Red Hat Enterprise Linux 8

8.8 リリースノート

Red Hat Enterprise Linux 8.8 リリースノート

Last Updated: 2024-06-08

Red Hat Enterprise Linux 8 8.8 リリースノート

Red Hat Enterprise Linux 8.8 リリースノート

法律上の通知

概要

このリリースノートでは、Red Hat Enterprise Linux 8.8 での改良点および実装された追加機能の概要、この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、テクニカルプレビュー、非推奨機能などの詳細も説明します。 Red Hat Enterprise Linux のインストールは、Installation を参照してください。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
5. ダイアログの下部にある **Create** をクリックします。

第1章 概要

1.1. RHEL 8.8 における主な変更点

インストーラーおよびイメージの作成

Image Builder の主なハイライト:

- Image Builder On-Prem では、Image Builder Web コンソールでブループリントとイメージを作成するための新しく改良された方法が提供されるようになりました。
- RHEL for Edge Simplified Installer イメージタイプが Image Builder Web コンソールで使用できるようになりました。

詳細については、新機能 - インストーラーとイメージの作成 を参照してください。

RHEL for Edge

RHEL for Edge に、RHEL 8.8 の次の新機能が導入されています。

- **simplified-installer** イメージのブループリントでのユーザーの指定がサポートされるようになりました。

詳細は、新機能 - RHEL for Edge を参照してください。

セキュリティー

セキュリティー関連の主なハイライト:

- カーネルの **FIPS モード** 設定が、連邦情報処理標準 (FIPS) 140-3 に準拠するように調整されました。この変更により、多くの暗号化アルゴリズム、関数、および暗号スイートに対して、より厳しい設定が導入されました。
- **Libreswan** IPsec 実装がバージョン 4.9 にリベースされました。
- **fapolicyd** ソフトウェアフレームワークを使用すると、RPM データベースをフィルターできるようになりました。
- **OpenSCAP** セキュリティーコンプライアンスユーティリティーがバージョン 1.3.7 にリベースされました。
- **Rsyslog** TLS 暗号化ログが複数の CA ファイルをサポートするようになりました。
- SELinux ポリシーの更新により、**systemd-socket-proxyd** サービスが独自の SELinux ドメインで実行されるようになりました。

詳細は、新機能 - セキュリティー を参照してください。

動的プログラミング言語、Web サーバー、およびデータベースサーバー

次のアプリケーションストリームの新しいバージョンが利用可能になりました。

- **Python 3.11**
- **nginx 1.22**
- **PostgreSQL 15**

以下のコンポーネントがアップグレードされました。

- Git がバージョン 2.39.1 へ
- Git LFS がバージョン 3.2.0 へ

詳細は、新機能 - 動的プログラミング言語、Web サーバー、およびデータベースサーバー を参照してください。

コンパイラーおよび開発ツール
パフォーマンスツールとデバッガーの更新
RHEL 8.8 では、以下のパフォーマンスツールおよびデバッガーが更新されました。

- Valgrind 3.19
- SystemTap 4.8
- elfutils 0.188

更新されたパフォーマンスモニタリングツール
RHEL 8.8 では、以下のパフォーマンス監視ツールが更新されました。

- PCP 5.3.7
- Grafana 7.5.15

更新されたコンパイラーツールセット
次のコンパイラーツールセットが RHEL 8.8 で更新されました。

- GCC Toolset 12
- LLVM Toolset 15.0.7
- Rust Toolset 1.66
- Go Toolset 1.19.4

詳しくは 新機能 - コンパイラーおよび開発ツール をご覧ください。

RHEL 8 の Java 実装
RHEL 8 AppStream リポジトリーには、以下が含まれます。

- **java-17-openjdk** パッケージ。OpenJDK 17 Java Runtime Environment および OpenJDK 17 Java Software Development Kit を提供します。
- **java-11-openjdk** パッケージ。OpenJDK 11 Java Runtime Environment および OpenJDK 11 Java Software Development Kit を提供します。
- **java-1.8.0-openjdk** パッケージ。OpenJDK 8 Java Runtime Environment および OpenJDK 8 Java Software Development Kit を提供します。

Red Hat build of OpenJDK パッケージは、ポータブル Linux リリースと RHEL 8.8 以降のリリース間で単一のバイナリーセットを共有します。この更新により、ソース RPM から RHEL 上で OpenJDK パッケージを再構築するプロセスが変更されました。新しい再構築プロセスの詳細は、Red Hat build of OpenJDK の SRPM パッケージで利用可能な **README.md** ファイルを参照してください。これは、**/usr/share/doc** ツリーの下にある **java-*-openjdk-headless** パッケージによってもインストールされます。

詳細は、OpenJDK のドキュメント を参照してください。

Web コンソール

RHEL Web コンソールは、LUKS で暗号化されたルートボリュームを **NBDE** デプロイメントにバインドするための追加手順を実行するようになりました。

また、グラフィカルインターフェイスを介して、**DEFAULT:SHA1**、**LEGACY:AD-SUPPORT**、および **FIPS:OSPP** の **暗号化サブポリシー** を適用できるようになりました。

詳細については、新機能 - Web コンソール を参照してください。

コンテナー

主な変更点は、以下のとおりです。

- **podman** RHEL システムロールが利用できるようになりました。
- Fulcio および Rekor を使用した sigstore 署名のクライアントが利用できるようになりました。
- Skopeo は、sigstore キーペアの生成をサポートするようになりました。
- Podman は監査用のイベントをサポートするようになりました。
- Container Tools パッケージが更新されました。
- Aardvark および Netavark ネットワークスタックは、カスタム DNS サーバーの選択をサポートするようになりました。
- ツールボックスが利用可能になりました。
- Podman Quadlet は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。
- **container-tools:3.0** モジュールストリームが非推奨になりました。
- CNI ネットワークスタックは非推奨になりました。

詳細については、新機能 - コンテナー を参照してください。

1.2. インプレースアップグレードおよび OS 移行

RHEL 7 から RHEL 8 へのインプレースアップグレード

現在、考えられるインプレースアップグレードパスは以下のとおりです。

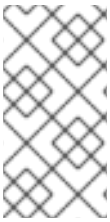
- 64 ビット Intel、IBM POWER 8 (little endian)、IBM Z アーキテクチャーでの RHEL 7.9 から RHEL 8.6 および RHEL 8.8 へのアップグレード。
- カーネルバージョン 4.14 を必要とするアーキテクチャー (IBM POWER 9 (リトルエンディアン) および IBM Z (Structure A)) での RHEL 7.6 から RHEL 8.8.4 のアップグレード。これは、これらのアーキテクチャーの最終のインプレースアップグレードパスです。
- 64 ビット Intel アーキテクチャーの SAP HANA 搭載システム上における、RHEL 7.9 から RHEL 8.6 および RHEL 8.8 へのアップグレード。

詳細は、Supported in-place upgrade paths for Red Hat Enterprise Linux を参照してください。

インプレースアップグレードの実行方法は、RHEL 7 から RHEL 8 へのアップグレード を参照してください。

SAP HANA で RHEL 8.8 にアップグレードする場合は、アップグレード前に、システムが SAP に対して認定されていることを確認してください。SAP 環境があるシステムでインプレースアップグレードを

実行する手順については、How to in-place upgrade SAP environments from RHEL 7 to RHEL 8 を参照してください。



注記

IBM POWER 9 (リトルエンディアン) および IBM Z (structure A) アーキテクチャー用の RHEL 7.6 のインプレースアップグレードを成功させるには、特定の Leapp データを手動でダウンロードする必要があります。詳細は、ナレッジベースの記事 Leapp data snapshots for an in-place upgrade を参照してください。

主な機能拡張は、次のとおりです。

- RHEL のインプレースアップグレードパスストラテジーが変更されました。詳細は、Supported in-place upgrade paths for Red Hat Enterprise Linux を参照してください。
- **leapp-upgrade-el7toel8** パッケージの最新リリースには、必要なデータファイルがすべて含まれるようになりました。これらのデータファイルを手動でダウンロードする必要がなくなりました。
- ターゲットバージョンを含む ISO イメージを使用したインプレースアップグレードが可能になりました。
- RPM 署名がインプレースアップグレード時に自動的にチェックされるようになりました。自動チェックを無効にするには、アップグレードの実行時に **--nogpgcheck** オプションを使用します。
- RHSM にサブスクライブしているシステムが、Red Hat Insights に自動的に登録されるようになりました。自動登録を無効にするには、**LEAPP_NO_INSIGHTS_REGISTER** 環境変数を **1** に設定します。
- Red Hat は、ユーティリティーの使用状況を分析するために、アップグレードの開始時間や終了時間などのアップグレード関連のデータを収集するようになりました。データ収集を無効にするには、**LEAPP_NO_RHSM_FACTS** 環境変数を **1** に設定します。

RHEL 6 から RHEL 8 へのインプレースアップグレード

RHEL 6.10 から RHEL 8 にアップグレードするには、RHEL 6 から RHEL 8 へのアップグレード の手順に従います。

RHEL 8 から RHEL 9 へのインプレースアップグレード

Leapp ユーティリティーを使用して RHEL 8 から RHEL 9 へのインプレースアップグレードを行う方法は、RHEL 8 から RHEL 9 へのアップグレード を参照してください。RHEL 8 と RHEL 9 の主な相違点は、RHEL 9 の導入における検討事項 を参照してください。

別の Linux ディストリビューションから RHEL への移行

CentOS Linux 8 または Oracle Linux 8 を使用している場合は、Red Hat がサポートする **Convert2RHEL** ユーティリティーを使用してオペレーティングシステムを RHEL 8 に変換できます。詳細は、RPM ベースの Linux ディストリビューションから RHEL への変換 を参照してください。

CentOS Linux または Oracle Linux の旧バージョン (バージョン 6 または 7) を使用している場合は、お使いのオペレーティングシステムを RHEL に移行してから、RHEL 8 へのインプレースアップグレードを実行できます。CentOS Linux 6 および Oracle Linux 6 変換は、サポート対象外の **Convert2RHEL** ユーティリティーを使用することに注意してください。サポートされていない変換の詳細については、How to perform an unsupported conversion from a RHEL-derived Linux distribution to RHEL を参照してください。

Red Hat が他の Linux ディストリビューションから RHEL への移行は、Convert2RHEL サポートポリシー を参照してください。

1.3. RED HAT CUSTOMER PORTAL LABS

Red Hat Customer Portal Labsは、カスタマーポータルのセクションにあるツールセットで、https://access.redhat.com/labs/ から入手できます。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
- Product Life Cycle Checker
- Kickstart Generator
- Kickstart Converter
- Red Hat Enterprise Linux Upgrade Helper
- Red Hat Satellite Upgrade Helper
- Red Hat Code Browser
- JVM Options Configuration Tool
- Red Hat CVE Checker
- Red Hat Product Certificates
- Load Balancer Configuration Tool
- Yum Repository Configuration Helper
- Red Hat Memory Analyzer
- Kernel Oops Analyzer
- Red Hat Product Errata Advisory Checker

1.4. 関連情報

- 他のバージョンと比較した Red Hat Enterprise Linux 8.0 の **機能および制限** は、Red Hat ナレッジベースの記事 Red Hat Enterprise Linux technology capabilities and limits を参照してください。
- Red Hat Enterprise Linux の **ライフサイクル** に関する情報は Red Hat Enterprise Linux のライフサイクル を参照してください。
- RHEL 8 の **パッケージリスト** は、パッケージマニフェスト を参照してください。
- 削除された機能を含む主な**RHEL 7 と RHEL 8 の相違点**は、RHEL 8 の導入における考慮事項 で説明されています。

- **RHEL 7 から RHEL 8 へのインプレースアップグレード**を実行する方法は、Upgrading from RHEL 7 to RHEL 8 を参照してください。

- すべての RHEL サブスクリプションで、既知の技術問題の特定、検証、および解決をプロアクティブに行う **Red Hat Insights** サービスが利用できるようになりました。Red Hat Insights クライアントをインストールし、システムをサービスに登録する方法は、Red Hat Insights を使い始める ページを参照してください。

第2章 アーキテクチャー

Red Hat Enterprise Linux 8.8 には、カーネルバージョン 4.18.0-477.10 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。

- AMD アーキテクチャーおよび Intel 64 ビットアーキテクチャー
- 64 ビット ARM アーキテクチャー
- IBM Power Systems (リトルエンディアン)
- 64 ビット IBM Z

各アーキテクチャーに適切なサブスクリプションを購入してください。詳細は Get Started with Red Hat Enterprise Linux - additional architectures を参照してください。利用可能なサブスクリプションのリストは、カスタマーポータルの サブスクリプションの使用状況 を参照してください。

第3章 RHEL 8 のコンテンツの配布

3.1. インストール

Red Hat Enterprise Linux 8 は、ISO イメージを使用してインストールします。AMD64、Intel 64 ビット、64 ビット ARM、IBM Power Systems、IBM Z アーキテクチャーで、以下の 2 種類のインストールメディアが利用できます。

- Binary DVD ISO - BaseOS リポジトリーおよび AppStream リポジトリーが含まれ、リポジトリーを追加しなくてもインストールを完了できる完全インストールイメージです。

注記

インストール用 ISO イメージのサイズは複数 GB であるため、光学メディア形式には適合しない場合があります。インストール ISO イメージを使用して起動可能なインストールメディアを作成する場合は、USB キーまたは USB ハードドライブを使用することが推奨されます。Image Builder ツールを使用すれば、RHEL イメージをカスタマイズできます。Image Builder の詳細は **RHEL システムイメージのカスタマイズの作成** を参照してください。

- Boot ISO - インストールプログラムを起動するのに使用する最小限の ISO ブートイメージです。このオプションでは、ソフトウェアパッケージをインストールするのに、BaseOS リポジトリーおよび AppStream リポジトリーにアクセスする必要があります。リポジトリーは、Binary DVD ISO イメージに含まれます。

ISO イメージのダウンロード、インストールメディアの作成、および RHEL インストールの完了の手順については 標準的な RHEL 8 インストールの実行 ドキュメントを参照してください。自動化したキックスタートインストールなどの高度なトピックは 高度な RHEL 8 インストールの実行 を参照してください。

3.2. リポジトリー

Red Hat Enterprise Linux 8 は、2 つのメインリポジトリーで配布されています。

- BaseOS
- AppStream

基本的な RHEL インストールにはどちらのリポジトリーも必要で、すべての RHEL サブスクリプションで利用できます。

BaseOS リポジトリーのコンテンツは、すべてのインストールのベースとなる、基本的な OS 機能のコアセットを提供します。このコンテンツは RPM 形式で提供されており、RHEL の以前のリリースと同様のサポート条件が適用されます。BaseOS から配布されるパッケージのリストは パッケージマニフェスト を参照してください。

アプリケーションストリーム (AppStream) リポジトリーのコンテンツには、さまざまなワークロードとユースケースに対応するために、ユーザー空間アプリケーション、ランタイム言語、およびデータベースが含まれています。Application Streams は、**モジュール** と呼ばれる RPM 形式への拡張、または Software Collections として通常の RPM 形式で利用できます。AppStream で利用可能なパッケージのリストは、パッケージマニフェスト を参照してください。

また、CodeReady Linux Builder リポジトリーは、すべての RHEL サブスクリプションで利用できます。このリポジトリーは、開発者向けの追加パッケージを提供します。CodeReady Linux Builder リポジトリーに含まれるパッケージには対応しません。

RHEL 8 リポジトリーの詳細は パッケージマニフェスト を参照してください。

3.3. アプリケーションストリーム

Red Hat Enterprise Linux 8 では、アプリケーションストリームの概念が導入されました。ユーザー空間コンポーネントのバージョンが複数配信され、オペレーティングシステムのコアパッケージよりも頻繁に更新されるようになりました。これによりプラットフォームや特定のデプロイメントの基本的な安定性に影響を及ぼすことなく、Red Hat Enterprise Linux をカスタマイズする柔軟性が向上します。

アプリケーションストリームとして使用できるコンポーネントは、モジュールまたは RPM パッケージとしてパッケージ化され、RHEL 8 の AppStream リポジトリーを介して配信されます。各 Application Stream コンポーネントには、RHEL 8 と同じか、より短いライフサイクルが指定されています。詳細は Red Hat Enterprise Linux のライフサイクル を参照してください。

モジュールは、論理ユニット (アプリケーション、言語スタック、データベース、またはツールセット) を表すパッケージの集まりです。これらのパッケージはまとめてビルドされ、テストされ、そしてリリースされます。

モジュールストリームは、アプリケーションストリームコンポーネントのバージョンを表します。たとえば、**postgresql:10** のデフォルトのストリーム以外に、**postgresql** モジュールでは、PostgreSQL データベースサーバーの複数のストリーム (バージョン) を利用できます。システムにインストールできるモジュールストリームは 1 つだけです。複数のコンテナーで異なるバージョンを使用できます。

詳細なモジュールコマンドは ユーザー空間コンポーネントのインストール、管理、および削除 を参照してください。AppStream で利用可能なモジュールのリストは、Package manifest を参照してください。

3.4. YUM/DNF を使用したパッケージ管理

Red Hat Enterprise Linux 8 へのソフトウェアのインストールは、**DNF** テクノロジーをベースとした **YUM** ツールにより行われます。以前のメジャーバージョンの RHEL との一貫性を保つために、**yum** の用語の使用が意図的に準拠しています。ただし、**yum** の代わりに **dnf** を呼び出すと、**yum** は互換性のために **dnf** のエイリアスであるため、コマンドが期待どおりに動作します。

詳細は、以下のドキュメントを参照してください。

- ユーザー空間コンポーネントのインストール、管理、および削除
- RHEL 8 の導入における検討事項

第4章 新機能

ここでは、Red Hat Enterprise Linux 8.8 に追加された新機能および主要な機能拡張を説明します。

4.1. インストーラーおよびイメージの作成

Image Builder Web コンソールでブループリントとイメージを作成するための新しく改良された方法

この機能強化により、イメージビルダーツールの統合バージョンにアクセスできるようになり、ユーザーエクスペリエンスが大幅に向上しました。

Image Builder ダッシュボード GUI の注目すべき機能強化は次のとおりです。

- カーネル、ファイルシステム、ファイアウォール、ロケール、その他のカスタマイズなど、これまで CLI のみでサポートされていたすべてのカスタマイズを使用してブループリントをカスタマイズできるようになりました。
- ブループリントを **.JSON** または **.TOML** 形式でアップロードまたはドラッグすることでブループリントをインポートし、インポートされたブループリントからイメージを作成できます。
- ブループリントを **.JSON** または **.TOML** 形式でエクスポートまたは保存することもできます。
- 並べ替え、フィルタリングが可能で、大文字と小文字が区別されるブループリントリストにアクセスします。
- Image Builder ダッシュボードを使用して、次のタブに移動してブループリント、イメージ、ソースにアクセスできるようになりました。
    - ブループリント - ブループリントタブで、ブループリントをインポート、エクスポート、または削除できるようになりました。
    - イメージ - イメージタブでは、次のことができます。
        - イメージをダウンロードします。
        - イメージログをダウンロードします。
        - イメージを削除します。
    - ソース - ソースタブでは、次のことができます。
        - イメージをダウンロードします。
        - イメージログをダウンロードします。
        - イメージのソースを作成します。
        - イメージを削除します。

Jira:RHELPLAN-139448

イメージビルダーで構築された .vhd イメージの 64 ビット ARM のサポート

以前は、イメージビルダーツールで作成された Microsoft Azure **.vhd** イメージは、64 ビット ARM アーキテクチャーではサポートされていませんでした。この更新プログラムでは、64 ビット ARM Microsoft Azure **.vhd** イメージのサポートが追加され、イメージビルダーを使用して **.vhd** イメージを

構築し、Microsoft Azure クラウドにアップロードできるようになりました。

Jira:RHELPLAN-139424

4.2. RHEL FOR EDGE

simplified-installer イメージのブループリントでユーザーを指定する機能

以前は、簡易インストーラーイメージのブループリントを作成するときに、カスタマイズが使用されずに破棄されたため、ブループリントのカスタマイズでユーザーを指定できませんでした。今回の更新により、ブループリントからイメージを作成すると、インストール時にこのブループリントによって **/usr/lib/passwd** ディレクトリーにユーザーが作成され、**/usr/etc/shadow** ディレクトリーにパスワードが作成されます。ブループリント用に作成したユーザー名とパスワードを使用してデバイスにログインできます。システムにアクセスした後、**useradd** コマンドなどでユーザーを作成する必要があることに注意してください。

Jira:RHELPLAN-149091

RHEL for Edge イメージに対する Red Hat build of MicroShift の有効化

この機能強化により、RHEL for Edge システムで Red Hat build of MicroShift サービスを有効にすることができます。**customizations.firewalld.zones** ブループリントカスタマイズを使用すると、ブループリントカスタマイズに **firewalld** ソースのサポートを追加できます。そのためには、ゾーンの名前とその特定のゾーン内のソースのリストを指定します。ソースは、**source[/mask]|MAC|ipset:ipset** の形式にすることができます。

以下は、RHEL for Edge システムで Red Hat build of MicroShift サービスのサポートを設定およびカスタマイズする方法に関するブループリントの例です。

```
[[packages]]
name = "microshift"
version = "*"
[customizations.services]
enabled = ["microshift"]
[[customizations.firewall.zones]]
name = "trusted"
sources = ["10.42.0.0/16", "169.254.169.1"]
```

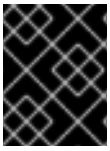
Red Hat build of MicroShift のインストール要件 (ファイアウォールポリシー、MicroShift RPM、**systemd** サービスなど) を使用すると、実稼働環境にすぐに使用できるデプロイメントを作成して、現場でデプロイされた最小限のエッジデバイスへのワークロードの移植性、およびデフォルトでの LVM デバイスマッパーの有効化を実現できます。

Jira:RHELPLAN-136489

4.3. ソフトウェア管理

RHEL でのオフライン更新のための新しい yum offline-upgrade コマンド

この機能強化により、YUM **system-upgrade** プラグインの新しい **yum offline-upgrade** コマンドを使用して、オフライン更新を RHEL に適用できるようになります。



重要

system-upgrade プラグインに含まれる **yum system-upgrade** コマンドは、RHEL ではサポートされていません。

Bugzilla:2054235

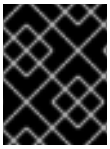
yum offline-upgrade へのアドバイザリーセキュリティーフィルターの適用がサポートされるようになりました。

この機能強化により、アドバイザリーフィルタリングの新しい機能が追加されました。その結果、**yum offline-upgrade** コマンドをアドバイザリーセキュリティーフィルター (**--advisory**、**--security**、**--bugfix**、およびその他のフィルター) とともに使用することにより、指定されたアドバイザリーのみからパッケージとその依存関係をダウンロードできるようになりました。

Bugzilla:2139324

unload_plugins 関数が YUM API で使用できるようになりました。

この機能強化により、プラグインのアンロードを可能にする新しい **unload_plugins** 関数が YUM API に追加されました。



重要

最初に **init_plugins** 関数を実行してから、**unload_plugins** 関数を実行する必要があることに注意してください。

Bugzilla:2047251

rpm2archive の新しい --nocompression オプション

この機能強化により、**--nocompression** オプションが **rpm2archive** ユーティリティーに追加されました。このオプションを使用すると、RPM パッケージを直接解凍するときに圧縮を回避できます。

Bugzilla:2129345

4.4. シェルおよびコマンドラインツール

ReaR は 64 ビット IBM Z アーキテクチャーでも完全にサポートされるようになりました。

Basic Relax and Recover (ReaR) 機能は、64 ビット IBM Z アーキテクチャーでテクノロジープレビューとして以前に利用可能でしたが、**rear** パッケージのバージョン 2.6-9.el8 以降で完全にサポートされています。ReaR レスキューイメージは、z/VM 環境の IBM Z アーキテクチャー上のみで作成できます。論理パーティション (LPAR) のバックアップとリカバリーは、現時点ではサポートされていません。ReaR は、Extended Count Key Data (ECKD) ダイレクトアクセスストレージデバイス (DASD) 上のみでディスクレイアウトの保存と復元をサポートします。ファイバーチャネルプロトコル (FCP) を介して接続された固定ブロックアクセス (FBA) DASD および SCSI ディスクは、この目的ではサポートされていません。現在利用可能な唯一の出力方法は、初期プログラムロード (IPL) です。これは、**zIPL** ブートローダーと互換性のあるカーネルと初期 RAM ディスク (initrd) を生成します。

詳細は、64 ビット IBM Z アーキテクチャーで ReaR レスキューイメージの使用 を参照してください。

Bugzilla:2130206、Bugzilla:1868421

4.5. インフラストラクチャーサービス

周波数同期用の新しい synce4l パッケージが利用可能になりました。

SyncE (同期イーサネット) は、PTP クロックが物理層で周波数の正確な同期を達成できるようにするハードウェア機能です。SyncE は、特定のネットワークインターフェイスカード (NIC) およびネットワークスイッチでサポートされています。

この機能強化により、SyncE のサポートを提供する新しい **synce4l** パッケージが利用できるようになりました。その結果、Telco Radio Access Network (RAN) アプリケーションは、より正確な時刻同期により、より効率的な通信を実現できるようになりました。

Bugzilla:2019751

powertop がバージョン 2.15 にリベースされました。

エネルギー効率を向上させる **powertop** パッケージがバージョン 2.15 に更新されました。注目すべき変更点と機能強化は次のとおりです。

- **powertop** ツールの安定性を向上させるために、いくつかの Valgrind エラーとバッファーオーバーランの可能性が修正されました。
- Ryzen プロセッサーおよび Kaby Lake プラットフォームとの互換性が向上しました。
- Lake Field、Alder Lake N、および Raptor Lake プラットフォームのサポートが可能になりました。
- Ice Lake NNPI および Meteor Lake のモバイルおよびデスクトップのサポートを有効にしました。

Bugzilla:2040070

tuned がバージョン 2.20.0 にリベースされました。

アプリケーションとワークロードのパフォーマンスを最適化するための TuneD ユーティリティーがバージョン 2.20.0 に更新されました。バージョン 2.19.0 に対する主な変更点および機能強化は、以下のとおりです。

- API の拡張機能により、実行時にプラグインインスタンス間でデバイスを移動できるようになります。
- CPU 関連のパフォーマンス設定を微調整する **plugin_cpu** モジュールには、次の機能強化が導入されています。
  - **pm_qos_resume_latency_us** 機能を使用すると、各 CPU がアイドル状態からアクティブ状態に移行するまでに許可される最大時間を制限できます。
  - TuneD は、さまざまな使用シナリオに基づいてシステムの電源管理を調整するためのスケーリングアルゴリズムを提供する **intel_pstate** スケーリングドライバーのサポートを追加します。
- Unix ドメインソケットを通じて TuneD を制御するソケット 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。詳細については、テクノロジープレビューとして利用可能な TuneD 用の Socket API を参照してください。

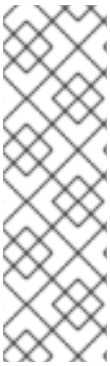
Bugzilla:2133814、Bugzilla:2113925、Bugzilla:2118786、Bugzilla:2095829、Bugzilla:2113900

4.6. セキュリティー

FIPS モードに、FIPS 140-3 を対象とするよりセキュアな設定が追加されました。

カーネルの FIPS モード設定が、連邦情報処理標準 (FIPS) 140-3 に準拠するように調整されました。この変更により、多くの暗号化アルゴリズム、関数、および暗号スイートに対して、より厳しい設定が導入されました。以下に例を示します。

- Triple Data Encryption Standard (3DES)、Elliptic-curve Diffie-Hellman (ECDH)、および Finite-Field Diffie-Hellman (FFDH) アルゴリズムが無効になりました。この変更は、カーネルキーリングの Bluetooth、DH 関連の操作、および Intel QuickAssist Technology (QAT) 暗号化アクセラレーターに影響します。
- ハッシュベースのメッセージ認証コード (HMAC) キーを 112 ビットより短くすることができなくなりました。Rivest-Shamir-Adleman (RSA) アルゴリズムの最小キー長は 2048 ビットに設定されます。
- **xts_check_key()** 関数を使用したドライバーが更新され、代わりに **xts_verify_key()** 関数が使用されるようになりました。
- 次の Deterministic Random Bit Generator (DRBG) ハッシュ関数が無効になりました。SHA-224、SHA-384、SHA512-224、SHA512-256、SHA3-224、および SHA3-384。



注記

FIPS モードの RHEL 8.6 (およびそれ以降) カーネルは、FIPS 140-3 に準拠するように設計されていますが、まだ米国国立標準技術研究所 (NIST) 暗号モジュール検証プログラム (CMVP) によって認定されていません。最新の認定カーネルモジュールは、RHSA-2021:4356 アドバイザリー更新後の更新された RHEL 8.5 カーネルです。この認定は FIPS 140-2 標準に適用されます。暗号化モジュールが FIPS 140-2 または 140-3 のどちらに準拠するかを選択することはできません。詳細は、ナレッジベースの記事 Compliance Activities and Government Standards: FIPS 140-2 and FIPS 140-3 を参照してください。

Bugzilla:2107595、Bugzilla:2158893、Bugzilla:2175234、Bugzilla:2166715、Bugzilla:2129392、Bugzilla:2152133

Libreswan が 4.9 にリベースされました。

libreswan パッケージがバージョン 4.9 にアップグレードされました。以前のバージョンに対する主な変更点は、以下のとおりです。

- **{left,right}pubkey=** のサポートを **addconn** および **whack** ユーティリティーに追加
- 鍵導出関数 (KDF) のセルフテストを追加
- **seccomp** フィルターの許可されるシステムコールのリストを更新
- ホストの認証キーを表示 (**showhostkey**):
  - Elliptic Curve Digital Signature Algorithm (ECDSA) 公開鍵のサポートを追加
  - Privacy-Enhanced Mail (PEM) でエンコードされた公開鍵を出力する **--pem** オプションを追加
- Internet Key Exchange プロトコルバージョン 2 (IKEv2):
  - 拡張認証プロトコル – トランスポート層セキュリティー (EAP-TLS) のサポート

- EAP のみの認証のサポート
- ラベル付き IPsec の改善

- **pluto** Internet Key Exchange (IKE) デーモン:
  - **maxbytes** カウンターと **maxpacket** カウンターのサポート
  - **replay-window** のデフォルト値を 32 から 128 に変更
  - **esn=** のデフォルト値を **either** に、推奨値を **yes** に変更
  - **replay-window=** が **0** に設定されている場合は、**esn** を無効化
  - **crypto-low** などの廃止されたデバッグオプションを削除

Bugzilla:2128672

SELinux が udftools を制限するようになりました。

selinux-policy パッケージの今回の更新により、SELinux は **udftools** サービスを制限します。

Bugzilla:1972230

systemd-socket-proxyd の新しい SELinux ポリシー

systemd-socket-proxyd サービスには特定のリソースの使用が必要なため、必要なルールを含む新しいポリシーが **selinux-policy** パッケージに追加されました。その結果、このサービスは SELinux ドメインで実行されるようになりました。

Bugzilla:2088441

OpenSCAP が 1.3.7 にリベースされました。

OpenSCAP パッケージがアップストリームバージョン 1.3.7 にリベースされました。このバージョンは、さまざまなバグ修正と機能拡張を提供します。特に、次のとおりです。

- OVAL フィルター処理時のエラーを修正しました (rhbz#2126882)。
- XPath が一致しない場合、OpenSCAP は無効な空の **xmlfilecontent** 項目を出力しなくなりました (rhbz#2139060)。
- **Failed to check available memory** エラーを防止しました (rhbz#2111040)。

Bugzilla:2159290

Rsyslog ログファイルの scap-security-guide ルールは、RainerScript と互換性があります。

Rsyslog ログファイルの所有権、グループ所有権、およびアクセス許可を確認および修正するための **scap-security-guide** のルールが、RainerScript 構文を使用して定義されたログファイルとも互換性を持つようになりました。最新のシステムはすでに Rsyslog 設定ファイルで RainerScript 構文を使用していますが、それぞれのルールはこの構文を認識できませんでした。その結果、**scap-security-guide** ルールは、使用可能な両方の構文で、Rsyslog ログファイルの所有権、グループ所有権、およびアクセス許可をチェックして修正できるようになりました。

Bugzilla:2072444

STIG セキュリティープロファイルがバージョン V1R9 に更新されました。

SCAP セキュリティーガイドの **DISA STIG for Red Hat Enterprise Linux 8** プロファイルが更新され、最新バージョンの **V1R9** に合わせて更新されました。このリリースには、**V1R8** で公開された変更も含まれています。

このプロファイルの以前のバージョンは有効でなくなったため、現行バージョンのみを使用してください。

以下の STIG ID が更新されました。

- V1R9
  - RHEL-08-010359 - ルール **aide_build_database** を選択
  - RHEL-08-010510 - ルール **sshd_disable_compression** を削除
  - RHEL-08-020040 - tmux キーバインディングを設定する新しいルール
  - RHEL-08-020041 - **exec tmux** の代わりに **tmux** の起動を設定する新しいルール
- V1R8
  - 複数の STIG ID - **sshd** および **sysctl** ルールにより、重複または競合する設定を特定して削除できます。
  - RHEL-08-010200 - SSHD ClientAliveCountMax の値が **1** に設定されています。
  - RHEL-08-020352 - チェックと修復が **.bash_history** を無視するようになりました。
  - RHEL-08-040137 - **/etc/fapolicyd/fapolicyd.rules** と **/etc/fapolicyd/complied.rules** の両方を調べるようにチェックが更新されました。

警告

自動修復によりシステムが機能しなくなる可能性があります。まずテスト環境で修復を実行してください。

Bugzilla:2152658

RHEL 8 STIG プロファイルのベンチマークとの整合性が向上しました。

RHEL 8 STIG 要件を満たす 4 つの既存のルールは、データストリームには組み込まれていましたが、以前は STIG プロファイル (**stig** および **stig_gui**) には含まれていませんでした。今回の更新により、以下のルールがプロファイルに含まれるようになりました。

- **accounts_passwords_pam_faillock_dir**
- **accounts_passwords_pam_faillock_silent**
- **account_password_selinux_faillock_dir**
- **fapolicy_default_deny**

その結果、RHEL 8 STIG プロファイルの対象範囲が向上しました。

Bugzilla:2156192

SCAP セキュリティーガイドが 0.1.66 にリベースされました。

SCAP セキュリティーガイド (SSG) パッケージがアップストリームバージョン 0.1.66 にリベースされました。このバージョンは、さまざまな拡張機能とバグ修正を提供します。特に、次のようなものがあります。

- RHEL 8 STIG プロファイルを更新
- ルール **account_passwords_pam_faillock_audit** を廃止し、代わりに **accounts_passwords_pam_faillock_audit** を使用

Bugzilla:2158404

OpenSSL ドライバーが Rsyslog で証明書チェーンを使用できるようになりました。

NetstreamDriverCaExtraFiles ディレクティブを使用すると、複数の追加の認証局 (CA) ファイルを設定できます。今回の更新により、複数の CA ファイルを指定できるようになり、SSL 証明書チェーンに必要な OpenSSL ライブラリーでそれらを検証できるようになりました。その結果、OpenSSL ドライバーを使用して Rsyslog で証明書チェーンを使用できるようになります。

Bugzilla:2124934

opencryptoki が 3.19.0 にリベースされました。

opencryptoki パッケージがバージョン 3.19.0 にリベースされ、多くの機能強化とバグ修正が提供されています。最も注目すべき点は、**opencryptoki** が次の機能をサポートするようになったということです。

- IBM 固有の Dilithium キー
- 二重機能暗号機能
- PKCS #11 暗号化トークンインターフェイスの基本仕様 v3.0 で説明されているように、新しい **C_SessionCancel** 関数を使用して、アクティブなセッションベースの操作をキャンセルする
- **CKM_IBM_ECDSA_OTHER** メカニズムによる Schnorr 署名
- **CKM_IBM_BTC_DERIVE** メカニズムによるビットコイン鍵の導出
- IBM z16 システムの EP11 トークン

Bugzilla:2110315

アイドルセッション終了の新しい SCAP ルール

新しい SCAP ルール **logind_session_timeout** が拡張レベルおよび高レベルの ANSSI-BP-028 プロファイルの **scap-security-guide** パッケージに追加されました。このルールは、**systemd** サービスマネージャーの新機能を使用し、一定時間が経過すると、アイドル状態のユーザーセッションを終了します。このルールは、複数のセキュリティーポリシーで必要とされる堅牢なアイドルセッション終了メカニズムの自動設定を提供します。その結果、OpenSCAP はアイドル状態のユーザーセッションの終了に関連するセキュリティー要件を自動的にチェックし、必要に応じて修正できます。

Bugzilla:2122322

fapolicyd は RPM データベースのフィルタリングを提供するようになりました。

新しい設定ファイル **/etc/fapolicyd/rpm-filter.conf** を使用すると、**fapolicyd** ソフトウェアフレーム

ワークが信頼データベースに保存する RPM データベースファイルのリストをカスタマイズできます。これにより、RPM によってインストールされた特定のアプリケーションをブロックしたり、デフォルトの設定フィルターによって拒否されたアプリケーションを許可したりできます。

Bugzilla:2165645

4.7. ネットワーク

デフォルトの MPTCP サブフロー制限は 2 です。

サブフローは、Multipath TCP (MPTCP) 接続の一部である単一の TCP 接続です。MPTCP のサブフロー制限は、2 つの MPTCP エンドポイント間で作成できる追加の接続の最大数を指します。この制限を使用すると、ネットワークとエンドポイントのオーバーロードを回避するために、エンドポイント間で作成できる追加の並列サブフローの数を制限できます。たとえば、値 0 では、初期サブフローのみが許可されます。

この機能強化により、デフォルトの MPTCP サブフロー制限が 0 から 2 に増加しました。これにより、デフォルトで複数の追加のサブフローを作成できます。別の値が必要な場合は、Systemd のワンショットユニットを作成できます。このユニットは、各ブートプロセス中にネットワーク (**network.target**) が動作可能になった後、**ip mptcp limits set subflows <YOUR_VALUE>** コマンドを実行します。

Bugzilla:2127136

カーネルは、SYN フラッドメッセージにリスニングアドレスを記録するようになりました。

この機能拡張により、リスニング IP アドレスが SYN フラッドメッセージに追加されます。

```
Possible SYN flooding on port <ip_address>:<port>.
```

その結果、多くのプロセスが異なる IP アドレスの同じポートにバインドされている場合、管理者は影響を受けるソケットを明確に特定できるようになりました。

Bugzilla:2143849

nm-initrd-generator プロファイルの優先度が自動接続プロファイルの優先度よりも低くなりました。

初期ブート NetworkManager 設定ジェネレーターユーティリティーの **nm-initrd-generator** は、ブートローダーの初期化された **initrd** RAM ディスクで実行されている NetworkManager インスタンスを使用して、接続プロファイルを生成および設定します。**nm-initrd-generator** ユーティリティーで生成されたプロファイルの自動接続の優先度は、デフォルト接続の自動接続の優先度よりも低くなります。これにより、**initrd** で生成されたネットワークプロファイルが、デフォルトの root アカウントのユーザー設定と共存できるようになります。

注記

initrd の root アカウントからデフォルトの root に切り替えた後も、同じプロファイルがアクティブ化されたままになり、新しい自動接続は行われません。

Bugzilla:2089707

nispor がバージョン 1.2.10 にリベースされました。

nispor パッケージがアップストリームバージョン 1.2.10 にアップグレードされ、以前のバージョンに対するバグ修正や機能強化が数多く追加されました。

- ネットワークルートおよびインターフェイスでカーネルフィルターを使用するための **NetStateFilter** のサポートが追加されました。
- Single Root Input and Output Virtualization (SR-IOV) インターフェイスで、SR-IOV Virtual Function (SR-IOV VF) 情報を (VF) ごとにクエリーできます。
- ボンディングオプション **lacp_active**、**arp_missed_max**、および **ns_ip6_target** が新しくサポートされました。

Bugzilla:2153166

NetworkManager がバージョン 1.40.16 にリベースされました。

NetworkManager パッケージがアップストリームバージョン 1.40.16 にアップグレードされ、以前のバージョンに対するバグ修正が数多く追加されました。

- **nm-cloud-setup** ユーティリティーが、外部から追加されたアドレスを保存します。
- 起動時の MACsec 接続の自動アクティブ化を妨げていた競合状態が修正されました。
- NetworkManager が、IPv6 近隣探索メッセージから設定されたアイテムの有効期限を正しく計算するようになりました。
- NetworkManager が、設定の変更時に **/etc/resolv.conf** ファイルを自動的に更新するようになりました。
- NetworkManager が、ボンディングをアクティブ化するときに、存在しないインターフェイスをプライマリーとして設定しなくなりました。
- ボンディングをアクティブにしたときにインターフェイスが存在しない場合でも、ボンド内のプライマリーインターフェイスの設定が常に機能するようになりました。
- **NetworkManager --print-config** コマンドが、重複するエントリーを出力しなくなりました。
- **ifcfg-rh** プラグインが、明示的なインターフェイス名なしで InfiniBand P-Key 接続プロファイルを読み取れるようになりました。
- **nmcli** ユーティリティーが、ボンドからボンドポート接続プロファイルを削除できるようになりました。
- ピアがすでに存在する場合に **veth** プロファイルのアクティブ化時に発生する可能性がある競合状態が修正されました。
- すべてのアドレスが IPv6 重複アドレス検出 (DAD) に失敗した場合、NetworkManager が DHCPv6 リースを拒否するようになりました。
- NetworkManager が、これらのインターフェイスのシステムホスト名を DNS から解決しようとする前に、インターフェイスが接続されるまで待機するようになりました。
- **nm-initrd-generator** ユーティリティーによって作成されたプロファイルの優先度が、デフォルトよりも低くなりました。

主な変更の詳細は、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。

Bugzilla:2134907

4.8. カーネル

RHEL 8.8 のカーネルバージョン

Red Hat Enterprise Linux 8.8 は、カーネルバージョン 4.18.0-477.10 で配布されます。

Bugzilla:2177769

顧客キーを使用した Secure Execution ゲストダンプ暗号化

この新機能により、Secure Execution ゲストは、**kdump** ユーティリティーが機能しない場合に、ハイパーバイザー開始ダンプを使用して、KVM からカーネルクラッシュ情報を収集できるようになります。Secure Execution のハイパーバイザー開始ダンプは、IBM Z シリーズ z16 および LinuxONE Emperor 4 ハードウェア向けに設計されていることに注意してください。

Bugzilla:2043833

sfc ドライバーが sfc と sfc_siena に分割されました。

アップストリームドライバーの変更に伴い、**sfc** NIC ドライバーが **sfc** と **sfc_siena** の 2 つの異なるドライバーに分割されました。**sfc_siena** は、非推奨の Siena ファミリーデバイスをサポートします。

カーネルモジュールパラメーターのカスタム設定と **sfc** に適用される **udev** ルールは、独立したドライバーになった **sfc_siena** には影響しないことに注意してください。両方のドライバーをカスタマイズするには、**sfc_siena** の設定オプションを複製します。

Bugzilla:2136107

stmmac ドライバーが完全にサポートされるようになりました。

Red Hat は、Intel® Elkhart Lake システムオンチップ (SoC) の **stmmac** ドライバーを完全にサポートするようになりました。

Bugzilla:1905243

rtla メタツールに、トレーサー機能を向上させるために osnoise および timerlat トレーサーが追加されました。

Real-Time Linux Analysis (**rtla**) は、Linux のリアルタイムプロパティーを分析する一連のコマンドを含むメタツールです。**rtla** は、カーネルトレース機能を利用して、予期しないシステム結果のプロパティーと根本原因に関する正確な情報を提供します。**rtla** には現在、**osnoise** および **timerlat** トレーサーコマンドのサポートが追加されています。**osnoise** トレーサーは、CPU ごとのカーネルスレッドを報告します。**timerlat** トレーサーは、タイマー IRQ ハンドラーおよびスレッドハンドラーでのタイマーレイテンシーを定期的に出力します。

rtla の **timerlat** 機能を使用するには、**sysctl -w kernel.sched_rt_runtime_us=-1** スクリプトを使用して、アドミッションコントロールを無効にする必要があることに注意してください。

Bugzilla:2075203

cgroups と irqs の出力形式が改善され、読みやすくなりました。

この機能強化により、**cgroup** ユーティリティーの **tuna show_threads** コマンド出力が端末のサイズに基づいて構造化されるようになりました。新しい **-z** または **--spaced** オプションを **show_threads** コマンドに追加することで、**cgroups** 出力に追加のスペースを設定することもできます。その結果、ターミナルのサイズに合わせて改善された読みやすい形式で **cgroups** 出力を表示できるようになりました。

Bugzilla:2121518

rteval コマンドの出力には、プログラムのロードと測定スレッドの情報が含まれるようになりました。

rteval コマンドは、プログラムのロード数、測定スレッド、およびこれらのスレッドを実行した対応する CPU を含むレポートの概要を表示するようになりました。この情報は、特定のハードウェアプラットフォームの負荷下でのリアルタイムカーネルのパフォーマンスを評価するのに役立ちます。

rteval レポートは、システムのブートログとともに XML ファイルに書き込まれ、**rteval-<date>-N-tar.bz2** 圧縮ファイルに保存されます。**date** はレポート生成日を指定し、**N** は N 回目の実行のカウンターです。

rteval レポートを生成するには、次のコマンドを入力します。

```
# rteval --summarize rteval-<date>-N.tar.bz2
```

Bugzilla:2082260

レイテンシーを測定するために、-W および --bucket-width オプションが oslat プログラムに追加されました。

この機能強化により、単一バケットのレイテンシー範囲をナノ秒の精度で指定できるようになりました。1000 ナノ秒の倍数ではない幅は、ナノ秒の精度を示します。新しいオプション **-W** または **--bucket-width** を使用すると、バケット間のレイテンシー間隔を変更して、マイクロ秒未満の遅延時間内のレイテンシーを測定できます。

たとえば、1 - 4 の CPU 範囲で実行するために 10 秒間にわたって 32 個のバケットのレイテンシーバケット幅を 100 ナノ秒に設定し、ゼロのバケットサイズを省略するには、次のコマンドを実行します。

```
# oslat -b 32 -D 10s -W 100 -z -c 1-4
```

このオプションを使用する前に、誤差測定に関してどのレベルの精度が重要であるかを判断する必要があることに注意してください。

Bugzilla:2122374

Intel Ice ドライバーを使用した E810 で、Ethernet Port Configuration Tool (EPCT) ユーティリティーのサポートが有効になりました。

この機能強化により、**devlink port Split** コマンドが Intel Ice ドライバーをサポートするようになりました。Ethernet Port Configuration Tool (EPCT) は、デバイスのリンクタイプを変更できるコマンドラインユーティリティーです。デバイス情報とデバイスのリソースを表示する **devlink** ユーティリティーは EPCT に依存しています。この機能強化の結果、Ice ドライバーに EPCT のサポートが実装され、Intel Ice ドライバーを使用して設定可能なデバイスをリストおよび表示できるようになりました。

Bugzilla:2009705

Intel Ice ドライバーがバージョン 6.0.0 にリベースされました。

Intel **ice** ドライバーはアップストリームバージョン 6.0.0 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機能強化とバグ修正が行われました。注目すべき機能強化には次のものがあります。

- Point-to-Point Protocol over Ethernet (**PPPoE**) プロトコルのハードウェアオフロード
- Inter-Integrated Circuit (**I2C**) プロトコル書き込みコマンド
- イーサネットスイッチデバイスドライバーモデル (**switchdev**) の VLAN タグプロトコル識別子 (**TPID**) フィルター

- **switchdev** での二重 VLAN タグ付け

Bugzilla:2103946

IBM zSystems のセキュアブート証明書のホスティング

IBM z16 A02/AGZ および LinuxONE Rockhopper 4 LA2/AGL 以降、ハードウェア管理コンソール (HMC) でセキュアブートを有効にしてシステムを起動するときに、Linux カーネルの検証に使用される証明書を管理できるようになりました。以下に例を示します。

- DPM およびクラシックモードで HMC を使用し、HMC からアクセスできる FTP サーバーからシステム証明書ストアに証明書をロードできます。HMC に接続された USB デバイスから証明書をロードすることもできます。
- 証明書ストアに保存されている証明書を LPAR パーティションに関連付けることができます。複数の証明書を 1 つのパーティションに関連付けたり、1 つの証明書を複数のパーティションに関連付けたりできます。
- HMC インターフェイスを使用して、証明書ストア内の証明書の関連付けをパーティションから解除できます。
- 証明書ストアから証明書を削除できます。
- 最大 20 個の証明書を 1 つのパーティションに関連付けることができます。

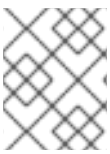
ビルトインのファームウェア証明書は引き続き使用できます。ユーザー管理の証明書ストアを使用するとすぐに、ビルトインの証明書は使用できなくなります。

証明書ストアにロードする証明書ファイルは、次の要件を満たしている必要があります。

- **PEM** または **DER-encoded X.509v3** 形式で、ファイル名拡張子が **.pem**、**.cer**、**.crt**、または **.der** のいずれかである。
- 有効期限が切れていない。
- キー使用属性が **デジタル署名** である。
- 拡張キー使用属性に **コード署名** が含まれている。

ファームウェアインターフェイスを使用すると、論理パーティションで実行されている Linux カーネルが、このパーティションに関連付けられた証明書をロードできるようになります。Linux on IBM Z は、これらの証明書を **.platform** キーリングに保存して、Linux カーネルが **kexec** カーネルを検証し、そのパーティションに関連付けられた証明書を使用してサードパーティーのカーネルモジュールを検証できるようにします。

検証済みの証明書のみをアップロードし、失効した証明書を削除するのは、オペレーターの責任です。



注記

HMC に読み込む必要がある **Red Hat Secureboot 302** 証明書は、Product Signing Keys から入手できます。

Bugzilla:2183445

zipl が 64 ビット IBM Z でのセキュアブート IPL とダンプをサポート

この更新により、**zipl** ユーティリティーは、64 ビット IBM Z アーキテクチャー上の Extended Count

Key Data (ECKD) Direct Access Storage Devices (DASD) からのList-Directed IPL および List-Directed ダンプをサポートします。その結果、IBM Z での RHEL のセキュアブートは、ECKD タイプの DASD でも動作します。

Bugzilla:2180568

4.9. 高可用性およびクラスター

新しい enable-authfile ブース設定オプション

クラスター設定でブースチケットマネージャーを使用するブース設定を作成する場合、**pcs boost setup** コマンドにより、新しい **enable-authfile** ブース設定オプションがデフォルトで有効になるようになりました。**pcsboothenable-authfile** コマンドを使用して、既存のクラスターでこのオプションを有効にできます。さらに、**pcs status** および **pcs boost status** コマンドは、**enable-authfile** の設定ミスの可能性を検出したときに警告を表示するようになりました。

Bugzilla:2132582

pcs はリソースおよび stonith エージェントの validate-all アクションを実行できるようになりました。

リソースまたは STONITH デバイスを作成または更新するときに、**--agent-validation** オプションを指定できるようになりました。このオプションを使用すると、**pcs** は、エージェントのメタデータに基づいて **pcs** によって実行される検証に加えて、エージェントの **validate-all** アクション (利用可能な場合) を使用します。

Bugzilla:1816852、Bugzilla:2159455

4.10. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー

Python 3.11 が RHEL 8 で利用できるようになりました。

RHEL 8.8 では、新しいパッケージ **python3.11** とそのために構築された一連のパッケージ、および **ubi8/python-311** コンテナーイメージによって提供される Python 3.11 が導入されています。

以前にリリースされた Python 3.9 と比較して注目すべき機能強化は次のとおりです。

- パフォーマンスが大幅に向上しました。
- 新しい **match** キーワードを使用した構造パターンマッチング (他の言語の **switch** と同様)。
- たとえば、閉じられていない丸かっこや角かっこを示すエラーメッセージが改善されました。
- デバッグやその他の使用例のための正確な行番号。
- 定義を丸かっこで囲むことにより、複数行にわたるコンテキストマネージャーの定義をサポートします。
- 新しい **X | Y** 型ユニオン演算子、variadic generics、新しい **Self** 型など、タイプヒントと **typing** モジュールに関連するさまざまな新機能。
- エラーの原因となった式を示すトレースバック内の正確なエラー位置。
- TOML の解析をサポートする新しい **tomllib** 標準ライブラリーモジュール。

- 例外グループと新しい **except*** 構文を使用して、無関係な複数の例外を同時に発生させて処理する機能。

Python 3.11 とそのためにビルドされたパッケージは、同じシステム上に Python 3.9、Python 3.8、および Python 3.6 と並行してインストールできます。

以前のバージョンとは異なり、Python 3.11 はモジュールではなく標準の RPM パッケージとして配布されることに注意してください。

python3.11 スタックからパッケージをインストールするには、たとえば、次を使用します。

```
# yum install python3.11
# yum install python3.11-pip
```

インタープリターを実行するには、たとえば、以下を使用します。

```
$ python3.11
$ python3.11 -m pip --help
```

詳細は、Python のインストールおよび使用 を参照してください。

Red Hat は、RHEL 8 のライフサイクルが終了するまで Python 3.6 のサポートを継続することに留意してください。Python 3.9 と同様に、Python 3.11 のライフサイクルは短くなります。Red Hat Enterprise Linux Application Streams のライフサイクル を参照してください。

Bugzilla:2137139

nodejs:18 がバージョン 18.14 にリベースされ、npm がバージョン 9 にリベースされました。

RHSA-2023:1583 でリリースされた **Node.js 18.14** には、**npm** のバージョン 8 からバージョン 9 への SemVer メジャーアップグレードが含まれています。この更新はメンテナンス上の理由から必要であり、**npm** 設定の調整が必要になる場合があります。

特に、特定のレジストリーに範囲を限定しない認証関連の設定はサポートされなくなりました。この変更はセキュリティー上の理由から行われました。スコープ指定されていない認証設定を使用した場合、指定されたトークンは **.npmrc** ファイルにリストされているすべてのレジストリーに送信されます。

スコープなしの認証トークンを使用する場合は、レジストリースコープ付きトークンを生成して **.npmrc** ファイルに指定します。

.npmrc ファイル内に **//registry.npmjs.org/:_auth** など、**_auth** を使用する設定行がある場合は、それらを **//registry.npmjs.org/:_authToken=${NPM_TOKEN}** に置き換え、生成したスコープ付きトークンを指定します。

変更の完全なリストについては、アップストリームの変更ログ を参照してください。

Bugzilla:2178087

git がバージョン 2.39.1 にリベースされました。

Git バージョン管理システムがバージョン 2.39.1 に更新され、以前にリリースされたバージョン 2.31 に比べて、バグ修正、拡張機能、およびパフォーマンスが向上しました。

主な機能拡張は、次のとおりです。

- **git log** コマンドは、**git describe** 出力のフォーマットプレースホルダーをサポートするようになりました。**git log --format=%(describe)**

- **git commit** コマンドで、ログメッセージを変更せずにコミットの内容を修正できる **--fixup<commit>** オプションがサポートされるようになりました。この更新により、以下も使用できるようになります。
  - **--fixup=amend:<commit>** オプションは、メッセージとコンテンツの両方を変更します。
  - **--fixup=reword:<commit>** オプションは、コミットメッセージのみを更新します。
- **git clone** コマンドで新しい **--reject-shallow** オプションを使用すると、浅いリポジトリーからのクローン作成を無効にすることができます。
- **git branch** コマンドで **--recurse-submodules** オプションがサポートされるようになりました。
- **git merge-tree** コマンドを使用して、次のことができるようになりました。
  - 2 つのブランチをマージできるかどうかをテストします。
  - ブランチがマージされた場合にマージコミットになるツリーを計算します。
- 新しい **safe.bareRepository** 設定変数を使用して、ベアリポジトリーをフィルタリングして除外できます。

Bugzilla:2139378

git-lfs がバージョン 3.2.0 にリベースされました。

Git Large File Storage (LFS) 拡張機能がバージョン 3.2.0 に更新され、以前にリリースされたバージョン 2.13 に比べて、バグ修正、拡張機能、およびパフォーマンスが向上しました。

主な変更点は、以下のとおりです。

- **Git LFS** は純粋な SSH ベースのトランスポートプロトコルを導入します。
- **Git LFS** はマージドライバーを提供するようになりました。
- **git lfs fsck** ユーティリティーは、ポインターが正規であること、および予期される LFS ファイルの形式が正しいことをさらにチェックするようになりました。
- NT LAN Manager (NTLM) 認証プロトコルのサポートは削除されました。代わりに Kerberos または Basic 認証を使用してください。

Bugzilla:2139382

新しいモジュールストリーム: nginx:1.22

nginx 1.22 Web およびプロキシーサーバーは、**nginx:1.22** モジュールストリームとして利用できるようになりました。この更新では、以前にリリースされたバージョン 1.20 に対して、多数のバグ修正、セキュリティー修正、新機能、機能強化が提供されます。

新機能:

- **nginx** は以下をサポートするようになりました。
  - OpenSSL 3.0、および OpenSSL 3.0 を使用する場合の **SSL_sendfile()** 関数。
  - PCRE2 ライブラリー。
  - **mail** プロキシーモジュールでの POP3 および IMAP パイプライン。

- **nginx** は、**Auth-SSL-Protocol** および **Auth-SSL-Cipher** ヘッダー行をメールプロキシー認証サーバーに渡すようになりました。

拡張されたディレクティブ:

- **ssl_conf_command**、**ssl_reject_handshake** など、新しいディレクティブが複数利用できるようになりました。
- **proxy_cookie_flags** ディレクティブが変数に対応するようになりました。
- **nginx** は、**proxy_ssl_certificate**、**proxy_ssl_certificate_key**、**grpc_ssl_certificate**、**grpc_ssl_certificate_key**、**uwsgi_ssl_certificate**、および **uwsgi_ssl_certificate_key** ディレクティブの変数をサポートするようになりました。
- ストリームモジュールの **listen** ディレクティブは、新しい **fastopen** パラメーターをサポートするようになりました。これにより、リスニングソケットの **TCP Fast Open** モードが有効になります。
- 新しい **max_errors** ディレクティブが **mail** プロキシーモジュールに追加されました。

その他の変更点:

- **nginx** は、次の場合、常にエラーを返すようになりました。
  - **CONNECT** メソッドが使用されます。
  - **Content-Length** と **Transfer-Encoding** の両方のヘッダーがリクエストに指定されます。
  - リクエストヘッダー名にスペースまたは制御文字が含まれています。
  - **Host** リクエストヘッダー行には、スペースまたは制御文字が含まれています。
- **nginx** は、**Transfer-Encoding** ヘッダーを含むすべての HTTP/1.0 リクエストをブロックするようになりました。
- **nginx** は、Application Layer Protocol Negotiation (ALPN) を使用して HTTP/2 接続を確立するようになり、Next Protocol Negotiation (NPN) プロトコルはサポートされなくなりました。

nginx:1.22 ストリームをインストールするには、次を使用します。

```
# yum module install nginx:1.22
```

nginx:1.20 ストリームからアップグレードする場合は、後続のストリームへの切り替え を参照してください。

詳細は、NGINX のセットアップと設定 を参照してください。

nginx モジュールストリームのサポート期間については、Red Hat Enterprise Linux アプリケーションストリームのライフサイクル を参照してください。

Bugzilla:2112345

mod_security がバージョン 2.9.6 にリベースされました。

Apache HTTP サーバーの **mod_security** モジュールがバージョン 2.9.6 に更新され、以前に利用可能だったバージョン 2.9.2 に新機能、バグ修正、セキュリティー修正が追加されました。

主な機能拡張は、次のとおりです。

- **modsecurity.conf-recommended** ファイル内のパーサーのアクティブ化ルールを調整しました。
- **mod_security** が HTTP マルチパートリクエストを解析する方法が強化されました。
- 新しい **MULTIPART_PART_HEADERS** コレクションが追加されました。
- フォーマットされたログのタイムスタンプに microsec のタイムスタンプ解像度を追加しました。
- 欠落している地域の国を追加しました。

Bugzilla:2143207

新しいパッケージ: tomcat

RHEL 8.8 では、Apache Tomcat サーバーバージョン 9 が導入されています。Tomcat は、Java Servlet および JavaServer Pages テクノロジーの公式リファレンス実装で使用されるサーブレットコンテナーです。Java Servlet および JavaServer Pages の仕様は、Java Community Process に基づいて Sun によって開発されました。Tomcat はオープンな参加型環境で開発され、Apache ソフトウェアライセンスバージョン 2.0 に基づいてリリースされています。

Bugzilla:2160455

新しいモジュールストリーム: postgresql:15

RHEL 8.8 リリースでは、**PostgreSQL 15** が導入されました。これは、バージョン 13 から多くの新機能および機能強化が追加されています。主な変更点は、以下のとおりです。

- サブスクリプトを使用して **PostgreSQL** JSON データにアクセスできるようになりました。クエリーの例:

```
SELECT ('{ "postgres": { "release": 15 }}'::jsonb)['postgres']['release'];
```

- **PostgreSQL** は、複数範囲のデータ型をサポートし、**range_agg** 関数を拡張して複数範囲のデータ型を集約するようになりました。
- **PostgreSQL** は監視と可観測性を向上させます。
  - **COPY** コマンドとログ先行書き込み (WAL) アクティビティーの進行状況を追跡できるようになりました。
  - **PostgreSQL** はレプリケーションスロットに関する統計を提供するようになりました。
  - **compute_query_id** パラメーターを有効にすることで、**pg_stat_activity** や **EXPLAIN VERBOSE** など、複数の **PostgreSQL** 機能を通じてクエリーを独自に追跡できるようになりました。
- **PostgreSQL** では、次のようにクエリー並列処理のサポートが向上しています。
  - 並列順次スキャンのパフォーマンスが向上しました。
  - **RETURN QUERY** コマンドの使用時に並列クエリーを実行する SQL 手続き型言語 (**PL/pgSQL**) の機能。
  - **REFRESH MATERIALIZED VIEW** コマンドで並列処理を有効にしました。

- **PostgreSQL** には SQL 標準の **MERGE** コマンドが含まれるようになりました。**MERGE** を使用すると、**INSERT**、**UPDATE**、および **DELETE** アクションを 1 つのステートメントに含めることができる条件付き SQL ステートメントを作成できます。
- **PostgreSQL** では、正規表現を使用して文字列を検査するための新しい関数 **regexp_count()**、**regexp_instr()**、**regexp_like()**、および **regexp_substr()** を提供します。
- **PostgreSQL** には、**security_invoker** パラメーターが追加されており、これを使用すると、ビュー作成者ではなくビュー呼び出し元の権限でデータをクエリーすることができます。これは、ビューの呼び出し元が基になるデータを操作するための適切な権限を持っていることを確認するのに役立ちます。
- **PostgreSQL** は、アーカイブ機能とバックアップ機能のパフォーマンスを向上させます。
- **PostgreSQL** では、**LZ4** および **Zstandard** (**zstd**) 可逆圧縮アルゴリズムのサポートが追加されています。
- **PostgreSQL** は、メモリー内およびディスク上のソートアルゴリズムを改善します。
- 更新された **postgresql.service** systemd ユニットファイルにより、ネットワークが起動した後に **postgresql** サービスが確実に開始されるようになりました。

次の変更には下位互換性がありません。

- パブリックスキーマのデフォルトの権限が変更されました。新規に作成されたユーザーは、**GRANT ALL ON SCHEMA public TO myuser;** コマンドを使用して、権限を明示的に付与する必要があります。以下に例を示します。

```
postgres=# CREATE USER mydbuser;
postgres=# GRANT ALL ON SCHEMA public TO mydbuser;
postgres=# \c postgres mydbuser
postgres=$ CREATE TABLE mytable (id int);
```

- **libpq PQsendQuery()** 関数はパイプラインモードではサポートされなくなりました。影響を受けるアプリケーションを変更して、代わりに **PQsendQueryParams()** 関数を使用します。

PostgreSQL の使用 も参照してください。

postgresql:15 ストリームをインストールするには、次を使用します。

```
# yum module install postgresql:15
```

RHEL 8 内で以前の **postgresql** ストリームからアップグレードする場合は 後続のストリームへの切り替え の説明に従い、Migrating to a RHEL 8 バージョンの PostgreSQL への移行 で説明されているように **PostgreSQL** データを移行します。

postgresql モジュールストリームのサポート期間については、Red Hat Enterprise Linux アプリケーションストリームのライフサイクル を参照してください。

Bugzilla:2128241

4.11. コンパイラーおよび開発ツール

新しいモジュールストリーム: swig:4.1

RHEL 8.8 では、新しいモジュールストリーム **swig:4.1** として利用できる、SWIG (Simplified Wrapper and Interface Generator) バージョン 4.1 が導入されました。

RHEL 8.4 でリリースされた **SWIG 4.0** と比較すると、**SWIG 4.1** は次のとおりです。

- **Node.js** バージョン 12 - 18 のサポートを追加し、 **Node.js** バージョン 6 より前のサポートを削除します。
- **PHP 8** のサポートを追加します。
- **PHP** C API を通じて完全に **PHP** ラッピングを処理し、デフォルトでは **.php** ラッパーを生成しなくなりました。
- **Perl 5.8.0** 以降のバージョンのみをサポートします。
- **Python** バージョン 3.9 から 3.11 のサポートを追加します。
- **Python 3.3** 以降の **Python 3** バージョンと **Python 2.7** のみをサポートします。
- **Python** で生成されたコードにおけるさまざまなメモリーリークの修正を提供します。
- C99、C++11、C++14、および C++17 標準のサポートが向上し、C++20 標準の実装が開始されます。
- C++ **std::unique_ptr** ポインタークラスのサポートを追加します。
- C++ テンプレートの処理に複数の小さな改善が含まれています。
- さまざまなケースでの C++ 宣言の使用法を修正しました。

swig:4.1 モジュールストリームをインストールするには、以下を使用します。

```
# yum module install swig:4.1
```

以前の **swig** モジュールストリームからアップグレードするには、後続のストリームへの切り替え を参照してください。

swig モジュールストリームのサポート期間の詳細は、Red Hat Enterprise Linux Application Streams のライフサイクル を参照してください。

Bugzilla:2139076

新しいモジュールストリーム: jaxb:4

RHEL 8.8 では、新しい **jaxb:4** モジュールストリームとして Jakarta XML Binding (JAXB) 4 が導入されています。JAXB は、開発者が Java クラスを XML 表現にマッピングしたり、XML 表現からマッピングしたりできるようにするフレームワークです。

jaxb:4 モジュールストリームをインストールするには、以下を使用します。

```
# yum module install jaxb:4
```

Bugzilla:2055539

GCC Toolset 12 の更新

GCC Toolset 12 は最新バージョンの開発ツールを提供するコンパイラーツールセットです。このツールセットは、**AppStream** リポジトリーにおいて、Software Collection の形式で、Application Streams として利用できます。

RHEL 8.8 で導入された注目すべき変更点は次のとおりです。

- GCC コンパイラーがバージョン 12.2.1 に更新され、アップストリームの GCC で利用可能なバグ修正および機能拡張が数多く追加されました。
- **annobin** がバージョン 11.08 に更新されました。

以下のツールおよびバージョンは、GCC Toolset 12 で利用できます。

ツール	バージョン
GCC	12.2.1
GDB	11.2
binutils	2.38
dwz	0.14
annobin	11.08

GCC Toolset 12 をインストールするには、root で以下のコマンドを実行します。

```
# yum install gcc-toolset-12
```

GCC Toolset 12 のツールを実行するには、以下のコマンドを実行します。

```
$ scl enable gcc-toolset-12 tool
```

GCC Toolset バージョン 12 のツールバージョンが、このようなツールのシステムバージョンをオーバーライドするシェルセッションを実行するには、次のコマンドを実行します。

```
$ scl enable gcc-toolset-12 bash
```

詳細は、GCC ツールセット 12 を参照してください。

Bugzilla:2110582

glibc のセキュリティー強化が追加されました。

SafeLinking 機能が **glibc** に追加されました。その結果、アロケーターのスレッドローカルキャッシュなど、特定の単一リンクリストの破損に対する **malloc** ファミリー関数の保護が向上します。

Bugzilla:1871383

glibc 動的ローダーのアルゴリズムが改善されました。

共有オブジェクトの依存関係が深くネストされている場合、共有オブジェクトを処理するための **glibc** 動的ローダーの $O(n^3)$ アルゴリズムにより、アプリケーションの起動時間とシャットダウン時間が遅く

なることがありました。この更新により、動的ローダーのアルゴリズムが改善され、深さ優先検索 (DFS) が使用されるようになりました。その結果、共有オブジェクトの依存関係が深くネストされている場合、アプリケーションの起動時間とシャットダウン時間が大幅に改善されます。

動的ローダーの O(n^3) アルゴリズムは、**glibc** ランタイム調整可能パラメーター **glibc.rtld.dynamic_sort** を使用して選択できます。調整可能パラメーターのデフォルト値は 2 です。この値は新しい DFS アルゴリズムを表します。互換性のために以前の O(n^3) アルゴリズムを選択するには、調整可能パラメーターを 1 に設定します。

```
# GLIBC_TUNABLES=glibc.rtld.dynamic_sort=1
# export GLIBC_TUNABLES
```

Bugzilla:1159809

LLVM Toolset がバージョン 15.0.7 にリベースされました。

LLVM Toolset がバージョン 15.0.7 に更新されました。主な変更点は、以下のとおりです。

- **-Wimplicit-function-declaration** および **-Wimplicit-int** 警告は、C99 以降ではデフォルトで有効になっています。これらの警告は、Clang 16 以降ではデフォルトでエラーになります。

Bugzilla:2118568

Rust Toolset がバージョン 1.66.1 にリベースされました。

Rust Toolset がバージョン 1.66.1 に更新されました。主な変更点は、以下のとおりです。

- **thread::scope** API は、新しく生成されたスレッドによってローカル変数を安全に借用できる字句スコープを作成します。また、それらのスレッドはスコープが終了する前にすべて終了することが保証されます。
- **hint::black_box** API はコンパイラーの最適化に障壁を追加します。これは、他の方法では最適化されてしまう可能性のあるベンチマークの動作を維持するのに役立ちます。
- **.await** キーワードは、**for** と **IntoIterator** の関係と同様に、**IntoFuture** 特性を使用して変換を行うようになりました。
- ジェネリック関連型 (GAT) を使用すると、特性にジェネリックパラメーターを持つ型エイリアスを含めることができ、型と有効期間の両方にわたる新しい抽象化が可能になります。
- 新しい **let-else** ステートメントでは、条件付きパターンマッチングでローカル変数をバインドし、パターンが一致しない場合に分岐 **else** ブロックを実行できます。
- ラベル付きブロックを使用すると、オプションで式の値を追加して、**break** ステートメントはブロックの末尾にジャンプできます。
- **rust-analyzer** は言語サーバープロトコルの新しい実装であり、多くのエディターで Rust のサポートを可能にします。これは以前の **rls** パッケージを置き換えますが、**rust-analyzer** に移行するにはエディターの設定を調整する必要がある場合があります。
- Cargo には、**Cargo.toml** から依存関係を削除するための新しい **cargo remove** サブコマンドがあります。

Bugzilla:2123899

Go Toolset がバージョン 1.19.4 にリベースされました。

Go Toolset がバージョン 1.19.4 に更新されました。主な変更点は、以下のとおりです。

- 次のパッケージに対するセキュリティー修正:
  - **crypto/tls**
  - **mime/multipart**
  - **net/http**
  - **path/filepath**
- バグ修正:
  - **go** コマンド
  - リンカー
  - ランタイム
  - **crypto/x509** パッケージ
  - **net/http** パッケージ
  - **time** パッケージ

Bugzilla:2174430

tzdata パッケージには /usr/share/zoneinfo/leap-seconds.list ファイルが含まれるようになりました。

以前は、**tzdata** パッケージには、**/usr/share/zoneinfo/leapseconds** ファイルのみが同梱されていました。一部のアプリケーションは、**/usr/share/zoneinfo/leap-seconds.list** ファイルによって提供される代替形式に依存しているため、エラーが発生する可能性があります。

今回の更新により、**tzdata** パッケージには両方のファイルが含まれるようになり、どちらの形式に依存するアプリケーションもサポートされるようになりました。

Bugzilla:2154109

4.12. IDENTITY MANAGEMENT

ホームディレクトリーを小文字に変換するための SSSD のサポート

この機能強化により、ユーザーのホームディレクトリーを小文字に変換するように SSSD を設定できるようになりました。これは、RHEL 環境の大文字と小文字を区別する性質とより適切に統合するのに役立ちます。**/etc/sssd/sssd.conf** ファイルの **[nss]** セクションの **override_homedir** オプションが **%h** テンプレート値を認識するようになりました。**override_homedir** 定義の一部として **%h** を使用すると、SSSD は **%h** をユーザーのホームディレクトリーの小文字に置き換えます。

Jira:RHELPLAN-139430

ipapwpolicy ansible-freeipa モジュールが新しいパスワードポリシーオプションをサポートするようになりました。

この更新により、**ansible-freeipa** パッケージに含まれる **ipapwpolicy** モジュールは、追加の **libpwquality** ライブラリーオプションをサポートします。

maxrepeat

同じ文字の最大数を連続して指定します。

maxsequence

単調な文字シーケンスの最大長を指定します (**abcd**)。

dictcheck

パスワードが辞書の単語であるかどうかを確認します。

usercheck

パスワードにユーザー名が含まれるかどうかを確認します。

新しいパスワードポリシーオプションのいずれかが設定されている場合、パスワードの最小長は 6 文字です。新しいパスワードポリシー設定は、新しいパスワードのみに適用されます。

RHEL 7 サーバーと RHEL 8 サーバーが混在する環境では、新しいパスワードポリシー設定は、RHEL 8.4 以降で実行されているサーバーのみに適用されます。ユーザーが IdM クライアントにログインし、IdM クライアントが RHEL 8.3 以前で実行されている IdM サーバーと通信している場合、システム管理者によって設定された新しいパスワードポリシー要件は適用されません。一貫した動作を保証するには、すべてのサーバーを RHEL 8.4 以降にアップグレードします。

Jira:RHELPLAN-137416

IdM が ipanetgroup Ansible 管理モジュールをサポートするようになりました。

Identity Management (IdM) システム管理者は、IdM を NIS ドメインおよびネットグループと統合できます。**ipanetgroup ansible-freeipa** モジュールを使用すると、次のことを実現できます。

- 既存の IdM ネットグループに特定の IdM ユーザー、グループ、ホスト、ホストグループ、およびネストされた IdM ネットグループが含まれていることを確認できます。
- 特定の IdM ユーザー、グループ、ホスト、ホストグループ、およびネストされた IdM ネットグループが既存の IdM ネットグループに存在しないことを確認できます。
- 特定のネットグループが IdM に存在するか存在しないかを確認できます。

Jira:RHELPLAN-137411

クライアントの DNS リゾルバーを指定する新しい ipaclient_configure_dns_resolver および ipaclient_dns_servers Ansible ipaclient ロール変数

以前は、**ansible-freeipa ipaclient** ロールを使用して Identity Management (IdM) クライアントをインストールする場合、インストールプロセス中に DNS リゾルバーを指定できませんでした。インストール前に DNS リゾルバーを設定する必要がありました。

この機能強化により、**ipaclient** ロールを使用して IdM クライアントをインストールするときに、**ipaclient_configure_dns_resolver** 変数と **ipaclient_dns_servers** 変数を使用して DNS リゾルバーを指定できるようになりました。その結果、**ipaclient** ロールは、**ansible-freeipa ipaserver** ロールが IdM サーバー上で行うのと同様の方法で、**resolv.conf** ファイル、**NetworkManager** および **systemd-resolved** ユーティリティーを変更して、クライアント上で DNS リゾルバーを設定します。その結果、**ipaclient** ロールを使用して IdM クライアントをインストールする際の DNS の設定がより効率的になりました。

注記

ipa-client-install コマンドラインインストーラーを使用して IdM クライアントをインストールするには、インストール前に DNS リゾルバーを設定する必要があります。

Jira:RHELPLAN-137406

ipaclient ロールを使用して IdM クライアントを OTP とともにインストールするには、Ansible コントローラーを事前に変更する必要はありません。

以前は、Ansible コントローラーの **kinit** コマンドは、Identity Management (IdM) クライアントのデプロイメント用のワンタイムパスワード (OTP) を取得するための前提条件でした。Red Hat Ansible Automation Platform (AAP) では、コントローラーで OTP を取得する必要性が問題でした。AAP では、**krb5-workstation** パッケージがデフォルトでインストールされませんでした。

この更新により、管理者の TGT に対するリクエストは、最初に指定または検出された IdM サーバーに委任されるようになりました。その結果、Ansible コントローラーを追加変更することなく、OTP を使用して IdM クライアントのインストールを承認できるようになりました。これにより、AAP での **ipaclient** ロールの使用が簡素化されます。

Jira:RHELPLAN-137403

SSSD が shadow パスワードポリシーを使用した LDAP ユーザーパスワードの変更をサポートするようになりました。

この機能強化により、**/etc/sssd/sssd.conf** ファイルで **ldap_pwd_policy** を **shadow** に設定すると、LDAP ユーザーは LDAP に保存されているパスワードを変更できるようになります。以前は、**ldap_pwd_policy** が **shadow** に設定されている場合、対応する **shadow** LDAP 属性が更新されているかどうかが明確ではないため、パスワードの変更は拒否されました。

さらに、LDAP サーバーが **shadow** 属性を自動的に更新できない場合は、**/etc/sssd/sssd.conf** ファイルで **ldap_chpass_update_last_change** オプションを **True** に設定して、属性を更新するように SSSD に指示します。

Bugzilla:2144519

設定ファイルを使用して pam_pwhistory を設定します。

この更新により、**/etc/security/pwhistory.conf** 設定ファイルで **pam_pwhistory** モジュールを設定できるようになりました。**pam_pwhistory** モジュールは、パスワード変更履歴を管理するために、各ユーザーの最後のパスワードを保存します。**authselect** にもサポートが追加され、**pam_pwhistory** モジュールを PAM スタックに追加できるようになりました。

Bugzilla:2068461、Bugzilla:2063379

getcert add-scep-ca が、ユーザー提供の SCEP CA 証明書が有効な PEM 形式であるかどうかをチェックするようになりました。

getcert add-scep-ca コマンドを使用して SCEP CA を **certmonger** に追加するには、提供された証明書が有効な PEM 形式である必要があります。以前は、このコマンドはユーザーが提供した証明書をチェックせず、形式が正しくない場合でもエラーを返しませんでした。今回の更新により、**getcert add-scep-ca** は ユーザーが提供した証明書をチェックし、証明書が有効な PEM 形式でない場合はエラーを返すようになりました。

Bugzilla:2150025

IdM が新しい Active Directory 証明書マッピングテンプレートをサポートするようになりました

Active Directory (AD) ドメイン管理者は、**altSecurityIdentities** 属性を使用して、証明書を AD 内のユーザーに手動でマッピングできます。この属性には 6 つの値がサポートされていますが、3 つのマッピングは安全ではないと考えられています。2022 年 5 月 10 日のセキュリティー更新 の一部として、この更新プログラムがドメインコントローラーにインストールされると、すべてのデバイスが互換モー

ドになります。証明書がユーザーに弱くマッピングされている場合、認証は期待どおりに行われますが、完全強制モードと互換性のない証明書を示す警告メッセージがログに記録されます。2023 年 11 月 14 日以降、すべてのデバイスは完全強制モードに更新され、証明書が強力なマッピング基準を満たさない場合、認証は拒否されます。

IdM は新しいマッピングテンプレートをサポートするようになったため、AD 管理者は両方を維持することなく、新しいルールを使用できるようになりました。IdM は、次の新しいマッピングテンプレートをサポートするようになりました。

- シリアル番号: **LDAPU1:(altSecurityIdentities=X509:<I>{issuer_dn!ad_x500}<SR>{serial_number!hex_ur})**
- Subject Key Id: **LDAPU1:(altSecurityIdentities=X509:<SKI>{subject_key_id!hex_u})**
- User SID: **LDAPU1:(objectsid={sid})**

新しい SID 拡張子を使用して証明書を再発行したくない場合は、AD のユーザーの **altSecurityIdentities** 属性に適切なマッピング文字列を追加して、手動マッピングを作成できます。

Bugzilla:2087247

samba がバージョン 4.17.5 にリベースされました。

samba パッケージがアップストリームバージョン 4.17.5 にアップグレードされ、以前のバージョンに対するバグ修正と拡張機能が提供されています。最も注目すべき変更点:

- 以前のリリースでのセキュリティーの向上は、高メタデータワークロードのサーバーメッセージブロック (SMB) サーバーのパフォーマンスに影響を与えました。この更新により、このシナリオでのパフォーマンスが向上します。
- 詳細なステータス情報を JSON 形式で表示するために、**--json** オプションが **smbstatus** ユーティリティーに追加されました。
- **samba.smb.conf** モジュールと **samba.samba3.smb.conf** モジュールが **smbconf** Python API に追加されました。これらを Python プログラムで使用すると、Samba 設定をネイティブに読み取ったり、必要に応じて書き込むことができます。

Samba 4.11 以降はサーバーメッセージブロックバージョン 1 (SMB1) プロトコルが非推奨となり、今後のリリースで削除されることに注意してください。

Samba を起動する前にデータベースファイルがバックアップされます。**smbd**、**nmbd**、または**winbind** サービスが起動すると、Samba が **tdb** データベースファイルを自動的に更新します。Red Hat は、**tdb** データベースファイルのダウングレードをサポートしていません。

Samba を更新した後、**testparm** ユーティリティーを使用して **/etc/samba/smb.conf** ファイルを確認します。

重要な変更点の詳細については、更新する前に、アップストリームリリースノート をお読みください。

Bugzilla:2132051

ipa-client-install が PKINIT による認証をサポートするようになりました。

以前は、**ipa-client-install** はパスワードベースの認証のみをサポートしていました。この更新により、PKINIT による認証のための **ipa-client-install** のサポートが提供されます。

以下に例を示します。

```
ipa-client-install --pkinit-identity=FILE:/path/to/cert.pem,/path/to/key.pem --pkinit-
anchor=FILE:/path/to/cacerts.pem
```

PKINIT 認証を使用するには、IdM と PKINIT 証明書の CA チェーンの間に信頼を確立する必要があります。詳細については、**ipa-cacert-manage(1)** man ページを参照してください。また、証明書 ID マッピングルールは、ホストの PKINIT 証明書を、ホストレコードを追加または変更する権限を持つプリンシパルにマップする必要があります。詳細については、**ipa certmaprule-add** man ページを参照してください。

Bugzilla:2075452

Directory Server が TLS の ECDSA 秘密キーをサポートするようになりました。

以前は、RSA より強力な暗号化アルゴリズムを使用して Directory Server 接続を保護することはできませんでした。この機能強化により、Directory Server は ECDSA キーと RSA キーの両方をサポートするようになりました。

Bugzilla:2096795

新しい pamModuleIsThreadSafe 設定オプションが利用可能になりました

PAM モジュールがスレッドセーフである場合、新しい **pamModuleIsThreadSafe** 設定オプションを **yes** に設定することで、その特定のモジュールの PAM 認証のスループットと応答時間を改善できます。

```
`pamModuleIsThreadSafe: yes`
```

この設定は、PAM モジュール設定エントリー (**cn=PAM Pass Through Auth,cn=plugins,cn=config** の子) に適用されます。

dse.ldif 設定ファイルまたは **ldapmodify** コマンドの **pamModuleIsThreadSafe** オプションを使用します。**ldapmodify** コマンドを使用するには、サーバーを再起動する必要があることに注意してください。

Bugzilla:2142639

Directory Server 監査ログ用の新しい nsslapd-auditlog-display-attrs 設定パラメーター

以前は、監査ログイベント内のターゲットエントリーを識別する方法は、識別名 (DN) のみでした。新しい **nsslapd-auditlog-display-attrs** パラメーターを使用すると、監査ログに追加の属性を表示するように Directory Server を設定できます。これにより、変更されたエントリーに関する詳細情報が提供されます。

たとえば、**nsslapd-auditlog-display-attrs** パラメーターを **cn** に設定すると、監査ログの出力にはエントリー **cn** 属性が表示されます。変更されたエントリーのすべての属性を含めるには、パラメーター値としてアスタリスク (*) を使用します。

詳細は、nsslapd-auditlog-display-attrs を参照してください。

Bugzilla:2136610

4.13. デスクトップ

inkscape が inkscape1 パッケージに置き換えられます。

このリリースでは、従来のモジュール式の **inkscape** パッケージが、新しい非モジュール式の **inkscape1** パッケージに置き換えられます。また、Inkscape アプリケーションもバージョン 0.92 からバージョン 1.0 にアップグレードされます。

Inkscape 1.0 は Python 2 ランタイムに依存しなくなり、代わりに Python 3 を使用します。

Inkscape 1.0 の変更点の完全なリストは、アップストリームのリリースノート https://inkscape.org/release/inkscape-1.0/ を参照してください。

Jira:RHELPLAN-121672

キオスクモードがオンスクリーンキーボードをサポートするようになりました。

キオスクモードセッションで GNOME オンスクリーンキーボード (OSK) を使用できるようになりました。

OSK を有効にするには、ログイン画面の歯車メニューから **Kiosk (with on-screen keyboard)** オプションを選択します。

RHEL 8 のキオスクモードは X11 プロトコルに基づいているため、OSK で特定の既知の問題が発生することに注意してください。特に、OSK では **é** や **ü** などのアクセント付き文字を入力できません。詳細は、BZ#1916470 を参照してください。

Bugzilla:2070976

libsoup および Evolution での NTLMv2 のサポート

libsoup ライブラリーが、NT LAN Manager バージョン 2 (NTLMv2) プロトコルを使用して Microsoft Exchange Server で認証できるようになりました。以前は、**libsoup** は NTLMv1 プロトコルのみをサポートしていましたが、セキュリティー上の問題により、特定の設定ではこのプロトコルが無効になる場合がありました。

その結果、Evolution および内部で **libsoup** を使用するその他のアプリケーションも、NTLMv2 を使用して Microsoft Exchange Server で認証できるようになります。

Bugzilla:1938011

デスクトップ上のカスタム右クリックメニュー

デスクトップの背景を右クリックしたときに開くメニューをカスタマイズできるようになりました。任意のコマンドを実行するカスタムエントリーをメニューに作成できます。

メニューをカスタマイズするには、デスクトップの右クリックメニューのカスタマイズ を参照してください。

Bugzilla:2033572

ワークスペースを切り替えるためのスワイプを無効にします。

以前は、3 本の指で上下にスワイプすると、常にタッチスクリーン上のワークスペースが切り替わっていました。このリリースでは、ワークスペースの切り替えを無効にすることができます。

詳細については、スワイプによるワークスペース切り替えの無効化 を参照してください。

Bugzilla:2138109

4.14. WEB コンソール

Web コンソールは、LUKS で暗号化されたルートボリュームを NBDE にバインドするための追加手順を実行するようになりました。

この更新により、RHEL Web コンソールは、LUKS で暗号化されたルートボリュームを Network-Bound Disk Encryption (NBDE) デプロイメントにバインドするために必要な追加の手順を実行します。暗号化されたルートファイルシステムと Tang サーバーを選択した後、カーネルコマンドラインへの **rd.neednet=1** パラメーターの追加、**clevis-dracut** パッケージのインストール、および初期 RAM ディスク (**initrd**) の再生成をスキップできます。非ルートファイルシステムの場合、Web コンソールは、**remote-cryptsetup.target** および **clevis-luks-akspass.path systemd** ユニットを有効にし、**clevis-systemd** パッケージをインストールし、**_netdev** パラメーターを **fstab** および **crypttab** 設定ファイルに追加するようになりました。その結果、LUKS で暗号化されたルートボリュームの自動ロック解除のための NBDE デプロイメントを作成するときに、すべての Clevis クライアント設定手順でグラフィカルインターフェイスを使用できるようになりました。

Jira:RHELPLAN-139125

特定の暗号化サブポリシーが Web コンソールで使用できるようになりました。

RHEL Web コンソールの今回の更新により、**Change crypto policy** ダイアログのオプションが拡張されました。4 つのシステム全体の暗号化ポリシーに加えて、グラフィカルインターフェイスを介して次のサブポリシーも適用できるようになりました。

- **DEFAULT:SHA1** は、**SHA-1** アルゴリズムが有効になっている **DEFAULT** ポリシーです。
- **LEGACY:AD-SUPPORT** は、Active Directory サービスの相互運用性を向上させるセキュリティーの低い設定を持つ **LEGACY** ポリシーです。
- **FIPS:OSPP** は、情報技術セキュリティー評価標準の Common Criteria に触発されたさらなる制限を備えた **FIPS** ポリシーです。

Jira:RHELPLAN-137505

4.15. RED HAT ENTERPRISE LINUX システムロール

vpn RHEL システムロールの新しい IPsec カスタマイズパラメーター。

特定のネットワークデバイスが正しく動作するには IPsec のカスタマイズが必要なため、次のパラメーターが **vpn** RHEL システムロールに追加されました。

重要

高度な知識がないかぎり、次のパラメーターを変更しないでください。ほとんどのシナリオでは、カスタマイズする必要はありません。

さらに、セキュリティー上の理由から、Ansible Vault を使用して **shared_key_content** パラメーターの値を暗号化します。

- トンネルパラメーター:
  - **shared_key_content**
  - **ike**
  - **esp**
  - **ikelifetime**

- **salifetime**
- **retransmit_timeout**
- **dpddelay**
- **dpdtimeout**
- **dpdaction**
- **leftupdown**

- ホストごとのパラメーター:
- **leftid**
- **rightid**

その結果、**vpn** ロールを使用して、幅広いネットワークデバイスへの IPsec 接続を設定できます。

Bugzilla:2119600

ha_cluster システムロールは、firewall、selinux、および certificate システムロールの自動実行をサポートするようになりました。

ha_cluster RHEL システムロールは、次の機能をサポートするようになりました。

firewall および selinux システムロールを使用してポートアクセスを管理する

firewalld および **selinux** サービスを実行するようにクラスターのポートを設定するには、新しいロール変数 **ha_cluster_manage_firewall** および **ha_cluster_manage_selinux** を **true** に設定します。これにより、**firewall** および **selinux** システムロールを使用するようにクラスターが設定され、**ha_cluster** システムロール内でこれらの操作が自動化および実行されます。これらの変数がデフォルト値の **false** に設定されている場合、ロールは実行されません。このリリースでは、ファイアウォールはデフォルトで設定されなくなりました。これは、ファイアウォールで **ha_cluster_manage_firewall** が **true** に設定されている場合のみ、設定されるためです。

certificate システムロールを使用して pcsd 秘密鍵と証明書のペアを作成する

ha_cluster システムロールは、**ha_cluster_pcsd_certificates** ロール変数をサポートするようになりました。この変数を設定すると、その値が **certificate** システムロールの **certificate_requests** 変数に渡されます。これは、**pcsd** の秘密鍵と証明書のペアを作成するための代替方法を提供します。

Bugzilla:2130019

ha_cluster システムロールがクォーラムデバイス設定をサポートするようになりました。

クォーラムデバイスは、クラスターのサードパーティー調停デバイスとして機能します。クォーラムデバイスは、偶数のノードを持つクラスターに推奨されます。2 ノードクラスターでクォーラムデバイスを使用すると、スプリットブレインの状況で存続するノードをより適切に判別できます。**ha_cluster** システムロール (クラスターの **qdevice** と調停ノードの **qnetd** の両方) を使用してクォーラムデバイスを設定できるようになりました。

Bugzilla:2143814

metrics システムロールは、ファクト収集が無効になっていると機能しません。

Ansible ファクト収集は、パフォーマンスまたはその他の理由により、環境内で無効になっている場合があります。このような設定では、現時点では **metrics** システムロールを使用することはできません。この問題を回避するには、ファクトキャッシングを有効にしてください。ファクト収集を使用できない

場合は、**metrics** システムロールを使用しないでください。

Bugzilla:2079009

postfix RHEL システムロールは、firewall および selinux RHEL システムロールを使用してポートアクセスを管理できるようになりました。

この機能強化により、新しいロール変数 **postfix_manage_firewall** および **postfix_manage_selinux** を使用してポートアクセスの管理を自動化できます。

- これらが **true** に設定されている場合、各ロールはポートアクセスの管理に使用されます。
- これらが **false** (デフォルト) に設定されている場合、ロールは関与しません。

Bugzilla:2130332

vpn RHEL システムロールは、firewall および selinux ロールを使用してポートアクセスを管理できるようになりました。

この機能強化により、**firewall** および **selinux** ロールを介した **vpn** RHEL システムロールでのポートアクセスの管理を自動化できます。新しいロール変数 **vpn_manage_firewall** および **vpn_manage_selinux** を **true** に設定すると、ロールはポートアクセスを管理します。

Bugzilla:2130345

metrics RHEL システムロールは、firewall および selinux ロールを使用してポートアクセスを管理できるようになりました。

この機能強化により、ポートへのアクセスを制御できるようになります。新しいロール変数 **metrics_manage_firewall** および **metrics_manage_firewall** を **true** に設定すると、ロールはポートアクセスを管理します。**metrics** ロールを使用して、これらの操作を自動化し、直接実行できるようになりました。

Bugzilla:2133532

nbde_server RHEL システムロールは、firewall および selinux ロールを使用してポートアクセスを管理できるようになりました。

この機能強化により、**firewall** および **selinux** ロールを使用してポートアクセスを管理できるようになります。新しいロール変数 **nbde_server_manage_firewall** および **nbde_server_manage_selinux** を **true** に設定すると、ロールはポートアクセスを管理します。**nbde_server** ロールを使用して、これらの操作を直接自動化できるようになりました。

Bugzilla:2133931

initscripts ネットワークプロバイダーは、デフォルトゲートウェイのルートメトリック設定をサポートします。

この更新により、**rhel-system-roles.network** RHEL システムロールの **initscripts** ネットワークプロバイダーを使用して、デフォルトゲートウェイのルートメトリックを設定できるようになりました。

このような設定の理由としては、次のことが考えられます。

- トラフィック負荷をさまざまなパスに分散する
- プライマリールートとバックアップルートを指定する
- ルーティングポリシーを利用して、特定のパスを介して特定の宛先にトラフィックを送信する

Bugzilla:2134201

network システムロールは、DNS 優先値の設定をサポートします。

この機能強化により、RHEL **network** システムロールに **dns_priority** パラメーターが追加されます。このパラメーターは、**-2147483648** から **2147483647** までの値に設定できます。デフォルト値は **0** です。値が小さいほど優先順位が高くなります。負の値を指定すると、システムロールにより優先順位の数値が大きい他の設定が除外されることに注意してください。したがって、少なくとも 1 つの負の優先順位値が存在する場合、システムロールは、最も低い優先順位値を持つ接続プロファイルの DNS サーバーのみを使用します。

その結果、**network** システムロールを使用して、さまざまな接続プロファイル内の DNS サーバーの順序を定義できます。

Bugzilla:2133856

クローン MAC アドレスのサポートを追加しました。

クローンされた MAC アドレスは、マシンの MAC アドレスと同じデバイスの WAN ポートの MAC アドレスです。この更新により、ユーザーは MAC アドレスを使用してボンディングインターフェイスまたはブリッジインターフェイスを指定したり、ボンディングインターフェイスまたはブリッジインターフェイスのデフォルトの MAC アドレスを取得するために **random** または **preserve** などの戦略を指定したりできるようになります。

Bugzilla:2143458

cockpit RHEL システムロールと firewall、selinux、および certificate ロールの統合

この機能拡張により、**cockpit** ロールを **firewall** ロール、ポートアクセスを管理するための **selinux** ロール、および証明書を生成するための **証明書** ロールと統合できるようになります。

ポートアクセスを制御するには、新しい **cockpit_manage_firewall** 変数と **cockpit_manage_selinux** 変数を使用します。どちらの変数もデフォルトでは **false** に設定されており、実行されません。これらを **true** に設定すると、**firewall** および **selinux** ロールが RHEL Web コンソールサービスポートアクセスを管理できるようになります。その後、操作は **cockpit** ロール内で実行されます。

ファイアウォールと SELinux のポートアクセスを管理する責任があることに注意してください。

証明書を生成するには、新しい **cockpit_certificates** 変数を使用します。この変数はデフォルトで **false** に設定されており、実行されません。この変数は、**certificate** ロールで **certificate_request** 変数を使用するのと同じ方法で使用できます。その後、**cockpit** ロールは **certificate** ロールを使用して RHEL Web コンソール証明書を管理します。

Bugzilla:2137667

selinux RHEL システムロールが local パラメーターをサポートするようになりました。

selinux RHEL システムロールのこの更新では、**local** パラメーターのサポートが導入されています。このパラメーターを使用すると、ローカルポリシーの変更のみを削除し、組み込みの SELinux ポリシーを保持できます。

Bugzilla:2143385

Active Directory と直接統合するための新しい RHEL システムロール

新しい **rhel-system-roles.ad_integration** RHEL システムロールが **rhel-system-roles** パッケージに追加されました。その結果、管理者は RHEL システムと Active Directory ドメインの直接統合を自動化できるようになりました。

Bugzilla:2144876

Red Hat Insights と Subscription Management のための新しい Ansible ロール

rhel-system-roles パッケージには、リモートホスト設定 (**rhc**) システムロールが含まれるようになりました。このロールにより、管理者は RHEL システムを Red Hat Subscription Management (RHSM) および Satellite サーバーに簡単に登録できるようになります。デフォルトでは、**rhc** システムロールを使用してシステムを登録すると、システムは Red Hat Insights に接続します。新しい **rhc** システムロールを使用すると、管理者はマネージドノードで次のタスクを自動化できるようになりました。

- システムの自動更新、修復、タグなど、Red Hat Insights への接続を設定します。
- リポジトリーを有効または無効にします。
- 接続に使用するプロキシーを設定します。
- システムのリリースを設定します。

これらのタスクを自動化する方法の詳細は、RHC システムロールを使用したシステムの登録 を参照してください。

Bugzilla:2144877

Microsoft SQL Server Ansible ロールは非同期高可用性レプリカをサポートします。

以前は、Microsoft SQL Server Ansible ロールは、プライマリー、同期、監視の高可用性レプリカのみをサポートしていました。**mssql_ha_replica_type** 変数を **asynchronous** に設定して、新規または既存のレプリカに対して非同期レプリカタイプを設定できるようになりました。

Bugzilla:2144820

Microsoft SQL Server Ansible ロールは読み取りスケールクラスタータイプをサポートします。

以前は、Microsoft SQL Ansible ロールは外部クラスタータイプのみをサポートしていました。これで、新しい変数 **mssql_ha_ag_cluster_type** を使用してロールを設定できるようになりました。デフォルト値は **external** です。これを使用して Pacemaker でクラスターを設定します。Pacemaker を使用せずにクラスターを設定するには、その変数に値 **none** を使用します。

Bugzilla:2144821

Microsoft SQL Server Ansible ロールは TLS 証明書を生成できます。

以前は、Microsoft SQL Ansible ロールを設定する前に、ノード上で TLS 証明書と秘密キーを手動で生成する必要がありました。この更新により、Microsoft SQL Server Ansible ロールは、その目的で **redhat.rhel_system_roles.certificate** ロールを使用できるようになりました。これで、**mssql_tls_certificates** 変数を **certificate** ロールの **certificate_requests** 変数の形式で設定して、ノード上に TLS 証明書と秘密鍵を生成できるようになりました。

Bugzilla:2144852

Microsoft SQL Server Ansible ロールは SQL Server バージョン 2022 の設定をサポートします。

以前は、Microsoft SQL Ansible ロールは SQL Server バージョン 2017 とバージョン 2019 の設定のみをサポートしていました。この更新プログラムでは、Microsoft SQL Ansible ロールの SQL Server バージョン 2022 のサポートが提供されます。新しい SQL Server 2022 を設定するか、SQL Server をバー

ジョン 2019 からバージョン 2022 にアップグレードするために、**mssql_version** 値を **2022** に設定できるようになりました。SQL Server をバージョン 2017 からバージョン 2022 にアップグレードすることはできないことに注意してください。

Bugzilla:2153428

Microsoft SQL Server Ansible ロールは、Active Directory 認証の設定をサポートします。

この更新により、Microsoft SQL Ansible ロールは SQL Server の Active Directory 認証の設定をサポートします。これで、**mssql_ad_** 接頭辞を使用して変数を設定することで、Active Directory 認証を設定できるようになりました。

Bugzilla:2163696

logging RHEL システムロールと firewall、selinux、および certificate ロールの統合

この機能拡張により、**logging** ロールを **firewall** ロール、ポートアクセスを管理するための **selinux** ロール、および証明書を生成するための **certificate** ロールと統合できるようになります。

ポートアクセスを制御するには、新しい **logging_manage_firewall** 変数と **logging_manage_selinux** 変数を使用します。どちらの変数もデフォルトでは **false** に設定されており、実行されません。**logging** ロール内でロールを実行するには、これらを **true** に設定します。

ファイアウォールと SELinux のポートアクセスを管理する責任があることに注意してください。

証明書を生成するには、新しい **logging_certificates** 変数を使用します。この変数はデフォルトで **false** に設定されており、**certificate** ロールは実行されません。この変数は、**certificate** ロールで **certificate_request** 変数を使用するのと同じ方法で使用できます。この変数を使用した場合、**logging** ロールは **certificate** ロールを使用して証明書を管理します。

Bugzilla:2130362

ルーティングルールは名前でルートテーブルを検索できます。

今回の更新により、**rhel-system-roles.network** RHEL システムロールは、ルーティングルールを定義するときに、名前によるルートテーブルの検索をサポートします。この機能は、ネットワークセグメントごとに異なるルーティングルールが必要な複雑なネットワーク設定を迅速にナビゲートします。

Bugzilla:2129620

Microsoft SQL Server Ansible ロールは SQL Server バージョン 2022 の設定をサポートします。

以前は、Microsoft SQL Ansible ロールは SQL Server バージョン 2017 とバージョン 2019 の設定のみをサポートしていました。この更新プログラムでは、Microsoft SQL Ansible ロールの SQL Server バージョン 2022 のサポートが提供されます。新しい SQL Server 2022 を設定するか、SQL Server をバージョン 2019 からバージョン 2022 にアップグレードするために、**mssql_version** 値を **2022** に設定できるようになりました。SQL Server をバージョン 2017 からバージョン 2022 にアップグレードすることはできないことに注意してください。

Bugzilla:2153427

journald RHEL システムロールが利用可能になりました。

journald サービスは、ログデータを収集し、一元化されたデータベースに保存します。この機能強化により、**journald** システムロール変数を使用して **systemd** ジャーナルの設定を自動化し、Red Hat Ansible Automation Platform を使用して永続的なログを設定できるようになりました。

Bugzilla:2165176

sshd RHEL システムロールが、firewall および selinux RHEL システムロールを使用してポートアクセスを管理できるようになりました。

この機能強化により、新しいロール変数 **sshd_manage_firewall** および **sshd_manage_selinux** を使用してポートアクセスの管理を自動化できます。これらが **true** に設定されている場合、各ロールはポートアクセスの管理に使用されます。これらが **false** (デフォルト) に設定されている場合、ロールは関与しません。

Bugzilla:2149683

4.16. 仮想化

ハードウェア暗号化デバイスを自動的にホットプラグできるようになりました。

以前は、仲介デバイスが開始される前に暗号化デバイスがホスト上に存在していた場合のみ、パススルー用の暗号化デバイスを定義できました。これで、仮想マシン (VM) にパススルーするすべての暗号化デバイスをリストする仲介デバイスマトリックスを定義できるようになりました。その結果、指定された暗号化デバイスは、後で使用可能になった場合、実行中の VM に自動的にパススルーされます。また、デバイスが使用できなくなると、デバイスは VM から削除されますが、ゲストオペレーティングシステムは正常に動作し続けます。

Bugzilla:1660908

IBM Z 上の PCI パススルーデバイスのパフォーマンスの向上

この更新では、I/O 処理に対する複数の改善により、IBM Z ハードウェアでの PCI パススルー実装が強化されました。その結果、IBM Z ホスト上の KVM 仮想マシン (VM) にパススルーされる PCI デバイスのパフォーマンスが大幅に向上しました。

さらに、ISM デバイスを IBM Z ホスト上の VM に割り当てることができるようになりました。

Bugzilla:1664379

RHEL 8 ゲストが SEV-SNP をサポートするようになりました。

RHEL 8 をゲストオペレーティングシステムとして使用する仮想マシン (VM) で、Secure Nested Paging (SNP) 機能を備えた AMD Secure Encrypted Virtualization (SEV) を使用できるようになりました。他の利点の中でも、SNP はメモリー整合性保護を改善することで SEV を強化します。これにより、データの再生やメモリーの再マッピングなどのハイパーバイザーベースの攻撃を防ぐことができます。SEV-SNP が RHEL 8 仮想マシンで機能するには、仮想マシンを実行しているホストも SEV-SNP をサポートしている必要があることに注意してください。

Bugzilla:2087262

zPCI デバイスの割り当て

IBM Z ハードウェア上で実行される RHEL でホストされる仮想マシン (VM) に、zPCI デバイスをパススルーデバイスとして接続できるようになりました。たとえば、これを使用すると、仮想マシンで NVMe フラッシュドライブを使用できます。

Jira:RHELPLAN-59528

4.17. サポート性

sos ユーティリティーは 4 週間ごとの更新頻度に移行しています。

RHEL マイナーリリースで **sos** 更新をリリースする代わりに、**sos** ユーティリティーのリリース頻度が 6 か月から 4 週間に変更されます。**sos** パッケージの更新の詳細については、RPM 変更ログで 4 週間ごとに確認できます。また、**sos** 更新の概要は RHEL リリースノートで 6 か月ごとに確認できます。

Bugzilla:2164987

sos clean コマンドで IPv6 アドレスが難読化されるようになりました。

以前は、**sos clean** コマンドは IPv6 アドレスを難読化せず、収集された **sos** レポートに顧客の機密データの一部が残っていました。この更新により、**sos clean** は期待どおりに IPv6 アドレスを検出し、難読化します。

Bugzilla:2134906

4.18. コンテナー

新しい podman RHEL システムロールが利用可能になりました。

Podman 4.2 以降では、**podman** システムロールを使用して、Podman 設定、コンテナー、および Podman コンテナーを実行する **systemd** サービスを管理できるようになりました。

Jira:RHELPLAN-118698

Podman は監査用のイベントをサポートするようになりました。

Podman v4.4 以降、コンテナーに関するすべての関連情報を 1 つのイベントと **journald** エントリーから直接収集できるようになりました。Podman 監査を有効にするには、**container.conf** 設定ファイルを変更し、**events_container_create_inspect_data=true** オプションを **engine** セクションに追加します。データは JSON 形式であり、**podman container inspect** コマンドからのものと同じです。詳細については、Podman 4.4 の新しいコンテナーイベントと監査機能の使用方法 を参照してください。

Jira:RHELPLAN-136601

Container Tools パッケージが更新される

Podman、Buildah、Skopeo、crun、runc ツールを含む、更新された Container Tools パッケージが利用可能になりました。この更新では、以前のバージョンに対する一連のバグ修正と機能強化が適用されます。

Podman v4.4 の注目すべき変更点は次のとおりです。

- Podman を使用して systemd サービスを簡単に作成および保守できる新しい systemd ジェネレーターである Quadlet を紹介します。
- 新しいコマンド **podman network update** が追加されました。これは、コンテナーと Pod のネットワークを更新します。
- buildah のバージョンを表示する新しいコマンド **podman buildx version** が追加されました。
- コンテナーに起動ヘルスチェックを設定できるようになり、通常のヘルスチェックがアクティブになる前にコマンドを実行してコンテナーが完全に起動していることを確認できるようになりました。
- **podman --dns** コマンドを使用して、カスタム DNS サーバーの選択をサポートします。
- Fulcio と Rekor を使用した sigstore 署名の作成と検証が利用できるようになりました。
- Docker との互換性が向上しました (新しいオプションとエイリアス)。

- Podman の Kubernetes 統合の改善 - コマンド **podman kubegenerate** および **podman kube play** が利用可能になり、**podmangenerate kube** および **podman play kube** コマンドに置き換わりました。**podman generated kube** および **podman play kube** コマンドは引き続き使用できますが、新しい **podman kube** コマンドを使用することを推奨します。

- **podman kube play** コマンドによって作成された Systemd 管理の Pod は、**io.containers.sdnotify** アノテーション (または特定のコンテナーの場合は **io.containers.sdnotify/$name**) を使用して sd-notify と統合されるようになりました。

- **podman kube play** によって作成された Systemd 管理の Pod は、 **io.containers.auto-update** アノテーション (または特定のコンテナーの場合は **io.containers.auto-update/$name**) を使用して自動更新できるようになりました。

Podman がバージョン 4.4 にアップグレードされました。注目すべき変更点の詳細については、アップストリームリリースノート を参照してください。

Jira:RHELPLAN-136608

Aardvark と Netavark がカスタム DNS サーバーの選択をサポートするようになりました。

Aardvark および Netavark ネットワークスタックは、ホスト上のデフォルトの DNS サーバーの代わりに、コンテナーのカスタム DNS サーバーの選択をサポートするようになりました。カスタム DNS サーバーを指定するには、次の 2 つのオプションがあります。

- **containers.conf** 設定ファイルに **dns_servers** フィールドを追加します。

- 新しい **--dns** Podman オプションを使用して、DNS サーバーの IP アドレスを指定します。

--dns オプションは、**container.conf** ファイル内の値をオーバーライドします。

Jira:RHELPLAN-138025

Skopeo は、sigstore キーペアの生成をサポートするようになりました。

skopeogenerate-sigstore-key コマンドを使用して、sigstore 公開キー/秘密キーのペアを生成できます。詳細については、**skopeo-generate-sigstore-key** man ページを参照してください。

Jira:RHELPLAN-151481

ツールボックスが利用可能になりました。

toolbox ユーティリティーを使用すると、トラブルシューティングツールをシステムに直接インストールしなくても、コンテナー化されたコマンドライン環境を使用できます。Toolbox は、Podman および OCI のその他の標準コンテナーテクノロジーを基盤として構築されています。詳細については、toolbx を参照してください。

Jira:RHELPLAN-150266

イメージに署名するための複数の信頼できる GPG キーの機能が利用可能です。

/etc/containers/policy.json ファイルは、信頼できるキーを含むファイルのリストを受け入れる新しい **keyPaths** フィールドをサポートします。このため、Red Hat の一般公開キーとベータ GPG キーで署名されたコンテナーイメージがデフォルト設定で受け入れられるようになりました。

以下に例を示します。

```
"registry.redhat.io": [
        {
```

```
            "type": "signedBy",
            "keyType": "GPGKeys",
            "keyPaths": ["/etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release", "/etc/pki/rpm-gpg/RPM-GPG-
KEY-redhat-beta"]
        }
]
```

Jira:RHELPLAN-118470

RHEL 8 延長更新サポート

RHEL コンテナーツールが RHEL 8 延長更新サポート(EUS) リリースでサポートされるようになりました。Red Hat Enterprise Linux EUS の詳細は、コンテナーツール Appstream コンテンツの提供、Red Hat Enterprise Linux (RHEL) Extended Update Support (EUS) の概要 を参照してください。

Jira:RHELPLAN-151121

sigstore 署名が利用可能になりました。

Podman 4.2 以降では、コンテナーイメージ署名の sigstore 形式を使用できます。sigstore 署名はコンテナーイメージと共にコンテナーレジストリーに格納されるため、イメージ署名を格納するために別の署名サーバーを用意する必要はありません。

Jira:RHELPLAN-75165

Podman が実行前フックをサポートするようになりました。

/usr/libexec/podman/pre-exec-hooks ディレクトリーと **/etc/containers/pre-exec-hooks** ディレクトリーにある root 所有のプラグインスクリプトは、コンテナー操作の詳細な制御、特に無許可のアクションのブロックを定義します。

/etc/containers/podman_preexec_hooks.txt ファイルは管理者が作成する必要があり、空でもかまいません。**/etc/containers/podman_preexec_hooks.txt** が存在しない場合、プラグインスクリプトは実行されません。すべてのプラグインスクリプトがゼロ値を返す場合、**podman** コマンドが実行されます。それ以外の場合、**podman** コマンドは継承された終了コードで終了します。

Red Hat では、スクリプトを正しい順序で実行するために、**DDD-plugin_name.lang** (例: **010-check-group.py**) という命名規則を使用することを推奨しています。プラグインスクリプトは作成時点で有効であることに注意してください。プラグインスクリプトの前に作成されたコンテナーは影響を受けません。

Bugzilla:2119200

第5章 外部カーネルパラメーターへの重要な変更

本章では、システム管理者向けに、Red Hat Enterprise Linux 8.8 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。変更には、たとえば、**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、または重要な動作の変更などが含まれます。

新しいカーネルパラメーター

nomodeset

このカーネルパラメーターを使用すると、カーネルモード設定を無効にすることができます。DRM ドライバーは、表示モードの変更や高速レンダリングを実行しません。システムフレームバッファーがファームウェアまたはブートローダーによって設定されている場合、システムフレームバッファーのみが使用可能になります。
nomodeset は、フォールバックとして、またはテストとデバッグに役立ちます。

sev=option[,option...] [X86-64]

詳細については、**Documentation/x86/x86_64/boot-options.rst** を参照してください。

amd_pstate=[X86]

- disable: サポートされているプロセッサーのデフォルトのスケーリングドライバーとして **amd_pstate** を有効にしないでください。
- passive: **amd_pstate** をスケーリングドライバーとして使用します。ドライバーはこの抽象的なスケールに基づいて必要なパフォーマンスを要求します。その要求を、電源管理ファームウェアがコア周波数、データファブリック、メモリークロックなどの実際のハードウェア状態に変換します。

retbleed=ibpb,nosmt

このパラメーターは **ibpb** に似ており、STIBP を持たないシステムの代替パラメーターです。このパラメーターを使用すると、STIBP が使用できない場合に SMT を無効にすることができます。

更新されたカーネルパラメーター

amd_iommu=[HW,X86-64]

このカーネルパラメーターを使用すると、システム内の AMD IOMMU ドライバーにパラメーターを渡すことができます。可能な値は次のとおりです。

- fullflush: 非推奨。**iommu.strict=1** と同等です。
- off: システムで見つかった AMD IOMMU を初期化しません。
- force_isolation: すべてのデバイスのデバイス分離を強制します。IOMMU ドライバーは、必要に応じて分離要件を引き上げることができなくなりました。
  - このオプションは **iommu=pt** をオーバーライドしません。
- force_enable: IOMMU を有効にするとバグがあることがわかっているプラットフォームで、IOMMU を強制的に有効にします。
  - このオプションは注意して使用してください。

crashkernel=size[KMG][@offset[KMG]]

[KNL] **kexec** を使用すると、Linux はパニック時にクラッシュカーネルに切り替えることができます。このパラメーターは、そのカーネルイメージの物理メモリー領域 [offset, offset + size] を予約します。**@offset** を省略すると、適切なオフセットが自動的に選択されます。
[KNL, X86-64, ARM64] 最初に 4G 未満の領域を選択し、**@offset** が指定されていない場合は 4G を超える予約領域にフォールバックします。

詳細については、**Documentation/admin-guide/kdump/kdump.rst** を参照してください。

crashkernel=size[KMG],low

- [KNL, X86-64, ARM64] このパラメーターを使用すると、2 番目のカーネルに 4G 未満の低範囲を指定できます。**crashkernel=X,high** が渡されると、ある程度の低メモリーが必要になります。たとえば、**swiotlb** には少なくとも 64M+32K の低メモリーが必要です。また、32 ビットデバイスの DMA バッファーが不足しないようにするために十分な追加の低メモリーも必要です。カーネルは、4G 未満のデフォルトサイズのメモリーを自動的に割り当てようとします。デフォルトサイズはプラットフォームによって異なります。
  - x86: max(swiotlb_size_or_default() + 8MiB, 256MiB)
  - arm64: 128MiB
    0: 低割り当てを無効にします。

    crashkernel=X,high が使用されない場合、または予約されたメモリーが 4G 未満の場合、このパラメーターは無視されます。
- [KNL, ARM64] このパラメーターを使用すると、クラッシュダンプカーネルの DMA ゾーンの下限範囲を指定できます。
  crashkernel=X,high が使用されていない場合、このパラメーターは無視されます。

intel_iommu=[DMAR]

Intel IOMMU ドライバー (DMAR) オプションを設定するためのカーネルパラメーター。

- on: intel iommu ドライバーを有効にします。
- off: intel iommu ドライバーを無効にします。
- igfx_off [デフォルトではオフ]: デフォルトでは、gfx は通常のデバイスとしてマッピングされます。gfx デバイスに専用の DMAR ユニットがある場合、このオプションで DMAR を有効にしないと、DMAR ユニットがバイパスされます。この場合、**gfx** デバイスは DMA に物理アドレスを使用します。
- strict [デフォルトではオフ]: 非推奨。**iommu.strict=1** と同等です。
- sp_off [デフォルトではオフ]: Intel IOMMU にスーパーページ機能がある場合、デフォルトではスーパーページがサポートされます。このオプションを使用すると、スーパーページはサポートされなくなります。
- sm_on [デフォルトではオフ]: ハードウェアがスケーラブルモード変換をサポートしていることをアドバタイズしている場合でも、デフォルトでは、スケーラブルモードは無効になります。このオプションが設定されていると、スケーラブルモードは、これをサポートすると主張するハードウェアで使用されます。
- tboot_noforce [デフォルトではオフ]: **tboot** でインテル IOMMU を強制的に有効にしません。デフォルトでは、**tboot** は Intel IOMMU を強制的にオンにします。これにより、ID マッピングが有効になっている場合でも、40 GBit ネットワークカードなど、一部の高スループットデバイスのパフォーマンスに悪影響が及ぶ可能性があります。

注記

このオプションを使用すると、システムが DMA 攻撃に対して脆弱になるため、**tboot** によって提供されるセキュリティーが低下します。

iommu.strict=[ARM64,X86]

このカーネルパラメーターを使用すると、TLB の無効化動作を設定できます。
形式: **{ "0" | "1" }**

- 0 - レイジーモード。DMA アンマップ操作でハードウェア TLB の遅延無効化を使用するように要求し、デバイスの分離を犠牲にしてスループットを向上させます。関連する IOMMU ドライバーでサポートされていない場合は、厳密モードにフォールバックします。
- 1 - 厳密モード。DMA アンマップ操作で IOMMU ハードウェア TLB を同期的に無効にします。
- unset - **CONFIG_IOMMU_DEFAULT_DMA_{LAZY,STRICT}** の値を使用します。

注記

x86 では、従来のドライバー固有のオプションの 1 つで指定された厳密モードが優先されます。

mem_encrypt=[X86-64]

AMD Secure Memory Encryption (SME) コントロールを設定するためのカーネルパラメーター。
有効な引数: on、off

デフォルトはカーネル設定オプションによって異なります。

- on (CONFIG_AMD_MEM_ENCRYPT_ACTIVE_BY_DEFAULT=y)
- off (CONFIG_AMD_MEM_ENCRYPT_ACTIVE_BY_DEFAULT=n)
- mem_encrypt=on: SME をアクティブ化する
- mem_encrypt=off: SME をアクティブ化しない
  メモリー暗号化をアクティブ化できる条件の詳細は、**Documentation/virt/kvm/x86/amd-memory-encryption.rst** を参照してください。

retbleed=[X86]

このカーネルパラメーターを使用すると、RETBleed (リターン命令による任意の投機的コード実行) 脆弱性の軽減を制御できます。
AMD ベースの UNRET および IBPB の軽減策だけでは、兄弟スレッドが他の兄弟スレッドの予測に影響を与えることを防ぐことはできません。そのため、STIBP はそれをサポートするプロセッサーで使用され、STIBP をサポートしないプロセッサーでは SMT を緩和します。

- オフ - 緩和策なし
- auto - 緩和策を自動的に選択します。
- auto,nosmt - 緩和策を自動的に選択し、完全な緩和策に必要な場合は SMT を無効にします (STIBP のない Zen1 以前のみ)。

- ibpb - AMD では、基本ブロック境界での短い推測ウィンドウも軽減します。安全で最高のパフォーマンスへの影響。STIBP が存在する場合は、それも有効になります。Intel には適していません。
- unret - トレーニングされていないリターンサンクを強制的に有効にします。AMD f15h-f17h ベースのシステムのみで有効です。
- unret,nosmt - unret と似ていますが、STIBP が利用できない場合は SMT を無効にします。これは、STIBP を持たないシステムの代替手段です。

swiotlb=[ARM,IA-64,PPC,MIPS,X86]

このカーネルパラメーターを使用すると、I/O TLB スラブの動作を設定できます。
形式: **{ <int> [,<int>] | force | noforce }**

- <int> - I/O TLB スラブの数。
- <int> - コンマの後の 2 番目の整数。独自のロックを持つ swiotlb エリアの数。**2** の累乗である必要があります。
- force - カーネルによって自動的に使用されない場合でも、バウンスバッファーの使用を強制します。
- noforce - バウンスバッファーを使用しません (デバッグ用)。

新しい sysctl パラメーター

page_lock_unfairness

この値は、ウェイターからページロックを奪うことができる回数を決定します。このファイルで指定された回数 (デフォルトは 5) だけロックが奪われると、**fair lock handoff** セマンティクスが適用され、ロックを取得できる場合にのみウェイターが起動されます。

rps_default_mask

新しく作成されたネットワークデバイスで使用されるデフォルトの RPS CPU マスク。空のマスクは、デフォルトで RPS が無効になっていることを意味します。

第6章 デバイスドライバー

6.1. 新しいドライバー

ネットワークドライバー

- Solarflare Siena ネットワークドライバー (**sfc-siena**)、IBM Power Systems、Little Endian、AMD および Intel 64 ビットアーキテクチャーのみ
- Nvidia sn2201 プラットフォームドライバー (**nvsw-sn2201**)、AMD および Intel 64 ビットアーキテクチャーのみ
- AMD SEV Guest Driver (**sev-guest**)、AMD および Intel 64 ビットアーキテクチャーのみ
- TDX ゲストドライバー (**tdx-guest**)、AMD および Intel 64 ビットアーキテクチャーのみ

グラフィックドライバーとその他のドライバー

- ACPI ビデオドライバー (**video**)、64 ビット ARM アーキテクチャーのみ
- DRM Buddy Allocator (**drm_buddy**)、64 ビット ARM アーキテクチャーおよび IBM Power Systems のみ、リトルエンディアン
- DRM ディスプレイアダプターヘルパー (**drm_display_helper**)、64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ
- Intel® GVT-g for KVM (**kvmgt**)、AMD および Intel 64 ビットアーキテクチャーのみ
- HP® iLO/iLO2 管理プロセッサー (**hpilo**)、64 ビット ARM アーキテクチャーのみ
- HPE ウォッチドッグドライバー (**hpwdt**)、64 ビット ARM アーキテクチャーのみ
- AMD HSMP Platform Interface Driver (**amd_hsmp.**)、AMD および Intel 64 ビットアーキテクチャーのみ

6.2. 更新されたドライバー

ネットワークドライバー

- Intel® 10 Gigabit PCI Express Network Driver (**ixgbe**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。
- Intel® 10 Gigabit Virtual Function Network Driver (**ixgbevf**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。
- Intel® 2.5G Ethernet Linux Driver (**igc.**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。
- Intel® Ethernet Adaptive Virtual Function Network Driver (**iavf**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- Intel® Ethernet Connection XL710 Network Driver (**i40e**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- Intel® Ethernet Switch Host Interface Driver (**fm10k**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- Intel® Gigabit Ethernet Network Driver (**igb**) がバージョン 4.18.0-477 に更新されました。(64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- Intel® Gigabit Virtual Function Network Driver (**igbvf**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- Intel® PRO/1000 Network Driver (**e1000e**) がバージョン 4.18.0-477 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- Mellanox 第 5 世代ネットワークアダプター (ConnectX シリーズ) コアドライバー (**mlx5_core**) がバージョン 4.18.0-477 に更新されました。

- Netronome Flow Processor (NFP) ドライバー (**nfp**) がバージョン 4.18.0-477 に更新されました。

ストレージドライバー

- Driver for Microchip Smart Family Controller (**smartpqi**) がバージョン 2.1.20-035 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- Emulex LightPulse Fibre Channel SCSI ドライバー (**lpfc**) がバージョン 14.0.0.18 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- LSI MPT Fusion SAS 3.0 デバイスドライバー (**mpt3sas**) がバージョン 43.100.00.00 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- MPI3 Storage Controller Device Driver (**mpi3mr**) がバージョン 8.2.0.3.0 に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- QLogic Fibre Channel HBA Driver (**qla2xxx**) がバージョン 10.02.07.900-k に更新されました (64 ビット ARM アーキテクチャー、IBM Power Systems、リトルエンディアン、AMD および Intel 64 ビットアーキテクチャーのみ)。

- SCSI デバッグアダプタードライバー (**scsi_debug**) がバージョン 0191 に更新されました。

第7章 利用可能な BPF 機能

この章では、Red Hat Enterprise Linux 8 のこのマイナーバージョンのカーネルで利用可能な **Berkeley Packet Filter** (**BPF**) 機能の完全なリストを提供します。表には次のリストが含まれます。

- システム設定とその他のオプション
- 利用可能なプログラムの種類とサポートされているヘルパー
- 利用可能なマップの種類

この章には、**bpftool feature** コマンドの自動生成された出力が含まれています。

表7.1 システム設定とその他のオプション

オプション	値
unprivileged_bpf_disabled	1 (特権ユーザーに限定された bpf() syscall、リカバリーなし)
JIT コンパイラー	1 (有効)
JIT コンパイラーの強化	1 (権限のないユーザーに対して有効)
JIT コンパイラー kallsyms エクスポート	1 (ルートで有効)
非特権ユーザーの JIT のメモリー制限	264241152
CONFIG_BPF	y
CONFIG_BPF_SYSCALL	y
CONFIG_HAVE_EBPF_JIT	y
CONFIG_BPF_JIT	y
CONFIG_BPF_JIT_ALWAYS_ON	y
CONFIG_DEBUG_INFO_BTF	y
CONFIG_DEBUG_INFO_BTF_MODULES	n
CONFIG_CGROUPS	y
CONFIG_CGROUP_BPF	y
CONFIG_CGROUP_NET_CLASSID	y
CONFIG_SOCK_CGROUP_DATA	y

オプション	値
CONFIG_BPF_EVENTS	y
CONFIG_KPROBE_EVENTS	y
CONFIG_UPROBE_EVENTS	y
CONFIG_TRACING	y
CONFIG_FTRACE_SYSCALLS	y
CONFIG_FUNCTION_ERROR_INJECTION	y
CONFIG_BPF_KPROBE_OVERRIDE	y
CONFIG_NET	y
CONFIG_XDP_SOCKETS	y
CONFIG_LWTUNNEL_BPF	y
CONFIG_NET_ACT_BPF	m
CONFIG_NET_CLS_BPF	m
CONFIG_NET_CLS_ACT	y
CONFIG_NET_SCH_INGRESS	m
CONFIG_XFRM	y
CONFIG_IP_ROUTE_CLASSID	y
CONFIG_IPV6_SEG6_BPF	n
CONFIG_BPF_LIRC_MODE2	n
CONFIG_BPF_STREAM_PARSER	y
CONFIG_NETFILTER_XT_MATCH_BPF	m
CONFIG_BPFILTER	n
CONFIG_BPFILTER_UMH	n

オプション	値
CONFIG_TEST_BPF	m
CONFIG_HZ	1000
bpf() syscall	available
大きなプログラムサイズの制限	available

表7.2 利用可能なプログラムの種類とサポートされているヘルパー

プログラムの種類	利用可能なヘルパー
socket_filter	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
kprobe	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_override_return, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
sched_cls	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf
sched_act	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
xdp	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_redirect, bpf_perf_event_output, bpf_csum_diff, bpf_get_current_task, bpf_get_numa_node_id, bpf_xdp_adjust_head, bpf_redirect_map, bpf_xdp_adjust_meta, bpf_xdp_adjust_tail, bpf_fib_lookup, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf
perf_event	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_perf_prog_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_read_branch_records, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
cgroup_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_skb_cgroup_id, bpf_get_local_storage, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_sk_cgroup_id, bpf_sk_ancestor_cgroup_id, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_sock	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_storage_get, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lwt_in	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_lwt_push_encap, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
lwt_out	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lwt_xmit	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_lwt_push_encap, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
sock_ops	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_sock_map_update, bpf_getsockopt, bpf_sock_ops_cb_flags_set, bpf_sock_hash_update, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_load_hdr_opt, bpf_store_hdr_opt, bpf_reserve_hdr_opt, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
sk_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_adjust_room, bpf_sk_redirect_map, bpf_sk_redirect_hash, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_device	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
sk_msg	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_msg_redirect_map, bpf_msg_apply_bytes, bpf_msg_cork_bytes, bpf_msg_pull_data, bpf_msg_redirect_hash, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_msg_push_data, bpf_msg_pop_data, bpf_spin_lock, bpf_spin_unlock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
raw_tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_sock_addr	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_getsockopt, bpf_bind, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lwt_seg6local	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
lirc_mode2	サポート対象外

プログラムの種類	利用可能なヘルパー
sk_reuseport	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_skb_load_bytes_relative, bpf_sk_select_reuseport, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
flow_dissector	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
cgroup_sysctl	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sysctl_get_name, bpf_sysctl_get_current_value, bpf_sysctl_get_new_value, bpf_sysctl_set_new_value, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
raw_tracepoint_writable	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

プログラムの種類	利用可能なヘルパー
cgroup_sockopt	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf
tracing	サポート対象外

プログラムの種類	利用可能なヘルパー
struct_ops	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_perf_event_read, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_stackid, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_xdp_adjust_head, bpf_probe_read_str, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_setsockopt, bpf_skb_adjust_room, bpf_redirect_map, bpf_sk_redirect_map, bpf_sock_map_update, bpf_xdp_adjust_meta, bpf_perf_event_read_value, bpf_perf_prog_read_value, bpf_getsockopt, bpf_override_return, bpf_sock_ops_cb_flags_set, bpf_msg_redirect_map, bpf_msg_apply_bytes, bpf_msg_cork_bytes, bpf_msg_pull_data, bpf_bind, bpf_xdp_adjust_tail, bpf_skb_get_xfrm_state, bpf_get_stack, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_sock_hash_update, bpf_msg_redirect_hash, bpf_sk_redirect_hash, bpf_lwt_push_encap, bpf_lwt_seg6_store_bytes, bpf_lwt_seg6_adjust_srh, bpf_lwt_seg6_action, bpf_rc_repeat, bpf_rc_keydown, bpf_skb_cgroup_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_sk_select_reuseport, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_msg_push_data, bpf_msg_pop_data, bpf_rc_pointer_rel, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sysctl_get_name, bpf_sysctl_get_current_value, bpf_sysctl_get_new_value, bpf_sysctl_set_new_value, bpf_strtol, bpf_strtoul, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_send_signal, bpf_tcp_gen_syncookie, bpf_skb_output, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_tcp_send_ack, bpf_send_signal_thread, bpf_jiffies64, bpf_read_branch_records, bpf_get_ns_current_pid_tgid, bpf_xdp_output, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_seq_printf, bpf_seq_write, bpf_sk_cgroup_id, bpf_sk_ancestor_cgroup_id, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_get_task_stack, bpf_load_hdr_opt, bpf_store_hdr_opt, bpf_reserve_hdr_opt, bpf_inode_storage_get, bpf_inode_storage_delete, bpf_d_path, bpf_copy_from_user, bpf_snprintf_btf, bpf_seq_printf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_bprm_opts_set, bpf_ktime_get_coarse_ns, bpf_ima_inode_hash, bpf_sock_from_file, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_sys_bpf, bpf_btf_find_by_name_kind, bpf_sys_close
ext	サポート対象外
lsm	サポート対象外

プログラムの種類	利用可能なヘルパー
sk_lookup	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf

表7.3 利用可能なマップの種類

マップの種類	Available
ハッシュ	はい
array	はい
prog_array	はい
perf_event_array	はい
percpu_hash	はい
percpu_array	はい
stack_trace	はい
cgroup_array	はい
lru_hash	はい
lru_percpu_hash	はい
lpm_trie	はい
array_of_maps	はい
hash_of_maps	はい
devmap	はい
sockmap	はい

マップの種類	Available
cpumap	はい
xskmap	はい
sockhash	はい
cgroup_storage	はい
reuseport_sockarray	はい
percpu_cgroup_storage	はい
queue	はい
stack	はい
sk_storage	はい
devmap_hash	はい
struct_ops	いいえ
ringbuf	はい
inode_storage	はい
task_storage	いいえ

第8章 バグ修正

このパートでは、Red Hat Enterprise Linux 8.8 で修正された、ユーザーに重大な影響を与えるバグについて説明します。

8.1. インストーラーおよびイメージの作成

インストーラーは、カスタムパーティショニング中にすべての PPC PreP Boot または BIOS Boot パーティションをリストするようになりました。

以前は、カスタムパーティショニング中に複数の **PPC PreP Boot** または **BIOS Boot** パーティションを追加すると、Custom Partitioning 画面には関連するタイプのパーティションが 1 つだけ表示されていました。その結果、カスタムパーティショニング画面には意図したパーティショニングレイアウトの実際の状態が反映されず、パーティショニングプロセスが困難かつ不透明になっていました。

この更新により、カスタムパーティショニング画面のパーティションリストにすべての **PPC PreP Boot** または **BIOS Boot** パーティションが正しく表示されるようになりました。その結果、ユーザーは意図したパーティショニングレイアウトをよりよく理解し、管理できるようになりました。

Bugzilla:1913035

インストーラーは、設定オプションを yum リポジトリーファイルに正しく追加するようになりました。

以前は、追加のインストールリポジトリーからパッケージを含めたり除外したりするときに、インストーラは yum リポジトリーファイルに設定オプションを正しく追加しませんでした。この更新により、yum リポジトリーファイルが正しく作成されるようになりました。その結果、**repo** キックスタートコマンドで **--excludepkgs=** または **--includepkgs=** オプションを使用すると、インストール中に指定されたパッケージが期待どおりに除外または組み込まれるようになりました。

Bugzilla:2014103

filename DHCP オプションを使用しても、インストール用の kickstart ファイルのダウンロードがブロックされなくなりました。

以前は、NFS サーバーからキックスタートファイルを取得するためのパスを構築するときに、インストーラーは **filename** DHCP オプションを考慮しませんでした。その結果、インストーラーはキックスタートファイルをダウンロードせず、インストールプロセスをブロックしていました。この更新により、**filename** DHCP オプションはキックスタートファイルへのパスを正しく構築します。その結果、キックスタートファイルが適切にダウンロードされ、インストールプロセスが正しく開始されます。

Bugzilla:1991516

インストーラーはカスタムパーティショニング中に新しい GPT ディスクレイアウトを作成するようになりました。

以前は、カーネルコマンドラインで **inst.gpt** が指定されている場合、インストーラはディスクレイアウトを GPT に変更せず、ユーザーはカスタムパーティショニングスポーク上の MBR ディスクレイアウトを持つディスクからすべてのパーティションを削除していました。その結果、MBR ディスクレイアウトがディスク上に残りました。

この更新により、カーネルコマンドラインで **inst.gpt** が指定されている場合、インストーラーはディスク上に新しい GPT ディスクレイアウトを作成し、カスタムパーティションスポーク上のディスクからすべてのパーティションが削除されます。

Bugzilla:2094977

combos-cli compose start コマンドの --size パラメーターが、その値を MiB として扱うようになりました。

以前は、**composer-cli compose start --size size_value blueprint_name image_type** コマンドを使用する場合、**composer-cli** ツールは **--size** パラメーター値をバイト単位として扱っていました。この更新により問題が修正され、**--size** パラメーター値が MiB 形式で正しく使用されるようになりました。

Bugzilla:2033192

8.2. ソフトウェア管理

fapolicyd サービスの再起動を伴うトランザクション中に RPM がハングしなくなりました

以前は、**fapolicyd** サービスの再起動を引き起こすパッケージ (**systemd** など) を更新しようとすると、**fapolicyd** プラグインが **fapolicyd** デーモンとの通信に失敗したため、RPM トランザクションが応答を停止していました。

この更新により、**fapolicyd** プラグインは **fapolicyd** デーモンと正しく通信できるようになりました。その結果、**fapolicyd** サービスの再起動を伴うトランザクション中に RPM がハングしなくなりました。

Bugzilla:2110787

アップグレードによってアーキテクチャーが変更されるパッケージに対してセキュリティー YUM アップグレードが可能になりました。

RHBA-2022:7711 とともに導入された BZ#2088149 のパッチにより、セキュリティーフィルターを使用した YUM アップグレードで、アップグレードを通じてアーキテクチャーが noarch から、または **noarch** に変更されたパッケージがスキップされるというリグレッションが発生しました。したがって、これらのパッケージのセキュリティーアップグレードが不足していると、システムが脆弱な状態になる可能性があります。

今回の更新により、この問題は修正され、セキュリティー YUM アップグレードで、アーキテクチャーを noarch から変更するパッケージ、または **noarch** に変更するパッケージがスキップされなくなりました。

Bugzilla:2124483

パッケージグループまたは環境に対して YUM アップグレードトランザクションを元に戻せるようになりました。

以前は、パッケージグループまたは環境のアップグレードトランザクションを元に戻そうとすると、**yum history rollback** コマンドが失敗していました。

今回の更新により、この問題は修正され、パッケージグループまたは環境の YUM アップグレードトランザクションを元に戻せるようになりました。

Bugzilla:2016070

8.3. シェルおよびコマンドラインツール

wsmancli は HTTP 401 Unauthorized ステータスを正しく処理します。

Web サービス管理プロトコルを使用してシステムを管理するための **wsmancli** ユーティリティーは、RFC 2616 への準拠を強化するために認証を処理するようになりました。

以前は、認証が必要なサービスに接続すると、**wsmancli** コマンドは、認証情報が不完全であるなどの理由で、HTTP 401 Unauthorized 応答を受信した直後、エラーメッセージ **Authentication failed,**

please retry を返していました。続行するには、認証情報の一部をすでに提供している場合でも、**wsmancli** はユーザー名とパスワードの両方を提供するように求めます。

この更新により、**wsmancli** は、以前に提供されていなかった認証情報のみを必要とするようになりました。その結果、最初の認証試行ではエラーメッセージが表示されません。エラーメッセージは、完全な認証情報を入力して認証が失敗した場合のみ、表示されます。

Bugzilla:2105316

translator.sty LaTeX スタイルドキュメントが追加されました。

以前は、**texlive-beamer** に依存する特定のツールに必要な **translator.sty** LaTeX スタイルドキュメントが不足していました。その結果、これらのツールは **LaTeX Error: File `translator.sty' not found.** というエラーで失敗していました。この更新により、**translator.sty** LaTeX スタイルドキュメントを含む、不足している **texlive-translator** パッケージが追加されます。これにより、**texlive-beamer** に依存するツールが正しく動作します。

Bugzilla:2150727

ReaR は、IBM Z アーキテクチャー上で除外された DASD を正しく処理します。

以前の IBM Z アーキテクチャーでは、ReaR は、ユーザーが保存されたレイアウトから除外し、コンテンツを復元するつもりがなかった DASD を含め、接続されているすべてのダイレクトアクセスストレージデバイス (DASD) をリカバリープロセス中に再フォーマットしていました。その結果、保存されたレイアウトから一部の DASD を除外すると、システムの回復中にそれらのデータが失われます。この更新により、ReaR は、(zIPL ブートローダーを使用して) ReaR レスキューシステムがブートされたデバイスを含む、システムリカバリー中に除外された DASD をフォーマットしなくなりました。ReaR が DASD を再フォーマットする前に、DASD フォーマットスクリプトを確認するように求められます。これにより、除外された DASD 上のデータはシステム回復後も確実に残ります。

Bugzilla:2172605

ReaR は非 LVM XFS ファイルシステムの復元に失敗しなくなりました。

以前は、ReaR を使用して特定の設定とディスクマッピングを使用して非 LVM XFS ファイルシステムを復元すると、ReaR は指定された設定ではなくデフォルト設定でファイルシステムを作成していました。

たとえば、ファイルシステムの **sunit** パラメーターと **swidth** パラメーターが 0 以外の値に設定されており、ディスクマッピングを備えた ReaR を使用してファイルシステムを復元した場合、ファイルシステムは、指定された値を無視してデフォルトの **sunit** パラメーターと **swidth** パラメーターで作成されます。

その結果、ReaR は特定の XFS オプションを使用してファイルシステムをマウントするときに失敗しました。この更新により、ReaR は指定された設定でファイルシステムを正しく復元します。

Bugzilla:2131946

8.4. インフラストラクチャーサービス

拡張属性に正規表現を使用している場合に rsync が失敗しなくなりました。

以前は、ファイルを転送および同期するための **rsync** ユーティリティーが、RHEL 8 の拡張属性を正しく処理できませんでした。たとえば、拡張属性の **--delete** オプションと **--filter '-x string.*'** オプションを **rsync** コマンドに渡したときに、システム上のファイルが正規表現を満たしている場合、プロトコルの非互換性を示すエラーメッセージが表示されました。この更新により、**rsync** ユーティリティーが拡張属性を正しく処理し、この属性に正規表現を使用できるようになりました。

Bugzilla:2139118

8.5. セキュリティー

スキャンと修復は SCAP 監査ルールを正しく無視します。

以前は、監査キー (**-k** または **-F** キー) を使用せずに定義された監査監視ルールでは、次の問題が発生しました。

- ルールの他の部分が正しい場合でも、ルールは非準拠としてマークされていました。
- Bash 修復により監視ルールのパスと権限が修正されましたが、監査キーが正しく追加されませんでした。
- 修復によって欠落したキーが修正されず、**fixed** 値の代わりに **error** が返されることがありました。

これは次のルールに影響を与えました。

- **audit_rules_login_events**
- **audit_rules_login_events_faillock**
- **audit_rules_login_events_lastlog**
- **audit_rules_login_events_tallylog**
- **audit_rules_usergroup_modification**
- **audit_rules_usergroup_modification_group**
- **audit_rules_usergroup_modification_gshadow**
- **audit_rules_usergroup_modification_opasswd**
- **audit_rules_usergroup_modification_passwd**
- **audit_rules_usergroup_modification_shadow**
- **audit_rules_time_watch_localtime**
- **audit_rules_mac_modification**
- **audit_rules_networkconfig_modification**
- **audit_rules_sysadmin_actions**
- **audit_rules_session_events**
- **audit_rules_sudoers**
- **audit_rules_sudoers_d**

この更新により、Audit キーがチェック、Bash および Ansible の修復から削除されました。その結果、チェックおよび修復中にキーフィールドによって引き起こされる不一致は発生しなくなり、監査人はこれらのキーを任意に選択して監査ログの検索を容易にすることができます。

Bugzilla:2119356

crypto-policies が不要なシンボリックリンクを作成しなくなりました。

システムのインストール中、**crypto-policies** スクリプトレットは、**/usr/share/crypto-policies/DEFAULT** ファイルまたは FIPS モードの **/usr/share/crypto-policies/FIPS** からシンボリックリンクを作成し、**/etc/crypto-policies/back-ends** ディレクトリーに保存します。以前は、**crypto-policies** が誤ってディレクトリーを含めていたため、**/usr/share/crypto-policies/DEFAULT** または **/usr/share/crypto-policies/FIPS** を参照する **/etc/crypto-policies/back-ends/.config** シンボリックリンクが作成されていました。今回の更新により、**crypto-policies** はディレクトリーからシンボリックリンクを作成しなくなるため、この不要なシンボリックリンクは作成されなくなります。

Bugzilla:1921646

crypto-policies が BIND の NSEC3DSA を無効にするようになりました。

以前は、システム全体の暗号化ポリシーは、BIND 設定の **NSEC3DSA** アルゴリズムを制御していませんでした。その結果、現在のセキュリティー要件を満たしていない **NSEC3DSA** は、DNS サーバーで無効になりませんでした。この更新により、すべての暗号化ポリシーはデフォルトで BIND 設定の **NSEC3DSA** を無効にします。

Bugzilla:2071981

Libreswan は、FUTURE および FIPS 暗号化ポリシーで SHA-1 署名検証を拒否しなくなりました

以前は、4.9 への更新以降、Libreswan は **FUTURE** および **FIPS** 暗号化ポリシーで SHA-1 署名検証を拒否し、**authby=rsasig** または **authby=rsa-sha1** 接続オプションが使用されている場合にピア認証が失敗しました。この更新では、Libreswan による **crypto-policies** 設定の処理方法を緩和することで、この動作を元に戻します。その結果、SHA-1 署名検証を使用して **authby=rsasig** および **authby=rsa-sha1** 接続オプションを使用できるようになりました。

Bugzilla:2176248

crontab bash スクリプトが不適切なコンテキストで実行されなくなりました。

以前は、エラータ RHBA-2022:7691 で公開されたバグ修正で、一般的すぎる移行ルールが使用されていました。その結果、**crontab** ファイルから実行された bash スクリプトが、**system_cronjob_t** コンテキストではなく **rpm_script_t** コンテキストで実行されていました。この更新により、bash スクリプトが正しいコンテキストで実行されるようになりました。

Bugzilla:2154242

selinux-policy は SAP ホストエージェントでのサービス実行をサポートします

以前は、SELinux ポリシーは、SAP ホストエージェントおよびその他のサービスと対話する **Insights-client** サービスをサポートしていませんでした。その結果、一部のコマンドは Red Hat Insights から開始した場合に正しく機能しませんでした。この更新により、SELinux ポリシーは SAP サービスの実行をサポートします。その結果、Insights から開始された SAP サービスは正常に実行されます。

Bugzilla:2134125

selinux-policy により、pmcd がプライベートの memfd: オブジェクトを実行できるようになりました。

以前は、SELinux ポリシーでは、パフォーマンスコパイロット (PCP) フレームワークの **pmcd** プロセスがプライベートメモリーファイルシステムオブジェクト (**memfd:**) を実行することを許可していませんでした。その結果、SELinux は、**memfd:** オブジェクトを実行する Performance Metric Domain

Agent (PMDA) BPF Compiler Collection (BCC) サービスを拒否していました。この更新では、SELinux ポリシーに **pcmd** の新しいルールが含まれています。その結果、enforcing モードの SELinux で **pmcd** が **memfd:** オブジェクトを実行できるようになりました。

Bugzilla:2090711

SELinux ポリシーにより、sysadm_r が subscription-manager を使用できるようになります。

以前は、SELinux ロール **sysadm_r** のユーザーは、**subscription-manager** ユーティリティーの一部のサブコマンドを実行できませんでした。その結果、そのサブコマンドでメモリーデバイスを読み取ることができませんでした。この更新により、**sysadm_t** タイプによる **/dev/mem** の読み取りを許可する新しいルールが SELinux ポリシーに追加されます。これにより、**subscription-manager** のサブコマンドが失敗しなくなります。

Bugzilla:2101341

samba-dcerpcd プロセスが nscd で正しく動作するようになりました。

以前は、SELinux ポリシーが原因で、**samba-dcerpcd** プロセスは **nscd** プロセスと通信できませんでした。その結果、**nscd** サービスが有効になっている場合、**samba-dcerpcd** サービスは正しく動作しませんでした。この更新により、SELinux ポリシーが更新され、**samba-dcerpcd** 用の新しいルールが追加されました。

Bugzilla:2121709

vlock が、制限のあるユーザーに対して適切に機能するようになりました。

以前は、SELinux ポリシーが原因で、制限のあるユーザーは **vlock** を使用できませんでした。その結果、**vlock** コマンドは制限されたユーザーに対しては適切に機能しませんでした。この更新により、SELinux ポリシーが更新され、制限のあるユーザー用の新しいルールが追加されました。

Bugzilla:2122838

制限のあるユーザーが、拒否の報告を受けることなくログインできるようになりました。

以前の SELinux ポリシーでは、GUI を使用して SELinux の制限のあるユーザーにログインするために必要なすべての権限が許可されていませんでした。その結果、AVC 拒否が監査され、**dbus** や **pulseaudio** などの一部のサービスが正しく動作しませんでした。この更新により、SELinux ポリシーが更新され、制限のあるユーザー用の新しいルールが追加されました。

Bugzilla:2124388

Insights-client に SELinux ポリシーで追加の権限が付与されるようになりました。

更新された **Insights-client** サービスには、以前のバージョンの **selinux-policy** パッケージには含まれていなかった追加の権限が必要です。その結果、**insights-client** の特定のコンポーネントが enforcing モードの SELinux で正しく動作せず、システムがアクセスベクターキャッシュ (AVC) エラーメッセージを報告していました。この更新により、不足している権限が SELinux ポリシーに追加されます。その結果、**insights-client** は AVC エラーを報告せずに正しく動作するようになります。

Bugzilla:2125008

SELinux ポリシーにより、ユーザー共有への smb アクセスが許可されます。

以前は、**samba-dcerpcd** プロセスは **smb** サービスから分離されていましたが、ユーザー共有にはアクセスできませんでした。その結果、**smb** クライアントがユーザー **smb** 共有上のファイルにアクセスできませんでした。この更新により、**samba_enable_home_dirs** ブール値が有効な場合に **samba-**

dcerpcd バイナリーのユーザーホームコンテンツを管理するルールが SELinux ポリシーに追加されます。その結果、**samba_enable_home_dirs** がオンの場合、**samba-dcerpcd** はユーザー共有にアクセスできるようになります。

Bugzilla:2143696

SELinux ポリシーにより、IPMItool の実行時に、制限のある管理者による ipmi デバイスへのアクセスが許可されます。

以前の SELinux ポリシーでは、IPMItool ユーティリティーの実行時に、制限のある管理者が **ipmi** デバイスの読み取りおよび書き込みを行うことはできませんでした。その結果、制限のある管理者が **ipmitool** を実行すると失敗しました。この更新により、SELinux ロール **sysadm_r** に割り当てられた管理者の許可ルールが **selinux-policy** に追加されます。その結果、制限のある管理者が **ipmitool** を実行したときに、ipmitool が正しく動作するようになります。

Bugzilla:2148561

SCAP セキュリティーガイドのルール file_permissions_sshd_private_key と STIG 設定 RHEL-08-010490 の整合性が確保されました。

以前は、ルール **file_permissions_sshd_private_key** の実装により、モード **0644** の **ssh_keys** グループによる SSH 秘密鍵の読み取りが許可されていましたが、DISA STIG バージョン RHEL-08-010490 では、SSH 秘密鍵のモードとして **0600** が要求されていました。その結果、設定 RHEL-08-010490 では、DISA の自動 STIG ベンチマークによる評価が失敗しました。

今回の更新のために、Red Hat は DISA と協力して、SSH 秘密鍵に求められるパーミッションを調整しました。現在、秘密鍵のモードには **0644** かそれ以上に厳しいパーミッションが求められます。その結果、ルール **file_permissions_sshd_private_key** と設定 RHEL-08-010490 の整合性が確保されました。

Bugzilla:2115343

sudo_require_reauthentication SCAP セキュリティーガイドルールが、sudoers に含まれる正しいスペースを受け入れます。

以前は、**xccdf_org.ssgproject.content_rule_sudo_require_reauthentication** ルールのチェックのバグにより、**/etc/sudoers** ファイルおよび **/etc/sudoers.d** ディレクトリー内の **timestamp_timeout** キーとその値の間に特定のスペースが必要でした。その結果、仕様に準拠した有効な構文でも、ルールが誤って失敗しました。今回の更新により、**xccdf_org.ssgproject.content_rule_sudo_require_reauthentication** のチェックが更新され、等号の前後の空白を受け入れるようになりました。その結果、ルールが、仕様に準拠した正しい **timestamp_timeout** の定義 (スペースの形式が次のいずれかであるもの) を受け入れるようになりました。

- **Defaults timestamp_timeout = 5**
- **Defaults timestamp_timeout= 5**
- **Defaults timestamp_timeout =5**
- **Defaults timestamp_timeout=5**

Bugzilla:2152208

古い Kerberos ルールが RHEL の新しいバージョンでは notapplicable に変更されました。

以前は、RHEL 8.8 以降のシステムで FIPS モードで DISA STIG プロファイルをスキャンしているときに、システムが規格に準拠しているはずであっても、一部の Kerberos 関連ルールが失敗していました。これは次のルールによって発生していました。

- **xccdf_org.ssgproject.content_rule_package_krb5-server_removed**
- **xccdf_org.ssgproject.content_rule_package_krb5-workstation_removed**
- **xccdf_org.ssgproject.content_rule_kerberos_disable_no_keytab**

この更新により、これらのルールは RHEL バージョン 8.8 以降には適用されなくなります。その結果、スキャンでこれらのルールに **notapplicable** という結果が正しく返されます。

Bugzilla:2099394

scap-security-guide STIG プロファイルで、/etc/audit/rules.d/11-loginuid.rules に特定のテキストが必要なくなりました。

以前は、RHEL 8 プロファイル **stig** および **stig_gui** で使用される SCAP ルール **audit_immutable_login_uids** は、ファイル **/etc/audit/rules.d/11-loginuid.rules** に正確なテキストが含まれている場合にのみ合格していました。ただし、これは STIG 要件 (RHEL-08-030122) を満たすために必要なわけではありません。この更新により、新しいルール **audit_rules_immutable_login_uids** が、RHEL 8 **stig** および **stig_gui** プロファイルの **audit_immutable_login_uids** に置き換わります。その結果、**audictl** または **augen-rules** の使用に応じて、**/etc/audit/rules.d** ディレクトリーまたは **/etc/audit/audit.rules** ファイル内の **.rules** 拡張子を持つ任意のファイルで、ルールを満たす **--loginuid-immutable** パラメーターを指定できるようになりました。

Bugzilla:2151553

scap-security-guide の CIS プロファイルのルールがより適切に割り当てられました。

以前は、一部のルールが特定の Center for Internet Security (CIS) プロファイル (**cis**、**cis_server_l1**、**cis_workstation_1**、および **cis_workstation_l2**) に誤って割り当てられていました。その結果、一部の CIS プロファイルに従ってスキャンすると、CIS ベンチマークからルールがスキップされたり、不要なルールがチェックされたりすることがありました。

次のルールが間違ったプロファイルに割り当てられました。

- ルール **kernel_module_udf_disabled**、**sudo_require_authentication** および **kernel_module_squashfs_disabled** が、CIS Server Level 1 および CIS Workstation Level 1 に誤って配置されていました。
- ルール **package_libselinux_installed**、**grub2_enable_selinux**、**selinux_policytype**、**selinux_confinement_of_daemons**、**rsyslog_nolisten**、**service_systemd-journald_enabled** が、CIS Server Level 1 および CIS Workstation Level 1 プロファイルから欠落していました。
- ルール **package_setroubleshoot_removed** および **package_mcstrans_removed** が CIS Server Level 1 プロファイルから欠落していました。

この更新により、割り当てが正しくなかったルールが正しい CIS プロファイルに割り当てられます。ただし、新しいルールが導入されたり、ルールが完全に削除されたりすることはありません。その結果、SCAP CIS プロファイルと元の CIS ベンチマークとの整合性が向上しました。

Bugzilla:2162803

Clevis が crypttab でコメントアウトされたデバイスを無視します。

以前は、Clevis が **crypttab** ファイル内のコメントアウトされたデバイスのロックを解除しようとしたため、デバイスが有効でない場合でも **clevis-luks-askpass** サービスが実行されてしまいました。これにより、不必要なサービスが実行され、トラブルシューティングが困難になりました。

この修正により、Clevis はコメントアウトされたデバイスを無視します。今後は、無効なデバイスがコメントアウトされている場合、Clevis はそのデバイスのロックを解除しようとせず、**clevis-luks-askpass.service** が適切に終了します。これにより、トラブルシューティングが容易になり、不必要なサービスの実行が削減されます。

Bugzilla:2159440

Clevis は pwmake に過剰なエントロピーを要求しなくなりました。

以前は、Clevis が **pwmake** を使用してデータを **LUKS** メタデータに保存するためのパスワードを作成するときに、**pwmake** パスワード生成ユーティリティーによって不要な警告が表示され、Clevis が使用するエントロピーが低下していました。この更新により、Clevis は **pwmake** に提供されるエントロピービットが 256 に制限され、不要な警告が排除され、正しい量のエントロピーが使用されます。

Bugzilla:2159736

logrotate はログローテーションで Rsyslog に誤って通知しなくなりました。

以前は、**logrotate** スクリプトで引数の順序が誤って設定されており、構文エラーが発生していました。これにより、**logrotate** がログローテーション中に Rsyslog に正しく信号を送信できなくなりました。

今回の更新により、**logrotate** の引数の順序が修正され、**POSIXLY_CORRECT** 環境変数が設定されている場合でも、**logrotate** はログローテーション後に Rsyslog に正しく通知するようになりました。

Bugzilla:2070496

imklog のバグにより Rsyslog がクラッシュしなくなりました。

以前は、**imklog** モジュールが有効になっており、無効なオブジェクトを使用した **free()** 呼び出しが使用中に解放された場合、Rsyslog でセグメンテーション違反が発生する可能性がありました。今回の更新により、解放されたオブジェクトが正しい場所で正しく割り当て解除されるようになりました。その結果、セグメンテーション違反が発生しなくなります。

Bugzilla:2157658

USBGuard で紛らわしい警告が表示されなくなりました。

以前は、親プロセスが最初の子プロセスよりも早く終了すると、USBGuard で競合状態が発生することがありました。その結果、**systemd** は、誤って識別された親 PID (PPID) を持つプロセスが存在すると報告しました。この更新により、親プロセスは最初の子プロセスが作業モードで終了するまで待機します。その結果、**systemd** は、そのような警告を報告しなくなります。

Bugzilla:2159409

usbguard サービスファイルで OOMScore が定義されていませんでした。

以前は、**usbguard** サービスファイルで **OOMScoreAdjust** オプションが定義されていませんでした。その結果、システムリソースが枯渇しそうになった場合、そのプロセスは、特権のないプロセスよりも先に強制終了の候補として特定されることがありました。この更新により、usbguard ユニットの OOM 強制終了プロセスを無効にするために、新しい **OOMScoreAdjust** 設定が **usbguard.service** ファイルに導入されました。

Bugzilla:2159411

USBGuard は、RuleFile が定義されていない場合でもルールを保存します。

以前は、USBGuard の **RuleFolder** 設定ディレクティブが設定されていても、**RuleFile** が設定されていない場合、ルールセットを変更できませんでした。今回の更新により、RuleFile が設定されていなくても、RuleFolder が設定されている場合は、ルールセットを変更できるようになりました。その結果、USBGuard の永続ポリシーを変更して、新しく追加されたルールを永続的に保存できます。

Bugzilla:2159413

8.6. ネットワーク

xdp-tools がバージョン 1.2.10 にリベースされました。

xdp-tools パッケージがアップストリームバージョン 1.2.10 にアップグレードし、以前のバージョンにバグ修正が数多く追加されました。

Bugzilla:2160069

HashSize と HashLimit が手動で設定されていない場合でも、conntrackd が適切に機能します。

以前は、**conntrackd** サービスは **HashSize** および **HashLimit** 設定変数のデフォルト値を設定していませんでした。したがって、これらの値を指定しないと、**conntrackd** が不安定になったり、機能が完全に停止したりすることがありました。この問題は、**conntrackd** が設定ファイルを解析する前に、設定リーダーが **HashSize** と **HashLimit** のデフォルト値を設定するようにすることで修正されました。その結果、値を指定しなくても **conntrackd** は正しく機能するようになりました。

Bugzilla:2126736

nm-cloud-setup サービスが、インターフェイスから手動で設定されたセカンダリー IP アドレスとルートを削除しなくなりました

クラウド環境から受け取った情報に基づいて、**nm-cloud-setup** サービスがネットワークインターフェイスを設定します。以前は、サービスによってルートとセカンダリー IP アドレスが削除されるのを避けるために、管理者が **nm-cloud-setup** を無効にしてインターフェイス上のルートとセカンダリー IP アドレスを手動で設定する必要がありました。この更新により、外部から追加されたアドレスとルートを保持するためのフラグが **Reapply()** 関数に追加されました。その結果、管理者は前述のシナリオで **nm-cloud-setup** サービスを無効にする必要がなくなりました。

Bugzilla:2132754

8.7. カーネル

kpatch-patch が、アイドル状態の分離された CPU を備えたシステム上で正しく動作します。

以前は、カーネル CPU 分離機能を備えたシステムに **kpatch-patch** CVE 軽減パッケージをインストールしようとすると、**kpatch-patch** RPM はインストールされましたが、CVE 軽減カーネルモジュールをロードできませんでした。この修正により、2 つの機能が共存し、CPU 分離が行われているときに **kpatch** CVE 修正を正常にデプロイできるようになりました。

Bugzilla:2134931

VMD の有効化が再び機能するようになりました。

以前は、ボリューム管理デバイス (VMD) が有効になっている場合、オペレーティングシステムが起動に失敗していました。この更新では、VMD が期待どおりに動作するために不可欠な多数のバグ修正が追加されました。

Bugzilla:2127028

8.8. ファイルシステムおよびストレージ

VDO ボリュームの起動中にソフトロックアップが発生せずにシステムが正常に動作します。

pv_mmu_ops 構造の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) のバグ修正により、カーネルバージョン **4.18.0-425.10.1.el8_7** を搭載した RHEL 8.7 システム (RHEL-8.7.0.2-BaseOS) で、Virtual Data Optimizer (VDO) ボリュームの起動中にソフトロックアップが発生し、ハングまたはカーネルパニックが発生していました。

この更新により、**kmod-kvdo** の現在のバージョンと kABI 互換性がなくなった新しいカーネルが利用可能になるたびに、**kmod-kvdo** パッケージが再構築されるようになりました。その結果、VDO ボリュームの起動中にシステムが正しく動作するようになりました。

Bugzilla:2119819

VDO ドライバーのバグによる、ジャーナルブロックを介したデバイスのフリーズが発生しなくなりました。

以前は、VDO ドライバーのバグにより、システムが一部のジャーナルブロックをメタデータ更新待ちとしてマークしていました。この問題は、VDO プールまたはその上の論理ボリュームのサイズを増加したとき、または LVM ツールで管理されている VDO デバイスで **pvmove** および **lvchange** 操作を使用したときに発生しました。このバグは、一部のジャーナルページが使用不可能な状態になる不完全なリセットと、書き込み可能なリカバリージャーナルのスロットの数に関する誤った概念が原因で発生していました。その結果、デバイスがフリーズしていました。

この問題は、Virtual Data Optimizer **kmod-kvdo-6.2.8.1-87.el8** のカーネルモジュールの最新バージョンで修正されました。現在は、すべての不完全なメタデータブロックが段階的にコードの各セクションに保存され、同時にメモリー内のデータ構造が更新され、必要に応じて再開時に状態がリセットされます。この修正により、この問題によるデバイスのフリーズが発生しなくなります。

Bugzilla:2109047

8.9. 高可用性およびクラスター

pcs では、変更すべきではないクラスターのプロパティーを変更できなくなりました。

以前は、**pcs** コマンドラインインターフェイスを使用して、変更すべきでないクラスタープロパティーや、変更が有効にならないクラスタープロパティーを変更できました。この修正により、**pcs** では、クラスタープロパティー **cluster-infrastructor**、**cluster-name**、**dc-version**、**have-watchdog**、および **last-lrm-refresh** を変更できなくなりました。

Bugzilla:2112263

pcs は、明示的に設定されていないクラスターのプロパティーを表示するようになりました。

以前は、特定のクラスタープロパティーの値を表示する **pcs** コマンドでは、CIB で明示的に設定されていない値がリストされませんでした。この修正により、クラスタープロパティーが設定されていない場合、**pcs** はプロパティーのデフォルト値を表示します。

Bugzilla:2112267

crm_mon を呼び出すクラスターリソースがシャットダウン時に正常に停止するようになりました。

以前は、Pacemaker のシャットダウン中に **crm_mon** ユーティリティーがゼロ以外の終了ステータスを

返していました。**ocf:heartbeat:pqsql** などのモニターアクションで **crm_mon** を呼び出したリソースエージェントが、クラスターのシャットダウン時に誤って失敗を返す可能性がありました。この修正により、クラスターがシャットダウン中であっても **crm_mon** は成功を返すようになりました。**crm_mon** を呼び出すリソースは、クラスターのシャットダウン時に正常に停止するようになりました。

Bugzilla:2133497

OCF リソースエージェントのメタデータアクションが、予期しないフェンシングを引き起こすことなく crm_node を呼び出せるようになりました。

RHEL 8.5 以降、OCF リソースエージェントのメタデータアクションはコントローラーをブロックし、**crm_node** クエリーはコントローラー要求を実行しました。その結果、エージェントのメタデータアクションが **crm_node** を呼び出した場合、アクションがタイムアウトになるまで 30 秒間コントローラーがブロックされました。これにより、他のアクションが失敗し、ノードが隔離される可能性があります。

この修正により、コントローラーはメタデータアクションを非同期で実行するようになりました。OCF リソースエージェントのメタデータアクションは問題なく **crm_node** を呼び出せるようになりました。

Bugzilla:2121852

単一のリソースと監視操作を有効にしても、リソースグループ内のすべてのリソースの監視操作は有効になりません。

以前は、リソースグループ内のすべてのリソースの管理を解除し、操作を監視した後、そのグループ内のリソースの 1 つをその監視操作とともに管理すると、リソースグループ内のすべてのリソースの監視操作が再び有効になりました。これにより、クラスターの予期しない動作が引き起こされる可能性があります。

この修正により、リソースを管理し、その監視操作を再度有効にすると、そのリソースに対してのみ監視操作が再度有効になり、リソースグループ内の他のリソースに対しては無効になります。

Bugzilla:1918527

Pacemaker は、リソースの順序が変更されたときにすぐにリソースの割り当てを再チェックするようになりました。

RHEL 8.7 以降、リソース定義を変更せずに CIB 内のリソースの順序が変更された場合、Pacemaker はリソース割り当てを再チェックしませんでした。設定の並べ替えによりリソースが移動する場合、次の自然な移行 (**cluster-recheck-interval-property** の値まで) まで移動は行われません。これにより、リソースの固定性がリソースに対して設定されていない場合に問題が発生する可能性があります。

この変更により、Pacemaker は、以前の Pacemaker リリースと同様に、CIB 内のリソースの順序が変更されたときにリソース割り当てを再チェックします。クラスターは、必要に応じてこれらの変更に即座に応答するようになりました。

Bugzilla:2122806

8.10. コンパイラーおよび開発ツール

すべてのアーキテクチャーで pip を使用して SciPy をインストールできます。

以前は、**openblas-devel** パッケージには OpenBLAS ライブラリーの pkg-config ファイルが含まれていませんでした。その結果、特定のシナリオでは、OpenBLAS でコンパイル中に **pkgconf** ユーティリティーを使用してコンパイラーとリンカーのフラグを決定することができませんでした。たとえば、こ

れにより、64 ビット IBM Z および IBM Power Systems のリトルエンディアンアーキテクチャー上で **pip install scipy** コマンドが失敗します。

この更新により、サポートされているすべてのアーキテクチャーの **openblas-devel** パッケージに **openblas.pc** ファイルが追加されます。その結果、**pip** パッケージインストーラーを使用して SciPy ライブラリーをインストールできます。

Bugzilla:2115722

go の関数でメモリーリークが発生しなくなりました。

以前は、**EVP_PKEY_sign_raw** 関数と **EVP_PKEY_verify_raw** 関数が、メモリーをクリーンアップするために free を呼び出しませんでした。その結果、メモリーがリークし、メモリーを回復できませんでした。この更新により、**EVP_PKEY_sign_raw** 関数と **EVP_PKEY_verify_raw** 関数が free を呼び出すようになり、メモリーリークが発生しなくなりました。

Bugzilla:2132767

golang が x509 FIPS モードで 4096 ビットキーをサポートするようになりました。

以前は、**golang** は x509 FIPS モードの 4096 ビットキーをサポートしていませんでした。その結果、ユーザーが 4096 ビットのキーを使用すると、プログラムがクラッシュしました。この更新により、**golang** は x509 FIPS モードで 4096 ビットキーをサポートするようになりました。

Bugzilla:2132694

SELinux が有効なときに、libff が実行可能メモリーをプローブできるようになりました。

デフォルトでは、SELinux が有効な場合、**libffi** は実行可能メモリーをプローブしません。その結果、SELinux が有効な場合、他のプロセスをすぐに実行せずに **libffi** クロージャーと **fork()** を使用するプログラムが予期せず終了します。今回の更新により、**libffi** が **/etc/sysconfig/libffi-force-shared-memory-check-first** ファイルを検索し、存在する場合は、SELinux が有効かどうかに関係なく、実行可能メモリーをプローブするようになります。その結果、**libffi** を使用するプログラムが、SELinux が有効な場合でも、クラッシュすることなく安全に **fork()** を実行できるようになります。

Bugzilla:2014228

golang の OpenSSL バインディングにビッグエンディアンのサポートを実装しました。

以前は、**golang** の **OpenSSL** バインディングはビッグエンディアンをサポートしていなかったため、**BigInt** 値の変換で潜在的な問題が発生していました。その結果、暗号化ルーチンがこの変換を実行できませんでした。この問題を解決するために、**golang** の **OpenSSL** バインディングにビッグエンディアンのサポートが実装されました。その結果、**BigInt** からの変換が成功し、テストも期待どおりに合格するようになりました。

Bugzilla:2132419

8.11. IDENTITY MANAGEMENT

クライアントシークレットを必要とする外部 IdP への認証が可能になりました。

以前は、SSSD はクライアントシークレットを外部 ID プロバイダー (IdP) に適切に渡しませんでした。その結果、クライアントシークレットを要求するように **ipa idp-add --secret** コマンドで以前に設定した外部 IdP に対する認証が失敗しました。この更新により、SSSD はクライアントシークレットを IdP に渡し、ユーザーは認証できるようになります。

Jira:RHELPLAN-148303

IdM は、Ansible を使用した sudo ルールのホストマスクの設定をサポートするようになりました。

以前は、**ipa sudorule-add-host** コマンドでは、**sudo** ルールで使用されるホストマスクを設定できましたが、このオプションは **ansible-freeipa** パッケージには存在していませんでした。この更新により、**ansible-freeipa hostmask** 変数を使用して、Identity Management (IdM) で定義された特定の **sudo** ルールが適用されるホストマスクのリストを定義できるようになりました。

その結果、Ansible を使用して IdM **sudo** ルールのホストマスクの設定を自動化できるようになりました。

Bugzilla:2127912

変更ログの圧縮をスケジュールした時間が正しく機能するようになりました。

以前は、変更ログの圧縮にカスタムのスケジュール時間を設定すると、サーバーは新しい設定を適用せず、変更ログの圧縮がピーク時に開始される可能性がありました。このリリースでは、サーバーは変更ログ圧縮のカスタム時間を正しく適用するようになりました。

Bugzilla:2130276

IdM クライアントは、信頼できる AD ユーザーの名前に大文字と小文字が混在している場合でも、当該 AD ユーザーの情報を適切に取得する

以前は、ユーザーの検索または認証を試行した際に、その信頼できる Active Directory (AD) ユーザーの名前に大文字と小文字が混在しており、かつ IdM でオーバーライドが設定されていた場合、エラーが返され、ユーザーは IdM リソースにアクセスできませんでした。

RHBA-2023:4359 のリリースにより、大文字と小文字を区別する比較は、大文字と小文字を区別しない比較に置き換えられました。その結果、IdM クライアントは、ユーザー名に大文字と小文字が混在しており、IdM でオーバーライドが設定されている場合でも、AD の信頼済みドメインのユーザーを検索できるようになりました。

Jira:SSSD-6096

8.12. グラフィックインフラストラクチャー

Matrox G200e が VGA ディスプレイで正しく動作するようになりました。

以前は、次のシステム設定を使用している場合、ディスプレイにグラフィカル出力が表示されないことがありました。

- Matrox G200e GPU
- VGA コントローラーで接続されたディスプレイ

したがって、この設定で RHEL を使用またはインストールできませんでした。

このリリースでは、この問題は修正されています。そのため、期待どおりに RHEL が起動し、グラフィック出力が表示されます。

Bugzilla:2130159

8.13. WEB コンソール

Web コンソールの NBDE バインディング手順が、ルートファイルシステムを持つボリュームグループで機能するようになる

RHEL 8.8.0 では、ユーザーがルートファイルシステムに Tang キーを追加したかどうかを判断するコードのバグが原因で、LUKS コンテナー上にファイルシステムがまったくない場合に、Web コンソールのバインディングプロセスがクラッシュしていました。**Verify key** ダイアログの **Trust key** ボタンをクリックした後、Web コンソールにエラーメッセージ **TypeError: Qe(...) is undefined** が表示されたため、説明されているシナリオのコマンドラインインターフェイスで必要な手順をすべて実行する必要がありました。

RHBA-2023:3829 アドバイザリーのリリースにより、Web コンソールはルートファイルシステムへの Tang キーの追加を正しく処理できるようになりました。その結果、Web コンソールは、さまざまなシナリオで Network-Bound Disk Encryption (NBDE) を使用した LUKS 暗号化ボリュームの自動ロック解除に必要なバインド手順をすべて完了します。

Bugzilla:2212371

8.14. RED HAT ENTERPRISE LINUX システムロール

nbde_client システムロールは、clevis-luks-askpass のさまざまな名前を正しく処理するようになりました。

nbde_client システムロールは、**clevis-luks-askpass systemd** ユニットの名前が異なるシステムを処理できるように更新されました。このロールは、マネージドノード上のさまざまな名前の **clevis-luks-askpass** で正しく動作するようになりました。これには、ブートプロセスの後半でマウントされる LUKS 暗号化ボリュームのロックも解除する必要があります。

Bugzilla:2126960

ha_cluster システムロールログに、暗号化されていないパスワードとシークレットが表示されなくなりました。

ha_cluster システムロールは、パスワードまたはその他の秘密のパラメーターを受け入れます。以前は、一部のタスクは入力と出力をログに記録していました。その結果、ロールログには暗号化されていないパスワードやその他の秘密が含まれる可能性があります。

この更新により、タスクは Ansible **no_log: true** ディレクティブを使用するように変更され、タスクの出力はロールログに表示されなくなりました。**ha_cluster** システムロールログには、パスワードやその他の秘密情報が含まれなくなりました。この更新によりセキュアな情報は保護されますが、ロールログで提供される情報は設定のデバッグ時に使用できる情報が少なくなります。

Bugzilla:2127497

SBD を使用し、ブート時に起動しないように ha_cluster システムロールで設定されたクラスターが正しく動作するようになりました。

以前は、ユーザーが **ha_cluster** システムロールを使用して SBD を使用し、起動時に起動しないようにクラスターを設定した場合、SBD サービスは無効になり、SBD は起動しませんでした。この修正により、クラスターが起動時に開始するように設定されているかどうかに関係なく、クラスターが SBD を使用するように設定されている場合、SBD サービスは常に有効になります。

Bugzilla:2153081

ha_cluster システムロールを使用した stonith-watchdog-timeout プロパティーの設定が、停止したクラスターでも機能するようになりました。

以前は、停止したクラスターで **ha_cluster** システムロールを使用して **stonith-watchdog-timeout** プロパティーを設定すると、プロパティーが以前の値に戻り、ロールが失敗していました。この修正により、**ha_cluster** システムロールを使用した **stonith-watchdog-timeout** プロパティーの設定が正しく機能するようになりました。

Bugzilla:2167941

rhel-system-roles SSSD 設定を修正するための暗黙的ファイルプロバイダーの有効化。

SSSD 暗黙的ファイルプロバイダーが無効になっているため、**rhel-system-roles** モジュールによって無効な System Security Services Daemon (SSSD) 設定が作成されていました。この更新により、ファイルプロバイダーが無条件で有効になり、その結果、**rhel-system-roles** によって作成された SSSD 設定が期待どおりに機能するようになりました。

Bugzilla:2153080

networking RHEL システムロールで initscripts を使用する場合、ネットワークトラフィックは目的のネットワークインターフェイス経由で送信されるようになりました。

以前は、**initscripts** プロバイダーを使用する場合、ネットワーク接続のルーティング設定で、トラフィックが通過する出力デバイスが指定されませんでした。その結果、カーネルはユーザーが意図したものとは異なる出力デバイスを使用する可能性があります。現在、接続用の Playbook でネットワークインターフェイス名が指定されている場合、その名前がルート設定ファイルの出力デバイスとして使用されます。これにより、デバイス上でプロファイルをアクティブ化するときにルート内の出力デバイスを設定する NetworkManager と動作が調整されます。その結果、ユーザーはトラフィックが意図したネットワークインターフェイスを介して確実に送信されるようになります。

Bugzilla:2168733

nbde_client_clevis ロールはユーザーにトレースバックを報告しなくなりました。

以前は、**nbde_client_clevis** ロールが例外で失敗することがあり、トレースバックが発生し、**encryption_password** フィールドなどの機密データがユーザーに報告されていました。今回の更新により、ロールは機密データを報告しなくなり、適切なエラーメッセージのみが報告されるようになりました。

Bugzilla:2162782

8.15. 仮想化

ネストされた VM 上のシステム時刻が確実に動作するようになりました。

以前は、ネストされた仮想マシン (VM) 上のシステム時刻がレベル 0 およびレベル 1 のホストから非同期になる場合がありました。これにより、ネストされた VM が応答しなくなったり、予期せず終了したりすることがありました。

この更新により、KVM ホストカーネルコードの時刻処理コードが修正され、上記のエラーの発生が防止されました。

Bugzilla:2151854

仮想マシンのネットワークトラフィックのパフォーマンスが低下しなくなりました。

以前は、RHEL 仮想マシンは、高レベルのネットワークトラフィックを処理する際のパフォーマンスが低下していました。基礎となるコードが修正され、ネットワークトラフィックのパフォーマンスには影響がなくなりました。

Bugzilla:2069047

memfd を使用する仮想マシンは期待どおりに実行されます

以前は、**memfd** を使用して hugepage でメモリーをバックアップする 64 ビット IBM Z プロセッサーアーキテクチャーで実行されている仮想マシン (VM) は実行できませんでした。今回の更新により、こ

の問題は修正され、**memfd** を使用する仮想マシンを 64 ビット IBM Z プロセッサーアーキテクチャー上で定義できるようになりました。その結果、**memfd** を使用して hugepage でメモリーをバックアップする仮想マシンを実行できるようになりました。

Bugzilla:2117149

仮想マシンのシステム時刻がホストと正しく同期するようになりました。

以前は、KVM モジュールは、意図したよりも少ない頻度でリアルタイムクロック (RTC) 同期を実行していました。その結果、RHEL 8 でホストされている仮想マシンのシステム時刻が、ホスト上のシステム時刻を正しく反映しない場合がありました。この更新により、KVM の RTC スケジューリングが修正され、前述の問題の発生が防止されます。

Bugzilla:2135417

第9章 テクノロジープレビュー

ここでは、Red Hat Enterprise Linux 8.8 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に対する Red Hat のサポート範囲の詳細は、テクノロジープレビューのサポート範囲 を参照してください。

9.1. インフラストラクチャーサービス

TuneD 用のソケット API がテクノロジープレビューとして利用可能になる

Unix ドメインソケットを通じて TuneD を制御するためのソケット 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。ソケット API は D-Bus API と 1 対 1 でマッピングされ、D-Bus が利用できない場合に代替通信方法を提供します。ソケット API を使用すると、TuneD デーモンを制御してパフォーマンスを最適化したり、さまざまなチューニングパラメーターの値を変更したりできます。ソケット API はデフォルトでは無効になっていますが、**tuned-main.conf** ファイルで有効にできます。

Bugzilla:2113900

9.2. ネットワーク

AF_XDP がテクノロジープレビューとして利用可能に

AF_XDP (**Address Family eXpress Data Path**) ソケットは、高性能パケット処理用に設計されています。さらに処理するために、**XDP** を取り入れ、プログラムにより選択されたパケットの効率的なリダイレクトをユーザー空間アプリケーションに付与します。

Bugzilla:1633143

テクノロジープレビューとして利用できる XDP 機能

Red Hat は、以下の eXpress Data Path (XDP) 機能をサポート対象外のテクノロジープレビューとして提供します。

- AMD および Intel 64 ビット以外のアーキテクチャーで XDP プログラムを読み込む。**libxdp** ライブラリーは、AMD および Intel 64 ビット以外のアーキテクチャーでは使用できません。
- XDP ハードウェアオフロード。

Bugzilla:1889737

TC のマルチプロトコルラベルスイッチがテクノロジープレビューとして利用可能に

Multi-protocol Label Switching (MPLS) は、エンタープライズネットワーク全体でトラフィックフローをルーティングするカーネル内データ転送メカニズムです。MPLS ネットワークでは、パケットを受信するルーターは、パケットに割り当てられたラベルに基づいて、パケットの追加のルートを決定します。ラベルを使用すると、MPLS ネットワークは特定の特性を持つパケットを処理する機能があります。たとえば、特定ポートから受信したパケットの管理や、特定のタイプのトラフィックを一貫した方法で伝送する **tc filters** を追加できます。

パケットがエンタープライズネットワークに入ると、MPLS ルーターは、パケット上で複数の操作を実行します。ラベルの追加には **push**、**swap** (ラベルの更新)、ラベルの削除の **pop** などが含まれます。MPLS では、RHEL の 1 つまたは複数のラベルに基づいて、アクションをローカルに定義できます。

ルーターを設定し、トラフィック制御 (**tc**) フィルターを設定して、**label**、**traffic class**、**bottom of stack**、**time to live** などの MPLS ラベルスタックエントリー (**lse**) 要素に基づいて、パケットに対して適切なアクションを実行するように設定することができます。

たとえば、次のコマンドは、フィルターを **enp0s1** ネットワークインターフェイスに追加して、最初のラベル **12323** と 2 番目のラベル **45832** を持つ着信パケットと一致させます。一致するパケットでは、以下のアクションが実行されます。

- 最初の MPLS TTL はデクリメントされます (TTL が 0 に達するとパケットがドロップされます)。
- 最初の MPLS ラベルが **549386** に変更
- 作成されるパケットは **enp0s2** 経由で送信されます。宛先 MAC アドレス **00:00:5E:00:53:01**、およびソース MAC アドレス **00:00:5E:00:53:02**。

```
# tc filter add dev enp0s1 ingress protocol mpls_uc flower mpls lse depth 1 label 12323 lse
depth 2 label 45832 \
action mpls dec_ttl pipe \
action mpls modify label 549386 pipe \
action pedit ex munge eth dst set 00:00:5E:00:53:01 pipe \
action pedit ex munge eth src set 00:00:5E:00:53:02 pipe \
action mirred egress redirect dev enp0s2
```

Bugzilla:1814836、Bugzilla:1856415

act_mpls モジュール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。

act_mpls モジュールが、テクノロジープレビューとして **kernel-modules-extra** rpm で利用可能になりました。モジュールを使用すると、トラフィック制御 (TC) フィルターを使用した Multiprotocol Label Switching (MPLS) アクション (TC フィルターを使用した MPLS ラベルスタックエントリーの push や pop など) の適用が可能になります。また、このモジュールでは、Label、Traffic Class、Botem of Stack、および Time to Live フィールドを独立して設定できます。

Bugzilla:1839311

systemd-resolved サービス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。

systemd-resolved サービスは、ローカルアプリケーションに名前解決を提供します。このサービスは、DNS スタブリゾルバー、LLMNR (Link-Local Multicast Name Resolution)、およびマルチキャスト DNS リゾルバーとレスポンダーのキャッシュと検証を実装します。

systemd パッケージが **systemd-resolved** を提供している場合でも、このサービスはサポートされていないテクノロジープレビューであることに注意してください。

Bugzilla:1906489

KTLS がテクノロジープレビューとして利用可能になる

RHEL は、テクノロジープレビューとして KTLS (Kernel Transport Layer Security) を提供します。KTLS は、AES-GCM 暗号化のカーネルで対称暗号化アルゴリズムまたは複号アルゴリズムを使用して TLS レコードを処理します。KTLS には、この機能を提供するネットワークインターフェイスコントローラー (NIC) に TLS レコード暗号化をオフロードするインターフェイスも含まれています。

Bugzilla:1570255

9.3. カーネル

テクノロジープレビューとして利用できる Soft-RoCE

Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) は、RDMA over Ethernet を実装するネットワークプロトコルです。Soft-RoCE は、RoCE v1 および RoCE v2 の 2 つのプロトコルバージョンを維持する RoCE のソフトウェア実装です。Soft-RoCE ドライバーの **rdma_rxe** は、RHEL 8 ではサポートされていないテクノロジープレビューとして利用できます。

Bugzilla:1605216

eBPF 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。

eBPF (extended Berkeley Packet Filter)は、限られた一連の関数にアクセスできる制限付きサンドボックス環境において、カーネル領域でのコード実行を可能にするカーネル内の仮想マシンです。

仮想マシンには、さまざまな種類のマップの作成を可能にする、新しいシステムコール **bpf()** が含まれ、特別なアセンブリーのコードでプログラムをロードすることも可能です。そして、このコードはカーネルにロードされ、実行時コンパイラーでネイティブマシンコードに変換されます。**bpf()** は、root ユーザーなど、**CAP_SYS_ADMIN** が付与されているユーザーのみが利用できます。詳細は、man ページの **bpf(2)** を参照してください。

ロードしたプログラムは、データを受信して処理するために、さまざまなポイント (ソケット、トレースポイント、パケット受信) に割り当てることができます。

eBPF 仮想マシンを使用する Red Hat には、多くのコンポーネントが同梱されています。各コンポーネントは異なる開発フェーズにあります。特定のコンポーネントがサポート対象と示されていない限り、すべてのコンポーネントはテクノロジープレビューとして提供されます。

現在、以下の主要 **eBPF** コンポーネントが、テクノロジープレビューとして利用可能です。

- **AF_XDP**。これは、**eXpress Data Path (XDP)**パスを、パケット処理のパフォーマンスを優先するアプリケーションのユーザー空間に接続するためのソケットです。

Bugzilla:1559616

kexec fast reboot 機能は、テクノロジープレビューとしてご利用いただけます。

kexec fast reboot 機能は、引き続きテクノロジープレビューとして利用できます。**kexec** 高速リブートでは、最初に基本入出力システム (BIOS) やファームウェアを経由せずに 2 番目のカーネルを直接ブートできるため、ブートプロセスが大幅に高速化されます。この機能を使用するには、以下を実行します。

1. **kexec** カーネルを手動で読み込みます。
2. 変更を有効にするために再起動します。

kexec 高速リブート機能は、RHEL 9 以降のリリースではサポート範囲が限定されていることに注意してください。

Bugzilla:1769727

カーネルの Intel データストリーミングタブレットドライバーがテクノロジープレビューとして利用可能になる

カーネルの Intel データストリーミングアクセラレータードライバー (IDXD) は、現在テクノロジープレビューとして利用できます。これは Intel CPU 統合アクセラレーターで、プロセスアドレス空間 ID (pasid) の送信および共有仮想メモリー (SVM) の共有ワークキューが含まれますます。

Bugzilla:1837187

accel-config パッケージ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。

accel-config パッケージが、テクノロジープレビューとして、Intel **EM64T** および **AMD64** アーキテクチャーで利用可能になりました。このパッケージは、Linux カーネルでデータストリーミング (DSA) サブシステムを制御し、設定するのに役立ちます。また、**sysfs** (pseudo-filesystem) を介してデバイスを設定し、設定を **json** 形式で保存および読み込みます。

Bugzilla:1843266

SGX がテクノロジープレビューとして利用可能

Software Guard Extensions(SGX) は、ソフトウェアコードおよび公開および修正からのデータを保護する Intel® テクノロジーです。RHEL カーネルは、SGX v1 および v1.5 の機能を部分的に提供します。バージョン 1 では、**Flexible Launch Control** メカニズムを使用するプラットフォームで SGX テクノロジーを使用できるようになります。バージョン 2 では、**Enclave Dynamic Memory Management** (EDMM) が追加されています。主な変更には以下のものがあります。

- 初期化されたエンクレーブに属する通常のエンクレーブページの EPCM 権限を変更します。
- 初期化されたエンクレーブへの通常のエンクレーブページの動的追加。
- より多くのスレッドを収容できるように初期化されたエンクレーブを拡張します。
- 初期化されたエンクレーブから通常のページと TCS ページを削除します。

Bugzilla:1660337

9.4. ファイルシステムおよびストレージ

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 で利用可能に

Red Hat Enterprise Linux 8 では、ファイルシステムの DAX がテクノロジープレビューとして利用できます。DAX は、永続メモリーをそのアドレス空間に直接マッピングする手段をアプリケーションに提供します。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 機能を提供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。これにより、dax をマウントしたファイルシステムのファイルの **mmap** が、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。

Bugzilla:1627455

OverlayFS

OverlayFS は、ユニオンファイルシステムのタイプです。これにより、あるファイルシステムを別のファイルシステムに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ーや 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。

OverlayFS は、ほとんどの状況で引き続きテクノロジープレビューになります。したがって、カーネルは、この技術がアクティブになると警告を記録します。

以下の制限下で、対応しているコンテナーエンジン (**podman**、**cri-o**、または **buildah**) とともに使用すると、OverlayFS に完全対応となります。

- OverlayFS は、コンテナーエンジングラフドライバーとしての使用、または圧縮された **kdump** initramfs などのその他の特殊なユースケースとしての使用のみサポートされています。その使用は主にコンテナー COW コンテンツでサポートされており、永続ストレージではサポートされていません。非 OverlayFS ボリュームに永続ストレージを配置する必要があります。デフォ

ルトのコンテナーエンジン設定のみを使用できます。つまり、あるレベルのオーバーレイ、1つの下位ディレクトリー、および下位と上位の両方のレベルが同じファイルシステムにあります。

- 下層ファイルシステムとして使用に対応しているのは現在 XFS のみです。

また、OverlayFS の使用には、以下のルールと制限が適用されます。

- OverlayFS カーネル ABI とユーザー空間の動作については安定しているとみなされていないため、今後の更新で変更が加えられる可能性があります。
- OverlayFS は、POSIX 標準の制限セットを提供します。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。以下のケースは、POSIX に準拠していません。
  - **O_RDONLY** で開いているファイルが少ない場合は、ファイルの読み取り時に **st_atime** の更新を受け取りません。
  - **O_RDONLY** で開いてから、**MAP_SHARED** でマッピングした下位ファイルは、後続の変更と一貫性がありません。
  - 完全に準拠した **st_ino** 値または **d_ino** 値は、RHEL 8 ではデフォルトで有効になっていませんが、モジュールオプションまたはマウントオプションを使用して、この値の完全な POSIX コンプライアンスを有効にできます。
    一貫した inode 番号を付けるには、**xino=on** マウントオプションを使用します。

    redirect_dir=on オプションおよび **index=on** オプションを使用して、POSIX コンプライアンスを向上させることもできます。この 2 つのオプションにより、上位レイヤーの形式は、このオプションなしでオーバーレイと互換性がありません。つまり、**redirect_dir=on** または **index=on** でオーバーレイを作成し、オーバーレイをアンマウントしてから、このオプションなしでオーバーレイをマウントすると、予期しない結果またはエラーが発生することがあります。
- 既存の XFS 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、次の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。

```
# xfs_info /mount-point | grep ftype
```

- SELinux セキュリティーラベルは、OverlayFS で対応するすべてのコンテナーエンジンでデフォルトで有効になっています。
- このリリースの既知の問題は、OverlayFS に関連しています。詳細は **Linux カーネルドキュメント** の Non-standard behavior を参照してください。

OverlayFS の詳細は、Linux カーネルのドキュメント を参照してください。

Bugzilla:1690207

Straits 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。

Stratis は、追加機能を備えたストレージプール上に管理されたファイルシステムを提供する、新しいローカルストレージマネージャーです。これはテクノロジープレビューとして提供されます。

Stratis を使用すると、次のストレージタスクを実行できます。

- スナップショットおよびシンプロビジョニングを管理する

- 必要に応じてファイルシステムのサイズを自動的に大きくする
- ファイルシステムを維持する

Stratis ストレージを管理するには、バックグランドサービス **stratisd** と通信する **stratis** ユーティリティーを使用します。詳細は、Stratis ファイルシステムのセットアップ ドキュメントを参照してください。

RHEL 8.5 は Stratis をバージョン 2.42 に更新した。詳細は、Stratis 2.4.2 リリースノート を参照してください。

Jira:RHELPLAN-1212

NVMe/TCP ホストはテクノロジープレビューとして利用可能です

TCP/IP ネットワーク (NVMe/TCP) および対応する **nvme-tcp.ko** カーネルモジュールへのアクセスおよび共有がテクノロジープレビューとして追加されました。ホストとしての NVMe/TCP の使用は、**nvme-cli** パッケージによって提供されるツールを使用して管理できます。NVMe/TCP ホストテクノロジープレビュー機能はテスト目的としてのみ同梱されており、現時点ではフルサポートの予定はありません。

Bugzilla:1696451

テクノロジープレビューとして、IdM ドメインメンバーで Samba サーバーを設定できるようになりました。

今回の更新で、Identity Management (IdM) ドメインメンバーに Samba サーバーを設定できるようになりました。同じ名前パッケージに含まれる新しい **ipa-client-samba** ユーティリティーは、Samba 固有の Kerberos サービスプリンシパルを IdM に追加し、IdM クライアントを準備します。たとえば、ユーティリティーは、**sss** ID マッピングバックエンドの ID マッピング設定で **/etc/samba/smb.conf** を作成します。その結果、管理者が IdM ドメインメンバーに Samba を設定できるようになりました。

IdM 信頼コントローラーが Global Catalog Service をサポートしないため、AD が登録した Windows ホストは Windows で IdM ユーザーおよびグループを見つけることができません。さらに、IdM 信頼コントローラーは、Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) プロトコルを使用する IdM グループの解決をサポートしません。これにより、AD ユーザーは、IdM クライアントから Samba の共有およびプリンターにしかアクセスできません。

詳細は、IdM ドメインメンバーでの Samba の設定 を参照してください。

Jira:RHELPLAN-13195

9.5. 高可用性およびクラスター

Pacemaker の podman バンドル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。

Pacemaker コンテナーバンドルは、テクノロジープレビューとして利用できるコンテナーバンドル機能を使用して、Podman で動作するようになりました。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が、例外が 1 つあります。Red Hat は、Red Hat OpenStack 用の Pacemaker バンドルの使用に完全対応します。

Bugzilla:1619620

テクノロジープレビューとして利用可能な corosync-qdevice のヒューリスティック

ヒューリスティックは、起動、クラスターメンバーシップの変更、**corosync-qnetd** への正常な接続でローカルに実行され、任意で定期的に実行される一連のコマンドです。すべてのコマンドが時間どおり

に正常に終了すると (返されるエラーコードがゼロである場合)、ヒューリスティックは渡されますが、それ以外の場合は失敗します。ヒューリスティックの結果は **corosync-qnetd** に送信され、クオーラムとなるべきパーティションを判断するための計算に使用されます。

Bugzilla:1784200

新しい fence-agents-heuristics-ping フェンスエージェント

Pacemaker は、テクノロジープレビューとして **fence_heuristics_ping** エージェントを提供するようになりました。このエージェントの目的は、実際にはフェンシングを行わず、フェンシングレベルの動作を新しい方法で活用する実験的なフェンスエージェントのクラスを開くことです。

ヒューリスティックエージェントが、実際のフェンシングを行うフェンスエージェントと同じフェンシングレベルで設定されいて、そのエージェントよりも順番が前に設定されているとします。その場合、フェンシグを行うエージェントで **off** 操作を行う前に、ヒューリスティックエージェントで、この操作を行います。このヒューリスティックエージェントが **off** アクションに対して失敗する場合、このフェンシングレベルが成功しないのはすでに明らかです。そのため、Pacemaker フェンシングは、フェンシングを行うエージェントで **off** 操作を行うステップをスキップします。ヒューリスティックエージェントはこの動作を利用して、特定の条件下で、実際のフェンシングを行うエージェントがフェンシングできないようにできます。

サービスを適切に引き継ぐことができないことを事前に把握できる場合は、ノードがピアをフェンシングする意味がないのであれば、ユーザーは特に 2 ノードクラスターでこのエージェントを使用できます。たとえば、ネットワークアップリンクに到達してサービスがクライアントに到達できない場合は、ノードがサービスを引き継ぐ意味はありません。これは、ルーターへの ping が検出できる状況が考えられます。

Bugzilla:1775847

9.6. IDENTITY MANAGEMENT

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。

以前では、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。これらの機能拡張により、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 Identity Management API を使用して IdM サーバーに接続する (テクノロジープレビュー) を参照してください。

Bugzilla:1664719

DNSSEC が IdM でテクノロジープレビューとして利用可能

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ーを強化する DNS に対する拡張セットである DNS Security Extensions (DNSSEC) を実装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 ゾーンを保護する場合は、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
- Secure Domain Name System (DNS) Deployment Guide
- DNSSEC Key Rollover Timing Considerations

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。これが、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。

Bugzilla:1664718

ACME がテクノロジープレビューとして利用可能

Automated Certificate Management Environment (ACME) サービスが、テクノロジープレビューとして Identity Management (IdM) で利用可能になりました。ACME は、自動化識別子の検証および証明書の発行に使用するプロトコルです。この目的は、証明書の有効期間を短縮し、証明書のライフサイクル管理での手動プロセスを回避することにより、セキュリティーを向上させることです。

RHEL では、ACME サービスは Red Hat Certificate System (RHCS) PKI ACME レスポンダーを使用します。RHCS ACME サブシステムは、IdM デプロイメントのすべての認証局 (CA) サーバーに自動的にデプロイされますが、管理者が有効にするまでリクエストに対応しません。RHCS は、ACME 証明書を発行する際に **acmeIPAServerCert** プロファイルを使用します。発行された証明書の有効期間は 90 日です。ACME サービスの有効化または無効化は、IdM デプロイメント全体に影響します。

重要

ACME は、すべてのサーバーが RHEL 8.4 以降を実行している IdM デプロイメントでのみ有効にすることが推奨されます。以前の RHEL バージョンには ACME サービスが含まれていないため、バージョンが混在するデプロイメントで問題が発生する可能性があります。たとえば、ACME のない CA サーバーは、異なる DNS サブジェクト代替名 (SAN) を使用しているため、クライアント接続が失敗する可能性があります。

警告

現在、RHCS は期限切れの証明書を削除しません。ACME 証明書は 90 日後に期限切れになるため、期限切れの証明書が蓄積され、パフォーマンスに影響を及ぼす可能性があります。

- IdM デプロイメント全体で ACME を有効にするには、**ipa-acme-manage enable** コマンドを使用します。

```
# ipa-acme-manage enable
The ipa-acme-manage command was successful
```

- IdM デプロイメント全体で ACME を無効にするには、**ipa-acme-manage disable** コマンドを使用します。

```
# ipa-acme-manage disable
The ipa-acme-manage command was successful
```

- ACME サービスがインストールされ、有効または無効であるかを確認するには、**ipa-acme-manage status** コマンドを使用します。

```
# ipa-acme-manage status
ACME is enabled
The ipa-acme-manage command was successful
```

Bugzilla:1628987

sssd-idp サブパッケージがテクノロジープレビューとして利用可能

SSSD の **sssd-idp** サブパッケージには、Identity Management (IdM) サーバーに対して OAuth2 認証を実行するクライアント側のコンポーネントである **oidc_child** プラグインおよび krb5 **idp** プラグインが含まれます。この機能は、RHEL 8.7 以降の IdM サーバーのみで使用できます。

Bugzilla:2065692

SSSD の内部 krb5 idp プラグインがテクノロジープレビューとして利用可能

SSSD krb5 **idp** プラグインを使用すると、OAuth2 プロトコルを使用して外部アイデンティティープロバイダー (IdP) に対して認証できます。この機能は、RHEL 8.7 以降の IdM サーバーのみで使用できます。

Bugzilla:2056483

RHEL IdM では、ユーザー認証をテクノロジープレビューとして外部 ID プロバイダーに委任できる

RHEL IdM のテクノロジープレビューとして、OAuth 2 デバイス認証フローをサポートする外部アイデンティティプロバイダー (IdP) にユーザーを関連付けられるようになりました。これらのユーザーが RHEL 8.7 以降で利用可能な SSSD バージョンで認証すると、外部 IdP で認証と認可を実行した後、Kerberos チケットを使用した RHEL IdMSingle Sign-On 機能を受け取ります。

主な変更には以下のものがあります。

- **ipa idp-*** コマンドによる外部 IdP への参照の追加、変更、および削除
- **ipa user-mod --user-auth-type=idp** コマンドを使用したユーザーの IdP 認証の有効化

追加情報は、外部 ID プロバイダーを使用した IdM への認証 を参照してください。

Bugzilla:2101770

9.7. デスクトップ

64 ビット ARM アーキテクチャーの GNOME 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。

GNOME デスクトップ環境は、テクノロジープレビューとして 64 ビット ARM アーキテクチャーで利用できます。

VNC を使用して 64 ビット ARM サーバーのデスクトップセッションに接続できるようになりました。その結果、グラフィカルアプリケーションを使用してサーバーを管理できます。

64 ビット ARM では、限定されたグラフィカルアプリケーションのセットを使用できます。以下に例を示します。

- Firefox Web ブラウザー
- Red Hat Subscription マネージャー (**subscription-manager-cockpit**)
- ファイアウォール設定 (**firewall-config**)
- ディスク使用状況アナライザー (**baobab**)

Firefox を使用して、サーバー上の Cockpit サービスに接続できます。

LibreOffice などの特定のアプリケーションは、コマンドラインインターフェイスのみを提供し、グラフィカルインターフェイスは無効になっています。

Jira:RHELPLAN-27394, Bugzilla:1667225, Bugzilla:1724302, Bugzilla:1667516

テクノロジープレビューとして利用可能な IBM Z アーキテクチャー用の GNOME

GNOME デスクトップ環境は、テクノロジープレビューとして IBM Z アーキテクチャーで利用できます。

VNC を使用して IBM Z サーバーのデスクトップセッションに接続できるようになりました。その結果、グラフィカルアプリケーションを使用してサーバーを管理できます。

IBM Z では、限定されたグラフィカルアプリケーションのセットを使用できます。たとえば、次のようになります。

- Firefox Web ブラウザー
- Red Hat Subscription マネージャー (**subscription-manager-cockpit**)
- ファイアウォール設定 (**firewall-config**)
- ディスク使用状況アナライザー (**baobab**)

Firefox を使用して、サーバー上の Cockpit サービスに接続できます。

LibreOffice などの特定のアプリケーションは、コマンドラインインターフェイスのみを提供し、グラフィカルインターフェイスは無効になっています。

Jira:RHELPLAN-27737

9.8. グラフィックインフラストラクチャー

64 ビット ARM アーキテクチャーで VNC リモートコンソールがテクノロジープレビューとして利用可能に

64 ビットの ARM アーキテクチャーでは、Virtual Network Computing (VNC) リモートコンソールがテクノロジープレビューとして利用できます。グラフィックススタックの残りの部分は、現在、64 ビット ARM アーキテクチャーでは検証されていません。

Bugzilla:1698565

Intel Arc A シリーズグラフィックスがテクノロジープレビューとして利用可能。

Alchemist または DG2 としても知られる Intel Arc A シリーズグラフィックス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。

Intel Arc A シリーズグラフィックスでハードウェアアクセラレーションを有効にするには、カーネルコマンドラインに次のオプションを追加します。

```
i915.force_probe=pci-id
```

このオプションでは、**pci-id** を次のいずれかに置き換えます。

- Intel GPU の PCI ID。
- * 文字は、すべてのアルファ品質のハードウェアで i915 ドライバーを有効にします。

Bugzilla:2041686

9.9. 仮想化

RHEL 8 Hyper-V 仮想マシンで KVM 仮想化が利用可能に

ネストされた KVM 仮想化は、テクノロジープレビューとして、Microsoft Hyper-V ハイパーバイザーで使用できるようになりました。これにより、Hyper-V ホストで実行している RHEL 8 ゲストシステムで仮想マシンを作成できます。

この機能は、現在 Intel および AMD システムでのみ有効です。また、ネストされた仮想化は、Hyper-V でデフォルトで有効になっていない場合があります。これを有効にするには、以下の Microsoft ドキュメントを参照してください。

https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization

Bugzilla:1519039

KVM 仮想マシンの AMD SEV および SEV-ES

テクノロジープレビューとして、RHEL 8 に、KVM ハイパーバイザーを使用する AMD EPYC ホストマシン用のセキュア暗号化仮想化 (SEV) 機能が同梱されます。仮想マシンで有効になっている場合は、SEV が仮想マシンのメモリーを暗号化して、ホストから仮想マシンへのアクセスを防ぎます。これにより、仮想マシンのセキュリティーが向上します。

さらに、強化された SEV (Encrypted State) バージョンの SEV (SEV-ES) もテクノロジープレビューとして提供されます。SEV-ES は、仮想マシンの実行が停止すると、すべての CPU レジスターの内容を暗号化します。これにより、ホストが仮想マシンの CPU レジスターを変更したり、そこから情報を読み取ったりできなくなります。

SEV および SEV-ES は、第 2 世代の AMD EPYC CPU (コードネーム Rome) 以降でのみ機能することに注意してください。また、RHEL 8 には SEV および SEV-ES の暗号化が含まれますが、SEV および SEV-ES のセキュリティー証明は含まれません。

Bugzilla:1501618, Bugzilla:1501607, Jira:RHELPLAN-7677

Intel vGPU

テクノロジープレビューとして、物理 Intel GPU デバイスを、**仲介デバイス** と呼ばれる複数の仮想デバイスに分割できるようになりました。この仲介デバイスは、仮想 GPU として複数の仮想マシンに割り当てることができます。これにより、この仮想マシンが、1 つの物理 Intel GPU のパフォーマンスを共有します。

選択した Intel GPU のみが vGPU 機能と互換性があることに注意してください。

さらに、Intel vGPU が操作する VNC コンソールを有効にすることもできます。これを有効にすると、ユーザーは仮想マシンの VNC コンソールに接続し、Intel vGPU がホストする仮想マシンのデスクトップを確認できます。ただし、これは現在 RHEL ゲストオペレーティングシステムでのみ動作します。

Bugzilla:1528684

入れ子仮想マシンの作成

入れ子 KVM 仮想化は、RHEL 8 で Intel、AMD64、IBM POWER および IBM Z システムホストで実行している KVM 仮想マシン用のテクノロジープレビューとして提供されます。この機能を使用すると、物理 RHEL 8 ホストで実行中の RHEL 7 または RHEL 8 仮想マシンがハイパーバイザーとして機能し、独自の仮想マシンをホストできます。

Jira:RHELPLAN-14047, Jira:RHELPLAN-24437

テクノロジープレビュー: 一部の Intel ネットワークアダプターが、Hyper-V の RHEL ゲストに SR-IOV を提供するようになりました

テクノロジープレビューとして、Hyper-V ハイパーバイザーで実行している Red Hat Enterprise Linux のゲストオペレーティングシステムは、**ixgbevf** および **ixgbevf** ドライバーがサポートする Intel ネットワークアダプターに、シングルルート I/O 仮想化 (SR-IOV) 機能を使用することができるようになりました。この機能は、以下の条件が満たされると有効になります。

- 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 からの VF (Virtual Function) が仮想マシンに割り当てられている

この機能は現在、Microsoft Windows Server 2016 以降で提供されています。

Bugzilla:1348508

RHEL ゲストのインテル TDX

テクノロジープレビューとして、Intel Trust Domain Extension (TDX) 機能が RHEL 8.8 ゲストオペレーティングシステムで使用できるようになりました。ホストシステムが TDX をサポートしている場合は、トラストドメイン (TD) と呼ばれる、ハードウェアから分離された RHEL 9 仮想マシン (VM) をデプロイできます。ただし、TDX は現在 **kdump** では機能せず、TDX を有効にすると VM 上で **kdump** が失敗することに注意してください。

Bugzilla:1836977

virtiofs を使用したホストと仮想マシン間でのファイルの共有

RHEL 8 では、テクノロジープレビューとして virtio ファイルシステム (**virtiofs**) が追加されました。**virtiofs** を使用すると、ホストシステムと仮想マシン (VM) との間で、ファイルを効率的に共有できます。

Bugzilla:1741615

9.10. クラウド環境の RHEL

RHEL Confidential VMs がテクノロジープレビューとして Azure で利用可能になりました

更新された RHEL カーネルを使用すると、Microsoft Azure で機密仮想マシン (VM) をテクノロジープレビューとして作成して実行できるようになりました。ただし、Azure での起動中に RHEL 機密 VM イメージを暗号化することはまだできません。

Jira:RHELPLAN-122316

9.11. コンテナー

Fulcio と Rekor を使用した sigstore 署名のクライアント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。

Fulcio および Rekor サーバーを使用すると、秘密キーを手動で管理する代わりに、OpenID Connect (OIDC) サーバー認証に基づく短期証明書を使用して署名を作成できるようになりました。Fulcio と Rekor を使用した sigstore 署名のクライアント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。この追加機能はクライアント側のサポートのみであり、Fulcio サーバーや Rekor サーバーは含まれません。

policy.json ファイルに **fulcio** セクションを追加します。コンテナーイメージに署名するには、**podman push --sign-by-sigstore=file.yml** または **skopeo copy --sign-by-sigstore=file.yml** コマンドを使用します。ここで、**file.yml** は sigstore 署名パラメーターファイルです。

署名を検証するには、**policy.json** ファイルに **fulcio** セクションと **rekorPublicKeyPath** または **rekorPublicKeyData** フィールドを追加します。詳細は、**containers-policy.json** の man ページを参照してください。

Jira:RHELPLAN-136610

Podman の Quadlet 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。

Podman v4.4 以降では、Quadlet を使用して、コンテナーの説明から **systemd** サービスファイルをテクノロジープレビューとして自動的に生成できます。コンテナーの説明は **systemd** ユニットファイル形式です。この説明では、関連するコンテナーの詳細に焦点を当てており、**systemd** でコンテナーを実行する際の技術的な複雑さは隠しています。Quadlet は、**systemd** ユニットファイルよりも作成と保守が簡単です。

詳細については、アップストリームのドキュメント と Make systemd better for Podman with Quadlet を参照してください。

Jira:RHELPLAN-148394

podman-machine コマンドはサポート対象外です。

仮想マシンを管理するための **podman-machine** コマンドは、テクノロジープレビューとしてのみ利用可能です。代わりに、コマンドラインから直接 Podman を実行してください。

Jira:RHELDOCS-16861

第10章 非推奨になった機能

ここでは、Red Hat Enterprise Linux 8 で **非推奨** となった機能の概要を説明します。

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版のリリースノートを参照してください。

非推奨機能のサポートステータスは、Red Hat Enterprise Linux 8 では変更されません。サポート期間の詳細は、Red Hat Enterprise Linux ライフサイクル および Red Hat Enterprise Linux Application Streams ライフサイクル 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ーの更新は、セキュリティーと重大な修正のみに行われます。Red Hat では、このようなハードウェアの早期交換を推奨します。

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。

RHEL 7 で使用され、RHEL 8 で **削除された** 機能の詳細は RHEL 8 の導入における検討事項 を参照してください。

10.1. インストーラーおよびイメージの作成

複数のキックスタートコマンドおよびオプションが非推奨になりました。

RHEL 8 キックスタートファイルで以下のコマンドとオプションを使用すると、ログに警告が表示されます。

- **auth** または **authconfig**
- **device**
- **deviceprobe**
- **dmraid**
- **install**
- **lilo**
- **lilocheck**
- **mouse**
- **multipath**
- **bootloader --upgrade**
- **ignoredisk --interactive**
- **partition --active**
- **reboot --kexec**

特定のオプションだけがリスト表示されている場合は、基本コマンドおよびその他のオプションは引き続き利用でき、非推奨ではありません。

キックスタートの詳細および変更点は、**RHEL 8 の導入における検討事項**の キックスタートの変更 を参照してください。

Bugzilla:1642765

キックスタートコマンド ignoredisk の --interactive オプションが非推奨になりました。

Red Hat Enterprise Linux の将来のリリースで **--interactive オプション** を使用すると、致命的なインストールエラーが発生します。このオプションを削除するには、キックスタートファイルを変更することが推奨されます。

Bugzilla:1637872

キックスタートの autostep コマンドが非推奨に

autostep コマンドが非推奨になりました。このコマンドに関連するセクションは、RHEL 8 のドキュメント から削除されました。

Bugzilla:1904251

10.2. サブスクリプションの管理

subscription-manager コマンドの --token オプションは非推奨になりました。

subscription-manager register コマンドの **--token=<TOKEN>** オプションは、システムを Red Hat に登録するのに役立つ認証方法です。このオプションは、エンタイトルメントサーバーが提供する機能に応じて異なります。デフォルトのエンタイトルメントサーバー **subscription.rhsm.redhat.com** は、この機能をオフにする予定です。その結果、**subscription-manager register --token=<TOKEN>** を使用しようとすると、次のエラーメッセージが表示されて失敗する可能性があります。

> Token authentication not supported by the entitlement server

subscription-manager register コマンドのペアのオプション **--username** / **--password** および **--org** / **--activationkey** を含めるなど、他の認証方法を使用してシステムの登録を続けることができます。

Bugzilla:2170082

10.3. ソフトウェア管理

rpmbuild --sign が非推奨になりました。

rpmbuild --sign コマンドは、RHEL 8.1 以降非推奨になりました。Red Hat Enterprise Linux の今後のリリースでこのコマンドを実行すると、エラーが発生します。代わりに **rpmsign** コマンドを使用することが推奨されます。

Bugzilla:1688849

10.4. シェルおよびコマンドラインツール

OpenEXR コンポーネントが非推奨になりました。

OpenEXR コンポーネントが非推奨になりました。そのため、**EXR** イメージ形式のサポートは **imagecodecs** モジュールから削除されました。

Bugzilla:1886310

dump からの dump ユーティリティーが非推奨になりました。

ファイルシステムのバックアップに使用される **dump** ユーティリティーが非推奨になり、RHEL 9 では使用できなくなります。

RHEL 9 では、使用方法に基づいて、**tar**、**dd**、または **bacula** のバックアップユーティリティーを使用することが推奨されています。これにより、ext2、ext3、および ext4 のファイルシステムで完全で安全なバックアップが提供されます。

dump パッケージの **restore** ユーティリティーは、RHEL 9 で引き続き利用可能で、サポートされており、**restore** パッケージとして利用できます。

Bugzilla:1997366

hidepid=n マウントオプションが、RHEL 8 systemd で未サポート

マウントオプションの **hidepid=n** は、**/proc/[pid]** ディレクトリーの情報にアクセスできるユーザーを制御しますが、RHEL 8 で提供されている **systemd** インフラストラクチャーと互換性がありません。

また、このオプションを使用すると、**systemd** が起動する特定のサービスで SELinux の AVC 拒否メッセージが生成され、その他の操作が完了しないようにする場合があります。

詳細は、関連するナレッジベースのソリューション記事 Is mounting /proc with "hidepid=2" recommended with RHEL7 and RHEL8? を参照してください。

Bugzilla:2038929

/usr/lib/udev/rename_device ユーティリティーは非推奨になる

ネットワークインターフェイスの名前を変更するための **udev** ヘルパーユーティリティー **/usr/lib/udev/rename_device** は非推奨になる

Bugzilla:1875485

ABRT ツールは非推奨になりました

アプリケーションのクラッシュを検出して報告するための自動バグ報告ツール (ABRT) は、RHEL8 で非推奨になりました。代わりに、**systemd-coredump** ツールを使用して、プログラムのクラッシュ後に自動的に生成されるファイルであるコアダンプをログに記録して保存します。

Bugzilla:2055826

ReaR crontab は非推奨になりました

rear パッケージの **/etc/cron.d/rear** は RHEL 8 で非推奨になり、RHEL 9 では使用できなくなります。crontab は、ディスクレイアウトが変更されたかどうかを毎晩チェックし、変更が発生した場合は **rear mkrescue** コマンドを実行します。

この機能が必要な場合は、RHEL 9 にアップグレードした後、ReaR の定期的な実行を手動で設定してください。

Bugzilla:2083301

Bacula の SQLite データベースバックエンドは廃止されました

Bacula バックアップシステムは、複数のデータベースバックエンド (PostgreSQL、MySQL、および SQLite) をサポートしていました。SQLite バックエンドは廃止され、RHEL の今後のリリースではサ

ポートされなくなります。代わりに、他のバックエンド (PostgreSQL または MySQL) のいずれかに移行し、新しい展開では SQLite バックエンドを使用しないでください。

Bugzilla:2089399

raw コマンドは廃止されました

raw (**/usr/bin/raw**) コマンドは廃止されました。Red Hat Enterprise Linux の今後のリリースでこのコマンドを実行すると、エラーが発生します。

Jira:RHELPLAN-133171

10.5. セキュリティー

NSS SEED 暗号が非推奨になりました。

Mozilla Network Security Services (**NSS**) ライブラリーでは、今後のリリースで SEED 暗号化を使用する TLS 暗号スイートのサポートがなくなります。NSS がサポートを削除した際に SEED 暗号に依存するデプロイメントを円滑に移行させるため、Red Hat は、他の暗号スイートのサポートを有効にすることを推奨します。

RHEL では、SEED 暗号はデフォルトですでに無効にされています。

Bugzilla:1817533

TLS 1.0 および TLS 1.1 が非推奨になりました。

TLS 1.0 プロトコルおよび TLS 1.1 プロトコルは、システム全体の暗号化ポリシーレベル **DEFAULT** で無効になります。たとえば、Firefox Web ブラウザーのビデオ会議アプリケーションで、非推奨のプロトコルを使用する必要がある場合は、システム全体の暗号化ポリシーを **LEGACY** レベルに変更してください。

```
# update-crypto-policies --set LEGACY
```

詳細は、Red Hat カスタマーポータルのナレッジベースの記事 Strong crypto defaults in RHEL 8 and deprecation of weak crypto algorithms および man ページの **update-crypto-policies(8)** を参照してください。

Bugzilla:1660839

RHEL 8 で DSA が非推奨になりました。

デジタル署名アルゴリズム (DSA) は、Red Hat Enterprise Linux 8 では非推奨であると考えられています。DSA キーに依存する認証メカニズムはデフォルト設定では機能しません。**OpenSSH** クライアントは、**LEGACY** のシステム全体の暗号化ポリシーレベルでも DSA ホストキーを許可しません。

Bugzilla:1646541

fapolicyd.rules が非推奨になる

実行ルールの許可と拒否を含むファイルの **/etc/fapolicyd/rules.d/** ディレクトリーは、**/etc/fapolicyd/fapolicyd.rules** ファイルを置き換えます。**fagenrules** スクリプトは、このディレクトリー内のすべてのコンポーネントルールファイルを **/etc/fapolicyd/compiled.rules** ファイルにマージするようになりました。**/etc/fapolicyd/fapolicyd.trust** のルールは引き続き **fapolicyd** フレームワークによって処理されますが、下位互換性を確保するためのみに使用されます。

Bugzilla:2054741

NSS で SSL2 Client Hello が非推奨に

TLS (Transport Layer Security) プロトコルバージョン 1.2 以前は、 **SSL** (Secure Sockets Layer) プロトコルバージョン 2 と後方互換性がある形式の **Client Hello** メッセージを使用してネゴシエーションを開始できます。**NSS** (Network Security Services) ライブラリーでのこの機能への対応は非推奨となっており、デフォルトで無効になっています。

この機能への対応が必要なアプリケーションを有効にするには、新しい API の **SSL_ENABLE_V2_COMPATIBLE_HELLO** を使用する必要があります。この機能への対応は、Red Hat Enterprise Linux 8 の将来のリリースから完全に削除される可能性があります。

Bugzilla:1645153

/etc/selinux/config を使用して SELinux を無効にするランタイムが非推奨になりました。

/etc/selinux/config ファイルの **SELINUX=disabled** オプションを使用して SELinux を無効にするランタイムが非推奨になりました。RHEL 9 では、**/etc/selinux/config** でのみ SELinux を無効にすると、システムは SELinux が有効化されますが、ポリシーが読み込まれずに開始します。

SELinux を完全に無効にする必要がある場合には、Red Hat は、**selinux=0** パラメーターをカーネルコマンドラインに追加して SELinux を無効にすることを推奨します。これは、SELinux の使用 タイトルの システムの起動時に SELinux モードの変更 セクションで説明されています。

Bugzilla:1932222

selinux-policy から ipa SELinux モジュールが削除されました。

ipa SELinux はメンテナンスされなくなったため、**selinux-policy** から削除されました。この機能は、**ipa-selinux** サブパッケージに含まれるようになりました。

ローカルの SELinux ポリシーで、**ipa** モジュールからタイプやインターフェイスを使用する必要がある場合は、**ipa-selinux** をインストールします。

Bugzilla:1461914

TPM 1.2 が非推奨になりました。

Trusted Platform Module (TPM) のセキュアな暗号化プロセッサーの標準バージョンが 2016 年に バージョン 2.0 に更新されました。TPM 2.0 は TPM 1.2 に対する多くの改良を提供しますが、以前のバージョンと後方互換性はありません。TPM 1.2 は RHEL 8 で非推奨となり、次のメジャーリリースで削除される可能性があります。

Bugzilla:1657927

crypto-policies から派生したプロパティーが非推奨に

カスタムポリシーにおける **crypto-policies** ディレクティブのスコープの導入により、**tls_cipher**、**ssh_cipher**、**ssh_group**、**ike_protocol**、および **sha1_in_dnssec** の派生プロパティーが非推奨になりました。さらに、スコープを指定しない **protocol** プロパティーの使用も非推奨になりました。推奨される代替は、**crypto-policies(7)** の man ページを参照してください。

Bugzilla:2011208

10.6. ネットワーク

RHEL 8 でネットワークスクリプトが非推奨に

Red Hat Enterprise Linux 8 では、ネットワークスクリプトが非推奨になっており、デフォルトでは提供

されなくなりました。基本的なインストールでは、**nmcli** ツール経由で、NetworkManager サービスを呼び出す **ifup** スクリプトおよび **ifdown** スクリプトの新しいバージョンが提供されます。Red Hat Enterprise Linux 8 で **ifup** スクリプトおよび **ifdown** スクリプトを実行する場合は、NetworkManager を実行する必要があります。

/sbin/ifup-local、**ifdown-pre-local**、および **ifdown-local** の各スクリプトでは、カスタムコマンドが実行されません。

このスクリプトが必要な場合は、次のコマンドを使用すれば、システムに非推奨のネットワークスクリプトをインストールできます。

```
# yum install network-scripts
```

ifup スクリプトと **ifdown** スクリプトが、インストールされている従来のネットワークスクリプトにリンクされます。

従来のネットワークスクリプトを呼び出すと、そのスクリプトが非推奨であることを示す警告が表示されます。

Bugzilla:1647725

dropwatch ツールが非推奨に

dropwatch ツールが非推奨になりました。このツールは今後のリリースではサポートされませんので、新規デプロイメントには推奨できません。このパッケージの代わりに、Red Hat は **perf** コマンドラインツールを使用することを推奨します。

perf コマンドラインツールの使用方法の詳細は、Red Hat カスタマーポータルの Getting started with Perf セクションまたは **perf** の man ページを参照してください。

Bugzilla:1929173

xinetd が非推奨に

xinetd サービスが非推奨になり、RHEL 9 では削除される予定です。代わりに **systemd** を使用します。詳細は、xinetd サービスを systemd に変換する方法 を参照してください。

Bugzilla:2009113

cgdcbxd パッケージが非推奨に

コントロールグループデータセンターブリッジング交換デーモン (**cgdcbxd**) は、データセンターのブリッジ (DCB) のネットリンクイベントをモニターし **net_prio control** グループサブシステムを管理するサービスです。RHEL 8.5 以降では、**cgdcbxd** パッケージは非推奨となり、次の RHEL メジャーリリースで削除されます。

Bugzilla:2006665

WEP Wi-Fi 接続方法が非推奨になりました。

安全でない WEP (wired equivalent privacy) の Wi-Fi 接続方法は、RHEL 8 では非推奨となり、RHEL 9.0 では削除されます。安全な Wi-Fi 接続には、Wi-Fi Protected Access 3 (WPA3) または WPA2 の接続方法を使用します。

Bugzilla:2029338

サポートされていない xt_u32 モジュールが非推奨になりました。

サポートされていない **xt_u32** を使用すると、**iptable** のユーザーはパケットヘッダーまたはペイロード内の任意の 32 ビットにマッチできます。RHEL 8.6 以降、**xt_u32** モジュールが非推奨になり、RHEL 9 では削除されます。

xt_u32 を使用する場合は、**nftable** パケットフィルタリングフレームワークに移行します。たとえば、最初にファイアウォールを、個々のルールを段階的に置き換えるために、ネイティブ一致で **iptable** を使用するように変更し、その後に **iptables-translate** と付属のユーティリティーを使用して **nftable** に移行します。**nftable** にネイティブマッチが存在しない場合は、**nftable** の raw ペイロードマッチング機能を使用します。詳細は、**nft(8)** man ページの **raw ペイロード表現** セクションを参照してください。

Bugzilla:2061288

スレーブ という用語は、 nmstate API では非推奨です。

Red Hat では、意識的な言語の使用に取り組んでいます。この取り組みの詳細は、オープンソースをより包括的にする を参照してください。したがって、**スレーブ** という用語は Nmstate API では非推奨です。**nmstatectl** を使用する場合は、**port** という用語を使用します。

(Jira:RHELDOCS-17641)

10.7. カーネル

rdma_rxe Soft-RoCE ドライバーが非推奨に

Remote Software Direct Memory Access over Converged Ethernet (Soft-RoCE) は RXE としても知られており、RDMA (Remote Direct Memory Access) をエミュレートする機能です。RHEL 8 では、Soft-RoCE 機能が、サポートされていないテクノロジープレビューとして利用できます。ただし、安定性の問題により、この機能は非推奨になり、RHEL 9 では削除されます。

Bugzilla:1878207

Linux firewire サブシステムおよび関連するユーザー空間コンポーネントは、RHEL 8 では非推奨になりました。

firewire サブシステムは、IEEE 1394 バスでリソースを使用し、維持するインターフェイスを提供します。RHEL 9 では、**firewire** は、**kernel** パッケージで対応しなくなります。**firewire** には、**libavc1394**、**libdc1394**、**libraw1394** パッケージで提供されるユーザー空間コンポーネントが複数含まれることに注意してください。これらのパッケージも非推奨になります。

Bugzilla:1871863

ディスクレスブートを使用した RHEL for Real Time 8 のインストールが非推奨になりました。

ディスクレスブートにより、複数のシステムがネットワーク経由で root ファイルシステムを共有できます。メリットはありますが、ディスクレスブートでは、リアルタイムのワークロードでネットワークレイテンシーが発生する可能性が高くなります。RHEL for Real Time 8 の将来のマイナー更新では、ディスクレスブート機能はサポートされなくなります。

Bugzilla:1748980

カーネルライブパッチが、すべての RHEL マイナーリリースに対応するようになりました。

RHEL 8.1 以降、カーネルライブパッチは、影響度が重大および重要な Common Vulnerabilities and Exposures (CVE) を修正するために、Extended Update Support (EUS) ポリシーの対象となる RHEL の一部のマイナーリリースストリームに提供されています。同時にカバーされるカーネルとユースケースの最大数に対応するため、各ライブパッチのサポート期間は、カーネルのマイナー、メジャー、および

zStream の各バージョンで 12 カ月から 6 カ月に短縮されました。これは、カーネルライブパッチがリリースされると、過去 6 カ月間に配信されたすべてのマイナーリリースとスケジュール済みのエラータカーネルが含まれます。

この機能の詳細は、Applying patches with kernel live patching を参照してください。

利用可能なカーネルライブパッチの詳細は、Kernel Live Patch life cycles を参照してください。

Bugzilla:1958250

crash-ptdump-command パッケージは非推奨です

クラッシュユーティリティーの **ptdump** 拡張モジュールである **crash-ptdump-command** パッケージは非推奨であり、将来の RHEL リリースでは利用できなくなる可能性があります。**ptdump** コマンドは、Single Range Output モードで作業している場合、ログバッファーの取得に失敗し、Table of Physical Addresses (ToPA) モードでのみ機能します。**crash-ptdump-command** は現在、アップストリームに維持されていません

Bugzilla:1838927

10.8. ブートローダー

kernelopts 環境変数は非推奨になる

RHEL 8 では、GRUB ブートローダーを使用するシステムのカーネルコマンドラインパラメーターが **kernelopts** 環境変数で定義されていました。変数は、カーネルブートエントリーごとに **/boot/grub2/grubenv** ファイルに保存されました。ただし、**kernelopts** を使用してカーネルコマンドラインパラメーターを保存することは堅牢ではありませんでした。したがって、RHEL の将来のメジャー更新では **kernelopts** が削除され、代わりにカーネルコマンドラインパラメーターが Boot Loader Specification (BLS) スニペットに格納されます。

Bugzilla:2060759

10.9. ファイルシステムおよびストレージ

elevator カーネルコマンドラインパラメーターが非推奨になりました。

カーネルコマンドラインパラメーターの **elevator** は、すべてのデバイスのディスクスケジューラーを設定するために、以前の RHEL リリースで使用されていました。RHEL 8 では、このパラメーターが非推奨になりました。

アップストリームの Linux カーネルでは、**elevator** パラメーターに対応しなくなりましたが、互換性のために RHEL 8 でも引き続き利用できます。

カーネルは、デバイスのタイプに基づいてデフォルトのディスクスケジューラーを選択することに注意してください。これは通常、最適な設定です。別のスケジューラーが必要な場合は、**udev** ルールまたは TuneD サービスを使用して設定することが推奨されます。選択したデバイスを一致させ、それらのデバイスのスケジューラーのみを切り替えます。

詳しい情報は、ディスクスケジューラーの設定 を参照してください。

Bugzilla:1665295

NFSv3 over UDP が無効になりました。

NFS サーバーは、デフォルトで UDP (User Datagram Protocol) ソケットを開いたり、リッスンしなくなりました。バージョン 4 では TCP (Transmission Control Protocol) が必要なため、この変更は NFS バージョン 3 にのみ影響を及ぼします。

RHEL 8 では、NFS over UDP に対応しなくなりました。

Bugzilla:1592011

peripety が非推奨に

peripety パッケージは、RHEL 8.3 以降で非推奨になりました。

Peripety ストレージイベント通知デーモンは、システムストレージログを構造化されたストレージイベントに解析します。ストレージの問題を調査するのに役立ちます。

Bugzilla:1871953

async 以外の VDO 書き込みモードが非推奨に

VDO は、RHEL 8 で複数の書き込みモードに対応します。

- **sync**
- **async**
- **async-unsafe**
- **auto**

RHEL 8.4 以降、以下の書き込みモードが非推奨になりました。

sync
: VDO レイヤー上のデバイスは、VDO が同期されているかどうかを認識できないため、デバイスは VDO **sync** モードを利用できません。

async-unsafe
: VDO は、ACID (Atomicity, Consistency, Isolation, and Durability) に準拠する **async** モードの回避策としてこの書き込みモードを追加しました。Red Hat は、ほとんどのユースケースで **async-unsafe** を推奨せず、それに依存するユーザーを認識しません。

auto
: この書き込みモードは、他の書き込みモードのいずれかのみを選択します。VDO が 1 つの書き込みモードのみに対応している場合は、不要になりました。

この書き込みモードは、今後の RHEL メジャーリリースで削除されます。

推奨される VDO 書き込みモードが **async** になりました。

VDO 書き込みモードの詳細は、VDO 書き込みモードの選択 を参照してください。

Jira:RHELPLAN-70700

VDO マネージャーが非推奨に

python ベースの VDO 管理ソフトウェアは非推奨となり、RHEL 9 から削除される予定です。RHEL 9 では、LVM-VDO 統合に置き換えられます。そのため、**lvcreate** コマンドを使用して VDO ボリュームを作成することが推奨されます。

VDO 管理ソフトウェアを使用して作成した既存のボリュームは、**lvm2** パッケージが提供する **/usr/sbin/lvm_import_vdo** スクリプトを使用して変換できます。LVM-VDO 実装の詳細は、RHEL での論理ボリュームの重複排除および圧縮 を参照してください。

Bugzilla:1949163

cramfs が非推奨になりました。

ユーザーの不足により、**cramfs** カーネルモジュールが非推奨になりました。代替策として **squashfs** が推奨されます。

Bugzilla:1794513

10.10. 高可用性およびクラスター

clufter ツールに対応する pcs コマンドが非推奨になりました。

クラスター設定フォーマットを分析する **clufter** ツールに対応する **pcs** コマンドが非推奨になりました。これらのコマンドにより、コマンドが非推奨になり、コマンドに関連するセクションが **pcs** ヘルプ表示と、**pcs(8)** man ページから削除されていることを示す警告が出力されるようになりました。

以下のコマンドが非推奨になりました。

- **pcs config import-cman**: CMAN / RHEL6 HA クラスター設定のインポート
- **pcs config export**: クラスター設定を、同じクラスターを再作成する **pcs** コマンドのリストにエクスポート

Bugzilla:1851335

10.11. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー

Apache HTTP サーバーで使用するために PHP に提供されている mod_php モジュールが非推奨になりました。

RHEL 8 の Apache HTTP サーバーで使用するために PHP に付属している **mod_php** モジュールは利用可能ですが、デフォルト設定では有効になっていません。このモジュールは RHEL 9 では使用できなくなりました。

RHEL 8 以降、PHP スクリプトはデフォルトで FastCGI Process Manager (**php-fpm**) を使用して実行されます。詳細は、Apache HTTP サーバーでの PHP の使用 を参照してください。

Bugzilla:2225332

10.12. コンパイラーおよび開発ツール

gdb.i686 パッケージが非推奨に

RHEL 8.1 では、別のパッケージの依存関係の問題が原因で、32 ビットバージョンの GNU Debugger(GDB) **gdb.i686** が同梱されていました。RHEL 8 は 32 ビットハードウェアに対応していないため、RHEL 8.4 以降、**gdb.i686** パッケージは非推奨になりました。64 ビットバージョンの GDB (**gdb.x86_64**) は、32 ビットアプリケーションをデバッグできます。

gdb.i686 を使用する場合は、以下の重要な問題に注意してください。

- **gdb.i686** パッケージは更新されなくなりました。代わりに **gdb.x86_64** をインストールする必要があります。
- **gdb.i686** をインストールしている場合は、**gdb.x86_64** をインストールすると、**yum** が **package gdb-8.2-14.el8.x86_64 obsoletes gdb < 8.2-14.el8 provided by gdb-8.2-12.el8.i686** を報告します。これは想定される状況です。**gdb.i686** をアンインストールするか、**--allowerasing** オプションを **dnf** に渡して **gdb.i686** を削除し、**gdb.x8_64** をインストールします。
- ユーザーは、64 ビットシステム (つまり、**libc.so.6()(64-bit)** パッケージのある) に **gdb.i686** パッケージをインストールすることができなくなります。

Bugzilla:1853140

libdwarf が非推奨に

RHEL 8 では、**libdwarf** ライブラリーが非推奨になりました。ライブラリーは、将来のメジャーリリースでサポートされない可能性があります。代わりに、ELF/DWARF ファイルを処理するアプリケーションに **elfutils** および **libdw** ライブラリーを使用してください。

libdwarf-tools dwarfdump プログラムの代替は、**binutils readelf** プログラムまたは **elfutils eu-readelf** プログラムになります。どちらも **--debug-dump** フラグを渡すことで使用されます。

Bugzilla:1920624

10.13. IDENTITY MANAGEMENT

openssh-ldap が非推奨に

openssh-ldap サブパッケージは、Red Hat Enterprise Linux 8 で非推奨になり、RHEL 9 で削除されます。**openssh-ldap** サブパッケージはアップストリームでは維持されないため、Red Hat は SSSD と **sss_ssh_authorizedkeys** ヘルパーを使用することを推奨しています。これは、他の IdM ソリューションよりも適切に統合でき、安全です。

デフォルトでは、**ldap** および **ipa** プロバイダーはユーザーオブジェクトの **sshPublicKey** LDAP 属性を読み取ります (利用可能な場合)。AD (Active Directory) には公開鍵を保存するためのデフォルトの LDAP 属性がないため、**ad** プロバイダーまたは IdM の信頼されるドメインのデフォルト SSSD 設定を使用して AD から SSH 公開鍵を取得することはできません。

sss_ssh_authorizedkeys ヘルパーが SSSD から鍵を取得できるようにするには、**sssd.conf** ファイルの **services** オプションに **ssh** を追加して **ssh** レスポンダーを有効にします。詳細は man ページの **sssd.conf(5)** を参照してください。

sshd が **sss_ssh_authorizedkeys** を使用できるようにするには、man ページの **sss_ssh_authorizedkeys(1)** に記載されているように、**AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys** および **AuthorizedKeysCommandUser nobody** オプションを **/etc/ssh/sshd_config** ファイルに追加します。

Bugzilla:1871025

DES および 3DES 暗号化タイプが削除されました。

RHEL 7 以降、セキュリティー上の理由から、データ暗号化標準 (DES) アルゴリズムが非推奨になり、デフォルトで無効化になりました。Kerberos パッケージの最近のリベースで、RHEL 8 からシングル DES (DES) およびトリプル DES (3DES) の暗号化タイプが削除されました。

DES または 3DES の暗号化のみを使用するようにサービスまたはユーザーが設定されている場合、以下のようなサービスの中断が発生する可能性があります。

- Kerberos 認証エラー
- **unknown enctype** 暗号化エラー
- DES で暗号化されたデータベースマスターキー (**K/M**) を使用した KDC (Kerberos Distribution Center) が起動しない

アップグレードを準備するには、以下の操作を実施します。

1. KDC が **krb5check** オープンソース Python スクリプトで DES または 3DES 暗号化を使用しているかどうかを確認します。GitHub の krb5check を参照してください。
2. Kerberos プリンシパルで DES または 3DES 暗号化を使用している場合は、Advanced Encryption Standard (AES) などのサポート対象の暗号化タイプでキーを変更します。キー変更の手順については、MIT Kerberos ドキュメントの Retiring DES を参照してください。
3. アップグレードの前に以下の Kerberos オプションを一時的に設定して、DES および 3DES からの独立性をテストします。
   a. KDC の **/var/kerberos/krb5kdc/kdc.conf** で、**supported_enctypes** を設定し、**des** または **des3** は含まれません。
   b. すべてのホストについて、**/etc/krb5.conf** および **/etc/krb5.conf.d** のすべてのファイルで、**allow_weak_crypto** を **false** に設定します。デフォルトは false です。
   c. すべてのホストについて、**/etc/krb5.conf** および **/etc/krb5.conf.d** のすべてのファイルで、**permitted_enctypes**、**default_tgs_enctypes**、**default_tkt_enctypes** を設定します。また、**des** または **des3** は含めません。
4. 前の手順で Kerberos 設定をテストしてサービスが中断されない場合は、サービスを削除してアップグレードします。最新の Kerberos パッケージにアップグレードした後は、この設定は必要ありません。

Bugzilla:1877991

SSSD バージョンの libwbclient が削除される

libwbclient パッケージの SSSD 実装は、RHEL 8.4 で非推奨になりました。最新バージョンの Samba で使用できないため、 **libwbclient** の SSSD 実装 が削除されています。

Bugzilla:1947671

ctdb サービスのスタンドアロン使用が非推奨になりました。

RHEL 8.4 以降、以下の条件がすべて適用されている場合に限り、**ctdb** クラスター Samba サービスを使用することが推奨されます。

- **ctdb** サービスは、resource-agent **ctdb** を使用して **pacemaker** リソースとして管理されます。
- **ctdb** サービスは、Red Hat Gluster Storage 製品または GFS2 ファイルシステムが提供する GlusterFS ファイルシステムのいずれかが含まれるストレージボリュームを使用します。

ctdb サービスのスタンドアロンユースケースは非推奨となり、Red Hat Enterprise Linux の次期メジャーリリースには含まれません。Samba のサポートポリシーの詳細は、ナレッジベースの記事 Support Policies for RHEL Resilient Storage - ctdb General Policies を参照してください。

Bugzilla:1916296

WinSync による IdM との間接的な AD 統合が非推奨に

WinSync は、さまざまな機能制限のため、RHEL 8 では積極的に開発されなくなりました。

- WinSync は、1 つの Active Directory (AD) ドメインのみをサポートします。
- パスワードの同期には、AD ドメインコントローラーに追加のソフトウェアをインストールする必要があります。

リソースとセキュリティーの分離を強化したより強固なソリューションとして、レッドハットは Active Directory との間接的な統合に**フォレスト間の信頼**を使用することを推奨しています。間接的な統合 のドキュメントを参照してください。

Jira:RHELPLAN-100400

SSSD 暗黙的なファイルプロバイダードメインは、デフォルトで無効になっています。

/etc/sssd/sssd.conf 設定ファイルの **enable_files_domain** 設定のデフォルト値が **true** から **false** に変更されました。これは、ローカルファイル **/etc/passwd** および **/etc/group** からユーザーおよびグループ情報を取得する SSSD 暗黙的 **files** プロバイダードメインがデフォルトで無効になったことを意味します。

SSSD の代わりに、デフォルトの **glibc files** モジュールがローカルユーザーにサービスを提供します。**sssd.conf** ファイルでドメインを定義していない限り、SSSD は自動的に起動しません。

SSSD **files** プロバイダーの実装は、ローカルユーザーのスマートカード認証など、特定のユースケースの明示的な設定に引き続き使用できます。

Jira:RHELPLAN-139456

Samba を PDC または BDC として実行することは非推奨になりました。

管理者が Samba を NT4 のようなプライマリードメインコントローラー (PDC) として実行し、バックアップドメインコントローラー (BDC) を実行できるようにする従来のドメインコントローラーモードが非推奨になりました。これらのモードを設定するためのコードおよび設定は、今後の Samba リリースで削除されます。

RHEL 8 の Samba バージョンが PDC モードおよび BDC モードを提供している限り、Red Hat は、NT4 ドメインに対応する Windows バージョンを使用する既存のインストールでのみ、これらのモードをサポートします。Red Hat は、新規の Samba NT4 ドメインのセットアップを推奨しません。なぜなら、Microsoft のオペレーティングシステム (Windows 7 以降) および Windows Server 2008 R2 は、NT4 ドメインをサポートしないからです。

PDC を使用して Linux ユーザーのみを認証する場合、Red Hat は、RHEL サブスクリプションに含まれる Red Hat Identity Management (IdM) への移行を推奨します。ただし、Windows システムを IdM ドメインに参加させることはできません。Red Hat は、引き続き IdM が使用する PDC 機能のサポートを継続することに注意してください。

Red Hat は、Samba を AD ドメインコントローラー (DC) として実行することはサポートしていません。

Bugzilla:1926114

SMB1 プロトコルは Samba では非推奨に

Samba 4.11 以降、安全でない Server Message Block バージョン 1 (SMB1) プロトコルは非推奨となり、今後のリリースでは削除される予定です。

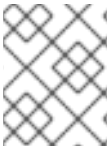
セキュリティーを向上させるために、デフォルトでは、Samba サーバーおよびクライアントユーティリティーで SMB1 が無効になっています。

Jira:RHELDOCS-16612

FreeRADIUS のサポートは限定的です

RHEL 8 では、FreeRADIUS サービスの一部として、次の外部認証モジュールが非推奨になりました。

- MySQL、PostgreSQL、SQlite、および unixODBC データベースコネクター
- **Perl** 言語モジュール
- REST API モジュール



注記

ベースパッケージの一部として提供される PAM 認証モジュールおよびその他の認証モジュールは影響を受けません。

廃止されたモジュールの代替は、Fedora プロジェクトなどのコミュニティーでサポートされているパッケージで見つけることができます。

さらに、**freeradius** パッケージのサポート範囲は、将来の RHEL リリースでは次のユースケースに限定されます。

- FreeRADIUS をワイヤレス認証プロバイダーとして使用し、Identity Management (IdM) を認証のバックエンドソースとして使用します。認証は、**krb5** および LDAP 認証パッケージを使用して、またはメインの FreeRADIUS パッケージの PAM 認証として行われます。
- FreeRADIUS を使用して、Python 3 認証パッケージで IdM の認証用に信頼できる情報源を提供します。

これらの廃止とは対照的に、Red Hat は FreeRADIUS による次の外部認証モジュールのサポートを強化します。

- **krb5** および LDAP に基づく認証
- **Python 3** 認証

これらのインテグレーションオプションに重点を置くことは、Red Hat IdM の戦略的方向性に一致します。

Jira:RHELDOCS-17573

10.14. デスクトップ

libgnome-keyring ライブラリーが非推奨になりました。

libgnome-keyring ライブラリーがアップストリームで維持されず、RHEL に必要な暗号化ポリシーに従っていないため、**libsecret** ライブラリーが **libgnome-keyring** ライブラリーを引き継ぎ、libgnome-keyring は非推奨となりました。新しい **libsecret** ライブラリーは、必要なセキュリティー標準に準拠す

る代替ライブラリーです。

Bugzilla:1607766

10.15. グラフィックインフラストラクチャー

AGP グラフィックカードがサポートされなくなりました。

AGP (Accelerated Graphics Port) バスを使用するグラフィックカードは、Red Hat Enterprise Linux 8 ではサポートされていません。推奨される代替として、PCI-Express バスを備えたグラフィックスカードを使用してください。

Bugzilla:1569610

Motif は非推奨になりました

アップストリームの Motif コミュニティーでの開発は非アクティブであるため、Motif ウィジェットツールキットは RHEL で非推奨になりました。

開発バリアントおよびデバッグバリアントを含む、以下の Motif パッケージが非推奨になりました。

- **motif**
- **openmotif**
- **openmotif21**
- **openmotif22**

さらに、**motif-static** パッケージが削除されました。

Red Hat は、GTK ツールキットを代替として使用することを推奨します。GTK は Motif と比較してメンテナンス性が高く、新機能を提供します。

Jira:RHELPLAN-98983

10.16. WEB コンソール

Web コンソールは、不完全な翻訳への対応を終了しました。

RHEL Web コンソールは、コンソールの翻訳可能な文字列の翻訳率が 50 % 未満の言語に対する翻訳提供を廃止しました。ブラウザーがこのような言語に翻訳を要求すると、ユーザーインターフェイスは英語になります。

Bugzilla:1666722

10.17. RED HAT ENTERPRISE LINUX システムロール

geoipupdate パッケージが非推奨に

geoipupdate パッケージにはサードパーティーのサブスクリプションが必要で、プロプライエタリーコンテンツもダウンロードします。したがって、**geoipupdate** パッケージは非推奨となり、次の RHEL メジャーバージョンで削除されます。

Bugzilla:1874892

RHEL 9 ノードでチームを設定すると、 network システムロールが非推奨の警告を表示します。

ネットワークチーミング機能は、RHEL 9 では非推奨になりました。その結果、RHEL 8 制御ノードで **network** RHEL システムロールを使用して RHEL 9 ノードでネットワークチームを設定すると、非推奨についての警告が表示されます。

Bugzilla:2021685

Ansible Engine は非推奨になりました

以前のバージョンの RHEL8 は、サポートの範囲が限定された Ansible Engine リポジトリーへのアクセスを提供し、RHEL System Roles や Insights 救済策などのサポートされた RHEL Automation ユースケースを有効にしました。Ansible Engine は非推奨になり、Ansible Engine 2.9 は 2023 年 9 月 29 日以降サポートされなくなります。サポートされているユースケースの詳細については、RHEL 9 および RHEL 8.6 以降の AppStream リポジトリーに含まれる Ansible Core パッケージのサポート対象範囲 を参照してください。

ユーザーは、システムを Ansible Engine から Ansible Core に手動で移行する必要があります。そのためには、以下の手順に従います。

手順

1. システムが RHEL 8.7 以降のリリースを実行しているかどうかを確認します。

```
# cat /etc/redhat-release
```

2. Ansible Engine 2.9 をインストールします。

```
# yum remove ansible
```

3. **ansible-2-for-rhel-8-x86_64-rpms** リポジトリーを無効にします。

```
# subscription-manager repos --disable
ansible-2-for-rhel-8-x86_64-rpms
```

4. RHEL 8 AppStream リポジトリーから Ansible Core パッケージをインストールします。

```
# yum install ansible-core
```

詳細については、RHEL8.6 以降での Ansible の使用 を参照してください。

Bugzilla:2006081

10.18. 仮想化

virsh iface-* コマンドが非推奨になりました。

virsh iface-start、**virsh iface-destroy** などの **virsh iface-*** コマンドは非推奨になり、将来のメジャーバージョンの RHEL では削除される予定です。また、このようなコマンドは設定の依存関係により頻繁に失敗します。

したがって、ホストネットワーク接続の設定および管理には **virsh iface-*** コマンドを使用しないことが推奨されます。代わりに、NetworkManager プログラムと、関連する管理アプリケーション (**nmcli** など) を使用します。

Bugzilla:1664592

virt-manager が非推奨になりました。

Virtual Machine Manager アプリケーション (**virt-manager**) は非推奨になっています。RHEL Web コンソール (**Cockpit**) は、後続のリリースで置き換えられる予定です。したがって、GUI で仮想化を管理する場合は、Web コンソールを使用することが推奨されます。ただし、**virt-manager** で利用可能な機能によっては、RHEL Web コンソールで利用できない場合があります。

Jira:RHELPLAN-10304

仮想マシンスナップショットのサポートが限定されました

仮想マシンのスナップショットの作成は、現在、UEFI ファームウェアを使用していない仮想マシンのみでサポートされています。さらに、スナップショット操作中に QEMU モニターがブロックされる可能性があり、これは特定のワークロードのハイパーバイザーのパフォーマンスに悪影響を及ぼします。

また、現在の仮想マシンスナップショットの作成メカニズムは非推奨となり、Red Hat は実稼働環境での仮想マシンスナップショットの使用を推奨していないことにも注意してください。

Bugzilla:1686057

Cirrus VGA 仮想 GPU タイプが非推奨に

Red Hat Enterprise Linux の将来のメジャー更新では、KVM 仮想マシンで **Cirrus VGA** GPU デバイスに対応しなくなります。したがって、Red Hat は **Cirrus VGA** の代わりに **stdvga** または **virtio-vga** デバイスの使用を推奨します。

Bugzilla:1651994

SPICE が非推奨になりました

SPICE リモートディスプレイプロトコルが非推奨になりました。その結果、SPICE は RHEL 8 でも引き続きサポートされますが、Red Hat はリモートディスプレイストリーミングに代替ソリューションを使用することを推奨しています。

- リモートコンソールへのアクセスには、VNC プロトコルを使用します。
- 高度なリモートディスプレイ機能には、RDP、HP RGS、または Mechdyne TGX などのサードパーティーツールを使用します。

SPICE で使用される **QXL** グラフィックスデバイスも非推奨になっていることに注意してください。

Bugzilla:1849563

IBM POWER 上の KVM が非推奨に

IBM POWER ハードウェアでの KVM 仮想化の使用は非推奨になりました。その結果、IBM POWER の KVM は、RHEL 8 でも引き続きサポートされますが、RHEL の今後のメジャーリリースではサポートされなくなります。

Jira:RHELPLAN-71200

SHA1 ベースの署名を使用した SecureBoot イメージ検証が非推奨に

UEFI (PE/COFF) 実行ファイルでの SHA1 ベースの署名を使用した SecureBoot イメージ検証の実行は非推奨になりました。代わりに、Red Hat は、SHA2 アルゴリズムまたはそれ以降に基づく署名を使用することを推奨します。

Bugzilla:1935497

SPICE を使用したスマートカードリーダーの仮想マシンへの接続が非推奨となりました

RHEL 8 では、SPICE リモートディスプレイプロトコルが非推奨になりました。スマートカードリーダーを仮想マシンに割り当てる唯一の推奨される方法は、SPICE プロトコルに依存するため、仮想マシンでのスマートカードの使用も RHEL 8 で非推奨になりました。

RHEL の将来のメジャーバージョンでは、スマートカードリーダーを仮想マシンに割り当てる機能は、サードパーティーのリモート可視化ソリューションでのみサポートされる予定です。

Bugzilla:2059626

RDMA ベースのライブマイグレーションは非推奨になりました。

この更新により、リモートダイレクトメモリーアクセス (RDMA) を使用した実行中の仮想マシンの移行は非推奨になりました。その結果、**rdma://** 移行 URI を使用して RDMA 経由の移行を要求することは可能ですが、この機能は RHEL の将来のメジャーリリースではサポートされなくなります。

Jira:RHELPLAN-153267

10.19. コンテナー

Podman varlink ベースの API v1.0 が削除されました

Podman varlink ベースの API v1.0 は、以前のリリースの RHEL 8 で非推奨となりました。Podman v2.0 には、新しい Podman v2.0 RESTful API が導入されました。Podman v3.0 のリリースでは、varlink ベースの API v1.0 が完全に削除されました。

Jira:RHELPLAN-45858

container-tools:1.0 が非推奨に

container-tools:1.0 モジュールは非推奨となり、セキュリティー更新を受信しなくなります。**container-tools:2.0** や **container-tools:3.0** などの新しいサポートされる安定したモジュールストリームを使用することが推奨されます。

Jira:RHELPLAN-59825

container-tools:2.0 モジュールは非推奨になりました

container-tools:2.0 モジュールは非推奨となり、セキュリティー更新を受信しなくなります。**container-tools:3.0** など、サポートされている新しい安定したモジュールストリームの使用を推奨します。

Jira:RHELPLAN-85066

GIMP 以外の Flatpak イメージは廃止されました

rhel8/firefox-flatpak、**rhel8/thunderbird-flatpak**、**rhel8/inkscape-flatpak**、および **rhel8/libreoffice-flatpak** RHEL 8 Flatpak アプリケーションは廃止され、RHEL 9 バージョンに置き換えられました。RHEL 9 にはまだ代替品がないため、**rhel8/gimp-flatpak** Flatpak アプリケーションは非推奨ではありません。

Bugzilla:2142499

CNI ネットワークスタックが非推奨なる

Container Network Interface (CNI) ネットワークスタックは、将来のマイナーバージョンで非推奨にな

る予定です。以前は、コンテナーは DNS 経由のみで単一の Container Network Interface (CNI) プラグインに接続していました。Podman v.4.0 では、新しい Netavark ネットワークスタックが導入されました。Netavark ネットワークスタックは、Podman およびその他の Open Container Initiative (OCI) コンテナー管理アプリケーションとともに使用できます。Podman 用の Netavark ネットワークスタックは、高度な Docker 機能とも互換性があります。複数のネットワーク内のコンテナーは、それらのネットワークのいずれかにあるコンテナーにアクセスできます。

詳細は、CNI から Netavark へのネットワークスタックの切り替え を参照してください。

Jira:RHELPLAN-145958

container-tools:3.0 が非推奨になりました。

container-tools:3.0 モジュールは非推奨となり、セキュリティー更新を受信しなくなります。RHEL 上で Linux コンテナーの構築と実行を続けるには、**container-tools:4.0** など、より新しく安定したサポートされているモジュールストリームを使用してください。

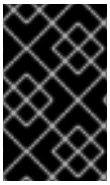
後続のストリームに切り替える手順については、後続のストリームへの切り替え を参照してください。

Jira:RHELPLAN-146398

10.20. 非推奨のパッケージ

このセクションでは、非推奨となり、将来バージョンの Red Hat Enterprise Linux には含まれない可能性があるパッケージのリストを示します。

RHEL 7 と RHEL 8 との間でパッケージを変更する場合は、**RHEL 8 の導入における考慮事項** ドキュメントの パッケージの変更 を参照してください。



重要

非推奨パッケージのサポート状況は、RHEL 8 内でも変更されません。サポート期間の詳細は、Red Hat Enterprise Linux のライフサイクル および Red Hat Enterprise Linux アプリケーションストリームのライフサイクル を参照してください。

次のパッケージは RHEL 8 で非推奨になりました。

- 389-ds-base-legacy-tools
- abrt
- abrt-addon-ccpp
- abrt-addon-kerneloops
- abrt-addon-pstoreoops
- abrt-addon-vmcore
- abrt-addon-xorg
- abrt-cli
- abrt-console-notification
- abrt-dbus

- abrt-desktop
- abrt-gui
- abrt-gui-libs
- abrt-libs
- abrt-tui
- adobe-source-sans-pro-fonts
- adwaita-qt
- alsa-plugins-pulseaudio
- amanda
- amanda-client
- amanda-libs
- amanda-server
- ant-contrib
- antlr3
- antlr32
- aopalliance
- apache-commons-collections
- apache-commons-compress
- apache-commons-exec
- apache-commons-jxpath
- apache-commons-parent
- apache-ivy
- apache-parent
- apache-resource-bundles
- apache-sshd
- apiguardian
- aspnetcore-runtime-3.0
- aspnetcore-runtime-3.1
- aspnetcore-runtime-5.0

- aspnetcore-targeting-pack-3.0
- aspnetcore-targeting-pack-3.1
- aspnetcore-targeting-pack-5.0
- assertj-core
- authd
- auto
- autoconf213
- autogen
- autogen-libopts
- awscli
- base64coder
- batik
- batik-css
- batik-util
- bea-stax
- bea-stax-api
- bind-export-devel
- bind-export-libs
- bind-libs-lite
- bind-pkcs11
- bind-pkcs11-devel
- bind-pkcs11-libs
- bind-pkcs11-utils
- bind-sdb
- bind-sdb
- bind-sdb-chroot
- bluez-hid2hci
- boost-jam
- boost-signals

- bouncycastle
- bpg-algeti-fonts
- bpg-chveulebrivi-fonts
- bpg-classic-fonts
- bpg-courier-fonts
- bpg-courier-s-fonts
- bpg-dedaena-block-fonts
- bpg-dejavu-sans-fonts
- bpg-elite-fonts
- bpg-excelsior-caps-fonts
- bpg-excelsior-condenced-fonts
- bpg-excelsior-fonts
- bpg-fonts-common
- bpg-glaho-fonts
- bpg-gorda-fonts
- bpg-ingiri-fonts
- bpg-irubaqidze-fonts
- bpg-mikhail-stephan-fonts
- bpg-mrgvlovani-caps-fonts
- bpg-mrgvlovani-fonts
- bpg-nateli-caps-fonts
- bpg-nateli-condenced-fonts
- bpg-nateli-fonts
- bpg-nino-medium-cond-fonts
- bpg-nino-medium-fonts
- bpg-sans-fonts
- bpg-sans-medium-fonts
- bpg-sans-modern-fonts
- bpg-sans-regular-fonts

- bpg-serif-fonts
- bpg-serif-modern-fonts
- bpg-ucnobi-fonts
- brlapi-java
- bsh
- buildnumber-maven-plugin
- byaccj
- cal10n
- cbi-plugins
- cdparanoia
- cdparanoia-devel
- cdparanoia-libs
- cdrdao
- cmirror
- codehaus-parent
- codemodel
- compat-exiv2-026
- compat-guile18
- compat-hwloc1
- compat-libpthread-nonshared
- compat-libtiff3
- compat-openssl10
- compat-sap-c++-11
- compat-sap-c++-10
- compat-sap-c++-9
- createrepo_c-devel
- ctags
- ctags-etags
- custodia

- cyrus-imapd-vzic
- dbus-c++
- dbus-c++-devel
- dbus-c++-glib
- dbxtool
- dhcp-libs
- directory-maven-plugin
- directory-maven-plugin-javadoc
- dirsplit
- dleyna-connector-dbus
- dleyna-core
- dleyna-renderer
- dleyna-server
- dnssec-trigger
- dnssec-trigger-panel
- dotnet-apphost-pack-3.0
- dotnet-apphost-pack-3.1
- dotnet-apphost-pack-5.0
- dotnet-host-fxr-2.1
- dotnet-host-fxr-2.1
- dotnet-hostfxr-3.0
- dotnet-hostfxr-3.1
- dotnet-hostfxr-5.0
- dotnet-runtime-2.1
- dotnet-runtime-3.0
- dotnet-runtime-3.1
- dotnet-runtime-5.0
- dotnet-sdk-2.1
- dotnet-sdk-2.1.5xx

- dotnet-sdk-3.0
- dotnet-sdk-3.1
- dotnet-sdk-5.0
- dotnet-targeting-pack-3.0
- dotnet-targeting-pack-3.1
- dotnet-targeting-pack-5.0
- dotnet-templates-3.0
- dotnet-templates-3.1
- dotnet-templates-5.0
- dotnet5.0-build-reference-packages
- dptfxtract
- drpm
- drpm-devel
- dump
- dvd+rw-tools
- dyninst-static
- eclipse-ecf
- eclipse-ecf-core
- eclipse-ecf-runtime
- eclipse-emf
- eclipse-emf-core
- eclipse-emf-runtime
- eclipse-emf-xsd
- eclipse-equinox-osgi
- eclipse-jdt
- eclipse-license
- eclipse-p2-discovery
- eclipse-pde
- eclipse-platform

- eclipse-swt
- ed25519-java
- ee4j-parent
- elfutils-devel-static
- elfutils-libelf-devel-static
- enca
- enca-devel
- environment-modules-compat
- evince-browser-plugin
- exec-maven-plugin
- farstream02
- felix-gogo-command
- felix-gogo-runtime
- felix-gogo-shell
- felix-scr
- felix-osgi-compendium
- felix-osgi-core
- felix-osgi-foundation
- felix-parent
- file-roller
- fipscheck
- fipscheck-devel
- fipscheck-lib
- firewire
- fonts-tweak-tool
- forge-parent
- freeradius-mysql
- freeradius-perl
- freeradius-postgresql

- freeradius-rest
- freeradius-sqlite
- freeradius-unixODBC
- fuse-sshfs
- fusesource-pom
- future
- gamin
- gamin-devel
- gavl
- gcc-toolset-10
- gcc-toolset-10-annobin
- gcc-toolset-10-binutils
- gcc-toolset-10-binutils-devel
- gcc-toolset-10-build
- gcc-toolset-10-dwz
- gcc-toolset-10-dyninst
- gcc-toolset-10-dyninst-devel
- gcc-toolset-10-elfutils
- gcc-toolset-10-elfutils-debuginfod-client
- gcc-toolset-10-elfutils-debuginfod-client-devel
- gcc-toolset-10-elfutils-devel
- gcc-toolset-10-elfutils-libelf
- gcc-toolset-10-elfutils-libelf-devel
- gcc-toolset-10-elfutils-libs
- gcc-toolset-10-gcc
- gcc-toolset-10-gcc-c++
- gcc-toolset-10-gcc-gdb-plugin
- gcc-toolset-10-gcc-gfortran
- gcc-toolset-10-gdb

- gcc-toolset-10-gdb-doc
- gcc-toolset-10-gdb-gdbserver
- gcc-toolset-10-libasan-devel
- gcc-toolset-10-libatomic-devel
- gcc-toolset-10-libitm-devel
- gcc-toolset-10-liblsan-devel
- gcc-toolset-10-libquadmath-devel
- gcc-toolset-10-libstdc++-devel
- gcc-toolset-10-libstdc++-docs
- gcc-toolset-10-libtsan-devel
- gcc-toolset-10-libubsan-devel
- gcc-toolset-10-ltrace
- gcc-toolset-10-make
- gcc-toolset-10-make-devel
- gcc-toolset-10-perftools
- gcc-toolset-10-runtime
- gcc-toolset-10-strace
- gcc-toolset-10-systemtap
- gcc-toolset-10-systemtap-client
- gcc-toolset-10-systemtap-devel
- gcc-toolset-10-systemtap-initscript
- gcc-toolset-10-systemtap-runtime
- gcc-toolset-10-systemtap-sdt-devel
- gcc-toolset-10-systemtap-server
- gcc-toolset-10-toolchain
- gcc-toolset-10-valgrind
- gcc-toolset-10-valgrind-devel
- gcc-toolset-9
- gcc-toolset-9-annobin

- gcc-toolset-9-build
- gcc-toolset-9-perftools
- gcc-toolset-9-runtime
- gcc-toolset-9-toolchain
- gcc-toolset-11-make-devel
- GConf2
- GConf2-devel
- gegl
- genisoimage
- genwqe-tools
- genwqe-vpd
- genwqe-zlib
- genwqe-zlib-devel
- geoipupdate
- geronimo-annotation
- geronimo-jms
- geronimo-jpa
- geronimo-parent-poms
- gfbgraph
- gflags
- gflags-devel
- glassfish-annotation-api
- glassfish-el
- glassfish-fastinfoset
- glassfish-jaxb-core
- glassfish-jaxb-txw2
- glassfish-jsp
- glassfish-jsp-api
- glassfish-legal

- glassfish-master-pom
- glassfish-servlet-api
- glew-devel
- glib2-fam
- glog
- glog-devel
- gmock
- gmock-devel
- gnome-abrt
- gnome-boxes
- gnome-menus-devel
- gnome-online-miners
- gnome-shell-extension-disable-screenshield
- gnome-shell-extension-horizontal-workspaces
- gnome-shell-extension-no-hot-corner
- gnome-shell-extension-window-grouper
- gnome-themes-standard
- gnu-free-fonts-common
- gnu-free-mono-fonts
- gnu-free-sans-fonts
- gnu-free-serif-fonts
- gnupg2-smime
- gnuplot
- gnuplot-common
- gobject-introspection-devel
- google-gson
- google-noto-sans-syriac-eastern-fonts
- google-noto-sans-syriac-estrangela-fonts
- google-noto-sans-syriac-western-fonts

- google-noto-sans-tibetan-fonts
- google-noto-sans-ui-fonts
- gphoto2
- gsl-devel
- gssntlmssp
- gtest
- gtest-devel
- gtkmm24
- gtkmm24-devel
- gtkmm24-docs
- gtksourceview3
- gtksourceview3-devel
- gtkspell
- gtkspell-devel
- gtkspell3
- guile
- gutenprint-gimp
- gutenprint-libs-ui
- gvfs-afc
- gvfs-afp
- gvfs-archive
- hamcrest-core
- hawtjni
- hawtjni
- hawtjni-runtime
- HdrHistogram
- HdrHistogram-javadoc
- highlight-gui
- hivex-devel

- hostname
- hplip-gui
- httpcomponents-project
- hwloc-plugins
- hyphen-fo
- hyphen-grc
- hyphen-hsb
- hyphen-ia
- hyphen-is
- hyphen-ku
- hyphen-mi
- hyphen-mn
- hyphen-sa
- hyphen-tk
- ibus-sayura
- icedax
- icu4j
- idm-console-framework
- inkscape
- inkscape-docs
- inkscape-view
- iptables
- ipython
- isl
- isl-devel
- isorelax
- istack-commons-runtime
- istack-commons-tools
- iwl3945-firmware

- iwl4965-firmware
- iwl6000-firmware
- jacoco
- jaf
- jaf-javadoc
- jakarta-oro
- janino
- jansi-native
- jarjar
- java-1.8.0-ibm
- java-1.8.0-ibm-demo
- java-1.8.0-ibm-devel
- java-1.8.0-ibm-headless
- java-1.8.0-ibm-jdbc
- java-1.8.0-ibm-plugin
- java-1.8.0-ibm-src
- java-1.8.0-ibm-webstart
- java-1.8.0-openjdk-accessibility
- java-1.8.0-openjdk-accessibility-slowdebug
- java_cup
- java-atk-wrapper
- javacc
- javacc-maven-plugin
- javaewah
- javaparser
- javapoet
- javassist
- javassist-javadoc
- jaxen

- jboss-annotations-1.2-api
- jboss-interceptors-1.2-api
- jboss-logmanager
- jboss-parent
- jctools
- jdepend
- jdependency
- jdom
- jdom2
- jetty
- jetty-continuation
- jetty-http
- jetty-io
- jetty-security
- jetty-server
- jetty-servlet
- jetty-util
- jffi
- jflex
- jgit
- jline
- jmc
- jnr-netdb
- jolokia-jvm-agent
- js-uglify
- jsch
- json_simple
- jss-javadoc
- jtidy

- junit5
- jvnet-parent
- jzlib
- kernel-cross-headers
- ksc
- kurdit-unikurd-web-fonts
- kyotocabinet-libs
- ldapjdk-javadoc
- lensfun
- lensfun-devel
- lftp-scripts
- libaec
- libaec-devel
- libappindicator-gtk3
- libappindicator-gtk3-devel
- libatomic-static
- libavc1394
- libblocksruntime
- libcacard
- libcacard-devel
- libcgroup
- libcgroup-tools
- libchamplain
- libchamplain-devel
- libchamplain-gtk
- libcroco
- libcroco-devel
- libcxl
- libcxl-devel

- libdap
- libdap-devel
- libdazzle-devel
- libdbusmenu
- libdbusmenu-devel
- libdbusmenu-doc
- libdbusmenu-gtk3
- libdbusmenu-gtk3-devel
- libdc1394
- libdnet
- libdnet-devel
- libdv
- libdwarf
- libdwarf-devel
- libdwarf-static
- libdwarf-tools
- libeasyfc
- libeasyfc-gobject
- libepubgen-devel
- libertas-sd8686-firmware
- libertas-usb8388-firmware
- libertas-usb8388-olpc-firmware
- libgdither
- libGLEW
- libgovirt
- libguestfs-benchmarking
- libguestfs-devel
- libguestfs-gfs2
- libguestfs-gobject

- libguestfs-gobject-devel
- libguestfs-java
- libguestfs-java-devel
- libguestfs-javadoc
- libguestfs-man-pages-ja
- libguestfs-man-pages-uk
- libguestfs-tools
- libguestfs-tools-c
- libhugetlbfs
- libhugetlbfs-devel
- libhugetlbfs-utils
- libIDL
- libIDL-devel
- libidn
- libiec61883
- libindicator-gtk3
- libindicator-gtk3-devel
- libiscsi-devel
- libjose-devel
- libkkc
- libkkc-common
- libkkc-data
- libldb-devel
- liblogging
- libluksmeta-devel
- libmalaga
- libmcpp
- libmemcached
- libmemcached-libs

- libmetalink
- libmodulemd1
- libmongocrypt
- libmtp-devel
- libmusicbrainz5
- libmusicbrainz5-devel
- libnbd-devel
- liboauth
- liboauth-devel
- libpfm-static
- libpng12
- libpurple
- libpurple-devel
- libraw1394
- libreport-plugin-mailx
- libreport-plugin-rhtsupport
- libreport-plugin-ureport
- libreport-rhel
- libreport-rhel-bugzilla
- librpmem
- librpmem-debug
- librpmem-devel
- libsass
- libsass-devel
- libselinux-python
- libsqlite3x
- libtalloc-devel
- libtar
- libtdb-devel

- libtevent-devel
- libtpms-devel
- libunwind
- libusal
- libvarlink
- libverto-libevent
- libvirt-admin
- libvirt-bash-completion
- libvirt-daemon-driver-storage-gluster
- libvirt-daemon-driver-storage-iscsi-direct
- libvirt-devel
- libvirt-docs
- libvirt-gconfig
- libvirt-gobject
- libvirt-lock-sanlock
- libvirt-wireshark
- libvmem
- libvmem-debug
- libvmem-devel
- libvmmalloc
- libvmmalloc-debug
- libvmmalloc-devel
- libvncserver
- libwinpr-devel
- libwmf
- libwmf-devel
- libwmf-lite
- libXNVCtrl
- libyami

- log4j12
- log4j12-javadoc
- lohit-malayalam-fonts
- lohit-nepali-fonts
- lorax-composer
- lua-guestfs
- lucene
- lucene-analysis
- lucene-analyzers-smartcn
- lucene-queries
- lucene-queryparser
- lucene-sandbox
- lz4-java
- lz4-java-javadoc
- mailman
- mailx
- make-devel
- malaga
- malaga-suomi-voikko
- marisa
- maven-antrun-plugin
- maven-assembly-plugin
- maven-clean-plugin
- maven-dependency-analyzer
- maven-dependency-plugin
- maven-doxia
- maven-doxia-sitetools
- maven-install-plugin
- maven-invoker

- maven-invoker-plugin
- maven-parent
- maven-plugins-pom
- maven-reporting-api
- maven-reporting-impl
- maven-resolver-api
- maven-resolver-connector-basic
- maven-resolver-impl
- maven-resolver-spi
- maven-resolver-transport-wagon
- maven-resolver-util
- maven-scm
- maven-script-interpreter
- maven-shade-plugin
- maven-shared
- maven-verifier
- maven-wagon-file
- maven-wagon-http
- maven-wagon-http-shared
- maven-wagon-provider-api
- maven2
- meanwhile
- mercurial
- mercurial-hgk
- metis
- metis-devel
- mingw32-bzip2
- mingw32-bzip2-static
- mingw32-cairo

- mingw32-expat
- mingw32-fontconfig
- mingw32-freetype
- mingw32-freetype-static
- mingw32-gstreamer1
- mingw32-harfbuzz
- mingw32-harfbuzz-static
- mingw32-icu
- mingw32-libjpeg-turbo
- mingw32-libjpeg-turbo-static
- mingw32-libpng
- mingw32-libpng-static
- mingw32-libtiff
- mingw32-libtiff-static
- mingw32-openssl
- mingw32-readline
- mingw32-sqlite
- mingw32-sqlite-static
- mingw64-adwaita-icon-theme
- mingw64-bzip2
- mingw64-bzip2-static
- mingw64-cairo
- mingw64-expat
- mingw64-fontconfig
- mingw64-freetype
- mingw64-freetype-static
- mingw64-gstreamer1
- mingw64-harfbuzz
- mingw64-harfbuzz-static

- mingw64-icu
- mingw64-libjpeg-turbo
- mingw64-libjpeg-turbo-static
- mingw64-libpng
- mingw64-libpng-static
- mingw64-libtiff
- mingw64-libtiff-static
- mingw64-nettle
- mingw64-openssl
- mingw64-readline
- mingw64-sqlite
- mingw64-sqlite-static
- modello
- mojo-parent
- mongo-c-driver
- mousetweaks
- mozjs52
- mozjs52-devel
- mozjs60
- mozjs60-devel
- mozvoikko
- msv-javadoc
- msv-manual
- munge-maven-plugin
- mythes-mi
- mythes-ne
- nafees-web-naskh-fonts
- nbd
- nbdkit-devel

- nbdkit-example-plugins
- nbdkit-gzip-plugin
- nbdkit-plugin-python-common
- nbdkit-plugin-vddk
- ncompress
- ncurses-compat-libs
- net-tools
- netcf
- netcf-devel
- netcf-libs
- network-scripts
- network-scripts-ppp
- nkf
- nodejs-devel
- nodejs-packaging
- nss_nis
- nss-pam-ldapd
- objectweb-asm
- objectweb-asm-javadoc
- objectweb-pom
- ocaml-bisect-ppx
- ocaml-camlp4
- ocaml-camlp4-devel
- ocaml-lwt
- ocaml-mmap
- ocaml-ocplib-endian
- ocaml-ounit
- ocaml-result
- ocaml-seq

- opencryptoki-tpmtok
- opencv-contrib
- opencv-core
- opencv-devel
- openhpi
- openhpi-libs
- OpenIPMI-perl
- openssh-cavs
- openssh-ldap
- openssl-ibmpkcs11
- opentest4j
- os-maven-plugin
- pakchois
- pandoc
- paps-libs
- paranamer
- parfait
- parfait-examples
- parfait-javadoc
- pcp-parfait-agent
- pcp-pmda-rpm
- pcp-pmda-vmware
- pcsc-lite-doc
- peripety
- perl-B-Debug
- perl-B-Lint
- perl-Class-Factory-Util
- perl-Class-ISA
- perl-DateTime-Format-HTTP

- perl-DateTime-Format-Mail
- perl-File-CheckTree
- perl-homedir
- perl-libxml-perl
- perl-Locale-Codes
- perl-Mozilla-LDAP
- perl-NKF
- perl-Object-HashBase-tools
- perl-Package-DeprecationManager
- perl-Pod-LaTeX
- perl-Pod-Plainer
- perl-prefork
- perl-String-CRC32
- perl-SUPER
- perl-Sys-Virt
- perl-tests
- perl-YAML-Syck
- phodav
- php-recode
- php-xmlrpc
- pidgin
- pidgin-devel
- pidgin-sipe
- pinentry-emacs
- pinentry-gtk
- pipewire0.2-devel
- pipewire0.2-libs
- platform-python-coverage
- plexus-ant-factory

- plexus-bsh-factory
- plexus-cli
- plexus-component-api
- plexus-component-factories-pom
- plexus-components-pom
- plexus-i18n
- plexus-interactivity
- plexus-pom
- plexus-velocity
- plymouth-plugin-throbgress
- pmreorder
- postgresql-test-rpm-macros
- powermock
- prometheus-jmx-exporter
- prometheus-jmx-exporter-openjdk11
- ptscotch-mpich
- ptscotch-mpich-devel
- ptscotch-mpich-devel-parmetis
- ptscotch-openmpi
- ptscotch-openmpi-devel
- purple-sipe
- pygobject2-doc
- pygtk2
- pygtk2-codegen
- pygtk2-devel
- pygtk2-doc
- python-nose-docs
- python-nss-doc
- python-podman-api

- python-psycopg2-doc
- python-pymongo-doc
- python-redis
- python-schedutils
- python-slip
- python-sqlalchemy-doc
- python-varlink
- python-virtualenv-doc
- python2-backports
- python2-backports-ssl_match_hostname
- python2-bson
- python2-coverage
- python2-docs
- python2-docs-info
- python2-funcsigs
- python2-ipaddress
- python2-mock
- python2-nose
- python2-numpy-doc
- python2-psycopg2-debug
- python2-psycopg2-tests
- python2-pymongo
- python2-pymongo-gridfs
- python2-pytest-mock
- python2-sqlalchemy
- python2-tools
- python2-virtualenv
- python3-bson
- python3-click

- python3-coverage
- python3-cpio
- python3-custodia
- python3-docs
- python3-flask
- python3-gevent
- python3-gobject-base
- python3-hivex
- python3-html5lib
- python3-hypothesis
- python3-ipatests
- python3-itsdangerous
- python3-jwt
- python3-libguestfs
- python3-mock
- python3-networkx-core
- python3-nose
- python3-nss
- python3-openipmi
- python3-pillow
- python3-ptyprocess
- python3-pydbus
- python3-pymongo
- python3-pymongo-gridfs
- python3-pyOpenSSL
- python3-pytoml
- python3-reportlab
- python3-schedutils
- python3-scons

- python3-semantic_version
- python3-slip
- python3-slip-dbus
- python3-sqlalchemy
- python3-syspurpose
- python3-virtualenv
- python3-webencodings
- python3-werkzeug
- python38-asn1crypto
- python38-numpy-doc
- python38-psycopg2-doc
- python38-psycopg2-tests
- python39-numpy-doc
- python39-psycopg2-doc
- python39-psycopg2-tests
- qemu-kvm-block-gluster
- qemu-kvm-block-iscsi
- qemu-kvm-block-ssh
- qemu-kvm-hw-usbredir
- qemu-kvm-device-display-virtio-gpu-gl
- qemu-kvm-device-display-virtio-gpu-pci-gl
- qemu-kvm-device-display-virtio-vga-gl
- qemu-kvm-tests
- qpdf
- qpdf-doc
- qpid-proton
- qrencode
- qrencode-devel
- qrencode-libs

- qt5-qtcanvas3d
- qt5-qtcanvas3d-examples
- rarian
- rarian-compat
- re2c
- recode
- redhat-lsb
- redhat-lsb-core
- redhat-lsb-cxx
- redhat-lsb-desktop
- redhat-lsb-languages
- redhat-lsb-printing
- redhat-lsb-submod-multimedia
- redhat-lsb-submod-security
- redhat-lsb-supplemental
- redhat-lsb-trialuse
- redhat-menus
- redhat-support-lib-python
- redhat-support-tool
- reflections
- regexp
- relaxngDatatype
- rhsm-gtk
- rpm-plugin-prioreset
- rpmemd
- rsyslog-udpspoof
- ruby-hivex
- ruby-libguestfs
- rubygem-abrt

- rubygem-abrt-doc
- rubygem-bson
- rubygem-bson-doc
- rubygem-bundler-doc
- rubygem-mongo
- rubygem-mongo-doc
- rubygem-net-telnet
- rubygem-xmlrpc
- s390utils-cmsfs
- samba-pidl
- samba-test
- samba-test-libs
- samyak-devanagari-fonts
- samyak-fonts-common
- samyak-gujarati-fonts
- samyak-malayalam-fonts
- samyak-odia-fonts
- samyak-tamil-fonts
- sane-frontends
- sanlk-reset
- sat4j
- scala
- scotch
- scotch-devel
- SDL_sound
- selinux-policy-minimum
- sendmail
- sgabios
- sgabios-bin

- shrinkwrap
- sisu-inject
- sisu-mojos
- sisu-plexus
- skkdic
- SLOF
- smc-anjalioldlipi-fonts
- smc-dyuthi-fonts
- smc-fonts-common
- smc-kalyani-fonts
- smc-raghumalayalam-fonts
- smc-suruma-fonts
- softhsm-devel
- sonatype-oss-parent
- sonatype-plugins-parent
- sos-collector
- sparsehash-devel
- spax
- spec-version-maven-plugin
- spice
- spice-client-win-x64
- spice-client-win-x86
- spice-glib
- spice-glib-devel
- spice-gtk
- spice-gtk-tools
- spice-gtk3
- spice-gtk3-devel
- spice-gtk3-vala

- spice-parent
- spice-protocol
- spice-qxl-wddm-dod
- spice-server
- spice-server-devel
- spice-qxl-xddm
- spice-server
- spice-streaming-agent
- spice-vdagent-win-x64
- spice-vdagent-win-x86
- sssd-libwbclient
- star
- stax-ex
- stax2-api
- stringtemplate
- stringtemplate4
- subscription-manager-initial-setup-addon
- subscription-manager-migration
- subscription-manager-migration-data
- subversion-javahl
- SuperLU
- SuperLU-devel
- supermin-devel
- swig
- swig-doc
- swig-gdb
- swtpm-devel
- swtpm-tools-pkcs11
- system-storage-manager

- tcl-brlapi
- testng
- tibetan-machine-uni-fonts
- timedatex
- tpm-quote-tools
- tpm-tools
- tpm-tools-pkcs11
- treelayout
- trousers
- trousers-lib
- tuned-profiles-compat
- tuned-profiles-nfv-host-bin
- tuned-utils-systemtap
- tycho
- uglify-js
- unbound-devel
- univocity-output-tester
- univocity-parsers
- usbguard-notifier
- usbredir-devel
- utf8cpp
- uthash
- velocity
- vinagre
- vino
- virt-dib
- virt-p2v-maker
- vm-dump-metrics-devel
- weld-parent

- wodim
- woodstox-core
- wqy-microhei-fonts
- wqy-unibit-fonts
- xdelta
- xmlgraphics-commons
- xmlstreambuffer
- xinetd
- xorg-x11-apps
- xorg-x11-drv-qxl
- xorg-x11-server-Xspice
- xpp3
- xsane-gimp
- xsom
- xz-java
- xz-java-javadoc
- yajl-devel
- yp-tools
- ypbind
- ypserv

10.21. 非推奨のデバイスおよび非保守のデバイス

このセクションは、

- RHEL 8 のライフサイクルが終了するまで継続してサポートされるデバイス (ドライバー、アダプター) を説明しますが、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いため、新たに実装することは推奨されません。記載以外のデバイスのサポートは変更しません。これは **非推奨** デバイスです。
- RHEL 8 では入手可能ですが、ルーチンベースでのテストや更新は行われていません。Red Hat は、独自の判断でセキュリティーバグなどの深刻なバグを修正する場合があります。このようなデバイスは実稼働環境では使用しなくなり、次のメジャーリリースでは無効になる可能性が高くなります。これは **未管理** デバイスです。

PCI デバイス ID は、**vendor:device:subvendor:subdevice** の形式です。デバイス ID が記載されていない場合は、対応するドライバーに関連するすべてのデバイスが非推奨になっています。ご使用の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。

表10.1 非推奨のデバイス

デバイス ID	ドライバー	デバイス名
	bnx2	QLogic BCM5706/5708/5709/5716 Driver
	hpsa	Hewlett-Packard Company: Smart アレイコントローラー
0x10df:0x0724	lpfc	Emulex Corporation: OneConnect FCoE Initiator (Skyhawk)
0x10df:0xe200	lpfc	Emulex Corporation: LPe15000/LPe16000 Series 8Gb/16Gb Fibre Channel Adapter
0x10df:0xf011	lpfc	Emulex Corporation: Saturn: LightPulse Fibre Channel Host Adapter
0x10df:0xf015	lpfc	Emulex Corporation: Saturn: LightPulse Fibre Channel Host Adapter
0x10df:0xf100	lpfc	Emulex Corporation: LPe12000 Series 8Gb Fibre Channel Adapter
0x10df:0xfc40	lpfc	Emulex Corporation: Saturn-X: LightPulse Fibre Channel Host Adapter
0x10df:0xe220	be2net	Emulex Corporation: OneConnect NIC (Lancer)
0x1000:0x005b	megaraid_sas	Broadcom / LSI: MegaRAID SAS 2208 [Thunderbolt]
0x1000:0x006E	mpt3sas	Broadcom / LSI: SAS2308 PCI-Express Fusion-MPT SAS-2
0x1000:0x0080	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0081	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0082	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0083	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0084	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0085	mpt3sas	Broadcom / LSI: SAS2208 PCI-Express Fusion-MPT SAS-2
0x1000:0x0086	mpt3sas	Broadcom / LSI: SAS2308 PCI-Express Fusion-MPT SAS-2
0x1000:0x0087	mpt3sas	Broadcom / LSI: SAS2308 PCI-Express Fusion-MPT SAS-2

デバイス ID	ドライバー	デバイス名
	myri10ge	Myricom 10G driver (10GbE)
	netxen_nic	QLogic/NetXen (1/10) GbE Intelligent Ethernet Driver
0x1077:0x2031	qla2xxx	QLogic Corp.: ISP8324-based 16Gb Fibre Channel to PCI Express Adapter
0x1077:0x2532	qla2xxx	QLogic Corp.: ISP2532-based 8Gb Fibre Channel to PCI Express HBA
0x1077:0x8031	qla2xxx	QLogic Corp.: 8300 Series 10GbE Converged Network Adapter (FCoE)
	qla3xxx	QLogic ISP3XXX ネットワークドライバー v2.03.00-k5
0x1924:0x0803	sfc	Solarflare Communications: SFC9020 10G Ethernet Controller
0x1924:0x0813	sfc	Solarflare Communications: SFL9021 10GBASE-T Ethernet Controller
	Soft-RoCE (rdma_rxe)	
	HNS-RoCE	HNS GE/10GE/25GE/50GE/100GE RDMA Network Controller
	liquidio	Cavium LiquidIO Intelligent Server Adapter Driver
	liquidio_vf	Cavium LiquidIO Intelligent Server Adapter Virtual Function Driver

表10.2 未管理デバイス

デバイス ID	ドライバー	デバイス名
	e1000	Intel® PRO/1000 ネットワークドライバー
	mptbase	Fusion MPT SAS ホストドライバー

デバイス ID	ドライバー	デバイス名
	mptsas	Fusion MPT SAS ホストドライバー
	mptscsih	Fusion MPT SCSI ホストドライバー
	mptspi	Fusion MPT SAS ホストドライバー
0x1000:0x0071 [a]	megaraid_sas	Broadcom / LSI: MR SAS HBA 2004
0x1000:0x0073 [a]	megaraid_sas	Broadcom / LSI: MegaRAID SAS 2008 [Falcon]
0x1000:0x0079 [a]	megaraid_sas	Broadcom / LSI: MegaRAID SAS 2108 [Liberator]
	nvmet_tcp	NVMe/TCP ターゲットドライバー

[a] RHEL 8.0 で無効になり、顧客の要求により RHEL 8.4 で再度有効になりました。

第11章 既知の問題

このパートでは、Red Hat Enterprise Linux 8.8 の既知の問題について説明します。

11.1. インストーラーおよびイメージの作成

LPAR およびセキュアブートが有効になっている IBM Power 10 システムでのインストールが失敗します

RHEL インストーラーは、IBM Power 10 システムの静的キーセキュアブートと統合されていません。したがって、セキュアブートオプションを使用して論理パーティション (LPAR) を有効にすると、インストールに失敗し、**Unable to proceed with RHEL-x.x Installation** というエラーが表示されます。

この問題を回避するには、セキュアブートを有効にせずに RHEL をインストールします。システムを起動したら、以下を行います。

1. **dd** コマンドを使用して、署名されたカーネルを PReP パーティションにコピーします。
2. システムを再起動し、セキュアブートを有効にします。

ファームウェアがブートローダーとカーネルを検証すると、システムは正常に起動します。

詳細については、https://www.ibm.com/support/pages/node/6528884 を参照してください。

Bugzilla:2025814

Anaconda がアプリケーションとして実行されているシステムでの予期しない SELinux ポリシー

Anaconda がすでにインストールされているシステムでアプリケーションとして実行されている場合 (たとえば、**–image** anaconda オプションを使用してイメージファイルに別のインストールを実行する場合)、システムはインストール中に SELinux のタイプと属性を変更することを禁止されていません。そのため、SELinux ポリシーの特定の要素は、Anaconda が実行されているシステムで変更される可能性があります。この問題を回避するには、実稼働システムで Anaconda を実行せず、一時的な仮想マシンで実行します。そうすることで、実稼働システムの SELinux ポリシーは変更されません。**boot.iso** や **dvd.iso** からのインストールなど、システムインストールプロセスの一部として anaconda を実行しても、この問題の影響は受けません。

Bugzilla:2050140

キックスタートコマンドの auth および authconfig で AppStream リポジトリーが必要になる

インストール中に、キックスタートコマンドの **auth** および **authconfig** で **authselect-compat** パッケージが必要になります。**auth** または **authconfig** を使用したときに、このパッケージがないとインストールに失敗します。ただし、設計上、 **authselect-compat** パッケージは AppStream リポジトリーでしか利用できません。

この問題を回避するには、BaseOS リポジトリーおよび AppStream リポジトリーがインストーラーで利用できることを確認するか、インストール中にキックスタートコマンドの **authselect** コマンドを使用します。

Bugzilla:1640697

reboot --kexec コマンドおよび inst.kexec コマンドが、予測可能なシステム状態を提供しない

キックスタートコマンド **reboot --kexec** またはカーネル起動パラメーター **inst.kexec** で RHEL インストールを実行しても、システムの状態が完全な再起動と同じになるわけではありません。これにより、

システムを再起動せずにインストール済みのシステムに切り替えると、予期しない結果が発生することがあります。

kexec 機能は非推奨になり、Red Hat Enterprise Linux の今後のリリースで削除されることに注意してください。

Bugzilla:1697896

USB CD-ROM ドライブが Anaconda のインストールソースとして利用できない

USB CD-ROM ドライブがソースで、キックスタート **ignoredisk --only-use=** コマンドを指定すると、インストールに失敗します。この場合、Anaconda はこのソースディスクを見つけ、使用できません。

この問題を回避するには、**harddrive --partition=sdX --dir=/** コマンドを使用して USB CD-ROM ドライブからインストールします。その結果、インストールは失敗しなくなりました。

Bugzilla:1914955

インストールプログラムでは、ネットワークアクセスがデフォルトで有効になっていない

一部のインストール機能、たとえば、コンテンツ配信ネットワーク (CDN) を使用したシステムの登録、NTP サーバーサポート、およびネットワークインストールソースなどには、ネットワークアクセスが必要です。ただし、ネットワークアクセスはデフォルトでは有効になっていません。そのためこの機能は、ネットワークアクセスが有効になるまで使用できません。

この問題を回避するには、インストールの開始時にネットワークアクセスを有効にする起動オプション **ip=dhcp** を追加します。オプションで、起動オプションを使用して、ネットワーク上にあるキックスタートファイルまたはリポジトリーを渡しても、問題が解決されます。結果として、ネットワークベースのインストール機能を使用できます。

Bugzilla:1757877

iso9660 ファイルシステムで、ハードドライブがパーティション分割されたインストールが失敗する

ハードドライブが **iso9660** ファイルシステムでパーティションが設定されているシステムには、RHEL をインストールできません。これは、**iso9660** ファイルシステムパーティションを含むハードディスクを無視するように設定されている、更新されたインストールコードが原因です。これは、RHEL が DVD を使用せずにインストールされている場合でも発生します。

この問題を回避するには、インストールの開始前に、キックスタートファイルに次のスクリプトを追加して、ディスクをフォーマットします。

メモ: 回避策を実行する前に、ディスクで利用可能なデータのバックアップを作成します。**wipefs** は、ディスク内の全データをフォーマットします。

```
%pre
wipefs -a /dev/sda
%end
```

その結果、インストールでエラーが発生することなく、想定どおりに機能します。

Bugzilla:1929105

HASH MMU モードの IBM 電源システムが、メモリー割り当ての障害で起動できない

HASH メモリー割り当てユニット (MMU) モードの IBM Power Systems は、最大 192 コアの **kdump** に対応します。そのため、**kdump** が 192 コア以上で有効になっていると、メモリー割り当て失敗が原因

でシステムの起動が失敗します。この制限は、**HASH MMU** モードの起動初期段階での RMA メモリーの割り当てによるものです。この問題を回避するには、**kdump** を使用する代わりに、**fadump** を有効にした **Radix MMU** モードを使用します。

Bugzilla:2028361

rpm-ostree ペイロードをインストールすると、RHEL for Edge インストーラーイメージがマウントポイントの作成に失敗する

RHEL for Edge インストーラーイメージなどで使用される **rpm-ostree** ペイロードをデプロイする場合、インストーラーはカスタムパーティションの一部のマウントポイントを適切に作成しません。その結果、インストールは以下のエラーで中止されます。

```
The command 'mount --bind /mnt/sysimage/data /mnt/sysroot/data' exited with the code 32.
```

この問題を回避するには、以下を実行します。

- 自動パーティション設定スキームを使用し、手動でマウントポイントを追加しないでください。
- マウントポイントは、**/var** ディレクトリー内のみに手動で割り当てます。たとえば、**/var/my-mount-point** や、/、**/boot**、**/var** などの標準ディレクトリーです。

その結果、インストールプロセスは正常に終了します。

Bugzilla:2126506

11.2. サブスクリプションの管理

syspurpose addons が subscription-manager attach --auto 出力に影響しない

Red Hat Enterprise Linux 8 では、**syspurpose** コマンドラインツールの 4 つの属性 (**role**、**usage**、**service_level_agreement**、および **addons**) が追加されました。現在、**role**、**usage**、および **service_level_agreement** のみが、**subscription-manager attach --auto** コマンドの実行の出力に影響します。**addons** 引数に値を設定しても、自動登録されたサブスクリプションには影響がありません。

Bugzilla:1687900

11.3. ソフトウェア管理

cr_compress_file_with_stat() がメモリーリークを引き起こす可能性がある

createrepo_c C ライブラリーには API **cr_compress_file_with_stat()** 関数があります。この関数は、**char **dst** を 2 番目のパラメーターとして宣言します。他のパラメーターによって、**cr_compress_file_with_stat()** は、入力パラメーターとして **dst** を使用するか、割り当てられた文字列を返すために使用します。**dst** の内容をいつ解放するかユーザーに通知しないため、この予測できない動作いよりメモリーリークが発生する可能性があります。

この問題を回避するために、**dst** パラメーターを入力としてのみ使用する新しい API **cr_compress_file_with_stat_v2** 関数が追加されました。これは **char *dst** として宣言されます。これにより、メモリーリークが回避されます。

cr_compress_file_with_stat_v2 関数は一時的で、RHEL 8 のみに存在することに注意してください。後で、**cr_compress_file_with_stat()** が代わりに修正されます。

Bugzilla:1973588

スクリプトレットが失敗したときに成功したと報告された YUM トランザクション

RPM バージョン 4.6 以降、インストール後のスクリプトレットは、トランザクションに致命的な影響を与えることなく失敗することが許可されています。この動作は YUM まで伝播します。これにより、スクリプトレットが作成され、パッケージトランザクション全体が成功したと報告されているときに失敗することがあります。

現在利用できる回避策はありません。

これは、RPM と YUM の間で一貫性を保つことが期待される動作であることに注意してください。スクリプトレットの問題は、パッケージレベルで対処する必要があります。

Bugzilla:1986657

11.4. シェルおよびコマンドラインツール

ipmitool は特定のサーバープラットフォームと互換性がありません

ipmitool ユーティリティーは、Intelligent Platform Management Interface (IPMI) をサポートするデバイスの監視、設定、および管理に役立ちます。現在のバージョンの **ipmitool** は、以前の Cipher Suite 3 の代わりに Cipher Suite 17 をデフォルトで使用します。その結果、**ipmitool** は、ネゴシエーション中に Cipher Suite 17 のサポートを発表しましたが、実際にはこの暗号スイートをサポートしていない特定のベアメタルノードとの通信に失敗します。その結果、**ipmitool** は、**no matching cipher suite** エラーメッセージで異常終了します。

詳細は、関連する ナレッジベースの記事 を参照してください。

この問題を解決するには、ベースボード管理コントローラー (BMC) ファームウェアを更新して、Cipher Suite 17 を使用します。

オプションで、BMC ファームウェアの更新が利用できない場合は、**ipmitool** に特定の暗号スイートを強制的に使用させることで、この問題を回避できます。**ipmitool** で管理タスクを呼び出す場合は、使用する暗号スイートの **番号** とともに **ipmitool** コマンドに **-C** オプションを追加します。以下の例を参照してください。

```
# ipmitool -I lanplus -H myserver.example.com -P mypass -C 3 chassis power status
```

Bugzilla:1873614

復元にクリーンディスクを使用しないと、ReaR がボリュームグループの再作成に失敗する

既存のデータを含むディスクに復元する場合、ReaR は復元の実行に失敗します。

この問題を回避するには、ディスクが以前に使用されていた場合、復元する前にディスクを手動でワイプします。レスキュー環境でディスクをワイプするには、**rear recover** コマンドを実行する前に、次のいずれかのコマンドを使用します。

- ディスクを上書きする **dd** コマンド。
- 使用可能なすべてのメタデータを消去するには、**-a** フラグを指定した **wipefs** コマンド。

/dev/sda ディスクからメタデータをワイプする次の例を参照してください。

```
# wipefs -a /dev/sda[1-9] /dev/sda
```

このコマンドは、最初に **/dev/sda** のパーティションからメタデータをワイプし、次にパーティションテーブル自体をワイプします。

Bugzilla:1925531

coreutils は、誤解を招く EPERM エラーコードを報告することがあります。

statx() システムコールを使用して、GNU コアユーティリティー (**coreutils**) が起動しました。**seccomp** フィルターが、不明なシステムコールに対して EPERM エラーコードを返す場合、EPERM は動作中の **statx()** の syscall が返す実際の **Operation not permitted** エラーと区別できないため、**coreutils** は、誤解を招く EPERM エラーコードを報告します。

この問題を回避するには、**seccomp** フィルターを更新して、**statx()** の syscall を許可するか、不明の syscall の ENOSYS エラーコードを返すようにします。

Bugzilla:2030661

11.5. インフラストラクチャーサービス

FIPS モードの Postfix TLS フィンガープリントアルゴリズムを SHA-256 に変更する必要があります。

RHEL 8 のデフォルトでは、**postfix** は後方互換性に TLS を使用する MD5 フィンガープリントを使用します。ただし、FIPS モードでは、MD5 ハッシュ関数が利用できないため、デフォルトの postfix 設定で TLS が誤って機能する可能性があります。この問題を回避するには、postfix 設定ファイルのハッシュ関数を SHA-256 に変更する必要があります。

詳細は、関連するナレッジベースの記事 Fix postfix TLS in the FIPS mode by switch to SHA-256 instead of the MD5 を参照してください。

Bugzilla:1711885

brltty パッケージは multilib 対応ではない

brltty パッケージの 32 ビット版と 64 ビット版の両方をインストールすることはできません。32 ビット版 (**brltty.i686**) または 64 ビット版 (**brltty.x86_64**) いずれかのパッケージをインストールすることができます。64 ビット版を推奨します。

Bugzilla:2008197

11.6. セキュリティー

tangd-keygen は デフォルト以外の umask を 正しく処理しません。

tangd-keygen スクリプトは、生成されたキーファイルのファイル権限を変更しません。その結果、他のユーザーへのキーの読み取りを防止するデフォルトのユーザーファイル作成モードマスク (**umask**) が設定されているシステムでは、**tang-show-keys** コマンドはキーを表示する代わりにエラーメッセージ **Internal Error 500** を返します。

この問題を回避するには、**chmod o+r *.jwk** コマンドを使用して、**/var/db/tang** ディレクトリー内のファイルのアクセス許可を変更します。

Bugzilla:2188743

sshd -T が、暗号、MAC、および KeX アルゴリズムに関する不正確な情報を提供する

sshd -T コマンドの出力には、システム全体の暗号化ポリシー設定や、**/etc/sysconfig/sshd** 内の環境

ファイルから取得でき、**sshd** コマンドの引数として適用されるその他のオプションは含まれていません。これは、アップストリームの OpenSSH プロジェクトが RHEL8 で Red-Hat が提供する暗号化のデフォルトをサポートするための Include ディレクティブをサポートしていなかったために発生します。暗号化ポリシーは、**EnvironmentFile** を使用してサービスを開始するときに、**sshd.service** ユニットの **sshd** 実行可能ファイルにコマンドライン引数として適用されます。この問題を回避するには、**sshd -T $CRYPTO_POLICY** のように、環境ファイルで **source** コマンドを使用し、暗号化ポリシーを引数として **sshd** コマンドに渡します。詳細については、暗号、MAC、または KeX アルゴリズムが **sshd -T** とは異なり、現在の暗号ポリシーレベルで提供されるものとは異なるを参照してください。その結果、**sshd -T** からの出力は、現在設定されている暗号化ポリシーと一致します。

Bugzilla:2044354

インストール中にシステムを強化すると、RHV ハイパーバイザーが正しく動作しないことがある

Red Hat Virtualization Hypervisor (RHV-H) をインストールし、Red Hat Enterprise Linux 8 STIG プロファイルを適用すると、OSCAP Anaconda Add-on が RVH-H ではなく RHEL としてシステムを強化し、RHV-H の必須パッケージを削除する場合があります。その結果、RHV ハイパーバイザーが機能しない場合があります。この問題を回避するには、プロファイルの強化を適用せずに RHV-H システムをインストールし、インストールが完了したら、OpenSCAP を使用してプロファイルを適用します。その結果、RHV ハイパーバイザーは正しく動作します。

Bugzilla:2075508

CVE OVAL フィードが圧縮形式のみになり、データストリームが SCAP 1.3 標準に準拠していない

Red Hat は、CVE OVAL フィードを bzip2 圧縮形式で提供しています。これらは XML ファイル形式では利用できなくなりました。圧縮されたコンテンツの参照は Security Content Automation Protocol (SCAP) 1.3 仕様で標準化されていないため、サードパーティーの SCAP スキャナーでは、フィードを使用するルールのスキャンで問題が発生する可能性があります。

Bugzilla:2028428

特定の Rsyslog 優先度文字列が正しく機能しない

imtcp に GnuTLS 優先度文字列を設定して、完成していない暗号化をきめ細かく制御できるようになりました。そのため、次の優先度文字列は、Rsyslog リモートログアプリケーションでは正しく機能しません。

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+DHE-RSA:+AES-256-GCM:+SIGN-RSA-SHA384:+COMP-ALL:+GROUP-ALL
```

この問題を回避するには、正しく機能する優先度文字列のみを使用します。

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+ECDHE-RSA:+AES-128-CBC:+SIGN-RSA-SHA1:+COMP-ALL:+GROUP-ALL
```

したがって、現在の設定は、正しく機能する文字列に限定する必要があります。

Bugzilla:1679512

CIS Server プロファイルを使用すると、Server with GUI および Workstation をインストールできない

CIS Server Level 1 および Level 2 のセキュリティープロファイルは、**Server with GUI** および **Workstation** ソフトウェアの選択と互換性がありません。そのため、**Server with GUI** ソフトウェアの

選択と CIS プロファイルを使用して RHEL 8 をインストールすることはできません。CIS Server Level 1 または Level 2 プロファイルと、これらのソフトウェアの選択のいずれかを使用したインストール試行では、エラーメッセージが生成されます。

> package xorg-x11-server-common has been added to the list of excluded packages, but it can't be removed from the current software selection without breaking the installation.

CIS ベンチマークに従ってシステムを **Server with GUI** または **Workstation** のソフトウェア選択に￥合わせる必要がある場合は、代わりに CIS Workstation Level 1 または Level 2 プロファイルを使用してください。

Bugzilla:1843932

RHEL 8 のキックスタートが、com_redhat_oscap の代わりに org_fedora_oscap を使用

キックスタートは、**com_redhat_oscap** ではなく、**org_fedora_oscap** として Open Security Content Automation Protocol (OSCAP) Anaconda アドオンを参照します。これが、混乱を招く可能性があります。これは、Red Hat Enterprise Linux 7 との互換性を維持するために必要です。

Bugzilla:1665082

libvirt が xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_forwarding をオーバーライドする

libvirt 仮想化フレームワークは、**route** または **nat** の転送モードを持つ仮想ネットワークが起動するたびに、IPv4 転送を有効にします。これにより、**xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_forwarding** ルールによる設定がオーバーライドされ、後続のコンプライアンススキャンでは、このルールを評価するときに **fail** という結果が報告されます。

この問題を回避するには、次のいずれかのシナリオを適用します。

- シナリオで必要がない場合は、**libvirt** パッケージをアンインストールします。
- **libvirt** によって作成された仮想ネットワークの転送モードを変更します。
- プロファイルを調整して、**xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_forwarding** ルールを削除します。

Bugzilla:2118758

FIPS モードの OpenSSL が、特定の D-H パラメーターのみを受け入れます。

FIPS モードでは、OpenSSL を使用する TLS クライアントは **bad dh value** エラーを返し、手動で生成されたパラメーターを使用するようにサーバーへの TLS 接続を中止します。これは、FIPS 140-2 に準拠するよう設定されている場合、OpenSSL が NIST SP 800-56A rev3 付録 D (RFC 3526 で定義されたグループ 14、15、16、17、18、および RFC 7919 で定義されたグループ) に準拠した Diffie-Hellman パラメーターでのみ機能するためです。また、OpenSSL を使用するサーバーは、その他のパラメーターをすべて無視し、代わりに同様のサイズの既知のパラメーターを選択します。この問題を回避するには、準拠するグループのみを使用します。

Bugzilla:1810911

crypto-policies が Camellia 暗号を誤って許可する。

RHEL 8 システム全体の暗号化ポリシーでは、製品ドキュメントで説明されているように、すべてのポリシーレベルで Camellia 暗号を無効にする必要があります。ただし、Kerberos プロトコルでは、デフォルトでこの Camellia 暗号が有効になります。

この問題を回避するには、**NO-CAMELLIA** サブポリシーを適用します。

```
# update-crypto-policies --set DEFAULT:NO-CAMELLIA
```

これまでに上記のコマンドで、**DEFAULT** から切り替えたことがある場合は、**DEFAULT** を暗号化レベルの名前に置き換えます。

その結果、この回避策を使用して Cemellia 暗号を無効にしている場合に限り、システム全体の暗号化ポリシーを使用する全ポリシーで、この暗号化を適切に拒否できます。

Bugzilla:1919155

OpenSC が CardOS V5.3 カードオブジェクトを正しく検出しない可能性がある

OpenSC ツールキットは、CardOS V5.3 システムを使用しているスマートカードのシリアル番号を正しく検出しません。その結果、**pkcs11-tool** ユーティリティーはカードオブジェクトをリストしない可能性があります。

この問題を回避するには、**/etc/opensc.conf** ファイルで`use_file_caching = false` オプションを設定してファイルキャッシュをオフにします。

Bugzilla:2176973

OpenSC pkcs15-init によるスマートカードのプロビジョニングプロセスが適切に動作しない

file_caching オプションは、デフォルトの OpenSC 設定で有効になっているため、キャッシュ機能は **pkcs15-init** ツールから一部のコマンドを適切に処理しません。したがって、OpenSC を使用したスマートカードのプロビジョニングプロセスは失敗します。

この問題を回避するには、以下のスニペットを **/etc/opensc.conf** ファイルに追加します。

```
app pkcs15-init {
        framework pkcs15 {
                use_file_caching = false;
        }
}
```

pkcs15-init を使用したスマートカードのプロビジョニングは、前述の回避策を適用している場合に限り機能します。

Bugzilla:1947025

SHA-1 署名を使用するサーバーへの接続が GnuTLS で動作しない

証明書の SHA-1 署名は、GuTLS セキュアな通信ライブラリーにより、セキュアでないものとして拒否されます。したがって、TLS のバックエンドとして GnuTLS を使用するアプリケーションは、このような証明書を提供するピアへの TLS 接続を確立することができません。この動作は、その他のシステム暗号化ライブラリーと一貫性がありません。

この問題を回避するには、サーバーをアップグレードして、SHA-256 または強力なハッシュを使用して署名した証明書を使用するか、LEGACY ポリシーに切り替えます。

Bugzilla:1628553

libselinux-python は、そのモジュールからのみ利用可能

libselinux-python パッケージには、SELinux アプリケーション開発用の Python 2 バインディングのみが含まれ、後方互換性に使用されます。このため、**yum install libselinux-python** コマンドを使用すると、デフォルトの RHEL 8 リポジトリーで **libselinux-python** コマンドを利用できなくなりました。

この問題を回避するには、**libselinux-python** モジュールおよび **python27** モジュールの両方を有効にし、以下のコマンドで **libselinux-python** パッケージとその依存関係をインストールします。

```
# yum module enable libselinux-python
# yum install libselinux-python
```

または、1 つのコマンドでインストールプロファイルを使用して **libselinux-python** をインストールします。

```
# yum module install libselinux-python:2.8/common
```

これにより、各モジュールを使用して **libselinux-python** をインストールできます。

Bugzilla:1666328

udica は、--env container=podman で開始したときにのみ UBI 8 コンテナーを処理します。

Red Hat Universal Base Image 8 (UBI 8) コンテナーは、**podman** の値ではなく、**コンテナー** 環境変数を **oci** 値に設定します。これにより、**udica** ツールがコンテナー JavaScript Object Notation (JSON) ファイルを分析しなくなります。

この問題を回避するには、**--env container=podman** パラメーターを指定して、**podman** コマンドで UBI 8 コンテナーを起動します。そのため、**udica** は、上記の回避策を使用している場合に限り、UBI 8 コンテナーの SELinux ポリシーを生成することができます。

Bugzilla:1763210

デフォルトのロギング設定がパフォーマンスに与える悪影響

デフォルトのログ環境設定は、メモリーを 4 GB 以上使用する可能性があり、**rsyslog** で **systemd-journald** を実行している場合は、速度制限値の調整が複雑になります。

詳細は、ナレッジベースの記事 Negative effects of the RHEL default logging setup on performance and their mitigations を参照してください。

Jira:RHELPLAN-10431

/etc/selinux/config の SELINUX=disabled が正常に動作しません。

/etc/selinux/config で **SELINUX=disabled** オプションを使用して SELinux を無効にすると、カーネルが SELinux を有効にして起動し、その後のブートプロセスで無効化モードに切り替わります。これにより、メモリーリークが生じる可能性があります。

この問題を回避するには、SELinux を完全に無効にする必要がある場合に SELinux の使用 の システムの起動時に SELinux モードの変更 で説明されているように、**selinux=0** パラメーターをカーネルコマンドラインに追加して SELinux を無効にすることが推奨されます。

Jira:RHELPLAN-34199

IKE over TCP 接続がカスタム TCP ポートで機能しない

tcp-remoteport Libreswan 設定オプションが適切に動作しません。したがって、デフォルト以外の TCP ポートを指定する必要があるシナリオでは、IKE over TCP 接続を確立することができません。

Bugzilla:1989050

scap-security-guide がアイドルセッションの終了を設定できない

sshd_set_idle_timeout ルールはデータストリームにまだ存在しますが、**sshd** を設定するアイドルセッションタイムアウトの以前の方法は使用できなくなりました。したがって、ルールは **applicable** としてマークされるため、何も強化できません。**systemd** (Logind) など、アイドルセッションの終了を設定する他の方法も使用できません。そのため、**scap-security-guide** は、一定時間が経過した後にアイドルセッションを確実に切断するようにシステムを設定できません。

この問題は、次のいずれかの方法で回避できます。これにより、セキュリティー要件を満たせる可能性があります。

- **accounts_tmout** ルールを設定します。ただし、この変数は **exec** コマンドを使用してオーバーライドできます。
- **configure_tmux_lock_after_time** ルールと **configure_bashrc_exec_tmux** ルールを設定します。これには、**tmux** パッケージをインストールする必要があります。
- 適切な SCAP ルールとともに **systemd** 機能がすでに実装されている RHEL 8.7 以降にアップグレードします。

Bugzilla:2167373

OSCAP Anaconda アドオンは、グラフィカルインストールで調整されたプロファイルをフェッチしません。

OSCAP Anaconda アドオンには、RHEL グラフィカルインストールでセキュリティープロファイルの調整を選択または選択解除するオプションがありません。RHEL 8.8 以降、アドオンはアーカイブまたは RPM パッケージからインストールするときにデフォルトで調整を考慮しません。その結果、インストールでは、OSCAP に合わせたプロファイルを取得する代わりに、次のエラーメッセージが表示されます。

```
There was an unexpected problem with the supplied content.
```

この問題を回避するには、キックスタートファイルの **%addon org_fedora_oscap** セクションにパスを指定する必要があります。次に例を示します。

```
xccdf-path = /usr/share/xml/scap/sc_tailoring/ds-combined.xml
tailoring-path = /usr/share/xml/scap/sc_tailoring/tailoring-xccdf.xml
```

その結果、OSCAP 調整プロファイルのグラフィカルインストールは、対応するキックスタート仕様のみで使用できます。

Bugzilla:2165948

スマートカードリーダーを取り外したときに自動画面ロックが機能しない

opensc パッケージが、USB スマートカードリーダーの取り外しを誤って処理します。したがって、スマートカードを取り外したときに画面をロックするように GNOME ディスプレイマネージャー (GDM) が設定されている場合でも、システムはロック解除されたままになります。さらに、USB リーダーを再接続してからスマートカードを取り外した後も画面はロックされません。

この問題を回避するには、次のいずれかのアクションを実行します。

- スマートカードリーダーではなく、常にスマートカードのみを取り外します。
- リーダーとカードを 1 つのパッケージに統合するハードウェアトークンを使用する場合は、RHEL 9 にアップグレードします。

Bugzilla:2097048

OpenSCAP のメモリー消費の問題

メモリーが限られているシステムでは、OpenSCAP スキャナが途中で終了するか、結果ファイルが生成されない可能性があります。この問題を回避するには、スキャンプロファイルをカスタマイズして、/ ファイルシステム全体の再帰を含むルールの選択を解除します。

- **rpm_verify_hashes**
- **rpm_verify_permissions**
- **rpm_verify_ownership**
- **file_permissions_unauthorized_world_writable**
- **no_files_unowned_by_user**
- **dir_perms_world_writable_system_owned**
- **file_permissions_unauthorized_suid**
- **file_permissions_unauthorized_sgid**
- **file_permissions_ungroupowned**
- **dir_perms_world_writable_sticky_bits**

詳細とその他の回避策については、関連する ナレッジベースの記事 を参照してください。

Bugzilla:2161499

キックスタートインストール時のサービス関連のルールの修正が失敗する場合があります。

キックスタートのインストール時に、OpenSCAP ユーティリティーで、サービス **enable** または **disable** 状態の修正が必要でないことが誤って表示されることがあります。これにより、OpenSCAP が、インストール済みシステムのサービスを非準拠状態に設定する可能性があります。回避策として、キックスタートインストール後にシステムをスキャンして修復できます。これにより、サービス関連の問題が修正されます。

Bugzilla:1834716

11.7. ネットワーク

IPv6_rpfilter オプションが有効になっているシステムでネットワークスループットが低下

firewalld.conf ファイルで **IPv6_rpfilter** オプションが有効になっているシステムでは、100 Gbps リンクなどの高いトラフィックシナリオの場合、現時点でパフォーマンスは最適ではなくネットワークスループットが低下します。この問題を回避するには、**IPv6_rpfilter** オプションを無効にします。これを行うには、**/etc/firewalld/firewalld.conf** ファイルに次の行を追加します。

```
IPv6_rpfilter=no
```

その結果、システムはパフォーマンスが向上しますが、同時にセキュリティーは低下します。

Bugzilla:1871860

11.8. カーネル

カーネル ACPI ドライバーは、PCIe ECAM メモリーリージョンにアクセスできないことを報告します。

ファームウェアが提供する Advanced Configuration and Power Interface (ACPI) テーブルは、PCI バスデバイスの現在のリソース設定 (_CRS) メソッドにおいて PCI バス上のメモリーリージョンを定義しません。したがって、システムの起動時に以下の警告メッセージが表示されます。

```
[    2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x30000000-0x31ffffff] not reserved in ACPI namespace
[    2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31ffffff] for [bus 00-1f]
```

ただし、カーネルは依然として **0x30000000-0x31ffffff** メモリーリージョンにアクセスできます。また、そのメモリーリージョンを PCI Enhanced Configuration Access Mechanism (ECAM) に適切に割り当てることができます。以下の出力で 256 バイトオフセットで PCIe 設定領域にアクセスして、PCI ECAM が正常に機能することを確認できます。

```
03:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN720 NVMe SSD (prog-if 02 [NVM Express])
 ...
        Capabilities: [900 v1] L1 PM Substates
                L1SubCap: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2+ ASPM_L1.1- L1_PM_Substates+
                          PortCommonModeRestoreTime=255us PortTPowerOnTime=10us
                L1SubCtl1: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2- ASPM_L1.1-
                           T_CommonMode=0us LTR1.2_Threshold=0ns
                L1SubCtl2: T_PwrOn=10us
```

これにより、警告メッセージを無視します。

問題の詳細は、Firmware Bug: ECAM area **mem 0x30000000-0x31ffffff** not reserved in ACPI namespace" appears during system boot を参照してください。

Bugzilla:1868526

tuned-adm profile powersave コマンドを使用すると、システムが応答しなくなる

tuned-adm profile powersave コマンドを実行すると、古い Thunderx (CN88xx) プロセッサーを持つ Penguin Valkyrie 2000 2 ソケットシステムが応答しなくなります。これにより、作業を再開するためシステムを再起動することになります。この問題を回避するには、システムが上記の仕様と一致する場合には **powersave** プロファイルの使用を避けてください。

Bugzilla:1609288

HP NMI ウォッチドッグが常にクラッシュダンプを生成しない

特定に場合において、HP NMI ウォッチドッグの **hpwdt** ドライバーは、マスク不可割り込み (NMI) が **perfmon** ドライバーにより使用されたため、HPE ウォッチドッグタイマーが生成した NMI を要求できません。

欠落している NMI は、以下の 2 つの条件のいずれかによって開始されます。

1. Integrated Lights-Out (iLO) サーバー管理ソフトウェアの **NMI 生成** ボタン。このボタンはユーザーがトリガーします。

2. **hpwdt** ウォッチドッグ。デフォルトでは、有効期限により NMI がサーバーに送信されます。

通常、両方のシーケンスは、システムが応答しない場合に発生します。通常、これらの状況の NMI ハンドラーは **kernel panic()** 関数を呼び出します。また、設定されていれば、**kdump** サービスが **vmcore** ファイルを生成します。

ただし、NMI が見つからないため、**kernel panic()** は呼び出されず、**vmcore** が収集されません。

最初のケース (1.) でシステムが応答しない場合は、その状態のままになります。このシナリオを回避するには、仮想 **電源** ボタンを使用してサーバーをリセットするか、電源を切って入れ直します。

2 つ目のケース (2.) では、欠落している NMI が Automated System Recovery (ASR) からのリセットの後 9 秒後に続きます。

HPE Gen9 Server ラインでは、1 桁台の割合でこの問題が発生します。Gen10 の周波数がさらに小さくなる。

Bugzilla:1602962

同一の crash 拡張機能を再読み込みすると、セグメンテーションフォルトが発生する場合がある

読み込み済みのクラッシュ拡張ファイルのコピーを読み込むと、セグメンテーションフォルトが発生する場合があります。現在、crash ユーティリティーは、元のファイルが読み込まれているかどうかを検出します。その結果、crash ユーティリティーに同一のファイルが 2 つ共存するため、名前空間コリジョンが発生し、クラッシュユーティリティーが起動してセグメンテーションフォルトが発生します。

この問題を回避するには、クラッシュ拡張ファイルを一度だけ読み込みます。その結果、セグメンテーションフォルトは上記のシナリオでは発生しなくなりました。

Bugzilla:1906482

仮想マシンへの仮想機能の割り当て時に接続に失敗する

ionic デバイスドライバーを使用する Pensando ネットワークカードは、VLAN タグ設定要求を許可し、ネットワーク仮想機能 (**VF**) を **VM** に割り当てる間にネットワーク接続の設定を試行します。この機能はカードのファームウェアではサポートされていないため、このようなネットワーク接続は失敗します。

Bugzilla:1930576

OPEN MPI ライブラリーは、デフォルトの PML でランタイムが失敗する可能性があります。

OPEN Message Passing Interface (OPEN MPI) 実装 4.0.x シリーズでは、UCX (Unified Communication X) がデフォルトの PPL (ポイントツーポイント) です。OPEN MPI 4.0.x シリーズの新しいバージョンでは、**openib** Byte Transfer Layer (BTL) が非推奨になりました。

ただし、OPEN MPI は **同種** クラスター (同じハードウェアおよびソフトウェア設定) で実行される場合も、UCX は MPI **openlib** の一方向操作に BTL を使用します。これにより、実行エラーが発生する可能性があります。この問題を回避するには、以下を実行します。

- 以下のパラメーターを使用して **mpirun** コマンドを実行します。

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

詳細は以下のようになります。

- **-mca btl openib** パラメーターは **openib** BTL を無効にします。
- **-mca pml ucx** パラメーターは、**ucx** PML を使用するように OPEN MPI を設定します。
- **x UCX_NET_DEVICES=** パラメーターは、指定したデバイスを使用するように UCX を制限します。

OPEN MPI は、**異種** クラスター (ハードウェアおよびソフトウェア設定に異なる) を実行する場合は、デフォルトの PML として UCX を使用します。これにより、OPEN MPI ジョブが不安定なパフォーマンス、応答しない動作で実行されたり、またはクラッシュによる不具合とともに実行される可能性があります。この問題を回避するには、UCX の優先度を以下のように設定します。

- 以下のパラメーターを使用して **mpirun** コマンドを実行します。

```
-mca pml_ucx_priority 5
```

これにより、OPEN MPI ライブラリーは、UCX を介して利用可能な別のトランスポート層を選択することができます。

Bugzilla:1866402

vmcore キャプチャーが、メモリーのホットプラグまたはアンプラグの操作を実行した後に失敗する

メモリーのホットプラグまたはホットアンプラグ操作の実行後に、メモリーのレイアウト情報を含むデバイスツリーを更新するとイベントが発生します。これにより、**makedumpfile** ユーティリティーは存在しない物理アドレスにアクセスしようとします。以下の条件を満たすと問題が発生します。

- IBM Power System (little endian) で RHEL 8 を実行する。
- システムで **kdump** サービスまたは **fadump** サービスが有効になっている。

このような場合に、メモリーホットプラグまたはホットアンプラグの操作後にカーネルクラッシュが発生すると、カーネルのキャプチャーで **vmcore** の保存に失敗します。

この問題を回避するには、ホットプラグまたはホットアンプラグ後に **kdump** サービスを再起動します。

```
# systemctl restart kdump.service
```

これにより、上記のシナリオで **vmcore** が正常に保存されます。

Bugzilla:1793389

irqpoll を使用すると vmcore の生成に失敗します。

アマゾンウェブサービス Graviton 1 プロセッサー上で実行される 64 ビット ARM アーキテクチャー上の **nvme** ドライバーの既存の問題により、最初のカーネルに **irqpoll** カーネルコマンドラインパラメーターを指定すると、**vmcore** の生成が失敗します。したがって、カーネルクラッシュ時に **vmcore** が **/var/crash/** ディレクトリーにダンプされません。この問題を回避するには、以下を実行します。

1. **/etc/sysconfig/kdump** ファイルの **KDUMP_COMMANDLINE_REMOVE** 変数に **irqpoll** を追加します。

```
# KDUMP_COMMANDLINE_REMOVE="hugepages hugepagesz slub_debug quiet
log_buf_len swiotlb"
```

2. **/etc/sysconfig/kdump** ファイルの **KDUMP_COMMANDLINE_APPEND** 変数から **irqpoll** を削除します。

```
# KDUMP_COMMANDLINE_APPEND="irqpoll nr_cpus=1 reset_devices
cgroup_disable=memory udev.children-max=2 panic=10 swiotlb=noforce novmcoredd"
```

3. **kdump** サービスを再起動します。

```
# systemctl restart kdump
```

その結果、最初のカーネルが正常に起動し、カーネルクラッシュ時に **vmcore** がキャプチャーされることが予想されます。

Amazon Web Services Graviton 2 および Amazon Web Services Graviton 3 プロセッサーでは、**/etc/sysconfig/kdump** ファイルの **irqpoll** パラメーターを手動で削除する必要がないことに注意してください。

kdump サービスは、大量のクラッシュカーネルメモリーを使用して **vmcore** ファイルをダンプする可能性があります。キャプチャーカーネルには、**kdump** サービス用のメモリーが十分あることを確認します。

この既知の問題の関連情報は、irqpoll カーネルコマンドラインパラメーターにより、vmcore 生成エラーが発生する場合がある を参照してください。

Bugzilla:1654962

RHEL 8 で、デバッグカーネルがクラッシュキャプチャー環境で起動に失敗する

デバッグカーネルはメモリーを大量に消費するので、デバッグカーネルが使用中で、カーネルパニックが発生すると、問題が発生します。その結果、デバッグカーネルはキャプチャーカーネルとして起動できず、代わりにスタックトレースが生成されます。この問題を回避するには、必要に応じてクラッシュカーネルメモリーを増やします。これにより、デバッグカーネルが、クラッシュキャプチャー環境で正常に起動します。

Bugzilla:1659609

起動時にクラッシュカーネルメモリーの割り当てに失敗する

一部の Ampere Altra システムでは、BIOS 設定で 32 ビットリージョンが無効になっていると、起動時にクラッシュカーネルメモリーを割り当てることに失敗します。したがって、**kdump** サービスが起動できません。これは、クラッシュカーネルメモリーを含むのに十分な大きさのフラグメントがない場合に、4 GB 未満のリージョンのメモリーの断片化によって生じます。

この問題を回避するには、以下のように BIOS で 32 ビットのメモリーリージョンを有効にします。

1. システムで BIOS 設定を開きます。
2. **Chipset** メニューを開きます。
3. **Memory Configuration** で、**Slave 32-bit** オプションを有効にします。

これにより、32 ビットリージョン内のクラッシュカーネルメモリー割り当てに成功し、**kdump** サービスが期待どおりに機能します。

Bugzilla:1940674

ネットワークインターフェイス名の予期しない変更により、IBM Z の RoCE インターフェイスの IP 設定が失われる

RHEL 8.6 以前では、IBM Z プラットフォーム上で、**udev** デバイスマネージャーが、一意の識別子 (UID) によって列挙される RoCE インターフェイスに、予測できないデバイス名を割り当てます。一方、RHEL 8.7 以降では、**udev** はこれらのインターフェイスに、**eno** 接頭辞が付いた予測可能なデバイス名を割り当てます。

RHEL 8.6 以前から 8.7 以降に更新すると、これらの UID 列挙インターフェイスには新しい名前が付けられ、NetworkManager 接続プロファイルのデバイス名と一致しなくなります。したがって、更新後、これらのインターフェイスには IP 設定がありません。

更新前に適用できる回避策と、すでにシステムを更新している場合の修正については、RoCE interfaces on IBM Z lose their IP settings after updating to RHEL 8.7 or later を参照してください。

Bugzilla:2169382

QAT マネージャーが LKCF のスペアデバイスを残さない

Intel® QuickAssist Technology(QAT) マネージャー (**qatmgr**) はユーザー空間プロセスであり、デフォルトではシステム内のすべての QAT デバイスを使用します。これにより、Linux Kernel Cryptographic Framework(LKCF) には QAT デバイスが残っていません。この動作は予想され、大多数のユーザーはユーザースペースからのアクセラレーションを使用するため、この状況を回避する必要はありません。

Bugzilla:1920086

Solarflare が、最大数の VF(Virtual Function) の作成に失敗する

Solarflare NIC は、リソースが十分にないため、最大数の VF の作成に失敗します。PCIe デバイスが作成できる VF の最大数は、**/sys/bus/pci/devices/PCI_ID/sriov_totalvfs** ファイルで確認できます。この問題を回避するには、起動時に **Solarflare Boot Manager** から、または Solarflare **sfboot** ユーティリティーの使用により、VF の数または VF MSI 割り込みの値を低い値に調整できます。デフォルトの VF MSI 割り込みの値は **8** です。

- **sfboot** を使用して VF MSI 割り込み値を調整するには、以下を実行します。

```
# sfboot vf-msix-limit=2
```

注記

VF MSI 割り込みの値を調整すると、VF のパフォーマンスに影響します。

調整されるパラメーターの詳細は、**Solarflare Server Adapter user guide** を参照してください。

Bugzilla:1971506

page_poison=1 を使用すると、カーネルクラッシュが発生する可能性がある

EFI 実装に問題のあるファームウェアでカーネルパラメーターとして **page_poison=1** を使用すると、オペレーティングシステムが原因でカーネルがクラッシュする可能性があります。デフォルトでは、このオプションは無効になっており、特に実稼働システムでは有効にすることは推奨しません。

Bugzilla:2050411

iwl7260-firmware により、Intel Wi-Fi 6 AX200、AX210、および Lenovo ThinkPad P1 Gen 4 で Wi-Fi が切断される

iwl7260-firmware または **iwl7260-wifi** ドライバーを RHEL 8.7 以降で提供されるバージョンに更新すると、ハードウェアが不正な内部状態になり、その状態を誤って報告します。その結果、Intel Wifi 6 カードが機能せず、次のエラーメッセージが表示される場合があります。

```
kernel: iwlwifi 0000:09:00.0: Failed to start RT ucode: -110
kernel: iwlwifi 0000:09:00.0: WRT: Collecting data: ini trigger 13 fired (delay=0ms)
kernel: iwlwifi 0000:09:00.0: Failed to run INIT ucode: -110
```

未確認の回避策は、システムの電源をオフにしてから再度オンにすることです。再起動しないでください。

Bugzilla:2106341

IBM Power Systems のセキュアブートは移行をサポートしていません

現在、IBM Power Systems では、物理ボリューム (PV) の移行が成功した後、論理パーティション (LPAR) が起動しません。その結果、パーティションでセキュアブートが有効になっているタイプの自動移行は失敗します。

Bugzilla:2126777

kmod の weak-modules がモジュールの相互依存関係で機能しない

kmod パッケージによって提供される **weak-modules** スクリプトは、どのモジュールがインストールされたカーネルと kABI 互換であるかを判別します。ただし、モジュールのカーネル互換性をチェックしている間、**weak-modules は** モジュールシンボルの依存関係を、それらがビルドされたカーネルの上位リリースから下位リリースへと処理します。結果として、異なるカーネルリリースに対して構築された相互依存関係を持つモジュールは互換性がないと解釈される可能性があるため、**weak-modules** はこのシナリオでは機能しません。

この問題を回避するには、新しいカーネルをインストールする前に、最新のストックカーネルに対して追加のモジュールをビルドまたは配置します。

Bugzilla:2103605

Ampere Altra サーバーの kdump が OOM 状態になる

現在、Ampere Altra および Altra Max サーバーのファームウェアが原因で、カーネルが大量のイベント、割り込み、およびコマンドキューを割り当て、メモリーを大量に消費します。その結果、**kdump** カーネルがメモリー不足 (OOM) 状態になります。

この問題を回避するには、**crashkernel=** カーネルオプションの値を 640M に増やして、**kdump** 用に追加のメモリーを予約します。

Bugzilla:2111855

コア数が大きいシステムのリアルタイムカーネルのハードウェア認定では、ロックの競合を回避するために skew-tick=1 ブートパラメーターを渡す必要がある場合があります。

多数のソケットとコアカウントが大きい大規模なシステムまたは中規模のシステムでは、タイムキーピングシステムで使用される **xtime_lock** のロック競合により、レイテンシーの急増が発生する可能性があります。その結果、レイテンシーの急増およびハードウェア認証のレイテンシーは、マルチプロセッシングシステムで発生する可能性があります。回避策として、**skew_tick=1** ブートパラメーターを追加することで、CPU ごとにタイマーティックをオフセットし、別のタイミングで開始できます。

ロックの競合を回避するには、**skew_tick=1** を有効にします。

1. **grubby** で **skew_tick=1** パラメーターを有効にします。

```
# grubby --update-kernel=ALL --args="skew_tick=1"
```

2. 変更を有効にするために再起動します。

3. **cat /proc/cmdline** コマンドを実行して、新しい設定を確認します。

skew_tick=1 を有効にすると、消費電力が大幅に増加するため、レイテンシーの影響を受けるリアルタイムワークロードを実行している場合にのみ有効にする必要があります。

Bugzilla:2214508

11.9. ブートローダー

grubby の動作はドキュメントから逸脱している

grubby ツールを使用して新しいカーネルを追加し、引数を指定しない場合、**grubby** はデフォルトの引数を新しいエントリーに渡します。**--copy-default** 引数を渡さなくても、この動作が発生します。**--args** および **--copy-default** オプションを使用すると、これらの引数が、**汚い** ドキュメントに記載されているデフォルトの引数に追加されます。

ただし、**$tuned_params** などの追加の引数を追加すると、**--copy-default** オプションが呼び出されない限り、**grubby** ツールはこれらの引数を渡しません。

この状況では、次の 2 つの回避策があります。

- **root=** 引数を設定し、**--args** を空のままにします:

```
# grubby --add-kernel /boot/my_kernel --initrd /boot/my_initrd --args "root=/dev/mapper/rhel-root" --title "entry_with_root_set"
```

- または、**root=** 引数と指定された引数を設定しますが、デフォルトのものは設定しません:

```
# grubby --add-kernel /boot/my_kernel --initrd /boot/my_initrd --args "root=/dev/mapper/rhel-root some_args and_some_more" --title "entry_with_root_set_and_other_args_too"
```

Bugzilla:1900829

11.10. ファイルシステムおよびストレージ

LUKS ボリュームを格納する LVM mirror デバイスが応答しなくなることがある

セグメントタイプが **mirror** のミラーリング LVM デバイスで LUKS ボリュームを格納すると、特定の条件下で応答しなくなる可能性があります。デバイスが応答しなくなると、すべての I/O 操作を拒否します。

耐障害性のソフトウェア定義ストレージに、LUKS ボリュームをスタックする必要がある場合に、この問題を回避するには、Red Hat は セグメントタイプが **mirror** ではなく **raid1** の LVM RAID 1 デバイスを使用することを推奨します。

raid1 のセグメントタイプは、デフォルトの RAID 設定タイプで、**mirror** の代わりに、推奨のソリューションとしてこのタイプが使用されます。

mirror デバイスを **raid1** に変換するには、ミラーリングされた LVM デバイスの RAID1 デバイスへの変換 を参照してください。

Bugzilla:1730502

/boot ファイルシステムを LVM に配置することができない

/boot ファイルシステムを LVM 論理ボリュームに配置することはできません。この制限は、以下の理由により存在します。

- EFI システムでは、**EFI システムパーティション** が従来の **/boot** ファイルシステムとして機能します。uEFI 標準では、特定の GPT パーティションタイプと、このパーティションの特定のファイルシステムタイプが必要です。
- RHEL 8 は、システムブートエントリーに **Boot Loader Specification** (BLS) を使用します。この仕様では、プラットフォームのファームウェアが **/boot** ファイルシステムを読み込める必要があります。EFI システムでは、プラットフォームファームウェアは uEFI 標準で定義された **/boot** 設定のみを読み取ることができます。
- GRUB 2 ブートローダーでの LVM 論理ボリュームに対するサポートは完全ではありません。Red Hat は、uEFI や BLS などの標準があるので、この機能のユースケース数が減少しているため、サポートを改善する予定はありません。

Red Hat では、LVM での **/boot** のサポートを提供する予定はありません。代わりに、Red Hat は、**/boot** ファイルシステムを LVM 論理ボリュームに配置する必要がないシステムスナップショットおよびロールバックを管理するツールを提供します。

Bugzilla:1496229

LVM で、複数のブロックサイズを持つボリュームグループが作成できない

vgcreate または **vgextend** などの LVM ユーティリティーでは、物理ボリューム (PV) の論理ブロックサイズが異なるボリュームグループ (VG) を作成できなくなりました。別のブロックサイズの PV で基礎となる論理ボリューム (LV) を拡張するとファイルシステムがマウントに失敗するため、LVM はこの変更を採用しました。

ブロックサイズが混在する VG の作成を再度有効にするには、**lvm.conf** ファイルの **allow_mixed_block_sizes=1** オプションを設定します。

Bugzilla:1768536

LVM writecache の制限

writecache LVM キャッシュメソッドには以下の制限がありますが、**cache** メソッドには存在しません。

- **pvmove** コマンドを使用すると、**writecache** 論理ボリュームに名前を付けることはできません。
- **writecache** を指定した論理ボリュームは、シンプールまたは VDO と組み合わせて使用できません。

以下の制限は、**cache** メソッドにも適用されます。

- **cache** または **writecache** がアタッチされている間は、論理ボリュームのサイズを変更することはできません。

Jira:RHELPLAN-27987, Bugzilla:1798631, Bugzilla:1808012

NVMe/TCP ドライバーを使用する場合、デバイスマッパーマルチパスがサポートされない

NVMe/TCP デバイス上でデバイスマッパーマルチパスを使用すると、パフォーマンスとエラー処理が低下する可能性があります。この問題を回避するには、DM マルチパスツールの代わりにネイティブ NVMe マルチパスを使用します。RHEL 8 の場合、カーネルコマンドラインにオプション **nvme_core.multipath=Y** を追加できます。

Bugzilla:2022359

blk-availability systemd サービスは、複雑なデバイススタックを非アクティブ化する

systemd では、デフォルトのブロック非アクティブ化コードは、仮想ブロックデバイスの複雑なスタックを常に正しく処理するとは限りません。一部の設定では、シャットダウン中に仮想デバイスが削除されない場合があり、エラーメッセージがログに記録されます。この問題を回避するには、次のコマンドを実行して、複雑なブロックデバイススタックを非アクティブ化します。

```
# systemctl enable --now blk-availability.service
```

その結果、複雑な仮想デバイススタックはシャットダウン中に正しく非アクティブ化され、エラーメッセージは生成されません。

Bugzilla:2011699

XFS クォータ警告が頻繁にトリガーされる

クォータタイマーを使用すると、クォータ警告が頻繁にトリガーされるため、ソフトクォータが必要以上に速く実行されます。この問題を回避するには、警告のトリガーを妨げるソフトクォータを使用しないでください。その結果、警告メッセージの量はソフトクォータ制限を強制せず、設定されたタイムアウトを尊重するようになります。

Bugzilla:2059262

11.11. 動的プログラミング言語、WEB サーバー、およびデータベースサーバー

virtualenv ユーティリティーを使用すると Python 3.11 仮想環境の作成が失敗する

python3-virtualenv パッケージによって提供される RHEL 8 の **virtualenv** ユーティリティーは、Python 3.11 と互換性がありません。**virtualenv** を使用して仮想環境を作成しようとすると、次のエラーメッセージが表示されて失敗します。

```
$ virtualenv -p python3.11 venv3.11
Running virtualenv with interpreter /usr/bin/python3.11
ERROR: Virtual environments created by virtualenv < 20 are not compatible with Python 3.11.
ERROR: Use `python3.11 -m venv` instead.
```

Python 3.11 仮想環境を作成するには、代わりに **python3.11 -m venv** コマンドを使用します。このコマンドは、標準ライブラリーの **venv** モジュールを使用します。

Bugzilla:2165702

python3.11-lxml が lxml.isoschematron サブモジュールを提供しない

python3.11-lxml パッケージは、オープンソースライセンスの下にないため、**lxml.isoschematron** サブモジュールなしで配布されます。サブモジュールは ISO Schematron サポートを実装します。代わりに、ISO-Schematron 前の検証を **lxml.etree.Schematron** クラスで利用できます。**python3.11-lxml**

パッケージの残りのコンテンツは影響を受けません。

Bugzilla:2157673

MariaDB では PAM プラグインバージョン 1.0 が機能しない

MariaDB 10.3 は、PAM (Pluggable Authentication Modules) プラグインバージョン 1.0 を提供します。**MariaDB 10.5** は、プラグインバージョン 1.0 および 2.0 を提供します。バージョン 2.0 がデフォルトです。

RHEL 8 では、**MariaDB** PAM プラグインバージョン 1.0 は機能しません。この問題を回避するには、**mariadb:10.5** モジュールストリームによって提供される PAM プラグインバージョン 2.0 を使用します。

Bugzilla:1942330

OpenLDAP ライブラリー間のシンボルの競合により、httpd でクラッシュが発生することがある

OpenLDAP が提供する **libldap** ライブラリーと **libldap_r** ライブラリーの両方が、単一のプロセス内にロードされ、使用されると、これらのライブラリー間でシンボルの競合が発生する可能性があります。そのため、**httpd** 設定によって **mod_security** または **mod_auth_openidc** モジュールもロードされると、PHP **ldap** 拡張機能を使用する Apache **httpd** 子プロセスが突然終了する可能性があります。

Apache Portable Runtime (APR) ライブラリーに対する RHEL 8.3 の更新では、**APR_DEEPBIND** 環境変数を設定することでこの問題を回避できます。これにより、**httpd** モジュールのロード時に **RTLD_DEEPBIND** 動的リンカーオプションを使用できるようになります。**APR_DEEPBIND** 環境変数を有効にすると、競合するライブラリーをロードする **httpd** 設定でクラッシュが発生しなくなります。

Bugzilla:1819607

32 ビットアプリケーションで呼び出されると getpwnam() が失敗する場合がある

NIS のユーザーが **getpwnam()** 関数を呼び出す 32 ビットアプリケーションを使用する場合は、**nss_nis.i686** パッケージがないと呼び出しに失敗します。この問題を回避するには、**yum install nss_nis.i686** コマンドを使用して、不足しているパッケージを手動でインストールします。

Bugzilla:1803161

11.12. IDENTITY MANAGEMENT

Samba をプリントサーバーとして実行し、RHEL 8.4 以前から更新する場合にアクションが必要です

今回の更新で、**samba** パッケージが **/var/spool/samba/** ディレクトリーを作成しなくなりました。プリントサーバーとして Samba を使用し、**[printers]** 共有の **/var/spool/samba/** を使用してプリントジョブをスプールすると、SELinux は Samba ユーザーがこのディレクトリーにファイルを作成しないようにします。したがって、印刷ジョブが失敗し、**auditd** サービスは **/var/log/audit/audit.log** に **denied** メッセージを記録します。8.4 以前からシステムを更新した後にこの問題を回避するには、以下を行います。

1. **/etc/samba/smb.conf** ファイルで **[printers]** 共有を探します。
2. 共有定義に **path = /var/spool/samba/** が含まれる場合は、設定を更新して、**path** パラメーターを **/var/tmp/** に設定します。
3. **smbd** サービスを再起動します。

```
# systemctl restart smbd
```

Samba を RHEL 8.5 以降に新しくインストールした場合、アクションは不要です。その場合、**samba-common** パッケージが提供するデフォルトの **/etc/samba/smb.conf** ファイルは、すでに **/var/tmp/** ディレクトリーを使用してプリントジョブをスプールします。

Bugzilla:2009213

--agent-uid pkidbuser オプションを指定して cert-fix ユーティリティーを使用すると、証明書システムが破損します。

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると、証明書システムの LDAP 設定が破損します。したがって、Certificate System は不安定になり、システムの復元に手動の操作が必要になる可能性があります。

Bugzilla:1729215

FIPS モードは、共有シークレットを使用したフォレスト間の信頼を確立することをサポートしません。

NTLMSSP 認証は FIPS に準拠していないため、FIPS モードでフォレスト間の信頼を確立できません。この問題を回避するには、FIPS モードが有効な IdM ドメインと AD ドメインとの間に信頼を確立する際に、Active Directory (AD) 管理アカウントで認証します。

Bugzilla:1924707

バージョン 1.2.2 へのリベース後の authselect のダウングレードにより、システム認証の破損

authselect パッケージが、最新のアップストリームバージョン **1.2.2** にリベースされました。**authselect** のダウングレードはサポートされておらず、**root** を含むすべてのユーザーに対してシステム認証が破損しています。

authselect パッケージを **1.2.1** 以前にダウングレードした場合は、この問題を回避するために以下の手順を実行します。

1. GRUB ブート画面で、起動するカーネルのバージョンを含む **Red Hat Enterprise Linux** を選択し、**e** を押してエントリーを編集します。
2. **linux** で始まる行の末尾で、**single** を、別の単語で入力し、**Ctrl+X** を押して起動プロセスを開始します。
3. シングルユーザーモードでの起動時に、root パスワードを入力します。
4. 以下のコマンドを使用して authselect 設定を復元します。

```
# authselect select sssd --force
```

Bugzilla:1892761

IdM から AD へのレルム間の TGS 要求が失敗します

IdM Kerberos チケットの 特権属性証明書 (PAC) 情報は、Active Directory (AD) でサポートされていない AES SHA-2 HMAC 暗号化で署名されるようになりました。

その結果、IdM から AD へのレルム間 TGS 要求 (双方向の信頼の設定) は、以下のエラーを出して失敗します。

> Generic error (see e-text) while getting credentials for <service principal>

Bugzilla:2125182

ldap_id_use_start_tls オプションのデフォルト値を使用する場合の潜在的なリスク。

ID ルックアップに TLS を使用せずに **ldap://** を使用すると、攻撃ベクトルのリスクが生じる可能性があります。特に、中間者 (MITM) 攻撃は、攻撃者が、たとえば、LDAP 検索で返されたオブジェクトの UID または GID を変更することによってユーザーになりすますことを可能にする可能性があります。

現在、TLS を強制する SSSD 設定オプション **ldap_id_use_start_tls** は、デフォルトで **false** に設定されています。セットアップが信頼できる環境で動作していることを確認し、**id_provider = ldap** に暗号化されていない通信を使用しても安全かどうかを判断してください。注記: **id_provider = ad** および **id_provider = ipa** は、SASL および GSSAPI によって保護された暗号化接続を使用するため、影響を受けません。

暗号化されていない通信を使用することが安全ではない場合は、**/etc/sssd/sssd.conf** ファイルで **ldap_id_use_start_tls** オプションを **true** に設定して TLS を強制します。デフォルトの動作は、RHEL の将来のリリースで変更される予定です。

Jira:RHELPLAN-155168

NSS で有効になっている暗号の default キーワードは、他の暗号と組み合わせても機能しません

Directory Server では、**default** キーワードを使用して、ネットワークセキュリティーサービス (NSS) で有効になっているデフォルトの暗号を参照することができます。しかし、コマンドラインまたは Web コンソールを使用してデフォルトの暗号および追加の暗号を有効にする場合、Directory Server は **default** キーワードの解決に失敗します。その結果、サーバーは追加で指定された暗号のみを有効にし、次のようなエラーをログに記録します。

> Security Initialization - SSL alert: Failed to set SSL cipher preference information: invalid ciphers <default,+cipher_name>: format is +cipher1,-cipher2... (Netscape Portable Runtime error 0 - no error)

回避策としては、追加で有効にしたいものも含めて、NSS でデフォルトで有効になっているすべての暗号を指定してください。

Bugzilla:1817505

RHEL 8.6 から RHEL 8.7 以降への pki-core-debuginfo の更新が失敗する

RHEL 8.6 から RHEL 8.7 以降への **pki-core-debuginfo** パッケージの更新が失敗します。この問題を回避するには、以下のコマンドを実行します。

1. **yum remove pki-core-debuginfo**
2. **yum update -y**
3. **yum install pki-core-debuginfo**
4. **yum install idm-pki-symkey-debuginfo idm-pki-tools-debuginfo**

Bugzilla:2134093

ドメイン SID の不一致により、移行した IdM ユーザーがログインできない可能性がある

ipa migrate-ds スクリプトを使用して IdM デプロイメントから別のデプロイメントにユーザーを移行す

る場合、そのユーザーの以前のセキュリティー識別子 (SID) には現在の IdM 環境のドメイン SID がないため、ユーザーが IdM サービスを使用する際に問題が発生する可能性があります。たとえば、これらのユーザーは **kinit** ユーティリティーを使用して Kerberos チケットを取得できますが、ログインできません。この問題を回避するには、ナレッジベースの記事 Migrated IdM users unable to log in due to mismatching domain SIDs を参照してください。

Jira:RHELPLAN-109613

FIPS モードの IdM は、双方向のフォレスト間信頼を確立するための NTLMSSP プロトコルの使用をサポートしない

FIPS モードが有効な Active Directory (AD)と Identity Management (IdM) との間で双方向のフォレスト間の信頼を確立すると、New Technology LAN Manager Security Support Provider (NTLMSSP) 認証が FIPS に準拠していないため、失敗します。FIPS モードの IdM は、認証の試行時に AD ドメインコントローラーが使用する RC4 NTLM ハッシュを受け入れません。

Bugzilla:2120572

FIPS モードで IdM Vault 暗号化および復号化に失敗する

FIPS モードが有効な場合は、OpenSSL RSA-PKCS1v15 パディング暗号化がブロックされます。その結果、現在は IdM が PKCS1v15 パディングを使用してセッションキーをトランスポート証明書でラップするため、Identity Management (IdM) Vault が正しく機能しません。

Bugzilla:2122919

Kerberos プリンシパルの有効期限を設定する際の誤った警告

Kerberos プリンシパルのパスワード有効期限を設定すると、32 ビットの符号付き整数変数を使用して、現在のタイムスタンプが有効期限のタイムスタンプと比較されます。有効期限が 68 年以上先の場合、整数変数のオーバーフローが発生し、次の警告メッセージが表示されます。

```
Warning: Your password will expire in less than one hour on [expiration date]
```

このメッセージは無視しても問題ありません。パスワードは設定された日時に正しく期限切れになります。

Bugzilla:2125318

11.13. デスクトップ

ソフトウェアリポジトリーからの flatpak リポジトリーの無効化ができません。

現時点で、GNOME Software ユーティリティーの Software Repositories ツールで **flatpak** リポジトリーを無効化または削除することはできません。

Bugzilla:1668760

Generation 2 の RHEL 8 仮想マシンが Hyper-V Server 2016 ホストで起動できない場合があります。

Microsoft Hyper-V Server 2016 ホストで実行している仮想マシンで RHEL 8 をゲストオペレーティングシステムとして使用すると、仮想マシンが起動しなくなり、GRUB ブートメニューに戻る場合があります。さらに、以下のエラーが Hyper-V イベントログに記録されます。

```
The guest operating system reported that it failed with the following error code: 0x1E
```

このエラーは、Hyper-V ホストの UEFI ファームウェアバグが原因で発生します。この問題を回避するには、Hyper-V Server2019 以降をホストとして使用します。

Bugzilla:1583445

ドラッグアンドドロップが、デスクトップとアプリケーション間で機能しません。

gnome-shell-extensions パッケージのバグにより、ドラッグアンドドロップ機能は現在、デスクトップとアプリケーションの間では機能しません。この機能のサポートは、今後のリリースで追加される予定です。

Bugzilla:1717947

11.14. グラフィックインフラストラクチャー

Radeon ドライバーがハードウェアを正しくリセットできない

現在、**radeon** カーネルドライバーは、**kexec** コンテキストでハードウェアを正しくリセットしません。代わりに **radeon** がフェイルオーバーします。これにより、**kdump** サービスの残りの部分が失敗します。

この問題を回避するには、**/etc/kdump.conf** ファイルに以下の行を追加して、**kdump** で **radeon** を無効にします。

```
dracut_args --omit-drivers "radeon"
force_rebuild 1
```

システムと **kdump** を再起動します。**kdump** の起動後、設定ファイルから **force_rebuild 1** 行が削除される場合があります。

このシナリオでは、ダンププロセス中にグラフィックは利用できませんが、**kdump** は正常に動作します。

Bugzilla:1694705

1 つの MST トポロジーで複数の HDR ディスプレイを使用すると、電源が入らないことがあります。

nouveau ドライバーの NVIDIA Turing GPUs を使用するシステムで、 **DisplayPort** ハブ (ラップトップのドックなど) を使用して HDR プラグインのサポートがあるモニターを複数接続すると、電源が入らないことがあります。これは、全ディスプレイをサポートする帯域幅がハブ上にないと、システムが誤って判断してしまうことが原因で発生します。

Bugzilla:1812577

ビデオメモリーが少なくなったため、ESXi の GUI がクラッシュする可能性がある

vCenter Server 7.0.1 を使用する VMware ESXi 7.0.1 ハイパーバイザーの RHEL 仮想マシンでグラフィカルユーザーインターフェイス (GUI) には、一定量のビデオメモリーが必要です。複数のコンソールまたは高解像度のモニターを仮想マシンに接続する場合、GUI には少なくとも 16 MB のビデオメモリーが必要です。ビデオメモリーが少ないで GUI を起動すると、GUI が突然終了する可能性があります。

この問題を回避するには、仮想マシンに 16 MB 以上のビデオメモリーを割り当てるようにハイパーバイザーを設定します。その結果、仮想マシンの GUI がクラッシュしなくなりました。

この問題が発生した場合は、VMware に報告することを推奨します。

VMware の記事、VMs with high resolution VM console may experience a crash on ESXi 7.0.1 (83194) 、も参照してください。

Bugzilla:1910358

VNC Viewer が、IBM Z で 16 ビットのカラーデプスで誤った色を表示

VNC Viewer アプリケーションは、16 ビットのカラーデプスで IBM Z サーバーの VNC セッションに接続すると、誤った色を表示します。

この問題を回避するには、VNC サーバーで 24 ビットのカラーデプスを設定します。**Xvnc** サーバーの場合は、**Xvnc** 設定で **-depth 16** オプションを **-depth 24** に置き換えます。

その結果、VNC クライアントで色が正しく表示されますが、サーバーでは、より多くのネットワーク帯域幅が使用されます。

Bugzilla:1886147

sudo コマンドを使用してグラフィカルアプリケーションを実行できません。

権限が昇格されたユーザーで、グラフィカルアプリケーションを実行しようとすると、エラーメッセージが表示され、アプリケーションを開くことができません。この障害は、 **Xauthority** ファイルで、通常ユーザーの認証情報を使用して認証するように、**Xwayland** に制限が加えられているため発生します。

この問題を回避するには、**sudo -E** コマンドを使用して、**root** ユーザーとしてグラフィカルアプリケーションを実行します。

Bugzilla:1673073

ARM でハードウェアアクセラレーションがサポートされない

組み込みグラフィックドライバーは、64 ビット ARM アーキテクチャー上のハードウェアアクセラレーションまたは Vulkan API に対応していません。

ARM でハードウェアアクセラレーションまたは Vulkan を有効にするには、プロプライエタリーの Nvidia ドライバーをインストールします。

Jira:RHELPLAN-57914

ASPEED 2600 を搭載したサーバーでインストーラーがフリーズする

ASPEED 2600 On System Management チップセットを搭載したサーバー上でグラフィカル RHEL 8.8 インストーラーを起動すると、インストーラーが応答しなくなり、黒い画面が表示されます。そのため、サーバーに RHEL 8.8 をインストールできません。

この問題を回避するには、インストーラーの起動時にカーネルコマンドラインに次のいずれかのオプションを追加します。

- **nomodeset**
- **drm_kms_helper.edid_firmware=edid/1024x768.bin**

その結果、インストールは期待どおりに進行します。

Bugzilla:2189645

11.15. WEB コンソール

VNC コンソールが特定の解像度で正しく動作しない

特定のディスプレイ解像度で Virtual Network Computing (VNC) コンソールを使用すると、マウスオフセットの問題が発生したり、インターフェイスの一部しか表示されない場合があります。そのため、VNC コンソールを使用できない場合があります。この問題を回避するには、VNC コンソールのサイズを拡大するか、代わりにコンソールタブのデスクトップビューアーを使用してリモートビューアーを起動します。

Bugzilla:2030836

11.16. RED HAT ENTERPRISE LINUX システムロール

Ansible 2.9 で RHEL システムロールを使用すると、command モジュールで dnf を使用することに関する警告が表示されることがあります。

RHEL 8.8 以降、RHEL システムロールは **dnf** モジュールで **warn** パラメーターを使用しなくなりました。これは、このパラメーターが Ansible Core 2.14 で削除されたためです。ただし、Ansible 2.9 で最新の **rhel-system-roles** パッケージを使用し、ロールがパッケージをインストールすると、次のいずれかの警告が表示される場合があります。

> [WARNING]: Consider using the dnf module rather than running 'dnf'. If you need to use command because dnf is insufficient you can add 'warn: false' to
> this command task or set 'command_warnings=False' in ansible.cfg to get rid of this message.

> [WARNING]: Consider using the yum, dnf or zypper module rather than running 'rpm'. If you need to use command because yum, dnf or zypper is insufficient
> you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get rid of this message.

これらの警告を非表示にする場合は、**ansible.cfg** ファイルの **[Defaults]** セクションに **command_warnings = False** 設定を追加します。ただし、この設定により Ansible のすべての警告が無効になることに注意してください。

Jira:RHELDOCS-17954

Playbook またはインベントリーでホスト名 localhost を使用して localhost を管理できません

RHEL に **ansible-core 2.13** パッケージが含まれているため、ノードを管理しているのと同じホストで Ansible を実行している場合は、Playbook またはインベントリーで **localhost** ホスト名を使用して実行することはできません。これは、**ansible-core 2.13** が **python38** モジュールを使用し、ライブラリーの多くが欠落しているために発生します。たとえば、**storage** ロールの場合は **blivet**、**network** ロールの場合は **gobject** です。この問題を回避するには、Playbook またはインベントリーでホスト名 **localhost** をすでに使用している場合は、**ansible_connection=local** を使用するか、**ansible_connection=local** オプションを使用して **localhost** をリストするインベントリーファイルを作成することで接続を追加できます。これにより、**localhost** 上のリソースを管理できます。詳細については、記事 ローカルホストで実行すると RHEL System Roles のPlaybookが失敗する を参照してください。

Bugzilla:2041997

firewalld.service がマスクされている場合、firewall RHEL システムロールの使用は失敗します。

RHEL システム上で **firewalld.service** がマスクされている場合、**firewall** RHEL システムロールは失敗します。この問題を回避するには、**firewalld.service** のマスクを解除します。

```
systemctl unmask firewalld.service
```

Bugzilla:2123859

rhc_auth にアクティベーションキーが含まれている場合、rhc システムロールはすでに登録されているシステムで失敗します。

rhc_auth パラメーターにアクティベーションキーが指定されている場合、すでに登録されているシステムで Playbook ファイルを実行すると失敗します。この問題を回避するには、登録済みのシステムで Playbook ファイルを実行するときにアクティベーションキーを指定しないでください。

Bugzilla:2186908

11.17. 仮想化

多数のキューを使用すると、Windows 仮想マシンで障害が発生することがある

仮想 Trusted Platform Module (vTPM) デバイスが有効で、**マルチキュー virtio-net** 機能が 250 を超えるキューを使用するように設定されている場合、Windows 仮想マシン (VM) が失敗することがあります。

この問題は、vTPM デバイスの制限が原因で発生します。vTPM デバイスには、開いているファイル記述子の最大数に関するハードコーディングされた制限があります。新しいキューごとに複数のファイル記述子が開かれるため、内部の vTPM 制限を超えて VM が失敗する可能性があります。

この問題を回避するには、次の 2 つのオプションのいずれかを選択します。

- vTPM デバイスを有効のままにしますが、使用するキューは 250 未満にします。
- 250 を超えるキューを使用するには、vTPM デバイスを無効にします。

Bugzilla:2020133

Milan 仮想マシンの CPU タイプは、AMD Milan システムで利用できないことがある

一部の AMD Milan システムでは、Enhanced REP MOVSB (**erms**) および Fast Short REP MOVSB (**fsrm**) 機能フラグがデフォルトで BIOS で無効になっています。したがって、**Milan** CPU タイプは、これらのシステムで利用できない可能性があります。さらに、機能フラグ設定が異なる Milan ホスト間の仮想マシンのライブマイグレーションが失敗する可能性があります。これらの問題を回避するには、ホストの BIOS で **erms** および **fsrm** を手動で有効にします。

Bugzilla:2077770

AMD EPYC でホストパススルーモードを使用する際に、SMT CPU トポロジーが仮想マシンで検出されない

AMD EPYC ホストで行われた CPU ホストパススルーモードで仮想マシンを起動すると、**TOPOEXT** 機能フラグは存在しません。したがって、仮想マシンは、コアごとに複数のスレッドを持つ仮想 CPU トポロジーを検出できません。この問題を回避するには、ホストパススルーの代わりに EPYC CPU モデルを使用して仮想マシンを起動します。

Bugzilla:1740002

virtio-blk を使用して仮想マシンに LUN デバイスを割り当てると機能しません。

q35 マシンタイプは、移行用の virtio 1.0 デバイスをサポートしないため、RHEL 8 では virtio 1.0 で非推奨となった機能はサポートされません。特に、RHEL 8 ホストで virtio-blk デバイスから SCSI コマンド

を送信することはできません。したがって、virtio-blk コントローラーを使用する場合は、物理ディスクを LUN デバイスとして仮想マシンに割り当てると失敗します。

物理ディスクをゲストオペレーティングシステムを通して渡すことは引き続き可能ですが、**device='lun'** オプションではなく、**device='disk'** オプションで設定する必要があることに留意してください。

Bugzilla:1777138

多数の virtio-blk ディスクを使用すると、仮想マシンが起動しないことがある

多数の virtio-blk デバイスを仮想マシンに追加すると、プラットフォームで利用可能な割り込みベクトルの数が使い切られる可能性があります。これが発生すると、仮想マシンのゲスト OS は起動できず、**dracut-initqueue[392]: Warning: Could not boot** エラーが表示されます。

Bugzilla:1719687

iommu_platform=on が IBM POWER で起動に失敗する

RHEL 8 は現在、IBM POWER システムの仮想マシン用の **iommu_platform=on** パラメーターに対応していません。これにより、IBM POWER ハードウェアでこのパラメーターを使用して仮想マシンを起動すると、仮想マシンがシステムの起動プロセス時に応答しなくなります。

Bugzilla:1910848

ibmvfc ドライバーの使用時に IBM POWER ホストが正しく動作するようになりました。

PowerVM 論理パーティション (LPAR) で RHEL 8 を実行すると、**ibmvfc** ドライバーの問題により、さまざまなエラーが発生することがありました。その結果、次のような特定の状況下で、ホスト上でカーネルパニックが発生していました。

- Live Partition Mobility (LPM) 機能の使用
- ホストアダプターのリセット
- SCSI エラー処理機能 (SCSI EH) 機能の使用

この更新により、**ibmvfc** の処理が修正され、前述のカーネルパニックは発生しなくなります。

Bugzilla:1961722

IBM POWER Systems で perf kvm レコード を使用すると、仮想マシンがクラッシュする可能性があります。

IBM POWER ハードウェアのリトルエンディアンバリアントで RHEL 8 ホストを使用する場合は、**perf kvm record** コマンドを使用して KVM 仮想マシンのイベントサンプルを収集すると、仮想マシンが応答しなくなることがあります。この状況は、以下の場合に発生します。

- **perf** ユーティリティーは権限のないユーザーによって使用され、**-p** オプションは仮想マシンを識別するために使用されます (**perf kvm record -e trace_cycles -p 12345**)。
- 仮想マシンが **virsh** シェルを使用して起動している。

この問題を回避するには、**perf kvm** ユーティリティーに **-i** オプションを指定して、**virsh** シェルを使用して作成した仮想マシンを監視します。以下に例を示します。

```
# perf kvm record -e trace_imc/trace_cycles/  -p <guest pid> -i
```

-i オプションを使用する場合、子タスクはカウンターを継承しないため、スレッドは監視されないことに注意してください。

Bugzilla:1924016

特定の CPU モデルの使用時に Hyper-V を有効化した Windows Server 2016 仮想マシンが起動に失敗する

現在、Windows Server 2016 をゲストオペレーティングシステムとして使用し、Hyper-V ロールが有効になっていて、以下の CPU モデルのいずれかを使用する仮想マシンを起動できません。

- EPYC-IBPB
- EPYC

この問題を回避するには、**EPYC-v3** CPU モデルを使用するか、仮想マシンの **xsaves** CPU フラグを手動で有効にします。

Bugzilla:1942888

RHEL 7-ALT ホストから RHEL 8 への POWER9 ゲストの移行に失敗する

現在のリリースでは、RHEL 7-ALT ホストシステムから RHEL 8 に POWER9 仮想マシンを移行すると、**Migration status: active** のステータスで応答がなくなります。

この問題を回避するには、RHEL 7-ALT ホストで Transparent Huge Pages (THP) を無効にすることで、移行が正常に完了します。

Bugzilla:1741436

virt-customize を使用すると、guestfs-firstboot が失敗することがあります。

virt-customize ユーティリティーを使用して仮想マシン (VM) ディスクイメージを変更すると、SELinux パーミッションが正しくないために **guestfs-firstboot** サービスが失敗します。これにより、ユーザーの作成やシステム登録の失敗など、仮想マシンの起動時にさまざまな問題が発生します。

この問題を回避するには、**virt-customize** コマンドに **--selinux-relabel** オプションを指定して使用します。

Bugzilla:1554735

macvtap 仮想ネットワークから正引きインターフェイスを削除すると、このネットワークの接続数がすべてリセットされます。

現在、複数のフォワードインターフェイスを持つ **macvtap** 仮想ネットワークからフォワードインターフェイスを削除すると、ネットワークの他のフォワードインターフェイスの接続ステータスもリセットされます。したがって、ライブネットワーク XML の接続情報が正しくありません。ただし、これは仮想ネットワークの機能に影響を与えるわけではないことに注意してください。この問題を回避するには、ホストで **libvirtd** サービスを再起動します。

Bugzilla:1332758

SLOF が指定された仮想マシンは netcat インターフェイスでの起動に失敗する

netcat(**nc**) インターフェイスを使用して、現在 Slimline Open Firmware(SLOF) プロンプトで待機中の仮想マシンのコンソールにアクセスすると、ユーザー入力は無視され、仮想マシンが応答しないままとなります。この問題を回避するには、仮想マシンに接続する場合は **nc -C** オプションを使用するか、代わりに telnet インターフェイスを使用します。

Bugzilla:1974622

場合によっては、virt-manager で仲介デバイスを仮想マシンに接続すると失敗します

virt-manager アプリケーションは現在、仲介されたデバイスを検出できますが、デバイスがアクティブであるかどうかを認識できません。結果として、**virt-manager** を使用して、非アクティブな仲介デバイスを実行中の仮想マシン (VM) に接続しようとすると失敗します。同様に、非アクティブな仲介デバイスを使用する新しい VM を作成しようとすると、**device not found** エラーで失敗します。

この問題を回避するには、**virt-manager** で使用する前に、**virsh nodedev-start** または **mdevctl start** コマンドを使用して仲介デバイスをアクティブにします。

Bugzilla:2026985

RHEL 9 仮想マシンが POWER8 互換モードでの起動に失敗する

現在、仮想マシン (VM) が次のような CPU 設定も使用している場合、ゲストオペレーティングシステムとして RHEL 9 を実行する仮想マシンの起動は失敗します。

```
<cpu mode="host-model">
  <model>power8</model>
</cpu>
```

この問題を回避するには、RHEL 9 仮想マシンで POWER8 互換モードを使用しないでください。

さらに、POWER8 ホストでは RHEL 9 VM を実行できないことに注意してください。

Bugzilla:2035158

SUID と SGID が virtiofs で自動的にクリアされない

killpriv_v2 機能を使用して **virtiofsd** サービスを実行すると、一部のファイルシステム操作を実行した後、システムが SUID および SGID アクセス許可を自動的にクリアしない場合があります。したがって、アクセス許可をクリアしないと、潜在的なセキュリティー上の脅威が発生する可能性があります。この問題を回避するには、次のコマンドを入力して **killpriv_v2** 機能を無効にします。

```
# virtiofsd -o no_killpriv_v2
```

Bugzilla:1966475

ホストで OVS サービスを再起動すると、実行中の VM でネットワーク接続がブロックされることがある

ホストで Open vSwitch (OVS) サービスが再起動またはクラッシュすると、このホストで実行されている仮想マシン (VM) はネットワークデバイスの状態を回復できません。その結果、仮想マシンがパケットを完全に受信できなくなる可能性があります。

この問題は、**virtio** ネットワークスタックで圧縮された virtqueue 形式を使用するシステムのみに影響します。

この問題を回避するには、**virtio** ネットワークデバイス定義で **packed=off** パラメーターを使用して、圧縮された virtqueue を無効にします。圧縮された virtqueue を無効にすると、状況によっては、ネットワークデバイスの状態を RAM から回復できます。

Bugzilla:1792683

VM 移行中の NFS 障害により、移行が失敗してソース仮想マシンのコアダンプが発生する

現在、仮想マシン (VM) の移行中に NFS サービスまたはサーバーがシャットダウンした場合、ソース VM の QEMU は、実行を再開したときに NFS サーバーに再接続できません。その結果、移行に失敗し、ソース VM でコアダンプが開始されます。現在、使用可能な回避策はありません。

Bugzilla:2177957

仮想マシンへの Watchdog カードのホットプラグが失敗する

現在、使用可能な PCI スロットがない場合、実行中の仮想マシン (VM) に Watchdog カードを追加すると、次のエラーが発生して失敗します。

```
Failed to configure watchdog
ERROR Error attempting device hotplug: internal error: No more available PCI slots
```

この問題を回避するには、Watchdog カードを追加する前に VM をシャットダウンします。

Bugzilla:2173584

11.18. クラウド環境の RHEL

VMware ホストの RHEL 仮想マシンで静的 IP を設定できない

現在、VMware ホストで RHEL を仮想マシンのゲストオペレーティングシステムとして使用すると、DatasourceOVF 機能は正しく機能しません。これにより、**cloud-init** ユーティリティーを使用して、仮想マシンのネットワークを静的 IP に設定し、仮想マシンを再起動すると、仮想マシンのネットワークが DHCP に変更されます。

この問題を回避するには、VMware ナレッジベース を参照してください。

Bugzilla:1750862

Azure および Hyper-V で kdump が起動しないことがある

Microsoft Azure または Hyper-V ハイパーバイザーでホストされている RHEL 8 ゲストオペレーティングシステムでは、実行後通知が有効な場合に **kdump** カーネルの起動が失敗することがあります。

この問題を回避するには、crash kexec post notifiers を無効にします。

```
# echo N > /sys/module/kernel/parameters/crash_kexec_post_notifiers
```

Bugzilla:1865745

複数のゲストディスクで Hyper-V 仮想マシンを起動する際に、SCSI ホストアドレスが変更することがある

現在、Hyper-V ハイパーバイザーで RHEL 8 仮想マシンを起動すると、場合によっては、**Host, Bus, Target, Lun** (HBTL) SCSI アドレスのホスト部分が変わることがあります。したがって、仮想マシンで HBTL SCSI 識別またはデバイスノードで設定した自動タスクは一貫して動作しません。これは、仮想マシンに複数のディスクがある場合、またはディスクに異なるサイズがある場合に発生します。

この問題を回避するには、以下のいずれかの方法でキックスタートファイルを変更します。

方法 1: SCSI デバイスに永続的な識別子を使用

たとえば、以下の powershell スクリプトを使用すると、特定のデバイス識別子を特定できます。

```
# Output what the /dev/disk/by-id/<value> for the specified hyper-v virtual disk.
# Takes a single parameter which is the virtual disk file.
# Note: kickstart syntax works with and without the /dev/ prefix.
param (
    [Parameter(Mandatory=$true)][string]$virtualdisk
)

$what = Get-VHD -Path $virtualdisk
$part = $what.DiskIdentifier.ToLower().split('-')

$p = $part[0]
$s0 = $p[6] + $p[7] + $p[4] + $p[5] + $p[2] + $p[3] + $p[0] + $p[1]

$p = $part[1]
$s1 =  $p[2] + $p[3] + $p[0] + $p[1]

[string]::format("/dev/disk/by-id/wwn-0x60022480{0}{1}{2}", $s0, $s1, $part[4])
```

このスクリプトは、ハイパーホストで使用することができます。以下に例を示します。

```
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_8.vhdx
/dev/disk/by-id/wwn-0x60022480e00bc367d7fd902e8bf0d3b4
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_9.vhdx
/dev/disk/by-id/wwn-0x600224807270e09717645b1890f8a9a2
```

その後、以下のようにキックスタートファイルでディスクの値を使用できます。

```
part / --fstype=xfs --grow --asprimary --size=8192 --ondisk=/dev/disk/by-id/wwn-
0x600224807270e09717645b1890f8a9a2
part /home --fstype="xfs" --grow --ondisk=/dev/disk/by-id/wwn-
0x60022480e00bc367d7fd902e8bf0d3b4
```

これらの値は仮想ディスクごとに固有であるため、仮想マシンインスタンスごとに設定を行う必要があります。そのため、**%include** 構文を使用して、ディスク情報を別のファイルに配置すると便利です。

方法 2: デバイス選択をサイズで設定

サイズに基づいてディスク選択を設定するキックスタートファイルには、以下のような行を含める必要があります。

```
...

# Disk partitioning information is supplied in a file to kick start
%include /tmp/disks

...

# Partition information is created during install using the %pre section
%pre --interpreter /bin/bash --log /tmp/ks_pre.log

 # Dump whole SCSI/IDE disks out sorted from smallest to largest ouputting
 # just the name
 disks=(`lsblk -n -o NAME -l -b -x SIZE -d -I 8,3`) || exit 1

 # We are assuming we have 3 disks which will be used
```

```
# and we will create some variables to represent
d0=${disks[0]}
d1=${disks[1]}
d2=${disks[2]}

echo "part /home --fstype="xfs" --ondisk=$d2 --grow" >> /tmp/disks
echo "part swap --fstype="swap" --ondisk=$d0 --size=4096" >> /tmp/disks
echo "part / --fstype="xfs" --ondisk=$d1 --grow" >> /tmp/disks
echo "part /boot --fstype="xfs" --ondisk=$d1 --size=1024" >> /tmp/disks

%end
```

Bugzilla:1906870

cloud-init によってプロビジョニングされ、NFSv3 マウントエントリーで設定された場合、Azure で RHEL インスタンスが起動しない

現在、仮想マシンが **cloud-init** ツールによってプロビジョニングされ、仮想マシンのゲストオペレーティングシステムで **/etc/fstab** ファイルに NFSv3 マウントエントリーがある場合、Microsoft Azure クラウドプラットフォームで RHEL 仮想マシンの起動に失敗します。

Bugzilla:2081114

11.19. サポート性

getattachment コマンドが複数の添付ファイルを一度にダウンロードできない

redhat-support-tool コマンドは、添付ファイルをダウンロードするための **getattachment** サブコマンドを提供します。ただし、**getattachment** は現在、1 つの添付ファイルしかダウンロードできず、複数の添付ファイルをダウンロードできません。

回避策として、**getattachment** サブコマンドで各添付ファイルのケース番号と UUID を渡すことにより、複数の添付ファイルを 1 つずつダウンロードできます。

Bugzilla:2064575

redhat-support-tool が FUTURE 暗号化ポリシーを使用すると機能しない

カスタマーポータル API の証明書が使用する暗号化キーは **FUTURE** のシステム全体の暗号化ポリシーが定義する要件を満たさないので、現時点で **redhat-support-tool** ユーティリティーは、このポリシーレベルでは機能しません。

この問題を回避するには、カスタマーポータル API への接続中に **DEFAULT** 暗号化ポリシーを使用します。

Bugzilla:1802026

IBM Power Systems (Little Endian) で sos report を実行するとタイムアウトする

数百または数千の CPU を搭載した IBM Power Systems (Little Endian) で **sos report** コマンドを実行すると、**/sys/devices/system/cpu** ディレクトリーの膨大なコンテンツを収集する際のプロセッサープラグインはデフォルトのタイムアウトである 300 秒に達します。回避策として、それに応じてプラグインのタイムアウトを増やします。

- 1 回限りの設定の場合は、次を実行します。

```
# sos report -k processor.timeout=1800
```

-

- 永続的な変更を行うには、**/etc/sos/sos.conf** ファイルの **[plugin_options]** セクションを編集します。

```
[plugin_options]
# Specify any plugin options and their values here. These options take the form
# plugin_name.option_name = value
#rpm.rpmva = off
processor.timeout = 1800
```

値の例は 1800 に設定されています。特定のタイムアウト値は、特定のシステムに大きく依存します。プラグインのタイムアウトを適切に設定するには、次のコマンドを実行して、タイムアウトなしで 1 つのプラグインを収集するために必要な時間を最初に見積もることができます。

```
# time sos report -o processor -k processor.timeout=0 --batch --build
```

Bugzilla:2011413

11.20. コンテナー

古いコンテナーイメージ内で systemd を実行すると動作しない

古いコンテナーイメージ (例:**centos:7**) で systemd を実行しても動作しません。

```
$ podman run --rm -ti centos:7 /usr/lib/systemd/systemd
 Storing signatures
 Failed to mount cgroup at /sys/fs/cgroup/systemd: Operation not permitted
 [!!!!!!] Failed to mount API filesystems, freezing.
```

この問題を回避するには、以下のコマンドを使用します。

```
# mkdir /sys/fs/cgroup/systemd
# mount none -t cgroup -o none,name=systemd /sys/fs/cgroup/systemd
# podman run --runtime /usr/bin/crun --annotation=run.oci.systemd.force_cgroup_v1=/sys/fs/cgroup -
-rm -ti centos:7 /usr/lib/systemd/systemd
```

Jira:RHELPLAN-96940

第12章 国際化

12.1. RED HAT ENTERPRISE LINUX 8 の多言語

Red Hat Enterprise Linux 8 は、複数の言語のインストールと、要件に応じた言語の変更に対応します。

- 東アジア言語 - 日本語、韓国語、簡体字中国語、および繁体字中国語。
- ヨーロッパ言語 - 英語、ドイツ語、スペイン語、フランス語、イタリア語、ポルトガル語、およびロシア語。

次の表は、さまざまな主要言語に提供されるフォントと入力方法を示しています。

言語	デフォルトフォント (フォントパッケージ)	入力メソッド
英語	dejavu-sans-fonts	
フランス語	dejavu-sans-fonts	
ドイツ語	dejavu-sans-fonts	
イタリア語	dejavu-sans-fonts	
ロシア語	dejavu-sans-fonts	
スペイン語	dejavu-sans-fonts	
ポルトガル語	dejavu-sans-fonts	
簡体字中国語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-libpinyin、libpinyin
繁体字中国語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin、libzhuyin
日本語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-kkc、libkkc
韓国語	google-noto-sans-cjk-ttc-fonts、google-noto-serif-cjk-ttc-fonts	ibus-hangul、libhangul

12.2. RHEL 8 における国際化の主な変更点

RHEL 8 では、RHEL 7 の国際化に以下の変更が加えられています。

- **Unicode 11** コンピューティングの業界標準のサポートが追加されました。

- 国際化は複数のパッケージで配布され、より小さなフットプリントのインストールを可能にします。詳細は、Using langpacks を参照してください。
- 多くの **glibc** ロケールが Unicode Common Locale Data Repository (CLDR) と同期されています。

付録A コンポーネント別のチケットリスト

参考のために、Bugzilla および JIRA チケットのリストをこのドキュメントに記載します。リンクをクリックすると、チケットについて説明したこのドキュメントのリリースノートにアクセスできます。

コンポーネント	チケット
389-ds-base	Bugzilla:2136610、Bugzilla:2096795、Bugzilla:2142639、Bugzilla:2130276、Bugzilla:1817505
NetworkManager	Bugzilla:2089707、Bugzilla:2134907、Bugzilla:2132754
SLOF	Bugzilla:1910848
accel-config	Bugzilla:1843266
anaconda	Bugzilla:1913035、Bugzilla:2014103、Bugzilla:1991516、Bugzilla:2094977、Bugzilla:2050140、Bugzilla:1914955、Bugzilla:1929105、Bugzilla:2126506
ansible-collection-microsoft-sql	Bugzilla:2144820、Bugzilla:2144821、Bugzilla:2144852、Bugzilla:2153428、Bugzilla:2163696、Bugzilla:2153427
ansible-freeipa	Bugzilla:2127912
apr	Bugzilla:1819607
authselect	Bugzilla:1892761
bacula	Bugzilla:2089399
brltty	Bugzilla:2008197
certmonger	Bugzilla:2150025
clevis	Bugzilla:2159440、Bugzilla:2159736
cloud-init	Bugzilla:1750862
cockpit	Bugzilla:2212371、Bugzilla:1666722
cockpit-appstream	Bugzilla:2030836
cockpit-machines	Bugzilla:2173584
conntrack-tools	Bugzilla:2126736
coreutils	Bugzilla:2030661

コンポーネント	チケット
corosync-qdevice	Bugzilla:1784200
crash	Bugzilla:1906482
crash-ptdump-command	Bugzilla:1838927
createrepo_c	Bugzilla:1973588
crypto-policies	Bugzilla:1921646、Bugzilla:2071981、Bugzilla:1919155、Bugzilla:1660839
device-mapper-multipath	Bugzilla:2022359、Bugzilla:2011699
distribution	Bugzilla:1657927
dnf	Bugzilla:2054235、Bugzilla:2047251、Bugzilla:2016070、Bugzilla:1986657
dnf-plugins-core	Bugzilla:2139324
edk2	Bugzilla:1741615、Bugzilla:1935497
fapolicyd	Bugzilla:2165645、Bugzilla:2054741
fence-agents	Bugzilla:1775847
firewalld	Bugzilla:1871860
gcc	Bugzilla:2110582
gdb	Bugzilla:1853140
git	Bugzilla:2139378
git-lfs	Bugzilla:2139382
glassfish-jaxb	Bugzilla:2055539
glibc	Bugzilla:1871383、Bugzilla:1159809
gnome-session	Bugzilla:2070976
gnome-shell-extensions	Bugzilla:2033572、Bugzilla:2138109、Bugzilla:1717947
gnome-software	Bugzilla:1668760

コンポーネント	チケット
gnutls	Bugzilla:1628553
golang	Bugzilla:2174430、Bugzilla:2132767、Bugzilla:2132694、Bugzilla:2132419
grub2	Bugzilla:1583445
grubby	Bugzilla:1900829
initscripts	Bugzilla:1875485
ipa	Bugzilla:2075452、Bugzilla:1924707、Bugzilla:2120572、Bugzilla:2122919、Bugzilla:1664719、Bugzilla:1664718、Bugzilla:2101770
ipmitool	Bugzilla:1873614
kernel	Bugzilla:2107595、Bugzilla:1660908、Bugzilla:1664379、Bugzilla:2136107、Bugzilla:2127136、Bugzilla:2143849、Bugzilla:1905243、Bugzilla:2009705、Bugzilla:2103946、Bugzilla:2087262、Bugzilla:2151854、Bugzilla:2134931、Bugzilla:2069047、Bugzilla:2135417、Bugzilla:1868526、Bugzilla:1694705、Bugzilla:1730502、Bugzilla:1609288、Bugzilla:1602962、Bugzilla:1865745、Bugzilla:1906870、Bugzilla:1924016、Bugzilla:1942888、Bugzilla:1812577、Bugzilla:1910358、Bugzilla:1930576、Bugzilla:1793389、Bugzilla:1654962、Bugzilla:1940674、Bugzilla:2169382、Bugzilla:1920086、Bugzilla:1971506、Bugzilla:2059262、Bugzilla:2050411、Bugzilla:2106341、Bugzilla:2127028、Bugzilla:2130159、Bugzilla:2189645、Bugzilla:1605216、Bugzilla:1519039、Bugzilla:1627455、Bugzilla:1501618、Bugzilla:1633143、Bugzilla:1814836、Bugzilla:1839311、Bugzilla:1570255、Bugzilla:1696451、Bugzilla:1348508、Bugzilla:1837187、Bugzilla:1660337、Bugzilla:2041686、Bugzilla:1836977、Bugzilla:1878207、Bugzilla:1665295、Bugzilla:1871863、Bugzilla:1569610、Bugzilla:1794513
kexec-tools	Bugzilla:2111855
kmod	Bugzilla:2103605
kmod-kvdo	Bugzilla:2119819、Bugzilla:2109047
krb5	Bugzilla:2125182、Bugzilla:2125318、Bugzilla:1877991
libdnf	Bugzilla:2124483
libffi	Bugzilla:2014228
libgnome-keyring	Bugzilla:1607766

コンポーネント	チケット
libguestfs	Bugzilla:1554735
libreswan	Bugzilla:2128672、Bugzilla:2176248、Bugzilla:1989050
libselinux-python-2.8-module	Bugzilla:1666328
libsoup	Bugzilla:1938011
libvirt	Bugzilla:1664592、Bugzilla:1332758、Bugzilla:1528684
llvm-toolset	Bugzilla:2118568
lvm2	Bugzilla:1496229、Bugzilla:1768536
mariadb	Bugzilla:1942330
mesa	Bugzilla:1886147
mod_security	Bugzilla:2143207
nfs-utils	Bugzilla:2081114、Bugzilla:1592011
nginx	Bugzilla:2112345
nispor	Bugzilla:2153166
nodejs	Bugzilla:2178087
nss	Bugzilla:1817533、Bugzilla:1645153
nss_nis	Bugzilla:1803161
openblas	Bugzilla:2115722
opencryptoki	Bugzilla:2110315
opencv	Bugzilla:1886310
openmpi	Bugzilla:1866402
opensc	Bugzilla:2176973、Bugzilla:1947025、Bugzilla:2097048
openscap	Bugzilla:2159290、Bugzilla:2161499

コンポーネント	チケット
openssh	Bugzilla:2044354
openssl	Bugzilla:1810911
oscap-anaconda-addon	Bugzilla:2075508、Bugzilla:1843932、Bugzilla:1665082、Bugzilla:2165948
pacemaker	Bugzilla:2133497、Bugzilla:2121852、Bugzilla:2122806
pam	Bugzilla:2068461
pcs	Bugzilla:2132582、Bugzilla:1816852、Bugzilla:2112263、Bugzilla:2112267、Bugzilla:1918527、Bugzilla:1619620、Bugzilla:1851335
pki-core	Bugzilla:1729215、Bugzilla:2134093、Bugzilla:1628987
podman	Jira:RHELPLAN-136601、Jira:RHELPLAN-136608、Bugzilla:2119200、Jira:RHELPLAN-136610
postfix	Bugzilla:1711885
postgresql	Bugzilla:2128241
powertop	Bugzilla:2040070
pykickstart	Bugzilla:1637872
python3.11	Bugzilla:2137139
python3.11-lxml	Bugzilla:2157673
python36-3.6-module	Bugzilla:2165702
qemu-kvm	Bugzilla:2117149、Bugzilla:2020133、Bugzilla:1740002、Bugzilla:1719687、Bugzilla:1966475、Bugzilla:1792683、Bugzilla:2177957、Bugzilla:1651994
rear	Bugzilla:2130206、Bugzilla:2172605、Bugzilla:2131946、Bugzilla:1925531、Bugzilla:2083301
redhat-support-tool	Bugzilla:2064575、Bugzilla:1802026
restore	Bugzilla:1997366

コンポーネント	チケット
rhel-system-roles	Bugzilla:2119600、Bugzilla:2130019、Bugzilla:2143814、Bugzilla:2079009、Bugzilla:2130332、Bugzilla:2130345、Bugzilla:2133532、Bugzilla:2133931、Bugzilla:2134201、Bugzilla:2133856、Bugzilla:2143458、Bugzilla:2137667、Bugzilla:2143385、Bugzilla:2144876、Bugzilla:2144877、Bugzilla:2130362、Bugzilla:2129620、Bugzilla:2165176、Bugzilla:2149683、Bugzilla:2126960、Bugzilla:2127497、Bugzilla:2153081、Bugzilla:2167941、Bugzilla:2153080、Bugzilla:2168733、Bugzilla:2162782、Bugzilla:2123859、Bugzilla:2186908、Bugzilla:2021685、Bugzilla:2006081
rpm	Bugzilla:2129345、Bugzilla:2110787、Bugzilla:1688849
rsync	Bugzilla:2139118
rsyslog	Bugzilla:2124934、Bugzilla:2070496、Bugzilla:2157658、Bugzilla:1679512、Jira:RHELPLAN-10431
rt-tests	Bugzilla:2122374
rteval	Bugzilla:2082260
rtla	Bugzilla:2075203
rust-toolset	Bugzilla:2123899
s390utils	Bugzilla:2043833
samba	Bugzilla:2132051、Bugzilla:2009213、Jira:RHELPLAN-13195、Jira:RHELDOCS-16612
scap-security-guide	Bugzilla:2052938、Bugzilla:2158210、Bugzilla:1991843、Bugzilla:2127100、Bugzilla:2093793、Bugzilla:2107346、Bugzilla:2050140、Bugzilla:1877697、Bugzilla:1914955、Bugzilla:1929105、Bugzilla:1997832、Bugzilla:2125542、Bugzilla:2115783、Bugzilla:2164216
selinux-policy	Bugzilla:1972230、Bugzilla:2088441、Bugzilla:2154242、Bugzilla:2134125、Bugzilla:2090711、Bugzilla:2101341、Bugzilla:2121709、Bugzilla:2122838、Bugzilla:2124388、Bugzilla:2125008、Bugzilla:2143696、Bugzilla:2148561、Bugzilla:1461914
sos	Bugzilla:2164987、Bugzilla:2134906、Bugzilla:2011413
spice	Bugzilla:1849563
sssd	Bugzilla:2144519、Bugzilla:2087247、Bugzilla:2065692、Bugzilla:2056483、Bugzilla:1947671
subscription-manager	Bugzilla:2170082

コンポーネント	チケット
swig	Bugzilla:2139076
synce4l	Bugzilla:2019751
tang	Bugzilla:2188743
texlive	Bugzilla:2150727
tomcat	Bugzilla:2160455
tuna	Bugzilla:2121518
tuned	Bugzilla:2133814、Bugzilla:2113900
tzdata	Bugzilla:2154109
udica	Bugzilla:1763210
usbguard	Bugzilla:2159409、Bugzilla:2159411、Bugzilla:2159413
vdo	Bugzilla:1949163
virt-manager	Bugzilla:2026985
wayland	Bugzilla:1673073
weldr-client	Bugzilla:2033192
wsmancli	Bugzilla:2105316
xdp-tools	Bugzilla:2160069
xorg-x11-server	Bugzilla:1698565

コンポーネント	チケット
その他	Bugzilla:2177769、Jira:RHELPLAN-139125、Jira:RHELPLAN-137505、Jira:RHELPLAN-139430、Jira:RHELPLAN-137416、Jira:RHELPLAN-137411、Jira:RHELPLAN-137406、Jira:RHELPLAN-137403、Jira:RHELPLAN-139448、Jira:RHELPLAN-151481、Jira:RHELPLAN-150266、Jira:RHELPLAN-151121、Jira:RHELPLAN-149091、Jira:RHELPLAN-139424、Jira:RHELPLAN-136489、Bugzilla:2183445、Jira:RHELPLAN-59528、Jira:RHELPLAN-148303、Bugzilla:2025814、Bugzilla:2077770、Bugzilla:1777138、Bugzilla:1640697、Bugzilla:1697896、Bugzilla:1961722、Bugzilla:1659609、Bugzilla:1687900、Bugzilla:1757877、Bugzilla:1741436、Jira:RHELPLAN-27987、Jira:RHELPLAN-34199、Jira:RHELPLAN-57914、Jira:RHELPLAN-96940、Bugzilla:1974622、Bugzilla:2028361、Bugzilla:2041997、Bugzilla:2035158、Jira:RHELPLAN-109613、Bugzilla:2126777、Bugzilla:1690207、Bugzilla:1559616、Bugzilla:1889737、Bugzilla:1906489、Bugzilla:1769727、Jira:RHELPLAN-27394、Jira:RHELPLAN-27737、Jira:RHELPLAN-148394、Bugzilla:1642765、Bugzilla:1646541、Bugzilla:1647725、Bugzilla:1932222、Bugzilla:1686057、Bugzilla:1748980、Jira:RHELPLAN-71200、Jira:RHELPLAN-45858、Bugzilla:1871025、Bugzilla:1871953、Bugzilla:1874892、Bugzilla:1916296、Jira:RHELPLAN-100400、Bugzilla:1926114、Bugzilla:1904251、Bugzilla:2011208、Jira:RHELPLAN-59825、Bugzilla:1920624、Jira:RHELPLAN-70700、Bugzilla:1929173、Jira:RHELPLAN-85066、Jira:RHELPLAN-98983、Bugzilla:2009113、Bugzilla:1958250、Bugzilla:2038929、Bugzilla:2006665、Bugzilla:2029338、Bugzilla:2061288、Bugzilla:2060759、Bugzilla:2055826、Bugzilla:2059626、Jira:RHELPLAN-133171、Bugzilla:2142499、Jira:RHELPLAN-145958、Jira:RHELPLAN-146398、Jira:RHELPLAN-153267

付録B 改訂履歴

0.2-3

2024 年 6 月 7 日金曜日、Brian Angelica (bangelic@redhat.com)

- Jira の既知の問題を更新しました: RHELDOCS-17954 (Red Hat Enterprise Linux システムロール)。

0.2-2

2024 年 5 月 15 日 (水) Brian Angelica (bangelic@redhat.com)

- BZ#1690207 でテクニカルプレビューを更新しました。

0.2-1

2024 年 5 月 9 日 (木)、Gabriela Fialova (gfialova@redhat.com)

- 既知の問題 BZ#1730502 (ストレージ) を更新しました。

0.1-10

2024 年 4 月 25 日 (木)、Gabriela Fialová (gfialova@redhat.com)

- 機能拡張 BZ#2165827 (Identity Management) を追加しました。

0.1-9

2023 年 3 月 2 日 (木)、Lucie Vařáková (lvarakova@redhat.com)

- バグ修正 Jira:SSSD-6096 (アイデンティティー管理) を追加しました

0.1-8

2024 年 2 月 1 日 (木)、Gabriela Fialová (gfialova@redhat.com)

- 非推奨の機能 Jira:RHELDOCS-17641 (ネットワーク) を追加しました。

0.1-7

2024 年 2 月 7 日 (水)、Lucie Vařáková (lvarakova@redhat.com)

- 非推奨の機能 Jira:RHELDOCS-17573 (アイデンティティー管理) を追加しました。

0.1-6

2024 年 2 月 7 日 (水)、Lucie Vařáková (lvarakova@redhat.com)

- 既知の問題 BZ#1834716 (セキュリティー) を追加しました。
- BZ#2183445 （カーネル）のテキストを更新しました。

0.1-5

2023 年 12 月 7 日木曜日、Lucie Vařáková (lvarakova@redhat.com)

- 新機能 BZ#2044200 (カーネル) を追加しました。

0.1-4

2023 年 11 月 10 日金曜日、Gabriela Fialová (gfialova@redhat.com)

- RHEL ドキュメントへのフィードバックの提供に関するモジュールを更新しました。

0.1-3

2023 年 10 月 17 日 (火) Gabriela Fialová (gfialova@redhat.com)

- DF JIRA-RHELDOCS-16755 (コンテナー) のドキュメントテキストを更新しました。

0.1-2

2023 年 10 月 13 日 (金) Gabriela Fialová (gfialova@redhat.com)

- テクノロジープレビュー JIRA:RHELDOCS-16861 (コンテナー) を追加しました。

0.1-1

2023 年 10月 9 日、Lucie Vařáková (lvarakova@redhat.com)

- 既知の問題 BZ#2169382 (カーネル) を更新しました。

0.1-0

2023 年 9 月 8 日、Lucie Vařáková (lvarakova@redhat.com)

- 非推奨機能のリリースノート JIRA:RHELDOCS-16612 (Samba) を追加しました。
- Red Hat ドキュメントへのフィードバック セクションを更新しました。

0.0-9

2023 年 8 月 24 日 Lucie Vařáková (lvarakova@redhat.com)

- 既知の問題 BZ#2214508 (カーネル) を追加しました。

0.0-8

2023 年 8 月 4 日 Lenka Špačková (lspackova@redhat.com)

- BZ#2225332 のセクションを修正しました。

0.0-7

2023 年 8 月 3 日 Lucie Vařáková (lvarakova@redhat.com)

- 非推奨の機能 Jira:RHELPLAN-139456 (Identity Management) を追加しました。

0.0-6

2023 年 8 月 1 日 Lenka Špačková (lspackova@redhat.com)

- 非推奨の機能 BZ#2225332 を追加しました。
- 概要の改善

0.0-5

2023 年 7 月 31 日 Mirek Jahoda (mjahoda@redhat.com)

- 既知の問題 BZ#2203361 がバグ修正 BZ#2212371 に変更されました。

0.0-4

2023 年 7 月 13 日 Lucie Vařáková (lvarakova@redhat.com)

- テクノロジープレビュー BZ#1570255 (ネットワーキング) を追加しました。
- インプレースアップグレードと OS 移行 セクションを更新しました。

0.0-3

2023 年 6 月 27 日、Lucie Vařáková (lvarakova@redhat.com)

- 機能拡張 BZ#2087247 (アイデンティティ管理) を追加しました。
- BZ#2176248 をバグフィックス (セキュリティー) に移動しました。
- 既知の問題 BZ#2176973 (セキュリティー) を追加しました。
- テクノロジープレビュー BZ#1769727 (カーネル) を更新しました。

0.0-2

2023 年 6 月 6 日、Lucie Vařáková (lvarakova@redhat.com)

- 既知の問題 BZ#2177957 (仮想化) を追加しました。
- その他の小規模の更新。

0.0-1

2023 年 5 月 17 日、Lucie Vařáková (lvarakova@redhat.com)

- Red Hat Enterprise Linux 8.8 リリースノートのリリース。

0.0-0

2023 年 5 月 29 日、Lucie Vařáková (lvarakova@redhat.com)

- Red Hat Enterprise Linux 8.8 Beta リリースノートのリリース。