



Red Hat Enterprise Linux 7

7.4 リリースノート

Red Hat Enterprise Linux 7.4 リリースノート

Red Hat Enterprise Linux 7 7.4 リリースノート

Red Hat Enterprise Linux 7.4 リリースノート

Red Hat Customer Content Services

法律上の通知

Copyright © 2017-2019 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

本リリースノートでは、Red Hat Enterprise Linux 7.4 での改良点および実装された追加機能の概要、本リリースにおける既知の問題などを説明します。また、重要なバグ修正、テクニカルレビュー、非推奨の機能などの詳細も説明します。

目次

はじめに	18
第1章 概要	19
セキュリティ	19
ID 管理	19
ネットワーク	19
カーネル	20
ストレージとファイルシステム	20
ツール	20
高可用性	20
仮想化	20
管理および自動化	21
Red Hat Insights	21
Red Hat Customer Portal Labs	21
第2章 アーキテクチャー	22
第3章 外部のカーネルパラメーターに対する重要な変更	23
更新された /PROC/SYS/KERNEL エントリー	23
更新された /PROC/SYS/USER エントリー	23
カーネルパラメーター	24
パート I. 新機能	26
第4章 全般的な更新	27
Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 7 へのインプレースアップグレード	27
ベースチャンネルに移動した cloud-init	27
第5章 認証および相互運用性	28
コンテナの SSSD が完全にサポートされるようになりました。	28
Identity Management が FIPS に対応	28
SSSD は、ユーザーがスマートカードで認証する際の Kerberos チケットの取得に対応しています。	28
SSSD を使用すると、同じスマートカード証明書を使用して別のユーザーアカウントにログインできます。	28
IdM Web UI により、スマートカードログインが有効になります。	29
新規パッケージ: keycloak-httpd-client-install	29
新しい Kerberos 認証情報キャッシュタイプ: KCM	29
AD ユーザーは Web UI にログインして、セルフサービスページにアクセスできます。	29
SSSD により、SSSD サーバーモードで AD サブドメインの設定が可能になります。	30
SSSD は、AD 環境でユーザーおよびグループの検索と、短縮名を使用した認証に対応しています。	30
SSSD は、UID または SID を使用しないセットアップで、ユーザーおよびグループの解決、認証、および認可に対応します。	30
SSSD で sssctl user-checks コマンドが導入されました。これは、1回の操作で SSSD の基本機能をチェックします。	31
サービスとしてのシークレットへのサポート	31
IdM を使用すると、外部 DNS サーバーで IdM DNS レコードの半自動アップグレードが可能になります。	31
IdM が、SHA-256 証明書および公開鍵フィンガープリントを生成するようになりました。	31
IdM は、スマートカード証明書をユーザーアカウントにリンクするための柔軟なマッピングメカニズムに対応します。	31
新しいユーザー空間ツールにより、より便利な LMDB デバッグが可能になりました。	32
openldap がバージョン 2.4.44 にリベースされました。	32
Identity Management での DNS ルックアップのセキュリティ改善とサービスプリンシパルルックアップの堅牢性	32
samba がバージョン 4.6.2 にリベースされました。	32

authconfig は、スマートカードでユーザーを認証するために SSSD を有効化できる	33
authconfig がアカウントロックを有効にできるようになりました。	33
IdM サーバーのパフォーマンスの改善	33
IdM Web UI のデフォルトのセッション有効期限が変更されました。	34
dbmon.sh スクリプトは、インスタンス名を使用して Directory Server インスタンスに接続するようになりました。	34
Directory Server が SSHA_512 パスワードストレージスキームをデフォルトとして使用するようになりました。	34
Directory Server が tcmmalloc メモリアロケーターを使用するようになりました。	34
Directory Server が nunc-stans フレームワークを使用するようになる	34
Directory Server memberOf プラグインのパフォーマンス向上	34
Directory Server がエラーログファイルで重大度レベルのログを記録するようになりました。	35
Directory Server が PBKDF2_SHA256 パスワードストレージスキームに対応	35
Directory Server での自動チューニングのサポートが改善されました。	35
新しい PKI 設定パラメーターにより、TCP keepalive オプションを制御できます。	35
PKI サーバーが、強力な暗号化を使用して PKCS #12 ファイルを作成するようになりました。	35
暗号化操作に使用できる CC 準拠のアルゴリズム	36
TPS インターフェイスでメニュー項目の表示を設定できるようにする新しいオプション	36
Subject Alternative Name エクステンションに、証明書の Subject Common Name をコピーするプロファイルコンポーネントの追加	36
LDIF のインポート前に LDAP エントリーを削除する新しいオプション	36
Certificate System が外部認証ユーザーに対応するようになりました。	36
Certificate System が、証明書および CRL 公開の有効化および無効化に対応するようになりました。	36
searchBase 設定オプションが DirAclAuthz PKI サーバープラグインに追加されました。	37
パフォーマンス向上のため、Certificate System が一時的にサポートされるようになりました。	37
PKI デプロイメント設定ファイルのセクションヘッダーでは、大文字と小文字が区別されなくなりました。	37
Certificate System は、FIPS が有効な Red Hat Enterprise Linux 上の HSM を使用した CA のインストールをサポートする	37
CMC 要求では、AES および 3DES の暗号化にランダム IV が使用されるようになりました。	37
第6章 クラスタリング	39
clufteer がバージョン 0.76.0 にリベースされ、完全にサポートされるようになる	39
Pacemaker クラスタにおけるクォーラムデバイスのサポート	39
Booth クラスタチケットマネージャーのサポート	40
SBD デーモンで共有ストレージを使用するために追加されたサポート	40
CTDB リソースエージェントへの完全なサポート	40
High Availability and Resilient Storage Add-Ons が、IBM POWER (リトルエンディアン) で利用できるようになりました。	40
pcs が、暗号化された corosync 通信でクラスタを設定できるようになりました。	40
リモートノードおよびゲストノードのサポートおよび削除に使用される新しいコマンド	40
pcsd バインドアドレスの設定機能	40
監視操作を無効にする pcs resource unmanage コマンドの新しいオプション	41
場所の制約を設定する際の pcs コマンドラインでの正規表現のサポート	41
正規表現またはノード属性とその値によるフェンシングトポロジーのノードの指定	41
リソースエージェント Oracle および OraLsnr の Oracle 11g のサポート	41
共有ストレージでの SBD の使用のサポート	41
NodeUtilization リソースエージェントのサポート	41
第7章 コンパイラおよびツール	43
pcp がバージョン 3.11.8 にリベース	43
systemtap がバージョン 3.1 にリベース	43
valgrind がバージョン 3.12 にリベース	43
新規パッケージ: unitsofmeasurement	44
HTTP クライアントの SSL/TLS 証明書の検証が、Python 標準ライブラリーでデフォルトで有効になりました。	

%gemspec_add_dep および %gemspec_remove_dep のサポートが追加されました。	44
ipmitool がバージョン 1.8.18 にリベース	44
IBM Power のリトルエンディアンバリエーション用に更新された lshw	44
perf が Intel Xeon v5 でアンコアイベントに対応	44
dmidecode が更新される	44
iSCSI が targetcli を使用した ALUA 操作の設定に対応	45
jansson がバージョン 2.10 にリベース	45
egrep および fgrep 用の新しい互換性環境変数	45
lastcomm が --pid オプションをサポートするようになりました。	45
新規パッケージ: perl-Perl4-CoreLibs	45
アーカイブから抽出する際に tar がディレクトリーへのシンボリックリンクに従うようになりました。	45
IO::Socket::SSL Perl モジュールが TLS バージョンの制限をサポート	45
Net::SSLLeay Perl モジュールが TLS バージョンの制限をサポート	45
wget が TLS プロトコルバージョンの仕様をサポートするようになりました	46
tcpdump がバージョン 4.9.0 にリベース	46
tcpdump のキャプチャー方向を設定するオプションが -P から -Q に変更になりました。	46
OpenJDK が 64 ビット ARM アーキテクチャーで SystemTap に対応	46
sos がバージョン 3.4 にリベース	46
targetd がバージョン 0.8.6 にリベース	46
shim がバージョン 12-1 にリベース	47
rubygem-abrt がバージョン 0.3.0 にリベース	47
新規パッケージ: http-parser	47
すべてのデフォルトの POSIX ミューテックスに対する Intel および IBM POWER のトランザクションメモリーのサポート	47
glibc がグループマージをサポートするようになりました。	47
glibc が、IBM POWER9 アーキテクチャーで最適化された文字列比較機能に対応	48
Intel SSE、AVX、および AVX512 の機能を使用して動的に読み込まれたライブラリーのパフォーマンスが改善されました。	48
elfutils がバージョン 0.168 にリベース	48
bison がバージョン 3.0.4 にリベース	48
システムのデフォルトの CA バンドルは、コンパイル済みデフォルト設定または Mutt の設定でデフォルトとして設定されています。	48
objdump 混合リストの速度	48
fjes ドライバーから人間が読める形式の出力に対する ethtool サポート	49
ecj がバージョン 4.5.2 にリベース	49
rhino がバージョン 1.7R5 にリベース	49
scap-security-guide および oscap-docker がコンテナをサポート	49
第8章 デスクトップ	50
GNOME がバージョン 3.22.3 にリベース	50
xorg-x11-drv-libinput ドライバーが X.Org 入力ドライバーに追加されました。	50
一部の Intel および nVidia ハードウェアにおけるデフォルトドライバーの変更	50
dconf-editor が別のパッケージで提供されるようになりました。	50
第9章 ファイルシステム	51
SELinux セキュリティーラベルが OverlayFS ファイルシステムでサポートされるようになる	51
NFSv4.1 サーバーが完全にサポートされるようになりました。	51
autofs が amd 形式マップの参照オプションに対応	51
ログの検索を容易にするため、autofs がマウント要求ログエントリーの識別子を提供するようになりました。	51
SSI 環境で IBM z Systems の GFS2 をサポート	51
gfs2-utils がバージョン 3.1.10 にリベース	52
FUSE が lseek 呼び出しで SEEK_HOLE および SEEK_DATA をサポート	52

NFS サーバーが限られたコピーオフロードをサポート	52
SELinux は GFS2 ファイルシステムでの使用がサポートされる	52
NFSv4.1 クライアントとサーバーが Kerberos 認証をサポート	53
rpc.idmapd が DNS からの NFSv4 ID ドメインの取得をサポート	53
NFSv4.1 がデフォルトの NFS マウントプロトコルになる	53
nfs-utils 設定オプションの設定は、nfs.conf で一元化されています。	53
特定のワークロードで、NFSv4.1 マウントのロックパフォーマンスが改善される	54
CephFS カーネルクライアントは Red Hat Ceph Storage 3 で完全にサポートされる	54
第10章 ハードウェアの有効化	55
ハードウェアユーティリティツールが、最近リリースされたハードウェアを正しく識別できるようになりました。	55
今後のタブレットをサポートするために 7.4 で導入された新しい Wacom ドライバー	55
Wacom カーネルドライバが ThinkPad X1 Yoga タッチスクリーンをサポート	55
タッチ機能が Wacom Cintiq 27 QHDT タブレットに追加されました。	55
AMDGPU が Southern Islands、Sea Islands、Volcanic Islands、および Arctic Islands のチップセットをサポート	55
AMD モバイルグラフィックスへのサポートの追加	56
Netronome NFP デバイスがサポートされている	56
nvme-cli がバージョン 1.3 にリベース	56
キューに入れられたスピロックは Linux カーネルに実装されています。	56
RAPL が Intel Xeon v2 サーバーをサポート	56
Intel Platform Controller Hub [PCH] デバイスへのさらなる対応	56
IBM Power および s390x でハードウェアアクセラレーションされた zLib の使用を可能にする genwqe-tools が同梱されています。	56
librtas がバージョン 2.0.1 にリベース	57
NFP ドライバー	57
Nouveau で最新の NVIDIA カードを有効にする	57
Wacom ExpressKey Remote のサポート	57
Wacom Cintiq 27 QHD が ExpressKey Remote をサポート	57
第11章 インストールおよび起動	58
Anaconda を使用すると、RAID チャンクサイズを設定できます。	58
Anaconda テキストモードが iPSec インターフェイスに対応	58
inst.debug を使用すると、Anaconda インストールの問題をより簡単にデバッグできます。	58
キックスタートのインストールに失敗すると、%onerror スクリプトが自動的にトリガーされる	58
Anaconda は、インストールを開始する前にネットワークが使用可能になるのを待機します。	58
stage2 またはキックスタートファイルのネットワーク上の場所を複数指定して、インストールの失敗を防ぐことができます。	58
キックスタートファイルの autopart --nohome は、自動パーティション設定で /home/ の作成を無効にします。	59
ハードディスクドライブおよび USB からのドライバーディスクの読み込みが有効化されている	59
LVM シンプルの自動パーティショニング動作の変更	60
32 ビットのブートローダーが、64 ビットのカーネルを UEFI で起動できるようになりなる	60
Lorax が SSL エラーを無視できるようになる	60
shim-signed がバージョン 12 にリベース	60
gnu-efi がバージョン 3.0.5.-9 にリベース	61
killproc () および status () の後方互換性が有効化されました。	61
DHCP_FQDN を使用すると、システムの完全修飾ドメイン名を指定できます。	61
これで、インストールプロセス時に、論理ボリュームのシンクナップショットを作成できるようになります。	61
第12章 カーネル	63
RHEL 7.4 のカーネルバージョン	63

NVMe ドライバーがカーネルバージョン 4.10 にリベース	63
crash がバージョン 7.1.9 にリベース	63
crash が IBM Power ISA 3.0 の vmcore ダンプを分析するようになりました。	63
IBM Power および IBM Power のリトルエンディアンバリエーション向けに更新された crash memkind がバージョン 1.3.0 に更新されました。	63
カーネルに追加された jitter エントロピー RNG	64
/dev/random が、urandom プールの初期化に関する通知と警告を表示するようになりました。	64
fjes がバージョン 1.2 に更新されました。	64
ユーザー名空間の完全なサポート	64
makedumpfile がバージョン 1.6.1 に更新される	65
QAT が最新のアップストリームバージョンに更新された	65
intel-cmt-cat パッケージの追加	65
i40e が信頼できる VF と信頼できない VF をサポート	65
OVS 802.1ad (QinQ) のカーネルサポート	66
共有メモリーと hugetlbfs のコピー後のライブマイグレーションサポート	66
新規パッケージ: dbxtool	66
mlx5 が SRIOV で信頼される VF をサポート	66
バックポートされた 4.9 カーネルからの rwsem パフォーマンス更新	66
Linux カーネルに追加された getrandom	67
新しいステータス行 Umask が /proc/<PID>/status に含まれます。	67
Intel® Omni-Path Architecture (OPA) ホストソフトウェア	67
XTS-AES の鍵認証が FIPS 140-2 の要件を満たす	67
IBM z Systems で mlx5 に対応	67
perf ツールがプロセッサのキャッシュライン競合検出に対応	68
lpfc ドライバーでの SCSI-MQ のサポート	68
第13章 REAL-TIME KERNEL	69
Red Hat Enterprise Linux for Real Time Kernel について	69
kernel-rt のリベース	69
第14章 ネットワーク	70
NetworkManager がバージョン 1.8 にリベース	70
NetworkManager がルートの追加機能に対応	70
NetworkManager がデバイスの状態をより適切に処理	70
NetworkManager が MACsec (IEEE 802.1AE)に対応	70
NetworkManager が 802-3 リンクプロパティの変更と強制に対応	70
NetworkManager がデバイス名に基づくボンディングスレーブの順序に対応	71
NetworkManager が SR-IOV デバイスの VF をサポート	71
カーネル GRE がバージョン 4.8 にリベース	71
dnsmasq がバージョン 2.76 にリベース	72
BIND は、URI リソースレコードの処理方法を変更し、URI の後方互換性にも影響を及ぼします。	73
Microsoft Azure クラウドの DDNS に追加された DHCP クライアントフックの例	73
dhcp_release6 が IPv6 アドレスをリリース	74
Sendmail が ECDHE をサポート	74
telnet が -6 オプションをサポート	74
Unboundで負の DNS 応答をキャッシュする調整可能な TTL 制限	74
UDP ソケットのスケラビリティの改善	74
IP がカーネルの IP_BIND_ADDRESS_NO_PORT をサポート	74
IPVS ソースハッシュスケジューリングが L4 ハッシュおよび SH フォールバックをサポート	74
iproute がブリッジポートオプションの変更をサポート	75
SCTP (RFC 6458) のソケット API 拡張の新しいオプションが実装される	75
ss が SCTP ソケットリストをサポート	75
wpa_supplicant がバージョン 2.6 にリベース	75

Linux カーネルに switchdev インフラストラクチャーと mlxswが含まれるようになりました	75
Linux ブリッジコードがバージョン 4.9 にリベース	77
bind-dyndb-ldap がバージョン 11.1 にリベース	78
Red Hat Enterprise Linux に追加された BIND のアップストリームバージョン 9.11.0 の DynDB API	78
tboot がバージョン 1.9.5 にリベース	78
rdma-core バージョン 13 へのリベースにより統合された rdma に関連するパッケージ	79
静的 MAC アドレスへの OVN IP アドレス管理サポートの追加	81
マルチホームホストでのネットワーク信頼性の強化	81
GENEVE トンネル、VXLAN トンネル、GRE トンネルのオフロードをサポート	81
トンネルトラフィックの LCO をサポート	81
NIC でのトンネルパフォーマンスの改善	81
NPT がカーネルでサポートされるようになりました。	81
D-Bus API を介して DNS 設定をサポート	81
PPP のサポートは別のパッケージへ移動	82
tc ユーティリティーが flower をサポート	82
SCTP 転送パスでの CRC32c 値の計算を修正しました。	82
新規パッケージ: iperf3	82
OVN のインストールで、簡単に設定可能な firewalld ルールがサポートされるようになりました。	82
netlink がブリッジマスター属性に対応	82
第15章 セキュリティー	83
新規パッケージ: tang、clevis、jose、luksmeta	83
新規パッケージ: usbguard	83
openssh がバージョン 7.4 にリベース	84
audit がバージョン 2.7.6 にリベース	85
opencsc がバージョン 0.16.0 にリベース	86
openssl がバージョン 1.0.2k にリベース	86
openssl-ibmca がバージョン 1.3.0 にリベース	87
OpenSCAP 1.2 は NIST 認定済み	87
libreswan がバージョン 3.20 にリベース	87
監査がセッション ID に基づくフィルターリングをサポート	88
libseccomp が IBM Power アーキテクチャーに対応	88
AUDIT_KERN_MODULE がモジュールロードを記録するようになりました。	88
OpenSSH が公開鍵署名に SHA-2 を使用するようになりました。	88
firewalld が追加の IP セットに対応	89
firewalld がリッチルールでの ICMP タイプに対するアクションに対応	90
firewalld が無効なヘルパー割り当てに対応	90
nss と nss-util がデフォルトで SHA-256 を使用	90
監査フィルターの除外ルールに追加フィールドが含まれる	90
PROCTITLE が監査イベントで完全なコマンドを提供するようになりました。	91
nss-softokn がバージョン 3.28.3 にリベース	91
libica がバージョン 3.0.2 にリベース	91
opencryptoki がバージョン 3.6.2 にリベース	91
AUDIT_NETFILTER_PKT イベントが正規化される	92
p11tool が、保存された ID を指定してオブジェクトの書き込みをサポートするようになりました	92
新規パッケージ: nss-pem	92
pmrfc3164 は、rsyslog の pmrfc3164sd を置き換えます	92
libreswan が right=%opportunisticgroup をサポート	92
ca-certificates が Mozilla Firefox 52.2 ESR の要件を満たす	93
nss が、証明書に関する Mozilla Firefox 52.2 ESR 要件を満たすようになりました。	93
scap-security-guide がバージョン 0.1.33 にリベース	93
第16章 サーバーおよびサービス	95

chrony がバージョン 3.1 にリベース	95
linuxptp がバージョン 1.8 にリベース	95
tuned がバージョン 2.8.0 にリベース	96
logrotate が /var/lib/logrotate/logrotate.status をデフォルトの状態ファイルとして使用するようになりました。	96
rsyslog がバージョン 8.24.0 にリベース	96
mod_nssの新しいキャッシュ設定オプション	98
データベースオプションおよび接頭辞オプションが nss_pcacheから削除されました。	98
新規パッケージ: libfastjson	98
tuned が initrd オーバーレイをサポート	98
openwsman が特定の SSL プロトコルの無効化に対応	99
rear がバージョン 2.0 にリベース	99
python-tornado がバージョン 4.2.1 にリベース	99
第17章 ストレージ	101
RAID レベルのテイクオーバーの LVM でのサポートが追加されました。	101
LVM が RAID 再成形をサポート	101
Device Mapper リニアデバイスが DAX をサポート	101
libstoragemgmt がバージョン 1.4.0 にリベース	101
mpt3sas がバージョン 15.100.00.00 に更新されました。	102
lpfc ドライバーの lpfc_no_hba_reset モジュールパラメーターが利用可能に	102
LVM が Veritas Dynamic Multi-Pathing システムを検出し、基本となるデバイスパスに直接アクセスしなくなる	102
libnvdimm カーネルサブシステムが PMEM サブディビジョンをサポート	103
multipathd が実行されていない場合の警告メッセージ	103
構造化された出力を提供するために multipathd に追加された c ライブラリーインターフェイス	103
新しい remove retries マルチパス設定値	103
新しい multipathd reset multipaths stats コマンド	103
新しい disable_changed_wwids mulitpath 設定パラメーター	103
HPE 3PAR アレイの組み込み設定を更新	104
NFINIDAT InfiniBox.* デバイスの組み込み設定の追加	104
device-mapper-multipath が max_sectors_kb 設定パラメーターをサポート	104
新しい detect_checker マルチパス設定パラメーター	104
マルチパスに Nimble Storage デバイス用のデフォルト設定が組み込まれる	105
LVM は、RAID 論理ボリュームのサイズの縮小をサポートします	105
iprutils がバージョン 2.4.14 にリベース	105
mdadm がバージョン 4.0 にリベース	105
シンプールが 50% 以上使用されると、LVM はシンプール論理ボリュームのサイズを拡張します。	105
LVM が dm-cache メタデータバージョン 2 をサポート	106
指定されたハードウェアでの DIF/DIX (T10 PI) のサポート	106
dmstats 機能により変更されるファイルの統計の追跡が可能に	108
キャッシュされた論理ボリュームのシンスナップショットのサポート	108
新規パッケージ: nvmetcli	108
デバイス DAX が NVDIMM デバイスで利用可能に	108
第18章 システムおよびサブスクリプション管理	109
yumに追加された新しい payload_gpgcheck オプション	109
virt-whoでは、プロキシーなしの設定を利用できます。	109
virt-who は、独立した間隔設定を考慮します。	109
virt-who-passwordに追加されたパスワードオプション	109
一部の virt-who 設定パラメーターでは、正規表現とワイルドカードを使用できます。	109
virt-who 設定ファイルは管理が簡単	110
第19章 仮想化	111

Amazon Web Services の ENA ドライバー	111
Synthetic Hyper-V FC アダプターは storvsc ドライバーによりサポートされています。	111
親 HBA は WWNN/WWPN ペアでの定義が可能	111
libvirt がバージョン 3.2.0 にリベース	111
KVM が MCE をサポート	111
tun/tap デバイスでの rx バッチのサポートを追加	112
libguestfs がバージョン 1.36.3 にリベース	112
QXL ドライバーの virt-v2v インストールの改善	112
virt-v2v は、ディスクイメージを qcow2 形式 1.1 にエクスポートできる	112
追加の virt ツールは、LUKS ディスク全体で暗号化されたゲストで機能できます。	112
すべての libguestfs コマンドのタブ補完	113
サイズを変更したディスクは、リモートの場所に直接書き込むことができます。	113
ユーザー名前空間が完全にサポートされるようになりました。	113
Hyper-V のゲスト仮想マシンで PCI Express バスを介して接続するデバイス用にドライバーが追加されました	113
第20章 ATOMIC HOST とコンテナ	114
Red Hat Enterprise Linux Atomic Host	114
第21章 RED HAT SOFTWARE COLLECTIONS	115
パート II. 主なバグ修正	116
第22章 一般的な更新	117
Systemd への CtrlAltDelBurstAction の追加	117
cgred が NSS ユーザーおよびグループに関するルールを解決できるようになりました。	117
第23章 認証および相互運用性	118
yum が、ipa-client のインストール後にパッケージの競合を報告しなくなりました。	118
FIPS モードでは、slapd_pk11_getInternalKeySlot () 関数を使用して、トークンのキースロットを取得するようになりました。	118
Certificate System は、FIPS モードのシステムで Thales HSM でインストールに失敗しなくなりました。	118
pkispawn の依存関係一覧に、openssl が正しく含まれるようになる	118
PKI サーバードプロファイルフレームワークからのエラーメッセージがクライアントに渡されるようになる	118
インストール時に、Certificate System が Lightweight CA 鍵のレプリケーションを開始しない	119
PKI サーバーが、起動時にサブジェクト DN を正しく比較するようになりました。	119
不完全な証明書チェーンを持つ中間 CA に接続したときに、KRA のインストールが失敗しなくなりました。	119
証明書プロファイルの startTime フィールドが長い整数形式を使用するようになりました。	119
PKCS#11 トークンがログインしていないため、下位 CA のインストールに失敗しなくなりました。	119
pkispawn スクリプトが ECC 鍵サイズを正しく設定するようになりました。	119
FIPS モードでの CA クローンのインストールに失敗しなくなりました。	120
entryUSN 属性に 32 ビットより大きい値が含まれている場合に、PKI サーバーの起動に失敗しなくなりました。	120
Tomcat はデフォルトで IPv6 で動作する	120
pkispawn が無効な NSS データベースパスワードを生成しなくなりました。	120
--serial オプションを使用してユーザー証明書を追加するときに、証明書の取得が失敗しなくなりました。	120
エントリーが1つだけの場合、CA Web インターフェイスに空の証明書要求ページが表示されなくなりました。	120
コンテナ環境に PKI サーバーをインストールしても警告が表示されなくなる	121
G&D スマートカードを使用したトークンの再登録が失敗しなくなる	121
PKI サーバーは、起動時の証明書検証エラーの詳細を提供します。	121
PKI サーバーが LDAPProfileSubsystem プロファイルの再初期化に失敗しなくなる	121
HSM で生成された秘密鍵の抽出に失敗しなくなりました。	121
pkispawn が数字のみで設定されるパスワードを生成しなくなりました	121
CA 証明書が正しい信頼フラグでインポートされる	122

--usage verify オプションの使用時に対称鍵の生成に失敗しなくなりました。	122
後続の PKI インストールが失敗しなくなる	122
FIPS モードでの 2 段階の subordinate CA インストールに失敗しなくなる	122
監査ログは、証明書の要求が拒否またはキャンセルされたときに成功を記録しなくなりました。	122
セルフテストに失敗した PKI サブシステムが、システムの起動時に自動的に再度有効になるようになりました。	122
CERT_REQUEST_PROCESSED 監査ログエントリーに、エンコードされたデータではなく証明書のシリアル番号が含まれるようになりました。	123
LDAPProfileSubsystem プロファイルの更新で属性の削除に対応	123
第24章 クラスタリング	124
クラスターへの接続が管理対象外の場合でも、Pacemaker リモートがシャットダウンすることがある	124
pcs が、リモートノードとゲストノードの名前とホストを検証するようになりました。	124
pcs resource create コマンドの master オプションの新しい構文により、メタ属性を正しく作成可能	124
第25章 コンパイラーおよびツール	125
PCRE ライブラリーが、Unicode で必要な非 ASCII 印刷可能文字を正しく認識するようになりました。	125
Bundler を使用して依存関係を管理するアプリケーションが、JSON ライブラリーを適切にロードできるようになりました。	125
Git を HTTP または HTTPS および SSO で使用できるようになりました。	125
rescan-scsi-bus.sh --luns=1 は、1 で番号が付けられた LUN のみをスキャンするようになりました。	125
ps が待機チャンネル名から接頭辞を削除しなくなりました。	125
.history ファイルがネットワークファイルシステムにある場合、tcsh が応答しなくなる	125
fcoeadm --target が原因で fcoeadm がクラッシュしなくなる	126
tar オプション --directory は無視されなくなりました	126
tar オプション --xattrs-exclude および --xattrs-include が無視されなくなる	126
tar が増分バックアップを正しく復元するようになりました。	126
perl-homedir プロファイルスクリプトが csh をサポート	126
getaddrinfo が初期化されていないデータにアクセスしなくなる	127
glibc の malloc 実装で実行される追加のセキュリティーチェック	127
chrpath がバージョン 0.16 にリベース	127
system-config-language パッケージの翻訳の更新	127
ホスト名がドメイン部分がない場合に、Puci が不完全な From ヘッダーを持つ電子メールを送信しなくなりました。	127
strace は、open () 関数の O_TMPFILE フラグおよびモードを正しく表示します。	128
大規模なプログラムをリンクする際に ld が無限ループにならなくなる	128
非表示シンボルへのクロスオブジェクト参照に関する ゴールド 警告メッセージの修正	128
Denverton SOC 搭載の Intel Xeon® C3xxx プロセッサでの OProfile デフォルトイベントの修正	128
第26章 デスクトップ	129
Empathy が Google Talk の証明書チェーンを検証できるようになりました。	129
第27章 ファイルシステム	130
再試行タイムアウトを設定すると、SSSD からのマウントなしで autofs が起動しないようになりました。	130
autofs パッケージに README.autofs-schema ファイルと更新されたスキーマが含まれる	130
NIS サーバーに保存されているマップにアクセスするために automount を再起動する必要がなくなりました。	130
autofs でローカルマウントの可用性をチェックすると、失敗する前に長いタイムアウトが発生しなくなりました。	130
GFS2 ファイルシステムを読み取り専用としてマウントすると、ジャーナルはアイドルとマークされる	131
id コマンドで誤った UID および GID が表示されなくなる	131
ラベル付けされた NFS がデフォルトでオフになる	131
autofs マウントがシャットダウン状態に達した後に無限ループにならなくなる	131
名前空間の処理時に autofs の信頼性が向上しました。	132

第28章 インストールおよび起動	133
IBM z Series の1つの FBA DASD にインストールする場合に、自動パーティション設定が機能する	133
キックスタートがディスクから起動したときに、キックスタートで設定したブリッジのアクティベーションが失敗しなくなる	133
Anaconda がパスワードなしでユーザーを正しく作成可能に	133
最小インストールで open-vm-tools-desktop と依存関係がインストールされなくなる	133
Anaconda が無効なキックスタートファイルを生成しなくなる	133
Anaconda は名前で指定された RAID アレイの識別に失敗しなくなりました	134
キックスタートでは、短すぎるパスワードが使用できなくなりました。	134
初期セットアップが IBM z Systems の SSH 経由のグラフィカルインターフェイスで正しく開くようになる	134
位置情報サービスが有効になると、インストールに追加の時間が必要なくなりました。	134
新しい IP アドレスの追加時に、ifup-aliases スクリプトが Gratuitous ARP 更新を送信するようになりました。	134
netconsole ユーティリティーが正しく起動するようになりました。	135
rc.debug カーネルを使用すると、initscripts のデバッグが容易になります。	135
iSCSI または NFS でシステムが /usr で終了しなくなる	135
rhel-autorelabel がファイルシステムを破損しなくなりました。	135
rpmbuild コマンドが Perl が必要とするものを正しく処理するようになりました。	135
キックスタートで ignoredisk を使用する場合に、インストーラーが BIOS RAID デバイスを正しく認識するようになりました。	135
ifcfg-* ファイル内の値に対して一重引用符が機能するようになる	136
rhel-import-state が /dev/shm/ のアクセス権限を変更しなくなり、システムが正常に起動できるようになりました。	136
Red Hat Enterprise Linux 6 initscripts で後方互換性を有効化	136
initscripts が設定ファイルとして /etc/rwtab および /etc/statetab を指定するようになりました。	136
ifup スクリプトが NetworkManager の速度を低下させなくなりました。	136
GNOME の初期設定は、キックスタートの firstboot --disable コマンドで無効にできるようになりました。	137
NM_CONTROLLED の設定がすべての ifcfg-* ファイルで正しく機能するようになりました。	137
hostname が設定されていない場合、dhclient コマンドが誤って localhost を使用しなくなりました。	137
initscripts ユーティリティーが LVM2 を正しく処理するようになりました。	137
service network stop コマンドは、すでに停止されているサービスを停止しようとしなくなりました。	137
ループバックデバイスの ifdown が正常に動作するようになりました。	137
initscripts のスクリプトは、静的 IPv6 アドレスの割り当てをより強固に処理	137
Software Selection でアドオンオプションの選択を解除すると、ダブルクリックが必要なくなる	138
ターゲットシステムのホスト名は、キックスタートインストールでインストーラーの起動オプションを使用して設定可能に	138
Anaconda は、ネットワーク設定後にインストールソースの検証を要求しなくなる	138
自動インストールで、OEMDRV ラベルを使用するディスクが正常に無視されるようになる	138
第29章 カーネル	139
RAID 4 および RAID 10 の作成とアクティブ化を完全にサポート	139
kdump がレガシタイプ 12 NVDIMM で動作するようになる	139
ACL を継承するファイルの作成でマスクが失われなくなる	139
第30章 REAL-TIME KERNEL	140
USB を削除しても、MRG Realtime カーネルで may_sleep () 警告が発生しなくなりました。	140
第31章 ネットワーク	141
SNMP 応答がタイムアウトしなくなる	141
ICMP リダイレクトでカーネルがクラッシュしなくなる	141
net.ipv4.ip_nonlocal_bind カーネルパラメーターは名前空間で設定されます。	141
netfilter REJECT ルールが SCTP パケットで動作するようになりました。	141
NetworkManager が設定済みの DHCP_HOSTNAME との接続を複製しなくなりました。	141
改善された SCTP congestion_window 管理	142

DCTCP alpha の値は 0 にドロップし、cwnd は 137 を超える値に残ります。	142
ss が cwnd を正しく表示	142
cwnd の値が DCTCP を使用して増加しなくなりました。	142
負の範囲の一致が修正されました。	142
nmcli connection show コマンドが、empty と NULL の両方の値に正しい出力を表示するようになりました。	143
snmpd が AgentX サブエージェントからの大きなパケットを拒否しなくなりました。	143
macvlan を正しく登録解除できるようになりました。	143
第32章 セキュリティー	144
ユーザーが検索できないパスでの chrooting に依存する設定が適切に機能するようになる	144
firewalld がすべての ICMP タイプに対応	144
selinux-policy で docker.pp が container.pp に置き換えられる	144
最近追加されたカーネルクラスとパーミッションは、selinux-policy で定義されています。	144
nss が PKCS#12 ファイルを適切に処理	144
OpenSCAP が有用なメッセージおよび警告のみを生成するようになりました。	144
AIDE が syslog 形式でログを記録するようになりました。	145
OpenSCAP セキュリティー強化プロファイルを使用したインストールが続行される	145
OpenSCAP および SSG が、RHV-H システムを正しくスキャンできるようになりました。	145
OpenSCAP が、CVE OVAL フィードで非圧縮 XML ファイルも処理するようになりました。	145
第33章 サーバーおよびサービス	146
ReaR が Linux 機能を正しく保持	146
sblim-cmpi-fsvol は、DM でマウントされたファイルシステムを無効として表示しなくなりました	146
Cyrus SASL の SPNEGO が Microsoft Windows と互換性を持つようになる	146
MariaDB init スクリプトが失敗した場合にデータが失われなくなる	146
yppbind がネットワークへのアクセスが保証される前に起動しなくなる	146
yppbind が原因で、リモートユーザーのアカウント設定が再起動時にデフォルト設定に戻されなくなりました。	147
ネットワーク情報システムのセキュリティ機能が使用されたため yppasswd がクラッシュしなくなる	147
Evince が PostScript ファイルを再度表示	147
db_verify により libdb の空きミューテックスが不足しなくなりました。	147
一部の状況で ghostscript が応答しなくなる	148
postscript を PDF に変換しても ps2pdf が予期せず終了しなくなる	148
sapconf が、より高い kernel.shmall および kernel.shmmax の値で正しく機能するようになりました。	148
第34章 ストレージ	149
キャッシュ論理ボリュームで lvconvert --repair が適切に動作するようになりました。	149
LVM2 ライブラリーの非互換性によるデバイスの監視の失敗やアップグレード中の消失がなくなる	149
be2iscsi ドライバーエラーが原因でシステムが応答しなくなる	149
mirror セグメントタイプが使用されている場合、lvmetad デーモンで相互作用の問題が発生しなくなりました。	149
multipathd デーモンは、ブラックリストに登録されたデバイスの誤ったエラーメッセージを表示しなくなりました。	149
マルチパスが、使用可能なパスがない場合にデバイスの再読み込みにフラグを立てるようになりました。	149
書き込みに失敗した後に送信される読み取り要求は、常にマルチパスデバイスで同じデータを返します。	150
マルチパスデバイスのパスデバイスが読み取り専用に切り替わると、マルチパスデバイスが読み取り専用に再読み込みされます。	150
ユーザーは確認されていないマルチパスデバイスの混同する可能性のある古いデータを取得しなくなる	150
失敗したパスで Prioritizer を実行すると、multipathd デーモンがハングしなくなりました。	150
システムのアップグレード後、新しい RAID4 ボリューム、および既存の RAID4 または RAID10 論理ボリュームが正しくアクティブ化されるようになる	151
PV のステータスが間違っているため、LVM ツールがクラッシュしなくなる	151
第35章 システムおよびサブスクリプション管理	152

リポジトリが設定されていないシステムでアンダー クラウドが失敗しなくなりました。	152
yum -plugin-verify が提供する yum コマンドは、不一致が見つかった場合に終了ステータスを 1 に設定するようになりました。	152
第36章 仮想化	153
SeaBIOS は LUN がゼロ以外の SCSI デバイスを認識	153
libguestfs ツールは、/usr/ が root と同じパーティションにないゲストを正しく処理するようになりました。	153
virt-v2v は、Windows レジストリーが破損しているか、破損している Windows ゲストを変換できます。	153
virt-v2v を使用したシステム以外の動的ディスクでの Windows ゲストの変換が正しく機能するようになりました。	153
Glance クライアントのバージョンに関係なく、ゲストを Glance イメージに変換できます。	153
virt-v2vを使用して、Red Hat Enterprise Linux 6.2 - 6.5 ゲスト仮想マシンを変換できるようになりました。	154
/etc/fstab の btrfs エントリーが libguestfsによって正しく解析されるようになりました。	154
libguestfs が、認証を必要とする libvirt ドメインディスクを正しく開くことができるようになりました	154
変換した Windows UEFI ゲストが適切に起動する	154
virt-v2v ユーティリティが、プロキシ環境変数を一貫して無視するようになりました。	154
virt-v2v は、必要に応じて RHEV-apt.exe と rhsrvany.exe のみをコピーします。	154
ボンディングされたインターフェイスを介した VLAN を持つゲストは、フェールオーバー後にトラフィックの通過を停止しなくなる	155
virt-v2v は、<ovf:Name> 属性を持たない OVA をインポートします。	155
パート III. テクノロジープレビュー	156
第37章 一般的な更新	157
systemd-importd 仮想マシンとコンテナイメージのインポートおよびエクスポートサービス	157
第38章 認証および相互運用性	158
AD および LDAP の sudo プロバイダーの使用	158
DNSSEC が IdM でテクノロジープレビューとして利用可能になりました。	158
Identity Management JSON-RPC API がテクノロジープレビューとして利用可能になりました。	158
Custodia シークレットサービスプロバイダーが利用可能に	159
コンテナ化された Identity Management サーバーがテクノロジープレビューとして利用可能に	159
第39章 クラスタリング	160
pcs ツールが Pacemaker でバンドルリソースを管理	160
第40章 コンパイラーおよびツール	161
Shenandoah ガベージコレクター	161
第41章 ファイルシステム	162
ファイルシステム DAX が、テクノロジープレビューとして ext4 および XFS で利用可能	162
pNFS およびブロックレイアウトのサポート	162
OverlayFS	162
pNFS SCSI レイアウトクライアントおよびサーバーのサポートが提供されるようになりました。	163
Btrfs ファイルシステム	164
第42章 ハードウェアの有効化	165
利用可能な Trusted Computing Group TPM 2.0 System API ライブラリーおよび管理ユーティリティ	165
新規パッケージ: tss2	165
LSI Syncro CS HA-DAS アダプター	165
第43章 インストールおよび起動	166
rpm-buildでのマルチスレッドのxz圧縮	166
第44章 カーネル	167

HMM (heterogeneous memory management) 機能がテクノロジープレビューとして利用可能に	167
criu がバージョン 2.12 にリベース	167
kexec がテクノロジープレビューとして利用可能に	167
テクノロジープレビューとしての kexec fast reboot	167
名前空間への非特権アクセスは、テクノロジープレビューとして有効化できる	168
テクノロジープレビューとしての KASLR	168
柔軟なファイルレイアウトで NFSv4 pNFS クライアントを更新	168
CUIR 拡張スコープ検出	169
qla2xxx ドライバーでテクノロジープレビューとしての SCSI-MQ	169
テクノロジープレビューとしての Intel Cache Allocation Technology	169
第45章 REAL-TIME KERNEL	170
新規スケジューラークラス: SCHED_DEADLINE	170
第46章 ネットワーク	171
Cisco usNIC ドライバー	171
Cisco VIC カーネルドライバ	171
TNC (Trusted Network Connect)	171
qlcnic ドライバーの SR-IOV 機能	171
libnftnl パッケージおよび nftables パッケージ	171
オフロードサポートのある flower 分類子	172
第47章 RED HAT ENTERPRISE LINUX SYSTEM ROLES POWERED BY ANSIBLE	173
新規パッケージ: ansible	173
第48章 セキュリティー	174
テクノロジープレビューとして利用可能な tang-nagios サブパッケージおよび clevis-udisk2 サブパッケージ	174
USBGuard がテクノロジープレビューとして IBM Power で利用可能になりました。	174
第49章 ストレージ	175
SCSI 向けのマルチキュー I/O スケジューリング	175
libStorageMgmt API の Targetd プラグイン	175
DIF/DIX (Data Integrity Field/Data Integrity Extension) への対応	175
第50章 仮想化	176
KVM ゲスト用の USB 3.0 サポート	176
一部の Intel ネットワークアダプターが Hyper-V のゲストとして SR-IOV をサポート	176
VFIO ドライバーの No-IOMMU モード	176
ibmvnic デバイスドライバが追加されました。	176
virt-v2v が vmx 設定ファイルを使用して VMware ゲストを変換できるようになりました。	177
virt-v2v が Debian ゲストおよび Ubuntu ゲストを変換できる	177
Virtio デバイスでの vIOMMU の使用が可能に	177
OVMF (Open Virtual Machine Firmware)	177
パート IV. デバイスドライバ	178
第51章 新しいドライバ	179
ストレージドライバ	179
ネットワークドライバ	179
グラフィックドライバおよびその他のドライバ	180
第52章 更新されたドライバ	183
ストレージドライバの更新	183
ネットワークドライバの更新	183
グラフィックドライバおよびその他のドライバの更新	184

パート V. 非推奨の機能	186
第53章 RED HAT ENTERPRISE LINUX 7 での非推奨の機能	187
Identity Management に関連する非推奨のパッケージ	187
非推奨の安全でないアルゴリズムとプロトコル	187
ca-certificates パッケージから削除されたレガシー CA 証明書	192
coolkey が opensc に置き換えられる	192
rsyslog imudp モジュールの inputname オプションが非推奨に	192
FedFS が非推奨に	193
Btrfs が非推奨に	193
tcp_wrappers が非推奨に	193
nautilus-open-terminal が gnome-terminal-nautilus に置き換えられる	193
Python から削除された sslwrap ()	193
依存関係としてリンクされたライブラリーのシンボルが ld によって解決されない	194
Windows ゲスト仮想マシンのサポートが限定	194
libnetlink が非推奨に	194
KVM の S3 および S4 の電源管理状態が非推奨に	194
Certificate Server の udnPwDirAuth プラグインが廃止	194
IdM 向けの Red Hat Access プラグインが廃止	195
統合方式のシングルサインオン向けの Ipsilon 認証プロバイダーサービス	195
rsyslog のいくつかのオプションが非推奨に	195
memkind ライブラリーで非推奨のシンボル	195
SCTP (RFC 6458) のソケットの API 拡張オプションが非推奨に	197
SSLv2 および SSLv3 を使用した NetApp ONTAP の管理は、libstorageMgmt ではサポートされなくなりました。	197
dconf-dbus-1 が非推奨になり、dconf-editor が個別に提供されるようになりました。	197
FreeRADIUS が Auth-Type := System を受け入れなくなりました。	197
非推奨となったデバイスドライバー	198
SFN4XXX アダプターが非推奨に	203
Software-initiated-only FCoE ストレージ技術が非推奨に	203
libvirt-lxc ツールを使用するコンテナが非推奨に	203
パート VI. 既知の問題	205
第54章 認証および相互運用性	206
グループルックアップの実行時に sudo がアクセスを拒否する	206
KCM 認証情報キャッシュは、1つの認証情報キャッシュ内で多数の認証情報を行うには適していない	207
sss-d-secrets コンポーネントは、読み込み中にクラッシュする	207
SSSD が同じ優先順位を持つ複数の証明書一致ルールを正しく処理しません。	207
SSSD は、ID オーバーライドで一意的な証明書のみを検索できる	207
ipa-adviser コマンドは、スマートカード認証を完全に設定しません。	207
libwbclient ライブラリーが、Red Hat Enterprise Linux 7.4 でホストされる Samba 共有に接続できない	207
Certificate System subsystem で、TLS_ECDHE_RSA_* 暗号および特定の HSM で通信の問題が発生しました。	208
第55章 コンパイラーおよびツール	209
実行可能スタックが無効になっていると、JIT 技術で正規表現のパフォーマンスを向上できません。	209
Gluster ライブラリーをアンロードした後、特定のアプリケーションが終了しない場合、メモリーリークが発生する	209
DISA SRG への URL が正しくない	209
ensure_gpgcheck_repo_metadata ルールが失敗する	209
SSG pam_faillock モジュール使用率の確認で、default=die が正しく受け入れられない	210
第56章 デスクトップ	211
totem だけの更新に失敗する	211

オペレーティングシステムは、起動時に常に Wacom Expresskeys Remote (EKR) モード 1 を想定する	211
ダウンロードした RPM ファイルを Nautilus からインストールできない	211
Yelp が HTML 形式のファイルを正しく表示しない	211
一部の AMD ハードウェアでモニターを接続すると、自動モード設定が失敗する	212
依存関係がないため、LibreOffice なしでインストールした場合、GNOME ドキュメントが一部のドキュメントを表示できない	212
Application Installer は、ビッグエンディアンアーキテクチャーにはインストールできない場合でもパッケージを表示します。	212
ソフトウェアの追加/削除(gpk-application)は、最初の試行で新しくインポートされた鍵を使用しません。	212
複数の PCI デバイスを使用して複数のディスプレイを持つ仮想マシンのディスプレイのサイズを変更すると、X がクラッシュする	213
Nautilus は、GNOME クラシックセッションでアイコンを非表示にしません。	213
flatpak で依存関係が間違っている	213
Firefox が更新後に起動しない	213
Xorg でのビジュアルの限定的なサポート	214
第57章 ファイルシステム	215
NFSv4 を提供する NetApp ストレージアプライアンスの設定を確認することが推奨される	215
第58章 ハードウェアの有効化	216
i40e ドライバーが、最も一般的な HWTSTAMP フィルターを拒否する	216
第59章 インストールおよび起動	217
HTTPS キックスタートソースからインストールする場合、FIPS モードはサポートされない	217
UEFI および IPv6 を使用した PXE ブートは、オペレーティングシステム選択メニューの代わりに GRUB2 シェルを表示します。	217
英数字以外の文字で driverdisk パーティションを指定すると、無効な出力キックスタートファイルが生成されます	217
Scientific Computing バリエーションには、特定のセキュリティープロファイルに必要なパッケージがありません	217
第60章 カーネル	218
セカンダリーコアがオフラインでないと kexec が失敗する	218
キャッシュの誤ったフラッシュによるファイルシステムの破損が修正されたが、I/O 操作が遅くなる可能性がある	218
Wacom Cintiq 12WX のプラグを抜き、すぐに差しした場合に再検出されない	218
GUI の起動時に、Virtual DVD を使用して一部の IBM POWER8 マシンにインストールすると失敗する	218
キーボードショートカットを使用してフルスクリーンモードに入ると、VMWare ESXi 5.5 でディスプレイの問題が発生する	219
現在、xz 圧縮には対応していません。	219
第61章 ネットワーク	220
Red Hat Enterprise Linux 7 で、MD5 ハッシュアルゴリズムを使用した署名の検証が無効になる	220
RHEL 7.3 からアップグレードすると FreeRADIUS が失敗する可能性がある	220
第62章 セキュリティー	221
certutil は、FIPS モードで NSS データベースパスワード要件を返しません。	221
systemd-importd は init_t として実行されます。	221
キックスタートインストールでは、SCAP パスワードの長さの要件は無視されます。	221
rhnsd.pid はグループまたはその他の方法で書き込み可能	221
第63章 ストレージ	222
クラスター内の RAID 上でのシンプロビジョニングはサポートされていません	222
LVM または md デバイスに、以前のインストールからのメタデータがあると、Anaconda インストールが失敗する場合があります。	222

第64章 システムおよびサブスクリプション管理	223
rdma-core がインストールされていると、システムのアップグレードにより、Yum が不要な 32 ビットパッケージをインストールする可能性があります。	223
第65章 仮想化	224
OVMF ゲストの起動に失敗する	224
virsh iface-bridge を使用したブリッジの作成に失敗する	224
ゲストは、ESXi 5.5 で起動できない場合があります。	224
STIG for Red Hat Virtualization Hypervisor プロファイルは Anaconda に表示されない	224
付録A コンポーネントのバージョン	225
付録B コンポーネント別の BUGZILLAS の一覧	226
付録C 更新履歴	240

はじめに

個別のセキュリティー、機能拡張、バグ修正によるエラータなどを集約したものが Red Hat Enterprise Linux のマイナーリリースになります。『Red Hat Enterprise Linux 7.4 リリースノート』ドキュメントでは、今回のマイナーリリースで Red Hat Enterprise Linux 7 オペレーティングシステム、および付随するアプリケーションに追加された主な変更を説明します。また、既知の問題、および現在利用可能なすべてのテクノロジープレビューの詳細な一覧も紹介します。

他のバージョンと比較した Red Hat Enterprise Linux 7 の機能および制限は、<https://access.redhat.com/articles/rhel-limits> で利用可能な Red Hat ナレッジベースの記事を参照してください。

このリリースで配布されるパッケージは、[Red Hat EnterpriseLinux7 パッケージマニフェスト](#) に記載されています。Red Hat Enterprise Linux 6 からの移行は、[Migration Planning Guide](#) で説明されています。

Red Hat Enterprise Linux のライフサイクルに関する詳細は、<https://access.redhat.com/support/policy/updates/errata/> を参照してください。

第1章 概要

セキュリティ

- Red Hat Enterprise Linux 7.4 は、Network Bound Disk Encryption (NBDE) に対応しています。これにより、システム管理者は、システムの再起動時にパスワードを手動で入力する必要なく、ベアメタルマシンのハードドライブの root ボリュームを暗号化できます。
- **USBGuard** ソフトウェアフレームワークは、デバイス属性に基づく基本的なホワイトリスト機能およびブラックリスト機能を実装することにより、侵入型 USB デバイスに対するシステム保護を提供します。
- **OpenSSH** ライブラリーの更新には、Secure File Transfer Protocol (SFTP) で中断されたアップロードを再開する機能が含まれ、SHA-256 アルゴリズムを使用する新しいフィンガープリントタイプのサポートが追加されました。この **OpenSSH** バージョンでは、SSH-1 プロトコルのサーバー側のサポートも削除されます。
- 複数の新しい Linux 監査機能が追加され、管理が容易になり、Audit システムによって記録されるイベントのフィルタリング、重要なイベントからのより多くの情報収集、および大量のレコードの解釈が可能になりました。
- **OpenSC** のライブラリーおよびユーティリティーのセットにより、Common Access Card (CAC) カードのサポートが追加され、**CoolKey** アプレット機能も提供されるようになりました。
- **OpenSSL** の更新には、Datagram Transport Layer Security (DTLS) バージョン 1.2 プロトコル、Application-Layer Protocol Negotiation (ALPN) のサポートなど、複数の機能拡張が含まれています。
- **OpenSCAP** ツールは NIST 認定であるため、規制環境での採用が容易になります。
- 安全でないと思われる暗号プロトコルおよび暗号アルゴリズムは非推奨となっています。ただし、このバージョンでは、その他の暗号関連の改善も多数導入されています。詳細は、[???](#) および Red Hat カスタマーポータル [ナレッジベースの記事 Enhancing the Security of the Operating System with Cryptography Changes in Red Hat Enterprise Linux 7.4](#) を参照してください。

セキュリティ強化の詳細は、[15章 セキュリティ](#) を参照してください。

ID 管理

- コンテナの System Security Services Daemon (SSSD) に完全に対応しました。Identity Management (IdM) サーバーコンテナは、テクノロジープレビュー機能として利用できません。
- ユーザーは、FIPS モードが有効になっているシステムに、新しい Identity Management サーバー、レプリカ、およびクライアントをインストールできるようになりました。
- スマートカード認証に関連する機能拡張がいくつか導入されました。

IdM の変更の詳細は、[5章 認証および相互運用性](#) を参照してください。IdM に関連する非推奨の機能の詳細は、[???](#) を参照してください。

ネットワーク

- **NetworkManager** は、ルーティングの追加機能をサポートし、Media Access Control Security (MACsec) テクノロジーを有効にし、管理対象外デバイスを処理できるようになりました。

- Kernel Generic Routing Encapsulation (GRE) トンネリングが拡張されました。

ネットワーク機能の詳細は、[14章 ネットワーク](#)を参照してください。

カーネル

- NVMe Over Fabric のサポートが NVMe-Express カーネルドライバーに追加されました。これにより、イーサネットインフラストラクチャーまたは Infiniband ファブリックインフラストラクチャーの両方のデータセンターにある高パフォーマンスの NVMe ストレージデバイスにアクセスする際の柔軟性が向上します。

カーネル関連の変更は、[12章 カーネル](#)を参照してください。

ストレージとファイルシステム

- LVM は、RAID テイクオーバーに完全に対応します。これにより、ユーザーは RAID 論理ボリュームを1つの RAID レベルから別の RAID レベルに変換し、RAID 再成形を行うことができます。これは、RAID アルゴリズム、ストライプサイズ、イメージ数などのプロパティを再生成できます。
- Docker で OverlayFS を使用する場合に、コンテナに対する SELinux サポートを有効にできるようになりました。
- NFS over RDMA (NFSoverRDMA) サーバーは、Red Hat Enterprise Linux クライアントからアクセスされるときに完全にサポートされるようになりました。

ストレージ関連の機能の詳細は [17章 ストレージ](#)を、ファイルシステムの機能拡張の詳細は [9章 ファイルシステム](#)を参照してください。

ツール

- Performance Co-Pilot (PCP)アプリケーションが拡張され、**pcp2influxdb**、**pcp-mpstat**、**pcp-pidstat** などの新しいクライアントツールがサポートされるようになりました。また、複数のサブシステムの新しい PCP パフォーマンスメトリクスが、さまざまな Performance Co-Pilot 分析ツールで利用できます。

さまざまなツールへの更新の詳細は、[7章 コンパイラーおよびツール](#)を参照してください。

高可用性

- Red Hat Enterprise Linux 7.4 では、以下の機能に完全に対応します。
 - **clutter** (クラスター設定形式を変換および分析するツール)
 - ストレッチクラスターを管理する Pacemaker クラスターの Quorum デバイス (QDevice)
 - **Booth** クラスターチケットマネージャー

このリリースで導入された高可用性機能の詳細は、[6章 クラスターリング](#)を参照してください。

仮想化

- Red Hat Enterprise Linux 7 ゲスト仮想マシンは Elastic Network Adapter (ENA) をサポートするようになり、Amazon Web Services (AWS) クラウドで実行するときに拡張ネットワーク機能を提供します。

仮想化の機能拡張の詳細は、[19章 仮想化](#)を参照してください。

管理および自動化

- Red Hat Enterprise Linux 7.4 には、**Ansible** を搭載した **Red Hat Enterprise Linux システムロール** が含まれています。これは、Red Hat Enterprise Linux デプロイメントの管理と保守を簡素化する設定インターフェイスです。この機能は、テクノロジープレビューとして利用できます。

詳細は、[47章 Red Hat Enterprise Linux System Roles Powered by Ansible](#) を参照してください。

Red Hat Insights

Red Hat Enterprise Linux 7.2 以降では、**Red Hat Insights** サービスを利用できます。Red Hat Insights は、デプロイメントに影響を与える前に既知の技術的問題を特定、検証、および解決できるように設計されたプロアクティブなサービスです。Insights は、Red Hat サポートエンジニアの知識、文書化されたソリューション、および解決された問題を活用して、関連する実用的な情報をシステム管理者に提供します。

このサービスは、カスタマーポータル[の https://access.redhat.com/insights/](https://access.redhat.com/insights/) で、または Red Hat Satellite を介してホストされ、提供されます。システムを登録するには、[Getting Started Guide for Insights](#) に従ってください。詳細情報、データセキュリティー、および制限は、<https://access.redhat.com/insights/splash/> を参照してください。

Red Hat Customer Portal Labs

Red Hat カスタマーポータルラボ は、カスタマーポータル[の https://access.redhat.com/labs/](https://access.redhat.com/labs/) セクションで利用可能なツールセットです。Red Hat Customer Portal Labs のアプリケーションは、パフォーマンスの向上、問題の迅速なトラブルシューティング、セキュリティー問題の特定、複雑なアプリケーションの迅速なデプロイメントおよび設定に役立ちます。最も一般的なアプリケーションには、以下のものがあります。

- [Registration Assistant](#)
- [Code Browser](#)
- [Red Hat Product Certificates](#)
- [Red Hat Network \(RHN\) System List Exporter](#)
- [Kickstart Generator](#)
- [Log Reaper](#)
- [Load Balancer Configuration Tool](#)
- [Multipath Helper](#)

第2章 アーキテクチャー

Red Hat Enterprise Linux 7.4 には、カーネルバージョン 3.10.0-693 が同梱されており、以下のアーキテクチャーに対応します。^[1]

- 64 ビット AMD
- 64 ビット Intel
- IBM POWER7+ および POWER8 (ビッグエンディアン)^[2]
- IBM POWER8 (リトルエンディアン)^[3]
- IBM z Systems^[4]

[1] Red Hat Enterprise Linux 7.4 インストールは、64 ビットハードウェアでのみ対応していることに注意してください。Red Hat Enterprise Linux 7.4 は、以前のバージョンの Red Hat Enterprise Linux を含む 32 ビットのオペレーティングシステムを仮想マシンとして実行できます。

[2] Red Hat Enterprise Linux 7.4 (ビッグエンディアン) は、現在、Red Hat Enterprise Virtualization for Power および PowerVM の KVM ゲストとしてサポートされています。

[3] Red Hat Enterprise Linux 7.4 (リトルエンディアン) は、現在、Red Hat Enterprise Virtualization for Power、PowerVM、および PowerNV (ベアメタル) で KVM ゲストとしてサポートされています。

[4] Red Hat Enterprise Linux 7.4 は、IBM zEnterprise 196 ハードウェア以降をサポートしていることに注意してください。IBM z10 システムのメインフレームシステムはサポートされなくなり、Red Hat Enterprise Linux 7.4 を起動しなくなります。

第3章 外部のカーネルパラメーターに対する重要な変更

本章では、システム管理者向けに、Red Hat Enterprise Linux 7.4 に同梱されるカーネルにおける重要な変更の概要について説明します。これらの変更には、**proc** エントリー、**sysctl** および **sysfs** のデフォルト値、ブートパラメーター、カーネル設定オプションの追加または更新、注目すべき動作の変更が含まれます。

更新された /PROC/SYS/KERNEL エントリー

hung_task_panic

応答しないタスクが検出された場合のカーネルの動作を制御します。このファイルは、**CONFIG_DETECT_HUNG_TASK** が有効な場合に発生します。

形式: { "0" | "1" }

0 - 操作を続行します。デフォルトの動作。

1 - すぐにパニックになる。

hung_task_check_count

チェックされるタスクの数の上限を指定します。このファイルは、**CONFIG_DETECT_HUNG_TASK** が有効な場合に発生します。

hung_task_timeout_secs

間隔を確認します。D 状態のタスクがこの値よりも長い時間スケジュールされていない場合に警告を報告します。このファイルは、**CONFIG_DETECT_HUNG_TASK** が有効な場合に発生します。

0 - 無限のタイムアウト - チェックは行われませんでした。

hung_task_warning

チェック間隔中に報告する警告の最大数を指定します。この値に到達すると、警告が報告されなくなります。このファイルは、**CONFIG_DETECT_HUNG_TASK** が有効な場合に発生します。

-1 - 無限の警告を報告します。

panic_on_rcu_stall

1 に設定すると、RCU ストール検出メッセージの後に panic() 関数を呼び出します。これは、vmcore を使用して RCU ストールの根本原因を定義する場合に役立ちます。

0 - RCU ストールが発生する際にパニックを起こさないでください。デフォルトの動作。

1 - RCU ストールメッセージを出力した後にパニックが発生します。

更新された /PROC/SYS/USER エントリー

`/proc/sys/user` ディレクトリーのファイルを使用して、namespace の数およびユーザーごとの namespace 制限を持つその他のオブジェクトのデフォルトの制限をオーバーライドできます。これらの制限の目的は、誤動作するプログラムを停止し、多数のオブジェクトの作成を試みることです。この制限のデフォルト値は、通常の操作で使用しているプログラムがこの制限に到達できないように調整されています。

ユーザーごとの名前空間オブジェクトの作成は、オブジェクトを作成し、そのユーザー名前空間のユーザーごとの制限を下回っていることを確認したユーザー名前空間のユーザーに課金されます。このよう

なオブジェクトの作成はユーザーの名前空間で行われ、ユーザーの名前空間を作成したすべてのユーザーに課金されます。

作成されたオブジェクトのこの再帰的なカウントにより、ユーザー名前空間を作成しても、ユーザーが現在の制限を超えることはありません。

`/proc/sys/user` で更新されたファイルは次のとおりです。

`max_cgroup_namespaces`

現在のユーザー名前空間内のすべてのユーザーが作成できる制御グループ名前空間の最大数。

`max_ipc_namespaces`

現在のユーザー名前空間内のユーザーが作成できるプロセス間通信の名前空間の最大数。

`max_mnt_namespaces`

現在のユーザー名前空間内のすべてのユーザーが作成できるマウント名前空間の最大数。

`max_net_namespaces`

現在のユーザー名前空間内のユーザーが作成できるネットワーク名前空間の最大数。

`max_pid_namespaces`

現在のユーザー名前空間内のすべてのユーザーが作成できるプロセス ID 名前空間の最大数。

`max_user_namespaces`

現在のユーザー名前空間内のすべてのユーザーが作成できるユーザー ID 名前空間の最大数。

`max_uts_namespaces`

現在のユーザー名前空間のすべてのユーザーが作成できる UNIX Timesharing System (UTS) 名前空間の最大数。

カーネルパラメーター

`acpi_force_table_verification` [HW,ACPI]

初期段階でテーブルチェックサム検証を有効にします。デフォルトでは、初期マッピングサイズの制限により、32 ビットの AMD アーキテクチャーおよび Intel アーキテクチャーでは無効になっています。

`acpi_no_auto_ssdt` [HW,ACPI]

Secondary System Description Table (SSDT) の自動読み込みを無効にします。

`acpi_no_static_ssdt` [HW,ACPI]

起動初期の静的 SSDT のインストールを無効にします。デフォルトでは、Root System Description Table (RSDT) または eXtended System Descriptor Table (XSDT) に含まれる SSDT は自動的にインストールされ、`/sys/firmware/acpi/tables` ディレクトリーに表示されます。

このオプションは、この機能をオフにします。このオプションを指定しても、SSDT テーブルを `/sys/firmware/acpi/tables/dynamic` ディレクトリーにインストールする動的テーブルのインストールには影響しません。

irqaffinity= [SMP]

次の形式で、デフォルトの irq アフィニティマスクを設定します。

形式: <cpu number>,..., <cpu number>

または

<cpu number>-<cpu number>

正の範囲は、昇順または組み合わせで使用できます。

<cpu number>,...,<cpu number>-<cpu number>

nokaslr [KNL]]

起動初期の静的 SSDT のインストールを無効にします。デフォルトでは、RSDT または XSDT に含まれる SSDT は自動的にインストールされ、**/sys/firmware/acpi/tables** ディレクトリーに表示されます。

CONFIG_RANDOMIZE_BASE が設定されている場合、カーネルおよびモジュールベースオフセット Address SpaceLayout Randomization (ASLR) を無効にします。

nohibernate

休止状態を無効にし、再開します。

crash_kexec_post_notifiers

panic-notifiers を実行し、kmsg をダンプした後に **kdump** を実行します。

[PCI] hpbussize=nn

ホットプラグブリッジの下のバス用に予約されている追加のバス番号の最小量を提供します。デフォルトは1です。

pcie_port_pm=[PCIE]

PCIe ポートの電源管理処理:

形式: { "off" | "force" }

off - すべての PCIe ポートの電源管理を無効にします。

1 - すべての PCIe ポートの電源管理を有効にします。

sunrpc.svc_rpc_per_connection_limit=[NFS,SUNRPC]

サーバーが単一の接続から並行して処理する要求の数を制限します。デフォルト値は0 (制限なし) です。

パート I. 新機能

ここでは、Red Hat Enterprise Linux 7.4 で導入された新機能と主な機能拡張について説明します。

第4章 全般的な更新

Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 7 へのインプレースアップグレード

インプレースアップグレードは、既存のオペレーティングシステムを置き換えて、システムを、次のメジャーリリースの Red Hat Enterprise Linux にアップグレードする方法を提供するものです。インプレースアップグレードを実行するには、**Preupgrade Assistant** を使用します。これは、実際のアップグレードを実行する前にシステムのアップグレード問題をチェックし、**Red Hat Upgrade Tool** に追加のスクリプトを提供するユーティリティーです。**Preupgrade Assistant** が報告するすべての問題を解決したら、**Red Hat Upgrade Tool** を使用してシステムをアップグレードします。

手順とサポートされるシナリオの詳細については、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Migration_Planning_Guide/chap-Red_Hat_Enterprise_Linux-Migration_Planning_Guide-Upgrading.html および <https://access.redhat.com/solutions/637583> を参照してください。

Preupgrade Assistant および **Red Hat Upgrade Tool** は、Red Hat Enterprise Linux 6 Extras チャンネルで利用できます。<https://access.redhat.com/support/policy/updates/extras> を参照してください。(BZ#1432080)

ベースチャンネルに移動した cloud-init

Red Hat Enterprise Linux 7.4 以降、cloud-init パッケージとその依存関係は、Red Hat Common チャンネルから Base チャンネルに移動しました。**cloud-init** は、環境によって提供されるメタデータを使用してシステムの早期初期化を処理するツールです。これは通常、OpenStack や Amazon Web Services などのクラウド環境で起動するサーバーを設定するために使用されます。cloud-init パッケージは、Red Hat Common チャンネルを通じて提供された最新バージョン以降は更新されていないことに注意してください。(BZ#1427280)

第5章 認証および相互運用性

コンテナの **SSSD** が完全にサポートされるようになりました。

System Security Services Daemon (SSSD) を提供する `rhel7/sss` コンテナイメージは、テクノロジープレビュー機能ではなくなりました。これで、イメージが完全にサポートされるようになります。`rhel7/ipa-server` コンテナイメージは依然としてテクノロジープレビュー機能であることに注意してください。

詳細は、https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html-single/using_containerized_identity_management_services を参照してください。(BZ#1467260)

Identity Management が FIPS に対応

この機能強化により、Identity Management (IdM) は Federal Information Processing Standard (FIPS) をサポートします。これにより、FIPS の基準を満たす必要がある環境で IdM を実行できます。FIPS モードを有効にして IdM を実行するには、FIPS モードを有効にして Red Hat Enterprise Linux 7.4 を使用し、IdM 環境ですべてのサーバーをセットアップする必要があります。

以下はできないことに注意してください。

- FIPS モードを無効にしてからインストールした既存の IdM サーバーで FIPS モードを有効にする。
- FIPS モードを無効にして既存の IdM サーバーを使用する場合に FIPS モードでレプリカをインストールする。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#prerequisites を参照してください。(BZ#1125174)

SSSD は、ユーザーがスマートカードで認証する際の **Kerberos** チケットの取得に対応しています。

System Security Services Daemon (SSSD) が、Kerberos PKINIT 事前認証メカニズムに対応するようになりました。Identity Management (IdM) ドメインに登録されているデスクトップクライアントシステムに対してスマートカードを使用して認証する場合、認証が成功すると、ユーザーは有効な Kerberos Ticket-Granting Ticket (TGT) を受け取ります。その後、TGT を使用して、クライアントシステムからさらにシングルサインオン (SSO) 認証を受けることができます。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/sc-pkinit-auth.html を参照してください。(BZ#1200767, BZ#1405075)

SSSD を使用すると、同じスマートカード証明書を使用して別のユーザーアカウントにログインできます。

以前では、System Security Services Daemon (SSSD) では、すべての証明書を1人のユーザーに一意にマッピングする必要がありました。スマートカード認証を使用する場合、複数のアカウントを持つユーザーは、同じスマートカード証明書を使用してこれらすべてのアカウントにログインできませんでした。たとえば、個人アカウントと機能アカウント(データベース管理者アカウントなど)を持つユーザーは、個人アカウントにのみログインできました。

今回の更新により、SSSD では証明書を単一のユーザーに一意にマッピングする必要がなくなりました。これにより、1つのスマートカード証明書で、別のアカウントにログインできるようになりました。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/smart-cards.html を参照してください。(BZ#1340711, BZ#1402959)

IdM Web UI により、スマートカードログインが有効になります。

Identity Management Web UI を使用すると、スマートカードを使用してユーザーがログインできます。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/sc-web-ui-auth.html を参照してください。(BZ#1366572)

新規パッケージ: keycloak-httpd-client-install

keycloak-httpd-client-install パッケージは、Red Hat Single Sign-On (RH-SSO) フェデレーションされたアイデンティティプロバイダー (IdP) クライアントとして登録する際に、Apache **httpd** 認証モジュールの設定を自動化および簡素化できるさまざまなライブラリーおよびツールを提供します。

RH-SSO の詳細は、<https://access.redhat.com/products/red-hat-single-sign-on> を参照してください。

この更新の一環として、Red Hat Enterprise Linux に新しい依存関係が追加されました。

- python-requests-oauthlib パッケージ: このパッケージは、python-requests パッケージに OAuth ライブラリーサポートを提供します。これにより、python-requests が OAuth を認証に使用できるようになります。
- python-oauthlib パッケージ: このパッケージは、OAuth 認証メッセージの作成および使用を提供する Python ライブラリーです。これは、メッセージトランスポートを提供するツールと併用されることを目的としています。(BZ#1401781, BZ#1401783, BZ#1401784)

新しい Kerberos 認証情報キャッシュタイプ: KCM

今回の更新で、**kcm** という名前の新しい SSSD サービスが追加されました。このサービスは、`sssd-kcm` サブパッケージに含まれています。

kcm サービスがインストールされたら、Kerberos ライブラリーが **KCM** という名前の新しい認証情報キャッシュタイプを使用するように設定できます。KCM 認証情報キャッシュタイプを設定すると、**sssd-kcm** サービスが認証情報を管理します。

KCM 認証情報キャッシュタイプは、コンテナ化された環境に適しています。

- KCM を使用すると、**kcm** サービスがリッスンする UNIX ソケットのマウントに基づいて、オンデマンドでコンテナ間で認証情報キャッシュを共有できます。
- **kcm** サービスは、RHEL がデフォルトで使用する KEYRING 認証情報キャッシュタイプとは異なり、カーネル外のユーザー空間で実行します。KCM を使用すると、選択したコンテナでのみ **kcm** サービスを実行できます。KEYRING を使用すると、すべてのコンテナがカーネルを共有するため、認証情報キャッシュを共有します。

また、KCM 認証情報キャッシュタイプは FILE ccache タイプとは異なり、キャッシュコレクションに対応します。

詳細は、man ページの `sssd-kcm(8)` を参照してください。(BZ#1396012)

AD ユーザーは Web UI にログインして、セルフサービスページにアクセスできます。

以前は、Active Directory (AD) ユーザーは、コマンドラインから **kinit** ユーティリティーを使用するのみ認証できました。この更新により、AD ユーザーは Identity Management (IdM) Web UI にログインすることもできます。IdM 管理者は、ユーザーがログインできるようにするには、AD ユーザーの ID オーバーライドを作成する必要があります。

これにより、AD ユーザーは IdM Web UI を介してセルフサービスページにアクセスできるようになります。セルフサービス ページには、AD ユーザーの ID オーバーライドの情報が表示されます。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/using-the-ui.html#ad-users-idm-web-ui を参照してください。(BZ#872671)

SSSD により、**SSSD** サーバーモードで **AD** サブドメインの設定が可能になります。

以前では、System Security Services Daemon (SSSD) は自動的に信頼された Active Directory (AD) ドメインを設定していました。今回の更新で、SSSD は、参加しているドメインと同じ方法で、信頼できる AD ドメインに特定のパラメーターを設定することに対応しました。

その結果、SSSD が通信するドメインコントローラーなど、信頼されるドメインに個別の設定を設定できます。これを行うには、`/etc/sss/sss.conf` ファイルに、このテンプレートに続く名前で作成したセクションを作成します。

```
[domain/main_domain/trusted_domain]
```

たとえば、メインの IdM ドメイン名が `ipa.com` で、信頼されている AD ドメイン名が `ad.com` の場合、対応するセクション名は次のようになります。

```
[domain/ipa.com/ad.com]
```

(BZ#1214491)

SSSD は、**AD** 環境でユーザーおよびグループの検索と、短縮名を使用した認証に対応しています。

以前は、System Security Services Daemon (SSSD) は、デーモンがスタンドアロンドメインに参加している場合にのみ、ユーザーとグループの解決と認証のために、ドメインコンポーネントなしのユーザー名 (ショートネームとも呼ばれる) をサポートしていました。現在、このような環境のすべての SSSD ドメインで、このような目的で短縮名を使用できます。

- Active Directory (AD) に参加しているクライアント
- AD フォレストと信頼関係を持つ Identity Management (IdM) デプロイメント

すべてのコマンドの出力形式は、短縮名を使用しても常に完全修飾されています。この機能は、ドメインの解決順序の一覧を以下のいずれかの方法 (優先度の高い順に表示) で設定すると、デフォルトで有効になります。

- ローカルで、`/etc/sss/sss.conf` ファイルの `[sss]` セクションで `domain_resolution_order` オプションを使用してリストを設定します。
- ID ビューを使用する方法
- グローバルで、IdM 設定での方法

この機能を無効にするには、`/etc/sss/sss.conf` ファイルの `[domain/example.com]` セクションで `use_fully_qualified_names` オプションを `True` に設定します。(BZ#1330196)

SSSD は、**UID** または **SID** を使用しないセットアップで、ユーザーおよびグループの解決、認証、および認可に対応します。

従来の System Security Services Daemon (SSSD) デプロイメントでは、ユーザーとグループに POSIX 属性が設定されているか、SSSD が、Windows のセキュリティ識別子 (SID) に基づいてユーザーとグループを解決できます。

今回の更新で、LDAP を ID プロバイダーとして使用する設定で、UID または SID が LDAP ディレクトリーに存在しない場合でも、SSSD が次の機能をサポートするようになりました。

- D-Bus インターフェイスを介したユーザーおよびグループの解決
- Pluggable Authentication Module (PAM) インターフェイスを介した認証および承認 (BZ#1425891)

SSSD で **sssctl user-checks** コマンドが導入されました。これは、1回の操作で SSSD の基本機能をチェックします。

sssctl ユーティリティーに、**user-checks** という名前の新しいコマンドが含まれるようになりました。**sssctl user-checks** コマンドは、ユーザーlookupアップ、認証、および認可のバックエンドとして System Security Services Daemon (SSSD)を使用するアプリケーションの問題のデバッグに役立ちます。

- **sssctl user-checks [USER_NAME]** コマンドは、NSS (Name Service Switch)および D-Bus インターフェイスの InfoPipe レスポンダーで利用可能なユーザーデータを表示します。表示されるデータは、ユーザーが **system-auth** のプラグ可能な認証モジュール(PAM)サービスを使用してログインすることを許可されているかどうかを示します。
- **sssctl user-checks** チェック認証または別の PAM サービスで使用できる追加オプション。

sssctl user-checks の詳細は、**sssctl user-checks --help** コマンドを使用します。(BZ#1414023)

サービスとしてのシークレットへのサポート

今回の更新で、**secrets** という名前のレスポンスが System Security Services Daemon (SSSD)に追加されました。このレスポンスを使用すると、アプリケーションは Custodia API を使用して UNIX ソケット経由で SSSD と通信できます。これにより、SSSD はローカルデータベースに秘密を保存したり、リモートの Custodia サーバーに転送したりできます。(BZ#1311056)

IdM を使用すると、外部 DNS サーバーで IdM DNS レコードの半自動アップグレードが可能になります。

外部 DNS サーバーで Identity Management (IdM) DNS レコードの更新を簡単にするために、IdM では **ipa dns-update-system-records --dry-run --out [file]** コマンドが導入されました。このコマンドは、**nsupdate** ユーティリティーで受け入れられる形式でレコードの一覧を生成します。

生成されたファイルを使用して、Transaction Signature (TSIG) プロトコルまたは TSIG (GSS-TSIG) の GSS アルゴリズムで保護された標準の動的 DNS 更新メカニズムを使用して、外部 DNS サーバーのレコードを更新できます。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/dns-updates-external.html を参照してください。(BZ#1409628)

IdM が、SHA-256 証明書および公開鍵フィンガープリントを生成するようになりました。

以前では、Identity Management (IdM) は、証明書および公開鍵にフィンガープリントを生成する際に MD5 ハッシュアルゴリズムを使用していました。セキュリティを向上させるため、IdM は、前述のシナリオで SHA-256 アルゴリズムを使用するようになりました。(BZ#1444937)

IdM は、スマートカード証明書をユーザーアカウントにリンクするための柔軟なマッピングメカニズムに対応します。

以前は、Identity Management (IdM) で特定のスマートカードに対応するユーザーアカウントを見つける唯一の方法は、スマートカード証明書全体を Base64 エンコード DER 文字列として提供することでした。今回の更新で、証明書文字列そのものではなく、スマートカード証明書の属性を指定してユーザーアカウントを検索することもできるようになりました。たとえば、管理者は、特定の認証局 (CA) が発行したスマートカード証明書を IdM のユーザーアカウントにリンクするために、一致ルールとマッピングルールを定義できるようになりました。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/smart-cards.html#sc-one-card-multiple-accounts-links を参照してください。(BZ#1402959)

新しいユーザー空間ツールにより、より便利な **LMDB** デバッグが可能になりました。今回の更新で、`/usr/libexec/openldap/` ディレクトリーに **mdb_copy**、**mdb_dump**、**mdb_load**、および **mdb_stat** ツールが追加されました。この追加には、**man/man1** サブディレクトリーに関連する **man** ページが含まれます。この新しいツールは、Lightning Memory-Mapped Database (LMDB) バックエンドに関連する問題のデバッグにのみ使用します。(BZ#1428740)

openldap がバージョン **2.4.44** にリベースされました。

openldap パッケージがアップストリームバージョン 2.4.44 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。特に、この新しいバージョンでは、多くのレプリケーションバグおよび Lightning Memory-Mapped Database (LMDB) バグが修正されました。(BZ#1386365)

Identity Management での DNS ルックアップのセキュリティー改善とサービスプリンシパルルックアップの堅牢性

Kerberos クライアントライブラリーは、Ticket-Granting Server (TGS) 要求の発行時にホスト名の正規化を試行しなくなりました。この機能は、以下を改善します。

- この機能により、従来は正規化時に必要であった DNS ルックアップが不要になり、セキュリティーが向上します
- クラウドやコンテナ化されたアプリケーションなど、より複雑な DNS 環境におけるサービスプリンシパルルックアップの堅牢性

ホストおよびサービスプリンシパルで、正しい完全修飾ドメイン名 (FQDN) を指定していることを確認してください。この動作の変更により、Kerberos は、短縮名など、プリンシパルの他の形式の名前を解決しようとはしません。(BZ#1404750)

samba がバージョン **4.6.2** にリベースされました。

samba パッケージがバージョン 4.6.2 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。

- Samba は、**winbindd** サービスの開始前に ID マッピング設定を検証するようになりました。設定が無効な場合、**winbindd** は起動に失敗します。**testparm** ユーティリティーを使用して、`/etc/samba/smb.conf` ファイルを検証します。詳細は、**smb.conf** の **man** ページの **IDENTITY MAPPING CONSIDERATIONS** セクションを参照してください。
- Windows 10 からプリンタードライバーをアップロードできるようになりました。
- 以前は、**rpc server dynamic port range** パラメーターのデフォルト値は 1024- 1300 でした。今回の更新で、デフォルトが **49152-65535** に変更され、Windows Server 2008 以降で使用される範囲に一致するようになりました。必要に応じてファイアウォールルールを更新します。
- **net ads unregister** コマンドが、ドメインを離れる際に、Active Directory DNS ゾーンからホストの DNS エントリーを削除できるようになりました。
- **smb2 leases** パラメーターで、SMB 2.1 リースがデフォルトで有効になりました。SMB リースを使用すると、クライアントがファイルを積極的にキャッシュできます。
- セキュリティーを向上させるため、NT LAN マネージャーバージョン 1 (NTLMv1) プロトコルがデフォルトで無効になりました。非セキュアな NTLMv1 プロトコルが必要な場合は、`/etc/samba/smb.conf` ファイルの **ntlm auth** パラメーターを **yes** に設定します。

- イベント スクリプトと対話するために、**ctdb** ユーティリティーに event サブコマンドが追加されました。
- **idmap_hash** ID マッピングバックエンドは非推奨としてマークされ、今後の Samba バージョンで削除されます。
- 非推奨の **user** パラメーターおよび **username** パラメーターのみ が削除されました。

Samba は、**smbd** デーモン、**nmbd** デーモン、または **winbind** デーモンが起動すると、その tdb データベースファイルを自動的に更新します。Samba を起動する前にデータベースファイルをバックアップします。Red Hat は、tdb データベースファイルのダウングレードには対応していないことに注意してください。

重要な変更の詳細は、更新の前にアップストリームのリリースノートを参照してください。
(BZ#1391954)

authconfig は、スマートカードでユーザーを認証するために **SSSD** を有効化できるこの新機能により、**authconfig** コマンドは、スマートカードでユーザーを認証するように System Security Services Daemon (SSSD)を設定できます。以下に例を示します。

```
# authconfig --enablesssd --enablesssdauth --enablesmartcard --smartcardmodule=sssd --smartcardaction=0 --updateall
```

今回の更新で、**pam_pkcs11** がインストールされていないシステムでスマートカード認証を実行できるようになりました。ただし、**pam_pkcs11** がインストールされている場合は、**--smartcardmodule=sssd** オプションは無視されます。代わりに、**/etc/pam_pkcs11/pam_pkcs11.conf** で定義された最初の **pkcs11_module** がデフォルトとして使用されます。

詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/auth-idm-client-sc.html を参照してください。(BZ#1378943)

authconfig がアカウントロックを有効にできるようになりました。

今回の更新で、**authconfig** コマンドの **--enablefaillock** オプションが追加されました。このオプションを有効にすると、15 分以内に連続して 4 回ログインに失敗すると、設定されたアカウントが 20 分間ロックされます。(BZ#1334449)

IdM サーバーのパフォーマンスの改善

Identity Management (IdM) サーバーのパフォーマンスは、一般的なワークフローおよびセットアップの多くで向上しています。この改善には以下が含まれます

- IdM サーバー管理フレームワーク内のラウンドトリップを減らすことで、Vault パフォーマンスが向上しました。
- IdM サーバー管理フレームワークは、内部通信および認証に費やす時間を短縮するように調整されています。
- Directory Server 接続管理は、**nunc-stans** フレームワークを使用することで、よりスケーラブルになりました。
- 新規インストールでは、Directory Server が、サーバーのハードウェアリソースに基づいて、データベースエントリキャッシュとスレッド数を自動調整するようになりました。
- 大規模なグループまたはネストされたグループを使用する際に、**memberOf** プラグインのパフォーマンスが改善されました。(BZ#1395940, BZ#1425906, BZ#1400653)

IdM Web UI のデフォルトのセッション有効期限が変更されました。

以前では、ユーザーがユーザー名とパスワードを使用して Identity Management (IdM) の Web UI にログインすると、Web UI は、20 分間操作しないと自動的にユーザーをログアウトしていました。この更新により、デフォルトのセッションの長さは、ログイン操作時に取得した Kerberos チケットの有効期限と同じになります。デフォルトのセッションの長さを変更するには、`/etc/ipa/default.conf` ファイルの `kinit_lifetime` オプションを使用して、`httpd` サービスを再起動します。(BZ#1459153)

`dbmon.sh` スクリプトは、インスタンス名を使用して Directory Server インスタンスに接続するようになりました。

`dbmon.sh` シェルスクリプトを使用すると、Directory Server データベースおよびエントリーキャッシュの使用状況を監視できます。今回の更新で、スクリプトで `HOST` および `PORT` 環境変数が使用されなくなりました。セキュアなバインドをサポートするために、スクリプトは `SERVID` 環境変数から Directory Server インスタンス名を読み取り、サーバーにセキュアな接続が必要な場合にそれを使用してホスト名、ポート、および情報を取得するようになりました。たとえば、`slapd-localhost` インスタンスを監視するには、次のように入力します。

```
SERVID=slapd-localhost INCR=1 BINDDN="cn=Directory Manager" BINDPW="password" dbmon.sh
```

(BZ#1394000)

Directory Server が `SSHA_512` パスワードストレージスキームをデフォルトとして使用するようになりました。

以前は、Directory Server は、`cn=config` エントリーの `passwordStorageScheme` および `nsslapd-rootpwstoragescheme` パラメーターで設定されたデフォルトのパスワードストレージスキームとして、弱い 160 ビットのソルトされたセキュアハッシュアルゴリズム(SSHA)を使用していました。セキュリティを向上させるために、両方のパラメーターのデフォルトが、強力な 512 ビット SSHA スキーム (`SSHA_512`) に変更されました。

新しいデフォルトが使用されます。

- 新しい Directory Server インストールを実行する場合。
- `passwordStorageScheme` パラメーターが設定されていない場合に、`userPassword` 属性に保存されているパスワードを更新する場合。
- `nsslapd-rootpwstoragescheme` パラメーターが設定されていない場合や、`nsslapd-rootpw` 属性に設定された Directory Server マネージャーパスワードを更新する場合。(BZ#1425907)

Directory Server が `tcmalloc` メモリーアロケータを使用するようになりました。

Red Hat Directory Server は、`tcmalloc` メモリーアロケータを使用するようになりました。以前使用されていた標準の `glibc` アロケータにはより多くのメモリーが必要でした。また、特定の状況では、サーバーがメモリー不足になる可能性があります。`tcmalloc` メモリーアロケータを使用すると、Directory Server に必要なメモリーが少なくなり、パフォーマンスが向上します。(BZ#1426275)

Directory Server が `nunc-stans` フレームワークを使用するようになる

`nunc-stans` イベントベースのフレームワークが Directory Server に統合されました。以前は、多くの同時着信接続が Directory Server に確立されていると、パフォーマンスが低下する場合があります。今回の更新で、サーバーはパフォーマンスの低下なしに、大量の接続を処理できるようになりました。(BZ#1426278, BZ#1206301, BZ#1425906)

Directory Server `memberOf` プラグインのパフォーマンス向上

以前は、大きなグループやネストされたグループで作業すると、プラグインの操作に時間がかかりました。今回の更新で、Red Hat Directory Server `memberOf` プラグインのパフォーマンスが改善されました。その結果、`memberOf` プラグインはグループに対してユーザーを追加および削除するようになりま

した。(BZ#1426283)

Directory Server がエラーログファイルで重大度レベルのログを記録するようになりました。

Directory Server は、`/var/log/dirsrv/slapd-instance_name/errors` ログファイルに重大度レベルのログを記録するようになりました。以前は、エラーログファイルのエントリーの重大度を区別するのが困難でした。この改善により、管理者は重大度レベルを使用してエラーログをフィルターにかけることができるようになりました。

詳細は、Red Hat Directory Server の Configuration, Command, and File Reference

<https://access.redhat.com/documentation/ja->

[JP/Red_Hat_Directory_Server/10/html/Configuration_Command_and_File_Reference/error-logs.html#error-logs-content](https://access.redhat.com/documentation/ja-JP/Red_Hat_Directory_Server/10/html/Configuration_Command_and_File_Reference/error-logs.html#error-logs-content) の対応するセクションを参照してください。(BZ#1426289)

Directory Server が **PBKDF2_SHA256** パスワードストレージスキームに対応

セキュリティを向上させるため、今回の更新で、Directory Server で対応しているパスワードストレージスキームの一覧に、256 ビットのパスワードベースの鍵導出関数 2 (PBKDF2_SHA256) が追加されました。このスキームでは、30,000 回の反復を使用して 256 ビットのセキュアハッシュアルゴリズム (SHA256) を適用します。

バージョン 7.4 より前の Red Hat Enterprise Linux のネットワークセキュリティサービス (NSS) データベースは、PBKDF2 をサポートしていないことに注意してください。そのため、以前のバージョンの Directory Server を使用したレプリケーショントポロジーでは、このパスワードスキームを使用できません。(BZ#1436973)

Directory Server での自動チューニングのサポートが改善されました。

以前は、データベースを監視し、設定を手動で調整してパフォーマンスを向上させる必要がありました。今回の更新で、Directory Server が、以下のために最適化された自動チューニングに対応しました。

- データベースとエントリーキャッシュ
- 作成されたスレッドの数

Directory Server は、サーバーのハードウェアリソースに基づいてこの設定を調整します。

新しい Directory Server インスタンスをインストールする場合、自動チューニングがデフォルトで自動的に有効になります。以前のバージョンからアップグレードしたインスタンスの場合、Red Hat は自動チューニングを有効にすることを推奨します。詳細は、次を参照してください。

- データベースおよびエントリーキャッシュ: https://access.redhat.com/documentation/ja-JP/Red_Hat_Directory_Server/10/html/Performance_Tuning_Guide/memoryusage.html#DB_and
- Directory Server スレッド: https://access.redhat.com/documentation/ja-JP/Red_Hat_Directory_Server/10/html/Performance_Tuning_Guide/ds-threads (BZ#1426286)

新しい **PKI** 設定パラメーターにより、**TCP keepalive** オプションを制御できます。

今回の更新で、**CS.cfg** 設定ファイルに **tcp.keepAlive** パラメーターが追加されました。このパラメーターはブール値を受け入れ、デフォルトで **true** に設定されます。このパラメーターを使用して、PKI サブシステムによって作成されたすべての LDAP 接続に **TCP キープアライブ** オプションを設定します。このオプションは、証明書の発行に非常に時間がかかり、アイドル状態が長く続いた後に接続が自動的に閉じられる場合に役立ちます。(BZ#1413132)

PKI サーバーが、強力な暗号化を使用して **PKCS #12** ファイルを作成するようになりました。

PKCS #12 ファイルを生成する際に、**pki pkcs12** コマンドは、以前は PKCS #12 非推奨の鍵導出関数 (KDF) およびトリプル DES (3DES) アルゴリズムを使用していました。今回の更新で、このコマンドは、パスワードベースの鍵導出関数 2 (PBKDF2) および Advanced Encryption Standard (AES) アルゴリズムを使用したパスワードベースの暗号化標準 2 (PBES2) スキームを使用して秘密鍵を暗号化するようになりました。その結果、この強化によりセキュリティが向上し、コモンクライテリアの認証要件に準拠しています。(BZ#1426754)

暗号化操作に使用できる CC 準拠のアルゴリズム

コモンクライテリアでは、承認されたアルゴリズムを使用して、暗号化と鍵の巻き込みを行うことが要求されています。これらのアルゴリズムは、Protection Profile for Certification Authorities の FCS_COP.1.1(1) のセクションで規定されています。今回の更新で、KRA での暗号化と復号を変更して、秘密と鍵のトランスポートおよびストレージで承認された AES 暗号化とラップアルゴリズムを使用するようになりました。この更新では、サーバーおよびクライアントソフトウェアの両方で変更が必要になりました。(BZ#1445535)

TPS インターフェイスでメニュー項目の表示を設定できるようにする新しいオプション

以前のバージョンでは、Token Processing **System** (TPS) ユーザーインターフェイスの System メニューの下にグループ化されたメニュー項目は、ユーザーロールに基づいて静的に決定されました。特定の状況では、表示されるメニュー項目が、ユーザーが実際にアクセスできるコンポーネントと一致しませんでした。今回の更新で、TPS ユーザーインターフェイスの **System** メニューには、TPS 管理者の **target.configure.list** パラメーターと TPS エージェントの **target.agent_approve.list** パラメーターに基づくメニュー項目のみが表示されるようになりました。これらのパラメーターは、アクセス可能なコンポーネントに一致するように、インスタンス **CS.cfg** ファイルで変更できます。(BZ#1391737)

Subject Alternative Name エクステンションに、証明書の Subject Common Name をコピーするプロファイルコンポーネントの追加

一部の TLS ライブラリーでは、DNS 名が Subject Common Name (CN) フィールドにのみ表示される場合に、DNS 名の検証を警告または拒否するようになりました。これは RFC 2818 で非推奨となった慣行です。今回の更新で、**CommonNameToSANDefault** プロファイルコンポーネントが追加され、Subject Common Name が Subject Alternative Name (SAN) 拡張機能にコピーされ、証明書が現在の標準に準拠するようになりました。(BZ#1305993)

LDIF のインポート前に LDAP エントリーを削除する新しいオプション

CA を移行するとき、LDIF のインポート前に LDAP エントリーが存在すると、LDAP インポートからエントリーが再作成されないため、一部のフィールドが欠落することがありました。その結果、リクエスト ID は未定義と表示されました。この更新では、pkispawn プロセスの終了時に署名証明書の LDAP エントリーを削除するオプションが追加されました。このエントリーは、その後の LDIF インポートで再作成されます。現在、署名エントリーが削除され、LDIF のインポートで再度追加されると、リクエスト ID とその他のフィールドが正しく表示されるようになりました。追加する正しいパラメーターは、以下のとおりです (X はインポートする署名証明書のシリアル番号を 10 進数で表す)。

```
pki_ca_signing_record_create=False
pki_ca_signing_serial_number=X
```

(BZ#1409946)

Certificate System が外部認証ユーザーに対応するようになりました。

以前は、Certificate System でユーザーとロールを作成する必要がありました。この機能強化により、外部の ID プロバイダーが認証したユーザーを許可するように Certificate System を設定できるようになりました。また、レルム固有の認証アクセス制御リスト (ACL) を使用できます。そのため、Certificate System でユーザーを作成する必要はありません。(BZ#1303683)

Certificate System が、証明書および CRL 公開の有効化および無効化に対応するようになりました。

今回の更新以前は、認証局 (CA) で公開が有効になっていると、認証システムが証明書失効リスト

(CRL) と証明書公開の両方を自動的に有効にしておきました。その結果、証明書の公開が有効になっていないサーバーでは、エラーメッセージがログに記録されました。Certificate System が拡張され、`/var/lib/pki/<instance>/ca/conf/CS.cfg` ファイルで個別に証明書および CRL 公開の有効化および無効化がサポートされるようになりました。

証明書および CRL 公開の両方を有効または無効にするには、以下を設定します。

```
ca.publish.enable = True|False
```

CRL 公開のみを有効にするには、以下を設定します。

```
ca.publish.enable = True
ca.publish.cert.enable = False
```

証明書の公開のみを有効にするには、以下を設定します。

```
ca.publish.enable = True
ca.publish.crl.enable = False
```

(BZ#1325071)

searchBase 設定オプションが **DirAclAuthz** PKI サーバープラグインに追加されました。

さまざまなセットの認証アクセス制御リスト(ACL)の読み取りをサポートするために、**DirAclAuthz** PKI サーバープラグインに **searchBase** 設定オプションが追加されました。その結果、プラグインが ACL を読み込むサブツリーを設定できます。(BZ#1388622)

パフォーマンス向上のため、**Certificate System** が一時的にサポートされるようになりました。

この更新の前に、Certificate System Key Recovery Agent (KRA) インスタンスは、常に LDAP バックエンドにシークレットの復旧要求とストレージ要求を保存します。これは、複数のエージェントが要求を承認する必要がある場合に状態を保存するために必要です。ただし、要求が即座に処理され、要求を承認する必要があるエージェントが1人のみの場合は、状態を保存する必要はありません。パフォーマンスを向上させるために、`/var/lib/pki/<instance>/kra/conf/CS.cfg` ファイルの **kra.**

ephemeralRequests=true オプションを設定して、要求を LDAP バックエンドに保存しないようにすることができます。(BZ#1392068)

PKI デプロイメント設定ファイルのセクションヘッダーでは、大文字と小文字が区別されなくなりました。

PKI デプロイメント設定ファイルのセクションヘッダー (**[Tomcat]** など) では、大文字と小文字が区別されておりました。この動作は、なんのメリットもなく、エラーが発生する可能性が高くなります。このリリース以降、設定ファイルのセクションヘッダーでは大文字と小文字が区別されなくなり、エラーが発生する可能性が低くなります。(BZ#1447144)

Certificate System は、**FIPS** が有効な **Red Hat Enterprise Linux** 上の **HSM** を使用した **CA** のインストールをサポートする

認証システム認証局 (CA) インスタンスのインストール時に、インストーラーがインスタンスを再起動する必要があります。この再起動時に、Federal Information Processing Standard (FIPS) モードが有効で、ハードウェアセキュリティーモジュール (HSM) を使用しているオペレーティングシステムのインスタンスは、HTTPS ポートではなくセキュアでない HTTP ポートに接続する必要があります。今回の更新で、HSM を使用して、FIPS が有効な Red Hat Enterprise Linux に Certificate System インスタンスをインストールできるようになりました。(BZ#1450143)

CMC 要求では、**AES** および **3DES** の暗号化にランダム IV が使用されるようになりました。

この更新により、PKI サーバーの Certificate Management over CMS (CMC) 要求は、アーカイブされるキーを暗号化するとき、ランダムに生成された初期化ベクトル (IV) を使用します。以前は、クライアントコードとサーバーコードでは、このシナリオで固定 IV が使用されていました。CMC クライアントコードが拡張されたため、Advanced Encryption Standard (AES) および Triple Data Encryption Algorithm (3DES) の両方で暗号化を実行する場合に、random IV を使用するとセキュリティが向上します。(BZ#[1458055](#))

第6章 クラスタリング

clufter がバージョン 0.76.0 にリベースされ、完全にサポートされるようになる

clufter パッケージでは、クラスタの設定形式を変換および分析するツールが提供されます。これを使用すると、古いスタック設定から、Pacemaker を利用する新しい設定への移行を支援できます。以前はテクノロジープレビューとして利用できた **clufter** ツールが完全にサポートされるようになります。 **clufter** の機能の詳細は、 **clufter (1)** man ページまたは **clufter -h** コマンドの出力を参照してください。 **clufter** の使用例は、Red Hat ナレッジベースの記事 <https://access.redhat.com/articles/2810031> を参照してください。

clufter パッケージがアップストリームバージョン 0.76.0 にアップグレードされ、バグ修正および新機能が数多く追加されました。更新内容は、以下のとおりです。

- CMAN + RGManger スタック固有の設定を、**ccs2pcs*** ファミリーのそれぞれの Pacemaker 設定（または一連の **pcs** コマンド）に変換する場合、**clufter** ツールは完全に有効な lvm リソースエージェント設定の変換を拒否しなくなりました。
- CMAN ベースの設定を、**ccs2pcs** ファミリーのコマンドで Pacemaker スタックに似た設定に変換すると、（障害をステータスチェックに返す前の最大失敗数など）処理で失われた設定ビットの一部が正しく伝播されるようになりました。
- **clufter** コマンドの **cib2 pcs** および **pcs2pcscmd** ファミリーを使用して pcs コマンドを生成すると、設定変更の単一ステッププッシュの（デフォルト）の動作が考慮されるアラートハンドラー定義に、適切なファイナライズされた構文が使用されるようになりました。
- **pcs** コマンドを生成する際に、**clufter** ツールは、設定全体の大規模な更新をプッシュするのではなく、異なる更新で設定に加えられた変更のみを更新する **pcs** コマンドを生成するのに推奨される機能に対応するようになりました。同様に、該当する場合、**clufter** ツールは、**pcs** ツールにユーザーパーミッション(ACL)を設定するよう指示できるようになりました。ドキュメントスキーマのさまざまなメジャーバージョンのインスタンスで動作するように、**clufter** は、**pacemaker** の内部メカニズムをミラーリングして、内部のオンデマンド形式アップグレードの概念を取得しました。同様に、**clufter** は、**bundle** 機能を設定できるようになりました。
- **clufter** コマンドの **ccs2pcscmd** および **pcs2pcscmd** ファミリーによって生成されたなどのスクリプトのような出力シーケンスでは、単なる POSIX シェルではなく Bash が想定される場所を明確にするために、オペレーティングシステムによっても直接認識されるように、意図されたシェルインタプリターが最初のコメント行として出力されるようになりました。これは、過去のある状況では誤解を招く可能性がありました。
- = 文字が、完了するシーケンスでオプションの値を指定する際に、**clufter** の Bash 補完ファイルが適切に機能しなくなりました。
- **clufter** ツールは、ターミナルでのインタラクティブな使用を適切に検出し、出力をより便利に表示できるようにし、以前に選択されていたエラー条件の診断を改善しました。(BZ#1387424, BZ#1381522, BZ#1440876, BZ#1381531, BZ#1381565)

Pacemaker クラスタにおけるクォーラムデバイスのサポート

Red Hat Enterprise Linux 7.4 は、以前はテクノロジープレビューとして利用できたクォーラムデバイスを完全にサポートします。この機能は、クラスタのサードパーティー調整デバイスとして機能する個別のクォーラムデバイス (QDevice) を設定する機能を提供します。主要な用途は、クォーラムルールによって許容されるノード障害の数よりも多くのノード障害をクラスタが許容するようにすることで、クォーラムデバイスは、偶数のノードで設定されるクラスタに推奨されます (2 ノード設定のクラスタには強く推奨されます)。クォーラムデバイスの設定方法の詳細

は、<https://access.redhat.com/documentation/ja->

[JP/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/](https://access.redhat.com/documentation/ja-Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/) を参照してください。

(BZ#1158805)

Booth クラスターチケットマネージャーのサポート

Red Hat Enterprise Linux 7.4 は、Booth クラスターチケットマネージャーを完全にサポートします。以前はテクノロジープレビューとして利用できたこの機能を使用すると、分散サービスを介して通信する別のサイトに複数の高可用性クラスターを設定して、リソースの管理を調整できます。Booth チケットマネージャーにより、個々のチケットに関するコンセンサススペースの決定プロセスが容易になり、チケットが付与されたときに指定したリソースが1度に1つのサイトでのみ実行されるようになります。

Booth チケットマネージャーでマルチサイトクラスターを設定する方法の詳細

は、<https://access.redhat.com/documentation/ja->

[JP/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/](https://access.redhat.com/documentation/ja-Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/) を参照してください。

(BZ#1302087、BZ#1305049)

SBD デーモンで共有ストレージを使用するために追加されたサポート

Red Hat Enterprise Linux 7.4 では、共有ブロックデバイスで SBD (Storage-Based Death) デーモンの使用をサポートしています。これにより、従来からサポートされていたウォッチドッグデバイスによるフェンシングに加えて、共有ブロックデバイスによるフェンシングを有効にできます。**fence-agents** パッケージは、RHCS 形式のフェンスエージェントを使用して実際のフェンシングをトリガーし、制御するために必要な **fence_sbd** フェンスエージェントを提供するようになりました。SBD は、Pacemaker リモートノードではサポートされていません。(BZ#1413951)

CTDB リソースエージェントへの完全なサポート

Samba デプロイメントの実装に使用される CTDB リソースエージェントが Red Hat Enterprise Linux でサポートされるようになりました。(BZ#1077888)

High Availability and Resilient Storage Add-Ons が、IBM POWER (リトルエンディアン) で利用できるようになりました。

Red Hat Enterprise Linux 7.4 では、リトルエンディアンアーキテクチャーである IBM POWER の高可用性および復元力のあるストレージアドオンのサポートを追加しています。このサポートは、POWER8 サーバーの PowerVM で実行しているクラスターノードにのみ提供されることに注意してください。

(BZ#1289662、BZ#1426651)

pcs が、暗号化された **corosync** 通信でクラスターを設定できるようになりました。

pcs cluster setup コマンドが、クラスターでの corosync 暗号化の設定を制御する新しい **--encryption** フラグに対応するようになりました。これにより、ユーザーは完全に信頼されていない環境で、暗号化された corosync 通信を使用してクラスターをセットアップできるようになります。(BZ#1165821)

リモートノードおよびゲストノードのサポートおよび削除に使用される新しいコマンド
Red Hat Enterprise Linux 7.4 では、リモートノードおよびゲストノードを作成および削除するための次のコマンドが追加されました。

- pcs cluster node add-guest
- pcs cluster node remove-guest
- pcs cluster node add-remote
- pcs cluster node remove-remote

このコマンドは、非推奨となった **pcs cluster remote-node add** コマンドおよび **pcs cluster remote-node remove** コマンドに代わるものです。(BZ#1176018、BZ#1386512)

pcsd バインドアドレスの設定機能

/etc/sysconfig/pcsd ファイルで pcsd バインドアドレスを設定できるようになりました。以前のリリースでは、**pcsd** がすべてのインターフェイスにバインドできました。これは、一部のユーザーに適さない状況です。デフォルトでは、**pcsd** はすべてのインターフェイスにバインドします。

(BZ#1373614)

監視操作を無効にする `pcs resource unmanage` コマンドの新しいオプション

リソースが管理対象外モードの場合でも、モニター操作はクラスターによって実行されます。これにより、リソースが管理対象外の場合に特定のユースケースでエラーが発生する可能性があるため、ユーザーが関心を持たないエラーをクラスターが報告する場合があります。`pcs resource unmanage` コマンドが `--monitor` オプションに対応するようになりました。これは、リソースを管理対象外モードにするときに監視操作を無効にします。また、`pcs resource manage` コマンドは、`--monitor` オプションもサポートします。これにより、リソースを管理モードに戻すときに監視操作が有効になります。(BZ#1303969)

場所の制約を設定する際の `pcs` コマンドラインでの正規表現のサポート

`pcs` が、コマンドラインの場所の制約における正規表現に対応するようになりました。この制約は、リソース名に一致する正規表現に基づいて、複数のリソースに適用されます。これにより、従来は複数の制約が必要だったものが、1つの制約で済むようになり、クラスター管理が容易になります。(BZ#1362493)

正規表現またはノード属性とその値によるフェンシングトポロジーのノードの指定

フェンシングトポロジーのノードは、ノード名に適用される正規表現、ノード属性、およびその値で指定できるようになりました。

たとえば、以下のコマンドは、ノード `node1`、`node2`、および `node3` がフェンスデバイス `apc1` および `apc2` を使用するように設定し、ノード `node4`、`node5`、および `node6` を、フェンスデバイス `apc3` および `apc4` を使用するように設定します。

```
pcs stonith level add 1 "regexp%node[1-3]" apc1,apc2
pcs stonith level add 1 "regexp%node[4-6]" apc3,apc4
```

次のコマンドでは、ノード属性のマッチングを使用して、同じように設定します。

```
pcs node attribute node1 rack=1
pcs node attribute node2 rack=1
pcs node attribute node3 rack=1
pcs node attribute node4 rack=2
pcs node attribute node5 rack=2
pcs node attribute node6 rack=2
pcs stonith level add 1 attrib%rack=1 apc1,apc2
pcs stonith level add 1 attrib%rack=2 apc3,apc4
```

(BZ#1261116)

リソースエージェント `Oracle` および `OraLsnr` の `Oracle 11g` のサポート

Red Hat Enterprise Linux 7.4 は、Pacemaker で使用される `Oracle` および `OraLsnr` リソースエージェントの `Oracle Database 11g` のサポートを提供します。(BZ#1336847)

共有ストレージでの `SBD` の使用のサポート

`pcs` コマンドを使用して共有ストレージで設定された `SBD` (Storage-Based Death) のサポートが追加されました。`SBD` フェンディングの詳細は、<https://access.redhat.com/articles/2943361> を参照してください。(BZ#1413958)

`NodeUtilization` リソースエージェントのサポート

Red Hat Enterprise Linux 7.4 は `NodeUtilization` リソースエージェントをサポートします。`NodeUtilization` エージェントは、利用可能な CPU、ホストメモリの可用性、およびハイパーバイザーメモリの可用性のシステムパラメーターを検出し、これらのパラメーターを `CIB` に追加します。エージェントをクローンリソースとして実行して、各ノードにこのようなパラメーターを自動的に入力することができます。`NodeUtilization` リソースエージェントおよびこのエージェントのリソース

オプションの詳細は、**pcs resource describe NodeUtilization** コマンドを実行します。Pacemaker での使用率と配置ストラテジーに関する詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/s1-utilization-HAAR.html を参照してください。(BZ#1430304)

第7章 コンパイラーおよびツール

pcp がバージョン 3.11.8 にリベース

Performance Co-Pilot アプリケーション(PCP)がアップストリームバージョン 3.11.81 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。主な機能強化は、次のとおりです。

- パフォーマンスメトリック値を **influxdb** データベースにエクスポートできるように、新しいクライアントツール **pcp2influxdb** が追加されました。
- **mpstat** および **pidstat** の値を過去に解析できるように、新しいクライアントツール **pcp-mpstat** および **pcp-pidstat** が追加されました。
- デバイスマッパー、**Ceph** デバイス、cpusched cgroups、プロセッサごとのソフト IRQ、**buddyinfo**、**zoneinfo**、共有メモリー、**libvirt**、同じページ-sharing、**lio**、**Redis**、および **Docker** に新しいパフォーマンスメトリクスが追加されました。
- さまざまな PCP 分析ツールで、複数のサブシステムのパフォーマンスメトリクスが追加で利用できるようになりました。(BZ#1423020)

systemtap がバージョン 3.1 にリベース

systemtap パッケージがアップストリームバージョン 3.1 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- システムコールのプロローブは、**debuginfo** 情報に基づくデフォルトではなくなりました。
- **Python** 関数のプロローブのサポートが追加されました。
- **Java** 関数パラメーターへのアクセスがより均一化されました。
- 統計集計変数のパフォーマンスが改善されました。
- 新しい統計演算子 **@variance** が追加されました。
- ユーザー空間の値を取得および設定するためのオプションが追加されました。
- サンプルで NFS の監視が改善されました。

スクリプトと tapset の互換性修正(BZ#1398393, BZ#1416204, BZ#1433391)

valgrind がバージョン 3.12 にリベース

valgrind パッケージがアップストリームバージョン 3.12 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- スタックポインターの下にあるメモリーアクセスを無視する **memcheck** ツールに新しいオプション **--ignore-range-below-sp** が追加されました。これは、現在非推奨となったオプション **--workaround-gcc296-bugs=yes** の一般的な代替手段です。
- **--gen-suppressions=yes** オプションによって生成された抑制エントリーの呼び出し元の最大数は、**--num-callers** オプションで指定された値と等しくなりました。
- AMD64 および Intel 64 アーキテクチャー上の **memcheck** ツールなど、最も一般的なユースケースのコードブロックをインストルメント化するコストが削減されました。
- 8KB 以下の命令アドレス範囲を大量に破棄するデバッグプログラムでは、パフォーマンスが改善されました。

- IBM Power 9 (ISA 3.0) アーキテクチャーのサポートが追加されました。
- AMD FMA4 命令の部分的なサポートが追加されました。
- 64 ビット ARM アーキテクチャーバージョン 8 での暗号化および CRC 命令のサポートが追加されました。(BZ#1391217)

新規パッケージ: **unitsofmeasurement**

unitsofmeasurement パッケージを使用すると、Java コードで測定単位を表現できます。新しい測定単位用の API により、物理量の処理が容易になり、エラーが発生しにくくなりました。パッケージの API は、メモリーとリソースを効率的に使用します。(BZ#1422263)

HTTP クライアントの SSL/TLS 証明書の検証が、Python 標準ライブラリーでデフォルトで有効になりました。

Python 標準ライブラリーでは、デフォルトで SSL/TLS 証明書を検証するために、HTTP クライアントのデフォルトのグローバル設定が変更されました。ファイルベースの設定を使用するお客様には影響しません。詳細は、<https://access.redhat.com/articles/2039753> を参照してください。(BZ#1219110)

%gemspec_add_dep および %gemspec_remove_dep のサポートが追加されました。

今回の更新で、**%gemspec_add_dep** マクロおよび **%gemspec_remove_dep** マクロのサポートが追加されました。このようなマクロを使用すると、`rubygem-*` パッケージの依存関係を簡単に調整できます。さらに、現在のすべてのマクロを拡張し、リリース前のバージョンのパッケージへの対応を改善しました。(BZ#1397390)

ipmitool がバージョン 1.8.18 にリベース

ipmitool パッケージがアップストリームバージョン 1.8.18 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- PEF ユーザーインターフェイスの設計が変更されました。
- IP バージョン 6 のローカルエリアネットワークパラメーターに新しいサブコマンド **lan6** が追加されました。
- VITA 固有のセンサータイプおよびイベントのサポートが追加されました。
- HMAC_MD5 および HMAC_SHA256 の暗号化のサポートが追加されました。
- PICMG 拡張機能 5.x のチェックのサポートが追加されました。
- 新しい通信インターフェイスとしての USB メディアのサポートが追加されました。
- USB ドライバーは、GNU Linux システム (BZ#1398658) でデフォルトで有効になっています。

IBM Power のリトルエンディアンバリエーション用に更新された lshw

マシンのハードウェア設定の詳細を提供する lshw パッケージが、IBM Power System のリトルエンディアンバリエーション向けに更新されました。(BZ#1368704)

perf が Intel Xeon v5 でアンコアイベントに対応

この更新により、Linux (perf) のパフォーマンス分析ツールが更新され、Intel Xeon v5 サーバー CPU でのアンコアイベントがサポートされるようになりました。これらのイベントは、上級ユーザーに追加のパフォーマンス監視情報を提供します。(BZ#1355919)

dmidecode が更新される

dmidecode パッケージが新しいバージョンに更新され、バグ修正およびハードウェア有効化の改善がいくつか行われました。(BZ#1385884)

iSCSI が `targetcli` を使用した ALUA 操作の設定に対応

イニシエーターからターゲットへのパスが複数ある場合は、非対称論理ユニットアクセス (ALUA) を使用して、パスを不均一に優先的に使用方法のプリファレンスを設定することができます。Linux-IO (LIO) カーネルターゲットは、常にこの機能をサポートしてきました。今回の更新で、`targetcli` コマンドシェルを使用して ALUA 操作を設定できるようになりました。(BZ#1243410)

jansson がバージョン 2.10 にリベース

`jansson` ライブラリーがバージョン 2.10 に更新され、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。特に、`clevis`、`tang`、および `jose` アプリケーションに対応するためにインターフェイスが追加されました。(BZ#1389805)

egrep および fgrep 用の新しい互換性環境変数

以前の `grep` リベースでは、`egrep` コマンドと `fgrep` コマンドは、それぞれ `grep -E` コマンドと `grep -F` に置き換えられました。`ps` コマンドのアウトアプットに `grep` のみが表示されたため、この変更はお客様のスクリプトに影響を与える可能性があります。このような問題を防ぐために、この更新により、新しい互換性環境変数 `GREP_LEGACY_EGREP_FGREP_PS` が導入されました。`ps` 出力に `egrep` と `fgrep` を表示し続けるには、変数を 1 に設定します。

```
GREP_LEGACY_EGREP_FGREP_PS=1
```

(BZ#1297441)

`lastcomm` が `--pid` オプションをサポートするようになりました。

`lastcomm` コマンドが `--pid` オプションをサポートするようになりました。このオプションは、カーネルでサポートされている場合、各レコードのプロセス ID (PID) と親プロセス ID (PPID) を表示します。(BZ#1255183)

新規パッケージ: perl-Perl4-CoreLibs

新しい `perl-Perl4-CoreLibs` パッケージが、Red Hat Enterprise Linux 7 のベースチャンネルで利用できるようになりました。このパッケージには、Perl 4 で利用可能であったけれども、Red Hat Enterprise Linux 7 で配布されている Perl 5.16 で削除されたライブラリーが含まれています。以前のリリースでは、これらのライブラリーは、Optional チャンネルを介して Perl サブパッケージで提供されていました。(BZ#1366724)

アーカイブから抽出する際に `tar` がディレクトリーへのシンボリックリンクに従うようになりました。

今回の更新で、`--keep-directory-symlink` オプションが `tar` コマンドに追加されました。このオプションは、抽出しようとしているディレクトリーと同じ名前のシンボリックリンクが発生した場合の `tar` の動作を変更します。デフォルトでは、`tar` は最初にシンボリックリンクを削除してから、ディレクトリーの抽出を続行します。`--keep-directory-symlink` オプションはこの動作を無効にし、アーカイブから抽出するときにディレクトリーへのシンボリックリンクに従うように `tar` に指示します。(BZ#1350640)

IO::Socket::SSL Perl モジュールが TLS バージョンの制限をサポート

`Net::SSL` Perl モジュールが、セキュリティを強化するために TLS プロトコルバージョン 1.1 または 1.2 の明示的な仕様をサポートするように更新され、`IO::Socket::SSL` モジュールがそれに応じて更新されました。新しい `IO::Socket::SSL` オブジェクトが作成されると、`SSL_version` オプションをそれぞれ `TLSv1_1` または `TLSv1_2` に設定して、`TLS` バージョンを 1.1 または 1.2 に制限できるようになりました。または、`TLSv11` および `TLSv12` を使用することもできます。この値では大文字と小文字が区別されることに注意してください。(BZ#1335035)

Net::SSL Perl モジュールが TLS バージョンの制限をサポート

`Net::SSL` Perl モジュールが、TLS プロトコルバージョンの明示的な仕様をサポートするように更新されました。これは、セキュリティを強化するために使用できます。TLS のバージョンを 1.1 または

1.2 に制限するには、**Net::SSLeay::ssl_version** 変数をそれぞれ **11** または **12** に設定します。
(BZ#1335028)

wget が TLS プロトコルバージョンの仕様をサポートするようになりました

以前は、**wget** ユーティリティーは、リモートサーバーに接続する際に、デフォルトで最も高い TLS プロトコルバージョン 1.2 を使用していました。今回の更新で、**wget** が拡張され、**wget** コマンドに `--secure-protocol=TLSv1_1` または `--secure-protocol=TLSv1_2` コマンドラインオプションを追加して、**TLS プロトコル** マイナーバージョンを明示的に選択できるようになりました。(BZ#1439811)

tcpdump がバージョン 4.9.0 にリベース

tcpdump パッケージがアップストリームバージョン 4.9.0 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- 多くのセキュリティ上の脆弱性が修正されました。
- 一般的なネットワークプロトコルの分析において、多くの改善が行われました。
- デフォルトの **snaplen** 機能が 262144 バイトに増えました。
- キャプチャーバッファが 4 MiB に拡大されました (BZ#1422473)

tcpdump のキャプチャー方向を設定するオプションが -P から -Q に変更になりました。

以前は、Red Hat Enterprise Linux の **tcpdump** ユーティリティーは **-P** オプションを使用してキャプチャーの方向を設定していましたが、アップストリームバージョンでは **-Q** を使用していました。**-Q** オプションが実装され、推奨されています。**-P** オプションは、以前の機能を **-Q** のエイリアスとして保持しますが、警告が表示されます。(BZ#1292056)

OpenJDK が 64 ビット ARM アーキテクチャーで SystemTap に対応

OpenJDK プラットフォームは、64 ビット ARM アーキテクチャー上の **SystemTap** インストルメンテーションツールを使用したイントロスペクションをサポートするようになりました。(BZ#1373986)

sos がバージョン 3.4 にリベース

sos パッケージがアップストリームバージョン 3.4 に更新され、以下のような機能拡張、新機能、バグ修正が数多く追加されました。

- **ceph_ansible**、**collectd**、**crypto**、**dracut**、**gnocchi**、**jars**、**nfsganesha**、**nodejs**、**npm**、**openstack_ansible**、**openstack_instack**、**openstack_manila**、**salt**、**salt master**、および **storageconsole** に新しいプラグインが追加されました。
- API プラグインの機能強化
- 国際化に関する更新
- ネットワーク名に一重引用符 ' が含まれている場合に、ネットワークプラグインがクラッシュしなくなりました。
- **foreman-debug** プラグインが、収集された **foreman-debug** 情報が不完全になるのを防ぐために、より長いタイムアウトで実行されるようになりました。
- 特定のプライベート SSL 証明書ファイルが収集されなくなりました。(BZ#1414879)

targetd がバージョン 0.8.6 にリベース

targetd パッケージがアップストリームバージョン 0.8.6 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。特に、**targetd** サービスは Python 2 または Python 3 のランタイムで実行され、次の API が追加されました：

`initiator_list`、`access_group_list`、`access_group_create`、`access_group_destroy`、`access_group_init_add`、`access_group_init_del`、`access_group_map_list`、`access_group_map_create`、および `access_group_map_destroy`

以下は、主なバグ修正です。

- **Targetd** が JSON-RPC 応答バージョン 2.0 に準拠するようになりました。
- **export_create** API を使用して、同じ LUN を複数のイニシエーターにマッピングできるようになりました。
- **targetd** は、起動時に SSL 証明書が存在するようになりました。(BZ#1162381)

shim がバージョン 12-1 にリベース

今回の更新で、shim パッケージがアップストリームバージョン 12-1 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、32 ビット UEFI ファームウェアおよび Extensible Firmware Interface (EFI) ユーティリティのサポートが追加されたことです。(BZ#1310766)

rubygem-abrt がバージョン 0.3.0 にリベース

rubygem-abrt パッケージがバージョン 0.3.0 にリベースされ、以前のバージョンに比べていくつかのバグ修正と機能拡張が提供されています。以下に例を示します。

- **Ruby ABRT** ハンドラーは、自動匿名マイクロレポートである **uReports** をサポートするようになりました。**uReports** を有効にすると、開発者はアプリケーションの問題について速やかに通知され、バグを修正し、問題を迅速に解決できます。
- 以前は、**Ruby** アプリケーションが **Bundler** を使用してその依存関係を管理し、エラーが発生した場合に、**Ruby ABRT** ハンドラーのコンポーネントを読み込むのに正しくないロジックを使用していました。その結果、適切な **ABRT** レポートではなく、予期しない **LoadReport** エラーが報告されていました。読み込みロジックが修正され、**Ruby** アプリケーションエラーが正しく処理され、**ABRT** を使用して報告されるようになりました。(BZ#1418750)

新規パッケージ: http-parser

新しい http-parser パッケージには、HTTP メッセージを解析するユーティリティが含まれます。要求と応答の両方を解析します。パーサーは、HTTP パフォーマンスを管理するアプリケーションで使用されるように設計されています。syscall や割り当ては行われず、データはバッファリングされず、いつでも中断される可能性があります。アーキテクチャーによっては、メッセージストリームごとに約 40 バイトのデータしか必要ありません。(BZ#1393819)

すべてのデフォルトの POSIX ミューテックスに対する Intel および IBM POWER のトランザクションメモリのサポート

デフォルトの POSIX ミューテックスは、Intel および IBM POWER のトランザクションメモリサポートに透過的に置き換えることができます。これにより、ロック取得コストが大幅に削減されます。すべてのデフォルトの POSIX ミューテックスに対してトランザクションメモリサポートを有効にするには、**RHEL_GLIBC_TUNABLES=glibc.elision.enable** 環境変数を 1 に設定します。その結果、一部のアプリケーションのパフォーマンスを改善できます。

開発者は、プロファイリングを使用して、この機能を有効にするとアプリケーションのパフォーマンスが向上するかどうかを判断することをお勧めします。(BZ#841653, BZ#731835)

glibc がグループマージをサポートするようになりました。

異なるネームサービスモジュールからグループメンバーをマージする機能が **glibc** に追加されました。その結果、集中型のユーザーアクセス制御と、複数のホストにわたるグループメンバーシップの管理が容易になりました。(BZ#1298975)

glibc が、IBM POWER9 アーキテクチャーで最適化された文字列比較機能に対応
glibc ライブラリーの文字列比較関数 **strcmp** および **strncmp** は、IBM POWER9 アーキテクチャー向けに最適化されています。(BZ#1320947)

Intel SSE、AVX、および AVX512 の機能を使用して動的に読み込まれたライブラリーのパフォーマンスが改善されました。
 Intel SSE、AVX、および AVX512 の機能を使用するライブラリーの動的ライブラリー読み込みが更新されました。その結果、このライブラリーの読み込み時のパフォーマンスが改善されました。さらに、LD_AUDIT スタイルの監査に対応するようになりました。(BZ#1421155)

elfutils がバージョン **0.168** にリベース

futils パッケージがアップストリームバージョン 0.168 にアップグレードされ、バグ修正および機能拡張が数多く追加されました。

- **eu-readelf** ユーティリティーのオプション **--symbols** で、シンボルを表示するセクションを選択できるようになりました。
- ELF/DWARF 文字列テーブルを作成する新しい関数が **libdw** ライブラリーに追加されました。
- **DW_UNDEFINED_PL1** 定数が **DW_UNDEFINED_PLI** に変更されました。以前の名前は引き続き使用できます。
- **libelf** ライブラリーの **gelf_newehdr** 関数および **gelf_newphdr** 関数の戻り値のタイプが、他の **libelf** 実装とのソースの互換性のために **void*** に変更されました。この変更により、Red Hat Enterprise Linux でサポートされているすべてのプラットフォームでバイナリー互換性が維持されます。(BZ#1400302)

bison がバージョン **3.0.4** にリベース

bison パッケージがアップストリームバージョン 3.0.4 にアップグレードされ、バグ修正および機能拡張が数多く追加されました。

- キャレットエラーによる永続的な診断が修正されました。
- 指定した警告をエラーとして扱うために、**-Werror=CATEGORY** オプションが追加されました。警告は、**-W** オプションを使用して明示的にアクティブ化する必要はありません。
- 優先ルールと役に立たないルールの処理に多くの改善が加えられました。

また、以下の変更により、後方互換性がなくなりました。

- **YYFAIL**、**YYLEX_PARAM**、**YYPARSE_PARAM**、**yystype**、**yylytype**の機能が非推奨になりました。
- アクションの最後に欠落しているセミコロンが自動的に追加されなくなりました。
- **autoconf** ユーティリティーバージョン 2.69 以前で Bison 拡張機能を使用するには、オプション **-Wno-yacc** を **(AM_) YFLAGS** に渡します。(BZ#1306000)

システムのデフォルトの **CA** バンドルは、コンパイル済みデフォルト設定または **Mutt** の設定でデフォルトとして設定されています。

以前は、TLS/SSL 経由で新しいシステムに接続する場合、**Mutt** メールクライアントはユーザーが証明書を保存する必要がありました。今回の更新で、システム認証局(CA)バンドルがデフォルトで **Mutt** に設定されます。その結果、**Mutt** は、証明書の承認または拒否を要求せずに、SSL/TLS 経由で、有効な証明書を持つホストに接続するようになりました。(BZ#1388511)

objdump 混合リストの速度

以前は、DWARF デバッグ情報を解析してソースコードを見つけるための BFD ライブラリーは非常に低速でした。BFD ライブラリーは、**objdump** ツールによって使用されます。その結果、ソースコードと逆アセンブリーの混合リストを作成すると、**objdump** が大幅に遅くなりました。BFD ライブラリーのパフォーマンスが改善されました。その結果、**objdump** を使用した混合リストの作成が速くなります。(BZ#1366052)

fjes ドライバーから人間が読める形式の出力に対する **ethtool** サポート

ethtool ユーティリティーが拡張され、**fjes** ドライバーから、人間が読める形式のレジスタダンプ出力が提供されるようになりました。これにより、**ethtool** のユーザーは、Fujitsu Extended Socket Network Device ドライバーをより詳細に検査できます。(BZ#1402701)

ecj がバージョン 4.5.2 にリベース

ecj パッケージがアップストリームバージョン 4.5.2 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、バージョン 8 で Java 言語に追加された機能のサポートが完了したことです。その結果、Java 8 機能を使用した Java コードのコンパイルに失敗することがなくなりました。これには、Java ランタイム環境が提供するシステムクラスなど、Java 8 の機能を使用していないコードが、これらの機能を使用しているコードを参照しているケースも含まれます。(BZ#1379855)

rhino がバージョン 1.7R5 にリベース

rhino パッケージがアップストリームバージョン 1.7R5 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、以前からあった正規表現の解析中に無限ループになる問題が修正されたことです。以前このバグに遭遇した **Rhino** を使用するアプリケーションが正しく機能するようになりました。(BZ#1350331)

scap-security-guide および **oscap-docker** がコンテナをサポート

ユーザーは、**oscap-docker** ユーティリティーおよび SCAP セキュリティガイドを使用して、誤検出の結果に遭遇することなく、コンテナまたはコンテナイメージのコンプライアンスを評価できるようになりました。パーティショニングなど、コンテナコンテキストでは意味のないテストが **not applicable** 値に設定されていると、選択したセキュリティポリシーでコンテナをスキャンできるようになりました。(BZ#1404392)

第8章 デスクトップ

GNOME がバージョン 3.22.3 にリベース

GNOME デスクトップがアップストリームバージョン 3.22.3 に更新され、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- デスクトップ通知の概要
- ワールドクロックおよびメディアプレーヤーとの組み込み統合
- 画面の明るさの自動調整 (統合型光センサーシステム用)
- 多くのアプリケーションでのキーボードショートカットを文書化するための標準ダイアログのサポート
- 複数の設定パネル (プリンター、マウス、タッチパッド、キーボードショートカット) の改善
- 複数のファイルの名前を一度に変更するオプション
- 圧縮ファイルおよび Google Drive 用のビルトインサポート
- ゴミ箱のサポートを元に戻す (BZ# 1383353)

xorg-x11-drv-libinput ドライバーが **X.Org** 入力ドライバーに追加されました。

xorg-x11-drv-libinput X.Org ドライバーは、低レベルの **libinput** ライブラリーのラップドライバーです。今回の更新で、ドライバーが X.Org 入力ドライバーに追加されました。**xorg-x11-drv-libinput** をインストールした後、**xorg-x11-drv-synaptics** ドライバーを削除し、**libinput** が提供する改善された入力デバイス処理の一部にアクセスできます。(BZ#1413811)

一部の **Intel** および **nVidia** ハードウェアにおけるデフォルトドライバーの変更

この変更は以下に影響します。

- 第 4 世代 Intel コアプロセッサ以降
- nVidia GeForce 8 ハードウェア以降

デフォルトの DDX ドライバーが **xf86-video-modesetting** に変更されました。

以前は、nVidia および Intel ハードウェアに対して、デフォルトは **xf86-video-nouveau** と **xf86-video-intel** でした。(BZ#1404868)

dconf-editor が別のパッケージで提供されるようになりました。

アップストリームの **dconf** チームは、**dconf-editor** を独自のパッケージに分割しました。このリリースは、その変更を反映しています。

さらに、ユーザーインターフェイスがバージョン 3.22 で設計変更されました。

- 左側のツリービューが削除されました。
- キーおよびディレクトリーが同じウィンドウに表示されるようになりました。
- 階層に戻る機能は、ヘッダーバーに表示されているパスに移動します。(BZ#1388931)

第9章 ファイルシステム

SELinux セキュリティーラベルが OverlayFS ファイルシステムでサポートされるようになる

今回の更新で、OverlayFS ファイルシステムが SELinux セキュリティーラベルをサポートするようになりました。OverlayFS ストレージドライバーで Docker コンテナを使用する場合は、コンテナの SELinux サポートを無効にするように Docker を設定する必要がなくなりました。(BZ#1297929)

NFSoverRDMA サーバーが完全にサポートされるようになりました。

テクノロジープレビューとして提供されていた NFS over RDMA (NFSoverRDMA) サーバーは、Red Hat Enterprise Linux クライアントがアクセスする際に完全に対応するようになりました。NFSoverRDMA の詳細は、Red Hat Enterprise Linux 7 Storage Administration Guide の

https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html-single/Storage_Administration_Guide/index.html#nfs-rdma セクションを参照してください。

(BZ#1400501)

autofs が amd 形式マップの参照オプションに対応

sun フォーマットマップのブラウズ機能により、マウントされた自動マウント管理マウントのディレクトリリストで、利用可能な自動マウントポイントが表示され、**autofs amd** 形式のマップでも利用できるようになりました。

マスターマップに対応するエントリーも追加しなくても、md 形式のマウントの **autofs** 設定にマウントポイントセクションを追加できるようになりました。その結果、共有マルチベンダー環境内の **autofs** マスターマップに互換性のないマスターマップエントリーが存在することを回避できます。

browsable_dirs オプションは、**autofs [amd]** 設定セクションまたは **amd** マウントポイントセクションの後に使用できます。**amd** タイプの **auto map** エントリーの **browsable** および **utimeout** マップオプションも使用できます。

browsable_dirs オプションは、**yes** または **no** にのみ設定できることに注意してください。(BZ#1367576)

ログの検索を容易にするため、**autofs** がマウント要求ログエントリーの識別子を提供するようになりました。

ビジーなサイトの場合、マウントの問題を調べるときに、特定のマウント試行のログエントリーを特定するのが難しい場合があります。ログに多くのアクティビティーが記録されている場合、エントリーは、他の同時マウント要求およびアクティビティーと混在していることが多いです。**autofs** 設定で要求ログエントリーをマウントするマウントリクエストログ識別子を追加できる場合は、特定のマウント要求のエントリーをすばやくフィルターリングできるようになりました。新しいロギングはデフォルトでオフになっており、**autofs.conf** ファイルで説明されているように **use_mount_request_log_id** オプションによって制御されます。(BZ#1382093)

SSI 環境で IBM z Systems の GFS2 をサポート

Red Hat Enterprise Linux 7.4 以降、IBM z Systems 上の GFS2 (s390x アドオンのストレージ) は、z/VM Single System Image (SSI)環境(CEC)でサポートされています。これにより、論理パーティション (LPAR) または CEC が再起動しても、クラスターは稼働したままになります。高可用性 (HA) クラスターリングのリアルタイム要件のため、ライブマイグレーションはサポートされていません。IBM

z Systems の最大ノード数 4 台は、従来どおり適用されます。IBM z Systems の高可用性と耐障害性を備えたストレージの設定方法は、<https://access.redhat.com/articles/1543363> を参照してください。(BZ#1273401)

gfs2-utils がバージョン 3.1.10 にリベース

gfs2-utils パッケージがアップストリームバージョン 3.1.10 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、この更新で以下が提供されることです。

- fsck.gfs2 コマンドのさまざまなチェックおよびパフォーマンスの向上
- mkfs.gfs2 コマンドでの奇数のブロックデバイスジオメトリの処理が改善されました。
- バグ修正を処理する gfs2_edit savemeta リーフチェーンブロック。
- カスタム関数ではなく、libuuid ライブラリーによる UUID の処理
- プロファイリング用の新しい --enable-gprof 設定オプション。
- ドキュメントの改善(BZ#1413684)

FUSE が lseek 呼び出しで SEEK_HOLE および SEEK_DATA をサポート

今回の更新で、FUSE (Filesystem in Userspace) lseek システムコールに SEEK_HOLE および SEEK_DATA 機能が追加されました。FUSE lseek を使用して、SEEK_DATA を使用したデータの次の場所(SEEK_DATA)または SEEK_HOLE を使用したホールを含むファイルのオフセットを調整できるようになりました。(BZ#1306396)

NFS サーバーが限られたコピーオフロードをサポート

NFS サーバー側のコピー機能により、NFS クライアントは、NFS クライアントを介してネットワーク経由でデータを送受信しなくても、同じ NFS サーバーの同じファイルシステムにある 2 つのファイル間でファイルデータをコピーできるようになりました。NFS プロトコルでは、複数のファイルシステム間またはサーバー間でのコピーも許可されていますが、現在、Red Hat Enterprise Linux 実装では、このような操作をサポートしていないことに注意してください。(BZ#1356122)

SELinux は GFS2 ファイルシステムでの使用がサポートされる

Security Enhanced Linux (SELinux) が GFS2 ファイルシステムで使用できるようになりました。

SELinux を GFS2 で使用するとパフォーマンスがわずかに低下するため、Enforcing モードの SELinux を使用するシステムでも、GFS2 で SELinux を使用しないことを選択できます。これを設定する方法の詳細は、https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Global_File_System_2/index.html を参照してください。(BZ#437984)

NFSv4.1 クライアントとサーバーが Kerberos 認証をサポート

今回の更新で、RDMA 経由の NFS (NFSv4.1) クライアントおよびサーバーに対する Kerberos 認証サポートが追加され、NFSv4.1 機能で krb5、krb5i、および krb5p の認証を使用できるようになりました。各 Remote Procedure Call (RPC) トランザクションのセキュア認証に、NFSv4.1 で Kerberos を使用できるようになりました。NFSv4.1 で Kerberos を使用するには、バージョン 1.3.0-0.36 以降の nfs-utils パッケージをインストールする必要があります。(BZ#1401797)

rpc.idmapd が DNS からの NFSv4 ID ドメインの取得をサポート

ID マッピングで使用されている NFS ドメイン名を、DNS から取得できるようになりました。Domain 変数が /etc/idmapd.conf ファイルに設定されていない場合、DNS は _nfsv4idmapdomain テキストレコードを検索するようにクエリーされます。値が見つかったら、それが NFS ドメインとして使用されます。(BZ#980925)

NFSv4.1 がデフォルトの NFS マウントプロトコルになる

今回の更新以前は、NFSv4.0 がデフォルトの NFS マウントプロトコルでした。NFSv4.1 は、セッション、pNFS、並列 OPEN、セッションランキングなど、NFSv4.0 に比べて大幅に改善された機能を提供します。今回の更新で、NFSv4.1 がデフォルトの NFS マウントプロトコルになりました。

マウントプロトコルのマイナーバージョンをすでに指定している場合は、この更新により動作が変更されません。サーバーが NFSv4.1 をサポートしている場合、特定のマイナーバージョンなしで NFSv4 を指定した場合、この更新により動作が変更されます。サーバーが NFSv4.0 のみをサポートしている場合、マウントは NFSv4.0 マウントのままです。マイナーバージョンとして 0 を指定すると、元の動作を保持することができます。

- mount コマンドラインの場合
- /etc/fstab ファイルで、
- または /etc/nfsmount.conf ファイル内。(BZ#1375259)

nfs-utils 設定オプションの設定は、nfs.conf で一元化されています。

今回の更新で、nfs-utils は nfs.conf ファイルで集中化された設定を使用します。これは、各 nfs-utils プログラムのスタンザに構造化されています。各 nfs-utils プログラムはファイルから直接設定を読み取ることができるため、systemctl restart nfs-config.service コマンドを使用する必要がなくなり

ましたが、特定のプログラムのみを再起動します。詳細は、`nfs.conf (5)` の `man` ページを参照してください。

以前のリリースとの互換性のために、古い `/etc/sysconfig/nfs` 設定方法は引き続き利用可能です。ただし、`/etc/sysconfig/nfs` ファイルと `/etc/nfs.conf` ファイルの両方で設定を指定しないことが推奨されます。(BZ#1418041)

特定のワークロードで、NFSv4.1 マウントのロックパフォーマンスが改善される

NFSv4 クライアントは、競合中のロックを取得するために、一定の間隔でサーバーをポーリングします。その結果、NFSv4 のコンテンツロックのロックパフォーマンスは、NFSv3 のパフォーマンスよりも低速になりました。

`CB_NOTIFY_LOCK` 操作が NFS クライアントとサーバーに追加されたため、NFSv4.1 以降では、サーバーはロックを待機しているクライアントにコールバックできます。

この更新により、特定のワークロードに対する NFSv4.1 マウントでのコンテンツロックのロックパフォーマンスが改善されました。ロックの競合時間が長くなると、パフォーマンスが改善されない可能性があることに注意してください。(BZ#1377710)

CephFS カーネルクライアントは Red Hat Ceph Storage 3 で完全にサポートされる

Ceph File System (CephFS) カーネルモジュールにより、Red Hat Enterprise Linux ノードは、Red Hat Ceph Storage クラスターから Ceph ファイルシステムをマウントできます。Red Hat Enterprise Linux のカーネルクライアントは、Red Hat Ceph Storage に同梱されている Filesystem in Userspace (FUSE) クライアントの効率的な代替手段です。現在、カーネルクライアントでは CephFS クォータに対応していないことに注意してください。

CephFS カーネルクライアントは、テクノロジープレビューとして Red Hat Enterprise Linux 7.3 に導入され、Red Hat Ceph Storage 3 のリリース以降、CephFS を完全にサポートしています。

詳細は、Red Hat Ceph Storage 3 の Ceph File System Guide https://access.redhat.com/documentation/ja-jp/red_hat_ceph_storage/3/html/ceph_file_system_guide/ を参照してください。(BZ#1626527)

第10章 ハードウェアの有効化

ハードウェアユーティリティーツールが、最近リリースされたハードウェアを正しく識別できるようになりました。

この更新の前は、廃止された ID ファイルにより、コンピューターに接続されている最近リリースされたハードウェアが不明として報告されていました。このバグを修正するために、PCI、USB、およびベンダーデバイス識別ファイルが更新されました。その結果、ハードウェアユーティリティーツールが、最近リリースされたハードウェアを正しく識別できるようになりました。(BZ#1386133)

今後のタブレットをサポートするために 7.4 で導入された新しい Wacom ドライバー

この更新では、最近リリースされたタブレットと今後リリースされるタブレットをサポートするために新しい Wacom ドライバーが導入されましたが、現在のドライバーは以前にリリースされたタブレットを引き続きサポートしています。

注目すべき機能:

- Wacom 27QHT (touch) がサポートされるようになりました
- ExpressKey リモート (BZ#1385026)

Wacom カーネルドライバーが ThinkPad X1 Yoga タッチスクリーンをサポート

今回の更新で、ThinkPad X1 Yoga タッチスクリーンのサポートが Wacom カーネルドライバーに追加されました。その結果、このマシンで Red Hat Enterprise Linux 7 を実行している場合にタッチスクリーンを適切に使用できます。(BZ#1388646)

タッチ機能が Wacom Cintiq 27 QHDT タブレットに追加されました。

今回の更新で、Wacom Cintiq 27 QHDT タブレットにタッチ機能のサポートが追加され、これらのマシンで Red Hat Enterprise Linux 7 を実行しているときにタッチスクリーンを適切に使用できるようになりました。(BZ#1391668)

AMDGPU が Southern Islands、Sea Islands、Volcanic Islands、および Arctic Islands のチップセットをサポート

Southern Islands、Sea Islands、Volcanic Islands、および Arctic Islands のチップセットのサポートが追加されました。AMDGPU グラフィックドライバーは、最新の AMD/ATI Radeon グラフィックカード用のオープンソースグラフィックスドライバーの次世代ファミリーです。これは、Southern Islands、Sea Islands、Volcanic Islands、および Arctic Islands のチップセットに基づいています。linux-firmware パッケージが提供するカードに適したファームウェアまたはマイクロコードをインストールする必要があります。(BZ#1385757)

AMD モバイルグラフィックスへのサポートの追加

Polaris アーキテクチャーに基づく AMD モバイルグラフィックスのサポートが追加されました。Polaris アーキテクチャーは、Arctic Islands チップセットに基づいています。linux-firmware が提供するカードに適したファームウェアまたはマイクロコードをインストールする必要があります。(BZ#1339127)

Netronome NFP デバイスがサポートされている

今回の更新で、nfp ドライバーが Linux カーネルに追加されました。その結果、Red Hat Enterprise Linux 7 では、Netronome Network Flow Processor (Netronome NFP 4000/6000 VF) デバイスをサポートするようになりました。(BZ#137767)

nvme-cli がバージョン 1.3 にリベース

nvme-cli ユーティリティーがバージョン 1.3 に更新され、NVMe (Nonvolatile Memory Express)に対応するようになりました。NVMe へのサポートにより、Remote Direct Memory Access (RDMA) を介してターゲットを検索し、これらのターゲットに接続できます。(BZ#1382119)

キューに入れられたスピンロックは Linux カーネルに実装されています。

この更新により、カーネルでのスピンロックの実装が、AMD64 および Intel64 アーキテクチャーでのチケットスピンロックからキューに入れられたスピンロックに変更されました。キューに入れられたスピンロックは、チケットのスピンロックよりもスケラビリティが高くなります。その結果、特に多数の CPU を搭載した Symmetric Multi Processing (SMP) システムで、システムパフォーマンスが向上しました。CPU 数が増えると、パフォーマンスが直線的に向上します。スピンロックの実装におけるこの変更により、Red Hat Enterprise Linux 7 に構築されたカーネルモジュールが、以前のリリースのカーネルで読み込めなくなる可能性があります。7.4 より前のバージョンの Red Hat Enterprise Linux (RHEL) でリリースされたカーネルモジュールは、RHEL 7.4 でリリースされたカーネルで読み込むことができます。(BZ#1241990)

RAPL が Intel Xeon v2 サーバーをサポート

Intel rapl ドライバーが、Intel Xeon v2 サーバーをサポートするように更新されました。(BZ#1379590)

Intel Platform Controller Hub [PCH] デバイスへのさらなる対応

Intel Xeon プロセッサ E3 v6 ファミリー CPU で新しい Intel PCH ハードウェアへのサポートを有効にするように、カーネルが更新されました。(BZ#1391219)

IBM Power および s390x でハードウェアアクセラレーションされた zLib の使用を可能にする genwqe-tools が同梱されています。

genwqe-tools パッケージにより、IBM Power および s390x ハードウェアのユーザーは、zLib の圧縮および解凍プロセスに FPGA ベースの PCIe カードを使用できます。

これらのツールを使用すると、RFC1950、RFC1951、および RFC1952 準拠のハードウェアを使用してパフォーマンスを向上させることができます。(BZ#1275663)

librtas がバージョン 2.0.1 にリベース

librtas パッケージがアップストリームバージョン 2.0.1 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、この更新で提供されたライブラリの名前を変更します。librtas.so.1 は librtas.so.2 に変更され、librtasevent.so.1 は librtasevent.so.2 に変わります。(BZ#1380656)

NFP ドライバー

Network Flow Processor (NFP) ドライバーは、Linux カーネルのバージョン 4.11 からバックポートされています。このドライバーは、高度なイーサネット NIC として機能する Netronome NFP4000 および NFP6000 ベースのカードをサポートします。このドライバーは、SR-IOV の物理機能および仮想機能の両方で機能します。(BZ#1406197)

Nouveau で最新の NVIDIA カードを有効にする

今回の更新には、Pascal プラットフォームに基づくハイエンドの NVIDIA カードが正しく機能するように、有効化コードが含まれます。(BZ#1330457)

Wacom ExpressKey Remote のサポート

Wacom ExpressKey Remote (EKR) が、Red Hat Enterprise Linux 7 でサポートされるようになりました。EKR は、ショートカット、メニュー、およびコマンドにアクセスできる外部デバイスです。(BZ#1346348)

Wacom Cintiq 27 QHD が ExpressKey Remote をサポート

今回の更新で、Wacom Cintiq 27 QHD タブレットが ExpressKey Remote (EKR) をサポートするようになりました。EKR は、ショートカット、メニュー、およびコマンドにアクセスできる外部デバイスです。(BZ#1342990)

第11章 インストールおよび起動

Anaconda を使用すると、RAID チャンクサイズを設定できます。

今回の更新で、キックスタートファイルの `raid` ユーティリティーの `--chunksize` パラメーターを設定して、RAID ストレージのチャンクサイズを KiB 単位で指定できます。`--chunksize` パラメーターを使用すると、デフォルトのパラメーターが上書きされます。その結果、新しいチャンクサイズにより、デフォルト値によるパフォーマンスへの悪影響を防ぐことができます。(BZ#1332316)

Anaconda テキストモードが IPoIB インターフェイスに対応

この更新により、テキストモードでの手動インストール中に IP over InfiniBand (IPoIB) ネットワークインターフェイスのサポートが追加されます。IPoIB インターフェイスのステータス情報を表示し、インターフェイス設定を変更できるようになりました。(BZ#1366935)

`inst.debug` を使用すると、Anaconda インストールの問題をより簡単にデバッグできます。

今回の更新で、`inst.debug` 起動オプションで Anaconda インストールを開始し、マシンの初期状態に関連するログを保存する機能が追加されました。このオプションは、3 つの追加ログ `lsblk`、`dmesg`、および `lvm dump` を `/tmp/pre-anaconda-logs/` ディレクトリーに保存し、インストール中に発生した問題のより便利なデバッグを可能にします。(BZ#1255659)

キックスタートのインストールに失敗すると、`%onerror` スクリプトが自動的にトリガーされる

今回の機能拡張により、Anaconda のインストールに失敗した場合にキックスタートファイルの `%onerror` セクションが確実に実行されるようになりました。このスクリプトを使用すると、ログを自動的に収集して詳細を調べることができます。この更新により、インストール中にトレースバックまたは別の致命的なエラーが発生した場合、インストーラーは `%onerror` スクリプトを実行し、`%traceback` スクリプトはエラーがトレースバックによって引き起こされているかどうかを確認します。(BZ#1412538)

Anaconda は、インストールを開始する前にネットワークが使用可能になるのを待機します。

一部の環境では、最初の DHCP 要求が失敗する可能性があります。以前は、最初の DHCP 障害により Anaconda がインストールを続行し、特に後で手動で接続を設定できなかった自動インストールで問題が発生する可能性がありました。今回の更新で、新しい Anaconda 起動オプション `inst.waitfornet=X` が導入されました。これにより、インストーラーは、次のステップに進む前に X 秒待機を中止するように強制します。接続が確立されるか、指定した間隔が経過すると、インストールが継続します。(BZ#1315160)

`stage2` またはキックスタートファイルのネットワーク上の場所を複数指定して、インストールの失敗を防ぐことができます。

今回の更新で、`stage2` のネットワークおよびキックスタートファイルで、`inst.stage2` および `inst.ks` の起動オプションを複数指定できるようになりました。これにより、`stage2` またはキックスタートファイルが置いてあるサーバーにアクセスできず、必要なファイルが使用できないためにインストールに失敗する状況を回避します。

この新しい更新により、複数の場所が指定されている場合にインストールに失敗することを回避できます。定義されたすべての場所が URL (HTTP、HTTPS、または FTP) の場合、要求されたファイルが正常にフェッチされるまで順番に試行されます。URL 以外の場所がある場合は、最後に指定した場所が試行されます。残りの場所は無視されます。(BZ#1391724)

キックスタートファイルの `autopart --nohome` は、自動パーティション設定で `/home/` の作成を無効にします。

今回の更新で、キックスタートファイルの `autopart` コマンドに `--nohome` オプションが追加され、`/home/` パーティションの自動作成が無効になります。今回の機能拡張により、`/home/` パーティションを反転する場合に手動パーティション設定を実行する必要がなくなりました。更新により、パーティション設定が自動的に行われると、`/home` パーティションが作成されません。(BZ#663099)

ハードディスクドライブおよび USB からのドライバーディスクの読み込みが有効化されている

今回の更新で、ネットワークを介して、または `initrd` から読み込む代わりに、ハードディスクドライブまたは同様のデバイスからドライバーディスクを読み込むことができるようになりました。インストールは、キックスタートまたは起動オプションを使用して続行できます。

手順は以下のとおりです。

- 1.ハードディスクドライブ、USB、または同様のデバイスにドライバーディスクを読み込みます。
- 2.このデバイスにラベルを設定します(DD など)。

注記:

キックスタートインストールの場合は、以下を

```
driverdisk LABEL=DD:/e1000.rpm
```

キックスタートファイルに追加します。

起動オプションの場合は、以下を起動引数として、

```
inst.dd=hd:LABEL=DD:/dd.rpm
```

インストールを開始します。

キックスタートと起動オプションの両方で、**DD** を特定のラベルに置き換え、**dd.rpm** を特定の名前に置き換えます。**LABEL** ではなく、**inst.repo** コマンドで対応している内容を使用して、ハードディスクドライブを指定します。キックスタート **driverdisk** コマンドの **LABEL** を指定する引数には英数字以外の文字を使用しないでください。(BZ#1377233)

LVM シンプルの自動パーティショニング動作の変更

以前では、キックスタートまたは対話式インストールのいずれを使用しても、インストールで作成または使用されるすべての論理ボリューム管理 (LVM) シンプルのサイズは 20 % が予約されていました。

今回の更新で、以下の変更が加えられました。

- 自動パーティション設定付きの LVM シンプルを作成する場合は、ボリュームグループのサイズの 20 % が予約され、最小 1 GiB と最大 100 GiB が使用されます。
- キックスタートファイルで **logvol --thinpool --grow** コマンドを使用すると、シンプルは最大サイズまで拡大します。つまり、ボリュームグループに拡張する領域は残されません。この場合は、**volgroup --reserved-space** コマンドまたは **volgroup --reserved-percent** コマンドを使用して、ボリュームグループの一部の領域を予約しておくことが推奨されます。(BZ#1131247)

32 ビットのブートローダーが、64 ビットのカーネルを UEFI で起動できるようになる

この更新により、UEFI ファームウェアを搭載したシステムで、**grub2-i386-efi**などの 32 ビットブートローダーを使用して 64 ビットカーネルを起動できるようになります。(BZ#1310775)

Lorax が SSL エラーを無視できるようになる

以前は、lorax ツールは自己署名証明書で HTTPS リポジトリを使用できませんでした。これを試みるとエラーになり、続行はできませんでした。今回の更新で、**--noverifyssl** コマンドラインオプションがユーティリティーに追加されました。これを使用して、サーバー証明書の検証を省略し、エラーを回避できます。(BZ#1430483)

shim-signed がバージョン 12 にリベース

今回の更新で、**shim-signed** パッケージがアップストリームバージョン 12 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、32 ビット UEFI ファームウェアおよび Extensible Firmware Interface (EFI) ユーティリティーのサポートが追加されたことです。(BZ#1310764)

gnu-efi がバージョン 3.0.5.-9 にリベース

今回の更新で、gnu-efi パッケージがアップストリームバージョン 3.0.5.-9 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、32 ビット UEFI ファームウェアおよび Extensible Firmware Interface (EFI) ユーティリティのサポートが追加されたことです。(BZ#1310782)

killproc () および status () の後方互換性が有効化されました。

今回の更新以前は、Red Hat Enterprise Linux 7 に同梱される /etc/rc.d/init.d/functions スクリプトには、対応する Red Hat Enterprise Linux 6 の機能の一部がありませんでした。initscripts パッケージが更新され、/etc/rc.d/init.d/functions ファイルの killproc () および status () 関数に -b オプションのサポートが追加されました。この追加により、Red Hat Enterprise Linux 6 との後方互換性が有効になり、Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 7 へのアップグレードを実行するときに発生する可能性のあるリグレッションが防止されます。(BZ#1428935)

DHCP_FQDN を使用すると、システムの完全修飾ドメイン名を指定できます。

以前は、ifcfg インターフェイス設定ファイルでは、DHCP_HOSTNAME ディレクティブを使用してシステムのホスト名を指定する必要がありました。新しい initscripts DHCP_FQDN ディレクティブにより、システムの完全修飾ドメイン名も指定できるようになりました。これは、DHCP_HOSTNAME ディレクティブを補完するものです。DHCP_HOSTNAME と DHCP_FQDN の両方が指定されている場合は、DHCP_FQDN のみが使用されます。(BZ#1260552)

これで、インストールプロセス時に、論理ボリュームのシンスナップショットを作成できるようになります。

今回の更新で、新しいキックスタートコマンド snapshot のサポートが追加されました。このコマンドを使用すると、インストールの前または後に、LVM シンボリュームスナップショットを作成できます。利用可能なオプションは以下の通りです。

- `<vg_name>/<lv_name >` スナップショットを作成するボリュームグループと論理ボリュームの名前を指定します。
- `--name=` スナップショットの名前を指定します。
- `--when=` インストールの開始前にスナップショットを作成する場合は、`pre-install` を指定します。これは、アップグレード前にシステムの状態を保持する場合に便利です。または、`post-install` を指定して、新たにインストールしたシステムのスナップショットを作成してから、追加の変更を行います。

3つのオプションはすべて必須です。また、このコマンドを1つのキックスタートファイルに複数回使用して、インストールの前後の両方でスナップショットを撮ったり、複数の論理ボリュームのスナッ

プッシュを撮ったりすることもできます。-name= パラメーターごとに一意の名前を指定していることを確認してください。(BZ#[1113207](#))

第12章 カーネル

RHEL 7.4 のカーネルバージョン

Red Hat Enterprise Linux 7.4 には、カーネルバージョン 3.10.0-693 が同梱されています。
(BZ#1801759)

NVMe ドライバーがカーネルバージョン 4.10 にリベース

NVM-Express カーネルドライバーが、アップストリームカーネルバージョン 4.10 に更新され、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。最も注目すべき変更は、既存の RDMA NIC (Infiniband、RoCE、iWARP) および既存の NVMe SSD を使用する初期の NVMe-over-Fabrics トランスポート実装がドライバーに追加されましたが、DIF/DIX およびマルチパスへのサポートが含まれていない点です。(BZ#1383834)

crash がバージョン 7.1.9 にリベース

今回の更新で、crash パッケージがアップストリームバージョン 7.1.9 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。(BZ#1393534)

crash が IBM Power ISA 3.0 の vmcore ダンプを分析できるようになりました。

crash ユーティリティーが、IBM Power ISA バージョン 3.0 アーキテクチャーに関連するカーネルページテーブルの変更に対応するように更新されました。その結果、crash ユーティリティーは、IBM Power ISA 3.0 システムのカーネルの vmcore ダンプを分析できるようになりました。(BZ#1368711)

IBM Power および IBM Power のリトルエンディアンバリエーション向けに更新された crash

crash パッケージが、IBM Power Systems および IBM Power Systems のリトルエンディアンバリエーションをサポートするように更新されました。このパッケージでは、コア分析スイートを利用できます。このツールは独立したもので、ライブシステムや、kexec-tools パッケージまたは Red Hat Enterprise Linux カーネルが作成したカーネルコアダンプを調べるために使用できます。(BZ#1384944)

memkind がバージョン 1.3.0 に更新されました。

memkind ライブラリーがバージョン 1.3.0 に更新され、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。

以下は、主な変更点です。

- ログメカニズムが導入されました。
- ハードウェアローカリティー(hwloc)が統合され、--with-hwloc オプションを使用してオン

にできます。

- **libmemkind.so** が公開しているシンボルは削除されました。たとえば、**libnuma** と **jemalloc** は公開されなくなりました。
- **autohbw** ファイルは **/memkind/autohbw/** ディレクトリーに移動し、コードがリファクタリングされ、テストが適切なシナリオに追加されました。
- **memkind** に、セキュリティーを改善するフラグが追加されました。フラグは、**--disable-secure** 設定時間オプションを使用してオフにできます。
- **jemalloc** の設定が変更され、未使用の機能をオフにするようになりました。
- いくつかのシンボルが非推奨になりました。詳細は、非推奨の機能のセクションを参照してください。(BZ#1384549)

カーネルに追加された jitter エントロピー RNG

今回の更新で、Linux カーネルへの CPU タイミングの相違を介してエントロピーを収集する **Jitter Entropy Random Number Generator (RNG)** が追加されました。この RNG は、デフォルトで **algif_rng** インターフェイスから利用できます。生成された数字は、**/dev/random** ファイルを介してカーネルに戻すことができます。これにより、他の **/dev/random** ユーザーが利用できるようになります。その結果、オペレーティングシステムではより多くのエントロピーソースが利用できるようになりました。(BZ#1270982)

/dev/random が、**urandom** プールの初期化に関する通知と警告を表示するようになりました。

この更新により、ランダムドライバー (**/dev/random**) が変更され、非ブロッキングプール (**/dev/urandom** が使用) が初期化されたときに、メッセージが出力されるようになりました。(BZ#1298643)

fjes がバージョン 1.2 に更新されました。

fjes ドライバーがバージョン 1.2 に更新され、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。(BZ#1388716)

ユーザー名空間の完全なサポート

Red Hat Enterprise Linux 7.2 でテクノロジープレビューとして導入されたユーザーネームスペース (**userns**) が完全にサポートされるようになりました。この機能は、ホストとコンテナ間の分離を改善

することにより、Linux コンテナを実行しているサーバーに追加のセキュリティーを提供します。コンテナの管理者は、ホスト上で管理操作を実行できなくなり、セキュリティーが向上します。

`user.max_user_namespaces` のデフォルト値は 0 です。この値をゼロ以外の値に設定すると、誤動作するアプリケーションを停止できます。`user.max_usernamespaces` は、15000 などの大きな値に設定することが推奨されます。これにより、通常の操作では値に再度アクセスする必要はありません。(BZ#1340238)

`makedumpfile` がバージョン 1.6.1 に更新される

`makedumpfile` パッケージは、`kexec-tools 2.0.14 rpm` の一部としてアップストリームバージョン 1.6.1 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。(BZ#1384945)

QAT が最新のアップストリームバージョンに更新された

`qat` ドライバーが最新のアップストリームバージョンに更新され、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。

バグ修正および機能強化

- Diffie-Hellman (DH) ソフトウェアのサポートが追加されました。
- Elliptic Curve Diffie-Hellman (ECDH) ソフトウェアのサポートが追加されました。
- 曲線 P-192 および P-256 の誤り訂正符号 (ECC) ソフトウェアのサポートが追加されました。(BZ#1382849)

`intel-cmt-cat` パッケージの追加

このパッケージで提供される `pqos` ユーティリティーを使用すると、管理者は L3 キャッシュを監視および操作して、ユーティリティーおよびパフォーマンスを向上させることができます。

ツールはカーネル API をバイパスし、ハードウェア上で直接動作します。これには、使用する前に CPU ピンがターゲットプロセスで使用されている必要があります。(BZ#1315489)

i40e が信頼できる VF と信頼できない VF をサポート

今回の更新で、信頼できる仮想機能と信頼できない仮想機能の両方のサポートが i40e NIC ドライバーに追加されました。(BZ#1384456)

OVS 802.1ad (QinQ) のカーネルサポート

今回の更新で、カーネル内の 802.1ad (QinQ) ネットワーク標準を有効にすることで、Open vSwitch (OVS) で 2 つの VLAN タグを使用できるようになりました。今回の更新で使用するユーザー空間は、`openvswitch` により提供されることに留意してください。(BZ#1155732)

共有メモリーと `hugetlbfs` のコピー後のライブマイグレーションサポート

今回の更新で、カーネルが強化され、コピー後のライブマイグレーションが可能になり、共有メモリーと `hugetlbfs` ファイルシステムがサポートされるようになりました。この機能を利用するには、以下のようにします。

- ホストで 2MiB の Huge Page を設定する
- 2MiB の Huge Page があるゲスト仮想マシンを作成する
- ゲスト仮想マシンと `stress-test` アプリケーションを実行してメモリーをテストする
- ポストコピーでゲスト仮想マシンをライブマイグレーションする(BZ#1373606)

新規パッケージ: `dbxtool`

`dbxtool` パッケージは、UEFI セキュアブート DBX 更新を適用するためのコマンドラインユーティリティとワンショット `systemd` サービスを提供します。(BZ#1078990)

`mlx5` が SRIOV で信頼される VF をサポート

この更新により、Single Root I/O Virtualization (SRIOV) で信頼される仮想機能(VF)のサポートが `mlx5` ドライバーに追加されました。(BZ#1383280)

バックポートされた 4.9 カーネルからの `rwsem` パフォーマンス更新

今回の更新で、Linux カーネルバージョン 4.9 までのほとんどのアップストリーム R/W semaphores (`rwsem`) パフォーマンス関連の変更が、カーネルアプリケーションバイナリーインターフェイス(kABI) を維持している一方で、Linux カーネルにバックポートされました。

以下は、主な変更点です。

- ライターに最適なスピニング。ロックの待ち時間を短縮し、ロックのパフォーマンスを向上させる。
- 内部のスピンロックを保持しないロックなしのウェイターのウェイクアップ。
(BZ#1416924)

Linux カーネルに追加された `getrandom`

今回の更新で、`getrandom` システムコールが Linux カーネルに追加されました。その結果、ユーザースペースは `/dev/urandom` で使用されるものと同じ非ブロッキングエントロピープールからランダム性を要求できるようになり、ユーザースペースは少なくとも 128 ビットのエントロピーがそのプールに蓄積されるまでブロックできます。(BZ#1432218)

新しいステータス行 `Umask` が `/proc/<PID>/status` に含まれます。

以前は、変更せずにプロセス `umask` を読み取ることはできませんでした。この変更を行わないと、特にメインプログラムがマルチスレッド化されている場合に、ライブラリーが `umask` を安全に読み取ることができません。proc ファイルシステム(`procf`s)が、`/proc/<PID>/status` ファイルの `umask` を公開するようになりました。形式は `Umask: OOOO` です。OOOO はタスクの `umask` の 8 進数表現です。(BZ#1391413)

Intel® Omni-Path Architecture (OPA) ホストソフトウェア

Intel®Omni-Path Architecture (OPA) ホストソフトウェアは、Red Hat Enterprise Linux 7.3 以降、完全にサポートされています。Intel® OPA は、クラスター環境のコンピュートと I/O ノード間の高性能データ転送(高帯域幅、高メッセージレート、低レイテンシー)のために、初期化とセットアップを行う Host Fabric Interface (HFI) ハードウェアを提供します。

Intel® Omni-Path Architecture のドキュメントを取得する方法については、<https://access.redhat.com/articles/2039623> を参照してください。(BZ#1459948)

XTS-AES の鍵認証が FIPS 140-2 の要件を満たす

この更新により、Red Hat Enterprise Linux を FIPS モードで実行し、カーネルの XTS-AES キー検証を使用すると、AES キーが強制的に `tweak` キーと異なるものになります。これにより、FIPS 140-2 IG A.9 の要件が満たされていることが保証されます。また、`ciphertext stealing (XTS)` テストベクトルを使用した XEX ベースの調整コードブックモードはスキップするようにマークできるようになりました。(BZ#1314179)

IBM z Systems で `mlx5` に対応

Mellanox `mlx5` デバイスドライバーは、IBM z Systems 上の Linux でもサポートされ、イーサネット TCP/IP ネットワークに使用できるようになりました。(BZ#1394197)

perf ツールがプロセッサのキャッシュライン競合検出に対応

perf ツールは、Shared Data Cache-to-Cache (C2C)分析用の `c2c` サブコマンドを提供するようになりました。これにより、キャッシュラインの競合を検証し、`true` 共有と `false` 共有の両方を検出できます。

競合は、対称型マルチプロセッシング (SMP) システムのプロセッサコアが、他のプロセッサによって使用されている同じキャッシュラインにあるデータオブジェクトを修正すると発生します。次に、このキャッシュラインを使用する他のすべてのプロセッサは、コピーを無効にして更新されたものを要求する必要があります。これにより、パフォーマンスが低下する可能性があります。

新しい `c2c` サブコマンドは、競合が検出されたキャッシュ行、データの読み取りおよび書き込みのプロセス、競合の原因となる命令、および関連する Non-Uniform Memory Access (NUMA) ノードに関する詳細情報を提供します。(BZ#1391243)

lpfc ドライバーでの SCSI-MQ のサポート

Red Hat Enterprise Linux 7.4 で更新された `lpfc` ドライバーは、`lpfc_use_blk_mq=1` モジュールパラメーターで SCSI-MQ (multiqueue) を使用できるようになりました。デフォルト値は 0 (無効) です。

SCSI-MQ を使用してファイバーチャネルアダプター上での非同期 IO のパフォーマンステストを実施したところ、特定の条件下ではパフォーマンスが大幅に低下した点に注意してください。修正はテスト中で、Red Hat Enterprise Linux 7.4 の一般提供に間に合うように準備できませんでした。(BZ#1382101)

第13章 REAL-TIME KERNEL

Red Hat Enterprise Linux for Real Time Kernel について

Red Hat Enterprise Linux for Real Time Kernel は、非常に高い決定論要件を持つシステム向けに、微調整を可能にするように設計されています。結果の一貫性を大幅に向上させるには、標準カーネルを調整する必要があります。リアルタイムカーネルを使用すると、標準カーネルを調整することで得られる増加に加え、わずかな増加も得ることができます。

リアルタイムカーネルは、`rhel-7-server-rt-rpms` リポジトリで利用できます。[Installation Guide](#) にはインストール手順が記載されています。その他のドキュメントは [Red Hat Enterprise Linux for Real Time の製品ドキュメント](#) で入手できます。

kernel-rt のリベース

kernel-rt ソースが最新の Red Hat Enterprise Linux カーネルソースツリーをベースとするようにアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。(BZ#1391779)

第14章 ネットワーク

NetworkManager がバージョン 1.8 にリベース

NetworkManager パッケージがアップストリームバージョン 1.8 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- 追加のルートオプションのサポートが追加されました。
- 再起動が持続するまでのデバイスの管理状態。
- 外部で管理されているデバイスが正しく処理されるようになりました。
- マルチホームホストのネットワーク化された信頼性が強化されました。
- ホスト名の管理がより柔軟に設定されるようになりました。
- 802-3 リンクプロパティの変更および適用のサポートが追加されました。 (BZ#1414103)

NetworkManager がルートの追加機能に対応

今回の更新で、NetworkManager は、`source_address` (src, IPv4 only)、`from`、`type_of_service` (tos)、`window`、`maximum_transmission_unit` (mtu)、`congestion_window` (cwnd)、`initial_congestion_window` (initcwnd)、一部の高度なオプションを設定できるようになりました。静的 IPv4 および接続の IPv6 ルート用の `initial_receiver_window` (initrwnd)。 (BZ#1373698)

NetworkManager がデバイスの状態をより適切に処理

今回の更新で、NetworkManager はサービスの再起動後にデバイスの状態を維持し、再起動時に `managed` モードに設定されたインターフェイスを引き継ぐようになりました。さらに、NetworkManager は、管理対象外として明示的に設定されていないが、ユーザーまたは別のネットワークサービスによって手動で制御されているデバイスを処理できます。 (BZ#1394579)

NetworkManager が MACsec (IEEE 802.1AE)に対応

今回の更新で、NetworkManager に Media Access Control Security (MACsec)暗号化を設定するサポートが追加されました。 (BZ#1337997)

NetworkManager が 802-3 リンクプロパティの変更と強制に対応

以前は、NetworkManager は 802-3 link properties : 802-3-ethernet.speed、802-3-ethernet.duplex、および 802-3-ethernet.auto-negotiate のみを公開していました。この更新により、それらを変更して適用することが可能になります。これは、auto-negotiate=yes を使用して自動的にを行うか、auto-negotiate=no、speed=<Mbit/s>、duplex=[half,full] を使用して手動で行うことができます。

auto-negotiate=no と speed または duplex のいずれかが設定されていない場合、リンクネゴシエーションはスキップされ、auto-negotiate=no、speed=0、duplex=NULL のデフォルト値が保持されることに注意してください。

また、後方互換性を維持するために、auto-negotiate のデフォルト値が yes から no に変更されていることに注意してください。以前は、プロパティは無視されていましたが、現在は自動ネゴシエート値 yes がリンクネゴシエーションを強制できるようになりました。speed および/または duplex の設定を解除して no に設定すると、リンクネゴシエーションは無視されます。(BZ#1353612)

NetworkManager がデバイス名に基づくボンディングスレーブの順序に対応

以前は、スレーブ接続のアクティブ化の既存の順序により、マスターインターフェイスの MAC アドレスの判断が問題になる場合があります。今回の更新で、デバイス名に基づく予測可能な順序が追加されました。NetworkManager 設定の slaves-order=name 設定を使用して、新しい順序を有効にできます。

新しい順序はデフォルトでは無効になっており、明示的に有効にする必要があります。
(BZ#1420708)

NetworkManager が SR-IOV デバイスの VF をサポート

今回の更新で、NetworkManager システムサービスは、Single Root I/O Virtualization (SR-IOV) PCI デバイスの仮想機能(VF)の作成に対応します。VF の数は、NetworkManager 設定ファイルの device セクションの sriov-num-vfs オプションを使用して指定できます。VF の作成後に、NetworkManager は VF の接続プロファイルをアクティベートできます。

Maximum Transmission Unit (MTU) などの VF インターフェイスのプロパティの一部は、物理インターフェイスに設定されているものと互換性のある値にのみ設定できることに注意してください。
(BZ#1398934)

カーネル GRE がバージョン 4.8 にリベース

Kernel Generic Routing Encapsulation (GRE) トンネリングがアップストリームバージョン 4.8 に更新されました。これにより、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されます。以下は、主な変更点です。

- **IPv4 GRE および IPv6 GRE の送受信パスのコードマージ**
- **gre (IPv4 GRE)デバイスまたは ip6gre (IPv6 GRE)デバイスをダウンせずにリンク層のアドレス変更を可能にする機能強化**
- **IPv6 GRE トラフィックでの checksum、scatter-gather、highdma、gso、gro などのさまざまなオフロードのサポート**
- **ip6gretap デバイスの追加時のカーネルモジュールの自動読み込み**
- **GRE トンネル (BZ#1369158) に影響を与える Linux カーネルバージョン 4.8 までのその他のトンネル修正 (エラー処理、MTU 計算、パス MTU 検出など)**

dnsmasq がバージョン 2.76 にリベース

dnsmasq パッケージがバージョン 2.76 にアップグレードされ、バグ修正および機能拡張が数多く追加されました。注目すべき変更点は次のとおりです。

- **dhcp_release6 ユーティリティに対応するようになりました。**
- **ra-param オプションが追加されました。**
- **DHCPv6 情報要求への応答で RFC-4242 information-refresh-time オプションのサポートが追加されました。**
- **RFC-3775- 準拠のモバイル IPv6 サポート用の ra-advrouter モードが追加されました。**
- **script-arp スクリプトが追加され、dhcp-script スクリプトに新しい関数が 2 つ追加されました。**
- **アルゴリズム的に決定された安定したアドレスの代わりに、DHCPv6 一時アドレスの割り当てにランダムアドレスを使用できるようになりました。**
-

新しいオプションの DNS Security Extensions (DNSSEC) のサポートが無効になりました。

- **dnsmasq** は IPv6 ルーター広告のデフォルト値を変更できます。その結果、**ra-param** オプションを使用して、**dnsmasq** によってアダプタイズされるルートのデフォルトの優先度と時間間隔を変更します。詳細は、**dnsmasq (1)** の man ページを参照してください。(BZ#1375527, BZ#1398337)

BIND は、URI リソースレコードの処理方法を変更し、URI の後方互換性にも影響を及ぼします。

この更新により、**BIND** スイートは、URI リソースレコードを使用するときに値フィールドに追加の長さバイトを追加しなくなりました。これは、Red Hat Enterprise Linux (RHEL) 7.4 の **BIND** が、RFC 7553 <https://tools.ietf.org/html/rfc7553> で説明されている形式でのみ通信することも意味します。

この更新により、新しい URI レコードが、以前のバージョンの RHEL の **BIND** を使用して作成されたレコードと互換性がないことに注意してください。つまり、RHEL 7.4 の **BIND** では、以下のことができません。

- RHEL の以前のバージョンの **BIND** によって提供された URI レコードを理解する
- RHEL で、以前のバージョンの **BIND** を使用して、クライアントに URI レコードを提供する

ただし、RHEL 7.4 の **BIND** は、引き続き以下のことができます。

- RHEL の **BIND** の以前のバージョンと将来のバージョンの両方からレコードをキャッシュおよび受信する
- 不明な DNS リソースレコードとしてエンコードされた古い URI 形式のレコードを処理する
詳細は、RFC 3597 <https://tools.ietf.org/html/rfc3597> を参照してください。

この更新後、DNS ゾーンファイルを変更する必要はありません。(BZ#1388534)

Microsoft Azure クラウドの DDNS に追加された DHCP クライアントフックの例

Microsoft Azure クラウドの動的 DNS (DDNS)用の DHCP クライアントフックの例が **dhclient** パッケージに追加されました。管理者はこのフックを簡単に有効にし、Red Hat Enterprise Linux クライア

ントを DDNS サーバーに登録できるようになりました。(BZ#1374119)

dhcp_release6 が IPv6 アドレスをリリース

今回の更新で、dhcp_release6 ユーティリティーが、ローカルの dnsmasq サーバーの IPv6 アドレスの動的ホスト設定プロトコルバージョン 6 (DHCPv6) リースをリリースできるようになりました。dhcp_release6 コマンドの詳細は、dhcp_release6 (1) の man ページを参照してください。(BZ#1375569)

Sendmail が ECDHE をサポート

今回の更新で、Elliptic Curve Diffie-Hellman Ephemeral Keys (ECDHE) のサポートが Red Hat Enterprise Linux 7 Sendmail に追加されました。ECDHE は、楕円曲線暗号を使用する Diffie-Hellman プロトコルのバリエーションです。これは、2 者が安全でないチャネルを介して共有秘密を確立できるようにする匿名の鍵共有プロトコルです。(BZ#1124827)

telnet が -6 オプションをサポート

今回の更新で、telnet ユーティリティーが IPv6 接続をテストする -6 オプションをサポートできるようになりました。(BZ#1367415)

Unbound で負の DNS 応答をキャッシュする調整可能な TTL 制限

今回の更新で、Unbound サービスの cache-max-negative-ttl 設定オプションが追加され、特に負の DNS 応答をキャッシュするための最大 TTL の調整が可能になりました。以前は、この制限はドメインの SOA レコードによって決定されていました。または、設定済みの場合は、すべての DNS 応答をキャッシュするための最大 TTL 制限と自動的に同じになりました。

Unbound が DNS 応答キャッシングの TTL を決定する場合、cache-min-ttl オプションに設定された値は、cache-max-negative-ttl で指定された値よりも優先されることに注意してください。(BZ#1382383)

UDP ソケットのスケラビリティの改善

この更新により、UDP フォワードメモリアカウンティングが改善され、UDP ソケットのロック競合が減少します。その結果、複数のピアからトラフィックを受信する UDP ソケットの全体的な入力スループットは、外部の機能を変更することなく大幅に向上します。(BZ#1388467)

IP がカーネルの IP_BIND_ADDRESS_NO_PORT をサポート

今回の更新で、IP_BIND_ADDRESS_NO_PORT ソケットオプションがカーネルに追加されました。これにより、bind () 要求がポート番号 0 に使用される場合に、カーネルが L4 タプル予約をスキップできます。その結果、異なる宛先ホストへの多くの同時接続を維持できます。(BZ#1374498)

IPVS ソースハッシュスケジューリングが L4 ハッシュおよび SH フォールバックをサポート

今回の更新により、IP Virtual Server (IPVS) Source Hash スケジューリングアルゴリズムには以下が含まれます。

- L4 ハッシュ
- 宛先サーバーの重みが 0 の場合に備えて、次のアクティブなサーバーへの要求の SH フォールバック。これは、宛先サーバーが非アクティブであることを示します。

その結果、ポート番号に基づいて、1つのソース IP アドレスからのリクエストの負荷を分散できるようになりました。非アクティブなサーバーへのリクエストがタイムアウトしなくなりました。
(BZ#1365002)

iproute がブリッジポートオプションの変更をサポート

今回の更新で、状態、優先度、コストなどのブリッジポートオプションの変更が、iproute パッケージに追加されました。その結果、iprouteをbridge-utilsパッケージの代わりに使用できます。
(BZ#1373971)

SCTP (RFC 6458) のソケット API 拡張の新しいオプションが実装される

今回の更新で、オプション SCTP_SNDINFO、SCTP_NXTINFO、SCTP_NXTINFO、および SCTP_DEFAULT_SNDINFO が、Stream Control Transmission Protocol (RFC 6458)のソケット API 拡張に実装されます。

これらの新しいオプションは、現在非推奨となっているオプション SCTP_SNDRCV、SCTP_EXTRCV、および SCTP_DEFAULT_SEND_PARAM を置き換えます。非推奨の機能のセクションも併せて参照してください。(BZ#1339791)

ss が SCTP ソケットリストをサポート

netstat ユーティリティーは、SCTP (Stream Control Transmission Protocol)ソケットの一覧を提供していました。今回の更新で、ss ユーティリティーが同じリストを表示できるようになりました。
(BZ#1063934)

wpa_supplicant がバージョン 2.6 にリベース

wpa_supplicant パッケージがアップストリームバージョン 2.6 にアップグレードされ、バグ修正および機能拡張が数多く追加されました。特に、wpa_supplicant ユーティリティーは Media Access Control Security (MACsec)暗号化 802.1AE に対応するようになりました。これにより、デフォルトで MACsec を設定で使用できるようになります。(BZ#1404793, BZ#1338005)

Linux カーネルに switchdev インフラストラクチャーと mlxswが含まれるようになりました

今回の更新で、Linux カーネルに、以下の機能がバックポートされました。

- Ethernet スイッチデバイスドライバーモデル(`switchdev` インフラストラクチャー)により、スイッチデバイスがカーネルからのデータプレーンの転送をオフロードできるようになりました。

- `mlxsw` ドライバー

`mlxsw` でサポートされるスイッチハードウェア :

- Mellanox SwitchX-2 (出力パスのみ)
- Mellanox SwitchIB および SwitchIB-2
- Mellanox スペクトラム

`mlxsw` でサポートされる機能 :

- ポートごとのジャンボフレーム、速度設定、状態設定、統計
- ポートの分割とスプリッターケーブル
- ポートミラーリング
- QoS: 802.1p、データセンターブリッジ (DCB)
- TC flower オフロードを使用したアクセス制御リスト (ACL) がテクノロジープレビューとして導入されました。

レイヤー 2 の機能

- **VLAN**
- **Spanning Tree Protocol (STP)**
- **チームまたはボンディングのオフロードを使用した Link Aggregation (LAG)**
- **Link Layer Discovery Protocol (LLDP)**

レイヤー 3 の機能

- **ユニキャストルーティング**

これらすべての機能を設定するには、同様に更新されたiprouteパッケージによって提供される標準ツールを使用します。(BZ#[1297841](#), BZ#[1275772](#), BZ#[1414400](#), BZ#[1434587](#), BZ#[1434591](#))

Linux ブリッジコードがバージョン 4.9 にリベース

Linux ブリッジコードがアップストリームバージョン 4.9 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- **802.1ad VLAN フィルターリングおよび Tx VLAN アクセラレーションのサポート**
- **802.11 Proxy Address Resolution Protocol (ARP) へのサポート**
- **switchdevを使用したオフロードの切り替えのサポート**
- **ユーザー mdb エントリに対する VLAN サポート**

- **mdb エントリーでの拡張属性のサポート**
- **一時ポートルーターのサポート**
- **VLAN 単位の統計のサポート**
- **Internet Group Management Protocol/Multicast Listener Discovery (IGMP/MLD) 統計のサポート**
- **sysfs を使用してサポートされるすべての設定が、netlink でもサポートされるようになりました。**
- **不明なマルチキャストフラッドを制御するためのポートごとのフラグを追加しました (BZ#1352289)**

bind-dyndb-ldap がバージョン 11.1 にリベース

bind-dyndb-ldap パッケージがアップストリームバージョン 11.1 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。

特に、`/etc/named.conf` ファイルは新しい DynDB API を使用するようになりました。**bind-dyndb-ldap** パッケージを更新すると、自動的に新しい API スタイルに変換されます。(BZ#1393889)

Red Hat Enterprise Linux に追加された BIND のアップストリームバージョン 9.11.0 の DynDB API

今回の更新で、アップストリームの **bind** パッケージバージョン 9.11.0 で導入された **dyndb** システムプラグインの API がバックポートされます。その結果、Red Hat Enterprise Linux の **bind-dyndb-ldap** プラグインは新しい API を使用するようになりました。以前のリリースの Red Hat Enterprise Linux で使用されていたダウンストリーム機能の **dynamic_db** はサポートされなくなりました。

アップストリームの **dyndb** はダウンストリームの **dynamic_db** とは異なる設定構文を使用するため、今回の更新で構文も変更されます。ただし、手動で設定を変更する必要はありません。(BZ#1393886)

tboot がバージョン 1.9.5 にリベース

tboot パッケージはアップストリームバージョン 1.9.5 にアップグレードされました。これにより、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されます。以下は、主な変更点です。

- この更新により、Trusted Platform Module (TPM) 2.0 用の第 2 世代の Link Control Protocol (LCP) 作成ユーティリティーと、更新された LCP 作成ユーティリティーのユーザーガイドが追加されます。
- Intel Platform Trust Technology (PTT) および Linux PTT ドライバーの正しい動作を確認するための回避策が実装されています。
- Linux カーネルの新機能に対応するために、Linux カーネルヘッダー構造体宣言に新しいフィールドが追加されました。(BZ#1384210)

rdma-core バージョン 13 へのリベースにより統合された rdma に関連するパッケージ

rdma パッケージに関連するパッケージがアップグレードされ、1 つのソースパッケージ (rdma-core バージョン 13) に統合されました。パッケージは以下のとおりです。

- rdma
- iwpmc
- libibverbs
- librdmacm
- ibacm
- libibumad
- libocrdma
- libmlx4

- **libmlx5**
- **libhfi1verbs**
- **libi40iw**
- **srp_daemon** (以前の **srptools**)
- **libmthca**
- **libcxgb3**
- **libcxgb4**
- **libnes**
- **libipathverbs**
- **librxe**
- **rdma-ndd**

以前は同梱されていない以下のパッケージが、新規パッケージ **rdma-core** に追加されました。

- **libqedr**
- **libhns**



libvmw_pvrdma

すべての `ibverbs` ハードウェア固有のプロバイダーライブラリーが `libibverbs` サブパッケージにバンドルされるようになりました。これにより、インストールが合理化され、バージョン管理の不一致を防ぐことができます。(BZ#1404035)

静的 MAC アドレスへの OVN IP アドレス管理サポートの追加

今回の更新で、ユーザー指定の静的 MAC アドレスを使用した動的 IP アドレスの割り当てのサポートが追加されます。これにより、Open Virtual Network (OVN) ユーザーが、静的 MAC アドレスに関連付けられる動的 IP を使用して設定を作成できるようになりました。(BZ#1368043)

マルチホームホストでのネットワーク信頼性の強化

別のインターフェイスにすでに存在するルートとのインターフェイスでは、NetworkManager ユーティリティーがリバースパスフィルターリングメソッドを Strict から Loose に自動的に切り替えるようになりました。これにより、マルチホームホストマシンでのネットワークの信頼性が向上します。(BZ#1394344)

GENEVE トンネル、VXLAN トンネル、GRE トンネルのオフロードをサポート

今回の更新で、GENEVE トンネル、VXLAN トンネル、および GRE トンネルのオフロードに対応するインフラストラクチャーが追加されました。さらに、GENEVE トンネルの実装でさまざまなバグが修正されました。(BZ#1326309)

トンネルトラフィックの LCO をサポート

今回の更新で、特定のネットワークカードがトンネルトラフィックにチェックサムオフロードを利用できるようにするために、Local Checksum Offloading (LCO)技術が追加されました。この機能拡張により、VXLAN、GRE、およびその他のトンネルのパフォーマンスが向上します。(BZ#1326318)

NIC でのトンネルパフォーマンスの改善

今回の更新で、デフォルトでトンネルオフロードに対応しない ネットワークインターフェイスカード (NIC) のトンネルパフォーマンスが改善されました。その結果、ユーザーは、この NIC 上の既存のハードウェアオフロードを利用できるようになりました。(BZ#1326353)

NPT がカーネルでサポートされるようになりました。

今回の更新で、RFC 6296 で定義された IPv6-to-IPv6 Network Prefix Translation (NPTv6)関数が、Netfilter フレームワークに追加されました。その結果、IPv6 接頭辞間のステートレス変換の NPT を有効にできるようになりました。(BZ#1432897)

D-Bus API を介して DNS 設定をサポート

以前は、外部アプリケーションは NetworkManager が使用する DNS パラメーターを簡単に取得できませんでした。今回の更新で、DNS 設定が D-Bus API を介してサポートされるようになりました。その結果、ネームサーバーやドメインを含む DNS 関連の情報はすべて、NetworkManager の D-Bus API を介してクライアントアプリケーションで利用できます。このようなアプリケーションの例としては、DNS 設定を表示できる nmcli ツールがあります。(BZ#1404594)

PPP のサポートは別のパッケージへ移動

今回の更新で、Point-to-Point Protocol (PPP) のサポートが、別のオプションの NetworkManager-ppp パッケージに移動されました。その結果、NetworkManager の依存関係チェーンが小さくなり、インストールされているパッケージの数を制限できます。

PPP 設定を設定する場合は、NetworkManager-ppp パッケージがインストールされていることを確認する必要があります。(BZ#1404598)

tc ユーティリティーが flower をサポート

tc ユーティリティーが、カーネル flower トラフィック制御分類子を使用するように拡張されました。今回の更新により、ユーザーはインターフェイスから flower 分類子ルールを追加、変更、または削除できるようになりました。(BZ#1422629)

SCTP 転送パスでの CRC32c 値の計算を修正しました。

以前は、カーネルがオフロードをサポートしていないインターフェイスにカーネルが転送した場合に、カーネルがオフロードされたチェックサムを使用して Stream Control Transmission Protocol (SCTP) パケットの CRC32c 値を誤って計算していました。今回の更新で、転送パスの CRC32c の計算が修正されました。その結果、上記の状況で SCTP パケットが正しく送信されるようになりました。(BZ#1072503)

新規パッケージ: iperf3

今回の更新で、iperf3 パッケージバージョン 3.1.7 が Red Hat Enterprise Linux 7 に追加されました。iperf3 ユーティリティーを使用すると、IP ネットワークで達成可能な最大帯域幅をアクティブに測定できます。(BZ#913329)

OVN のインストールで、簡単に設定可能な firewalld ルールがサポートされるようになりました。

この機能は、Open Virtual Network (OVN) の firewalld 設定ルールを openvswitch パッケージに追加します。その結果、firewalld 設定を手動で作成する代わりに、firewalld を有効にして OVN を簡単にインストールできます。(BZ#1390938)

netlink がブリッジマスター属性に対応

今回の更新で、ブリッジ属性が変更されるたびに、通知がリスナーに送信されるようになりました。これには、sysfs、rtnl、ioctl、またはユーザーアプリケーション (NetworkManager など) によってトリガーされる変更が含まれます。(BZ#950243)

第15章 セキュリティー

新規パッケージ: tang、clevis、jose、luksmeta

Network Bound Disk Encryption (NBDE) を使用すると、システムの再起動時にパスワードを手動で入力することなく、物理マシンおよび仮想マシンのハードドライブの root ボリュームを暗号化できます。

- Tang は、データをネットワークの存在にバインドするサーバーです。これには、リモートサービスにバインドするための暗号化操作を提供するデーモンが含まれます。tang パッケージは、NBDE プロジェクトのサーバー側を提供します。
- Clevis は、自動化された復号用のプラグイン可能なフレームワークです。これを使用すると、データの自動復号化や LUKS ボリュームの自動ロック解除を行うこともできます。clevis パッケージは、NBDE プロジェクトのクライアント側を提供します。
- Joséは、Javascript Object Signing and Encryption 標準の C 言語実装です。jose パッケージは、clevis パッケージおよび tang パッケージの依存関係です。
- LUKSMeta は、LUKSv1 ヘッダーにメタデータを保存する単純なライブラリーです。luksmeta パッケージは、clevis パッケージおよび tang パッケージの依存関係です。

tang-nagios サブパッケージおよび clevis-udisk2 サブパッケージは、テクノロジープレビューとしてのみ利用できます。(BZ#1300697, BZ#1300696, BZ#1399228, BZ#1399229)

新規パッケージ: usbguard

USBGuard ソフトウェアフレームワークは、デバイス属性に基づく基本的なホワイトリスト機能およびブラックリスト機能を実装することにより、侵入型 USB デバイスに対するシステム保護を提供します。ユーザー定義のポリシーを適用するために、USBGuard は Linux カーネルの USB デバイス認証機能を使用します。USBGuard フレームワークは、以下のコンポーネントを提供します。

- 動的対話およびポリシー強制向けの IPC (inter-process communication) インターフェイスを使用したデーモンコンポーネント
- 実行中の USBGuard インスタンスと対話するコマンドラインインターフェイス
- USB デバイス認証ポリシーを記述するルール言語

- 共有ライブラリー (BZ#1395615) に実装されているデーモンコンポーネントと相互作用する C++ API

openssh がバージョン 7.4 にリベース

openssh パッケージがアップストリームバージョン 7.4 に更新され、以下のような機能拡張、新機能、バグ修正が数多く追加されました。

- SFTP で中断されたアップロードの再開のサポートが追加されました。
- 認証失敗メッセージの拡張ログ形式が追加されました。
- SHA-256 アルゴリズムを使用する新しいフィンガープリントタイプを追加しました。
- 外部 PIN エントリーデバイスで PKCS#11 デバイスの使用サポートを追加しました。
- OpenSSH サーバーから SSH-1 プロトコルに対応しなくなりました。
- 従来の v00 証明書形式のサポートを削除しました。
- キータイプを選択的に無効にできるように、ssh ユーティリティーおよび sshd デーモンの PubkeyAcceptedKeyTypes および HostKeyAlgorithms 設定オプションを追加しました。
- OpenSSH クライアントに AddKeysToAgent オプションを追加しました。
- ProxyJump ssh オプションと対応する -J コマンドラインフラグが追加されました。
- Diffie-Hellman 2K、4K、および 8K グループの鍵交換方法へのサポートが追加されました。
- ssh_config ファイルに Include ディレクティブを追加しました。

- UseLogin オプションのサポートを削除しました。
- サーバーでの事前認証圧縮のサポートを削除しました。
- `seccomp` フィルターが、事前認証プロセスに使用されるようになりました。
(BZ#1341754)

audit がバージョン 2.7.6 にリベース

`audit` パッケージがアップストリームバージョン 2.7.6 に更新され、以下のような機能拡張、新機能、バグ修正が数多く追加されました。

- `auditd` サービスは、起動時にログディレクトリーのパーミッションを自動的に調整するようになりました。これにより、パッケージのアップグレードを実行した後も、ディレクトリーのパーミッションを正しく維持できます。
- `ausearch` ユーティリティーには、新しい `--format` 出力オプションがあります。`--format text` オプションは、発生している内容を説明する英語の文としてイベントを表示します。`--format csv` オプションは、CSV (Comma Separated Value)形式で出力されるメタデータフィールドのほかに、サブジェクト、オブジェクト、アクション、結果、発生方法にログを正規化します。これは、イベント情報をデータベース、スプレッドシート、またはその他の分析プログラムにプッシュして監査イベントを表示、チャート、または分析する場合に適しています。
- `auditctl` ユーティリティーは、`--reset-lost` コマンドラインオプションを使用して、カーネルの失われたイベントカウンターをリセットできるようになりました。これにより、値を毎日ゼロにリセットできるため、失われたイベントのチェックが容易になります。
- `ausearch` および `aureport` には、システムが起動してからイベントを検索する `--start` コマンドラインオプションの起動オプションが追加されました。
- `ausearch` および `aureport` は、監査フィールドに行われるエスケープの種類をより適切に制御するための新しい `--escape` コマンドラインオプションを提供します。現在、`raw`、`tty`、`shell`、および `shell_quote` エスケープをサポートしています。
- `auditctl` では、エントリーフィルターを使用したルールが許可されなくなりました。このフィルターは、Red Hat Enterprise Linux 5 以降はサポートされていません。このリリース以前は、Red Hat Enterprise Linux 6 および 7 では、`auditctl` はエントリールールを終了フィル

ターに移動し、エントリーフィルターが非推奨であるという警告を表示していました。
(BZ#1381601)

opensc がバージョン 0.16.0 にリベース

OpenSC のライブラリーおよびユーティリティーセットは、スマートカードの使用をサポートします。OpenSC は、暗号化操作に対応し、認証、メールの暗号化、またはデジタル署名に使用できるカードにフォーカスします。

Red Hat Enterprise Linux 7.4 の注目すべき機能強化は、以下のとおりです。

- OpenSC は、Common Access Card (CAC)カードのサポートを追加します。
- OpenSC は PKCS#11 API を実装し、CoolKey アプレット機能も提供するようになりました。opensc パッケージは、coolkey パッケージを置き換えます。

coolkey パッケージは、Red Hat Enterprise Linux 7 の有効期間中サポートされ続けますが、新しいハードウェアの有効化は、opensc パッケージで提供されることに注意してください。(BZ#1081088, BZ#1373164)

openssl がバージョン 1.0.2k にリベース

openssl パッケージがアップストリームバージョン 1.0.2k に更新され、以下のような機能拡張、新機能、バグ修正が数多く追加されました。

- Datagram Transport Layer Security TLS (DTLS) プロトコルバージョン 1.2 のサポートが追加されました。
- TLS での ECDHE 鍵交換に対する自動楕円曲線選択のサポートが追加されました。
- Application-Layer Protocol Negotiation (ALPN) のサポートが追加されました。
- Cryptographic Message Syntax (CMS) のサポートが、RSA-PSS、RSA-OAEP、ECDH、および X9.42 DH のスキームに追加されました。

このバージョンは、Red Hat Enterprise Linux 7 の以前のリリースの OpenSSL ライブラリーバー

ジョンの API および ABI と互換性があることに注意してください。(BZ#1276310)

openssl-ibmca がバージョン 1.3.0 にリベース

openssl-ibmca パッケージがアップストリームバージョン 1.3.0 に更新され、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- SHA-512 のサポートが追加されました。
- 暗号化メソッドは、ibmca エンジンの起動時に動的に読み込まれます。これにより、libica ライブラリーを介してハードウェアでサポートされている場合、ibmca は暗号化メソッドを指示できます。
- ストリーム暗号モードでのブロックサイズ処理のバグを修正しました。(BZ#1274385)

OpenSCAP 1.2 は NIST 認定済み

Security Content Automation Protocol (SCAP) スキャナーである OpenSCAP 1.2 は、米国国立標準技術研究所(NIST)によって、Red Hat Enterprise Linux 6 および 7 の米国政府が評価した設定および脆弱性スキャナーとして認定されています。OpenSCAP は、セキュリティ自動化のコンテンツを正しく分析および評価し、機密性の高いセキュリティ意識の高い環境で実行するために NIST が必要とする機能およびドキュメントを提供します。さらに、OpenSCAP は、Linux コンテナを評価するための最初の NIST 認定設定スキャナーです。ユースケースには、PCI および DoD セキュリティー技術実装ガイド (STIG) に準拠するための Red Hat Enterprise Linux 7 ホストの設定の評価、および Red Hat Common Vulnerabilities and Exposures (CVE) データを使用した既知の脆弱性スキャンの実行が含まれます。(BZ#1363826)

libreswan がバージョン 3.20 にリベース

libreswan パッケージがアップストリームバージョン 3.20 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。主な機能強化は、次のとおりです。

- Opportunistic IPsec (Mesh Encryption) へのサポートが追加されました。これにより、すべてのホストで 1 つの単純な設定を使用して、多数のホストをカバーする IPsec デプロイメントが有効になりました。
- FIPS は更に強化されました。
- Virtual Tunnel Interface (VTI) を使用したルーティングベースの VPN のサポートが追加されました。

- root 以外の設定に対するサポートが改善されました。
- Online Certificate Status Protocol (OCSP) および Certificate Revocation Lists (CRL) へのサポートが改善されました。
- 新しい whack コマンドオプション(--fipsstatus、--fetchcrls、--globalstatus、および --shuntstatus)を追加しました。
- NAT Opportunistic Encryption (OE) Client Address Translation: leftcat=yes のサポートが追加されました。
- トラフィックフローの機密性メカニズムのサポートが追加されました : tfc=
- RFC 4307bis および RFC 7321bis に従って暗号設定を更新しました。
- 拡張シーケンス番号(ESN)のサポートを追加 : esn=yes
- 再生ウィンドウの無効化と拡大のサポートを追加 : replay-window=(BZ#1399883)

監査がセッション ID に基づくフィルターリングをサポート

今回の更新で、Linux Audit システムは、sessionid 値に基づいて監査メッセージをフィルターするユーザールールをサポートします。(BZ#1382504)

libseccomp が IBM Power アーキテクチャーに対応

今回の更新で、libseccomp ライブラリーが IBM Power、64 ビット IBM Power、および 64 ビットのリトルエンディアン of IBM Power アーキテクチャーをサポートし、GNOME リベースが可能になりました。(BZ#1425007)

AUDIT_KERN_MODULE がモジュールロードを記録するようになりました。

AUDIT_KERN_MODULE 補助レコードが、init_module ()、finit_module ()、および delete_module () 関数の AUDIT_SYSCALL レコードに追加されました。この情報は、audit_context 構造体に保存されます。(BZ#1382500)

OpenSSH が公開鍵署名に SHA-2 を使用するようになりました。

以前は、OpenSSH は、RSA 鍵および DSA 鍵を使用した公開鍵署名に SHA-1 ハッシュアルゴリズムを使用していました。SHA-1 は安全とは見なされなくなり、新しい SSH プロトコル拡張機能により SHA-2 を使用できるようになりました。今回の更新で、公開鍵署名のデフォルトアルゴリズムが SHA-2 になりました。SHA-1 は、後方互換性の目的でのみ利用できます。(BZ#1322911)

firewalld が追加の IP セットに対応

firewalld サービスデーモンの更新により、以下の ipset タイプのサポートが追加されました。

- hash:ip,port
- hash:ip,port,ip
- hash:ip,port,net
- hash:ip,mark
- hash:net,net
- hash:net,port
- hash:net,port,net
- hash:net,iface

同時にソースと宛先の組み合わせを提供する以下の ipset タイプは、firewalld のソースとしてサポートされていません。このタイプを使用した IP セットは firewalld によって作成されますが、使用は直接ルールに限定されます。

- hash:ip,port,ip
- hash:ip,port,net

- `hash:net,net`
- `hash:net,port,net`

`ipset` パッケージがアップストリームバージョン 6.29 にリベースされ、以下の `ipset` タイプもサポートされるようになりました。

- `hash:mac`
- `hash:net,port,net`
- `hash:net,net`
- `hash:ip,mark` (BZ#[1419058](#))

`firewalld` がリッチルールでの ICMP タイプに対するアクションに対応

今回の更新で、`firewalld` サービスデーモンは、`accept`、`log`、および `mark` のアクションが含まれるリッチルールで Internet Control Message Protocol (ICMP)タイプを使用できるようになりました。(BZ#[1409544](#))

`firewalld` が無効なヘルパー割り当てに対応

`firewalld` サービスデーモンの更新により、無効にされた自動ヘルパー割り当て機能がサポートされるようになりました。自動ヘルパー割り当てがオフになっている場合でも、ルールを追加せずに `firewalld` ヘルパーを使用できるようになりました。(BZ#[1006225](#))

`nss` と `nss-util` がデフォルトで SHA-256 を使用

この更新により、NSS ライブラリーのデフォルト設定が変更され、デジタル署名を作成するときに強力なハッシュアルゴリズムが使用されるようになりました。RSA、EC、および 2048 ビット (またはそれ以上) の DSA 鍵では、SHA-256 アルゴリズムが使用されるようになりました。

`certutil`、`crlutil`、`cmsutil` などの NSS ユーティリティーもデフォルト設定で SHA-256 を使用するようになりました。(BZ#[1309781](#))

監査フィルターの除外ルールに追加フィールドが含まれる

除外フィルターが強化され、`msgtype` フィールドだけでなく、`pid`、`uid`、`gid`、`uid`、`sessionID`、および SELinux タイプが含まれるようになりました。(BZ#1382508)

`PROCTITLE` が監査イベントで完全なコマンドを提供するようになりました。

今回の更新で、Audit イベントに `PROCTITLE` レコードが追加されました。`PROCTITLE` は、実行中の完全なコマンドを提供します。`PROCTITLE` 値はエンコードされるため、Audit イベントパーサーを回避できません。`PROCTITLE` 値は、ユーザー空間の日付で操作できるため、依然として信頼されていないことに注意してください。(BZ#1299527)

`nss-softokn` がバージョン 3.28.3 にリベース

`nss-softokn` パッケージがアップストリームバージョン 3.28.3 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。

- TLS (RFC 7905)、Internet Key Exchange Protocol (IKE)、および IPsec (RFC 7634) が使用する ChaCha20-Poly1305 (RFC 7539) アルゴリズムのサポートが追加されました。
- 鍵交換の目的で、Curve25519/X25519 カーブのサポートが追加されました。
- Extended Master Secret (RFC 7627) 拡張機能のサポートが追加されました。(BZ#1369055)

`libica` がバージョン 3.0.2 にリベース

`libica` パッケージがアップストリームバージョン 3.0.2 にアップグレードされ、以前のバージョンに比べて多くのバグ修正が提供されています。注目すべき追加項目は以下のとおりです。

- Federal Information Processing Standards (FIPS) モードのサポート
- 更新されたセキュリティ仕様 NIST SP 800-90A に準拠した Deterministic Random Bit Generator の生成を含む、疑似ランダム番号の生成サポートが強化されました。(BZ#1391558)

`opencryptoki` がバージョン 3.6.2 にリベース

`opencryptoki` パッケージがアップストリームバージョン 3.6.2 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。

- **OpenSSL 1.1 のサポートを追加**
- **非推奨の OpenSSL インターフェイスを置き換えました。**
- **非推奨の libica インターフェイスを置き換えました。**
- **IBM Crypto Accelerator (ICA) のパフォーマンスが改善されました。**
- **icsf トークンの rc=8, reasoncode=2028 エラーメッセージのサポートが追加されました。(BZ#1391559)**

AUDIT_NETFILTER_PKT イベントが正規化される

AUDIT_NETFILTER_PKT 監査イベントが単純化され、メッセージフィールドが一貫した方法で表示されるようになりました。(BZ#1382494)

p11tool が、保存された ID を指定してオブジェクトの書き込みをサポートするようになりました

今回の更新で、p11tool GnuTLS PKCS#11 ツールは、保存された ID を指定してオブジェクトを書き込む新しい --id オプションをサポートするようになりました。これにより、書き込まれたオブジェクトを p11tool よりも多くのアプリケーションでアドレス指定できます。(BZ#1399232)

新規パッケージ: nss-pem

この更新では、以前は nss パッケージの一部であった nss-pem パッケージが別のパッケージとして導入されています。nss-pem パッケージは、PKCS#11 モジュールとして実装された Network Security Services (NSS) 用の PEM ファイルリーダーを提供します。(BZ#1316546)

pmrfc3164 は、rsyslog の pmrfc3164sd を置き換えます

rsyslog パッケージの更新により、BSD syslog プロトコル形式(RFC 3164)でログを解析するために使用される pmrfc3164sd モジュールが、公式の pmrfc3164 モジュールに置き換えられました。公式モジュールは pmrfc3164sd 機能を完全にカバーしていないため、rsyslog で引き続き利用できます。ただし、可能な限り新しい pmrfc3164 モジュールを使用することが推奨されます。pmrfc3164sd モジュールはサポートされなくなりました。(BZ#1431616)

libreswan が right=%opportunisticgroup をサポート

今回の更新で、Libreswan 設定の conn 部分の right オプションの %opportunisticgroup 値がサポートされるようになりました。これにより、X.509 認証を使用した日和見的 IPsec が可能になり、大

規模な環境での管理オーバーヘッドが大幅に削減されます。(BZ#1324458)

ca-certificates が Mozilla Firefox 52.2 ESR の要件を満たす

Network Security Services (NSS) コードおよび認証局 (CA) リストが、最新の Mozilla Firefox Extended Support Release (ESR) で公開された推奨に合わせて更新されました。更新された CA リストにより、インターネット公開鍵インフラストラクチャー (PKI) で使用される証明書との互換性が改善されました。証明書の検証が拒否されないようにするため、Red Hat では、2017 年 6 月 12 日に更新された CA リストをインストールすることを推奨しています。(BZ#1444413)

nss が、証明書に関する Mozilla Firefox 52.2 ESR 要件を満たすようになりました。

認証局 (CA) の一覧が、最新の Mozilla Firefox Extended Support Release (ESR) で公開された推奨に合わせて更新されました。更新された CA リストにより、インターネット公開鍵インフラストラクチャー (PKI) で使用される証明書との互換性が改善されました。証明書の検証が拒否されないようにするため、Red Hat では、2017 年 6 月 12 日に更新された CA リストをインストールすることを推奨しています。(BZ#1444414)

scap-security-guide がバージョン 0.1.33 にリベース

scap-security-guide パッケージがアップストリームバージョン 0.1.33 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。特に、この新しいバージョンでは、既存のコンプライアンスプロファイルが強化され、適用範囲が拡張されて、2 つの新しい設定ベースラインが追加されました。

- PCI-DSS v3 コントロールベースラインの拡張サポート
- 米国政府の Commercial Cloud Services (C2S) への拡張サポート
- 認定クラウドプロバイダー向け Red Hat コーポレートプロファイルへの拡張サポート
- Red Hat Enterprise Linux V1R1 プロファイルの米国国防情報システム局 (DISA) およびセキュリティ技術実装ガイド (STIG) に合わせて、Red Hat Enterprise Linux 7 プロファイルの DISA STIG へのサポートが追加されました。
- 非連邦情報システムおよび組織の非機密情報 (NIST 800-171) プロファイルのサポートが追加され、Red Hat Enterprise Linux 7 を管理対象非機密情報 (CUI) を保護するために特定された NIST Special Publication 800-53 コントロールに設定します。
- 米国政府共通設定基準 (USGCB/STIG) プロファイルへのサポートが追加されました。これは、米国立標準技術研究所 (NIST)、米国防総省、米国家安全保障局、および Red Hat とのパー

トナーシップで開発されました。

USGCB/STIG プロファイルは、以下のドキュメントにある設定要件を実装しています。

- 国家安全保障システム委員会指示 No. 1253 (CNSSI 1253)
- NIST 管理対象非機密情報 (NIST 800-171)
- NIST 800-53 中程度の影響を受けるシステムの選択の制御 (NIST 800-53)
- 米国政府共通設定基準 (USGCB)
- NIAP 汎用オペレーティングシステムのプロテクションプロファイル v4.0 (OSPP v4.0)
- DISA オペレーティングシステムセキュリティー要件ガイド (OS SRG)

以前に含まれていたいくつかのプロファイルが削除またはマージされていることに注意してください。(BZ#[1410914](#))

第16章 サーバーおよびサービス

chrony がバージョン 3.1 にリベース

chrony パッケージがアップストリームバージョン 3.1 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。主な機能強化は、次のとおりです。

- 精度を向上させるために、ソフトウェアおよびハードウェアのタイムスタンプへのサポートが追加されました (マイクロ秒未満の精度が可能な場合があります)。
- ネットワークジッターの非対称性により、精度が向上しました。
- インターリーブモードのサポートが追加されました。
- 認証をコマンドキーに置き換えるために、Unix ドメインソケットを介した設定と監視のサポートが追加されました (リモート設定はできなくなりました)。
- サーバーの自動交換が改善されました。
- ntpd デーモンと互換性のある孤立モードが追加されました。
- NTP サーバーの応答速度制限が追加されました。
- info 形式のドキュメントに代わる詳細な man ページが追加されました。 (BZ#1387223)

linuxptp がバージョン 1.8 にリベース

linuxptp パッケージがアップストリームバージョン 1.8 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。主な機能強化は、次のとおりです。

- 大規模なネットワークでネットワークトラフィックを削減するために、ユニキャストメッセージを使用したハイブリッドのエンドツーエンド (E2E) 遅延測定をサポートが追加されました。
- 独立した Precision Time Protocol (PTP) ハードウェアクロックを使用したバウンダリーク

ロック (BC) を実行するためのサポートが追加されました。

- PTP メッセージの Time to Live (TTL) および Differentiated Services Code Point (DSCP) を設定するオプションが追加されました。(BZ#1359311)

tuned がバージョン 2.8.0 にリベース

tuned パッケージがアップストリームバージョン 2.8.0 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべき変更点は次のとおりです。

- CPU パーティションプロファイルが追加されました。
- コアの分離のサポートが追加されました。
- initrd オーバーレイのサポートが追加されました。
- 継承が改善されました。
- udev デバイスマネージャーに基づく regexp デバイスのマッチングが実装されました。(BZ#1388454, BZ#1395855, BZ#1395899, BZ#1408308, BZ#1394965)

logrotate が `/var/lib/logrotate/logrotate.status` をデフォルトの状態ファイルとして使用するようになりました。

以前は、logrotate cron ジョブが logrotate 状態ファイルへの変更されたパスを使用していました。そのため、cron ジョブで使用されるパスは、logrotate 自体が使用するデフォルトの状態ファイルパスと一致しませんでした。混乱を防ぐため、logrotate で使用されるデフォルトの状態ファイルパスは、logrotate cron ジョブで使用される状態ファイルパスに一致するように変更されました。その結果、logrotate は、両方のシナリオでデフォルトの状態ファイルパスとして `/var/lib/logrotate/logrotate.status` を使用するようになりました。(BZ#1381719)

rsyslog がバージョン 8.24.0 にリベース

rsyslog ユーティリティーがアップストリームバージョン 8.24.0 にリベースされ、多くの機能拡張、新機能、バグ修正が含まれています。以下は、主な改善点です。

- 新しいコアエンジンが実装され、メッセージ処理が速くなりました。

- JSON 形式のデータを処理する際の速度と安定性が改善されました。
- RainerScript 設定形式がデフォルトとして選択され、より多くのオプションで改善されました。
- 外部アプリケーションを使用して rsyslog 内のメッセージを操作するための新しい mmexternal モジュールが追加されました。
- omprog モジュールは、外部バイナリーとの通信を改善するために改善されました。
- imrelp モジュールおよび omrelp モジュールが、TLS プロトコルを使用した暗号化された送信をサポートするようになりました。
- imuxsock モジュールは、グローバルルールセットをオーバーライドする個々のソケットのルールセットをサポートするようになりました。
- imuxsock モジュールを使用すると、レート制限メッセージに、レート制限の原因となるプロセスの PID が含まれるようになりました。
- TCP サーバーのエラーメッセージに、リモートホストの IP アドレスが含まれるようになりました。
- 永続的な journald 設定に切り替えた後、imjournal モジュールがログの受信を停止しなくなりました。
- マシンのクロックが以前の時刻に設定されていた場合、再起動後にランタイムジャーナルへのロギングが完全に停止することはなくなりました。
- 以前は、copytruncate オプションを指定した logrotate ユーティリティーがログファイルをローテーションしている場合、imfile モジュールは、ローテーションされるファイルからすべてのログメッセージを読み取らない可能性がありました。結果として、これらのログメッセージは失われました。この状況に対応するために、imfile モジュールが拡張されました。そのため、ログファイルで logrotate copytruncate を使用すると、メッセージが失われなくなりました。

カスタムモジュールを使用する場合は、現在の `rsyslog` バージョンのモジュールを更新することが推奨されます。

非推奨の `rsyslog` オプションについては、非推奨の機能の章も参照してください。(BZ#1313490, BZ#1174345, BZ#1053641, BZ#1196230, BZ#1326216, BZ#1088021, BZ#1419228, BZ#1133687)

mod_nssの新しいキャッシュ設定オプション

今回の更新で、`mod_nss` モジュールへの OCSP 応答のキャッシュを制御する新しいオプションが追加されました。新しいオプションにより、ユーザーは以下を制御できます。

- OCSP 応答を待つ時間
- OCSP キャッシュのサイズ
- キャッシュをまったく行わないことを含む、キャッシュに存在するアイテムの最小および最大期間 (BZ#1392582)

データベースオプションおよび接頭辞オプションが `nss_pcache` から削除されました。

`nss_pcache` ピンキャッシュサービスは、`nss_pcache` がトークンにアクセスする必要がないため、`mod_nss` Apache モジュールの Network Security Services (NSS) データベースを共有しなくなりました。NSS データベースおよび接頭辞のオプションが削除され、`mod_nss` によって自動的に処理されるようになりました。(BZ#1382102)

新規パッケージ: libfastjson

今回の更新で、`rsyslog` の `json-c` ライブラリーの代わりに `libfastjson` ライブラリーが導入されました。`libfastjson` の限定された機能セットにより、`json-c` と比較してパフォーマンスが大幅に向上します。(BZ#1395145)

tuned が initrd オーバーレイをサポート

Tuned は、デフォルトの(Dracut) `initrd` イメージを拡張できる `initrd` オーバーレイをサポートするようになりました。これは、ブートローダープラグインでサポートされています。この例は、Tuned プロファイルでの一般的な使用方法を示しています。

```
[bootloader]
initrd_add_dir=${i:PROFILE_DIR}/overlay.img
```

プロファイルがアクティブになると、`overlay.img` ディレクトリーの内容が現在の `initrd` に追加されます。(BZ#1414098)

openwsman が特定の SSL プロトコルの無効化に対応

以前は、`openwsman` ユーティリティーを使用して特定の SSL プロトコルを無効にする方法はありませんでした。無効なプロトコルの一覧に対する新しい設定ファイルオプションが追加されました。これにより、`openwsman` 設定ファイルを介して特定の SSL プロトコルを無効にできるようになりました。(BZ#1190689)

rear がバージョン 2.0 にリベース

いくつかのバグを修正し、さまざまな拡張機能を追加した更新された `rear` パッケージが、Red Hat Enterprise Linux 7 で利用できるようになりました。以下は、主な変更点です。

- Cyclic Redundancy Check (CRC)機能は、XFS ファイルシステムでデフォルトで有効にされるようになりました。以前は、`rear` はこの動作の変更を無視し、互換性のない UUID フラグで `/boot` パーティションをフォーマットしていました。これにより、復元プロセスが失敗しました。このリベースにより、CRC 機能の `rear` チェックが行われ、リカバリー中に UUID が適切に保持されます。
- IBM Power Systems アーキテクチャー用の GRUB および GRUB2 ブートローダーのサポートが追加されました。
- ディレクティブ `NETFS_RESTORE_CAPABILITIES` が `/usr/share/rear/conf/default.conf` 設定ファイルで `y` オプションに設定されている場合、Linux の機能が保持されるようになりました。
- CIFS 認証情報がレスキューイメージで保持されるようになりました。
- 現在実行しているシステムで GRUB2 ブートローダーの予期しない動作変更を回避するために、`GRUB_SUPERUSER` ディレクティブおよび `GRUB_RESCUE_PASSWORD` ディレクティブが削除されました。
- ドキュメントが改善されました。
- 複数のバックアップの作成が有効になっています。(BZ#1355667)

python-tornado がバージョン 4.2.1 にリベース

`python-tornado` パッケージがアップストリームバージョン 4.2.1 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と新機能が提供されています。以下は、主な変更点です。

- DNS 解決への非同期インターフェイスを提供する新しい `tornado.netutil.Resolver` クラス
- ノンブロッキング DNS、SSL ハンドシェイク、および IPv6 のサポートを持つ TCP 接続を作成する新しい `tornado.tcpclient` モジュール
- `IOLoop.instance ()` 関数がスレッドセーフになりました。
- ログが改善され、低レベルのログの頻度が低くなりました。Tornado はルートロガーではなく独自のロガーを使用するため、より詳細な設定が可能になりました。
- `python-tornado` 内で複数の参照サイクルが分離され、CPythonでより効率的なガベージコレクションが可能になりました。
- コルーチンはより高速になり、Tornado 内で広く使用されています。(BZ#1158617)

第17章 ストレージ

RAID レベルのテイクオーバーの LVM でのサポートが追加されました。

LVM は、以前はテクノロジープレビューとして利用可能だった RAID テイクオーバーを完全にサポートするようになりました。これにより、ユーザーは RAID 論理ボリュームをある RAID レベルから別のレベルに変換できます。このリリースでは、RAID テイクオーバーの組み合わせの数が拡張されました。一部の移行のサポートには、中間ステップが必要になる場合があります。RAID テイクオーバーによって追加された新しい RAID タイプは、以前にリリースされたカーネルバージョンではサポートされていません。これらの RAID タイプは、raid0、raid0_meta、raid5_n、および raid6_{ls,rs,la,ra,n}_6 です。Red Hat Enterprise Linux 7.4 でこれらの RAID タイプを作成したり、これらの RAID タイプに変換したりするユーザーは、以前のリリースを実行しているシステムで論理ボリュームをアクティブ化できません。RAID テイクオーバーは、シングルマシンモードのトップレベル論理ボリュームでのみ利用できます (つまり、テイクオーバーはクラスターボリュームグループで使用できず、RAID がスナップショットまたはシンプールの一部である場合にのみ利用できます)。(BZ#1366296)

LVM が RAID 再成形をサポート

LVM が RAID 再成形をサポートするようになりました。テイクオーバーにより、ユーザーは RAID タイプを変更できますが、再成形により、RAID アルゴリズム、ストライプサイズ、領域のサイズ、イメージ数などのプロパティを変更できます。たとえば、2つのデバイスを追加することで、3 way ストライプを 5 way ストライプに変更できます。再成形は、単一マシンモードの最上位論理ボリュームでのみ利用でき、論理ボリュームが使用中でない場合 (ファイルシステムにマウントされている場合など) に限り利用できます。(BZ#1191935, BZ#834579, BZ#1191978, BZ#1392947)

Device Mapper リニアデバイスが DAX をサポート

dm-linear および dm-stripe ターゲットに、ダイレクトアクセス(DAX)サポートが追加されました。複数の Non-Volatile Dual In-line Memory Module (NVDIMM) デバイスを組み合わせて、より大きな永続メモリー (PMEM) ブロックデバイスを提供できるようになりました。(BZ#1384648)

libstoragemgmt がバージョン 1.4.0 にリベース

libstoragemgmt パッケージがアップストリームバージョン 1.4.0 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、以下のライブラリーが追加されたことです。

- ローカルディスクのシリアル番号のクエリー:
lsm_local_disk_serial_num_get()/lsm.LocalDisk.serial_num_get()
- ローカルディスクの LED ステータスのクエリー:
lsm_local_disk_led_status_get()/lsm.LocalDisk.led_status_get()
- ローカルディスクのリンク速度のクエリー:
lsm_local_disk_link_speed_get()/lsm.LocalDisk.link_speed_get()

以下は、主なバグ修正です。

- Dell PowerEdge RAID Controller (PERC)の megaraid プラグインが修正されました。
- NVM Express (NVMe) ディスクのローカルディスクローテーション速度クエリーが修正されました。
- ローカルディスククエリーでの lsmcli の誤ったエラー処理が修正されました。
- gcc のコンパイルに関する警告がすべて修正されました。
- autoconf AC_OUTPUT マクロの廃止された使用が修正されました。(BZ#1403142)

mpt3sas がバージョン 15.100.00.00 に更新されました。

mpt3sas ストレージドライバーがバージョン 15.100.00.00 に更新され、新しいデバイスのサポートが追加されました。詳細はベンダーにお問い合わせください。(BZ#1306453)

lpfc ドライバーの lpfc_no_hba_reset モジュールパラメーターが利用可能に

今回の更新で、lpfc_no_hba_reset モジュールパラメーターを追加することで、Emulex Fibre Channel Host Bus Adapters (HBAs)の特定のモデルの lpfc ドライバーが強化されました。このパラメーターでは、SCSI エラー処理中にリセットされない HBA の 1 つ以上の 16 進数の World-Wide Port Number (WWPN) の一覧を受け入れます。

lpfc では、SCSI エラー処理時に HBA のどのポートをリセットするかを制御できるようになりました。また、lpfc では、SCSI エラー処理時間の上限を表す eh_deadline パラメーターを設定できるようになりました。(BZ#1366564)

LVM が Veritas Dynamic Multi-Pathing システムを検出し、基本となるデバイスパスに直接アクセスしなくなる

LVM が Veritas Dynamic Multi-Pathing と正しく機能するようにするには、設定ファイル /etc/lvm/lvm.conf の devices セクションで obtain_device_list_from_udev を 0 に設定する必要があります。このようなマルチパスのデバイスは、標準の udev インターフェイスを介して公開されないため、この設定がないと LVM はその存在を認識しません。(BZ#1346280)

libnvdimm カーネルサブシステムが PMEM サブディビジョンをサポート

Intel の Non-Volatile Dual In-line Memory Module (NVDIMM) ラベル仕様が拡張され、リージョンごとに複数の永続メモリー (PMEM) 名前空間を設定できるようになりました (インターリーブセット)。Red Hat Enterprise Linux 7.4 に同梱されるカーネルが、このような新しい設定をサポートするように変更されています。

サブディビジョンのサポートがないと、以前は 1 つのリージョンを 1 つのモード (pmem、device dax、または sector) でしか使用できませんでした。今回の更新で、1 つのリージョンを細分化し、各サブディビジョンをその他のリージョンから独立して設定できるようになりました。 (BZ#1383827)

multipathd が実行されていない場合の警告メッセージ

multipathd の実行中にマルチパスデバイスを作成または一覧表示する multipath コマンドを実行すると、警告メッセージが表示されるようになりました。

multipathd が実行されていない場合、デバイスは障害が発生したパスを復元したり、デバイス設定の変更に反応したりできません。multipathd デーモンは、マルチパスデバイスがあり、multipathd が実行されていない場合に、警告メッセージを出力するようになりました。 (BZ#1359510)

構造化された出力を提供するために multipathd に追加された c ライブラリーインターフェイス

これにより、libdmmp ライブラリーを使用して、multipathd から構造化された情報を取得できるようになりました。multipathd から情報を取得したい他のプログラムは、コマンドを実行して結果を解析しなくても、この情報を取得できるようになりました。 (BZ#1430097)

新しい remove_retries マルチパス設定値

マルチパスが削除を試みた際に、マルチパスデバイスが一時的に使用されている場合、削除は失敗します。remove_retries 設定値を設定することで、multipath コマンドがビジー状態のマルチパスデバイスの削除を再試行する回数を制御できるようになりました。デフォルト値は 0 です。この場合、マルチパスは失敗した削除を再試行しません。 (BZ#1368211)

新しい multipathd reset multipaths stats コマンド

マルチパスが、multipathd reset multipaths stats と multipathd reset multipath dev stats の 2 つの新しい multipathd コマンドに対応するようになりました。このコマンドは、multipathd がすべてのデバイスまたは指定されたデバイスに対してそれぞれ追跡するデバイス統計をリセットします。これにより、デバイスに変更を加えた後で、デバイスの統計をリセットできます。 (BZ#1416569)

新しい disable_changed_wwids mulitpath 設定パラメーター

マルチパスが新しい multipath.conf のデフォルトセクションパラメーター disable_changed_wwids をサポートするようになりました。これを設定すると、パスデバイスが使用

中に `wwid` を変更したときにマルチパス通知が行われ、`wwid` が以前の値に戻るまでパスデバイスへのアクセスが無効になります。

`scsi` デバイスの `wwid` が変更された場合、これはデバイスが別の LUN に再マップされたことを示していることが多いです。`scsi` デバイスの使用中にこの現象が発生すると、データが破損する可能性があります。`disable_changed_wwids` パラメーターを設定すると、`scsi` デバイスが `wwid` を変更したときにユーザーに警告します。多くの場合、`multipathd` は、元の LUN からマッピングが解除されるとすぐにパスデバイスへのアクセスを無効にし、破損の可能性を削除します。ただし、`multipathd` は、`scsi` デバイスが再マップされる前に変更を常にキャッチできるとは限りません。つまり、破損のウィンドウがまだある可能性があります。使用中の `scsi` デバイスの再マッピングは、現在サポートされていません。(BZ#1169168)

HPE 3PAR アレイの組み込み設定を更新

3PAR アレイの組み込み設定では、`no_path_retry` が 12 に設定されるようになりました。(BZ#1279355)

NFINIDAT InfiniBox.* デバイスの組み込み設定の追加

マルチパスが、NFINIDAT InfiniBox.* デバイスを自動設定するようになりました (BZ#1362409)

device-mapper-multipath が `max_sectors_kb` 設定パラメーターをサポート

今回の更新で、`device-mapper-multipath` が `multipath.conf` ファイルの `defaults` セクション、`devices` セクション、`multipaths` セクションに新しい `max_sectors_kb` パラメーターを提供するようになりました。`max_sectors_kb` パラメーターを使用すると、マルチパスデバイスが最初にアクティブ化される前に、`max_sectors_kb` デバイスキューパラメーターをマルチパスデバイスのすべての基礎となるパスで指定された値に設定できます。

マルチパスデバイスが作成されると、デバイスはパスデバイスから `max_sectors_kb` 値を継承します。手動でこの値をマルチパスデバイス向けに高めたり、パスデバイス向けにこの値を低くすると、マルチパスデバイスはパスデバイスが許可するよりも大きな I/O 操作を作成する場合があります。

`max_sectors_kb` `multipath.conf` パラメーターを使用すると、パスデバイス上にマルチパスデバイスを作成する前に、これらの値を簡単に設定でき、無効なサイズの I/O 操作が渡されるのを防ぐことができます。(BZ#1394059)

新しい `detect_checker` マルチパス設定パラメーター

VNX2 などの一部のデバイスは、ALUA モードで任意に設定できます。このモードでは、ALUA 以外のモードとは異なる `path_checker` および `prioritizer` を使用する必要があります。マルチパスが `multipath.conf` のデフォルトセクションと `devices` セクションで `detect_checker` パラメーターをサポートするようになりました。これが設定されている場合、マルチパスはデバイスが ALUA をサポートしているかどうかを検出し、その場合は設定された `path_checker` を上書きし、代わりに TUR

チェッカーを使用します。detect_checker オプションを使用すると、オプションの ALUA モードを持つデバイスをどのモードであるかに関係なく、正しく自動設定できます。(BZ#1372032)

マルチパスに Nimble Storage デバイス用のデフォルト設定が組み込まれる

マルチパスのデフォルトハードウェアテーブルに、Nimble Storage アレイのエントリーが含まれるようになりました。(BZ#1406226)

LVM は、RAID 論理ボリュームのサイズの縮小をサポートします

Red Hat Enterprise Linux 7、4 以降では、lvreduce または lvresize コマンドを使用して、RAID 論理ボリュームのサイズを縮小できます。(BZ#1394048)

iprutils がバージョン 2.4.14 にリベース

iprutils パッケージがアップストリームバージョン 2.4.14 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下に例を示します。

- エンディアンでスワップされた device_id が、以前のバージョンと互換性を持つようになりました。
- ベアメタルモードの VSET 書き込みキャッシュが許可されるようになりました。
- デュアルアダプター設定での RAIDS の作成が修正されました。
- 単一のアダプター設定での再構築の確認がデフォルトで無効になりました。(BZ#1384382)

mdadm がバージョン 4.0 にリベース

mdadm パッケージがアップストリームバージョン 4.0 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべきは、この更新により、Intel Matrix Storage Manager (IMSM) メタデータに不良ブロック管理サポートが追加されたことです。この更新に含まれる機能は、外部メタデータ形式でサポートされており、Red Hat は引き続き Intel Rapid Storage Technology enterprise (Intel RSTe) ソフトウェアスタックをサポートしています。(BZ#1380017)

シンプールの 50% 以上使用されると、LVM はシンプール論理ボリュームのサイズを拡張します。

シンプールの論理ボリュームが 50% を超える場合、デフォルトで dmeventd thin プラグインが 5 パーセント増加するたびに dmeventd thin_command コマンドを呼び出すようになりました。これにより、設定ファイルの activation セクションで設定された thin_pool_autoextend_threshold の上にシンプールがいっぱいになると、シンプールのサイズが変更されます。ユーザーは、外部コマンドを設定

し、`lvm.conf` ファイルの `dmeventd` セクションで `thin_command` の値としてこのコマンドを指定することで、このデフォルトを上書きすることができます。thin プラグインの詳細と、シンプールの維持するように外部コマンドを設定する方法は、`dmeventd (8)` の man ページを参照してください。

以前のリリースでは、シンプールのサイズ変更失敗すると、コンパイル時の定義されたしきい値に達したときに、`dmeventd` プラグインはシンプールに関連付けられたすべてのシンポリュームのアンマウントを試みていました。`dmeventd` プラグインは、デフォルトでボリュームをアンマウントしなくなりました。以前のロジックを再現するには、外部スクリプトを設定する必要があります。
(BZ#1442992)

LVM が dm-cache メタデータバージョン 2 をサポート

LVM/DM キャッシュが大幅に改善されました。これにより、より大きなキャッシュサイズのサポート、変化するワークロードへのより良い適応、起動とシャットダウン時間の大幅な改善、そして全体的なパフォーマンスの向上を実現します。LVM でキャッシュ論理ボリュームを作成する場合、`dm-cache` メタデータ形式のバージョン 2 がデフォルトになりました。バージョン 1 は、以前に作成した LVM キャッシュ論理ボリュームで引き続きサポートされます。バージョン 2 にアップグレードするには、古いキャッシュ層を削除し、新しいキャッシュ層を作成する必要があります。(BZ#1436748)

指定されたハードウェアでの DIF/DIX (T10 PI) のサポート

SCSI T10 DIF/DIX は、ハードウェアベンダーが認定し、特定の HBA およびストレージレイ設定を完全にサポートしている場合、Red Hat Enterprise Linux 7.4 で完全にサポートされます。DIF/DIX は、他の設定ではサポートされていません。ブートデバイスでの使用もサポートされておらず、仮想化ゲストでの使用もサポートされていません。

現在、このサポートを提供するベンダーは以下のとおりです。

FUJITSU は、以下で DIF および DIX をサポートしています。

EMULEX 16G FC HBA:

- EMULEX LPe16000/LPe16002、10.2.254.0 BIOS、10.4.255.23 FW (以下と共に)
- FUJITSU ETERNUS DX100 S3、DX200 S3、DX500 S3、DX600 S3、DX8100 S3、DX8700 S3、DX8900 S3、DX200F、DX60 S3、AF250、AF650

QLOGIC 16G FC HBA:

- QLOGIC QLE2670/QLE2672、3.28 BIOS、8.00.00 FW (以下と共に)
- FUJITSU ETERNUS DX100 S3、DX200 S3、DX500 S3、DX600 S3、DX8100 S3、DX8700 S3、DX8900 S3、DX200F、DX60 S3

T10 DIX には、ディスクブロックでチェックサムの生成および検証を行うデータベースまたはその他のソフトウェアが必要です。現在サポートされている Linux ファイルシステムにはこの機能はありません。

EMC は以下で DIF をサポートしています。

EMULEX 8G FC HBA:

- LPe12000-E および LPe12002-E with firmware 2.01a10 以降 (以下と共に)
- EMC VMAX3 Series with Enginuity 5977、EMC Symmetrix VMAX Series with Enginuity 5876.82.57 以降

EMULEX 16G FC HBA:

- ファームウェア 10.0.803.25 以降の LPe16000B-E および LPe16002B-E (以下と共に)
- EMC VMAX3 Series with Enginuity 5977、EMC Symmetrix VMAX Series with Enginuity 5876.82.57 以降

QLOGIC 16G FC HBA:

- QLE2670-E-SP および QLE2672-E-SP (以下と共に)
- EMC VMAX3 Series with Enginuity 5977、EMC Symmetrix VMAX Series with Enginuity 5876.82.57 以降

最新のステータスは、ハードウェアベンダーのサポート情報を参照してください。

他の HBA およびストレージアレイの場合、DIF/DIX へのサポートはテクノロジープレビューのままとなります。(BZ#1457907)

dmstats 機能により変更されるファイルの統計の追跡が可能に

以前は、**dmstats** 機能は、サイズが変更されなかったファイルの統計を報告できました。ファイルのサイズの変更 (またはファイルに含まれる可能性があるホールを埋める) 中でも、ファイルの変更を監視し、ファイルの I/O を追跡するマッピングを更新できるようになりました。(BZ#1378956)

キャッシュされた論理ボリュームのシンスナップショットのサポート

Red Hat Enterprise Linux 7.4 の LVM では、キャッシュされた論理ボリュームのシンスナップショットを作成できます。この機能は、以前のリリースでは利用できませんでした。これらの外部オリジンのキャッシュされた論理ボリュームは読み取り専用状態に変換されるため、さまざまなシンプールで使用できます。(BZ#1189108)

新規パッケージ: **nvmectl**

nvmectl ユーティリティを使用すると、NVME-over-RDMA ファブリックタイプを使用して、Red Hat Enterprise Linux を NVMeoF ターゲットとして設定できます。**nvmectl** を使用すると、**nvmet** を対話的に設定するか、JSON ファイルを使用して設定を保存および復元できます。(BZ#1383837)

デバイス DAX が NVDIMM デバイスで利用可能に

デバイス DAX を使用すると、ハイパーバイザーやデータベースなどのユーザーは、ファイルシステムを介さずに永続メモリーに raw アクセスできます。特に、Device DAX を使用すると、アプリケーションで予測可能な障害の粒度と、ユーザースペースから永続ドメインにデータをフラッシュする機能を利用できます。Red Hat Enterprise Linux 7.4 以降、Device Dax は Non-Volatile Dual In-line Memory Module (NVDIMM) デバイスで利用できます。(BZ#1383489)

第18章 システムおよびサブスクリプション管理

yumに追加された新しい `payload_gpgcheck` オプション

今回の更新で、新しい設定オプション `payload_gpgcheck` が yum ユーティリティーに追加されました。このオプションにより、パッケージのペイロードセクションで GNU Privacy Guard (GPG) 署名チェックが有効になり、パッケージのインストール時のセキュリティおよび整合性が強化されます。以前は、`gpgcheck` オプションを有効にすると、yum はヘッダーで GPG 署名チェックのみを実行していました。そのため、ペイロードデータが改ざんされていたり、破損していたりすると RPM のアンパックエラーが発生し、パッケージが部分的にインストールされた状態のままになりました。これにより、オペレーティングシステムが一貫性のない脆弱な状態になっている可能性があります。

新しい `payload_gpgcheck` オプションを `gpgcheck` オプションまたは `localpkg_gpgcheck` オプションとともに使用して、この問題を防ぐことができます。その結果、`payload_gpgcheck` を有効にすると、yum はペイロードで GPG 署名チェックを実行し、検証されていない場合はトランザクションを中止します。`payload_gpgcheck` の使用は、ダウンロードしたパッケージで `rpm -K` を手動で実行するのと同じです。(BZ#1343690)

`virt-who`では、プロキシなしの設定を利用できます。

今回の更新で、プロキシネットワーク設定を無視するように `virt-who` サービスを設定できるようになりました。これにより、`virt-who` は一方向通信でプロキシ接続を使用する環境で適切に機能します。

この機能を設定するには、`NO_PROXY` 環境変数を `/etc/sysconfig/virt-who` ファイルに追加します。または、`/etc/rhsm/rhsm.conf` ファイルの `[server]` セクションに `no_proxy` 変数を追加できます。

Red Hat Satellite 5 を使用してハイパーバイザーを同期している場合は、`NO_PROXY` 設定が機能しないことに注意してください。(BZ#1299643)

`virt-who` は、独立した間隔設定を考慮します。

今回の更新で、`virt-who` コマンドは、更新があるすべてのソースについて各間隔を報告するようになりました。さらに、`virt-who` が、Red Hat Satellite インスタンスや Red Hat Subscription Management (RHSM)などの複数の宛先に更新を送信するように設定されている場合、それぞれの間隔は別々に維持されます。つまり、他の宛先との通信の状態に関係なく、設定した各宛先にすべての更新を送信できます。(BZ#1436811)

`virt-who-password`に追加されたパスワードオプション

今回の更新で、`-p` オプションおよび `--password` オプションが `virt-who-password` ユーティリティーに追加されました。これにより、ユーティリティーをスクリプトで使用できるようになります。(BZ#1426058)

一部の `virt-who` 設定パラメーターでは、正規表現とワイルドカードを使用できます。

今回の更新で、`filter_hosts` および `exclude_hosts` 設定パラメーターで正規表現とワイルドカードを使用できるようになりました。これにより、`virt-who` のユーザーは、ホストの一覧を維持して、はるかに簡単にレポートすることができます。

正規表現とワイルドカードを使用して、報告するホストまたは除外するホストを指定すると、ホストの一覧がより簡潔になります。(BZ#[1405967](#))

virt-who 設定ファイルは管理が簡単

`virt-who` サービスは、拡張子 `.conf` で終わる `/etc/virt-who.d/` ディレクトリーの設定ファイルのみを使用するようになりました。これにより、テストやバックアップなど、`virt-who` 設定ファイルの管理が容易になります。(BZ#[1369107](#))

第19章 仮想化

Amazon Web Services の ENA ドライバー

今回の更新で、Red Hat Enterprise Linux 7 カーネルに、Amazon Elastic Network Adapter (ENA) ドライバーのサポートが追加されました。ENA は、Amazon Web Services クラウドの特定のインスタンスタイプに対して、Red Hat Enterprise Linux 7 ゲスト仮想マシンのネットワーク効率を大幅に改善します。

ENA の詳細は、<https://aws.amazon.com/blogs/aws/elastic-network-adapter-high-performance-network-interface-for-amazon-ec2> を参照してください。(BZ#1357491, BZ#1410047)

Synthetic Hyper-V FC アダプターは storvsc ドライバーによりサポートされています。

今回の更新で、storvsc ドライバーが Hyper-V 仮想化でファイバーチャネル(FC)デバイス进行处理する方法が改善されました。特に、新しい合成ファイバーチャネル(FC)アダプターが Hyper-V ハイパーバイザーに設定されている場合、`/sys/class/fc_host/` ディレクトリーおよび `/sys/class/scsi_host/` ディレクトリーに新しい `hostX` (`host1` など) ファイルが作成されます。このファイルには、Hyper-V FC アダプターのワールドワイドポート番号(WWPN)およびワールドワイドノード番号(WWNN)によって決定される `port_name` エントリーおよび `host_name` エントリーが含まれます。(BZ#1308632, BZ#1425469)

親 HBA は WWNN/WWPN ペアでの定義が可能

今回のリリースにより、親ホストバスアダプター(HBA)は、`scsi_host#` に加えて World Wide Node Name (WWNN)および World Wide Port Name (WWPN)で識別できるようになりました。`scsi_host#` で定義されている場合、ハードウェアがホストマシンに追加されると、ホストマシンの再起動後に `scsi_host#` が変更される可能性があります。WWNN/WWPN ペアを使用すると、ホストマシンのハードウェア変更に関係なく、割り当てが変更されません。(BZ#1349696)

libvirt がバージョン 3.2.0 にリベース

libvirt パッケージがアップストリームバージョン 3.2.0 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。注目すべき変更は、以下のとおりです。

- 今回の更新で、特定の libvirt ストレージサブドライバーのインストールおよびアンインストールが可能になり、インストールのフットプリントが削減されます。
- `/etc/nsswitch.conf` ファイルを設定して、KVM ゲストの名前をネットワークアドレスに自動的に解決するように Name Services Switch (NSS)に指示できるようになりました。(BZ#1382640)

KVM が MCE をサポート

今回の更新で、KVM カーネルモジュールに、Machine Check Exception (MCE) のサポートが追加

されました。これにより、KVM ゲスト仮想マシンの Intel Xeon v5 プロセッサの Local MCE (LMCE) 機能を使用できるようになりました。LMCE は、すべてのスレッドにブロードキャストするのではなく、単一のプロセッサスレッドに MCE を配信できるため、マシンチェックが必要以上の vCPU のパフォーマンスに影響を与えないようにすることが可能です。その結果、プロセッサスレッドが多数あるマシンで MCE を処理する際に、ソフトウェアの負荷が軽減されます。(BZ#1402102, BZ#1402116)

tun/tap デバイスでの rx バッチのサポートを追加

今回のリリースで、tun/tap デバイス用の rx バッチがサポートされるようになりました。これにより、バンドルされたネットワークフレームを受信できるため、パフォーマンスを向上できます。(BZ#1414627)

libguestfs がバージョン 1.36.3 にリベース

libguestfs パッケージがアップストリームバージョン 1.36.3 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。以下は、主な変更点です。

- 今回の更新で、tail -f コマンドと同様に、ゲスト内の(tail)ログファイルを追跡するために使用できる virt-tail ユーティリティーが追加されました。詳細は、virt-tail(1) の man ページを参照してください。
- virt-v2v ユーティリティーは、より多くのオペレーティングシステムおよびより多くの入力ソースをサポートします。さらに、Windows ゲストの変換が大幅に書き直され、簡素化されました。
- virt-customize ユーティリティー、virt-builder ユーティリティー、および virt-systprep ユーティリティーに複数のオプションが追加されました。(BZ#1359086)

QXL ドライバーの virt-v2v インストールの改善

今回の更新で、Windows ゲスト仮想マシンでの QXL ドライバーインストールの virt-v2v 実装が再機能し、QXL ドライバーがこれらのゲストに正しくインストールされるようになりました。(BZ#1233093, BZ#1255610, BZ#1357427, BZ#1374651)

virt-v2v は、ディスクイメージを qcow2 形式 1.1 にエクスポートできる

今回の更新で、-o RHEV オプションの使用時に、virt-v2v ユーティリティーが qcow2 形式バージョン 1.1 と互換性のあるディスクイメージをエクスポートするようになりました。さらに、virt-v2v は、vdsmd 出力モードに --vdsmd-compat=COMPAT オプションを追加します。このオプションは、-o vdsmd オプションでイメージをエクスポートする際に、virt-v2v が使用する qcow2 形式のバージョンを指定します。(BZ#1400205)

追加の virt ツールは、LUKS ディスク全体で暗号化されたゲストで機能できます。

今回の更新で、`virt-customize`、`virt-get-kernel`、`virt-sparsify`、および `virt-sysprep` ツールを使用して、LUKS ディスク全体の暗号化ゲストでの作業がサポートされるようになりました。これにより、このツールで、LUKS ディスク全体で暗号化したゲストを開くための鍵やパスワードを提供できるようになりました。(BZ#1362649)

すべての `libguestfs` コマンドのタブ補完

すべての `libguestfs` ツールに `Bash` 補完スクリプトが追加されました。これにより、すべての `libguestfs` コマンドで、`bash` で `Tab` 補完を使用できるようになりました。(BZ#1367738)

サイズを変更したディスクは、リモートの場所に直接書き込むことができます。

今回の更新で、`virt-resize` ユーティリティーが出力をリモートの場所に書き込めるようになりました。これは、サイズを変更したディスクイメージを `Ceph` ストレージボリュームに直接書き込む場合などに役立ちます。`virt-resize` 出力ディスクは、`URI` を使用して指定できます。サポートされている入力プロトコルとフォーマットを使用して、出力を指定できます。(BZ#1404182)

ユーザー名前空間が完全にサポートされるようになりました。

以前はテクノロジープレビューとして利用可能だったユーザー名前空間機能が、完全にサポートされるようになりました。これにより、`Linux` コンテナを実行しているサーバーで、ホストとコンテナの分離が改善され、セキュリティが強化されます。コンテナの管理者がホストで管理操作を実行できなくなり、セキュリティが向上します。(BZ#1138782)

`Hyper-V` のゲスト仮想マシンで `PCI Express` バスを介して接続するデバイス用にドライバーが追加されました

今回の更新で、`PCI Express` バス経由で接続するデバイスを、`Hyper-V` ハイパーバイザーで実行している `Red Hat Enterprise Linux` ゲスト仮想マシンに渡す際に、`root PCI` バスを公開する新しいドライバーが追加されました。この機能は現在、`Microsoft Windows Server 2016` でサポートされています。(BZ#1302147)

第20章 ATOMIC HOST とコンテナ

Red Hat Enterprise Linux Atomic Host

Red Hat Enterprise Linux Atomic Host は、Linux コンテナの実行のために最適化された安全かつ軽量で、フットプリントを最小限に抑えたオペレーティングシステムです。最新の新機能、既知の問題、テクノロジープレビューについては、[Atomic Host and Containers Release Notes](#) を参照してください。

第21章 RED HAT SOFTWARE COLLECTIONS

Red Hat Software Collections とは、動的なプログラミング言語、データベースサーバー、関連パッケージを提供する Red Hat のコンテンツセットのことで、AMD64 および Intel 64 のアーキテクチャ上の Red Hat Enterprise Linux 6 および Red Hat Enterprise Linux 7 のすべてのサポートされるリリースにインストールして使用できます。Red Hat Developer Toolset は、別の Software Collection として提供されています。

Red Hat Developer Toolset は、Red Hat Enterprise Linux プラットフォームで作業する開発者向けに設計されています。GNU Compiler Collection、GNU Debugger、その他の開発用ツールやデバッグ用ツール、およびパフォーマンス監視ツールの現行バージョンを提供します。Red Hat Software Collections 2.3 以降、Eclipse 開発プラットフォームは別の Software Collection として提供されています。

Red Hat Software Collections で配信される動的言語、データベースサーバーなどのツールは Red Hat Enterprise Linux で提供されるデフォルトのシステムツールに代わるものでも、これらのデフォルトのツールよりも推奨されるツールでもありません。Red Hat Software Collections は、scl ユーティリティーをベースとした代替パッケージメカニズムを使用して、パッケージの並列セットを提供します。Red Hat Software Collections を利用すると、Red Hat Enterprise Linux で別のバージョンのパッケージを使用することもできます。scl ユーティリティーを使用すると、いつでも実行するパッケージバージョンを選択できます。

**重要**

Red Hat Software Collections のライフサイクルおよびサポート期間は、Red Hat Enterprise Linux に比べて短くなります。詳細は、[Red Hat Software Collections Product Life Cycle](#) を参照してください。

セットに含まれるコンポーネント、システム要件、既知の問題、使用方法、および各 Software Collection の詳細は、[Red Hat Software Collections documentation](#) を参照してください。

このソフトウェアコレクション、インストール、使用方法、既知の問題などに含まれるコンポーネントの詳細は、[Red Hat Developer Toolset のドキュメント](#) を参照してください。

パート II. 主なバグ修正

ここでは、ユーザーに大きな影響を及ぼしていた Red Hat Enterprise Linux 7.4 のバグで修正されたものを説明します。

第22章 全般的な更新

Systemd への CtrlAltDelBurstAction の追加

複数の CTRL+ALT+DEL イベントに対する systemd 応答は、`/etc/systemd/system.conf` で `CtrlAltDelBurstAction` オプションを設定することで設定できるようになりました(BZ#1353028)。

`cgred` が NSS ユーザーおよびグループに関するルールを解決できるようになりました。

以前は、`cgred` サービスは、Name Service Switch (NSS)のユーザーおよびグループを提供するサービスの後に起動するように設定されませんでした。また、無効なルールのスキップに関する情報は、デバッグモードでのみ表示されていました。そのため、NSS ユーザーおよびグループに関する `cgrules.conf` ファイルのルールが、ログメッセージなしで無視されることがありました。今回の更新で、`cgred` が `nss-user-lookup` ターゲットの後に起動するように設定され、ルールのスキップに関するログメッセージのレベルが `warning` に変更されました。これは、`cgred` デーモンのデフォルトのログレベルとしても設定されます。これにより、NSS ユーザーおよびグループは、を開始する前に常に解決されるようになりました。また、`cgrules.conf` の一部のルールが無効になっている場合、警告メッセージがログに記録されます。(BZ#1406927)

第23章 認証および相互運用性

yum が、ipa-clientのインストール後にパッケージの競合を報告しなくなりました。

ユーザーが ipa-client パッケージをインストールすると、yum ユーティリティーが、ipa パッケージと freeipa パッケージ間のパッケージの競合を予期せず報告しました。このエラーは、トランザクションの失敗後、または yum check コマンドの使用後に発生しました。今回の更新で、RPM でこのような競合が発生するため、yum は自己競合パッケージに関するエラーを報告しなくなりました。その結果、yum は、ipa-client のインストール後に上記のエラーを表示しなくなりました。(BZ#1370134)

FIPS モードでは、slapd_pk11_getInternalKeySlot () 関数を使用して、トークンのキースロットを取得するようになりました。

Red Hat Directory Server は、セキュリティーデータベースで FIPS モードが有効になっているときに、固定トークン名からキースロットを取得しようとして失敗しました。ただし、トークン名は変更できます。キースロットが見つからないと、Directory Server がレプリケーションマネージャーのパスワードをデコードできず、レプリケーションセッションが失敗します。この問題を修正するために、slapd_pk11_getInternalKeySlot () 関数は FIPS モードを使用して現在のキースロットを取得するようになりました。その結果、上記の状況では、SSL または STARTTLS を使用したレプリケーションセッションが失敗しなくなりました。(BZ#1378209)

Certificate System は、FIPS モードのシステムで Thales HSM でインストールに失敗しなくなりました。

Thales ハードウェアセキュリティーモジュール (HSM) で Certificate System (CS) を使用してインストールした後、HSM ですべてのシステムキーを生成した場合、SSL プロトコルが正しく機能しませんでした。そのため、CS は FIPS モードが有効になっているシステムにインストールできず、server.xml ファイルの sslRangeCiphers パラメーターを手動で変更する必要がありました。このバグが修正され、Thales HSM を使用したインストールの FIPS 対応システムが期待どおりに機能するようになりました。(BZ#1382066)

pkispawn の依存関係一覧に、openssl が正しく含まれるようになる

以前は、openssl パッケージがインストールされていない場合、pkispawn ユーティリティーの使用が以下のエラーで失敗していました。

```
Installation failed: [Errno 2] No such file or directory
```

この問題は、openssl パッケージが、pki-core パッケージに含まれる pki-server パッケージのランタイム依存関係として含まれていなかったために発生しました。このバグは、不足している依存関係を追加することで修正され、openssl がないため pkispawn のインストールに失敗しなくなりました。(BZ#1376488)

PKI サーバープロファイルフレームワークからのエラーメッセージがクライアントに渡されるようになる

以前は、PKI サーバーは、証明書要求のプロファイルフレームワークにより生成された特定のエラー

メッセージをクライアントに渡していませんでした。そのため、Web UI または pki コマンドの出力に表示されるエラーメッセージで、要求が失敗した理由が説明されませんでした。コードが修正され、エラーメッセージが渡されるようになりました。ユーザーは、登録に失敗した理由や、登録が拒否された理由を確認できるようになりました。(BZ#1249400)

インストール時に、Certificate System が Lightweight CA 鍵のレプリケーションを開始しない

Certificate System は、2 段階のインストールで、Lightweight CA 鍵のレプリケーションを間違っ
て開始していました。その結果、インストールに失敗し、エラーが表示されました。この更新では、2
段階のインストールで Lightweight CA キーの複製は開始されず、インストールは正常に完了します。
(BZ#1378275)

PKI サーバーが、起動時にサブジェクト DN を正しく比較するようになりました。

プライマリー CA に Lightweight CA エントリーを追加するルーチンのバグにより、PKI サーバー
は、UTF8String 以外のエンコーディングを使用する属性が含まれている場合に、サブジェクト識別名
(DN)の比較に失敗していました。その結果、プライマリー CA が起動するたびに、Lightweight CA エ
ントリーが追加されました。PKI サーバーは、サブジェクト DN を正規の形式で比較するようになりま
した。その結果、PKI サーバーは、前述のシナリオで Lightweight CA エントリーを追加しなくなりま
した。(BZ#1378277)

不完全な証明書チェーンを持つ中間 CA に接続したときに、KRA のインストールが失敗しなくなりま
した。

以前は、信頼できる CA 証明書があるがルート CA 証明書がない中間 CA への接続を試みると、KRA
(Key Recovery Authority)サブシステムのインストールが UNKNOWN_ISSUER エラーで失敗していま
した。この更新により、KRA のインストールはエラーを無視し、正常に完了します。(BZ#1381084)

証明書プロファイルの startTime フィールドが長い整数形式を使用するようになりました。

以前は、Certificate System は、証明書プロファイルの startTime フィールドに 整数 として値を保
存していました。これより大きな数字を入力すると、Certificate System により、この値が負の数とし
て解釈されます。その結果、認証局は、過去の開始日を含む証明書を発行しました。今回の更新
で、startTime フィールドの入力形式が長い整数に変更されました。これにより、発行した証明書の開
始日が正しくなりました。(BZ#1385208)

PKCS#11 トークンがログインしていないため、下位 CA のインストールに失敗しなくなりました。

以前は、Network Security Services (NSS)ライブラリーのバグが原因で、下位認証局(sub-CA)のイ
ンストールに失敗していました。これにより、SEC_ERROR_TOKEN_NOT_LOGGED_IN エラーが生
成されていました。今回の更新で、インストーラーに回避策が追加され、インストールを続行できるよ
うになりました。それでもエラーが表示される場合は、無視できるようになりました。(BZ#1395817)

pkispawn スクリプトが ECC 鍵サイズを正しく設定するようになりました。

以前は、ユーザーが Elliptic Curve Cryptography (ECC)キーサイズパラメーターをデフォルト値(
nistp256)とは異なる値に設定して pkispawn スクリプトを実行すると、設定は無視されていました。
そのため、作成された PKI サーバーインスタンスがシステム証明書を発行しました。これは、デフォル
トの ECC 鍵曲線を誤って使用していました。今回の更新で、PKI サーバーは、ECC 鍵曲線名に

pkispawn 設定に設定された値を使用するようになりました。その結果、PKI サーバーインスタンスは、インスタンスの設定時に設定された ECC 鍵サイズを使用するようになりました。(BZ#1397200)

FIPS モードでの CA クローンのインストールに失敗しなくなりました。

以前は、CA クローンまたは Key Recovery Authority (KRA) のインストールは、内部 NSS トークン名の処理に一貫性がないため、FIPS モードで失敗していました。今回の更新で、トークン名を処理するコードが統合され、すべてのトークン名が一貫して処理されるようになりました。T を使用すると、FIPS モードで KRA および CA クローンのインストールが適切に完了します。(BZ#1411428)

entryUSN 属性に 32 ビットより大きい値が含まれている場合に、PKI サーバーの起動に失敗しなくなりました。

以前は、*LDAP プロファイルモニターと Lightweight CA Monitor は、**entryUSN** 属性の値を 32 ビット整数として解析していました。その結果、属性にそれより大きい値が含まれる場合、**NumberFormatException** エラーがログに記録され、サーバーが起動しませんでした。この問題は修正され、前述のシナリオでサーバーの起動に失敗することはなくなりました。(BZ#1412681)

Tomcat はデフォルトで IPv6 で動作する

IPv4固有の 127.0.0.1 ループバックアドレスは、以前はデフォルトのサーバー設定ファイルでデフォルトの AJP ホスト名として使用されていました。これにより、IPv6のみの環境で実行されるサーバーで接続が失敗しました。今回の更新で、デフォルト値は **localhost** に変更され、IPv4 プロトコルと IPv6 プロトコルの両方で機能します。さらに、既存のサーバーインスタンスの AJP ホスト名を自動的に変更するためのアップグレードスクリプトを使用できます。(BZ#1413136)

pkispawn が無効な NSS データベースパスワードを生成しなくなりました。

今回の更新以前は、**pkispawn** は NSS データベース用に無作為のパスワードを生成していましたが、場合によってはバックスラッシュ(\)文字が含まれていました。これにより、NSS が SSL 接続を確立したときに問題が発生し、**ACCESS_SESSION_ESTABLISH_FAILURE** エラーでインストールが失敗しました。

この更新により、ランダムに生成されたパスワードにバックスラッシュ文字を含めることができなくなり、接続を常に確立できるため、インストールを正常に完了することができます。(BZ#1447762)

--serial オプションを使用してユーザー証明書を追加するときに、証明書の取得が失敗しなくなりました。

--serial パラメーターを指定して **pki user-cert-add** コマンドを使用すると、認証局(CA)への SSL 接続が正しく設定されていなかったため、証明書の取得に失敗していました。この更新では、コマンドは CA への適切に設定された SSL 接続を使用し、操作は正常に完了します。(BZ#1246635)

エントリーが 1 つだけの場合、CA Web インターフェイスに空の証明書要求ページが表示されなくなりました。

以前は、CA Web ユーザーインターフェイスの証明書要求ページにエントリーが1つしか含まれていなかった場合、単一のエントリーではなく空のページが表示されていました。今回の更新で Web ユーザーインターフェイスが修正され、証明書の要求ページがすべての状況で正しくエントリーを表示できるようになりました。(BZ#1372052)

コンテナ環境に PKI サーバーをインストールしても警告が表示されなくなる

以前は、コンテナ環境に pki-server RPM パッケージをインストールすると、systemd デーモンが再読み込みされていました。その結果、警告が表示されました。RPM アップグレード時のみデーモンを再ロードするパッチが適用されました。その結果、上記のシナリオで警告が表示されなくなります。(BZ#1282504)

G&D スマートカードを使用したトークンの再登録が失敗しなくなる

以前は、Giesecke & Devrient (G&D) スマートカードを使用してトークンを再登録すると、特定の状況でトークンの登録が失敗する可能性がありました。問題が修正され、トークンの再登録が想定どりに機能するようになりました。(BZ#1404881)

PKI サーバーは、起動時の証明書検証エラーの詳細を提供します。

以前は、サーバーの起動時に証明書の検証エラーが発生した場合、PKI サーバーが十分な情報を提供していませんでした。その結果、問題のトラブルシューティングは困難でした。PKI サーバーは、新しい Java セキュリティーサービス (JSS) API を使用するようになりました。これにより、前述のシナリオでのエラーの原因に関するより詳細な情報が提供されます。(BZ#1330800)

PKI サーバーが LDAPProfileSubsystem プロファイルの再初期化に失敗しなくなる

LDAPProfileSubsystem プロファイルの再初期化中の競合状態が原因で、PKI サーバーは以前に要求されたプロファイルが存在しないと誤って報告する可能性がありました。その結果、プロファイルを使用する要求が失敗する可能性がありました。問題が修正され、プロファイルを使用する要求が失敗しなくなりました。(BZ#1376226)

HSM で生成された秘密鍵の抽出に失敗しなくなりました。

以前は、鍵回復エージェント (KRA) で新しい Asymmetric Key Generation REST サービスを使用して、Lunasa または Thales ハードウェアセキュリティーモジュール (HSM) で非対称鍵を生成すると、PKI サーバーが間違ったフラグを設定していました。その結果、生成された秘密鍵をユーザーが取得できませんでした。このコードは、この HSM で生成された鍵に正しいフラグを設定するように更新されました。これにより、前述のシナリオでユーザーが秘密鍵を取得できるようになりました。(BZ#1386303)

pkispawn が数字のみで設定されるパスワードを生成しなくなりました

以前は、pkispawn は数字のみで設定される NSS データベースの無作為なパスワードを生成する可能性があります。このようなパスワードは FIPS に準拠していません。今回の更新で、インストーラーが、数字、小文字、大文字、および特定の句読点を混在させた FIPS 準拠のランダムパスワードを生成するように変更されました。(BZ#1400149)

CA 証明書が正しい信頼フラグでインポートされる

以前のリリースでは、`pki client-cert-import` コマンドは、`CT,c` 信頼フラグを使用して CA 証明書をインポートしていましたが、これは不十分で、他の PKI ツールと一貫性がありませんでした。今回の更新で、コマンドが修正され、CA 証明書の信頼フラグが `CT,C,C` に設定されるようになりました。(BZ#1458429)

`--usage verify` オプションの使用時に対称鍵の生成に失敗しなくなりました。

`pki` ユーティリティーは、生成される対称鍵の有効な使用法のリストをチェックします。以前は、このリストに `verify` の使用がありませんでした。これにより、`key-generate --usage verify` オプションを使用するとエラーメッセージが返されました。コードが修正され、`verify` オプションが期待どおりに機能するようになりました。(BZ#1238684)

後続の PKI インストールが失敗しなくなる

以前は、複数の公開鍵インフラストラクチャー (PKI) インスタンスをバッチモードでインストールする場合、インストールスクリプトは CA インスタンスが再起動されるまで待機しませんでした。その結果、後続の PKI インスタンスのインストールが失敗する可能性がありました。スクリプトが更新され、新しいサブシステムが要求を処理できるようになるまで待機してから続行します。(BZ#1446364)

FIPS モードでの 2 段階の subordinate CA インストールに失敗しなくなる

以前は、FIPS モードでの subordinate CA インストールのバグにより、2 つ目の手順でインスタンスが存在しないことをインストーラーが要求するため、2 段階のインストールが失敗していました。今回の更新で、最初の手順 (インストール) ではインスタンスが存在しないことが要求され、2 番目の手順 (設定) ではインスタンスが存在することが要求されるようにワークフローが変更されました。

以前の `pki_skip_configuration` および `pki_skip_installation` デプロイメントパラメーターを置き換えるために、`pkispawn` コマンドに 2 つの新しいオプション `--skip-configuration` および `--skip-installation` が追加されました。これにより、変更を加えずに、両方の手順で同じデプロイメント設定ファイルを使用できます。(BZ#1454450)

監査ログは、証明書の要求が拒否またはキャンセルされたときに成功を記録しなくなりました。

以前は、証明書要求が拒否またはキャンセルされた場合、サーバーは `Outcome=Success` で `CERT_REQUEST_PROCESSED` 監査ログエントリを生成していました。要求に対して証明書が発行されていないため、これは間違っていました。このバグは修正され、拒否またはキャンセルされたリクエストの `CERT_REQUEST_PROCESSED` 監査ログエントリが `Outcome=Failure` を読み取るようになりました。(BZ#1452250)

セルフテストに失敗した PKI サブシステムが、システムの起動時に自動的に再度有効になるようになりました。

以前は、セルフテストの失敗が原因で PKI サブシステムを開始できなかった場合に、一貫性のない状態で実行されないように、PKI サブシステムは自動的に無効にされていました。管理者は、問題を修正した後、`pki-server` サブシステムを有効にして手動でサブシステムを再度有効にすることが想定されました。しかし、これは明確に伝達されておらず、この要件を常に認識しているとは限らない管理者の

間で混乱を引き起こす可能性があります。

この問題を軽減するため、すべての PKI サブシステムが、デフォルトでシステムの起動時に自動的に再度有効になりました。セルフテストが失敗すると、サブシステムは以前と同様に無効になりますが、手動で再度有効にする必要はありません。

この動作は、`/etc/pki/pki.conf` ファイルの新しいブール値オプション `PKI_SERVER_AUTO_ENABLE_SUBSYSTEMS` によって制御されます。(BZ#1454471)

`CERT_REQUEST_PROCESSED` 監査ログエントリーに、エンコードされたデータではなく証明書のシリアル番号が含まれるようになりました。

以前は、`CERT_REQUEST_PROCESSED` 監査ログエントリーに Base64 でエンコードされた証明書データが含まれていました。以下に例を示します。

```
[AuditEvent=CERT_REQUEST_PROCESSED]...[InfoName=certificate][InfoValue=MIIDBD...]
```

証明書データは個別にデコードする必要があるため、この情報はあまり役に立ちませんでした。以下の例のように、コードが変更され、証明書のシリアル番号がログエントリーに直接含まれるようになりました。

```
[AuditEvent=CERT_REQUEST_PROCESSED]...[CertSerialNum=7]
```

(BZ#1452344)

LDAPProfileSubsystem プロファイルの更新で属性の削除に対応

以前は、PKI サーバーで `LDAPProfileSubsystem` プロファイルを更新すると、属性を削除できませんでした。そのため、特定の状況でプロファイルを更新した後、PKI サーバーがプロファイルを読み込んだり、証明書を発行したりできませんでした。パッチが適用され、PKI サーバーが新しい設定を読み込む前に、既存のプロファイル設定を消去するようになりました。その結果、`LDAPProfileSubsystem` プロファイルの更新で、設定属性を削除できるようになりました。(BZ#1445088)

第24章 クラスタリング

クラスターへの接続が管理対象外の場合でも、Pacemaker リモートがシャットダウンすることがある

以前は、Pacemaker リモート接続が管理対象外の場合、Pacemaker リモートデーモンはクラスターからシャットダウンの確認を受け取ることはありませんでした。その結果、Pacemaker リモートはシャットダウンできなくなりました。この修正により、Pacemaker リモート接続が管理対象外の場合、クラスターはリソースの停止を待つのではなく、シャットダウンを要求するシャットダウン確認を Pacemaker リモートノードに即座に送信するようになりました。その結果、クラスターへの接続が管理対象外の場合でも、Pacemaker リモートがシャットダウンする可能性があります。(BZ#1388489)

pcs が、リモートノードとゲストノードの名前とホストを検証するようになりました。

以前は、pcs コマンドは、リモートノードまたはゲストノードの名前またはホストがリソース ID またはクラスターノードと競合しているかどうかを検証しませんでした。これにより、クラスターが正しく機能しませんでした。今回の修正により、関連するコマンドに検証が追加され、pcs では、ユーザーがリモートまたはゲストノードの競合する名前または競合するホストを使用してクラスターを設定できなくなりました。(BZ#1386114)

pcs resource create コマンドの master オプションの新しい構文により、メタ 属性を正しく作成可能

以前は、pcs resource creation コマンドに --master フラグが含まれる場合、キーワード meta 以降のすべてのオプションがマスターメタ属性として解釈されていました。これにより、--master フラグが指定されている場合にプリミティブのメタ属性を作成できませんでした。この修正により、コマンドに次の形式を使用し、リソースをマスタースレーブクローンとして指定する新しい構文が追加されました。

```
pcs resource create resource_id standard:provider:type|type [resource options] master
[master_options...]
```

これにより、以下のようにメタ オプションを指定できます。

```
pcs resource create resource_id standard:provider:type|type [resource_options] meta meta_options...
master [master_options...]
```

さらに、今回の修正では、以前のリリースと同様に、--clone フラグではなく clone オプションでクローンリソースを指定します。クローンリソースを指定する新しい形式は、以下のとおりです。

```
pcs resource create resource_id standard:provider:type|type [resource_options] clone
```

(BZ#1378107)

第25章 コンパイラーおよびツール

PCRE ライブラリーが、Unicode で必要な非 ASCII 印刷可能文字を正しく認識するようになりました。

Perl Compatible Regular Expressions (PCRE) ライブラリーを使用して、Unicode 文字列と、ASCII 以外の印刷可能な文字を一致させると、ライブラリーが、以前は印刷可能な ASCII 以外の文字を正しく認識できませんでした。パッチが適用され、PCRE ライブラリーが、UTF-8 モードで出力可能な非 ASCII 文字を認識するようになりました。(BZ#1400267)

Bundler を使用して依存関係を管理するアプリケーションが、JSON ライブラリーを適切にロードできるようになりました。

以前は、Bundler を使用して Ruby アプリケーションの依存関係を管理すると、JSON ライブラリーを読み込むことができないことがありました。その結果、アプリケーションは LoadError で失敗しました。これにより、Ruby on Rails が JSON ライブラリーの依存関係を明示的に指定しなくなったため、問題が発生していました。今回の更新により、ロードパスで JSON が常に利用可能になり、上記の問題は発生しなくなりました。(BZ#1308992)

Git を HTTP または HTTPS および SSO で使用できるようになりました。

libcurl バージョン 7.21.7 以降、CVE-2011-2192 のために Kerberos チケットを委譲するための新しいパラメーターが必要です。以前のバージョンでは、Git はそのようなパラメーターを設定する方法を提供していませんでした。そのため、HTTP または HTTPS 接続のシングルサインオンでの Git の使用に失敗していました。今回の更新により、Git は cURL --delegation パラメーターに対応する新しい http.delegation 設定変数を提供します。Kerberos チケットの委任が必要な場合、ユーザーはこのパラメーターを設定する必要があります。(BZ#1369173)

rescan-scsi-bus.sh --luns= 1 は、1 で番号が付けられた LUN のみをスキャンするようになりました。

sg3-utils には、SCSI コマンドをデバイスに送信するユーティリティーが同梱されています。バージョン 1.28-5 およびそれ以前のすべてのバージョンの sg3_utils では、rescan-scsi-bus.sh --luns= 1 コマンドは、1 で番号が付けられた論理ユニット番号(LUN)のみを再スキャンしました。バージョン 1.28-6 に更新した後、rescan-scsi-bus.sh --luns=1 はすべての LUN を誤って再スキャンしました。今回の更新で、基礎となるソースコードが修正され、rescan-scsi-bus.sh --luns= 1 は 1 で番号が付けられた LUN のみをスキャンするようになりました。(BZ#1380744)

ps が待機チャンネル名から接頭辞を削除しなくなりました。

ps ユーティリティーは、以前は待機チャンネル(WCHAN)データから sys_ および do_ 接頭辞を削除していました。これにより、ユーザーは、ps の出力にこれらの接頭辞を意図的に含む名前の関数を区別できませんでした。接頭辞を削除するコードが削除され、ps に完全な待機チャンネル名が表示されるようになりました。(BZ#1373246)

.history ファイルがネットワークファイルシステムにある場合、tcsh が応答しなくなる

以前は、.history ファイルが NFS や Samba などのネットワークファイルシステムにある場合、ログインプロセス中に tcsh コマンド言語インタープリターが応答しなくなることがありました。.history

がネットワークファイルシステムにある場合、`.history` ファイルロックを回避するためにパッチが適用され、上記の状況では `tcsh` が応答しなくなることはなくなりました。

`tcsh` の複数のインスタンスを実行すると、`.history` が破損する可能性があることに注意してください。この問題を解決するには、`savehist` オプションに `lock` パラメーターを追加して、明示的なファイルロックメカニズムを有効にします。以下に例を示します。

```
$ cat /etc/csh.cshrc
# csh configuration for all shell invocations.
set savehist = (1024 merge lock)
```

`.history` がネットワークファイルシステムにある場合に `tcsh` がファイルロックを使用するように強制するには、`lock` オプションは `savehist` オプションの 3 番目のパラメーターである必要があります。Red Hat は、`lock` パラメーターを使用すると、ログインプロセス中に `tcsh` が応答しなくなることを保証しません。(BZ#1388426)

`fcoeadm --target` が原因で `fcoeadm` がクラッシュしなくなる

以前は、`fcoeadm --target` コマンドを実行すると、`fcoeadm` ユーティリティーがセグメンテーション違反で予期せず終了することがありました。今回の更新で、`fcoeadm` が FCoE 以外のターゲットの `sysfs` パスを見逃すように変更され、`fcoeadm --target` により `fcoeadm` がクラッシュしなくなりました。(BZ#1384707)

`tar` オプション `--directory` は無視されなくなりました

以前は、`--remove-files` オプションと組み合わせて使用すると、`tar` コマンドの `--directory` オプションが無視されていました。その結果、`--directory` オプションで指定したディレクトリ内のファイルではなく、現在の作業ディレクトリのファイルが削除されました。このバグを修正するために、`--directory` オプションを取得、保存、および操作する新しい関数と属性が追加されました。その結果、`--directory` オプションで指定したディレクトリからファイルが正しく削除されるようになりました。(BZ#1319820)

`tar` オプション `--xattrs-exclude` および `--xattrs-include` が無視されなくなる

以前は、`tar` コマンドは `--xattrs-exclude` オプションおよび `--xattrs-include` オプションを無視していました。このバグを修正するために、拡張属性をフェッチするときに包含マスクと除外マスクを適用するように `tar` が変更されました。その結果、`--xattrs-exclude` オプションおよび `--xattrs-include` オプションは無視されなくなりました。(BZ#1341786)

`tar` が増分バックアップを正しく復元するようになりました。

以前は、`tar` コマンドは増分バックアップを正しく復元しませんでした。そのため、増分バックアップで削除されたファイルは、復元時に削除されませんでした。バグが修正され、`tar` が増分バックアップを正しく復元するようになりました。(BZ#1184697)

`perl-homedir` プロファイルスクリプトが `csh` をサポート

以前は、perl-homedir プロファイルスクリプトは C シェル (csh) 構文を処理できませんでした。そのため、perl-homedir パッケージがインストールされ、/etc/sysconfig/perl-homedir ファイルに PERL_HOMEDIR=0 行が含まれていた場合、プロファイルスクリプトを実行すると、以下のエラーが発生します。

```
PERL_HOMEDIR=0: Command not found.
```

今回の更新で、csh 構文のサポートが追加され、上記の問題は発生しなくなりました。
(BZ#1122993)

getaddrinfo が初期化されていないデータにアクセスしなくなる

nscd デーモンが有効になっているシステムでは、glibc ライブラリーの getaddrinfo () 関数が初期化されていないデータにアクセスする可能性があるため、誤ったアドレス情報を返す可能性があります。この更新により、初期化されていないデータアクセスが阻止され、正しいアドレスが返されるようになります。(BZ#1324568)

glibc の malloc 実装で実行される追加のセキュリティチェック

以前は、glibc ライブラリーがアサーションなしでコンパイルされているため、malloc を実装する関数はヒープの整合性をチェックしませんでした。これにより、ヒープベースのバッファオーバーフローが悪用されるリスクが高まりました。ヒープの整合性チェックは、アサーションから明示的なチェックに変換されました。その結果、glibc での malloc 実装への呼び出しのセキュリティが強化されました。(BZ#1326739)

chrpath がバージョン 0.16 にリベース

chrpath パッケージがアップストリームバージョン 0.16 にアップグレードされ、以前のバージョンに比べて多くのバグ修正が提供されています。注目すべきは、chrpath ツールは、64 ビットシステムで 64 ビットバイナリーの実行パスプロパティと、32 ビットシステムの 32 ビットバイナリーのみを変更できることです。このバグが修正され、64 ビットシステムの chrpath が、64 ビットシステムの 32 ビットシステムのバイナリーと、32 ビットシステムのバイナリーの実行パスを変更できるようになりました。(BZ#1271380)

system-config-language パッケージの翻訳の更新

system-config-language の欠落している翻訳を解決するために、de、es、fr、it、ja、ko、pt_BR、ru、zh_CN、zh_TW の 10 言語が追加されました。(BZ#1304223)

ホスト名がドメイン部分がない場合に、Puci が不完全な From ヘッダーを持つ電子メールを送信しなくなりました。

以前は、ホスト名にドメイン名が含まれていない場合、Mutt 電子メールクライアントは、ホスト名がない From ヘッダーを含む電子メールを送信していました。結果として、そのような電子メールに返

信することは不可能でした。このバグは修正され、Mutt はドメイン部分を含まないホスト名を正しく処理するようになりました。(BZ#1388512)

strace は、open () 関数の O_TMPFILE フラグおよびモードを正しく表示します。

以前は、strace ユーティリティーは、システム関数 open () の O_TMPFILE フラグの存在と、モードオプションの存在の要件を認識していませんでした。そのため、strace 出力にはそれぞれのフラグの名前が表示されず、mode オプションの値がありませんでした。strace ユーティリティーは、この状況を認識するように拡張されました。その結果、O_TMPFILE フラグおよびモードが正しく表示されます。(BZ#1377847)

大規模なプログラムをリンクする際に ld が無限ループにならなくなる

IBM Power Systems アーキテクチャーの大規模なプログラムでは、.text セグメントは 2 つのスタブセクションで提供されます。以前は、セクションのいずれかを拡張する必要があるため、このようなセグメントのサイズを設定する際に、ld リンカーのサイジング終了条件が満たされませんでした。そのため、ld は無限ループに入り、終了する必要がありました。ld は、この状況を認識し、サイジングの終了条件を変更するように拡張されました。その結果、ld が正常に終了します。(BZ#1406498)

非表示シンボルへのクロスオブジェクト参照に関する ゴールド 警告メッセージの修正

共有ライブラリーをリンクすると、gold リンカーにより、1 つのライブラリーのコードが 2 番目のライブラリーまたはオブジェクトファイルで非表示のシンボルを参照する場合に警告メッセージが生成されます。以前は、別のライブラリーまたはオブジェクトファイルが同じシンボルの視認可能な定義を提供していても、gold はこの警告メッセージを生成していました。このバグを修正するために、gold はこの特定のケースの確認で拡張され、シンボルの表示される定義がない場合にのみ警告メッセージを生成します。その結果、gold は間違った警告メッセージを表示しなくなりました。(BZ#1326710)

Denverton SOC 搭載の Intel Xeon® C3xxx プロセッサでの OProfile デフォルトイベントの修正

以前は、Denverton SOC 搭載の Intel Xeon® C3xxx プロセッサの OProfile のデフォルトサイクルカウントイベントで誤った値が使用されていました。そのため、デフォルトイベントを使用した OProfile のサンプリングおよびカウントは機能していませんでした。関連する OProfile 設定が修正されました。その結果、デフォルトイベントは、Denverton SOC 搭載の Intel Xeon® C3xxx プロセッサで機能するようになりました。(BZ#1380809)

第26章 デスクトップ

Empathy が Google Talk の証明書チェーンを検証できるようになりました。

以前は、Empathy インスタントメッセージングクライアントは、チェーン内の Equifax Secure Certificate Authority などの無効なレガシー認証局を無視することで、Google Talk の証明書チェーンを検証できませんでした。そのため、チェーンに問題がなくても、Empathy は Google トークに接続する際に無効な証明書についてユーザーに尋ねました。今回の更新でバグが修正され、Empathy はサーバーが返すリスト内の無効なレガシー認証局を無視し、有効な可能性のある代替チェーンの構築を試みるようになりました。(BZ#1386616)

第27章 ファイルシステム

再試行タイムアウトを設定すると、SSSD からのマウントなしで `autofs` が起動しないようになりました。

`autofs` ユーティリティーを起動すると、`sss` マップソースがマップ情報を提供する準備ができていませんでしたが、`sss` は、マップが存在しない状態と利用できない状態を区別するための適切なエラーを返しませんでした。その結果、自動マウントが正しく機能せず、SSSD からのマウントなしで `autofs` が起動しました。このバグを修正するために、`map does not exist` エラーが発生すると、`autofs` は、設定可能な期間にわたって SSSD にマスターマップを要求することを再試行します。これで、再試行タイムアウトを適切な値に設定し、マスターマップが読み込まれ、`autofs` が期待どおりに開始するようになりました。(BZ#1101782)

`autofs` パッケージに `README.autofs-schema` ファイルと更新されたスキーマが含まれる

`samples/autofs.schema` ディストリビューションファイルが古く、正しくありませんでした。結果として、誰かが誤った LDAP スキーマを使用している可能性があります。ただし、使用中のスキーマの変更は強制できません。今回の更新により、以下が可能になります。

- 問題を記述し、可能な場合はどのスキーマを使用するかを推奨するために、`README.autofs-schema` ファイルが追加されました。
- `autofs` パッケージに含まれるスキーマが `samples/autofs.schema.new` に更新されました。(BZ#1383910)

NIS サーバーに保存されているマップにアクセスするために `automount` を再起動する必要がなくなりました。

以前は、`autofs` ユーティリティーは、起動時に NIS クライアントサービスを待ちませんでした。そのため、プログラムの起動時にネットワークマップソースが利用できなかった場合、マスターマップを読み取ることができませんでした。また、NIS サーバーに保存されているマップにアクセスするには、自動マウントサービスを再起動する必要がありました。今回の更新で、`autofs` は、マスターマップが利用可能になり、起動マップを取得するまで待機します。その結果、`automount` は NIS ドメインからマップにアクセスできるようになり、起動ごとに `autofs` を再起動する必要がなくなりました。

設定された待機時間後も NIS マップが利用できない場合は、`autofs` 設定の `master_wait` オプションを増やす必要がある場合があります。ほとんどの場合、パッケージで使用される待機時間は十分です。(BZ#1383194)

`autofs` でローカルマウントの可用性をチェックすると、失敗する前に長いタイムアウトが発生しなくなりました。

以前は、ローカルマシンのバインドマウントが利用可能であることが予想されるため、`autofs` がローカルと見なされるマウント要求に対してサーバー可用性プローブは実行されませんでした。バインドマウントが失敗した場合は、ローカルマシンへの NFS マウントが試行されました。ただし、NFS

サーバーがローカルマシンで実行していないと、マウントの試行に失敗する前にタイムアウトが長くなる場合があります。

バインドマウントが最初に試行されたにも関わらず失敗するケースに可用性プローブが追加され、`autofs` はローカルマシンで NFS サーバーを使用しようとするようにフォールバックするようになりました。その結果、ローカルマシンのバインドマウントに失敗すると、ローカルの NFS サーバーが実行していない場合に、ローカルマシンで NFS マウントを試行するフォールバックがすぐに失敗します。(BZ#1420574)

GFS2 ファイルシステムを読み取り専用としてマウントすると、ジャーナルはアイドルとマークされる

GFS2 ファイルシステムを読み取り専用としてマウントする場合、カーネルはファイルシステムジャーナルをアイドルとマークしませんでした。その結果、`gfs2_log_flush ()` 関数が誤ってヘッダーブロックをジャーナルに書き込もうとし、シーケンス順不同のエラーがログに記録されました。GFS2 ファイルシステムを読み取り専用としてマウントするときに、ジャーナルをアイドル状態とマークするパッチが適用されました。その結果、上記のエラーは上記のシナリオでは発生しなくなりました。(BZ#1213119)

`id` コマンドで誤った UID および GID が表示されなくなる

NFSv4 サーバーに接続されている NFSv4 クライアントで Red Hat Enterprise Linux を実行すると、NFS `id mapper` キーリングからキーが期限切れになった後、`id` コマンドで誤った UID および GID が表示されました。この問題は、期限切れの鍵がガベージコレクションされるまで 5 分間持続します。その後、新しいキーがキーリングに作成され、`id` コマンドで正しい出力が提供されました。今回の更新で、キーリング機能が修正され、上記の状況で `id` コマンドが誤った出力を表示しなくなりました。(BZ#1408330)

ラベル付けされた NFS がデフォルトでオフになる

Red Hat Enterprise Linux NFS サーバー上の SELinux ラベルは、通常、NFS クライアントには表示されません。代わりに、NFS クライアントは、サーバー上のファイルのラベルに関係なく、タイプ `nfs_t` としてラベル付けされたすべてのファイルを認識します。

Red Hat Enterprise Linux 7.3 以降、NFS サーバーは、各ファイルラベルをクライアントと通信できるようになりました。最近の Fedora クライアントなど、最近のクライアントは、それらのファイルがサーバー上に持っているものと同じラベルでラベル付けされた NFS ファイルを参照します。これは特定のケースで役立ちますが、サーバーを Red Hat Enterprise Linux 7.3 以降にアップグレードした後に、最近のクライアントで予期せぬアクセスパーミッションの問題が発生する可能性があります。

ラベル付き NFS サポートは、NFS サーバーではデフォルトでオフになっていることに注意してください。`security_label` エクスポートオプションを使用して、ラベル付き NFS サポートを再度有効にできます。(BZ#1406885)

`autofs` マウントがシャットダウン状態に達した後に無限ループにならなくなる

autofs マウントがシャットダウン状態に達し、マウント処理スレッドがシャットダウン通知を読み取る前にマウント要求が到着して処理された場合、マウント処理スレッドは以前は **autofs** マウントをクリーンアップせずに終了していました。その結果、**autofs-managed** マウントがマウントされたままになると、メインプログラムは終了条件に到達せず、無限ループに入りました。このバグを修正するために、リクエストを処理するたびに終了条件の確認が行われるようになり、**autofs** マウントがシャットダウン状態に達した場合にクリーンアップ操作が実行されるようになりました。その結果、**autofs** デーモンは、シャットダウン時に想定どおりに終了するようになりました。(BZ#1420584)

名前空間の処理時に **autofs** の信頼性が向上しました。

以前は、**autofs** カーネルモジュールは、パスの最後のコンポーネントが現在の名前空間のマウントポイントであるかどうかを確認できず、どの名前空間でもマウントポイントであるかどうかしか確認できませんでした。このバグにより、**autofs** は、伝播プライベート名前空間にクローンされたマウントポイントがすでに存在しているかどうかを誤って判断することがありました。

その結果、自動マウントポイントのマウントに失敗し、エラーメッセージ **Too many levels of symbolic links** が返されました。これは、たとえば、**autofs** マウントがアクティブなときに **PrivateTmp** オプションを使用する **systemd** サービスが再起動した場合などに発生しました。

今回の更新で、名前空間を認識したマウントチェックがカーネルに追加されました。その結果、**autofs** は、**autofs** マウントを含むマウント名前空間が伝播プライベート名前空間にクローンされている場合に、より回復力があります。

詳細は、KBase の記事 <https://access.redhat.com/articles/3104671> を参照してください。(BZ#1320588)

第28章 インストールおよび起動

IBM z Series の 1 つの FBA DASD にインストールする場合に、自動パーティション設定が機能する

以前は、cms ディスクレイアウトをターゲットとする単一の Fixed Block Architecture (FBA) Direct Access Storage Device (DASD)を持つ IBM z Series システムに Red Hat Enterprise Linux 7 をインストールすると、cms 形式の FBA DASD ではサポートされていないデバイス上に複数のパーティションを作成しようとするため、自動パーティション設定に失敗していました。これが原因でディスクが破損し、インストールが終了しました。

今回の更新で、インストーラーはまず、ターゲットの DASD に msdos パーティションテーブルを作成します。これにより、デバイスで最大 3 つのパーティションが許可されます。インストーラーが作成するパーティションの数が 3 つ以下であれば、インストールは成功します。autopart --nohome キックスタートオプションを使用して、インストーラーが別の /home パーティションを作成しないようにすることが推奨されます。(BZ#1214407)

キックスタートがディスクから起動したときに、キックスタートで設定したブリッジのアクティベーションが失敗しなくなる

以前は、ブリッジデバイスがキックスタートファイルで設定されており、キックスタートファイルがディスクからフェッチされている場合、ネットワーク接続がないためにブリッジが作成されず、インストールが初期段階で失敗していました。今回の更新で、ブリッジキックスタート設定が初期段階で dracut ツールに渡されます。その結果、インストールの初期段階でネットワークが不要な場合でも、dracut はブリッジデバイスを作成およびアクティベートできます。(BZ#1373360)

Anaconda がパスワードなしでユーザーを正しく作成可能に

以前は、対話型インストール中に Create User 画面で、Require a password to use this account オプションの選択を解除することができませんでした。これにより、インストール時に作成されたすべてのユーザーアカウントにパスワードが必要になりました。このバグが修正され、パスワードを使用しないユーザーの作成が可能になりました。(BZ#1380277)

最小インストールで open-vm-tools-desktop と依存関係がインストールされなくなる

open-vm-tools-desktop パッケージは、以前は @platform-vmware パッケージグループ (VMware 用の仮想化ユーティリティーおよびドライバー) でデフォルトのマークが付けられていました。このグループは、インストールが VMWare ハイパーバイザーを使用していることを検出すると、Anaconda により自動的にインストールされます。同時に、このパッケージには、最小インストールでは役に立たない多数の X ライブラリーなど、多くの依存関係があり、Anaconda は多くの不要なパッケージをインストールしていました。

open-vm-tools-desktop パッケージは、@platform-vmware グループでオプションになったため、デフォルトではインストールされなくなりました。グループ内の別のパッケージである open-vm-tools は必須のままであるため、デフォルトでインストールされます。(BZ#1408694)

Anaconda が無効なキックスタートファイルを生成しなくなる

以前は、インストール中にキックスタートファイルを使用して、一部の LVM 論理ボリュームを絶対的に定義(`--size=` パラメーター)、その他が相対的に(`--percent=` パラメーター)場合、インストール済みシステムに保存されているキックスタートファイルである `anaconda-ks.cfg` は、これらのパラメーターを使用してすべての論理ボリュームを定義していました。これらのパラメーターは相互に排他的であるため、生成されたキックスタートファイルは無効でした。今回の更新で、Anaconda が相対サイズおよび絶対サイズの使用を正しく処理し、インストール後のキックスタートファイルが有効になります。(BZ#1317370)

Anaconda は名前で指定された RAID アレイの識別に失敗しなくなりました

以前は、キックスタートファイルの `ignoredisk` コマンドまたは `clearpart` コマンドで RAID アレイが名前指定されていると、インストールの初期段階で RAID 名が利用できないため、インストールを続行できませんでした。今回の更新で、Anaconda が `/dev/md/` 内のデバイスに一致する名前もチェックするようにすることで、RAID サポートが改善されました。たとえば、キックスタートファイルにコマンド `ignoredisk --only-use=myraid` が含まれている場合、Anaconda は `/dev/md/myraid` にあるアレイの検索も試行するようになりました。これにより、インストーラーはインストール中の任意の時点で名前指定された RAID アレイを見つけることができ、キックスタートファイルで RAID アレイ名のみを指定できるようになります。(BZ#1327439)

キックスタートでは、短すぎるパスワードが使用できなくなりました。

以前は、キックスタートファイルを使用して Red Hat Enterprise Linux 7 をインストールすると、パスワードが十分に強力な場合(デフォルトでは品質値 50 以上)、Anaconda インストーラーは `--minlen` キックスタートオプションで定義された最小長よりも短いパスワードをすぐに受け付けていました。このバグは修正され、`--minlen` オプションが強力なパスワードでも機能するようになりました。(BZ#1356975)

初期セットアップが IBM z Systems の SSH 経由のグラフィカルインターフェイスで正しく開くようになる

以前は、SSH を使用して IBM z Systems マシンに接続すると、X 転送が有効になっている場合でも、Initial Setup インターフェイスのテキストバージョンが開かれていました。このバグは修正され、X 転送の使用時に、グラフィカルバージョンの Initial Setup が正しく開くようになりました。(BZ#1378082)

位置情報サービスが有効になると、インストールに追加の時間が必要なくなりました。

インターネットアクセスが制限されているか、またはインターネットアクセスのない Red Hat Enterprise Linux 7.3 をインストールすると、インストーラーはインストールの概要画面で数分間一時停止し、セキュリティーポリシーセクションは `Not ready` となっています。これは、位置情報サービスがシステムの場所を判断できないために発生しました。そのため、サービスがタイムアウトになる前にインストールを続行できませんでした。今回の更新で、位置情報サービスが 3 秒以内に場所を見つけられない場合にタイムアウトになり、ネットワーク接続が限られていたり、まったくない場合でも、インストールをすぐに続行できるようになりました。(BZ#1380224)

新しい IP アドレスの追加時に、`ifup-aliases` スクリプトが Gratuitous ARP 更新を送信するようになりました。

サーバー間で1つ以上のIPエイリアスを移動する場合は、アップストリームルーターで設定されているAddress Resolution Protocol (ARP) のタイムアウト値により、関連するIPアドレスがしばらく到達不能になることがあります。このバグは `initscripts` パッケージで対処され、`ifup-aliases` は、この状況でネットワーク上の他のシステムを大幅に高速に更新するようになりました。(BZ#1367554)

`netconsole` ユーティリティーが正しく起動するようになりました。

以前は、`nameserver` アドレスの行が `/etc/resolv.conf` ファイルに存在しない場合は、`netconsole` の起動時にエラーが発生し、`netconsole` が起動しませんでした。`initscripts` パッケージが更新され、この状況では `netconsole` が正しく起動するようになりました。(BZ#1278521)

`rc.debug` カーネルを使用すると、`initscripts` のデバッグが容易になります。

今回の機能拡張により、カーネルコマンドラインの `rc.debug` オプションが導入されました。起動前に `rc.debug` オプションをカーネルコマンドラインに追加すると、ブートおよび終了プロセス中に `initscripts` ファイルのすべてのアクティビティーのログが生成されます。ログは、`/var/log/dmesg` ログファイルの一部として表示されます。その結果、必要に応じて `rc.debug` オプションをカーネルコマンドラインに追加すると、`initscripts` のデバッグが容易になります。(BZ#1394191)

iSCSI または NFS でシステムが `/usr` で終了しなくなる

以前のバージョンの Red Hat Enterprise Linux 7 では、`/usr` フォルダーがネットワーク経由でマウントされている場合 (NFS や iSCSI など)、システムの終了に失敗し、システムがハングしたままになることがありました。この問題は解決し、システムは通常の方法でシャットダウンするようになりました。(BZ#1369790, BZ#1446171)

`rhel-autorelabel` がファイルシステムを破損しなくなりました。

以前のバージョンの Red Hat Enterprise Linux 7 では、`/.autorelabel` ファイルを作成して SELinux の自動再ラベル付けを強制すると、ファイルシステムが部分的に破損することがありました。これにより、システムが起動できなくなりました。この動作を防ぐためにパッチが適用されています。その結果、`touch /.autorelabel` コマンドを使用して自動再ラベル操作を適用すると、ファイルシステムが破損することはなくなりました。(BZ#1385272)

`rpmbuild` コマンドが Perl が必要とするものを正しく処理するようになりました。

以前は、`rpmbuild` コマンドを使用してパッケージを構築する際に、`rpm` のバグにより、`my variable = <<` ブロックが文字列定数ではなくコードとして扱われていました。これにより、変数に `use` という単語とそれに続く別の単語が含まれる場合、`rpm` はビルド中のパッケージに意図しない依存関係を追加していました。今回の更新で、`rpm` は依存関係の検索時にこのブロックを正しくスキップし、パッケージに意図しない依存関係が含まれなくなりました。(BZ#1378307)

キックスタートで `ignoredisk` を使用する場合に、インストーラーが BIOS RAID デバイスを正しく認識するようになりました。

以前は、`ignoredisk --onlyuse=<bios raid name>` コマンドでキックスタートファイルを使用すると、インストール時に一部の BIOS RAID デバイスが正しく認識されませんでした。これにより、インストールに失敗し、デバイスを使用できないために空き領域が不足していると報告されました。今回の

更新で、**Anaconda** がキックスタートファイルで指定された **BIOS RAID** デバイスを確実に認識させ、このような状況でインストールが失敗しなくなりました。(BZ#1327463)

ifcfg-* ファイル内の値に対して一重引用符が機能するようになる

以前は、**ifcfg-*** ファイルで二重引用符を使用するだけで値を指定できました。一重引用符の使用は機能していませんでした。今回の更新で、一重引用符も機能するようになりました。以下に例を示します。

```
ONBOOT='yes'
```

(BZ#1428574)

rhel-import-state が **/dev/shm/** のアクセス権限を変更しなくなり、システムが正常に起動できるようになりました。

以前は、**dracut** 更新に新しいスクリプトの導入により、起動プロセス中に問題が発生していました。新しいスクリプトは、**dracut** ユーティリティーがディレクトリーを **/run/initramfs/state/** に配置したときに、**/dev/shm/** ディレクトリーへのアクセスパーミッションを変更しました。今回の更新により、**rhel-import-state** は **/dev/shm/** のアクセス権限を変更しなくなり、システムが正常に起動します。(BZ#1406254)

Red Hat Enterprise Linux 6 **initscripts** で後方互換性を有効化

Red Hat Enterprise Linux 7 の **initscripts** ファイルにはパッチが当てられ、後方互換性を有効化し、Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 7 へのアップグレード時に発生する可能性のあるリグレッションを防ぐことができます。(BZ#1392766)

initscripts が設定ファイルとして **/etc/rwtab** および **/etc/statetab** を指定するようになりました。

以前は、**initscripts** パッケージを再インストールすると、**/etc/rwtab** ファイルおよび **/etc/statetab** ファイルが置き換えられていました。このファイルにユーザーの設定が含まれていた場合、再インストールプロセスにより上書きされていました。

initscripts パッケージが更新され、設定ファイルとして **/etc/rwtab** および **/etc/statetab** ファイルが指定されるようになりました。これらのファイルがユーザーが変更した場合、再インストールを実行すると、**/etc/** フォルダに新しい設定が含まれる ***.rpmnew** ファイルが作成されるようになりました。今回の更新で、**initscripts** パッケージを再インストールすると、**/etc/rwtab** ファイルおよび **/etc/statetab** ファイルがそのまま残ります。(BZ#1434075)

ifup スクリプトが **NetworkManager** の速度を低下させなくなりました。

以前は、**NetworkManager** に通知する際に **ifup** スクリプトが非常に遅くなっていました。これは、**Red Hat Virtualization (RHV)** ネットワークの起動時間に特に影響を及ぼしていました。**initscripts** にパッチが適用され、上記の問題は発生しなくなりました。(BZ#1408219)

GNOME の初期設定は、キックスタートの `firstboot --disable` コマンドで無効にできるようになりました。

今回の更新で、`gnome-initial-setup` パッケージが `firstboot --disable` キックスタートコマンドに対応するように修正されました。その結果、キックスタートのインストール中に Gnome の初期セットアップを堅牢にオフにすることができ、インストールキックスタートに `firstboot --disable` コマンドが含まれている限り、ユーザーは上記の状況で最初の起動時にユーザーアカウントを作成する必要がなくなりました。(BZ#1226819)

NM_CONTROLLED の設定がすべての `ifcfg-*` ファイルで正しく機能するようになりました。

`ifcfg-*` ファイルのインターフェイスに `NM_CONTROLLED=no` パラメーターが設定されている場合、他のインターフェイスがこの設定を継承する場合があります。この動作により、NetworkManager デーモンがこれらのインターフェイスを制御できなくなりました。この問題は解決され、`NM_CONTROLLED` パラメーターの設定はすべての `ifcfg-*` ファイルで適切に機能するようになりました。その結果、ユーザーは NetworkManager で制御されるインターフェイスと、そうでないインターフェイスを選択できます。(BZ#1374837)

`hostname` が設定されていない場合、`dhclient` コマンドが誤って `localhost` を使用しなくなりました。

`dhclient` コマンドは、`hostname` 変数が設定されていない場合に、ホスト名として DHCP サーバーに `localhost` を誤って送信しました。これは修正され、`dhclient` はこのような状況で間違ったホスト名を送信しなくなりました。(BZ#1398686)

`initscripts` ユーティリティーが LVM2 を正しく処理するようになりました。

以前は、`initscripts` ユーティリティーの新しいバージョンでは、システムの起動時に `vgchange` コマンドに新しい `--ignoresthecluster` オプションを使用していました。このオプションは、以前のバージョンの `lvm2` ユーティリティーではありませんでした。その結果、以前のバージョンの Logical Volume Manager デバイスマッパー (LVM2) を使用するシステムが正しく起動しなくなる可能性があります。今回の更新で、`initscripts` RPM が必要な `lvm2` のバージョンを示し、十分なバージョンがインストールされている場合は、LVM2 を使用するシステムが正しく起動します。(BZ#1398683)

`service network stop` コマンドは、すでに停止されているサービスを停止しようとしなくなりました。

以前は、トンネルインターフェイスが存在する場合、`service network stop` コマンドは、すでに停止されているサービスを誤って停止しようとし、エラーメッセージが表示されていました。このバグは修正され、`service network stop` コマンドは実行中のサービスのみを停止するようになりました。(BZ#1398679)

ループバックデバイスの `ifdown` が正常に動作するようになりました。

以前のバージョンの Red Hat Enterprise Linux 7 では、ローカルループバックデバイスで `ifdown` コマンドを実行すると、デバイスを削除できませんでした。パッチが適用され、`ifdown` を使用した既存のループバックデバイスの削除が成功するようになりました。(BZ#1398678)

`initscripts` のスクリプトは、静的 IPv6 アドレスの割り当てをより強固に処理

以前は、システムの初期化中にルーター通知 (RA) を受信した場合、`initscripts` パッケージ内のスクリプトが静的 IPv6 アドレスを正しく割り当てることに失敗していました。このバグは修正され、静的に割り当てられたアドレスが、上述の状況で正しく適用されるようになりました。(BZ#1398671)

Software Selection でアドオン オプションの選択を解除すると、ダブルクリックが必要なくなる

Red Hat Enterprise Linux 7.3 をインストールする場合は、**Base environment** の変更後にアドオン チェックボックスの選択を解除するためにダブルクリックする必要がありました。グラフィカルインストールの **Software Selection** ダイアログでバグが発生しました。今回の更新で、**Base environment** の変更後にオプションの選択を解除する際に、ダブルクリックする必要がなくなりました。クリック 1 回で十分です。(BZ#1404158)

ターゲットシステムのホスト名は、キックスタートインストールでインストーラーの起動オプションを使用して設定可能に

Red Hat Enterprise Linux 7.3 では、キックスタートインストール時に **Anaconda** インストーラーの起動オプションで指定されたホスト名が、インストール済みシステムに誤って設定されず、代わりにデフォルトの `localhost.localdomain` ホスト名値が使用されていました。今回の更新で、**Anaconda** が、起動オプションで設定したホスト名をターゲットシステム設定に適用するように修正されました。これにより、キックスタートインストールでも、インストーラーの起動オプションを使用して、ターゲットシステムのホスト名を設定できるようになりました。(BZ#1441337)

Anaconda は、ネットワーク設定後にインストールソースの検証を要求しなくなる

以前は、リポジトリからの **Anaconda** のインストール時に、リポジトリパッケージがすでに選択された後にユーザーがネットワーク設定を変更した場合に、インストールソースで検証が必要でした。この要求は、ネットワークの変更後にリポジトリに到達できた場合でも行われたため、不要な手順が発生していました。この更新により、**Anaconda** インストーラーは元のソースリポジトリを保持し、ネットワークとホスト名の設定後も到達可能かどうかを確認します。その結果、ユーザーは、元のリポジトリに到達できない場合にのみ、インストールソースを再設定する必要があります。(BZ#1358778)

自動インストールで、**OEMDRV** ラベルを使用するディスクが正常に無視されるようになる

OEMDRV ディスクラベルは、インストール時にドライバー更新ディスクで使用されます。バグにより、このラベルが付いたディスクが、自動インストール時にインストールターゲットとして **Anaconda** により使用されていました。これは、このディスクが消去され、インストール済みシステムストレージの一部として使用されることを意味していました。この更新により、**Anaconda** は、インストールターゲットとして明示的に選択されていない限り、このラベルが付いたディスクを無視し、問題は発生しなくなりました。(BZ#1412022)

第29章 カーネル

RAID 4 および RAID 10 の作成とアクティブ化を完全にサポート

Red Hat Enterprise Linux 7.3 では、以前のリリースで作成した既存の RAID 4 または RAID 10 論理ボリュームがアクティブになりませんでした。また、Red Hat Enterprise Linux 7.3 で作成した RAID 4 論理ボリュームは、その後のリリースおよび更新ではアクティベートできない場合があるため、作成しないように指示されていました。今回の更新で、Red Hat Enterprise Linux 7.4 が RAID 4 および RAID 10 の作成とアクティブ化を完全にサポートし、Red Hat Enterprise Linux 7.3 で作成された可能性のある無効な RAID 4 および RAID 10 のレイアウトを拒否するようになりました。(BZ#1385149)

kdump がレガシタイプ 12 NVDIMM で動作するようになる

以前は、レガシタイプ 12 の Non-Volatile Dual In-line Memory Modules (NVDIMMs) (実際のデュアルインラインメモリーモジュール(DIMM)、または memmap=XG!YG カーネルコマンドラインパラメーターを使用してエミュレート) のシステムは、カーネルクラッシュダンプを正常にキャプチャーできませんでした。実際の NVDIMM を使用するシステムでは、カーネルクラッシュダンプをキャプチャーしようとするデータが破損する場合があります。今回の更新で、基盤となるソースコードが修正され、レガシタイプ 12 NVDIMM を使用するシステムが、想定どおりにカーネルクラッシュダンプをキャプチャーできるようになりました。(BZ#1351098)

ACL を継承するファイルの作成でマスクが失われなくなる

以前は、アクセス制御リスト (ACL) を継承するファイルを作成すると、ローカルファイルシステムとは異なり、マスクが失われていました。今回の更新で、ファイルの作成時に NFSv4.2 を使用するクライアントが umask 属性を設定して、親ディレクトリーからパーミッションを継承する場合を除き、サーバーが umask を常に適用できるようになりました。その結果、新しい NFS ファイルには、ローカルで作成されたファイルと同じ権限が付与されます。この更新は、NFS クライアントと NFS サーバーの両方に適用し、-overs=4.2 パラメーターでマウントする必要があります。(BZ#1217546)

第30章 REAL-TIME KERNEL

USB を削除しても、MRG Realtime カーネルで `may_sleep ()` 警告が発生しなくなりました。

MRG Realtime カーネルで USB デバイスを削除すると、以前はスリープ状態のスピンロックが発生し、割り込みは無効になっていました。その結果、システムは `might_sleep ()` 警告をログに記録しました。今回の更新で、`local_irq_disable` および `local_irq_enable` 呼び出しが `local_irq_disable_nort` および `local_irq_enable_nort` に置き換えられ、このバグが修正されています。(BZ#1443711)

第31章 ネットワーク

SNMP 応答がタイムアウトしなくなる

以前は、SNMPv3 メッセージに続くすべての Simple Network Management Protocol バージョン 1 (SNMPv1) および SNMPv2c 応答が、最後に記録された SNMPv3 max message size プロパティに対してチェックされていました。これにより、最大メッセージサイズが小さい SNMPv3 要求により、SNMPv1 および SNMPv2c の一括要求がタイムアウトになる可能性があります。今回の更新で、SNMPv3 要求でのみセッションの最大メッセージサイズが確認され、SNMPv1 および SNMPv2c の応答のタイムアウトがなくなりました。(BZ#1324306)

ICMP リダイレクトでカーネルがクラッシュしなくなる

以前は、ソケットがユーザー空間と Internet Control Message Protocol (ICMP) リダイレクトパケットのプロセスとの間でロックされず、競合状態が発生していました。その結果、カーネルが予期せず終了しました。このバグは、ソケットがユーザー空間でロックされているときに ICMP リダイレクトパケットのプロセスをスキップすることで修正され、上述の問題は発生しなくなりました。(BZ#1387485)

`net.ipv4.ip_nonlocal_bind` カーネルパラメーターは名前空間で設定されます。

以前は、ネットワーク名前空間内でフローティング IP アドレスを使用すると、次のエラーメッセージが表示されて失敗する場合があります。

```
bind: Cannot assign requested address.
```

今回の更新で、カーネルは名前空間での `net.ipv4.ip_nonlocal_bind` パラメーターの設定を 1 に尊重し、フローティング IP アドレスが期待どおりに割り当てられるようになりました。(BZ#1363661)

netfilter REJECT ルールが SCTP パケットで動作するようになりました。

以前は、`contrack` ツールは Stream Control Transmission Protocol (SCTP) パケットの CRC32c 値を確認しませんでした。そのため、netfilter REJECT ルールは SCTP パケットで期待どおりに適用されませんでした。このバグは、有効な CRC32c を持つ SCTP パケットに `CHECKSUM_UNNECESSARY` を設定して修正されています。その結果、netfilter REJECT は Internet Control Message Protocol (ICMP) 応答を生成できます。(BZ#1353218)

NetworkManager が設定済みの `DHCP_HOSTNAME` との接続を複製しなくなりました。

以前は、NetworkManager サービスの再起動後に、設定済みの `DHCP_HOSTNAME` プロパティとの接続が重複していました。したがって、DHCP リースの有効期限が切れたときに、常に更新されるとは限りませんでした。この更新により、接続が複製されなくなり、このシナリオで DHCP リースが正しく更新されます。

この修正では、一致するプロセスで設定済みのホスト名プロパティが無視されることに注意してください。発生する可能性のある問題を回避するには、誤った `ipv4.dhcp-hostname` で未使用の接続をす

べて削除します。詳細は、<https://access.redhat.com/articles/2948041> を参照してください。
(BZ#1393997)

改善された SCTP congestion_window 管理

以前のバージョンでは、小さなデータチャンクにより、ゼロウィンドウからのリカバリー時に Stream Control Transmission Protocol (SCTP)の値が receiver_window (rwnd)の値を誤って考慮していました。そのため、ウィンドウの更新はピアに送信されず、rwnd が人為的に増加するとパケットドロップが発生する可能性があります。今回の更新で、このような小さなデータチャンクが適切に考慮され、ウィンドウを再度開くときに rwnd pressure 値は無視されます。その結果、ウィンドウの更新が送信されるようになり、アナウンスされた rwnd は、受信バッファの実際の状態をより適切に反映するようになりました。(BZ#1084802)

DCTCP alpha の値は 0 にドロップし、cwnd は 137 を超える値に残ります。

以前は、データセンター TCP (DCTCP)の alpha 値は減算前にシフトしていたため、精度が低下していました。その結果、実際の alpha 値は 15 未満ではなく、最終的には congestion_window (cwnd)値にドロップされました。このバグは、alpha が少ない場合にシフト操作をキャンセルすることで修正されました。その結果、alpha は 0 にドロップし、cwnd は明らかなフローの 137 を超える値に残ります。(BZ#1370638)

ss が cwnd を正しく表示

以前は、ss ユーティリティーは、カーネルからの Transmission Control Protocol congestion window (TCP cwnd)値を表示し、未署名から署名済みの 32 ビット整数にキャストを実行していました。結果として、一部の値はオーバーフローし、負の値として解釈される可能性があります。今回の更新で、ss コードが修正され、ユーティリティーに負の cwnd 値が表示されなくなりました。(BZ#1375215)

cwnd の値が DCTCP を使用して増加しなくなりました。

以前は、パケットロス後に congestion_window (cwnd)が予想外に増加していました。その結果、データセンターの TCP (DCTCP) 輻輳制御モジュールは、同じフローで繰り返し問題が発生したため、輻輳の回避には効果がなくなりました。今回の更新で、cwnd 値は損失時に保存され、古い値はリカバリーで復元されます。その結果、cwnd は安定した状態を維持します。(BZ#1386923)

負の範囲の一致が修正されました。

以前では、否定一致の値の範囲を使用しても、true と評価されることはありませんでした。今回の更新で、このような一致が期待どおりに機能するようになりました。以下に例を示します。

```
# nft add rule ip ip_table filter_chain_input ip length != 100-200 drop
```

100 バイトよりも小さいパケット、または 200 バイトより大きいパケットを正しく破棄するようになりました。(BZ#1418967)

nmcli connection show コマンドが、empty と NULL の両方の値に正しい出力を表示するようになり

ました。

以前は、`nmcli connection show` コマンドの出力は、異なるプロパティ間で `empty` および `NULL` の値を一貫して表示しませんでした。その結果、空の値は `--` または値なしで表示されました。今回の更新で、`nmcli connection show` コマンドの出力に、`normal` モードまたは `pretty` モードの空の値と `NULL` 値の両方に `--` が表示されます。

`terse` モードでは、値は `raw` 形式でのみ出力され、`empty` および `NULL` 値はまったく出力されないことに注意してください。(BZ#1391170)

`snmpd` が `AgentX` サブエージェントからの大きなパケットを拒否しなくなりました。

以前では、`SNMP` デーモン (`snmpd`) により、`AgentX` サブエージェントから送信されるパケットのサイズが 1472 バイトに制限されていました。これにより、`snmpd` が `AgentX` サブエージェントからの大きなパケットを拒否していました。パケットサイズの制限が 65535 バイトに引き上げられました。その結果、`snmpd` は `AgentX` サブエージェントからの大きなパケットを拒否しなくなりました。(BZ#1286693)

`macvlan` を正しく登録解除できるようになりました。

以前は、`Macvlan` ドライバーの登録を解除しようとする、別の名前空間のデバイスとの間の `sysfs` リンクが破損して失敗していました。今回の更新で、`Macvlan` が修正され、このバグが修正されました。(BZ#1412898)

第32章 セキュリティー

ユーザーが検索できないパスでの `chrooting` に依存する設定が適切に機能するようになる

Red Hat Enterprise Linux 7.3 では、OpenSSH ツールの `chroot` プロセスが変更され、SELinux システムポリシーが強化され、`chroot` を実行する前に `root` UID が削除されていました。その結果、ユーザーが検索できないパスでの `chrooting` に依存する既存の設定が動作を停止しました。この `openssh` パッケージの更新により、変更は元に戻されました。さらに、管理者が `selinuxuser_use_ssh_chroot` ブール値を有効にしている場合に、制限されたユーザーが OpenSSH `chroot` を使用できるようにすることで、SELinux システムポリシーでこの問題が修正されています。上述の設定は、Red Hat Enterprise Linux 7.2 と同じように機能するようになりました。(BZ#1418062)

`firewalld` がすべての ICMP タイプに対応

以前は、Internet Control Message Protocol (ICMP) タイプの一覧が完了していませんでした。そのため、`packet-too-big` などの一部の ICMP タイプはブロックまたは許可できませんでした。今回の更新で、追加の ICMP タイプへの対応が追加され、`firewalld` サービスデーモンですべての ICMP タイプを処理できるようになりました。(BZ#1401978)

`selinux-policy` で `docker.pp` が `container.pp` に置き換えられる

今回の更新以前は、`container-selinux` パッケージの `container.te` ファイルには、同等のコンテナインターフェイスを参照する Docker インターフェイスと `docker.if` ファイルが含まれていました。そのため、`container.te` ファイルをコンパイルする際に、コンパイラーは重複するインターフェイスについて警告していました。今回の更新で、`selinux-policy` パッケージの `docker.pp` ファイルが `container.pp` ファイルに置き換えられ、上記のシナリオで警告が発生しなくなりました。(BZ#1386916)

最近追加されたカーネルクラスとパーミッションは、`selinux-policy` で定義されています。

以前では、いくつかの新しいクラスとパーミッションがカーネルに追加されていました。その結果、システムポリシーで定義されていないクラスとパーミッションにより、SELinux の拒否や警告が発生しました。今回の更新で、最近追加したすべてのカーネルクラスとパーミッションが `selinux-policy` パッケージで定義され、拒否と警告が発生しなくなりました。(BZ#1368057)

`nss` が PKCS#12 ファイルを適切に処理

以前は、`pk12util` ツールを使用して PKCS#5 v2.0 形式を使用して強力な暗号を持つ PKCS#12 ファイルの証明書を一覧表示すると、出力はありませんでした。さらに、`pk12util` を使用して PKCS#12 ファイルの証明書を SHA-2 メッセージ認証コード (MAC) で一覧表示すると、MAC エラーが報告されましたが、証明書は出力されませんでした。今回の更新で、PKCS#12 ファイルのインポートおよびエクスポートが OpenSSL 処理と互換性を持つように変更され、PKCS#12 ファイルが上記のシナリオで適切に処理されるようになりました。(BZ#1220573)

OpenSCAP が有用なメッセージおよび警告のみを生成するようになりました。

以前では、デフォルトのスキャン出力設定が変更され、デバッグメッセージも標準出力に出力されていました。その結果、OpenSCAP 出力はエラーおよび警告に完全でした。この出力は読みにく

く、SCAP Workbench もこれらのメッセージを処理できませんでした。今回の更新で、デフォルトの出力設定の変更が元に戻され、OpenSCAP が有用な出力を生成するようになりました。(BZ#1447341)

AIDE が syslog 形式でログを記録するようになりました。

今回の更新で、syslog_format オプションを指定した AIDE 検出システムは、rsyslog互換形式でログに記録されます。マルチラインログにより、リモート rsyslog サーバーでの解析中に問題が発生します。新しい syslog_format オプションを使用すると、AIDE は 1 行でログに記録されるすべての変更でログに記録できるようになりました。(BZ#1377215)

OpenSCAP セキュリティー強化プロファイルを使用したインストールが続行される

今回の更新以前は、scap-security-guide パッケージのタイプミスにより、Anaconda インストールプログラムが終了し、マシンを再起動していました。そのため、Red Hat Enterprise Linux 7.4 のインストールプロセスで、Criminal Justice Information Services (CJIS) などのセキュリティ強化プロファイルを選択することができませんでした。タイプミスが修正され、OpenSCAP セキュリティー強化プロファイルを使用したインストールが続行されるようになりました。(BZ#1450731)

OpenSCAP および SSG が、RHV-H システムを正しくスキャンできるようになりました。

以前は、OpenSCAP および SCAP Security Guide (SSG) ツールを使用して、Red Hat Virtualization Host (RHV-H) として機能する Red Hat Enterprise Linux システムをスキャンすると、Not Applicable 結果が返されていました。この更新により、OpenSCAP と SSG は RHV-H を Red Hat Enterprise Linux として正しく識別します。これにより、OpenSCAP と SSG は RHV-H システムを適切にスキャンできます。(BZ#1420038)

OpenSCAP が、CVE OVAL フィードで非圧縮 XML ファイルも処理するようになりました。

以前は、OpenSCAP ツールは、フィードからの圧縮された CVE OVAL ファイルのみを処理できませんでした。その結果、RedHat が提供する CVE OVAL フィードを脆弱性スキャンのベースとして使用することはできません。今回の更新で、OpenSCAP は ZIP および BZIP2 ファイルだけでなく、CVE OVAL フィードの非圧縮 XML ファイルもサポートし、CVE OVAL ベースのスキャンは追加手順なしで適切に機能するようになりました。(BZ#1440192)

第33章 サーバーおよびサービス

ReaR が Linux 機能を正しく保持

以前は、バックアップフェーズで、`rear` は元のシステムに設定された Linux 機能を保持しませんでした。その後、復元したシステムにはこの機能がありませんでした。今回の更新で、ディレクティブ `NETFS_RESTORE_CAPABILITIES` が `/usr/share/rear/conf/default.conf` 設定ファイルの `y` オプションに設定されている場合、Linux 機能が正しく保持されるようになりました。(BZ#1343119)

`sblim-cmpi-fsvol` は、DM でマウントされたファイルシステムを無効として表示しなくなりました

以前は、`sblim-cmpi-fsvol` Common Information Model (CIM) プロバイダーは、デバイスマッパー (DM) でマウントされたファイルシステム (FS) を正しく識別できませんでした。その結果、`CIM_UnixLocalFileSystem` クラスインスタンスを列挙すると、`sblim-cmpi-fsvol` は、すでに無効としてマウントされている一部の FS を示しました。今回の更新で、DM でマウントした FS の `mount` コマンドの出力を解析するのではなく、`dmsetup` コマンドの出力を解析するように `sblim-cmpi-fsvol` が修正されました。これにより、`sblim-cmpi-fsvol` が、DM でマウントされた FS を正しく表示するようになりました。(BZ#1136116)

Cyrus SASL の SPNEGO が Microsoft Windows と互換性を持つようになる

今回の更新以前は、Cyrus Simple Authentication and Security Layer (SASL) における Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) の Red Hat Enterprise Linux 実装と、Microsoft Windows の互換性がありませんでした。そのため、`cyrus-sasl` パッケージを使用する Red Hat Enterprise Linux ツールは、Windows サービスへの接続を試行する際に SPNEGO を使用できませんでした。また、このツールでは、Windows クライアントからの接続を受け入れることもできませんでした。`cyrus-sasl` パッケージが修正され、Red Hat Enterprise Linux Cyrus SASL バージョンの SPNEGO が、Microsoft Windows の対応するバージョンと互換性を持つようになりました。(BZ#1421663)

MariaDB init スクリプトが失敗した場合にデータが失われなくなる

以前は、MariaDB init スクリプトが失敗すると、ディレクトリー全体で `rm -rf` が呼び出されていました。その結果、データが失われたり、マウントポイントが削除されたりする可能性があります。今回の更新で、init スクリプトにいくつかの確認メカニズムが追加されました。これで、スクリプトが失敗した場合、重要なファイル操作の前に生成されたタイムスタンプよりも新しいファイルのみが削除されます。さらに、人間が判読できる状態レポートとエラーメッセージのセットが追加されました。(BZ#1356897)

ypbind がネットワークへのアクセスが保証される前に起動しなくなる

`ypbind` サービスは、`systemd` ターゲット `network.target` の後に起動するように設定されました。ただし、`network.target` は、`ypbind` で必要なネットワーク機能を保証しません。その結果、起動プロセス中に開始したときに、`ypbind` サービスがネットワークにアクセスできないことがあります。また、`ypbind` のサービスファイルは、ターゲットの `network-online.target` の後に `ypbind` を開始するように変更され、システムの起動時に `ypbind` がネットワークにアクセスできることが保証されるようになりました。(BZ#1382804)

ypbindが原因で、リモートユーザーのアカウント設定が再起動時にデフォルト設定に戻されなくなりました。

サービスの起動順序が間違っているため、すべての Name Service Switch (NSS) ルックアップ操作が完了する前に ypbind が起動しませんでした。これにより、次のすべての条件を満たすユーザーの再起動時に、ユーザーのアカウント設定ファイルがデフォルト設定に戻りました。

- Gnome Display Manager の自動ログインの使用
- NIS 認証の使用
- NFS にあるホームディレクトリー

ypbind サービスファイルの順序が修正され、ユーザー/グループデータベースを設定する前に ypbind が起動するように修正されました。ユーザーのアカウント設定ファイルが適切に処理されるようになりました。(BZ#1217435)

ネットワーク情報システムのセキュリティー機能が使用されたため yppasswd がクラッシュしなくなる

yppasswd クライアントは、以下の状況を認識しないため、パスワードをチェックする際に誤った文字列を salt として使用しようとしていました。

- NIS サーバーが passwd.adjunct マップを使用するように設定されている。
- 変数 MERGE_PASSWD=false が NIS サーバーのファイル /var/yp/Makefile に設定されていました。

これにより、yppasswd が次のエラーメッセージで失敗していました： crypt

() failed。yppasswd クライアントがこのような状況を認識するように修正され、サーバーで実行している yppasswd デーモンにチェックを委譲するようになりました。(BZ#1401432)

Evince が PostScript ファイルを再度表示

バグにより、evince ドキュメントビューアーは、Script ファイルの内容を表示できませんでした。パッチが適用され、evince が、再びアプリケーションを表示するようになりました。(BZ#1411725)

db_verify により libdb の空きミューテックスが不足しなくなりました。

以前は、**libdb** データベースはすべての未使用のミューテックスを正しく解放していませんでした。**libdb** データベースファイルで **db_verify** コマンドを複数回実行すると、**libdb** はミューテックス操作のソースがすぐに不足していました。そのため、**libdb** はエラーメッセージで終了しました。

```
Unable to allocate memory for mutex; resize mutex region
```

これにより、データベースを一貫性のない状態のままにしていました。このバグが修正され、**libdb** がミューテックスを正しく解放し、上記の問題は発生しなくなりました。(BZ#1277887)

一部の状況で **ghostscript** が応答しなくなる

特定の状況では、**ghostscript** アプリケーションは無限ループに入り、応答しなくなり、CPU 負荷が過剰に発生しました。今回の更新で、前述の問題が発生しないように、基本的なコードが修正されました。(BZ#1424752)

postscript を PDF に変換しても **ps2pdf** が予期せず終了しなくなる

以前は、**Postscript** ファイルを PDF に変換すると、**ps2pdf** ユーティリティーがセグメンテーション違反で予期せず終了していました。このバグが修正され、**postscript** を PDF に変換しても **ps2pdf** がクラッシュしなくなりました。(BZ#1390847)

sapconf が、より高い **kernel.shmall** および **kernel.shmmax** の値で正しく機能するようになりました。

以前は、**kernel.shmall** および **kernel.shmmax** の値がデフォルトで増加し、**sapconf** ユーティリティーにエラーが表示されていました。そのため、**sapconf** は以下のエラーメッセージを出して失敗しました。

```
integer expression expected
```

今回の更新で、**kernel.shmall** および **kernel.shmmax** の高い値を可能にする新しいチェックが追加され、上記の問題は発生しなくなりました。(BZ#1391881)

第34章 ストレージ

キャッシュ論理ボリュームで `lvconvert --repair` が適切に動作するようになりました。

Red Hat Enterprise Linux 7.3 でリリースされた `lvm2-2.02.166-1.el` パッケージのリグレッションにより、`lvconvert --repair` コマンドをキャッシュ論理ボリュームで適切に実行できませんでした。その結果、`Cannot convert internal LV` エラーが発生しました。このバグを修正するために基礎となるソースコードが変更され、`lvconvert --repair` が期待どおりに機能するようになりました。(BZ#1380532)

LVM2 ライブラリーの非互換性によるデバイスの監視の失敗やアップグレード中の消失がなくなる

Red Hat Enterprise Linux 7.3 でリリースされた `lvm2-2.02.166-1.el` パッケージのバグにより、ライブラリーは以前のバージョンの Red Hat Enterprise Linux 7 と互換性がありませんでした。互換性がないと、デバイスの監視に失敗し、アップグレード中に消失する可能性があります。その結果、デバイスの障害が見過ごされたり (RAID)、スペース不足の状態が適切に処理されなかったりする可能性があります (thin-p)。今回の更新で非互換性が修正され、論理ボリュームの監視が想定どおりに機能するようになりました。(BZ#1382688)

be2iscsi ドライバーエラーが原因でシステムが応答しなくなる

以前は、`be2iscsi` ドライバーエラーが原因で、オペレーティングシステムが応答しなくなることがありました。今回の更新で `be2iscsi` が修正され、`be2iscsi` エラーが原因でオペレーティングシステムがハングしなくなりました。(BZ#1324918)

mirror セグメントタイプが使用されている場合、`lvmetad` デーモンで相互作用の問題が発生しなくなりました。

以前は、従来の `mirror` セグメントタイプを使用して、3 つ以上のレグでミラー化論理ボリュームを作成すると、`lvmetad` デーモンで相互作用の問題が発生する可能性があります。発生した問題は、ミラー障害ポリシーがデフォルト以外の `allocate` オプションに設定され、`lvmetad` が使用され、デバイスの障害の間にマシンの再起動が行われなかったときに、2 番目のデバイス障害後にのみ発生しました。このバグは修正され、上述の相互作用の問題は発生しなくなりました。(BZ#1380521)

`multipathd` デーモンは、ブラックリストに登録されたデバイスの誤ったエラーメッセージを表示しなくなりました。

以前は、`multipathd` デーモンは、ブラックリストに登録されたデバイスを見つけられなかった誤ったエラーメッセージを表示していたため、何も問題がない場合にユーザーにエラーメッセージが表示されていました。今回の修正により、マルチパスは、エラーメッセージを発行する前にデバイスがブラックリストに登録されているかどうかをチェックします。(BZ#1403552)

マルチパスが、使用可能なパスがない場合にデバイスの再読み込みにフラグを立てるようになりました。

以前は、マルチパスデバイスへの最後のパスデバイスが削除されると、`lvmetad` の状態が間違っており、マルチパス上の `lvm` デバイスが正しく機能しなくなる可能性があります。これは、マルチパスデバイスが再読み込みされたときに、デバイスマッパーが動作中のパスの数を知る方法がなかったためです。このため、スキャンやその他の `dm` ルールを無効にするマルチパス `udev` ルールは、マルチパスデ

パスがデバイステーブルのリロードではなく、障害により最後に使用可能なパスを失った場合にのみ機能します。今回の修正により、使用可能なパスがない場合にマルチパスがデバイスのリロードにフラグを立てるようになりました。また、マルチパスデバイスが最後に使用可能なパスを失うたびに、マルチパス udev ルールはスキャンやその他の dm ルールを正しく無効にするようになりました。その結果、lvmetad の状態は正しく残り、マルチパス上の LVM デバイスは引き続き正常に機能します。(BZ#1239173)

書き込みに失敗した後に送信される読み取り要求は、常にマルチパスデバイスで同じデータを返します。

以前は、書き込み要求が rbd モジュールでハングし、iSCSI イニシエーターとマルチパスレイヤーがアプリケーションへの要求の失敗を決定した場合、失敗後に送信された読み取り要求は書き込みの状態を反映しない可能性があります。これは、複数の iSCSI ターゲットを介して Ceph rbd イメージをエクスポートすると、書き込み要求を受信すると rbd カーネルモジュールが排他ロックを取得するためです。今回の修正により、rbd モジュールは読み取りおよび書き込みの両方の排他ロックを取得します。これにより、ハングした書き込みがフラッシュされ、読み取りを実行する前に失敗します。このため、書き込みに失敗した後に送信される読み取り要求は、常に同じデータを返します。(BZ#1380602)

マルチパスデバイスのパスデバイスが読み取り専用に切り替わると、マルチパスデバイスが読み取り専用に再読み込みされます。

以前は、マルチパスデバイスを再読み込みするときに、マルチパスコードは常にデバイスを最初に読み取り/書き込みで再読み込みしようとし、次に読み取り専用でフェイルバックしていました。パスデバイスがカーネルですでに読み取り/書き込みで開かれている場合、デバイスが読み取り専用モードに切り替わり、読み取り/書き込みの再読み込みが成功した場合でも、パスデバイスは読み取り/書き込みで開かれ続けます。その結果、パスデバイスが読み取り/書き込みから読み取り専用に切り替わった場合でも、マルチパスデバイスは読み取り/書き込みのままになりました(読み取り専用デバイスへのすべての書き込みが失敗した場合でも)。今回の修正により、multipathd は、パスデバイスが読み取り専用になったことを示す uevent を取得したときに、マルチパスデバイスを読み取り専用で再読み込みするようになりました。その結果、マルチパスデバイスのパスデバイスが読み取り専用に切り替わると、マルチパスデバイスは読み取り専用で再読み込みされます。(BZ#1431562)

ユーザーは確認されていないマルチパスデバイスの混同する可能性のある古いデータを取得しなくなる

以前は、パスデバイスが孤立している場合(マルチパスデバイスのメンバーではない)、デバイスの状態とチェッカーの状態が孤立する前のデバイスの状態の show paths コマンドで表示されていました。その結果、show paths コマンドは、チェックされなくなったデバイスの古い情報を表示していました。今回の修正により、show paths コマンドは、孤立したパスのデバイスの状態として undef をチェッカーの状態として表示し、ユーザーがチェックされていないデバイスの混乱を生じさせる可能性のある古いデータを取得しなくなりました。(BZ#1402092)

失敗したパスで Prioritizer を実行すると、multipathd デーモンがハングしなくなりました。

以前は、multipathd は、場合によっては失敗したパスで Prioritizer を実行していました。このため、multipathd が同期優先順位付けで設定されている場合、失敗したパスで Prioritizer を実行しようとするハングする可能性があります。今回の修正により、パスが失敗したときに multipathd が Prioritizer を実行しなくなり、この理由で失敗しなくなりました。(BZ#1362120)

システムのアップグレード後、新しい RAID4 ボリューム、および既存の RAID4 または RAID10 論理ボリュームが正しくアクティブ化されるようになる

Red Hat Enterprise Linux バージョン 7.3 で RAID4 論理ボリュームを作成した後、または既存の RAID4 または RAID10 論理ボリュームを持つシステムをバージョン 7.3 にアップグレードした後、システムがこれらのボリュームのアクティブ化に失敗することがありました。この更新により、システムはこれらのボリュームを正常にアクティブにします。(BZ#1386184)

PV のステータスが間違っているため、LVM ツールがクラッシュしなくなる

LVM が、ボリュームグループ (VG) 内の物理ボリューム (PV) のメタデータ間で特定タイプの不整合を観察すると、LVM がそれらを自動的に修復できます。このような不整合は、たとえば、一部の PV がシステムから一時的に見えないときに VG が変更された後、PV が再表示された場合に発生します。

今回の更新以前は、このような修復作業が行われた場合、そうでない場合でも、一時的にすべての PV が戻ったと見なされることがありました。これにより、LVM ツールがセグメンテーション障害で予想外に終了する場合があります。今回の更新で、上記の問題は発生しなくなりました。(BZ#1434054)

第35章 システムおよびサブスクリプション管理

リポジトリが設定されていないシステムで アンダー クラウドが失敗しなくなりました。

以前は、ユーザーがリポジトリが設定されていないシステムに OpenStack Undercloud をインストールしようとする、yum パッケージマネージャーはすでにインストールされている MySQL 依存関係をインストールする必要がありました。結果として、アンダー クラウドのインストールスクリプトは失敗しました。この不具合を修正するために、yum が、インストール済みの MySQL 依存関係を正しく検出するように修正されました。その結果、リポジトリが設定されていないシステムで、アンダー クラウドのインストールスクリプトが失敗することはなくなりました。(BZ#1352585)

yum -plugin-verify が提供する yum コマンドは、不一致が見つかった場合に終了ステータスを 1 に設定するようになりました。

yum -plugin-verify プラグインが提供する yum コマンドは、パッケージにある不一致に対して終了コード 0 を返しました。バグが修正され、不一致が見つかった場合に終了ステータスが 1 に設定されるようになりました。(BZ#1406891)

第36章 仮想化

SeaBIOS は LUN がゼロ以外の SCSI デバイスを認識

SeaBIOS は、論理ユニット番号 (LUN) がゼロに設定されている場合に、SCSI デバイスのみを認識していました。そのため、SCSI デバイスがゼロ以外の LUN で定義されていると、SeaBIOS が起動に失敗します。今回の更新で、SeaBIOS が、ゼロ以外の LUN を持つ SCSI デバイスを認識するようになりました。その結果、SeaBIOS が正常に起動します。(BZ#1020622)

libguestfs ツールは、`/usr/` が `root` と同じパーティションにないゲストを正しく処理するようになりました。

以前は、`/usr/` ディレクトリーが `root` ディレクトリーと同じパーティションにない場合、libguestfs ライブラリーはゲストオペレーティングシステムを認識しませんでした。そのため、`virt-v2v` ユーティリティーなどの複数の libguestfs ツールは、このようなゲストで使用されると期待どおりに機能しませんでした。今回の更新で、`/usr/` が `root` と同じパーティションにない場合に、libguestfs がゲストオペレーティングシステムを認識するようになりました。その結果、影響を受ける libguestfs ツールは期待どおりに動作します。(BZ#1401474)

`virt-v2v` は、Windows レジストリーが破損しているか、破損している Windows ゲストを変換できません。

以前は、libguestfs が Windows レジストリーを操作するために使用する `hivex` ライブラリーは、破損したレジストリーを処理できませんでした。そのため、`virt-v2v` ユーティリティーは、Windows レジストリーが破損したり、破損したりする Windows ゲストを変換できませんでした。今回の更新により、libguestfs は、Windows レジストリーの読み取り時に `hivex` が厳格ではないように設定します。その結果、`virt-v2v` は、Windows レジストリーが破損したり破損しているほとんどの Windows ゲストを変換できるようになりました。(BZ#1311890, BZ#1423436)

`virt-v2v` を使用したシステム以外の動的ディスクでの Windows ゲストの変換が正しく機能するようになりました。

以前は、`virt-v2v` ユーティリティーを使用して、システム以外の動的ディスクを持つ Windows ゲスト仮想マシンを変換することは正しく機能せず、変換後にゲストが使用できませんでした。この更新により、基本となるコードが修正されるため、上記の問題が回避されます。

システムディスク (C: ドライブ) で動的ディスクを使用する Windows ゲストの変換は、依然としてサポートされていないことに注意してください。(BZ#1265588)

Glance クライアントのバージョンに関係なく、ゲストを Glance イメージに変換できます。

以前は、Glance コマンドラインクライアントバージョン 1.0.0 以降が `virt-v2v` 変換サーバーにインストールされている場合、`virt-v2v` ユーティリティーを使用してゲスト仮想マシンを Glance イメージに変換できませんでした。このリリースでは、イメージをエクスポートする際に、`virt-v2v` がイメージのすべてのプロパティーを直接設定します。その結果、`virt-v2v` 変換サーバーにインストールされている Glance クライアントのバージョンに関係なく、Glance への変換が機能します。(BZ#1374405)

virt-v2vを使用して、Red Hat Enterprise Linux 6.2 - 6.5 ゲスト仮想マシンを変換できるようになりました。

以前は、Red Hat Enterprise Linux バージョン 6.2 - 6.5 の SELinux file_contexts ファイルのエラーにより、virt-v2v ユーティリティーを使用したこれらのゲストが変換されませんでした。今回の更新で、virt-v2v は、SELinux file_contexts ファイルのエラーを自動的に修正します。その結果、virt-v2v を使用して、Red Hat Enterprise Linux 6.2-6.5 ゲスト仮想マシンを変換できるようになりました。(BZ#[1374232](#))

/etc/fstab の btrfs エントリーが libguestfsによって正しく解析されるようになりました。

以前は、/etc/fstab に複数のコンマ区切りオプションを持つ Btrfs サブボリュームエントリーは、libguestfs で正しく解析されませんでした。そのため、この設定を備えた Linux ゲスト仮想マシンは検証できず、virt-v2v ユーティリティーはそれらを変換できませんでした。今回の更新で、libguestfs は、/etc/fstab に複数のコンマ区切りオプションを持つ Btrfs サブボリュームエントリーを正しく解析するようになりました。その結果、このエントリーは virt-v2v により検査および変換できます。(BZ#[1383517](#))

libguestfs が、認証を必要とする libvirt ドメインディスクを正しく開くことができるようになりました

以前は、libvirt ドメインからディスクを追加する場合、libguestfs はディスクシークレットを読み取りませんでした。そのため、libguestfs は認証を必要とするディスクを開くことができませんでした。今回の更新で、libguestfs は、libvirt ドメインのディスクのシークレットを読み取ります（存在する場合）。これにより、libguestfs が、認証を必要とする libvirt ドメインのディスクを正しく開くことができるようになりました。(BZ#[1392798](#))

変換した Windows UEFI ゲストが適切に起動する

以前は、Windows 8 UEFI ゲストを変換すると、virtio ドライバーが正しくインストールされませんでした。その結果、変換したゲストが起動しませんでした。今回の更新で、virtio ドライバーが Windows UEFI ゲストに正しくインストールされるようになりました。その結果、変換した Windows UEFI ゲストが適切に起動します。(BZ#[1431579](#))

virt-v2v ユーティリティーが、プロキシ環境変数を一貫して無視するようになりました。

今回の更新以前は、virt-v2v ユーティリティーを使用して VMware ゲスト仮想マシンを変換する際に、virt-v2v は VMware への接続にプロキシ環境変数を使用していましたが、その他の接続には使用しませんでした。これにより、変換が失敗する場合があります。virt-v2v は、変換中にすべてのプロキシ設定を無視するようになり、上記の問題が回避されます。(BZ#[1354507](#))

virt-v2v は、必要に応じて RHEV-apt.exe と rshrvany.exe のみをコピーします。

以前は、virt-v2v は、Windows ゲストを変換する際に、常に RHEV-apt.exe ファイルおよび rshrvany.exe ファイルをコピーしていました。そのため、これらのゲストは必要なくても、変換した Windows ゲストに存在していました。今回の更新で、virt-v2v は、Windows ゲストに必要な場合にのみこれらのファイルをコピーします。(BZ#[1161019](#))

ボンディングされたインターフェイスを介した VLAN を持つゲストは、フェールオーバー後にトラフィックの通過を停止しなくなる

以前のリリースでは、ixgbe 仮想機能(VF)を使用するボンディングされたインターフェイス上で VLAN が設定されたゲスト仮想マシンでは、フェールオーバーの発生時にボンディングされたネットワークインターフェイスがトラフィックの通過を停止していました。ハイパーバイザーコンソールは、このエラーを要求された MACVLAN フィルターとしてログに記録しましたが、管理上のメッセージも記録されています。この更新により、フェールオーバーが適切に処理されるようになり、上記の問題が回避されます。(BZ#1379787)

virt-v2v は、< ovf:Name> 属性を持たない OVA をインポートします。

以前は、virt-v2v ユーティリティーは、< ovf:Name> 属性のない Open Virtual Appliances (OVA)のインポートを拒否していました。そのため、virt-v2v ユーティリティーは、Amazon Web Services (AWS)がエクスポートした OVA をインポートしませんでした。本リリースでは、< ovf:Name > 属性がない場合、virt-v2v はディスクイメージファイルのベース名を仮想マシンの名前として使用します。その結果、virt-v2v ユーティリティーは、AWS がエクスポートした OVA をインポートするようになりました。(BZ#1402301)

パート III. テクノロジープレビュー

ここでは、Red Hat Enterprise Linux 7.4 で利用可能なすべてのテクノロジープレビュー機能の一覧を提示します。

テクノロジープレビュー機能に対する Red Hat のサポート範囲の詳細は、<https://access.redhat.com/support/offerings/techpreview/> を参照してください。

第37章 全般的な更新

systemd-importd 仮想マシンとコンテナイメージのインポートおよびエクスポートサービス

最新の `systemd` バージョンには、以前のビルドで有効にされていない `systemd-importd` デーモンが含まれるようになりました。これにより、`machinectl pull-*` コマンドが失敗しました。`systemd-importd` デーモンはテクノロジープレビューとして提供され、安定しているとみなされないことに注意してください。(BZ#[1284974](#))

第38章 認証および相互運用性

AD および LDAP の sudo プロバイダーの使用

AD (Active Directory) プロバイダーは、AD サーバーへの接続に使用するバックエンドです。Red Hat Enterprise Linux 7.2 以降では、AD sudo プロバイダーを LDAP プロバイダーとともに使用することがテクノロジープレビューとして利用できます。AD sudo プロバイダーを有効にするには、`sssd.conf` ファイルの `[domain]` セクションに `sudo_provider=ad` 設定を追加します。(BZ#1068725)

DNSSEC が IdM でテクノロジープレビューとして利用可能になりました。

統合 DNS のある Identity Management (IdM) サーバーは、DNS プロトコルのセキュリティを強化する DNS に対する拡張セットである DNS Security Extensions (DNSSEC) に対応するようになりました。IdM サーバーでホストされる DNS ゾーンは、DNSSEC を使用して自動的に署名できます。暗号鍵は、自動的に生成およびローテートされます。

DNSSEC で DNS ゾーン的安全性を強化する場合は、以下のドキュメントを参照することが推奨されます。

- DNSSEC Operational Practices, Version 2: <http://tools.ietf.org/html/rfc6781#section-2>
- Secure Domain Name System (DNS) Deployment Guide: <http://dx.doi.org/10.6028/NIST.SP.800-81-2>
- DNSSEC Key Rollover Timing Considerations: <http://tools.ietf.org/html/rfc7583>

統合 DNS のある IdM サーバーは、DNSSEC を使用して、他の DNS サーバーから取得した DNS 回答を検証することに注意してください。これは、Red Hat Enterprise Linux Networking Guide https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices で説明されている、推奨される命名方法に従って設定されていない DNS ゾーンの可用性に影響を与える可能性があります。(BZ#1115294)

Identity Management JSON-RPC API がテクノロジープレビューとして利用可能になりました。

Identity Management (IdM) では API が利用できます。API を表示するために、IdM は、テクノロジープレビューとして API ブラウザーも提供します。

Red Hat Enterprise Linux 7.3 では、複数のバージョンの API コマンドを有効にするために、IdM API が拡張されました。以前は、機能拡張により、互換性のない方法でコマンドの動作が変更すること

がありました。IdM API を変更しても、既存のツールおよびスクリプトを引き続き使用できるようになりました。これにより、以下が可能になります。

- 管理者は、管理しているクライアント以外のサーバーで、IdM の以前のバージョンもしくは最近のバージョンを使用できます。
- サーバーで IdM のバージョンを変更しても、開発者は特定バージョンの IdM コールを使用できます。

すべてのケースでサーバーとの通信が可能になります。たとえば、ある機能向けの新オプションが新しいバージョンに追加されていて、通信の一方の側でこれを使用していたとしても、特に問題はありません。

API の使用方法は、<https://access.redhat.com/articles/2728021> (BZ#1298286) 参照してください。

Custodia シークレットサービスプロバイダーが利用可能に

テクノロジープレビューとして、シークレットサービスプロバイダーの Custodia を使用できるようになりました。Custodia は鍵やパスワードなどのシークレットのプロキシとして保存または機能します。

詳細は、<http://custodia.readthedocs.io> のアップストリームのドキュメントを参照してください。(BZ#1403214)

コンテナ化された Identity Management サーバーがテクノロジープレビューとして利用可能に

rhel7/ipa-server コンテナイメージは、テクノロジープレビュー機能として利用できません。rhel7/sss コンテナイメージが完全にサポートされるようになりました。

詳細は、https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html-single/using_containerized_identity_management_services を参照してください。(BZ#1405325, BZ#1405326)

第39章 クラスタリング

pcs ツールが Pacemaker でバンドルリソースを管理

Red Hat Enterprise Linux 7.4 以降のテクノロジープレビューとして、`pcs` ツールはバンドルリソースに対応します。`pcs resource bundle create` コマンドおよび `pcs resource bundle update` コマンドを使用して、バンドルを作成および変更できるようになりました。`pcs resource create` コマンドを使用すると、既存のバンドルにリソースを追加できます。バンドルリソースに設定できるパラメーターの詳細は、`pcs resource bundle --help` コマンドを実行します。(BZ#[1433016](#))

第40章 コンパイラーおよびツール

Shenandoah ガベージコレクター

新規の休止時間の短い Shenandoah ガベージコレクターが、Intel 64、AMD64、および 64 ビット ARM アーキテクチャー上の OpenJDK のテクノロジープレビューとして利用できるようになりました。Shenandoah は同時退避を実行します。これにより、ユーザーは長い休止時間なしで大きなヒープで実行できます。詳細は、<https://wiki.openjdk.java.net/display/shenandoah/Main> を参照してください。(BZ#1400306)

第41章 ファイルシステム

ファイルシステム DAX が、テクノロジープレビューとして ext4 および XFS で利用可能

Red Hat Enterprise Linux 7.3 以降、Direct Access (DAX) は、テクノロジープレビューとして、永続メモリーをそのアドレス領域に直接マッピングする手段を提供します。

DAX を使用するには、システムで利用可能な永続メモリーの形式が必要になります。通常は、NVDIMM (Non-Volatile Dual In-line Memory Module) の形式で、DAX に対応するファイルシステムを NVDIMM に作成する必要があります。また、ファイルシステムは `dax` マウントオプションでマウントする必要があります。次に、`dax` をマウントしたファイルシステムのファイルの `mmap` により、アプリケーションのアドレス空間にストレージを直接マッピングされます。(BZ#1274459)

pNFS およびブロックレイアウトのサポート

テクノロジープレビューとして、アップストリームコードが Red Hat Enterprise Linux クライアントにバックポートされ、pNFS ブロックレイアウト機能を提供します。

また、Red Hat Enterprise Linux 7.4 には、pNFS SCSI レイアウトのテクノロジープレビューが同梱されています。この機能は pNFS ブロックレイアウトに似ていますが、SCSI デバイスに限定されるため、使用しやすくなります。そのため、Red Hat では、pNFS ブロックレイアウトではなく、pNFS SCSI レイアウトの使用を推奨しています。(BZ#1111712)

OverlayFS

OverlayFS は、ユニオンファイルシステムのタイプです。ユーザーは、あるファイルシステムに別のファイルシステムを重ねることができます。変更は上位のファイルシステムに記録され、下位のファイルシステムは変更しません。これにより、ベースイメージが読み取り専用メディアにあるコンテナや DVD-ROM などのファイルシステムイメージを、複数のユーザーが共有できるようになります。詳細は、カーネルファイル `Documentation/filesystems/overlayfs.txt` を参照してください。

OverlayFS は、ほとんどの状況で引き続き Red Hat Enterprise Linux 7.4 のテクノロジープレビューになります。このため、OverlayFS を有効にすると、カーネルにより警告のログが記録されます。

Docker で次の制約を付けて使用する場合は、OverlayFS が完全対応となります。

- OverlayFS は Docker のグラフィックドライバーとして使用する場合にのみサポートされます。サポートはコンテナ COW コンテンツでの使用に限定され、永続ストレージとしてはサポートされません。永続ストレージは OverlayFS 以外のボリュームに配置している場合に限りサポートの対象となります。使用できるのはデフォルトの Docker 設定のみです。つまり、オー

パーレイレベル 1 つ、下層側ディレクトリー 1 つ、同じファイルシステムに配置された上層レベルと下層レベルという設定です。

- 下層ファイルシステムとして使用がサポートされているのは現在 XFS のみです。
- Red Hat Enterprise Linux 7.3 以前では、物理マシンで SELinux を有効にして Enforcing モードにする必要がありますが、コンテナの分離を実行する際にコンテナで無効にする必要があります。これは、`/etc/sysconfig/docker` ファイルに `--selinux-enabled` を含めないでください。Red Hat Enterprise Linux 7.4 以降、OverlayFS は SELinux セキュリティーラベルをサポートし、`/etc/sysconfig/docker` で `--selinux-enabled` を指定すると、コンテナの SELinux サポートを有効にできます。
- OverlayFS カーネル ABI とユーザー空間の動作については安定性に欠けると見なされているため、今後の更新で変更が加えられる可能性があります。
- コンテナ内で `yum` および `rpm` のユーティリティーを正常に機能させるには、`yum-plugin-ovl` パッケージを使用する必要があります。

OverlayFS は制限付きで POSIX 標準セットを提供しています。OverlayFS を使用してアプリケーションをデプロイする前に、アプリケーションを十分にテストしてください。

オーバーレイとして使用するために、`-n ftype=1` オプションを有効にして XFS ファイルシステムを作成する必要があることに注意してください。`rootfs` およびシステムのインストール時に作成されたファイルシステムを使用して、Anaconda キックスタートに `--mkfsoptions=-n ftype=1` パラメーターを設定します。インストール後に新しいファイルシステムを作成する場合は、`# mkfs -t xfs -n ftype=1 /PATH/TO/DEVICE` コマンドを実行します。既存のファイルシステムがオーバーレイとして使用できるかどうかを確認するには、`# xfs_info /PATH/TO/DEVICE | grep ftype` コマンドを実行して、`ftype=1` オプションが有効になっているかどうかを確認します。

Red Hat Enterprise Linux 7.3 リリース以降、OverlayFS には既知の問題が複数存在します。詳細は、`Documentation/filesystems/overlayfs.txt` ファイルの `Non-standard behavior` を参照してください。(BZ#1206277)

pNFS SCSI レイアウトクライアントおよびサーバーのサポートが提供されるようになりました。

並列 NFS (pNFS) SCSI レイアウトのクライアントおよびサーバーのサポートは、Red Hat Enterprise Linux 7.3 以降のテクノロジープレビューとして提供されます。ブロックレイアウトの作業に基づいて、pNFS レイアウトは SCSI デバイス全体で定義され、SCSI 永続予約をサポートできる必要がある論理ユニットとして一連の固定サイズブロックが含まれています。論理ユニット (LU) デバイ

スは、SCSI デバイス識別子で識別され、フェンシングは予約の割り当てを介して処理されます。
(BZ#1305092)

Btrfs ファイルシステム

Btrfs (B-Tree)ファイルシステムは、Red Hat Enterprise Linux 7 でテクノロジープレビューとして利用できます。

この機能の更新は、Red Hat Enterprise Linux 7.4 で最後となることが予定されています。**Btrfs** は非推奨になりました。つまり、Red Hat は **Btrfs** を完全にサポートしていない機能に移行しなくなり、Red Hat Enterprise Linux の将来のメジャーリリースで削除される予定です。(BZ#1477977)

第42章 ハードウェアの有効化

利用可能な Trusted Computing Group TPM 2.0 System API ライブラリーおよび管理ユーティリティー

Trusted Computing Group の Trusted Platform Module (TPM) 2.0 ハードウェアをテクノロジープレビューとしてサポートするために、Red Hat Enterprise Linux に、新しいパッケージが 2 つ追加されました。

- **tpm2-tss** パッケージは、TPM 2.0 System API ライブラリーの Intel 実装を追加します。このライブラリーを使用すると、プログラムが TPM 2.0 デバイスと対話できます。
- **tpm2-tools** パッケージは、ユーザースペースから TPM2.0 デバイスを管理および利用するための一連のユーティリティーを追加します。(BZ#1275027, BZ#1275029)

新規パッケージ: tss2

tss2 パッケージには、IBM による Trusted Computing Group Software Stack (TSS) 2.0 の実装がテクノロジープレビューとして追加されました。このパッケージにより、TPM 2.0 デバイスとの対話が可能になります。(BZ#1384452)

LSI Syncro CS HA-DAS アダプター

Red Hat Enterprise Linux 7.1 には、LSI Syncro CS の HA-DAS (high-availability direct-attached storage) アダプターを有効にするため、`megaraid_sas` ドライバーにコードが含まれていました。`megaraid_sas` ドライバーは、これまで有効であったアダプターに対して完全にサポートされますが、Syncro CS に対してはテクノロジープレビューとして提供されます。このアダプターのサポートは、LSI、システムインテグレーター、またはシステムベンダーにより直接提供されます。Red Hat Enterprise Linux 7.2 以上に Syncro CS をデプロイする場合は、Red Hat および LSI へのフィードバックにご協力ください。LSI Syncro CS ソリューションの詳細は、<http://www.lsi.com/products/shared-das/pages/default.aspx> を参照してください。(BZ#1062759)

第43章 インストールおよび起動

rpm-buildでのマルチスレッドの xz 圧縮

現在、圧縮は1つのコアのみを使用しているため、高度に並列化されたビルドでは長い時間がかかる可能性があります。これは、多くのコアを備えたハードウェア上に構築された大規模なプロジェクトを継続的に統合する場合に特に問題になります。

この機能はテクノロジープレビューとして提供され、`%_source_payload` マクロまたは `%_binary_payload` マクロを `wLTX.xz dio` パターンに設定する際に、ソースパッケージおよびバイナリパッケージのマルチスレッドの xz 圧縮を有効にします。この中で、L は圧縮レベル（デフォルトでは 6）を表し、X は使用するスレッドの数です（複数の数字である可能性があります）（例：`w6T12.xzdio`）。これは、`/usr/lib/rpm/macros` ファイルを編集するか、`spec` ファイルまたはコマンドラインでマクロを宣言することで実行できます。(BZ#1278924)

第44章 カーネル

HMM (heterogeneous memory management) 機能がテクノロジープレビューとして利用可能に

Red Hat Enterprise Linux 7.3 では、テクノロジープレビューとして **heterogeneous memory management (HMM)** 機能が導入されました。この機能は、プロセスアドレス空間を独自のメモリー管理ユニット (MMU) にミラーする必要があるデバイスのヘルパーレイヤーとして、カーネルに追加されています。これにより、CPU 以外のデバイスプロセッサは、統一システムアドレス空間を使用してシステムメモリーを読み取ることができます。この機能を有効にするには、`experimental_hmm=enable` をカーネルコマンドラインに追加します。(BZ#1230959)

criu がバージョン 2.12 にリベース

Red Hat Enterprise Linux 7.2 では、テクノロジープレビューとして **criu** ツールが導入されました。このツールは、**CRIU (Checkpoint/Restore in User-space)** を実装します。これを使用して、実行中のアプリケーションをフリーズし、ファイルのコレクションとして保存できます。アプリケーションは、後にフリーズ状態から復元できます。

criu ツールは **Protocol Buffers** に依存することに注意してください。これは、構造化データをシリアル化するための、言語に依存しない、プラットフォームに依存しない拡張可能なメカニズムです。依存パッケージを提供する **protobuf** パッケージと **protobuf-c** パッケージも、Red Hat Enterprise Linux 7.2 にテクノロジープレビューとして導入されています。

Red Hat Enterprise Linux 7.4 では、**criu** パッケージがアップストリームバージョン 2.12 にアップグレードされ、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。(BZ#1400230)

kexec がテクノロジープレビューとして利用可能に

kexec システムコールがテクノロジープレビューとして提供されます。このシステムコールを使用すると現在実行中のカーネルから別のカーネルを読み込んだり、起動したりすることが可能で、カーネル内のブートローダーとして機能します。通常、標準のシステム起動時に実行されるハードウェアの初期化は **kexec** の起動時に実行されないため、再起動に必要な時間が大幅に短縮されます。(BZ#1460849)

テクノロジープレビューとしての kexec fast reboot

テクノロジープレビューとして、**kexec fast reboot** 機能が追加され、再起動が大幅に速くなりました。この機能を使用するには、**kexec** カーネルを手動で読み込んでから、オペレーティングシステムを再起動する必要があります。**kexec fast reboot** をデフォルトの再起動アクションとして実行することはできません。

特別なケースでは、**Anaconda** に **kexec fast reboot** を使用します。この場合でも、**kexec fast reboot** をデフォルトにすることはできません。ただし、**Anaconda** で使用すると、**anaconda** オプションを使用してカーネルを起動した場合に、インストールの完了後に、オペレーティングシステムが自動的に **kexec fast reboot** を使用できます。**kexec** の再起動をスケジュールするには、カーネルコマ

ンドラインで `inst.kexec` コマンドを使用するか、キックスタートファイルに `reboot --kexec` 行を追加します。(BZ#1464377)

名前空間への非特権アクセスは、テクノロジープレビューとして有効化できる

必要に応じて、`namespace.unpriv_enable` カーネルコマンドラインオプションをテクノロジープレビューとして設定できるようになりました。

デフォルト設定は `off` です。

1 に設定すると、非特権ユーザーとしてフラグ `CLONE_NEWNS` を使用して `clone ()` 関数への呼び出しを発行しても、エラーが返されなくなり、操作が許可されます。

ただし、名前空間への非特権アクセスを有効にするには、一部のユーザー名前空間で `CAP_SYS_ADMIN` フラグを設定して、マウント名前空間を作成する必要があります。(BZ#1350553)

テクノロジープレビューとしての KASLR

Kernel Address Space Layout Randomization (KASLR) がテクノロジープレビューとして利用できるようになりました。KASLR は、カーネルテキスト KASLR と mm KASLR の 2 つの部分を含むカーネル機能です。この 2 つの部分は相互に作用し、Linux カーネルのセキュリティーを強化します。

カーネルテキストの物理アドレスと仮想アドレスの場所が、個別にランダム化されます。カーネルの物理アドレスは 64 TB の任意の場所に配置できますが、カーネルの仮想アドレスは、`[0xffffffff80000000, 0xffffffffc0000000]` の間の 1 GB 領域に制限されます。

3 つの mm セクション (直接マッピング、`vmalloc`、および `vmemmap` セクション) の開始アドレスは、特定のエリアでランダム化されます。以前は、このセクションの開始アドレスが固定値になっていました。

したがって、悪意のコードが、カーネルアドレス領域にその記号が置かれていることを知る必要がある場合に、KASLR は悪意のコードにカーネルの実行を挿入またはリダイレクトしないようにすることができます。

KASLR コードは、Linux カーネルでコンパイルされましたが、デフォルトでは無効になっていることに注意してください。これを使用する場合は、カーネルコマンドラインに `kaslr` カーネルオプションを追加して、明示的に有効にします。(BZ#1449762)

柔軟なファイルレイアウトで NFSv4 pNFS クライアントを更新

NFSv4 クライアントでの柔軟なファイルレイアウトは、最初に Red Hat Enterprise Linux 7.2 でテクノロジープレビューとして導入されました。Red Hat Enterprise Linux 7.4 は、この機能に更新を追加していますが、これは引き続きテクノロジープレビューとして提供されています。

NFSv4 の柔軟なファイルレイアウトにより、ノンストップファイルモビリティやクライアント側のミラーリングなどの高度な機能を利用できます。これにより、データベース、ビッグデータ、仮想化などの領域での使いやすさが向上します。NFS フレキシブルファイルレイアウトの詳細は、<https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/> を参照してください。(BZ#1349668)

CUIR 拡張スコープ検出

Linux による Control Unit Initiated Reconfiguration (CUIR) のサポートにより、ダウンタイムが発生しないか、最小限に抑えられた同時ストレージサービスが可能になります。論理パーティション (LPAR) モードで実行している Linux インスタンスのサポートに加えて、IBM z/VM システムでの Linux インスタンスのサポートがテクノロジープレビューとして追加されました。(BZ#1274456)

qla2xxx ドライバーでテクノロジープレビューとしての SCSI-MQ

Red Hat Enterprise Linux 7.4 で更新された qla2xxx & ドライバーは、ql2xmqsupport=1 モジュールパラメーターで SCSI-MQ (multiqueue)を使用できるようになりました。デフォルト値は 0 (無効) です。SCSI-MQ の機能は、qla2xxx ドライバーで使用すると、テクノロジープレビューとして提供されます。

SCSI-MQ を使用してファイバーチャネルアダプター上での非同期 IO のパフォーマンステストを実施したところ、特定の条件下ではパフォーマンスが大幅に低下した点に注意してください。修正はテスト中で、Red Hat Enterprise Linux 7.4 の一般提供に間に合うように準備できませんでした。(BZ#1414957)

テクノロジープレビューとしての Intel Cache Allocation Technology

今回の更新で、テクノロジープレビューとして Intel Cache Allocation Technology (CAT) が追加されました。このテクノロジーにより、ソフトウェアはキャッシュ割り当てを定義されたキャッシュのサブセットに制限できます。定義されたサブセットは、他のサブセットと重複する可能性があります。(BZ#1288964)

第45章 REAL-TIME KERNEL

新規スケジューラークラス： SCHED_DEADLINE

今回の更新で、テクノロジープレビューとして、リアルタイムカーネル用の SCHED_DEADLINE スケジューラークラスが導入されました。新しいスケジューラーにより、アプリケーションの期限に基づいた予測可能なタスクのスケジューリングが可能になりました。SCHED_DEADLINE は、アプリケーションタイマーの操作を減らすことで、定期的なワークロードの利点を発揮します。(BZ#1297061)

第46章 ネットワーク

Cisco usNIC ドライバー

UCM (Cisco Unified Communication Manager) サーバーには Cisco 専用の usNIC (User Space Network Interface Controller) を提供するオプション機能があります。これを使用すると、ユーザー空間のアプリケーションに対して RDMA (Remote Direct Memory Access) のような動作を実行できるようになります。テクノロジープレビューとして利用可能な libusnic_verbs ドライバーにより、Verbs API に基づいた標準の InfiniBand RDMA プログラミングを介して usNIC デバイスを使用できます。(BZ#916384)

Cisco VIC カーネルドライバー

Cisco VIC Infiniband のカーネルドライバーをテクノロジープレビューとして利用できます。これにより、専用の Cisco アーキテクチャーで、RDMA (Remote Directory Memory Access) のようなセマンティックが使用可能になります。(BZ#916382)

TNC (Trusted Network Connect)

Trusted Network Connect (TNC) は、テクノロジープレビューとして利用可能で、TLS、802.1X、IPsec など既存のネットワークアクセス制御 (NAC) ソリューションと併用し、エンドポイントのポスター評価を一体化します。つまりエンドポイントのシステムの情報を収集します (オペレーティングシステムを設定している設定、インストールしているパッケージ、そのほか整合性測定と呼ばれているもの)。TNC を使用して、このような測定値をネットワークアクセスポリシーと照合してから、エンドポイントがネットワークにアクセスできるようにします。(BZ#755087)

qlcnic ドライバーの SR-IOV 機能

SR-IOV (Single-Root I/O virtualization) のサポートがテクノロジープレビューとして qlcnic ドライバーに追加されています。この機能のサポートは QLogic から直接提供されます。QLogic および Red Hat へのご意見ご感想をお寄せください。qlcnic ドライバーのその他の機能は引き続きフルサポートになります。(BZ#1259547)

libnftnl パッケージおよび nftables パッケージ

nftables パッケージおよび libnftnl パッケージは、Red Hat Enterprise Linux 7.3 以降でテクノロジープレビューとして利用できます。

nftables パッケージでは、パケットフィルターリングツールが提供され、従来のパケットフィルターリングツールに比べ、利便性、機能、および性能が数多く改善されました。これは、iptables ユーティリティー、ip6tables ユーティリティー、arptables ユーティリティー、および ebtables ユーティリティーの後継となります。

libnftnl パッケージは、libmnl ライブラリーを介して、nftables Netlink の API との低レベルの対話を行うライブラリーを提供します。(BZ#1332585)

オフロードサポートのある flower 分類子

Flower は、ユーザーがさまざまなプロトコルのよく知られているパケットフィールドで一致を設定できるようにするトラフィック制御(TC)分類子です。これは、複雑なフィルターリングおよび分類タスクの **u32** 分類子に対するルールの設定を容易にすることを目的としています。また、**Flower** は、ハードウェアがサポートしている場合に、基礎となるハードウェアに分類およびアクションルールをオフロードする機能もサポートします。**flower TC** 分類子がテクノロジープレビューとして提供されるようになりました。(BZ#1393375)

第47章 RED HAT ENTERPRISE LINUX SYSTEM ROLES POWERED BY ANSIBLE

新規パッケージ: ansible

テクノロジープレビューとして利用可能になった Red Hat Enterprise Linux システムロールは、Red Hat Enterprise Linux サブシステムの設定インターフェイスです。これにより、Ansible ロールが含まれることでシステム設定が容易になります。このインターフェイスにより、Red Hat Enterprise Linux の複数のバージョンにわたるシステム設定の管理と、新しいメジャーリリースの導入が可能になります。

Red Hat Enterprise Linux 7.4 では、Red Hat Enterprise Linux システムロールパッケージは Extras チャンネルを介して配布されています。Red Hat Enterprise Linux システムロールの詳細は、<https://access.redhat.com/articles/3050101> を参照してください。

注記:

- 現在、Ansible は Red Hat Enterprise Linux FIPS 検証プロセスの一部ではありません。今後のリリースでこれに対処したいと考えています。
- Ansible はサポート対象外のランタイム依存関係として含まれています。(BZ#1313263)

第48章 セキュリティー

テクノロジープレビューとして利用可能な **tang-nagios** サブパッケージおよび **clevis-udisk2** サブパッケージ

Red Hat Enterprise Linux Network Bound Disk Encryption (NBDE) プロジェクトの一部である **tang** および **clevis** パッケージには、**tang-nagios** および **clevis-udisk2** サブパッケージも含まれています。これらのサブパッケージは、テクノロジープレビューとしてのみ提供されます。
(BZ#1467338)

USBGuard がテクノロジープレビューとして **IBM Power** で利用可能になりました。

侵入型 USB デバイスに対するシステムプロテクションを提供する **usbguard** パッケージが利用できるようになりました。今回の更新で、**IBM Power** アーキテクチャー用の **USBGuard** ソフトウェアフレームワークがテクノロジープレビューとして提供されます。フルサポートの対象は、Red Hat Enterprise Linux の今後のリリースになります。

USB は **IBM z Systems** ではサポートされておらず、これらのシステムでは **USBGuard** フレームワークを提供することができないことに注意してください。 (BZ#1467369)

第49章 ストレージ

SCSI 向けのマルチキュー I/O スケジューリング

Red Hat Enterprise Linux 7 には、blk-mq と呼ばれるブロックデバイス用の新しいマルチキュー I/O スケジューリングメカニズムが同梱されています。scsi-mq パッケージにより、Small Computer System Interface (SCSI) サブシステムが、この新しいキューイングメカニズムを利用できるようになります。この機能はテクノロジープレビューのため、デフォルトでは有効になっていません。これを有効にするには、`scsi_mod.use_blk_mq=Y` をカーネルコマンドラインに追加します。

blk-mq は、パフォーマンスを改善するために導入されていますが (特に低レイテンシーデバイス向け)、常にパフォーマンスが改善することは保証されていません。具体的には、特に CPU が多いシステムで scsi-mq を有効にすると、パフォーマンスが大幅に低下する場合があります。(BZ#1109348)

libStorageMgmt API の Targetd プラグイン

Red Hat Enterprise Linux 7.1 から、ストレージレイから独立した API である libStorageMgmt を使用したストレージレイの管理が完全サポートされています。提供される API は安定性と整合性を備え、開発者は異なるストレージレイをプログラマ的に管理し、ハードウェアアクセラレーション機能を使用できます。また、システム管理者は libStorageMgmt を使用して手動でストレージを設定したり、コマンドラインインターフェイスを使用してストレージ管理タスクを自動化したりできます。

Targetd プラグインは完全サポートされず、引き続きテクノロジープレビューとして提供されます。(BZ#1119909)

DIF/DIX (Data Integrity Field/Data Integrity Extension) への対応

DIF/DIX は、SCSI 標準に新しく追加されたものです。これは、Red Hat Enterprise Linux 7 では、機能の章で指定されている HBA およびストレージレイに対して完全に対応していますが、その他の HBA およびストレージレイはテクノロジープレビューのままとなっています。

DIF/DIX により DIF (Data Integrity Field) が追加され、一般的に使用される 512 バイトのディスクブロックのサイズが 520 バイトに増えます。DIF は、書き込みの発生時に HBA (Host Bus Adapter) により算出されるデータブロックのチェックサム値を保存します。その後、受信時にストレージデバイスがチェックサムを確認し、データとチェックサムの両方を保存します。読み取りが発生すると、チェックサムが、ストレージデバイス、および受信する HBA により検証されます。(BZ#1072107)

第50章 仮想化

KVM ゲスト用の USB 3.0 サポート

Red Hat Enterprise Linux 7.4 では、KVM ゲスト向けの USB 3.0 ホストアダプター (xHCI) エミュレーションが引き続きテクノロジープレビューとなります。(BZ#1103193)

一部の Intel ネットワークアダプターが Hyper-V のゲストとして SR-IOV をサポート

Hyper-V で実行している Red Hat Enterprise Linux ゲスト仮想マシン用の今回の更新では、新しい PCI パススルードライバーにより、ixgbevf ドライバーでサポートされている Intel ネットワークアダプターの Single Root I/O Virtualization (SR-IOV) 機能を使用できるようになります。この機能は、以下の条件が満たされた場合に有効になります。

- ネットワークインターフェイスコントローラー (NIC) に対して SR-IOV サポートが有効になっている
- 仮想 NIC の SR-IOV サポートが有効になっている
- 仮想スイッチの SR-IOV サポートが有効になっている

NIC の VF (Virtual Function) は、仮想マシンに接続されている

この機能は現在、Microsoft Windows Server 2016 でサポートされています。(BZ#1348508)

VFIO ドライバーの No-IOMMU モード

今回の更新により、VFIO (Virtual Function I/O) ドライバーの No-IOMMU モードがテクノロジープレビューとして追加されました。No-IOMMU モードは、I/O メモリー管理ユニット (IOMMU) を使用せずに直接メモリアccess (DMA) 対応デバイスへの完全なユーザー空間 I/O (UIO) アクセスを提供します。しかし、このモードはサポートされないだけでなく、IOMMU で提供される I/O 管理機能がないため、安全に使用することができません。(BZ#1299662)

ibmvnic デバイスドライバーが追加されました。

ibmvnic デバイスドライバーは、Red Hat Enterprise Linux 7.3 for IBM POWER アーキテクチャーでテクノロジープレビューとして導入されました。vNIC (Virtual Network Interface Controller) は、エンタープライズ機能を提供し、ネットワーク管理を簡素化する新しい PowerVM 仮想ネットワークテクノロジーです。SR-IOV NIC と組み合わせると、仮想 NIC レベルで帯域幅制御サービス品質 (QoS) 機能が提供される、高性能で効率的な技術です。vNIC は、仮想化のオーバーヘッドを大幅に削減するた

め、ネットワーク仮想化に必要な CPU やメモリーなど、待機時間が短縮され、サーバーリソースが少なくなります。(BZ#947163)

virt-v2v が vmx 設定ファイルを使用して VMware ゲストを変換できるようになりました。

テクノロジープレビューとして、virt-v2v ユーティリティーに vmx 入力モードが含まれるようになりました。これにより、ユーザーはゲスト仮想マシンを VMware vmx 設定ファイルから変換できるようになりました。これを行うには、たとえば NFS を使用してストレージをマウントすることにより、対応する VMware ストレージにもアクセスする必要があることに注意してください。(BZ#1441197)

virt-v2v が Debian ゲストおよび Ubuntu ゲストを変換できる

テクノロジープレビューとして、virt-v2v ユーティリティーがゲスト仮想マシン Debian および Ubuntu を変換できるようになりました。現時点では、この変換を行うときに以下の問題が発生することに注意してください。

- virt-v2v は GRUB2 設定のデフォルトカーネルを変更できず、ゲストで設定されたカーネルは、ゲストでより最適なバージョンのカーネルが利用可能であっても、変換中には変更されません。
- Debian または Ubuntu の VMware ゲストを KVM に変換すると、ゲストのネットワークインターフェイス名が変更し、手動での設定が必要になる場合があります。(BZ#1387213)

Virtio デバイスでの vIOMMU の使用が可能に

テクノロジープレビューとして、この更新により、virtio デバイスは仮想入出力メモリー管理ユニット (vIOMMU) を使用できるようになります。これにより、デバイスが許可されたアドレスにのみ Direct Memory Access (DMA) を実行できるようになるため、DMA のセキュリティーが保証されます。ただし、この機能を使用できるのは、Red Hat Enterprise Linux 7.4 以降を使用するゲスト仮想マシンのみであることに注意してください。(BZ#1283251, BZ#1464891)

OVMF (Open Virtual Machine Firmware)

Red Hat Enterprise Linux 7 では、OVMF (Open Virtual Machine Firmware) がテクノロジープレビューとして利用できます。OVMF は、AMD64 および Intel 64 ゲストに対する、UEFI のセキュアブート環境です。ただし、OVMF は、RHEL 7 で利用可能な仮想化コンポーネントでは起動できません。OVMF は、RHEL 8 で完全に対応することに注意してください。(BZ#653382)

パート IV. デバイスドライバー

ここでは、Red Hat Enterprise Linux 7.4 で新規または更新されたすべてのデバイスドライバーの包括的な一覧を提供します。

第51章 新しいドライバー

ストレージドライバー

- `nvme-fabrics`
- `nvme-rdma`
- `nvmet`
- `nvmet-rdma`
- `nvme-loop`
- `qedi`
- `qedf`

ネットワークドライバー

- `qedr`
- `rdma_rxe`
- `ntb_transport`
- `ntb_perf`
- `mdev`
- `vfio_mdev`

- **amd-xgbe**
- **atlantic**
- **libcxgb**
- **ena**
- **rocker**
- **amd8111e**
- **nfp**
- **mlxsw_core**
- **mlxsw_i2c**
- **mlxsw_spectrum**
- **mlxsw_pci**
- **mlxsw_switchx2**
- **mlxsw_switchib**
- **mlxsw_minimal**

グラフィックスドライバーおよびその他のドライバー

- `ccp`
- `chcr`
- `uio_hv_generic`
- `usbip-core`
- `vhost_vsock`
- `tpm_tis_spi`
- `gpio-amdpt`
- `joydev`
- `sdio_uart`
- `ptp_kvm`
- `mei_wdt`
- `dell-rbtn`
- `dell-smo8800`
- `intel-hid`

- **dell-smbios**
- **skx_edac**
- **kvmgt**
- **pinctrl-intel**
- **pinctrl-sunrisepoint**
- **pinctrl-amd**
- **dax_pmem**
- **DAX**
- **nfit**
- **ledtrig-usbport**

第52章 更新されたドライバー

ストレージドライバーの更新

- aacraid ドライバーがバージョン 1.2.1[50792]-custom に更新されました。
- lpfc ドライバーがバージョン 0:11.2.0.6 に更新されました。
- vmw_pvscsi ドライバーがバージョン 1.0.7.0-k に更新されました。
- megaraid_sas ドライバーがバージョン 07.701.17.00-rh1 に更新されました。
- bfa ドライバーがバージョン 3.2.25.1 に更新されました。
- hpsa ドライバーがバージョン 3.4.18-0-RH1 に更新されました。
- be2iscsi ドライバーがバージョン 11.2.1.0 に更新されました。
- qla2xxx ドライバーがバージョン 8.07.00.38.07.4-k1 に更新されました。
- mpt2sas ドライバーがバージョン 20.103.00.00 に更新されました。
- mpt3sas ドライバーがバージョン 15.100.00.00 に更新されました。

ネットワークドライバーの更新

- ntb ドライバーがバージョン 1.0 に更新されました。
- igbvf ドライバーがバージョン 2.4.0-k に更新されました。
- igb ドライバーがバージョン 5.4.0-k に更新されました。

- ixgbevf ドライバーがバージョン 3.2.2-k-rh7.4 に更新されました。
- i40e ドライバーがバージョン 1.6.27-k に更新されました。
- fm10k ドライバーがバージョン 0.21.2-k に更新されました。
- i40evf ドライバーがバージョン 1.6.27-k に更新されました。
- ixgbe ドライバーがバージョン 4.4.0-k-rh7.4 に更新されました。
- be2net ドライバーがバージョン 11.1.0.0r に更新されました。
- qede ドライバーがバージョン 8.10.10.21 に更新されました。
- qlge ドライバーがバージョン 1.00.00.35 に更新されました。
- qed ドライバーがバージョン 8.10.10.21 に更新されました。
- bna ドライバーがバージョン 3.2.25.1r に更新されました。
- bnxt ドライバーがバージョン 1.7.0 に更新されました。
- enic ドライバーがバージョン 2.3.0.31 に更新されました。
- fjes ドライバーがバージョン 1.2 に更新されました。
- hpwdt ドライバーがバージョン 1.4.02 に更新されました。

グラフィックドライバーおよびその他のドライバーの更新

- **vmwgfx** ドライバーがバージョン **2.12.0.0** に更新されました。
- **hpilo** ドライバーがバージョン **1.5.0** に更新されました。

パート V. 非推奨の機能

ここでは、Red Hat Enterprise Linux 7.4 までのすべてのマイナーリリースで非推奨になった機能の概要を説明します。

非推奨の機能は、Red Hat Enterprise Linux 7 のライフサイクルが終了するまでサポートされます。非推奨の機能は、本製品の今後のメジャーリリースではサポートされない可能性が高く、新たに実装することは推奨されません。特定のメジャーリリースにおける非推奨機能の最新情報は、そのメジャーリリースの最新バージョンのリリースノートを参照してください。

現行および今後のメジャーリリースでは、非推奨のハードウェア コンポーネントの新規実装は推奨されません。ハードウェアドライバの更新は、セキュリティと重大な修正にのみ行われます。Red Hat は、このようなハードウェアの早期交換をお勧めします。

パッケージが非推奨となり、使用の継続が推奨されない場合があります。製品からパッケージが削除されることもあります。その場合には、製品のドキュメントで、非推奨となったパッケージと同様、同一、またはより高度な機能を提供する最近のパッケージが指定され、詳しい推奨事項が記載されます。

第53章 RED HAT ENTERPRISE LINUX 7 での非推奨の機能

Identity Management に関連する非推奨のパッケージ

以下のパッケージは非推奨となり、Red Hat Enterprise Linux の今後のメジャーリリースには含まれません。

非推奨パッケージ	代替として提案されるパッケージまたは製品
authconfig	authselect
pam_pkcs11	sssd [a]
pam_krb5	sssd [b]
openldap-servers	ユースケースに応じて、Red Hat Enterprise Linux に同梱されている Identity Management または Red Hat Directory Server に移行します。 [c]

[a] SSSD (System Security Services Daemon) には、拡張スマートカード機能が含まれています。

[b] pam_krb5 から sssd への移行の詳細については、Red Hat カスタマーポータルナレッジベースの記事 [How to migrate from pam_krb5 to SSSD](#) を参照してください。

[c] Red Hat Directory Server には、有効な Directory Server サブスクリプションが必要です。

非推奨の安全でないアルゴリズムとプロトコル

暗号化ハッシュと暗号化、および暗号化プロトコルを提供するアルゴリズムには使用可能な期間があり、それを過ぎるとリスクが高すぎるか、または安全でないとみなされます。詳細は、Red Hat カスタマーポータルナレッジベースの記事 [Enhancing the Security of the Operating System with Cryptography Changes in Red Hat Enterprise Linux 7.4](#) を参照してください。

OpenSSHでは

今回の更新で、OpenSSH ライブラリーは、デフォルト設定からいくつかの弱い暗号とアルゴリズムを削除します。ただし、ほとんどの場合、後方互換性は保証されています。

OpenSSH サーバーおよびクライアントから以下が削除されました。

- ホスト鍵アルゴリズム

- **ssh-rsa-cert-v00@openssh.com**

- **ssh-dss-cert-v00@openssh.com**

- **暗号:**

- **arcfour256**

- **arcfour128**

- **arcfour**

- **rijndael-cbc@lysator.liu.se**

- **MACs:**

- **hmac-md5**

- **hmac-md5-96**

- **hmac-md5-96-etm@openssh.com**

- **hmac-md5-etm@openssh.com**

- `hmac-ripemd160`
- `hmac-ripemd160-etm@openssh.com`
- `hmac-ripemd160@openssh.com`
- `hmac-sha1-96`
- `hmac-sha1-96-etm@openssh.com`

OpenSSH クライアントから以下が削除されました。

- 暗号:
 - `blowfish-cbc`
 - `cast128-cbc`
 - `3des-cbc`

OpenSSH は

今回の更新で、FIPS モードのデフォルトリストから SHA-1 ベースの鍵交換アルゴリズムが削除されました。これらのアルゴリズムを有効にするには、`~/.ssh/config` および `/etc/ssh/sshd_config` ファイルに以下の設定スニペットを使用します。

```
KexAlgorithms=+diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1
```

SSH-1 プロトコルが OpenSSH サーバー から削除されました(

SSH-1 プロトコルサポートは OpenSSH サーバーから削除されました。詳細は、[The server-side SSH-1 protocol removal from RHEL 7.4](#) のナレッジベースの記事を参照してください。

MD5

今回の更新で、証明書、証明書失効リスト (CRL) およびメッセージ署名における MD5、MD4、および SHA0 の署名の検証へのサポートが削除されました。

また、デジタル署名を生成するデフォルトのアルゴリズムが SHA-1 から SHA-256 に変更されました。SHA-1 署名の検証は、レガシー目的で引き続き有効になっています。

システム管理者は、`etc/pki/tls/legacy-settings` ポリシー設定ファイルの `LegacySigningMDs` オプションを変更することで、MD5、MD4、または SHA0 サポートを有効にできます。以下に例を示します。

```
echo 'LegacySigningMDs algorithm' >> /etc/pki/tls/legacy-settings
```

複数のレガシーアルゴリズムを追加するには、新しい行を除いて、コンマまたは任意の空白文字を使用します。詳細は、OpenSSL パッケージの `README.legacy-settings` ファイルを参照してください。

`OPENSSL_ENABLE_MD5_VERIFY` 環境変数を設定して MD5 検証を有効にする こともできます。

OpenSSL クライアントは

今回の更新で、OpenSSL クライアントが 1024 ビットより短い Diffie-Hellman (DH) パラメーターを使用してサーバーに接続できなくなりました。これにより、OpenSSL を使用するクライアントが Logjam などの脆弱性の影響を受けにくくなります。

システム管理者は、`/etc/pki/tls/legacy-settings` の `MinimumDHBits` オプションを変更することで、より短い DH パラメーターサポートを有効にできます。以下に例を示します。

```
echo 'MinimumDHBits 768' > /etc/pki/tls/legacy-settings
```

このオプションは、システム管理者が必要とする場合に、最小値を上げるためにも使用できません。

SSL 2.0 のサポートが OpenSSL から完全に削除されました

7 年以上にわたって安全でないと考えられていた SSL プロトコルバージョン 2.0 は、2011 年に RFC 6176 により非推奨となりました。Red Hat Enterprise Linux では、SSL 2.0 のサポートはデフォルトですでに無効になっています。今回の更新で、SSL 2.0 のサポートが完全に削除されました。このプロトコルバージョンを使用する OpenSSL ライブラリー API コールは、エラーメッセージを返すようになりました。

OpenSSL の EXPORT 暗号スイートが非推奨になりました。

この変更により、OpenSSL ツールキットから EXPORT 暗号スイートのサポートが削除されます。これらの弱い暗号スイートを無効にすると、OpenSSL を使用するクライアントが FREAK などの脆弱性の影響を受けにくくなります。EXPORT 暗号スイートは、TLS プロトコル設定で不要になりました。

GnuTLS クライアントは

この変更により、GNU Transport Layer Security (GnuTLS) クライアントが 1024 ビットより短い Diffie-Hellman (DH) パラメーターを持つサーバーに接続できなくなりました。これにより、GnuTLS を使用するクライアントが Logjam などの脆弱性の影響を受けにくくなります。

ユーザーまたは設定から優先度文字列を直接受け入れるアプリケーションでは、使用されている優先度文字列に優先度文字列 `%PROFILE_VERY_WEAK` を追加することで、この変更を元に戻すことができます。

TLS を使用する NSS クライアントは

この変更により、Network Security Services (NSS) クライアントが 1024 ビットより短い Diffie-Hellman (DH) パラメーターを持つサーバーに接続できなくなります。これにより、NSS を使用するクライアントが Logjam などの脆弱性の影響を受けにくくなります。

システム管理者は、`/etc/pki/nss-legacy/nss-rhel7.config` ポリシー設定ファイルを変更して、より短い DH パラメーターサポートを有効にできます。

```
library=  
name=Policy  
NSS=flags=policyOnly,moduleDB  
config="allow=DH-MIN=767:DSA-MIN=767:RSA-MIN=767"
```

ファイルの最後に空の行が必要であることを注意してください。

NSS の EXPORT 暗号スイートが非推奨になりました。

この変更により、Network Security Services (NSS) ライブラリーの EXPORT 暗号スイートのサポートが削除されます。これらの弱い暗号スイートを無効にすると、FREAK などの脆弱性から保護されます。EXPORT 暗号スイートは、TLS プロトコル設定では必要ありません。

ca-certificates パッケージから削除されたレガシー CA 証明書

以前は、古いバージョンの GnuTLS、OpenSSL、および glib-networking ライブラリーが公開鍵インフラストラクチャー(PKI)との互換性を維持できるように、ca-certificates パッケージには 1024 ビット RSA 鍵のレガシー CA 証明書のセットがデフォルトで信頼されるように含まれていました。

Red Hat Enterprise Linux 7.4 以降、OpenSSL、GnuTLS、および glib-networking の更新バージョンが利用可能になり、ルート CA 証明書の置き換えを正しく識別できます。パブリック Web PKI の互換性の場合、これらのレガシー CA 証明書を信頼することは不要になりました。

以前は、レガシー CA 証明書を無効にするために使用できたレガシー設定メカニズムは、サポートされなくなりました。レガシー CA 証明書のリストが空に変更されました。

ca-legacy ツールは引き続き利用でき、今後再利用できるように現在の設定も維持されます。

coolkey が opensc に置き換えられる

OpenSC ライブラリーは PKCS#11 API を実装し、coolkey パッケージを置き換えます。Red Hat Enterprise Linux 7 では、CoolKey Applet 機能も opensc パッケージにより提供されます。

coolkey パッケージは、Red Hat Enterprise Linux 7 の有効期間中サポートされ続けますが、新しいハードウェアの有効化は、opensc パッケージで提供されます。

rsyslog imudp モジュールの inputname オプションが非推奨に

`rsyslog` サービスの `imudp` モジュールの `inputname` オプションが非推奨になりました。代わりに `name` オプションを使用してください。

FedFS が非推奨に

アップストリームの FedFS プロジェクトが積極的に保守されなくなったため、FedFS (Federated File System) が非推奨となりました。Red Hat は、FedFS インストールを移行して `autofs` を使用することを推奨します。これにより、柔軟な機能が提供されます。

Btrfs が非推奨に

Btrfs ファイルシステムは、Red Hat Enterprise Linux 6 の初期リリース以降、テクノロジープレビュー状態になっています。Red Hat は、Btrfs を完全にサポートされる機能に移行せず、Red Hat Enterprise Linux の今後のメジャーリリースで削除される予定です。

Btrfs ファイルシステムは、Red Hat Enterprise Linux 7.4 のアップストリームから多くの更新を受け取り、Red Hat Enterprise Linux 7 シリーズで引き続き利用できます。ただし、この機能に対する更新はこれで最後となる予定です。

tcp_wrappers が非推奨に

`tcp_wrappers` パッケージ。ライブラリーと、`systat`、`finger`、`FTP`、`telnet`、`rlogin`、`rlogin`、`rsh`、`exec`、`fttp`、`tquit`、および他のネットワークサービスに対する着信要求を監視およびフィルターリングできる小さなデーモンプログラムを提供します。

nautilus-open-terminal が gnome-terminal-nautilus に置き換えられる

Red Hat Enterprise Linux 7.3 以降、`nautilus-open-terminal` パッケージは非推奨になり、`gnome-terminal-nautilus` パッケージに置き換えられました。このパッケージは、Nautilus で右クリックコンテキストメニューに `Open in Terminal` オプションを追加する Nautilus 拡張機能を提供します。システムアップグレード中、`nautilus-open-terminal` は `gnome-terminal-nautilus` に置き換えられます。

Pythonから削除された `sslwrap ()`

`sslwrap ()` 関数は Python 2.7 から削除されました。[466 Python Enhancement Proposal](#) が実装されて以降、この機能を使用するとセグメンテーションフォールトになります。この削除は、アップストリームと一致しています。

Red Hat は、代わりに `ssl.SSLContext` クラスと `ssl.SSLContext.wrap_socket ()` 関数を使用することを推奨します。ほとんどのアプリケーションは、`ssl.create_default_context ()` 関数を使用す

るだけで、安全なデフォルト設定でコンテキストを作成できます。デフォルトのコンテキストでは、システムのデフォルトのトラストストアが使用されます。

依存関係としてリンクされたライブラリーのシンボルが `ld` によって解決されない

以前は、一部のライブラリーが他のライブラリーの依存関係として暗示的にしかリンクされていない場合でも、リンクされたライブラリーに存在するシンボルをすべて `ld` リンカーが解決していました。そのため、開発者が暗示的にリンク付けされたライブラリーのシンボルをアプリケーションコードに使用するのに、これらのライブラリーのリンクを明示的に指定する必要はありませんでした。

セキュリティ上の理由から、`ld` は、依存関係として暗黙的にリンクされたライブラリーのシンボルへの参照を解決しないように変更されました。

その結果、アプリケーションコードがリンクを宣言せず、依存関係として暗黙的にリンク付けされていないライブラリーからのシンボルを使用しようとすると、`ld` とのリンクに失敗します。依存関係としてリンク付けされたライブラリーのシンボルを使用する場合、開発者はこれらのライブラリーとも明示的にリンク付けする必要があります。

`ld` の以前の動作を復元するには、コマンドラインオプション `-copy-dt-needed-entries` を使用します。(BZ#[1292230](#))

Windows ゲスト仮想マシンのサポートが限定

Red Hat Enterprise Linux 7 以降、Windows ゲスト仮想マシンは、Advanced Mission Critical (AMC) などの特定のサブスクリプションプログラムにおいてのみサポートされています。

`libnetlink` が非推奨に

`iproute-devel` パッケージに含まれる `libnetlink` ライブラリーが非推奨になりました。代わりに `libnl` ライブラリーおよび `libmnl` ライブラリーを使用する必要があります。

KVM の S3 および S4 の電源管理状態が非推奨に

S3 (Suspend to RAM) および S4 (Suspend to Disk) の電源管理状態に対する KVM のネイティブサポートが廃止されました。この機能は、以前はテクノロジープレビューとして提供されていました。

Certificate Server の `udnPwdDirAuth` プラグインが廃止

Red Hat Certificate Server の `udnPwdDirAuth` 認証プラグインは、Red Hat Enterprise Linux 7.3 で削除されました。このプラグインを使用するプロファイルはサポートされなくなりまし

た。udnPwdDirAuth プラグインを使用してプロファイルで作成された証明書は、承認されている場合は引き続き有効です。

IdM 向けの Red Hat Access プラグインが廃止

Red Hat Enterprise Linux 7.3 で、Identity Management (IdM) 向けの Red Hat Access プラグインが廃止されました。更新中に、redhat-access-plugin-ipa が自動的にアンインストールされます。ナレッジベースへのアクセスやサポートケースエンゲージメントなど、このプラグインにより提供されていた機能は、Red Hat カスタマーポータルで引き続き利用できます。Red Hat は、redhat-support-tool ツールなどの代替手段を確認することを推奨します。

統合方式のシングルサインオン向けの Ipsilon 認証プロバイダーサービス

ippsilon パッケージは、Red Hat Enterprise Linux 7.2 でテクノロジープレビューとして導入されました。Ipsilon は認証プロバイダーと、アプリケーションまたはユーティリティーをリンクして、シングルサインオン (SSO) を可能にします。

Red Hat は、テクノロジープレビューの Ipsilon を、完全にサポートされる機能にアップグレードする予定はありません。ippsilon パッケージは、今後のマイナーリリースで Red Hat Enterprise Linux から削除される予定です。

Red Hat は、Keycloak コミュニティープロジェクトをベースとした Web SSO ソリューションとして Red Hat Single Sign-On をリリースしました。Red Hat Single Sign-On は、Ipsilon よりも優れた機能を提供し、Red Hat の製品ポートフォリオ全体の標準 Web SSO ソリューションとして設計されています。

rsyslog のいくつかのオプションが非推奨に

Red Hat Enterprise Linux 7.4 の rsyslog ユーティリティーバージョンでは、多くのオプションが非推奨になりました。これらのオプションは有効ではなくなり、警告が表示されます。

- -c、-u、-q、-x、-A、-Q、-4、および -6 のオプションが以前提供していた機能は、rsyslog 設定を使用して実現できます。
- -l オプションおよび -s ありません。

memkind ライブラリーで非推奨のシンボル

memkind ライブラリーで、以下のシンボルが非推奨になりました。

- `memkind_finalize()`
- `memkind_get_num_kind()`
- `memkind_get_kind_by_partition()`
- `memkind_get_kind_by_name()`
- `memkind_partition_mmap()`
- `memkind_get_size()`
- `MEMKIND_ERROR_MEMALIGN`
- `MEMKIND_ERROR_MALLCTL`
- `MEMKIND_ERROR_GETCPU`
- `MEMKIND_ERROR_PMTT`
- `MEMKIND_ERROR_TIEDISTANCE`
- `MEMKIND_ERROR_ALIGNMENT`
- `MEMKIND_ERROR_MALLOCX`
- `MEMKIND_ERROR_REPNAME`

- `MEMKIND_ERROR_PTHREAD`
- `MEMKIND_ERROR_BADPOLICY`
- `MEMKIND_ERROR_REPPOLICY`

SCTP (RFC 6458) のソケットの API 拡張オプションが非推奨に

Stream Control Transmission Protocol のソケット API 拡張機能の `SCTP_SNDRCV` オプション、`SCTP_EXTRCV` オプション、および `SCTP_DEFAULT_SEND_PARAM` オプションは、RFC 6458 仕様に従って非推奨になりました。

非推奨のオプションの代わりに、`SCTP_SNDINFO`、`SCTP_NXTINFO`、`SCTP_NXTINFO`、および `SCTP_DEFAULT_SNDINFO` が実装されています。

SSLv2 および SSLv3 を使用した NetApp ONTAP の管理は、`libstorageMgmt` ではサポートされなくなりました。

NetApp ONTAP ストレージレイへの SSLv2 および SSLv3 接続は、`libstorageMgmt` ライブラリーではサポートされなくなりました。ユーザーは、NetApp サポートに連絡して Transport Layer Security (TLS) プロトコルを有効にすることができます。

`dconf-dbus-1` が非推奨になり、`dconf-editor` が個別に提供されるようになりました。

今回の更新で、`dconf-dbus-1` API が削除されました。ただし、バイナリー互換性を維持するために `dconf-dbus-1` ライブラリーがバックポートされています。Red Hat は、`dconf-dbus-1` の代わりに GDBus ライブラリーを使用することを推奨します。

`dconf-error.h` ファイルの名前が `dconf-enums.h` に変更されました。さらに、`dconf Editor` が別の `dconf-editor` パッケージで提供されるようになりました。詳細は、[8章 デスクトップ](#) を参照してください。

FreeRADIUS が `Auth-Type := System` を受け入れなくなりました。

FreeRADIUS サーバーは、`rlm_unix` 認証モジュールの `Auth-Type := System` オプションを受け入れなくなりました。このオプションは、設定ファイルの `authorize` セクションで `unix` モジュールを使用することに置き換えられました。

非推奨となったデバイスドライバー

- **3w-9xxx**
- **3w-sas**
- **mptbase**
- **mptctl**
- **mptsas**
- **mptscsih**
- **mptspi**
- **mvsas**
- **qla3xxx**
- **megaraid_sas** ドライバーの以下のコントローラーが非推奨になりました。
 - **Dell PERC5, PCI ID 0x15**
 - **SAS1078R, PCI ID 0x60**
 - **SAS1078DE, PCI ID 0x7C**

- SAS1064R, PCI ID 0x411
- VERDE_ZCR, PCI ID 0x413
- SAS1078GEN2, PCI ID 0x78
- qla2xxx ドライバーで、次のアダプターが非推奨になりました。
 - ISP24xx, PCI ID 0x2422
 - ISP24xx, PCI ID 0x2432
 - ISP2422, PCI ID 0x5422
 - QLE220, PCI ID 0x5432
 - QLE81xx, PCI ID 0x8001
 - QLE10000, PCI ID 0xF000
 - QLE84xx, PCI ID 0x8044
 - QLE8000, PCI ID 0x8432
 - QLE82xx, PCI ID 0x8021
- be2net ドライバーが制御する次のイーサネットアダプターが非推奨になりました。

- **TIGERSHARK NIC, PCI ID 0x0700**
- **be2iscsi ドライバーの以下のコントローラーが非推奨になりました。**
 - **Emulex OneConnect 10Gb iSCSI イニシエーター (一般)、PCI ID 0x212**
 - **OCe10101、OCm10101、OCe10102、OCm10102 BE2 アダプターファミリー、PCI ID 0x702**
 - **OCe10100 BE2 アダプターファミリー、PCI ID 0x703**
- **lpfc ドライバーの以下の Emulex ボードが非推奨になりました。**

BladeEngine 2 (BE2) デバイス

- **TIGERSHARK FCOE, PCI ID 0x0704**

ファイバーチャネル (FC) デバイス

- **FIREFLY, PCI ID 0x1ae5**
- **PROTEUS_VF, PCI ID 0xe100**
- **BALIUS, PCI ID 0xe131**
- **PROTEUS_PF, PCI ID 0xe180**
- **RFLY, PCI ID 0xf095**

- PFLY, PCI ID 0xf098
- LP101, PCI ID 0xf0a1
- TFLY, PCI ID 0xf0a5
- BSMB, PCI ID 0xf0d1
- BMID, PCI ID 0xf0d5
- ZSMB, PCI ID 0xf0e1
- ZMID, PCI ID 0xf0e5
- NEPTUNE, PCI ID 0xf0f5
- NEPTUNE_SCSP, PCI ID 0xf0f6
- NEPTUNE_DCSP, PCI ID 0xf0f7
- FALCON, PCI ID 0xf180
- SUPERFLY, PCI ID 0xf700
- DRAGONFLY, PCI ID 0xf800
- CENTAUR, PCI ID 0xf900

- **PEGASUS, PCI ID 0xf980**
- **THOR, PCI ID 0xfa00**
- **VIPER, PCI ID 0xfb00**
- **LP10000S, PCI ID 0xfc00**
- **LP11000S, PCI ID 0xfc10**
- **LPE11000S, PCI ID 0xfc20**
- **PROTEUS_S, PCI ID 0xfc50**
- **HELIOS, PCI ID 0xfd00**
- **HELIOS_SCSP, PCI ID 0xfd11**
- **HELIOS_DCSP, PCI ID 0xfd12**
- **ZEPHYR, PCI ID 0xfe00**
- **HORNET, PCI ID 0xfe05**
- **ZEPHYR_SCSP, PCI ID 0xfe11**
- **ZEPHYR_DCSP, PCI ID 0xfe12**

システムでハードウェアの PCI ID を確認するには、`lspci -nn` コマンドを実行します。

上述のドライバーのうち、ここに記載されていないその他のコントローラーには変更はありません。

SFN4XXX アダプターが非推奨に

Red Hat Enterprise Linux 7.4 以降、SFN4XXX Solarflare ネットワークアダプターが非推奨となっています。以前は、Solarflare のすべてのアダプターに単一のドライバー `sfc` が含まれていました。最近、SFN4XXX のサポートは `sfc` から分割され、`sfc-falcon` と呼ばれる新しい SFN4XXX のみのドライバーに移動しました。現時点では、両方のドライバーは引き続きサポートされますが、`sfc-falcon` および SFN4XXX のサポートは今後のメジャーリリースで削除される予定です。

Software-initiated-only FCoE ストレージ技術が非推奨に

Fibre Channel over Ethernet (FCoE) ストレージ技術の `software-initiated-only` 部分は、広く使用されなかったため非推奨となりました。`software-initiated-only` ストレージ技術は、Red Hat Enterprise Linux 7 のライフサイクル期間中はサポートされます。非推奨化の通知では、Red Hat Enterprise Linux の今後のメジャーリリースでは `software-initiated` ベースの FCoE がサポートされない意向が示されています。ハードウェアサポートと関連するユーザー空間ツール（ドライバー、`libfc`、`libfcOE`など）は、この非推奨通知の影響を受けないことに注意してください。

libvirt-lxc ツールを使用するコンテナが非推奨に

以下の `libvirt-lxc` パッケージは、Red Hat Enterprise Linux 7.1 以降で非推奨になりました。

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

Linux コンテナフレームワークでの今後の開発は、`docker` コマンドラインインターフェイスをベースにしています。`libvirt-lxc` ツールは今後の Red Hat Enterprise Linux リリース (Red Hat Enterprise Linux 7 を含む) からは削除される可能性があるため、カスタムなコンテナ管理アプリケーションを開発する際には依存しないようにしてください。

詳細は、[Red Hat KnowledgeBase article](#) を参照してください。

パート VI. 既知の問題

ここでは、Red Hat Enterprise Linux 7.4 の既知の問題について説明します。

第54章 認証および相互運用性

グループルックアップの実行時に `sudo` がアクセスを拒否する

この問題は、以下のすべての条件を満たすシステムで発生します。

- グループ名は、`files` や `sss` などの複数の Name Service Switch (NSS) ソースで利用可能な `sudoers` ルールで設定されます。
- NSS の優先度は、ローカルグループ定義に設定されます。これは、`/etc/nsswitch.conf` ファイルに以下の行が含まれている場合に当てはまります。

```
sudoers: files sss
```

- `match_group_by_gid` という名前の `sudo Defaults` オプションは `true` に設定されます。これは、オプションのデフォルト値です。

NSS ソースの優先度により、`sudo` ユーティリティーが指定されたグループの `GID` を検索しようとすると、`sudo` はローカルグループ定義のみを説明する結果を受け取ります。したがって、ユーザーがリモートグループのメンバーであるが、ローカルグループのメンバーではない場合、`sudoers` ルールは一致せず、`sudo` はアクセスを拒否します。

この問題を回避するには、以下のいずれかを実行します。

- `sudoers` の `match_group_by_gid` デフォルトを明示的に無効にします。`/etc/sudoers` ファイルを開き、以下の行を追加します。

```
Defaults !match_group_by_gid
```

- ファイルよりも `sss` NSS ソースを優先するように NSS を設定します。`/etc/nsswitch.conf` ファイルを開き、`files` の前に `sss` がリストされていることを確認します。

```
sudoers: sss files
```

これにより、`sudo` はリモートグループに属するユーザーへのアクセスを許可します。(BZ#1293306)

KCM 認証情報キャッシュは、1つの認証情報キャッシュ内で多数の認証情報を行うには適していない

認証情報キャッシュに含まれる認証情報が多すぎると、`sssd-kcm` コンポーネントと `sssd-secrets` コンポーネント間でデータを転送するために使用されるバッファーにハードコードされた制限があるため、`klist` などの Kerberos 操作は失敗します。

この問題を回避するには、`/etc/sss/sss.conf` ファイルの `[kcm]` セクションに `ccache_storage = memory` オプションを追加します。これにより、`kcm` レスポンダーが、認証情報キャッシュを永続的ではなく、メモリー内にのみ保存するように指示されます。これを実行すると、システムを再起動するか、`sssd-kcm` により認証情報キャッシュがクリアされることに注意してください。(BZ#1448094)

`sssd-secrets` コンポーネントは、読み込み中にクラッシュする

`sssd-secrets` コンポーネントが多くの要求を受信すると、`Network Security Services (NSS)` ライブラリーのバグがトリガーされ、`sssd-secrets` が予期せず終了します。ただし、`systemd` サービスは次の要求に対して `sssd-secrets` を再起動します。つまり、サービス拒否は一時的なものです。(BZ#1460689)

SSSD が同じ優先順位を持つ複数の証明書一致ルールを正しく処理しません。

指定した証明書が、優先順位が同じ複数の証明書の一致ルールに一致する場合、`System Security Services Daemon (SSSD)` は、いずれか一方のみを使用します。回避策として、`LDAP` フィルターが | (または) 演算子と連結した個々のルールのフィルターで設定される単一の証明書マッチングルールを使用します。証明書一致ルールの例は、`man` ページの `sss-certamp (5)` を参照してください。(BZ#1447945)

SSSD は、ID オーバーライドで一意的な証明書のみを検索できる

複数の ID オーバーライドに同じ証明書が含まれる場合、`SSSD (System Security Services Daemon)` は証明書に一致するユーザーのクエリーを解決できません。これらのユーザーを検索しようとしても、ユーザーは返されません。ユーザー名または `UID` を使用してユーザーを検索すると、期待通りに機能します。(BZ#1446101)

`ipa-adviser` コマンドは、スマートカード認証を完全に設定しません。

`ipa-adviser config-server-for-smart-card-auth` コマンドおよび `ipa-adviser config-client-for-smart-card-auth` コマンドは、スマートカード認証用に `Identity Management (IdM)` サーバーおよびクライアントを完全に設定しません。これにより、`ipa-adviser` コマンドが生成したスクリプトを実行すると、スマートカード認証が失敗します。この問題を回避するには、`Linux Domain Identity, Authentication, and Policy Guide` の個々のユースケースの手動による手順 https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/smart-cards.html を参照してください。(BZ#1455946)

`libwbclient` ライブラリーが、`Red Hat Enterprise Linux 7.4` でホストされる `Samba` 共有に接続できない

`Samba` と `System Security Services Daemon (SSSD)` の `Winbind` プラグインの実装間のインター

フェイスが変更されました。ただし、SSSD ではこの変更が欠けています。これにより、Winbind デーモンの代わりに SSSD libwbclient ライブラリーを使用するシステムは、Red Hat Enterprise Linux 7.4 で実行している Samba が提供する共有にアクセスできなくなります。利用可能な回避策はありません。Winbind デーモンを実行せずに libwbclient ライブラリーを使用している場合は、Red Hat Enterprise 7.4 にアップグレードしないことを推奨します。(BZ#1462769)

Certificate System subsystem で、TLS_ECDHE_RSA_* 暗号および特定の HSM で通信の問題が発生しました。

TLS_ECDHE_RSA_* 暗号が有効な場合に特定の HSM を使用すると、サブシステムで通信の問題が発生します。この問題は、以下のシナリオで発生します。

- CA がインストールされた後、2 番目のサブシステムをインストールする際に、セキュリティドメインとして CA にコンタクトしようとするため、正常にインストールすることができません。
- CA で証明書登録を実行している最中にアーカイブが必要になると、CA が KRA と同じ通信問題に遭遇します。このシナリオは、問題のある暗号がインストールで一時的に無効になっている場合に限り発生します。

この問題を回避するには、可能な場合は TLS_ECDHE_RSA_* 暗号をオフのままにします。Perfect Forward Secrecy は、TLS_ECDHE_RSA_* 暗号を使用してセキュリティを強化しますが、各 SSL セッションの確立には約 3 倍の時間がかかることに注意してください。また、Certificate System の操作には、デフォルトの TLS_RSA_* 暗号で十分です。(BZ#1256901)

第55章 コンパイラーおよびツール

実行可能スタックが無効になっていると、JIT 技術で正規表現のパフォーマンスを向上できません。

SELinux ポリシーが実行スタックを許可しないと、PCRE ライブラリーは JIT コンパイルを使用して正規表現を高速化できません。その結果、正規表現に対する JIT コンパイラーの試行は無視され、パフォーマンスが向上しません。

この問題を回避するには、影響を受ける SELinux ドメインで `execmem` アクションを有効にするルールで SELinux ポリシーを修正し、JIT コンパイルを有効にします。一部のルールはすでに提供されており、特定の SELinux ブール値で有効にできます。ブール値の一覧を表示するには、以下のコマンドの出力を参照してください。

```
getsebool -a | grep execmem
```

別の回避策は、`pcre_study ()` 関数への呼び出しで JIT コンパイルを要求しないようにアプリケーションコードを変更することです。(BZ#1290432)

Gluster ライブラリーをアンロードした後、特定のアプリケーションが終了しない場合、メモリーリークが発生する

Gluster は、多くの内部コンポーネントと、関数や機能を実装するさまざまなトランスレーターで設定されています。Gluster をアプリケーションと密接に統合するために、`gfapi` アクセスメソッドが追加されました。ただし、すべてのコンポーネントおよびトランスレーターが、実行中のアプリケーションでアンロードできるように設計されているわけではありません。そのため、Gluster ライブラリーのアンロード後に終了しないプログラムは、Gluster が内部的に実行しているメモリー割り当ての一部を解放できません。

メモリーリークの量を減らすために、アプリケーションが可能な限り `glfs_init ()` および `glfs_fini ()` 関数を呼び出さないようにします。リークしたメモリーを解放するには、長時間実行しているアプリケーションを再起動する必要があります。(BZ#1409773)

DISA SRG への URL が正しくない

SCAP Security Guide (SSG) ルールは、米国国防情報システム局セキュリティ要件ガイド (DISA SRG) を参照しています。URL への接続に失敗し、404 - not found エラーが表示されます。そのため、ユーザーは SRG を直接参照することができません。この問題を回避するには、新しい URL を使用します。<http://iase.disa.mil/stig/os/general/Pages/index.aspx/> (BZ#1464899)

`ensure_gpgcheck_repo_metadata` ルールが失敗する

`ensure_gpgcheck_repo_metadata` ルールの修復中に、特定のプロファイルは `yum.conf` ファイルを更新して `repo_gpgcheck` オプションを有効にします。Red Hat は現在、署名付きリポジトリメタデータを提供していません。これにより、`yum` ユーティリティーは、公式リポジトリからパッケージをインストールできなくなりました。この問題を回避するには、テーラリングファイルを使用して、

プロファイルから `ensure_gpgcheck_repo_metadata` を削除します。修復によりシステムが壊れている場合は、`yum.conf` を更新し、`repo_gpgcheck` を 0 に設定します。(BZ#1465677)

SSG `pam_faillock` モジュール使用率の確認で、`default=die` が正しく受け入れられない

SCAP セキュリティーガイド(SSG)の `pam_faillock` モジュールの使用率チェックでは、`default=die` オプションが正しく受け入れられません。したがって、`pam_unix` モジュールを使用したユーザー認証が失敗すると、`pam_faillock` のカウンターをインクリメントせずに、`pam` スタックの評価がただちに停止します。この問題を回避するには、`authfail` オプションの前に `default=die` を使用しないでください。これにより、`pam_faillock` カウンターが適切にインクリメントされます。(BZ#1448952)

第56章 デスクトップ

totem だけの更新に失敗する

totem パッケージと gstreamer1-plugins-bad-free パッケージ間に明示的な依存関係がありません。したがって、totem パッケージのみを更新しようとすると、操作が失敗します。この問題を回避するには、totem パッケージを単独で更新せず、代わりにシステム更新に依存する必要があります。(BZ#1451211)

オペレーティングシステムは、起動時に常に Wacom Expresskeys Remote (EKR) モード 1 を想定する

Wacom Expresskeys Remote (EKR) はスタンドアロンデバイスであるため、オペレーティングシステム (OS) の起動時に任意のオペレーティングモードに切り替えることができます。ただし、OS は現在、起動時に EKR がモード 1 に設定されていることを常に前提としています。システムの起動前に EKR モードを 1 に設定していないと、EKR が OS と同期しません。この問題を回避するには、OS を起動する前に EKR をモード 1 に設定します。(BZ#1458351)

ダウンロードした RPM ファイルを Nautilus からインストールできない

Nautilus ファイルマネージャーで RPM ファイルをダブルクリックすると、インストールされるファイルではなく、次のエラーが返されます。

```
Sorry, this did not work, File is not supported
```

これは、PackageKit への yum バックエンドがローカルファイルの詳細の取得をサポートしていないために発生します。

この問題は、gnome-packagekit をインストールしてダブルクリックアクションを処理するか、yum を使用してファイルを手動でインストールすることで回避できます。(BZ#1434477)

Yelp が HTML 形式のファイルを正しく表示しない

以前のバージョンの yelp では、HTML 形式のファイルを表示できました。バージョン 3.22 ではこの機能は機能せず、適格なテキスト URL を持つ Unknown エラーを返すことはできません。

この問題は yelp 自体のアーキテクチャーの変更に関連している可能性があるため、現時点では回避策はありません。

システム管理者は、yelp はこのユースケースに対応しておらず、入力として Mallard または Docbook データを想定していることに注意してください。

HTML 形式のコンテンツを表示するその他の方法を検討する必要があります。(BZ#1443179)

一部の AMD ハードウェアでモニターを接続すると、自動モード設定が失敗する

設定によっては、AMD ハードウェアを使用してシステムにモニターを追加しても、新しいハードウェアを自動的にアクティブにできない場合があります。

この問題は現在調査中です。

この問題を回避するには、システム管理者が `xrandr(1)` を手動で呼び出して監視を有効にする必要があります。(BZ#1393951)

依存関係がないため、LibreOffice なしでインストールした場合、GNOME ドキュメントが一部のドキュメントを表示できない

GNOME Documents は、LibreOffice スイートが提供するライブラリーを使用して、OpenDocument Text や Open Office XML 形式などの特定のタイプのドキュメントをレンダリングします。ただし、必要なライブラリー (`libreoffice-filters`) が、`gnome-documents` パッケージの依存関係リストにありません。したがって、LibreOffice を持たないシステムに Gnome Documents をインストールすると、前述のドキュメントタイプをレンダリングできません。

この問題を回避するには、LibreOffice 自体を使用する予定がない場合でも、`libreoffice-filters` パッケージを手動でインストールします。(BZ#1466164)

Application Installer は、ビッグエンディアンアーキテクチャーにはインストールできない場合でもパッケージを表示します。

IBM Power Systems や IBM z Systems などのビッグエンディアンシステムで Application Installer グラフィカルパッケージインストーラー (`gnome-software` パッケージ) を使用すると、利用可能なパッケージの一部をインストールすることはできず、これを試みると `installing not available` というエラーメッセージが表示されます。これは、パッケージのメタデータが現在 64 ビットの AMD および Intel 互換 (リトルエンディアン) システム用にのみ生成されているけれど、すべてのパッケージがビッグエンディアンのアーキテクチャーでも利用可能であると想定している (実際は違う) ことが原因の既知の問題です。

この問題は回避できませんが、パッケージがインストールできないこと以外には、エラーメッセージによる影響はありません。(BZ#1464139)

ソフトウェアの追加/削除 (`gpk-application`) は、最初の試行で新しくインポートされた鍵を使用しません。

GNOME でソフトウェアの追加/削除 グラフィカルインターフェイスを使用して、まだインポートさ

れていない鍵で署名されたパッケージをインストールすると、このツールに鍵のインポートに使用するプロンプトが表示されます。ただし、鍵をインポートしても、鍵をすぐに使用できないバグがあるため、インストールは失敗します。この問題を回避するには、同じパッケージを再度インストールします。その時点で、鍵は前回の試行からすでにインポートされており、インストールは成功します。(BZ#1387181)

複数の PCI デバイスを使用して複数のディスプレイを持つ仮想マシンのディスプレイのサイズを変更すると、X がクラッシュする

QXL ドライバーのバグ(xorg-x11-drv-qxl)により、仮想マシンに複数の PCI デバイスを使用するように複数のディスプレイが設定されている場合、ディスプレイのサイズ変更時に仮想マシンの X.Org ディスプレイサーバーがクラッシュします。複数のモニターで Red Hat Enterprise Linux を実行しているゲスト仮想マシンが、1つの PCI デバイスを使用するように設定されていることを確認します。Red Hat Virtualization では、この設定は Edit -> Console の Single PCI Device チェックボックスによって制御され、デフォルトで有効になっています。(BZ#1428340)

Nautilus は、GNOME クラシックセッションでアイコンを非表示にしません。

アイコンがデフォルトで非表示になっている、gnome セッションでアイコンを表示または非表示にする GNOME Tweak Tool は、GNOME Classic Session では無視されます。そのため、GNOME Tweak Tool でこのオプションが表示されている場合でも、GNOME Classic Session ではアイコンを非表示にできません。(BZ#1474852)

flatpak で依存関係が間違っている

flatpak パッケージの依存関係が間違っていると、以下のエラーメッセージが表示される場合があります。

```
flatpak: error while loading shared libraries: libostree-1.so.1: cannot open shared object file: No such file or directory
```

この問題を回避するには、flatpak-libs パッケージをインストールします。または、flatpak のみをインストールする代わりに、以下のコマンドを実行して両方のパッケージをインストールします。

```
sudo yum -y install flatpak flatpak-libs
```

(BZ#1476905)

Firefox が更新後に起動しない

firefox-52.1.2-el7.x86_64 以降にアップグレードすると、ブラウザーが起動しなくなる場合があります。これは、nspr パッケージおよび nss パッケージが Red Hat Enterprise Linux 7.4 バッチから更新されていないことが原因です。この問題を回避するには、Red Hat Enterprise 7.4 リリースの nspr パッケージおよび nss パッケージを更新します。別の回避策として、Firefox をダウングレードするこ

とが考えられますが、このオプションは推奨されません。結果として、Firefox Web ブラウザーを再起動することができます。(BZ#[1455798](#))

Xorg でのビジュアルの限定的なサポート

Xorg サーバーでは、ハードウェアドライバーで、深度 16 以降の TrueColor および DirectColor のビジュアルのみがサポートされています。PseudoColor ビジュアルを必要とするレガシーアプリケーションは、Xephyr ネスト X サーバーに対して実行できます。これにより、TrueColor 画面に表示されたときに PseudoColor 変換を実装します。(BZ#[1185690](#))

第57章 ファイルシステム

NFSv4 を提供する NetApp ストレージプライアンスの設定を確認することが推奨される

NFSv4 を提供する NetApp ストレージプライアンスを使用する場合は、マイナーバージョンごとに機能を有効または無効にできることに注意してください。

以下の Data ONTAP コマンドを使用するなどして、適切な機能が必要に応じて有効になるように設定を検証することが推奨されます。

```
vserver nfs show -vserver <vserver-name> -fields v4.0-acl,v4.0-read-delegation,v4.0-write-delegation,v4.0-referrals,v4.0-migration,v4.1-referrals,v4.1-migration,v4.1-acl,v4.1-read-delegation,v4.1-write-delegation
```

(BZ#1450447)

第58章 ハードウェアの有効化

i40e ドライバーが、最も一般的な HWTSTAMP フィルターを拒否する

i40e デバイスドライバーは、INTEL-SA-00063 アドバイザリーで説明されている Intel Ethernet Controller X710 および XL710 ファミリーのセキュリティー修正で、L4 タイムスタンプ (UDP) を無効にしているため、最も一般的な HWTSTAMP フィルターを拒否します。この問題は Intel X710 デバイスにのみ影響し、新しい X722 デバイスには影響しません。(BZ#1431964)

第59章 インストールおよび起動

HTTPS キックスタートソースからインストールする場合、FIPS モードはサポートされない

インストールイメージは、HTTPS キックスタートソースを使用したインストール中の FIPS モードをサポートしていません。そのため、現在、コマンドラインに追加された `fips=1` および `inst.ks=https://<location>/ks.cfg` オプションを使用してシステムをインストールすることはできません。(BZ#1341280)

UEFI および IPv6 を使用した PXE ブートは、オペレーティングシステム選択メニューの代わりに GRUB2 シェルを表示します。

UEFI および IPv6 で設定したクライアントで Pre-Boot Execution Environment (PXE) を起動すると、`/boot/grub/grub.cfg` ファイルに設定したブートメニューは表示されません。タイムアウトすると、設定したオペレーティングシステム選択メニューの代わりに GRUB2 シェルが表示されます。(BZ#1154226)

英数字以外の文字で `driverdisk` パーティションを指定すると、無効な出力キックスタートファイルが生成されます

Anaconda インストーラーを使用して Red Hat Enterprise Linux をインストールする場合は、キックスタートファイルにドライバーディスクを含むパーティションへのパスを含めることで、ドライバーディスクを追加できます。現在、英数字以外の文字を含む LABEL または CDLABEL でパーティションを指定すると、次のようになります。

```
driverdisk "CDLABEL=Fedora 23 x86_64:/path/to/rpm"
```

Anaconda のインストール時に作成された出力キックスタートファイルには、誤った情報が含まれます。この問題を回避するには、LABEL または CDLABEL でパーティションを指定する際に、英数字のみを使用してください。(BZ#1452770)

Scientific Computing バリエーションには、特定のセキュリティープロファイルに必要なパッケージがありません

コンピュータノードとも呼ばれる Red Hat Enterprise Linux for Scientific Computing バリエーションをインストールする場合は、他のバリエーションのインストールプロセスと同様のセキュリティープロファイルを選択できます。ただし、このバリエーションは最小限であることが意図されているため、米国政府の設定ベースラインなどの特定のプロファイルに必要なパッケージがありません。このプロファイルを選択すると、一部のパッケージが欠落していることを示す警告が表示されます。

警告により、パッケージが欠落している場合でもインストールを続行できます。これを使用して、問題を回避できます。インストールは正常に完了しますが、警告されたにもかかわらず、システムをインストールし、インストール後にセキュリティースキャンを実行しようとする、これらのパッケージがないためにスキャンが失敗したと報告されることに注意してください。この動作は想定されています。(BZ#1462647)

第60章 カーネル

セカンダリーコアがオフラインでないと `kexec` が失敗する

特定の状況では、HP ProLiant m400 や AppliedMicro Mustang などの AppliedMicro X-Gene プラットフォームで、セカンダリーコアのオフライン化が失敗します。その結果、カーネルパニックが発生すると、カーネルが `kexec` を介して `kdump` クラッシュダンプメカニズムをトリガーできない場合があります。その結果、カーネルクラッシュダンプファイルは保存されません。(BZ#1218374)

キャッシュの誤ったフラッシュによるファイルシステムの破損が修正されたが、I/O 操作が遅くなる可能性がある

`megaraid_sas` ドライバーのバグが原因で、以前はシステムのシャットダウン、再起動、または電源の損失中に、ファイルシステムがディスク書き込みのキャッシュとともに使用された場合に、ファイルシステムが破損していました。今回の更新で、キャッシュコマンドを正しく RAID カードに転送する `megaraid_sas` が修正されました。その結果、RAID カードファームウェアも更新すると、ファイルシステムの破損は上記の状況では発生しなくなります。

Broadcom `megaraid_sas` RAID アダプターを使用すると、システムログ(`dmesg`)で機能を確認できます。適切な機能は、以下のテキスト文字列で示されます。

```
FW supports sync cache Yes
```

この修正により、キャッシュが適切にフラッシュされるようになったため、I/O 操作が遅くなる可能性があることに注意してください。(BZ#1380447)

Wacom Cintiq 12WX のプラグを抜き、すぐに差しした場合に再検出されない

同じ USB ポート内で Wacom Cintiq 12WX を取り外してすばやく接続すると、現在タブレットは認識されません。この問題を回避するには、タブレットを再度接続する前に 3 ~ 5 秒待ちます。(BZ#1458354)

GUI の起動時に、Virtual DVD を使用して一部の IBM POWER8 マシンにインストールすると失敗する

Red Hat Enterprise Linux 7.4 は、Anaconda GUI の起動時に、一部の IBM POWER8 ハードウェア (S822LC マシンを含む) にインストールできない場合があります。

この問題は、X11 の起動エラーに特徴があり、Anaconda 画面で `Pane is dead` メッセージが続きます。

回避策として、`inst.text` をカーネルコマンドラインに追加し、テキストモードでインストールします。

この問題は、仮想 DVD のインストールに限定されており、ネットブートイメージを使用した追加のテストにより GUI のインストールが可能になります。(BZ#1377857)

キーボードショートカットを使用してフルスクリーンモードに入ると、VMWare ESXi 5.5 でディスプレイの問題が発生する

Red Hat Enterprise Linux 7.4 を VMWare ESXi 5.5 ホストで実行している仮想マシンゲストとして使用する場合は、Ctrl+Alt+Enter を押してコンソールでフルスクリーンモードに入ると、ディスプレイが使用できなくなります。同時に、以下の例のようなエラーはシステムログ(dmesg)に保存されます。

```
[drm:vmw_cmdbuf_work_func [vmwgfx]] *ERROR* Command buffer error.
```

この問題を回避するには、仮想マシンをシャットダウンし、.vmx 設定ファイルを開き、以下のパラメーターを追加または変更します。

```
svga.maxWidth = X
svga.maxHeight = Y
svga.vramSize = "X * Y * 4"
```

上記では、X と Y を画面の水平解像度と垂直解像度に置き換えます。svga.vramSize パラメーターは、X の Y 倍の値を取ります。したがって、解像度が 1920x1080 の画面のセットアップ例は次のとおりです。

```
svga.maxWidth = 1920
svga.maxHeight = 1080
svga.vramSize = "8294400"
```

このバグが発生したと報告されているバージョンは VMWare ESXi 5.5 のみであることに注意してください。他のバージョンは問題なくフルスクリーンモードに入ることができます。(BZ#1451242)

現在、xz 圧縮には対応していません。

カーネルモジュールのソースチェッカー(ksc ツール)は、現在 xz 圧縮方法を処理できず、以下のエラーを報告します。

```
Invalid architecture, supported architectures are x86_64, ppc64, s390x
```

この制限が解決されるまで、システム管理者は ksc ツールを実行する前に、xz 圧縮を使用してサードパーティモジュールを手動で圧縮解除する必要があります。(BZ#1463600)

第61章 ネットワーク

Red Hat Enterprise Linux 7 で、MD5 ハッシュアルゴリズムを使用した署名の検証が無効になる

MD5 で署名された証明書を必要とする WPA (Wi-Fi Protected Access) の AP (Enterprise Access Point) に接続することはできません。この問題を回避するには、`/usr/lib/systemd/system/` ディレクトリーから `/etc/systemd/system/` ディレクトリーに `wpa_supplicant.service` ファイルをコピーして、ファイルの `Service` セクションに次の行を追加します。

```
Environment=OPENSSL_ENABLE_MD5_VERIFY=1
```

次に、`root` で `systemctl daemon-reload` コマンドを実行し、サービスファイルをリロードします。

重要: MD5 証明書は安全性が非常に低く、Red Hat では使用を推奨していないことに注意してください。(BZ#1062656)

RHEL 7.3 からアップグレードすると FreeRADIUS が失敗する可能性がある

`/etc/raddb/radiusd.conf` ファイルの新しい設定プロパティー `correct_escapes` が、RHEL 7.4 以降配布された FreeRADIUS バージョンに導入されました。管理者が `correct_escapes` を `true` に設定すると、バックスラッシュエスケープ用の新しい正規表現構文が想定されます。`correct_escapes` を `false` に設定すると、バックスラッシュもエスケープされる古い構文が予想されます。後方互換性の理由から、`false` がデフォルト値になります。

アップグレード時に、`/etc/raddb/` ディレクトリーの設定ファイルは管理者によって変更されない限り上書きされます。そのため、`correct_escapes` の値は、すべての設定ファイルで使用される構文のタイプに常に対応しているとは限りません。その結果、`freeradius` での認証が失敗する場合があります。

この問題を回避するには、`freeradius` バージョン 3.0.4 (RHEL 7.3 で配布)以前からアップグレードした後、`/etc/raddb/` ディレクトリー内のすべての設定ファイルが新しいエスケープ構文 (二重のバックスラッシュ文字は見つかりません) を使用し、`/etc/raddb/radiusd.conf` の `correct_escapes` の値が `true` に設定されていることを確認してください。

詳細と例については、<https://access.redhat.com/solutions/3241961> のソリューションを参照してください。(BZ#1489758)

第62章 セキュリティー

`certutil` は、FIPS モードで NSS データベースパスワード要件を返しません。

`certutil` ツールを使用して新しい Network Security Services (NSS) データベースを作成する場合、FIPS モードで実行する際にデータベースパスワードの要件を確認することはできません。プロンプトメッセージはパスワード要件を提供しておらず、`certutil` は一般的なエラーメッセージのみを返します。

```
certutil: could not authenticate to token NSS FIPS 140-2 Certificate DB.: SEC_ERROR_IO: An I/O error occurred during security authorization.
```

(BZ#1401809)

`systemd-importd` は `init_t` として実行されます。

`systemd-importd` サービスは、`systemd` ユニットファイルの `NoNewPrivileges` セキュリティーフラグを使用しています。これにより、`init_t` ドメインから `systemd_importd_t` ドメインへの SELinux ドメインの移行がブロックされます。(BZ#1365944)

キックスタートインストールでは、SCAP パスワードの長さの要件は無視されます。

対話型キックスタートインストールは、SCAP ルールで定義されたパスワードの長さのチェックを強制せず、より短い `root` パスワードを受け入れます。この問題を回避するには、キックスタートファイルの `pwpolicy root` コマンドで `--strict` オプションを使用します。(BZ#1372791)

`rhnsd.pid` はグループまたはその他の方法で書き込み可能

Red Hat Enterprise Linux 7.4 では、`/var/run/rhnsd.pid` ファイルのデフォルトパーミッションは `-rw-rw-rw-` に設定されます。この設定は安全ではありません。この問題を回避するには、このファイルのパーミッションを変更して、所有者のみが書き込み可能にします。

```
# chmod go-w /var/run/rhnsd.pid
```

(BZ#1480306)

第63章 ストレージ

クラスター内の RAID 上でのシンプロビジョニングはサポートされていません

RAID 論理ボリュームとシンプロビジョニングされた論理ボリュームは、排他的にアクティブ化されたときにクラスターで使用できますが、現在、クラスター内の RAID の上にシンプロビジョニングすることはサポートされていません。組み合わせが排他的にアクティブになっている場合でも、これが当てはまります。現在、この組み合わせは、LVM のシングルマシンの非クラスターモードでのみサポートされています。(BZ#1014758)

LVM または md デバイスに、以前のインストールからのメタデータがあると、Anaconda インストールが失敗する場合があります。

マルチパスされるディスクが以前のインストールから LVM や md メタデータですでに起動しているマシン上での Red Hat Enterprise Linux 7 インストール中に、マルチパスはデバイス上で設定されず、Anaconda が起動している間に LVM/md はパスデバイスの 1 つに設定されます。これにより、Anaconda で問題が発生し、インストールに失敗する場合があります。この問題を回避するには、インストール用に起動時に `mpath.wwid=<WWID>` をカーネルコマンドラインに追加します。<WWID> は、マルチパスを要求するデバイスの `wwid` です。この値は、`scsi` デバイスの `ID_SERIAL udev` データベース値、および `DASD` デバイスの `ID_UID` と同じです。(BZ#1378714)

第64章 システムおよびサブスクリプション管理

`rdma-core` がインストールされていると、システムのアップグレードにより、`Yum` が不要な 32 ビットパッケージをインストールする可能性があります。

Red Hat Enterprise Linux 7.4 では、`rdma-core.noarch` パッケージは `rdma-core.i686` および `rdma-core.x86_64` により廃止されました。システムのアップグレード中に、`Yum` は元のパッケージを両方の新しいパッケージに置き換え、必要な依存関係をインストールします。これは、32 ビットパッケージと、その 32 ビット依存パッケージの潜在的な大部分が、必要でない場合でも、デフォルトでインストールされることを意味します。

この問題を回避するには、`--exclude=*.i686` オプションで `yum update` コマンドを使用するか、アップグレード後に `yum remove rdma-core.i686` を使用して 32 ビットパッケージを削除します。
(BZ#1458338)

第65章 仮想化

OVMF ゲストの起動に失敗する

現在、`qemu-kvm`パッケージを使用して Red Hat Enterprise Linux ホストで Open Virtual Machine Firmware (OVMF) を使用するゲスト仮想マシンを起動しようとするると失敗し、ゲストが応答しなくなり、空白の画面が表示されます。(BZ#1174132)

`virsh iface-bridge` を使用したブリッジの作成に失敗する

ネットワーク以外のソースから Red Hat Enterprise Linux 7 をインストールする場合は、インターフェイス設定ファイルでネットワークデバイス名はデフォルトで指定されません(`DEVICE=` 行で行われます)。これにより、`virsh iface-bridge` コマンドを使用したネットワークブリッジの作成に失敗し、エラーメッセージが表示されます。この問題を回避するには、`/etc/sysconfig/network-scripts/ifcfg-*` ファイルに `DEVICE=` 行を追加します。

詳細は、Red Hat ナレッジベース <https://access.redhat.com/solutions/2792701> (BZ#1100588) を参照してください。

ゲストは、ESXi 5.5 で起動できない場合があります。

VMware ESXi 5.5 ハイパーバイザーで RAM が 12GB 以上の Red Hat Enterprise Linux 7 ゲストを実行している場合、一部のコンポーネントは現在、間違ったメモリータイプ範囲レジスター (MTRR) 値で初期化されていたり、システムの起動時に MTRR 値が間違っって再設定されています。これにより、ゲストカーネルがパニック状態になったり、ゲストがシステムの起動時に応答しなくなることがあります。

この問題を回避するには、ゲストのカーネルコマンドラインに `disable_mtrr_trim` オプションを追加します。これにより、MTRR が正しく設定されていない場合にゲストが起動し続けることができます。このオプションを使用すると、ゲストは起動時に `WARNING: BIOS bug` メッセージを出力することに注意してください。これは無視しても問題ありません。(BZ#1429792)

STIG for Red Hat Virtualization Hypervisor プロファイルは Anaconda に表示されない

`oscap-anaconda-addon` モジュールは現在、STIG for Red Hat Virtualization Hypervisor のセキュリティ強化プロファイルを適切に解析できません。これにより、プロファイルの名前は、Anaconda インターフェイスの選択で `DISA STIG for Red Hat Enterprise Linux 7` または `United States Government Configuration Baseline (USGCB / STIG)- DRAFT` と表示されます。ただし、これは表示の問題にすぎず、STIG for Red Hat Virtualization Hypervisor プロファイルの代わりに `DISA STIG for Red Hat Enterprise Linux 7` プロファイルを安全に使用できます。(BZ#1437106)

付録A コンポーネントのバージョン

この付録では、Red Hat Enterprise Linux 7.4 リリースにおける主要コンポーネントとそのバージョンの一覧を説明します。

表A.1 コンポーネントのバージョン

Component	Version
カーネル	3.10.0-693
QLogic qla2xxx ドライバー	8.07.00.38.07.4-k1
QLogic qla4xxx ドライバー	5.04.00.00.07.02-k0
Emulex lpfc ドライバー	0:11.2.0.6
iSCSI イニシエーター utils	iscsi-initiator-utils-6.2.0.874-4
DM Multipath	device-mapper-multipath-0.4.9-111
LVM	lvm2-2.02.171-8

付録B コンポーネント別の BUGZILLAS の一覧

この付録では、このドキュメントに含まれるすべてのコンポーネントと関連する Bugzilla の一覧を説明します。

表B.1 コンポーネント別の Bugzillas の一覧

Component	新機能	主なバグ修正	テクノロジーブ レビュー	既知の問題
389-ds-base	BZ#1394000, BZ#1395940, BZ#1425907	BZ#1378209		
Doc-administration-guide	BZ#1426286, BZ#1426289			
Doc-release-notes	BZ#1426275, BZ#1426278, BZ#1426283, BZ#1436973			
NetworkManager	BZ#1337997, BZ#1353612, BZ#1373698, BZ#1394344, BZ#1394579, BZ#1398934, BZ#1404594, BZ#1404598, BZ#1414103, BZ#1420708	BZ#1391170, BZ#1393997		
aide		BZ#1377215		
anaconda	BZ#663099, BZ#1113207, BZ#1131247, BZ#1255659, BZ#1315160, BZ#1332316, BZ#1366935, BZ#1377233, BZ#1391724, BZ#1412538	BZ#1317370, BZ#1327439, BZ#1356975, BZ#1358778, BZ#1373360, BZ#1380224, BZ#1380277, BZ#1404158, BZ#1412022, BZ#1441337		BZ#1378714
ansible			BZ#1313263	
audit	BZ#1381601			

Component	新機能	主なバグ修正	テクノロジーブ レビュー	既知の問題
authconfig	BZ#1334449, BZ#1378943			
autofs	BZ#1367576, BZ#1382093	BZ#1101782, BZ#1383194, BZ#1383910, BZ#1420574, BZ#1420584, BZ#1320588		
bind	BZ#1388534, BZ#1393886			
bind-dyndb-ldap	BZ#1393889			
binutils	BZ#1366052	BZ#1326710, BZ#1406498		
bison	BZ#1306000			
booth	BZ#1302087			
ca-certificates	BZ#1444414			
chrony	BZ#1387223			
chrpath		BZ#1271380		
clevis	BZ#1300697			
cloud-init	BZ#1427280			
clutter	BZ#1387424			
crash	BZ#1368711, BZ#1384944, BZ#1393534			
criu			BZ#1400230	
custodia			BZ#1403214	
cyrus-sasl		BZ#1421663		
dbxtool	BZ#1078990			

Component	新機能	主なバグ修正	テクノロジーブ レビュー	既知の問題
dconf-editor	BZ#1388931			
device-mapper-multipath	BZ#1169168 , BZ#1279355 , BZ#1359510 , BZ#1362409 , BZ#1368211 , BZ#1372032 , BZ#1394059 , BZ#1406226 , BZ#1416569 , BZ#1430097	BZ#1239173 , BZ#1362120 , BZ#1380602 , BZ#1402092 , BZ#1403552 , BZ#1431562		
dhcp	BZ#1374119			
distribution				BZ#1062656
dmidecode	BZ#1385884			
dnsmasq	BZ#1375527 , BZ#1375569			
ecj	BZ#1379855			
elfutils	BZ#1400302			
empathy		BZ#1386616		
ethtool	BZ#1402701			
fcoe-utils		BZ#1384707		
firefox				BZ#1455798
firewalld	BZ#1006225 , BZ#1409544 , BZ#1419058	BZ#1401978		
flatpak				BZ#1476905
freeradius				BZ#1489758
genwqe-tools	BZ#1275663			
gfs2-utils	BZ#1413684			

Component	新機能	主なバグ修正	テクノロジープレビュー	既知の問題
ghostscript		BZ#1390847, BZ#1411725, BZ#1424752		
git		BZ#1369173		
glibc	BZ#841653, BZ#1298975, BZ#1320947, BZ#1421155	BZ#1324568, BZ#1326739		
glusterfs				BZ#1409773
gnome-initial-setup		BZ#1226819		
gnome-packagekit				BZ#1387181
gnome-shell	BZ#1383353			
gnome-software				BZ#1434477, BZ#1464139
gnu-efi	BZ#1310782			
gnutls	BZ#1399232			
grep	BZ#1297441			
grub2				BZ#1154226
gstreamer1-plugins-good				BZ#1451211
http-parser	BZ#1393819			
hwdata	BZ#1386133			
initial-setup		BZ#1378082		

Component	新機能	主なバグ修正	テクノロジーブ レビュー	既知の問題
initscripts	BZ#1260552, BZ#1428935	BZ#1278521, BZ#1367554, BZ#1369790, BZ#1374837, BZ#1385272, BZ#1392766, BZ#1394191, BZ#1398671, BZ#1398678, BZ#1398679, BZ#1398683, BZ#1398686, BZ#1406254, BZ#1408219, BZ#1428574, BZ#1434075		
intel-cmt-cat	BZ#1315489			
ipa	BZ#872671, BZ#1125174, BZ#1200767, BZ#1366572, BZ#1402959, BZ#1404750, BZ#1409628, BZ#1459153		BZ#1115294, BZ#1298286	BZ#1455946
ipa-server-docker			BZ#1405325	
iperf3	BZ#913329			
ipmitool	BZ#1398658			
iproute	BZ#1063934, BZ#1422629	BZ#1375215		
iprutils	BZ#1384382			
jansson	BZ#1389805			
java-1.7.0-openjdk	BZ#1373986			
java-1.8.0-openjdk			BZ#1400306	
kernel	BZ#437984, BZ#950243, BZ#1072503,	BZ#1084802, BZ#1213119, BZ#1217546,	BZ#916382, BZ#947163, BZ#1109348,	BZ#1377857, BZ#1380447, BZ#1429792,

Component	BZ#1138782, 新機能 BZ#135732, BZ#1241990,	BZ#1324918, 主なバグ修正 BZ#1331098, BZ#1353218,	BZ#1111712, テクノロジーブ レビュー BZ#1298277, BZ#1230959,	BZ#1431964, 既知の問題 BZ#1451242, BZ#1458354
	BZ#1270982, BZ#1273401, BZ#1297841, BZ#1297929, BZ#1298643, BZ#1299527, BZ#1302147, BZ#1306396, BZ#1306453, BZ#1308632, BZ#1314179, BZ#1326309, BZ#1326318, BZ#1326353, BZ#1330457, BZ#1339127, BZ#1339791, BZ#1340238, BZ#1346348, BZ#1352289, BZ#1355919, BZ#1356122, BZ#1357491, BZ#1365002, BZ#1366564, BZ#1369158, BZ#1373606, BZ#1373971, BZ#1374498, BZ#1377710, BZ#1377767, BZ#1379590, BZ#1382101, BZ#1382494, BZ#1382500, BZ#1382504, BZ#1382508, BZ#1382849, BZ#1383280, BZ#1383827, BZ#1383834, BZ#1384456, BZ#1384648, BZ#1385026, BZ#1385757, BZ#1388467, BZ#1388646, BZ#1388716, BZ#1391219, BZ#1391243, BZ#1391413, BZ#1391668, BZ#1394197,	BZ#1363661, BZ#1370638, BZ#1379787, BZ#1385149, BZ#1386923, BZ#1387485, BZ#1406885, BZ#1408330, BZ#1412898	BZ#1274456, BZ#1274459, BZ#1299662, BZ#1305092, BZ#1348508, BZ#1349668, BZ#1350553, BZ#1393375, BZ#1414957, BZ#1449762, BZ#1460849, BZ#1288964	

Component	新機能 BZ#1400501, BZ#1401797, BZ#1402102, BZ#1406197, BZ#1416924, BZ#1432218, BZ#1432897, BZ#1383489, BZ#1626527	主なバグ修正	テクノロジーブ レビュー	既知の問題
kernel-aarch64				BZ#1218374
kernel-rt	BZ#1391779	BZ#1443711	BZ#1297061	
kexec-tools	BZ#1384945			
keycloak-httpd-client- install	BZ#1401781			
libcgroup		BZ#1406927		
libdb		BZ#1277887		
libfastjson	BZ#1395145			
libguestfs	BZ#1233093, BZ#1359086, BZ#1362649, BZ#1367738, BZ#1400205, BZ#1404182	BZ#1161019, BZ#1265588, BZ#1311890, BZ#1354507, BZ#1374232, BZ#1374405, BZ#1383517, BZ#1392798, BZ#1401474, BZ#1402301, BZ#1431579	BZ#1387213, BZ#1441197	
libica	BZ#1391558			
libnfsidmap	BZ#980925			
libnftnl		BZ#1418967	BZ#1332585	
libreoffice				BZ#1466164
libreswan	BZ#1324458, BZ#1399883			
librtas	BZ#1380656			
libseccomp	BZ#1425007			

Component	新機能	主なバグ修正	テクノロジープレビュー	既知の問題
libstoragemgmt	BZ#1403142		BZ#1119909	
libusnic_verbs			BZ#916384	
libvirt	BZ#1349696, BZ#1382640, BZ#1414627		BZ#1283251	
libwacom	BZ#1342990			BZ#1458351
linuxptp	BZ#1359311			
logrotate	BZ#1381719			
lorax	BZ#1310775, BZ#1430483			BZ#1341280
lshw	BZ#1368704			
lvm2	BZ#1189108, BZ#1191935, BZ#1346280, BZ#1366296, BZ#1378956, BZ#1394048, BZ#1436748, BZ#1442992	BZ#1380521, BZ#1380532, BZ#1382688, BZ#1386184, BZ#1434054		BZ#1014758
mariadb		BZ#1356897		
mdadm	BZ#1380017			
memkind	BZ#1384549			
mod_nss	BZ#1382102, BZ#1392582			
mutt	BZ#1388511	BZ#1388512		
mutter				BZ#1393951
nautilus				BZ#1474852
net-snmp		BZ#1286693, BZ#1324306		

Component	新機能	主なバグ修正	テクノロジーブ レビュー	既知の問題
netcf				BZ#1100588
nfs-utils	BZ#1375259, BZ#1418041			BZ#1450447
nss	BZ#1309781, BZ#1316546, BZ#1444413	BZ#1220573		BZ#1401809
nss-softokn	BZ#1369055			
nvme-cli	BZ#1382119			
nvmetcli	BZ#1383837			
opencryptoki	BZ#1391559			
openldap	BZ#1386365, BZ#1428740			
opensc	BZ#1081088			
openscap	BZ#1363826	BZ#1420038, BZ#1440192, BZ#1447341		
openssh	BZ#1322911, BZ#1341754	BZ#1418062		
openssl	BZ#1276310			
openssl-ibmca	BZ#1274385			
openvswitch	BZ#1368043, BZ#1390938			
openwsman	BZ#1190689			
oprofile		BZ#1380809		
oscap-anaconda-addon				BZ#1372791, BZ#1437106, BZ#1462647

Component	新機能	主なバグ修正	テクノロジーブ レビュー	既知の問題
other	BZ#1432080, BZ#1444937, BZ#1457907, BZ#1459948, BZ#1467260	BZ#1408694	BZ#1062759, BZ#1072107, BZ#1259547, BZ#1464377, BZ#1467338, BZ#1477977	BZ#1174132, BZ#1458338, BZ#1463600
OVMF			BZ#653382	
pacemaker	BZ#1289662	BZ#1388489		
pcp	BZ#1422263, BZ#1423020			
pcrc		BZ#1400267		BZ#1290432
pcs	BZ#1158805, BZ#1165821, BZ#1176018, BZ#1261116, BZ#1303969, BZ#1362493, BZ#1373614, BZ#1413958	BZ#1386114, BZ#1378107	BZ#1433016	
perl-IO-Socket-SSL	BZ#1335035			
perl-Net-SSLeay	BZ#1335028			
perl-Perl4-CoreLibs	BZ#1366724			
perl-local-lib		BZ#1122993		

Component	新機能	主なバグ修正	テクノロジープレビュー	既知の問題
pki-core	BZ#1303683, BZ#1305993, BZ#1325071, BZ#1388622, BZ#1391737, BZ#1392068, BZ#1409946, BZ#1413132, BZ#1426754, BZ#1445535, BZ#1447144, BZ#1450143, BZ#1458055	BZ#1238684, BZ#1246635, BZ#1249400, BZ#1282504, BZ#1330800, BZ#1372052, BZ#1376226, BZ#1376488, BZ#1378275, BZ#1378277, BZ#1381084, BZ#1382066, BZ#1385208, BZ#1386303, BZ#1395817, BZ#1397200, BZ#1400149, BZ#1404881, BZ#1411428, BZ#1412681, BZ#1413136, BZ#1445088, BZ#1446364, BZ#1447762, BZ#1452250, BZ#1452344, BZ#1454450, BZ#1454471, BZ#1458429		BZ#1256901
procps-ng		BZ#1373246		
psacct	BZ#1255183			
pykickstart				BZ#1452770
python	BZ#1219110			
python-blivet		BZ#1214407, BZ#1327463		
python-tornado	BZ#1158617			
qemu-kvm			BZ#1103193	
rdma-core	BZ#1404035			
rear	BZ#1355667	BZ#1343119		

Component	新機能	主なバグ修正	テクノロジープレビュー	既知の問題
resource-agents	BZ#1077888, BZ#1336847, BZ#1430304			
rhino	BZ#1350331			
rhnsd				BZ#1480306
rpm		BZ#1378307	BZ#1278924	
rsyslog	BZ#1313490, BZ#1431616			
ruby	BZ#1397390	BZ#1308992		
rubygem-abrt	BZ#1418750			
samba	BZ#1391954			
sapconf		BZ#1391881		
sbd	BZ#1413951			
sblim-cmpi-fsvol		BZ#1136116		
scap-security-guide	BZ#1404392, BZ#1410914	BZ#1450731		BZ#1448952, BZ#1464899, BZ#1465677
seabios		BZ#1020622		
selinux-policy		BZ#1368057, BZ#1386916		BZ#1365944
sendmail	BZ#1124827			
sg3_utils		BZ#1380744		
shim	BZ#1310766			
shim-signed	BZ#1310764			
sos	BZ#1414879			

Component	新機能	主なバグ修正	テクノロジーブ レビュー	既知の問題
sssd	BZ#1214491, BZ#1311056, BZ#1330196, BZ#1340711, BZ#1396012, BZ#1414023, BZ#1425891		BZ#1068725	BZ#1446101, BZ#1447945, BZ#1448094, BZ#1460689, BZ#1462769
strace		BZ#1377847		
strongimcv			BZ#755087	
sudo				BZ#1293306
system-config-language		BZ#1304223		
systemd		BZ#1353028	BZ#1284974	
systemtap	BZ#1398393			
tar	BZ#1350640	BZ#1184697, BZ#1319820, BZ#1341786		
targetcli	BZ#1243410			
targetd	BZ#1162381			
tboot	BZ#1384210			
tcpdump	BZ#1292056, BZ#1422473			
tcsh		BZ#1388426		
telnet	BZ#1367415			
tpm2-tss	BZ#1275027			
tss2	BZ#1384452			
tuned	BZ#1388454, BZ#1414098			
unbound	BZ#1382383			

Component	新機能	主なバグ修正	テクノロジープレビュー	既知の問題
usbguard	BZ#1395615		BZ#1467369	
valgrind	BZ#1391217			
virt-who	BZ#1299643 , BZ#1369107 , BZ#1405967 , BZ#1426058 , BZ#1436811			
wget	BZ#1439811			
wpa_supplicant	BZ#1404793			
xorg-x11-drv-libinput	BZ#1413811			
xorg-x11-drv-qxl				BZ#1428340
xorg-x11-server	BZ#1404868			BZ#1185690
yelp				BZ#1443179
yp-tools		BZ#1401432		
ypbind		BZ#1217435 , BZ#1382804		
yum	BZ#1343690	BZ#1352585 , BZ#1370134		
yum-utils		BZ#1406891		

付録C 更新履歴

改訂 0.5-0	Wed Feb 12 2020	Jaroslav Klech
アーキテクチャーおよび新機能への完全なカーネルバージョンを指定。		
改訂 0.4-9	Mon Oct 07 2019	Jiří Herrmann
OVMF に関するテクノロジープレビューの注意事項を明確にしました。		
改訂 0.4-8	Mon May 13 2019	Lenka Špačková
FreeRADIUS アップグレード (ネットワーク) に関連する既知の問題を追加しました。		
改訂 0.4-7	Sun Apr 28 2019	Lenka Špačková
テクノロジープレビュー機能の説明 (ファイルシステム) の表現が改善されました。		
改訂 0.4-6	Mon Feb 04 2019	Lenka Špačková
ブックの構造が改善されました。		
改訂 0.4-5	Thu Sep 13 2018	Lenka Špačková
テクノロジープレビューから完全にサポートされる機能 (ファイルシステム) に CephFS を移動しました。		
改訂 0.4-4	Tue Apr 17 2018	Lenka Špačková
ssllwrap () の非推奨に関連する推奨事項を更新しました。		
改訂 0.4-3	Tue Apr 10 2018	Lenka Špačková
rsyslog imudp モジュールの inputname オプションに関連する非推奨の注意書きを追加しました。		
改訂 0.4-2	Thu Apr 05 2018	Lenka Špačková
CAT をテクノロジープレビュー (カーネル) に移動。		
改訂 0.4-1	Thu Mar 22 2018	Lenka Špačková
openldap-servers パッケージの名前 (非推奨の機能) が修正されました。		
改訂 0.4-0	Fri Mar 16 2018	Lenka Špačková
pcs 関連のバグ修正 (クラスタリング) を追加しました。		
改訂 0.3-9	Mon Feb 19 2018	Mirek Jahoda
間違って配置されていた TPM 関連の機能が、テクノロジープレビューセクションに移動しました。		
改訂 0.3-8	Tue Feb 06 2018	Lenka Špačková
不足しているテクノロジープレビュー - OVMF (仮想化) を追加しました。 libvirt-lxc ツールを使用したコンテナの非推奨に関する情報を追加しました。		
改訂 0.3-7	Wed Jan 17 2018	Lenka Špačková
FCoE の非推奨通知が更新されました。		
改訂 0.3-6	Wed Jan 10 2018	Lenka Špačková
Device DAX for NVDIMM デバイスのステータスをテクノロジープレビューから完全にサポートされている (ストレージ) に変更しました。		
改訂 0.3-5	Thu Dec 14 2017	Lenka Špačková
非推奨のドライバーの構造が統一されました。		
改訂 0.3-4	Tue Dec 12 2017	Lenka Špačková

qla2xxx ドライバーから非推奨のアダプターを更新しました。		
改訂 0.3-3 pam_krb5 から sssd への移行 (非推奨機能) に関する情報を追加しました。	Wed Nov 22 2017	Lenka Špačková
改訂 0.3-2 タイプミスを修正しました。	Wed Nov 15 2017	Lenka Špačková
改訂 0.3-1 LVM 関連のバグ修正の説明 (ストレージ) を追加しました。	Tue Oct 31 2017	Lenka Špačková
改訂 0.3-3 autofs バグ修正の説明 (ファイルシステム) を追加しました。 ld リンカーの動作の変更に関する情報を非推奨の機能に追加。	Mon Oct 30 2017	Lenka Špačková
改訂 0.3-2 Xorg サーバーでのビジュアルへの限られたサポートに関する情報を追加しました。	Wed Sep 13 2017	Lenka Špačková
改訂 0.3-1 テクノロジープレビュー (カーネル) に CUIR 拡張スコープ検出が追加されました。 新機能 (セキュリティー) の openssh リベースの説明を更新しました。	Mon Sep 11 2017	Lenka Špačková
改訂 0.3-0 2つの既知の問題 (セキュリティー、デスクトップ) を追加しました。	Mon Sep 04 2017	Lenka Špačková
改訂 0.2-9 非推奨機能にtcp_wrappersが追加されました。	Mon Aug 21 2017	Lenka Špačková
改訂 0.2-8 新機能と既知の問題がいくつか追加されました。	Tue Aug 15 2017	Lenka Špačková
改訂 0.2-7 重複するメモを削除しました。	Mon Aug 14 2017	Lenka Špačková
改訂 0.2-6 いくつかの既知の問題を更新しました。	Thu Aug 10 2017	Lenka Špačková
改訂 0.2-5 2つの既知の問題が追加されました。	Tue Aug 08 2017	Lenka Špačková
改訂 0.2-4 FCoE の非推奨通知が更新されました。 マイナーな更新および追加。	Mon Aug 07 2017	Lenka Špačková
改訂 0.2-3 いくつかの新機能を仮想化からシステムおよびサブスクリプション管理に移動しました。	Fri Aug 04 2017	Lenka Špačková
改訂 0.2-2 Btrfs に関する情報を更新し、テクノロジープレビューと非推奨の機能の両方に含まれるようになりました。 マイナーな更新および追加。	Thu Aug 03 2017	Lenka Špačková
改訂 0.2-1 Red Hat Enterprise Linux 7.4 リリースノートのリリース。	Tue Aug 01 2017	Lenka Špačková
改訂 0.0-4	Tue May 23 2017	Lenka Špačková

Red Hat Enterprise Linux 7.4 Beta リリースノートのリリース。