Red Hat Enterprise Linux 8

RHEL 7 から RHEL 8 へのアップグレード

Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのインプレースアップグレードの手順

Last Updated: 2024-06-07

Red Hat Enterprise Linux 8 RHEL 7 から RHEL 8 へのアップグレード

Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのインプレースアップグレードの手順

法律上の通知

概要

本ガイドは、Leapp ユーティリティーを使用した、Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのインプレースアップグレードを実行する方法を説明します。既存の RHEL 7 オペレーティングシステムは、インプレースアップグレード時に RHEL 8 バージョンに置き換えられます。

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、用語の置き換えは、今後の複数のリリースにわたって段階的に実施されます。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。

主な移行の用語

以下の移行用語はソフトウェア業界で一般的に使用されますが、これらの定義は Red Hat Enterprise Linux (RHEL) に固有のものです。

更新

ソフトウェアパッチと呼ばれることもあります。更新は現行バージョン、オペレーティングシステム、または実行中のソフトウェアに追加されます。ソフトウェア更新は、問題またはバグに対応し、テクノロジーの操作が改善されます。RHEL では、更新は、RHEL 8.1 から 8.2 への更新といったマイナーリリースに関連します。

アップグレード

アップグレードは、現在実行しているアプリケーション、オペレーティングシステム、またはソフトウェアを置き換える場合です。通常、まず Red Hat の指示に従い、データをバックアップします。RHEL をアップグレードすると、以下の 2 つのオプションがあります。

- **In-place upgrade:** インプレースアップグレードの場合は、以前のバージョンを削除せずに、以前のバージョンを新しいバージョンに置き換えます。設定や設定と共にインストールされたアプリケーションとユーティリティーは、新規バージョンに組み込まれています。

- **clean install:** clean install は、以前にインストールされたオペレーティングシステム、システムデータ、設定、およびアプリケーションのすべてのトレースを削除し、最新バージョンのオペレーティングシステムをインストールします。システムに以前のデータまたはアプリケーションが必要ない場合や、以前のビルドに依存しない新規プロジェクトを開発する場合は、クリーンインストールに適しています。

オペレーティングシステムへの変換

変換は、オペレーティングシステムを別の Linux ディストリビューションから Red Hat Enterprise Linux に変換する際に使用されます。通常、まず Red Hat の指示に従い、データをバックアップします。

マイグレーション

通常、マイグレーションとは、ソフトウェアやハードウェアといったプラットフォームの変更を示しています。Windows から Linux への移行はマイグレーションです。ユーザーがあるラップトップから別のラップトップに移動したり、企業があるサーバーから別のサーバーに移動することもマイグレーションです。ただし、ほとんどのマイグレーションにはアップグレードも含まれており、この2つの用語が同様の意味で使用されることがあります。

- **RHEL へのマイグレーション:** 既存のオペレーティングシステムを RHEL に変換すること。

- **RHEL 間でのマイグレーション:** RHEL のあるバージョンから別のバージョンへのアップグレード。

第1章 サポート対象のアップグレードパス

インプレースアップグレードは、システムの RHEL 7 オペレーティングシステム (OS) を RHEL 8 バージョンに置き換えます。

現在、RHEL 7 から次の RHEL 8 マイナーバージョンへのインプレースアップグレードを実行できます。

表1.1 サポート対象のアップグレードパス

システムの設定	ソース OS バージョン	ターゲット OS バージョン	サポート終了日
RHEL	RHEL 7.9	RHEL 8.8	2025 年 5 月 31 日 (EUS)
		RHEL 8.10 (デフォルト)	2028 年 6 月 30 日
RHEL with SAP HANA	RHEL 7.9	RHEL 8.8 (デフォルト)	2025 年 5 月 31 日 (EUS)
		RHEL 8.10	2028 年 6 月 30 日

サポートされているアップグレードパスの詳細は、Red Hat Enterprise Linux のサポート対象のインプレースアップグレードパス および インプレースアップグレードのサポートポリシー を参照してください。

第2章 アップグレードプロセスの概要

RHEL 7 から RHEL 8 へのインプレースアップグレードプロセスは、次のように要約できます。

1. **アップグレードを計画する**
   システム要件と制限事項を確認します。システムがインプレースアップグレードに適しているかどうか、または代わりに RHEL 8 のクリーンインストールを実行する必要があるかを判断します。

2. **アップグレードを準備する**
   アップグレードプロセスを開始する前に、RHEL 7 システムのバックアップの作成など、必要な準備手順を完了してください。

3. **アップグレード前レポートを実行して確認する**
   アップグレード前ユーティリティーを実行して、アップグレード前に解決する必要がある潜在的な問題をまとめたレポートを生成します。見つかった問題の重大度と影響、およびそれらを解決するために必要な作業量に応じて、以下のいずれかを実行します。

   - 見つかった問題を修正し、推奨される解決策を適用します。アップグレード前のユーティリティーを再実行して、重大な問題がすべて解決されたことを確認します。システムのアップグレード準備が整う前に、アップグレード前レポートを実行し、見つかった問題を解決する作業を複数回実行することを推奨します。

   - インプレースアップグレードを続行する代わりに、RHEL 8 のクリーンインストールに切り替えます。

4. **インプレースアップグレードを実行する**
   RHEL 8 へのアップグレードを実行し、アップグレードが正しく完了したことを確認します。アップグレードで解決できない問題が発生した場合は、RHEL 7 バックアップへのロールバックを実行します。

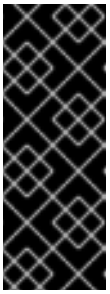
5. **アップグレード後の手順を実行する**
   RHEL 8 システムが適切に設定されていることを確認するために、必要なアップグレード後の手順を実行します。

第3章 アップグレードの計画

インプレースアップグレードは、システムを RHEL の次のメジャーバージョンにアップグレードする方法です。この方法は、推奨され、サポートされています。

RHEL 8 にアップグレードする前に、次の点を考慮してください。

- **オペレーティングシステム** - オペレーティングシステムは、以下の条件下で、**Leapp** ユーティリティーによりアップグレードされます。
  - 64 ビット Intel、IBM POWER 8 (リトルエンディアン)、64 ビット IBM Z アーキテクチャー、SAP HANA 上の場合は 64-bit Intel アーキテクチャー上のサーバーバリアントの **RHEL 7.9** がインストールされている。
    詳細は Supported in-place upgrade paths for Red Hat Enterprise Linux を参照してください。
  - RHEL 8 の最小 ハードウェア要件 が満たされている。
  - 最新の RHEL 7.9 およびターゲットオペレーティングシステム (OS) バージョン (RHEL 8.10 など) のコンテンツにアクセスできる。詳細は、アップグレードに向けて RHEL 7 システムの準備 を参照してください。
- **アプリケーション** - **Leapp** を使用して、システムにインストールされているアプリケーションを移行できます。ただし、特定のケースでは、アップグレード時に **Leapp** が実行するアクションを指定するカスタムアクターを作成する必要があります。たとえば、アプリケーションの再設定や特定のハードウェアドライバーのインストールなどです。詳細は、Handling the migration of your custom and third-party applications を参照してください。Red Hat はカスタムアクターをサポートしていないことに注意してください。
- **セキュリティー** - アップグレード前にこの要素を評価し、アップグレードプロセスの完了時に追加の手順を実行する必要があります。特に以下の点を考慮してください。
  - アップグレードの前に、システムが準拠する必要のあるセキュリティー標準を定義し、RHEL 8 のセキュリティー変更 を理解します。
  - **Leapp** ユーティリティーは、アップグレードプロセス時に SELinux モードを Permissive に設定します。
  - Federal Information Processing Standard (FIPS) モードでのシステムのインプレースアップグレードは、**Leapp** で完全に自動化することはできません。**FIPS モード** で実行されている RHEL 7 システムをアップグレードする必要がある場合は、次のことを行う必要があります。



重要

すべての暗号化キーを FIPS 140-2 標準に準拠したものにするには、すでにデプロイされているシステムのインプレースアップグレードを実行する代わりに、FIPS モードで新しいインストール を開始します。次の手順は、会社のセキュリティーポリシーでこの代替アップグレードプロセスが許可されている場合、およびアップグレードしたシステムですべての暗号化キーの再生成と再評価を確実に実行できる場合にのみ使用してください。

1. RHEL 7 で FIPS モードを無効にします。

2. **Leapp** を使用してシステムをアップグレードします。他のインプレースアップグレードと同様に、アップグレード前、アップグレード、およびアップグレード後の手順に従う必要があります。

3. RHEL 8 で FIPS モードを有効にします。詳細は、RHEL 8 セキュリティーの強化ドキュメントの FIPS モードへのシステムの切り替え を参照してください。

4. システムで暗号化キーを再生成します。詳細は、付録C *RHEL 8 の暗号化キーの場所* を参照してください。

- アップグレードが完了したら、セキュリティーポリシーを再評価し、再適用します。アップグレード中に無効になった、または RHEL 8 で新たに導入されたセキュリティーポリシーを適用する方法は、セキュリティーポリシーの適用 を参照してください。

- **ストレージとファイルシステム** - アップグレードの前に必ずシステムをバックアップしてください。たとえば、Relax-and-Recover (ReaR) ユーティリティー、LVM スナップショット、RAID 分割、または仮想マシンスナップショットを使用できます。

注記

ファイルシステム形式はそのままです。その結果、ファイルシステムには、最初に作成されたときと同じ制限があります。

- **高可用性** - 高可用性アドオンを使用している場合は、ナレッジベース記事 Recommended Practices for Applying Software Updates to a RHEL High Availability or Resilient Storage Cluster に従ってください。

- **ダウンタイム** - アップグレードプロセスには数分から数時間かかる場合があります。

- **Satellite** - Satellite を介してホストを管理する場合は、Satellite Web UI を使用して、RHEL 7 から RHEL 8 に複数のホストを同時にアップグレードできます。詳細は、次の Red Hat Enterprise Linux リリースへのホストのアップグレード を参照してください。

- **SAP HANA** - SAP HANA を使用している場合は、SAP 環境を RHEL 7 から RHEL 8 にインプレースアップグレードする方法 に従ってください。SAP HANA を使用した RHEL のアップグレードパスは異なる場合があることに注意してください。

- **RHEL for Real Time** - リアルタイムシステムでのアップグレードがサポートされています。

- **Red Hat OpenStack Platform の Real Time for Network Functions Virtualization (NFV)**- リアルタイムシステムでのアップグレードがサポートされています。

- **Red Hat Software Collections (RHSCL)**- RHSCL は、インプレースアップグレード中に完全に移行されません。RHEL 8 パッケージは通常、RHSCL パッケージを自動的に置き換えますが、カスタマイズされた設定とデータは手動で移行および設定する必要があります。たとえば、RHSCL からデータベースをインストールした場合は、RHSCL パッケージの削除中にデータが失われないように、アップグレード前にすべてのデータをダンプし、システムのアップグレード後に必要に応じてデータを復元する必要があります。Red Hat Satellite サーバーをアップグレードすると、プロジェクトに必要な RHSCL パッケージが自動的に移行されることに注意してください。

- **Red Hat JBoss Enterprise Application Platform (EAP)**- JBoss EAP は RHEL 9 へのアップグレードではサポートされません。アップグレード後に、システムに手動で JBoss EAP をインストールして設定する必要があります。詳細は、In-place Migrating of Jboss EAP and websphere servers along with Linux using leapp utility を参照してください。

- **パブリッククラウド**: インプレースアップグレードは、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform のオンデマンドインスタンスでのみ、Red Hat Update Infrastructure (RHUI) を使用するオンデマンド Pay-As-You-Go (PAYG) インスタンスでサポートされます。インプレースアップグレードは、RHEL サブスクリプションに Red Hat Subscription Manager (RHSM) を使用するすべてのパブリッククラウドの Bring Your Own Subscription インスタンスでもサポートされます。

- **言語**: すべての **Leapp** のレポート、ログ、その他の生成されたドキュメントは、言語設定に関わらず、英語で表示されます。

- **ブートローダー** - RHEL 7 または RHEL 8 でブートローダーを BIOS から UEFI に切り替えることはできません。RHEL 7 システムが BIOS を使用し、RHEL 8 システムで UEFI を使用する場合は、インプレースアップグレードの代わりに RHEL 8 の新規インストールを実行します。詳細は、Is it possible to switch the BIOS boot to UEFI boot on preinstalled Red Hat Enterprise Linux machine? を参照してください。

- **既知の制限** - 現在、**Leapp** の注目すべき既知の制限には以下が含まれます。

  - 現在、ディスク全体またはパーティションの暗号化、またはファイルシステムの暗号化は、インプレースアップグレードの対象となるシステムでは使用できません。

  - イーサネットまたは Infiniband を使用するネットワークベースのマルチパスおよびネットワークストレージは、アップグレードではサポートされていません。これには、FCoE を使用した SAN と FC を使用した SAN からの起動が含まれます。FC を使用した SAN はサポートされていることに注意してください。

  - インプレースアップグレードは、RHEL サブスクリプション用の RHSM ではなく Red Hat Update Infrastructure を使用するパブリッククラウド上のオンデマンド PAYG インスタンスでは現在サポートされていません。

  - インプレースアップグレードは、Ansible Tower を含む Ansible 製品がインストールされているシステムではサポートされません。RHEL 8 で RHEL 7 Ansible Tower インストールを使用する場合は、How do I migrate my Ansible Automation Platform installation from one environment to another?(ナレッジベースのソリューション記事) を参照してください。

既知の問題 も参照してください。

Red Hat Insights を使用して、Insights に登録したどのシステムが RHEL 8 に対する対応アップグレードパスであるかを確認できます。これを行うには、Insights でそれぞれの Advisor の推奨事項 に移動し、**Actions** ドロップダウンメニューで推奨事項を有効にして、**影響を受けるシステム** 見出しの下のリストを調べます。Advisor 推奨は RHEL 7 マイナーバージョンのみを考慮し、システムのアップグレード前の評価は行わないことに注意してください。advisor サービスの推奨事項の概要 も参照してください。

関連情報

- The best practices and recommendations for performing RHEL Upgrade using Leapp

- Leapp upgrade FAQ (Frequently Asked Questions)

第4章 アップグレードの準備

アップグレード後に問題を回避し、システムを RHEL の次のメジャーバージョンにアップグレードできることを確認するには、アップグレード前に必要なすべての準備手順を完了してください。

すべてのシステムで、Preparing a RHEL 7 system for the upgrade で説明されている準備手順を実施する必要があります。さらに、Satellite Server に登録されているシステムでは、Satellite に登録されたシステムのアップグレードの準備 で説明されている準備手順も実行する必要があります。

4.1. アップグレードに向けて RHEL 7 システムの準備

この手順では、**Leapp** ユーティリティーを使用して、RHEL 8 へのインプレースアップグレードを実行する前に必要な手順を説明します。

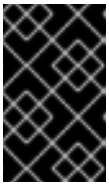
アップグレードプロセス中に Red Hat Subscription Manager を使用する予定がない場合は、Upgrading to RHEL 8 without Red Hat Subscription Manager を参照してください。

前提条件

- システムは、アップグレードの計画 に記載されている条件を満たしている。
- 以前に RHEL 6 から RHEL 7 にアップグレードした場合は、アップグレード後の必要な手動手順がすべて完了しています。これには、RHEL 7 マシン上の GRUB2 ブートローダーへの手動移行が含まれます。詳細は、GRUB Legacy から GRUB 2 へのアップグレード を参照してください。

手順

1. オプション: ナレッジベース記事 The best practices and recommendations for performing RHEL Upgrade using Leapp のベストプラクティスを確認します。
2. Red Hat Subscription Manager を使用して、システムが Red Hat コンテンツ配信ネットワーク (CDN) または Red Hat Satellite に正常に登録されていることを確認します。
3. システムが Satellite Server に登録されている場合は、アップグレードに向けた Satellite 登録システムの準備 の手順を実行して、システムがアップグレードの要件を満たしていることを確認します。



重要

システムが Satellite Server に登録されている場合は、問題の発生を防ぐために、この手順に進む前に アップグレードのための Satellite 登録システムの準備 の手順を完了する必要があります。

4. オプション: システム自体に関係のないデータファイルのみを含むファイルシステムなど、アップグレードに必要のない非システム OS ファイルシステムをアンマウントし、**/etc/fstab** ファイルからコメントアウトします。これにより、アップグレードプロセスに必要な時間が短縮されます。また、アップグレード時にカスタムまたはサードパーティーのアクターによって適切に移行されないサードパーティーアプリケーションに関連する、潜在的な問題を防ぐことができます。
5. subscription-manager を使用してシステムがサブスクライブされていることを確認します。

a. Simple Content Access (SCA) が有効になっているアカウントを使用してシステムが登録されている場合は、**Content Access Mode is set to Simple Content Access** というメッセージが表示されることを確認します。

```
# subscription-manager status
+-------------------------------------------+
   System Status Details
+-------------------------------------------+
Overall Status: Disabled
Content Access Mode is set to Simple Content Access. This host has access to content,
regardless of subscription status.
System Purpose Status: Disabled
```

b. SCA が無効になっているアカウントを使用してシステムが登録されている場合は、Red Hat Linux Server サブスクリプションがアタッチされていること、製品名が **Server** で、ステータスが **Subscribed** であることを確認します。

```
# subscription-manager list --installed
+-------------------------------------------+
     Installed Product Status
+-------------------------------------------+
Product Name:   Red Hat Enterprise Linux Server
Product ID:     69
Version:        7.9
Arch:           x86_64
Status:         Subscribed
```

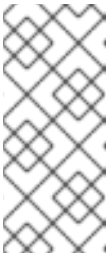
6. 適切なリポジトリーが有効になっていることを確認します。次のコマンドは、64 ビット Intel アーキテクチャーのリポジトリーのリストを示します。他のアーキテクチャーについては、RHEL 7 リポジトリー を参照してください。

a. Base リポジトリーを有効にします。

```
# subscription-manager repos --enable rhel-7-server-rpms
```

b. **Leapp** およびその依存関係が利用可能な Extras リポジトリーを有効にします。

```
# subscription-manager repos --enable rhel-7-server-extras-rpms
```



注記

必要に応じて、オプション (CodeReady Linux Builder とも呼ばれる) または補助リポジトリーを有効にすることができます。リポジトリー ID の詳細は、RHEL 7 リポジトリー のオプションおよび補足リポジトリーのリストを参照してください。これらのリポジトリーの内容の詳細は、CodeReady Linux Builder リポジトリー および 補足リポジトリー を参照してください。

7. 最新の RHEL 7 コンテンツを使用するように Red Hat Subscription Manager を設定します。

```
# subscription-manager release --unset
```

8. オプション: カスタムリポジトリーを使用するには、ナレッジベースの記事 Configuring custom repositories を参照してください。

9. 指定したバージョンにパッケージをロックするために **yum-plugin-versionlock** プラグインを使用している場合は、次のコマンドを実行してロックを解除します。

```
# yum versionlock clear
```

詳細は 指定したバージョンのパッケージ (または指定したバージョン以前のパッケージ) だけをインストールまたはアップグレードできるように yum の使用を制限する方法 を参照してください。

10. パブリッククラウドで Red Hat Update Infrastructure(RHUI) を使用してアップグレードする場合は、必要な RHUI リポジトリーを有効にして、必要な RHUI パッケージをインストールし、システムをアップグレードする準備ができていることを確認します。

a. AWS の場合:

```
# yum-config-manager --enable rhui-client-config-server-7
# yum-config-manager --enable rhel-7-server-rhui-extras-rpms
# yum -y install rh-amazon-rhui-client leapp-rhui-aws
```

b. For Microsoft Azure:

```
# yum-config-manager --enable rhui-microsoft-azure-rhel7
# yum -y install rhui-azure-rhel7
# yum-config-manager --enable rhui-rhel-7-server-rhui-extras-rpms
# yum -y install leapp-rhui-azure
```

注記

Azure 仮想マシンをマイナーリリースにロックした場合は、バージョンロックを削除します。詳細は、Switch a RHEL 7.x VM back to non-EUS を参照してください。

c. Google Cloud Platform の場合は、ナレッジベース記事 Leapp RHUI packages for Google Cloud Platform (GCP) に従います。

11. Docker でコンテナーを管理する場合は、Podman を使用して適切なコンテナーイメージでコンテナーを再作成し、使用中のボリュームを割り当てます。詳細は、How do I migrate my Docker containers to Podman prior to moving from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8? を参照してください。

12. すべてのパッケージを最新の RHEL 7 バージョンに更新します。

```
# yum update
```

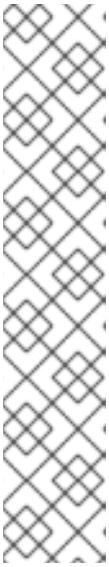
13. システムを再起動します。

```
# reboot
```

14. **Leapp** ユーティリティーをインストールします。

```
# yum install leapp-upgrade
```

現在、**leapp** パッケージのバージョン 0.17.0 以降と、**leapp-upgrade-el7toel8** RPM パッケージを含む **leapp-repository** パッケージのバージョン 0.20.0 以降が必要であることに注意してください。



注記

システムにインターネットアクセスがない場合は、Red Hat カスタマーポータルから以下のパッケージをダウンロードします。

- **leapp**
- **leapp-deps**
- **python2-leapp**
- **leapp-upgrade-el7toel8**
- **leapp-upgrade-el7toel8-deps** 詳細は、How to install leapp packages on an offline system for RHEL 7.9 to RHEL 8.X upgrade? を参照してください。詳細は、ナレッジベースの記事を参照してください。

15. **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ています。これらのデータファイルを古いバージョンに置き換えた場合は、**/etc/leapp/files** ディレクトリー内のすべての JSON ファイルを削除し、**leapp-upgrade-el7toel8** パッケージを再インストールして、データファイルが最新であることを確認します。

16. アップグレードの失敗を防ぐために一時的にウイルス対策ソフトウェアを無効にします。

17. 設定管理システムがインプレースアップグレードプロセスに干渉しないことを確認します。

    - Puppet、Salt、Chef などのクライアントサーバーアーキテクチャーで設定管理システムを使用する場合は、**leapp preupgrade** コマンドを実行する前にシステムを無効にします。アップグレード時に問題が発生するのを防ぐために、アップグレードが完了するまで設定管理システムを有効にしないでください。

    - Ansible などのエージェントレスアーキテクチャーで設定管理システムを使用する場合は、Performing the upgrade from RHEL 7 to RHEL 8 で説明されているように、インプレースアップグレード中に Ansible Playbook などの設定およびデプロイメントファイルを実行しないでください。
      設定管理システムを使用したアップグレード前およびアップグレードプロセスの自動化は、Red Hat ではサポートされていません。詳細は、Using configuration management systems to automate parts of the Leapp pre-upgrade and upgrade process on Red Hat Enterprise Linux を参照してください。

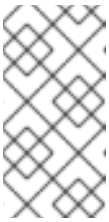
18. システムで、カーネル (**eth**) が使用する接頭辞に基づいた名前で、複数の Network Interface Card (NIC) が使用されていないことを確認します。RHEL 8 へのインプレースアップグレードの前に別の命名スキームに移行する方法は RHEL 7 でカーネルの NIC 名を使用している場合に RHEL 8 へのインプレースアップグレードを実行する方法 を参照してください。

19. ISO イメージを使用してアップグレードする場合は、ISO イメージにターゲット OS バージョン (RHEL 8.8 など) が含まれていること、およびアップグレードプロセス全体を通じて **Leapp** ユーティリティーがイメージにアクセスできるように永続的なローカルマウントポイントに保存されていることを確認してください。

20. システム全体のバックアップまたは仮想マシンのスナップショットが存在することを確認してください。これにより、ご利用の環境で、以下の標準の災害復旧手順に従って、システムを

アップグレード前と同じ状態に戻せるようになります。次のバックアップオプションを使用できます。

- Relax-and-Recover (ReaR) ユーティリティーを使用して、システムの完全バックアップを作成します。詳細は、ReaR documentation および What is Relax and Recover (ReaR) and how can I use it for disaster recovery? を参照してください。
- LVM スナップショット または RAID 分割 を使用して、システムのスナップショットを作成します。仮想マシンをアップグレードする場合は、仮想マシン全体のスナップショットを作成できます。Boom ユーティリティーを使用して、スナップショットとロールバックのブートエントリーを管理することもできます。詳細は、What is BOOM and how to install it? および スナップショットを使用したシステムアップグレードの管理 を参照してください。

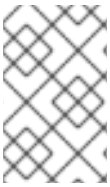


注記

LVM スナップショットではシステムの完全バックアップが作成されないため、特定のアップグレードの失敗後にシステムを復元できない可能性があります。したがって、ReaR ユーティリティーを使用して完全バックアップを作成する方が安全です。

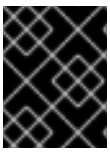
4.2. アップグレードのための SATELLITE 登録システムの準備

この手順では、RHEL 8 へのアップグレード用に Satellite に登録されているシステムを準備するために必要な手順を説明します。



注記

Satellite システム自体をアップグレードする予定の場合は、Leapp を使用して Satellite または Capsule を Red Hat Enterprise Linux 8 にインプレースアップグレードする で説明されている手順に従ってください。



重要

Satellite システムのユーザーは、この手順と Preparing a RHEL 7 system for the upgrade で説明されている準備手順を完了する必要があります。

前提条件

- Satellite Server の管理者権限がある。

手順

1. Satellite は、フルサポートまたはメンテナンスサポートがあるバージョンです。詳細は、Red Hat Satellite の製品ライフサイクル を参照してください。
2. RHEL 8 リポジトリーを使用したサブスクリプションマニフェストを Satellite Server にインポートします。詳細は、Red Hat Satellite の特定のバージョン (バージョン 6.12 など) のコンテンツ管理ガイドの Red Hat サブスクリプションの管理の章を参照してください。
3. Satellite Server で必要なすべての RHEL 7 および RHEL 8 リポジトリーを有効にし、RHEL 7.9 およびターゲット OS バージョン (RHEL 8.10 など) の最新の更新と同期します。必要なリポジトリーはコンテンツビューで利用可能であり、関連付けられたアクティベーションキーで有効になっている必要があります。

注記

RHEL 8 リポジトリーの場合は、各リポジトリーのターゲット OS バージョン (8.10 など) を有効にします。RHEL 8 バージョンのリポジトリーのみを有効にした場合は、インプレースアップグレードは行われません。

たとえば、延長更新サポート (EUS) サブスクリプションがない Intel アーキテクチャーの場合は、少なくとも以下のリポジトリーを有効にします。

- Red Hat Enterprise Linux 7 Server (RPM)
  rhel-7-server-rpms

  x86_64 7Server

- Red Hat Enterprise Linux 7 Server - Extras (RPM)
  rhel-7-server-extras-rpms

  x86_64

- Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
  rhel-8-for-x86_64-appstream-rpms

  x86_64 **<target_os_version>**

- Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
  rhel-8-for-x86_64-baseos-rpms

  x86_64 **<target_os_version>**

  target_os_version は、ターゲット OS バージョン (例: 8.10) に置き換えます。

  その他のアーキテクチャーは、RHEL 7 リポジトリー および RHEL 8 リポジトリー を参照してください。

  詳細は、Red Hat Satellite の特定のバージョン (バージョン 6.12 など) の **コンテンツ管理ガイド** の **コンテンツのインポート** の章を参照してください。

4. 必要な RHEL 7 リポジトリーおよび RHEL 8 リポジトリーを含むコンテンツビューにコンテンツホストを割り当てます。
   詳細は、Red Hat Satellite の特定のバージョン (バージョン 6.12 など) の **コンテンツ管理ガイド** の **コンテンツビューの管理** の章を参照してください。

検証

1. 正しい RHEL 7 リポジトリーおよび RHEL 8 リポジトリーが Satellite Server の正しいコンテンツビューに追加されていることを確認します。

   a. Satellite Web UI で、**Content > Lifecycle > Content Views**に移動して、コンテンツビューの名前をクリックします。

   b. **Repositories** タブをクリックして、リポジトリーが正しく表示されることを確認します。

注記

以下のコマンドを使用して、リポジトリーがコンテンツビューに追加されていることを確認することもできます。

```
# hammer repository list --search 'content_label ~ rhel-7' --content-view <content_view_name> --organization <organization> --lifecycle-environment <lifecycle_environment>
# hammer repository list --search 'content_label ~ rhel-8' --content-view <content_view_name> --organization <organization> --lifecycle-environment <lifecycle_environment>
```

<content_view_name> をコンテンツビューの名前に、**<organization>** を組織に、**<lifecycle_environment>** をライフサイクル環境の名前に置き換えます。

2. コンテンツビューに関連付けられたアクティベーションキーで、正しい RHEL 8 リポジトリーが有効になっていることを確認します。

   a. Satellite Web UI で、**Content > Lifecycle > Activation Keys**に移動し、アクティベーションキーの名前をクリックします。

   b. **Repository Sets** タブをクリックし、必要なリポジトリーのステータスが **Enabled** であることを確認します。

3. 予想されるすべての RHEL 7 リポジトリーがホストで有効になっていることを確認します。以下に例を示します。

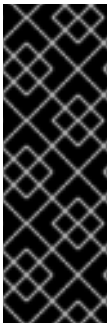
```
# subscription-manager repos --list-enabled | grep "^Repo ID"
Repo ID:   rhel-7-server-extras-rpms
Repo ID:   rhel-7-server-rpm
```

第5章 アップグレード前のレポートの確認

システムのアップグレード可能性を評価するには、**leapp preupgrade** コマンドでアップグレード前のプロセスを開始します。このフェーズでは、**Leapp** ユーティリティーがシステムに関するデータを収集し、アップグレードの可能性を評価し、アップグレード前のレポートを生成します。アップグレード前のレポートは、潜在的な問題についてまとめ、推奨される解決策を提案します。このレポートは、アップグレードを進めることが可能かどうかの判断にも役立ちます。

注記

アップグレード前の評価ではシステム設定は変更されませんが、**/var/lib/leapp** ディレクトリーの無視できないサイズの領域が消費されます。ほとんどの場合、アップグレード前の評価には最大 4 GB の領域が必要ですが、実際のサイズはシステム設定によって異なります。ホストされたファイルシステムに十分な領域がない場合、アップグレード前のレポートに完全な分析結果が表示されない可能性があります。問題を防ぐには、システムの **/var/lib/leapp** ディレクトリーに十分な領域があることを確認するか、領域の消費がシステムの他の部分に影響を与えないようにディレクトリーを専用のパーティションに移動してください。



重要

レポートでアップグレードの阻害要因が見つからない場合でも、必ずアップグレード前レポート全体を確認してください。アップグレード前のレポートには、アップグレードされたシステムが正しく機能することを確認するために、アップグレード前に完了する推奨アクションが含まれています。

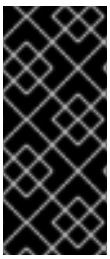
インプレースアップグレードプロセスではなく、RHEL 8 システムの新規インストールを実行する場合も、アップグレード前のレポートを確認すると有用です。

次のいずれかの方法を使用して、アップグレード前の段階でアップグレード可能性を評価できます。

- 生成された **leapp-report.txt** ファイルのアップグレード前レポートを確認し、コマンドラインインターフェイスを使用して、報告された問題を手動で解決します。
- Web コンソールを使用してレポートを確認し、利用可能な場合は自動修復を適用し、推奨される修復ヒントを使用して残りの問題を修正します。

注記

たとえば、独自のカスタムスクリプトを使用してアップグレード前のレポートを処理し、異なる環境間にある複数のレポートの結果を比較できます。詳細は Red Hat Enterprise Linux のアップグレード前のレポートワークフローの自動化 を参照してください。



重要

アップグレード前のレポートでは、インプレースアップグレードプロセス全体をシミュレートできないため、システムの阻害要因となる問題をすべて特定することはできません。その結果、レポート内のすべての問題を確認して修正した後でも、インプレースアップグレードが終了する可能性があります。たとえば、アップグレード前のレポートでは、壊れたパッケージのダウンロードに関連する問題は検出できません。

5.1. コマンドラインからのアップグレード可能性の評価

コマンドラインインターフェイスを使用して、アップグレード前のフェーズで潜在的なアップグレードの問題を特定します。

前提条件

- Preparing for the upgrade に記載されている手順が完了しました。

手順

1. RHEL 7 システムで、アップグレード前のフェーズを別途実行します。

```
# leapp preupgrade --target <target_os_version>
```

<target_os_version> は、ターゲット OS バージョン (例: 8.10) に置き換えます。ターゲット OS バージョンが定義されていない場合、**Leapp** は表 1.1 で指定されたデフォルトのターゲット OS バージョンを使用します (サポートされるアップグレードパス)。

- アップグレードに **/etc/yum.repos.d/** ディレクトリーの カスタムリポジトリー を使用する場合は、以下のように選択したリポジトリーを有効にします。

```
# leapp preupgrade --enablerepo <repository_id1> --enablerepo <repository_id2> ...
```

- RHSM なしでアップグレード する場合、または RHUI を使用する場合は、**--no-rhsm** オプションを追加します。

- Extended Upgrade Support (EUS)、Advanced Update Support (AUS)、または Update Services for SAP Solutions (E4S) のサブスクリプションがある場合は、**--channel <channel>** オプションを追加します。

  - RHEL 8.8 にアップグレードする場合は、**チャネル** をチャネル名 (**eus**、**aus**、**e4s** など) に置き換えます。SAP HANA を利用している場合はHow to in-place upgrade SAP environments from RHEL 7 to RHEL 8 ガイドを使用してインプレースアップグレードを実行する必要があることに注意してください。

  - RHEL 8.10 にアップグレードする場合は、**チャネル** を **ga** に置き換えます。

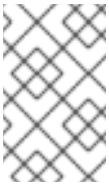
2. **/var/log/leapp/leapp-report.txt** ファイル内のレポートを調べて、報告されたすべての問題を手動で解決します。報告された問題の中には、修正の提案が含まれているものもあります。**阻害**要因の問題があると、それを解決するまでアップグレードできません。レポートに表示される可能性のあるさまざまな問題の詳細は、Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 にアップグレードするにはどうすればよいですか? のアップグレード前の手順を参照してください。
レポートには次のリスク因子レベルが含まれます。

High
: システム状態が悪化する可能性が非常に高い

中
: システムとアプリケーションの両方に影響を与える可能性がある

Low
: システムに影響はないが、アプリケーションに影響を与える可能性がある

Info
: システムまたはアプリケーションへの影響がないと考えられる情報



注記

見つかった問題の重大度と影響、およびそれらを解決するために必要な作業量に応じて、インプレースアップグレードを続行するのではなく、RHEL 8 のクリーンインストールを実行する方が望ましい場合があります。

3. 特定のシステム設定では、**Leapp** ユーティリティーは手動で回答する必要がある True/false の質問表を生成します。アップグレード前のレポートに **Missing required answers in the answer file** のメッセージが含まれる場合は、次の手順を実行します。

   a. **/var/log/leapp/answerfile** ファイルを開き、true または false の質問を確認します。

   b. **/var/log/leapp/answerfile** ファイルを手動で編集し、**#** 記号を削除してファイルの確認行のコメントを解除し、**True** または **False** として回答を確定します。詳細は、Leapp 回答ファイル を参照してください。

注記

または、以下のコマンドを実行して、True/false の質問に回答できます。

```
# leapp answer --section <question_section>.<field_name>=<answer>
```

たとえば、**PAM 設定で pam_pkcs11 モジュールを無効にするか ?**という質問に **False** を確定するには、以下のコマンドを実行します。

```
# leapp answer --section
remove_pam_pkcs11_module_check.confirm=False
```

4. 前の手順を繰り返してアップグレード前レポートを再実行し、すべての重要な問題が解決されたことを確認します。

5.2. WEB コンソールを介したアップグレードの可能性の評価および自動修復の適用

アップグレード前のフェーズで潜在的な問題と、Web コンソールを使用して自動修復を適用する方法を特定します。

前提条件

- アップグレードの準備 に記載されている手順を完了している。

手順

1. **cockpit-leapp** プラグインをインストールします。

```
# dnf install cockpit-leapp
```

root として、または **sudo** で管理コマンドを入力するパーミッションがあるユーザーとして Web コンソールにログインします。Web コンソールの詳細は、RHEL 7 Web コンソールを使用したシステムの管理 を参照してください。

2. RHEL 7 システムで、コマンドラインインターフェイスまたは Web コンソールの端末からアップグレード前のフェーズを実行します。

```
# leapp preupgrade --target <target_os_version>
```

<target_os_version> は、ターゲット OS バージョン (例: 8.10) に置き換えます。ターゲット OS バージョンが定義されていない場合、**Leapp** は表 1.1 で指定されたデフォルトのターゲット OS バージョンを使用します (サポートされるアップグレードパス)。

- アップグレードに **/etc/yum.repos.d/** ディレクトリーの カスタムリポジトリー を使用する場合は、以下のように選択したリポジトリーを有効にします。

```
# leapp preupgrade --enablerepo <repository_id1> --enablerepo <repository_id2> ...
```

- RHSM なしでアップグレード する場合、または RHUI を使用する場合は、 **--no-rhsm** オプションを追加します。

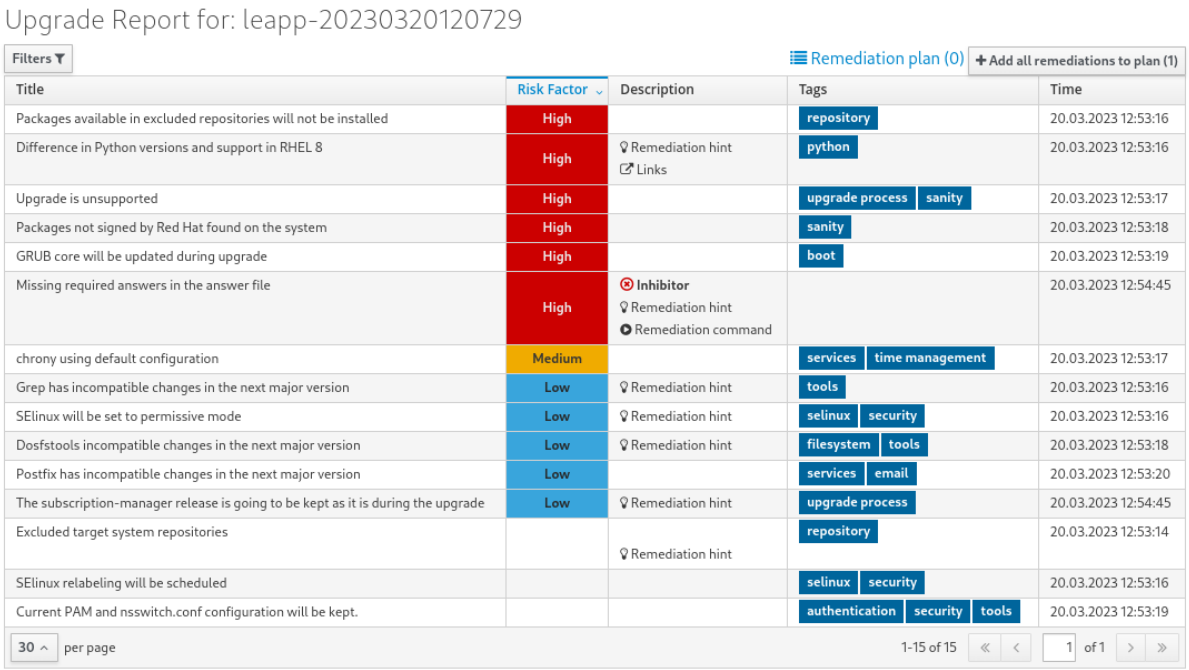
- Extended Upgrade Support (EUS)、Advanced Update Support (AUS)、または Update Services for SAP Solutions (E4S) のサブスクリプションがある場合は、**--channel <channel>** オプションを追加します。

  - RHEL 8.8 にアップグレードする場合は、**チャネル** をチャネル名 (**eus**、**aus**、**e4s** など) に置き換えます。SAP HANA を利用している場合はHow to in-place upgrade SAP environments from RHEL 7 to RHEL 8 ガイドを使用してインプレースアップグレードを実行する必要があることに注意してください。

  - RHEL 8.10 にアップグレードする場合は、**チャネル** を **ga** に置き換えます。

3. Web コンソールで、ナビゲーションメニューから **Upgrade Report** を選択し、報告されたすべての問題を確認します。**阻害** 要因の問題があると、それを解決するまでアップグレードできません。レポートに表示される可能性のあるさまざまな問題の詳細は、Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 にアップグレードするにはどうすればよいですか? のアップグレード前の手順を参照してください。
問題を詳細に表示するには、行を選択して詳細ペインを開きます。

図5.1 Web コンソールのインプレースアップグレードレポート



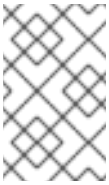
レポートには次のリスク因子レベルが含まれます。

High
システム状態が悪化する可能性が非常に高い

中
システムとアプリケーションの両方に影響を与える可能性がある

Low
システムに影響はないが、アプリケーションに影響を与える可能性がある

Info
システムまたはアプリケーションへの影響がないと考えられる情報



注記

見つかった問題の重大度と影響、およびそれらを解決するために必要な作業量に応じて、インプレースアップグレードを続行するのではなく、RHEL 8 のクリーンインストールを実行する方が望ましい場合があります。

4. 特定の設定では、**Leapp** ユーティリティーは手動で回答する必要がある True/false の質問表を生成します。アップグレードレポートの **回答ファイルで必須の回答が抜けている** 行が含まれている場合は、次の手順を実行します。

   a. **回答ファイルで必須の回答が抜けている** 行を選択し、**Detail** ペインを開きます。デフォルトの回答は修復コマンドの最後に記載されています。

   b. デフォルトの応答を確定するには、**Add to Remediation Plan** を選択して修復を後で実行するか、**Run Remediation** を選択して修復をすぐに実行します。

   c. 代わりにデフォルト以外の回答を選択するには、回答する質問と確認済みの回答を指定して、ターミナルで **Leapp Answer** コマンドを実行します。

   ```
   # leapp answer --section <question_section>.<field_name>=<answer>
   ```

   たとえば、**PAM 設定で pam_pkcs11 モジュールを無効にするか ?**という質問に **False** を確定するには、以下のコマンドを実行します。

   ```
   # leapp answer --section remove_pam_pkcs11_module_check.confirm=False
   ```

   注記

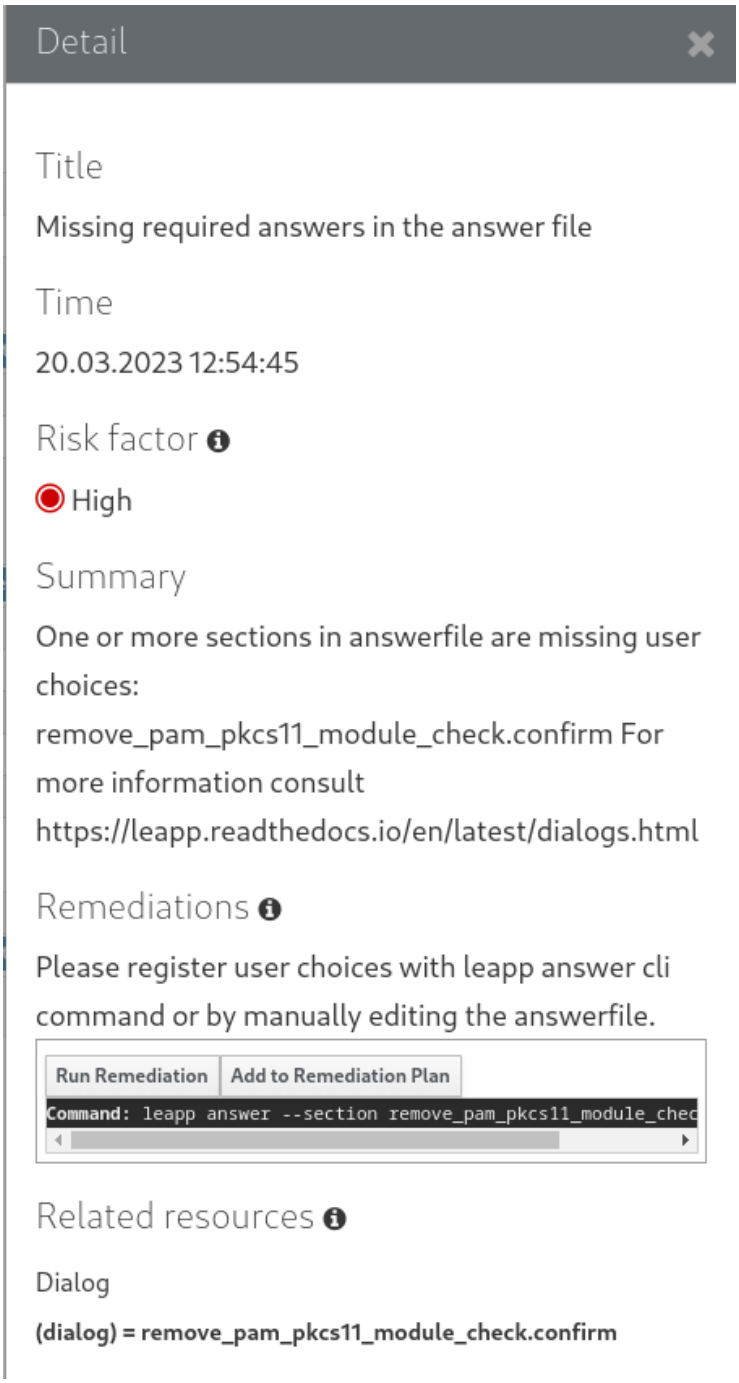
   /var/log/leapp/answerfile ファイルを手動で編集し、**#** 記号を削除してファイルの confirm 行のコメントを解除し、**True** または **False** として回答を確定します。詳細は、Leapp 回答ファイルの例 を参照してください。

5. 一部の問題には、問題を自動的に解決するために実行できる修復コマンドがあります。修復コマンドは個別に実行することも、修復コマンドでまとめて実行することもできます。

   a. 単一の修復コマンドを実行するには、問題の **Detail** ペインを開き、**Run Remediation** をクリックします。

   b. 修復コマンドを修復計画に追加するには、問題の **Detail** ペインを開き、**Add to Remediation Plan** をクリックします。

図5.2 詳細ペイン



c. 追加されたすべての修復コマンドを含む修復計画を実行するには、レポートの右上隅にある **Remediation plan** リンクをクリックします。**Execute Remediation Plan** をクリックして、一覧表示されたすべてのコマンドを実行します。

6. レポートを確認し、報告されたすべての問題を解決したら、手順 3 ~ 7 を繰り返してレポートを再実行し、すべての重要な問題が解決されたことを確認します。

第6章 RHEL 7 から RHEL 8 へのアップグレードの実行

Leapp ユーティリティーを使用して RHEL 8 にアップグレードします。

前提条件

- フルシステムバックアップを含め、Preparing for the upgrade の手順が完了しました。
- アップグレード前のレポートの確認 に記載されている手順が完了し、報告されたすべての問題が解決されました。

手順

1. RHEL 7 システムで、アップグレードプロセスを開始します。

```
# leapp upgrade --target <target_os_version>
```

<target_os_version> は、ターゲットオペレーティングシステム (OS) バージョン (例: 8.10) に置き換えます。ターゲット OS バージョンが定義されていない場合、**Leapp** は表 1.1 で指定されたデフォルトのターゲット OS バージョンを使用します (サポートされるアップグレードパス)。

注記

アップグレードに **/etc/yum.repos.d/** ディレクトリーの カスタムリポジトリー を使用する場合は、以下のように選択したリポジトリーを有効にします。

```
# leapp upgrade --enablerepo <repository_id1> --enablerepo
<repository_id2> ...
```

RHSM なしでアップグレード する場合、または RHUI を使用する場合は、**--no-rhsm** オプションを追加します。

ISO イメージを使用してアップグレードする場合は、**--no-rhsm** および **--iso <file_path>** オプションを追加します。**<file_path>** は、保存された ISO イメージへのファイルパス (**/home/rhel8.iso** など) に置き換えます。

Extended Upgrade Support (EUS)、Advanced Update Support (AUS)、または Update Services for SAP Solutions (E4S) のサブスクリプションがある場合は、**--channel <channel>** オプションを追加します。

- RHEL 8.8 にアップグレードする場合は、**チャネル** を **leapp preupgrade** コマンドで使用した値 (**eus**、**aus**、**e4s** など) に置き換えます。**leapp preupgrade** および **leapp upgrade** コマンドの両方で、**--channel** オプションで同じ値を使用する必要があります。
- RHEL 8.10 にアップグレードする場合は、**チャネル** を **ga** に置き換えます。

アップグレードプロセスの開始時に、**Leapp** は、アップグレード前のレポートの確認 で説明されているアップグレード前のフェーズを実行します。

システムをアップグレードできる場合は、**Leapp** が必要なデータをダウンロードし、アップグレード用の RPM トランザクションを作成します。

システムで、信頼できるアップグレードの設定要因が満たされていない場合は、**Leapp** がアップグレードプロセスを中止し、問題を説明する記録と、推奨される解決策を **/var/log/leapp/leapp-report.txt** ファイルに出力します。詳細は、トラブルシューティング を参照してください。

2. システムを手動で再起動します。

```
# reboot
```

このフェーズでは、システムが RHEL 8 ベースの初期 RAM ディスクイメージ initramfs で起動します。**Leapp** は、すべてのパッケージをアップグレードして、自動的に RHEL 8 システムを再起動します。

または、**--reboot** オプションを指定して **leapp upgrade** コマンドを入力し、この手動の手順を省略することもできます。

失敗した場合は、トラブルシューティング の説明に従ってログを調べてください。

3. RHEL 8 システムにログインし、RHEL 8 システムのアップグレード後の状態の確認 で説明されているように状態を確認します。

4. アップグレードレポートおよびアップグレード後のタスク の実行で説明されているすべてのアップグレード後のタスクを 実行します。特に、セキュリティーポリシーを再評価して再適用します。

5. **FIPS モード** で実行されているシステムをアップグレードする場合は、RHEL 7 カーネルをすべて削除します。次に、暗号化キーの再生成などを行い、すべての暗号化キーの FIPS 準拠を確認します。詳細は、RHEL 8 の暗号化キーの場所 を参照してください。

第7章 RHEL 8 システムのアップグレード後の状態の確認

この手順は、RHEL 8 へのインプレースアップグレード後に実行が推奨される検証手順を紹介します。

前提条件

- RHEL 7 から RHEL 8 へのアップグレードの実行 に記載されている手順に従ってシステムをアップグレードし、RHEL 8 にログインできる。

手順

アップグレードが完了したら、システムが必要な状態になっていることを確認します。少なくとも以下の確認を行います。

- 現在のオペレーティングシステムのバージョンが Red Hat Enterprise Linux 8 であることを確認します。

```
# cat /etc/redhat-release
Red Hat Enterprise Linux release <target_os_version> (Ootpa)
```

target_os_version は、ターゲット OS バージョン (例: 8.10) に置き換えます。

- オペレーティングシステムのカーネルバージョンを確認します。

```
# uname -r
4.18.0-305.el<target_os>.x86_64
```

target_os は、**8** またはターゲット OS バージョンのいずれかである必要があります (例: **8_10**)。**.el8** は重要であるため、このバージョンは 4.18.0-305 よりも前のバージョンにはならないことに注意してください。

- Red Hat Subscription Manager を使用している場合:
  - 正しい製品がインストールされていることを確認します。

```
# subscription-manager list --installed
+-------------------------------------------+
    Installed Product Status
+-------------------------------------------+
Product Name: Red Hat Enterprise Linux for x86_64
Product ID:   479
Version:      <target_os_version>
Arch:         x86_64
Status:       Subscribed
```

target_os_version は、ターゲット OS バージョン (例: 8.10) に置き換えます。

  - アップグレード直後にリリースバージョンがターゲットの OS バージョンに設定されていることを確認します。

```
# subscription-manager release
Release: <target_os_version>
```

target_os_version は、ターゲット OS バージョン (例: 8.10) に置き換えます。

- ネットワークサービスが機能していることを確認します。たとえば、SSH を使用してサーバーに接続します。
- アプリケーションのアップグレード後のステータスを確認します。場合によっては、移行や設定を手動で変更しないといけない場合があります。たとえば、データベースを移行するには、RHEL 8 データベースサーバーのドキュメント の説明に従ってください。

第8章 アップグレード後のタスクの実行

RHEL 8 へのインプレースアップグレード後に、次の主要なタスクが推奨されます。

前提条件

- RHEL 7 から RHEL 8 へのアップグレード の実行で説明されている手順に従ってシステムをアップグレードし、RHEL 8 にログインできる。
- RHEL 8 システムのアップグレード後のステータスの確認 で説明されている手順に従って、インプレースアップグレードのステータスを確認している。

手順

アップグレードが完了したら、以下のタスクを実行します。

1. **snactor** パッケージを含む、**/etc/dnf/dnf.conf** 設定ファイルの exclude リストから残りの **Leapp** パッケージを削除します。インプレースアップグレード中に、**Leapp** ユーティリティーでインストールされた **Leapp** パッケージが exclude リストに自動的に追加され、重要なファイルが削除または更新されないようにします。インプレースアップグレードの後、これらの **Leapp** パッケージをシステムから削除する前に、除外リストから削除する必要があります。
   - exclude リストからパッケージを手動で削除するには、**/etc/dnf/dnf.conf** 設定ファイルを編集し、**除外** リストから必要な **Leapp** パッケージを削除します。
   - **除外** リストからすべてのパッケージを削除するには、次のコマンドを実行します。

     ```
     # yum config-manager --save --setopt exclude=''
     ```

2. 残りの **Leapp** パッケージを含む残りの RHEL 7 パッケージを削除します。
   a. 以前のカーネルバージョンを確認します。

      ```
      # cd /lib/modules && ls -d *.el7*
      ```

   b. 以前のカーネルから弱いモジュールを削除します。以前のカーネルが複数ある場合は、カーネルごとに次の手順を繰り返します。

      ```
      # [ -x /usr/sbin/weak-modules ] && /usr/sbin/weak-modules --remove-kernel <version>
      ```

      <version> を、前の手順で確認したカーネルバージョンに置き換えます。以下に例を示します。

      ```
      #  [ -x /usr/sbin/weak-modules ] && /usr/sbin/weak-modules --remove-kernel 3.10.0-1160.25.1.el7.x86_64
      ```

      注記

      以下のエラーメッセージは無視してください。これは、カーネルパッケージが過去に削除されている場合に生成されます。

      ```
      /usr/sbin/weak-modules: line 1081: cd: /lib/modules/<version>/weak-updates: No such file or directory
      ```

c. 古いカーネルをブートローダーエントリーから削除します。以前のカーネルが複数ある場合は、カーネルごとにこの手順を繰り返します。

```
# /bin/kernel-install remove <version> /lib/modules/<version>/vmlinuz
```

version を、前の手順で確認したカーネルバージョンに置き換えます。以下に例を示します。

```
# /bin/kernel-install remove 3.10.0-1160.25.1.el7.x86_64 /lib/modules/3.10.0-1160.25.1.el7.x86_64/vmlinuz
```

d. 残りの RHEL 7 パッケージを見つけます。

```
# rpm -qa | grep -e '\.el[67]' | grep -vE '^(gpg-pubkey|libmodulemd|katello-ca-consumer)' | sort
```

e. RHEL 8 システムから、古いカーネルパッケージなど、残りの RHEL 7 パッケージと **kernel-workaround** パッケージを削除します。

f. 残りの **Leapp** 依存関係パッケージを削除します。

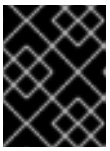
```
# yum remove leapp-deps-el8 leapp-repository-deps-el8
```

g. 残りの空のディレクトリーを削除します。

```
# rm -r /lib/modules/*el7*
```

3. オプション: 残っているすべてのアップグレード関連データをシステムから削除します。

```
# rm -rf /var/log/leapp /root/tmp_leapp_py3 /var/lib/leapp
```



重要

このデータを削除すると、Red Hat サポートによるアップグレード後の問題の調査とトラブルシューティングが制限される可能性があります。

4. RHEL 8 でパッケージをインストールまたは使用できない YUM リポジトリーを無効にします。RHSM によって管理されるリポジトリーは自動的に処理されます。これらのリポジトリーを無効にするには、以下を実行します。

```
# yum config-manager --set-disabled <repository_id>
```

<repository_id> はリポジトリー ID に置き換えます。

5. 現在のカーネルコマンドラインの引数を新しいデフォルトに設定して、将来のカーネル更新が正しいパラメーターで起動するようにします。

- IBM Z アーキテクチャーの場合:

```
# BOOT_OPTIONS="$(tr -s "$IFS" '\n' </proc/cmdline | grep -ve '^BOOT_IMAGE=' -e '^initrd=' | tr '\n' ' ')"
# echo $BOOT_OPTIONS > /etc/kernel/cmdline
```

- その他のアーキテクチャーの場合:

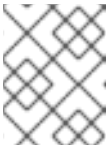
```
# BOOT_OPTIONS="$(tr -s "$IFS" '\n' </proc/cmdline | grep -ve '^BOOT_IMAGE=' -e
'^initrd=' | tr '\n' ' ')"
# grub2-editenv - set "kernelopts=$BOOT_OPTIONS"
```

6. 古いレスキューカーネルと初期 RAM ディスクを現在のカーネルとディスクに置き換えます。
   a. 既存のレスキューカーネルと初期 RAM ディスクを削除します。

```
# rm /boot/vmlinuz-*rescue* /boot/initramfs-*rescue*
```

   b. レスキューカーネルと関連する初期 RAM ディスクを再インストールします。

```
# /usr/lib/kernel/install.d/51-dracut-rescue.install add "$(uname -r)" /boot "/boot/vmlinuz-
$(uname -r)"
```



注記

リアルタイムシステムなど、システムのカーネルパッケージの名前が異なる場合は、**kernel-core** を正しいパッケージ名に置き換えます。

   c. システムが IBM Z アーキテクチャーを使用している場合は、zipl ブートローダーを更新します。

```
# zipl
```

7. セキュリティーポリシーを再評価して再適用します。具体的には、SELinux モードを Enforcing に変更します。詳細は、セキュリティーポリシーの適用 を参照してください。

検証手順

1. 古いカーネルがブートローダーエントリーから削除されていることを確認します。

```
# grubby --info=ALL | grep "\.el7" || echo "Old kernels are not present in the bootloader."
```

2. 以前に削除したレスキューカーネルとレスキュー初期 RAM ディスクファイルが現在のカーネル用に作成されていることを確認します。

```
# ls /boot/vmlinuz-*rescue* /boot/initramfs-*rescue*
# lsinitrd /boot/initramfs-*rescue*.img | grep -qm1 "$(uname -r)/kernel/" && echo "OK" || echo
"FAIL"
```

3. レスキューブートエントリーが既存のレスキューファイルを参照していることを確認します。grubby の出力を参照してください。

```
# grubby --info $(ls /boot/vmlinuz-*rescue*)
```

第9章 セキュリティーポリシーの適用

インプレースアップグレードプロセスでは、特定のセキュリティーポリシーを無効にしたままにする必要があります。さらに、RHEL 8 ではシステム全体の暗号化ポリシーという概念が新たに導入され、セキュリティープロファイルにはメジャーリリース間の変更が含まれる可能性があります。システムのセキュリティーを強化するには、SELinux を enforcing モードに切り替えて、システム全体の暗号化ポリシーを設定します。特定のセキュリティープロファイルに準拠するようにシステムを修正することもできます。

9.1. SELINUX モードの ENFORCING への変更

Leapp ユーティリティーは、インプレースアップグレードプロセス時に SELinux モードを Permissive に設定します。システムが正常にアップグレードされたら、手動で SELinux モードを Enforcing に変更する必要があります。

前提条件

- システムがアップグレードされ、RHEL 8 システムのアップグレード後の状態の確認 で説明されている検証手順を実行している。

手順

1. **ausearch** ユーティリティーなどを使用して、SELinux 拒否がないことを確認します。

```
# ausearch -m AVC,USER_AVC -ts boot
```

前述の手順では、最も一般的なシナリオのみが扱われることに注意してください。可能な SELinux 拒否をすべて確認するには、完全な手順を説明する SELinux の使用の SELinux 拒否の特定 セクションを参照してください。

2. 任意のテキストエディターで **/etc/selinux/config** ファイルを開きます。以下に例を示します。

```
# vi /etc/selinux/config
```

3. **SELINUX=enforcing** オプションを設定します。

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

4. 変更を保存して、システムを再起動します。

```
# reboot
```

検証

1. システムの再起動後に、**getenforce** コマンドが **Enforcing** を返すことを確認します。

```
$ getenforce
Enforcing
```

関連情報

- SELinux 関連の問題のトラブルシューティング
- SELinux のステータスおよびモードの変更

9.2. システム全体の暗号化ポリシーの設定

システム全体の暗号化ポリシーは、コア暗号化サブシステムを設定するシステムコンポーネントで、TLS、IPSec、SSH、DNSSec、および Kerberos の各プロトコルに対応します。

インストールまたはインプレースアップグレードプロセスに成功すると、システム全体の暗号化ポリシーは自動的に **DEFAULT** に設定されます。**DEFAULT** のシステム全体の暗号化ポリシーレベルで、現在の脅威モデルに対して安全なものです。

現在のシステム全体の暗号化ポリシーを表示または変更するには、update-crypto-policies tool ツールを使用します。

```
$ update-crypto-policies --show
DEFAULT
```

たとえば、以下のコマンドは、システム全体の暗号化ポリシーレベルを **FUTURE** に切り替えます。これで、近い将来の攻撃に耐えられるはずです。

```
# update-crypto-policies --set FUTURE
Setting system policy to FUTURE
```

システム全体の暗号化ポリシーをカスタマイズすることもできます。詳細は、サブポリシーを使用したシステム全体の暗号化ポリシーのカスタマイズ および システム全体のカスタム暗号化ポリシーの作成および設定 を参照してください。

関連情報

- システム全体の暗号化ポリシーの使用
- **update-crypto-policies(8)** の man ページ。

9.3. セキュリティーベースラインが強化されたシステムのアップグレード

正常に RHEL 8 へアップグレードした後に、システムを完全に強化するには、OpenSCAP スイートが提供する自動修復を使用できます。OpenSCAP 修復は、PCI-DSS、OSPP、または ACSC Essential Eight などのセキュリティーベースラインに、お使いのシステムを合わせます。設定コンプライアンスに関する推奨事項は、セキュリティーオファリングが進化したため、Red Hat Enterprise Linux のメジャーバージョン間で異なります。

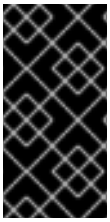
強化された RHEL 7 システムをアップグレードする場合、**Leapp** ツールは完全な強化を保持する直接的な手段を **提供しません**。コンポーネント設定の変更によっては、アップグレード中に RHEL 8 の推奨環境とは異なる場合があります。

注記

RHEL 7 および RHEL 8 のスキャンに同じ SCAP コンテンツを使用することはできません。システムのコンプライアンスが Red Hat Satellite や Red Hat Insights などのツールで管理されている場合は、管理プラットフォームを更新します。

自動修復の代わりに、OpenSCAP で生成されたレポートに従って、手動で変更を行うことができます。コンプライアンスレポートの生成に関する情報は、セキュリティーコンプライアンスと脆弱性についてのシステムのスキャン を参照してください。

以下の手順に従って、PCI-DSS プロファイルでシステムを自動的に強化します。



重要

自動修復は、デフォルト設定の RHEL システムで対応しています。インストール後にシステムのアップグレードが変更されたため、修復を実行しても、必要なセキュリティープロファイルに完全に準拠しない場合があります。一部の要件を手動で修正する必要がある場合があります。

前提条件

- RHEL 8 システムに、**scap-security-guide** パッケージがインストールされている。

手順

1. 適切なセキュリティーコンプライアンスデータストリームの **.xml** ファイルを見つけます。

```
$ ls /usr/share/xml/scap/ssg/content/
ssg-firefox-cpe-dictionary.xml  ssg-rhel6-ocil.xml
ssg-firefox-cpe-oval.xml        ssg-rhel6-oval.xml
...
ssg-rhel6-ds-1.2.xml          ssg-rhel8-oval.xml
ssg-rhel8-ds.xml              ssg-rhel8-xccdf.xml
...
```

   詳細は、コンプライアンスプロファイルの表示 を参照してください。

2. 適切なデータストリームから選択したプロファイルに従って、システムを修正します。

```
# oscap xccdf eval --profile pci-dss --remediate /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

   --profile 引数の **pci-dss** 値は、システムを強化するプロファイルの ID に置き換えることができます。RHEL 8 でサポートされるプロファイルの完全なリストについては、SCAP security profiles supported in RHEL を参照してください。

警告

Remediate オプションを有効にしてシステム評価を実行した場合、慎重に行わないと、システムが機能不全に陥る場合があります。Red Hat は、セキュリティーを強化した修復で加えられた変更を元に戻す自動手段は提供していません。修復は、デフォルト設定の RHEL システムで対応しています。インストール後にシステムが変更した場合は、修復を実行しても、必要なセキュリティープロファイルに準拠しない場合があります。

3. システムを再起動します。

```
# reboot
```

検証

1. システムがプロファイルに準拠していることを確認し、結果を HTML ファイルに保存します。

```
$ oscap xccdf eval --report pcidss_report.html --profile pci-dss
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

関連情報

- **scap-security-guide(8)** および **oscap(8)`** の man ページ
- セキュリティーコンプライアンスおよび脆弱性スキャンの開始
- Red Hat Insights セキュリティーポリシーのドキュメント
- Red Hat Satellite セキュリティーポリシーのドキュメント

第10章 トラブルシューティング

RHEL 7 から RHEL 8 へのアップグレードのトラブルシューティングには、以下のヒントを参照してください。

10.1. トラブルシューティングのリソース

以下のトラブルシューティングリソースを参照してください。

コンソールの出力

デフォルトでは、**Leapp** ユーティリティーにより、エラーおよび重要なログレベルメッセージのみがコンソールに出力されます。ログレベルを変更するには、**leapp upgrade** コマンドで **--verbose** オプションまたは **--debug** オプションを使用します。

- verbose モードでは、**Leapp** により情報、警告、エラー、および重要なメッセージが出力されます。
- debug モードでは、**Leapp** によりデバッグ、情報、警告、エラー、および重要なメッセージを出力します。

ログ

- **/var/log/leapp/leapp-upgrade.log** ファイルには、initramfs フェーズで見つかった問題が記載されます。
- **/var/log/leapp/dnf-debugdata/** ディレクトリーには、トランザクションのデバッグデータが含まれます。このディレクトリーは、**leapp upgrade** コマンドに **--debug** オプションを使用して実行した場合に限り表示されます。
- **/var/log/leapp/answerfile** には、**Leapp** による回答が必要な質問が含まれています。
- **journalctl** ユーティリティーでは、すべてのログが出力されます。

レポート

- **/var/log/leapp/leapp-report.txt** ファイルには、アップグレード前のフェーズで見つかった問題が記載されます。レポートは、Web コンソールでも利用できます。アップグレードの可能性と、Web コンソールで自動修復の適用 を参照してください。
- **/var/log/leapp/leapp-report.json** ファイルには、マシンが判読可能な形式でアップグレード前のフェーズで見つかった問題が記載され、カスタムスクリプトを使用してレポートを処理することができます。詳細は Red Hat Enterprise Linux のアップグレード前のレポートワークフローの自動化 を参照してください。

10.2. トラブルシューティングのヒント

以下のトラブルシューティングのヒントを参照してください。

アップグレード前のフェーズ

- アップグレードの計画 に記載されている条件をすべて満たしていることを確認します。
- Preparing for the upgrade に記載されているすべての手順を行ってください。たとえば、システムで、カーネル (**eth**) が使用する接頭辞に基づいた名前を持つ NIC (Network Interface Card) を複数使用しないようにします。

- **/var/log/leapp/answerfile** ファイルで、**Leapp** に必要な質問をすべて回答している。回答が見つからない場合は、**Leapp** によりアップグレードが行われません。質問例:
  - PAM 設定で pam_pkcs11 モジュールを無効にするか？
  - PAM 設定で pam_krb5 モジュールを無効にするか？
  - 以下の authselect コールで PAM および nsswitch.conf を設定しますか？
- アップグレード前のレポートで特定されたすべての問題は、**/var/log/leapp/leapp-report.txt** にあることを確認してください。これを行うには、Web コンソールでアップグレードの可能性の評価および自動修復の適用 で説明されているように、Web コンソールを使用することも可能です。

例10.1 Leapp answerfile

以下は、編集されていない **/var/log/leapp/answerfile** ファイルの例です。

```
[remove_pam_pkcs11_module_check]
# Title:          None
# Reason:         Confirmation
# ================== remove_pam_pkcs11_module_check.confirm ==================
# Label:          Disable pam_pkcs11 module in PAM configuration? If no, the upgrade process will be interrupted.
# Description:    PAM module pam_pkcs11 is no longer available in RHEL-8 since it was replaced by SSSD.
# Type:           bool
# Default:        None
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
# confirm =
```

Label フィールドは、回答が必要な質問を指定します。この例の質問は、**PAM 設定の pam_pkcs11 モジュールを無効にしますか ?**です。

この質問に回答するには、**confirm** 行のコメントを解除して **True** または **False** の回答を入力します。この例では、選択した回答は **True** です。

```
[remove_pam_pkcs11_module_check]
...
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
confirm = True
```

ダウンロードフェーズ

- RPM パッケージのダウンロード中に問題が発生した場合は、**/var/log/leapp/dnf-debugdata/** ディレクトリーにあるトランザクションデバッグデータを調べてください。

注記

/var/log/leapp/dnf-debugdata/ ディレクトリーは空であるか、トランザクションデバッグデータが生成されていない場合は存在しません。これは、必要なリポジトリーが利用できない場合に発生する可能性があります。

initramfs フェーズ

- このフェーズでは、潜在的な失敗により Dracut シェルにリダイレクトされます。ジャーナルを確認してください。

  ```
  # journalctl
  ```

  あるいは、**reboot** コマンドを実行して、Dracut シェルからシステムを再起動し、**/var/log/leapp/leapp-upgrade.log** ファイルを確認します。

アップグレード後のフェーズ

- 一見、システムが正常にアップグレードしていても、古い RHEL 7 カーネルでシステムが起動する場合は、システムを再起動して、GRUB でデフォルトエントリーのカーネルバージョンを確認します。
- RHEL 8 システムのアップグレード後の状態の確認 の推奨手順を行ってください。
- SELinux を Enforcing モードに切り替えてから、アプリケーションやサービスが停止したり、適切に動作しなかったりした場合は、**ausearch**、**journalctl**、**dmesg** のいずれかのユーティリティーで、サービスの拒否を検索します。

  ```
  # ausearch -m AVC,USER_AVC -ts boot
  # journalctl -t setroubleshoot
  # dmesg | grep -i -e selinux -e type=1400
  ```

  最も一般的な問題は、ラベルが間違っていることにより発生します。詳細は Troubleshooting problems related to SELinux を参照してください。

10.3. 既知の問題

以下は、RHEL 7 から RHEL 8 にアップグレードする際に発生する可能性のある既知の問題です。

- 現在、ネットワークチーミングは、Network Manager を無効にするかインストールしていない場合にインプレースアップグレードを実行すると動作しません。
- HTTP プロキシーを使用する場合は、Red Hat Subscription Manager がこのようなプロキシーを使用するように設定するか、**--proxy <hostname>** オプションで **subscription-manager** コマンドを実行する必要があります。そうでない場合は、**subscription-manager** コマンドの実行に失敗します。設定変更の代わりに **--proxy** オプションを使用する場合は、**Leapp** がプロキシーを検出できないため、アップグレードプロセスが失敗します。この問題が発生しないようにするには、Red Hat Subscription Management に HTTP プロキシーを設定する の説明に従って **rhsm.conf** ファイルを手動で編集します。(BZ#1689294)
- RHEL 7 システムで、Red Hat が提供しているにもかかわらず RHEL 8 で利用できないデバイスドライバーを使用している場合は、**Leapp** でアップグレードが行われません。ただし、RHEL 7 システムが、**Leapp** が **/etc/leapp/files/device_driver_deprecation_data.json** ファイルにデータを持たないサードパーティーのデバイスドライバーを使用している場合、**Leapp** はそのようなドライバーを検出せず、アップグレードを続行します。したがって、アップグレード後にシステムが起動しない場合があります。
- **/etc/nsswitch.conf** ファイルで **winbind** および **wins** Samba モジュールが使用されている場合は、インプレースアップグレードを実行できません。このシナリオでは、アップグレードトランザクションが失敗して次のエラーが表示され、**Leapp** により更新が行われません。

```
upgrade[469]: STDERR:
upgrade[469]: Error in PREIN scriptlet in rpm package unbound-libs
upgrade[469]: Error: Transaction failed
upgrade[469]: Container el8userspace failed with error code 1.
unbound-libs has a PREIN failure
```

この問題を回避するには、更新時に、データベース **user**、**groups**、および **hosts** にのみローカルプロバイダーを使用できるようにシステムを設定します。

1. システムの設定ファイル **/etc/nsswitch.conf** を開き、**winbind** 文字列または **wins** 文字列を含むエントリーを検索します。
2. そのようなエントリーを確認するには、**/etc/nsswitch.conf** のバックアップを作成します。
3. **/etc/nsswitch.conf** を編集し、**winbind** または **wins** を含むエントリーからそれらを削除します。
4. インプレースアップグレードを実行します。
5. アップグレード後、システム設定要件に基づいて、**winbind** および **wins** 文字列を **/etc/nsswitch.conf** のエントリーに追加します。
(BZ#1410154)

- **Leapp** ユーティリティーは、アップグレードプロセス時にカスタマイズされた認証設定を変更しません。非推奨の **authconfig** ユーティリティーを使用して RHEL 7 システムで認証を設定した場合は、RHEL 8 での認証が正しく機能しない場合があります。RHEL 8 システムでカスタム設定が正しく機能するようにするには、**authselect** ユーティリティーを使用して RHEL 8 システムを再設定します。

重要

インプレースアップグレード中に、非推奨のプラグ可能認証モジュール (PAM) の **pam_krb5** または **pam_pkcs11** が削除されます。その結果、RHEL 7 システムの PAM 設定に **pam_krb5** または **pam_pkcs11** モジュールが含まれており、これらのモジュールに **required** または **requisite** の制御値がある場合、インプレースアップグレードを実行すると、システムからロックアウトされる可能性があります。この問題を回避するには、アップグレードプロセスを開始する前に、RHEL 7 システムを再設定して、**pam_krb5** または **pam_pkcs11** を使用しないようにします。

- お使いのシステムに (Red Hat が署名していない) サードパーティーパッケージの名前が、Red Hat が提供するパッケージの名前と同じ場合は、インプレースアップグレードに失敗します。この問題を回避するには、アップグレードの前に次のいずれかのオプションを選択してください。
    a. サードパーティーパッケージの削除
    b. サードパーティーパッケージを、Red Hat が提供するパッケージに置き換えます。
- セキュリティー上の理由から、シングル DES (DES) およびトリプル DES (3DES) 暗号化タイプのサポートは RHEL 8 から削除されました。ただし、RHEL 7 Identity Management (IdM) は引き続き 3DES 暗号化に対応しています。
IdM クライアントのアップグレードまたは IdM 環境全体の RHEL 7 から RHEL 8 への移行は可能です。これは、RHEL の両方のバージョンがデフォルトでより強力な AES 暗号化タイプを優先するためです。

IdM のバージョン	デフォルトの暗号化タイプ	その他のサポートされる暗号化タイプ
RHEL 7	**aes256-cts** **aes128-cts**	**camellia256-cts** **camellia128-cts** **des3-hmac** **arcfour-hmac**
RHEL 8	**aes256-cts** **aes128-cts**	**aes256-sha2** **aes128-sha2** **camellia256-cts** **camellia128-cts** **arcfour-hmac** [a]

[a] RC4 暗号化は、新しい暗号化タイプ AES-128 および AES-256 よりも安全ではないと見なされるため、RHEL 8 ではデフォルトで非推奨となり、無効にされています。古い Active Directory 環境との互換性のために RC4 サポートを有効にする方法は、AD および RHEL で一般的な暗号化タイプに対応を参照してください。

IdM 以外の Kerberos Distribution Center (KDC)、サービス、またはユーザーが DES または 3DES の暗号化 **のみ** を使用するように手動で設定した場合、RHEL 8 の最新の Kerberos パッケージに更新した後に、以下のようなサービス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**) を使用する KDC が起動に失敗する

Red Hat では、お使いの環境で DES または 3DES 暗号化を使用しないことを推奨します。Kerberos プリンシパルが強力な暗号化タイプを使用するように設定する方法の詳細は、MIT Kerberos ドキュメントの Retiring DES を参照してください。

- インプレースアップグレードは、ソフトウェア Redundant Array of Independent Disks (RAID) を備えたシステムでは失敗する可能性があります。(RHEL-3279)
- Puppet を使用するシステムなど、無効な GRUB ブートローダー仕様のシステムは、新しいカーネル用に新しい initramfs を作成できません。この問題を回避するには、第 6 章 アップグレード後のタスクの実行 で説明されているように、ブートローダーエントリーからパッケージと古いカーネルを手動で削除します。(BZ#1955099)
- Relax-and-Recover(ReaR) ユーティリティーは、IBM Z アーキテクチャーでは利用できません。そのため、IBM Z システムは OpenSCAP スイートで完全に修正することはできず、セキュリティーベースラインに完全に準拠しない場合があります。(BZ#1958939)
- **Leapp** ユーティリティーは、インプレースアップグレード時に、通常 RHEL 7 から RHEL 8 の間にネットワークインターフェイスコントローラー (NIC) 名を保持します。ただし、ネットワークボンディングを備えたシステムなどの一部のシステムでは、RHEL 7 と RHEL 8 の間で NIC 名を更新する必要があります。これらのシステムで、以下の手順を実行します。

  a. **Leapp** ユーティリティーが元の RHEL 7 の NIC 名を誤って保持しないように、**LEAPP_NO_NETWORK_RENAMING=1** 環境変数を設定します。

  b. インプレースアップグレードを実行します。

c. ネットワークが正常に機能していることを確認します。必要に応じて、ネットワーク設定を手動で更新します。
(BZ#1919382)

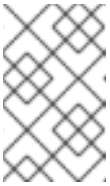
- BIOS を使用してシステムを起動する場合は、コアイメージのインストールに十分な領域が、ブートディスクの埋め込み領域に含まれていないと、GRUB2 ブートローダーをアップグレードするときにインプレースアップグレードが失敗します。これによりシステムが破損し、RHEL 6 **fdisk** ユーティリティーなどを使用してディスクが手動でパーティション分割された場合に発生する可能性があります。この問題がユーザーに影響するかどうかを確認するには、以下の手順を実行します。

a. インストールされたブートローダーを使用してディスク上の最初のパーティションを開始するセクターを決定します。

```
# fdisk -l
```

コアイメージに十分なスペースを確保する標準のパーティショニングは、セクター 2048 から始まります。

b. 開始セクターに十分なスペースがあるかどうかを判断します。RHEL 8 コアイメージには少なくとも 32 KiB が必要です。たとえば、セクターサイズが標準の 512 バイトの場合、セクター 66 以下から開始すると十分なスペースが得られません。



注記

RHEL 8 コアイメージは 32 KiB より大きい場合があり、開始セクターの値を高く指定しなければいけない可能性があります。現在の RHEL 8 コアに必要な領域を常に確認してください。

c. 埋め込み領域に十分なストレージ領域が含まれていない場合は、インプレースアップグレードを実行する代わりに、RHEL 8 システムの新規インストールを実行します。
(BZ#2181380)

- インプレースアップグレード後、システムが以下の条件を満たす場合、SSH キーは自動生成されなくなりました。

  - システムがクラウド上にあります。
  - cloud-init パッケージがインストールされている。
  - ssh_genkeytypes 設定は、/etc/cloud/cloud.cfg ファイルで ~ に設定されます。これはデフォルトです。
    この問題により、元のキーが削除された場合にシステムが SSH を使用して接続できなくなります。この問題を回避するには、ナレッジベースソリューション Unable to SSH to new Virtual Machine after upgrading the template to RHEL 8.7 or 9 を参照してください。
    (BZ#2210012)

- ハードウェアレベル 13 で作成され、UEFI で起動している VMWare 仮想マシンでは、NVRAM ファイルが小さすぎるため、アップグレード中に問題が発生する可能性があります。この問題と解決方法の詳細は、VMWare: Getting "No space left on device" when executing efibootmgr or mokutil command to add entries を参照してください。(RHEL-3362)

- ISO イメージを含む RHUI を使用してアップグレードしようとすると、アップグレードが失敗する可能性があります。この問題を回避するには、**--iso** オプションを使用せずにアップグレードを実行するか、Offline Leapp upgrade using ISO fails with "Failed to synchronize cache for

repo 'rhul-microsoft-azure-rhel8', ignoring this repo に記載されている手順を実行します。(RHEL-3296)

- アップグレード前のプロセスが、以下のエラーメッセージで失敗する可能性があります。**MountError: failed to create mount target directory ...**

  この問題が発生した場合は、**LEAPP_OVL_IMG_FS_EXT4=1** 環境変数をエクスポートします。詳細は、Leapp can fail with a MountError (OverlayFS + XFS ftype=1) を参照してください。(RHEL-3330)

- マウントされているファイルシステムが多すぎると、アップグレード前のプロセスが失敗し、次のエラーメッセージが表示される可能性があります。

  ```
  OperationalError: unable to open database file
  Cannot create XFS filesystem in ...
  ```

  この問題が発生した場合は、以下の手順を実行します。

  1. システムパーティションに関係がなく、アップグレードプロセス中に必要のないファイルシステムをすべてアンマウントします。
  2. **/etc/fstab** ファイルのアンマウントされたファイルシステムのエントリーをコメントアウトして、アップグレードプロセス中にマウントされないようにします。
  3. アップグレード後に元のファイルシステム設定を復元します。

  (RHEL-3320)

- システムに **/etc/sysconfig/kernel** システム設定ファイルがない場合、アップグレードは失敗し、システムが破損します。この問題を回避するには、予想される設定でファイルを手動で作成します。詳細は、ブートローダーの検証 を参照してください。(RHEL-22306)

- **/etc/fstab** ファイルで定義されているマウントされたファイルシステムのいずれかに **shared** 伝播フラグが設定されていない場合、アップグレードが失敗する可能性があります。この問題を回避するには、これらのファイルシステムを再マウントして shared として設定します。

  ```
  # mount -o remount --make-shared <mountpoint>
  ```

  mountpoint は、各ファイルシステムのマウントポイントに置き換えます。

  詳細は、Leapp "Can not load RPM file" during the DNF transaction check を参照してください。(RHEL-23449)

- RHEL 8 リポジトリーが存在しないという問題により、EUS、E4S、および AUS サブスクリプションを持つシステムでは、RHEL 8.10 へのアップグレードが失敗する可能性があります。この問題を回避するには、**--channel ga** オプションを指定して preupgrade コマンドと upgrade コマンドを実行します。(RHEL-24720)

- アップグレードプロセスに制限されたリソースが設定されている場合、アップグレードは失敗する可能性があります。たとえば、**maximum number of open files descriptors** や、**maximum size of files written by the process and its children** が設定されている場合は、アップグレードプロセスによってそれらの値に到達する可能性があります。これらの問題を防ぐには、アップグレードプロセスの前にこれらの制限を増やすか削除します。詳細は、Why does leapp preupgrade fail with sqlite3.OperationalError: unable to open database file traceback error ? および Ensure that there is enough diskspace in /var/lib/leapp/scratch/diskimages/root_boot at least XXX mib are needed を参照してください。(RHEL-16881、RHEL-26459)

10.4. サポートの利用

サポートケースを作成するには、製品で **RHEL 7** を選択し、システムの **sosreport** を添付します。

- システムで **sosreport** を生成するには、次のコマンドを実行します。

```
# sosreport
```

ケース ID は空のままにできます。

sosreport を生成する方法は、ナレッジベースのソリューション Red Hat Enterprise Linux 上での sosreport のロールと取得方法 を参照してください。

カスタマーポータルでサポートケースを作成し、管理する方法の詳細は、ナレッジベースのアーティクル記事 How do I open and manage a support case on the Customer Portal? を参照してください。

第11章 関連情報

以下の説明情報を参照できます。

- Upgrade your Red Hat Enterprise Linux Infrastructure
- Red Hat Enterprise Linux technology capabilities and limits
- Supported in-place upgrade paths for Red Hat Enterprise Linux
- インプレースアップグレードサポートポリシー
- RHEL 8 の導入における検討事項
- Customizing your Red Hat Enterprise Linux in-place upgrade
- Red Hat Enterprise Linux のアップグレード前のレポートワークフローの自動化
- Using configuration management systems to automate parts of the Leapp pre-upgrade and upgrade process on Red Hat Enterprise Linux
- RHEL 6 から RHEL 7 へのアップグレード
- RHEL 6 から RHEL 8 へのアップグレード
- RPM ベースの Linux ディストリビューションから RHEL への変換
- Red Hat Satellite での RHEL 7 から RHEL 8 へのホストのアップグレード
- SAP 環境を RHEL 7 から RHEL 8 にインプレースアップグレードする方法
- Red Hat Insights ドキュメント
- Upgrades-related Knowledgebase articles and solutions
- The best practices and recommendations for performing RHEL Upgrade using Leapp
- Leapp upgrade FAQ (Frequently Asked Questions)

付録A RHEL 7 リポジトリー

アップグレードの前に、Preparing a RHEL 7 system for the upgrade の手順 4 で説明されているように、適切なリポジトリーを有効になっていることを確認してください。

アップグレード時に Red Hat Subscription Manager を使用する予定がある場合には、**subscription-manager repos --enable repository_id** コマンドを使用して、アップグレードの前に以下のリポジトリーを **有効にする必要があります**。

アーキテクチャー	リポジトリー	リポジトリー ID
64 ビット Intel	Base	**rhel-7-server-rpms**
	Extras	**rhel-7-server-extras-rpms**
IBM POWER8 (リトルエンディアン)	Base	**rhel-7-for-power-le-rpms**
	Extras	**rhel-7-for-power-le-extras-rpms**
IBM Z	Base	**rhel-7-for-system-z-rpms**
	Extras	**rhel-7-for-system-z-extras-rpms**

次のリポジトリーは、アップグレード前に **subscription-manager repos --enable repository_id** コマンドを使用して **有効にできます**。

アーキテクチャー	リポジトリー	リポジトリー ID
64 ビット Intel	任意	**rhel-7-server-optional-rpms**
	Supplementary	**rhel-7-server-supplementary-rpms**
IBM POWER8 (リトルエンディアン)	任意	**rhel-7-for-power-le-optional-rpms**
	Supplementary	**rhel-7-for-power-le-supplementary-rpms**
IBM Z	任意	**rhel-7-for-system-z-optional-rpms**
	Supplementary	**rhel-7-for-system-z-supplementary-rpms**

注記

インプレースアップグレードの前に RHEL 7 Optional または RHEL 7 Supplementary リポジトリーを有効にすると、**Leapp** は、RHEL 8 CodeReady Linux Builder リポジトリーまたは RHEL 8 Supplementary リポジトリーをそれぞれ有効にします。

カスタムリポジトリーを使用する場合は、Configuring custom repositories の指示に従って、カスタムリポジトリーを有効にします。

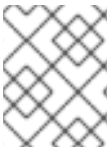
付録B RHEL 8 リポジトリー

Red Hat Subscription Manager(RHSM) を使用して Red Hat コンテンツ配信ネットワーク (CDN) に登録されている場合は、インプレースアップグレード時に RHEL 8 リポジトリーが自動的に有効になります。ただし、RHSM を使用して Red Hat Satellite に登録したシステムでは、アップグレード前のレポートを実行する前に、RHEL 7 と RHEL 8 の両方のリポジトリーを手動で有効化して同期する必要があります。

注記

各リポジトリーのターゲットオペレーティングシステム (OS) バージョン (RHEL 8.10 など) を必ず有効にしてください。リポジトリーの RHEL 8 バージョンのみを有効にすると、インプレースアップグレードは抑制されます。

アップグレード時に Red Hat Satellite を使用する予定の場合には、Satellite Web UI または **hammer repository-set enable** コマンドおよび **hammer product synchronize** コマンドを使用して、アップグレードの前に以下の RHEL 8 リポジトリーを**有効にして同期する必要** があります。



注記

<target_os_version> は、ターゲットオペレーティングシステム (OS) バージョン (例: 8.10) に置き換えます。

表B.1 RHEL 8 リポジトリー

アーキテクチャー	リポジトリー	リポジトリー ID	リポジトリー名	リリースバージョン
64 ビット Intel	BaseOS	**rhel-8-for-x86_64-baseos-rpms**	Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)	x86_64 **<target_os_version>**
	AppStream	**rhel-8-for-x86_64-appstream-rpms**	Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)	x86_64 **<target_os_version>**
IBM POWER8 (リトルエンディアン)	BaseOS	**rhel-8-for-ppc64le-baseos-rpms**	Red Hat Enterprise Linux 8 for Power, little endian - BaseOS (RPMs)	ppc64le **<target_os_version>**
	AppStream	**rhel-8-for-ppc64le-appstream-rpms**	Red Hat Enterprise Linux 8 for Power, little endian - AppStream (RPMs)	ppc64le **<target_os_version>**

アーキテクチャー	リポジトリー	リポジトリー ID	リポジトリー名	リリースバージョン
IBM Z	BaseOS	**rhel-8-for-s390x-baseos-rpms**	Red Hat Enterprise Linux 8 for IBM z Systems - BaseOS (RPMs)	s390x **<target_os_version>**
	AppStream	**rhel-8-for-s390x-appstream-rpms**	Red Hat Enterprise Linux 8 for IBM z Systems - AppStream (RPMs)	s390x **<target_os_version>**

付録C RHEL 8 の暗号化キーの場所

Federal Information Processing Standard (FIPS) モードで実行されているシステムをアップグレードした後は、暗号化キーの再生成などを行い、すべての暗号化キーの FIPS 準拠を確認する必要があります。よく知られた暗号化キーの場所を次の表に示します。リストは完全ではないことに注意してください。他の場所も確認してください。

表C.1 RHEL 8 の暗号化キーの場所

アプリケーション	キーの場所	注記
Apache mod_ssl	**/etc/pki/tls/private/localhost.key**	**/etc/pki/tls/private/localhost.key** が存在しない場合、**/usr/lib/systemd/system/httpd-init.service** サービスは **/usr/libexec/httpd-ssl-gencerts** ファイルを実行します。
Bind9 RNDC	**/etc/rndc.key**	**named-setup-rndc.service** サービスは、**/etc/rndc.key** ファイルを生成する **/usr/libexec/generate-rndc-key.sh** スクリプトを実行します。
Cyrus IMAPd	**/etc/pki/cyrus-imapd/cyrus-imapd-key.pem**	**cyrus-imapd-init.service** サービスは、起動時に **/etc/pki/cyrus-imapd/cyrus-imapd-key.pem** ファイルを生成します。
DNSSEC-Trigger	**/etc/dnssec-trigger/dnssec_trigger_control.key**	**dnssec-triggerd-keygen.service** サービスは、**/etc/dnssec-trigger/dnssec_trigger_control.key** ファイルを生成します。
Dovecot	**/etc/pki/dovecot/private/dovecot.pem**	**dovecot-init.service** サービスは、起動時に **/etc/pki/dovecot/private/dovecot.pem** ファイルを生成します。
OpenPegasus	**/etc/pki/Pegasus/file.pem**	**tog-pegasus.service** サービスは、**/etc/pki/Pegasus/file.pem** 秘密鍵ファイルを生成します。

アプリケーション	キーの場所	注記
OpenSSH	**/etc/ssh/ssh_host*_key**	Ed25519 および DSA キーは FIPS に準拠していません。 カスタム Diffie-Hellman (DH) パラメーターは、FIPS モードではサポートされていません。FIPS モードとの互換性を確保するために、**sshd_config** ファイルの **ModuliFile** オプションをコメントアウトしてください。**moduli** ファイル (デフォルトでは **/etc/ssh/moduli**) はそのままにしておくことができます。
postfix	**/etc/pki/tls/private/postfix.key**	**postfix** パッケージに含まれるインストール後のスクリプトは、**/etc/pki/tls/private/postfix.key** ファイルを生成します。
RHEL Web コンソール	**/etc/cockpit/ws-certs.d/**	Web コンソールは **/usr/libexec/cockpit-certificate-ensure –for-cockpit-tls** ファイルを実行し、**/etc/cockpit/ws-certs.d/** ディレクトリーにキーを作成します。
Sendmail	**/etc/pki/tls/private/sendmail.key**	**sendmail** パッケージに含まれるインストール後のスクリプトは、**/etc/pki/tls/private/sendmail.key** ファイルを生成します。

サードパーティー製アプリケーションの暗号化キーが FIPS に準拠していることを確認するには、それぞれのアプリケーションの対応するドキュメントを参照してください。また、以下に注意してください。

- ポートを開くサービスが、TLS 証明書を使用する場合があります。
  - すべてのサービスが暗号化キーを自動的に生成するわけではありませんが、自動的に起動する多くのサービスはデフォルトで自動生成します。
- NSS、GnuTLS、OpenSSL、libgcrypt などの暗号化ライブラリーを使用するサービスにも注意してください。
- バックアップ、ディスク暗号化、ファイル暗号化、および同様のアプリケーションも確認してください。

重要

RHEL 8 の FIPS モードは DSA キー、DH パラメーター、1024 ビットより短い RSA キー、およびその他のいくつかの暗号を制限するため、古い暗号化キーは RHEL 7 からのアップグレード後に機能しなくなります。詳細は、「RHEL 8 の導入における検討事項」ドキュメントの コア暗号化コンポーネントの変更点 セクションと、RHEL 8「セキュリティーの強化」ドキュメントの システム全体の暗号化ポリシーの使用 の章を参照してください。

関連情報

- RHEL 8 セキュリティーの強化ドキュメントの FIPS モードへのシステムの切り替え
- **update-crypto-policies (8)** および **fips-mode-setup (8)** man ページ