Red Hat Enterprise Linux 9

Mise à niveau de RHEL 8 vers RHEL 9

Instructions pour une mise à niveau en place de Red Hat Enterprise Linux 8 vers Red Hat Enterprise Linux 9

Last Updated: 2024-02-16

Red Hat Enterprise Linux 9 Mise à niveau de RHEL 8 vers RHEL 9

Instructions pour une mise à niveau en place de Red Hat Enterprise Linux 8 vers Red Hat Enterprise Linux 9

Notice légale

Résumé

Ce document fournit des instructions sur la manière d'effectuer une mise à niveau sur site de Red Hat Enterprise Linux 8 vers Red Hat Enterprise Linux 9 à l'aide de l'utilitaire Leapp. Lors de la mise à niveau en place, le système d'exploitation RHEL 8 existant est remplacé par une version RHEL 9.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

TERMINOLOGIE CLÉ DE LA MIGRATION

Bien que les termes de migration suivants soient couramment utilisés dans l'industrie du logiciel, ces définitions sont spécifiques à Red Hat Enterprise Linux (RHEL).

Update

Parfois appelée correctif logiciel, une mise à jour est un ajout à la version actuelle de l'application, du système d'exploitation ou du logiciel que vous utilisez. Une mise à jour logicielle corrige les problèmes ou les bogues afin d'améliorer l'expérience de travail avec la technologie. Dans RHEL, une mise à jour concerne une version mineure, par exemple, la mise à jour de RHEL 8.1 à 8.2.

Upgrade

Une mise à niveau consiste à remplacer l'application, le système d'exploitation ou le logiciel que vous utilisez actuellement par une version plus récente. En règle générale, vous devez d'abord sauvegarder vos données conformément aux instructions de Red Hat. Lorsque vous mettez à niveau RHEL, deux options s'offrent à vous :

- **In-place upgrade:** Lors d'une mise à niveau sur place, vous remplacez la version précédente par la nouvelle version sans supprimer au préalable la version précédente. Les applications et les utilitaires installés, ainsi que les configurations et les préférences, sont intégrés dans la nouvelle version.

- **Clean install:** Une installation propre supprime toutes les traces du système d'exploitation, des données système, des configurations et des applications précédemment installés et installe la dernière version du système d'exploitation. Une installation propre est idéale si vous n'avez besoin d'aucune des données ou applications précédentes sur vos systèmes ou si vous développez un nouveau projet qui ne repose pas sur des versions antérieures.

Operating system conversion

Une conversion a lieu lorsque vous convertissez votre système d'exploitation d'une distribution Linux différente à Red Hat Enterprise Linux. En règle générale, vous commencez par sauvegarder vos données en suivant les instructions de Red Hat.

Migration

En règle générale, une migration indique un changement de plate-forme : logiciel ou matériel. Passer de Windows à Linux est une migration. Le passage d'un utilisateur d'un ordinateur portable à un autre ou d'une entreprise d'un serveur à un autre est une migration. Cependant, la plupart des migrations impliquent également des mises à niveau, et les termes sont parfois utilisés de manière interchangeable.

- **Migration to RHEL:** Conversion d'un système d'exploitation existant vers RHEL

- **Migration across RHEL:** Passer d'une version de RHEL à une autre

CHAPITRE 1. CHEMINS DE MISE À NIVEAU PRIS EN CHARGE

La mise à niveau en place remplace le système d'exploitation RHEL 8 de votre système par une version RHEL 9.

IMPORTANT

Il n'est pas possible d'effectuer une mise à niveau directement de RHEL 7 à RHEL 9. Toutefois, vous pouvez effectuer une mise à niveau de RHEL 7 à RHEL 8, puis une seconde mise à niveau vers RHEL 9. Pour plus d'informations, voir Mise à niveau de RHEL 7 à RHEL 8.

Actuellement, il est possible d'effectuer une mise à niveau sur place à partir des versions mineures RHEL 8 suivantes vers les versions mineures RHEL 9 suivantes :

Tableau 1.1. Chemins de mise à niveau pris en charge

Configuration du système	Source Version du système d'exploitation	Version du système d'exploitation cible
RHEL	RHEL 8.6	RHEL 9.0
	RHEL 8.8	RHEL 9.2
RHEL avec SAP HANA	RHEL 8.6	RHEL 9.0

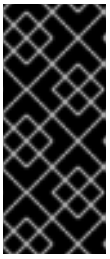
Pour plus d'informations sur les chemins de mise à niveau pris en charge, voir Chemins de mise à niveau in situ pris en charge pour Red Hat Enterprise Linux.

CHAPITRE 2. PLANIFIER UNE MISE À NIVEAU

An in-place upgrade is the recommended and supported way to upgrade your system to the next major version of RHEL.

Avant de procéder à la mise à niveau vers RHEL 9, vous devez tenir compte des éléments suivants :

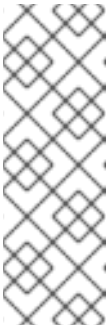
- **Operating system** - Le système d'exploitation peut être mis à niveau par l'utilitaire **Leapp** dans les conditions suivantes :
  - La version du système d'exploitation source est installée sur un système doté de l'une des architectures suivantes :
    - 64 bits Intel, AMD et ARM
    - IBM POWER (petit endian)
    - iBM Z 64 bits
      Pour plus d'informations, voir Matériel certifié Red Hat.
  - La configuration matérielle minimale requise pour RHEL 9 est respectée.
  - Vous avez accès à un contenu actualisé pour les versions du système d'exploitation source et cible sélectionnées. Pour plus d'informations, voir Préparation d'un système RHEL 8 pour la mise à niveau.
- **Applications** - Vous pouvez migrer les applications installées sur votre système à l'aide de **Leapp**. Cependant, dans certains cas, vous devez créer des acteurs personnalisés, qui spécifient les actions à effectuer par **Leapp** pendant la mise à niveau, par exemple, la reconfiguration d'une application ou l'installation d'un pilote matériel spécifique. Pour plus d'informations, voir Gérer la migration de vos applications personnalisées et tierces . Notez que les acteurs personnalisés ne sont pas pris en charge par Red Hat.



IMPORTANT

SHA1 a été supprimé dans RHEL 9. Si votre système contient des paquets avec des signatures **RSA/SHA1**, la mise à niveau est inhibée. Avant la mise à niveau, supprimez ces paquets ou contactez le vendeur pour obtenir des paquets avec des signatures **RSA/SHA256**. Pour plus d'informations, consultez SHA-1 deprecation in Red Hat Enterprise Linux 9.

- **Security** - Vous devez évaluer cet aspect avant la mise à niveau et prendre des mesures supplémentaires lorsque le processus de mise à niveau est terminé. Tenez compte en particulier des éléments suivants :
  - Avant la mise à niveau, définissez la norme de sécurité à laquelle votre système doit se conformer et comprenez les modifications apportées à la sécurité dans RHEL 9 .
  - Au cours du processus de mise à niveau, l'utilitaire **Leapp** définit le mode SELinux sur permissif.
  - Les mises à niveau sur place des systèmes en mode FIPS ne sont pas prises en charge.

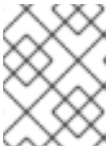


NOTE

Désactiver FIPS, mettre à niveau de RHEL 8 à 9, puis activer FIPS n'est pas pris en charge par Red Hat. Pour être conforme à la norme FIPS, toutes les clés cryptographiques doivent être utilisées uniquement par les modules cryptographiques validés par la norme FIPS. Par conséquent, l'activation de FIPS après la mise à niveau ne peut pas être prise en charge sans régénérer les clés cryptographiques. Notez que Red Hat ne suit pas chaque clé cryptographique créée et ne peut donc pas automatiser cette tâche.

- Une fois la mise à niveau terminée, réévaluez et appliquez à nouveau vos stratégies de sécurité. Pour plus d'informations sur l'application et la mise à jour des stratégies de sécurité, voir Application des stratégies de sécurité.

- **Storage and file systems**- Vous devez toujours sauvegarder votre système avant de procéder à une mise à niveau. Par exemple, vous pouvez utiliser l'utilitaire Relax-and-Recover (ReaR), des instantanés LVM, le fractionnement RAID ou un instantané de machine virtuelle.



NOTE

Les formats des systèmes de fichiers sont intacts. Par conséquent, les systèmes de fichiers ont les mêmes limitations que lorsqu'ils ont été créés à l'origine.

- **High Availability** - Si vous utilisez le module complémentaire de haute disponibilité, suivez l'article de la base de connaissances Pratiques recommandées pour l'application de mises à jour logicielles à un cluster de haute disponibilité ou de stockage résilient RHEL.

- **Downtime** - Le processus de mise à niveau peut durer de quelques minutes à plusieurs heures.

- **Satellite** - Si vous gérez vos hôtes via Satellite, vous pouvez mettre à niveau plusieurs hôtes simultanément de RHEL 8 à RHEL 9 à l'aide de l'interface utilisateur Web de Satellite. Pour plus d'informations, voir Mise à niveau d'hôtes vers la prochaine version majeure de Red Hat Enterprise Linux.

- **SAP HANA** - Si vous utilisez SAP HANA, suivez plutôt le guide How to in-place upgrade SAP environments from RHEL 8 to RHEL 9. Notez que le chemin de mise à niveau pour RHEL avec SAP HANA peut être différent.

- **Public clouds** - La mise à niveau en place est prise en charge pour les instances Pay-As-You-Go (PAYG) à la demande sur Amazon Web Services (AWS), Microsoft Azure, et Google Cloud Platform avec Red Hat Update Infrastructure (RHUI) . La mise à niveau in situ est également prise en charge pour les instances Bring Your Own Subscription sur tous les clouds publics qui utilisent RHSM pour un abonnement RHEL.

- **Language** - Tous les rapports, journaux et autres documents générés par **Leapp** sont en anglais, quelle que soit la configuration linguistique.

- **Bootloader** - Il n'est pas possible de basculer le chargeur de démarrage de BIOS à UEFI sur RHEL 8 ou RHEL 9. Si votre système RHEL 8 utilise BIOS et que vous souhaitez que votre système RHEL 9 utilise UEFI, effectuez une nouvelle installation de RHEL 9 au lieu d'une mise à niveau sur place. Pour plus d'informations, voir Est-il possible de passer du démarrage BIOS au démarrage UEFI sur une machine Red Hat Enterprise Linux préinstallée ?

- **Known limitations** - Les principales limites connues de **Leapp** sont actuellement les suivantes :

- Le chiffrement de l'ensemble du disque ou d'une partition, ou le chiffrement du système de fichiers ne peut actuellement pas être utilisé sur un système destiné à une mise à niveau en place.
- Aucun chemin multiple basé sur le réseau et aucun type de montage de stockage en réseau ne peut être utilisé comme partition du système (par exemple, iSCSI ou NFS).
- La mise à niveau sur place n'est actuellement pas prise en charge pour les instances PAYG à la demande sur les nuages publics restants (Huawei Cloud, Alibaba Cloud) qui utilisent Red Hat Update Infrastructure mais pas Red Hat Subscription Manager (RHSM) pour un abonnement RHEL.
- La mise à jour sur place n'est pas prise en charge pour les systèmes sur lesquels Ansible Tower est installé.

Voir aussi les problèmes connus.

Vous pouvez utiliser **Red Hat Insights** pour déterminer lequel des systèmes que vous avez enregistrés dans Insights se trouve sur un chemin de mise à niveau pris en charge vers RHEL 9. Pour ce faire, naviguez jusqu'à la recommandation Advisor correspondante dans Insights, activez la recommandation dans le menu déroulant *Actions* et consultez la liste sous l'en-tête *Affected systems*. Notez que la recommandation du conseiller ne prend en compte que la version mineure de RHEL 8 et n'effectue pas d'évaluation du système avant la mise à niveau. Voir également l'aperçu des recommandations du service Advisor.

CHAPITRE 3. PRÉPARATION DE LA MISE À NIVEAU

Pour éviter tout problème après la mise à niveau et s'assurer que votre système est prêt à être mis à niveau vers la prochaine version majeure de RHEL, effectuez toutes les étapes de préparation nécessaires avant la mise à niveau.

Vous devez effectuer les étapes de préparation décrites dans Préparation d'un système RHEL 8 pour la mise à niveau sur tous les systèmes. En outre, sur les systèmes enregistrés auprès du serveur Satellite, vous devez également effectuer les étapes de préparation décrites dans Préparation d'un système enregistré auprès du serveur Satellite pour la mise à niveau.

3.1. PRÉPARATION D'UN SYSTÈME RHEL 8 POUR LA MISE À NIVEAU

Cette procédure décrit les étapes nécessaires avant d'effectuer une mise à niveau sur place vers RHEL 9 à l'aide de l'utilitaire **Leapp**.

Si vous ne prévoyez pas d'utiliser le Gestionnaire d'abonnements Red Hat (RHSM) pendant le processus de mise à niveau, suivez les instructions de la section Mise à niveau vers RHEL 9 sans le Gestionnaire d'abonnements Red Hat.

Conditions préalables

- Le système répond aux conditions énumérées dans Planification d'une mise à niveau .

Procédure

1. Assurez-vous que votre système a été enregistré avec succès auprès du Red Hat Content Delivery Network (CDN) ou de Red Hat Satellite à l'aide du Gestionnaire d'abonnement Red Hat.

2. Si vous avez enregistré votre système auprès du serveur Satellite, suivez les étapes de la section Préparation d'un système enregistré auprès du serveur Satellite pour la mise à niveau afin de vous assurer que votre système répond aux exigences de la mise à niveau.

3. Vérifiez que l'abonnement au serveur Red Hat Enterprise Linux est attaché. Par exemple :

```
# subscription-manager list --installed
+-------------------------------------------+
    Installed Product Status
+-------------------------------------------+
Product Name:   Red Hat Enterprise Linux x86_64
Product ID:     479
Version:        8.6
Arch:           x86_64
Status:         Subscribed
```

4. Assurez-vous que les référentiels appropriés sont activés. La commande suivante active les dépôts Base et AppStream pour l'architecture Intel 64 bits ; pour les autres architectures, voir les dépôts RHEL 8.

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

NOTE

En option, vous pouvez activer les référentiels CodeReady Linux Builder (également connu sous le nom d'Optional) ou Supplementary. Pour plus d'informations sur les ID de référentiel, voir Référentiels RHEL 8 . Pour plus d'informations sur le contenu de ces référentiels, voir le manifeste des paquets.

5. Pour les systèmes abonnés à l'aide de RHSM, verrouillez le système sur la version du système d'exploitation source souhaitée :

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

Remplacez *<source_os_version>* par la version du système d'exploitation source, par exemple **8.6**.

6. Facultatif : Pour utiliser des référentiels personnalisés, voir l'article de la base de connaissances Configurer les référentiels personnalisés .

7. Si vous utilisez le plugin **dnf versionlock** pour verrouiller les paquets à une version spécifique, effacez le verrou en exécutant la commande suivante

```
# dnf versionlock clear
```

Voir Comment restreindre dnf à l'installation ou à la mise à niveau d'un paquetage vers une version spécifique fixe ? pour plus d'informations.

8. Si vous effectuez une mise à niveau en utilisant Red Hat Update Infrastructure (RHUI) sur un cloud public, activez les dépôts RHUI requis et installez les paquets RHUI requis afin de vous assurer que votre système est prêt pour la mise à niveau :

   a. Pour AWS :

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

   b. Pour Microsoft Azure :

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

   c. Pour Google Cloud Platform, suivez l'article de la base de connaissances Leapp RHUI packages for Google Cloud Platform (GCP).

9. Mettre à jour tous les paquets vers la dernière version de RHEL 8 :

```
# dnf update
```

10. Redémarrer le système :

```
# reboot
```

11. Installez l'utilitaire **Leapp**:

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

Notez qu'actuellement vous avez besoin de la version 0.15.1 ou plus récente du paquet **leapp** et de la version 0.18.0 ou plus récente du paquet **leapp-repository**, qui contient le paquet RPM **leapp-upgrade-el8toel9**.

NOTE

Si votre système ne dispose pas d'un accès à Internet, téléchargez les paquets suivants à partir du portail client de Red Hat :

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

12. Assurez-vous d'avoir accès à la dernière version des fichiers de données supplémentaires requis, y compris les modifications apportées aux paquets RPM, le mappage des dépôts RPM et les pilotes et périphériques non pris en charge.

    a. Si vous utilisez RHSM pour la mise à niveau, que le système a accès à cloud.redhat.com et que vous n'avez pas téléchargé une version antérieure des fichiers de données requis, aucune autre action n'est requise de votre part. Les fichiers de données sont automatiquement téléchargés depuis cloud.redhat.com.

    b. Si vous accédez à Red Hat CDN à l'aide d'un serveur proxy, définissez la variable d'environnement **$LEAPP_PROXY_HOST** afin d'accéder à la dernière version des fichiers de données requis.

    c. Si nécessaire, téléchargez les fichiers de données joints à l'article de la base de connaissances intitulé Leapp utility metadata in-place upgrades of RHEL for disconnected upgrades et placez-les dans le répertoire **/etc/leapp/files/**. Cette opération est nécessaire à la réussite de la mise à niveau dans les scénarios suivants :

        i. Vous effectuez une mise à niveau sur un nuage public en utilisant RHUI. Si vous ne disposez pas d'un abonnement Red Hat ou d'un compte Red Hat Customer Portal, créez un abonnement de développeur RHEL gratuit afin de pouvoir accéder à l'article de la base de connaissances et télécharger les paquets de données requis. Pour plus d'informations, voir Comment obtenir un abonnement gratuit de développeur Red Hat Enterprise Linux ou le renouveler ?

        ii. Votre système n'a pas d'accès à l'internet.

        iii. Vous utilisez RHSM pour la mise à niveau et vous avez précédemment téléchargé une ancienne version des fichiers de données requis, mais vous n'avez pas effectué la mise à niveau, par exemple pour créer des scripts automatisés. Vous pouvez également supprimer votre ancienne version des fichiers de données pour lancer le téléchargement automatique de la dernière version des fichiers.

13. Désactiver temporairement le logiciel antivirus pour éviter que la mise à niveau n'échoue.

14. Veiller à ce qu'aucun système de gestion de la configuration n'interfère avec le processus de mise à niveau en place :

- Si vous utilisez un système de gestion de la configuration avec une architecture client-serveur, tel que **Puppet**, **Salt**, ou **Chef**, désactivez le système avant d'exécuter la commande **leapp preupgrade**. N'activez le système de gestion de la configuration qu'une fois la mise à niveau terminée afin d'éviter tout problème pendant la mise à niveau.

- Si vous utilisez un système de gestion de la configuration avec une architecture sans agent, tel que **Ansible**, n'exécutez pas le fichier de configuration et de déploiement, tel qu'un playbook Ansible, pendant la mise à niveau en place, comme décrit dans Exécution de la mise à niveau de RHEL 8 vers RHEL 9.
  L'automatisation du processus de pré-mise à niveau et de mise à niveau à l'aide d'un système de gestion de la configuration n'est pas prise en charge par Red Hat. Pour plus d'informations, voir Utilisation de systèmes de gestion de configuration pour automatiser certaines parties du processus de pré-mise à niveau et de mise à niveau de Leapp sur Red Hat Enterprise Linux.

15. Assurez-vous que votre système n'utilise pas plus d'une carte d'interface réseau (NIC) avec un nom basé sur le préfixe utilisé par le noyau (**eth**). Pour savoir comment migrer vers un autre schéma de dénomination avant une mise à niveau sur place vers RHEL 9, voir Comment effectuer une mise à niveau sur place vers RHEL 8 lors de l'utilisation de noms de cartes d'interface réseau du noyau sur RHEL 7. Le processus de migration des schémas de nommage est le même pour la mise à niveau de RHEL 7 vers RHEL 8 et la mise à niveau de RHEL 8 vers RHEL 9.

16. Si votre base de données NSS a été créée sous RHEL 7 ou une version antérieure, vérifiez qu'elle a été convertie du format DBM au format SQLite. Pour plus d'informations, voir Mise à jour des bases de données NSS de DBM à SQLite.

17. RHEL 9 ne prend pas en charge l'ancien package **network-scripts**, qui a été supprimé dans RHEL 8. Avant la mise à niveau, déplacez vos scripts réseau personnalisés et écrivez un script de distribution NetworkManager qui exécute vos scripts personnalisés existants. Pour plus d'informations, voir Migration des scripts réseau personnalisés vers des scripts de distribution NetworkManager.

18. Si vous effectuez une mise à niveau à l'aide d'une image ISO, vérifiez que l'image ISO contient la version du système d'exploitation cible, par exemple RHEL 9.0, et qu'elle est enregistrée sur un point de montage local persistant afin de garantir que l'utilitaire **Leapp** puisse accéder à l'image tout au long du processus de mise à niveau.

19. Assurez-vous de disposer d'une sauvegarde complète du système ou d'un instantané de la machine virtuelle. Vous devriez pouvoir ramener votre système à l'état antérieur à la mise à niveau si vous suivez les procédures standard de reprise après sinistre dans votre environnement. Par exemple, vous pouvez utiliser l'utilitaire Relax-and-Recover (ReaR). Pour plus d'informations, consultez la documentation ReaR et la page Qu'est-ce que Relax and Recover (ReaR) et comment puis-je l'utiliser pour la reprise après sinistre ? Vous pouvez également utiliser des instantanés LVM ou le fractionnement RAID. En cas de mise à niveau d'une machine virtuelle, vous pouvez créer un instantané de l'ensemble de la machine virtuelle.

3.2. PRÉPARATION D'UN SYSTÈME ENREGISTRÉ PAR SATELLITE POUR LA MISE À NIVEAU

Cette procédure décrit les étapes nécessaires à la préparation d'un système enregistré auprès de Satellite pour la mise à niveau vers RHEL 9. Ces étapes sont effectuées sur le serveur Satellite.

IMPORTANT

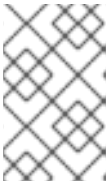
Les utilisateurs des systèmes Satellite doivent effectuer les étapes préparatoires décrites dans cette procédure et dans Préparation d'un système RHEL 8 pour la mise à niveau.

Conditions préalables

- Vous disposez de droits d'administration pour le serveur Satellite.

Procédure

1. Vérifiez que Satellite est sur une version avec un support complet ou de maintenance. Pour plus d'informations, consultez le cycle de vie du produit Red Hat Satellite .
2. Importez un manifeste d'abonnement avec des référentiels RHEL 9 dans le serveur Satellite. Pour plus d'informations, consultez le chapitre Gestion des abonnements Red Hat dans le Guide de gestion du contenu pour la version particulière de Red Hat Satellite , par exemple, pour la version 6.12.
3. Activez et synchronisez tous les référentiels RHEL 8 et RHEL 9 requis sur le serveur satellite avec les dernières mises à jour pour les versions du système d'exploitation source et cible. Les référentiels requis doivent être disponibles dans la vue de contenu et activés dans la clé d'activation associée.



NOTE

Pour les référentiels RHEL 9, activez la version du système d'exploitation cible, par exemple RHEL 9.0, de chaque référentiel. Si vous n'activez que la version RHEL 9 des référentiels, la mise à niveau en place est inhibée.

Par exemple, pour l'architecture Intel sans abonnement Extended Update Support (EUS), activez au minimum les dépôts suivants :

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

  x86_64 8 ou *<source_os_version>*
- Red Hat Enterprise Linux 8 pour x86_64 - BaseOS (RPMs)
  rhel-8-for-x86_64-baseos-rpms

  x86_64 8 ou *<source_os_version>*
- Red Hat Enterprise Linux 9 pour x86_64 - AppStream (RPMs)
  rhel-9-for-x86_64-appstream-rpms

  x86_64 *<target_os_version>*
- Red Hat Enterprise Linux 9 pour x86_64 - BaseOS (RPMs)
  rhel-9-for-x86_64-baseos-rpms

  x86_64 *<target_os_version>*

  Remplacez *<source_os_version>* et *<target_os_version>* par la version du système d'exploitation source et la version du système d'exploitation cible, par exemple, 8.6 et 9.0.

Pour les autres architectures, voir les référentiels RHEL 8 et RHEL 9.

Pour plus d'informations, consultez le chapitre *Importing Content* dans le site *Managing Content Guide* pour la version particulière de Red Hat Satellite, par exemple, pour la version 6.12.

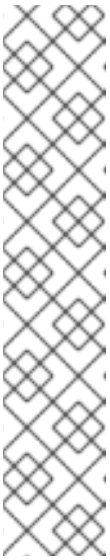
4. Attachez l'hôte de contenu à une vue de contenu contenant les référentiels RHEL 8 et RHEL 9 requis.
   Pour plus d'informations, consultez le chapitre *Managing Content Views* dans le site *Managing Content Guide* pour la version particulière de Red Hat Satellite, par exemple, pour la version 6.12.

Vérification

1. Vérifiez que les bons référentiels RHEL 8 et RHEL 9 ont été ajoutés à la bonne vue de contenu sur le serveur Satellite.

   a. Dans l'interface web de Satellite, naviguez jusqu'à **Content > Lifecycle > Content Views**et cliquez sur le nom de la vue de contenu.

   b. Cliquez sur l'onglet **Repositories** et vérifiez que les référentiels apparaissent comme prévu.



NOTE

Vous pouvez également vérifier que les référentiels ont été ajoutés à la vue Contenu à l'aide des commandes suivantes :

```
# 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>
```

Remplacer *<content_view_name>* par le nom de la vue de contenu, *<organization>* par l'organisation et *<lifecycle_environement>* par le nom de l'environnement du cycle de vie.

2. Vérifiez que les bons référentiels RHEL 9 sont activés dans la clé d'activation associée à la vue de contenu :

   a. Dans l'interface web de Satellite, naviguez vers **Content > Lifecycle > Activation Keys**et cliquez sur le nom de la clé d'activation.

   b. Cliquez sur l'onglet **Repository Sets** et vérifiez que les statuts des référentiels requis sont **Enabled**.

CHAPITRE 4. EXAMEN DU RAPPORT DE PRÉ-MISE À NIVEAU

Pour évaluer la possibilité de mise à niveau de votre système, lancez le processus de pré-mise à niveau à l'aide de la commande **leapp preupgrade**. Au cours de cette phase, l'utilitaire **Leapp** recueille des données sur le système, évalue la possibilité de mise à niveau et génère un rapport de pré-mise à niveau. Le rapport de pré-mise à niveau résume les problèmes potentiels et propose des solutions. Il vous aide également à décider s'il est possible ou conseillé de procéder à la mise à niveau.

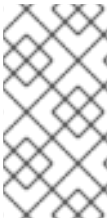
IMPORTANT

Examinez toujours l'intégralité du rapport de pré-mise à niveau, même si celui-ci ne fait état d'aucun obstacle à la mise à niveau. Le rapport de pré-mise à niveau contient des recommandations sur les actions à entreprendre avant la mise à niveau pour garantir le bon fonctionnement du système mis à niveau.

L'examen d'un rapport de pré-mise à niveau peut également s'avérer utile si vous souhaitez effectuer une nouvelle installation d'un système RHEL 9 au lieu de procéder à une mise à niveau sur place.

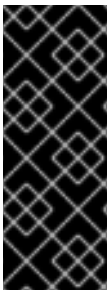
Vous pouvez évaluer la possibilité de mise à niveau au cours de la phase de pré-mise à niveau en utilisant l'une des méthodes suivantes :

- Examinez le rapport de pré-mise à niveau dans le fichier **leapp-report.txt** généré et résolvez manuellement les problèmes signalés à l'aide de l'interface de ligne de commande.
- Utilisez la console web pour examiner le rapport, appliquer les mesures correctives automatisées lorsqu'elles sont disponibles et résoudre les problèmes restants à l'aide des conseils de remédiation suggérés.



NOTE

Vous pouvez traiter le rapport de pré-mise à niveau en utilisant vos propres scripts personnalisés, par exemple, pour comparer les résultats de plusieurs rapports dans différents environnements. Pour plus d'informations, voir Automatiser le flux de travail de votre rapport de pré-mise à niveau de Red Hat Enterprise Linux.



IMPORTANT

Le rapport de pré-mise à niveau ne peut pas simuler l'ensemble du processus de mise à niveau sur place et ne peut donc pas identifier tous les problèmes inhibiteurs de votre système. Par conséquent, il se peut que votre mise à niveau en place soit interrompue même après que vous ayez examiné et résolu tous les problèmes mentionnés dans le rapport. Par exemple, le rapport de pré-mise à niveau ne peut pas détecter les problèmes liés à des téléchargements de paquets interrompus.

4.1. ÉVALUER L'ÉVOLUTIVITÉ À PARTIR DE LA LIGNE DE COMMANDE

Identifier les problèmes potentiels de mise à niveau pendant la phase de pré-mise à niveau en utilisant l'interface de ligne de commande.

Conditions préalables

- Les étapes énumérées dans la section Préparation de la mise à niveau ont été effectuées.

Procédure

1. Sur votre système RHEL 8, effectuez la phase de pré-mise à niveau :

```
# leapp preupgrade
```

   - Si vous utilisez des référentiels personnalisés du répertoire **/etc/yum.repos.d/** pour la mise à niveau, activez les référentiels sélectionnés comme suit :

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

   - Si vous effectuez une mise à niveau sans RHSM ou en utilisant RHUI, ajoutez l'option **--no-rhsm**.

   - Si vous avez un abonnement Extended Upgrade Support (EUS), Advanced Update Support (AUS) ou Update Services for SAP Solutions (E4S), ajoutez l'option **--channel *<channel>*** option. Remplacez *<channel>* par le nom du canal, par exemple, **eus**, **aus**, ou **e4s**. Notez que les clients SAP HANA doivent effectuer la mise à niveau in situ en utilisant le guide Comment mettre à niveau in situ des environnements SAP de RHEL 8 à RHEL 9 .

2. Examinez le rapport dans le fichier **/var/log/leapp/leapp-report.txt** et résolvez manuellement tous les problèmes signalés. Certains problèmes signalés contiennent des suggestions de remédiation. **Inhibitor** problèmes vous empêchent de procéder à la mise à niveau tant que vous ne les avez pas résolus.
   Le rapport contient les niveaux de facteurs de risque suivants :

   Haut

   Il est très probable que cela entraîne une détérioration de l'état du système.

   Moyen

   Peut avoir un impact à la fois sur le système et sur les applications.

   Faible

   Ne devrait pas avoir d'incidence sur le système, mais peut en avoir sur les applications.

   Info

   Information sans impact attendu sur le système ou les applications.

3. Dans certaines configurations du système, l'utilitaire **Leapp** génère des questions vraies ou fausses auxquelles vous devez répondre manuellement. Si le rapport de pré-mise à niveau contient un message **Missing required answers in the answer file** procédez comme suit :

   a. Ouvrez le fichier **/var/log/leapp/answerfile** et passez en revue les questions vrai ou faux.

   b. Modifiez manuellement le fichier **/var/log/leapp/answerfile file**, décommentez la ligne de confirmation du fichier en supprimant le symbole **#**, et confirmez votre réponse en tant que **True** ou **False**. Pour plus d'informations, voir le fichier de réponse Leapp.

NOTE

Vous pouvez également répondre à la question "vrai ou faux" en exécutant la commande suivante :

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

Par exemple, pour confirmer une réponse **True** à la question **Are all VDO devices, if any, successfully converted to LVM management?**, exécutez la commande suivante :

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

4. Répétez les étapes précédentes pour réexécuter le rapport de pré-mise à niveau afin de vérifier que vous avez résolu tous les problèmes critiques.

4.2. ÉVALUER LA POSSIBILITÉ DE MISE À NIVEAU ET APPLIQUER DES MESURES CORRECTIVES AUTOMATISÉES PAR LE BIAIS DE LA CONSOLE WEB

Identifier les problèmes potentiels dans la phase de pré-mise à niveau et appliquer des remèdes automatisés en utilisant la console web.

Conditions préalables

- Vous avez effectué les étapes énumérées dans la section Préparation de la mise à niveau .

Procédure

1. Installer le plug-in **cockpit-leapp**:

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

2. Connectez-vous à la console web en tant que **root** ou en tant qu'utilisateur disposant d'autorisations pour entrer des commandes administratives avec **sudo**. Voir Gestion des systèmes à l'aide de la console web RHEL 8 pour plus d'informations sur la console web.

3. Sur votre système RHEL 8, effectuez la phase de pré-mise à niveau soit à partir de l'interface de ligne de commande, soit à partir du terminal de la console web :

```
# leapp preupgrade
```

   - Si vous utilisez des référentiels personnalisés du répertoire **/etc/yum.repos.d/** pour la mise à niveau, activez les référentiels sélectionnés comme suit :

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

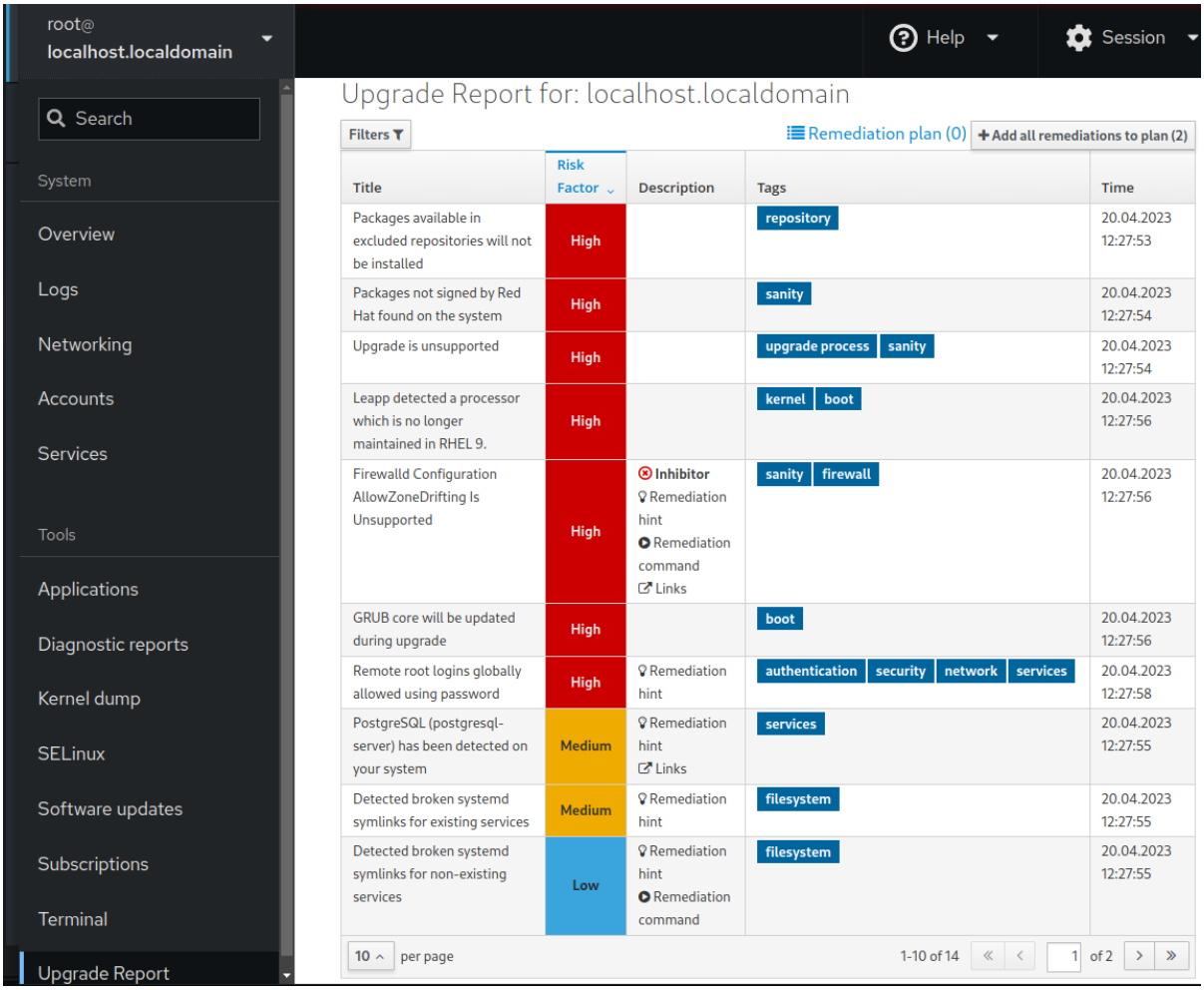
   - Si vous effectuez une mise à niveau sans RHSM ou en utilisant RHUI, ajoutez l'option **--no-rhsm**.

   - Si vous avez un abonnement Extended Upgrade Support (EUS), Advanced Update Support (AUS) ou Update Services for SAP Solutions (E4S), ajoutez l'option **--channel *<channel>***

option. Remplacez *<channel>* par le nom du canal, par exemple, **eus**, **aus**, ou **e4s**. Notez que les clients SAP HANA doivent effectuer la mise à niveau in situ en utilisant le guide Comment mettre à niveau in situ des environnements SAP de RHEL 8 à RHEL 9 .

4. Dans la console web, sélectionnez **Upgrade Report** dans le menu de navigation pour passer en revue tous les problèmes signalés. Les problèmes **Inhibitor** vous empêchent de procéder à la mise à niveau tant que vous ne les avez pas résolus. Pour visualiser un problème en détail, sélectionnez la ligne pour ouvrir le volet Détails.

Figure 4.1. Rapport de mise à jour sur place dans la console web



Le rapport contient les niveaux de facteurs de risque suivants :

Haut

Il est très probable que cela entraîne une détérioration de l'état du système.

Moyen

Peut avoir un impact à la fois sur le système et sur les applications.

Faible

Ne devrait pas avoir d'incidence sur le système, mais peut en avoir sur les applications.

Info

Information sans impact attendu sur le système ou les applications.

5. Dans certaines configurations, l'utilitaire **Leapp** génère des questions vraies ou fausses auxquelles vous devez répondre manuellement. Si le rapport de mise à niveau contient une ligne **Missing required answers in the answer file** procédez comme suit :

a. Sélectionnez la ligne **Missing required answers in the answer file** pour ouvrir le volet

a. Sélectionnez la ligne **Missing required answers in the answer file** pour ouvrir le volet **Detail**. La réponse par défaut est indiquée à la fin de la commande de remédiation.

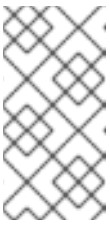
b. Pour confirmer la réponse par défaut, sélectionnez **Add to Remediation Plan** pour exécuter la remédiation ultérieurement ou **Run Remediation** pour exécuter la remédiation immédiatement.

c. Pour sélectionner une réponse autre que celle par défaut, exécutez la commande **leapp answer** dans le terminal, en précisant la question à laquelle vous répondez et la réponse que vous avez confirmée.

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

Par exemple, pour confirmer une réponse **True** à la question **Are all VDO devices, if any, successfully converted to LVM management?**, exécutez la commande suivante :

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



NOTE

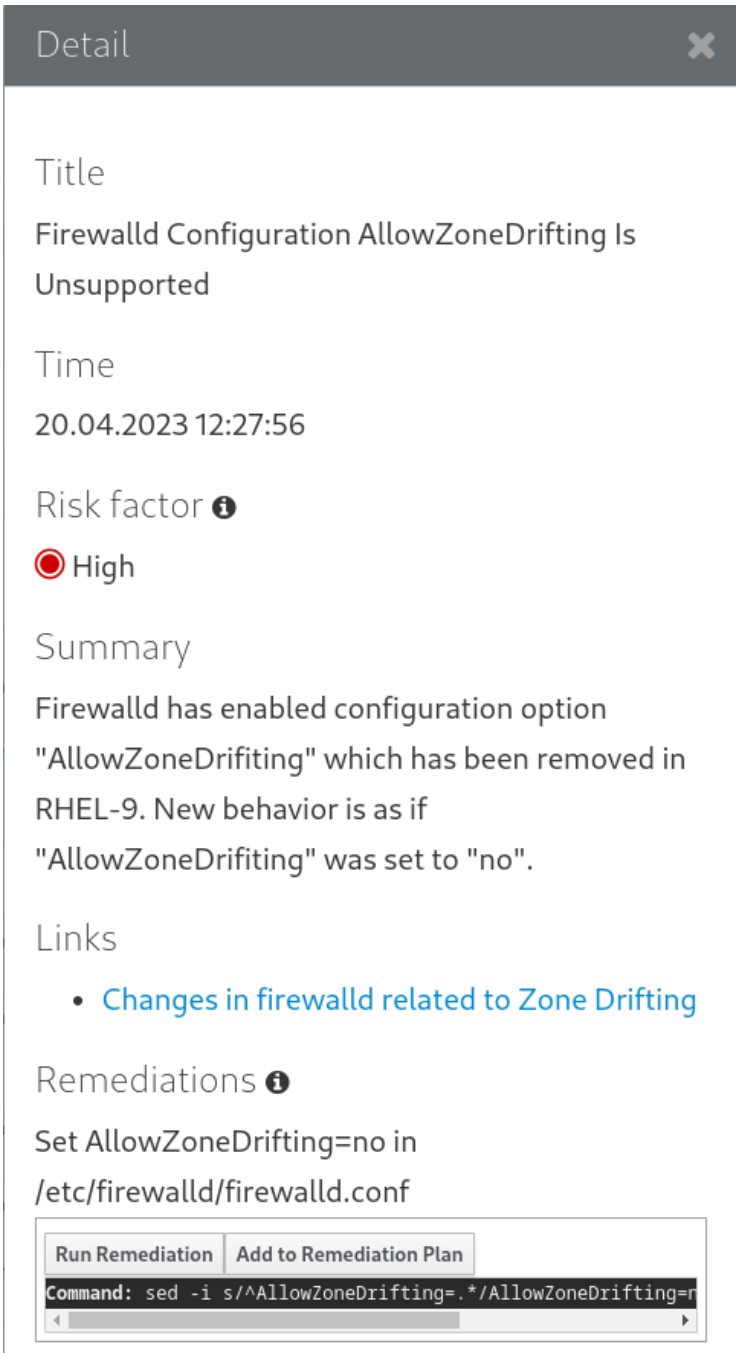
Vous pouvez également éditer manuellement le fichier **/var/log/leapp/answerfile**, décommenter la ligne de confirmation du fichier en supprimant le symbole **#** et confirmer votre réponse en tant que **True** ou **False**. Pour plus d'informations, voir l' exemple de fichier de réponse Leapp.

6. Certains problèmes ont des commandes de remédiation que vous pouvez exécuter pour résoudre automatiquement les problèmes. Vous pouvez exécuter les commandes de remédiation individuellement ou toutes ensemble dans la commande de remédiation.

a. Pour exécuter une seule commande de remédiation, ouvrez le volet **Detail** pour le problème et cliquez sur **Run Remediation**.

b. Pour ajouter une commande de remédiation au plan de remédiation, ouvrez le volet **Detail** pour le problème et cliquez sur **Add to Remediation Plan**.

Figure 4.2. Volet de détail



c. Pour exécuter le plan de remédiation contenant toutes les commandes de remédiation ajoutées, cliquez sur le lien **Remediation plan** dans le coin supérieur droit au-dessus du rapport. Cliquez sur **Execute Remediation Plan** pour exécuter toutes les commandes listées.

7. Après avoir examiné le rapport et résolu tous les problèmes signalés, répétez les étapes 3 à 7 pour réexécuter le rapport et vérifier que vous avez résolu tous les problèmes critiques.

CHAPITRE 5. EFFECTUER LA MISE À NIVEAU DE RHEL 8 VERS RHEL 9

Cette procédure répertorie les étapes nécessaires pour effectuer la mise à niveau de RHEL 8 vers RHEL 9 à l'aide de l'utilitaire **Leapp**.

Conditions préalables

- Les étapes énumérées dans la section Préparation de la mise à niveau ont été effectuées, y compris une sauvegarde complète du système.
- Les étapes énumérées dans la section Examen du rapport de pré-mise à niveau ont été effectuées et tous les problèmes signalés ont été résolus.

Procédure

1. Sur votre système RHEL 8, lancez le processus de mise à niveau :

```
# leapp upgrade
```

   - Si vous utilisez des référentiels personnalisés du répertoire **/etc/yum.repos.d/** pour la mise à niveau, activez les référentiels sélectionnés comme suit :

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

   - Si vous effectuez une mise à niveau sans RHSM ou en utilisant RHUI, ajoutez l'option **--no-rhsm**.
   - Si vous effectuez une mise à niveau à l'aide d'une image ISO, ajoutez les options **--no-rhsm** et **--iso *<file_path>*** . Remplacez *<file_path>* par le chemin d'accès à l'image ISO enregistrée, par exemple **/home/rhel9.iso**.
   - Si vous avez un abonnement Extended Upgrade Support (EUS), Advanced Update Support (AUS) ou Update Services for SAP Solutions (E4S) , ajoutez l'option **--channel *channel*** (option). Remplacez *channel* par la valeur utilisée dans la commande **leapp preupgrade**, par exemple **eus**, **aus** ou **e4s**. Notez que vous devez utiliser la même valeur avec l'option **--channel** dans les commandes **leapp preupgrade** et **leapp upgrade**.

2. Au début du processus de mise à niveau, **Leapp** exécute la phase de pré-mise à niveau décrite dans la section Examen du rapport de pré-mise à niveau .
   - Si le système peut être mis à niveau, **Leapp** télécharge les données nécessaires et prépare une transaction RPM pour la mise à niveau.
   - Si votre système ne répond pas aux paramètres d'une mise à niveau fiable, **Leapp** met fin au processus de mise à niveau et fournit un enregistrement décrivant le problème et une solution recommandée dans le fichier **/var/log/leapp/leapp-report.txt**. Pour plus d'informations, voir Dépannage.
3. Redémarrer manuellement le système :

```
# reboot
```

Au cours de cette phase, le système démarre dans une image disque RAM initiale basée sur RHEL 9, initramfs. **Leapp** met à jour tous les paquets et redémarre automatiquement sur le système RHEL 9.

Vous pouvez également exécuter la commande **leapp upgrade** avec l'option **--reboot** et sauter cette étape manuelle.

En cas de défaillance, examinez les journaux et les problèmes connus comme indiqué dans la section Dépannage.

4. Connectez-vous au système RHEL 9 et vérifiez son état comme décrit dans la section Vérification de l'état post-mise à niveau du système RHEL 9 .

5. Effectuez toutes les tâches postérieures à la mise à niveau décrites dans le rapport de mise à niveau et dans la section Exécution des tâches postérieures à la mise à niveau .

CHAPITRE 6. VÉRIFICATION DE L'ÉTAT POST-MISE À NIVEAU DU SYSTÈME RHEL 9

Cette procédure énumère les étapes de vérification qu'il est recommandé d'effectuer après une mise à niveau en place vers RHEL 9.

Conditions préalables

- Le système a été mis à niveau en suivant les étapes décrites dans Effectuer la mise à niveau de RHEL 8 vers RHEL 9 et vous avez pu vous connecter à RHEL 9.

Procédure

Une fois la mise à niveau terminée, déterminez si le système se trouve au moins dans l'état requis :

- Vérifiez que la version actuelle du système d'exploitation est RHEL 9. Par exemple :

```
# cat /etc/redhat-release
Red Hat Enterprise Linux release 9.0 (Plow)
```

- Vérifiez la version du noyau du système d'exploitation. Par exemple :

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

  Notez que **.el9** est important et que la version ne doit pas être antérieure à 5.14.0.

- Si vous utilisez le Gestionnaire d'abonnements Red Hat :
  - Vérifiez que le bon produit est installé. Par exemple :

```
# subscription-manager list --installed
+-------------------------------------------+
    Installed Product Status
+-------------------------------------------+
Product Name: Red Hat Enterprise Linux for x86_64
Product ID:   479
Version:      9.0
Arch:         x86_64
Status:       Subscribed
```

  - Vérifiez que la version de mise à jour correspond à la version du système d'exploitation cible prévue immédiatement après la mise à niveau. Par exemple :

```
# subscription-manager release
Release: 9.0
```

- Vérifiez que les services réseau sont opérationnels. Par exemple, essayez de vous connecter à un serveur à l'aide de SSH.

- Vérifiez l'état de vos applications après la mise à niveau. Dans certains cas, vous devrez peut-être procéder manuellement à la migration et aux modifications de configuration. Par exemple, pour migrer vos bases de données, suivez les instructions de la section Configuration et utilisation des serveurs de base de données.

CHAPITRE 7. EXÉCUTION DES TÂCHES POSTÉRIEURES À LA MISE À NIVEAU

Cette procédure énumère les principales tâches qu'il est recommandé d'effectuer après une mise à niveau en place vers RHEL 9.

Conditions préalables

- Le système a été mis à niveau en suivant les étapes décrites dans Effectuer la mise à niveau de RHEL 8 vers RHEL 9 et vous avez pu vous connecter à RHEL 9.
- L'état de la mise à niveau en place a été vérifié en suivant les étapes décrites dans la section Vérification de l'état post-mise à niveau du système RHEL 9 .

Procédure

Après avoir effectué la mise à niveau, effectuez les tâches suivantes :

1. Supprimez tous les paquets **Leapp** restants de la liste d'exclusion dans le fichier de configuration **/etc/dnf/dnf.conf**, y compris le paquet **snactor**, qui est un outil de développement d'extension de mise à niveau. Pendant la mise à niveau sur place, les paquets **Leapp** qui ont été installés avec l'utilitaire **Leapp** sont automatiquement ajoutés à la liste d'exclusion pour éviter que des fichiers critiques ne soient supprimés ou mis à jour. Après la mise à niveau en place, ces paquets **Leapp** doivent être supprimés de la liste d'exclusion avant de pouvoir être retirés du système.
   - Pour supprimer manuellement des paquets de la liste d'exclusion, modifiez le fichier de configuration **/etc/dnf/dnf.conf** et supprimez les paquets **Leapp** souhaités de la liste d'exclusion.
   - Pour supprimer tous les paquets de la liste d'exclusion :

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

2. Supprimer les paquets RHEL 8 restants, y compris les paquets **Leapp** restants.
   a. Localisez les paquets RHEL 8 restants :

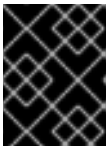
      ```
      # rpm -qa | grep -e '\.el[78]' | grep -vE '^(gpg-pubkey|libmodulemd|katello-ca-consumer)' | sort
      ```

   b. Supprimez les paquets RHEL 8 restants, y compris l'ancien paquetage du noyau, de votre système RHEL 9.
   c. Supprimer les paquets de dépendance restants de **Leapp**:

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

3. Facultatif : Supprimez du système toutes les données restantes relatives à la mise à niveau :

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



IMPORTANT

La suppression de ces données pourrait limiter la capacité de l'assistance Red Hat à enquêter et à résoudre les problèmes postérieurs à la mise à niveau.

4. Désactiver les dépôts DNF dont les paquets ne sont pas compatibles avec RHEL 9. Les dépôts gérés par RHSM sont gérés automatiquement. Pour désactiver ces dépôts :

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

Remplacez *repository_id* par l'identifiant du référentiel.

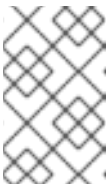
5. Remplacer l'ancien noyau de secours et le disque RAM initial par le noyau et le disque actuels :

   a. Supprimez le noyau de secours existant et le disque RAM initial :

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

   b. Réinstallez le noyau actuel pour récupérer le noyau de secours et le disque RAM initial correspondant :

```
# dnf reinstall -y kernel-core-$(uname -r)
```



NOTE

Si le paquetage du noyau de votre système a un nom différent, comme sur les systèmes temps réel, remplacez **kernel-core** par le nom du paquetage correct.

6. Réévaluez et appliquez à nouveau vos politiques de sécurité. En particulier, modifiez le mode SELinux pour qu'il soit appliqué. Pour plus de détails, voir Application des politiques de sécurité.

Vérification

1. Vérifiez que les fichiers du noyau de secours et du disque RAM initial de secours précédemment supprimés ont été créés pour le noyau actuel :

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

2. Vérifiez que l'entrée du boot de secours fait référence aux fichiers de secours existants. Voir la sortie de grubby :

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

CHAPITRE 8. APPLICATION DES POLITIQUES DE SÉCURITÉ

Au cours du processus de mise à niveau en place, la politique SELinux doit être commutée en mode permissif. En outre, les profils de sécurité peuvent contenir des modifications entre les versions majeures. Cette section vous guide dans la sécurisation de vos systèmes RHEL mis à niveau et couvre les détails des étapes préalables à la mise à niveau des composants liés à la sécurité.

8.1. CHANGEMENT DU MODE SELINUX EN MODE "ENFORCING

Au cours du processus de mise à niveau, l'utilitaire **Leapp** définit le mode SELinux sur permissif. Lorsque le système est mis à niveau avec succès, vous devez changer manuellement le mode SELinux en mode "enforcing".

Conditions préalables

- Le système a été mis à niveau et vous avez effectué les étapes de vérification décrites dans la section Vérification de l'état post-mise à niveau du système RHEL 9 .

Procédure

1. Assurez-vous qu'il n'y a pas de refus SELinux, par exemple en utilisant l'utilitaire **ausearch**:

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

   Notez que l'étape précédente ne couvre que le scénario le plus courant. Pour vérifier tous les refus SELinux possibles, voir la section Identifier les refus SELinux dans le titre Utiliser SELinux, qui fournit une procédure complète.

2. Ouvrez le fichier **/etc/selinux/config** dans un éditeur de texte de votre choix, par exemple :

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

3. Configurez l'option **SELINUX=enforcing**:

```
# 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. Enregistrez la modification et redémarrez le système :

```
# reboot
```

Vérification

1. Après le redémarrage du système, confirmez que la commande **getenforce** renvoie **Enforcing**:

```
$ getenforce
Enforcing
```

Ressources supplémentaires

- Résolution des problèmes liés à SELinux
- Modifier les états et les modes SELinux

8.2. POLITIQUES CRYPTOGRAPHIQUES À L'ÉCHELLE DU SYSTÈME

Les politiques cryptographiques à l'échelle du système sont un composant du système qui configure les sous-systèmes cryptographiques de base, couvrant les protocoles TLS, IPSec, SSH, DNSSec et Kerberos.

Le processus de mise à niveau en place préserve la stratégie cryptographique utilisée dans RHEL 8. Par exemple, si vous avez utilisé la stratégie cryptographique **DEFAULT** dans RHEL 8, votre système mis à niveau vers RHEL 9 utilise également **DEFAULT**. Notez que les paramètres spécifiques des politiques prédéfinies diffèrent et que les politiques cryptographiques de RHEL 9 contiennent des valeurs par défaut plus strictes et plus sûres. Par exemple, la stratégie cryptographique RHEL 9 **DEFAULT** restreint l'utilisation de SHA-1 pour les signatures et la stratégie **LEGACY** n'autorise plus les algorithmes de chiffrement DH et RSA de moins de 2048 bits. Pour plus d'informations, voir la section " Strong crypto defaults " du document " Security hardening" (renforcement de la sécurité) . Les règles cryptographiques personnalisées sont préservées lors de la mise à niveau en place.

Pour afficher ou modifier la politique cryptographique actuelle du système, utilisez l'outil update-crypto-policies :

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

Par exemple, la commande suivante fait passer le niveau de la politique cryptographique de l'ensemble du système à **FUTURE**, ce qui devrait permettre de résister à toute attaque future à court terme :

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

Si votre scénario nécessite l'utilisation de SHA-1 pour la vérification des signatures cryptographiques existantes ou de tiers, vous pouvez l'activer en entrant la commande suivante :

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

Vous pouvez également basculer les stratégies cryptographiques du système vers la stratégie **LEGACY**. Cependant, **LEGACY** autorise également de nombreux autres algorithmes qui ne sont pas sûrs.

AVERTISSEMENT

L'activation de la sous-politique **SHA** rend votre système plus vulnérable que les paramètres par défaut de RHEL 9. Le passage à la stratégie **LEGACY** est encore moins sûr et doit être utilisé avec prudence.

Vous pouvez également personnaliser les politiques cryptographiques à l'échelle du système. Pour plus d'informations, reportez-vous aux sections Personnaliser les politiques cryptographiques à l'échelle du système à l'aide de modificateurs de politique et Créer et paramétrer une politique cryptographique personnalisée à l'échelle du système. Si vous utilisez une stratégie cryptographique personnalisée, pensez à la revoir et à la mettre à jour pour atténuer les menaces liées aux progrès de la cryptographie et du matériel informatique.

Ressources supplémentaires

- Utilisation de politiques cryptographiques à l'échelle du système
- **update-crypto-policies(8)** page de manuel.

8.3. MISE À NIVEAU D'UN SYSTÈME DURCI À UN NIVEAU DE SÉCURITÉ DE BASE

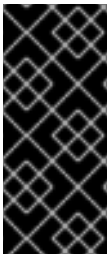
Pour obtenir un système entièrement renforcé après une mise à niveau réussie vers RHEL 9, vous pouvez utiliser la remédiation automatisée fournie par la suite OpenSCAP. Les mesures correctives d'OpenSCAP alignent votre système sur les normes de sécurité de base, telles que PCI-DSS, OSPP ou ACSC Essential Eight. Les recommandations de conformité de la configuration diffèrent d'une version majeure de RHEL à l'autre en raison de l'évolution de l'offre de sécurité.

not Lors de la mise à niveau d'un système RHEL 8 durci, l'outil **Leapp** ne fournit pas de moyen direct de conserver le durcissement complet. En fonction des modifications apportées à la configuration des composants, le système peut s'écarter des recommandations pour RHEL 9 au cours de la mise à niveau.

NOTE

Vous ne pouvez pas utiliser le même contenu SCAP pour scanner RHEL 8 et RHEL 9. Mettez à jour les plates-formes de gestion si la conformité du système est gérée par des outils tels que Red Hat Satellite ou Red Hat Insights.

Au lieu de procéder à des remédiations automatisées, vous pouvez effectuer les changements manuellement en suivant un rapport généré par OpenSCAP. Pour plus d'informations sur la génération d'un rapport de conformité, voir Analyse de la conformité et des vulnérabilités du système en matière de sécurité.



IMPORTANT

Les remédiations automatisées prennent en charge les systèmes RHEL dans leur configuration par défaut. La configuration du système ayant été modifiée après la mise à niveau, l'exécution des mesures correctives automatisées risque de ne pas rendre le système totalement conforme au profil de sécurité requis. Il se peut que vous deviez corriger certaines exigences manuellement.

L'exemple de procédure suivant permet de renforcer les paramètres de votre système conformément au profil PCI-DSS.

Conditions préalables

- Le paquetage **scap-security-guide** est installé sur votre système RHEL 9.

Procédure

1. Trouvez le fichier de flux de données de conformité à la sécurité approprié **.xml**:

```
$ ls /usr/share/xml/scap/ssg/content/
...
ssg-rhel9-ds.xml
...
```

   Pour plus d'informations, voir la section Afficher les profils de conformité .

2. Remédier au système en fonction du profil sélectionné dans le flux de données approprié :

```
# oscap xccdf eval --profile pci-dss --remediate /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml
```

   Vous pouvez remplacer la valeur **pci-dss** dans l'argument **--profile** par l'ID du profil selon lequel vous souhaitez renforcer votre système. Pour une liste complète des profils pris en charge dans RHEL 9, voir Profils de sécurité SCAP pris en charge dans RHEL .

AVERTISSEMENT

Si elle n'est pas utilisée avec précaution, l'exécution de l'évaluation du système avec l'option **--remediate** activée peut rendre le système non fonctionnel. Red Hat ne fournit aucune méthode automatisée pour annuler les changements effectués par les remédiations de renforcement de la sécurité. Les remédiations sont prises en charge sur les systèmes RHEL dans la configuration par défaut. Si votre système a été modifié après l'installation, l'exécution de la remédiation pourrait ne pas le rendre conforme au profil de sécurité requis.

3. Redémarrez votre système :

```
# reboot
```

Vérification

1. Vérifiez que le système est conforme au profil et enregistrez les résultats dans un fichier HTML :

```
$ oscap xccdf eval --report pcidss_report.html --profile pci-dss
/usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml
```

Ressources supplémentaires

- **scap-security-guide(8)** and **oscap(8)** man pages
- Analyse de la conformité et des vulnérabilités du système en matière de sécurité
- Politique de sécurité de Red Hat Insights
- Politique de sécurité de Red Hat Satellite

8.4. VÉRIFICATION DES POLITIQUES USBGUARD

Avec le cadre logiciel USBGuard, vous pouvez protéger vos systèmes contre les périphériques USB intrusifs en utilisant des listes de périphériques autorisés et interdits basées sur la fonction d'autorisation des périphériques USB dans le noyau.

Conditions préalables

- Vous avez créé un ensemble de règles pour les périphériques USB qui reflète les exigences de votre scénario avant la mise à niveau.
- Le service **usbguard** est installé et fonctionne sur votre système RHEL 9.

Procédure

1. Sauvegardez vos fichiers *.conf stockés dans le répertoire /**etc**/**usbguard**/.
2. Utilisez le site **usbguard generate-policy** pour générer un nouveau fichier de règles. Notez que la commande génère des règles uniquement pour les périphériques USB actuellement présents.
3. Comparer les règles nouvellement générées avec les règles de la politique précédente :
   a. Si vous constatez des différences entre les règles applicables aux dispositifs présents lors de la création de la nouvelle politique et les règles applicables aux mêmes dispositifs avant la mise à niveau, modifiez les règles d'origine en conséquence, y compris pour les dispositifs susceptibles d'être insérés ultérieurement.
   b. S'il n'y a pas de différences entre les règles nouvellement générées et les règles antérieures à la mise à niveau, vous pouvez utiliser les fichiers de stratégie créés dans RHEL 8 sans aucune modification.

Ressources supplémentaires

- Protéger les systèmes contre les dispositifs USB intrusifs .

8.5. MISE À JOUR DES BASES DE DONNÉES FAPOLICYD

Le cadre logiciel **fapolicyd** contrôle l'exécution des applications sur la base d'une politique définie par l'utilisateur.

Dans de rares cas, un problème peut survenir avec le format de la base de données **fapolicyd** trust. Pour reconstruire la base de données :

1. Arrêter le service :

```
# systemctl stop fapolicyd
```

2. Supprimer la base de données :

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

3. Start the service:

```
# systemctl start fapolicyd
```

Si vous avez ajouté des fichiers de confiance personnalisés à la base de données de confiance, mettez-les à jour soit individuellement à l'aide de la commande **fapolicyd-cli -f update *<FILE>*** soit en utilisant la commande **fapolicyd-cli -f update**. Pour appliquer les modifications, utilisez la commande **fapolicyd-cli --update** ou redémarrez le service **fapolicyd**.

En outre, les binaires personnalisés peuvent nécessiter une reconstruction pour la nouvelle version de RHEL. Effectuez ces mises à jour avant de mettre à jour la base de données fapolicyd.

Ressources supplémentaires

- Bloquer et autoriser des applications à l'aide de fapolicyd

8.6. MISE À JOUR DES BASES DE DONNÉES DES SSN DE DBM À SQLITE

De nombreuses applications convertissent automatiquement le format de base de données NSS de DBM à SQLite après avoir défini la variable d'environnement **NSS_DEFAULT_DB_TYPE** à la valeur **sql** sur le système. Vous pouvez vous assurer que toutes les bases de données sont converties en utilisant l'outil **certutil**.

NOTE

Convertissez vos bases de données NSS stockées au format DBM avant de procéder à la mise à niveau vers RHEL 9. En d'autres termes, effectuez les étapes suivantes sur les systèmes RHEL (6, 7 et 8) à partir desquels vous souhaitez procéder à la mise à niveau vers RHEL 9.

Conditions préalables

- Le paquetage **nss-tools** est installé sur votre système.

Procédure

1. Définissez **NSS_DEFAULT_DB_TYPE** sur **sql** dans le système :

```
# export NSS_DEFAULT_DB_TYPE=sql
```

2. Utiliser la commande de conversion dans chaque répertoire[1] rHEL contient des fichiers de base de données NSS au format DBM, par exemple :

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

Notez que vous devez fournir un mot de passe ou un chemin d'accès à un fichier de mots de passe comme valeur de l'option **-f** si votre fichier de base de données est protégé par un mot de passe, par exemple :

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

Ressources supplémentaires

- **certutil(1)** page de manuel.

8.7. MIGRATION DES BASES DE DONNÉES SASL DE CYRUS DU FORMAT BERKELEY DB VERS GDBM

Le paquetage RHEL 9 **cyrus-sasl** est construit sans la dépendance **libdb**, et le plugin **sasldb** utilise le format de base de données GDBM au lieu de Berkeley DB.

Conditions préalables

- Le paquetage **cyrus-sasl-lib** est installé sur votre système.

Procédure

- Pour migrer vos bases de données SASL (Simple Authentication and Security Layer) existantes stockées dans l'ancien format Berkeley DB, utilisez l'outil **cyrusbdb2current** avec la syntaxe suivante :

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

Ressources supplémentaires

- **cyrusbdb2current(1)** page de manuel

[1] RHEL contient une base de données NSS à l'échelle du système dans le répertoire **/etc/pki/nssdb**. Les autres emplacements dépendent des applications que vous utilisez. Par exemple, Libreswan stocke sa base de données dans le répertoire **/etc/ipsec.d/** et Firefox utilise le répertoire **/home/<username>/.mozilla/firefox/**.

CHAPITRE 9. RÉSOLUTION DE PROBLÈMES

Vous pouvez vous référer aux conseils suivants pour résoudre les problèmes de mise à niveau de RHEL 8 vers RHEL 9.

9.1. RESSOURCES DE DÉPANNAGE

Vous pouvez consulter les ressources de dépannage suivantes.

Console output

Par défaut, seuls les messages d'erreur et de niveau critique sont imprimés sur la console par l'utilitaire **Leapp**. Pour modifier le niveau de journalisation, utilisez les options **--verbose** ou **--debug** avec la commande **leapp upgrade**.

- En mode *verbose*, **Leapp** imprime des messages d'information, d'avertissement, d'erreur et critiques.
- En mode *debug*, **Leapp** imprime des messages de débogage, d'information, d'avertissement, d'erreur et de critique.

Logs

- Le fichier **/var/log/leapp/leapp-upgrade.log** répertorie les problèmes rencontrés lors de la phase d'initramfs.
- Le répertoire **/var/log/leapp/dnf-debugdata/** contient les données de débogage des transactions. Ce répertoire n'est présent que si la commande **leapp upgrade** est exécutée avec l'option **--debug**.
- Le site **/var/log/leapp/answerfile** contient des questions auxquelles **Leapp** doit répondre.
- L'utilitaire **journalctl** fournit des journaux complets.

Reports

- Le fichier **/var/log/leapp/leapp-report.txt** répertorie les problèmes détectés lors de la phase de pré-mise à niveau. Le rapport est également disponible dans la console web, voir Évaluer la possibilité de mise à niveau et appliquer des correctifs automatisés via la console web.
- Le fichier **/var/log/leapp/leapp-report.json** répertorie les problèmes trouvés lors de la phase de pré-mise à niveau dans un format lisible par une machine, ce qui vous permet de traiter le rapport à l'aide de scripts personnalisés. Pour plus d'informations, voir Automatiser le flux de travail de votre rapport de pré-mise à niveau de Red Hat Enterprise Linux.

9.2. CONSEILS DE DÉPANNAGE

Vous pouvez vous référer aux conseils de dépannage suivants.

Pre-upgrade phase

- Vérifiez que votre système remplit toutes les conditions énumérées dans la section Planification d'une mise à niveau.

- Assurez-vous d'avoir suivi toutes les étapes décrites dans la section Préparation de la mise à niveau - par exemple, votre système n'utilise pas plus d'une carte d'interface réseau (NIC) dont le nom est basé sur le préfixe utilisé par le noyau (**eth**).

- Assurez-vous d'avoir répondu à toutes les questions posées par **Leapp** dans le fichier **/var/log/leapp/answerfile**. Si des réponses manquent, **Leapp** bloque la mise à niveau. Par exemple :

  - Le système ne comporte-t-il aucun dispositif VDO ?

- Assurez-vous d'avoir résolu tous les problèmes identifiés dans le rapport de pré-mise à niveau, situé à l'adresse **/var/log/leapp/leapp-report.txt**. Pour ce faire, vous pouvez également utiliser la console web, comme décrit dans la section Évaluer la possibilité de mise à niveau et appliquer des mesures correctives automatisées via la console web.

Exemple 9.1. Fichier de réponses Leapp

Voici un exemple de fichier **/var/log/leapp/answerfile** non édité qui comporte une question sans réponse :

```
[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 =
```

Le champ **Label** précise la question à laquelle il faut répondre. Dans cet exemple, la question est **Are all VDO devices, if any, successfully converted to LVM management?**

Pour répondre à la question, décommentez la dernière ligne et entrez une réponse de **True** ou **False**. Dans cet exemple, la réponse sélectionnée est **True**:

```
[check_vdo]
...
```

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

Download phase

- Si un problème survient lors du téléchargement des paquets RPM, examinez les données de débogage des transactions situées dans le répertoire **/var/log/leapp/dnf-debugdata/**.

NOTE

Le répertoire **/var/log/leapp/dnf-debugdata/** est vide ou n'existe pas si aucune donnée de débogage de transaction n'a été produite. Cela peut se produire lorsque les référentiels requis ne sont pas disponibles.

Initramfs phase

- Au cours de cette phase, les défaillances potentielles vous redirigent vers l'interpréteur de commandes Dracut. Consultez le journal :

```
# journalctl
```

Sinon, redémarrez le système à partir de l'interpréteur de commandes Dracut en utilisant la commande **reboot** et vérifiez le fichier **/var/log/leapp/leapp-upgrade.log**.

Post-upgrade phase

- Si votre système semble avoir été mis à niveau avec succès mais démarre avec l'ancien noyau RHEL 8, redémarrez le système et vérifiez la version du noyau de l'entrée par défaut dans GRUB.
- Assurez-vous d'avoir suivi les étapes recommandées dans la section Vérification de l'état post-mise à niveau du système RHEL 9.
- Si votre application ou un service cesse de fonctionner ou se comporte de manière incorrecte après que vous avez mis SELinux en mode d'application, recherchez les dénis à l'aide de la commande **ausearch**, **journalctl**ou **dmesg** pour rechercher les refus :

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

Les problèmes les plus courants sont dus à un étiquetage incorrect. Pour plus de détails, voir Résolution des problèmes liés à SELinux.

9.3. PROBLÈMES CONNUS

Voici les problèmes connus que vous pouvez rencontrer lors de la mise à niveau de RHEL 8 vers RHEL 9.

- Actuellement, le teaming réseau ne fonctionne pas lorsque la mise à niveau en place est effectuée alors que Network Manager est désactivé ou non installé.
- Si vous utilisez un proxy HTTP, le Gestionnaire d'abonnement Red Hat doit être configuré pour

utiliser un tel proxy, ou la commande **subscription-manager** doit être exécutée avec l'option **--proxy <hostname>**. Dans le cas contraire, l'exécution de la commande **subscription-manager** échoue. Si vous utilisez l'option **--proxy** au lieu du changement de configuration, le processus de mise à niveau échoue car **Leapp** n'est pas en mesure de détecter le proxy. Pour éviter que ce problème ne se produise, modifiez manuellement le fichier **rhsm.conf** comme décrit dans Comment configurer le proxy HTTP pour Red Hat Subscription Management . (BZ#1689294)

- Si votre système RHEL 8 utilise un pilote de périphérique fourni par Red Hat mais qui n'est pas disponible dans RHEL 9, **Leapp** empêche la mise à niveau. Cependant, si le système RHEL 8 utilise un pilote de périphérique tiers pour lequel **Leapp** n'a pas de données dans le fichier **/etc/leapp/files/device_driver_deprecation_data.json**, **Leapp** ne détecte pas un tel pilote et procède à la mise à niveau. Par conséquent, le système risque de ne pas démarrer après la mise à niveau.

- Si le nom d'un paquetage tiers (non signé par Red Hat) installé sur votre système est le même que le nom d'un paquetage fourni par Red Hat, la mise à niveau sur place échoue. Pour contourner ce problème, choisissez l'une des options suivantes avant de procéder à la mise à niveau :

  a. Supprimer le paquet tiers

  b. Remplacez le paquetage tiers par le paquetage fourni par Red Hat

- Dans RHEL 8, vous pouvez gérer les volumes Virtual Data Optimizer (VDO) à l'aide du gestionnaire VDO ou du Logical Volume Manager (LVM). Dans RHEL 9, il n'est possible de gérer les volumes VDO qu'à l'aide de LVM. Pour continuer à utiliser des volumes gérés par VDO sur RHEL 9, importez ces volumes en volumes VDO gérés par LVM avant la mise à niveau. Pour plus d'informations, voir Importation de volumes VDO existants vers LVM .

- La mise à niveau en place échoue sur les systèmes dotés d'une matrice redondante de disques indépendants (RAID). (BZ#1957192)

- Au cours de la mise à niveau en place, l'utilitaire **Leapp** préserve généralement les noms des contrôleurs d'interface réseau (NIC) entre RHEL 8 et RHEL 9. Toutefois, sur certains systèmes, tels que les systèmes avec liaison réseau, les noms des NIC peuvent devoir être mis à jour entre RHEL 8 et RHEL 9. Sur ces systèmes, effectuez les étapes suivantes :

  a. Définissez la variable d'environnement **LEAPP_NO_NETWORK_RENAMING=1** pour empêcher l'utilitaire Leapp de préserver de manière incorrecte les noms originaux des cartes réseau de RHEL 8.

  b. Effectuer la mise à niveau en place.

  c. Vérifiez que votre réseau fonctionne correctement. Si nécessaire, mettez à jour manuellement la configuration du réseau.
  (BZ#1919382)

- La mise à niveau en place peut échouer si l'espace disque disponible est insuffisant. Les messages d'erreur et les journaux peuvent contenir des informations trompeuses ou invalides sur le problème et sa résolution. Pour résoudre ce problème, consultez la solution de la base de connaissances Leapp fails with "There is not enough space on the file system hosting /var/lib/leapp directory to extract the packages" (Il n'y a pas assez d'espace sur le système de fichiers hébergeant le répertoire /var/lib/leapp pour extraire les paquets). (BZ#1832730, BZ#2210300)

- Si votre système démarre à l'aide du BIOS, la mise à niveau sur place échoue lors de la mise à niveau du chargeur d'amorçage GRUB2 si la zone d'intégration du disque de démarrage ne

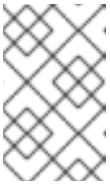
contient pas suffisamment d'espace pour l'installation de l'image de base. Ce problème peut se produire lorsque le disque a été partitionné manuellement, par exemple à l'aide de l'utilitaire RHEL 6 **fdisk**. Pour vérifier si ce problème vous concerne, procédez comme suit :

a. Déterminez quel secteur démarre la première partition sur le disque avec le chargeur de démarrage installé :

```
# fdisk -l
```

Le partitionnement standard, qui garantit suffisamment d'espace pour l'image de base, commence au secteur 2048.

b. Déterminez si le secteur de départ offre suffisamment d'espace. L'image de base de RHEL 9.0 nécessite au moins 36 KiB. Par exemple, si la taille du secteur est la taille standard de 512 octets, le fait de commencer sur le secteur 73 ou inférieur n'offrira pas suffisamment d'espace.



NOTE

L'image du noyau RHEL 9 peut être plus grande que 36 KiB et nécessiter un secteur de départ plus élevé. Vérifiez toujours l'espace requis par le noyau RHEL 9 actuel.

c. Si la zone d'intégration ne contient pas suffisamment d'espace de stockage, procédez à une nouvelle installation du système RHEL 9 au lieu d'effectuer une mise à niveau sur place. (BZ#2181380)

- Après la mise à niveau en place, les clés SSH ne sont plus générées automatiquement si le système remplit les conditions suivantes :
  - Le système est sur un nuage.
  - Le paquetage cloud-init est installé.
  - La configuration de ssh_genkeytypes est fixée à ~ dans le fichier /etc/cloud/cloud.cfg, ce qui est la valeur par défaut.
    Ce problème empêche le système de se connecter en utilisant SSH si les clés d'origine ont été supprimées. Pour éviter ce problème, consultez la solution de la base de connaissances Unable to SSH to new Virtual Machine after upgrading the template to RHEL 8.7 or 9 . (BZ#2210012)

9.4. OBTENIR UN SOUTIEN

Pour ouvrir un dossier d'assistance, sélectionnez *RHEL 8* comme produit et fournissez une adresse **sosreport** de votre système.

- Pour générer un site **sosreport** sur votre système, exécutez la commande suivante :

```
# sosreport
```

Notez que vous pouvez laisser l'identifiant du cas vide.

Pour plus de détails sur la génération d'un rapport sos, consultez la solution Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

Pour plus d'informations sur l'ouverture et la gestion d'un dossier d'assistance sur le portail client, voir l'article Comment ouvrir et gérer un dossier d'assistance sur le portail client ?

CHAPITRE 10. INFORMATIONS CONNEXES

Vous pouvez vous référer au matériel pédagogique suivant :

- Capacités et limites de la technologie Red Hat Enterprise Linux
- Chemins de mise à niveau en place pris en charge pour Red Hat Enterprise Linux
- Considérations relatives à l'adoption de RHEL 9
- Personnalisation de la mise à niveau en place de Red Hat Enterprise Linux
- Automatiser le flux de travail du rapport de pré-mise à niveau de Red Hat Enterprise Linux
- Utilisation de systèmes de gestion de la configuration pour automatiser certaines parties du processus de pré-mise à niveau et de mise à niveau de Leapp sur Red Hat Enterprise Linux
- Leapp utility metadata in-place upgrades of RHEL for disconnected upgrades (métadonnées de l'utilitaire Leapp)
- Mise à niveau de RHEL 7 vers RHEL 8
- Conversion d'une distribution Linux basée sur RPM vers RHEL
- Comment mettre à niveau les environnements SAP de RHEL 8 à RHEL 9 ?
- Documentation Red Hat Insights

ANNEXE A. DÉPÔTS RHEL 8

Avant la mise à niveau, assurez-vous que les référentiels appropriés sont activés, comme décrit à l'étape 4 de la procédure de préparation d'un système RHEL 8 pour la mise à niveau .

Si vous prévoyez d'utiliser le Gestionnaire d'abonnements Red Hat pendant la mise à niveau, vous devez **must enable** les dépôts suivants avant la mise à niveau à l'aide de la commande **subscription-manager repos --enable *repository_id*** avant la mise à niveau :

Tableau A.1. Dépôts RHEL 8

Architecture	Référentiel	ID du référentiel
64-bit Intel et AMD	Base	**rhel-8-for-x86_64-baseos-rpms**
	AppStream	**rhel-8-for-x86_64-appstream-rpms**
aRM 64 bits	Base	**rhel-8-for-aarch64-baseos-rpms**
	Extras	**rhel-8-for-aarch64-appstream-rpms**
IBM POWER (petit endian)	Base	**rhel-8-for-ppc64le-baseos-rpms**
	AppStream	**rhel-8-for-ppc64le-appstream-rpmss**
IBM Z	Base	**rhel-8-for-s390x-baseos-rpms**
	AppStream	**rhel-8-for-s390x-appstream-rpms**

Vous **can enable** les dépôts suivants avant la mise à niveau en utilisant la commande **subscription-manager repos --enable *repository_id*** avant la mise à niveau :

Tableau A.2. Dépôts volontaires RHEL 8

Architecture	Référentiel	ID du référentiel
64-bit Intel et AMD	Code Ready Linux Builder	**codeready-builder-for-rhel-8-x86_64-rpms**
	Supplémentaire	**rhel-8-for-x86_64-supplementary-rpms**
aRM 64 bits	Code Ready Linux Builder	**codeready-builder-for-rhel-8-aarch64-rpms**
	Supplémentaire	**rhel-8-for-aarch64-supplementary-rpms**
IBM POWER (petit endian)	Code Ready Linux Builder	**codeready-builder-for-rhel-8-ppc64le-rpms**

Architecture	Référentiel	ID du référentiel
	Supplémentaire	**rhel-8-for-ppc64le-supplementary-rpms**
IBM Z	Code Ready Linux Builder	**codeready-builder-for-rhel-8-s390x-rpms**
	Supplémentaire	**rhel-8-for-s390x-supplementary-rpms**

NOTE

Si vous avez activé un Linux Builder RHEL 8 Code Ready ou un référentiel RHEL 8 Supplementary avant une mise à niveau sur site, **Leapp** active le Linux Builder RHEL 8 CodeReady ou les référentiels RHEL 8 Supplementary, respectivement. Pour plus d'informations, voir le manifeste des paquets.

Si vous décidez d'utiliser des référentiels personnalisés, activez-les en suivant les instructions de la section Configuration des référentiels personnalisés.

ANNEXE B. DÉPÔTS RHEL 9

Si votre système est enregistré auprès du Red Hat Content Delivery Network (CDN) à l'aide du Red Hat Subscription Manager (RHSM), les référentiels RHEL 9 sont automatiquement activés lors de la mise à niveau en place. Cependant, sur les systèmes enregistrés auprès de Red Hat Satellite à l'aide du RHSM, vous devez activer et synchroniser manuellement les référentiels RHEL 8 et RHEL 9 avant d'exécuter le rapport de pré-mise à niveau.

NOTE

Veillez à activer la version du système d'exploitation cible de chaque référentiel, par exemple 9.0. Si vous n'avez activé que la version RHEL 9 des référentiels, la mise à niveau en place est inhibée.

Si vous prévoyez d'utiliser Red Hat Satellite pendant la mise à niveau, vous devez vous rendre sur le site **must enable and synchronize** pour consulter au moins les référentiels RHEL 9 suivants avant la mise à niveau, en utilisant l'interface Web Satellite ou les commandes **hammer repository-set enable** et **hammer product synchronize**:

Tableau B.1. Dépôts RHEL 9

Architecture	Référentiel	ID du référentiel	Nom du référentiel	Version de lancement
64-bit Intel et AMD	BaseOS	**rhel-9-for-x86_64-baseos-rpms**	Red Hat Enterprise Linux 9 pour x86_64 - BaseOS (RPMs)	x86_64 *<target_os_version>*
	AppStream	**rhel-9-for-x86_64-appstream-rpms**	Red Hat Enterprise Linux 9 pour x86_64 - AppStream (RPMs)	x86_64 *<target_os_version>*
aRM 64 bits	BaseOS	**rhel-9-for-aarch64-baseos-rpms**	Red Hat Enterprise Linux 9 pour ARM 64 - BaseOS (RPMs)	aarch64 *<target_os_version>*
	AppStream	**rhel-9-for-aarch64-appstream-rpms**	Red Hat Enterprise Linux 9 pour ARM 64 - AppStream (RPMs)	aarch64 *<target_os_version>*
IBM Power (little endian)	BaseOS	**rhel-9-for-ppc64le-baseos-rpms**	Red Hat Enterprise Linux 9 for Power, little endian - BaseOS (RPMs)	ppc64le *<target_os_version>*

Architecture	Référentiel	ID du référentiel	Nom du référentiel	Version de lancement
	AppStream	**rhel-9-for-ppc64le-appstream-rpms**	Red Hat Enterprise Linux 9 pour Power, little endian - AppStream (RPMs)	ppc64le <*target_os_version*>
IBM Z	BaseOS	**rhel-9-for-s390x-baseos-rpms**	Red Hat Enterprise Linux 9 pour les systèmes IBM z - BaseOS (RPMs)	s390x <*target_os_version*>
	AppStream	**rhel-9-for-s390x-appstream-rpms**	Red Hat Enterprise Linux 9 pour les systèmes IBM z - AppStream (RPMs)	s390x <*target_os_version*>

Remplacez <*target_os_version*> par la version du système d'exploitation cible, par exemple **9.0**.