



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

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

Copyright © 2020 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

概要

本ガイドは、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

RED HAT ドキュメントへのフィードバック (英語のみ)	3
第1章 アップグレードの計画	4
第2章 アップグレードに向けて RHEL 7 システムの準備	6
第3章 アップグレード前のレポートの確認	9
3.1. コマンドラインからのアップグレード可能性の評価	9
3.2. 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	10
第4章 RHEL 7 から RHEL 8 へのアップグレードの実行	15
第5章 RHEL 8 システムのアップグレード後の状態の確認	17
第6章 セキュリティポリシーの適用	19
6.1. SELINUX モードの ENFORCING への変更	19
6.2. システム全体の暗号化ポリシーの設定	20
6.3. セキュリティベースラインへのシステムの修復	20
第7章 トラブルシューティング	22
7.1. トラブルシューティングのリソース	22
7.2. トラブルシューティングのヒント	22
7.3. 既知の問題	23
7.4. サポートの利用	24
第8章 関連情報	26
付録A RHEL 7 リポジトリ	27

RED HAT ドキュメントへのフィードバック (英語のみ)

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。改善点を報告する場合は、以下のように行います。

- 特定の文章に簡単なコメントを記入する場合は、以下の手順を行います。
 1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上端に **Feedback** ボタンがあることを確認してください。
 2. マウスカーソルで、コメントを追加する部分を強調表示します。
 3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
 4. 表示される手順に従ってください。
- より詳細なフィードバックを行う場合は、Bugzilla のチケットを作成します。
 1. [Bugzilla](#) の Web サイトにアクセスします。
 2. Component で **Documentation** を選択します。
 3. **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記入してください。
 4. **Submit Bug** をクリックします。

第1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移行する方法です。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、以下の点を検討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** ユーティリティーによりアップグレードされます。
 - **利用可能な最新の RHEL 7 バージョン** の Server バリエーションがインストールされている。現在は以下のとおりです。
 - 64 ビット Intel、IBM POWER 8 (リトルエンディアン)、および IBM Z アーキテクチャーでの **RHEL 7.8**
 - **カーネルバージョン 4.14 を必要とする** アーキテクチャー (64-bit ARM、IBM POWER 9 (リトルエンディアン)、および IBM Z (Structure A)) での **RHEL 7.6**
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。
 - 提供されている最新の RHEL 7.8 および RHEL 8.2 コンテンツへのアクセス。詳細は、[2 章 アップグレードに向けて RHEL 7 システムの準備](#)の手順 1 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。
- **Security** - 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標準を定義し、「[RHEL 8 のセキュリティ変更](#)」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。
 - 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サポートされていません。
 - アップグレードが完了したら、セキュリティ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ポリシーを適用する方法は、[6 章 セキュリティポリシーの適用](#)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、[ReaR \(Relax-and-Recover\) ユーティリティー](#)、[LVM スナップショット](#)、[RAID 分割](#)、または仮想マシンのスナップショットを使用できます。
- **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。
- **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。

- ネットワークベースのマルチパスやネットワークストレージマウントは、システムパーティション (iSCSI、NFS など) として使用できません。
- 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 を使用しないパブリッククラウド (Amazon EC2、Azure、Huawei Cloud、Alibaba Cloud、Google Cloud) のオンデマンドインスタンスではサポートされません。

「[既知の問題](#)」も併せて参照してください。

[Red Hat Insights](#) を使用して、Insights に登録したどのシステムを RHEL 8 にアップグレードできるかを確認できます。これを行うには、[該当する Insights ルール](#) に移動し、見出しの **Affected systems** の下にある一覧を確認します。Insights ルールは 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。

第2章 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** コ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

- システムが、[1章 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。

手順

- Red Hat Subscription Manager を使用して、システムが Red Hat Content Delivery Network (CDN) または Red Hat Satellite 6.5 以降に適切に登録され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、Satellite が以下の条件を満たしていることを確認してください。

- Satellite には、RHEL 8 リポジトリをインポートしたサブスクリプションマニフェストがあります。詳細は、[Red Hat Satellite](#) の特定のバージョン ([バージョン 6.7](#) など) の『[コンテンツ管理ガイド](#)』の「[サブスクリプションの管理](#)」を参照してください。
- 以下のリポジトリが有効になり、最新の更新と同期され、Satellite で公開されます。
 - Red Hat Enterprise Linux 7 Server RPMs x86_64 7 または Red Hat Enterprise Linux 7 Server RPMs x86_64 7.8
 - Red Hat Enterprise Linux 7 Server - Extras (RPM)
 - Red Hat Enterprise Linux 8 for x86_64 - AppStream RPMs x86_64 8.2
 - Red Hat Enterprise Linux 8 for x86_64 - BaseOS RPMs x86_64 8.2
詳細は、[Red Hat Satellite](#) の特定バージョン ([バージョン 6.7](#) など) の『[コンテンツ管理ガイド](#)』の「[Red Hat コンテンツのインポート](#)」の章を参照してください。

- [Red Hat Enterprise Linux Server](#) サーバーのサブスクリプション が割り当てら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 Server
Product ID:    69
Version:      7.8
Arch:         x86_64
Status:       Subscribed
```

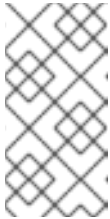
- 適切なリポジトリが有効になっていることを確認します。次のコマンドは、64 ビット Intel アーキテクチャーのリポジトリの一覧を示します。他のアーキテクチャーについては、[付録A RHEL 7 リポジトリ](#)を参照してください。

- Base リポジトリを有効にします。

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

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

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



注記

Optional リポジトリまたは Supplementary リポジトリも有効にすることができます。[付録A RHEL 7 リポジトリ](#)の一覧をご覧ください。この場合、**Leapp** は、[RHEL 8 CodeReady Linux Builder](#) リポジトリまたは [RHEL 8 Supplementary](#) リポジトリをそれぞれ有効にします。

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

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

- 必要に応じて、カスタムリポジトリを使用する場合は、「[Customizing your Red Hat Enterprise Linux in-place upgrade](#)」の指示に従って設定します。

- yum-plugin-versionlock** プラグインを使用して、パッケージを特定バージョンにロックする場合は、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。

- システムロケールが **en_US.UTF-8** に設定されていることを確認します。

```
$ cat /etc/locale.conf
```

ロケールが異なる場合は、「[RHEL7 のシステムロケールを変更する](#)」を参照してください。

- 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
```

- システムを再起動します。

```
# reboot
```

- Leapp** ユーティリティーをインストールします。

```
# yum install leapp leapp-repository
```

現在、**leapp** パッケージおよび **leapp-repository** パッケージの両方に、バージョン 0.10.0-2 以降が必要になります。

11. ナレッジベースの記事「[RHEL 7 から RHEL 8 へのインプレースアップグレード時に Leapp ユーティリティーに必要なデータ](#)」に添付されている追加の必須データファイル (RPM パッケージの変更および RPM リポジトリマッピング) をダウンロードして、`/etc/leapp/files/` ディレクトリに保存します。これは、アップグレードを成功させるために必要です。現在、**leapp-data8.tar.gz** アーカイブまたはそれ以降のデータファイルが必要になることに注意してください。
12. GRUB がデフォルトの場所 (`/boot`) 以外にインストールされている場合は、以下のように各環境変数をエクスポートします。

```
# export LEAPP_GRUB_DEVICE="/path_to_device"
```

13. (**Salt**、**Chef**、**Puppet**、**Ansible** などの) 設定管理を無効にしているか、元の RHEL7 システムを復元しないように適切に再設定していることを確認します。
14. 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。
15. 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。たとえば、ReaR (Relax-and-Recover) ユーティリティーを使用できます。詳細は、[ReaR のドキュメント](#) および「[Relax and Recover\(ReaR\) の概要](#)」を参照してください。または、[LVM スナップショット](#) または [RAID 分割](#) を使用することもできます。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。

第3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、**/var/log/leapp/leapp-report.txt** ファイルと Web コンソールの両方で利用できます。レポートは潜在的な問題を要約し、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。

アップグレード前のフェーズでアップグレード可能性を評価するには、以下のオプションがあります。

- 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ースを使用して、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。



重要

アップグレード前のフェーズでは、**Leapp** が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したり、すべての RPM パッケージをダウンロードしません。

アップグレード前のレポートを確認すると、インプレースアップグレードプロセスなしで RHEL 8 システムを再デプロイする必要がある場合にも役立ちます。

3.1. コマンドラインからのアップグレード可能性の評価

この手順では、コマンドラインインターフェースを使用して、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する方法を説明します。

前提条件

- 2章 [アップグレードに向けて RHEL 7 システムの準備](#) に記載されている手順を完了している。

手順

- 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
```



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](#) を使用する場合は、以下のように選択したリポジトリを有効にします。

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

[RHSM を使用しないアップグレード](#) を行う場合は、**--no-rhsm** オプションを追加します。

2. `/var/log/leapp/leapp-report.txt` ファイルのレポートを調べて、インプレースアップグレードに進む前に、報告されたすべての問題を手動で解決します。

3.2. 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

この手順では、アップグレード前のフェーズで潜在的な問題を特定する方法と、Web コンソールを使用して自動修復を適用する方法を説明します。

前提条件

- [2章 アップグレードに向けて RHEL 7 システムの準備](#)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。

```
# yum install cockpit-leapp
```

2. ブラウザーで Web コンソールに移動し、`root` または十分な権限を持つユーザーでログインします。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。
3. RHEL 7 システムで、コマンドラインインターフェースまたは 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
```



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 preupgrade --enablerepo repository_id1 --enablerepo repository_id2 ...
```

[RHSM を使用しないアップグレード](#) を行う場合は、`--no-rhsm` オプションを追加します。

4. Web コンソールで、左側のメニューから [インプレースアップグレードレポート](#) を選択します。

図3.1 Web コンソールのインプレースアップグレードレポート

In-Place Upgrade Report for: localhost.localdomain

Title	Risk Factor	Description	Tags	Time
Repositories map file is invalid (/etc/leapp/files/repomap.csv)	High	Inhibitor	upgrade process	26.08.2019 15:18:04
OpenSSH configured to use removed ciphers	High	Inhibitor Remediation hint	authentication security network services	26.08.2019 15:23:56
OpenSSH configured to use removed mac	High	Inhibitor Remediation hint	authentication security network services	26.08.2019 15:23:56
Packages not signed by Red Hat found in the system	High	Remediation command	sanity	26.08.2019 15:23:57
LUKS encrypted partition detected	High	Inhibitor	boot encryption	26.08.2019 15:23:59
Possible problems with remote login using root account	High	Inhibitor Remediation hint	authentication security network services	26.08.2019 15:23:59
chrony using default configuration	Medium		services time management	26.08.2019 15:23:57
Postfix has incompatible changes in the next major version	Low		services email	26.08.2019 15:23:58
The subscription-manager release is going to be set to 8.0	Low		upgrade process	26.08.2019 15:23:58
Schedule SELinux relabeling	Low		selinux security	26.08.2019 15:23:58

10 per page 1-10 of 16 1 of 2

レポートの表には、見つかった問題の概要、リスク評価、および修復 (利用可能な場合) が記載されています。

- リスク要因:
 - 高 - 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
 - 低 - 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
 - インヒビター - アップグレードプロセスを抑制 (ハードストップ) する。抑制しないと、システムが起動できず、アクセスできず、または機能しなくなる可能性があります。
 - 修復 - 報告された問題に対する実行可能な解決策
 - 修復コマンド - Web コンソールから直接実行可能
 - 修復のヒント - 問題を手動で解決する方法の手順
5. レポートの内容を調べます。ヘッダーをクリックして、テーブルを並べ替えることができます。詳細ペインを開くには、選択した行をクリックします。

図3.2 詳細ペイン

Title

Packages not signed by Red Hat found in the system

Time

26.08.2019 15:23:57

Risk factor ⓘ

● High

Summary

The following packages have not been signed by Red Hat and may be removed in the upgrade process: - leapp - leapp-deps - leapp-repository - leapp-repository-deps - leapp-repository-sos-plugin - python2-leapp - snactor

Links

- [Information about package signatures](#)

Remediations ⓘ

Run Remediation
Add to Remediation Plan

```
Command: yum remove leapp leapp-deps leapp-repository le
```

Related resources ⓘ

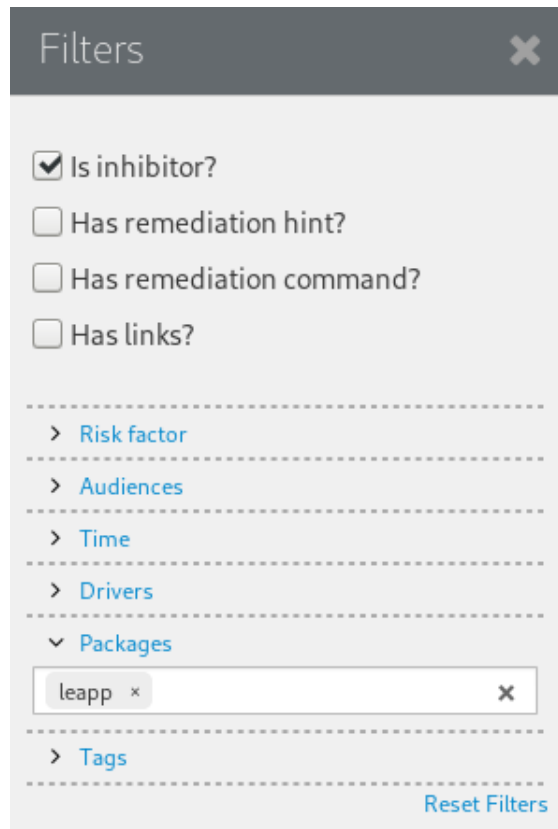
Package

- 📦 [leapp](#)
- 📦 [leapp-deps](#)
- 📦 [leapp-repository](#)

詳細ペインには、次の追加情報が表示されます。

- 問題の概要と、問題を詳細に説明するナレッジベース記事へのリンク
 - 修復 - 自動修復 (利用可能な場合) を実行またはスケジュールし、適用時にその結果を確認できます。
 - 影響を受けるシステムリソース: パッケージ、リポジトリ、ファイル (構成、データ)、ディスク、ボリューム
6. 必要に応じて、結果をフィルタリングします。レポートの左上隅にある **フィルター** ボタンをクリックし、設定に基づいてフィルターを適用します。フィルターカテゴリーは、相互に関連して適用されます。

図3.3 フィルター



7. 自動修復を適用する問題を選択します。2つのオプションがあります。
 - a. 詳細ペインの **Add to Remediation Plan** ボタンをクリックして、個々の項目を選択します。また、詳細ペインで **Run Remediation** をクリックして、個々の修正を直接実行できます。
 - b. レポートの右上隅にある **Add all remediations to plan** ボタンをクリックして、修復が利用可能なすべての項目を選択します。
8. レポートの右上隅にある **Remediation plan** リンクをクリックして、修復計画を開きます。修復計画には、実行した修復、または予定されている修復の一覧が表示されます。

図3.4 修復計画



9. **Execute Remediation Plan** をクリックして、予定されている修復をすべて処理します。修復エントリーごとに次の情報が表示されます。
 - 修復の一意の ID
 - コマンドの終了ステータス

- 実行された修復の経過時間
 - 標準出力
 - 標準エラー
10. 選択した修復を実行した後に、**leapp preupgrade** コマンドを使用してアップグレード前のレポートを再生成し、新しいレポートを調べてから、必要に応じて追加の修復手順を実行します。

第4章 RHEL 7 から RHEL 8 へのアップグレードの実行

この手順は、**Leapp** ユーティリティーを使用して RHEL 8 へアップグレードする方法を説明します。

前提条件

- [2章 アップグレードに向けて RHEL 7 システムの準備](#)の手順 (システム全体のバックアップも含む) が完了している。
- [3章 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 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
```



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 を使用しないアップグレード](#) を行う場合は、`--no-rhsm` オプションを追加します。

アップグレードプロセスの開始時、**Leapp** は、[3章 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[7章 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` コマンドを実行し、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、[7章 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、[5章 RHEL 8 システムの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。

4. セキュリティ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 [6章 セキュリティポリシーの適用](#) を参照してください。

第5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手順を紹介します。

前提条件

- [4章 RHEL 7 から RHEL 8 へのアップグレードの実行](#)の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 8.2 (Ootpa)
```

- 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
4.18.0-193.el8.x86_64
```

.el8 が重要です。

- 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: 8.2
Arch: x86_64
Status: Subscribed
```

- リリースバージョンが 8.2 に正しく設定されていることを確認します。

```
# subscription-manager release
Release: 8.2
```

リリースのバージョンが 8.2 に設定されている場合は、この特定のバージョンの RHEL に対してのみ **yum** 更新を受け取ります。RHEL 8 の最新のマイナーバージョンからの更新を利用できるように、リリースバージョンの設定を解除する場合は、次のコマンドを使用します。

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

- 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6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。本セクションでは、アップグレードした RHEL システムのセキュリティーを保護する方法を説明します。

6.1. 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
```

検証手順

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](#)

6.2. システム全体の暗号化ポリシーの設定

暗号化ポリシーは、コア暗号化サブシステムを構成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
```

RHEL 8.2 では、システム全体の暗号化ポリシーのカスタマイズが利用できます。詳細は「[ポリシー修飾子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

- 詳細は「[システム全体の暗号化ポリシーの使用](#)」と、man ページの `update-crypto-policies(8)` を参照してください。

6.3. セキュリティーベースラインへのシステムの修復

OpenSCAP スイートは、システムが PCI-DSS、OSPP、ACSC E8 などのセキュリティーベースラインに準拠する修正を提供します。以下の手順に従って、PCI-DSS プロファイルに準拠するようにシステム設定を変更します。



重要

Red Hat は、セキュリティーを強化した修正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。修正は、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、修正を実行しても、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。

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. **oscap** コマンドに **--remediate** オプションを指定して使用します。

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

前述の例の **pci-dss** は、シナリオに必要なプロファイルに置き換えることができます。

2. システムを再起動します。

```
# reboot
```

検証手順

1. そのシステムが PCI-DSS プロファイルにどのように準拠しているかを評価し、結果を **pcidss_report.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

- 詳細は「[セキュリティコンプライアンスおよび脆弱性スキャンの開始](#)」と、*man* ページの **scap-security-guide(8)** および **oscap(8)** を参照してください。

第7章 トラブルシューティング

本章では、トラブルシューティングに使用するリソースおよびヒントを紹介します。

7.1. トラブルシューティングのリソース

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。
- **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](#)」を参照)。

7.2. トラブルシューティングのヒント

アップグレード前のフェーズ

- システムが、[1章アップグレードの計画](#)に記載される条件をすべて満たしていることを確認します。
- [2章アップグレードに向けてRHEL 7システムの準備](#)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。
- 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](#)」の説明に従ってWeb コンソールを使用することもできます。

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。

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。
- [5章 RHEL 8 システムのアップグレード後の状態の確認](#) で推奨される手順を行います。
- 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で、サービスの拒否を検索します。

```
# ausearch -m AVC,USER_AVC -ts boot
# journalctl -t settroubleshoot
# 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。

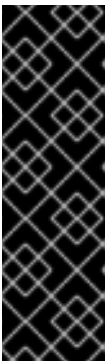
7.3. 既知の問題

- 現在、ネットワークチームは、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 プロキシを使用する場合は、Red Hat Subscription Manager がこのようなプロキシ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 システムが FCoE 論理ユニット番号 (LUN) にインストールされ、`bnx2fc` ドライバーを使用するネットワークカードに接続している場合、その LUN はアップグレード後に RHEL 8 で検出されません。したがって、アップグレードしたシステムは起動できません。(BZ#1718147)
- 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、削除されたドライバーのリスト (`/etc/leapp/repos.d/system_upgrade/el7toel8/actors/kernel/checkkerneldrivers/files/removed_drivers.txt`) に含まれていないサードパーティーのデバイスドライバを使用している場合、**Leapp** はそのようなドライバーを検出しないため、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。
- この時点では、Samba モジュールの `winbind` および `wins` が `/etc/nsswitch.conf` ファイルで使用されていると、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** によりアップデートが行われません。

```
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. アップグレードを行ったら、システムの設定要件に従って、**winbind** 文字列および **wins** 文字列を、**/etc/nsswitch.conf** の各エントリーに追加します。
(BZ#1410154)
- **Leapp** ユーティリティは、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** ユーティリティを使用して RHEL 7 システムで認証を構成した場合は、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構成が正しく機能するようにするには、**authselect** ユーティリティを使用して RHEL 8 システムを再構成します。



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。したがって、RHEL 7 システムの PAM 構成に、**pam_krb5** モジュールまたは **pam_pkcs11** モジュールが含まれ、これらのモジュールに **必要不可欠** または **必須** の制御値がある場合は、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 システムを再構成して、**pam_krb5** または **pam_pkcs11** を使用しないようにします。

- IBM Z システムでは、**Leapp** では、DASD ディスクが常に接続されていることが必要になります。したがって、**/etc/dasd.conf** ファイルが存在しない場合、インプレースアップグレードは失敗します。この問題を回避するには、**touch > /etc/dasd.conf** コマンドを使用して、空の **dasd.conf** ファイルを作成します。(BZ#1783248)
- 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。

7.4. 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 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 の役割と取得方法」](#) 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、管理する方法は、ナレッジベースのアーティクル [「カスタマーポータルでサポートケースを作成および管理する」](#) を参照してください。

第8章 関連情報

- [Red Hat Enterprise Linux テクノロジーの機能と制限](#)
- [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 6 から Red Hat Enterprise Linux 7 への移行方法](#)
- [RHEL 6 から RHEL 8 へのアップグレード](#)
- [How to convert from CentOS or Oracle Linux to RHEL](#)
- [Red Hat Insights ドキュメント](#)

付録A RHEL 7 リポジトリー

アップグレードの前に、2章アップグレードに向けてRHEL 7 システムの準備の手順3 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
64 ビット ARM	Base	rhel-7-for-arm-64-rpms
	Extras	rhel-7-for-arm-64-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 POWER9 (リトルエンディアン)	Base	rhel-7-for-power-9-rpms
	Extras	rhel-7-for-power-9-extras-rpms
IBM Z	Base	rhel-7-for-system-z-rpms
	Extras	rhel-7-for-system-z-extras-rpms
IBM Z (Structure A)	Base	rhel-7-for-system-z-a-rpms
	Extras	rhel-7-for-system-z-a-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
64 ビット ARM	任意	rhel-7-for-arm-64-optional-rpms
	Supplementary	該当なし

アーキテクチャー	リポジトリ	リポジトリ ID
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 POWER9 (リトルエン ディアン)	任意	rhel-7-for-power-9-optional-rpms
	Supplementary	rhel-7-for-power-9-supplementary-rpms
IBM Z	任意	rhel-7-for-system-z-optional-rpms
	Supplementary	rhel-7-for-system-z-supplementary-rpms
IBM Z (Structure A)	任意	rhel-7-for-system-z-a-optional-rpms
	Supplementary	該当なし



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 リポジトリを有効にすると、**Leapp** は、[RHEL 8 CodeReady Linux Builder](#) リポジトリまたは [RHEL 8 Supplementary](#) リポジトリをそれぞれ有効にします。

カスタムリポジトリを使用する場合は、[「Configuring custom repositories」](#) の指示に従って、カスタムリポジトリを有効にします。