Leapp について

Leapp は、Red Hat® Enterprise Linux® のあるメジャーバージョンから他のメジャーバージョンにインプレース・システム・アップグレードを実行する際に使用するサポートツールです。Leapp を使用すると、システムを再インストールすることなく、安心してアップグレードし、Red Hat Enterprise Linux の新機能のメリットを得ることができます。

アップグレードすべき理由

「Red Hat Enterprise Linux にアップグレードする主な理由チェックリスト」をご覧ください。

アップグレードをすると、最新の拡張機能、修正、パッチに加え、Red Hat Enterprise Linux の新しいメジャーバージョンに含まれる新機能が適用されたサポート製品を利用して、ビジネス継続性を維持できます。

Red Hat Enterprise Linux のパフォーマンス向上により、総所有コスト (TCO) を削減し、生産性に影響を与え、技術投資を最大化できます。

Red Hat Enterprise Linux は予測可能な 3 年間のメジャーリリースサイクルで提供されており、サブスクリプションは Red Hat Enterprise Linux の現在サポートされているすべてのバージョンで利用できます。このため、最新の先進的なテクノロジーにアクセスし、新しいバージョンが提供された際にはそのテクノロジーを活用できます。Red Hat Enterprise Linux の各メジャーバージョンのサポート期間は 10 年間で、2 つのサポートフェーズに分かれています。

最初のフェーズは一般提供 (GA) から 5 年間のフルサポートです。新機能の追加、新しいハードウェアのサポート、問題やバグの修正が行われます。その後の 5 年間はメンテナンスサポートとなり、重大および重要評価のセキュリティエラータの発行、一部の機能やバグ修正の改善が継続して行われます。10 年間の通常ライフサイクルの終了後は、Red Hat 延長ライフサイクルサポートアドオンを購入することで、「重大および重要」のセキュリティエラータを含むサポートをさらに 2 年間受けることができます。詳細については、「Red Hat Enterprise Linux のライフサイクル」ページをご覧ください。

Red Hat Enterprise Linux にアップグレードすることで、次のような複数の新機能によるメリットを得ることができます。

- アプリケーション・ストリームによって提供される更新ソフトウェアから Red Hat Enterprise Linux メジャーリリースのフルサポートフェーズを通じて提供される、新しい言語ランタイム、データベース、その他のアプリケーション
- コンテナの構築、デプロイ、管理をサポートする、Podman、Buildah、Skopeo などの Red Hat Enterprise Linux コンテナツール
- 再起動することなく、選択された重要および重大な共通脆弱性識別子 (CVE) に対してカーネルにパッチを適用できる、カーネルライブパッチ (kpatch)

- eBPF ベースのツールを使用した、システムパフォーマンスの側面に関するインサイトをすばやく得るためのパフォーマンス観測ツール
- 通常はデスクトップ・アプリケーションに使用されるアプリケーションを実行するための Flatpak サポート
- プロセスが消費するリソースを調整するための最適化された機能を備えた Cgroup2

スムーズな管理を実現する改良された Web コンソール・インタフェースなど、自動化と管理に関する拡張機能が多数提供されています。

自動化の拡張機能には次のようなものがあります。

- Red Hat Ansible® Automation Platform で駆動し、大規模な管理を自動化する、Red Hat Enterprise Linux の新しいシステムロール
- すべての Red Hat Enterprise Linux サブスクリプションに含まれ、脆弱性、ロールの欠落、その他の事前定義済みの条件をプロアクティブにスキャンする Red Hat Insights

ハードウェアを最大限に活用したいと考えている場合、一般的に Red Hat Enterprise Linux 9 のパフォーマンスは Red Hat Enterprise Linux 7 や Red Hat Enterprise Linux 8 より優れていることに注目してください。これを実現している変更点は次のとおりです。

- カーネル用の新しいディスクエレベーター
- 新しいチューニングされたパフォーマンスプロファイル

製品情報については「Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 8 へのアップグレード」をご覧ください。

Leapp の概要と使用すべき理由

サーバーのアップグレードは困難な作業ですが、Red Hat Enterprise Linux ではサポート付きのアップグレード管理ツールとして Leapp が一緒に提供されています。Leapp は Red Hat Enterprise Linux の次のメジャーバージョンにアップグレードするための単一パスを提供します。Leapp を使用すると、元のサブスクリプション (システムに関連付けられている)、システム設定、カスタムリポジトリ、サードパーティ・アプリケーションを維持できます。

Leapp は Red Hat Enterprise Linux 7 と Red Hat Enterprise Linux 8 に含まれており、Red Hat Enterprise Linux 7.9 から Red Hat Enterprise Linux 8 へのアップグレードが可能です。また、Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9 へのアップグレードにも使用できます。

Red Hat Enterprise Linux 6 を使用している場合、Leapp を使用して Red Hat Enterprise Linux 8 または Red Hat Enterprise Linux 9 にアップグレードする前に、他のツールを使用して Red Hat Enterprise Linux 7 にアップグレードする必要があります。

以下の表は、Leapp を使用してサーバーをアップグレードするメリットの一覧です。

Leapp を使用したインプレース・アップグレード	再インストール
設定を保持	設定データのバックアップと再起動が必要
マシンは既存のサブスクリプションデータを保持	サブスクリプション・マネージャーを使用してマシンをサブスクライブする必要がある
自動化により生産性に好影響を与える	追加の時間とコストが必要

仕組み

Leapp の仕組みを理解しておくと、アップグレードを成功させやすくなります。Leapp を使用する際は、アップグレード可能性の分析と実際のアップグレードという 2 段階のプロセスに分かれます。アップグレード後は再起動が必要であり、アップグレードの計画時にはこの点を考慮することが重要です。

単一のホストで Leapp を使用する場合、アップグレード可能性の分析は *cloud.redhat.com* からメタデータとしてダウンロードされるアップグレードの検討事項に基づいて行われます。

Red Hat Satellite に接続されているホストの場合、メタデータは Satellite から Leapp を使用しているサーバーに配布される必要があります。その後 Red Hat Satellite 用の Leapp プラグインを使用して、アップグレード可能性の分析を大規模に行うことができます。

アップグレード可能性の分析ではレポートが生成され、レポートにはアップグレードを実行する前に解決すべき項目が含まれる場合があります。

Leapp はワークフローの一部として複数の Python プログラムを使用します。これらの Python プログラムはアクターと呼ばれ、システムに変更を加えることができます。

「Using Red Hat Satellite to upgrade with Leapp」をご覧ください。

アクターの一例は **CheckOSRelease** で、現在の Red Hat Enterprise Linux のマイナーバージョンがサポートされているかどうかをチェックします。サポートされていない場合は、アップグレードプロセスを阻止します。

既存の一連のアクターで対処できないアップグレードの検討事項がある場合は、それらの検討事項を修正、阻止、または通知する独自のカスタムアクターを作成できます。作成したアクターは Leapp のワークフローに組み込むことができます。

Leapp は Red Hat Insights と統合されており、登録されたマシンをスキャンしてアップグレードの対象となるマシンを特定します。

Leapp を使用したアップグレードは、コマンドラインや Red Hat Satellite から実行できます。

制限

サーバーのアップグレードに進む前に、次のような Leapp を使用する際のいくつかの重要な制限について理解する必要があります。

- Leapp は Red Hat Enterprise Linux のあるメジャーバージョンから次のメジャーバージョンへのアップグレードにのみ使用できます。
- Leapp はシステムでルートファイルシステムにディスク暗号化を使用している場合、動作しません。
- VDO デバイスは LVM で管理されるよう変換する必要があります。
- ネットワークベースのマルチパスや、iSCSI やネットワークファイルシステム (NFS) などのネットワーク・ストレージ・マウントは、システムパーティションには使用できません。
- Red Hat Update Infrastructure (Red Hat Subscription Manager とは異なります) を使用しているパブリッククラウドのオンデマンドインスタンスは、Leapp を使用してアップグレードできません。

アップグレードの準備ができたら最初に行うこと

Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのアップグレードがどのように行われるか見てみましょう。Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9 へのアップグレードの場合も同様のワークフローになります。次のように **yum update** を使用して、システムが Red Hat Enterprise Linux 7.9 に更新済みであることを確認します。

```
[root@leapp7to8 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.9 (Maipo)
```

Leapp パッケージをインストールする必要があります。マシンが Red Hat CDN または Satellite サーバーをサブスクライブしており、Red Hat Enterprise Linux 7 Extras チャンネルが有効になっていることを確認します。これは次のコマンドを使用して確認できます。

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-7-server-extras-rpms
Repo Name: Red Hat Enterprise Linux 7 Server - Extras (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/7Server/$basearch/extras/os
Enabled:   1


Repo ID:   rhel-7-server-rpms
Repo Name: Red Hat Enterprise Linux 7 Server (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/$releasever/$basearch/os
Enabled:   1
```

rhel-7-server-extras-rpms リポジトリが有効になっていない場合は、次のコマンドを使用して有効化します。

```
[root@leapp7to8 ~]# subscription-manager repos --enable
rhel-7-server-extras-rpm
```

これで次のコマンドを使用して Leapp を Red Hat Enterprise Linux 7 にインストールできるようになりました。

```
[root@leapp7to8 ~]# yum install -y leapp
```

Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9 にアップグレードする場合、次の手順を確認して Leapp インプレース・アップグレード・ユーティリティをインストールします。Red Hat Enterprise Linux 9 にアップグレードする前に Red Hat Enterprise Linux 8 サーバーの更新が必要な場合があります。詳細については、「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」をご覧ください。

```
[root@leapp8to9 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.6 (Ootpa)
```

leapp と **leapp-upgrade-el8toel9** パッケージをインストールする必要があり、どちらのパッケージも **rhel-8-for-x86_64-appstream-rpms** リポジトリで入手できます。これらのパッケージをインストールするには、次のコマンドを使用します。

```
[root@leapp8to9 ~]# yum install -y leapp leapp-upgrade-el8toel9
```

過去に Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのインプレース・アップグレードを行っており、**/root/tmp_leapp_py3** ディレクトリがシステム上に存在する場合は、次のコマンドを使用して削除します。

```
[root@leapp8to9 ~]# rm -rf /root/tmp_leapp_py3
```

Red Hat Enterprise Linux リリース用の Leapp インプレース・アップグレード・パッケージをインストールしたら、アップグレードを実行する前に **leapp preupgrade** でサーバーを分析して、潜在的な問題を特定する必要があります。システムは変更されず、アップグレードパスを示す重要なファイルが作成されます。

```
[root@leappXtoY ~]# leapp preupgrade
```

preupgrade コマンドを実行すると、以下のような出力が表示されます。

```
…
出力内容省略
…

==========================================================
                    UPGRADE INHIBITED
==========================================================
```

```
Upgrade has been inhibited due to the following problems:
    1. Inhibitor: Use of NFS detected. Upgrade can't proceed
Consult the pre-upgrade report for details and possible remediation.

====================================================================
                        UPGRADE INHIBITED
====================================================================

Debug output written to /var/log/leapp/leapp-preupgrade.log

====================================================================
                              REPORT
====================================================================

A report has been generated at /var/log/leapp/leapp-report.json
A report has been generated at /var/log/leapp/leapp-report.txt

====================================================================
                          END OF REPORT
====================================================================

Answerfile has been generated at /var/log/leapp/answerfile
```

注目すべきファイル：

/var/log/leapp/leapp-report.txt	leapp アップグレードレポートに関する読みやすく理解しやすい情報
/var/log/leapp/leapp-report.json	同じ情報が JSON 形式で記述されたもの
/var/log/leapp/leapp-preupgrade.log	leapp preupgrade コマンドのデバッグ出力
/var/log/leapp/answerfile	leapp upgrade コマンドで尋ねられる質問に対する回答

アップグレード可能性の分析レポートは **/var/log/leapp/leapp-report.txt** に保存されます。このレポートには、アップグレードを実行する前に対処すべき重要な検討事項が記載されている場合があります。これらの検討事項にはユーザーの入力が必要なものもあり、レポート内の指示に従うことで対応できます。

Leapp のアップグレード前の検討事項に対処する

/var/log/leapp/leapp-report.txt にある Leapp のアップグレード前のレポートには、対処すべき項目が複数記載されている場合があります。***inhibitor*** (阻害要因) は、アップグレードを進めるために対処する必要がある障害となる項目です。阻害要因が解決されない場合、leapp upgrade はシステムで実行されません。

risk factor (リスク要因) は、アップグレードの検討事項の影響を以下のキーを使用して表しています。

High (高)	状態が悪化する可能性が非常に高い
Medium (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 (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
Info (情報)	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

Title (タイトル) は Leapp のアップグレード前レポートの要素を示し、より詳しい内容が Summary (概要) 記載されます。

Summary (概要) は、対処が必要な可能性がある検出された問題の短い説明文です。

Remediation (対策) は報告された問題に対する実用的な解決策です。よくある対策として、次のものがあります。

- 設定ファイルの編集
- システムの動作を変更するコマンドの実行
- Leapp answerfile を使用した対策
- Python、PHP、Node.js、PostgreSQL など Red Hat Enterprise Linux 7 Software Collections Library のモジュール式ソフトウェアに影響を与える対策
- NFS エクスポートの一時的なアンマウント

高リスク要因および中リスク要因のアップグレードにおける検討事項の例は、このセクションで紹介しており、次の内容で構成されています。

- Leapp レポートで報告されたメッセージ (例ではスニペット)
- 影響を受けるソフトウェア・サブシステム
- 報告された項目の具体的な内容の説明
- 実施すべきアクション
- 報告された対処可能な項目に対応しなかった場合の結果

アップグレードする Red Hat Enterprise Linux のバージョンや設定により、異なる検討事項が表示される場合があります。

例 1：システムの一時的な変更が必要な高リスクの阻害要因

以下は事前評価レポートで報告された高評価の阻害要因の例です。この問題が解決されない場合、このシステムで leapp upgrade を実行するとエラーが表示され、システムはアップグレードされません。ここではメッセージに加え、システムでこの問題を解決する方法を確認します。

```
Risk Factor: high (inhibitor)
Title: Use of NFS detected. Upgrade can’t proceed
Summary: NFS is currently not supported by the inplace upgrade.
We have found NFS usage at the following locations:
- One or more NFS entries in /etc/fstab
- Currently mounted NFS shares

Remediation: [hint] Disable NFS temporarily for the upgrade if possible.
Key: 9881b25faceeeaa7a6478bcdac29afd7f6baaaed
```

この内容に従わなかった場合どうなるか

これは阻害要因であり、適切なアクションが実行されるまでアップグレードは進みません。変更が行われるのはローカルサーバーのみで、NFS 共有には行われない見込みのため、リスク要因は高です。

影響を受けるサブシステム

NFS マウント

具体的な内容

NFS マウントはアップグレード処理中は使用できません。アップグレードが終了するまで、アンマウントして無効にする必要があります。

必要な対応

etc/fstab を編集して NFS 共有を一時的にコメントアウトし、現在マウントされている NFS 共有をアンマウントします。autofs.service を一時的に停止し、無効にします。アップグレードが完了したら、NFS エントリーと autofs.service を再び有効にします。

```
[root@leapp8to9 ~]# systemctl disable –now autofs.service
```

例 2：既存の設定ファイルへの変更が必要な高リスクの阻害要因

これは主に Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのアップグレードに当てはまります。

```
Risk Factor: high (inhibitor)

Title: Possible problems with remote login using root account

Summary: OpenSSH configuration file does not explicitly state the option
PermitRootLogin in sshd_config file, which will default in Red Hat
Enterprise Linux8 to “prohibit-password”.

Remediation: [hint] If you depend on remote root logins using passwords,
consider setting up a different user for remote administration or adding
“PermitRootLogin yes” to sshd_config.

Key: 3d21e8cc9e1c09dc60429de7716165787e99515f
```

この内容に従わなかった場合どうなるか

これは阻害要因でアップグレードを進めることはできませんが、リスク要因が高であり、この項目に対処しなかった場合、セキュアシェル (SSH) を使用してサーバーにリモートログインできなくなる可能性があることを覚えておいてください。

影響を受けるサブシステム

SSH サーバー (sshd.service)

具体的な内容

このスニペットは、Red Hat Enterprise Linux 7 と Red Hat Enterprise Linux 8 の間で SSH サーバーの動作方法に影響の高い変更があることを示しています。Red Hat Enterprise Linux 8 ではデフォルトで root ユーザーにパスワード認証が許可されていません。Red Hat Enterprise Linux 7 では PermitRootLogin の暗黙のデフォルト値は yes ですが、Red Hat Enterprise Linux 8 では暗黙のデフォルト値は prohibit-password です。

暗黙の設定のディレクティブは /etc/ssh/sshd_config 内にコメントで表示されますが、これはコメントではありません。ディレクティブのデフォルト値を通知する目的で表示されます。

必要な対応

他のユーザーでログインできることを確認してください。パスワードの有無は問いません。

etc/ssh/sshd_config 内の PermitRootLogin の値を明示的に設定する必要があります。root ユーザーの SSH によるログインを許可する場合は値を yes にして、許可しない場合は no にします。重要なのは、このディレクティブが明示的に設定されているという点です。

Linux の man ページには詳細な情報が豊富に存在します。**man sshd_config** コマンドを使用して *PermitRootLogin* の文字列を検索すると、この設定ディレクティブの詳細を確認できます。

例 3：leapp answerfile の使用が必要な高リスクの阻害要因

この特定の問題は、主に Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのアップグレードに当てはまります。この例の特徴は、Leapp ユーティリティにデータを自動で渡すことができるファイルである、leapp answerfile を使用した対策が必要である点です。

```
Risk Factor: high (inhibitor)

Title: Missing required answers in the answer file

Summary: One or more sections in answerfile are missing user choices:
remove_pam_pkcs11_module_check.confirm

For more information consult https://leapp.readthedocs.io/en/latest/
dialogs.html

Remediation: [hint] Please register user choices with leapp answer cli
command or by manually editing the answerfile.

[command] leapp answer --section remove_pam_pkcs11_module_check.
confirm=True

Key: d35f6c6b1b1fa6924ef442e3670d90fa92f0d54b
```

この内容に従わなかった場合どうなるか

これは阻害要因であり、pam_pkcs11 モジュールの削除を許可するまでアップグレードは進みません。リスク要因は高です。これは、PAM 設定に pam_pkcs11 モジュールに関連する*必要*な制御値が含まれている可能性があり、Red Hat Enterprise Linux 8 でこのモジュールを削除するとシステムからロックアウトされる可能性があるためです。

このアップグレード項目は Leapp の回答ファイルを使用すること**でしか**解決できない可能性があります。

影響を受けるサブシステム

認証 (pam)

具体的な内容

このスニペットは、pam_pkcs11 モジュールが Red Hat Enterprise Linux 8 から削除され、その機能が sssd によって提供されるようになったことを示しています。

必要な対応

var/log/leapp/answerfile を次のとおり編集します。

```
[remove_pam_pkcs11_module_check]

confirm = True
```

または、次のコマンドを実行してanswerfile /var/log/leapp/answerfile を編集します。

```
leapp answer --section
remove_pam_pkcs11_module_check.confirm=true
```

また、pam_pkcs11 モジュールに依存しない他の認証方法があることを確認する必要があります。

これは **grep pam_pkcs11 /etc/pam.d/*** を実行して確認できます。

「Managing software from an application stream」ハンズオンラボをご覧ください。

例 4：アップグレード後の Python プログラムに影響を与える、高リスクの阻害要因でない検討事項

この問題は、主に Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 にアップグレードするマシンに当てはまります。先の例とは異なり、これは阻害要因ではないため、この検出された問題が解決されなかった場合でも、Leapp アップグレードツールはアップグレードを実行します。この問題の解決が必要か否かは、システム管理者が判断します。また、このマシンが Python2 ベースのアプリケーションを使用しているか、それらのアプリケーションがアップグレードされたオペレーティングシステムが提供する Python3 と互換性があるかという点についても、システム管理者が判断します。

```
Risk Factor: high

Title: Difference in Python versions and support in Red Hat Enterprise
Linux 8

Summary: In Red Hat Enterprise Linux 8, there is no ‘python’
command. Python 3 (backward incompatible) is the primary Python
version and Python 2 is available with limited support and
limited set of packages. Read more here: https://access.redhat.
com/documentation/en-us/red_hat_enterprise_linux/8/html-single/
configuring_basic_system_settings/#using-python3

Remediation: [hint] Please run “alternatives --set python /usr/bin/
python3” after upgrade

Key: 0c98585b1d8d252eb540bf61560094f3495351f5
```

この内容に従わなかった場合どうなるか

これは阻害要因ではなく、対策に従わなかった場合でも leapp upgrade コマンドは続行されます。リスク要因は高です。これは、バージョン指定されていない python コマンド (/usr/bin/python) は Red Hat Enterprise Linux 8 ではデフォルトで使用できないためです。Python インタープリターを直接 (ターミナルからなど) または間接的に実行する (別のプロセスでコマンドが実行される) と失敗します。

影響を受けるサブシステム

バージョン指定されていない /usr/bin/python コマンドに依存する Python とアプリケーション

具体的な内容

Python 2 は非推奨で Python 3 が望ましいですが、アプリケーション・ストリームを使用してインストールすることは可能です。アプリケーション・ストリーム・リポジトリには、サーバーに同時にインストールできる Python モジュールが複数存在します。Python のインストール、呼び出し、操作のいずれの場合においても、常に Python のバージョンを指定してください。バージョン指定されていない Python コマンドはデフォルトでは使用できませんが、必要に応じて設定することは可能です。

必要な対応

次のコマンドを実行すると、/usr/bin/python3 を Python のデフォルトバージョンとして使用できます。

```
alternatives --set python /usr/bin/python3
```

Python2 を明示的に必要とするアプリケーションは、/usr/bin/python2 を参照する必要があります。または、次のコマンドを使用して Python のデフォルトバージョンを Python2 に設定します。

```
alternatives --set python /usr/bin/python2
```

例 5：中リスクの阻害要因でない検討事項

この例は、主に Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へのアップグレードに当てはまります。

```
Risk Factor: medium

Title: chrony using default configuration

Summary: default chrony configuration in Red Hat Enterprise Linux8
uses leapsectz directive, which cannot be used with leap smearing
NTP servers, and uses a single pool directive instead of four server
directives

Key: c4222ebd18730a76f6bc7b3b66df898b106e6554
```

この内容に従わなかった場合どうなるか

これは阻害要因ではなく、leapp upgrade は続行されます。リスク要因は中です。これはネットワーク・タイム・プロトコル (NTP) クライアントが、同じうるう秒の調整機能を実装していない、またはすべてがうるう秒の調整機能を実装していない複数のサーバーから時刻を取得するよう設定されている場合、うるう秒の調整時にそれぞれのサーバーから異なる時刻を取得するためです。この結果、NTP クライアントが時刻の更新を停止したり、各サーバーの時刻にランダムに変わったりする可能性があります。

影響を受けるサブシステム

chrony を使用する時刻同期

具体的な内容

chrony は NTP を使用する時刻同期を実装しています。Red Hat Enterprise Linux 8 は、デフォルトで pool ディレクティブを使用し、同じ機能の NTP サーバーのプールを参照します。異なる機能の NTP サーバーを参照する複数の server ディレクティブを使用した場合、時刻同期の機能が低下する可能性があります。

「Red Hat Enterprise Linux にアップグレードする主な理由チェックリスト」をご覧ください。

必要な対応

etc/chrony.conf から *leapsectz* ディレクティブと *leapfile* ディレクティブをすべて削除し、/etc/chrony.conf 内で server ディレクティブの代わりに pool ディレクティブを使用します。これにより、同じ機能の NTP サーバーが使用されるようになります。

明示的に定義されたサーバーとシステム時刻を同期させるには、すべてのサーバーで同じ機能を使用するようにしてください。

「BOOM の概要とインストール方法」をご覧ください。

詳細については、「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」をご覧ください。

アップグレードの準備が完了したら

アップグレード前のレポートで特定された問題に対処したら、**leapp preupgrade** コマンドをもう一度実行してレポートファイルを再確認し、アップグレードの成功を妨げるような対応の漏れがないことを確認することをお勧めします。

システムのアップグレード準備が整ったら、**leapp upgrade** または **leapp upgrade --reboot** のどちらかのコマンドを実行します。

leapp upgrade コマンドの場合、アップグレード処理はキューに入り、完了するには再起動が数回必要になります。そのため、計画しておくことが重要です。初回の起動までは、現在使用中のバージョンの Red Hat Enterprise Linux を引き続き使用できます。

leapp upgrade reboot コマンドの場合、サーバーは自動で再起動します。

初回の起動では、ブートローダーはメニューエントリー **Red Hat Enterprise Linux-Upgrade-Initramfs** を使用して、特別なアップグレード環境を自動で初期化します。サーバーはこのアップグレード環境下でアップグレードされます。アップグレードを元に戻して前のメジャーバージョンの Red Hat Enterprise Linux を引き続き使用する場合は、バックアップが必要になります。

2 回目の起動では、SELinux ラベルが復元され、サーバーが再び再起動します。

3 回目の起動では、アップグレードを検証して、新しい Red Hat Enterprise Linux を使用できるようになります。

現在使用中の Red Hat Enterprise Linux のバージョンを検証するには、次のコマンドを使用します。

```
[root@leapp7to8 ~]# rpm -q redhat-release
redhat-release-8.6-0.1.el8.x86_64
```

```
[root@leapp8to9 ~]# rpm -q redhat-release
redhat-release-9.0-2.17.el9.x86_64
```

Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 にアップグレードする場合、*rhel-8-server-rpms* というリポジトリになると思われるかもしれませんが、Red Hat Enterprise Linux 8 では 2 つのリポジトリが提供されています。1 つ目は *rhel-8-for-x86_64-baseos-rpms* で、基盤となる OS 機能のコアセットを提供します。2 つ目は *rhel-8-for-x86_64-appstream-rpms* で、さまざまなワークロードやユースケースをサポートする追加のユーザー・スペース・アプリケーション、ランタイム言語、データベースが含まれます。これを検証するには、次のコマンドを使用します。

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-8-for-x86_64-appstream-rpms
```

```
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/x86_64/
appstream/os
Enabled:   1


Repo ID:   rhel-8-for-x86_64-baseos-rpms
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/x86_64/baseos/os
Enabled:   1
```

システムのアップグレードと再起動が完了すると、**/var/log/leapp/leapp-report.txt** にアップグレード後のレポートが表示されるので、再度確認してください。完了すべき追加のアクション項目が記載されている場合があります。

ヒント

開始する前に、以下の推奨事項について検討してください。

sosreport

弊社からのサポートが必要な場合に提供できるよう sosreport の生成を検討してください。

1. **yum install sos** を使用して、sos パッケージがインストールされていることを確認します。
2. **sosreport** コマンドを使用してレポートを生成します。
3. Red Hat サポートが必要な場合は、生成された tar アーカイブを **/var/tmp/** から安全な場所にコピーします。

バックアップを必ず取る

予期しない事態によりシステムが操作できなくなったり、データにアクセスできなくなったりした場合、タイムリーに復旧して運用を再開できることが最も重要になります。データのバックアップがあると復旧プロセスが容易になるため、すでに実践されていると思いますが、重要なのは、Leapp を使用してサーバーをアップグレードする前にデータをバックアップしておく必要があるという点です。

現在使用しているツールを使って、バックアップ戦略を実践しましょう。

- サーバーが動作するために必要なデータを特定します。
- アップグレード対象のサーバー以外の安全な場所にデータをバックアップします。
- バックアップをテストして、データが正常にバックアップされたことを確認します。
- バックアップからデータが復元できることを確認します。
- 障害復旧計画を検証して、サーバーの損失の可能性に十分に備えていることを確認します。

Red Hat Insights を使用する

Red Hat Insights を使用すると、アップグレードの適合性を特定できます。

Red Hat Satellite Server を活用する

Red Hat Satellite Server では Leapp プラグインを活用して、対象のシステムを大規模にスキャンし、アップグレードできます。

Web コンソールを使用する

Web コンソールを使用すると、アップグレード前のレポートが読みやすい形式で表示されるため、Web コンソールの使用を検討してアップグレードプロセスをスムーズに進めましょう。

yum install cockpit cockpit-leapp を使用して、cockpit パッケージと cockpit-leapp パッケージがインストールされていることを確認する必要があります。

次に **systemctl enable --now cockpit.socket** を使用して、cockpit ソケットを有効にします。

firewall-cmd --add-port 9090/tcp を使用して Web コンソールのポートをファイアウォールに追加し、**firewall-cmd --add-port 9090/tcp --permanent** を使用して、ルールが永続的なファイアウォールの設定に追加されていることを確認します。

Web コンソール *https://サーバー名:9090* にログインします。

Satellite リポジトリの要件

Satellite Server を使用してパッケージを管理している場合は、次のリポジトリが使用可能であることを確認してください。

- rhel-7-server-rpms
- rhel-7-server-extras-rpms
- rhel-8-for-x86_64-baseos-rpms
- rhel-8-for-x86_64-appstream-rpms

yum versionlock

yum versionlock コマンドを使用してパッケージを特定のバージョンにロックしている場合は、**yum versionlock clear** でクリアします。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
#F31715_0822