Red Hat Enterprise Linux 9

RHEL 8 から RHEL 9 へのアップグレード

Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9 へのインプレースアップグレードの手順

Last Updated: 2024-07-09

Red Hat Enterprise Linux 9 RHEL 8 から RHEL 9 へのアップグレード

Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9 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

本書は、Leapp ユーティリティーを使用して、Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9 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 8 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 9 バージョンに置き換えられます。

目次

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 8 オペレーティングシステムを RHEL 9 バージョンに置き換えます。

重要

RHEL 7 から RHEL 9 へのインプレースアップグレードを直接実行することはできません。ただし、RHEL 7 から RHEL 8 へのインプレースアップグレードを実行してから、RHEL 9 への 2 回目のインプレースアップグレードを実行することはできます。詳細は、RHEL7 から RHEL8 へのアップグレードを 参照してください。

現在、以下のソースの RHEL 8 マイナーバージョンから、以下のターゲットの RHEL 9 マイナーバージョンへ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 8.8	RHEL 9.2	2025 年 5 月 31 日 (EUS)
	RHEL 8.10	RHEL 9.4	2026 年 5 月 31 日
RHEL with SAP HANA	RHEL 8.8	RHEL 9.2	2025 年 5 月 31 日 (EUS)
	RHEL 8.10	RHEL 9.4	2026 年 5 月 31 日 (EUS)

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 RHEL 9 へのアップグレードの計画

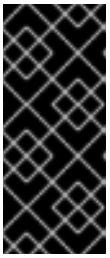
RHEL 8 から RHEL 9 へのアップグレードを開始する前に、システム要件、制限事項、およびその他の考慮事項を確認してください。

2.1. RHEL 8.10 から RHEL 9.4 への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 9 にアップグレードする前に、以下を考慮する必要があります。

- **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** ユーティリティーでアップグレードが可能です。
  - ソース OS のバージョンは、以下のサポートされるアーキテクチャーのいずれかを持つシステムにインストールされています。
    - 64 ビット Intel、AMD、および ARM
    - IBM POWER (リトルエンディアン)
    - 64 ビット IBM Z
      詳細は、Red Hat certified hardware を参照してください。
  - RHEL 9 の最小 ハードウェア要件 が満たされている。
  - 選択したソースおよびターゲット OS バージョンの最新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た RHEL 8 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、カスタムアクターに対応していません。



重要

SHA-1 アルゴリズムは RHEL 9 で非推奨となりました。システムに RSA/SHA-1 署名を持つパッケージが含まれている場合、アップグレードは禁止されます。アップグレードする前に、これらのパッケージを削除するか、RSA/SHA-256 署名を含むパッケージについてベンダーに問い合わせてください。詳細は、SHA-1 deprecation in Red Hat Enterprise Linux 9 を参照してください。

- **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、システムが準拠しなければならないセキュリティー標準を定義し、RHEL 9 におけるセキュリティーの変更 について理解してください。
  - **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。

- **Leapp** は、連邦情報処理標準 (FIPS) 140 モードの RHEL 8.8 以降のシステムから RHEL 9 FIPS モード対応システムへのインプレースアップグレードをサポートしています。**FIPS モード** は、完全なアップグレードプロセス中も有効なままになります。
- 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。セキュリティーポリシーの適用および更新の詳細は、セキュリティーポリシーの適用 を参照してください。

- **ストレージおよびファイルシステム** - アップグレードする前に、必ずシステムのバックアップを作成してください。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。つまり、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 8 から RHEL 9 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 メジャー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、代わりに SAP 環境の RHEL 8 から RHEL 9 へのアップグレード ガイドに従ってください。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 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 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 8 または RHEL 9 のブートローダーを BIOS から UEFI に切り替えることはできません。RHEL 8 システムで BIOS を使用し、RHEL 9 システムでは UEFI を使用する必要がある場合は、インプレースアップグレードの代わりに RHEL 9 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。
  - 現在、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 Update Infrastructure を使用して Red Hat Subscription Manager (RHSM) を使用しない、残りのパブリッククラウドのオンデマンドインスタンスではサポートされません。
  - 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 9 で RHEL 8 Ansible Tower インストールを使用するには、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 9 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 の該当する Advisor 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、**Affected system** の見出しにあるリストを確認します。Advisor 推奨は RHEL 8 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)

2.2. RHEL 8.8 から RHEL 9.2 へのアップグレードの計画

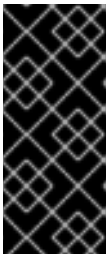
インプレースアップグレードは、システムを RHEL の次のメジャーバージョンにアップグレードする方法です。この方法は、推奨され、サポートされています。

RHEL 9.2 にアップグレードする前に、以下を考慮する必要があります。

- **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** ユーティリティーでアップグレードが可能です。
  - ソース OS のバージョンは、以下のサポートされるアーキテクチャーのいずれかを持つシステムにインストールされています。
    - 64 ビット Intel、AMD、および ARM
    - IBM POWER (リトルエンディアン)
    - 64 ビット IBM Z
      詳細は、Red Hat certified hardware を参照してください。
  - RHEL 9 の最小 ハードウェア要件 が満たされている。

- 選択したソースおよびターゲット OS バージョンの最新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た RHEL 8 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、カスタムアクターに対応していません。



重要

SHA-1 アルゴリズムは RHEL 9 で非推奨となりました。システムに RSA/SHA-1 署名を持つパッケージが含まれている場合、アップグレードは禁止されます。アップグレードする前に、これらのパッケージを削除するか、RSA/SHA-256 署名を含むパッケージについてベンダーに問い合わせてください。詳細は、SHA-1 deprecation in Red Hat Enterprise Linux 9 を参照してください。

- **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、システムが準拠しなければならないセキュリティー標準を定義し、RHEL 9 におけるセキュリティーの変更 について理解してください。

  - **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。

  - **Leapp** は、連邦情報処理標準 (FIPS) 140 モードの RHEL 8.8 以降のシステムから RHEL 9 FIPS モード対応システムへのインプレースアップグレードをサポートしています。**FIPS モード** は、完全なアップグレードプロセス中も有効なままになります。

  - 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。セキュリティーポリシーの適用および更新の詳細は、セキュリティーポリシーの適用 を参照してください。

- **ストレージおよびファイルシステム** - アップグレードする前に、必ずシステムのバックアップを作成してください。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。つまり、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 8 から RHEL 9 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 メジャー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、代わりに SAP 環境の RHEL 8 から RHEL 9 へのアップグレード ガイドに従ってください。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。

- **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 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 8 または RHEL 9 のブートローダーを BIOS から UEFI に切り替えることはできません。RHEL 8 システムで BIOS を使用し、RHEL 9 システムでは UEFI を使用する必要がある場合は、インプレースアップグレードの代わりに RHEL 9 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。

  - 現在、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 Update Infrastructure を使用して Red Hat Subscription Manager (RHSM) を使用しない、残りのパブリッククラウドのオンデマンドインスタンスではサポートされません。

  - 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 9 で RHEL 8 Ansible Tower インストールを使用するには、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 9 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 の該当する Advisor 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、**Affected system** の見出しにあるリストを確認します。Advisor 推奨は RHEL 8 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3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 8 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 アップグレードのための Satellite 登録システムの準備 で説明されている準備手順も実行する必要があります。

3.1. アップグレードに向けた RHEL 8 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 9 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。

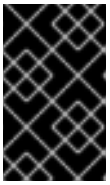
アップグレードプロセス中に Red Hat Subscription Manager (RHSM) を使用する予定がない場合は、Upgrading to RHEL 9 without Red Hat Subscription Manager の手順に従ってください。

前提条件

- システムが、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。
- システムを以前 RHEL 7 から RHEL 8 にアップグレードした場合は、アップグレード後に必要な手順をすべて完了した。詳細は、RHEL 7 から RHEL 8 へのアップグレードガイドの アップグレード後のタスクの実行 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. システムを Satellite Server に登録した場合は、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てください。



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。

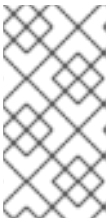
```
# subscription-manager status
+-------------------------------------------+
   System Status Details
+-------------------------------------------+
Overall Status: Disabled
Content Access Mode is set to Simple Content Access. This host has access to content,
regardless of subscription status.
System 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。以下に例を示します。

```
# subscription-manager list --installed
+-------------------------------------------+
     Installed Product Status
+-------------------------------------------+
Product Name:   Red Hat Enterprise Linux for x86_64
Product ID:     479
Version:        8.10
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。以下のコマンドは、64 ビット Intel アーキテクチャーの Base リポジトリーおよび AppStream リポジトリーを有効にします。その他のアーキテクチャーについては、RHEL 8 リポジトリー を参照してください。

```
# subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms --enable rhel-8-for-
x86_64-appstream-rpms
```



注記

オプションで、CodeReady Linux Builder (オプションとも呼ばれます) 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 の詳細については、RHEL 8 リポジトリー 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、パッケージマニフェスト を参照してください。

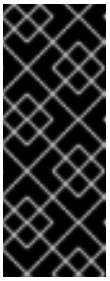
7. システムのリリースバージョンを設定します。

a. RHSM を使用してサブスクライブしたシステムの場合は、システムを目的のソース OS バージョンにロックします。

```
# subscription-manager release --set <source_os_version>
```

b. パブリッククラウド上の Red Hat Update Infrastructure (RHUI) を使用してアップグレードする場合は、予想されるシステムリリースバージョンを手動で設定します。

```
# rhui-set-release --set <source_os_version>
```



重要

rhui-set-release コマンドがシステムで使用できない場合は、**/etc/dnf/vars/release** ファイルを更新することで、予想されるシステムリリースバージョンを設定できます。

```
# echo "<source_os_version>" > /etc/dnf/vars/releasever
```

source_os_version は、ソース OS バージョン (例: **8.8**) に置き換えます。

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 カスタムリポジトリーの設定 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 **dnf 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。

```
# dnf versionlock clear
```

詳細は、How to restrict dnf to install or upgrade a package to a fixed specific package version? 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:

```
# dnf config-manager --set-enabled rhui-client-config-server-8
# dnf -y install leapp-rhui-aws
```

    b. For Microsoft Azure:

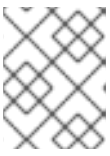
```
# dnf config-manager --set-enabled rhui-microsoft-azure-rhel8
# dnf -y install rhui-azure-rhel8 leapp-rhui-azure
```

    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. **Leapp** ユーティリティーをインストールします。

```
# dnf install leapp-upgrade
```

最新の **leapp** および **leapp-repository** パッケージが必要な点に注意してください。パッケージは、インストールされている RHEL 8 のバージョンによって異なります。現在の最新のパッケージのバージョンは次のとおりです。



注記

leapp-repository パッケージには、**leapp-upgrade-el8toel9** RPM パッケージが含まれています。

- RHEL 8.8: **leapp** パッケージのバージョン **0.15.1** および **leapp-repository** パッケージのバージョン **0.18.0**

- RHEL 8.10: **leapp** パッケージの **leapp** バージョン **0.17.0** および **leapp-repository** パッケージのバージョン **0.20.0**

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**
- **python3-leapp**
- **leapp-upgrade-el8toel9**
- **leapp-upgrade-el8toel9-deps**

12. すべてのパッケージを最新の RHEL 8 バージョンに更新し、再起動します。

```
# dnf update
# reboot
```

13. **leapp-upgrade-el8toel9** 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-el8toel9** 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。

14. 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。

15. 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、アップグレードの実行 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。

16. 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 9 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の手順については、How to perform an in-place upgrade to RHEL 8 when using kernel NIC names on RHEL 7 を参照してください。命名スキームを移行するプロセスは、RHEL 7 から RHEL 8 へのアップグレードと、RHEL 8 から RHEL 9 へのアップグレードの両方で同じになります。

17. NSS データベースが RHEL 7 以前で作成された場合は、データベースが DBM データベース形式から SQLite に変換されていることを確認します。詳細は、Updating NSS databases from DBM to SQLite を参照してください。

18. RHEL 9 は、RHEL 8 で廃止された従来の **network-scripts** パッケージをサポートしていません。アップグレードする前に、カスタムネットワークスクリプトを移動し、既存のカスタムスクリプトを実行する NetworkManager ディスパッチャースクリプトを記述します。詳細は、Migrating custom network scripts to NetworkManager dispatcher scripts 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 9.4 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。

3.2. 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 9 へのアップグレードに向け、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について説明します。Satellite Server では以下の手順を実行します。

重要

Satellite システムのユーザーは、この手順と アップグレードに向けた RHEL 8 システムの準備 の両方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 9 リポジトリーが含まれる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 8 および RHEL 9 リポジトリーを有効にし、ソースおよびターゲット OS バージョン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 9 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 (RHEL 9.4 など) を有効にします。RHEL 9 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 8 for x86_64 - AppStream (RPMs)
  rhel-8-for-x86_64-appstream-rpms

  x86_64 **<source_os_version>**

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

  x86_64 **<source_os_version>**

- Red Hat Enterprise Linux 9 for x86_64 - AppStream (RPMs)
  rhel-9-for-x86_64-appstream-rpms

  x86_64 **<target_os_version>**

- Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)
  rhel-9-for-x86_64-baseos-rpms

  x86_64 **<target_os_version>**

  <source_os_version> と **<target_os_version>** は、それぞれソース OS バージョンとターゲット OS バージョン (たとえば、8.10 と 9.4) に置き換えます。

  その他のアーキテクチャーについては、RHEL 8 リポジトリー および RHEL 9 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 8 リポジトリーおよび RHEL 9 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アタッチします。
   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 **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 8 リポジトリーおよび RHEL 9 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、リポジトリーが期待どおりに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-8' --content-view
<content_view_name> --organization <organization> --lifecycle-
environment <lifecycle_environment>
# hammer repository list --search 'content_label ~ rhel-9' --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 9 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。

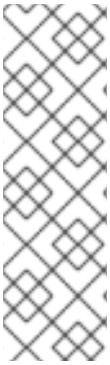
b. **Repository Sets** タブをクリックし、必要なリポジトリーのステータスが **Enabled** であることを確認します。

3. .予想されるすべての RHEL 8 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-8-for-x86_64-baseos-rpms
Repo ID:   rhel-8-for-x86_64-appstream-rpms
```

第4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 9 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。

4.1. コマンドラインからの RHEL 8.10 から RHEL 9.4 へ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前の段階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

- 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. RHEL 8 システムで、アップグレード前のフェーズを実行します。

```
# leapp preupgrade
```

   - 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。**<channel>** はチャネル名 (例: **eus**、**aus**、**e4s)** に置き換えます。SAP HANA を利用している場合は、SAP 環境の RHEL 8 から RHEL 9 へのアップグレード 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。

   - Red Hat OpenStack Platform で RHEL for Real Time または Real Time for Network Functions Virtualization (NFV) を使用している場合は、**--enablerepo** オプションを使用してデプロイメントを有効にします。以下に例を示します。

```
# leapp preupgrade --enablerepo rhel-9-for-x86_64-rt-rpms
```

     詳細は、Real-time Compute の設定 を参照してください。

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

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、**Are all VDO devices, if any, successfully converted to LVM management?** という質問に対して **True** の回答を確定するには、以下のコマンドを実行します。

```
# leapp answer --section check_vdo.confirm=True
```

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。

4.2. コマンドラインから RHEL 8.8 から RHEL 9.2 へ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、RHEL 8.8 から RHEL 9.2 にアップグレードする前の段階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

- 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. RHEL 8 システムで、アップグレード前のフェーズを実行します。

```
# leapp preupgrade
```

   - 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。**<channel>** はチャネル名 (例: **eus**、**aus**、**e4s)** に置

き換えます。SAP HANA を利用している場合は、SAP 環境の RHEL 8 から RHEL 9 へのアップグレード 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。

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

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、**Are all VDO devices, if any, successfully converted to LVM management?** という質問に対して **True** の回答を確定するには、以下のコマンドを実行します。

```
# leapp answer --section check_vdo.confirm=True
```

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。

4.3. WEB コンソールを使用した RHEL 8.10 から RHEL 9.4 へのアップグレード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アップグレード前のフェーズで潜在的な問題を特定し、Web コンソールを使用して自動修復を適用します。

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
```

2. **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、Managing systems using the RHEL 8 web console を参照してください。

3. RHEL 8 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
```

   - 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。**<channel>** はチャネル名 (例: **eus**、**aus**、**e4s)** に置き換えます。SAP HANA を利用している場合は、SAP 環境の RHEL 8 から RHEL 9 へのアップグレード 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。

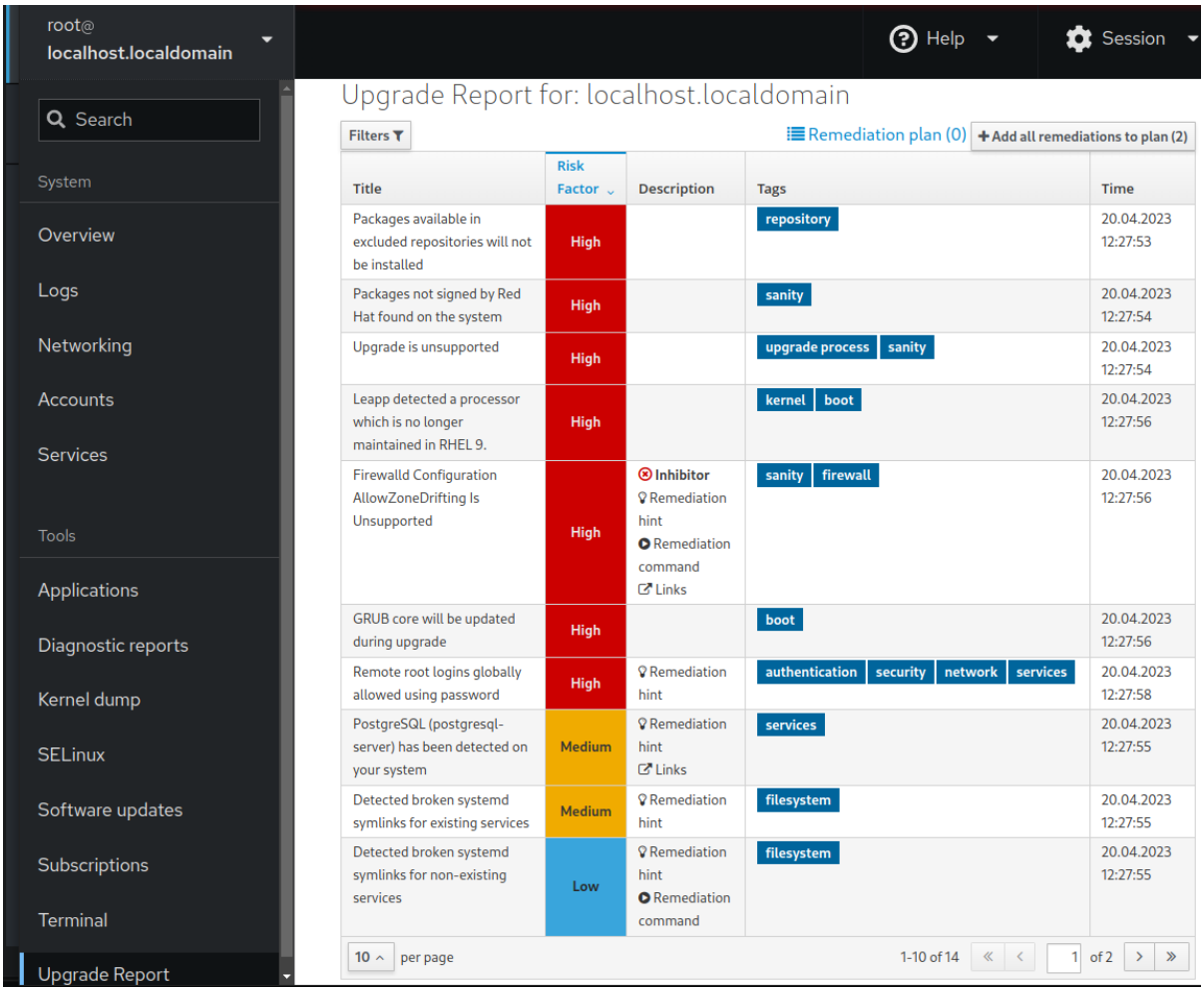
   - Red Hat OpenStack Platform で RHEL for Real Time または Real Time for Network Functions Virtualization (NFV) を使用している場合は、**--enablerepo** オプションを使用してデプロイメントを有効にします。以下に例を示します。

```
# leapp preupgrade --enablerepo rhel-9-for-x86_64-rt-rpms
```

     詳細は、Real-time Compute の設定 を参照してください。

4. 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。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4.1 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

5. 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、**Are all VDO devices, if any, successfully converted to LVM management?**という質問に対して **True** の回答を確定するには、以下のコマンドを実行します。

```
# leapp answer --section check_vdo.confirm=True
```

注記

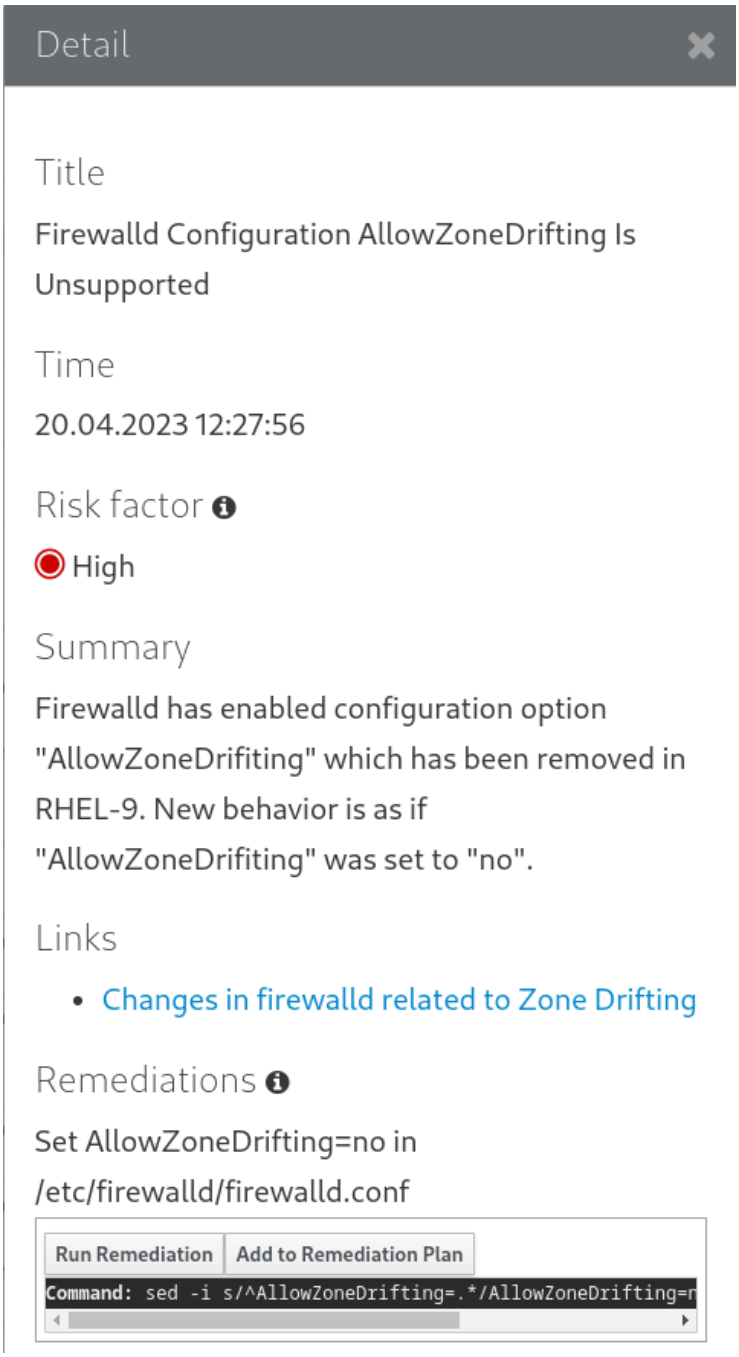
/var/log/leapp/answerfile ファイルを手動で編集し、**#** 記号を削除してファイルの confirm 行のコメントを解除し、**True** または **False** として回答を確定します。詳細は、Leapp 回答ファイルの例 を参照してください。

6. 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4.2 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。

7. 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。

4.4. WEB コンソールを使用した RHEL 8.8 から RHEL 9.2 へのアップグレード可能性の評価および自動修復の適用

Web コンソールを使用して、RHEL 8.8 から RHEL 9.2 にアップグレードする前の段階で潜在的な問題を特定し、自動修復を適用します。

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
```

2. **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、Managing systems using the RHEL 8 web console を参照してください。

3. RHEL 8 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
```

   - 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。

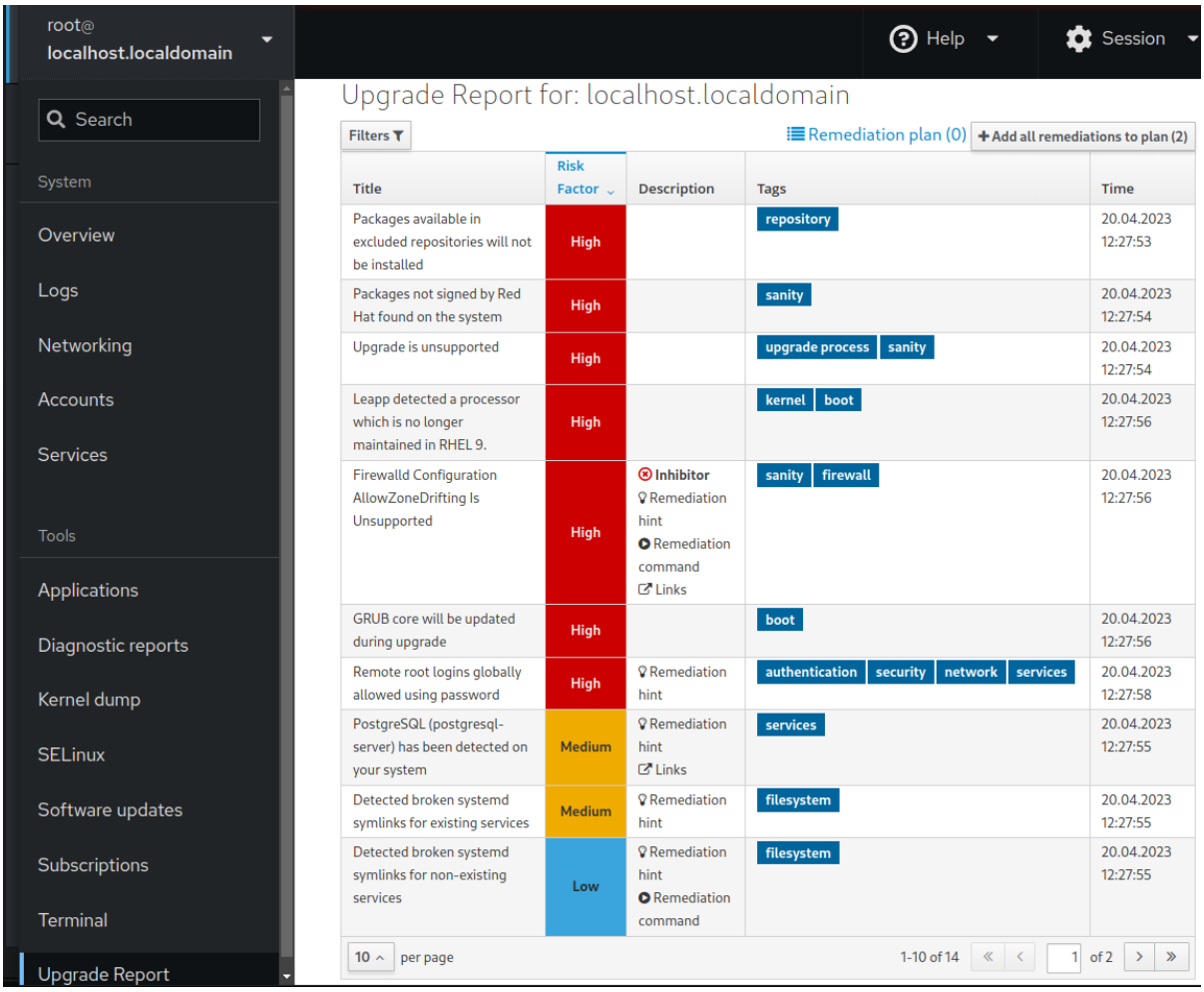
```
# leapp preupgrade --enablerepo <repository_id1> --enablerepo <repository_id2> ...
```

   - 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。**<channel>** はチャネル名 (例: **eus**、**aus**、**e4s)** に置き換えます。SAP HANA を利用している場合は、SAP 環境の RHEL 8 から RHEL 9 へのアップグレード 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。

4. 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。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4.3 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

5. 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、**Are all VDO devices, if any, successfully converted to LVM management?**という質問に対して **True** の回答を確定するには、以下のコマンドを実行します。

```
# leapp answer --section check_vdo.confirm=True
```

注記

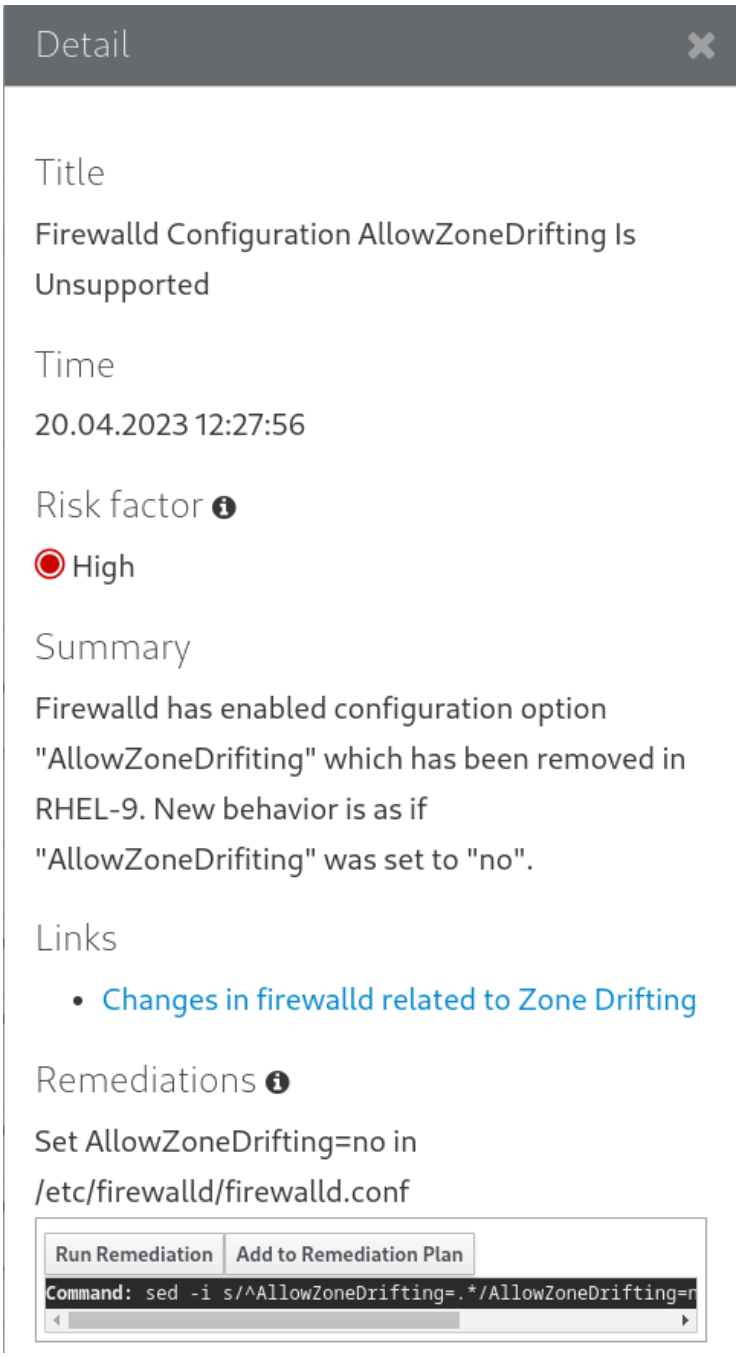
/var/log/leapp/answerfile ファイルを手動で編集し、**#** 記号を削除してファイルの confirm 行のコメントを解除し、**True** または **False** として回答を確定します。詳細は、Leapp 回答ファイルの例 を参照してください。

6. 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4.4 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。

7. 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5章 アップグレードの実行

準備手順を完了し、アップグレード前のレポートで見つかった問題を確認および解決したら、システムでインプレースアップグレードを実行できます。

5.1. RHEL 8.10 から RHEL 9.4 へのアップグレードの実行

この手順では、**Leapp** ユーティリティーを使用してアップグレードを実行するために必要な手順を説明します。

前提条件

- フルシステムバックアップを含め、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。
- 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を完了し、報告されたすべての問題が解決されている。

手順

1. RHEL 8 システムで、アップグレードプロセスを開始します。

```
# leapp upgrade
```

   - 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/rhel9.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。**<channel>** は **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。
   - Red Hat OpenStack Platform で RHEL for Real Time または Real Time for Network Functions Virtualization (NFV) を使用している場合は、**--enablerepo** オプションを使用してデプロイメントを有効にします。以下に例を示します。

```
# leapp upgrade --enablerepo rhel-9-for-x86_64-rt-rpms
```

     詳細は、Real-time Compute の設定 を参照してください。

2. 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、Troubleshooting を参照してください。

3. システムを手動で再起動します。

```
# reboot
```

このフェーズでは、システムは RHEL 9 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 9 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** コマンドを実行し、この手動の手順を省略することもできます。

障害が発生した場合は、トラブルシューティング で説明されているように、ログと既知の問題を調査してください。

4. RHEL 9 システムにログインし、アップグレード後の状態の確認 の説明に従ってその状態を確認します。
5. 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。

5.2. RHEL 8.8 から RHEL 9.2 へのアップグレードの実行

この手順では、**Leapp** ユーティリティーを使用して RHEL 8.8 から RHEL 9.2 へのアップグレードを実行するために必要なステップを説明します。

前提条件

- フルシステムバックアップを含め、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。
- 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を完了し、報告されたすべての問題が解決されている。

手順

1. RHEL 8 システムで、アップグレードプロセスを開始します。

```
# leapp upgrade
```

- 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/rhel9.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。**<channel>** は **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。

2. 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、Troubleshooting を参照してください。

3. システムを手動で再起動します。

   ```
   # reboot
   ```

   このフェーズでは、システムは RHEL 9 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 9 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** コマンドを実行し、この手動の手順を省略することもできます。

   障害が発生した場合は、トラブルシューティング で説明されているように、ログと既知の問題を調査してください。

4. RHEL 9 システムにログインし、アップグレード後の状態の確認 の説明に従ってその状態を確認します。

5. 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。

第6章 アップグレード後の状態の確認

RHEL 9 へのインプレースアップグレードを実行した後、システムが正しい状態にあることを確認します。これにより、システムに影響を与える可能性のある重大なエラーを特定して修正できます。

6.1. RHEL 9 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 9 へのインプレースアップグレード後に実行することが推奨される検証手順を紹介します。

前提条件

- 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がアップグレードされ、RHEL 9 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 OS バージョンが RHEL 9 であることを確認します。以下に例を示します。

```
# cat /etc/redhat-release
Red Hat Enterprise Linux release 9.4 (Plow)
```

- 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。以下に例を示します。

```
# uname -r
5.14.0-70.10.1.el9_0.x86_64
```

  .el9 は重要であるため、このバージョンは 5.14.0 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。以下に例を示します。

```
# subscription-manager list --installed
+-------------------------------------------+
    Installed Product Status
+-------------------------------------------+
Product Name: Red Hat Enterprise Linux for x86_64
Product ID:   479
Version:      9.4
Arch:         x86_64
Status:       Subscribed
```

  - アップグレード直後に、リリースバージョンが予想されるターゲット OS バージョンに設定されていることを確認します。以下に例を示します。

```
# subscription-manager release
Release: 9.4
```

- 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、Configuring and using database servers の手順に従ってください。

第7章 RHEL 9 システムでのアップグレード後のタスクの実行

インプレースアップグレード後、不要なパッケージを削除し、互換性のないリポジトリーを無効にし、レスキューカーネルと初期 RAM ディスクを更新して、RHEL 9 システムをクリーンアップします。

7.1. アップグレード後のタスクの実行

この手順では、RHEL 9 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主要タスクを紹介します。

前提条件

- アップグレードの実行 で説明されている手順に従って、システムがアップグレードされている。

RHEL 9 にログインできる。

- アップグレード後の状態の確認 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. **/etc/dnf/dnf.conf** 設定ファイルの除外リストから残りの **Leapp** パッケージを削除します。これには、アップグレードエクステンション開発用のツールである **snactor** パッケージが含まれます。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後、システムから削除する前に、これらの **Leapp** パッケージを exclude 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。

   - exclude 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。

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

2. 残りの **Leapp** パッケージを含む残りの RHEL 8 パッケージを削除します。

   a. RHEL 9 システムから古いカーネルパッケージを削除します。カーネルパッケージの削除の詳細は、What is the proper method to remove old kernels from a Red Hat Enterprise Linux system? を参照してください。

   b. 残りの RHEL 8 パッケージを見つけます。

      ```
      # rpm -qa | grep -e '\.el[78]' | grep -vE '^(gpg-pubkey|libmodulemd|katello-ca-consumer)' | sort
      ```

   c. RHEL 9 システムから残りの RHEL 8 パッケージを削除します。RPM の依存関係を確実に維持するには、このアクションを実行する際に **DNF** を使用します。承認する前にトランザクションを確認し、意図せずにパッケージが削除されていないことを確認します。
   以下に例を示します。

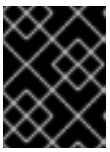
```
# dnf remove $(rpm -qa | grep \.el[78] | grep -vE 'gpg-pubkey|libmodulemd|katello-ca-consumer`)
```

d. 残りの **Leapp** 依存関係パッケージを削除します。

```
# dnf remove leapp-deps-el9 leapp-repository-deps-el9
```

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. パッケージが RHEL 9 と互換性がない DNF 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。

```
# dnf 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。

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

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)"
```

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

1. 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"
```

2. 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8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中に、SELinux ポリシーを Permissive モードに切り替える必要があります。さらに、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復元するには、SELinux を再度強制モードに切り替え、システム全体の暗号化ポリシーを確認します。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。また、一部のセキュリティー関連コンポーネントでは、正しくアップグレードするために更新前の手順が必要です。

8.1. 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、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。考えられる SELinux 拒否をすべて確認するには、完全な手順を説明する Using SELinux の Identifying SELinux denials 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

8.2. システム全体の暗号化ポリシー

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。

インプレースアップグレードプロセスでは、RHEL 8 で使用した暗号化ポリシーが保持されます。たとえば、RHEL 8 で **DEFAULT** 暗号化ポリシーを使用した場合、RHEL 9 にアップグレードしたシステムでは **DEFAULT** も使用します。事前定義されたポリシーの特定の設定は異なり、RHEL 9 暗号化ポリシーには、より厳密でより安全なデフォルト値が含まれていることに注意してください。たとえば、RHEL 9 **DEFAULT** 暗号化ポリシーは署名の SHA-1 の使用を制限し、**LEGACY** ポリシーは 2048 ビット未満の DH および RSA 暗号を許可しなくなりました。詳細は、セキュリティーの強化 の システム全体の暗号化ポリシーの使用 セクションを参照してください。カスタム暗号化ポリシーは、インプレースアップグレード全体で保持されます。

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
```

既存またはサードパーティーの暗号署名を検証するために SHA-1 を使用する必要がある場合は、次のコマンドを入力して有効にできます。

```
# update-crypto-policies --set DEFAULT:SHA1
```

または、システム全体の暗号化ポリシーを **LEGACY** ポリシーに切り替えることもできます。ただし、**LEGACY** は、安全ではない他の多くのアルゴリズムも有効にします。

警告

SHA サブポリシーを有効にすると、システムがデフォルトの RHEL 9 設定よりも脆弱になります。**LEGACY** ポリシーへの切り替えはセキュリティーレベルがさらに低くなるため、使用に際して注意が必要です。

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。カスタム暗号化ポリシーを使用する場合は、暗号化とコンピューターハードウェアの進歩によってもたらされる脅威を軽減するために、ポリシーを確認および更新することを検討してください。

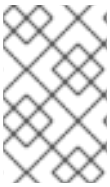
関連情報

- 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

8.3. 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 9 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、RHEL のメジャーバージョン間で異なります。

強化された RHEL 8 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 9 の推奨環境とは異なる場合があります。



注記

RHEL 8 および RHEL 9 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。

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。アップグレード後にシステム設定が変更されたため、自動修復を実行しても、システムが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。

以下の手順の例では、PCI-DSS プロファイルに従ってシステム設定を強化します。

前提条件

- RHEL 9 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-rhel9-ds.xml
...
```

詳細は、Viewing compliance profiles のセクション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-rhel9-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 9 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-rhel9-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 Security Policy
- Red Hat Satellite Security Policy

8.4. USBGUARD ポリシーの確認

USBGuard ソフトウェアフレームワークを使用すると、カーネルの USB デバイス認証機能に基づいて、許可されているデバイスおよび禁止されているデバイスのリストを使用して、侵入型 USB デバイスからシステムを保護できます。

前提条件

- アップグレードの前に、シナリオの要件を反映した USB デバイス用のルールセットを作成している。
- **usbguard** サービスが RHEL 9 システムにインストールされ、実行されている。

手順

1. **/etc/usbguard** ディレクトリーに保存されている *.conf ファイルをバックアップします。
2. **usbguard generate-policy** を使用して、新しいポリシーファイルを生成します。このコマンドは、現在存在する USB デバイスのルールのみを生成することに注意してください。
3. 新たに生成されたルールを、以前のポリシーのルールと比較します。
   a. 新しいポリシーを生成したときに存在したデバイスのルールと、同じデバイスのアップグレード前のルールに違いがあることが確認された場合、後で挿入される可能性のあるデバイスについても、元のルールを相応に修正する必要があります。
   b. 新規生成されたルールとアップグレード前のルールに違いがない場合は、RHEL8 で作成されたポリシーファイルを変更せずに使用できます。

関連情報

- Protecting systems against intrusive USB devices .

8.5. FAPOLICYD データベースの更新

fapolicyd ソフトウェアフレームワークは、ユーザー定義のポリシーに基づいてアプリケーションの実行を制御します。

まれに、**fapolicyd** 信頼データベース形式で問題が発生する場合があります。データベースを再構築するには、以下を実行します。

1. サービスを停止します。

```
# systemctl stop fapolicyd
```

2. データベースを削除します。

```
# fapolicyd-cli --delete-db
```

3. サービスを起動します。

```
# systemctl start fapolicyd
```

カスタム信頼ファイルを信頼データベースに追加した場合は、**fapolicyd-cli -f update <FILE>** コマンドを使用して個別に更新するか、**fapolicyd-cli -f update** を使用してまとめて更新します。変更を適用するには、**fapolicyd-cli –update** コマンドを使用するか、**fapolicyd** サービスを再起動します。

また、カスタムバイナリーには、新しい RHEL バージョン用の再構築が必要になる場合があります。このような更新は、fapolicyd データベースを更新する前に行ってください。

関連情報

- fapolicyd を使用したアプリケーションの拒否および許可

8.6. DBM から SQLITE への NSS データベースの更新

多くのアプリケーションでは、**NSS_DEFAULT_DB_TYPE** 環境変数をシステムの **sql** に設定すると、NSS データベース形式が DBM から SQLite に自動的に変換されます。**certutil** ツールを使用すると、すべてのデータベースが変換されていることを確認できます。

注記

RHEL 9 にアップグレードする前に、DBM 形式に保存されている NSS データベースを変換します。つまり、RHEL 9 にアップグレードする RHEL システム (6、7、および 8) で以下の手順を実行します。

前提条件

- **nss-tools** パッケージがシステムにインストールされている。

手順

1. **NSS_DEFAULT_DB_TYPE** を、システム上で **sql** に設定します。

```
# export NSS_DEFAULT_DB_TYPE=sql
```

2. すべてのディレクトリーでの変換コマンドの使用[1] これには、以下のように DBM 形式の NSS データベースファイルが含まれます。

```
# certutil -K -X -d /etc/ipsec.d/
```

データベースファイルがパスワードで保護されている場合は、**-f** オプションの値としてパスワードまたはパスワードファイルへのパスを指定する必要があります。以下に例を示します。

```
# certutil -K -X -f /etc/ipsec.d/nsspassword -d /etc/ipsec.d/
```

関連情報

- **certutil(1)** man ページ。

8.7. BERKELEY DB 形式から GDBM への CYRUS SASL データベースの移行

RHEL 9 の **cyrus-sasl** パッケージは **libdb** 依存関係なしでビルドされ、**sasldb** プラグインは Berkeley DB の代わりに GDBM データベース形式を使用します。

前提条件

- **cyrus-sasl-lib** パッケージがシステムにインストールされている。

手順

- 古い Berkeley DB 形式で保存されている既存の Simple Authentication and Security Layer (SASL) データベースを移行するには、**cyrusbdb2current** を使用します。以下の構文を使用します。

```
# cyrusbdb2current <sasldb_path> <new_path>
```

関連情報

- **cyrusbdb2current (1)** man ページ

---

[1] RHEL には、システム全体の NSS データベースが **/etc/pki/nssdb** ディレクトリーに含まれています。その他の場所は、使用するアプリケーションによって異なります。たとえば、Libreswan はデータベースを **/etc/ipsec.d/** ディレクトリーに保存し、Firefox は **/home/<username>/.mozilla/firefox/** ディレクトリーを使用します。

第9章 トラブルシューティング

RHEL 8 から RHEL 9 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。

9.1. 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。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 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。

9.2. 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

- システムが 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てください。

- アップグレードの準備 に記載されているすべての手順を実行してください。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。以下に例を示します。
  - Are there no VDO devices on the system?
- 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 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できます。

例9.1 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。

```
[check_vdo]
# Title:            None
# Reason:           Confirmation
# ============================== check_vdo.confirm
==============================
# Label:            Are all VDO devices, if any, successfully converted to LVM management?
# Description:      Enter True if no VDO devices are present on the system or all VDO devices on
the system have been successfully converted to LVM management. Entering True will circumvent
check of failures and undetermined devices. Recognized VDO devices that have not been
converted to LVM management can still block the upgrade despite the answer.All VDO devices
must be converted to LVM management before upgrading.
# Reason:           To maximize safety all block devices on a system that meet the criteria as
possible VDO devices are checked to verify that, if VDOs, they have been converted to LVM
management. If the devices are not converted and the upgrade proceeds the data on unconverted
VDO devices will be inaccessible. In order to perform checking the 'vdo' package must be
installed. If the 'vdo' package is not installed and there are any doubts the 'vdo' package should be
installed and the upgrade process re-run to check for unconverted VDO devices. If the check of
any device fails for any reason an upgrade inhibiting report is generated. This may be problematic
if devices are dynamically removed from the system subsequent to having been identified during
device discovery. If it is certain that all VDO devices have been successfully converted to LVM
management this dialog may be answered in the affirmative which will circumvent block device
checking.
# 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。この例では、質問は **Are all VDO devices, if any, successfully converted to LVM management?** です。

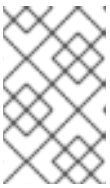
この質問に回答するには、最後の行をコメント解除し、回答として **True** または **False** を入力します。この例では、選択した回答は **True** です。

```
[check_vdo]
...
# 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

- システムが正常にアップグレードされたように見えても、古い RHEL 8 カーネルで起動した場合は、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てください。
- アップグレード後の状態の確認 で推奨されている手順を必ず行ってください。
- 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。

9.3. RHEL 8.10 から RHEL 9.4 へのアップグレードに関する既知の問題

アップグレード時に発生する可能性のある既知の問題を以下に示します。

- 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 8 システムが、Red Hat が提供しているにもかかわらず RHEL 9 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、**Leapp** はアップグレードを行いません。ただし、RHEL 8 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。

- 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、アップグレードする前に、以下のいずれかのオプションを選択します。

  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。

- RHEL 8 では、VDO マネージャーまたは論理ボリュームマネージャー (LVM) を使用して、Virtual Data Optimizer (VDO) ボリュームを管理できます。RHEL 9 では、LVM を使用した VDO ボリュームの管理のみが可能です。RHEL 9 で VDO 管理のボリュームを引き続き使用するには、アップグレード前にそれらのボリュームを LVM 管理の VDO ボリュームにインポートします。詳細は、LVM への既存 VDO ボリュームのインポート 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。(BZ#1957192)

- **Leapp** ユーティリティーは通常、インプレースアップグレード時に、RHEL 8 と RHEL 9 の間の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持つシステムなど、一部のシステムでは、RHEL 8 と RHEL 9 の間で NIC 名を更新する必要がある場合があります。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 8 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)

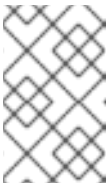
- BIOS を使用してシステムを起動する場合は、コアイメージのインストールに十分な領域が、ブートディスクの埋め込み領域に含まれていないと、GRUB2 ブートローダーをアップグレードするときにインプレースアップグレードが失敗します。これによりシステムが破損し、RHEL 6 **fdisk** ユーティリティーなどを使用してディスクが手動でパーティション分割された場合に発生する可能性があります。この問題がユーザーに影響するかどうかを確認するには、以下の手順を実行します。

  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 9.0 コアイメージには少なくとも 36 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 73 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 9 コアイメージは 36 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 9 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 9 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 'rhui-microsoft-azure-rhel8', ignoring this repo に記載されている手順を実行します。(RHEL-3296)

- 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
  ```

  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)

- **/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)

- 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)

- ARM アーキテクチャーを備えた Amazon Web Services (AWS)での Red Hat Update Infrastructure (RHUI)を使用したインプレースアップグレードで、現在問題が発生しています。代わりに Red Hat Subscription Management (RHSM)を使用してください。(RHEL-38909)

- RHUI を使用してアップグレードする場合、**/usr/share/leapp-repository/repositories/system_upgrade/common/files/rhui/** ディレクトリーのファイルは、アップグレード前のレポートのカスタムファイルとして誤って報告されます。このファイルを手動で変更しない限り、レポート内のこれらのファイルに関する警告を無視し、インプレースアップグレードは影響を受けません。(RHEL-40115)

9.4. RHEL 8.8 から RHEL 9.2 へのアップグレードに関する既知の問題

以下は、RHEL 8.8 から RHEL 9.2 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 8 システムが、Red Hat が提供しているにもかかわらず RHEL 9 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、**Leapp** はアップグレードを行いません。ただし、RHEL 8 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。

- 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、アップグレードする前に、以下のいずれかのオプションを選択します。

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。

- RHEL 8 では、VDO マネージャーまたは論理ボリュームマネージャー (LVM) を使用して、Virtual Data Optimizer (VDO) ボリュームを管理できます。RHEL 9 では、LVM を使用した VDO ボリュームの管理のみが可能です。RHEL 9 で VDO 管理のボリュームを引き続き使用するには、アップグレード前にそれらのボリュームを LVM 管理の VDO ボリュームにインポートします。詳細は、LVM への既存 VDO ボリュームのインポート 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。(BZ#1957192)

- **Leapp** ユーティリティーは通常、インプレースアップグレード時に、RHEL 8 と RHEL 9 の間の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持つシステムなど、一部のシステムでは、RHEL 8 と RHEL 9 の間で NIC 名を更新する必要がある場合があります。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 8 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)

- 利用可能なディスク容量が十分にない場合には、インプレースアップグレードが失敗する可能性があります。エラーメッセージとログには、問題および解決に関する誤解を招く情報や無効な情報が含まれる場合があります。この問題を解決するには、leapp fails with "There is not enough space on the file system hosting /var/lib/leapp directory to extract the packages" を参照してください。(BZ#1832730、BZ#2210300)

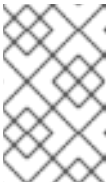
- BIOS を使用してシステムを起動する場合は、コアイメージのインストールに十分な領域が、ブートディスクの埋め込み領域に含まれていないと、GRUB2 ブートローダーをアップグレードするときにインプレースアップグレードが失敗します。これによりシステムが破損し、RHEL 6 **fdisk** ユーティリティーなどを使用してディスクが手動でパーティション分割された場合に発生する可能性があります。この問題がユーザーに影響するかどうかを確認するには、以下の手順を実行します。

  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 9.0 コアイメージには少なくとも 36 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 73 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 9 コアイメージは 36 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 9 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 9 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)
- 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
```

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)

- * ARM アーキテクチャーを使用した Amazon Web Services (AWS)での Red Hat Update Infrastructure (RHUI)を使用したインプレースアップグレードでは、現在問題が発生しています。代わりに Red Hat Subscription Management (RHSM)を使用してください。(RHEL-38909)

9.5. 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 8** 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10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 9 の採用における考慮事項
- 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 7 から RHEL 8 へのアップグレード
- Convert2RHEL ユーティリティーを使用した Linux ディストリビューションから RHEL への変換
- SAP 環境の RHEL 8 から RHEL 9 へのアップグレード
- 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 8 リポジトリー

アップグレードの前に、Preparing a RHEL 8 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が有効になっていることを確認します。

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**。

表A.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
64 ビット Intel および AMD	Base	**rhel-8-for-x86_64-baseos-rpms**
	AppStream	**rhel-8-for-x86_64-appstream-rpms**
64-bit ARM	Base	**rhel-8-for-aarch64-baseos-rpms**
	Extras	**rhel-8-for-aarch64-appstream-rpms**
IBM POWER (リトルエンディアン)	Base	**rhel-8-for-ppc64le-baseos-rpms**
	AppStream	**rhel-8-for-ppc64le-appstream-rpms**
IBM Z	Base	**rhel-8-for-s390x-baseos-rpms**
	AppStream	**rhel-8-for-s390x-appstream-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**。

表A.2 自発的な 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
64 ビット Intel および AMD	CodeReady Linux Builder	**codeready-builder-for-rhel-8-x86_64-rpms**
	Supplementary	**rhel-8-for-x86_64-supplementary-rpms**
64-bit ARM	CodeReady Linux Builder	**codeready-builder-for-rhel-8-aarch64-rpms**
	Supplementary	**rhel-8-for-aarch64-supplementary-rpms**
IBM POWER (リトルエンディアン)	CodeReady Linux Builder	**codeready-builder-for-rhel-8-ppc64le-rpms**

アーキテクチャー	リポジトリー	リポジトリー ID
	Supplementary	**rhel-8-for-ppc64le-supplementary-rpms**
IBM Z	CodeReady Linux Builder	**codeready-builder-for-rhel-8-s390x-rpms**
	Supplementary	**rhel-8-for-s390x-supplementary-rpms**

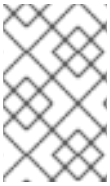
注記

インプレースアップグレードの前に、RHEL 8 CodeReady Linux Builder または RHEL 8 Supplementary リポジトリーを有効にすると、**Leapp** は RHEL 8 CodeReady Linux Builder または RHEL 8 Supplementary リポジトリーをそれぞれ有効にします。詳細は、Package manifest を参照してください。

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 9 のリポジトリー

システムが、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 9 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 8 と RHEL 9 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 OS バージョン (RHEL 9.4 など) を必ず有効にしてください。RHEL 9 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。

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、アップグレード前に少なくとも以下の RHEL 9 リポジトリーを **有効にして同期する必要** があります。

表B.1 RHEL 9 のリポジトリー

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 および AMD	BaseOS	**rhel-9-for-x86_64-baseos-rpms**	Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)	x86_64 **<target_os_version>**
	AppStream	**rhel-9-for-x86_64-appstream-rpms**	Red Hat Enterprise Linux 9 for x86_64 - AppStream (RPMs)	x86_64 **<target_os_version>**
64-bit ARM	BaseOS	**rhel-9-for-aarch64-baseos-rpms**	Red Hat Enterprise Linux 9 for ARM 64 - BaseOS (RPM)	aarch64 **<target_os_version>**
	AppStream	**rhel-9-for-aarch64-appstream-rpms**	Red Hat Enterprise Linux 9 for ARM 64 - AppStream (RPM)	aarch64 **<target_os_version>**
IBM Power (リトルエンディアン)	BaseOS	**rhel-9-for-ppc64le-baseos-rpms**	Red Hat Enterprise Linux 9 for Power, little endian - BaseOS (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
	AppStream	**rhel-9-for-ppc64le-appstream-rpms**	Red Hat Enterprise Linux 9 for Power, little endian - AppStream (RPMs)	ppc64le **<target_os_version>**
IBM Z	BaseOS	**rhel-9-for-s390x-baseos-rpms**	Red Hat Enterprise Linux 9 for IBM z Systems - BaseOS (RPMs)	s390x **<target_os_version>**
	AppStream	**rhel-9-for-s390x-appstream-rpms**	Red Hat Enterprise Linux 9 for IBM z Systems - AppStream (RPMs)	s390x **<target_os_version>**

<target_os_version> は、ターゲットの OS バージョン (例: **9.4**) に置き換えます。