red Hat Enterprise Linux 6.4 durchgeführt wird. Zudem muss ausreichender Festplattenplatz verfügbar sein, um im Falle eines Systemabsturzes den Crash-Dump zu speichern.

Sie können kdump mittels **`/etc/kdump.conf`**, **system-config-kdump** oder **firstboot** aktivieren bzw. deaktivieren.

TSC-Deadline-Unterstützung für KVM

TSC-Deadline-Timer ist ein neuer Modus im Local APIC (LAPIC) Timer, der einmalige Timer-Interrupts basierend auf der TSC Deadline generiert, anstelle des aktuellen APIC-Systemuhrintervalls. Er bietet präzisere Timer-Interrupts (unter 1 Tick), zum Vorteil des Betriebssystem-Schedulers. KVM stellt dieses Feature nun Gästen zur Verfügung.

Persistente Gerätebenennung

Dieses Feature speichert die Zuordnung von Gerätenamen (z.B. **`sda`**, **`sdb`** etc.) und persistente Gerätenamen (bereitgestellt durch **udev** in **`/dev/disk/by-*/`**) in Kernel-Meldungen. Dies ermöglicht

es Benutzern, ein Gerät anhand der Kernel-Meldungen zu identifizieren. Das Kernel-Protokoll **/dev/kmsg**, das mithilfe des **dmesg**-Befehls angezeigt werden kann, zeigt nun die Meldungen für die symbolischen Links, die **udev** für Kernel-Geräte erzeugt hat. Diese Meldungen werden im folgenden Format dargestellt:

```
udev-alias: <Geräte_Name> (<Symbolischer_Link> <Symbolischer Link> …)
```

Jedes beliebige Tool zur Protokollanalyse kann diese Meldungen anzeigen, die auch in **/var/log/messages** durch **syslog** gespeichert werden.

Neues linuxptp-Paket

Das linuxptp-Paket, das in Red Hat Enterprise Linux 6.4 als Technologievorschau enthalten ist, ist eine Implementierung des Precision Time Protocol (PTP) gemäß dem IEEE-Standard 1588 für Linux. Dabei wird ein doppeltes Entwicklungsziel verfolgt: die Entwicklung einer robusten Implementierung des Standards sowie der Einsatz der relevantesten und modernsten Programmierschnittstellen (APIs) des Linux-Kernels. Die Unterstützung von veralteten APIs und anderen Plattformen ist dagegen kein Entwicklungsziel.

Dokumentation für transparente Hugepages

Dokumentation für transparente Hugepages steht nun in der folgenden Datei zur Verfügung:

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

Status der Unterstützung von Dump-Zielen

In Red Hat Enterprise Linux 6.4 enthält die **/usr/share/doc/kexec-tools-2.0.0/kexec-kdump-howto.txt**-Datei eine umfassende Liste mit unterstützten, nicht unterstützten und unbekannten Dump-Zielen im Abschnitt »Dump Target support status«.

KAPITEL 3. GERÄTETREIBER

Speichertreiber

- Der Gerätetreiber für Direct Access Storage Devices (**DASD**) wurde aktualisiert, um Pfadkonfigurationsfehler zu entdecken, die nicht von der Hardware oder Microcode erkannt werden. Sobald diese Pfade entdeckt wurden, verwendet der Gerätetreiber sie nicht länger. Mit diesem Feature entdeckt der DASD-Gerätetreiber beispielsweise Pfade, die einem bestimmten Unterkanal zugeordnet sind, jedoch zu unterschiedlichen Speicherservern führen.

- Der **zfcp**-Gerätetreiber wurde aktualisiert und Datenstrukturen und Fehlerhandhabung hinzugefügt, um den erweiterten Modus der System z Fibre Channel Protocol (FCP) Adapterkarte zu unterstützen. In diesem Modus übergibt der Adapter Daten direkt vom Speicher in das SAN (Datenrouting), wenn Speicher auf der Adapterkarte von großen und langsamen I/O-Anfragen blockiert wird.

- Der **mtip32xx**-Treiber wurde aktualisiert, um Unterstützung für die neuesten PCIe SSD-Laufwerke hinzuzufügen.

- Der **lpfc**-Treiber für Emulex Fibre-Channel Host-Bus-Adapter wurde auf Version 8.3.5.82.1p aktualisiert.

- Der **qla2xxx**-Treiber für QLogic Fibre-Channel-HBAs wurde auf Version 8.04.00.04.06.4-k aktualisiert und bietet nun Unterstützung für QLogics 83XX Converged Network Adapter (CNA), 16 GBps FC Unterstützung für QLogic-Adapter und neue Form Factor CNA für HP ProLiant Server.

- Der **qla4xxxx**-Treiber wurde auf Version v5.03.00.00.06.04-k0 aktualisiert, um ***change_queue_depth***-API-Unterstützung hinzuzufügen, eine Reihe von Fehlern zu beheben und verschiedene weitere Verbesserungen einzubringen.

- Die **ql2400-firmware**-Firmware für QLogic 4Gbps Fibre-Channel-HBA wurde auf Version 5.08.00 aktualisiert.

- Die **ql2500-firmware**-Firmware für QLogic 4Gbps Fibre-Channel-HBA wurde auf Version 5.08.00 aktualisiert.

- Der **ipr**-Treiber für IBM Power Linux RAID SCSI HBAs wurde auf Version 2.5.4 aktualisiert, um Unterstützung für Power7 6Gb SAS Adapter hinzuzufügen und SAS-VRAID-Fähigkeiten auf diesen Adaptern zu ermöglichen.

- Der **hpsa**-Treiber wurde auf Version 2.0.2-4-RH1 aktualisiert, um PCI-IDs für die HP Smart Array Generation 8 Controller-Familie hinzuzufügen.

- Der **bnx2i**-Treiber für Broadcom NetXtreme II iSCSI wurde auf Version 2.7.2.2 aktualisiert für allgemeine Hardware-Unterstützung.

  Unterstützung für iSCSI- und FCoE-Boot auf Broadcom-Geräten wird in Red Hat Enterprise Linux 6.4 nun vollständig unterstützt. Diese beiden Features werden von den bnx2i und bnx2fc Broadcom-Treibern bereitgestellt.

- Der **bnx2fc**-Treiber für den Broadcom Netxtreme II 57712 Chip wurde auf Version 1.0.12 aktualisiert.

Unterstützung für iSCSI- und FCoE-Boot auf Broadcom-Geräten wird in Red Hat Enterprise Linux 6.4 nun vollständig unterstützt. Diese beiden Features werden von den bnx2i und bnx2fc Broadcom-Treibern bereitgestellt.

- Der **mpt2sas**-Treiber wurde auf Version 13.101.00.00 aktualisiert, um Unterstützung für den Multi-Segment-Modus für den Linux BSG Treiber hinzuzufügen.
- Der Brocade **bfa** Fibre-Channel und FCoE-Treiber wurde auf Version 3.0.23.0 aktualisiert und bietet nun Unterstützung für Brocade 1860 16Gbps Fibre-Channel-Adapter, für neue Hardware in Dell PowerEdge 12th Generation Server sowie für **issue_lip**. Die **bfa**-Firmware wurde auf Version 3.0.3.1 aktualisiert.
- Der **be2iscsi**-Treiber für ServerEngines BladeEngine 2 Open iSCSI-Geräte wurde auf Version 4.4.58.0r aktualisiert, um iSCSI netlink VLAN-Unterstützung hinzuzufügen.
- Der **qib**-Treiber für TrueScale HCAs wurde auf die neueste Version aktualisiert mit den folgenden Verbesserungen:
  - Verbesserte NUMA-Fähigkeiten
  - Congestion Control Agent (CCA) für Performance Scale Messaging (PSM) Strukturen
  - Dual Rail für PSM-Strukturen
  - Leistungsverbesserungen und Fehlerbehebungen
- Die folgenden Treiber wurden aktualisiert, um die neuesten Upstream-Features und Fehlerbehebungen zu implementieren: **ahci**, **md**/**bitmap**, **raid0**, **raid1**, **raid10** und **raid456**

Netzwerktreiber

- Der **netxen_nic**-Treiber für NetXen Multiport (1/10) Gigabit Network wurde auf Version 4.0.80 aktualisiert, um miniDIMM-Unterstützung hinzuzufügen. Die **netxen_nic**-Firmware wurde auf Version 4.0.588 aktualisiert.
- Der **bnx2x**-Treiber wurde auf die Version 1.72.51-0 aktualisiert, um Unterstützung für Broadcom 57800/57810/57811/57840 Chips sowie allgemeine Fehlerbehebungen und aktualisierte Firmware für Broadcom 57710/57711/57712 Chips zu implementieren. Diese Aktualisierung enthält zudem die folgenden Verbesserungen:
  - Unterstützung für iSCSI-Offload und Data Center Bridging/Fibre Channel over Ethernet (DCB/FCOE) auf Broadcom 57712/578xx Chips. Der Broadcom 57840 Chip wird nur in einer 4x10G Konfiguration unterstützt und unterstützt weder iSCSI-Offload noch FCoE. Zukünftige Releases werden weitere Konfigurationen sowie iSCSI-Offload und FCoE unterstützen.
  - Zusätzliche Unterstützung für Physical Layer, einschließlich Energy Efficient Ethernet (EEE).
  - iSCSI-Offload-Verbesserungen
  - OEM-spezifische Features
- Der **be2net**-Treiber für ServerEngines BladeEngine2 10Gbps Netzwerkgeräte wurde auf Version 4.4.31.0r aktualisiert, um Unterstützung für RDMA over Converged Ethernet (RoCE) zu implementieren.

Darüber hinaus wird die SR-IOV-Funktionalität des Emulex **be2net**-Treibers in Red Hat Enterprise Linux 6.4 nun vollständig unterstützt. SR-IOV läuft auf allen Emulex- und OEM-Varianten von BE3-basierter Hardware, die alle die **be2net**-Treibersoftware benötigen.

- Der **ixgbevf**-Treiber wurde auf Version 2.6.0-k aktualisiert, um Unterstützung für die neueste Hardware, Verbesserungen und Fehlerbehebungen zu implementieren.
- Der **cxgb4**-Treiber für Chelsio Terminator4 10G Unified Wire Network Controller wurde aktualisiert, um Unterstützung für Chelsios T480-CR und T440-LP-CR Adapter hinzuzufügen.
- Der **cxgb3**-Treiber für die Chelsio T3 Netzwerktreiberfamilie wurde auf Version 1.1.5-ko aktualisiert.
- Der **ixgbe**-Treiber für Intel 10 Gigabit PCI Express Netzwerkgeräte wurde auf Version 3.9.15-k aktualisiert, um Unterstützung für SR-IOV mit Data Center Bridging (DCB) oder Receive-Side Scaling (RSS), Unterstützung für PTP als Technologievorschau sowie Unterstützung für die neueste Hardware, Verbesserungen und Fehlerbehebungen zu implementieren.
- Der **iw_cxgb3**-Treiber wurde aktualisiert.
- Der **iw_cxgb4**-Treiber wurde aktualisiert.
- Der **e1000e**-Treiber für Intel PRO/1000 Netzwerkgeräte wurde aktualisiert, um Unterstützung für die neueste Hardware, die neuesten Features sowie eine Reihe von Fehlerbehebungen zu implementieren.
- Der **enic**-Treiber für Cisco 10G Ethernet-Geräte wurde auf Version 2.1.1.39 aktualisiert.
- Der **igbvf**-Treiber ('Intel Gigabit Virtual Function' Netzwerktreiber) wurde auf die neueste Upstream-Version aktualisiert.
- Der **igb**-Treiber für Intel Gigabit Ethernet-Adapter wurde auf Version 4.0.1 aktualisiert, um Unterstützung für die neueste Hardware hinzuzufügen. Zudem wurde PTP-Unterstützung zum **igb**-Treiber als Technologievorschau hinzugefügt.
- Der **tg3**-Treiber für Broadcom Tigon3 Ethernet-Geräte wurde auf Version 3.124 aktualisiert, um Unterstützung für neue Hardware hinzuzufügen. Zudem wurde PTP-Unterstützung zum **tg3**-Treiber als Technologievorschau hinzugefügt.
- Der **qlcnic**-Treiber für die HP NC-Series QLogic 10 Gigabit Server-Adapter wurde auf Version 5.0.29 aktualisiert.
- Der Brocade **bna**-Treiber für Brocade 10Gb PCIe Ethernet-Controller-Treiber wurde auf Version 3.0.23.0 aktualisiert, um neue Hardware-Unterstützung für Dell PowerEdge 12th Generation Server hinzuzufügen, und ermöglicht nun die Verwendung von nicht-Brocade Twinax-Kupferkabeln. Die **bna**-Firmware wurde auf Version 3.0.3.1 aktualisiert.
- Der Broadcom NetXtreme II **cnic**-Treiber wurde auf Version 2.5.13 aktualisiert, um neue Features, Fehlerbehebungen und Unterstützung für neue OEM-Plattformen zu implementieren.

Sonstige Treiber

- Der **intel_idle**-cpuidle-Treiber für Intel-Prozessoren wurde aktualisiert, um Unterstützung für Intels Xeon E5-XXX V2 Prozessorserie zu implementieren.

- Der **wacom**-Treiber wurde aktualisiert, um Unterstützung für den CTL-460 Wacom Bamboo Pen, das Wacom Intuos5 Tablet und das Wacom Cintiq 22HD Pen Display zu implementieren.
- Der ALSA HDA Audiotreiber wurde aktualisiert, um verbesserte Unterstützung für neue Hardware sowie eine Reihe von Fehlerbehebungen zu implementieren.
- Der **mlx4_en**-Treiber wurde auf die neueste Upstream-Version aktualisiert.
- Der **mlx4_ib**-Treiber wurde auf die neueste Upstream-Version aktualisiert.
- Der **mlx4_core**-Treiber wurde auf die neueste Upstream-Version aktualisiert.
- Der **z90crypt**-Gerätetreiber wurde aktualisiert, um Unterstützung für die neue Crypto Express 4 (CEX4) Adapterkarte zu implementieren.

KAPITEL 4. NETZWERK

HAProxy

HAProxy ist ein eigenständiger Layer 7 Hochleistungsnetzwerklastverteiler für TCP- und HTTP-basierte Applikationen, der basierend auf dem Inhalt der HTTP-Anfragen verschiedene Scheduling-Typen durchführen kann. Red Hat Enterprise Linux 6.4 führt das haproxy-Paket als Technologievorschau ein.

KAPITEL 5. AUTHENTIFIZIERUNG UND INTEROPERABILITÄT

Vollständig unterstützte SSSD-Features

Eine Reihe von Features, die in Red Hat Enterprise Linux 6.3 eingeführt wurden, werden in Red Hat Enterprise Linux 6.4 nunmehr vollständig unterstützt. Insbesondere:

- Unterstützung für zentrale Verwaltung von SSH-Schlüsseln,
- SELinux-Benutzerzuordnung,
- sowie Unterstützung für Automount-Map-Caching.

Neuer SSSD-Cache-Speichertyp

Kerberos-Version 1.10 fügt den neuen Cache-Speichertyp **`DIR:`** hinzu, der es Kerberos erlaubt, Ticket Granting Tickets (TGTs) für mehrere Key Distribution Centers (KDCs) simultan zu bewahren und bei der Verhandlung mit Kerberos-fähigen Ressourcen automatisch zwischen diesen auszuwählen. In Red Hat Enterprise Linux 6.4 wurde SSSD verbessert, so dass Sie nun den **`DIR:`**-Cache für Benutzer auswählen können, die sich per SSSD anmelden. Dieses Feature wird als Technologievorschau eingeführt.

Hinzufügen von AD-basierten vertrauenswürdigen Domains zu `external`-Gruppen

In Red Hat Enterprise Linux 6.4 ermöglicht es Ihnen der **`ipa group-add-member`**-Befehl, Mitglieder von Active Directory-basierten vertrauenswürdigen Domains zu Gruppen hinzuzufügen, die in der Identitätsverwaltung als **`external`** gekennzeichnet sind. Diese Mitglieder können anhand ihres Namens mithilfe von Domain- oder UPN-basierter Syntax spezifiziert werden, z.B. **`AD\UserName`** oder **`AD\GroupName`** oder **`User@AD.Domain`**. Wenn Mitglieder in dieser Form spezifiziert werden, so werden sie anhand des globalen Katalogs der Active Directory-basierten vertrauenswürdigen Domain aufgelöst, um ihren Security Identifier (SID) Wert zu erhalten.

Alternativ kann direkt ein SID-Wert spezifiziert werden. In diesem Fall wird der **`ipa group-add-member`**-Befehl nur verifizieren, dass der Domain-Teil des SID-Werts zu einer der vertrauenswürdigen Active Directory Domains gehört. Dagegen wird kein Versuch unternommen, die Gültigkeit der SID innerhalb der Domain zu verifizieren.

Es wird empfohlen, Benutzer- oder Benutzergruppensyntax zur Angabe von externen Mitgliedern zu verwenden, statt deren SID-Werte direkt anzugeben.

Automatische Verlängerung von Zertifikaten im Identity-Management-Untersystem

Die standardmäßige Gültigkeit für eine neue Certificate Authority beträgt 10 Jahre. Die CA gibt eine Reihe von Zertifikaten für ihre Untersysteme (OCSP, Audit-Log u.a.) aus. Untersystemzertifikate sind normalerweise für 2 Jahre gültig. Falls die Zertifikate ablaufen, startet die CA nicht oder funktioniert nicht ordnungsgemäß. Aus diesem Grund sind Identity-Management-Server in Red Hat Enterprise Linux 6.4 dazu in der Lage, automatisch ihre Untersystemzertifikate zu verlängern. Die Untersystemzertifikate werden von **certmonger** überwacht, der automatisch eine Verlängerung der Zertifikate versucht, bevor diese ablaufen.

Automatische Konfiguration von OpenLDAP-Clienttools auf Clients unter Identity Management

In Red Hat Enterprise Linux 6.4 wird OpenLDAP während der Installation des Identity-Management-Clients automatisch mit der standardmäßigen LDAP-URI, einer Basis-DN und einem TLS-Zertifikat konfiguriert. Dies verbessert die Benutzerfreundlichkeit bei der Durchführung von LDAP-Suchen auf dem Directory Server des Identity Managements.

PKCS#12 Unterstützung für python-nss

Das python-nss-Paket, das Python-Bindings für Network Security Services (NSS) und die Netscape Portable Runtime (NSPR) bereitstellt, wurde aktualisiert, um Unterstützung für PKCS #12 zu implementieren.

Vollständig persistente Suche für DNS

LDAP in Red Hat Enterprise Linux 6.4 enthält Unterstützung für persistente Suchen sowohl nach Zonen als auch nach deren Ressourceneinträgen. Persistente Suchen ermöglichen es dem **bind-dyndb-ldap**-Plugin, unverzüglich über alle Änderungen in einer LDAP-Datenbank informiert zu sein. Sie verringern darüber hinaus die Netzwerklast durch wiederholte Abrufe.

Neue CLEANALLRUV-Operation

Obsolete Elemente im Replica Update Vector (RUV) der Datenbank können mit der **`CLEANRUV`**-Operation entfernt werden, die diese Elemente auf einem einzelnen Anbieter oder Master entfernt. Red Hat Enterprise Linux 6.4 fügt eine neue **`CLEANALLRUV`**-Operation hinzu, die obsolete RUV-Daten von allen Kopien entfernt und nur auf einem einzigen Anbieter/Master ausgeführt werden muss.

samba4-Bibliotheken aktualisiert

Die **samba4**-Bibliotheken (bereitgestellt vom samba4-libs-Paket) wurden auf die neueste Upstream-Version aktualisiert, um die Interoperabilität mit Active Directory (AD) Domains zu verbessern. SSSD verwendet nun die **`libndr-krb5pac`**-Bibliothek, um das Privilege Attribute Certificate (PAC) zu verarbeiten, das von einem AD Key Distribution Center (KDC) ausgegeben wird. Darüber hinaus wurden mehrere Verbesserungen an den Local Security Authority (LSA) und Net-Logon-Diensten vorgenommen, um die Vertrauenswürdigkeit von einem Windows-System aus bestätigen zu können. Weitere Informationen über die Einführung der Cross-Realm Kerberos-Trust-Funktionalität, die auf samba4-Paketen beruht, finden Sie in »Cross-Realm Kerberos-Trust-Funktionalität in Identity Management«.

WARNUNG

Falls Sie von Red Hat Enterprise Linux 6.3 auf Red Hat Enterprise Linux 6.4 aktualisieren und Samba verwenden, stellen Sie sicher, dass Sie zunächst das samba4-Paket deinstallieren, um Konflikte während des Upgrades zu vermeiden.

Die es sich bei der Cross-Realm Kerberos-Trust-Funktionalität um eine Technologievorschau handelt, gelten ausgewählte **samba4**-Komponenten als Technologievorschau. Weitere Informationen darüber, welche Samba-Pakete als Techologievorschau gelten, finden Sie in Tabelle 5.1, »Samba4-Paketunterstützung«.

Tabelle 5.1. Samba4-Paketunterstützung

Paketname	Neues Paket in 6.4?	Status
samba4-libs	Nein	Technologievorschau, mit Ausnahme der für OpenChange notwendigen Funktionalität
samba4-pidl	Nein	Technologievorschau, mit Ausnahme der für OpenChange notwendigen Funktionalität
samba4	Nein	Technologievorschau

Paketname	Neues Paket in 6.4?	Status
samba4-client	Ja	Technologievorschau
samba4-common	Ja	Technologievorschau
samba4-python	Ja	Technologievorschau
samba4-winbind	Ja	Technologievorschau
samba4-dc	Ja	Technologievorschau
samba4-dc-libs	Ja	Technologievorschau
samba4-swat	Ja	Technologievorschau
samba4-test	Ja	Technologievorschau
samba4-winbind-clients	Ja	Technologievorschau
samba4-winbind-krb5-locator	Ja	Technologievorschau

Cross-Realm Kerberos-Trust-Funktionalität in Identity Management

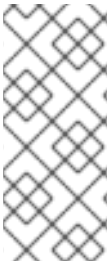
Die Cross-Realm Kerberos-Trust-Funktionalität im Identity Management ist als Technologievorschau enthalten. Dieses Feature ermöglicht die Erstellung einer Vertrauensbeziehung zwischen einer Identity-Management-Domain und einer Active-Directory-Domain. Das bedeutet, dass Benutzer von der AD-Domain auf Ressourcen und Dienste von der Identity-Management-Domain zugreifen können unter Verwendung ihrer AD-Berechtigungsnachweise. Zwischen den Controllern der Identity-Management-Domain und der AD-Domain müssen keinerlei Daten synchronisiert werden; AD-Benutzer werden immer beim AD-Domain-Controller authentifiziert und Informationen über Benutzer werden abgerufen, ohne dass eine Synchronisation nötig ist.

Dieses Feature wird von dem optionalen ipa-server-trust-ad-Paket bereitgestellt. Dieses Paket basiert auf Features, die nur in **samba4** verfügbar sind. Da samba4-*-Pakete mit den entsprechenden samba-*-Paketen kollidieren, müssen zunächst alle samba-*-Pakete entfernt werden, bevor ipa-server-trust-ad installiert werden kann.

Wenn das ipa-server-trust-ad-Paket installiert ist, muss der **`ipa-adtrust-install`**-Befehl auf allen Identity-Management-Servern und Kopien ausgeführt werden, um die Handhabung dieser Vertrauensbeziehungen im Identity Management zu aktivieren. Sobald dies erledigt ist, kann per Befehlszeile mithilfe des Befehls **`ipa trust-add`** oder per Weboberfläche eine Vertrauensbeziehung eingerichtet werden. Weitere Informationen finden Sie in Abschnitt *Integrating with Active Directory Through Cross-Realm Kerberos Trusts* im *Identity Management Guide* unter https://access.redhat.com/knowledge/docs/Red_Hat_Enterprise_Linux/.

Posix-Schema-Unterstützung für 389 Directory Server

Windows Active Directory (AD) unterstützt das POSIX-Schema (RFC 2307 und 2307bis) für Benutzer- und Gruppeneinträge. In vielen Fällen wird AD als autoritative Quelle für Benutzer- und Gruppendaten einschließlich POSIX-Attributen verwendet. Ab Red Hat Enterprise Linux 6.4 ignoriert der Directory Server Windows-Sync diese Attribute nicht mehr. Benutzer können nun POSIX-Attribute mit Windows-Sync zwischen AD und 389 Directory Server synchronisieren.



ANMERKUNG

Beim Hinzufügen von neuen Benutzer- und Gruppeneinträgen im Directory Server werden die POSIX-Attribute nicht mit dem AD synchronisiert. Werden dagegen neue Benutzer- und Gruppeneinträge zum AD hinzugefügt, so werden diese mit dem Directory Server synchronisiert, und werden Attribute verändert, so werden diese in beide Richtungen synchronisiert.

KAPITEL 6. SICHERHEIT

Autoritative Ergebnisse beim Nachschlagen von Sudo-Einträgen

Das **sudo**-Hilfsprogramm ist dazu in der Lage, die **/etc/nsswitch.conf**-Datei auf Sudo-Einträge zu untersuchen und diese in Dateien oder per LDAP nachzuschlagen. Bislang wurde diese Nachschlage-Operation auch dann in anderen Datenbanken (einschließlich Dateien) fortgeführt, wenn ein übereinstimmender Eintrag in der ersten Datenbank für Sudo-Einträge gefunden wurde. In Red Hat Enterprise Linux 6.4 wurde eine Option zur **/etc/nsswitch.conf**-Datei hinzugefügt, die es Benutzern ermöglicht, eine Datenbank festzulegen, nach der eine Übereinstimmung mit einem Sudo-Eintrag ausreicht. Dadurch werden Abfragen weiterer Datenbanken überflüssig und die Leistung beim Nachschlagen von Sudo-Einträgen in großen Umgebungen wird mithin verbessert. Dieses Verhalten ist standardmäßig nicht aktiviert und muss konfiguriert werden, indem die Zeichenfolge ***[SUCCESS=return]*** nach der gewählten Datenbank eingefügt wird. Wenn in der Datenbank, die dieser Zeichenfolge direkt vorausgeht, eine Übereinstimmung gefunden wird, so werden keine weiteren Datenbanken mehr überprüft.

Zusätzliche Passwortprüfungen für `pam_cracklib`

Das **pam_cracklib**-Modul wurde aktualisiert, um mehrere neue Prüfungen der Passwortstärke zu implementieren:

- Bestimmte Authentifizierungsrichtlinien erlauben keine Passwörter, die lange, fortlaufende Sequenzen wie z.B. "abcd" oder "98765" enthalten. Diese Aktualisierung führt nun die Möglichkeit ein, mithilfe der neuen **maxsequence**-Option die Höchstlänge dieser Sequenzen zu begrenzen.

- Das **pam_cracklib**-Modul ermöglicht nun die Prüfung, ob ein neues Passwort Wörter aus dem GECOS-Feld aus Einträgen in der **/etc/passwd**-Datei enthält. Das GECOS-Feld wird dazu verwendet, um zusätzliche Informationen über den Benutzer zu speichern, beispielsweise den vollständigen Namen des Benutzers oder eine Telefonnummer. Diese Informationen könnten von einem Angreifer dazu verwendet werden, um gegebenenfalls ein solches Passwort zu knacken.

- Das **pam_cracklib**-Modul ermöglicht mithilfe der **maxrepeatclass**-Option nun die Angabe der maximal zulässigen Anzahl aufeinanderfolgender Zeichen derselben Zeichenklasse (Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen) in einem Passwort.

- Das **pam_cracklib**-Modul unterstützt nun die **enforce_for_root**-Option, die Komplexitätsvorgaben für neue Passwörter des Root-Accounts erzwingen.

size-Option für tmpfs-Polyinstantiierung

Auf einem System mit mehreren tmpfs-Mounts ist es notwendig, deren Größe zu beschränken, damit sie nicht den gesamten Systemspeicher in Anspruch nehmen. PAM wurde aktualisiert, um es Benutzern nun mithilfe der **mntopts=size=<*size*>**-Option in der **/etc/namespace.conf**-Konfigurationsdatei zu ermöglichen, die maximale Größe des tmpfs-Dateisystem-Mounts zu spezifizieren, wenn tmpfs-Polyinstantiierung verwendet wird.

Sperren inaktiver Benutzerkonten

Bestimmte Authentifizierungsrichtlinien erfordern Unterstützung zur Sperrung eines Benutzerkontos, das während einer bestimmten Zeitspanne nicht benutzt wurde. Red Hat Enterprise Linux 6.4 bringt eine zusätzliche Funktion in das **pam_lastlog**-Modul ein, die es Benutzern ermöglicht, Benutzerkonten nach einer konfigurierbaren Anzahl von Tagen zu sperren.

Neue Operationsmodi für `libica`

Die **libica**-Bibliothek, die eine Reihe von Funktionen und Tools zum Zugriff auf die IBM eServer Cryptographic Accelerator (ICA) Hardware auf IBM System z enthält, wurde bearbeitet, um die

Verwendung neuer Algorithmen zu ermöglichen, welche die Message Security Assist Extension 4 Instruktionen in der Central Processor Assist for Cryptographic Function (CPACF) unterstützen. Für die DES und 3DES Blockchiffren werden nun die folgenden Operationsmodi unterstützt:

- Cipher Block Chaining with Ciphertext Stealing (CBC-CS)
- Cipher-based Message Authentication Code (CMAC)

Für die AES-Blockchiffre werden nun die folgenden Operationsmodi unterstützt:

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

Diese Beschleunigung komplexer kryptographischer Algorithmen verbessert wesentlich die Leistung von IBM System z Rechnern.

Optimierung und Unterstützung der `zlib`-Komprimierungsbibliothek für System z

Die zlib-Bibliothek - eine Bibliothek für allgemeine, verlustfreie Datenkomprimierung - wurde aktualisiert, um die Komprimierungsleistung auf IBM System z zu verbessern.

Ausweichkonfiguration für Firewall

Die **`iptables`**- und **`ip6tables`**-Dienste bieten nun die Fähigkeit, der Firewall eine Ausweichkonfiguration zuzuweisen, falls die standardmäßigen Konfigurationen nicht angewendet werden können. Falls das Anwenden der Firewall-Regeln aus **`/etc/sysconfig/iptables`** fehlschlägt, wird die Ausweichdatei angewendet, sofern eine existiert. Die Ausweichdatei heißt **`/etc/sysconfig/iptables.fallback`** und verwendet das **`iptables-save`**-Dateiformat (dasselbe Format wie **`/etc/sysconfig/iptables`**). Falls das Anwenden der Ausweichdatei ebenfalls fehlschlägt, gibt es keine weitere Ausweichlösung. Um eine Ausweichdatei zu erstellen, verwenden Sie die standardmäßigen Firewall-Konfigurationstools und benennen Sie die Datei in die Ausweichdatei um bzw. kopieren Sie sie entsprechend. Dasselbe Vorgehen gilt für den **`ip6tables`**-Dienst, ersetzen Sie einfach überall »iptables« durch »ip6tables«.

KAPITEL 7. BERECHTIGUNGEN

Aktualisierte Terminologie

In Red Hat Enterprise Linux 6.4 wurden im Subscription Manager mehrere Begriffe umbenannt:

- *subskribieren* wurde umbenannt in *verknüpfen*
- *automatisch subskribieren* wurde umbenannt in *automatisch verknüpfen*
- *abmelden* wurde umbenannt in *entfernen*
- *Verbraucher* wurde umbenannt in *System* bzw. *Einheit*

Testen der Proxy-Verbindung

Der Dialog zur Proxy-Konfiguration erlaubt es Benutzern nun, eine Verbindung zu einem Proxy zu testen, nachdem ein Wert eingegeben wurde.

Subskribieren oder Abmelden von mehreren Berechtigungen

Subscription Manager ist nun dazu in der Lage, mehrere Berechtigungen gleichzeitig zu subskribieren (zu verknüpfen) bzw. davon abzumelden (zu entfernen), indem deren Seriennummern gleichzeitig angegeben werden.

Unterstützung für Aktivierungsschlüssel im GUI

Die grafische Benutzeroberfläche des Subscription Managers ermöglicht es Ihnen nun, ein System mithilfe eines *Aktivierungsschlüssels* zu registrieren. Aktivierungsschlüssel ermöglichen es Benutzern, Subskriptionen für ein System vorzukonfigurieren, bevor es registriert wird.

Registrierung bei externen Servern

Im Subscription Manager wird nun während der Registrierung eines Systems die Auswahl eines entfernten Servers unterstützt. Die Benutzeroberfläche des Subscription Managers bietet während des Registrierungsvorgangs eine Option zur Angabe einer URL, eines Ports und eines Präfixes für den Server, bei dem registriert werden soll. Zudem kann bei einer Registrierung per Befehlszeile die Option `--serverurl` verwendet werden, um den Server anzugeben, bei dem registriert werden soll. Weitere Informationen über dieses Feature finden Sie im Abschnitt *Registering, Unregistering, and Reregistering a System* im *Subscription Management Guide*.

Änderungen der grafischen Benutzeroberfläche

Die grafische Benutzeroberfläche des Subscription Managers wurde auf Grundlage von Kundenfeedback in verschiedenen Aspekten verbessert.

KAPITEL 8. VIRTUALISIERUNG

8.1. KVM

virtio-SCSI

Der Speicherstapel der KVM-Virtualisierung wurde verbessert, indem virtio-SCSI (eine Speicherarchitektur für KVM basierend auf SCSI) Fähigkeiten hinzugefügt wurden. Virtio-SCSI bietet die Fähigkeit, direkt mit SCSI LUNs zu verbinden und verbessert signifikant die Skalierbarkeit im Vergleich zu virtio-blk. Der Vorteil von virtio-SCSI besteht darin, dass es zur Handhabung von Hunderten von Geräten in der Lage ist, im Gegensatz zu virtio-blk, das nur ungefähr 25 Geräte handhaben kann und PCI-Slots verbraucht.

Virtio-SCSI ist nun dazu fähig, das Feature-Set des Zielgeräts zu erben, mit folgenden Fähigkeiten:

- Verknüpfen einer virtuellen Festplatte oder CD mittels virtio-scsi-Controller
- Durchreichen eines physischen SCSI-Geräts vom Host an den Gast mittels QEMU scsi-block-Gerät
- Verwenden von Hunderten von Geräten pro Gast, eine Verbesserung verglichen mit dem ~25-Gerätelimit von virtio-blk

virtio-scsi wurde in Red Hat Enterprise Linux 6.3 als Technologievorschau eingeführt und wird in Red Hat Enterprise Linux 6.4 nun vollständig unterstützt. Windows-Gäste (ausgenommen Windows XP) werden ebenfalls unterstützt mit den neuesten virtio-win-Treibern.

Unterstützung für Intels Next-generation Core Prozessor

Red Hat Enterprise Linux 6.4 fügt Unterstützung für Intels Next-Generation Core Prozessor zu **qemu-kvm** hinzu, so dass KVM-Gäste die neuen Features dieses Prozessors ausnutzen können, insbesondere: Advanced Vector Extensions 2 (AVX2), Bit-Manipulation Instructions 1 (BMI1), Bit-Manipulation Instructions 2 (BMI2), Hardware Lock Elision (HLE), Restricted Transactional Memory (RTM), Process-Context Identifier (PCID), Invalidate Process-Context Identifier (INVPCID), Fused Multiply-Add (FMA), Big-Endian Move instruction (MOVBE), F Segment and G Segment BASE instruction (FSGSBASE), Supervisor Mode Execution Prevention (SMEP), Enhanced REP MOVSB/STOSB (ERMS).

Unterstützung für CPUs der AMD Opteron 4xxx Serie

Die Prozessoren der AMD Opteron 4xxx Serie werden nun von **qemu-kvm** unterstützt. Dadurch können neue Features dieser Prozessorserie nun KVM-Gästen zur Verfügung gestellt werden, wie z.B.: das F16C Instruktionsset, Trailing Bit Manipulation, Bit-Manipulation Instructions 1 (BMI1) decimate-Funktionen und das Fused Multiply-Add (FMA) Instruktionsset.

Live-Migration von Gästen mittels USB-Weiterleitung mit SPICE

In Red Hat Enterprise Linux 6.4 unterstützt KVM die Live-Migration von Gästen mittels USB-Weiterleitung unter Verwendung von SPICE, während vorhandene USB-Geräteumleitungen für alle konfigurierten Geräte beibehalten werden.

Live-Migration von Gästen mit USB-Geräten

In Red Hat Enterprise Linux 6.4 unterstützt KVM die Live-Migration von Gästen mit USB-Geräten. Die folgenden Geräte werden unterstützt: Enhanced Host Controller Interface (EHCI) und Universal Host Controller Interface (UHCI) lokaler Passthrough und emulierte Geräte wie Speichergeräte, Mäuse, Tastaturen, Hubs u.a.

QEMU-Gastagent aktualisiert

Der QEMU-Gastagent (bereitgestellt vom qemu-guest-agent-Paket) wird in Red Hat Enterprise Linux 6.4 nun vollständig unterstützt. Er wurde auf Upstream-Version 1.1 aktualisiert und enthält die folgenden nennenswerten Verbesserungen und Fehlerbehebungen:

- Die **`guest-suspend-disk`**- und **`guest-suspend-ram`**-Befehle können nun dazu verwendet werden, um auf einem Windows-System Suspend-to-RAM oder Suspend-to-Disk auszuführen.
- Der **`guest-network-get-interfaces`**-Befehl kann nun dazu verwendet werden, um Informationen über Netzwerkschnittstellen in Linux abzurufen.
- Diese Aktualisierung implementiert Verbesserungen und Fehlerbehebungen am Dateisystem-Freeze.
- Diese Aktualisierung bringt verschiedene Fehlerbehebungen und kleinere Verbesserungen an der Dokumentation ein.

Paravirtualized End-of-Interrupt (PV-EOI)

Hosts und Gäste, auf denen Red Hat Enterprise Linux 6.3 oder älter läuft, erfordern zwei VM-Exits (Kontextwechsel von einer VM zu einem Hypervisor) für jeden Interrupt: einen zum Injizieren des Interrupts und einen weiteren, um das Ende des Interrupts zu signalisieren. Wenn sowohl Host- als auch Gastsysteme auf Red Hat Enterprise Linux 6.4 oder neuer aktualisiert werden, können sie ein Paravirtualized End-of-Interrupt Feature verhandeln und erfordern dann nur einen Kontextwechsel pro Interrupt. Infolgedessen verringert der Einsatz von Red Hat Enterprise Linux 6.4 oder neuer als Host und Gast die Anzahl der Exits um die Hälfte für interruptintensive Arbeitslasten, wie z.B. für eingehenden Netzwerkverkehr mit einem virtio-Netzwerkgerät. Dies führt zu einer deutlich verringerten Beanspruchung der Host-CPU für diese Arbeitslasten. Beachten Sie, dass nur Flankeninterrupts verbessert werden: beispielsweise nutzt e1000-Networking Levelinterrupts und wurde daher nicht verbessert.

Konfigurierbare Audioweiterleitung

Ein Audiogerät kann nun als ein **`Mikrofon`** oder als ein **`Lautsprecher`** im Gastsystem erkannt werden (zusätzlich zu der Erkennung als **`Line-in`** und **`Line-out`**). Audiogeräte können nun ordnungsgemäß in solchen Gastapplikationen funktionieren, die nur bestimmte Eingabearten für Stimmaufzeichnungen und Audio akzeptieren.

8.2. HYPER-V

Integration und Unterstützung der Gastinstallation für Microsoft Hyper-V-Treiber

Integrierte Red Hat Enterprise Linux Gastinstallation und Unterstützung von Hyper-V paravirtualisierten Geräten in Red Hat Enterprise Linux 6.4 auf Microsoft Hyper-V ermöglicht es Benutzern, Red Hat Enterprise Linux 6.4 als Gast auf Microsoft Hyper-V Hypervisoren auszuführen. Die folgenden Hyper-V Treiber und eine Zeitquelle wurden zum Kernel, der in Red Hat Enterprise Linux 6.4 enthalten ist, hinzugefügt:

- ein Netzwerktreiber (**`hv_netvsc`**)
- ein Speichertreiber (**`hv_storvsc`**)
- ein HID-konformer Maustreiber (**`hid_hyperv`**)
- ein VMbus-Treiber (**`hv_vmbus`**)
- ein Util-Treiber (**`hv_util`**)
- ein IDE-Festplattentreiber (**`ata_piix`**)

- eine Zeitquelle (i386, AMD64/Intel 64: **hyperv_clocksource**)

Red Hat Enterprise Linux 6.4 enthält zudem Unterstützung für Hyper-V als Zeitquelle und einen Hyper-V Key-Value Pair (KVP) Gast-Daemon (**hypervkvpd**), der grundlegende Informationen wie die Gast-IP, den FQDN, Betriebssystemnamen und die Betriebssystem-Releasenummer über VMbus an den Host übergibt.

8.3. VMWARE ESX

Paravirtualisierte VMware-Treiber

Die paravirtualisierten Treiber für VMware wurden aktualisiert, um den nahtlosen Einsatz ohne weitere Konfiguration von Red Hat Enterprise Linux 6.4 in VMware ESX zu ermöglichen. Der Anaconda-Installer wurde ebenfalls aktualisiert, um die Treiber während des Installationsvorgangs aufzulisten. Die folgenden Treiber wurden aktualisiert:

- ein Netzwerktreiber (**vmxnet3**)
- ein Speichertreiber (**vmw_pvscsi**)
- ein Memory-Ballooning-Treiber (**vmware_balloon**)
- ein Maustreiber (**vmmouse_drv**)
- ein Grafiktreiber (**vmware_drv**)

KAPITEL 9. CLUSTERING

Unterstützung für IBM iPDU Fencing-Gerät

Red Hat Enterprise Linux 6.4 fügt Unterstützung für das IBM iPDU Fencing-Gerät hinzu. Weitere Informationen über die Parameter dieses Fencing-Geräts finden Sie im Anhang *Parameter der Fencing-Geräte* des Red Hat Enterprise Linux 6 *Cluster-Administrationshandbuchs*.

Unterstützung für Eaton-Netzwerkschalter Fencing-Gerät

Red Hat Enterprise Linux 6.4 fügt Unterstützung für **`fence_eaton_snmp`** hinzu, den Fencing-Agent für den Eaton-over-SNMP-Netzwerkschalter. Weitere Informationen über die Parameter dieses Fencing-Agents finden Sie im Anhang *Fence Device Parameters* des Red Hat Enterprise Linux 6 *Cluster-Administrationshandbuchs*.

Neues keepalived-Paket

Red Hat Enterprise Linux 6.4 enthält das keepalived-Paket als Technologievorschau. Das keepalived-Paket stellt simple und robuste Funktionalitäten zur Lastverteilung und Hochverfügbarkeit bereit. Das Lastverteilungs-Framework basiert auf dem bekannten und weit verbreiteten Linux Virtual Server Kernel-Modul, das Layer 4 Netzwerklastverteilung bereitstellt. Der **`keepalived`**-Daemon implementiert eine Reihe von Prüfungen für lastverteilte Server-Gruppen abhängig von deren Status. Der keepalived-Daemon implementiert zudem das Virtual Router Redundancy Protocol (VRRP), wodurch Router- oder Verteiler-Ausfallsicherung zwecks Hochverfügbarkeit erreicht wird.

Watchdog-Wiederherstellung

Neue **`fence_sanlock`**- und **`checkquorum.wdmd`**-Fencing-Agents, die in Red Hat Enterprise Linux 6.4 als Technologievorschau enthalten sind, liefern neue Mechanismen zum Auslösen der Wiederherstellung eines Knotens per Watchdog-Gerät. Anleitungen zur Aktivierung dieser Technologievorschau werden unter https://fedorahosted.org/cluster/wiki/HomePage zur Verfügung stehen.

Unterstützung für VMDK-basierten Speicher

Red Hat Enterprise Linux 6.4 fügt Unterstützung für Cluster hinzu, die VMwares VMDK (Virtual Machine Disk) Festplatten-Image-Technologie mit der Multi-Writer-Option verwenden. Dies ermöglicht es Ihnen beispielsweise, VMDK-basierten Speicher mit der Multi-Writer-Option für geclusterte Dateisysteme wie GFS2 zu verwenden.

KAPITEL 10. SPEICHER

Parallel NFS vollständig unterstützt

Parallel NFS (pNFS) ist ein Teil des NFS v4.1 Standards, der Clients den direkten und parallelen Zugriff auf Speichergeräte gestattet. Die pNFS-Architektur kann die Skalierbarkeit und Performance von NFS-Servern für übliche Arbeitslasten verbessern. In Red Hat Enterprise Linux 6.4 wird pNFS nun vollständig unterstützt.

pNFS unterstützt 3 verschiedene Speicherprotokolle oder Layouts: Dateien, Objekte und Blocks. Der Red Hat Enterprise Linux 6.4 NFS Client unterstützt das Datei-Layout-Protokoll.

Verwenden Sie eine der folgenden Einhängeoptionen auf Mounts von einem pNFS-fähigen Server, um diese neue Funktion zu aktivieren: **`-o minorversion=1`** oder **`-o v4.1`**.

Wenn der Server pNFS-fähig ist, wird bei der ersten Einhängung automatisch das Kernel-Modul **`nfs_layout_nfsv41_files`** geladen. Überprüfen Sie mit dem folgenden Befehl, ob dieses Modul geladen wurde:

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

Weitere Informationen über pNFS finden Sie unter http://www.pnfs.com/.

Unterstützung für XFS-Online-Discard

Eine Online-Discard-Operation auf einem eingehängten Dateisystem verwirft Speicherblöcke, die vom Dateisystem nicht verwendet werden. Online-Discard-Operationen werden nun auf XFS-Dateisystemen unterstützt. Weitere Informationen finden Sie im Abschnitt *Discard Unused Blocks* im Red Hat Enterprise Linux 6 *Storage Administration Guide*.

LVM-Unterstützung für Micron PCIe SSD

In Red Hat Enterprise Linux 6.4 fügt LVM Unterstützung für Micron PCIe Solid State Drives (SSDs) hinzu als Geräte, die Teil einer Datenträgergruppe sein können.

LVM-Unterstützung für 2-Wege-Mirror RAID10

LVM ist nun dazu in der Lage, RAID10 logische Datenträger zu erstellen, zu entfernen und zu verkleinern/vergrößern. Um einen RAID10 logischen Datenträger zu erstellen, spezifizieren Sie wie für andere RAID-Typen auch den Typ wie folgt:

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

Beachten Sie, dass sich die Parameter **`-m`** und **`-i`** auf dieselbe Weise verhalten, wie auch für andere Typen. Das heißt, **`-i`** bezeichnet die Gesamtanzahl der Stripes, während **`-m`** die Anzahl der (zusätzlichen) Kopien bezeichnet (z.B. ergibt **`-m 1 -i 2`** 2 Stripes auf 2-Wege Spiegelplatten).

Einrichten und Verwalten von SCSI persistenten Reservierungen über Device-Mapper-Geräte

Um persistente Reservierungen auf Multipath-Geräten einzurichten, war es bislang notwendig, dies auf allen Geräten einzurichten. Falls ein Multipath-Gerät später hinzugefügt wurde, war es nötig, manuell Reservierungen zu diesem Pfad hinzuzufügen. Red Hat Enterprise Linux 6.4 ist nun dazu in der Lage, mithilfe des **`mpathpersist`**-Befehls SCSI persistente Reservierungen über Device-Mapper-Geräte einzurichten und zu verwalten. Wenn Multipath-Geräte hinzugefügt werden, werden auch auf diesen Geräten persistente Reservierungen eingerichtet.

KAPITEL 11. COMPILER UND WERKZEUGE

SystemTap aktualisiert auf Version 1.8

SystemTap ist ein Werkzeug zur Ablaufverfolgung und Überprüfung, das es Benutzern ermöglicht, Aktivitäten des Betriebssystems (insbesondere des Kernels) sehr detailliert zu untersuchen und zu überwachen. Es liefert Informationen, die der Ausgabe von Werkzeugen wie **netstat**, **ps**, **top** und **iostat** ähneln. SystemTap ist jedoch konzipiert, um mehr Filter- und Analyse-Optionen für gesammelte Informationen zu bieten.

Das systemtap-Paket in Red Hat Enterprise Linux 6.4 wurde auf Upstream-Version 1.8 aktualisiert und bietet eine Reihe von Fehlerbehebungen und Verbesserungen:

- Die **`@var`**-Syntax ist nun eine alternative Sprachsyntax zum Zugriff auf DWARF-Variablen in **`uprobe`**- und **`kprobe`**-Handlern (Prozess, Kernel, Modul).
- SystemTap wandelt nun lokale Variablen um, damit Konflikte mit den in Tapsets enthaltenen C-Headern vermieden werden.
- Der SystemTap-Kompilierungsserver und -client unterstützen nun IPv6-Netzwerke.
- SystemTap Runtime (**staprun**) akzeptiert nun die Option **`-T`** zur Zeitüberschreitung, um es weniger häufigen Wake-ups zu ermöglichen, Ausgaben mit niedrigem Durchsatz von Skripten abzurufen.
- Der SystemTap Skriptübersetzungs-Treiber (**`stap`**) bietet nun die folgenden Optionen zur Ressourcenbegrenzung:

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

- SystemTap-Module sind nun kleiner und kompilieren schneller. Die Debug-Informationen des Moduls werden nunmehr standardmäßig unterdrückt.
- Bug CVE-2012-0875 (Kernel-Panic bei der Verarbeitung von fehlerhaften DWARF-Unwind-Daten) ist nun behoben.

Die lscpu- und chcpu-Hilfsprogramme

Das **lscpu**-Hilfsprogramm, das detaillierte Informationen über die verfügbaren CPUs anzeigt, wurde aktualisiert, um zahlreiche neue Features zu implementieren. Darüber hinaus wurde ein neues Hilfsprogramm namens **chcpu** implementiert, das es Ihnen erlaubt, den CPU-Status zu ändern (Online/Offline, Standby/Aktiv u.a.), CPUs zu aktivieren bzw. zu deaktivieren sowie spezifizierte CPUs zu konfigurieren.

Weitere Informationen über diese Hilfsprogramme finden Sie in den **lscpu(1)**- und **chcpu(8)**-Handbuchseiten.

KAPITEL 12. ALLGEMEINE AKTUALISIERUNGEN

Aktualisierte samba-Pakete

Red Hat Enterprise Linux 6.4 enthält grundlegend erneuerte samba-Pakete, die mehrere Fehlerbehebungen und Verbesserungen einbringen, insbesondere Unterstützung für das SMB2-Protokoll. SMB2-Unterstützung kann mittels des folgenden Parameters im **[global]**-Abschnitt der **/etc/samba/smb.conf**-Datei aktiviert werden:

```
max protocol = SMB2
```

Darüber hinaus unterstützt Samba nun AES-Kerberos-Verschlüsselung. AES-Unterstützung steht in Microsoft Windows Betriebssystemen seit Windows Vista und Windows Server 2008 zur Verfügung. Dies soll der neue standardmäßige Kerberos-Verschlüsselungstyp seit Windows 7 sein. Samba fügt nun AES-Kerberos-Schlüsssel zu den von ihm verwalteten Schlüsseltabellen hinzu. Das bedeutet, dass andere kerberisierte Dienste, die die Samba-Schlüsseltabelle nutzen und auf demselben Rechner laufen, von der AES-Verschlüsselung profitieren können. Um AES-Sitzungsschlüssel (und nicht nur AES-verschlüsselte Ticket-Granting-Tickets) zu verwenden, muss der Samba-Recheraccount im LDAP-Server des Active Directorys manuell bearbeitet werden. Weitere Informationen finden Sie im Microsoft Open Specifications Support Team Blog.

WARNUNG

Die aktualisierten samba-Pakete ändern auch die Art und Weise, wie ID-Mapping konfiguriert wird. Benutzer werden gebeten, Ihre vorhandenen Samba-Konfigurationsdateien entsprechend anzupassen.

Beachten Sie, dass mehrere Trivial Database (TDB) Dateien aktualisiert wurden und die Druckunterstützung überarbeitet wurde, um die tatsächliche Registry-Implementierung zu verwenden. Das bedeutet, dass alle TDB-Dateien aktualisiert werden, sobald Sie die neue Version von **smbd** starten. Sie können kein Downgrade auf eine ältere Samba 3.x Version durchführen, wenn Sie keine Sicherungskopien der TDB-Dateien haben.

Weitere Informationen über diese Änderungen finden Sie in den Release Notes for Samba 3.6.0.

Neues SciPy-Paket

Red Hat Enterprise Linux 6.4 enthält ein neues scipy-Paket. Das SciPy-Paket stellt Software für die Mathematik, Wissenschaft und Technik bereit. Das NumPy-Paket, das zur Verarbeitung großer mehrdimensionaler Arrays beliebiger Daten konzipiert wurde, ist die Kernbibliothek für SciPy. Die SciPy-Bibliothek wurde zur Handhabung von NumPy-Arrays konzipiert und stellt verschiedene effiziente numerische Routinen bereit, z.B. Routinen für numerische Integration und Optimierung.

TLS v1.1 Unterstützung in NSS

Die nss- und nss-util-Pakete wurden auf Upstream-Version 3.14 aktualisiert, um neben anderen Features nun auch Unterstützung für TLS-Version 1.1 zu bieten. Zudem wurde das nspr-Paket grundlegend überarbeitet auf Version 4.9.2. Weitere Informationen finden Sie in den NSS 3.14 Release Notes.

Eingebetteter Valgrind-**gdbserver**

Das valgrind-Paket wurde auf Upstream-Version 3.8.1 aktualisiert. Diese aktualisierte Version enthält neben anderen Verbesserungen und Fehlerbehebungen einen eingebetteten **gdbserver**. Weitere Informationen finden Sie im *Valgrind*-Kapitel und im Anhang *Changes in Valgrind 3.8.1* des *Red Hat Developer Toolset 1.1 User Guide*.

Neue libjpeg-turbo-Pakete

Red Hat Enterprise Linux 6.4 enthält eine Gruppe neuer Pakete: libjpeg-turbo. Diese Pakete ersetzen die herkömmlichen libjpeg-Pakete und bieten dieselbe Funktionalität und API wie libjpeg, jedoch bessere Leistung.

Neues redhat-lsb-core-Paket

Bei der Installation des redhat-lsb-Pakets werden zahlreiche Abhängigkeiten in das System geladen, um dem LSB-Standard gerecht zu werden. Red Hat Enterprise Linux 6.4 stellt nun ein neues redhat-lsb-core-Unterpaket zur Verfügung, das es Ihnen ermöglicht, auf einfache Weise eine minimale Gruppe der erforderlichen Pakete abzurufen, indem Sie das redhat-lsb-core-Paket installieren.

createrepo-Hilfsprogramm aktualisiert

Das **createrepo**-Hilfsprogramm wurde auf die neueste Upstream-Version aktualisiert, die den Speicherverbrauch deutlich verringert und Multitasking-Unterstützung mit der **--workers**-Option einbringt.

ANHANG A. VERSIONSGESCHICHTE

Version 1-1.13.2.400 **2013-10-31** **Rüdiger Landmann**
Rebuild with publican 4.0.0

Version 1-1.13.2 **Mon Jan 21 2013** **Hedda Peters**
Deutsche Übersetzung fertiggestellt

Version 1-1.13.1 **Fri Jan 11 2013** **Chester Cheng**
Übersetzungsdateien synchronisiert mit XML-Quelldateien 1-1.12

Version 1-1.12 **Wed Dec 4 2012** **Martin Prpič**
Release der Red Hat Enterprise Linux 6.4 Beta Versionshinweise.