Ce qu'il faut savoir sur Leapp

Leapp est un outil de mise à niveau sur place des systèmes qui permet de passer d'une version majeure de Red Hat® Enterprise Linux® à une autre. Avec Leapp, vous pouvez réaliser vos mises à niveau en toute confiance et bénéficier des nouvelles fonctions de Red Hat Enterprise Linux sans réinstaller vos systèmes.

Lire la liste d'avantages « 8 raisons de passer à Red Hat Enterprise Linux »

L'importance des mises à niveau

Les mises à niveau permettent aux entreprises de poursuivre leurs activités en continuant à offrir à leurs clients des produits pris en charge qui incluent les derniers correctifs et améliorations, ainsi que les fonctions ajoutées aux nouvelles versions majeures de Red Hat Enterprise Linux.

La solution Red Hat Enterprise Linux offre de meilleures performances qui réduisent votre coût total de possession, renforcent votre productivité et optimisent vos investissements technologiques.

Red Hat Enterprise Linux suit un cycle de version majeure régulier de trois ans. Toute souscription à la solution est valable pour toutes ses versions actuellement prises en charge. Vous bénéficiez ainsi des technologies émergentes les plus récentes à chaque nouvelle version. Chaque version majeure de Red Hat Enterprise Linux est prise en charge pendant une période de 10 ans divisée en deux phases.

La première phase est la prise en charge complète qui dure cinq ans à compter de la date de disponibilité générale. Elle inclut l'ajout de nouvelles fonctions, la prise en charge de nouveaux équipements matériels et la correction des problèmes et bogues. Pendant les cinq ans qui suivent, la version rentre en phase de prise en charge de la maintenance. À ce stade, la publication des erratas de sécurité de niveau Critique ou Important ainsi que certaines fonctions et améliorations de correctifs se poursuit. Au terme du cycle de vie habituel de 10 ans, les clients peuvent acheter le module complémentaire Red Hat Extended Life Cycle Support Add-On, qui rallonge la prise en charge de deux ans, durant lesquels ils continuent de recevoir des erratas de sécurité de niveau Critique ou Important. Consultez la page sur le cycle de vie de Red Hat Enterprise Linux pour en savoir plus.

En optant pour une mise à niveau vers Red Hat Enterprise Linux, les clients bénéficient de nouvelles fonctions, notamment :

- Un logiciel à jour disponible via le flux d'applications, qui donne accès à des environnements d'exécution de langages, bases de données et autres applications plus récents durant la phase de prise en charge complète d'une version majeure de Red Hat Enterprise Linux
- Des outils de conteneurisation Red Hat Enterprise Linux tels que Podman, Buildah et Skopeo, qui prennent en charge la conception, le déploiement et la gestion des conteneurs
- L'application de correctifs en direct sur le noyau (kpatch), qui permet de corriger les CVE (Common Vulnerabilities and Exposures) critiques sur le noyau sans le redémarrer

- Des outils de surveillance des performances, qui se basent sur des outils eBPF pour offrir des informations sur différents aspects des performances système
- La prise en charge de Flatpak pour l'exécution d'applications généralement utilisées pour les applications de bureau
- Le groupe de contrôle cgroup2, qui offre des fonctionnalités rationalisées pour réguler l'utilisation des ressources par les processus

La mise à niveau inclut plusieurs améliorations pour l'automatisation et la gestion, notamment une interface de console web plus claire qui simplifie l'administration.

Voici les améliorations apportées au niveau de l'automatisation :

- Ajout de rôles système dans Red Hat Enterprise Linux, alimentés par Red Hat Ansible® Automation Platform, qui permettent d'automatiser la gestion à grande échelle
- Red Hat Insights, service inclus dans les souscriptions Red Hat Enterprise Linux qui effectue des analyses proactives des vulnérabilités, des omissions de rôle et d'autres critères prédéfinis

Si vous cherchez à exploiter au mieux votre matériel, notez que la version 9 de Red Hat Enterprise Linux est plus performante que les versions 7 et 8, notamment en raison des quelques changements suivants :

- Nouveaux algorithmes « elevator » pour le noyau
- Nouveaux profils d'optimisation des performances

Consultez la page sur la mise à niveau de la version 6 à la version 8 de Red Hat Enterprise Linux pour en savoir plus sur le produit.

Leapp : définition et usage

La mise à niveau des serveurs se révèle parfois difficile. C'est pourquoi la solution Red Hat Enterprise Linux inclut Leap, un outil de gestion des mises à niveau qui offre un processus unique et automatisé pour passer à la prochaine version majeure de Red Hat Enterprise Linux. Leapp permet aux clients de conserver leur souscription d'origine (qui est rattachée au système), les configurations du système, ainsi que les référentiels personnalisés et les applications tierces.

L'outil Leapp est fourni avec les versions 7 et 8 de Red Hat Enterprise Linux, ce qui vous permet de passer de la version 7.9 à la version 8, et de la version 8 à la version 9.

Si vous disposez de la version 6 de Red Hat Enterprise Linux, vous devez effectuer une mise à niveau vers la version 7 avec un autre outil avant de pouvoir utiliser Leapp pour passer aux versions 8 ou 9.

Le tableau ci-dessous présente les avantages de Leapp pour la mise à niveau de votre serveur.

Mise à niveau sur place avec Leapp	Réinstallation
Configuration conservée	Sauvegarde et redémarrage nécessaires des données de configuration
Données de souscription existantes conservées par les machines	Enregistrement des machines requis à l'aide de subscription-manager
Productivité améliorée grâce à l'automatisation	Coûts et délais supplémentaires

Fonctionnement de Leapp

En comprenant le fonctionnement de l'outil Leapp, vous aurez plus de chances de réussir votre mise à niveau. Le processus se décompose en deux phases : une analyse de la capacité de mise à niveau suivie de la mise à niveau à proprement parler. Notez que vous devrez effectuer des redémarrages après la mise à niveau. Tenez-en compte dans votre planning.

Si vous n'utilisez Leapp qu'avec un seul hôte, l'analyse de la capacité de mise à niveau se base sur des caractéristiques de mise à niveau, que vous pouvez télécharger sous forme de métadonnées sur la page *cloud.redhat.com*.

Pour les hôtes connectés à Red Hat Satellite, les métadonnées doivent être distribuées par Satellite aux serveurs qui utilisent Leapp. L'analyse de la capacité de mise à jour peut alors s'effectuer à grande échelle à l'aide du plug-in Leapp pour Red Hat Satellite.

Cette analyse génère un rapport qui indique les éventuels éléments à corriger avant de procéder à la mise à niveau.

Leapp utilise un workflow composé de plusieurs programmes Python, des « acteurs » capables d'apporter des modifications à votre système.

Lisez la présentation détaillée « Utiliser Red Hat Satellite pour les mises à niveau avec Leapp »

Par exemple, **CheckOSRelease** est un acteur qui vérifie que votre version mineure de Red Hat Enterprise Linux est prise en charge. Si ce n'est pas le cas, il empêchera le processus de mise à niveau.

Si les acteurs proposés ne couvrent pas toutes vos exigences, vous pouvez créer un acteur personnalisé pour corriger, bloquer ou signaler un problème. Vous pouvez ensuite l'intégrer au workflow Leapp.

Leapp est inclus avec Red Hat Insights pour analyser votre matériel enregistré et déterminer les machines prêtes pour la mise à niveau.

Pour effectuer la mise à niveau avec Leapp, vous pouvez passer par l'interface en lignes de commande ou utiliser Red Hat Satellite.

Limites

Avant de procéder à la mise à niveau de votre serveur, vous devez tenir compte des limitations de l'outil Leapp :

- Il ne sert qu'aux mises à niveau entre versions majeures de Red Hat Enterprise Linux directement consécutives.
- Leapp ne fonctionne pas si votre système utilise le chiffrement de disque pour protéger le système de fichiers root.
- Les appareils VDO doivent être convertis pour être pris en charge par le gestionnaire de volumes logiques (LVM).
- Les montages de stockage réseau ou multivoies en réseau, comme les protocoles iSCSI ou NFS, ne peuvent pas être utilisés pour une partition de système.
- Leapp ne peut pas mettre à niveau les instances à la demande dans le cloud public qui utilisent Red Hat Update Infrastructure (qui diffère de Red Hat Subscription Manager).

Entamer la mise à niveau

Prenons l'exemple d'une mise à niveau de la version 7 vers la version 8 de Red Hat Enterprise Linux. Notez que le workflow est similaire pour le passage de la version 8 à la version 9. Si ce n'est pas encore fait, commencez par mettre à jour votre système vers Red Hat Enterprise Linux 7.9 en utilisant la commande **yum update** :

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

Vous devez installer le paquet **leapp**. Assurez-vous que votre machine est enregistrée sur le réseau de diffusion de contenu Red Hat ou sur votre serveur Satellite et que le canal Red Hat Enterprise Linux 7 Extras est activé. Pour ce faire, utilisez la commande suivante :

```
[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
```

Si le référentiel rhel-7-server-extras-rpms n'est pas activé, activez-le avec la commande :

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

Vous pouvez désormais installer Leapp sur Red Hat Enterprise Linux 7 à l'aide de la commande suivante :

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

Si vous passez de la version 8 à la version 9 de Red Hat Enterprise Linux, suivez les étapes suivantes pour installer l'utilitaire de mise à niveau sur place Leapp. Vous devrez peut-être mettre à jour les serveurs Red Hat Enterprise Linux 8 avant leur mise à niveau vers la version 9. Pour en savoir plus, consultez la page sur les processus de mise à niveau sur place pris en charge pour Red Hat Enterprise Linux.

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

Installez les paquets **leapp** et **leapp-upgrade-el8toel9** (tous deux disponibles dans le référentiel **rhel-8-for-x86_64-appstream-rpms**) avec la commande suivante :

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

Si vous avez déjà effectué une mise à niveau sur place de la version 7 à la version 8 de Red Hat Enterprise Linux, supprimez le répertoire **/root/tmp_leapp_py3** s'il est présent sur votre système :

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

Après avoir installé le ou les paquets de mise à niveau sur place pour votre version de Red Hat Enterprise Linux, vous devez analyser votre serveur en utilisant la commande **leapp preupgrade** afin d'identifier tout problème potentiel avant la mise à niveau. Cette étape n'apporte aucune modification au système, mais elle crée d'importants fichiers qui prépareront votre mise à niveau.

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

Après avoir exécuté la commande preupgrade, vous obtiendrez probablement un résultat similaire à ceci :

```
…
 output omitted
…

============================================================
                    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
```

Fichiers d'intérêt :

/var/log/leapp/leapp-report.txt	Informations lisibles et compréhensibles sur le rapport de mise à niveau Leapp
/var/log/leapp/leapp-report.json	Équivalent JSON mis en forme
/var/log/leapp/leapp-preupgrade.log	Résultat de débogage de la commande leapp preupgrade
/var/log/leapp/answerfile	Réponses aux questions posées par la commande leapp preupgrade

Le rapport d'analyse de la capacité de mise à niveau se trouve à l'emplacement **/var/log/leapp/leapp-report.txt**. Il peut contenir des informations importantes et indiquer des mesures à prendre avant la mise à niveau, ainsi que les instructions à suivre, le cas échéant.

Mesures préalables à la mise à niveau avec Leapp

Le rapport de vérification avant mise à niveau disponible à l'emplacement /var/log/leapp/leapp-report.txt contient les éventuelles mesures que vous devez prendre. Un ***inhibitor*** désigne un élément bloquant qui empêche la mise à niveau Leapp. Vous devez résoudre le problème pour continuer.

Le ***risk factor*** (facteur de risque) décrit les effets du problème à l'aide des adjectifs suivants :

High	Risque très élevé de détérioration de l'état
Medium	Conséquences possibles sur le système et les applications
Low	Faible risque de conséquence sur le système, conséquences possibles sur les applications
Info	À titre d'information, aucune conséquence attendue sur le système ou les applications

Le ***title*** (titre) désigne un élément du rapport de vérification avant mise à niveau avec Leapp, et le résumé fournit des informations complémentaires.

Le ***summary*** (résumé) fournit une brève description du problème que vous devrez potentiellement traiter.

La ***remediation*** (correction) désigne la solution permettant de résoudre le problème signalé. Voici les types de corrections courants :

- Modifier un fichier de configuration
- Exécuter une commande qui modifie le comportement du système
- Appliquer une correction par le biais du fichier Leapp answerfile
- Appliquer une mesure corrective qui affecte la modularité logicielle à partir d'une bibliothèque Red Hat Enterprise Linux 7 Software Collections comme Python, PHP, Node.js, PostgreSQL, etc.
- Démonter temporairement des exports NFS

Dans cette section, vous trouverez des exemples de problèmes à facteur de risque élevé et moyen qui incluent :

- le message figurant dans le rapport Leapp (dans l'encadré d'exemple) ;
- le sous-système logiciel affecté ;
- une explication de l'élément signalé ;
- la mesure à prendre ;
- les conséquences si vous ne traitez pas les problèmes signalés.

Les problèmes signalés par votre système dépendent de la version de Red Hat Enterprise Linux à laquelle vous souhaitez passer et de votre configuration.

Exemple 1 : élément bloquant à facteur de risque élevé qui requiert une modification temporaire de votre système

Dans l'exemple ci-dessous, le rapport signale un élément bloquant à facteur de risque élevé. Si ce problème n'est pas traité et que vous exécutez la commande leapp upgrade, vous obtiendrez une erreur et ne pourrez pas procéder à la mise à niveau. Après le message, vous trouverez une explication sur la manière de résoudre ce problème sur votre système.

```
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
```

Que se passe-t-il si j'ignore ce message ?

Ce message signale un élément bloquant qui vous empêchera de poursuivre si vous n'effectuez pas l'action requise. Le facteur de risque est élevé, car les modifications ne doivent concerner que le serveur local, pas les partages NFS.

Quel est le sous-système concerné ?

Les montages NFS.

Qu'est-ce que cela implique ?

Les montages NFS ne sont pas utilisables pendant le processus de mise à niveau. Vous devez les démonter et les désactiver jusqu'à la fin de la mise à niveau.

Que dois-je faire ?

Modifiez le fichier /etc/fstab pour désactiver temporairement les partages NFS en les changeant en commentaire et démonter les partages NFS actuellement montés. Arrêtez et désactivez temporairement autofs.service. Les entrées NFS et autofs.service peuvent être réactivées une fois la mise à niveau terminée.

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

Exemple 2 : élément bloquant à facteur de risque élevé qui requiert la modification d'un fichier de configuration existant

Ce scénario s'applique souvent aux mises à jour de la version 7 à la version 8 de Red Hat Enterprise Linux.

```
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
```

Que se passe-t-il si j'ignore ce message ?

Il s'agit d'un élément bloquant à risque élevé qui empêchera la mise à niveau et qui, s'il n'est pas correctement traité, vous empêchera de vous connecter à votre serveur à distance à l'aide de Secure Shell (SSH).

Quel est le sous-système concerné ?

Le serveur SSH (sshd.service).

Qu'est-ce que cela implique ?

Ce message signale une différence de fonctionnement conséquente du serveur SSH entre la version 7 et la version 8 de Red Hat Enterprise Linux. Par défaut, l'authentification par mot de passe n'est pas autorisée pour l'utilisateur root dans Red Hat Enterprise Linux 8. La valeur implicite par défaut pour PermitRootLogin est « yes » dans la version 7, et « prohibit-password » dans la version 8.

Vous remarquerez l'apparition d'une directive de configuration implicite sous la forme d'un commentaire dans le fichier /etc/ssh/sshd_config, mais ce n'en est pas un. Elle s'affiche pour vous informer des valeurs par défaut de la directive.

Que dois-je faire ?

Assurez-vous de pouvoir vous connecter avec un autre identifiant, avec ou sans mot de passe.

Vous devez définir une valeur de façon explicite pour la directive PermitRootLogin dans le fichier /etc/ssh/sshd_config. Vous pouvez, par exemple, indiquer l'argument « yes » pour autoriser l'utilisateur root à se connecter via le SSH. Ce qui importe ici, c'est que la directive soit explicitement définie.

Vous trouverez de nombreuses autres informations sur les pages man de Linux. Utilisez la commande **man sshd_config** et recherchez la chaîne *PermitRootLogin* pour en savoir plus sur cette directive de configuration.

Exemple 3 : élément bloquant à facteur de risque élevé qui requiert l'utilisation du fichier Leapp answerfile

Ce problème apparaît surtout lors de la mise à niveau de la version 7 à la version 8 de Red Hat Enterprise Linux. La particularité de cet exemple tient au fait que pour corriger le problème vous devez utiliser le fichier Leapp answerfile, dont les données automatiquement transmissibles à l'utilitaire Leapp.

```
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
```

Que se passe-t-il si j'ignore ce message ?

Il s'agit d'un élément bloquant qui empêchera la mise à niveau tant que vous n'aurez pas autorisé la suppression du module pam_pkcs11. Le facteur de risque est élevé, car il est possible que les valeurs de contrôle *requisite ou required* soient associées au module pam_pkcs11 de votre configuration PAM et que la suppression de ce module dans la version 8 de Red Hat Enterprise Linux vous empêche d'accéder à votre système.

Ce problème de mise à niveau peut être résolu **uniquement** via le fichier Leapp answerfile.

Quel est le sous-système concerné ?

Authentification (gestion des accès privilégiés)

Qu'est-ce que cela implique ?

Ce message indique que le module pam_pkcs11 a été supprimé de Red Hat Enterprise Linux 8 et que la fonctionnalité est désormais fournie par sssd.

Que dois-je faire ?

Modifiez le fichier /var/log/leapp/answerfile comme suit :

```
[remove_pam_pkcs11_module_check]

confirm = True
```

Autrement, exécutez la commande suivante pour modifier le fichier /var/log/leapp/answerfile :

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

Vous devez également vérifier que vous disposez d'autres méthodes d'authentification qui ne reposent pas sur le module pam_pkcs11.

Pour ce faire, exécutez la commande **grep pam_pkcs11 /etc/pam.d/***.

Consultez la page Gérer les logiciels à l'aide de flux d'applications pour accéder aux travaux pratiques.

Exemple 4 : problème non bloquant à risque élevé, qui affecte les programmes Python après la mise à niveau

Cet exemple s'applique surtout aux machines qui passent de la version 7 à la version 8 de Red Hat Enterprise Linux. Contrairement aux exemples précédents, il ne s'agit pas d'un élément bloquant, ce qui signifie que l'outil Leapp effectuera la mise à niveau même si le problème détecté n'est pas corrigé. Il incombe à l'administrateur système de déterminer si ce problème doit être corrigé ou non. C'est également lui qui saura dire si la machine utilise des applications basées sur Python2 et si elles sont compatibles avec Python3 inclus dans le système d'exploitation mis à niveau.

```
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
```

Que se passe-t-il si j'ignore ce message ?

Il ne s'agit pas d'un élément bloquant. La commande de mise à niveau Leapp pourra être exécutée même si vous ne corrigez pas le problème. Le facteur de risque est élevé, car la commande python sans version (/usr/bin/python) n'est pas disponible par défaut dans Red Hat Enterprise Linux 8. L'exécution de l'interpréteur Python échouera, qu'elle soit directe (à partir d'un terminal par exemple) ou indirecte (la commande est exécutée par un autre processus pour votre compte).

Quel est le sous-système concerné ?

Python, et les applications qui dépendent de la commande /usr/bin/python sans version.

Qu'est-ce que cela implique ?

Bien que le langage Python 2 ait été remplacé par Python 3, vous pouvez toujours l'installer par le biais des flux d'applications. Le référentiel des flux d'applications donne accès à plusieurs modules Python que vous pouvez installer en parallèle sur votre serveur. Indiquez toujours la version de Python que vous installez, appelez, ou avec laquelle vous interagissez. La commande Python sans version n'est pas disponible par défaut, mais vous pouvez la configurer si besoin.

Que dois-je faire ?

Exécutez la commande suivante pour vous assurer que /usr/bin/python3 est utilisée comme version de Python par défaut :

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

Toute application qui requiert Python2 doit indiquer /usr/bin/python2. Vous pouvez également indiquer Python2 comme version par défaut en utilisant la commande suivante :

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

Exemple 5 : problème non bloquant à facteur de risque moyen

Cet exemple s'applique surtout aux mises à jour de la version 7 à la version 8 de Red Hat Enterprise Linux.

```
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
```

Que se passe-t-il si j'ignore ce message ?

Il ne s'agit pas d'un élément bloquant. Il n'empêchera pas l'exécution de la commande de mise à niveau Leapp. Le facteur de risque est moyen, car les clients NTP qui obtiennent l'heure à partir de plusieurs serveurs qui n'appliquent pas le même étalement des secondes intercalaires ou qui n'en appliquent pas tous obtiendront des heures différentes de la part de serveurs différents. En conséquence, les clients NTP peuvent cesser de mettre à jour leurs horloges ou passer aléatoirement d'un serveur à un autre.

Quel est le sous-système concerné ?

La synchronisation du système avec chrony.

Qu'est-ce que cela implique ?

L'utilitaire chrony s'appuie sur le protocole NTP pour synchroniser l'heure. Dans Red Hat Enterprise Linux 8, la directive « pool » est utilisée par défaut pour référencer un pool de serveurs NTP doté des mêmes fonctionnalités. L'utilisation de plusieurs directives « server » qui font référence à des serveurs NTP dotés de capacités différentes peut entraîner une dégradation de la synchronisation temporelle.

Que dois-je faire ?

Dans le fichier /etc/chrony.conf, supprimez toutes les directives *leapsectz* et *leapfile*, et remplacez la directive « server » par la directive « pool » dans /etc/chrony.conf. Ces modifications garantissent que tous les serveurs NTP utilisés sont dotés des mêmes capacités.

Si vous souhaitez synchroniser l'heure de votre système avec des serveurs explicitement définis, assurez-vous que tous les serveurs sont dotés des mêmes capacités.

Lire la liste d'avantages « 8 raisons de passer à Red Hat Enterprise Linux »

Mon système est prêt pour la mise à niveau

Après avoir corrigé les problèmes figurant dans le rapport de vérification avant mise à niveau, nous vous conseillons d'exécuter de nouveau la commande **leapp preupgrade** et de consulter le rapport pour vous assurer qu'il ne contient aucun problème susceptible d'empêcher la mise à niveau.

Une fois que votre système est prêt pour la mise à niveau, exécutez l'une des commandes suivantes : **leapp upgrade** ou **leapp upgrade --reboot**.

Consulter la page sur BOOM et son utilisation

La commande **leapp upgrade** place le processus dans la file d'attente, et le système passe par plusieurs redémarrages. Tenez-en compte dans votre planning. Avant le premier redémarrage, vous pouvez continuer à utiliser votre version actuelle de Red Hat Enterprise Linux.

En savoir plus sur la gestion des mises à niveau du système à l'aide d'instantanés

La commande **leapp upgrade reboot** permet le redémarrage automatique du serveur.

Premier redémarrage : le chargeur de démarrage initialise automatiquement un environnement de mise à niveau spécial via l'entrée de menu **Red Hat Enterprise Linux-Upgrade-Initramfs**. Votre serveur sera mis à niveau dans cet environnement. Effectuez une sauvegarde au cas où vous souhaiteriez annuler la mise à niveau et continuer d'utiliser la version majeure de Red Hat Enterprise Linux précédente.

Deuxième redémarrage : les étiquettes SELinux sont restaurées et votre serveur redémarre une nouvelle fois.

Troisième redémarrage : confirmez la mise à niveau et profitez de votre nouvelle version de Red Hat Enterprise Linux.

Vérifiez la version de Red Hat Enterprise Linux actuellement utilisée :

```
[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
```

Lorsque vous effectuez une mise à niveau de la version 7 vers la version 8 de Red Hat Enterprise Linux, à la place d'un unique référentiel *rhel-8-server-rpms*, vous constaterez la présence de deux référentiels : *rhel-8-for-x86_64-baseos-rpms*, qui fournit l'ensemble des fonctionnalités de base du système d'exploitation sous-jacent, et *rhel-8-for-x86_64-appstream-rpms*, qui comprend les applications supplémentaires de l'espace utilisateur, les langages d'exécution ainsi que les bases de données nécessaires aux différents cas d'utilisation et charges de travail. Vous pouvez les afficher avec la commande suivante :

```
[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
```

Une fois votre système mis à niveau et redémarré, consultez de nouveau le fichier **/var/log/leapp/leapp-report.txt** qui contient désormais le rapport post-mise à niveau. Celui peut éventuellement indiquer d'autres mesures à prendre.

Conseils

Voici quelques recommandations, avant de vous lancer.

Générez un rapport sosreport

Pensez à générer un rapport sosreport pour que nous puissions vous aider en cas de besoin.

1. Utilisez la commande **yum install sos** pour vous assurer que votre paquet sos est installé.
2. Générez le rapport à l'aide de la commande **sosreport**.
3. Copiez l'archive tar générée sous **/var/tmp/** dans un emplacement sûr. Elle vous sera utile si vous devez faire appel au service d'assistance Red Hat.

Réalisez une sauvegarde

Il est essentiel de pouvoir récupérer rapidement vos données et reprendre vos activités en cas d'imprévu entraînant une panne de votre système ou bloquant l'accès à vos données. La sauvegarde des données facilite le processus de récupération, et vous savez probablement déjà comment en réaliser. Nous souhaitons quand même insister sur l'importance de sauvegarder vos données avant d'utiliser Leapp pour effectuer la mise à niveau de vos serveurs.

Utilisez les outils dont vous disposez déjà pour mettre en place une stratégie de sauvegarde.

- Identifiez les données nécessaires au fonctionnement de votre serveur.
- Sauvegardez vos données dans un emplacement hors du serveur que vous souhaitez mettre à niveau.
- Testez votre sauvegarde pour vous assurer que vos données ont bien été sauvegardées.
- Assurez-vous que vous pouvez restaurer vos données à partir de votre sauvegarde.
- Vérifiez votre plan de récupération après sinistre pour vous assurer d'être suffisamment préparé à une perte éventuelle de votre serveur.

Utilisez Red Hat Insights

Le service Red Hat Insights vous permet de déterminer si vous êtes éligible à une mise à niveau.

Tirez parti du serveur Red Hat Satellite

Le serveur Red Hat Satellite se sert du plug-in Leapp pour analyser et mettre à jour les systèmes éligibles à grande échelle.

Utilisez la console web

La console web facilite le processus de mise à niveau en affichant le rapport de vérification avant mise à niveau dans un format facile à lire.

Assurez-vous que les paquets cockpit et cockpit-leapp sont bien installés en utilisant la commande **yum install cockpit cockpit-leapp**.

Utilisez ensuite **systemctl enable --now cockpit.socket** pour activer le socket Cockpit.

Ajoutez le port de la console web à votre pare-feu avec la commande **firewall-cmd --add-port 9090/tcp** et assurez-vous que la règle est ajoutée à la configuration permanente du pare-feu avec la commande **firewall-cmd --add-port 9090/tcp --permanent**.

Connectez-vous ensuite à la console web à l'adresse *https://your_server_name:9090*.

Exigences relatives au référentiel Satellite

Si vous utilisez le serveur Satellite pour gérer vos paquets, assurez-vous que les référentiels suivants sont disponibles :

- 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

Si vous avez utilisé la commande yum versionlock pour verrouiller les paquets dans une version spécifique, effacez-la à l'aide de la commande **yum versionlock clear**.

À propos de Red Hat

Premier éditeur mondial de solutions Open Source, Red Hat s'appuie sur une approche communautaire pour fournir des technologies Linux, de cloud hybride, de conteneurs et Kubernetes fiables et performantes. Red Hat aide ses clients à développer des applications cloud-native, à intégrer des applications nouvelles et existantes ainsi qu'à gérer et à automatiser des environnements complexes. Conseiller de confiance auprès des entreprises du Fortune 500, Red Hat propose des services d'assistance, de formation et de consulting reconnus qui apportent à tout secteur les avantages de l'innovation ouverte. Situé au cœur d'un réseau mondial d'entreprises, de partenaires et de communautés, Red Hat participe à la croissance et à la transformation des entreprises et les aide à se préparer à un avenir toujours plus numérique.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
#F31715_0822