Red Hat Enterprise Linux 7
7.2 Versionshinweise

Versionshinweise für Red Hat Enterprise Linux 7.2

Red Hat Customer Content Services

Red Hat Enterprise Linux 7 7.2 Versionshinweise

Versionshinweise für Red Hat Enterprise Linux 7.2

Red Hat Customer Content Services

Rechtlicher Hinweis

Zusammenfassung

Die Versionshinweise liefern einen allgemeinen Überblick über die Verbesserungen und Erweiterungen, die in Red Hat Enterprise Linux 7.2 implementiert wurden und dokumentieren bekannte Probleme in dieser Release. Eine detaillierte Dokumentation aller Neuerungen in Red Hat Enterprise Linux 7.2 steht in den Technical Notes zur Verfügung.

Inhaltsverzeichnis

Vorwort

Nebenversionen (Minor Releases) von Red Hat Enterprise Linux sind eine Sammlung individueller Verbesserungen, Sicherheits-Errata und Bugfix-Errata. Die *Red Hat Enterprise Linux 7.2 Versionshinweise* dokumentieren die wesentlichen Änderungen, Features und Verbesserungen, die für diese Nebenversion des Red Hat Enterprise Linux 7 Betriebssystems und der darin enthaltenen Applikationen implementiert wurden. Darüber hinaus dokumentieren sie bekannte Probleme und enthalten eine Liste aller verfügbaren Technologievorschauen.

Die Möglichkeiten und Grenzen von Red Hat Enterprise Linux 7 im Vergleich zu anderen Versionen des Systems finden Sie im Knowledge Base Artikel unter https://access.redhat.com/articles/rhel-limits.

Informationen zum Red Hat Enterprise Linux Lebenszyklus finden Sie unter https://access.redhat.com/support/policy/updates/errata/.

Kapitel 1. Architekturen

Red Hat Enterprise Linux 7.2 ist bei den folgenden Architekturen als Einzel-Kit verfügbar: [1]

- 64-Bit AMD
- 64-Bit Intel
- IBM POWER7+ und POWER8 (Big-Endian)
- IBM POWER8 (Little Endian) [2]
- IBM System z [3]

In dieser Release vereint Red Hat Verbesserungen für Server und Systeme sowie für das Red Hat Open-Source-Erlebnis im Allgemeinen.

---

[1] Beachten Sie, dass die folgende Red Hat Enterprise Linux 7.2-Installation nur auf 64-bit Hardware unterstützt wird. Red Hat Enterprise Linux 7.2 kann als virtuele Maschine auf 32-bit Betriebssystemen laufen, einschließlich früherer Versionen von Red Hat Enterprise Linux.

[2] Red Hat Enterprise Linux 7.2 (Little Endian) wird derzeit nur als KVM-Gast unter **Red Hat Enteprise Virtualization for Power** und **PowerVM**-Hypervisoren unterstützt.

[3] Beachten Sie, dass Red Hat Enterprise Linux 7.2 die IBM zEnterprise 196 Hardware und höher unterstützt; IBM System z10 Mainframe-Systeme werden nicht mehr unterstützt und werden Red Hat Enterprise Linux 7.2 nicht booten.

Teil I. Neue Features

Dieser Teil beschreibt die neuen Features und wichtigen Verbesserungen, die mit Red Hat Enterprise Linux 7.2 eingeführt werden.

Kapitel 2. Authentifizierung

ca-certificate überarbeitet auf Version 2.4

Das ca-certificates-Paket wurde aktualisiert auf die Upstream-Version 2.4, die eine Reihe von Fehlerbehebungen und Verbesserungen gegenüber der vorherigen Version enthält. Insbesondere umfasst ca-certificates nun die folgenden Änderungen:

Mozilla entfernte in der Vergangenheit das Vertrauensmodell aus mehreren Legacy-CA-Zertifikaten, die 1024-bit RSA-Schlüssel enthielten. Diese Version des ca-certificates-Pakets bearbeitet die Mozilla-Liste, so dass diese die standardmäßig vertrauenswürdigen Legacy-CA-Zertifikate als solche beibehält. Die Änderung wurde vorgenommen, um die Kompatibilität mit vorhandenen PKI-Bereitstellungen und mit auf OpenSSL oder GnuTLS basierender Software zu gewährleisten.

Das ca-certificates Paket beinhaltet jetzt auch den **`ca-legacy`**-Befehl, der für die Aktivierung der erwähnten Kompatibilitätsänderungen verwendet weden kann. Auf der ca-legacy(8) man-Seite finden Sie weitere Informationen zur Verwendung des Befehls.

Benutzer, die die Legacy-Änderungen deaktivieren möchten, sollten den Knowledge Base Artikel 1413643 lesen, der Informationen zu diesen Änderungen liefert und mögliche Folgen von deren Deaktivierung nennt.

Beachten Sie, dass der CA-Speicher für die Verwendung des **`ca-legacy`**-Befehls erforderlich ist. Auf der update-ca-trust(8) man-Seite erfahren Sie, wie Sie den vereinheitlichten CA-Speicher aktivieren.

Support für unidirektionale Vertrauensmodelle

Identitätsverwaltung erlaubt es dem Benutzer jetzt, unidirektionale Vertrauensmodelle mit dem **`ipa trust-add`**-Befehl zu konfigurieren.

`openldap` Überarbeitung auf Version 2.4.40

Die *openldap*-Pakete wurden auf Upstream-Version 2.4.40 aktualisiert und bieten eine Reihe von Fehlerbehebungen sowie eine Verbesserung gegenüber der vorherigen Version. Insbesondere wurde die Reihenfolge übereinstimmender Regeln den **`ppolicy`**-Attributstypbeschreibungen hinzugefügt. Die Fehlerbehebungen umfassen unter anderem: Der Server beendet die Bearbeitung von SRV-Einträgen nicht mehr unerwartet, und es wurden fehlende **`objectClass`**-Informationen hinzugefügt, so dass der Benutzer die Front-end-Konfiguration standardmäßig bearbeiten kann.

Cache-Authentifizierung in SSSD

Die Authentifizierung beim Cache ohne Wiederverbindungsversuch ist jetzt sogar im Online-Modus in SSSD verfügbar. Die wiederholte Authentifizierung beim Netzwerkserver konnte zu einer exzessiven Applikationslatenz führen und den Anmeldeprozess ausgesprochen zeitaufwänding machen.

SSSD aktiviert UID- und GID-Mapping an individuellen Clients

Es ist jetzt möglich, Benutzer durch Konfiguration auf Clientseite mittels SSSD bei bestimmten Red Hat Enterprise Linux Clients zu unterschiedlichen UID und GID zu mappen. Diese Möglichkeit der clientseitigen Außerkraftsetzung kann durch UID- und GID-Duplizierung verursachte Probleme beheben .

SSSD kann jetzt den SSH-Zugriff auf gesperrte Accounts verweigern

In der Vergangenheit, als SSSD noch OpenLDAP als seine Authentifizierungsdatenbank verwendete, konnten sich Benutzer erfolgreich mittels eines SSH-Schlüssels beim System authentifizieren, selbst

nachdem das Account gesperrt worden war. Der **`ldap_access_order`**-Parameter akzeptiert jetzt den **`ppolicy`**-Wert, der in der beschriebenen Situation dem Benutzer den SSH-Zugriff verweigern kann. Weitere Informationen zur Verwendung von **`ppolicy`** finden Sie in der **`ldap_access_order`**-Beschreibung auf der sssd-ldap(5) man-Seite.

Das sudo-Dienstprogramm kann jetzt den Befehl checksum prüfen

Die Konfiguration des sudo-Dienstprogramms kann jetzt die Prüfsumme eines Befehls oder Skripts das genehmigt wird speichern. Werden der Befehl oder das Skript erneut ausgeführt, so wird die Prüfsumme mit der gespeicherten Prüfsumme verglichen und so überprüft, dass sich nichts verändert hat. Bei Änderungen am Befehl oder der Binärdatei verweigert das sudo-Dienstprogramm die Ausführung des Befehls oder protokolliert eine Warnung. Diese Funktionalität gestattet die korrekte Übertragung von Verantwortlichkeit sowie die Fehlerbehebung, falls ein Problem auftritt.

SSSD Smartcard-Support

SSSD unterstützt jetzt Smartcards für die lokale Authentifizierung. Mit diesem Feature kann der Benutzer eine Smartcard beim System mittels einer textbasierten oder grafischen Konsole sowie lokale Dienste wie den sudo-Dienst verwenden. Der Benutzer platziert die Smartcard im Reader und gibt bei der Anmeldeaufforderung den Benutzernamen und die Smartcard-PIN ein. Wird das Zertifikat der Smartcard verifiziert, so ist der Benutzer erfolgreich authentifiziert.

Beachten Sie, dass SSSD dem Benutzer derzeit nicht den Erhalt eines Kerberos-Tickets mittels einer Smartcard ermöglicht. Für den Erhalt eines Kerberos-Tickets ist nach wie vor die Authentifizierung mittels des kinit-Dienstprogramms erforderlich.

Unterstützung mehrerer Profil-Zertifikate

Identitätsverwaltung unterstützt jetzt mehrere Profile für das Herausgeben von Server- und anderen Zertifikaten, statt nur ein Einzelserver-Zertifikatsprofil. Die Profile sind im Certificate System gespeichert.

Passwort-Vault

Ein neues Feature ermöglicht die sichere und zentrale Speicherung von privaten Benutzerdaten wie Passwörtern, und der Identitätsverwaltung wurden Schlüssel hinzugefügt. Der Passwort-Vault befindet sich auf dem Public Key Infrastructure (PKI) Key Recovery Authority (KRA) Subsystem.

DNSSEC-Support bei der Identitätsverwaltung

Identitätsverwaltungsserver mit integriertem DNS unterstützen jetzt DNS Security Extensions (DNSSEC), einen Satz von Erweiterungen zu DNS, die die Sicherheit des DNS-Protokolls verbessern. DNS-Zonen auf Identitätsverwaltungsservern können mittels DNSSEC automatisch unterschrieben werden. Die kryptografischen Schlüssel werden automatisch generiert und rotiert.

Benutzer, die ihre DNS-Bereiche mit DNSSEC sichern, sollten die folgenden Dokumente lesen und befolgen:

DNSSEC Betriebliche Praxis, Version 2: http://tools.ietf.org/html/rfc6781#section-2

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

Beachten Sie, dass Identitätsverwaltungsserver mit integriertem DNS DNSSEC zur Validierung von DNS-Antworten anderer DNS-Server verwenden. Dies kann Einfluss auf die nicht in Übereinstimmung mit den im 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 empfohlenen Namensgebungspraktiken konfigurierten DNS-Zonen haben.

Kerberos HTTPS Proxy in Identitätsverwaltung

Eine vollständig mit der Microsoft Kerberos KDC Proxy Protocol (MS-KKDCP) Implementierung kompatible Key Distribution Center (KDC) Proxy-Funktion ist jetzt in der Identitätsverwaltung verfügbar und erlaubt Clients den Zugriff auf KDC- und **kpasswd**-Dienste mittels HTTPS. Systemadministratoren können das Proxy jetzt am Netzwerkrand mit einem einfachen HTTPS-Reverse-Proxy offenlegen, ohne eine dedizierte Applikation einzurichten und zu verwalten.

Aktualisierungen im Hintergrund für gecachte Einträge

SSSD erlaubt nun die Out-of-Band-Aktualisierung gecachter Einträge im Hintergrund. Vor dieser Aktualisierung rief SSSD nach Ablauf der Gültigkeit gecachter Einträge, diese vom Remote-Server ab und speicherte diese erneut in der Datenbank, was zeitaufwändig war. Durch diese Aktualisierung werden Einträge sofort wiedergegeben, da das Back-End diese kontinuierlich aktualisiert. Beachten Sie, dass dies zu einer höheren Serverauslastung führt, da SSSD die Einträge periodisch herunterlädt statt nur auf Anfrage.

Caching für `initgroups`-Vorgänge

Das SSSD Fast Memory Cache unterstützt jetzt **initgroups**-Vorgänge, was die Bearbeitung von initgroups sowie die Performance mancher Applikationen wie GlusterFS und **slapi-nis** verbessert.

Mit `mod_auth_gssapi` optimierte Authentifizierung

Identitätsverwaltung verwendet jetzt das **mod_auth_gssapi**-Modul, welches GSSAPI-Aufrufe statt der direkten Kerberos-Aufrufe des früheren **mod_auth_kerb**-Moduls verwendet.

Benutzer-Lebenszyklusverwaltung

Die Benutzer-Lebenszyklusverwaltung verleiht dem Administrator eine größere Kontrolle hinsichtlich der Aktivierung und Deaktivierung von Benutzerkonten. Der Administrator kann jetzt neue Benutzerkonten bereitstellen, indem er diese einem speziellen Bereich hinzufügt, ohne diese vollständig zu aktivieren, inaktive Benutzerkonten aktiviert und somit vollständig betriebsbereit macht oder aber Benutzerkonten deaktiviert, ohne sie jedoch vollständig aus der Datenbank zu löschen.

Die Benutzer-Lebenszyklusverwaltung bringt maßgebliche Vorteile für IdM-Bereitstellungen. Beachten Sie, dass Benutzer dem Stage-Bereich direkt von einem standardmäßigen LDAP-Client mittels direkter LDAP-Operationen hinzugefügt werden können. In der Vergangenheit gestattete IdM die Benutzerverwaltung nur mittels IdM-Befehlszeilen-Tools oder dem IdM-Web-UI.

SCEP-Support in `certmonger`

Der **certmonger**-Dienst wurde aktualisiert, um das Simple Certificate Enrollment Protocol (SCEP) zu unterstützen. Es ist jetzt möglich, ein neues Zertifikat auszustellen und zu erneuern oder bestehende Zertifikate über SCEP zu ersetzen.

Neue Pakete: ipsilon

Die *ipsilon*-Pakete liefern den Ipsilon Identity-Provider-Dienst für vereinten Single-Sign-on (SSO). Ipsilon verbindet Authentifizierungs-Provider und Applikationen oder Dienstprogramme, um SSO zu ermöglichen. Es umfasst einen Server und Dienstprogramme zur Konfiguration von Apache-basierten Dienstanbietern.

Benutzer-Authentifizierung für Ipsilon-geliefertes SSO wird gegen ein separates Identity Management System, wie einen Identity Management Server durchgeführt. Ipsilon kommuniziert über vereinte Protokolle wie SAML oder OpenID mit verschiedenen Applikationen und Dienstprogrammen.

NSS erhöht die akzeptierten Mindestwerte für Schlüsselstärken

Die Network Security Services (NSS) Bibliothek in Red Hat Enterprise Linux 7.2 akzeptiert weder Diffie-Hellman (DH) Key-Exchange-Parameter, die kleiner als 768 Bits sind noch RSA- und DSA-Zertifikate mit Schlüsselgrößen von weniger als 1023 Bits. Das Erhöhen der minimalen Schlüsselstärke verhindert Angriffe, die bekannte Sicherheitsschwachstellen wie Logjam (CVE-2015-4000) und FREAK (CVE-2015-0204) ausnutzen.

Beachten Sie, dass Verbindungsversuche mit einem Server mit Schlüsseln, die schwächer als die neuen Mindestwerte sind, jetzt fehlschlagen, selbst wenn solche Verbindungen in früheren Versionen von Red Hat Enterprise Linux funktionierten.

nss und nss-util überarbeitet auf Version 3.19.1

Die *nss*- und *nss-util*-Pakete wurden auf Upstream-Version 3.19.1 aktualisiert, das eine Reihe von Fehlerbehebungen und Verbesserungen gegenüber der vorherigen Version bietet. Insbesondere ermöglicht die Aktualisierung Benutzern das Upgrade auf die Mozilla Firefox 38 Extended Support Release und verhindert Angriffe, die die Logjam-Sicherheitsschwachstelle CVE-2015-4000 ausnutzen.

Apache-Modules für IdM jetzt voll unterstützt

Die folgenden Apache-Module für Identity Management (IdM), die in Red Hat Enterprise Linux 7.1 als Technologievorschau hinzugefügt waren, werden jetzt voll unterstützt: **`mod_authnz_pam`**, **`mod_lookup_identity`** und **`mod_intercept_form_submit`**. Die Apache-Module können von externen Applikationen verwendet werden, um eine engere Interaktion mit IdM über eine einfache Authentifizierung hinaus zu erreichen.

Kapitel 3. Clustering

systemd und pacemaker koordinieren jetzt ordnungsgemäß während das System heruntergefahren wird

In der Vergangenheit funktionierte die Koordination von systemd und pacemaker beim Herunterfahren des Systems nicht ordnungsgemäß, wodurch pacemaker-Ressourcen nicht korrekt beendet wurden. Dieses Update weist pacemaker dazu an, vor dbus und anderen systemd-Diensten zu stoppen, die pacemaker gestartet hatte. Dies ermöglicht es sowohl pacemaker als auch den von pacemaker verwalteten Ressourcen, ordnungsgemäß herunterzufahren.

Die `pcs resource move`- und `pcs resource ban`-Befehle zeigen jetzt einen Warnhinweis an, um das Verhalten der Befehle zu erläutern.

Der **`pcs resource move`**-Befehl und der **`pcs resource ban`**-Befehl schaffen Speicherorteinschränkungen, die die Ressource wirksam daran hindern am aktuellen Knoten zu laufen bis die Einschränkung entfernt wird oder deren Gültigkeitsdauer abläuft. Dieses Verhalten war Benutzern bis dato nicht bekannt. Bei diesen Befehlen wird jetzt ein Warnhinweis angezeigt, der auf dieses Verhalten hinweist und auch die Hilfsbildschirme und Dokumentation zu diesen Befehlen wurden für mehr Klarheit überarbeitet.

Neuer Befehl für das Verschieben einer Pacemaker-Ressource zum bevorzugten Knoten

Nachdem eine Pacemaker-Ressource entweder aufgrund eines Failover oder durch manuelles Verschieben des Knotens durch einen Administrator verschoben wurde, gelangt diese nicht notwendigerweise nach Korrektur der Umstände die zum Failover geführt hatten wieder an ihren Ursprungsknoten zurück. Sie können jetzt den **`pcs resource relocate run`**-Befehl dazu verwenden, um eine Ressource (je nach aktuellem Cluster-Status, Einschränkungen, Speicherort der Ressourcen und anderen Einstellungen) an ihren bevorzugten Knoten zu verschieben. Mit dem **`pcs resource relocate show`**-Befehl können Sie außerdem die migrierten Ressourcen anzeigen. Informationen zu dieser Ressource finden Sie in der High Availability Add-On Referenz.

Support für clufter-Befehl für die Transformation und Analyse von Cluster-Konfigurationsformaten

Der clufter-Befehl liefert ein Tool für die Transformation und Analyse von Cluster-Konfigurationsformaten. Der clufter-Befehl kann auch für die Migration von einer älteren Stack-Konfiguration zu einer neueren Konfiguration die Pacemaker nutzt. Weitere Informationen zum clufter-Befehl finden Sie auf der clufter(1) man-Seite oder der Ausgabe des **`clufter -h`**-Befehls.

Kapitel 4. Compiler und Werkzeuge

tail --follow funktioniert jetzt ordnungsgemäß bei Dateien im Veritas Clustered Dateisystem (VXFS)

Das Veritas Clustered Dateisystem (VXFS) ist ein Remote-Dateisystem, und für Remote-Dateisysteme kann **`tail`** die »inotify« Funktionalität für den »--follow«-Modus nicht verwenden. Das Veritas Clustered Dateisystem wurde nun der Liste von Remote-Dateisystemen hinzugefügt, für die der Polling-Modus statt »inotify« verwendet wird. Daher funktioniert **`tail --follow`** jetzt selbst bei Anwendung an Dateien auf VXFS ordnungsgemäß.

Der dd-Befehl kann jetzt den Übertragungsfortschritt anzeigen

Der für das Kopieren von Dateien nach Bytes verwendete **dd**-Befehl bietet jetzt die »status=progress«-Option, um den Fortschritt der Übertragung anzuzeigen. Dies ist besonders bei der Übertragung großer Dateien nützlich, da es dem Benutzer gestattet, die ungefähre Dauer abzuschätzen und mögliche Probleme bei der Übertragung zu erkennen.

Verbesserte Wartezeiten in libcurl

Die **`libcurl`**-Bibliothek verwendete eine unnötig lange Blocking-Verzögerung für Aktionen ohne aktive Dateideskriptoren, selbst für kurze Vorgänge. Dies bedeutete, dass manche Vorgänge wie etwa das Auflösen eines Host-Namens mittels **`/etc/hosts`** unnötig viel Zeit in Anspruch nahmen. Der Blocking-Code in **`libcurl`** wurde jetzt bearbeitet, so dass die anfängliche Verzögerung kurz ist und sich graduell erhöht, bis ein Ereignis stattfindet. Schnelle **`libcurl`**-Vorgänge werden jetzt auch schneller abgeschlossen.

Die libcurl-Bibliothek implementiert jetzt einen nicht sperrenden SSL-Handshake

In der Vergangenheit implementierte die **`libcurl`**-Bibliothek keinen nicht sperrenden SSL-Handshake, was negative Auswirkungen auf die Performance von auf dem **`libcurl`**-Multi-API basierenden Applikationen hatte. Um dieses Problem zu beheben, wurde der nicht sperrende SSL-Handshake in **`libcurl`** implementiert und das **`libcurl`**-Multi-API gibt die Kontrolle nun sofort an die Applikation zurück, wenn es Daten vom zu Grunde liegenden Netzwerk-Socket nicht lesen oder schreiben kann.

GDB auf IBM Power Systemen schlägt beim Zugriff auf die Symboltabelle nicht mehr fehl

In der Vergangenheit hob GDB bei 64-bit IBM Power Systemen inkorrekter Weise die Zuteilung einer wichtiger Variablen auf, die die Symboltabelle der Binärdatei enthielt bei der die Fehlerbehebung stattfand, wodurch ein Segmentierungsfehler auftrat, wenn GDB versuchte, auf diese Symboltabelle zuzugreifen. Um dieses Problem zu beheben wurde diese bestimmte Variable persistent gemacht und GDB kann nun später im Fehlerbehebungsprozess auf die benötigten Informationen zugreifen, ohne einen ungültigen Bereich des Arbeitsspeichers zu lesen.

nscd aktualisiert, so dass Konfigurationsdaten jetzt automatisch neu geladen werden

Diese Aktualisierung des Name Server Caching Daemon (nscd) fügt ein System von inotify-basierter Überwachung und stat-basierter Sicherungsüberwachung für nscd-Konfigurationsdateien hinzu, so dass nscd-Änderungen an seiner Konfiguration jetzt ordnungsgemäß auffindet und die Daten neu lädt. Dies hindert nscd daran, veraltete Daten wiederzugeben.

Die dlopen-Bibliothek stürzt bei rekursiven Aufrufen nicht mehr ab

In der Vergangenheit konnte ein Fehler in der Bibliotheksfunktion **dlopen** dazu führen, dass rekursive Aufrufe an diese Funktion mit Bibliotheksaussage abstürzten oder abgebrochen wurden. Rekursive Aufrufe sind möglich, wenn eine vom Benutzer bereitgestellte **malloc**-Implementierung **dlopen** aufruft.

Die Implementierung ist jetzt ablaufinvariant und rekursive Aufrufe stürzen jetzt bei einer Aussage weder ab noch werden sie abgebrochen.

Das operf-Tool erkennt jetzt statische Huge-Page-Bezeichner

Beim Profiling der Leistung von per JIT (just-in-time) kompiliertem Java-Code mit aktivierten statischen Huge-Pages, meldete der operf-Befehl von OProfile einen hohen Prozentsatz von Zeit an den anonymen Arbeitsspeicher (in anon_hugepage) statt im perf-Bericht. Operf erkennt jetzt die statischen Huge-Page-Bezeichner und mappt Samples korrekt zu Java-Methoden, wenn statisch zugeteilte Huge-Pages verwendet werden.

Der rsync -X-Befehl funktioniert jetzt ordnungsgemäß

In der Vergangenheit wechselte das rsync-Tool den Dateibesitzer nach (nicht vor) dem Einstellen der Sicherheitsattribute. Die Folge war, dass die Sicherheitsattribute am Ziel fehlten und der **rsync -X**-Befehl unter bestimmten Umständen nicht ordnungsgemäß funktionierte. Diese Aktualisierung ändert die Reihenfolge der Vorgänge und rsync ändert jetzt den Eigentümer, ehe die Sicherheitsattribute eingestellt werden. Die Sicherheitsattribute sind in der beschriebenen Situation jetzt wie erwartet vorhanden.

Subversion-Anwendungsdateien jetzt mit vollständgen RELRO-Daten erstellt

Die mit diesem *subversion*-Paket gelieferten ausführbaren Dateien bieten jetzt schreibgeschützte Relocation Data (RELRO), welche Schutz vor bestimmten Types von Angriffen auf Arbeitsspeicher bieten. Dadurch ist es schwieriger Subversion auszunutzen, wenn zukünftige Schwachstellen aufgedeckt werden.

Die Thread-Erweiterung funktioniert jetzt ordnungsgemäß

In der Vergangenheit war der Threading-Support in Tool Command Language (TCL) nicht optimal implementiert. Wurde der Fork()-Aufruf mit der im TLC-Interpreter aktivierten Thread-Erweiterung verwendet, so konnte es vorkommen, dass der Prozess nicht mehr reagierte. Deshalb wurden in der Vergangenheit der TCL-Interpreter und die TK-Applikation mit deaktivierter Thread-Erweiterung geliefert. Die Folge war, dass Applikationen von Drittanbietern, die von threaded TCL oder TK abhingen, nicht ordnungsgemäß funktionierten. Ein Patch zur Behebung dieses Fehlers wurde implementiert, und die Thread-Erweiterung bei TCL und TK ist jetzt standardmäßig aktiviert.

Kapitel 5. Desktop

GNOME 3.14

Das **GNOME Desktop** wurde auf Upstream-Version 3.14 aktualisiert, das neue Features und eine Reihe von Verbesserungen enthält. Darunter:

Eine Reihe von Features wurde dem **Wayland** Windowing-Protokoll hinzugefügt, darunter Tastaturkonfiguration, Touch-Screen-Support, Support für das Ziehen und Ablegen, funktionale Kontextmenüs, Tool-Tipps und Comboboxes, Display-Support mit hoher Auflösung und Verschieben sowie Größenänderung von Fenstern.

Multitouch-Gesten können jetzt an Touchscreens für die Systemnavigation sowie in Applikationen verwendet werden. Gesten können zum Öffnen der Aktivitäten-Übersicht, der Applikationsansicht und dem Nachrichtenfeld sowie zum Wechsel von Applikationen und Arbeitsflächen verwendet werden.

GNOME 3.14 bietet verbesserten Support für WLAN-Hotspots. Bei der Verbindung mit einem WLAN-Portal, das Authentifizierung erfordert zeigt GNOME automatisch die Anmeldeseite als Teil des Verbindungsvorgangs an.

Personal **File Sharing (WebDAV)**, **Media Sharing (DLNA)** und **Screen Sharing (VNC)** speichern jetzt, an welchem Netzwerk sie aktiv sein sollen. Außerdem bieten die »Einstellungen« jetzt die Möglichkeit zu steuern, an welchen Netzwerken Freigaben erfolgen. Dieses Feature verhindert die Freigabe von Content und Diensten an öffentlichen Orten.

Bei der Verwendung mehrerer Bildschirme stellt GNOME 3.14 Displays in ihrer ursprünglichen Position wieder her, wenn Bildschirme getrennt und wieder angeschlossen werden.

Die GNOME-Applikation für virtuelle und Remote-Maschinen **Boxes** führt Snapshots ein. Außerdem liefern **Boxes** jetzt automatischen Download, das Ausführen mehrerer Boxes in separaten Fenstern und Verbesserungen bei der Benutzeroberfläche ein, darunter verbessertes Verhalten im Vollbildmodus und bei Vorschaubildern.

GTK+ 3.14 beinhaltet eine Reihe von Fehlerbehebungen und Verbesserungen, wie das automatische Laden von Menüs aus Ressourcen, Mehrauswahl-Support in **GtkListBox**, Property-Bindings in **GtkBuilder**-Dateien, Support bei der Widget-Zuordnung (gtk_widget_set_clip()), neue Transitionstypen in GtkStack sowie das Laden und Speichern von Dateien mit **GtkSourceView**. Außerdem liefert **GTK+** jetzt Support für Gesten-Interaktion. Mit 3.14 ist nun die Mehrzahl an Multitouch-Gesten in GTK+ Applikationen verfügbar, so etwa Tippen, Ziehen, Streichen, Zusammenziehen und Drehen. Gesten können vorhandenen GTK+-Applikationen mittels **GtkGesture** hinzugefügt werden.

GLib 3.14 bietet jetzt Support für die neue MIME Applications Associations Spezifikation, SHA-512 Support in GHmac, Support für Implementierungen in Desktop-Dateien und Unicode 7.0 Support.

Der GNOME **Help**-Dokumentation-Browser wurde neu entworfen, um konsistent mit anderen GNOME 3 Applikationen zu sein. Die Hilfe verwendet jetzt eine Kopfleiste und bietet eine integrierte Suchfunktion sowie eine Oberfläche für Lesezeichen.

Die GNOME-Shell-Erweiterung **Looking Glass Inspector** bietet eine Reihe von Features für Entwickler: Anzeige aller Methoden, Klassen usw. in einem Namensraum bei Untersuchung, Objekt-Inspektor Verlaufserweiterung oder das Kopieren von Looking Glass Ergebnissen als Strings und Weitergabe von Ereignissen an gnome-shell.

Das ibus-gtk2-Paket aktualisiert jetzt die immodules.cache-Datei

In der Vergangenheit suchte das **`update-gtk-immodules`**-Skript nach einem nicht mehr vorhandenen **`/etc/gtk-2.0/$host`**-Verzeichnis. Die Folge war, dass das Post-Installationsskript des *ibus-gtk2*-Pakets fehlschlug und ohne das Cache zu erstellen oder zu aktualisieren beendete. Das Post-Installationsskript wurde nun geändert und ersetzt **`update-gtk-immodules`** durch **`gtk-query-immodules-2.0-BITS`**, so dass das Problem nicht mehr auftritt.

Kapitel 6. Dateisysteme

gfs2-utils überarbeitet auf Version 3.1.8

Das *gfs2-utils*-Paket wurde auf Version 3.1.8 überarbeitet, das wichtige Fehlerbehebungen und eine Reihe von Verbesserungen liefert:

* Die Performance der **`fsck.gfs2`**-, **`mkfs.gfs2`**- und **`gfs2_edit`**-Dienstprogramme wurde verbessert.

* Das **`fsck.gfs2`**-Dienstprogramm führt jetzt eine bessere Überprüfung von Journals, des jindex, System-inodes und der inode »goal«-Werte durch.

* Die **`gfs2_jadd`**- und **`gfs2_grow`** -Dienstprogramme sind jetzt separate Programme statt symlinks zu **`mkfs.gfs2`**.

* Die Testsuite und verwandte Dokumentation wurden verbessert.

* Das Paket ist nicht mehr von Perl abhängig.

GFS2 hindert Benutzer jetzt daran ihre Kontingente zu überschreiten

Bislang prüfte GFS2 nur nach Beendigung von Vorgängen auf Kontingentverletzungen, was dazu führen konnte, dass Benutzer oder Gruppen ihre zugewiesenen Kontingente überschritten. Dieses Verhalten wurde korrigiert und GFS2 sagt jetzt voraus, wieviele Blocks ein Vorgang zuteilen würde und prüft, ob diese Zuteilung Kontingente überschreiten würde. Vorgänge, die Kontingente überschreiten würden, werden nicht gestattet und Benutzer überschreiten nun nie die ihnen zugeteilten Kontingente.

XFS überarbeitet auf Version 4.1

XFS wurde auf Upstream-Version 4.1 aktualisiert, einschließlich kleinerer Fehlerbehebungen, Neuordnungen, Überarbeitungen bestimmter interner Mechanismen, wie Protokollierung, pcpu-Berechnungen und neues mmap-Sperren. Zusätzlich zu den Upstream-Änderungen erweitert diese Aktualisierung die rename()-Funktion um cross-rename (eine symmetrische Variante von rename()) und die Whiteout-Verarbeitung.

ext4- und jbd2-Upgrade

Die ext4- und jbd2-Geräte wurde zur aktuellsten Upstream-Version aktualisiert, das eine Reihe von Fehlerbehebungen und Verbesserungen gegenüber der vorherigen Version bietet.

cifs überarbeitet auf Version 3.17

Das CIFS-Modul wurde auf Upstream-Version 3.17 aktualisiert, das verschiedene kleinere Fehlerbehebungen und neue Features für Server Message Block 2 und 3 (SMB2 und SMB3) liefert.

Kapitel 7. Allgemeine Aktualisierungen

lftp handhabt 302-Umleitung jetzt ordnungsgemäß

lftp wurde aktualisiert und handhabt 302-Umleitung jetzt ordnungsgemäß, wenn es im Mirror-Modus läuft. In der Vergangenheit stoppte lftp mit einem Fehler.

Mehr diagnostische Informationen und ein umbenanntes Plug-in für sosreport

Das sosreport-Tool wurde verbessert und sammelt prozessbezogene Informationen von verschiedenen Applikationen, einschließlich ptp, lastlog und ethtool. Als Teil dieser Änderungen wurde das **`startup`**-Plug-in in **`services`** umbenannt, damit diese Funktion deutlicher erkennbar ist.

Kapitel 8. Installation und Bootvorgang

Netzwerkeinrichtung in initrd behoben, wenn Netzwerkkonfiguration in Kickstart bereitgestellt wird

Wenn in der Vergangenheit der Installer Netzwerkschnittstellen nicht einrichtete oder in **`initrd`** neu konfigurierte, so wurden diese Schnittstellen in Kickstart-Dateien definiert. Dies konnte zum Fehlschlagen der Installation und dem Wechsel in den Rettungsmodus führen, wenn von anderen Befehlen in der Kickstart-Datei Netzwerkzugriff erfordert wurde.

Dieses Problem ist behoben, so dass Anaconda die Netzwerkkonfiguration jetzt von Kickstart-Dateien in **`initrd`** ab einem frühen Zeitpunkt im Boot-Prozess ordnungsgemäß handhabt.

Anaconda unterstützt jetzt das Erstellen gecachter Logical Volumes

Der Installer unterstützt jetzt das Erstellen gecachter LVM Logical Volumes und das Installieren des Systems auf diesen Volumes.

Diese Vorgehensweise wird nur in Kickstart unterstützt. Um ein gecachtes Logical Volume zu erstellen, verwenden Sie die neuen **`--cachepvs=`**-, **`--cachesize=`**- und **`--cachemode=`**-Optionen des **`logvol`**-Kickstart-Befehle.

Ausführliche Informationen zu diesen neuen Optionen finden Sie im Red Hat Enterprise Linux 7 Installationshandbuch.

Verbessertes Sortieren von GRUB2-Bootmenü

Ein Problem mit dem vom **`grub2-mkconfig`**-Befehl verwendeten Sortiermechanismus konnte dazu führen, dass die grub.cfg-Konfigurationsdatei mit inkorrekt sortierten verfügbaren Kernels generiert wurde.

GRUB2 verwendet jetzt das *rpmdevtools*-Paket für das Sortieren verfügbarer Kernels und die Konfigurationsdatei wird ordnungsgemäß generiert, wobei die aktuellste Kernelversion ganz oben erscheint.

Anaconda setzt Disk-Aktionen jetzt ordnungsgemäß zurück, wenn die Diskauswahl sich ändert

In der Vergangenheit setzten Anaconda und Blivet auf Disks geplante Aktionen nicht ordnungsgemäß zurück, wenn die Diskauswahl verändert wurde, wodurch es zu verschiedenen Problemen kam. In dieser Aktualisierung wurde dies bei Anaconda behoben, so dass ein Snapshot der Original-Speicherkonfiguration erstellt wird und bei Änderungen der Diskauswahl darauf zurückgegriffen wird, so dass alle für Disks geplante Aktionen rückgängig gemacht werden.

Verbesserte Erkennung von device-mapper Disknamen

In der vorherigen Release von Red Hat Enterprise Linux 7 konnte es vorkommen, dass der Installer bei der Installation auf Disks abstürzte, die zuvor LVM Logical Volumes enthielten wenn die Metadaten für diese Volumes noch vorhanden waren. Der Installer erkannte die korrekten **`device-mapper`**-Namen nicht und das Erstellen von neuen LVM Logical Volumes schlug fehl.

Die Methode für den Erhalt von **`device-mapper`**-Gerätenamen wurde aktualisiert und die Installation auf Disks, die vorhandene LVM-Metadaten enthalten, ist jetzt zuverlässiger.

Korrigierte Handhabung von PReP-Boot während der Partitionierung

Unter bestimmten Umständen konnte die **PReP Boot**-Partition bei IBM Power Systems während der benutzerdefinierten Partitionierung auf eine ungültige Größe eingestellt werden. In dieser Situation führte das Entfernen einer Partition zum Absturz des Installers.

Überprüfungen sind jetzt in *anaconda* implementiert um sicherzustellen, dass die Partition stets die korrekte Größe zwischen **4096 KiB** und **10 MiB** besitzt. Außerdem ist es nicht mehr notwendig, das Format der **PReP Boot**-Partition zu ändern, um deren Größe zu ändern.

EFI-Partitionen auf RAID1-Geräten

EFI-Systempartitionen können jetzt auf einem RAID1-Gerät erstellt werden,um bei einem Fehlschlagen der Boot-Disk die Wiederherstellung des Systems zu ermöglichen. Falls jedoch **Boot####** und **BootOrder** und das Volume des von der Firmware erkannten ESP korrumpiert werden, dieses aber nach wie vor als gültiges ESP erscheint, so wird die Boot-Reihenfolge nicht automatisch neu erstellt. Das System sollte von der zweiten Disk jedoch trotzdem manuell booten.

Installation im Textmodus stürzt während der Netzwerkkonfiguration nicht mehr ab

In der Vergangenheit konnte es vorkommen, dass bei Verwendung eines Leerzeichens bei der Angabe von Namensservern im Bildschirm zur Netzwerkkonfiguration im interaktiven Textmodusinstaller der Installer abstürzte.

Anaconda handhabt jetzt Namensserver-Definitionen im Textmodus ordnungsgemäß und der Installer stürzt nicht mehr ab, wenn ein Leerzeichen zur Trennung von Namensserver-Adressen verwendet wird.

Die Bildschirme im Wiederherstellungsmodus bei IBM System z werden nicht mehr abgeschnitten

In der Vergangenheit wurden der zweite und dritte Bildschirm im Wiederherstellungsmodus bei IBM System z Servern nicht ordnungsgemäß angezeigt, und Teile der Oberfläche waren abgeschnitten. Der Wiederherstellungsmodus bei dieser Architektur wurde verbessert und alle Bildschirme funktionieren jetzt ordnungsgemäß.

OpenSCAP Add-on in Anaconda

Es ist jetzt möglich, Security Content Automation Protocol (SCAP) Inhalte während des Installationsprozesses anzuwenden. Dieser neue Installer Add-on bietet eine zuverlässige und bequeme Weise eine Sicherheitsrichtlinie zu konfigurieren, ohne von benutzerdefinierten Skripten abhängig zu sein.

Dieses Add-on bietet einen neuen Kickstart-Abschnitt (»%addon org_fedora_oscap«) sowie einen neuen Bildschirm in der grafischen Benutzeroberfläche während der interaktiven Installation. Alle drei Teile sind im Red Hat Enterprise Linux 7 Installationshandbuch dokumentiert.

Das Anwenden von Sicherheitsrichtlinien während der Installation führt während und nach der Installation zu verschiedenen Änderungen, je nachdem, welche Richtlinie Sie aktivieren. Wird ein Profil gewählt, so wird das *openscap-scanner*-Paket (ein OpenSCAP-Konformitäts-Scanning-Tool) Ihrer Paketauswahl hinzugefügt und ein erstmaliger Scan im Hinblick auf Konformität wird nach Beendigung der Installation durchgeführt. Die Ergebnisse des Scans werden in **/root/openscap_data** gespeichert.

Durch das *scap-security-guide*-Paket werden mehrere Profile auf Installationsmedien bereitgestellt. Sie können falls notwendig auch andere Inhalte als Datastream, Archiv oder RPM-Paket von einem HTTP-, HTTPS- oder FTP-Server laden.

Beachten Sie, dass das Anwenden einer Sicherheitsrichtlinie nicht bei allen Systemen notwendig ist. Dieser Add-on sollte nur verwendet werden, wenn eine spezifische Richtlinie auf Grund der Regeln Ihres Unternehmens oder Regierungsauflagen zwingend erforderlich ist. Andernfalls kann der Add-on in seinem Standardstatus belassen werden und es muss keine Sicherheitsrichtlinie angewendet werden.

Es kommt beim Warten auf eine Kickstart-Datei auf einer CD oder DVD nicht mehr zu einer Zeitüberschreitung bei Anaconda.

Wenn in der Vergangenheit Anaconda zum Laden einer Kickstart-Datei aus optischen Medien mittels **`inst.ks=cdrom:/ks.cfg`**-Befehl konfiguriert war und das System auch von einer CD oder DVD gebootet wurde, so wartete der Installer kurze Zeit, bis die Disk gewechselt wurde. Dieses Zeitfenster war standardmäßig ziemlich kurz - nur 30 Sekunden. Nach Ablauf dieser Zeit wechselte das System in den Rettungsmodus.

Es wurden Änderungen an Anaconda vorgenommen, und es kommt nun beim Warten auf die Bereitstellung einer Kickstart-Datei auf einer CD oder DVD nicht mehr zu einer Zeitüberschreitung. Wird die **`inst.ks=cdrom`**-Boot-Option verwendet und die Kickstart-Datei wird nicht aufgefunden, so zeigt Anaconda nun eine Eingabeaufforderung an und wartet darauf, dass Sie die Datei bereitstellen oder neu booten.

Kapitel 9. Kernel

Zurücksetzen der Kernelparameter SHMMAX und SHMALL auf Standardwerte

In der Vergangenheit waren die Werte der **`kernel.shmmax`**- und **`kernel.shmall`**-Parameter, die in der **`/usr/lib/sysctl.d/00-system.conf`**-Datei eingestellt waren, zu niedrig. Dadurch funktionierten einige Anwendungen wie etwa SAP nicht ordnungsgemäß. Die unpassenden Außerkraftsetzungen wurden entfernt, und es werden nun die ausreichend hohen Kernelstandards verwendet.

Transparente Huge-Pages verursachen keine Fehler beim Arbeitsspeicher mehr

Transparente Huge-Pages wurden während Lese- und Schreibvorgängen nicht ordnungsgemäß synchronisiert. Unter bestimmten Umständen konnte dies zu Fehlern beim Arbeitsspeicher führen, wenn Huge-Pages aktiviert waren. Es wurden bei der Verarbeitung von Huge-Pages Arbeitsspeicherbarrieren hinzugefügt, um sicherzustellen, dass diese Fehler nicht mehr auftreten.

SCSI LIO Überarbeitung

Das SCSI-Kernelziel LIO wurde von Linux-4.0.stable überarbeitet. Dies beinhaltet zahlreiche Fehlerbehebungen, insbesondere für iSER, umfasst aber auch Support für XCOPY-, WRITE SAME- und ATS-Befehle und für DIF-Datenintegrität.

makedumpfile unterstützt jetzt das neue sadump-Format, das bis zu 16 TB an physischem Speicher darstellt

Der makedumpfile-Befehl unterstützt nun das neue sadump-Format, das mehr als 16 TB physischen Speichers darstellen kann. Dies erlaubt es Benutzern von makedumpfile, Dump-Dateien über 16 TB zu lesen, die von sadump auf bestimmten aufkommenden Servermodellen generiert werden.

Beim Entfernen oder dem Upgrade des Kernel wird keine Warnung mehr angezeigt

Das weak-modules-Skript, das von **`kmod`** zur Verwaltung von kABI-kompatiblen symbolischen Modul-Links verwendet wird, entfernte in der Vergangenheit das **`/lib/modules/<version>/weak-updates`**-Verzeichnis, wenn mit einem Kernel assoziierte Dateien entfernt wurden. Dieses Verzeichnis gehört dem *kernel*-Paket und dessen Entfernung verursachte eine Inkonsistenz zwischen dem Dateisystem und dem vom **`rpm`** erwarteten Status. Dadurch wurde jedes Mal wenn ein Kernel-Upgrade oder eine Kernel-Entfernung durchgeführt wurde, ein Warnhinweis angezeigt.

Das Skript wurde aktualisiert und entfernt nun die Inhalte des **`weak-updates`**-Verzeichnisses, belässt aber das Verzeichnis selbst, so dass keine Warnungen mehr gemeldet werden.

Neues Paket: libevdev

Bei Libevdev handelt es sich um eine Bibliothek auf niedriger Ebene für das Linux-Kernel Eingabegerät-Interface. Es liefert sichere Schnittstellen zur Abfrage von Gerätefähigkeiten und Prozessereignissen von Geräten. Aktuelle Versionen von xorg-x11-drv-evdev und xorg-x11-drv-synaptics benötigen diese Bibliothek als Abhängigkeit.

»Tuned« kann jetzt im no-daemon-Modus laufen

In der Vergangenheit konnte »Tuned« nur als Daemon laufen, was wegen der Auswirkungen auf den Arbeitsspeicher die Leistung kleiner Systeme beeinflussen konnte. Mit dieser Aktualisierung wurde »Tuned« ein no-daemon-Modus hinzugefügt, der keinen lokalen Arbeitsspeicher erfordert. Der no-daemon-Modus ist standardmäßig deaktiviert, weil ein Großteil der Funktionalität von »Tuned« in diesem Modus fehlt.

Neues Paket: tuned-profiles-realtime

Das *tuned-profiles-realtime*-Paket wurde dem Red Hat Enterprise Linux Server und Red Hat Enterprise Linux für Real Time hinzugefügt. Es enthält ein Echtzeitprofil, das vom **tuned**-Dienstprogramm zur Durchführung von CPU-Isolation und IRQ-Feinabstimmung verwendet wird. Wird das Profil aktiviert, so liest es einen variablen Abschnitt, der die zu isolierenden CPUs festlegt und alle Threads, die verschoben werden können, von diesen CPU-Kernen verschiebt.

Multiqueue I/O-Scheduling mit blk-mq

Red Hat Enterprise Linux 7.2 beinhaltet einen neuen I/O-Scheduling-Mechanismus für mehrere Warteschlangen für als »blk-mq« bekannte Blockgeräte. Es kann die Performance verbessern, indem es bestimmten Gerätetreibern das Mappen von I/O-Anfragen zu mehreren Hardware- oder Software-Warteschlangen gestattet. Die bessere Performance resultiert aus einer Reduktion von Sperrkonflikten, wenn mehrere Threads I/O an einem einzelnen Gerät ausführen. Neuere Geräte, wie etwa Non-Volatile Memory Express (NVMe), nutzen die Vorteile dieses Features am besten, da sie nativen Support für mehrfache Hardware-Eingaben und Ausführungswarteschlangen und deren Performance-Eigenschaften mit geringer Latenz bieten. Die genauen Vorteile im Hinblick auf die Performance hängen wie immer von der genauen Hardware und Arbeitslast ab.

Das blk-mq Feature ist derzeit implementiert und standardmäßig bei den folgenden Treibern aktiviert: virtio-blk, mtip32xx, nvme und rbd.

Das verwandte Feature, scsi-mq, gestattet Small Computer System Interface (SCSI) Gerätetreibern die Verwendung der blk-mq-Infrastruktur. Das scsi-mq-Feature steht in Red Hat Enterprise Linux 7.2 als Technologievorschau zur Verfügung. Um scsi-mq zu aktivieren, legen Sie **scsi_mod.use_blk_mq=y** in der Kernel-Befehlszeile fest. Der Standardwert ist **n** (deaktiviert).

Das Device-Mapper (DM) Multipath-Ziel, das anfragenbasierte DM verwendet, kann ebenfalls für die Verwendung der blk-mq-Infrastruktur konfiguriert werden, wenn die **dm_mod.use_blk_mq=y**-Kerneloption festgelegt ist. Der Standardwert lautet **n** (deaktiviert).

Es kann von Nutzen sein **dm_mod.use_blk_mq=y** einzustellen, wenn die zugrundeliegenden SCSI-Geräte ebenfalls blk-mq verwenden, da es den Sperr-Overhead an der DM-Schicht verringert.

Um zu bestimmen, ob DM-Multipath blk-mq auf einem System verwendet, nutzen Sie cat an der Datei **/sys/block/dm-X/dm/use_blk_mq**, wobei **dm-X** durch das DM-Multipath-Gerät von Interesse ersetzt wird. Diese Datei ist schreibgeschützt und reflektiert was der allgemeine Wert in **/sys/module/dm_mod/parameters/use_blk_mq** zu dem Zeitpunkt war, als das DM-Multipath-Gerät erstellt wurde.

SCSI-Fehlermeldungen können jetzt bequem interpretiert werden

Frühere Kerneländerungen an der printk()-Funktion hatten zur Protokollierung von Small Computer System Interface (SCSI) Fehlermeldungen über mehrere Zeilen geführt. Es konnte beim Auftreten mehrerer Fehler über verschiedene Geräte schwierig werden, die Fehlermeldungen korrekt zu deuten. Diese Aktualisierung ändert den SCSI-Fehlerprotokollierungscode, so dass Fehlermeldungen die dev_printk()-Option verwenden, die jede Fehlermeldung mit dem Gerät assoziiert, das den Fehler generiert hat.

libATA-Subsystem und Treiber aktualisiert

Diese Aktualisierung bietet eine Reihe von Fehlerbehebungen und Verbesserungen des libATA-Subsystems und der Treiber.

Upgrade von FCoE und DCB

Fibre Channel over Ethernet (FCoE) und Data Center Bridging (DCB) Kernelkomponenten wurden auf die neuesten Upstream-Versionen aktualisiert, was eine Reihe von Fehlerbehebungen und Verbesserungen gegenüber der vorherigen Version bietet.

perf Überarbeitung auf Version 4.1

Es wurde ein Upgrade der perf-Pakete auf Upstream-Version 4.1 durchgeführt, das eine Reihe von Verbesserungen bei der Performance und Stabilität gegenüber der früheren Version bietet. Insbesondere fügt diese Überarbeitung Intel Cache QoS Monitoring und AMD IBS Ops Features hinzu und liefert Support für Intel Xeon v4, für komprimierte Kernelmodule, für parametrisierte Ereignisse und Support für die Festlegung der Breakpoint-Länge. Außerdem wurden dem perf-Tool eine Reihe von Optionen wie **`--system-wide`**, **`top -z`**, **`top -w`**, **`trace --filter-pids`** und **`trace --event`** hinzugefügt.

Support für TPM 2.0

Dieses Update fügt Support auf Treiberebene für Version 2.0 konforme Trusted Platform Module (TPM)-Geräte hinzu.

Turbostat liefert jetzt korrekte Ausgabe

In der Vergangenheit fand das turbostat-Tool heraus, ob das System den MSR-Gerätesupport hatte, indem es die /dev/cpu/0/msr-Datei für **`cpu0`** statt **`cpu`** las. Dies führte dazu, dass das Deaktivieren einer CPU die CPUs aus der turbostat-Ausgabe löschte. Dieser Fehler wurde behoben, und das Ausführen des **`turbostat ls`**-Befehls liefert jetzt die korrekte Ausgabe.

Intel Xeon v5 Prozessor-Support

Diese Verbesserung fügt dem turbostat-Tool Intel Xeon v5 Prozessor-Support hinzu.

Das zswap-Tool nutzt das zpool-API

In der Vergangenheit verwendete das zswap-Tool zbud direkt, einen Speicherpool, der komprimierte Seiten im Verhältnis von 2:1 (wenn voll) speichert. Diese Aktualisierung führt das zpool-API, das Zugriff auf die zbud- oder zsmalloc-Pools liefert: zsmalloc speichert komprimierte Seiten in potenziell höherer Dichte, wodurch mehr Speicher für hoch komprimierbare Seiten verfügbar ist. Diese Aktualisierung überträgt zsmalloc zu den /mm-Treibern, so dass zpool wie vorgesehen funktioniert.

Die /proc/pid/cmdline Dateilänge ist jetzt unbeschränkt

Die Grenze für die Dateilänge von /proc/pid/cmdline für den ps-Befehl war in der Vergangenheit im Kernel auf 4096 Zeichen hartkodiert. Diese Aktualisierung stellt sicher, dass die Länge von /proc/pid/cmdline unbegrenzt ist, was besonders nützlich bei der Auflistung von Prozessen mit langen Befehlszeilenargumenten ist.

Support für dma_rmb und dma_wmb wird jetzt bereitgestellt

Diese Aktualisierung führt zwei neue Typen von Primitiven für das Synchronisieren von Cache-kohärenten Lese- und Schreibvorgängen im Arbeitsspeicher, dma_wmb() und dma_rmb(), ein. Dieses Feature ist zur

angemessenen Verwendung in Treibern verfügbar.

Kapitel 10. Netzwerk

SNMP folgt jetzt ordnungsgemäß der clientaddr-Directive über IPv6

In der Vergangenheit betraf die **`clientaddr`**-Option in **`snmp.conf`** nur ausgehende Nachrichten, die über IPv4 versendet wurden. Ab dieser Release werden die ausgehenden IPv6-Nachrichten jetzt korrekt von der durch **`clientaddr`** festgelegten Schnittstelle versendet.

tcpdump unterstützt die Optionen -J, -j und --time-stamp-precision

Da der Kernel, glibc und libpcap nun APIs zum Erhalt von Timestamps im Nanosekundenbereich bieten, wurde tcpdump aktualisiert, um diese Funktionalität zu nutzen. Benutzer können nun abfragen, welche Timestamp-Quellen verfügbar sind (-J), eine bestimmte Timestamp-Quelle festlegen (-j) und Timestamps mit der gewünschten Auflösung anfordern (--time-stamp-precision).

TCP/IP-Upgrade

TCP-/IP-Stack wurde auf Upstream-Version 3.18 aktualisiert, was eine Reihe von Fehlerbehebungen und Verbesserungen gegenüber der vorherigen Version bietet. Insbesondere behebt diese Aktualisierung die TCP schnelle offene Erweiterung, die bei der Verwendung mit IPv6 jetzt wie erwartet funktioniert. Außerdem bietet diese Aktualisierung Support für optionales TCP-Autocorking und implementiert Data Center TCP (DCTCP).

Kapitel 11. Server und Dienste

Die ErrorPolicy-Direktive ist jetzt validiert

Die ErrorPolicy-Konfigurationsdirektive wurde beim Startup nicht validiert und es konnte ohne Warnung unbeabsichtigt eine standardmäßige Fehlerrichtlinie verwendet werden. Die Direktive wird jetzt beim Startup validiert und auf den Standard zurückgesetzt, wenn der konfigurierte Wert inkorrekt ist. Es wird die vorgesehene Richtlinie verwendet oder eine Warnmeldung wird protokolliert.

CUPS deaktiviert SSLv3-Verschlüsselung jetzt standardmäßig

In der Vergangenheit war es nicht möglich, SSLv3-Verschlüsselung im CUPS-Scheduler zu deaktivieren, so dass Angriffe gegen SSLv3 möglich waren. Um dieses Problem zu beheben, wurde das **`cupsd.conf`** **`SSLOptions`** Schlüsselwort um zwei neue Optionen erweitert: **`AllowRC4`** und **`AllowSSL3`**. Jede der beiden aktiviert das benannte Feature in **`cupsd`**. Die neuen Optionen werden auch in der **`/etc/cups/client.conf`**-Datei unterstützt. Sowohl RC4 als auch SSL3 werden jetzt standardmäßig für **`cupsd`** deaktiviert.

Cups gestattet jetzt das Unterstrich-Zeichen in Druckernamen

Der **`cups`**-Dienst gestattet es Benutzern jetzt, das Unterstrich-Zeichen (_) in lokalen Druckernamen zu verwenden.

Nicht benötigte Abhängigkeit wurde aus dem tftp-server-Paket entfernt

In der Vergangenheit wurde standardmäßig ein zusätzliches Paket installiert, wenn das *tftp-server*-Paket installiert wurde. Diese Aktualisierung entfernt die überflüssige Paketabhängigkeit und das nicht benötigte Paket wird bei der Installation von *tftp-server* nicht mehr standardmäßig installiert.

Die veraltete /etc/sysconfig/conman-Datei wurde entfernt

Vor der Einführung des **`systemd`**-Managers sollten verschiedene Grenzen für Dienste in der **`/etc/sysconfig/conman`**-Datei konfiguriert werden. Nach Migration zu **`systemd`** wird **`/etc/sysconfig/conman`** nicht mehr verwendet und wurde daher entfernt. Um Grenzen zu setzen und andere Daemon-Parameter wie LimitCPU=, LimitDATA=, oder LimitCORE= einzustellen, bearbeiten Sie die **`conman.service`**-Datei. Weitere Informationen finden Sie auf der systemd.exec(5) man-Seite. Außerdem wurde die neue Variable LimitNOFILE=10000 der **`systemd.service`**-Datei hinzugefügt. Diese Variable ist standardmäßig auskommentiert. Beachten Sie, dass nach Änderungen an der **`systemd`**-Konfiguration der **`systemctl daemon-reload`**-Befehl ausgeführt werden muss, damit die Änderungen wirksam werden.

Kapitel 12. Storage

Neue Optionen delay_watch_checks und delay_wait_checks in der multipath.conf-Datei

Ist ein Pfad nicht zuverlässig und die Verbindung fällt oft aus, so versucht multipathd trotzdem weiterhin, diesen Pfad zu verwenden. Die Zeitüberschreitung bei welcher multipathd erkennt, dass der Pfad nicht mehr zugänglich ist, beträgt 300 Sekunden, wodurch der Eindruck entstehen kann, dass multipathd festhängt.

Um dies zu beheben, wurden zwei neue Konfigurationsoptionen hinzugefügt: delay_watch_checks und delay_wait_checks. Stellen Sie delay_watch_checks darauf ein, für wieviele Zyklen multipathd den Pfad beobachten soll, wenn dieser online kommt. Sollte der Pfad mit dem zugewiesenen Wert fehlschlagen, so verwendet multipathd ihn nicht. multipathd verlässt sich in diesem Fall nur auf die delay_wait_checks-Option für die Information, wieviele aufeinanderfolgende Zyklen durchlaufen werden müssen, ehe der Pfad seine Gültigkeit wiedererlangt. Dies verhindert, dass unzuverlässige Pfade sofort wiederverwendet werden, wenn sie wieder online sind.

Neue config_dir-Option in der multipath.conf-Datei

Benutzer waren nicht dazu in der Lage, ihre Konfiguration auf /etc/multipath.conf und andere Konfigurationsdateien aufzuteilen. Dies hinderte Benutzer daran, eine einzige Hauptkonfigurationsdatei für alle ihre Rechner anzulegen und die rechnerspezifischen Konfigurationsinformationen in separate Konfigurationsdateien für jeden Rechner auszulagern.

Zu diesem Zweck wurde die neue Option config_dir in der Datei multipath.config hinzugefügt. Benutzer müssen die Option config_dir auf entweder einen leeren String oder einen vollständigen Verzeichnispfad ändern. Wenn die Option nicht leer ist, wird Multipath alle .conf-Dateien in alphabetischer Reihenfolge lesen. Die Konfigurationen werden dann genauso angewendet, als seien diese in /etc/multipath.conf enthalten. Falls diese Änderung nicht vorgenommen wird, lautet config_dir standardmäßig /etc/multipath/conf.d.

DM-Upgrade

Device Mapper (DM) wurde auf Upstream-Version 4.0 aktualisiert, was eine Reihe von Fehlerbehebungen und Verbesserungen gegenüber der vorherigen Version bietet. Diese Verbesserungen umfassen unter anderem eine DM Crypt-Performance sowie eine DM-Core-Aktualisierung für den Support des Multi-Queue Block I/O Warteschlangen-Mechanismus (blk-mq).

Neuer dmstats-Befehl zum Anzeigen und Verwalten von I/O-Statistiken für benutzerdefinierte Bereiche von Geräten, die den device-mapper-Treiber verwenden.

Der **`dmstats`**-Befehl liefert Benutzerbereich-Support für device-mapper I/O-Statistiken. Dies erlaubt Benutzern das Erstellen, Verwalten und Erstellen von Berichten zu I/O-Zählern, Metriken und Latenzhistogramm-Daten für arbiträre Bereiche von device-mapper-Geräten. Statistikfelder sind jetzt in **`dmsetup`**-Berichten verfügbar und der **`dmstats`**-Befehl fügt neue, spezialisierte Berichtsmodi hinzu, die zur Verwendung mit statistischen Information entworfen wurden. Informationen zum **`dmstats`**-Befehl finden Sie auf der dmstats(8) man-Seite.

Support für DIX bei spezifizierter Hardware

SCSI T10 DIX wird in Red Hat Enterprise Linux 7.2 nur für die folgenden HBAs und Speicher-Arrays voll unterstützt, nicht an LUNs, die für das Booten von einer SAN-Umgebung verwendet werden. Außerdem wird T10 DIX in RHEL 7 nur an nativer Hardware unterstützt, nicht beim Ausführen an virtualisierten Gästen.

* 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

Support für DIX verbleibt für HBAs und Storage-Arrays in Technologievorschau.

Beachten Sie, dass T10 DIX Database oder eine andere Software erfordert, die die Generierung und Verifizierung von Prüfsummen auf Disk-Blöcken bereitstellt. Keine derzeit unterstützten Linux-Dateisysteme besitzen diese Fähigkeit.

LVM-Cache

Das LVM-Cache wird seit Red Hat Enterprise Linux 7.1 voll unterstützt. Dieses Feature gestattet Benutzern das Erstellen logischer Volumes (LVs) mit einem kleinen, schnellen Gerät als Cache für größere, langsamere Geräte zu fungieren. Auf der lvmcache(7) man-Seite finden Sie Informationen zur Erstellung von logischen Cache-Volumes.

Beachten Sie bitte die folgenden Einschränkungen bei der Verwendung von Cache-LVs:

* Das Cache-LV muss ein Gerät der obersten Ebene sein. Es kann nicht als Thin-Pool-LV, als Image eines RAID LV oder als ein anderer Sub-LV-Typ verwendet werden.

* Die Cache LV Sub-LVs (das Ursprungs-LV, Metadata-LV und Daten-LV) können nur vom Typ linear, Stripe oder RAID sein.

* Die Properties des Cache-LV können nach dem Erstellen nicht geändert werden. Um die Cache-Eigenschaften zu ändern, entfernen Sie das Cache wie in lvmcache(7) beschrieben und erstellen Sie es mit den gewünschten Eigenschaften neu.

Neue LVM/DM Cache-Richtlinie

Es wurde eine neue **`smq`** dm-cache Richtlinie geschrieben, die den Speicherverbrauch senkt und in den meisten Anwendungsfällen die Performance verbessert. Dies ist jetzt die standardmäßige Cache-Richtlinie für neue logische Volumes des LVM-Cache. Benutzer, die lieber die alte **`mq`**-Cache-Richtlinie verwenden möchten, können dies tun, indem sie das **`–cachepolicy`**-Argument beim Erstellen des logischen Cache-Volumes eingeben.

LVM-systemID

LVM-Volume-Gruppen können jetzt einem Besitzer zugewiesen werden. Der Besitzer der Volume-Gruppe ist die System-ID eines Host. Nur der Host mit der gegebenen System-ID kann die VG verwenden. Dies kann für Volume-Gruppen von Nutzen sein, die auf gemeinsam genutzten Geräten existieren, für mehrere Hosts sichtbar sind, die andernfalls nicht vor der gleichzeitigen Verwendung durch mehrere Hosts geschützt wären. LVM-Volume-Gruppen auf gemeinsam genutzten Geräten mit einer zugewiesenen System-ID gehören einem Host und sind von anderen Hosts geschützt.

Kapitel 13. System- und Subskriptionsverwaltung

PowerTOP berücksichtigt jetzt benutzerdefinierte Berichtsdateinamen

In der Vergangenheit wurden Dateinamen von PowerTOP-Berichten auf unklare, undokumentierte Weise generiert. Mit dieser Aktualisierung wird die Implementierung verbessert und die generierten Dateinamen berücksichtigen nun die vom Benutzer angefragten Namen. Dies gilt für sowohl CSV- als auch HTML-Berichte.

Geänderte `yum-config-manager`-Befehle

In der Vergangenheit deaktivierte der **`yum-config-manager --disable`**-Befehl alle konfigurierten Repositories, während der **`yum-config-manager --enable`**-Befehl keine aktivierte. Diese Inkonsistenz wurde behoben. Die **`--disable`**- und **`--enable`**-Befehle erfordern nun die Verwendung von »*« in der Syntax und **`yum-config-manager --enable \*`** aktiviert Repositories. Werden die Befehle ohne Zusatz von »*« ausgeführt, so wird eine Nachricht ausgegeben, die den Benutzer auffordert **`yum-config-manager --disable \*`** oder **`yum-config-manager --enable \*`** auszuführen, wenn Repositories deaktiviert oder aktiviert werden sollen.

Neues search-disabled-repos Plug-in für yum

Das search-disabled-repos Plug-in für yum wurde den subscription-manager-Paketen hinzugefügt. Dieser Plug-in ermöglicht es Benutzern yum-Operationen abzuschließen, die fehlschlagen da das Quell-Repository von einem deaktivierten Repository abhängig ist. Wird search-disabled-repos im beschriebenen Szenario installiert, so zeigt yum Anweisungen zum temporären Aktivieren deaktierter Repositories und der Suche nach fehlenden Abhängigkeiten an. Nachdem die notwendigen Änderungen an der /etc/yum/pluginconf.d/search-disabled-repos.conf-Datei vorgenommen wurden, kann die yum-Operation fortgesetzt werden, wobei die deaktivierten Repositories verwendet werden als seien sie aktiviert.

Kapitel 14. Virtualisierung

Weitere PCI root-Buses werden jetzt mittels PCI-Expander Bridge-Geräten unterstützt

Im Gegensatz zu PCI-PCI Bridges kann ein Bus an einer PCI-Expander-Bridge mit einem NUMA-Knoten assoziiert werden, so dass das Gast-Betriebssystem die Nähe eines Geräts zu RAM und CPUs erkennt. Mit dieser Aktualisierung können zugewiesene Geräte mit dem entsprechenden NUMA-Knoten assoziiert werden, was zu einer optimalen Performance führt.

qemu-kvm unterstützt Tracepoints beim Herunterfahren virtueller Maschinen

In qemu-kvm werden nun Ereignisse zur Ablaufverfolgung während des Shutdown-Vorgangs unterstützt. Diese ermöglichen es Benutzern, detaillierte Diagnoseinformationen über die Shutdown-Anfragen eines Gastsystem zu erhalten, die vom Befehl **`virsh shutdown`** oder von der virt-manager-Applikation ausgegeben werden. Benutzer können diese erweiterten Fähigkeiten nutzen, um Probleme ihrer KVM-Gäste während des Herunterfahrens zu isolieren und zu beheben.

Offenlegen von Intel MPX für den Gast

In dieser Aktualisierung erlaubt das Offenlegen qemu-kvm dem Intel Memory Protection Extensions (MPX) Feature gegenüber dem Gast. Bei Intel 64 Host-Systemen, die MPX unterstützen, ermöglicht dies die Verwendung eines Satzes von Erweiterungen, die Hardware-Support für Grenzenschutz an Zeigerreferenzen unterstützen.

Gast-Arbeitsspeicher Dump-Auszug vom qemu-kvm-Kern

Das dump-guest-memory.py-Skript wurde in QEMU eingeführt, was die Analyse des Gast-Memory-Dump vom qemu-kvm-Kern im Falle eines Kernelfehlers am Gast ermöglicht. Weitere Informationen finden Sie im zugehörigen Hilfstext mittels des **`help dump-guest-memory`**-Befehls.

virt-v2v wird voll unterstützt

Mit Red Hat Enterprise Linux 7.2 wird das virt-v2v-Befehlszeilentool nun voll unterstützt. Dieses Tool konvertiert virtuelle Maschinen, die auf fremden Hypervisors laufen dahingehend, dass sie auf KVM laufen. Derzeit kann virt-v2v Red Hat Enterprise Linux und Windows Gäste konvertieren, die auf Red Hat Enterprise Linux 5 Xen und VMware vCenter laufen.

Virtualisierung bei IBM Power Systems

Red Hat Enterprise Linux mit KVM wird auf AMD64- und Intel 64 Systemen unterstützt, nicht jedoch auf IBM Power Systemen. Red Hat liefert momentan eine POWER8-basierte Lösung mit Red Hat Enterprise Virtualization für IBM Power Systeme.

Weitere Informationen zu unterstützten Versionen und Installationsvorgängen finden Sie im folgenden Knowledge Base Artikel: https://access.redhat.com/articles/1247773

VirtIO-1-Support

Virtio-Treiber wurden auf Kernel 4.1 aktualisiert und liefern jetzt VirtIO 1.0 Gerätesupport.

Hyper-V TRIM Support

Die Verwendung der Thin Provisioned Hyper-V virtual Hard Disk (VHDX) ist jetzt möglich. Die Aktualisierung fügt Support für das Verkleinern der zugrundeliegenden VHDX-Dateien für Microsoft Hyper-V virtuelle Maschinen zum tatsächlich verwendeten Platz hinzu.

Kapitel 15. Red Hat Software Collections

Red Hat Software Collections ist ein Red Hat Inhaltsset, das eine Reihe dynamischer Programmiersprachen, Datenbankserver und zugehöriger Pakete bereitstellt, die Sie auf allen unterstützten Releases von Red Hat Enterprise Linux 6 und Red Hat Enterprise Linux 7 auf AMD64 und Intel 64 Architekturen installieren und verwenden können.

Dynamische Sprachen, Datenbankserver und andere Tools, die in Red Hat Software Collections bereitgestellt werden, ersetzen nicht die standardmäßigen Systemtools, die in Red Hat Enterprise Linux enthalten sind, und sind diesen nicht notwendigerweise vorzuziehen. Red Hat Software Collections verwenden einen abweichenden Paketmechanismus basierend auf dem **`scl`**-Dienstprogramm, um eine parallele Gruppe von Paketen bereitzustellen. Diese Gruppe ermöglicht die optionale Verwendung alternativer Paketversionen auf Red Hat Enterprise Linux. Mithilfe des **`scl`**-Dienstprogramms können Benutzer jederzeit frei entscheiden, welche Paketversion sie ausführen möchten.

Red Hat Developer Toolset ist nun Teil der Red Hat Software Collections, enthalten als separate Software Collection. Red Hat Developer Toolset wurde konzipiert für Entwickler, die auf der Red Hat Enterprise Linux Plattform arbeiten. Es bietet aktuelle Versionen der GNU Compiler Collection, GNU Debugger, Eclipse Entwicklungsplattform sowie andere Tools für Entwicklung, Debugging und Leistungsüberwachung.

Wichtig

Red Hat Software Collections hat einen kürzeren Lebenszyklus und Supportzeitraum als Red Hat Enterprise Linux. Weitere Informationen finden Sie unter Red Hat Software Collections Product Life Cycle.

Siehe Red Hat Software Collections Dokumentation für eine Liste der im Set enthaltenen Komponenten, die Systemanforderungen, bekannte Probleme, die Verwendung sowie Einzelheiten über die einzelnen Software Collections.

Siehe Red Hat Developer Toolset Dokumentation für weitere Informationen über die in dieser Software Collection enthaltenen Komponenten, die Verwendung, bekannte Probleme usw.

Teil II. Technologievorschauen

Dieser Teil bietet eine Übersicht der mit Red Hat Enterprise Linux 7.2 eingeführten Technologievorschauen.

Weitere Informationen zu Red Hat Technologievorschauen finden Sie unter https://access.redhat.com/support/offerings/techpreview/.

Kapitel 16. Authentifizierung

Verwendung von AD- und LDAP-Sudo-Providern

Der Active Directory-Provider (AD) ist ein Back-End, das zur Verbindung mit einem Active Directory Server verwendet wird. In Red Hat Enterprise Linux 7.2 wird die Verwendung des AD-Sudo-Providers zusammen mit dem LDAP-Provider als Technologievorschau unterstützt. Um den AD-Sudo-Provider zu aktivieren, fügen Sie die Einstellung **`sudo_provider=ad`** zum Domain-Abschnitt der **`sssd.conf`**-Datei hinzu.

Kapitel 17. Dateisysteme

OverlayFS

OverlayFS ist eine Art gemeinsames Dateisystem. Es gestattet dem Benutzer den **`overlay`** von einem Dateisystem auf einem anderen. Änderungen werden im oberen Dateisystem festgehalten, während das tiefer liegende Dateisystem unverändert bleibt. Dies ermöglicht mehreren Benutzern die gemeinsame Nutzung eines file-system-Image, wie eines Containers oder einer DVD-ROM ermöglicht, wo das Basis-Image sich auf einem schreibgeschützten Medium befindet. Weitere Informationen finden Sie in der Kerneldatei Documentation/filesystems/overlayfs.txt.

OverlayFS bleibt in Red Hat Enterprise Linux 7.2 eine Technologievorschau. Der Kernel protokolliert in diesem Fall Warnmeldungen, wenn diese Technologie aktiviert wird.

Voller Support ist für OverlayFS bei der Verwendung mit Docker verfügbar, allerdings mit folgenden Einschränkungen:

* OverlayFS wird nur bei Verwendung als ein Docker Graph-Treiber unterstützt. Seine Verwendung kann für Container COW-Inhalte, nicht für persistenten Speicher unterstützt werden. Jeder persistente Speicher auf nicht-OverlayFS-Volumes platziert werden, um unterstützt zu werden. Nur die standardmäßige Docker-Konfiguration kann verwendet werden; das bedeutet eine Ebene an Overlay, eine lowerdir und beide Ebenen befinden sich in demselben Dateisystem).

* Nur XFS wird derzeit für die Verwendung als Dateisystem der unteren Schicht unterstützt.

* SELinux muss aktiviert und im Erzwingungsmodus an der physischen Maschine sein, muss jedoch im Container während der Container-Separation deaktiviert sein; das heißt /etc/sysconfig/docker darf --selinux-enabled nicht enthalten. Am SELinux-Support für OverlayFS wird Upstream gearbeitet und es wird in einer zukünftigen Release erwartet.

* Das OverlayFS Kernel-ABI und Userspace-Verhalten gelten nicht als stabil und es sind Änderungen in zukünftigen Aktualisierungen möglich.

Beachten Sie, dass OverlayFS einen eingeschränkten Satz von POSIX-Standards bereitstellt. Testen Sie Ihre Applikation gründlich, ehe Sie diese mit OverlayFS bereitstellen.

Es werden außerdem mehrere bekannte Probleme mit OverlayFS im Zusammenhang mit der Red Hat Enterprise Linux 7.2 Release assoziiert. Weitere Informationen finden Sie unter **`Non-standard behavior`** in der Documentation/filesystems/overlayfs.txt-Datei.

Support für NFSv4-Clients mit flexiblem Datei-Layout

Red Hat Enterprise Linux 7.2 beinhaltet Support für flexibles Datei-Layout auf NFSv4-Clients. Diese Technologie ermöglicht fortgeschrittene Features wie nicht disruptive Dateimobilität und Client-seitiges Mirroring, wodurch verbesserte Nutzbarkeit in Bereichen wie Datenbanken, Big Data und Virtualisierung erreicht wird.

Siehe https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/ für ausführliche Informationen zu NFS flexibles Datei-Layout.

NFS auf RDMA

Der NFSoRDMA-Dienst wird für Red Hat Enterprise Linux 7.2 als eine Technologievorschau bereitgestellt. Dadurch wird das svcrdma-Modul verfügbar für Benutzer, die Remote Direct Memory Access (RDMA) Transport mit dem Red Hat Enterprise Linux 7 NFS Server zu verwenden beabsichtigen.

Btrfs-Dateisystem

Das Btrfs (B-Tree) Dateisystem wird als eine Technologievorschau in Red Hat Enterprise Linux 7.2 unterstützt. Dieses Dateisystem bietet fortgeschrittene Verwaltung, Zuverlässigkeit und Skalierbarkeit. Es ermöglicht Benutzern das Erstellen von Snapshots, es ermöglicht Kompression und integrierte Geräteverwaltung.

Kapitel 18. Hardwareunterstützung

Support für OSA-Express5s-Karten in qethqoat

Support für OSA-Express5s-Karten wurde dem qethqoat-Tool hinzugefügt, das Teil des s390utils-Pakets ist. Diese Verbesserung erweitert die Bedienbarkeit von Netzerk- und Karten-Einstellungen für OSA-Express5s-Karten und ist als eine Technologievorschau in Red Hat Enterprise Linux 7.2 auf IBM System z enthalten.

Runtime-Instrumentierung für IBM System z

Support für die Runtime-Instrumentierung ist in Red Hat Enterprise Linux 7.2 auf IBM System z als Technologievorschau verfügbar. Runtime-Instrumentierung ermöglicht die erweiterte Analyse und Ausführung für eine Reihe von Applikationen im Benutzerbereich, die mit dem IBM zEnterprise EC12 System verfügbar sind.

LSI Syncro CS HA-DAS Adapter

Red Hat Enterprise Linux 7.1enthält Code im megaraid_sas-Treiber, um LSI Syncro CS HA-DAS-Treiber (High-Availability Direct-Attached Storage) zu aktivieren. Der megaraid_sas-Treiber wird für bereits aktivierte Adapter vollständig unterstützt, die Verwendung dieses Treibers für Syncro CS steht dagegen als Technologievorschau zur Verfügung. Support für diesen Adapter erhalten Sie direkt von LSI (Ihrem Systemintegrator) oder vom Systemanbieter. Benutzer, die Syncro CS auf Red Hat Enterprise Linux 7.2 einsetzen, werden dazu ermutigt, Red Hat und LSI ihr Feedback zu geben. Weitere Informationen über LSI Syncro CS Lösungen finden Sie unterhttp://www.lsi.com/products/shared-das/pages/default.aspx.

Kapitel 19. Kernel

Multipler CPU-Support in kdump bei AMD64 und Intel 64 Systemen

Bei AMD64- und Intel 64-Systems kann der **kdump** Kernel-Crash-Dumping-Mechanismus jetzt mit mehr als einer aktivierten CPU booten. Das löst ein Problem bei Systemen mit großem Arbeitsspeicher wo wegen hoher Ein- und Ausgabeaktivität beim Erstellen eines Kernel-Crash-Dumps Linux für Geräte mit nur einer aktivierten CPU ("maxcpus=1" oder **nr_cpus=1**) keine Interrupts zuteilte.

Um mehrere CPUs im Crash-Kernel zu aktivieren, geben Sie **nr_cpus=X** (wobei **X** die Anzahl an Prozessoren ist) und **disable_cpu_apicid=0**-Optionen an der Kernel-Befehlszeile an.

Das criu-Tool

Red Hat Enterprise Linux 7.2 präsentiert das **criu**-Tool als eine Technologievorschau. Dieses Tool implementiert **Checkpoint/Restore in User-space**, das zum Einfrieren einer laufenden Applikation und deren Aufbewahrung als Dateisammlung verwendet werden kann. Später kann die Applikation aus dem eingefrorenen Status wiederhergestellt werden.

Das **criu**-Tool hängt vom **Protocol Buffers** ab, einem sprachen- und plattformneutralen Erweiterungsmechanismus für die Serialisierung strukturierter Daten. Die *protobuf*- und *protobuf-c*-Pakete, die diese Abhängigkeit bereitstellen, sind in Red Hat Enterprise Linux 7.2 ebenfalls als eine Technologievorschau enthalten.

Benutzer-Namensraum

Dieses Feature bietet zusätzliche Sicherheit für Server auf denen Linux-Container laufen, da es eine bessere Isolierung zwischen dem Host und den Containern liefert. Administratoren eines Containers können keine administrativen Vorgänge mehr am Host durchführen, wodurch sich die Sicherheit erhöht.

LPAR Watchdog für IBM System z

Ein verbesserter Watchdog-Treiber für IBM System z ist als eine Technologievorschau verfügbar. Dieser Treiber unterstützt Linux logische Partitionen (LPAR) sowie Linux-Gäste im z/VM-Hypervisor und liefert automatischen Reboot und automatische Dump-Fähigkeiten, wenn ein Linux-System nicht mehr reagiert.

Dynamische Kernel-Aktualisierungen mit kpatch

Das kpatch-Dienstprogramm ermöglicht Benutzern das Verwalten einer Sammlung von binären Kernel-Patches, die dazu genutzt werden können, den Kernel dynamisch zu patchen ohne Neustart. Beachten Sie, dass kpatch nur als Technologiervorschau auf AMD64 und Intel 64 Architekturen unterstützt wird.

i40evf handhabt große Resets

Der gängigste Typ von Reset dem eine Virtual Function (VF) begegnet ist ein Physical Function (PF) Reset, der einen VF-Reset für jede VF herunterkaskadiert. Für »größere« Resets jedoch, wie einem Core- oder EMP-Reset wenn das Gerät neu initialisiert wird, erhielt die VF bislang nicht dieselbe VSI, so dass die VF nicht wiederhergestellt werden konnte, da sie Ressourcen für ihr Original-VSI anfragte. Diese Aktualisierung fügt als Technologievorschau einen zusätzlichen Status zur Admin-Warteschlange hinzu, so dass der Treiber die Konfigurationsinformationen zur Runtime erneut anfragen kann. Während der Reset-Wiederherstellung wird dies im aq_required-Feld eingestellt, und die Konfigurationsinformationen werden abgerufen, ehe der Treiber wieder hochgefahren wird.

Kapitel 20. Netzwerk

Intel Ethernet Server Adapter X710/XL710 Treiber-Aktualisierungen

Die i40e- und i40evf-Kerneltreiber wurden auf Version 1.3.4-k aktualisiert. Diese aktualisierten Treiber sind als Technologievorschau in Red Hat Enterprise Linux 7.2 enthalten.

Korrekte ethtool-Ausgabe

Die Netzwerkabfrage-Fähigkeiten des ethtool-Dienstprogramms wurden in einer Technologievorschau für Red Hat Enterprise Linux 7.2 auf IBM System z verbessert.Wird nun mit dem neuen Abfragetool kompatible Hardware verwendet, so liefert ethtool bessere Überwachungsoptionen und zeigt Einstellungen von Netzwerkkarten und Werte genauer an.

Cisco usNIC-Treiber

Cisco Unified Communication Manager (UCM) Server besitzen ein optionales Feature zur Bereitstellung eines Cisco proprietären User Space Network Interface Controller (usNIC), der die Ausführung von Remote Direct Memory Access (RDMA)-artigen Operationen für Applikationen im Benutzerbereich gestattet. Der libusnic_verbs-Treiber, der als Technologievorschau unterstützt wird, macht die Verwendung von usNIC-Geräten über standardmäßige InfiniBand RDMA-Programmierung basierend auf die Verbs API möglich.

Cisco VIC Kernel-Treiber

Der Cisco VIC Infiniband Kernel-Treiber wird als Technologievorschau unterstützt. Dieser Treiber ermöglicht die Verwendung von Remote Directory Memory Access (RDMA)-ähnlichen Semantiken auf proprietären Cisco-Architekturen.

Trusted Network Connect

Trusted Network Connect wird als als Technologievorschau unterstützt. Trusted Network Connect wird mit vorhandenen Lösungen zur Network Access Control (NAC) wie TLS, 802.1X oder IPsec verwendet, um Endpoint Posture Assessment zu integrieren. Dabei werden Systeminformationen vom Endpunkt gesammelt wie z. B. Konfigurationseinstellungen des Betriebssystems, installierte Pakete und mehr zur Integritätsmessung. Trusted Network Connect dient zum Abgleich dieser Messwerte mit den Richtlinien zum Netzwerkzugriff, bevor es dem Endpunkt gestattet wird, auf das Netzwerk zuzugreifen.

SR-IOV-Funktionalität im qlcnic-Treiber

Unterstützung für Single Root I/O Virtualisierung (SR-IOV) wurde zum qlcnic-Treiber als Technologievorschau hinzugefügt. Support für diese Funktionalität wird direkt von QLogic bereitgestellt, und Kunden werden dazu ermutigt, QLogic und Red Hat ihr Feedback mitzuteilen. Andere Funktionalitäten im qlcnic-Treiber bleiben vollständig unterstützt.

Kapitel 21. Speicher

Multiqueue I/O-Scheduling für SCSI

Red Hat Enterprise Linux 7.2 beinhaltet einen neuen I/O-Scheduling-Mechanismus für mehrere Warteschlangen für als blk-mq bekannte Blockgeräte. Das scsi-mq-Paket erlaubt dem Small Computer System Interface (SCSI) Subsystem diesen neuen Warteschlangenmechanismus zu nutzen. Diese Funktionalität wird als Technologievorschau bereitgestellt und ist nicht standardmäßig aktiviert. Um sie zu aktivieren, fügen Sie der Kernel-Befehlszeile **`scsi_mod.use_blk_mq=Y`** hinzu.

Verbesserte LVM-Locking-Infrastruktur

`lvmlockd` ist eine Locking-Infrastruktur der nächsten Generation für LVM. Es ermöglicht LVM das sichere Verwalten von gemeinsam genutzten Speicher von mehreren Hosts unter Verwendung von entweder dem **`dlm`**- oder **`sanlock`**Sperr-Manager. **`sanlock`** erlaubt **`lvmlockd`** die Koordination von Hosts durch speicherbasiertes Sperren, ohne dass eine komplette Cluster-Infrastruktur erforderlich ist. Weitere Informationenfinden Sie auf der `lvmlockd`(8) man-Seite.

Targetd Plug-in vom libStorageMgmt-API

Red Hat Enterprise Linux 7.1 unterstützt die Verwaltung von Storage Arrays mit libStorageMgmt voll. libStorageMgmt ist eine Programmierschnittstelle unabhängig vom Storage Array. Sie liefert eine stabile und konsistente API, die es Entwicklern ermöglicht, befehlsorientiert verschiedene Storage Arrays zu verwalten und die bereitgestellten Features der Hardwarebeschleunigung zu nutzen. Systemadministratoren können libStorageMgmt auch zur manuellen Speicherverwaltung und zur Automatisierung von Speicherverwaltungsaufgaben per Befehlszeile nutzen.

Der Targetd Plug-in wird nicht komplett unterstützt und verbleibt eine Technologievorschau.

DIF/DIX

DIF/DIX wurde dem SCSI-Standard neu hinzugefügt. Es wird von Red Hat Enterprise Linux 7.2 für die im Kapitel »Features« angegebenen HBAs und Storage-Arrays voll unterstützt, verbleibt für alle anderen HBAs und Storage-Arrays jedoch in der Technologievorschau.

DIF/DIX erhöht die Größe des üblicherweise verwendeten 512-Byte-Festplattenblocks von 512 auf 520 Bytes, indem das Data Integrity Field (DIF) hinzugefügt wurde. Das DIF speichert den Prüfsummenwert für den Datenblock, der vom Host Bus Adapter (HBA) berechnet wird, wenn ein Schreibvorgang erfolgt. Das Speichergerät bestätigt anschließend die Prüfsumme und speichert sowohl die Daten als auch die Prüfsumme. Umgekehrt kann die Prüfsumme während eines Lesevorgangs vom Speichergerät und vom empfangenden HBA gelesen werden.

dm-era device-mapper Ziel

Red Hat Enterprise Linux 7.1 führt das dm-era Device-Mapper-Ziel als Technolgievorschau ein. dm-era beobachtet, welche Blöcke innerhalb eines benutzerdefinierten Zeitraums, genannt **`era`**, geschrieben wurden. Jede Ära-Zielinstanz führt die aktuelle Ära als gleichmäßig fortlaufenden 32-Bit-Zähler. Dieses Ziel ermöglicht es Backup-Software nachzuverfolgen, welche Blöcke seit dem letzten Backup verändert wurden. Es ermöglicht auch eine teilweise Invalidierung von Cache-Inhalten, um die Cache-Kohärenz nach dem Zurücksetzen auf einen Anbieter-Snapshot wiederherzustellen. Das dm-era-Ziel wird voraussichtlich in erster Linie mit dem dm-cache-Ziel verknüpft.

Kapitel 22. Virtualisierung

Verschachtelte Virtualisierung

Als eine Technologievorschau bietet Red Hat Enterprise Linux 7.2 das verschachtelte Virtualisierungs-Feature an. Dieses ermöglicht die Verwendung von KVM-QEMU-Gästen als Hosts, so dass der Benutzer Gäste innerhalb dieser Gäste erstellen kann.

Das virt-p2v-Tool

Red Hat Enterprise Linux 7.2 bietet das virt-p2v-Tool als eine Technologievorschau an. Virt-p2v (»physical to virtual«) ist ein CD-ROM, ISO- oder PXE-Image, das der Benutzer auf einer physischen Maschine booten kann und es konvertiert die physische Maschine in eine virtuelle Maschine, die auf KVM läuft.

USB 3.0-Support für KVM-Gäste

USB 3.0 Host Adapter (xHCI) Emulation für KVM-Gäste verbleibt in Red Hat Enterprise Linux 7.2 eine Technologievorschau.

Teil III. Gerätetreiber

Dieses Kapitel liefert eine umfassende Liste aller Gerätetreiber, die in Red Hat Enterprise Linux 7.2 aktualisiert wurden.

Kapitel 23. Aktualisierte Storage-Treiber

- Der hpsa-Treiber wurde auf Version 3.4.4-1-RH4 aktualisiert.
- Der qla2xxx wurde auf Version 8.07.00.18.07.2-k aktualisiert.
- Der lpfc-Treiber wurde auf Version 10.7.0.1 aktualisiert.
- Der megaraid_sas-Treiber wurde auf Version 06.807.10.00 aktualisiert.
- Der fnic-Treiber wurde auf Version 1.6.0.17 aktualisiert.
- Der mpt2sas-Treiber wurde auf Version 20.100.00.00 aktualisiert.
- Der mpt3sas-Treiber wurde auf Version 9.100.00.00 aktualisiert.
- Der Emulex be2iscsi-Treiber wurde auf Version 10.6.0.0r aktualisiert.
- Der aacraid-Treiber wurde auf Version 1.2 aktualisiert.
- Der bnx2i-Treiber wurde auf Version 2.7.10.1 aktualisiert.
- Der bnx2fc-Treiber wurde auf Version 2.4.2 aktualisiert.

Kapitel 24. Aktualisierte Netzwerktreiber

- Der tg3-Treiber wurde auf Version 3.137 aktualisiert.
- Der e1000-Treiber wurde auf Version 7.3.21-k8-NAPI aktualisiert, der bei Verwendung der xmit_more booleschen Variable Support für txtd-Aktualisierungsverzögerung bietet.
- Der e1000e-Treiber wurde auf Version 2.3.2-k aktualisiert.
- Der igb-Treiber wurde auf Version 5.2.15-k aktualisiert.
- Der igbvf-Treiber wurde auf Version 2.0.2-k aktualisiert.
- Der ixgbevf-Treiber wurde auf Version 2.12.1-k aktualisiert.
- Der ixgbe-Treiber wurde auf Version 4.0.1-k aktualisiert.
- Der bna-Treiber und Firmware wurden auf Version 3.2.23.0r aktualisiert.
- Der bnx2-Treiber wurde auf Version 2.4.2 aktualisiert.
- Der CNIC-Treiber wurde auf Version 2.5.21 aktualisiert.
- Der bnx2x-Treiber wurde auf Version 1.710.51-0 aktualisiert, wodurch auch qlogic NPAR-Support für qlogic-nx2-Adapter hinzugefügt wird.
- Der be2net-Treiber wurde auf Version 10.6.0.2 aktualisiert.
- Der bna-Treiber wurde auf Version 3.2.23.0r aktualisiert.
- Der qlcnic-Treiber wurde auf Version 5.3.62 aktualisiert.
- Der qlge-Treiber wurde auf Version 1.00.00.34 aktualisiert, was eine Wettbewerbsbedingung zwischen der New API (NAPI) Registrierung und Deregistrierung aufhebt, die in der Vergangenheit zum Systemabsturz führte und auftrat, wenn bestimmte Parameter geändert wurden, während die Network Interface Card (NIC) auf »down« eingestellt war.
- Der r8169-Treiber wurde auf Version 2.3LK-NAPI aktualisiert.
- Die i40e- und i40evf-Treiber wurden auf Version 1.3.4-k aktualisiert.
- Der netxen_nic-Treiber wurde auf Version 4.0.82 aktualisiert.
- Der sfc-Treiber wurde auf die aktuellste Upstream-Version aktualisiert.
- Diese Aktualisierung fügt den fm10k-Treiber von Version 0.15.2-k hinzu.
- Diese Aktualisierung fügt VTI6-Support hinzu, einschließlich netns-Fähigkeiten.
- Der Bonding-Treiber wurde auf Version 3.7.1 aktualisiert.
- Der iwlwifi-Treiber wurde auf die aktuellste Upstream-Version aktualisiert.
- Der vxlan-Treiber wurde auf Version 0.1 aktualisiert.

Kapitel 25. Aktualisierte Grafiktreiber und andere Treiber

- Der HDA-Treiber wurde auf die aktuellste Upstream-Version aktualisiert und verwendet jetzt die neue jack kctls-Methode.
- Der HPI-Treiber wurde auf Version 4.14 aktualisiert.
- Der Realtek HD-audio Codec-Treiber und enthält die aktualisierten EAPD init-Codes.
- Der IPMI-wurde aktualisiert und ersetzt die timespec-Verwendung durch timespec64.
- Der i915-Treiber wurde aktualisiert und beinhaltet jetzt die Überarbeitung von ACPI Video Extensions-Treiber in Red Hat Enterprise Linux 7.2.
- Der ACPI Fan-Treiber wurde auf Version 0.25 aktualisiert.
- Der Update NVM-Express -Treiber wurde auf Version 3.19 aktualisiert.
- Der rtsx-Treiber wurde auf Version 4.0 aktualisiert und unterstützt rtl8402, rts524A, rts525A Chips.
- Der Generic WorkQueue Engine-Gerätetreiber wurde auf die aktuellste Upstream-Version aktualisiert.
- Der PCI-Treiber wurde auf Version 3.16 aktualisiert.
- Das EDAC-Kernelmodul wurde aktualisiert und bietet Support für Intel Xeon v4 Prozessoren.
- Der pstate-Treiber wurde aktualisiert und unterstützt Intel Core Prozessoren der 6. Generation.
- Der intel_idle-Treiber wurde aktualisiert und unterstützt Intel Core Prozessoren der 6. Generation.

Teil IV. Bekannte Probleme

Dieser Teil dokumentiert bekannte Probleme bei Red Hat Enterprise Linux 7.2.

Kapitel 26. Compiler und Werkzeuge

Mehrere Fehler beim Booten von SAN über FCoE

Mehrere Fehler treten bei der aktuellen Implementierung beim Booten vom Storage Area Network (SAN) mittels Fibre Channel über Ethernet (FCoE) auf. Red Hat plant diese Fehler in einer zukünftigen Release von Red Hat Enterprise Linux 7 zu beheben. Eine Liste der betreffenden Fehler und Problemumgehungen (wo verfügbar) erhalten Sie von Ihrem Red Hat Support-Mitarbeiter.

Valgrind kann keine für eine frühere Version von Open MPI erstellten Programme ausführen

Red Hat Enterprise Linux 7.2 unterstützt nur das Open MPI Application Binary Interface (ABI) in Version 1.10, welches mit der zuvor gelieferten 1.6 Version des Open MPI ABI inkompatibel ist. Daher können für die vorherige Version von Open MPI erstellte Programme nicht unter dem in Red Hat Enterprise Linux 7.2 enthaltenen Valgrind laufen. Um dieses Problem zu umgehen können Sie die Red Hat Developer Toolset Version von Valgrind für mit Open MPI Version 1.6 verbundene Programme verwenden.

Kapitel 27. Desktop

Fehlerhafte pygobject3 Paketabhängigkeiten verhindern das Upgrade von Red Hat Enterprise Linux 7.1

Das *pygobject3-devel.i686* 32-bit Paket wurde in Red Hat Enterprise Linux 7.2 entfernt und durch eine multilib-Version ersetzt. Falls bei Ihnen die 32-bit-Version auf einem Red Hat Enterprise Linux 7.1 System installiert ist, so tritt ein **yum**-Fehler beim Versuch des Upgrades auf Red Hat Enterprise Linux 7.2 auf.

Um dieses Problem zu umgehen, verwenden Sie den **yum remove pygobject3-devel.i686**-Befehl als **root** zur Deinstallation der 32-bit-Version, bevor Sie ein Upgrade Ihres Systems durchführen.

Kapitel 28. Allgemeine Aktualisierungen

Neu zugewiesene Gerätenamen können zu Störungen der Netzwerkverbindung führen

In der Vergangenheit war es nicht möglich, virtio-Geräten stabile Netzwerkschnittstellennamen zuzuweisen, da die Aufzählungsreihenfolge dieser Geräte nicht vorhersehbar war. Mit dieser Fehlerbehebung gibt es nur ein übergeordnetes PCI-Gerät je virtio-Bus, und virtio-Netzwerkgeräte haben jetzt persistente Gerätenamen in virtuellen Maschinen (gemäß http://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/).

Bitte beachten Sie, dass nach einer Aktualisierung von systemd und dem Neustart der virtuellen Maschine, die zuvor Interface-Namen von einem Kernel-Namensraum (eth0, eth1,...) hatte, beim nächsten Start neue Gerätenamen zugewiesen werden, was zu einer Unterbrechung der Netzwerkverbindung zur virtuellen Verbindung führen kann.

Kapitel 29. Installation und Bootvorgang

Installation im Textmodus stürzt während der Netzwerkkonfiguration nicht mehr ab

In der Vergangenheit konnte es vorkommen, dass bei Verwendung eines Leerzeichens bei der Angabe von Namensservern im Bildschirm zur Netzwerkkonfiguration im interaktiven Textmodusinstaller der Installer abstürzte.

Anaconda handhabt jetzt Namensserver-Definitionen im Textmodus ordnungsgemäß und der Installer stürzt nicht mehr ab, wenn ein Leerzeichen zur Trennung von Nameserver-Adressen verwendet wird.

Mögliche NetworkManager-Fehlermeldung während der Installation

Bei der Installation ist es möglich, dass die folgende Fehlermeldung angezeigt wird:

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

Für diesen Fehler ist derzeit keine Problemumgehung verfügbar.

Atomic Host Installation bietet cryptsetup an, obwohl dieses nicht verfügbar ist

Während der Installation von Red Hat Enterprise Linux 7 Atomic Host bietet der Installer die Option zur Verschlüsselung von Partitionen mittels **`cryptsetup`** im Bildschirm »Manuelle Partitionierung« auf dieselbe Weise wie während der Installation von Red Hat Enterprise Linux 7.2 an.

Allerdings werden verschlüsselte Partitionen nicht vom Atomic Host unterstützt. Wenn Sie Partitionen während der Installation verschlüsseln, so werden Sie später nicht in der Lage sein, diese zu entsperren.

Um dieses Problem zu umgehen, verschlüsseln Sie keine Partitionen oder Logical Volumes während der Installation des Red Hat Enterprise Linux Atomic Host, selbst wenn der Installer Ihnen diese Option anbietet.

Installer kann nur bei erstmaliger Eingabe des Storage Spoke erweiterten Speicher hinzufügen

Während einer interaktiven Installation mittels der grafischen Oberfläche von Anaconda funktioniert das Hinzufügen von erweitertem Speicher (iSCSI, zFCP, FCoE) zu Ihrer Disk-Auswahl nicht, wenn Sie den Storage Spoke bereits eingegeben und verlassen haben. Um das Problem zu umgehen, stellen Sie sicher, dass das Netzwerk (falls benötigt) aktiv ist, geben Sie dann den Storage Spoke ein und fügen Sie alle Geräte für den erweiterten Speicher hinzu.

Kapitel 30. Kernel

Die Größe mancher ext4-Dateisysteme kann nicht geändert werden

Wegen eines Fehlers im ext4-Code ist es derzeit nicht möglich, die Größe von ext4-Dateisystemen zu ändern, wenn diese 1 Kilobyte Blockgröße haben und kleiner als 32 Megabytes sein.

Wiederholter Verbindungsverlust mit iSER-aktivierten iSCSI-Zielen

Bei der Verwendung des Servers als ein iSER-aktiviertes iSCSI-Ziel tritt ein wiederholter Verbindungsverlust auf, das Ziel antwortet nicht mehr und der Kernel reagiert nicht mehr. Um dieses Problem zu umgehen, minimieren Sie iSER-Verbindungsverluste oder setzen Sie auf nicht-iSER iSCSI-Modus zurück.

SCSI mittlere Schicht ruft I/O-System auf, bis Abschalten von System erzwungen wird

Gibt ein Speicher-Array einen CHECK CONDITION Status wieder, aber die Sense-Daten sind ungültig, so unternimmt der Code der mittleren Schicht des Small Computer Systems Interface (SCSI) einen weiteren Versuch den I/O-Vorgang auszuführen. Erhalten nachfolgende I/O-Vorgänge dasselbe Ergebnis, so versucht SCSI weiterhin unendlich oft den I/O-Vorgang auszuführen. Für diesen Fehler gibt es derzeit keine Problemumgehung.

Red Hat Beta öffentliches Schlüsselzertifikat muss manuell geladen werden

Der Systemadministrator kann den Machine Owner Key (MOK) Mechanismus dazu verwenden, das entsprechende Red Hat Beta öffentliche Schlüsselzertifikat zu laden, das für die Authentifizierung des in einer Red Hat Enterprise Linux Beta Release enthaltenen Kernels erforderlich ist. Die Einschreibung des Red Hat Certificate Authority (CA) Beta öffentlichen Schlüssels ist ein einmaliger Vorgang an jedem System, an dem Red Hat Enterprise Linux 7.2 Beta mit aktiviertem UEFI Secure Boot ausgeführt wird:

1. Schalten Sie UEFI Secure Boot ab und installieren Sie Red Hat Enterprise Linux 7.2 Beta.

2. Installieren Sie das kernel-doc-Paket, falls es nicht bereits installiert ist. Es liefert eine Zertifikatsdatei, die den Red Hat CA öffentlichen Beta-Schlüssel in der Datei: /usr/share/doc/kernel-keys/<kernel-ver>/kernel-signing-ca.cer enthält, wobei <kernel-ver> der Kernelversionsstring ohne den Plattform-Architekture-Suffix ist, z.B. 3.10.0-314.el7.

3. Fragen Sie manuelle mittels des mokutil-Dienstprogramms um das Enrollment des öffentlichen Schlüssels bei der Machine Owner Key (MOK) Liste im System an. Führen Sie als root-Benutzer den folgenden Befehl aus:

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

Sie werden dazu aufgefordert, ein Passwort für die Enrollment-Anfrage bereitzustellen.

4. Beim nächsten Booten des Systems werden Sie in der Systemkonsole zur Fertigstellung des Enrollments der MOK-Anfrage aufgefordert. Sie müssen den Eingabeaufforderungen nachkommen und das mokutil in Schritt 3 angegebene Passwort eingeben.

5. Wenn Sie das MOK-Enrollment beendet haben wird das System zurückgesetzt und startet neu. Sie können UEFI Secure Boot bei diesem Neustart oder einem der späteren Neustarts wieder aktivieren.

Kapitel 31. Netzwerk

Zeitüberschreitungsrichtlinie in Red Hat Enterprise Linux 7.2 Kernel nicht aktiviert

Der **`nfct timeout`**-Befehl wird in Red Hat Enterprise Linux 7.2 nicht unterstützt. Um das Problem zu umgehen, benutzen Sie die allgemeinen Zeitüberschreitungswerte unter **`/proc/sys/net/netfilter/nf_conntrack_*_timeout_*`**, um den Zeitüberschreitungswert einzustellen.

Kapitel 32. System- und Subskriptionsverwaltung

Unvollständige Registrierung im Falle eines Fehlers

Schlägt die Registrierung eines Systems im Subscription Manager GUI fehl, so wird das Hauptregistrierungsfenster nicht geschlossen, wenn der Benutzer im Fehlerdialog **OK** klickt. Die Folge ist, dass das Hauptregistrierungsfenster offen bleibt und zwar in einem Zustand, in dem die Aufgabe nicht erfolgreich beendet werden kann.Dieses Problem tritt zum Beispiel auf, wenn der Benutzer ungültige Anmeldeinformationen eingibt oder automatische Verknüpfung für die Registrierung verwendet wird. Um dieses Problem zu umgehen, klicken Sie auf die **Cancel**-Schaltfläche im Hauptregistrierungsfenster, wenn während des Vorgangs ein Fehler auftritt.

Nicht funktionierende Back-Schaltfläche im Subskriptionsmanager-Add-on bei der Ersteinrichtung

Die **Back**-Schaltfläche des ersten Panels des Subskriptionsmanager-Add-ons für das Ersteinrichtungsdienstprogrammfunktioniert nicht. Um dieses Problem zu umgehen, klicken Sie auf **Done** ganz oben in der Ersteinrichtungund verlassen Sie den Registrierungs-Workflow.

Kapitel 33. Virtualisierung

Problematische GRUB 2 Navigation mit KVM

Bei der Verwendung der seriellen Konsole durch KVM führt das längere Drücken der Pfeiltaste zur Navigation im GRUB 2-Menü zu erratischem Verhalten. Um dieses Problem zu umgehen, vermeiden Sie die schnelle Eingabe, die durch das lange Drücken der Pfeiltaste verursacht wird.

Die Größenänderung von GUID Partition Table (GPT) Disks führt bei Hyper-V-Gästen zu Fehlern in der Partitionstabelle

Der Hyper-V-Manager unterstützt die Größenreduzierung einer GPT-partitionierten Disk an einem Gast, wenn nach der letzten Partition freier Platz vorhanden ist, indem der Benutzer den unbenutzten letzten Teil der Disk fallenlassen kann. Allerdings wird durch diesen Vorgang der sekundäre GPT-Header auf der Disk gelöscht, was zu Fehlermeldungen führen kann, wenn der Gast die Partitionstabelle untersucht (zum Beispiel bei parted(8)). Dies ist ein bekanntes Problem bei Hyper-V.

Um dieses Problem zu umgehen kann der sekundäre GPT-Header manuell mit dem gdisk(8) expert-Befehl **e** wiederhergestellt werden, nachdem die Größe der GPT-Disk reduziert wurde. Dies kommt ebenfalls vor, wenn die Expand-Option von Hyper-V verwendet wird, kann jedoch ebenfalls mit dem parted(8)-Tool behoben werden.

Anhang A. Komponentenversionen

Dieser Anhang zeigt eine Liste von Komponenten und deren Versionen in der Red Hat Enterprise Linux 7.2 Release.

Tabelle A.1. Komponentenversionen

Komponente	Version
Kernel	3.10.0-306.0.1
QLogic **`qla2xxx`**-Treiber	8.07.00.08.07.1-k1
QLogic **`qla4xxx`**-Treiber	5.04.00.04.07.01-k0
Emulex **`lpfc`**-Treiber	10.2.8021.1
iSCSI-Initiator-Dienstprogramme	*iscsi-initiator-utils-6.2.0.873-32*
DM-Multipath	*device-mapper-multipath-0.4.9-82*
LVM	*lvm2-2.02.128-1*

Anhang B. Versionsgeschichte

Version 0.0-1.16.2 **Thu Nov 12 2015** **Francesco Valente**

Translation completed

Version 0.0-1.16.1 **Thu Nov 12 2015** **Francesco Valente**

Übersetzungsdateien synchronisiert mit XML-Quellen 0.0-1.16

Version 0.0-1.16 **Mon Oct 12 2015** **Lenka Špačková**

Hat mehrere neue Features und bekannte Probleme hinzugefügt.

Version 0.0-1.15 **Thu Oct 8 2015** **Lenka Špačková**

Hat Bekannte Probleme neu strukturiert und diesem Kapitel mehrere Elemente hinzugefügt. Hat Architekturen hinzugefügt und die Technologievorschau aktualisiert.

Version 0.0-1.14 **Thu Oct 1 2015** **Lenka Špačková**

Hat Gerätetreiber aktualisiert und mehrere bekannte Probleme hinzugefügt.

Version 0.0-1.13 **Wed Sep 16 2015** **Lenka Špačková**

Hat mehrere Feature-Beschreibungen und bekannte Probleme hinzugefügt.

Version 0.0-1.10 **Wed Sep 09 2015** **Laura Bailey**

Hat Treiber-Aktualisierungen für 7.2 Beta hinzugefügt.

Version 0.0-1.9 **Wed Sep 09 2015** **Laura Bailey**

Hat bekannte Probleme im Zusammenhang mit der OverlayFS-Technologievorschau hinzugefügt.

Version 0.0-1.8 **Mon Sep 07 2015** **Laura Bailey**

Neuverfassen der Versionshinweise basierend auf Features und Vorteilen, Kernelparameter-Änderungen, bekannte Probleme, Treiberaktualisierungen und Technologievorschau.

Version 0.0-1.7 **Fri Sep 04 2015** **Laura Bailey**

Hinzufügen von Elementen zur Technologievorschau der Versionshinweise.

Version 0.0-1.4 **Mon Aug 31 2015** **Laura Bailey**

Release der Red Hat Enterprise Linux 7.2 Beta Versionshinweise.