Red Hat Enterprise Linux 6

6.9 リリースノート

Red Hat Enterprise Linux 6.9 リリースノート

エディッション 9

Last Updated: 2018-08-07

Red Hat Enterprise Linux 6 6.9 リリースノート

Red Hat Enterprise Linux 6.9 リリースノート
エディッション 9

Red Hat Customer Content Services
rhel-notes@redhat.com

法律上の通知

概要

リリースノートでは、Red Hat Enterprise Linux 6.9 での改良点や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について説明しています。重要なバグ修正、テクニカルプレビュー、使用されなくなった機能などの詳細については、Technical Notes を参照してください。

目次

前書き

Red Hat Enterprise Linux のマイナーリリースとは、機能強化、セキュリティーエラータ、およびバグ修正によるエラータなどを集めたものです。『Red Hat Enterprise Linux 6.9 リリースノート』 では、今回のマイナーリリースで Red Hat Enterprise Linux 6 オペレーティングシステムと付随するアプリケーションに加えられた主要な変更および既知の問題について説明しています。Technical Notes では、主なバグ修正、現在利用可能なすべてのテクノロジープレビュー、使用されなくなった機能について説明しています。

他のバージョンと比較した Red Hat Enterprise Linux 6 の機能および制限については https://access.redhat.com/articles/rhel-limits にある Red Hat ナレッジベースの記事を参照してください。

Red Hat Enterprise Linux のライフサイクルについては https://access.redhat.com/support/policy/updates/errata/ をご覧ください。

第1章 概要

製品ライフサイクルに関する注記
Red Hat Enterprise Linux 6 は現在、製品ライフサイクルのメンテナンスサポートフェーズ 2 に入っているため、新機能およびハードウェアの機能強化が提供される予定はありません。したがって、Red Hat Enterprise Linux 6.9 は、バグ修正に重点を置いた安定したリリースを提供します。これに続く更新は、条件を満たした重大なセキュリティー修正や、業務に影響を与える緊急の問題に限られます。詳細は 「Red Hat Enterprise Linux のライフサイクル」 を参照してください。

インプレースアップグレード
Red Hat Enterprise Linux のサブスクリプションは特定のリリースに紐付けられているわけではないので、既存のお客様はいつでも無料で Red Hat Enterprise Linux 6 インフラストラクチャーを Red Hat Enterprise Linux 7 に更新して、アップストリームからの最新の技術革新を活用することができます。Red Hat Enterprise Linux 7 へのアップグレードを簡素化するために、Red Hat では **Preupgrade Assistant** と **Red Hat Upgrade Tool** を用意しています。詳細情報については、*2章 全般的な更新* を参照してください。

セキュリティー

- **GnuTLS** コンポーネントに TLS プロトコルのバージョン 1.2 のサポートが追加されたことで、Red Hat Enterprise Linux 6 は提供されるセキュリティーライブラリーで TLS 1.2 の完全サポートを提供します。TLS 1.2 は PCI-DSS 3.1 などの最新のセキュリティー標準で推奨されています。詳細情報は、*11章 セキュリティー* を参照してください。

- **OpenSCAP** 1.2.13 は、米国標準技術局 (NIST) の Security Content Automation Protocol (SCAP) 1.2 により、認証設定カテゴリーの Common Vulnerabilities and Exposure (CVE) オプションで認証されています。詳細情報は、*11章 セキュリティー* を参照してください。

- MD5、SHA0、RC4、または 1024 ビットよりも短い DH といった暗号化プロトコルやアルゴリズムは安全でないとみなされ、廃止されました。また、EXPORT 暗号スイートのサポートも削除されました。詳細は、Red Hat Enterprise Linux 6.9 Technical Notes を参照してください。

Red Hat Insights

Red Hat Enterprise Linux 6.7 以降では、**Red Hat Insights** サービスが利用可能になっています。Red Hat Insights は、使用中のデプロイメントに影響が及ぶ前に既知の技術的問題を特定し、分析、解決することを可能にするよう設計されたプロアクティブなサービスです。Insights は Red Hat Support Engineers、文書化されたソリューション、および解決済みの問題からなる複合情報を活用して、システム管理者に関連性のある実行可能な情報を提供します。

このサービスは、カスタマーポータル https://access.redhat.com/insights/ または Red Hat Satellite でホストされており、そこから提供されます。ご使用中のシステムを登録するには、Getting Started Guide for Insights にある手順に従ってください。データセキュリティーや制限に関する詳細情報は、https://access.redhat.com/insights/splash/ を参照してください。

Red Hat Customer Portal Labs

Red Hat Customer Portal Labs は、カスタマーポータル上で利用できるツールセット (https://access.redhat.com/labs/) です。Red Hat Customer Portal Labs のアプリケーションは、パフォーマンスの改善、迅速なトラブルシュート、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と設定に役立ちます。一般的なアプリケーションは以下の通りです。

- Kickstart Configurator

- Registration Assistant

- NFS Helper

- Linter for Dockerfile
- Multipath Helper
- iSCSI Helper
- Code Browser

パート I. 新しい機能

ここでは Red Hat Enterprise Linux 6.9 に導入された新機能および主な機能強化について説明しています。

第2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では、既存のオペレーティングシステムを置換することで Red Hat Enterprise Linux の新たなメジャーリリースにシステムをアップグレードすることができます。インプレースアップグレードを実行するには、実際のアップグレード実行前にすべてのアップグレード問題を検査するユーティリティーである **Preupgrade Assistant** を使用します。これは、**Red Hat Upgrade Tool** 向けの追加スクリプトも提供します。**Preupgrade Assistant** が報告したすべての問題を解決したら、**Red Hat Upgrade Tool** を使ってシステムをアップグレードします。

手順およびサポートされるシナリオの詳細については、Migration Planning Guide と Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 7 への移行方法 を参照してください。

Preupgrade Assistant と **Red Hat Upgrade Tool** は Extras channel から入手できます。

preupgrade-assistant がバージョン 2.3.3 にリベース

preupgrade-assistant パッケージがバージョン 2.3.3 にアップグレードされ、バグ修正および以下のような機能拡張が加えられています。

- 新規ツール **`preupg-diff`** が追加され、複数の Preupgrade Assistant XML レポートを比較します。特定されていない問題のレポートと既に分析済みの問題のレポートを比較します。これにより、新規レポートと少なくとも 1 つの分析済み XML ファイルをフィルターにかけることで、新規レポートに現れた問題が見つけやすくなります。短縮されたレポートの出力は、XML と HTML の形式で入手できます。

- 新たなリターンコードが 2 つ追加されました。**`29`** は **`internal error`**、**`30`** は **`user abort`** になります。

- リターンコード **`22`** の意味が **`invalid CLI option`** に変更されました。

- Preupgrade Assistant の STDOUT および STDERR 出力は、2 つの分野に分けられました。**`Additional output`** は STDOUT に、**`Logs`** は STDERR になります。

- Python で書かれた Preupgrade Assistant モジュールがインポートする **`python`** モジュールの名前が、**`preup`** から **`preupg`** に変更されました。また、**`preup_ui_manage`** 実行可能ファイルも **`preupg-ui-manage`** に名前が変更されました。

- **`exit_unknown`** 関数と **`$RESULT_UNKNOWN`** 変数が削除されました。**`unknown`** 結果ではなく、**`exit_error`** 関数を使ってエラー結果を設定します。

- **`set_component`** モジュールの API 関数が削除されました。

- **`component`** 入力パラメーターが以下のモジュール API 関数から削除されました。**`log_error`**、**`log_warning`**、**`log_info`**、および **`log_debug`**。(BZ#1427713, BZ#1418697, BZ#1392901, BZ#1393080, BZ#1372100, BZ#1372871)

Preupgrade Assistant がブラックリスト化をサポートしてパフォーマンスが改善されます

Preupgrade Assistant がブラックリストファイルの作成をサポートするようになり、リスト化された接頭辞のあるパス上の実行可能ファイルすべてを省略できるようになりました。この機能は **`/etc/preupgrade-assistant.conf`** ファイルの **`xccdf_preupg_rule_system_BinariesRebuild_check`** セクションで **`exclude_file`** の値を設定すると有効になります。例を示します。

```
[xccdf_preupg_rule_system_BinariesRebuild_check]
exclude_file=/etc/pa_blacklist
```

ブラックリストファイルの各行には、除外する実行可能ファイルのパスの接頭辞を含めます。これまでは、大きなパーティションがマウントされ、**RHEL6_7/system/BinariesRebuild** モジュールが実行可能ファイルのリストにある数多くのファイルをチェックする際に、大きなパフォーマンス上の問題が発生していました。今回の更新で、重要でない実行可能ファイルをフィルターで除外することで、モジュールが消費する時間を節約することが可能になっています。この機能は今後、変更が加えられる予定であることに注意してください。(BZ#1392018)

Preupgrade Assistant モジュールの主要ファイル名が統一されました

これまでは、Preupgrade Assistant の各モジュールで特定の必須ファイルに異なるファイル名を使用しており、テストと方向性が複雑になっていました。今回の更新では、主要なファイル名が各モジュールで **module.ini** (メタデータ INI ファイル)、**check** (チェックスクリプト)、および **solution.txt** (ソリューションテキスト) に統一されました。また、複数のルール (モジュール ID) の名前がこれに合わせて変更され、たとえば、**result.html** と **result.xml** のファイルで各ルールには統一された **_check** 接尾辞が含まれるようになります。

新 **RHDS** モジュールが **RHDS** システムにおけるインプレースアップグレードの可能性をチェックします

今回の更新では新たな Red Hat Directory Server (RHDS) モジュールが導入され、関連するインストール済み RHDS パッケージをチェックして RHDS システムのインプレースアップグレードの可能性について情報を提供します。このため、関連パッケージがインストールされており、基本的なディレクトリーインスタンスが設定されていると、このモジュールは設定ファイルのバックアップを作成し、それについての情報をプリントします。(BZ#1406464)

cloud-init をベースチャネルに移動

Red Hat Enterprise Linux 6.9 から、cloud-init パッケージとその依存関係は Red Hat Common チャネルからベースチャネルに移動されました。**Cloud-init** は、環境が提供するメタデータを使ってシステムの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の設定に使用されます。cloud-init パッケージは、Red Hat Common チャネルで提供されている最新バージョンから更新されていないことに注意してください。(BZ#1421281)

第3章 認証および相互運用性

AD フォレストから連絡を受けるドメインを管理者がSSSD で選択できるようになりました

環境によっては、ジョインされた Active Directory (AD) フォレストないのドメインのサブセットしか到達できない場合があります。到達不能なドメインに連絡しようとすると、タイムアウトになったり、System Security Services Daemon (SSSD) がオフラインモードに切り替えられたりします。

これを回避するために、管理者が **/etc/sssd/sssd.conf/** ファイルの **ad_enabled_domains** オプションを設定することで、SSSD が接続するドメイン一覧を設定できるようになりました。詳細は、sssd-ad(5) man ページを参照してください。(BZ#1324428)

pam_sss から環境変数を受信しない PAM サービス一覧を SSSD で選択できるようになりました

場合によっては、**pam_sss** Pluggable Authentication Module (PAM) が設定した環境変数を反映しない方が良いこともあります。たとえば **sudo -i** コマンドの使用時に、元のユーザーの **KRB5CCNAME** 変数をターゲット環境に送信したい場合などです。

これまでは、権限のないユーザーが **sudo -i** コマンドを使用して別の権限のないユーザーになると、この新たな権限のないユーザーには、**KRB5CCNAME** がポイントする Kerberos 認証情報キャッシュを読み取るパーティションが与えられませんでした。

このユースケースにおいて、今回の更新では **pam_response_filter** という新オプションが追加されました。**pam_response_filter** を使用すると、管理者はログイン中に **KRB5CCNAME** のような環境変数を受け取らない PAM サービス (例: **sudo-i**) を一覧表示できます。**pam_response_filter** が **sudo-i** を一覧表示することで、ユーザーはターゲット環境で **KRB5CCNAME** を設定せずにある権限のないユーザーか別の権限のないユーザーに切り替わることができます。(BZ#1329378)

IdM サーバーで TLS 1.2 以上を必須とするように設定できるようになりました

Transport Layer Security (TLS) プロトコルのバージョン 1.2 はこれまでのバージョンよりも大幅に安全であるとみなされています。今回の更新では、Identity Management (IdM) サーバーが **TLS** の 1.2 未満のバージョンを使用した通信を禁止するように設定できるようになりました。

詳細については、以下の Red Hat のナレッジベースの記事を参照してください https://access.redhat.com/articles/2801181。 (BZ#1367026)

pam_faillock の設定で unlock_time=never が利用可能になりました

pam_faillock モジュールで **unlock_time=never** オプションを使用すると、複数回の認証失敗によるユーザー認証のロックが解除されないよう指定することができます。(BZ#1404832)

libkadm5* ライブラリーが libkadm5 パッケージに移動しました。

Red Hat Enterprise Linux 6.9 では、**libkadm5*** ライブラリーが krb5-libs から libkadm5 パッケージに移動しました。そのため、**yum** は krb5-libs パッケージを自動的にダウングレードできません。ダウングレードする前に手作業で libkadm5 パッケージを削除してください。

```
# rpm -e --nodeps libkadm5
```

このパッケージを手作業で削除したら、**yum downgrade** コマンドを使用して krb5-libs パッケージを前のバージョンにダウングレードします。(BZ#1351284)

第4章 クラスタリング

Oracle and OrLsnr Pacemaker リソースエージェントでの **Oracle 11g** のサポートが追加されました

Red Hat Enterprise Linux リソース 6.9 から、Pacemaker リソースエージェント **`Oracle`** と **`OraLsnr`** が Oracle データベース 11g をサポートするようになりました。(BZ#1336846)

`Pacemaker` がアラートエージェントをサポートするようになりました

クラスターイベントの発生時に **`Pacemaker`** アラートエージェントを作成して外部で一部の処理を行うことができるようになりました。 クラスターは環境変数を用いてイベントの情報をエージェントに渡します。エージェントは、E メールメッセージの送信、ログのファイルへの記録、監視システムの更新など、この情報を自由に使用できます。アラートエージェントの設定に関する詳細は、『Pacemaker を使用した Red Hat High Availability Add-On の設定』を参照してください。(BZ#1253325, BZ#1376480)

`clufter` が完全サポートされています

clufter パッケージは、クラスター設定の形式を変換/分析するツールを提供し、旧スタック設定から Pacemaker を活用した新設定への移行支援に使用できます。**`clufter`** ツールはこれまでテクノロジープレビューとして提供されていましたが、今回の更新では完全にサポートされています。**`clufter`** の機能に関する情報は、**`clufter(1)`** の 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`** の使用例については、以下の Red Hat ナレッジベースの記事を参照してください: https://access.redhat.com/articles/2810031。(BZ#1318326)

clufter がバージョン **0.59.8** にリベースされました

clufter パッケージは、アップストリームのバージョン 0.59.8 にアップグレードされました。このバージョンでは、多数のバグが修正され、以前のバージョンに比べて数多くの機能が拡張されて、ユーザーエクスペリエンスが向上しました。中でも注目すべき更新点は以下のとおりです。

- CMAN または Pacemaker スタック固有の設定を **`*2pcscmd`** のコマンドファミリーを使用する **`pcs`** コマンドの 各シーケンスに変換する際に、後に続くローカル変更の **`pcs`** コマンドには現在機能しない **`clufter`** ツールは **`pcs cluster cib file --config`** を候補に表示しなくなりました。その代わりに、**`pcs cluster cib file`** が候補として表示されます。(RHBZ#1328078)

- **`clufter`** ツールの出力は、指定したディストリビューションターゲットによって、大幅に異なるようになりました。これは、その環境が何をサポート可能であるか (例: **`pcs`** のバージョンなど) に応じてツールの出力が調整されるようになったためです。このため、お使いのディストリビューションまたは環境がサポートされていない可能性があり、 **`clufter`** ツールが生成する単一の **`pcs`** コマンドシーケンスは完全に異なる環境に移植可能であると想定しないようにする必要があります。

- **`clufter`** は、通知ハンドラーを含む、**`pcs`** ツールの新機能を複数サポートするようになりました。また、**`clufter`** ツールは、チケットの制約やコロケーション用のリソースセット、順序の制約など、**`pcs`** ツールに最近追加されていた以前の機能もサポートします。

- CMAN および RGManager スタック固有の設定を、**`ccs2pcs*`** ファミリーのコマンドで各 Pacemaker 設定 (もしくは同じモノを反映する **`pcs`** コマンドのシーケンスで) 変換する際に、**`clufter`** ツールは以前は拒否していた有効な lvm リソースエージェント設定を拒否しなくなりました。(BZ#1367536)

`luci` インターフェースで管理者がリモートマシンの信頼性を確認できるようになりました

暗号化チャネルは、ある程度の安全性を確保して、中間者攻撃に対して保護するためにエンドポイント間で確立された信頼性を必要とします。**`luci`** を使用してクラスターを管理している管理者には、新規

クラスターを作成し、ノードをクラスターに追加、または既存のクラスターを luci の管理に追加する際に入力されたクラスターノードに対応する証明書フィンガープリントが自動的に提供されるようになりました。これにより、管理者は標準の逆認証 (リモートに対する自分の認証) 中に認証情報をでリモートノードを信頼する前に、リモートマシンの信頼性を先に確認することができます。(BZ#885028)

luci が個別リソースの明示的な設定済みアクションを一覧表示します

クラスターの設定では、特定リソースの設定済みアクションを見直しできると便利です。**status** アクションの **depth** パラメーターなど、暗黙的な操作がユーザー設定で上書きされたことを検証する場合などに特に便利です。より一般的には、設定済みアクションを見直すことができると、暗黙的アクションへの修正や追加による現行クラスター動作への影響が分かります。

luci は **Service Groups** ブレイクダウンビューで個別のリソースごとの設定済みアクションを一覧表示するようになり、特定のアクションで無視されるパラメーターを表示し、それらが enforced として設定されている場合は、タイムアウトを強調表示します。このビューでは、アクションのアクティブな修正はできないことに注意してください。アクションを修正する場合は、**ccs** CLI ツールの **--addaction** と **--rmaction** のパラメーターを使用します。(BZ#1173942)

第5章 コンパイラーとツール

el_GR@euro、ur_IN、および wal_ET ロケールのサポートが追加されました

el_GR@euro、ur_IN、および wal_ET ロケールはユーロなどの新たな通貨記号に特化されたサポートを提供し、これらのロケールがサポートされていなかったインスタンスが完全にサポートされるようになりました。

ユーザーは関連する環境変数を使用してこれらのロケールを指定し、新たなローカライゼーションサポートを活用できます。(BZ#1101858)

`Net:SSLeay` Perl モジュールが TLS バージョンの制限をサポートするようになりました

`Net:SSLeay` Perl モジュールが更新され、セキュリティー改善に使用可能な TLS プロトコルのバージョンを明示的に指定できるようになりました。TLS をバージョン 1.1 または 1.2 に限定するには、**`Net::SSLeay::ssl_version`** の変数をそれぞれ **`11`** もしくは **`12`** に設定します。(BZ#1325407)

`IO::Socket::SSL` Perl モジュールが TLS バージョンの制限をサポートするようになりました

`Net:SSLeay` Perl モジュールが更新され、セキュリティー改善に使用可能な TLS プロトコルのバージョンを明示的に指定できるようになったのを受け、**`IO::Socket::SSL`** モジュールも更新されました。新規 **`IO::Socket::SSL`** オブジェクトの作成時に、**`SSL_version`** オプションを **`TLSv1_1`** または **`TLSv1_2`** に設定すると、TLS をバージョン 1.1 または 1.2 にそれぞれ限定することができます。別の方法では、**`TLSv11`** および **`TLSv12`** を使用することもできます。これらの値は、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#1331037)

ca-certificates がバージョン 2.10 にリベース

証明書ストアが更新され、Mozilla Foundation が発行する証明機関証明書リストのバージョン 2.10 に含まれる変更点が Network Security Services (NSS) バージョン 3.27 の一部に含まれるようになりました。既存の PKI デプロイメントおよび OpenSSL と GnuTLS ベースのソフトウェアとの互換性を維持するために、1024 ビットの RSA キーがある root CA 証明書のいくつかがデフォルトで信頼済みとして保持されています。これらレガシーの修正を無効にする方法については、以下のナレッジベースの記事を参照してください。https://access.redhat.com/articles/1413643 (BZ#1368996)

第6章 RED HAT ENTERPRISE LINUX での DIRECTORY サーバー

Directory サーバーが特定の TLS バージョンの有効化および無効化に対応

これまでは、Red Hat Enterprise Linux 6 で稼働する Directory サーバーには特定の TLS バージョンを有効、無効にするオプションがありませんでした。たとえば、セキュアでない TLS 1.0 プロトコルを無効にしつつ、それ以降のバージョンを有効にするということができませんでした。今回の更新では、**nsTLS10**、**nsTLS11**、および **nsTLS12** のパラメーターが **cn=encryption,cn=config** エントリーに追加されています。これによって、Directory サーバーで特定の TLS プロトコルバージョンを設定することが可能になりました。

これらのパラメーターは、すべての TLS プロトコルバージョンを有効、無効にする **nsTLS1** パラメーターよりも優先されることに注意してください。(BZ#1330758)

第7章 ハードウェアの有効化

`cpuid` が利用できるようになりました。

今回の更新により、Red Hat Enterprise Linux で **`cpuid`** ユーティリティーが利用できるようになりました。このユーティリティーは、CPUID 命令から収集される CPU についての詳細情報をダンプするのに加えて、具体的な CPU モデルを特定するツールで、Intel、AMD、VIA の CPU に対応しています。(BZ#1316998)

RealTek RTS5250S SD4.0 コントローラーのサポート

Realtek RTS5205 カードリーダーコントローラーがカーネルに追加されました。(BZ#1167938)

第8章 インストールと起動

NO_DHCP_HOSTNAME オプションが追加されました

NO_DHCP_HOSTNAME オプションを **/etc/sysconfig/network** 設定ファイルで指定できるようになりました。これまでは、静的設定を使用している場合でも、初期化スクリプトが DHCP でホスト名を取得することを回避することができないことがありました。今回の更新では、**NO_DHCP_HOSTNAME** オプションを **/etc/sysconfig/network** ファイルで **yes**、**true**、**1** のいずれかに設定すると、初期化スクリプトはホスト名を DHCP から取得できなくなります。(BZ#1157856)

第9章 カーネル

Chelsio ファームウェアをバージョン 1.15.37.0 に更新

Chelsio ファームウェアがバージョン 1.15.37.0 に更新されました。これには、多くのバグ修正および機能拡張が加えられています。

主なバグ修正は以下の通りです。

- `iscsi tlv` ドライバーが間違ってホストに送信されることがなくなりました。
- Data Center Bridging Capability Exchange (DCBX) プロトコルの有効および無効化によってファームウェアが予期せず終了することがなくなりました。
- app 優先度の値がファームウェアで正常に処理されるようになりました。(BZ#1349112)

`bnxt_en` ドライバーを最新のアップストリームバージョンに更新

`bnxt_en` ドライバーが複数のマイナーフィクスで更新され、BCM5731X、BCM5741X、および 57404 のネットワークパーティション設定 (NPAR) デバイスをサポートするようになりました。(BZ#1347825)

`ahci` ドライバーが Marwell 88SE9230 をサポート

`ahci` ドライバーが Marvell 88SE9230 コントローラーをサポートするようになりました。(BZ#1392941)

第10章 ネットワーク

`NetworkManager` が手動の DNS 設定 `dns=none` オプションに対応
今回の更新では、**`NetworkManager`** による**`/etc/resolv.conf`** ファイルの修正を回避するオプションが加わりました。これは、DNS 設定の手動での管理に便利です。ファイルの修正を防ぐには、**`dns=none`** オプションを **`/etc/NetworkManager/NetworkManager.conf`** ファイルに追加します。(BZ#1308730)

第11章 セキュリティー

すべてのシステムコンポーネントに TLS 1.2 サポートが追加されました

GnuTLS コンポーネントに **TLS** 1.2 サポートが追加されたことで、Red Hat Enterprise Linux 6 は **OpenSSL**、**NSS**、および **GnuTLS** の同梱セキュリティーライブラリー内の **TLS** 1.2 を完全サポートします。PCI-DSS v3.1 を含む複数の最新標準で、最新の **TLS** プロトコルである **TLS** 1.2 を推奨しています。これが追加されたことで、**TLS** 1.2 のサポートを必須とする可能性のある将来のセキュリティー標準改訂で Red Hat Enterprise Linux 6 が使用可能になります。

Red Hat Enterprise Linux 6 における暗号化変更の詳細については、以下の Red Hat カスタマーポータルの記事を参照してください。https://access.redhat.com/blogs/766093/posts/2787271 (BZ#1339222)

OpenSCAP 1.2.13 が NIST 認定を受けました

OpenSCAP 1.2.13 は、米国標準技術局 (NIST) の Security Content Automation Protocol (SCAP) 1.2 により、認証設定カテゴリーの Common Vulnerabilities and Exposure (CVE) オプションで認証されています。**OpenSCAP** は、SCAP 標準の各コンポーネントを分析して評価することが可能なライブラリーを提供します。これにより、新たな SCAP ツールの作成が容易になります。また、**OpenSCAP** は、コンテンツをドキュメントに書式設定したり、このコンテンツに基づいてシステムをスキャンするように設計されている多目的ツールを提供します。(BZ#1364207)

vsftpd がデフォルトで TLS 1.2 を使用します

Very Secure File Transfer Protocol (FTP) デーモン (vsftpd) のユーザーは、最大 1.2 までの **TLS** プロトコルのバージョンを選択できるようになりました。**TLS** 1.2 はデフォルトで有効にされ、vsftpd のセキュリティーレベルは Red Hat Enterprise Linux 7 のパッケージのものと同等レベルに引き上げられています。**TLS** 1.2 に固有の新たなデフォルトの暗号である **ECDHE-RSA-AES256-GCM-SHA384** と **ECDHE-ECDSA-AES256-GCM-SHA384** が追加されました。これらの変更は、既存設定に影響しません。(BZ#1350724)

auditd が incremental_async をサポートするようになりました

audit デーモンが **incremental_async** と呼ばれる新たなフラッシュ技術をサポートするようになりました。この新規モードは、セキュリティーのためにフラッシュの間隔を短く保ちながら **audit** デーモンのロギングパフォーマンスを大幅に改善します。(BZ#1369249)

scap-security-guide が ComputeNode をサポートします

scap-security-guide プロジェクトが Red Hat Enterprise Linux の ComputeNode バリアントのスキャンをサポートするようになり、scap-security-guide パッケージは関連チャネルで配布されるようになっています。(BZ#1311491)

rsyslog7 が TLS 1.2 を有効にします

今回の更新で、**rsyslog7** マルチスレッド syslog デーモンが、**GnuTLS** コンポーネント内の **TLS** 1.2 を明示的に有効にするようになりました。(BZ#1323199)

第12章 サーバーとサービス

Microsoft Azure クラウド向け DDNS 用の DHCP クライアントフック例を追加

Microsoft Azure クラウド向け DDNS 用の **DHCP** クライアントフックの例が dhcp パッケージに追加されました。管理者はこのフックを有効にして、Red Hat Enterprise Linux クライアントを容易に **DDNS** サーバーに登録することができます。(BZ#1321945)

postfix がユーザー制御の TLS 設定をサポート

今回の更新では、postfix でより正確な Transport Layer Security (TLS) プロトコルバージョンを制御する設定オプションが提供されています。たとえば、**TLS** v1.1 を無効にしながら **TLS** v1.2 を有効にするということが可能になっています。これを実行するには、**main.cf** ファイルに以下の行を追加します。

```
smtpd_tls_mandatory_protocols = !TLSv1.1
```

(BZ#1287192)

第13章 ストレージ

smartPQI (`smartpqi`) ドライバーが利用可能になりました

今回の更新では smartPQI (**smartpqi**) ドライバーが、2017 から利用可能になっている新たな Microsemi ストレージアダプターハードウェア用に提供されています。この新規ハードウェアは、Red Hat Enterprise Linux 6.5、6.6、6.7、および 6.8 の **aacraid** ドライバーとも使用できましたが、**aacraid** ドライバーと比べると、**smartpqi** ドライバーではパフォーマンスが改善され、機能が強化されています。

Red Hat Enterprise Linux 6.8 から Red Hat Enterprise Linux 6.9 に移行すると、ドライバーが **aacraid** から **smartpqi** に変更されます。標準のインストール設定が使用されていれば、このドライバー変更はユーザーには透過的で、アクションは不要です。Red Hat Enterprise Linux 6.9 の起動後に新たな **smartpqi** ドライバーが自動的に使用されます。(BZ#1343743)

`mpt3sas` の更新

mpt3sas ストレージドライバーがバージョン 14.100.00.00-rh に更新され、以下の PCI ID の新規デバイスをサポートするようになりました。

- 0x1000:0x00AA
- 0x1000:0x00AB SAS3516 Fusion-MPT Tri-Mode RAID On Chip (ROC)
- 0x1000:0x00AC SAS3416 Fusion-MPT Tri-Mode I/O Controller Chip (IOC)
- 0x1000:0x00AD
- 0x1000:0x00AE SAS3508 Fusion-MPT Tri-Mode RAID On Chip (ROC)
- 0x1000:0x00AF SAS3408 Fusion-MPT Tri-Mode I/O Controller Chip (IOC) (BZ#1306469)

`megaraid_sas` の更新

megaraid_sas ドライバーがバージョン 07.700.00.00-rc1 に更新され、以下の PCI ID の新規デバイスをサポートするようになりました。

- 0x1000:0x0014
- 0x1000:0x0016
- 0x1000:0x0017
- 0x1000:0x001B
- 0x1000:0x001C (BZ#1306457)

Huawei XSG1 アレイ向けの新規デフォルト設定が `device-mapper-multipath` に追加されました

Red Hat Enterprise Linux 6 では、Huawei XSG1 アレイ用に **device-mapper-multipath** ツール設定で特別な設定が推奨されています。この設定がデフォルトで使用されるようになりました。(BZ#1333334)

`disable_changed_wwids` `multipath.conf` オプションがマルチパスで利用可能になり、データ破損が避けられます

マルチパスツールに **disable_changed_wwids** **multipath.conf** オプションが追加されました。**disable_changed_wwids** を **yes** に設定すると、**multipathd** サービスがパスデバイスを監視

し、World Wide Identifier (WWID) に変更があると、WWID の変更が戻るまで **multipathd** がパスデバイスへのアクセスを無効にします。

論理ユニット番号 (LUN) 上にマルチパスデバイスが存在する間に LUN がリマップされると、場合によっては I/O が間違った LUN に書き込まれる可能性があり、データ破損につながります。間違った LUN への書き込みは **multipathd** が検出し、これが LUN WWID の変更を登録して、デバイスへのアクセスを無効にします。

LUN がリマップされる時と **multipathd** にデバイス変更が通知される時のギャップのために、場合によってはデータ破損のリスクがなくなることはなく、使用中の LUN のリマップはまだサポートされていないことに注意してください。(BZ#1377532)

device-mapper-multipath が **max_sectors_kb** 設定パラメーターをサポートします

今回の更新で、**device-mapper-multipath** は **max_sectors_kb** パラメーターを **multipath.conf** ファイルのデフォルト、デバイス、およびマルチパスセクションでサポート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の初回アクティベート前にマルチパスデバイスのすべての基本的なパスで **max_sectors_kb** デバイスキューパラメーターを特定の値に設定することができます。

マルチパスデバイスの作成時には、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容易にこれらの値が設定でき、無効なサイズの I/O 操作が渡されることを回避できます。(BZ#1355669)

kpartx パーティション作成を省略できる **skip_kpartx multipath.conf** オプションが追加されました

今回の更新では、デバイスにパーティションテーブルがある場合でも、パーティションを作成せずにマルチパスデバイスが作成できるようになりました。マルチパスデバイスを **skip_kpartx** オプションで設定すると、マルチパスデバイス向けのパーティションデバイスは作成されません。(BZ#1310320)

multipathd が稼働していない場合にマルチパスデバイスを作成すると、警告が表示されます

今回の更新では、**multipathd** サービスが稼働していない場合にマルチパスデバイスを追加、一覧表示すると、警告が表示されます。(BZ#1305589)

第14章 仮想化

設定オプションで脆弱な暗号を除外できる

これまでは、libvirt は **GnuTLS** のデフォルトであるハードコード化された暗号に依存していました。このため、脆弱な暗号を使用することが可能でした。今回の更新では、**libvirtd.conf** と **libvirt.conf** のファイルに脆弱な暗号を除外する設定オプションが追加されました。さらに、**TLS** 優先度サポートが libvirt URI に追加されたので、使用済み暗号のリストをカスタマイズして脆弱な暗号を除外できます。(BZ#1333415)

Hyper-V ストレージドライバーのパフォーマンスが改善

storvsc Hyper-V ストレージドライバーがアップストリームから更新されました。これにより、特定のワークロードに Hyper-V storvsc ドライバーを使用する際の I/O 操作のパフォーマンスが強化されました。(BZ#1352824)

Hyper-V クロックソースが TSC ページを使用するように変更されました

今回の更新により、タイムスタンプカウンター (TSC) ページが Hyper-V クロックソースとして使用されます。TSC ページは、これまで使用されたモデル固有レジスター (MSR) よりも効率的なゲスト別の参照カウンター値の計算方法になります。これにより、タイムスタンプの読み取りが関係するカーネル操作がより高速になります。

この機能は 64-bit カーネルでのみサポートされることに注意してください。(BZ#1365049)

すべてのゲストユーザーにアカウントパスワードの設定が可能

guest-set-user-password コマンドが QEMU ゲストエージェント用に導入され、QEMU および KVM 使用時に root を含むすべてのゲストユーザーにアカウントパスワードを設定できるようになりました。(BZ#1303906)

第15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、関連パッケージなどを提供する Red Hat のコンテンツセットのことで、AMD 64 および Intel 64 アーキテクチャーをベースにした Red Hat Enterprise Linux 6 および Red Hat Enterprise Linux 7 のサポートされているどのリリースに対してもインストールして使用することができます。Red Hat Developer Toolset は、別の Software Collection として含まれています。

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おり、最新版の GNU Compiler Collection、GNU Debugger、その他の各種開発用ツールやデバッグ用ツール、パフォーマンス監視用ツールなども提供しています。Red Hat Developer Toolset 以降のバージョンでは、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 では、**scl** ユーティリティーをベースにした別のパッケージメカニズムを使用しており、複数のパッケージセットを並行して提供できます。Red Hat Software Collections を利用すると、Red Hat Enterprise Linux で別のバージョンをオプションで使用できます。**scl** ユーティリティーを使用すると、いつでも任意のパッケージバージョンを選択して実行することができます。

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 製品ライフサイクル」を参照してください。

Red Hat Software Collections のセットに収納されているコンポーネント、システム要件、既知の問題、使い方、各 Software Collection の詳細などについては Red Hat Software Collections のドキュメント を参照してください。

Red Hat Software Collections の一部となる Red Hat Developer Toolset に収納されているコンポーネント、インストール、使い方、既知の問題など詳細については Red Hat Developer Toolset のドキュメント を参照してください。

パート II. 既知の問題

ここでは Red Hat Enterprise Linux 6.9 の既知の問題について説明します。

第16章 全般的な更新

Dovecot の **first_valid_uid** のデフォルト値が **Red Hat Enterprise Linux 7** で変更される

Red Hat Enterprise Linux 7.3 以降、**Dovecot** の **first_valid_uid** 設定オプションのデフォルト値が Red Hat Enterprise Linux 6 の **500** から **1000** に変更されました。このため、Red Hat Enterprise Linux 6 インストールで **first_valid_uid** を明示的に定義しないと、Red Hat Enterprise Linux 7 への更新後に **Dovecot** 設定は UID が **1000** 未満のユーザーによるログインを許可しなくなります。

この設定の齟齬を回避するには、**/etc/dovecot/conf.d/10-mail.conf** ファイル内の **first_valid_uid** を **500** に再定義します。この問題の影響を受けるのは、**first_valid_uid** が明示的に定義されていないインストールのみであることに留意してください。(BZ#1388967)

Red Hat Enterprise Linux 7 でサービスの予期されるデフォルト設定についての情報が誤っている

起動スクリプトを処理する Preupgrade Assistant は、Red Hat Enterprise Linux 7 では **/usr/lib/systemd/system-preset/90-default.preset** ファイルに従って、Red Hat Enterprise Linux 6 では現行設定に従ってサービスの予期されるデフォルト設定について間違った情報を提供します。さらに、このモジュールはシステムのデフォルト設定をチェックせず、チェックスクリプトの処理中に使用されるランレベルの設定のみをチェックします。これは、システムのデフォルトのランレベルではない可能性があります。このため、起動スクリプトは予期される方法では処理されず、新規システムでは本来よりも多くの手動操作が必要になります。ただし、想定されるデフォルト設定にもかかわらず、関連サービスに選択される設定についてユーザーは情報提供されます。

アップグレードの後、**named-chroot** サービスでは、手動で作成された設定は正常に機能しない可能性がある

named-chroot サービスを使用し、**/var/named/chroot/** ディレクトリー内に手動で作成した独自の設定ファイルがある場合、このサービスは、Red Hat Enterprise Linux 7 へのアップグレード後にターゲットシステムで正常に機能しない可能性があります。使用している設定ファイルの **options** セクションには、**session-keyfile** および **pid-file** ディレクティブが格納されている必要があります。以下に例を示します。

```
session-keyfile "/run/named/session.key";
pid-file "/run/named/named.pid";
```

Preupgrade Assistant モジュールは、**/var/named/chroot/** ディレクトリー内に手動で作成されたファイルを確認したり、修正したりしません。この問題を回避するには、上記に示した例を **options** セクションに手動で挿入します。手動で作成した独自の設定ファイルが **/var/named/chroot/** にない場合、**/etc/named.conf** ファイルを含む **bind** の設定ファイルが使用されます。これらの設定ファイルは、**Preupgrade Assistant** モジュールによって確認および修正されます。(BZ#1473233)

第17章 認証および相互運用性

SSSD が IdM LDAP ツリーからの sudo ルールの管理に失敗する

System Security Services Daemon (SSSD) は現在、デフォルトで IdM LDAP ツリーを使用します。このため、sudo ルールを非 POSIX グループに割り当てることができません。この問題を回避するには、**/etc/sssd/sssd.conf** ファイルを修正し、ドメインが **compat** ツリーを再度使用するように設定します。

```
[domain/EXAMPLE]
...
ldap_sudo_search_base = ou=sudoers,dc=example,dc=com
```

こうすることで、SSSD は sudo ルールを **compat** ツリーから読み込むようになり、ルールを非 POSIX グループに割り当てることができるようになります。

Red Hat では、sudo ルールで言及されるグループを POSIX グループと設定するよう推奨しています。(BZ#1336548)

winbindd が新規 AD 信頼のインストール時にクラッシュする

新規にインストールされたシステムで新たな Active Directory (AD) 信頼を設定すると、**winbindd** サービスが予期せず終了したと **ipa-adtrust-install** ユーティリティーが報告する場合があります。この報告がなければ、**ipa-adtrust-install** は正常に完了しています。

この問題が発生したら、**ipa-adtrust-install** を実行した後に **ipactl restart** コマンドを使用して IdM サービスを再起動します。これで **winbindd** も再起動します。

この問題による機能面での影響については、完全に分かっているわけではないことに注意してください。信頼の機能のなかには、**winbindd** を再起動するまで機能しないものもあります。(BZ#1399058)

ネットワーク接続が完全に確立される前に nslcd を起動すると、ユーザーやグループのアイデンティティーの解決に失敗する

ローカルの LDAP ネームサービスデーモンである **nslcd** をネットワーク接続が完全にアップする前に起動すると、デーモンが LDAP サーバーへの接続に失敗します。このため、ユーザーやグループのアイデンティティーの解決に失敗します。この問題を回避するには、ネットワーク接続が確立されてから **nslcd** を起動します。(BZ#1401632)

第18章 デスクトップ

`vmware` ドライバーが複数画面をサポートしない

X11 window 向けの **`vmware`** ビデオドライバーには、複数画面サポートに関連する特定の機能がありません。このため、VMware 上で稼働する Red Hat Enterprise Linux 6 ゲストは正常に複数画面を使用することができず、サポートされるのは単一画面のみになります。

複数画面のサポートが必要な場合は、Red Hat サポートに連絡してください。(BZ#1320480)

VMWare 11 または VMWare 12 での仮想マシンで画面の向きを回転させるとマウスのポインターの動きがおかしくなる

VMWare 11 または VMWare 12 での仮想マシンで画面の向きを回転させても、ポインターの動きは変更されません。これは、**`xorg-x11-drv-vmware`** ドライバーを使用している場合にのみ発生します。このドライバーは、相対軸デバイスではなく絶対軸デバイスを初期化します。ポインターが思ったように動かないのは、ドライバーが元の座標系にマッピングしたままだからです。この問題を回避するには、以下のコマンドを使用するなどして、デバイスを手動で回転させます。

```
xinput set-prop "ImPS/2 Generic Wheel Mouse" "Coordinate Transformation
Matrix" 0 -1 1 1 0 0 0 0 1
```

上記のコマンドは一例にすぎないことに注意してください。一般的には、特定のシナリオによってマトリックスを調節することが必要です。マトリックスが適用されたら、ポインターの動きも画面の向きに一致します。(BZ#1322712, BZ#1318340)

Radeon または Nouveau を使用するとグラフィックスが不正確にレンダリングされる

非常に稀な環境では、 Radeon または Nouveau グラフィックスデバイスドライバーを使用した場合、Xorg サーバー内のバグによってグラフィックスが不正確にレンダリングされる場合があります。例えば、Thunderbird のメッセージペインが正確に表示されないことがあります。

Nouveau の場合の回避策は、以下のように **`WrappedFB`** オプションを **`xorg.conf`** ファイルに追加します。

```
Section "Device"
    Identifier "nouveau-device"
    Driver "nouveau"
    Option "WrappedFB" "true"
EndSection
```

この回避策により X サーバーでの間違った論理が避けられ、Thunderbird のメッセージペインが正常に表示されるようになります。(BZ#1076595)

第19章 RED HAT ENTERPRISE LINUX での DIRECTORY サーバー

Red Hat Enterprise Linux 7 から 6.9 への IdM スキーマ複製が失敗する

Red Hat Enterprise Linux 6.9 のアイデンティティー管理 (IdM) では、Red Hat Enterprise Linux 7.3 の IdM とは異なる **nsEncryptionConfig** オブジェクトクラスのスキーマ定義を使用しています。スキーマ学習メカニズムは定義をマージすることができないため、サーバー間でのスキーマ複製が失敗します。このため、このスキーマに依存するメカニズムは失敗する可能性があります。たとえば、スキーマ違反およびプラグインの失敗、複製の失敗、アクセス制御指示 (ACI) が無視されるなどの事態が発生する可能性があります。今後の Red Hat Enterprise Linux 7.3 更新では、**nsTLS10**、**nsTLS11**、および **nsTLS12** 属性が **nsEncryptionConfig** オブジェクトクラスで許可される属性一覧に追加され、これでこのスキーマに依存するメカニズムにが上記のシナリオで失敗しないようになる予定です。(BZ#1404443)

第20章 インストールと起動

インストーラーが間違った数のマルチパスデバイスと選択されたマルチパスデバイスを表示する

マルチパスデバイス自体は正常に設定されても、インストーラーが間違った数のマルチパスデバイスと選択されたマルチパスデバイスを表示します。現時点では回避策は分かっていません。(BZ#914637)

マルチパス内の間違ったディスク領域をインストーラーが表示する

マルチパスデバイス自体は正常に設定されても、インストーラーが間違った数のマルチパスデバイスとディスク領域を表示します。現時点では回避策は分かっていません。(BZ#1014425)

Anaconda の生成する **device.map** 設定ファイルが正しくない場合がある

カーネルの制限により、BIOS ドライブをオペレーティングシステムデバイスにマッピングする **device.map** 設定ファイルは、特定の条件では間違って生成される場合があります。USB キーからインストールする場合は、特にこれが該当します。このため、インストール後に起動に失敗することがあります。この問題を回避するには、**/boot/grub** ディレクトリーにある **device.map** ファイルを手動で更新します。**device.map** を更新してシステム上のデバイスを適切にマッピングするようになると、Red Hat Enterprise Linux 6 は正常に起動するようになります。(BZ#1253223)

手動で定義したデフォルトのルートを **ifup** スクリプトが間違って置換する

デフォルトのルートが手動でルーティングテーブルに追加されると、**GATEWAY** パラメーターが指定された状態で、他のインターフェースを設定する際に、**ifup** スクリプトが間違ってこれを置換します。この問題を回避するには、手動で追加するルートにゼロ以外のメトリックを指定するか、**ifup** でルートを追加する際にゼロ以外のメトリックを指定します。(BZ#1090559)

UEFI のあるシステム上で **Red Hat Enterprise Linux 6** をアップグレードすると、ブートローダーのパスワードが削除される

ブートローダーのパスワードが設定されており、UEFI ファームウェアがあるシステム上で Red Hat Enterprise Linux 6 をアップグレードすると、このパスワードが削除されます。このため、パスワードなしでブートレコードの修正が可能になってしまいます。この問題を回避するには、アップグレード前に **/boot/efi/EFI/redhat/grub.conf** 設定ファイルからパスワード設定のバックアップを作成し、新システムの **/boot/efi/EFI/redhat/grub.conf** ファイルにこの設定を復元します。(BZ#1416653)

第21章 カーネル

一部の NIC ファームウェアは bnx2x ドライバーに反応しない

プリブートドライバーのアンロードシーケンスのバグにより、 **bnx2x** ドライバーがデバイスを引き継いだ後に一部のインターネットアダプターのファームウェアが反応しなくなります。 **bnx2x** ドライバーはこの問題を検出し、以下のメッセージをカーネルログに返します。

```
Storm stats were not updated for 3 times.
```

この問題を回避するには、ハードウェアベンダーが提供する最新の NIC ファームウェアの更新を適用します。これにより、プリブートファームウェアのアンロードが想定どおりに動作し、**bnx2x** がデバイスを引き継いだ後もファームウェアはハングしないようになります。 (BZ#1012684)

e1000e カードが IPv4 アドレスを取得しない

e1000e ネットワークインターフェースカード (NICs) のなかには、システムの再起動後に割り当てられた IPv4 アドレスの取得に失敗するものがあります。この問題を回避するには、以下の行を /etc/sysconfig/network-scripts/ifcfg-<interface> ファイルに追加します。

```
LINKDELAY=10
```

(BZ#822725)

dracut がアップグレードされていないと ecb カーネルモジュールが失敗する

カーネル rpm のみを Red Hat Enterprise Linux 6.7 からバージョン 6.8 にアップグレードする際には、dracut パッケージを最新バージョン (dracut-004-409.el6.rpm) にアップグレードしてください。

dracut をアップグレードすることで **ecb** モジュールが機能します。非 x86 アーキテクチャー上で高度暗号化標準 (AES) の実装を使用する際に、**drbg** カーネルモジュールは **ecb** カーネルモジュールを必要とします。dracut をアップグレードしないと、**drbg** モジュールは機能するものの、**drbg** AES 実装は警告メッセージが出て失敗します。(BZ#1315832)

ゲストが ESXi 5.5 で起動に失敗することがある

VMware ESXi 5.5 ハイパーバイザーで Red Hat Enterprise Linux 7 ゲストを実行する際に、特定のコンポーネントが間違った Memory Type Range Register (MTRR) 値で初期化されるか、起動ごとに MTRR 値が間違って再設定されます。これにより、ゲストのカーネルでパニックが発生したり、ゲストが起動中に応答しなくなったりすることがあります。

この問題を回避するには、`disable_mtrr_trim` オプションをゲストのカーネルコマンドラインに追加して、MTRR が間違って設定された場合にゲストが起動し続けることができるようにします。このオプションを使用した場合は、起動中にゲストにより `WARNING: BIOS bug` というメッセージが表示されますが、無視しても安全です。(BZ#1422774)

キャッシュの間違ったフラッシュによるファイルシステムの破損は修正されたものの、I/O 操作が遅い

megaraid_sas ドライバーのバグのために、システムシャットダウン、再起動、または電源切れの際にディスク書き込みバックキャッシュでファイルシステムが使用されると、以前はファイルシステムの破損がケースによっては発生していました。今回の更新では **megaraid_sas** を修正し、フラッシュキャッシュコマンドを正確に RAID カードに送信します。この結果、RAID カードファームウェアも更新すると、このような状況下では、ファイルシステムは破損しなくなりました。

Broadcom **megaraid_sas** RAID アダプターを使用すると、システムログ (dmesg) の機能を確認できます。適切な機能は以下の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ので、I/O 操作が遅くなる場合があることに留意してください。(BZ#1392499)

第22章 ネットワーク

radvd が競合状態により、予期せず終了することがある

Router Advertisement Daemon (radvd) では、**radvd** タイマー処理に競合状態があります。このため、**radvd** は予期せず終了することがあります。(BZ#1058698)

第23章 セキュリティー

OpenSSL のランタイムバージョンがマスクされているため、アプリケーションが **OpenSSL 1.0.0** で実行する際、 **SSL_OP_NO_TLSv1_1** を使用してはならない

一部のアプリケーションでは **OpenSSL** のバージョンチェックが適切に実行されないため、実際のランタイムバージョンの **OpenSSL** がマスクされ、代わりにビルド時のバージョンが報告されます。このため **SSLeay()** 関数を使用して、現在実行中の **OpenSSL** のバージョンを検出することができません。

さらに、**OpenSSL** 1.0.0 で実行しているときに、**OpenSSL** 1.0.1 の **SSL_OP_NO_TLSv1_1** オプションと同じ値を **SSL_CTX_set_options()** 関数に渡すと、SSL/TLS のサポートが完全になくなります。

この問題を回避するには、別の方法で、現在実行している **OpenSSL** バージョンを検出します。たとえば、**SSL_get_ciphers()** 関数で有効な暗号の一覧を取得し、**SSL_CIPHER_description()** 関数を使用してその一覧を解析して、**TLS** 1.2 の暗号を検索します。**TLS** 1.2 がサポートされるのはバージョン 1.0.1 以降であるため、これにより、**OpenSSL** のバージョンが 1.0.0 以降のものを使用して実行しているアプリケーションが示されます。(BZ#1497859)

第24章 サーバーとサービス

PDF ファイルを cups で上下逆さまに印刷することができない

CUPS 印刷システムでは、印刷ページを上下逆さまに回転させるはずの **lp -d [printer] -o orientation-requested=6 [filename]** コマンドの **-o orientation-requested=6** オプションが機能しません。(BZ#1099617)

PDF ファイルを fit-to-page (ページ幅に合わせる) と fitplot のオプションを使用して印刷するとハードウェアマージンのあるプリンターで機能しない

CUPS 印刷システムでは、**lp -d printer-with-hwmargins -o fit-to-page** および **lp -d printer-with-hwmargins -o fitplot** コマンドは、**-o fit-to-page** と **-o fitplot** のオプションを使用してドキュメントがページサイズに収まるようにサイズ変更します。このオプションは、ハードウェアマージンのあるプリンターで PDF ファイルをプリントする際には機能しません。(BZ#1268131)

DHCP クライアントが間違ったインターフェースでユニキャストリクエストを送信する

DHCP クライアントは同一サブネット上で複数のインターフェースをサポートしておらず、ユニキャストリクエストが適切なインターフェースで送信することを保証できません。このため、**DHCP** クライアントはリースの更新に失敗し、ネットワーク設定が機能しなくなります。現時点では回避策はわかっていません。同一サブネットに 2 つのインターフェースが接続されている設定では、**DHCP** クライアントを使用することができません。(BZ#1297445)

pdf2dsc スクリプトで *.pdf ファイルから変換した *.dsc ファイルを Evince で開くことができない

*.pdf (Portable Document Format) ファイルを **pdf2dsc** スクリプトで *.dsc (Document Structure Convention) ファイルに変換し、この変換された *.dsc ファイルを Ghostscript のサンドボックスの外にある Evince GNOME で開くことができなくなりました。これは固定オプション **-dSAFER** によるもので、これにより Ghostscript は強制的にサンドボックスモードで動作します。この問題に対する回避策の詳細は、https://access.redhat.com/articles/2948831 を参照してください。(BZ#1411843)

第25章 システムとサブスクリプション管理

ReaR が eth0 インターフェースでのみ機能する

ReaR は、eth0 以外のインターフェースを使用した NFS サーバーのマウントをサポートしないレスキューシステムを作成します。このため、バックアップファイルのダウンロードとシステムの復旧ができません。この問題を回避するには、dhclient を再起動して、使用しているインターフェースが eth0 であることを確認します。(BZ#1313417)

ReaR が 1 つではなく 2 つの ISO イメージを作成する

ReaR では、**`OUTPUT_URL`** ディレクティブにより レスキューシステムが含まれている ISO イメージの場所を指定することができます。現在、このディレクティブを設定すると、ReaR は、ISO イメージのコピーを 2 つ作成します (指定したディレクトリーに 1 つと **`/var/lib/rear/output/`** のデフォルトディレクトリー 1 つ)。このため、イメージを保管する追加の容量が必要となります。これは、ISO イメージに完全なシステムのバックアップが含まれる場合に特に重要となります (**`BACKUP=NETFS`** と **`BACKUP_URL=iso:///backup/`** の設定を使用)。

この動作による問題を回避するには、ReaR の作業が終了したら追加の ISO イメージを削除するか、イメージをデフォルトのディレクトリーに作成してから希望の場所に手動で移動することにより一定期間にストレージが 2 倍消費されるのを防ぎます。

この動作を変更して、ReaR が ISO イメージのコピーを 1 つだけ作成するようにする機能拡張がリクエストされています。(BZ#1320551)

第26章 仮想化

`Coolkey` が Windows 7 ゲストで読み込まれない

現時点では `Coolkey` モジュールの Windows 7 ゲスト仮想マシンでの読み込みが失敗するので、スマートカードのリダイレクトがこれらのゲストでは正常に機能しません。(BZ#1331471)

Hyper-V ゲストでの vCPU の無効化が失敗する

Microsoft Azure クラウドを含む Microsoft Hyper-V で稼働するゲスト仮想マシン上での CPU の無効化ができません。これは、ホスト側空のサポートがないためです。ただし、カーネルコマンドラインで `nr_cpus=XX` パラメーターを渡してゲストを起動すると、オンラインのCPU 数を減らすことができます。ここまでの `XX` は、必要なオンライン CPU の数になります。

詳細は、https://access.redhat.com/solutions/2790331 を参照してください。(BZ#1396336)

VMware ESX ハイパーバイザーでハードディスクをバッチでホットプラグすると正常に認識されない

VMware ESXi ハイパーバイザー上で稼働している Red Hat Enterprise Linux 6 ゲスト仮想マシンに同時に複数のハードディスクをホットプラグすると、ホストは追加されたディスクすべてをゲストに知らせず、使用できないディスクが出てきます。この問題を回避するには、一度に 1 つのハードディスクをホットプラグするようにします。(BZ#1224673)

ゲストが 1.44 MB を超えるフロッピーディスクにアクセスできない

ゲスト仮想マシンの稼働中に 1.44 MB を超えるフロッピードライブイメージを挿入すると、ゲストはこれにアクセスできません。この問題を回避するには、ゲストの起動前にフロッピードライブイメージを挿入します。(BZ#1209362)

Hyper-V ゲスト統合サービスを無効にしてから再度有効にすると、機能しなくなる

Microsoft Hyper-V 上で稼働する Red Hat Enterprise Linux 6 ゲスト仮想マシンは、データ交換やバックアップといった Hyper-V ゲスト統合サービスを無効にしてから再度有効にすると、`hyperv-daemons` スイートを自動的に再起動しません。このため、Hyper-V Manager インターフェースでこれらのサービスを無効にした後に有効にしても、機能しなくなります。

この問題を回避するには、Hyper-V Manager から統合サービスを再有効化した後に `hypervkvpd`、`hypervvssd`、および `hypervfcopyd` のサービスをゲストで再起動するか、ゲストの稼働中に統合サービスのステータスを変更しないようにします。(BZ#1121888)

古いホスト CPU で `fsgsbase` と `smep` のフラグを使って仮想マシンを起動すると失敗する

`fsgsbase` と `smep` の CPU フラグは、初期の Intel Xeon E プロセッサーなどの特定の古い CPU モデルでは適切にエミュレートされません。このため、これらの CPU のあるホストでゲスト仮想マシンの起動時に `fsgsbase` または `smep` を使用すると、起動に失敗します。この問題を回避するには、CPUが `fsgsbase` および `smep` をサポートしない場合はこれらを使用しないようにします。(BZ#1371765)

`hv_relaxed` を使用すると、最近の Windows システムを稼働するゲストが起動に失敗する場合がある

`-cpu` オプションで `SandyBridge` または `Opteron_G4` の値にし `hv_relaxed` オプションを使用すると、以下のオペレーティングシステムを使った KVM ゲストは起動時に `error code: 0x0000001E` のエラーメッセージが出て起動に失敗します。

- 64-bit Windows 8 以降
- 64-bit Windows Server 2012 以降

この問題を回避するには、`hv_relaxed` を使用しないでください。(BZ#1063124)

Windows 10 および Windows Server 2016 ゲストでの CPU サポートが限定的

Red Hat Enterprise 6 ホスト上では、Windows 10 および Windows Server 2016 ゲストを作成できるのは以下の CPU モデルに限られます。

- Intel Xeon E シリーズ
- Intel Xeon E7 ファミリー
- Intel Xeon v2、v3、および v4
- Opteron G2、G3、G4、G5、および G6

これらの CPU モデルでは、ホスト上で **`virsh capabilities`** コマンドを実行して検出された CPU モデルにゲストの CPU モデルが一致するように設定してください。アプリケーションまたはハイパーバイザーのデフォルトを使用すると、ゲストが正常に起動できなくなります。

Windows 10 ゲストをレガシーの Intel Core 2 プロセッサー (Penryn) または Intel Xeon 55xx および 75xx プロセッサーファミリー (Nehalem) で使用可能とするには、以下のフラグで MODELNAME を Penryn か Nehalemadd に置き換えて Domain XML ファイルに追加します。

```
<cpu mode='custom' match='exact'>
 <model>MODELNAME</model>
 <feature name='erms' policy='require'/>
</cpu>
```

他の CPU モデルはサポートされておらず、これらのモデルで作成された Windows 10 ゲストおよび Windows Server 2016 ゲストは、起動プロセス中に反応しなくなる可能性があります。(BZ#1346153)

vnic を有効にすると、ネットワーク接続が再開されない

`netdev(tap)` リンクをオフに設定し、**`vnic(virtio-net/e1000)`** リンクをオンに設定すると、ネットワーク接続は再開しません。ただし、**`vnic(virtio-net/e1000)`** リンクをオフに設定し、**`netdev(tap)`** リンクをオンに設定すると、ネットワーク接続は再開します。

この問題を解決するには、リンク制御に常に同じデバイスを使用します。 **`netdev(tap)`** リンクをオフに設定していれば、これを使用するとリンクが正常にオンに戻ります。(BZ#1198956)

KVM ゲストは、物理的な DVD/CD-ROM メディアを適切に読み取ることに失敗

物理的な DVD/CD-ROM を KVM ゲスト仮想マシンと使用する際、複数の問題が発生する可能性があります。この問題を回避するには、物理メディアで ISO ファイルを作成し、これを仮想マシンで使用します。物理的な DVD/CD-ROM の使用は推奨されません。詳細は https://access.redhat.com/solutions/2543131. (BZ#1360581) を参照してください。

付録A コンポーネントのバージョン

Red Hat Enterprise Linux 6.9 リリースを構成しているコンポーネントとそのバージョンを以下に示します。

表A.1 コンポーネントのバージョン

コンポーネント	バージョン
Kernel	2.6.32-696
QLogic `qla2xxx` ドライバー	8.07.00.26.06.8-k
QLogic ql2xxx ファームウェア	ql2100-firmware-1.19.38-3.1 ql2200-firmware-2.02.08-3.1 ql23xx-firmware-3.03.27-3.1 ql2400-firmware-7.03.00-1 ql2500-firmware-7.03.00-1
Emulex `lpfc` ドライバー	0:11.0.0.5
iSCSI initiator utils	iscsi-initiator-utils-6.2.0.873-26
DM-Multipath	device-mapper-multipath-0.4.9-100
LVM	lvm2-2.02.143-12

付録B 改訂履歴

改訂 0.2-0.1 **Mon Aug 6 2018** **Terry Chuang**
翻訳ファイルを XML ソースバージョン 0.2-0 と同期

改訂 0.2-0 **Thu Aug 02 2018** **Lenka Špačková**
確認および更新が必要な既知の問題 (ストレージ) を一時的に削除

改訂 0.1-9 **Fri Jul 20 2018** **Lenka Špačková**
ブロックデバイスへの I/O 要求に関連する既知の問題 (ストレージ) を修正

改訂 0.1-8 **Fri Mar 16 2018** **Lenka Špačková**
ライフサイクルに関する注記を更新

改訂 0.1-7 **Wed Nov 29 2017** **Lenka Špačková**
OpenSSL に関する既知の問題を追加

改訂 0.1-6 **Mon Sep 04 2017** **Lenka Špačková**
全般的な更新に関する既知の問題を追加

改訂 0.1-5 **Mon Jul 03 2017** **Jiří Herrmann**
仮想化に関する既知の問題を追加
カーネルに関する既知の問題を追加

改訂 0.1-2 **Thu Apr 27 2017** **Lenka Špačková**
Red Hat Access Labs の名前を Red Hat Customer Portal Labs に変更

改訂 0.1-1 **Fri Mar 31 2017** **Lenka Špačková**
仮想化に関する既知の問題を追加

改訂 0.1-0 **Tue Mar 28 2017** **Lenka Špačková**
仮想化の新機能 1 つと 3 つの既知の問題を追加

改訂 0.0-8 **Tue Mar 21 2017** **Lenka Špačková**
Red Hat Enterprise Linux 6.9 リリースノートの公開

改訂 0.0-4 **Thu Jan 05 2017** **Lenka Špačková**
Red Hat Enterprise Linux 6.9 Beta 版リリースノートの公開