Red Hat Enterprise Linux 9

9.0 Notes de mise à jour

Notes de mise à jour pour Red Hat Enterprise Linux 9.0

Last Updated: 2023-06-12

Red Hat Enterprise Linux 9 9.0 Notes de mise à jour

Notes de mise à jour pour Red Hat Enterprise Linux 9.0

Notice légale

Résumé

Les notes de mise à jour fournissent une couverture de haut niveau des améliorations et des ajouts qui ont été mis en œuvre dans Red Hat Enterprise Linux 9.0 et documentent les problèmes connus dans cette version, ainsi que les corrections de bogues notables, les aperçus technologiques, les fonctionnalités obsolètes et d'autres détails.

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**.

CHAPITRE 1. VUE D'ENSEMBLE

1.1. PRINCIPAUX CHANGEMENTS DANS RHEL 9.0

Sécurité

L'utilisation du condensé de message **SHA-1** à des fins cryptographiques a été supprimée dans RHEL 9. Le condensé produit par SHA-1 n'est pas considéré comme sûr en raison des nombreuses attaques réussies documentées basées sur la recherche de collisions de hachage. Les composants cryptographiques de base de RHEL ne créent plus de signatures à l'aide de SHA-1 par défaut. Les applications de RHEL 9 ont été mises à jour pour éviter d'utiliser SHA-1 dans les cas d'utilisation liés à la sécurité.

Parmi les exceptions, le code d'authentification des messages HMAC-SHA1 et les valeurs UUID (Universal Unique Identifier) peuvent encore être créés à l'aide de SHA-1, car ces cas d'utilisation ne présentent actuellement aucun risque pour la sécurité. SHA-1 peut également être utilisé dans des cas limités liés à d'importants problèmes d'interopérabilité et de compatibilité, tels que Kerberos et WPA-2. Pour plus de détails, consultez la section Liste des applications RHEL utilisant une cryptographie non conforme à la norme FIPS 140-3.

Pour résoudre les problèmes de compatibilité avec les systèmes qui requièrent encore SHA-1, voir les articles KCS suivants :

- SSH ne fonctionne pas entre les systèmes RHEL 9 et RHEL 6
- Les paquets signés avec SHA-1 ne peuvent pas être installés ou mis à niveau
- Échec de la connexion avec les serveurs et clients SSH qui ne prennent pas en charge l'extension "server-sig-algs"

OpenSSL est désormais disponible dans la version 3.0.1, qui ajoute un concept de fournisseur, un nouveau schéma de version, un client HTTP(S) amélioré, la prise en charge de nouveaux protocoles, formats et algorithmes, ainsi que de nombreuses autres améliorations.

Le site **cryptographic policies** a été ajusté pour fournir des valeurs par défaut actualisées et sécurisées.

OpenSSH est distribué dans la version 8.7p1, qui apporte de nombreuses améliorations, des corrections de bogues et des améliorations de sécurité par rapport à la version 8.0p1, qui est distribuée dans RHEL 8.5.

Le protocole SFTP remplace le protocole SCP/RCP précédemment utilisé dans **OpenSSH**. SFTP offre une gestion plus prévisible des noms de fichiers et ne nécessite pas l'expansion des motifs **glob(3)** par l'interpréteur de commandes du côté distant.

SELinux les performances de SELinux ont été considérablement améliorées, notamment en ce qui concerne le temps de chargement de la politique SELinux dans le noyau, la surcharge de mémoire et d'autres paramètres. Pour plus d'informations, voir l'article du blog Improving the performance and space efficiency of SELinux.

RHEL 9 fournit le cadre **fapolicyd** dans la version 1.1 en amont. Entre autres améliorations, vous pouvez désormais utiliser les nouveaux répertoires **rules.d/** et **trust.d/**, le script **fagenrules** et de nouvelles options pour la commande **fapolicyd-cli**.

Les paquets du guide de sécurité SCAP (SSG) sont fournis dans la version 0.1.60, qui introduit l'adaptation delta, la mise à jour des profils de sécurité et d'autres améliorations.

Voir Section 4.7, « Sécurité » pour plus d'informations.

L'utilisation de SHA-1 pour les signatures est restreinte dans la politique cryptographique DEFAULT. À l'exception de HMAC, SHA-1 n'est plus autorisé dans les protocoles TLS, DTLS, SSH, IKEv2, DNSSEC et Kerberos.

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**. Notez que **LEGACY** active également de nombreux autres algorithmes qui ne sont pas sécurisés.

Cyrus SASL utilise désormais GDBM au lieu de Berkeley DB, et les bibliothèques Network Security Services (NSS) ne prennent plus en charge le format de fichier DBM pour la base de données de confiance.

La prise en charge de la désactivation de SELinux par l'option **SELINUX=disabled** du fichier **/etc/selinux/config** a été supprimée du noyau. Lorsque vous désactivez SELinux uniquement via **/etc/selinux/config**, le système démarre avec SELinux activé mais sans politique chargée. Si votre scénario nécessite la désactivation de SELinux, ajoutez le paramètre **selinux=0** à votre ligne de commande du noyau.

Voir la section Sécurité du document *Considerations in adopting RHEL 9* pour plus d'informations sur les différences majeures liées à la sécurité entre RHEL 9 et RHEL 8.

Mise en réseau

Vous pouvez utiliser le nouveau démon MultiPath TCP (mptcpd) pour configurer les points d'extrémité MultiPath TCP (MPTCP) sans utiliser l'utilitaire **iproute2**. Pour rendre les sous-flux MPTCP et les points d'extrémité persistants, utilisez un script de distribution NetworkManager.

Par défaut, NetworkManager utilise désormais les fichiers clés pour stocker les nouveaux profils de connexion. Notez que le format **ifcfg** est toujours pris en charge.

Pour plus d'informations sur les fonctionnalités introduites dans cette version et les modifications apportées aux fonctionnalités existantes, voir la section Nouvelles fonctionnalités - Mise en réseau .

La technologie WireGuard VPN est maintenant disponible en tant qu'aperçu technologique non supporté. Pour plus de détails, voir Aperçus technologiques - Réseau .

Le service **teamd** et la bibliothèque **libteam** sont obsolètes. En remplacement, configurez un lien au lieu d'une équipe réseau.

Les paquets **iptables-nft** et **ipset** sont obsolètes. Ces paquets comprennent des utilitaires, tels que **iptables**, **ip6tables**, **ebtables** et **arptables**. Utilisez le cadre **nftables** pour configurer les règles de pare-feu.

Pour plus d'informations sur les fonctionnalités obsolètes, voir Fonctionnalité obsolète - Mise en réseau .

Le paquet **network-scripts** a été supprimé. Utilisez NetworkManager pour configurer les connexions réseau. Pour plus d'informations sur les fonctionnalités qui ne font plus partie de RHEL, voir la section Networking dans le document *Considerations in adopting RHEL 9* .

Langages de programmation dynamiques, serveurs web et de base de données

RHEL 9.0 propose les langages de programmation dynamique suivants :

- Node.js 16

- **Perl 5.32**
- **PHP 8.0**
- **Python 3.9**
- **Ruby 3.0**

RHEL 9.0 inclut les systèmes de contrôle de version suivants :

- **Git 2.31**
- **Subversion 1.14**

Les serveurs web suivants sont distribués avec RHEL 9.0 :

- **Apache HTTP Server 2.4.51**
- **nginx 1.20**

Les serveurs proxy de mise en cache suivants sont disponibles :

- **Varnish Cache 6.6**
- **Squid 5.2**

RHEL 9.0 propose les serveurs de base de données suivants :

- **MariaDB 10.5**
- **MySQL 8.0**
- **PostgreSQL 13**
- **Redis 6.2**

Voir Section 4.13, « Langages de programmation dynamiques, serveurs web et de base de données » pour plus d'informations.

Compilateurs et outils de développement

Chaîne d'outils du système

Les composants suivants de la chaîne d'outils système sont disponibles avec RHEL 9.0 :

- **GCC 11.2.1**
- **glibc 2.34**
- **binutils 2.35.2**

Les composants de la chaîne d'outils système RHEL 9 incluent la prise en charge de POWER10.

Outils de performance et débogueurs

Les outils de performance et les débogueurs suivants sont disponibles avec RHEL 9.0 :

- **GDB 10.2**
- **Valgrind 3.18.1**

- **SystemTap 4.6**
- **Dyninst 11.0.0**
- **elfutils 0.186**

Outils de contrôle des performances
Les outils de surveillance des performances suivants sont disponibles avec RHEL 9.0 :

- **PCP 5.3.5**
- **Grafana 7.5.11**

Outils de compilation
Les compilateurs suivants sont disponibles avec RHEL 9.0 :

- **LLVM Toolset 13.0.1**
- **Rust Toolset 1.58.1**
- **Go Toolset 1.17.7**

Pour plus de détails sur les changements, voir Section 4.14, « Compilateurs et outils de développement ».

Implémentations Java dans RHEL 9
Le référentiel RHEL 9 AppStream comprend :

- Les paquets **java-17-openjdk**, qui fournissent l'environnement d'exécution Java OpenJDK 17 et le kit de développement logiciel Java OpenJDK 17.
- Les paquets **java-11-openjdk**, qui fournissent l'environnement d'exécution Java OpenJDK 11 et le kit de développement logiciel Java OpenJDK 11.
- Les paquets **java-1.8.0-openjdk**, qui fournissent l'environnement d'exécution Java OpenJDK 8 et le kit de développement logiciel Java OpenJDK 8.

Pour plus d'informations, voir la documentation OpenJDK.

Outils Java
Les outils Java suivants sont disponibles avec RHEL 9.0 :

- **Maven 3.6**
- **Ant 1.10**

Voir Section 4.14, « Compilateurs et outils de développement » pour plus d'informations.

Bureau

L'environnement GNOME a été mis à jour de GNOME 3.28 à GNOME 40 avec de nombreuses nouvelles fonctionnalités.

Le serveur d'affichage **X.org** est obsolète et sera supprimé dans une prochaine version majeure de RHEL. La session de bureau par défaut est désormais la session **Wayland** dans la plupart des cas.

Lors de l'utilisation des pilotes NVIDIA, la session de bureau sélectionne désormais le protocole d'affichage Wayland par défaut, si la configuration du pilote prend en charge Wayland. Dans les versions précédentes de RHEL, les pilotes NVIDIA désactivaient toujours Wayland.

Le service **PipeWire** gère désormais toutes les entrées et sorties audio. **PipeWire** remplace le service **PulseAudio** dans les cas d'utilisation générale et le service **JACK** dans les cas d'utilisation professionnelle.

Voir Section 4.16, « Bureau » pour plus d'informations.

Virtualisation

Dans RHEL 9, la bibliothèque **libvirt** utilise des démons modulaires qui gèrent des ensembles de pilotes de virtualisation individuels sur votre hôte. Cela permet d'affiner une variété de tâches impliquant des pilotes de virtualisation, telles que l'optimisation de la charge des ressources et la surveillance.

L'émulateur QEMU est désormais construit à l'aide du compilateur Clang. Cela permet à l'hyperviseur KVM de RHEL 9 d'utiliser un certain nombre de fonctions de sécurité et de débogage avancées. L'une de ces fonctionnalités est SafeStack, qui rend les machines virtuelles (VM) hébergées sur RHEL 9 nettement plus sûres contre les attaques basées sur la programmation orientée retour (Return-Oriented Programming, ROP).

En outre, le module de plate-forme virtuelle de confiance (vTPM) est désormais entièrement pris en charge. Grâce à vTPM, vous pouvez ajouter un crypto-processeur virtuel TPM à une VM, qui peut alors être utilisé pour générer, stocker et gérer des clés cryptographiques.

Enfin, la fonction **virtiofs** a été mise en œuvre. Elle permet de partager plus efficacement des fichiers entre un hôte RHEL 9 et ses machines virtuelles.

Pour plus d'informations sur les fonctionnalités de virtualisation introduites dans cette version, voir Section 4.20, « Virtualisation ».

1.2. MISE À NIVEAU SUR PLACE

Mise à niveau en place de RHEL 8 à RHEL 9

- De RHEL 8.6 à RHEL 9.0 sur les architectures suivantes :
  - 64-bit Intel
  - 64-bit AMD
  - aRM 64 bits
  - IBM POWER 9 (little endian)
  - Architectures IBM Z, à l'exception de z13
- De RHEL 8.6 à RHEL 9.0 sur des systèmes avec SAP HANA

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

Pour obtenir des instructions sur l'exécution d'une mise à niveau en place, voir Mise à niveau de RHEL 8 vers RHEL 9.

Pour obtenir des instructions sur l'exécution d'une mise à niveau en place sur des systèmes dotés d'environnements SAP, voir Comment mettre à niveau en place des environnements SAP de RHEL 8 à RHEL 9.

Mise à niveau en place de RHEL 7 à RHEL 9

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 .

1.3. PORTAIL CLIENTS DE RED HAT

Red Hat Customer Portal Labs est un ensemble d'outils dans une section du portail client disponible sur https://access.redhat.com/labs/. Les applications de Red Hat Customer Portal Labs peuvent vous aider à améliorer les performances, à résoudre rapidement les problèmes, à identifier les problèmes de sécurité et à déployer et configurer rapidement des applications complexes. Certaines des applications les plus populaires sont :

- Assistant d'inscription
- Générateur de démarrage
- Certificats de produits Red Hat
- Red Hat CVE Checker
- Analyseur d'erreurs du noyau
- Red Hat Code Browser
- Configurateur VNC
- Graphique de mise à jour de la plateforme de conteneurs Red Hat OpenShift
- Aide à la mise à niveau de Red Hat Satellite
- Outil de configuration des options de la JVM
- Outil de configuration de l'équilibreur de charge
- Red Hat OpenShift Data Foundation Supportability and Interoperability Checker (vérificateur de supportabilité et d'interopérabilité de Red Hat OpenShift Data Foundation)
- Assistant de mise à niveau de la plateforme d'automatisation Ansible
- Calculateur de groupes de placement de céphales (PG) par pool

1.4. RESSOURCES SUPPLÉMENTAIRES

Capabilities and limits de Red Hat Enterprise Linux 9 par rapport à d'autres versions du système sont disponibles dans l'article de la base de connaissances Capacités et limites de la technologie Red Hat Enterprise Linux.

Les informations relatives à Red Hat Enterprise Linux **life cycle** sont fournies dans le document Red Hat Enterprise Linux Life Cycle.

Le document Package manifest fournit une adresse **package listing** pour RHEL 9, y compris les licences et les niveaux de compatibilité des applications.

Application compatibility levels sont expliquées dans le document Red Hat Enterprise Linux 9 : Guide de compatibilité des applications.

Les principaux sites **differences between RHEL 8 and RHEL 9**, y compris les fonctionnalités supprimées, sont documentés dans le document Considerations in adopting RHEL 9 (considérations relatives à l'adoption de RHEL 9).

Le document Upgrading from RHEL 8 to RHEL 9 fournit des instructions sur la manière d'effectuer un **in-place upgrade from RHEL 8 to RHEL 9**.

Le service **Red Hat Insights**, qui vous permet d'identifier, d'examiner et de résoudre de manière proactive les problèmes techniques connus, est disponible avec tous les abonnements RHEL. Pour obtenir des instructions sur l'installation du client Red Hat Insights et l'enregistrement de votre système au service, consultez la page Red Hat Insights Get Started .

CHAPITRE 2. ARCHITECTURES

Red Hat Enterprise Linux 9.0 est distribué avec la version 5.14.0 du noyau, qui prend en charge les architectures suivantes à la version minimale requise :

- Architectures AMD et Intel 64 bits (x86-64-v2)
- L'architecture ARM 64 bits (ARMv8.0-A)
- IBM Power Systems, Little Endian (POWER9)
- 64 bits IBM Z (z14)

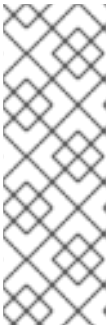
Assurez-vous d'acheter l'abonnement approprié pour chaque architecture. Pour plus d'informations, voir Démarrer avec Red Hat Enterprise Linux - architectures supplémentaires .

CHAPITRE 3. DISTRIBUTION DU CONTENU DANS RHEL 9

3.1. INSTALLATION

Red Hat Enterprise Linux 9 est installé à l'aide d'images ISO. Deux types d'images ISO sont disponibles pour les architectures AMD64, Intel 64 bits, ARM 64 bits, IBM Power Systems et IBM Z :

- ISO d'installation : une image d'installation complète qui contient les référentiels BaseOS et AppStream et vous permet de terminer l'installation sans référentiels supplémentaires. Sur la page Téléchargements de produits , le site **Installation ISO** est appelé **Binary DVD**.



NOTE

L'image ISO d'installation est d'une taille de plusieurs Go et, par conséquent, elle peut ne pas être compatible avec les formats de supports optiques. Il est recommandé d'utiliser une clé USB ou un disque dur USB lors de l'utilisation de l'image ISO d'installation pour créer un support d'installation amorçable. Vous pouvez également utiliser l'outil Image Builder pour créer des images RHEL personnalisées. Pour plus d'informations sur Image Builder, consultez le document *Composing a customized RHEL system image* document.

- ISO de démarrage : une image ISO de démarrage minimale qui est utilisée pour démarrer le programme d'installation. Cette option nécessite l'accès aux référentiels BaseOS et AppStream pour l'installation des logiciels. Les référentiels font partie de l'image ISO d'installation. Vous pouvez également vous enregistrer auprès de Red Hat CDN ou Satellite pendant l'installation afin d'utiliser les derniers contenus BaseOS et AppStream de Red Hat CDN ou Satellite.

Consultez le document Exécution d'une installation RHEL 9 standard pour obtenir des instructions sur le téléchargement d'images ISO, la création de supports d'installation et l'achèvement d'une installation RHEL. Pour les installations Kickstart automatisées et d'autres sujets avancés, voir le document Exécution d'une installation RHEL 9 avancée .

3.2. RÉFÉRENTIELS

Red Hat Enterprise Linux 9 est distribué par le biais de deux dépôts principaux :

- BaseOS
- AppStream

Ces deux dépôts sont nécessaires pour une installation RHEL de base et sont disponibles avec tous les abonnements RHEL.

Le contenu du référentiel BaseOS est destiné à fournir l'ensemble des fonctionnalités du système d'exploitation sous-jacent qui constitue la base de toutes les installations. Ce contenu est disponible au format RPM et est soumis à des conditions de support similaires à celles des versions précédentes de RHEL. Pour plus d'informations, voir le document Scope of Coverage Details.

Le contenu du référentiel AppStream comprend des applications supplémentaires pour l'espace utilisateur, des langages d'exécution et des bases de données afin de prendre en charge les différentes charges de travail et les différents cas d'utilisation.

En outre, le référentiel CodeReady Linux Builder est disponible avec tous les abonnements RHEL. Il fournit des paquets supplémentaires à l'usage des développeurs. Les paquets inclus dans le dépôt CodeReady Linux Builder ne sont pas pris en charge.

Pour plus d'informations sur les dépôts RHEL 9 et les paquets qu'ils fournissent, voir le manifeste des paquets.

3.3. FLUX D'APPLICATIONS

Les versions multiples des composants de l'espace utilisateur sont fournies sous forme de flux d'applications et mises à jour plus fréquemment que les paquets du système d'exploitation principal. Cela offre une plus grande flexibilité pour personnaliser RHEL sans impacter la stabilité sous-jacente de la plateforme ou des déploiements spécifiques.

Les flux d'applications sont disponibles dans le format RPM habituel, en tant qu'extension du format RPM appelée modules, en tant que collections de logiciels ou en tant que Flatpaks.

Chaque composant Application Stream a un cycle de vie donné, soit identique à celui de RHEL 9, soit plus court. Pour plus d'informations sur le cycle de vie de RHEL, voir Red Hat Enterprise Linux Life Cycle.

RHEL 9 améliore l'expérience des flux d'applications en fournissant des versions initiales des flux d'applications qui peuvent être installées en tant que paquets RPM à l'aide de la commande traditionnelle **dnf install**.

NOTE

Certains flux d'applications initiaux au format RPM ont un cycle de vie plus court que Red Hat Enterprise Linux 9.

Certaines versions supplémentaires d'Application Stream seront distribuées sous forme de modules avec un cycle de vie plus court dans les prochaines versions mineures de RHEL 9. Les modules sont des ensembles de paquets représentant une unité logique : une application, une pile de langues, une base de données ou un ensemble d'outils. Ces paquets sont construits, testés et publiés ensemble.

Déterminez toujours la version d'un flux d'applications que vous souhaitez installer et assurez-vous de consulter d'abord le cycle de vie du flux d'applications de Red Hat Enterprise Linux .

Les contenus nécessitant une mise à jour rapide, tels que les compilateurs alternatifs et les outils de conteneur, sont disponibles dans des flux continus qui ne fourniront pas de versions alternatives en parallèle. Les flux roulants peuvent être conditionnés sous forme de RPM ou de modules.

Pour obtenir des informations sur les flux d'applications disponibles dans RHEL 9 et leur niveau de compatibilité avec les applications, consultez le manifeste du paquetage. Les niveaux de compatibilité des applications sont expliqués dans le document Red Hat Enterprise Linux 9 : Guide de compatibilité des applications.

3.4. GESTION DES PAQUETS AVEC YUM/DNF

Dans Red Hat Enterprise Linux 9, l'installation du logiciel est assurée par **DNF**. Red Hat continue à soutenir l'utilisation du terme **yum** par souci de cohérence avec les versions majeures précédentes de RHEL. Si vous tapez **dnf** au lieu de **yum**, la commande fonctionne comme prévu car il s'agit dans les deux cas d'alias de compatibilité.

Bien que RHEL 8 et RHEL 9 soient basés sur **DNF**, ils sont compatibles avec **YUM** utilisé dans RHEL 7.

Pour plus d'informations, voir Gestion des logiciels avec l'outil DNF .

CHAPITRE 4. NOUVELLES FONCTIONNALITÉS

Cette partie décrit les nouvelles fonctionnalités et les améliorations majeures introduites dans Red Hat Enterprise Linux 9.0.

4.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

Anaconda prend en charge **rhsm** pour le provisionnement des machines par le biais d'installations Kickstart pour Satellite

Auparavant, le provisionnement des machines dépendait d'un script personnalisé **%post** pour l'installation de Kickstart sur Red Hat Satellite. Ce script **%post** importait le certificat auto-signé personnalisé de Satellite, enregistrait la machine, attachait un abonnement et installait les paquets résidant dans les dépôts.

Avec RHEL 9, la prise en charge de Satellite a été ajoutée à la commande **rhsm** pour le provisionnement des machines. Vous pouvez désormais utiliser **rhsm** pour toutes les tâches de provisionnement telles que l'enregistrement du système, l'attachement des abonnements RHEL et l'installation à partir d'une instance satellite.

(BZ#1951709)

RHEL prend en charge **localhost** en tant que nom d'hôte statique

À partir de RHEL 9, la définition de **localhost** comme nom d'hôte statique dans **/etc/hostname** est valide. Dans ce cas, NetworkManager n'essaie pas d'obtenir un nom d'hôte transitoire par DHCP ou par une recherche DNS inversée.

(BZ#2190045)

Les écrans de configuration des licences, du système et des paramètres utilisateur ont été désactivés après l'installation standard

Auparavant, les utilisateurs de RHEL configuraient les paramètres de licence, de système (gestionnaire d'abonnement) et d'utilisateur avant les écrans **gnome-initial-setup** et de connexion. Avec cette mise à jour, les écrans de configuration initiale ont été désactivés par défaut afin d'améliorer l'expérience des utilisateurs.

Si vous devez exécuter la configuration initiale pour la création d'utilisateurs ou l'affichage des licences, installez les paquets suivants en fonction des besoins.

1. Installer les paquets d'installation initiaux.

```
# dnf install initial-setup initial-setup-gui
```

2. Activer la configuration initiale lors du prochain redémarrage du système.

```
# systemctl enable initial-setup
```

3. Redémarrez le système pour afficher la configuration initiale.

Pour les installations Kickstart, ajoutez **initial-setup-gui** à la section des paquets et activez le service **initial-setup**.

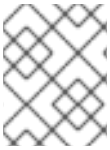
```
firstboot --enable
```

```
%packages
@^graphical-server-environment
initial-setup-gui
%end
```

(BZ#1878583)

Anaconda active automatiquement le réseau pour les installations interactives

Auparavant, lors d'une installation interactive sans que le réseau soit activé par Kickstart ou les options de démarrage, les utilisateurs devaient activer le réseau manuellement dans le réseau. Avec cette mise à jour, Anaconda active le réseau automatiquement, sans que les utilisateurs aient à visiter le réseau et à l'activer manuellement.



NOTE

Cette mise à jour ne modifie pas l'expérience d'installation pour les installations Kickstart et les installations utilisant l'option de démarrage **ip=**.

(BZ#1978264)

Image Builder prend désormais en charge la configuration du système de fichiers

Grâce à cette amélioration, vous pouvez spécifier une configuration personnalisée du système de fichiers dans vos plans et créer des images avec la disposition de disque souhaitée. Par conséquent, en ayant des dispositions différentes de celles par défaut, vous pouvez bénéficier de références de sécurité, d'une cohérence avec les configurations existantes, de performances et d'une protection contre les erreurs hors disque.

Pour personnaliser la configuration du système de fichiers dans votre plan, définissez la personnalisation suivante :

```
[[customizations.filesystem]]
mountpoint = "MOUNTPOINT"
size = MINIMUM-PARTITION-SIZE
```

NOTE

Après avoir ajouté une personnalisation du système de fichiers à votre plan, le système de fichiers est converti en partition LVM.

(BZ#2011448)

Nouvelles options pour **Lock root account** et **Allow root SSH login with password**

Les nouvelles options suivantes ont été ajoutées à l'écran de configuration du mot de passe root dans l'installation graphique de RHEL :

- Verrouiller le compte racine : Cette option permet de verrouiller l'accès racine à la machine.
- Allow root SSH login with password (Autoriser la connexion SSH de la racine avec un mot de passe) : cette option permet d'activer les connexions SSH de la racine basées sur un mot de passe.

Pour activer **password-based SSH root logins**, ajoutez la ligne suivante au fichier Kickstart avant de lancer le processus d'installation.

```
%post
echo "PermitRootLogin yes" > /etc/ssh/sshd_config.d/01-permitrootlogin.conf
%end
```

(BZ#1940653)

Image Builder permet désormais de créer des images d'installation amorçables

Grâce à cette amélioration, vous pouvez utiliser Image Builder pour créer des images ISO amorçables composées d'un fichier **tarball**, qui contient un système de fichiers racine. Par conséquent, vous pouvez utiliser l'image ISO amorçable pour installer le système de fichiers **tarball** sur un système métallique nu.

(BZ#2019318)

4.2. RHEL POUR EDGE

RHEL for Edge prend désormais en charge par défaut les contrôles de santé intégrés de Greenboot

Avec cette mise à jour, RHEL for Edge **Greenboot** inclut désormais des contrôles de santé intégrés avec la fonctionnalité **watchdog** pour s'assurer que le matériel ne se bloque pas ou ne se fige pas lors du redémarrage. Vous pouvez ainsi bénéficier des fonctionnalités suivantes :

- Il facilite l'adoption des contrôles de santé intégrés par les utilisateurs du matériel **watchdogs**
- Un ensemble de contrôles de santé par défaut qui apportent de la valeur aux composants intégrés du système d'exploitation
- L'adresse **watchdog** est désormais présente dans les préréglages par défaut, ce qui facilite l'activation ou la désactivation de cette fonction
- Possibilité de créer des contrôles de santé personnalisés sur la base des contrôles de santé déjà disponibles.

(BZ#2083036)

RHEL 9 fournit rpm-ostree v2022.2

RHEL 9 est distribué avec la version **rpm-ostree** v2022.2, qui apporte de nombreuses corrections de bogues et améliorations. Les changements notables sont les suivants :

- Les arguments du noyau peuvent désormais être mis à jour de manière idempotente, en utilisant les nouveaux drapeaux **--append-if-missing** et **--delete-if-present** kargs.
- La fonctionnalité **Count Me** de DNF est maintenant entièrement désactivée par défaut dans toutes les requêtes de repo et ne sera déclenchée que par les unités **rpm-ostree-countme.timer** et **rpm-ostree-countme.service** correspondantes. Voir countme.
- La logique de post-traitement peut maintenant traiter l'attribut étendu **user.ima** IMA. Lorsqu'un attribut étendu **xattr** est trouvé, le système le traduit automatiquement en **security.ima** dans le contenu final du paquet **OSTree**.
- Le fichier **treefile** comporte un nouveau champ **repo-packages**. Vous pouvez l'utiliser pour épingler un ensemble de paquets à un dépôt spécifique.

(BZ#1961324)

RHEL 9 fournit OSTree v2021.2

RHEL 9 est distribué avec la version v2021.2 du paquet **OSTree**, qui apporte de nombreuses corrections de bogues et améliorations. Les changements notables sont les suivants :

- Nouvelles API pour l'écriture de fichiers, utilisées dans le nouveau projet ostree-rs-ext, pour améliorer les importations à partir de tarballs.
- La commande **rofiles-fuse** gère désormais les attributs étendus de **xattrs**. Note : La commande **rofiles-fuse** est considérée comme obsolète, voir #2281.
- Amélioration de l'API **introspection** et des tests.

(BZ#1961254)

L'outil rpm-ostree rebase prend en charge la mise à niveau de RHEL 8 vers RHEL 9

Grâce à cette amélioration, vous pouvez mettre à niveau votre système RHEL 8 vers RHEL 9 à l'aide de l'outil **rpm-ostree rebase**. Il prend entièrement en charge l'ensemble de paquets par défaut de RHEL pour les mises à niveau Edge entre les mises à jour les plus récentes de RHEL 8 et les mises à jour les plus récentes de RHEL 9.

(BZ#2082306)

4.3. GESTION DES ABONNEMENTS

Fusion des commandes d'objectifs du système sous subscription-manager syspurpose

Auparavant, il existait deux commandes différentes pour définir les attributs de l'objectif du système : **syspurpose** et **subscription-manager**. Afin d'unifier tous les attributs d'objectif du système dans un seul module, toutes les commandes **addons**, **role**, **service-level**, et **usage** du gestionnaire d'abonnements ont été déplacées dans le nouveau sous-module, **subscription-manager syspurpose**.

Les commandes **subscription-manager** existantes en dehors du nouveau sous-module sont obsolètes. Le paquet séparé (**python3-syspurpose**) qui fournit l'outil de ligne de commande **syspurpose** a été supprimé dans RHEL 9.

Cette mise à jour fournit un moyen cohérent de visualiser, de définir et de mettre à jour tous les attributs de l'objectif du système à l'aide d'une seule commande du gestionnaire d'abonnements ; elle remplace toutes les commandes existantes de l'objectif du système par leurs versions équivalentes disponibles sous la forme d'une nouvelle sous-commande. Par exemple, **subscription-manager role --set SystemRole** devient **subscription-manager syspurpose role --set SystemRole** et ainsi de suite.

Pour des informations complètes sur les nouvelles commandes, options et autres attributs, voir la section **SYSPURPOSE OPTIONS** dans la page de manuel **subscription-manager**.

(BZ#1898563)

4.4. GESTION DES LOGICIELS

RHEL 9 fournit RPM 4.16

RHEL 9 est distribué avec la version 4.16 du RPM. Les corrections de bogues et améliorations notables par rapport à la version 4.14 sont les suivantes :

- Nouvelles fonctionnalités SPEC, notamment :
  - Générateurs de dépendances rapides basés sur des macros
  - La section **%generate_buildrequires** qui permet de générer des dépendances de construction dynamiques
  - Méta-dépendances (non ordonnées)
  - Augmentation du parallélisme dans la construction des paquets
  - Comparaison native des versions dans les expressions
  - Opérateur de version Caret, opposé au tilde
  - **%enif**, **%enifos** et **%enifarch** déclarations
  - En option, numérotation automatique des patchs et des sources
  - **topatch** accepte désormais les plages de correctifs
  - **%patchlist** et **%sourcelist** sections
  - Validation UTF-8 des données d'en-tête au moment de la compilation
- La base de données rpm est désormais basée sur la bibliothèque **sqlite**. La prise en charge en lecture seule des bases de données **BerkeleyDB** a été conservée à des fins de migration et d'interrogation.
- Un nouveau plug-in **rpm-plugin-audit** pour l'émission d'événements de journal d'audit sur les transactions, précédemment intégré dans RPM lui-même

(JIRA:RHELPLAN-80734)

Le nouveau plugin RPM notifie à fapolicyd les changements survenus lors des transactions RPM

Cette mise à jour des paquets **rpm** introduit un nouveau plugin RPM qui intègre le cadre **fapolicyd** avec la base de données RPM. Le plugin notifie à **fapolicyd** les fichiers installés et modifiés au cours d'une transaction RPM. Par conséquent, **fapolicyd** prend désormais en charge la vérification de l'intégrité.

Notez que le plugin RPM remplace le plugin DNF car sa fonctionnalité n'est pas limitée aux transactions DNF mais couvre également les changements effectués par RPM.

(BZ#1942549)

RPM prend désormais en charge l'algorithme de clé publique EdDSA

Avec cette amélioration, la commande **rpm** prend en charge les clés de signature utilisant l'algorithme de clé publique EdDSA. Par conséquent, les clés de signature générées à l'aide de l'algorithme EdDSA peuvent désormais être utilisées pour signer et vérifier les paquets.

Notez que, bien que les clés de signature utilisant EdDSA soient maintenant supportées, RSA continue d'être l'algorithme de clé publique par défaut dans GnuPG.

(BZ#1962234)

RPM supporte maintenant l'algorithme de compression Zstandard (zstd)

Avec cette amélioration, l'algorithme de compression par défaut des RPM est passé à Zstandard (**zstd**). Les utilisateurs peuvent ainsi bénéficier d'une installation plus rapide des paquets, ce qui peut être particulièrement appréciable lors de transactions importantes.

(JIRA:RHELPLAN-117903)

Nouvelles options DNF exclude_from_weak_autodetect et exclude_from_weak

Avec cette amélioration, le comportement par défaut de la DNF n'installe pas de dépendances faibles indésirables. Pour modifier ce comportement, utilisez les nouvelles options suivantes :

- **exclude_from_weak_autodetect**
  Si elle est activée, l'option **exclude_from_weak_autodetect** détecte automatiquement les dépendances faibles non satisfaites (Recommends : ou Supplements :) des paquets installés sur votre système. Par conséquent, les fournisseurs de ces dépendances faibles ne sont pas installés en tant que dépendances faibles, mais, s'ils sont intégrés, ils sont installés en tant que dépendances normales. La valeur par défaut est **true**.

- **exclude_from_weak**
  Si elle est activée, l'option **exclude_from_weak** empêche l'installation de paquets en tant que dépendances faibles (Recommends : ou Supplements :). Vous pouvez spécifier les paquets soit par un nom de paquet, soit par un glob, et les séparer par une virgule. La valeur par défaut est **[]**.

(BZ#2005305)

RHEL 9 fournit libmodulemd 2.13.0

RHEL 9 est distribué avec le paquet **libmodulemd** version 2.13.0. Les corrections de bogues et améliorations notables par rapport à la version 2.9.4 sont les suivantes :

- Ajout de la prise en charge de la suppression des paquets démodularisés d'un module.
- Ajout d'un support pour la validation des documents **modulemd-packager-v3** avec une nouvelle option **--type** de l'outil **modulemd-validator**.
- Renforcement de l'analyse des nombres entiers.
- Correction de divers problèmes liés à **modulemd-validator**.

(BZ#1984403)

4.5. SHELLS ET OUTILS DE LIGNE DE COMMANDE

Le collage entre crochets est désormais activé par défaut dans bash

La version 8.1 de la bibliothèque bash **readline** est désormais disponible et active par défaut le mode de collage entre crochets. Lorsque vous collez du texte dans votre terminal, **bash** met le texte en surbrillance et vous devez appuyer sur **enter** pour exécuter la commande collée. Le mode de collage entre crochets est le paramètre par défaut pour éviter d'exécuter accidentellement des commandes malveillantes.

Pour désactiver le mode de collage entre crochets pour un utilisateur spécifique, ajoutez la ligne suivante à **~/.inputrc**:

```
set enable-bracketed-paste off
```

Pour désactiver le mode de collage entre crochets pour tous les utilisateurs, ajoutez la ligne suivante à **/etc/inputrc**:

```
set enable-bracketed-paste off
```

Lorsque vous désactivez le mode de collage entre crochets, les commandes sont directement exécutées lors du collage et vous n'avez pas besoin de les confirmer en appuyant sur **enter**.

(BZ#2079078)

RHEL 9 comprend powerpc-utils 1.3.9

RHEL 9 fournit la version 1.3.9 du paquet **powerpc-utils**. Les corrections de bogues et améliorations notables par rapport à la version 1.3.8 sont les suivantes :

- Augmentation de la taille du journal à 1 Mo dans **drmgr**.
- Correction de la taille du tableau **HCIND** au démarrage.
- Mise en œuvre de **autoconnect-slaves** sur les connexions HNV à l'adresse **hcnmgr**.
- Amélioration des connexions à la liste des obligations HNV sur le site **hcnmgr**.
- Utilisez **hexdump** à partir de **util-linux** dans **hcnmgr**.
- Le site **hcn-init.service** commence par le NetworkManager.
- Correction de l'OF pour la recherche de la FC logique pour le multipath dans **ofpathname**.
- Correction de l'OF pour la recherche logique avec les partitions dans **ofpathname**.
- Correction de la liste de démarrage pour les dispositifs à chemins multiples ayant plus de 5 chemins.
- Ajout de l'extraction des sous-chaînes manquantes de **devpart** dans l2of_vd() de **ofpathname**.
- Introduit **lpamumascore**.
- Correction de la suppression par **index operation** dans **drmgr**.
- La définition de **SYS_PATH** a été déplacée de **l2of_vs()** à **l2of_scsi()** dans **ofpathname**.
- Ajout de l'option **-x** pour améliorer la sécurité dans partstat.
- Correction des avertissements et des erreurs de **nroff** dans la page de manuel **lparstat**.
- Mise en œuvre de la suppression des LMB basée sur les NUMA dans **drmgr**.
- Correction de l'erreur **ofpathname** avec le renommage de **udev** dans **hcnmgr**.
- Utilisez **NetworkManager nmcli** pour vérifier l'état de l'interface de liaison dans **hcnmgr**.
- Utilisez **NetworkManager nmcli** pour nettoyer l'interface de liaison au moment du démarrage lorsque HNV n'existe pas.

(BZ#1873868)

RHEL 9 est distribué avec opal-prd 6.7.1

La version 6.7.1 du paquet **opal-prd** apporte les corrections de bogues et améliorations suivantes par rapport à la version 6.6.3 précédemment disponible :

- Correction des problèmes de journalisation des erreurs **xscom** causés par l'appel à **xscom OPAL**.
- Correction d'un blocage possible avec la version **DEBUG**.
- Retour à **full_reboot** en cas d'échec de **fast-reboot** dans **core/platform**.
- Correction de **next_ungarded_primary** dans **core/cpu**.
- Amélioration des demandes de minuterie de limitation de débit et de l'état de la minuterie dans le moteur d'auto-amorçage (SBE).

(BZ#1869560)

RHEL 9 fournit lsvpd 1.7.12

RHEL 9 est distribué avec le paquet **lsvpd** version 1.7.12. Les corrections de bogues et améliorations notables par rapport à la version 1.7.11 sont les suivantes :

- Ajout de la propriété UUID dans **sysvpd**.
- Amélioration de la version du micrologiciel de **NVMe**.
- Correction de la logique d'analyse du fabricant de périphériques PCI.
- Ajout de **recommends clause** au fichier de configuration de **lsvpd**.

(BZ#1869564)

ppc64-diag version 2.7.7 disponible

La version 2.7.7 du paquet **ppc64-diag** est fournie dans RHEL 9. Les corrections de bogues et améliorations notables par rapport à la version 2.7.6 sont les suivantes :

- Amélioration des tests unitaires.
- Ajout de la propriété UUID dans **sysvpd**.
- **rtas_errd** ne fonctionne pas dans les conteneurs Linux.
- Les options de journalisation obsolètes ne sont plus disponibles dans les fichiers de service **systemd**.

(BZ#1869567)

RHEL 9 comprend Fetchmail 6.4.24

RHEL 9 est distribué avec le paquet **fetchmail** version 6.4.24. **Fetchmail** est un utilitaire de récupération et de transfert de courrier à distance.

Pour plus d'informations, voir :

- le fichier **/usr/share/doc/fetchmail/NEWS**,
- la page de manuel **fetchmail(1)**,

- le fichier **/usr/share/doc/fetchmail/README.SSL** pour les informations relatives à SSL au cas où vous devriez modifier la configuration.

(BZ#1999276)

RHEL 9 comprend Eigen 3.4

RHEL 9 est distribué avec le paquetage **eigen3** version 3.4. **Eigen 3.4** est une bibliothèque de modèles C pour l'algèbre linéaire, qui prend désormais en charge les instructions d'assistance à la multiplication de matrices POWER10.

Ainsi, les utilisateurs de **Eigen 3.4** peuvent effectuer des calculs d'algèbre linéaire optimisés sur les systèmes POWER10.

(BZ#2032423)

RHEL 9 introduit le paquetage cdrskin

RHEL 9 introduit le paquetage **cdrskin** pour la gravure de données sur CD, DVD ou BD. Le paquet **cdrskin** remplace l'exécutable **cdrecord** du paquet **wodim**, qui n'est pas disponible dans RHEL 9.

Le paquet **cdrskin** comprend

- Mise à blanc, formatage et gravure de données sur des supports optiques.
- Multi session sur CD.
- Emulation ISO-9660 multi-session sur DVD RW, DVD-RW, DVD-RAM, BD-RE.

Le paquetage **cdrskin** fournit également la commande **cdrecord** sous forme de lien symbolique vers le binaire **cdrskin**, de sorte que vous n'avez pas besoin de modifier les scripts de l'utilisateur. Voir la page de manuel **cdrskin(1)** pour l'ensemble des fonctionnalités.

(BZ#2015861)

La collection Ansible redhat.rhel_mgmt est prise en charge dans la version RHEL 9

Cette mise à jour assure la prise en charge des modules Ansible Intelligent Platform Management Interface (**IPMI**). **IPMI** est une spécification pour un ensemble d'interfaces de gestion permettant de communiquer avec les dispositifs BMC (Baseboard Management Controller). Les modules **IPMI** - **ipmi_power** et **ipmi_boot** - sont disponibles dans la collection **redhat.rhel_mgmt**, à laquelle vous pouvez accéder en installant le paquetage **ansible-collection-redhat-rhel_mgmt**.

(BZ#2023381)

RHEL 9 introduit le paquetage util-linux-core

Outre le paquet **util-linux**, RHEL 9 fournit le sous-paquet **util-linux-core** pour les scénarios dans lesquels la taille des paquets installés est une caractéristique critique, par exemple les buildroots, certains conteneurs et les images de démarrage.

Le sous-paquet **util-linux-core** contient un sous-ensemble limité des utilitaires **util-linux**, qui sont nécessaires pour démarrer le système Linux, par exemple l'utilitaire **mount**.

Le sous-paquetage **util-linux-core** ne contient aucune dépendance externe. Par exemple, les utilitaires de connexion ne sont pas disponibles car ils dépendent d'une bibliothèque PAM.

Pour les cas d'utilisation standard, comme les installations, utilisez le paquetage standard **util-linux**. Le paquet **util-linux** dépend de **util-linux-core**, ce qui signifie que si vous installez **util-linux**, **util-linux-core** est installé automatiquement.

(BZ#2079313)

4.6. SERVICES D'INFRASTRUCTURE

s-nail remplace mailx

Le système de traitement du courrier **s-nail** a remplacé l'utilitaire **mailx**. L'utilitaire **s-nail** est compatible avec **mailx** et ajoute de nombreuses fonctionnalités. Le paquet **mailx** n'est plus maintenu en amont.

(BZ#1940863)

TuneD 2.18 est disponible

RHEL 9 est distribué avec la version 2.18 de TuneD. Les changements notables par rapport à la version 2.16 sont les suivants :

- Le plugin **net**: ajout de la prise en charge de l'accord **txqueuelen**.
- Le plugin **disk**: ajout de la prise en charge de l'optimisation des disques NVMe.
- **tuned-gui** corrections de bugs.

(BZ#2003838)

RHEL 9 fournit mod_security_crs 3.3

RHEL 9 est distribué avec le paquet **mod_security_crs** version 3.3. Les corrections de bogues et améliorations notables sont les suivantes :

- Introduit **libinjection**.
- Blocage des fichiers de sauvegarde se terminant par ~ dans les noms de fichiers.
- Ajout de nouvelles règles d'injection **LDAP** et de séparation **HTTP**.
- Ajout de **.swp** aux extensions restreintes.
- Ajout de balises CAPEC (Common Attack Pattern Enumeration and Classification) pour la classification des attaques.
- Ajout de la prise en charge de la détection des scanners de vulnérabilité **Nuclei**, **WFuzz**, et **ffuf**.
- Amélioration des variables en minuscules (**modsec3 behavior fix**)
- Ajout d'une prise en charge de la détection des techniques de contournement RCE Unix par le biais de variables non initialisées, de concaténations de chaînes et de motifs de globbing.
- Suppression des étiquettes de règles obsolètes : **WASCTC**, **OWASP_TOP_10**, **OWASP_AppSensor/RE1**, et **OWASP_CRS/FOO/BAR**. **OWASP_CRS** et **attack-type** sont toujours inclus dans le paquet **mod_security_crs**.

- Le format de la variable **crs-setup.conf tx.allowed_request_content_type** a été modifié pour s'aligner sur les autres variables. Si la variable est remplacée, veuillez consulter l'exemple dans le fichier **crs-setup.conf** pour le nouveau séparateur.

(BZ#1947962)

RHEL 9 fournit chrony 4.1

RHEL 9 est distribué avec **chrony** version 4.1. Les corrections de bogues et améliorations notables par rapport à la version 3.5 sont les suivantes :

- La prise en charge de l'authentification Network Time Security (NTS) a été ajoutée. Pour plus d'informations, voir Vue d'ensemble de Network Time Security (NTS) dans chrony .
- Par défaut, les sources NTP (Network Time Protocol) authentifiées sont plus fiables que les sources NTP non authentifiées. Pour rétablir le comportement d'origine, ajoutez l'argument **autselectmode ignore** dans le fichier **chrony.conf**.
- La prise en charge de l'authentification avec les clés **RIPEMD** - **RMD128**, **RMD160**, **RMD256**, **RMD320** - n'est plus disponible.
- La prise en charge des MAC longs non standard dans les paquets NTPv4 n'est plus disponible. Si vous utilisez les clés **chrony 2.x**, **non-MD5/SHA1**, vous devez configurer **chrony** avec l'option **version 3**.

En outre, ce qui suit diffère de la version RHEL 8 de **chrony**:

- Le filtre **seccomp** est activé par défaut (**-F 2** est défini dans **/etc/sysconfig/chronyd**). Le filtre **seccomp** est en conflit avec la directive **mailonchange**. Si vous avez la directive **mailonchange** dans **/etc/chrony.conf**, supprimez le paramètre **-F 2** dans **/etc/sysconfig/chronyd**.

(BZ#1961131)

4.7. SÉCURITÉ

Le système crypto-policies est désormais plus sûr

Avec cette mise à jour, les politiques cryptographiques du système ont été ajustées pour fournir des valeurs par défaut sécurisées et actualisées :

- Désactivation de TLS 1.0, TLS 1.1, DTLS 1.0, RC4, Camellia, DSA, 3DES et FFDHE-1024 dans toutes les politiques.
- Augmentation de la taille minimale des clés RSA et de la taille minimale des paramètres Diffie-Hellman dans LEGACY.
- Désactivation des algorithmes TLS et SSH utilisant SHA-1, à l'exception de l'utilisation de SHA-1 dans les codes d'authentification des messages basés sur le hachage (HMAC).

Si votre scénario nécessite l'activation de certains algorithmes et chiffrements désactivés, utilisez des stratégies ou sous-politiques personnalisées.

(BZ#1937651)

RHEL 9 fournit OpenSSL 3.0.1

RHEL 9 fournit les paquets **openssl** dans la version amont 3.0.1, qui comprend de nombreuses améliorations et corrections de bogues par rapport à la version précédente. Les changements les plus notables sont les suivants :

- Ajout du nouveau concept de fournisseur. Les fournisseurs sont des collections d'algorithmes, et vous pouvez choisir différents fournisseurs pour différentes applications.
- Introduction du nouveau schéma de version dans le format suivant : *<major>.<minor>.<patch>*.
- Ajout de la prise en charge du protocole de gestion des certificats (CMP, RFC 4210), du format de message de demande de certificat (CRMF) et du transfert HTTP (RFC 6712).
- Introduction d'un client HTTP(S) qui prend en charge GET et POST, la redirection, les contenus en clair et codés ASN.1-, les proxies et les délais d'attente.
- Ajout d'une nouvelle API de fonction de dérivation de clé (EVP_KDF) et d'une API de code d'authentification de message (EVP_MAC).
- Ajout de la prise en charge de Linux Kernel TLS (KTLS) en compilant avec l'option de configuration **enable-ktls**.
- Ajout de la prise en charge de la vérification de la signature CAdES-BES.
- Ajout de la prise en charge du schéma de signature CAdES-BES et de ses attributs (RFC 5126) à l'API de la CMS.
- Prise en charge de nouveaux algorithmes, par exemple :
  - Algorithmes KDF "SINGLE STEP" et "SSH".
  - Algorithmes MAC "GMAC" et "KMAC".
  - Algorithme KEM "RSASVE".
  - Algorithme de chiffrement "AES-SIV"
- Ajout de la structure du type de contenu AuthEnvelopedData (RFC 5083) utilisant AES_GCM.
- Les algorithmes par défaut pour la création de PKCS #12 avec la fonction **PKCS12_create()** ont été remplacés par des algorithmes plus modernes basés sur PBKDF2 et AES.
- Ajout d'une nouvelle API générique de traçage.

(BZ#1990814)

OpenSSL inclut désormais les fournisseurs

La boîte à outils OpenSSL dans sa version 3.0.1, qui est incluse dans RHEL 9, a ajouté le concept de fournisseurs. Les fournisseurs sont des collections d'algorithmes, et vous pouvez choisir différents fournisseurs pour différentes applications. OpenSSL inclut actuellement les fournisseurs suivants : **base**, **default**, **fips**, **legacy**, et **null**.

Par défaut, OpenSSL charge et active le fournisseur **default**, qui comprend des algorithmes couramment utilisés tels que RSA, DSA, DH, CAMELLIA, SHA-1 et SHA-2.

Lorsque le drapeau FIPS est activé dans le noyau, OpenSSL charge automatiquement le fournisseur FIPS et n'utilise que des algorithmes approuvés par le FIPS. Par conséquent, il n'est pas nécessaire de basculer manuellement OpenSSL en mode FIPS.

Pour changer de fournisseur au niveau du système, modifiez le fichier de configuration **openssl.cnf**. Par exemple, si votre scénario nécessite l'utilisation du fournisseur **legacy**, décommentez la section correspondante.

AVERTISSEMENT

L'activation explicite d'un fournisseur annule l'activation implicite du fournisseur par défaut et peut rendre le système inaccessible à distance, par exemple par la suite OpenSSH.

Pour plus d'informations sur les algorithmes inclus dans chaque fournisseur, consultez les pages de manuel correspondantes. Par exemple, la page de manuel **OSSL_PROVIDER-legacy(7)** pour le fournisseur **legacy**.

(BZ#2010291)

Le générateur de bits aléatoires OpenSSL prend désormais en charge CPACF

Cette version des paquets **openssl** introduit la prise en charge du CP Assist for Cryptographic Functions (CPACF) dans le générateur de bits aléatoires déterministes (DRBG) OpenSSL conforme à la norme NIST SP800-90A.

(BZ#1871147)

openssl-spkac peut désormais créer des fichiers SPKAC signés avec SHA-1 et SHA-256

L'utilitaire **openssl-spkac** peut désormais créer des fichiers de clés publiques et de défis signés Netscape (SPKAC) signés avec des hachages différents de MD5. Vous pouvez également créer et vérifier des fichiers SPKAC signés avec des hachages SHA-1 et SHA-256.

(BZ#1970388)

RHEL 9 fournit openCryptoki 3.17.0

RHEL 9 est distribué avec **openCryptoki** version 3.17.0. Les corrections de bogues et améliorations notables par rapport à la version 3.16.0 sont les suivantes :

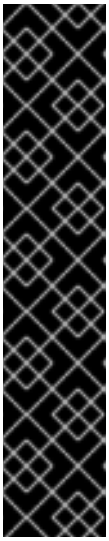
- L'utilitaire **p11sak** ajoute une nouvelle fonction pour lister les touches.
- **openCryptoki** prend désormais en charge :
  - OpenSSL 3.0.
  - Notifications d'événements.
  - Les solutions de repli logiciel dans les jetons ICA.
- Le démarrage de WebSphere Application Server n'échoue plus lorsque l'adaptateur cryptographique matériel est activé.

RHEL 9 inclut OpenSSL avec des correctifs supplémentaires, qui sont spécifiques à RHEL. Si le système est en mode FIPS (Federal Information Processing Standards), OpenSSL charge automatiquement le fournisseur FIPS et le fournisseur de base et force les applications à utiliser le fournisseur FIPS. Par

conséquent, le comportement de **openCryptoki** sur RHEL 9 diffère de celui en amont :

- Les jetons qui s'appuient sur l'implémentation par OpenSSL des opérations cryptographiques (soft tokens et fallbacks logiciels des jetons ICA) ne prennent désormais en charge que les mécanismes approuvés par le FIPS, même si les mécanismes non approuvés sont toujours répertoriés comme étant disponibles.

- **openCryptoki** prend en charge deux formats de données différents pour les jetons : l'ancien format de données, qui utilise des algorithmes non approuvés par la FIPS (tels que DES et SHA1), et le nouveau format de données, qui utilise uniquement des algorithmes approuvés par la FIPS.
  L'ancien format de données ne fonctionne plus car le fournisseur FIPS n'autorise l'utilisation que d'algorithmes approuvés par le FIPS.



IMPORTANT

Pour que **openCryptoki** fonctionne sur RHEL 9, migrez les jetons pour utiliser le nouveau format de données avant d'activer le mode FIPS sur le système. Cette opération est nécessaire car l'ancien format de données est toujours utilisé par défaut dans **openCryptoki 3.17**. Les installations **openCryptoki** existantes qui utilisent l'ancien format de données des jetons ne fonctionneront plus lorsque le système passera en mode FIPS.

Vous pouvez migrer les jetons vers le nouveau format de données en utilisant l'utilitaire **pkcstok_migrate**, fourni avec **openCryptoki**. Notez que **pkcstok_migrate** utilise des algorithmes non approuvés par le FIPS pendant la migration. Par conséquent, il convient d'utiliser cet outil avant d'activer le mode FIPS sur le système. Pour plus d'informations, voir Migration vers la conformité FIPS - utilitaire pkcstok_migrate.

(BZ#1869533)

GnuTLS fourni dans la version 3.7.3

Dans RHEL 9, les paquets **gnutls** sont fournis dans la version amont 3.7.3. Cette version apporte de nombreuses améliorations et corrections de bogues par rapport aux versions précédentes, notamment :

- Introduction d'une API pour les indicateurs explicites de la norme FIPS 140-3.

- Défauts renforcés pour l'exportation de fichiers PKCS#12.

- Fixation du moment de l'échange des données anticipées (données zéro round trip, 0-RTT).

- L'outil **certutil** n'hérite plus du point de distribution de la liste de révocation des certificats (CRL) de l'autorité de certification (CA) lors de la signature d'une demande de signature de certificat (CSR).

(BZ#2033220)

RHEL 9 fournit NSS 3.71

RHEL 9 est distribué avec la version 3.71 des bibliothèques NSS (Network Security Services). Les changements notables sont les suivants :

- La prise en charge de l'ancien format de base de données DBM a été complètement supprimée. NSS ne prend en charge que le format de base de données SQLite dans RHEL 9.

- Les algorithmes de chiffrement PKCS #12 utilisent désormais les algorithmes AES-128-CBC avec PBKDF2 et SHA-256 au lieu de PBE-SHA1-RC2-40 et PBE-SHA1-2DES.

(BZ#2008320)

Les NSS ne prennent plus en charge les clés RSA de moins de 1023 bits

La mise à jour des bibliothèques Network Security Services (NSS) modifie la taille minimale des clés pour toutes les opérations RSA de 128 à 1023 bits. Cela signifie que les NSS n'exécutent plus les fonctions suivantes :

- Générer des clés RSA plus courtes que 1023 bits.
- Signer ou vérifier des signatures RSA avec des clés RSA de moins de 1023 bits.
- Chiffrer ou déchiffrer des valeurs avec une clé RSA inférieure à 1023 bits.

(BZ#2099438)

Option de longueur minimale des bits de la clé RSA dans OpenSSH

L'utilisation accidentelle de clés RSA courtes peut rendre le système plus vulnérable aux attaques. Avec cette mise à jour, vous pouvez définir la longueur minimale des bits de la clé RSA pour les serveurs et les clients OpenSSH. Pour définir la longueur minimale de la clé RSA, utilisez la nouvelle option **RSAMinSize** dans le fichier **/etc/ssh/sshd_config** pour les serveurs OpenSSH et dans le fichier **/etc/ssh/ssh_config** pour les clients OpenSSH.

(BZ#2119694)

OpenSSH distribué dans la version 8.7p1

RHEL 9 inclut **OpenSSH** dans la version 8.7p1. Cette version apporte de nombreuses améliorations et corrections de bogues par rapport à la version 8.0p1 de **OpenSSH**, qui est distribuée dans RHEL 8.5, notamment :

New Features

- Prise en charge des transferts utilisant le protocole SFTP en remplacement du protocole SCP/RCP précédemment utilisé. SFTP offre une gestion plus prévisible des noms de fichiers et ne nécessite pas l'expansion des motifs glob(3) par l'interpréteur de commandes du côté distant.
  Le support SFTP est activé par défaut. Si SFTP n'est pas disponible ou incompatible dans votre scénario, vous pouvez utiliser le drapeau **-O** pour forcer l'utilisation du protocole SCP/RCP d'origine.
- La directive de configuration **LogVerbose** qui permet de forcer la journalisation maximale du débogage par des listes de motifs de fichiers/fonctions/lignes.
- Limitation du débit en fonction de l'adresse du client avec les nouvelles directives **sshd_config** **PerSourceMaxStartups** et **PerSourceNetBlockSize**. Cela permet un contrôle plus fin que la limite globale de **MaxStartups**.
- Le mot-clé **HostbasedAcceptedAlgorithms** filtre désormais sur la base de l'algorithme de signature au lieu de filtrer par type de clé.
- Le mot-clé **Include sshd_config** du démon **sshd** qui permet d'inclure des fichiers de configuration supplémentaires en utilisant des motifs **glob**.

- Prise en charge des authentificateurs matériels U2F (Universal 2nd Factor) spécifiés par l'alliance FIDO. U2F/FIDO sont des normes ouvertes pour le matériel d'authentification à deux facteurs peu coûteux qui sont largement utilisées pour l'authentification des sites web. Dans **OpenSSH**, les dispositifs FIDO sont pris en charge par les nouveaux types de clés publiques **ecdsa-sk** et **ed25519-sk** et par les types de certificats correspondants.

- Prise en charge des clés FIDO qui nécessitent un code PIN pour chaque utilisation. Vous pouvez générer ces clés en utilisant **ssh-keygen** avec la nouvelle option **verify-required**. Lorsqu'une clé nécessitant un code PIN est utilisée, l'utilisateur est invité à saisir son code PIN pour terminer l'opération de signature.

- Le fichier **authorized_keys** prend désormais en charge une nouvelle option **verify-required**. Cette option exige que les signatures FIDO fassent appel à une vérification par jeton de la présence de l'utilisateur avant de procéder à la signature. Le protocole FIDO prend en charge plusieurs méthodes de vérification de l'utilisateur. OpenSSH ne prend actuellement en charge que la vérification du code PIN.

- Ajout de la prise en charge de la vérification des signatures FIDO **webauthn**. **webauthn** est une norme permettant d'utiliser les clés FIDO dans les navigateurs web. Ces signatures ont un format légèrement différent des signatures FIDO ordinaires et nécessitent donc une prise en charge explicite.

Bug fixes

- Clarification de la sémantique du mot-clé **ClientAliveCountMax=0**. Désormais, il désactive entièrement l'arrêt de la connexion au lieu du comportement précédent qui consistait à arrêter instantanément la connexion après le premier test de vivacité, quel que soit son succès.

Security

- Correction d'un débordement d'entier exploitable dans le code d'analyse de la clé privée pour le type de clé XMSS. Ce type de clé est encore expérimental et son support n'est pas compilé par défaut. Aucune option autoconf orientée utilisateur n'existe dans OpenSSH portable pour l'activer.

- Ajout d'une protection pour les clés privées au repos dans la RAM contre la spéculation et les attaques par canal latéral de la mémoire comme Spectre, Meltdown et Rambleed. Cette version chiffre les clés privées lorsqu'elles ne sont pas utilisées avec une clé symétrique dérivée d'une "préclé" relativement importante composée de données aléatoires (actuellement 16 Ko).

(BZ#1952957)

La redirection des langues est désactivée par défaut dans OpenSSH

L'utilisation des paramètres régionaux **C.UTF-8** dans les petites images, telles que les conteneurs et les machines virtuelles, réduit la taille et améliore les performances par rapport à l'utilisation des paramètres régionaux traditionnels **en_US.UTF-8**.

La plupart des distributions envoient des variables d'environnement locales par défaut et les acceptent côté serveur. Cependant, cela signifie que la connexion via SSH de clients utilisant des locales autres que **C** ou **C.UTF-8** à des serveurs sur lesquels les paquets **glibc-langpack-en** ou **glibc-all-langpacks** n'étaient pas installés entraînait une dégradation de l'expérience de l'utilisateur. En particulier, la sortie au format UTF-8 était défectueuse et certains outils ne fonctionnaient pas ou envoyaient des messages d'avertissement fréquents.

Avec cette mise à jour, la redirection des paramètres linguistiques est désactivée par défaut dans OpenSSH. La locale reste ainsi viable même si les clients se connectent à des serveurs dotés d'installations minimales qui ne prennent en charge qu'un petit nombre de locales.

(BZ#2002734)

OpenSSH prend en charge les clés de sécurité U2F/FIDO

Auparavant, les clés OpenSSH stockées dans le matériel n'étaient prises en charge que par la norme PKCS #11, ce qui limitait l'utilisation d'autres clés de sécurité dans SSH. La prise en charge des clés de sécurité U2F/FIDO a été développée en amont et est désormais implémentée dans RHEL 9, ce qui améliore l'utilisation des clés de sécurité dans SSH indépendamment de l'interface PKCS #11.

(BZ#1821501)

Libreswan fourni dans la version 4.6

Dans RHEL 9, Libreswan est fourni dans la version amont 4.6. Cette version apporte de nombreuses corrections de bogues et améliorations, notamment sur l'IPsec labellisé utilisé avec l'Internet Key Exchange version 2 (IKEv2).

(BZ#2017355)

Libreswan n'accepte pas les paquets IKEv1 par défaut

Le protocole IKEv2 (Internet Key Exchange v2) étant désormais largement déployé, Libreswan ne prend plus en charge les paquets IKEv1 par défaut. IKEv2 offre un environnement plus sûr et une meilleure résistance aux attaques. Si votre scénario nécessite l'utilisation d'IKEv1, vous pouvez l'activer en ajoutant l'option **ikev1-policy=accept** au fichier de configuration **/etc/ipsec.conf**.

(BZ#2039877)

RHEL 9 fournit stunnel 5.62

RHEL 9 est distribué avec le paquet **stunnel** version 5.62. Les corrections de bogues et améliorations notables sont les suivantes :

- Sur les systèmes en mode FIPS, **stunnel** utilise désormais toujours le mode FIPS.
- Les options **NO_TLSv1.1**, **NO_TLSv1.2**, et **NO_TLSv1.3** ont été renommées respectivement **NO_TLSv1_1**, **NO_TLSv1_2**, et **NO_TLSv1_3**.
- La nouvelle option de niveau de service **sessionResume** permet d'activer et de désactiver la reprise de session.
- LDAP est désormais pris en charge par les clients **stunnel** à l'aide de l'option **protocol**.
- Un script de complétion Bash est désormais disponible.

(BZ#2039299)

RHEL 9 fournit nettle 3.7.3

RHEL 9 fournit la version 3.7.3 du paquet **nettle** avec de nombreuses corrections de bogues et améliorations. Les changements notables sont les suivants :

- Prise en charge de nouveaux algorithmes et modes, par exemple **Ed448**, **SHAKE256**, **AES-XTS**, **SIV-CMAC**.

- Ajoute des optimisations spécifiques à l'architecture pour les algorithmes existants.

(BZ#1986712)

RHEL 9 fournit p11-kit 0.24

RHEL 9 fournit le paquet **p11-kit** avec la version 0.24. Cette version apporte de nombreuses corrections de bogues et améliorations. Notamment, le sous-répertoire de stockage des autorités de certification de confiance a été renommé **blocklist**.

(BZ#1966680)

cyrus-sasl utilise désormais GDBM au lieu de Berkeley DB

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

(BZ#1947971)

La politique SELinux de RHEL 9 est à jour avec le noyau actuel

La politique SELinux inclut de nouvelles permissions, classes et capacités qui font également partie du noyau. Par conséquent, SELinux peut utiliser tout le potentiel fourni par le noyau. En particulier, SELinux dispose d'une meilleure granularité pour l'octroi des permissions, ce qui présente des avantages ultérieurs en termes de sécurité. Cela permet également de faire fonctionner les systèmes avec la politique SELinux MLS, car la politique MLS empêcherait certains systèmes de démarrer s'ils contenaient des permissions inconnues de la politique.

(BZ#1941810, BZ#1954145)

La politique SELinux par défaut interdit les commandes contenant des bibliothèques de relocalisation de texte

Le booléen **selinuxuser_execmod** est désormais désactivé par défaut afin d'améliorer l'empreinte de sécurité des systèmes installés. En conséquence, les utilisateurs de SELinux ne peuvent pas entrer de commandes utilisant des bibliothèques qui nécessitent une relocalisation de texte, à moins que les fichiers de la bibliothèque ne portent l'étiquette **textrel_shlib_t**.

(BZ#2055822)

OpenSCAP est fourni dans la version 1.3.6

RHEL 9 inclut OpenSCAP dans la version 1.3.6, qui apporte des corrections de bogues et des améliorations, notamment :

- Vous pouvez fournir des copies locales des composants du flux de données de la source SCAP distante au lieu de les télécharger pendant l'analyse en utilisant l'option **--local-files**
- OpenSCAP accepte plusieurs arguments **--rule** pour sélectionner plusieurs règles sur la ligne de commande.
- Vous pouvez ignorer l'évaluation de certaines règles en utilisant l'option **--skip-rule**.

- Vous pouvez limiter la mémoire consommée par les sondes OpenSCAP en utilisant la variable d'environnement **OSCAP_PROBE_MEMORY_USAGE_RATIO**.
- OpenSCAP supporte désormais le Blueprint OSBuild comme type de remédiation.

(BZ#2041782)

OSCAP Anaconda Add-on supporte désormais un nouveau nom d'add-on

Grâce à cette amélioration, vous pouvez utiliser le nouveau nom du module **com_redhat_oscap** plutôt que l'ancien nom du module **org_fedora_oscap** dans le fichier Kickstart du module **OSCAP Anaconda Add-on**. Par exemple, la section Kickstart peut être structurée comme suit :

```
%addon com_redhat_oscap
  content-type = scap-security-guide
%end
```

OSCAP Anaconda Add-on est actuellement compatible avec l'ancien nom de l'add-on, mais la prise en charge de l'ancien nom de l'add-on sera supprimée dans une prochaine version majeure de RHEL.

(BZ#1893753)

Les flux CVE OVAL sont désormais compressés

Avec cette mise à jour, Red Hat fournit les flux CVE OVAL sous une forme compressée. Ils ne sont plus disponibles sous forme de fichiers XML, mais au format **bzip2**. L'emplacement des flux pour RHEL9 a également été mis à jour pour refléter ce changement. Notez que les scanners SCAP tiers peuvent avoir des problèmes avec les règles d'analyse qui utilisent un flux compressé parce que le référencement du contenu compressé n'est pas standardisé.

(BZ#2028435)

Guide de sécurité SCAP fourni dans la version 0.1.60

RHEL 9 inclut les paquets **scap-security-guide** dans la version 0.1.60. Cette version apporte des corrections de bogues et des améliorations, notamment :

- Les règles de renforcement de la pile PAM utilisent désormais **authselect** comme outil de configuration.
- Le SCAP Security Guide fournit désormais un fichier d'adaptation delta pour le profil STIG. Ce fichier d'adaptation définit un profil qui représente les différences entre le contenu automatisé STIG et SSG de la DISA.

(BZ#2014561)

Profils du guide de sécurité SCAP pris en charge dans RHEL 9.0

Grâce aux profils de conformité du guide de sécurité SCAP inclus dans RHEL 9.0, vous pouvez renforcer le système conformément aux recommandations des organisations émettrices. Par conséquent, vous pouvez configurer et automatiser la conformité de vos systèmes RHEL 9 selon le niveau de renforcement requis en utilisant les remédiations et les profils SCAP associés.

Nom du profil	ID du profil	Version de la politique
Agence nationale de la sécurité des systèmes d'information (ANSSI) BP-028 niveau renforcé	**xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced**	1.2
Agence nationale de la sécurité des systèmes d'information (ANSSI) BP-028 Haut niveau	**xccdf_org.ssgproject.content_profile_anssi_bp28_high**	1.2
Agence nationale de la sécurité des systèmes d'information (ANSSI) BP-028 Niveau intermédiaire	**xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary**	1.2
Agence nationale de la sécurité des systèmes d'information (ANSSI) BP-028 Niveau minimal	**xccdf_org.ssgproject.content_profile_anssi_bp28_minimal**	1.2
[PROJET] CIS Red Hat Enterprise Linux 9 Benchmark pour le niveau 2 - Serveur	**xccdf_org.ssgproject.content_profile_cis**	PROJET[a]
[PROJET] CIS Red Hat Enterprise Linux 9 Benchmark pour le niveau 1 - Serveur	**xccdf_org.ssgproject.content_profile_cis_server_l1**	PROJET[a]
[PROJET] CIS Red Hat Enterprise Linux 9 Benchmark pour le niveau 1 - Station de travail	**xccdf_org.ssgproject.content_profile_cis_workstation_l1**	PROJET[a]
[PROJET] CIS Red Hat Enterprise Linux 9 Benchmark pour le niveau 2 - Station de travail	**xccdf_org.ssgproject.content_profile_cis_workstation_l2**	PROJET[a]
[Informations non classifiées dans les systèmes d'information et les organisations non fédérales (NIST 800-171)	**xccdf_org.ssgproject.content_profile_cui**	r2
Centre australien de cybersécurité (ACSC) Huit éléments essentiels	**xccdf_org.ssgproject.content_profile_e8**	non versionné
Loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA)	**xccdf_org.ssgproject.content_profile_hipaa**	non versionné

Nom du profil	ID du profil	Version de la politique
Centre australien de cybersécurité (ACSC) ISM Official	**xccdf_org.ssgproject.content_profile_ism_o**	non versionné
[Profil de protection pour les systèmes d'exploitation généraux	**xccdf_org.ssgproject.content_profile_ospp**	4.2.1
Base de contrôle PCI-DSS v3.2.1 pour Red Hat Enterprise Linux 9	**xccdf_org.ssgproject.content_profile_pci-dss**	3.2.1
[PROJET] STIG DISA pour Red Hat Enterprise Linux 9	**xccdf_org.ssgproject.content_profile_stig**	PROJET[b]
[DRAFT] DISA STIG avec GUI pour Red Hat Enterprise Linux 9	**xccdf_org.ssgproject.content_profile_stig_gui**	PROJET[b]

[a] Le CIS n'a pas encore publié de benchmark officiel pour RHEL 9

[b] La DISA n'a pas encore publié de référence officielle pour RHEL 9

AVERTISSEMENT

La remédiation automatique peut rendre le système non fonctionnel. Exécutez d'abord la remédiation dans un environnement de test.

(BZ#2045341, BZ#2045349, BZ#2045361, BZ#2045368, BZ#2045374, BZ#2045381, BZ#2045386, BZ#2045393, BZ#2045403)

RHEL 9 fournit fapolicyd 1.1

RHEL 9 est distribué avec le paquet **fapolicyd** version 1.1. Les améliorations les plus notables sont les suivantes :

- Le répertoire **/etc/fapolicyd/rules.d/**, qui contient les fichiers contenant les règles d'exécution d'autorisation et de refus, remplace le fichier **/etc/fapolicyd/fapolicyd.rules**. Le script **fagenrules** fusionne désormais tous les fichiers de règles de ce répertoire dans le fichier **/etc/fapolicyd/compiled.rules**. Voir la nouvelle page de manuel **fagenrules(8)** pour plus de détails.
- En plus du fichier **/etc/fapolicyd/fapolicyd.trust** qui permet de marquer comme fiables les fichiers ne faisant pas partie de la base de données RPM, vous pouvez désormais utiliser le nouveau répertoire **/etc/fapolicyd/trust.d**, qui permet de séparer une liste de fichiers fiables en

plusieurs fichiers. Vous pouvez également ajouter une entrée pour un fichier en utilisant la sous-commande **fapolicyd-cli -f** avec la directive **--trust-file** dans ces fichiers. Consultez les pages de manuel **fapolicyd-cli(1)** et **fapolicyd.trust(13)** pour plus d'informations.

- La base de données de confiance **fapolicyd** prend désormais en charge les espaces blancs dans les noms de fichiers.
- **fapolicyd** enregistre désormais le chemin d'accès correct à un fichier exécutable lorsqu'il ajoute le fichier à la base de données de confiance.

(BZ#2032408)

Rsyslog inclut le module mmfields pour des opérations plus performantes et CEF

Rsyslog comprend désormais le sous-paquetage **rsyslog-mmfields** qui fournit le module **mmfields**. Il s'agit d'une alternative à l'utilisation de l'extraction de champs du substitut de propriété, mais contrairement à ce dernier, tous les champs sont extraits en une seule fois et stockés dans la partie des données structurées. Par conséquent, vous pouvez utiliser **mmfields** en particulier pour traiter des formats d'enregistrement basés sur des champs, par exemple Common Event Format (CEF), et si vous avez besoin d'un grand nombre de champs ou si vous réutilisez des champs spécifiques. Dans ces cas, **mmfields** est plus performant que les fonctions Rsyslog existantes.

(BZ#2027971)

logrotate inclus dans un paquet séparé rsyslog-logrotate

La configuration **logrotate** a été séparée du paquet principal **rsyslog** dans le nouveau paquet **rsyslog-logrotate**. Ceci est utile dans certains environnements minimaux, par exemple lorsque la rotation des journaux n'est pas nécessaire, pour éviter d'installer des dépendances inutiles.

(BZ#1992155)

sudo supporte les plugins Python

Avec le programme **sudo** version 1.9, qui est inclus dans RHEL 9, vous pouvez écrire des plugins **sudo** en Python. Il est ainsi plus facile d'améliorer **sudo** pour l'adapter plus précisément à des scénarios spécifiques.

Pour plus d'informations, voir la page de manuel **sudo_plugin_python(8)**.

(BZ#1981278)

libseccomp fourni dans la version 2.5.2

RHEL 9.0 fournit les paquets **libseccomp** dans la version amont 2.5.2. Cette version apporte de nombreuses corrections de bogues et améliorations par rapport aux versions précédentes, notamment :

- Mise à jour de la table syscall pour Linux vers la version **v5.14-rc7**.
- Ajout de la fonction **get_notify_fd()** aux liaisons Python pour obtenir le descripteur de fichier de notification.
- Consolidation en un seul endroit de la gestion des appels de service multiplexés pour toutes les architectures.
- Ajout de la prise en charge du syscall multiplexé pour les architectures PowerPC (PPC) et MIPS.

- Modification de la signification de l'opération **SECCOMP_IOCTL_NOTIF_ID_VALID** dans le noyau.
- Modification de la logique de notification du descripteur de fichier **libseccomp** pour prendre en charge l'ancienne et la nouvelle utilisation de **SECCOMP_IOCTL_NOTIF_ID_VALID** par le noyau.
- Correction d'un bug où **seccomp_load()** ne pouvait être appelé qu'une seule fois.
- Modification de la gestion des notifications **fd** pour ne demander une notification **fd** que si le filtre a une action **_NOTIFY**.
- Ajout de la documentation sur **SCMP_ACT_NOTIFY** à la page de manuel **seccomp_add_rule(3)**.
- Clarification des clés GPG des mainteneurs.

(BZ#2019887)

Clevis prend désormais en charge SHA-256

Grâce à cette amélioration, le cadre Clevis prend en charge l'algorithme **SHA-256** en tant que hachage par défaut pour les empreintes de clés Web JSON (JWK), conformément aux recommandations de **RFC 7638**. Comme les anciennes empreintes (SHA-1) sont toujours prises en charge, vous pouvez toujours décrypter les données précédemment cryptées.

(BZ#1956760)

4.8. MISE EN RÉSEAU

Les modules diag sont désormais disponibles dans le noyau

Les modules **diag** sont désormais inclus dans l'image du noyau. Avec cette mise à jour, les modules **diag** n'ont plus besoin d'être chargés dynamiquement lorsque la commande **ss** est utilisée. Cela permet un meilleur débogage des problèmes de réseau, quelle que soit la politique du client concernant les modules du noyau. Modules inclus dans le noyau :

```
CONFIG_INET_DIAG
CONFIG_INET_RAW_DIAG
CONFIG_INET_TCP_DIAG
CONFIG_INET_UDP_DIAG
CONFIG_INET_MPTCP_DIAG
CONFIG_NETLINK_DIAG
CONFIG_PACKET_DIAG
CONFIG_UNIX_DIAG
```

(BZ#1948340)

Nouveaux paramètres du noyau et des réseaux liés à IPv4 sysctl

Par rapport aux versions précédentes de RHEL, le noyau RHEL 9.0 fournit les nouveaux paramètres de base et de réseau IPv4 suivants : **sysctl**:

- **net.core.devconf_inherit_init_net**
- **net.core.gro_normal_batch**

- **net.core.high_order_alloc_disable**
- **net.core.netdev_unregister_timeout_secs**
- **net.ipv4.fib_multipath_hash_fields**
- **net.ipv4.fib_notify_on_flag_change**
- **net.ipv4.fib_sync_mem**
- **net.ipv4.icmp_echo_enable_probe**
- **net.ipv4.ip_autobind_reuse**
- **net.ipv4.nexthop_compat_mode**
- **net.ipv4.raw_l3mdev_accept**
- **net.ipv4.tcp_comp_sack_slack_ns**
- **net.ipv4.tcp_migrate_req**
- **net.ipv4.tcp_mtu_probe_floor**
- **net.ipv4.tcp_no_ssthresh_metrics_save**
- **net.ipv4.tcp_reflect_tos**

Pour plus de détails sur ces paramètres, installez le paquetage **kernel-doc** et consultez les fichiers suivants :

- **/usr/share/doc/kernel-doc-<version>/Documentation/admin-guide/sysctl/net.rst**
- **/usr/share/doc/kernel-doc-<version>/Documentation/networking/ip-sysctl.rst**

(BZ#2068532)

Modification du comportement de firewalld lors de la transmission de paquets entre zones

Dans les pare-feu basés sur des zones, les paquets n'entrent que dans une seule zone. La transmission implicite de paquets est une violation du concept et peut autoriser le trafic ou les services de manière inattendue. Dans Red Hat Enterprise Linux 9, le service **firewalld** ne permet plus la transmission implicite de paquets entre deux zones différentes.

Pour plus d'informations sur ce changement, voir l'article de connaissance sur le comportement modifié de **firewalld** lors de la transmission de paquets entre zones .

(BZ#2029211)

Le transfert intra-zone a été activé par défaut

La fonctionnalité **firewalld** intra-zone forwarding permet de transférer le trafic entre des interfaces ou des sources au sein d'une zone firewalld. Depuis RHEL 9.0, cette fonctionnalité est activée par défaut. Utilisez l'option **--add-forward** de l'utilitaire **firewall-cmd** pour activer le transfert intra-zone pour une zone particulière. La commande **firewall-cmd --list-all** indique si le transfert intrazone est activé ou désactivé pour une zone :

```
# firewall-cmd --list-all
```

```
public (active)
  ...
  forward: no
```

(BZ#2089193)

Rendre Nmstate plus inclusif

Red Hat s'engage à utiliser un langage conscient. Pour plus de détails sur cette initiative, consultez le site Rendre l'open source plus inclusif . Par conséquent, le terme **slave** dans l'API **nmstate** a été remplacé par le terme **port**.

(BZ#1969941)

NetworkManager supporte les noms d'interface définis dans l'option du noyau **rd.znet_ifname** sur IBM Z

Avec cette amélioration, sur la plateforme IBM Z, NetworkManager interprète maintenant les options de ligne de commande **rd.znet** et **rd.znet_ifname** du noyau lors de l'installation ou du démarrage de Red Hat Enterprise Linux à partir du réseau. Par conséquent, il est possible de spécifier le nom d'une interface réseau identifiée par les sous-canaux au lieu du nom par défaut.

(BZ#1980387)

Le paquetage **hostapd** a été ajouté à RHEL 9.0

Avec cette version, RHEL fournit le paquetage **hostapd**. Cependant, Red Hat prend en charge **hostapd** uniquement pour configurer un hôte RHEL en tant qu'authentificateur 802.1X dans les réseaux Ethernet. D'autres scénarios, tels que les points d'accès Wi-Fi ou les authentificateurs dans les réseaux Wi-Fi, ne sont pas pris en charge.

Pour plus de détails sur la configuration de RHEL en tant qu'authentificateur 802.1X avec un back-end FreeRADIUS, voir Configuration d'un service d'authentification réseau 802.1x pour les clients LAN à l'aide d'hostapd avec un back-end FreeRADIUS.

(BZ#2019830)

ModemManager fourni dans la version 1.18.2

RHEL 9.0 fournit les paquets **ModemManager** dans la version amont 1.18.2. Cette version comprend des corrections de bogues et des améliorations par rapport à la version précédente, notamment :

- Amélioration des capacités et de la gestion des modes pour les appareils dotés de capacités 5G
- Prise en charge de dispositifs supplémentaires

Pour une liste complète des changements notables, lisez les notes de version en amont :

- https://github.com/freedesktop/ModemManager/blob/7a85bc243bc1be9f720ae1bda92e9eba7b
- https://github.com/freedesktop/ModemManager/blob/7a85bc243bc1be9f720ae1bda92e9eba7b

(BZ#1996716)

NetworkManager permet de modifier **queue_id** du port de liaison

Les ports NetworkManager dans un lien supportent maintenant le paramètre **queue_id**. En supposant que **eth1** est un port de l'interface de liaison, vous pouvez activer **queue_id** pour un port de liaison avec :

```
# nmcli connection modify eth1 bond-port.queue-id 1
# nmcli connection up eth1
```

Toute interface réseau qui doit utiliser cette option doit la configurer avec plusieurs appels jusqu'à ce que les priorités appropriées soient définies pour toutes les interfaces. Pour plus d'informations, voir le fichier **/usr/share/docs/kernel-doc-_<version>/Documentation/networking/bonding.rst** fourni par le paquetage **kernel-doc**.

(BZ#1949127)

Support de la configuration des types de routes blackhole, prohibit et unreachable avec la dernière version de NetworkManager

Le noyau prend en charge plusieurs types d'itinéraires en plus des types d'itinéraires communs **unicast**, **broadcast** et **local**. En outre, les utilisateurs peuvent désormais configurer les types de routes statiques **blackhole**, **prohibit** et **unreachable** dans le profil de connexion du NetworkManager. Le NetworkManager ajoutera un profil lorsque celui-ci sera activé.

(BZ#2060013)

Les adaptateurs RoCE Express utilisent désormais un schéma de dénomination des interfaces amélioré

Avec cette amélioration, les adaptateurs RDMA over Converged Ethernet (RoCE) Express utilisent le schéma de dénomination prévisible de l'interface et le connecteur Peripheral Communication Interface on z-system (zPCI). Dans ce schéma de dénomination, RHEL utilise l'identifiant de l'utilisateur (UID) ou l'identifiant de la fonction (FID) pour générer des noms uniques. Si aucun UID unique n'est disponible, RHEL utilise le FID pour définir le schéma de dénomination.

(BZ#2091653)

4.9. NOYAU

Version du noyau dans RHEL 9.0

Red Hat Enterprise Linux 9.0 est distribué avec la version 5.14.0-70 du noyau.

(BZ#2077836)

Red Hat, par défaut, active eBPF dans toutes les versions de RHEL pour les utilisateurs privilégiés uniquement

Extended Berkeley Packet Filter (**eBPF**) est une technologie complexe qui permet aux utilisateurs d'exécuter un code personnalisé à l'intérieur du noyau Linux. En raison de sa nature, le code **eBPF** doit passer par le vérificateur et d'autres mécanismes de sécurité. Il y a eu des cas de vulnérabilités et d'expositions communes (CVE), où des bogues dans ce code pouvaient être utilisés pour des opérations non autorisées. Pour atténuer ce risque, Red Hat a activé par défaut **eBPF** dans toutes les versions de RHEL pour les utilisateurs privilégiés uniquement. Il est possible d'activer **eBPF** pour les utilisateurs non privilégiés en utilisant le paramètre de ligne de commande kernel. **unprivileged_bpf_disabled=0**.

Il convient toutefois de noter que

- L'application de **unprivileged_bpf_disabled=0** disqualifie votre noyau de la prise en charge par Red Hat et expose votre système à des risques de sécurité.
- Red Hat vous conseille vivement de traiter les processus ayant la capacité **CAP_BPF** comme si cette capacité était égale à **CAP_SYS_ADMIN**.

- Le réglage de **unprivileged_bpf_disabled=0** ne sera pas suffisant pour exécuter de nombreux programmes BPF par des utilisateurs non privilégiés, car le chargement de la plupart des types de programmes BPF nécessite des capacités supplémentaires (généralement **CAP_SYS_ADMIN** ou **CAP_PERFMON**).

Pour plus d'informations sur l'application des paramètres de la ligne de commande du noyau, voir Configuration des paramètres de la ligne de commande du noyau .

(BZ#2091643)

Red Hat ne protège les symboles du noyau que pour les versions mineures

Red Hat garantit qu'un module du noyau continuera à se charger dans toutes les mises à jour futures au sein d'une version Extended Update Support (EUS), uniquement si vous compilez le module du noyau à l'aide de symboles protégés du noyau. Il n'y a pas de garantie d'ABI (Application Binary Interface) du noyau entre les versions mineures de RHEL 9.

(BZ#2059183)

Noyaux RHEL 9 Beta signés avec des certificats SecureBoot de confiance

Auparavant, les versions bêta de RHEL exigeaient des utilisateurs qu'ils inscrivent une clé publique bêta distincte à l'aide de la fonction MOK (Machine Owner Key). À partir de RHEL 9 Beta, les noyaux sont signés avec des certificats SecureBoot approuvés, et les utilisateurs n'ont donc plus besoin d'enregistrer une clé publique Beta distincte pour utiliser les versions Beta sur des systèmes dont l'UEFI Secure Boot est activé.

(BZ#2002499)

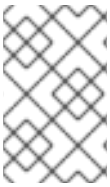
cgroup-v2 activé par défaut dans RHEL 9

La fonctionnalité des groupes de contrôle version 2 (**cgroup-v2**) met en œuvre un modèle hiérarchique unique qui simplifie la gestion des groupes de contrôle. Elle garantit également qu'un processus ne peut être membre que d'un seul groupe de contrôle à la fois. L'intégration approfondie avec **systemd** améliore l'expérience de l'utilisateur final lors de la configuration du contrôle des ressources sur un système RHEL.

Le développement de nouvelles fonctionnalités est principalement effectué pour **cgroup-v2**, qui possède certaines fonctionnalités manquantes dans **cgroup-v1**. De même, **cgroup-v1** contient certaines fonctionnalités héritées du passé qui sont absentes de **cgroup-v2**. En outre, les interfaces de contrôle sont différentes. Par conséquent, les logiciels tiers qui dépendent directement de **cgroup-v1** peuvent ne pas fonctionner correctement dans l'environnement **cgroup-v2**.

Pour utiliser **cgroup-v1**, vous devez ajouter les paramètres suivants à la ligne de commande du noyau :

```
systemd.unified_cgroup_hierarchy=0
systemd.legacy_systemd_cgroup_controller
```



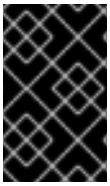
NOTE

cgroup-v1 et **cgroup-v2** sont tous deux pleinement activés dans le noyau. Il n'y a pas de version de groupe de contrôle par défaut du point de vue du noyau, et c'est **systemd** qui décide du montage au démarrage.

(BZ#1953515)

Modifications du noyau susceptibles d'affecter les modules tiers du noyau

Les distributions Linux dont la version du noyau est antérieure à la version 5.9 prenaient en charge l'exportation des fonctions GPL en tant que fonctions non GPL. Par conséquent, les utilisateurs pouvaient lier des fonctions propriétaires à des fonctions GPL du noyau par le biais du mécanisme **shim**. Avec cette version, le noyau RHEL incorpore des changements en amont qui améliorent la capacité de RHEL à appliquer la GPL en repoussant **shim**.



IMPORTANT

Les partenaires et les fournisseurs de logiciels indépendants (ISV) devraient tester leurs modules de noyau avec une version préliminaire de RHEL 9 pour s'assurer de leur conformité avec la GPL.

(BZ#1960556)

L'architecture ARM 64 bits a une taille de page de 4 Ko dans RHEL 9

Red Hat a sélectionné une taille de page de mémoire physique de 4 Ko pour l'architecture ARM 64 bits dans Red Hat Enterprise Linux 9. Cette taille correspond bien aux charges de travail et aux quantités de mémoire présentes sur la majorité des systèmes basés sur ARM. Pour utiliser efficacement des tailles de page importantes, utilisez l'option "huge pages" pour traiter une plus grande quantité de mémoire ou des charges de travail avec de grands ensembles de données.

Pour plus d'informations sur les grandes pages, voir Surveillance et gestion de l'état et des performances du système.

(BZ#1978382)

L'utilitaire **strace** affiche désormais correctement les incompatibilités de contexte SELinux

L'option **--secontext** de **strace** a été complétée par le paramètre **mismatch**. Ce paramètre permet d'imprimer le contexte attendu en même temps que le contexte réel en cas de non-concordance uniquement. La sortie est séparée par un double point d'exclamation (**!!**), d'abord le contexte réel, puis le contexte attendu. Dans les exemples ci-dessous, les paramètres **full,mismatch** affichent le contexte complet attendu en même temps que le contexte réel parce que la partie utilisateur des contextes ne correspond pas. Cependant, lors de l'utilisation d'un **mismatch** solitaire, il ne vérifie que la partie type du contexte. Le contexte attendu n'est pas imprimé car la partie type des contextes correspond.

```
[...]
$ strace --secontext=full,mismatch -e statx stat /home/user/file
statx(AT_FDCWD, "/home/user/file"
[system_u:object_r:user_home_t:s0!!unconfined_u:object_r:user_home_t:s0], ...

$ strace --secontext=mismatch -e statx stat /home/user/file
statx(AT_FDCWD, "/home/user/file" [user_home_t:s0], ...
```

Les erreurs de contexte SELinux sont souvent à l'origine de problèmes de contrôle d'accès associés à SELinux. Les incohérences indiquées dans les traces d'appels système peuvent accélérer considérablement les vérifications de l'exactitude du contexte SELinux. Les traces d'appels système peuvent également expliquer le comportement spécifique du noyau en ce qui concerne les vérifications du contrôle d'accès.

(BZ#2038965)

perf-top peut maintenant être trié par une certaine colonne

Avec cette mise à jour de l'outil de profilage du système **perf-top**, vous pouvez trier les échantillons en fonction d'une colonne d'événements arbitraire. Auparavant, les événements étaient triés par la première colonne dans le cas où plusieurs événements d'un groupe étaient échantillonnés. Pour trier les échantillons, utilisez l'option de ligne de commande **--group-sort-idx** et appuyez sur une touche numérique pour trier le tableau par la colonne de données correspondante. Notez que la numérotation des colonnes commence à **0**.

(BZ#1851933)

Nouveau paquet : jigawatts

Checkpoint/Restore In Userspace (CRIU) est un utilitaire Linux qui permet de vérifier et de restaurer des processus. Le paquetage **jigawatts** contient une bibliothèque Java qui vise à améliorer l'utilisation des mécanismes CRIU à partir d'applications Java.

(BZ#1972029)

La commande trace-cmd reset a un nouveau comportement

Auparavant, la commande **trace-cmd reset** réinitialisait la configuration de **tracing_on** à 0. Le nouveau comportement de **trace-cmd reset** est de réinitialiser **tracing_on** à sa valeur par défaut 1.

(BZ#1933980)

Le filtre de paquets Berkeley étendu est pris en charge dans RHEL 9

Le site **Extended Berkeley Packet Filter (eBPF)**est une machine virtuelle intégrée au noyau qui permet l'exécution de code dans l'espace du noyau, dans l'environnement restreint du bac à sable, avec un accès à un ensemble limité de fonctions. La machine virtuelle exécute un code spécial de type assemblage.

Le bytecode **eBPF** est d'abord chargé dans le noyau. Ensuite, le bytecode est vérifié et traduit en code machine natif avec une compilation juste à temps. Enfin, la machine virtuelle exécute le code.

Red Hat fournit de nombreux composants qui utilisent la machine virtuelle **eBPF**. Dans RHEL 9, ces composants incluent :

- Le paquet **BPF Compiler Collection (BCC)**, qui fournit des outils pour l'analyse des E/S, la mise en réseau et la surveillance des systèmes d'exploitation Linux utilisant **eBPF**.
- La bibliothèque **BCC**, qui permet de développer des outils similaires à ceux fournis dans le paquet d'outils **BCC**.
- Le langage de traçage **bpftrace**.
- Le paquet **libbpf**, qui est essentiel pour le développement de **bpf** et les applications liées à **bpf** comme **bpftrace**.
    - Les parties de l'API **XDP** et **AF_XDP** de la bibliothèque **libbpf** ne sont pas prises en charge et pourraient être supprimées dans une prochaine version.
- La fonction **eBPF for Traffic Control (tc)** qui permet un traitement programmable des paquets à l'intérieur du chemin de données du réseau du noyau.
- La fonction **eXpress Data Path (XDP)**, qui permet d'accéder aux paquets reçus avant que la pile réseau du noyau ne les traite. Red Hat prend en charge **XDP** uniquement s'il est utilisé par le biais de la bibliothèque **libxdp**.

- Le paquet **xdp-tools**, qui contient des utilitaires de prise en charge de l'espace utilisateur pour la fonctionnalité **XDP** et qui est pris en charge par les architectures AMD64 et Intel64. Le paquetage **xdp-tools** comprend :
  - La bibliothèque **libxdp**.
  - L'utilitaire **xdp-loader** pour le chargement des programmes XDP.
  - Le programme d'exemple **xdp-filter** pour le filtrage de paquets.
  - L'utilitaire **xdpdump** pour capturer les paquets d'une interface réseau avec **XDP** activé. L'utilitaire **xdpdump** n'est actuellement pris en charge que sur les architectures AMD64 et Intel64. Il est disponible pour d'autres architectures en tant qu'aperçu technologique.
- La prise **AF_XDP** pour connecter le chemin **eXpress Data Path (XDP)** à l'espace utilisateur.

(BZ#2070506)

RHEL 9 fournit l'utilitaire crash version 8.0.0

RHEL 9 est distribué avec l'utilitaire **crash** version 8.0.0. Les corrections de bogues et les améliorations notables sont les suivantes :

- Ajoute le nouveau paramètre **offset** dans la commande **add-symbol-file**. Ce support permet d'établir le lien entre **kaslr_offset** et **gdb**.
- Mise à jour du site **gdb-7.6** vers **gdb-10.2**.

(BZ#1896647)

makedumpfile prend désormais en charge une capacité de compression améliorée de zstd

Avec cette amélioration, le site **makedumpfile** inclut désormais la capacité de compression Zstandard (**zstd**), qui offre des taux de compression élevés. Cette amélioration est particulièrement utile pour les systèmes à grande mémoire.

La capacité de compression de **zstd** présente désormais un bon équilibre entre la taille du vidage de **vmcore** et la durée de la compression par rapport aux taux de compression précédents. En conséquence, le mécanisme de compression amélioré crée maintenant un fichier **vmcore** plus petit avec un temps de compression acceptable.

Notez qu'un bon taux de compression dépend également de la manière dont le système est utilisé et du type de données stockées dans la mémoire vive.

(BZ#1988894)

numatop activé sur les processeurs de serveurs évolutifs Intel Xeon

numatop est un outil qui suit et analyse le comportement des processus et des threads s'exécutant sur des systèmes NUMA et affiche des mesures permettant d'identifier les goulets d'étranglement liés aux performances des NUMA.

numatop utilise les technologies d'échantillonnage des compteurs de performance d'Intel et associe les données de performance aux informations du système Linux **runtime**, afin de fournir une analyse des systèmes de production.

(BZ#1874125)

kexec_file_load a été ajouté comme option par défaut pour RHEL 9

Cette mise à jour ajoute l'appel système **kexec_file_load** pour l'architecture ARM 64 bits. Elle fournit un chargeur in-kernel **kexec** pour **kdump**. Auparavant, le noyau empêchait le chargement d'images de noyau non signées lorsque l'option de démarrage sécurisé était activée. Le mécanisme **kdump** essayait d'abord de détecter si l'amorçage sécurisé était activé et choisissait ensuite l'interface d'amorçage à exécuter. Par conséquent, un noyau non signé ne parvenait pas à se charger lorsque l'amorçage sécurisé était activé et que **kexec_file_load()** était spécifié.

Cette mise à jour corrige le problème et un noyau non signé fonctionne correctement dans le scénario décrit.

(BZ#1895232)

makedumpfile inclut désormais des options améliorées pour obtenir une estimation de la taille de vmcore

Avec cette implémentation, l'utilitaire **makedumpfile** inclut maintenant les options suivantes qui aident à imprimer une estimation de la taille du dump pour le noyau en cours d'exécution :

- **--dry-run** effectue toutes les opérations spécifiées par les autres options mais n'écrit pas le fichier de sortie.
- **--show-stats** imprime les messages du rapport. Il s'agit d'une alternative à l'activation du bit 4 dans l'option level provided to **--message-level**.

L'exemple suivant montre l'utilisation de **--dry-run** et **--show-stats**:

```
$ makedumpfile --dry-run --show-stats -l --message-level 7 -d 31 /proc/kcore dump.dummy
```

Notez que la taille du fichier dump peut varier en fonction de l'état du système au moment de la panique et que l'estimation fournie par les options peut différer de l'état réel.

(BZ#1958452)

Le paquet kexec-tools prend désormais en charge les valeurs de réservation de mémoire par défaut de crashkernel pour RHEL 9

Le paquetage **kexec-tools** conserve désormais les valeurs par défaut de réservation de la mémoire **crashkernel**. Le service **kdump** utilise la valeur par défaut pour réserver la mémoire **crashkernel** pour chaque noyau. Cette implémentation améliore également l'allocation de la mémoire pour **kdump** lorsqu'un système dispose de moins de 4 Go de mémoire disponible.

Pour demander la valeur par défaut du crashkernel :

```
$ kdumpctl get-default-crashkernel
```

Si la mémoire réservée par la valeur par défaut **crashkernel** n'est pas suffisante sur votre système, augmentez le paramètre **crashkernel**.

Notez que l'option **crashkernel=auto** de la ligne de commande de démarrage n'est plus prise en charge dans RHEL 9 et les versions ultérieures.

Pour plus d'informations, voir le fichier **/usr/share/doc/kexec-tools/crashkernel-howto.txt**.

(BZ#2034490)

L'ordonnancement des noyaux est pris en charge dans RHEL 9

Grâce à la fonctionnalité de planification de base, les utilisateurs peuvent empêcher les tâches qui ne devraient pas se faire confiance de partager le même cœur d'unité centrale. De même, les utilisateurs peuvent définir des groupes de tâches qui peuvent partager un cœur d'unité centrale.

Ces groupes peuvent être spécifiés :

- Améliorer la sécurité en atténuant certaines attaques SMT (Multithreading symétrique)
- Pour isoler les tâches qui nécessitent un cœur entier. Par exemple, pour les tâches dans des environnements en temps réel, ou pour les tâches qui reposent sur des caractéristiques spécifiques du processeur telles que le traitement SIMD (Single Instruction, Multiple Data)

Pour plus d'informations, voir Core Scheduling.

(JIRA:RHELPLAN-100497)

Amélioration des performances sur l'architecture ARM 64 bits en utilisant par défaut le mode iommu non strict

Avec cette mise à jour, l'architecture ARM 64 bits utilise par défaut le domaine d'accès direct à la mémoire (DMA) paresseux pour l'unité de gestion de la mémoire système (SMMU). Tout en apportant un gain de performance significatif, cela peut introduire une fenêtre entre un désappairage d'adresse et un vidage du Translation Lookaside Buffer (TLB) sur l'unité de gestion de la mémoire du système. Dans les versions précédentes, l'architecture ARM 64 bits configurait par défaut les domaines DMA stricts, ce qui entraînait une baisse des performances en raison de la taille de page de 4 Ko.

Si vous devez utiliser le mode de domaine DMA strict, spécifiez le mode **iommu.strict=1** à l'aide de la ligne de commande du noyau. Notez que l'utilisation de domaines DMA stricts peut entraîner une baisse des performances sur les architectures ARM 64 bits.

(BZ#2050415)

L'arborescence des sources de kernel-rt a été mise à jour vers l'arborescence RHEL 9.0

Les sources de **kernel-rt** ont été mises à jour pour utiliser la dernière arborescence des sources du noyau Red Hat Enterprise Linux. Le jeu de correctifs en temps réel a également été mis à jour vers la dernière version en amont, v5.15-rt19. Ces mises à jour apportent un certain nombre de corrections de bogues et d'améliorations.

(BZ#2002474)

Prise en charge du hotplug de l'unité centrale dans les PMU hv_24x7 et hv_gpci

Avec cette mise à jour, les compteurs PMU réagissent correctement au branchement à chaud d'une unité centrale. Par conséquent, si un compteur d'événements **hv_gpci** fonctionne sur une unité centrale qui est désactivée, le comptage est redirigé vers une autre unité centrale.

(BZ#1844416)

Les mesures pour les événements de nidification du POWERPC hv_24x7 sont maintenant disponibles

Des mesures pour les événements de nidification POWERPC **hv_24x7** sont maintenant disponibles pour **perf**. En agrégeant plusieurs événements, ces mesures permettent de mieux comprendre les valeurs obtenues à partir des compteurs **perf** et l'efficacité avec laquelle l'unité centrale est capable de traiter la charge de travail.

(BZ#1780258)

Le pilote IRDMA a été introduit dans RHEL 9

Le pilote IRDMA active la fonctionnalité RDMA sur les périphériques réseau Intel® compatibles RDMA. Les périphériques pris en charge par ce pilote sont les suivants :

- Contrôleur Ethernet Intel® E810
- Adaptateur réseau Ethernet Intel® X722

RHEL 9 propose une mise à jour du pilote Intel® Ethernet Protocol Driver for RDMA (IRDMA) pour le périphérique X722 Internet Wide-area RDMA Protocol (iWARP). RHEL 9 introduit également un nouveau périphérique E810 qui prend en charge iWARP et RDMA over Converged Ethernet (RoCEv2). Le module IRDMA remplace l'ancien module i40iw pour X722 et étend l'interface ABI (Application Binary Interface) définie pour i40iw. Ce changement est rétrocompatible avec l'ancien fournisseur RDMA-Core de X722 (libi40iw).

- L'appareil X722 ne prend en charge que l'iWARP et un ensemble plus limité de paramètres de configuration.
- Le périphérique E810 prend en charge l'ensemble des fonctions RDMA et de gestion de la congestion suivantes :
  - transports RDMA iWARP et RoCEv2
  - Contrôle de flux prioritaire (PFC)
  - Notification explicite de congestion (ECN)

(BZ#1874195)

Un nouveau paramètre pour le module kernel bonding: lacp_active

RHEL 9 introduit le paramètre **lacp_active** pour le module du noyau **bonding**. Ce paramètre indique s'il faut envoyer des trames LACPDU (Link Aggregation Control Protocol Data Unit) à des intervalles spécifiés. Les options sont les suivantes :

- **on** (par défaut) - permet d'envoyer les trames LACPDU avec le paramètre configuré **lacp_rate**
- **off** - les trames LACPDU jouent le rôle de "parler quand on vous parle"

Notez que les trames d'état LACPDU sont toujours envoyées lorsque vous initialisez ou libérez un port.

(BZ#1951951)

4.10. CHARGEUR DE DÉMARRAGE

Les fichiers de configuration du chargeur d'amorçage sont unifiés pour toutes les architectures de processeurs

Les fichiers de configuration du chargeur de démarrage GRUB sont désormais stockés dans le répertoire **/boot/grub2/** sur toutes les architectures de processeurs prises en charge. Le fichier **/boot/efi/EFI/redhat/grub.cfg**, que GRUB utilisait auparavant comme fichier de configuration principal sur les systèmes UEFI, charge désormais simplement le fichier **/boot/grub2/grub.cfg**.

Cette modification simplifie la présentation du fichier de configuration GRUB, améliore l'expérience de l'utilisateur et apporte les avantages notables suivants :

- Vous pouvez démarrer la même installation avec le système EFI ou le BIOS traditionnel.
- Vous pouvez utiliser la même documentation et les mêmes commandes pour toutes les architectures.
- Les outils de configuration de GRUB sont plus robustes, car ils ne s'appuient plus sur les liens symboliques et n'ont pas à gérer les cas spécifiques à une plate-forme.
- L'utilisation des fichiers de configuration GRUB est alignée sur les images générées par CoreOS Assembler (COSA) et OSBuild.
- L'utilisation des fichiers de configuration GRUB est alignée sur les autres distributions Linux.

(JIRA:RHELPLAN-101246)

4.11. SYSTÈMES DE FICHIERS ET STOCKAGE

Les options des utilitaires Samba ont été renommées et supprimées pour une expérience utilisateur cohérente

Les utilitaires Samba ont été améliorés afin de fournir une interface de ligne de commande cohérente. Ces améliorations comprennent des options renommées ou supprimées. Par conséquent, pour éviter tout problème après la mise à jour, passez en revue vos scripts qui utilisent les utilitaires Samba et mettez-les à jour si nécessaire.

Samba 4.15 apporte les modifications suivantes aux utilitaires Samba :

- Auparavant, les utilitaires de ligne de commande Samba ignoraient silencieusement les options inconnues. Pour éviter tout comportement inattendu, les utilitaires rejettent désormais systématiquement les options inconnues.
- Plusieurs options de ligne de commande ont maintenant une variable **smb.conf** correspondante pour contrôler leur valeur par défaut. Consultez les pages de manuel des utilitaires pour savoir si une option de ligne de commande a un nom de variable **smb.conf**.
- Par défaut, les utilitaires Samba se connectent à l'erreur standard (**stderr**). Utilisez l'option **--debug-stdout** pour modifier ce comportement.
- L'option **--client-protection=off|sign|encrypt** a été ajoutée à l'analyseur commun.
- Les options suivantes ont été renommées dans tous les utilitaires :
  - **--kerberos** à **--use-kerberos=required|desired|off**
  - **--krb5-ccache** à **--use-krb5-ccache=*CCACHE***
  - **--scope** à **--netbios-scope=*SCOPE***
  - **--use-ccache** à **--use-winbind-ccache**
- Les options suivantes ont été supprimées de tous les utilitaires :
  - **-e** et **--encrypt**
  - **-C** retiré de **--use-winbind-ccache**
  - **-i** retiré de **--netbios-scope**

    - **-S** et **--signing**

- Pour éviter les doublons, certaines options ont été supprimées ou renommées dans les utilitaires suivants :
    - **ndrdump**le site **-l** n'est plus disponible pour les **--load-dso**
    - **net**le site **-l** n'est plus disponible pour les **--long**
    - **sharesec**le site **-V** n'est plus disponible pour les **--viewsddl**
    - **smbcquotas**: **--user** a été renommé en **--quota-user**
    - **nmbd**: **--log-stdout** a été renommé en **--debug-stdout**
    - **smbd**: **--log-stdout** a été renommé en **--debug-stdout**
    - **winbindd**: **--log-stdout** a été renommé en **--debug-stdout**

(BZ#2065646)

Changements dans le client et le serveur NFS dans RHEL 9

- Le serveur et le client NFS RHEL 9.0 ne prennent plus en charge le type de chiffrement GSS Kerberos 5 non sécurisé **des-cbc-crc**.
- Le client NFS ne prend plus en charge le montage de systèmes de fichiers utilisant des transports UDP.

(BZ#1952863)

Les systèmes de fichiers GFS2 sont désormais créés avec le format version 1802

Les systèmes de fichiers GFS2 dans RHEL 9 sont créés avec le format version 1802. Cela permet les fonctionnalités suivantes :

- Les attributs étendus de l'espace de noms **trusted** ("trusted.* xattrs") sont reconnus par **gfs2** et **gfs2-utils**.
- L'option **rgrplvb** est active par défaut. Elle permet à **gfs2** d'attacher des données de groupe de ressources mises à jour aux demandes de verrouillage DLM, de sorte que le nœud qui acquiert le verrouillage n'a pas besoin de mettre à jour les informations de groupe de ressources à partir du disque. Cela améliore les performances dans certains cas.

Les systèmes de fichiers créés avec la nouvelle version du format ne pourront pas être montés sous les versions antérieures de RHEL et les anciennes versions de l'utilitaire **fsck.gfs2** ne pourront pas les vérifier.

Les utilisateurs peuvent créer un système de fichiers avec l'ancienne version du format en exécutant la commande **mkfs.gfs2** avec l'option **-o format=1801**.

Les utilisateurs peuvent mettre à jour la version du format d'un ancien système de fichiers fonctionnant sur un système de fichiers non monté **tunegfs2 -r 1802 *device*** sur un système de fichiers non monté. La rétrogradation de la version du format n'est pas prise en charge.

(BZ#1616432)

RHEL 9 fournit la version 1.10.1 du paquet nvml

RHEL 9.0 met à jour le paquetage **nvml** vers la version 1.10.1. Cette mise à jour ajoute des fonctionnalités et corrige un bogue potentiel de corruption de données en cas de perte d'alimentation.

(BZ#1874208)

La prise en charge du système de fichiers exFAT a été ajoutée

RHEL 9.0 prend en charge le système de fichiers Extensible File Allocation Table (exFAT). Vous pouvez désormais monter, formater et utiliser de manière générale ce système de fichiers, qui est généralement utilisé par défaut sur la mémoire flash.

(BZ#1943423)

rpcctl la commande affiche désormais les informations de connexion SunRPC

Avec cette mise à jour, vous pouvez utiliser la commande **rpcctl** pour afficher les informations collectées dans les fichiers SunRPC **sysfs** sur les objets SunRPC du système. Vous pouvez afficher, supprimer et définir des objets dans la couche réseau SunRPC via le système de fichiers **sysfs**.

(BZ#2059245)

Limiter l'ensemble des périphériques pour LVM

Par défaut, LVM dans RHEL 9 n'utilise que les périphériques que vous sélectionnez explicitement. Utilisez les nouvelles commandes **lvmdevices** et **vgimportdevices** pour sélectionner des périphériques spécifiques. L'utilisation des commandes **pvcreate**, **vgcreate** et **vgextend** sélectionne indirectement de nouveaux périphériques pour **lvm**, s'ils n'ont pas déjà été sélectionnés. LVM ignore les périphériques attachés au système jusqu'à ce que vous les sélectionniez à l'aide de l'une de ces commandes. La commande **lvm** enregistre la liste des périphériques sélectionnés dans le fichier de périphériques **/etc/lvm/devices/system.devices**. Le filtre **lvm.conf** ou tout autre filtre de configuration en ligne de commande ne fonctionne pas lorsque vous activez la fonctionnalité du nouveau fichier de périphériques. Si vous supprimez ou désactivez le fichier de périphériques, LVM applique le filtre à tous les périphériques connectés. Pour obtenir des informations détaillées sur cette fonctionnalité, consultez la page de manuel **lvmdevices(8)**.

(BZ#1749513)

L'hôte NVMe/TCP avec nvme_tcp.ko est désormais entièrement pris en charge

Le stockage Nonvolatile Memory Express (NVMe) sur les réseaux TCP/IP (NVMe/TCP) avec le module du noyau **nvme_tcp.ko** est désormais entièrement pris en charge. La cible NVMe/TCP avec le module **nvmet_tcp.ko** est disponible avec un statut Unmaintained dans RHEL 9.0.

(BZ#2054441)

multipathd permet désormais de détecter les événements FPIN-Li

Lorsque vous ajoutez une nouvelle valeur **fpin** à l'option de configuration **marginal_pathgroups**, vous permettez à **multipathd** de surveiller les événements PFIN-Li (Link Integrity Fabric Performance Impact Notification) et de déplacer les chemins présentant des problèmes d'intégrité de lien vers un groupe de chemins marginaux. Avec la valeur **fpin**, **multipathd** remplace les méthodes de détection des chemins marginaux existantes et s'appuie sur la structure Fibre Channel pour identifier les problèmes d'intégrité des liens.

Grâce à cette amélioration, la méthode **multipathd** devient plus robuste dans la détection des chemins marginaux sur les tissus Fibre Channel qui peuvent émettre des événements PFIN-Li.

(BZ#2053642)

4.12. HAUTE DISPONIBILITÉ ET CLUSTERS

Le méta-attribut de ressource **resource-stickiness** est désormais fixé par défaut à 1 au lieu de 0 pour les grappes nouvellement créées

Auparavant, la valeur par défaut du méta-attribut **resource-stickiness** resource était de 0 pour les clusters nouvellement créés. La valeur par défaut de ce méta-attribut est désormais de 1.

Avec une adhérence de 0, une grappe peut déplacer des ressources si nécessaire pour équilibrer les ressources entre les nœuds. Les ressources peuvent donc se déplacer lorsque des ressources non apparentées démarrent ou s'arrêtent. Avec un taux de fidélité positif, les ressources préfèrent rester là où elles sont et ne se déplacent que si d'autres circonstances l'emportent sur le taux de fidélité. Cela peut avoir pour conséquence que les nœuds nouvellement ajoutés ne se voient pas attribuer de ressources sans l'intervention de l'administrateur. Les deux approches ont un comportement potentiellement inattendu, mais la plupart des utilisateurs préfèrent une certaine rigidité. La valeur par défaut de ce méta-attribut a été fixée à 1 pour refléter cette préférence.

Seules les grappes nouvellement créées sont concernées par cette modification, de sorte que le comportement ne change pas pour les grappes existantes. Les utilisateurs qui préfèrent l'ancien comportement pour leur cluster peuvent supprimer l'entrée **resource-stickiness** des ressources par défaut.

(BZ#1850145)

Nouvel indicateur de groupe de volume LVM pour contrôler l'auto-activation

Les groupes de volumes LVM prennent désormais en charge l'indicateur **setautoactivation** qui détermine si les volumes logiques que vous créez à partir d'un groupe de volumes seront automatiquement activés au démarrage. Lors de la création d'un groupe de volumes qui sera géré par Pacemaker dans un cluster, définissez cet indicateur sur **n** avec la commande **vgcreate --setautoactivation n** pour le groupe de volumes afin d'éviter une éventuelle corruption des données. Si vous disposez d'un groupe de volumes existant utilisé dans un cluster Pacemaker, définissez l'indicateur avec **vgchange --setautoactivation n**.

(BZ#1899214)

Nouvelles commandes d'affichage de l'état des ressources pcs

Les commandes **pcs resource status** et **pcs stonith status** prennent désormais en charge les options suivantes :

- Vous pouvez afficher l'état des ressources configurées sur un nœud spécifique à l'aide de la commande **pcs resource status node=*node_id*** et la commande **pcs stonith status node=*node_id*** et la commande Vous pouvez utiliser ces commandes pour afficher l'état des ressources sur les nœuds de cluster et les nœuds distants.

- Vous pouvez afficher l'état d'une seule ressource à l'aide des boutons **pcs resource status *resource_id*** et la commande **pcs stonith status *resource_id*** pour afficher l'état d'une seule ressource.

- Vous pouvez afficher l'état de toutes les ressources avec une balise spécifiée à l'aide des boutons **pcs resource status *tag_id*** et la commande **pcs stonith status *tag_id*** pour afficher l'état de toutes les ressources dont la balise est spécifiée.

(BZ#1290830, BZ#1285269)

Nouvelle option d'affichage réduit pour la commande **pcs resource safe-disable**

Les commandes **pcs resource safe-disable** et **pcs resource disable --safe** impriment un long résultat de simulation après un rapport d'erreur. Vous pouvez désormais spécifier l'option **--brief** pour ces commandes afin de n'imprimer que les erreurs. Le rapport d'erreur contient toujours les identifiants des ressources affectées.

(BZ#1909901)

Nouvelle commande pcs pour mettre à jour le dispositif de clôture SCSI sans provoquer le redémarrage de toutes les autres ressources

La mise à jour d'un dispositif de clôture SCSI à l'aide de la commande **pcs stonith update** entraîne le redémarrage de toutes les ressources s'exécutant sur le même nœud que celui où s'exécutait la ressource stonith. La nouvelle commande **pcs stonith update-scsi-devices** vous permet de mettre à jour les périphériques SCSI sans provoquer le redémarrage des autres ressources du cluster.

(BZ#1872378)

Possibilité de configurer un SBD avec chien de garde uniquement pour la clôture d'un sous-ensemble de nœuds de la grappe

Auparavant, pour utiliser une configuration SBD avec chien de garde uniquement, tous les nœuds de la grappe devaient utiliser le SBD. Cela empêchait d'utiliser le SMD dans un cluster où certains nœuds le supportent mais où d'autres nœuds (souvent des nœuds distants) ont besoin d'une autre forme de clôture. Les utilisateurs peuvent désormais configurer une configuration SBD avec chien de garde uniquement à l'aide du nouvel agent **fence_watchdog**, qui permet de configurer des clusters dans lesquels seuls certains nœuds utilisent le SBD avec chien de garde uniquement pour le clôturage et d'autres nœuds utilisent d'autres types de clôturage. Un cluster ne peut avoir qu'un seul dispositif de ce type, et il doit être nommé **watchdog**.

(BZ#1443666)

Affichage détaillé de l'état du stimulateur cardiaque pour les erreurs internes

Si Pacemaker ne peut pas exécuter une ressource ou un agent de clôture pour une raison quelconque, par exemple si l'agent n'est pas installé ou s'il y a eu un dépassement de délai interne, les écrans d'état de Pacemaker affichent désormais un motif de sortie détaillé pour l'erreur interne.

(BZ#1470834)

Le paramètre pcmk_delay_base peut désormais prendre des valeurs différentes selon les nœuds

Lors de la configuration d'un dispositif de clôture, vous pouvez désormais spécifier des valeurs différentes pour différents nœuds à l'aide de l'adresse **pcmk_delay_base parameter**. Cela permet d'utiliser un seul dispositif de clôture dans un cluster à deux nœuds, avec un délai différent pour chaque nœud. Cela permet d'éviter que chaque nœud tente de clôturer l'autre nœud en même temps. Pour spécifier des valeurs différentes pour les différents nœuds, vous mappez les noms d'hôte à la valeur de délai pour ce nœud en utilisant une syntaxe similaire à celle de pcmk_host_map. Par exemple, node1:0;node2:10s n'utilise pas de délai pour clôturer le nœud 1 et un délai de 10 secondes pour clôturer le nœud 2.

(BZ#1082146)

Prise en charge des caractères spéciaux dans les valeurs pcmk_host_map

La propriété **pcmk_host_map** prend désormais en charge les caractères spéciaux dans les valeurs **pcmk_host_map** en utilisant une barre oblique inverse (\N) devant la valeur. Par exemple, vous pouvez spécifier **pcmk_host_map="node3:plug\ 1"** pour inclure un espace dans l'alias de l'hôte.

(BZ#1376538)

Nouvel agent de clôture pour OpenShift

L'agent de clôture **fence_kubevirt** est désormais disponible pour une utilisation avec RHEL High Availability sur Red Hat OpenShift Virtualization. Pour plus d'informations sur l'agent **fence_kubevirt**, consultez la page de manuel **fence_kubevirt**(8).

(BZ#1977588)

La version en mode local de la commande pcs cluster setup est désormais entièrement prise en charge

Par défaut, la commande **pcs cluster setup** synchronise automatiquement tous les fichiers de configuration sur les nœuds du cluster. La commande **pcs cluster setup** prend désormais en charge l'option **--corosync-conf**. En spécifiant cette option, la commande passe en mode **local**. Dans ce mode, l'interface de ligne de commande **pcs** crée un fichier **corosync.conf** et l'enregistre dans un fichier spécifié sur le nœud local uniquement, sans communiquer avec aucun autre nœud. Cela vous permet de créer un fichier **corosync.conf** dans un script et de gérer ce fichier au moyen du script.

(BZ#2008558)

Suppression automatique des contraintes de localisation à la suite d'un déplacement de ressources

Lorsque vous exécutez la commande **pcs resource move**, vous ajoutez une contrainte à la ressource pour l'empêcher de s'exécuter sur le nœud sur lequel elle s'exécute actuellement. Par défaut, la contrainte d'emplacement créée par la commande est automatiquement supprimée une fois que la ressource a été déplacée. Cela ne ramène pas nécessairement les ressources sur le nœud d'origine ; l'endroit où les ressources peuvent s'exécuter à ce moment-là dépend de la manière dont vous avez configuré vos ressources au départ. Si vous souhaitez déplacer une ressource et laisser en place la contrainte qui en résulte, utilisez la commande **pcs resource move-with-contraint**.

(BZ#2008575)

pcs support pour la norme OCF Resource Agent API 1.1

L'interface en ligne de commande **pcs** prend désormais en charge les agents OCF 1.1 resource et STONITH. Dans le cadre de la mise en œuvre de ce support, les métadonnées de tout agent doivent être conformes au schéma OCF, que l'agent soit un agent OCF 1.0 ou OCF 1.1. Si les métadonnées d'un agent ne sont pas conformes au schéma OCF, **pcs** considère que l'agent n'est pas valide et ne créera pas ou ne mettra pas à jour une ressource de l'agent, sauf si l'option **--force** est spécifiée. L'interface Web **pcsd** et les commandes **pcs** pour lister les agents omettent désormais les agents dont les métadonnées ne sont pas valides.

(BZ#2018969)

pcs accepte désormais Promoted et Unpromoted comme noms de rôle

L'interface de ligne de commande **pcs** accepte désormais **Promoted** et **Unpromoted** partout où des rôles sont spécifiés dans la configuration de Pacemaker. Ces noms de rôles sont l'équivalent fonctionnel des rôles **Master** et **Slave** de Pacemaker dans les versions précédentes de RHEL, et ce sont les noms de rôles qui sont visibles dans les affichages de configuration et les pages d'aide.

(BZ#2009455)

Version actualisée de l'interface web pcsd

L'interface Web **pcsd**, l'interface utilisateur graphique permettant de créer et de configurer les clusters

Pacemaker/Corosync, a été mise à jour. L'interface Web mise à jour offre une expérience utilisateur améliorée et une interface standardisée qui est construite avec le cadre PatternFly utilisé dans d'autres applications Web de Red Hat.

(BZ#1996067)

4.13. LANGAGES DE PROGRAMMATION DYNAMIQUES, SERVEURS WEB ET DE BASE DE DONNÉES

Python dans RHEL 9

Python 3.9 est l'implémentation par défaut de **Python** dans RHEL 9. **Python 3.9** est distribué dans un paquet RPM **python3** non modulaire dans le dépôt BaseOS et est généralement installé par défaut. **Python 3.9** sera pris en charge pendant toute la durée de vie de RHEL 9.

Les versions supplémentaires de **Python 3** seront distribuées sous forme de paquets RPM avec un cycle de vie plus court via le dépôt AppStream et pourront être installées en parallèle.

La commande **python** (**/usr/bin/python**), ainsi que d'autres commandes liées à **Python**, telles que **pip**, sont disponibles sous forme non versionnée et renvoient à la version par défaut **Python 3.9**.

Python 2 n'est pas distribué avec RHEL 9.

Pour plus d'informations sur **Python** dans RHEL 9, voir Introduction à Python.

(BZ#1941595, JIRA:RHELPLAN-80598)

Node.js 16 disponible dans RHEL 9

RHEL 9 fournit la version 16 du support à long terme (LTS) de **Node.js**, une plate-forme de développement logiciel pour la création d'applications réseau rapides et évolutives dans le langage de programmation JavaScript.

Les changements notables survenus sur **Node.js 16** à partir de **Node.js 14** sont les suivants :

- Le moteur **V8** est passé à la version 9.4.
- Le gestionnaire de paquets **npm** a été mis à niveau vers la version 8.3.1.
- Une nouvelle API **Timers Promises** fournit un ensemble alternatif de fonctions de minuterie qui renvoient des objets **Promise**.
- **Node.js** est désormais compatible avec **OpenSSL 3.0**.
- **Node.js** fournit désormais une nouvelle API expérimentale **Web Streams** et une API expérimentale de crochets de chargement de modules ECMAScript (ESM).

Node.js 16 est la version initiale de ce flux d'applications, que vous pouvez installer facilement en tant que paquetage RPM. **Node.js 16** a un cycle de vie plus court que RHEL 9. Pour plus de détails, consultez le document Red Hat Enterprise Linux Application Streams Life Cycle (cycle de vie des flux d'applications Red Hat Enterprise Linux). D'autres versions de **Node.js** seront fournies en tant que modules ayant également un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

(BZ#1953491)

RHEL 9 fournit Ruby 3.0

RHEL 9 est distribué avec **Ruby 3.0.3**, qui apporte un certain nombre d'améliorations de performance, de corrections de bogues et de sécurité, ainsi que de nouvelles fonctionnalités par rapport à **Ruby 2.7**.

Parmi les améliorations notables, citons

- Caractéristiques de concurence et de parallélisme :
  - **Ractor**une abstraction de modèle d'acteur qui permet une exécution parallèle sûre pour les threads, est fournie à titre expérimental.
  - **Fiber Scheduler** a été introduit à titre expérimental. **Fiber Scheduler** intercepte les opérations bloquantes, ce qui permet une concurrence légère sans modifier le code existant.
- Caractéristiques de l'analyse statique :
  - Le langage **RBS**, qui décrit la structure des programmes **Ruby**, a été introduit. La gemme **rbs** a été ajoutée pour analyser les définitions de type écrites en **RBS**.
  - L'utilitaire **TypeProf** a été introduit. Il s'agit d'un outil d'analyse de type pour le code **Ruby**.
- La recherche de motifs avec l'expression **case/in** n'est plus expérimentale.
- La recherche de motifs sur une ligne, qui est une fonctionnalité expérimentale, a été repensée.
- La fonction de recherche de motifs a été ajoutée à titre expérimental.

Les améliorations suivantes ont été apportées aux performances :

- Le collage d'un long code sur le site **Interactive Ruby Shell (IRB)** est désormais beaucoup plus rapide.
- La commande **measure** a été ajoutée à **IRB** pour la mesure du temps.

D'autres changements notables sont à signaler :

- Les arguments de type mot-clé sont désormais séparés des autres arguments.
- Le répertoire par défaut pour les gemmes installées par l'utilisateur est désormais **$HOME/.local/share/gem/**, sauf si le répertoire **$HOME/.gem/** est déjà présent.

Ruby 3.0 est la version initiale de ce flux d'applications que vous pouvez installer facilement sous la forme d'un paquetage RPM. D'autres versions de **Ruby** seront fournies sous forme de modules avec un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

(JIRA:RHELPLAN-80758)

RHEL 9 présente Perl 5.32

RHEL 9 inclut **Perl 5.32**, qui apporte un certain nombre de corrections de bogues et d'améliorations par rapport à la version 5.30.

Parmi les améliorations notables, on peut citer

- **Perl** supporte désormais la version 13.0 d'Unicode.
- L'opérateur de citation **qr** a été amélioré.

- Les fonctions **POSIX::mblen()**, **mbtowc**, et **wctomb** fonctionnent désormais sur les locales shift state et sont thread-safe sur les compilateurs C99 et supérieurs lorsqu'elles sont exécutées sur une plateforme qui dispose de la thread-safety locale ; les paramètres length sont désormais optionnels.
- Le nouvel opérateur infixe expérimental **isa** vérifie si un objet donné est une instance d'une classe donnée ou une classe dérivée.
- Les assertions alpha ne sont plus expérimentales.
- Les exécutions de scripts ne sont plus expérimentales.
- Les vérifications des caractéristiques sont désormais plus rapides.
- **Perl** peut désormais extraire les motifs compilés avant l'optimisation.

Perl 5.32 est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM. D'autres versions de **Perl** seront fournies sous forme de modules avec un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

(JIRA:RHELPLAN-80759)

RHEL 9 comprend PHP 8.0

RHEL 9 est distribué avec **PHP 8.0**, qui apporte un certain nombre de corrections de bogues et d'améliorations par rapport à la version 7.4.

Parmi les améliorations notables, citons

- Les nouveaux arguments nommés sont indépendants de l'ordre et auto-documentés, et vous permettent de ne spécifier que les paramètres requis.
- De nouveaux attributs permettent d'utiliser des métadonnées structurées avec la syntaxe native de PHP.
- Les nouveaux types d'union vous permettent d'utiliser des déclarations de type d'union natives qui sont validées au moment de l'exécution au lieu des annotations PHPDoc pour une combinaison de types.
- Les fonctions internes lèvent désormais plus systématiquement une exception d'erreur au lieu d'un avertissement en cas d'échec de la validation des paramètres.
- Les nouveaux moteurs de compilation Just-In-Time améliorent considérablement les performances des applications.
- L'extension de débogage et de productivité **Xdebug** pour PHP a été mise à jour à la version 3. Cette version introduit des changements majeurs dans les fonctionnalités et la configuration par rapport à **Xdebug 2**.

PHP 8.0 est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM. D'autres versions de **PHP** seront fournies sous forme de modules avec un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

Pour plus d'informations, voir Utilisation du langage de script PHP .

(BZ#1949319)

RHEL 9 fournit Git 2.31 et Git LFS 2.13

RHEL 9 est distribué avec **Git 2.31** qui fournit un certain nombre d'améliorations et de performances par rapport à la version 2.27 disponible dans RHEL 8. Les changements les plus importants sont les suivants :

- La commande **git status** indique désormais l'état de la vérification des données éparses (sparse checkout).
- Vous pouvez désormais utiliser l'option **--add-file** avec la commande **git archive** pour inclure des fichiers non suivis dans un instantané à partir d'un identifiant de type arbre.
- Vous pouvez utiliser la variable de configuration **clone.defaultremotename** pour personnaliser le surnom du référentiel distant source.
- Vous pouvez configurer la longueur maximale des noms de fichiers de sortie créés par la commande **git format-patch**. Auparavant, la limite de longueur était de 64 octets.
- La prise en charge de la bibliothèque PCRE1, obsolète, a été supprimée.

En outre, la version 2.13 de l'extension **Git Large File Storage (LFS)** est désormais disponible. Les améliorations par rapport à la version 2.11 distribuée dans RHEL 8 sont les suivantes :

- **Git LFS** supporte désormais les dépôts SHA-256.
- **Git LFS** prend désormais en charge le protocole **socks5h**.
- Une nouvelle option **--worktree** est disponible pour les commandes **git lfs install** et **git lfs uninstall**.
- Un nouveau paramètre **--above** est disponible pour la commande **git lfs migrate import**.

(BZ#1956345, BZ#1952517)

Subversion 1.14 dans RHEL 9

RHEL 9 est distribué avec **Subversion 1.14**. **Subversion 1.14** est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM. D'autres versions de **Subversion** seront fournies sous forme de modules avec un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

(JIRA:RHELPLAN-82578)

Changements notables dans le serveur HTTP Apache

RHEL 9.0 fournit la version 2.4.51 du serveur HTTP Apache. Les changements notables par rapport à la version 2.4.37 sont les suivants :

- Interface de contrôle du serveur HTTP Apache (**apachectl**) :
  - Le pager **systemctl** est maintenant désactivé pour la sortie **apachectl status**.
  - La commande **apachectl** échoue maintenant au lieu de donner un avertissement si vous passez des arguments supplémentaires.
  - La commande **apachectl graceful-stop** revient maintenant immédiatement.
  - La commande **apachectl configtest** exécute désormais la commande **httpd -t** sans modifier le contexte SELinux.

- La page de manuel **apachectl(8)** de RHEL documente désormais pleinement les différences avec la version amont **apachectl**.

- Outil Apache eXtenSion (**apxs**) :
  - La commande **/usr/bin/apxs** n'utilise ni n'expose plus les drapeaux d'optimisation du compilateur tels qu'ils sont appliqués lors de la construction du paquet **httpd**. Vous pouvez maintenant utiliser la commande **/usr/lib64/httpd/build/vendor-apxs** pour appliquer les mêmes drapeaux de compilateur que ceux utilisés pour construire **httpd**. Pour utiliser la commande **vendor-apxs**, vous devez d'abord installer le paquetage **redhat-rpm-config**.

- Modules Apache :
  - Le module **mod_lua** est désormais fourni dans un paquet séparé.
  - Un nouveau connecteur **mod_jk** pour le serveur Apache HTTP est un module qui utilise le protocole Apache JServ (AJP) pour connecter les serveurs web avec Apache Tomcat et d'autres backends.
  - Un nouveau module **mod_proxy_cluster** fournit un équilibreur de charge basé sur httpd qui utilise un canal de communication pour transmettre les demandes de l'équilibreur de charge à l'un des nœuds du serveur d'application. Les nœuds de serveurs d'application utilisent cette connexion pour transmettre à l'équilibreur de charge les facteurs d'équilibrage de la charge côté serveur et les événements du cycle de vie par le biais d'un ensemble personnalisé de méthodes HTTP appelé Mod-Cluster Management Protocol (MCMP). Ce canal de retour d'information supplémentaire permet à **mod_proxy_cluster** d'offrir un niveau d'intelligence et de granularité que l'on ne trouve pas dans d'autres solutions d'équilibrage de charge. Ce module nécessite que le client **ModCluster** soit installé sur le serveur dorsal pour communiquer avec succès.

- Modifications de la syntaxe de configuration :
  - Dans la directive obsolète **Allow** fournie par le module **mod_access_compat**, un commentaire (le caractère **#**) déclenche désormais une erreur de syntaxe au lieu d'être ignoré silencieusement.

- Autres modifications :
  - Les identifiants des threads du noyau sont désormais utilisés directement dans les messages du journal des erreurs, ce qui les rend à la fois précis et plus concis.
  - Nombreuses améliorations mineures et corrections de bugs.
  - Un certain nombre de nouvelles interfaces sont à la disposition des auteurs de modules.

L'API du module **httpd** n'a fait l'objet d'aucune modification rétrocompatible depuis RHEL 8.

Apache HTTP Server 2.4 est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM.

Pour plus d'informations, voir Configuration du serveur web Apache HTTP .

(JIRA:RHELPLAN-68364, BZ#1931976, JIRA:RHELPLAN-80725)

nginx 1.20 disponible dans RHEL 9

RHEL 9 inclut le serveur web et proxy **nginx 1.20**. Cette version apporte un certain nombre de corrections de bogues, de correctifs de sécurité, de nouvelles fonctionnalités et d'améliorations par rapport à la version 1.18.

Nouvelles fonctionnalités :

- **nginx** prend désormais en charge la validation des certificats SSL des clients avec le protocole OCSP (Online Certificate Status Protocol).
- **nginx** prend désormais en charge l'effacement du cache en fonction de la quantité minimale d'espace libre. Ce support est implémenté dans le paramètre **min_free** de la directive **proxy_cache_path**.
- Un nouveau module **ngx_stream_set_module** a été ajouté, qui permet de définir une valeur pour une variable.
- Un nouveau paquetage **nginx-mod-devel** a été ajouté, qui fournit tous les fichiers nécessaires, y compris les macros RPM et le code source de **nginx**, pour construire des modules dynamiques externes pour **nginx**.

Directives renforcées :

- Plusieurs nouvelles directives sont désormais disponibles, telles que **ssl_conf_command** et **ssl_reject_handshake**.
- La directive **proxy_cookie_flags** prend désormais en charge les variables.

Amélioration de la prise en charge de HTTP/2 :

- Le module **ngx_http_v2** comprend désormais les directives **lingering_close**, **lingering_time**, **lingering_timeout**.
- La gestion des connexions dans HTTP/2 a été alignée sur HTTP/1.x. À partir de **nginx 1.20**, utilisez les directives **keepalive_timeout** et **keepalive_requests** au lieu des directives **http2_recv_timeout**, **http2_idle_timeout** et **http2_max_requests** qui ont été supprimées.

nginx 1.20 est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM. D'autres versions de **nginx** seront fournies sous forme de modules avec un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

Pour plus d'informations, voir Installation et configuration de NGINX .

(BZ#1953639, BZ#1991720)

Varnish Cache 6.6 dans RHEL 9

RHEL 9 comprend **Varnish Cache 6.6**, un proxy inverse HTTP très performant.

Les changements notables depuis la version 6.0 sont les suivants :

- Amélioration des performances des outils de traitement des journaux, tels que **varnishlog**
- Amélioration de la précision des statistiques
- Un certain nombre d'optimisations dans les consultations du cache
- Diverses modifications de la configuration

- Nombreuses améliorations et corrections de bugs

Varnish Cache 6 est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM.

(BZ#1984185)

RHEL 9 présente Squid 5

RHEL 9 est distribué avec **Squid 5.2**, un serveur proxy de mise en cache haute performance pour les clients web, prenant en charge les objets de données FTP, Gopher et HTTP. Cette version propose un certain nombre de corrections de bogues, de correctifs de sécurité, de nouvelles fonctionnalités et d'améliorations par rapport à la version 4.

Nouvelles fonctionnalités :

- **Squid** améliore la responsabilité en utilisant l'algorithme Happy Eyeballs (HE).
  - **Squid** utilise désormais une adresse IP reçue dès que la demande de transfert l'exige, au lieu d'attendre que toutes les destinations de transfert potentielles soient entièrement résolues.
  - De nouvelles directives sont désormais disponibles : **happy_eyeballs_connect_gap** les directives **happy_eyeballs_connect_limit** et **happy_eyeballs_connect_timeout**.
  - La directive **dns_v4_first** a été supprimée.
- **Squid** utilise désormais l'en-tête **CDN-Loop** comme source de détection des boucles dans les réseaux de diffusion de contenu (CDN).
- **Squid** introduit la prise en charge du peering pour le bumping SSL.
- Une nouvelle fonctionnalité pour les remorques du protocole d'adaptation du contenu Internet (ICAP) est disponible. Elle permet aux agents ICAP d'envoyer de manière fiable les métadonnées du message après le corps du message.

Modifications des options de configuration :

- L'option de configuration **mark_client_packet** a remplacé **clientside_mark**.
- L'option de configuration **shared_transient_entries_limit** a remplacé **collapsed_forwarding_shared_entries_limit**.

Squid 5 est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM.

Pour plus d'informations, voir Configuration du serveur proxy de mise en cache Squid .

(BZ#1990517)

MariaDB 10.5 dans RHEL 9

RHEL 9 fournit **MariaDB 10.5**. **MariaDB 10.5** est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM. D'autres versions de **MariaDB** seront fournies sous forme de modules ayant un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

Pour plus d'informations, voir Utilisation de MariaDB .

(BZ#1971248)

RHEL 9 comprend MySQL 8.0

RHEL 9 est distribué avec **MySQL 8.0**. **MySQL 8.0** est la version initiale de ce flux d'applications, que vous pouvez installer facilement en tant que paquetage RPM. **MySQL 8.0** a un cycle de vie plus court que RHEL 9. Pour plus de détails, consultez le document Red Hat Enterprise Linux Application Streams Life Cycle (cycle de vie des flux d'applications).

Pour plus d'informations sur l'utilisation, voir Utilisation de MySQL.

(JIRA:RHELPLAN-78673)

RHEL 9 fournit PostgreSQL 13

PostgreSQL 13 est disponible avec RHEL 9. **PostgreSQL 13** est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM. D'autres versions de **PostgreSQL** seront fournies sous forme de modules avec un cycle de vie plus court dans les prochaines versions mineures de RHEL 9.

Pour plus d'informations, voir Utilisation de PostgreSQL.

(JIRA:RHELPLAN-78675)

Redis 6.2 dans RHEL 9

RHEL 9 est distribué avec **Redis 6.2**, qui apporte un certain nombre de corrections de bogues et de sécurité, ainsi que des améliorations par rapport à la version 6.0 disponible dans RHEL 8.

Notamment, les fichiers de configuration du serveur **Redis** sont désormais situés dans un répertoire dédié : **/etc/redis/redis.conf** et **/etc/redis/sentinel.conf**. Dans la version RHEL 8, l'emplacement de ces fichiers était respectivement **/etc/redis.conf** et **/etc/redis-sentinel.conf**.

Redis 6 est la version initiale de ce flux d'applications, que vous pouvez installer facilement sous la forme d'un paquetage RPM.

(BZ#1959756)

Nouveau paquet : perl-Module-Signature

RHEL 9 introduit le module Perl **perl-Module-Signature**. Avec ce nouveau module, vous pouvez activer la vérification des signatures pour **cpan** afin d'atténuer la CVE-2020-16156. Pour plus d'informations, voir Comment atténuer CVE-2020-16154 dans perl-App-cpanminus et CVE-2020-16156 dans perl-CPAN.

(BZ#2039361)

4.14. COMPILATEURS ET OUTILS DE DÉVELOPPEMENT

RHEL 9 prend en charge les processeurs IBM POWER10

Du noyau Linux à la chaîne d'outils système (GCC, binutils, glibc), Red Hat Enterprise Linux 9 a été mis à jour pour inclure la prise en charge du dernier processeur POWER d'IBM, le POWER10. RHEL 9 est prêt pour la production de charges de travail sur POWER10, avec des améliorations à venir dans les prochaines versions.

(BZ#2027596)

GCC 11.2.1 est disponible

RHEL 9 est distribué avec la version 11.2.1 de GCC. Les corrections de bogues et améliorations notables incluent :

General improvements

- GCC utilise désormais par défaut le format de débogage DWARF Version 5.
- Les numéros de colonne indiqués dans les diagnostics représentent par défaut des numéros de colonne réels et respectent les caractères multicolonnes.
- Le vecteur de code linéaire prend en compte l'ensemble de la fonction lors de la vectorisation.
- Une série d'expressions conditionnelles qui comparent la même variable peut être transformée en une instruction de commutation si chacune d'entre elles contient une expression de comparaison.
- Amélioration de l'optimisation interprocédurale :
  - Une nouvelle passe IPA-modref, contrôlée par l'option **-fipa-modref**, permet de suivre les effets secondaires des appels de fonction et d'améliorer la précision de l'analyse points-to.
  - La passe de pliage du code identique, contrôlée par l'option **-fipa-icf**, a été considérablement améliorée pour augmenter le nombre de fonctions unifiées et réduire l'utilisation de la mémoire au moment de la compilation.
- Amélioration de l'optimisation du temps de liaison :
  - L'optimisation au moment de la liaison (LTO) permet au compilateur d'effectuer diverses optimisations sur toutes les unités de traduction de votre programme en utilisant sa représentation intermédiaire au moment de la liaison. Pour plus d'informations, voir Optimisation au moment de la liaison.
  - L'allocation de la mémoire lors de l'établissement des liens a été améliorée afin de réduire l'utilisation de la mémoire en période de pointe.
- En utilisant une nouvelle variable d'environnement **GCC_EXTRA_DIAGNOSTIC_OUTPUT** dans les IDE, vous pouvez demander des "conseils de réparation" lisibles par la machine sans avoir à ajuster les drapeaux de construction.
- L'analyseur statique, exécuté par l'option **-fanalyzer**, a été amélioré de manière significative avec de nombreuses corrections de bogues et améliorations.

Language-specific improvements

C family

- Les compilateurs C et C prennent en charge les imbrications de boucles non rectangulaires dans les constructions OpenMP et les routines d'allocation de la spécification OpenMP 5.0.
- Attributs :
  - Le nouvel attribut **no_stack_protector** marque les fonctions qui ne doivent pas être instrumentées avec une protection de la pile (**-fstack-protector**).
  - L'attribut **malloc** amélioré peut être utilisé pour identifier les paires d'API d'allocation et de désallocation.

- Nouveaux avertissements :
  - **-Wsizeof-array-div**, activée par l'option **-Wall**, signale les divisions de deux opérateurs **sizeof** lorsque le premier est appliqué à un tableau et que le diviseur n'est pas égal à la taille de l'élément du tableau.
  - **-Wstringop-overread**, activée par défaut, signale les appels à des fonctions de chaîne de caractères qui tentent de lire au-delà de la fin des tableaux qui leur sont transmis en tant qu'arguments.
- Avertissements renforcés :
  - **-Wfree-nonheap-object** détecte plus de cas d'appels à des fonctions de désallocation avec des pointeurs non renvoyés par une fonction d'allocation de mémoire dynamique.
  - **-Wmaybe-uninitialized** diagnostique le passage de pointeurs et de références à des mémoires non initialisées dans des fonctions qui prennent des arguments qualifiés **const**.
  - **-Wuninitialized** détecte les lectures à partir d'une mémoire allouée dynamiquement et non initialisée.

C

- Plusieurs nouvelles caractéristiques de la prochaine révision C2X de la norme ISO C sont prises en charge par les options **-std=c2x** et **-std=gnu2x**. Par exemple :
  - L'attribut est pris en charge.
  - L'opérateur de préprocesseur **__has_c_attribute** est pris en charge.
  - Les étiquettes peuvent apparaître avant les déclarations et à la fin d'une déclaration composée.

C

- Le mode par défaut devient **-std=gnu 17**.
- La bibliothèque C **libstdc** supporte désormais mieux le C 17.
- Plusieurs nouvelles fonctionnalités du C 20 sont mises en œuvre. Notez que la prise en charge du C 20 est expérimentale.
  Pour plus d'informations sur les fonctionnalités, voir C 20 Language Features.
- L'interface C prend en charge, à titre expérimental, certaines des futures fonctionnalités de la version préliminaire de C 23.
- Nouveaux avertissements :
  - **-Wctad-maybe-unsupported**, désactivée par défaut, avertit de l'exécution d'une déduction d'argument de modèle de classe sur un type n'ayant pas de guides de déduction.
  - **-Wrange-loop-construct**, activée par **-Wall**, signale qu'une boucle for basée sur un intervalle crée des copies inutiles et inefficaces en termes de ressources.
  - **-Wmismatched-new-delete**, activée par **-Wall**, signale les appels à l'opérateur delete avec des pointeurs renvoyés par des formes non concordantes de l'opérateur new ou par d'autres fonctions d'allocation non concordantes.

- **-Wvexing-parse**, activée par défaut, signale la règle d'analyse la plus gênante : les cas où une déclaration ressemble à une définition de variable, mais où le langage C exige qu'elle soit interprétée comme une déclaration de fonction.

Architecture-specific improvements

The 64-bit ARM architecture

- L'architecture Armv8-R est prise en charge par l'option **-march=armv8-r**.
- GCC peut autovectoriser les opérations d'addition, de soustraction et de multiplication, ainsi que les variantes d'accumulation et de soustraction sur les nombres complexes.

AMD and Intel 64-bit architectures

- Un nouveau support d'extension ISA pour Intel AVX-VNNI est ajouté. Le commutateur du compilateur **-mavxvnni** contrôle les éléments intrinsèques AVX-VNNI.
- Les processeurs AMD basés sur le noyau znver3 sont pris en charge par la nouvelle option **-march=znver3**.
- Trois niveaux de microarchitecture définis dans le supplément psABI x86-64 sont pris en charge par les nouvelles options **-march=x86-64-v2**, **-march=x86-64-v3**, et **-march=x86-64-v4**.

IBM Z architectures

- GCC 11.2.1 utilise par défaut le processeur IBM z14.

IBM Power Systems

- GCC 11.2.1 utilise par défaut le processeur IBM POWER9.
- Le compilateur GCC prend désormais en charge les instructions POWER10 grâce à la nouvelle option de ligne de commande **-mcpu=power10**

(BZ#1986836, BZ#1870016, BZ#1870025, BZ#1870028, BZ#2019811, BZ#2047296)

Nouvelle commande pour capturer les données d'optimisation de glibc

La nouvelle commande **ld.so --list-diagnostics** capture les données qui influencent les décisions d'optimisation **glibc**, telles que la sélection IFUNC et la configuration **glibc-hwcaps**, dans un seul fichier lisible par une machine.

(BZ#2023422)

Changements notables binutils

RHEL 9 apporte les modifications suivantes à **binutils**:

- **binutils** prend désormais en charge le jeu d'instructions AMX/TMUL d'Intel, ce qui se traduit par une amélioration des performances des applications qui peuvent utiliser cette nouvelle fonctionnalité.
- L'assembleur, l'éditeur de liens et d'autres utilitaires binaires prennent désormais en charge les instructions POWER10.

(BZ#2030554, BZ#1870021)

sched_getcpu peut désormais, en option, utiliser rseq (séquences redémarrables) pour améliorer les performances sur les architectures ARM 64 bits et d'autres architectures

La précédente implémentation de **sched_getcpu** sur les architectures ARM 64 bits utilise l'appel système **getcpu**, qui est trop lent pour une utilisation efficace dans la plupart des algorithmes parallèles. D'autres architectures utilisent l'accélération vDSO (virtual dynamic shared object) pour contourner ce problème. L'implémentation de **sched_getcpu** à l'aide de **rseq** améliore considérablement les performances sur les architectures ARM 64 bits. Les autres architectures n'enregistrent qu'une légère amélioration.

Pour configurer **sched_getcpu** afin qu'il utilise **rseq**, définissez la variable d'environnement **GLIBC_TUNABLES=glibc.pthread.rseq=1**:

```
# GLIBC_TUNABLES=glibc.pthread.rseq=1
# export GLIBC_TUNABLES
```

(BZ#2024347)

Mise à jour des outils de performance et des débogueurs

Les outils de performance et les débogueurs suivants sont disponibles avec RHEL 9.0 :

- GDB 10.2
- Valgrind 3.18.1
- SystemTap 4.6
- Dyninst 11.0.0
- elfutils 0.186

(BZ#2019806)

Amélioration de la fonctionnalité DAWR dans GDB sur IBM POWER10

RHEL 9 est distribué avec GDB 10.2 qui fournit une fonctionnalité DAWR améliorée. De nouvelles capacités de surveillance matérielle sont activées pour GDB sur les processeurs IBM POWER10. Par exemple, un nouvel ensemble de registres DAWR/DAWRX a été ajouté.

(BZ#1870029)

GDB supporte les nouvelles instructions préfixées sur IBM POWER10

GDB 10.2 prend entièrement en charge les instructions préfixées Power ISA 3.1 sur POWER10, qui comprennent des instructions préfixées de huit octets. Dans RHEL 8.4, GDB ne prenait en charge que les instructions de quatre octets.

(BZ#1870031)

RHEL 9 fournit boost 1.75.0

RHEL 9 est distribué avec le paquet **boost** version 1.75.0. Les corrections de bogues et améliorations notables par rapport à la version 1.67.0 sont les suivantes :

- La bibliothèque **Boost.Signals** a été supprimée et remplacée par le composant **Boost.Signals2** qui ne contient que des en-têtes.

- L'outil **bjam** du paquet **boost-jam** a été remplacé par **b2** dans le paquet **boost-b2**.
- Nouvelles bibliothèques :
  - **Boost.Contracts**
  - **Boost.HOF**
  - **Boost.YAP**
  - **Boost.Safe Numerics**
  - **Boost.Outcome**
  - **Boost.Histogram**
  - **Boost.Variant2**
  - **Boost.Nowide**
  - **Boost.StaticString**
  - **Boost.STL_Interfaces**
  - **Boost.JSON**
  - **Boost.LEAF**
  - **Boost.PFR**

(BZ#1957950)

RHEL 9 fournit le jeu d'outils LLVM 13.0.1

RHEL 9 est distribué avec la version 13.0.1 du jeu d'outils LLVM. Les corrections de bogues et améliorations notables par rapport à la version 12.0.1 sont les suivantes :

- Clang supporte maintenant les appels de queue garantis avec les attributs de déclaration **[[clang::musttail]]** en C et **__attribute__((musttail))** en C.
- Clang supporte maintenant l'avertissement **-Wreserved-identifier**, qui prévient les développeurs lorsqu'ils utilisent des identifiants réservés dans leur code.
- Le drapeau **-Wshadow** de Clang vérifie maintenant aussi les liens structurés ombragés.
- Le **-Wextra** de Clang implique désormais également le **-Wnull-pointer-subtraction**.
- Clang supporte maintenant les appels de queue garantis avec les attributs de déclaration **[[clang::musttail]]** en C et **__attribute__((musttail))** en C.

Dans RHEL 9, vous pouvez facilement installer **llvm-toolset** en tant que paquetage RPM.

(BZ#2001107)

Changements notables dans CMake 3.20.2

RHEL 9 est distribué avec CMake 3.20.2. Pour utiliser CMake sur un projet qui nécessite la version 3.20.2 ou moins, utilisez la commande **cmake_minimum_required**(version 3.20.2).

Les changements les plus notables sont les suivants :

- Les modes du compilateur C 23 peuvent désormais être spécifiés en utilisant les propriétés de la cible **CXX_STANDARD**, **CUDA_STANDARD**, **OBJCXX_STANDARD**, ou en utilisant la méta-caractéristique **cxx_std_23** de la fonction compile features.
- La prise en charge du langage CUDA permet désormais au compilateur NVIDIA CUDA d'être un lien symbolique.
- Les compilateurs Intel oneAPI NextGen LLVM sont maintenant supportés avec l'ID de compilateur **IntelLLVM**.
- CMake facilite désormais la compilation croisée pour Android en fusionnant avec le fichier de la chaîne d'outils du NDK Android.
- Lors de l'exécution de **cmake(1)** pour générer un système de construction de projet, les arguments de ligne de commande inconnus commençant par un trait d'union sont désormais rejetés.

Pour plus d'informations sur les nouvelles fonctionnalités et les fonctionnalités obsolètes, voir les notes de mise à jour de CMake.

(BZ#1957948)

RHEL 9 fournit Go 1.17.7

RHEL 9 est distribué avec la version 1.17.7 de Go Toolset. Les corrections de bogues et améliorations notables par rapport à la version 1.16.7 sont les suivantes :

- Ajout d'une option pour convertir les tranches en pointeurs de tableau.
- Ajout de la prise en charge des lignes //go:build.
- Amélioration des performances des appels de fonction sur amd64.
- Les arguments des fonctions sont formatés plus clairement dans les traces de pile.
- Les fonctions contenant des fermetures peuvent être mises en ligne.
- Réduction de la consommation de ressources dans l'analyse des certificats x509.

Dans RHEL 9, vous pouvez facilement installer **go-toolset** en tant que paquetage RPM.

(BZ#2014087)

Le mode Go FIPS est pris en charge par OpenSSL 3

Vous pouvez désormais utiliser la bibliothèque OpenSSL 3 en mode Go FIPS.

(BZ#1984110)

RHEL 9 fournit Rust Toolset 1.58.1

RHEL 9 est distribué avec la version 1.58.1 de Rust Toolset. Les corrections de bogues et améliorations notables par rapport à la version 1.54.0 sont les suivantes :

- Le compilateur Rust prend désormais en charge l'édition 2021 du langage, avec la capture disjointe dans les fermetures, **IntoIterator** pour les tableaux, un nouveau résolveur de fonctionnalités Cargo, et bien plus encore.

- Ajout du support Cargo pour les nouveaux profils personnalisés.
- Cargo dédouble les erreurs de compilation.
- Ajout de nouveaux modèles de champs de tir ouverts.
- Ajout d'identifiants capturés dans les chaînes de format.

Pour plus d'informations, voir Rust 1.55Rust1.56Rust1.57Rust 1.58

Dans RHEL 9, vous pouvez facilement installer **rust-toolset** en tant que paquetage RPM.

(BZ#2002885)

RHEL 9 fournit le paquet pcp version 5.3.5

RHEL 9 est distribué avec le paquet Performance Co-Pilot (**pcp**) version 5.3.5. Depuis la version 5.3.1, un nouveau sous-paquet **pcp-pmda-bpf** a été ajouté. Il fournit des données sur les performances des programmes **eBPF** utilisant BPF CO-RE (**libbpf** et **BTF**).

(BZ#1991764)

Authentification Active Directory pour l'accès aux métriques du serveur SQL dans PCP

Grâce à cette mise à jour, un administrateur système peut configurer **pmdamssql(1)** pour qu'il se connecte en toute sécurité aux métriques du serveur SQL à l'aide de l'authentification Active Directory (AD).

(BZ#1847808)

Le nouvel utilitaire pcp-ss PCP est maintenant disponible

L'utilitaire **pcp-ss** PCP fournit des statistiques sur les sockets collectées par **pmdasockets(1)** PMDA. La commande est compatible avec la plupart des options de ligne de commande et des formats de rapport de **ss**. Il offre également les avantages d'une surveillance locale ou à distance en mode direct et d'une relecture historique à partir d'une archive PCP précédemment enregistrée.

(BZ#1981223)

RHEL 9 fournit grafana 7.5.11

RHEL 9 est distribué avec le paquet **grafana** version 7.5.11. Les changements notables par rapport à la version 7.5.9 sont les suivants :

- Ajout d'une nouvelle transformation **prepare time series** pour la rétrocompatibilité des panneaux qui ne supportent pas le nouveau format de cadre de données.
- Mise à jour de la fonctionnalité de récupération de mot de passe afin d'utiliser HMAC-SHA-256 au lieu de SHA-1 pour générer des jetons de réinitialisation de mot de passe.

(BZ#1993215)

RHEL 9 fournit grafana-pcp 3.2.0

RHEL 9 est distribué avec la version 3.2.0 du paquet **grafana-pcp**. Les corrections de bogues et améliorations notables par rapport à la version 3.1.0 sont les suivantes :

- Ajout d'un nouveau tableau de bord MS SQL Server pour PCP Redis.

- Ajout de la visibilité des histogrammes vides dans le tableau de bord PCP Vector eBPF/BCC Overview.
- Correction d'un bug où la fonction **metric()** de PCP Redis ne retournait pas tous les noms de métriques.

(BZ#1993156)

L'accès aux hôtes distants par l'intermédiaire d'un site central pmproxy pour la source de données Vector dans grafana-pcp

Dans certains environnements, la politique de réseau n'autorise pas les connexions du navigateur de l'observateur du tableau de bord aux hôtes surveillés directement. Cette mise à jour permet de personnaliser le site **hostspec** afin de se connecter à un site central **pmproxy**, qui transmet les demandes aux différents hôtes.

(BZ#1845592)

Un nouveau paquet : ansible-pcp

Le package **ansible-pcp** contient des rôles pour Performance Co-Pilot (PCP) et des logiciels connexes, tels que Redis et Grafana, utilisés pour mettre en œuvre le rôle de système RHEL **metrics**.

(BZ#1957566)

RHEL 9 fournit python-jsonpointer 2.0

RHEL 9 est distribué avec le paquet **python-jsonpointer** version 2.0.

Les changements notables par rapport à la version 1.9 sont les suivants :

- Les versions 2.6 et 3.3 de Python sont obsolètes.
- Le module **python-jsonpointer** vérifie désormais automatiquement que les pointeurs ne contiennent pas de séquences d'échappement invalides.
- Vous pouvez désormais écrire des pointeurs en tant qu'arguments dans la ligne de commande.
- Les pointeurs ne peuvent plus être soumis dans un format codé en URL.

(BZ#1980256)

.NET 6.0 est disponible

RHEL 9 est distribué avec **.NET** version 6.0. Les améliorations notables sont les suivantes :

- Prise en charge de Arm 64 bits (aarch64)
- Support pour IBM Z et LinuxONE (s390x)

Pour plus d'informations, voir les notes de mise à jour pour les paquets RPM .NET 6.0 et les notes de mise à jour pour les conteneurs .NET 6.0.

.NET 6.0 est la version initiale de ce flux d'applications, que vous pouvez installer facilement en tant que paquetage RPM. **.NET 6.0** a un cycle de vie plus court que RHEL 9. Pour plus de détails, consultez le document Red Hat Enterprise Linux Application Streams Life Cycle (cycle de vie des flux d'applications Red Hat Enterprise Linux).

(BZ#1986211)

Implémentations Java dans RHEL 9

Le référentiel RHEL 9 AppStream comprend :

- Les paquets **java-17-openjdk**, qui fournissent l'environnement d'exécution Java OpenJDK 17 et le kit de développement logiciel Java OpenJDK 17.
- Les paquets **java-11-openjdk**, qui fournissent l'environnement d'exécution Java OpenJDK 11 et le kit de développement logiciel Java OpenJDK 11.
- Les paquets **java-1.8.0-openjdk**, qui fournissent l'environnement d'exécution Java OpenJDK 8 et le kit de développement logiciel Java OpenJDK 8.

Pour plus d'informations, voir la documentation OpenJDK.

(BZ#2021262)

Outils Java dans RHEL 9

Le référentiel RHEL 9 AppStream comprend les outils Java suivants :

- **Maven 3.6.3**un outil de gestion et de compréhension des projets de logiciels.
- **Ant 1.10.9**le logiciel de gestion des applications Java est une bibliothèque Java et un outil de ligne de commande permettant de compiler, d'assembler, de tester et d'exécuter des applications Java.

Maven 3.6 et **Ant 1.10** sont les versions initiales de ces flux d'applications, que vous pouvez installer facilement sous forme de paquets RPM non modulaires.

(BZ#1951482)

SWIG 4.0 disponible dans le répertoire du CRB

La version 4.0 du SWIG (Simplified Wrapper and Interface Generator) est disponible dans le dépôt CodeReady Linux Builder (CRB). Cette version ajoute la prise en charge de **PHP 8**.

Dans RHEL 9, vous pouvez facilement installer **SWIG** en tant que paquetage RPM.

Notez que les paquets inclus dans le référentiel CodeReady Linux Builder ne sont pas pris en charge.

(BZ#1943580)

4.15. GESTION DE L'IDENTITÉ

Directory Server n'utilise plus de journal des modifications global

Avec cette amélioration, le journal des modifications de Directory Server a été intégré dans la base de données principale. Auparavant, Directory Server utilisait un journal des modifications global. Cependant, cela pouvait poser des problèmes si l'annuaire utilisait plusieurs bases de données. Par conséquent, chaque suffixe a maintenant son propre journal des modifications dans le même répertoire que les fichiers de la base de données principale.

(BZ#1805717)

ansible-freeipa est maintenant disponible dans le dépôt AppStream avec toutes les dépendances

Auparavant, dans RHEL 8, avant d'installer le paquet **ansible-freeipa**, vous deviez d'abord activer le référentiel Ansible et installer le paquet **ansible**. Dans RHEL 8.6 et RHEL 9, vous pouvez installer **ansible-freeipa** sans aucune étape préalable. L'installation de **ansible-freeipa** installe automatiquement le paquetage **ansible-core**, une version plus basique de **ansible**, en tant que dépendance. Les paquets **ansible-freeipa** et **ansible-core** sont disponibles dans le dépôt **rhel-9-for-x86_64-appstream-rpms**.

ansible-freeipa dans RHEL 8.6 et RHEL 9 contient tous les modules qu'il contenait dans RHEL 8.

(JIRA:RHELPLAN-100359)

IdM supporte désormais les modules Ansible automountlocation, automountmap, et automountkey

Avec cette mise à jour, le paquet **ansible-freeipa** contient les modules **ipaautomountlocation**, **ipaautomountmap**, et **ipaautomountkey**. Vous pouvez utiliser ces modules pour configurer les répertoires à monter automatiquement pour les utilisateurs IdM connectés aux clients IdM dans un emplacement IdM. Notez qu'actuellement, seules les cartes directes sont prises en charge.

(JIRA:RHELPLAN-79161)

La prise en charge de la gestion des plages de sous-identifiants est disponible dans le module shadow-utils

Auparavant, **shadow-utils** configurait automatiquement les plages de sous-identifiants à partir des fichiers **/etc/subuid** et **/etc/subgid**. Avec cette mise à jour, la configuration des plages de sous-identifiants est disponible dans le fichier **/etc/nsswitch.conf** en définissant une valeur dans le champ **subid**. Pour plus d'informations, voir **man subuid** et **man subgid**. De plus, avec cette mise à jour, une implémentation SSSD du plugin **shadow-utils** est disponible, qui fournit les plages de sous-identifiants à partir du serveur IPA. Pour utiliser cette fonctionnalité, ajoutez la valeur **subid: sss** au fichier **/etc/nsswitch.conf**. Cette solution pourrait être utile dans l'environnement conteneurisé pour faciliter les conteneurs sans racine.

Notez que si le fichier **/etc/nsswitch.conf** est configuré par l'outil **authselect**, vous devez suivre les procédures décrites dans la documentation **authselect**. Si ce n'est pas le cas, vous pouvez modifier le fichier **/etc/nsswitch.conf** manuellement.

(BZ#1859252)

La gestion des plages de sous-identifiants est prise en charge par IdM

Avec cette mise à jour, vous pouvez gérer les sous-gammes d'ID pour les utilisateurs dans la gestion des identités. Vous pouvez utiliser l'outil CLI **ipa** ou l'interface WebUI IdM pour attribuer à un utilisateur des plages de sous-ID configurées automatiquement, ce qui peut s'avérer utile dans un environnement conteneurisé.

(BZ#1952028)

Les paquets d'installation de la gestion des identités ont été démodularisés

Auparavant, dans RHEL 8, les paquets IdM étaient distribués sous forme de modules, ce qui nécessitait d'activer un flux et d'installer le profil correspondant à l'installation souhaitée. Les paquets d'installation IdM ont été démodularisés dans RHEL 9, de sorte que vous pouvez utiliser les commandes **dnf** suivantes pour installer les paquets de serveur IdM :

Pour un serveur sans services DNS intégrés :

```
# dnf install ipa-server
```

Pour un serveur avec services DNS intégrés :

```
# dnf install ipa-server ipa-server-dns
```

(BZ#2080875)

Une alternative au dépôt traditionnel RHEL ansible-freeipa : Hub d'automatisation Ansible

Avec cette mise à jour, vous pouvez télécharger les modules **ansible-freeipa** depuis Ansible Automation Hub (AAH) au lieu de les télécharger depuis le dépôt RHEL standard. En utilisant AAH, vous pouvez bénéficier des mises à jour plus rapides des modules **ansible-freeipa** disponibles dans ce dépôt.

Dans AAH, les rôles et modules **ansible-freeipa** sont distribués sous forme de collection. Notez que vous avez besoin d'un abonnement à Ansible Automation Platform (AAP) pour accéder au contenu du portail AAH. Vous avez également besoin de **ansible** version 2.9 ou ultérieure.

La collection **redhat.rhel_idm** a le même contenu que le paquet traditionnel **ansible-freeipa**. Toutefois, le format de la collection utilise un nom de collection entièrement qualifié (FQCN) qui se compose d'un espace de noms et du nom de la collection. Par exemple, le module **redhat.rhel_idm.ipadnsconfig** correspond au module **ipadnsconfig** dans **ansible-freeipa** fourni par un dépôt RHEL. La combinaison d'un espace de noms et d'un nom de collection garantit que les objets sont uniques et peuvent être partagés sans conflit.

(JIRA:RHELPLAN-103147)

les modules ansible-freeipa peuvent désormais être exécutés à distance sur les clients IdM

Auparavant, les modules **ansible-freeipa** ne pouvaient être exécutés que sur les serveurs IdM. Cela nécessitait que votre administrateur Ansible ait un accès **SSH** à votre serveur IdM, ce qui constituait une menace potentielle pour la sécurité. Avec cette mise à jour, vous pouvez exécuter les modules **ansible-freeipa** à distance sur des systèmes qui sont des clients IdM. Par conséquent, vous pouvez gérer la configuration et les entités IdM de manière plus sécurisée.

Pour exécuter les modules **ansible-freeipa** sur un client IdM, choisissez l'une des options suivantes :

- Définissez la variable **hosts** de l'ordre de lecture sur un hôte client IdM.
- Ajoutez la ligne **ipa_context: client** à la tâche du playbook qui utilise le module **ansible-freeipa**.

Vous pouvez également définir la variable **ipa_context** sur **client** sur un serveur IdM. Toutefois, le contexte du serveur offre généralement de meilleures performances. Si **ipa_context** n'est pas défini, **ansible-freeipa** vérifie s'il est exécuté sur un serveur ou un client et définit le contexte en conséquence. Notez que l'exécution d'un module **ansible-freeipa** avec la variable **context** définie sur **server** sur un hôte client IdM entraîne une erreur de **missing libraries**.

(JIRA:RHELPLAN-103146)

Le module ipadnsconfig exige désormais que action: member exclue un transitaire global

Avec cette mise à jour, l'exclusion des expéditeurs globaux dans la gestion de l'identité (IdM) en utilisant le module **ansible-freeipa ipadnsconfig** nécessite l'utilisation de l'option **action: member** en plus de l'option **state: absent**. Si vous n'utilisez que **state: absent** dans votre manuel de jeu sans utiliser également **action: member**, le manuel de jeu échoue. Par conséquent, pour supprimer tous les transitaires globaux, vous devez tous les spécifier individuellement dans le cahier d'exécution. En revanche, l'option **state: present** ne nécessite pas **action: member**.

(BZ#2046325)

Les groupes privés automatiques pour les utilisateurs AD permettent une configuration centralisée

Vous pouvez désormais définir de manière centralisée la façon dont les versions compatibles de SSSD sur les clients IdM gèrent les groupes privés pour les utilisateurs des domaines Active Directory de confiance. Grâce à cette amélioration, vous pouvez désormais définir explicitement la valeur de l'option **auto_private_groups** de SSSD pour une plage d'identifiants qui gère les utilisateurs AD.

Lorsque l'option **auto_private_groups** n'est pas explicitement définie, elle utilise une valeur par défaut :

- Pour une plage d'ID **ipa-ad-trust-posix**, la valeur par défaut est **false**. SSSD utilise toujours les adresses **uidNumber** et **gidNumber** de l'entrée AD. Un groupe portant l'adresse **gidNumber** doit exister dans AD.
- Pour une plage d'ID **ipa-ad-trust**, la valeur par défaut est **true**. SSSD mappe le **uidNumber** à partir du SID d'entrée, le **gidNumber** est toujours défini sur la même valeur et un groupe privé est toujours mappé.

Vous pouvez également attribuer à **auto_private_groups** un troisième paramètre : **hybrid**. Avec ce paramètre, SSSD crée un groupe privé si l'entrée de l'utilisateur a un GID égal à l'UID mais qu'il n'y a pas de groupe avec ce GID. Si l'UID et le GID sont différents, un groupe avec ce numéro de GID doit exister.

Cette fonction est utile pour les administrateurs qui souhaitent cesser de gérer des objets de groupe distincts pour les groupes privés d'utilisateurs, mais qui veulent également conserver les groupes privés d'utilisateurs existants.

(BZ#1957736)

Paramètres de journalisation personnalisables pour BIND

Avec cette amélioration, vous pouvez maintenant configurer les paramètres de journalisation pour le composant serveur DNS BIND d'un serveur de gestion d'identité dans le fichier de configuration **/etc/named/ipa-logging-ext.conf**.

(BZ#1966101)

Découverte automatique des serveurs IdM lors de la récupération d'un keytab IdM

Grâce à cette amélioration, il n'est plus nécessaire de spécifier le nom d'hôte d'un serveur IdM lors de la récupération d'un keytab Kerberos à l'aide de la commande **ipa-getkeytab**. Si vous ne spécifiez pas de nom d'hôte de serveur, la recherche DNS est utilisée pour trouver un serveur IdM. Si aucun serveur n'est trouvé, la commande revient à la valeur **host** spécifiée dans le fichier de configuration **/etc/ipa/default.conf**.

(BZ#1988383)

RHEL 9 fournit Samba 4.15.5

RHEL 9 est distribué avec Samba 4.15.5, qui apporte des corrections de bogues et des améliorations par rapport à la version 4.14 :

- Les options des utilitaires Samba ont été renommées et supprimées pour une expérience utilisateur cohérente
- Le support multicanal du serveur est désormais activé par défaut.
- Les dialectes **SMB2_22**, **SMB2_24** et **SMB3_10**, qui n'étaient utilisés que par les versions préliminaires techniques de Windows, ont été supprimés.

Sauvegardez les fichiers de base de données avant de démarrer Samba. Lorsque les services **smbd**, **nmbd**, ou **winbind** démarrent, Samba met automatiquement à jour ses fichiers de base de données **tdb**. Notez que Red Hat ne prend pas en charge la rétrogradation des fichiers de base de données **tdb**.

Après avoir mis à jour Samba, vérifiez le fichier **/etc/samba/smb.conf** à l'aide de l'utilitaire **testparm**.

Pour plus d'informations sur les changements notables, lisez les notes de version en amont avant de procéder à la mise à jour.

(BZ#2013578)

Suivi des demandes des clients à l'aide de l'outil d'analyse des logs

Le démon des services de sécurité du système (SSSD) comprend désormais un outil d'analyse des journaux qui suit les demandes du début à la fin dans les fichiers journaux de plusieurs composants SSSD.

L'outil d'analyse des journaux vous permet d'examiner plus facilement les journaux de débogage de SSSD afin de vous aider à résoudre les problèmes de SSSD. Par exemple, vous pouvez extraire et imprimer les journaux SSSD concernant uniquement certaines demandes de clients à travers les processus SSSD. Pour exécuter l'outil d'analyse, utilisez la commande **sssctl analyze**.

(JIRA:RHELPLAN-97899)

SSSD enregistre désormais les backtraces par défaut

Avec cette amélioration, SSSD stocke désormais des journaux de débogage détaillés dans une mémoire tampon et les ajoute aux fichiers journaux lorsqu'une erreur se produit. Par défaut, les niveaux d'erreur suivants déclenchent une trace arrière :

- Niveau 0 : échecs fatals
- Niveau 1 : défaillances critiques
- Niveau 2 : défaillances graves

Vous pouvez modifier ce comportement pour chaque processus SSSD en définissant l'option **debug_level** dans la section correspondante du fichier de configuration **sssd.conf**:

- Si vous définissez le niveau de débogage sur 0, seuls les événements de niveau 0 déclenchent une rétro-trace.
- Si vous définissez le niveau de débogage sur 1, les niveaux 0 et 1 déclenchent une rétro-trace.
- Si vous réglez le niveau de débogage sur 2 ou plus, les événements des niveaux 0 à 2 déclenchent une rétrotrace.

Vous pouvez désactiver cette fonction pour chaque processus SSSD en définissant l'option **debug_backtrace_enabled** sur **false** dans la section correspondante de **sssd.conf**:

```
[sssd]
debug_backtrace_enabled = true
debug_level=0
...

[nss]
debug_backtrace_enabled = false
...
```

```
[domain/idm.example.com]
debug_backtrace_enabled = true
debug_level=2
...

...
```

(BZ#1949149)

La valeur de hachage SSH par défaut de SSSD est désormais cohérente avec les paramètres d'OpenSSH

La valeur par défaut de **ssh_hash_known_hosts** a été changée en false. Elle est maintenant cohérente avec la configuration d'OpenSSH, qui ne hache pas les noms d'hôtes par défaut.

Toutefois, si vous devez continuer à hacher les noms d'hôtes, ajoutez **ssh_hash_known_hosts = True** à la section **[ssh]** du fichier de configuration **/etc/sssd/sssd.conf**.

(BZ#2014249)

Directory Server 12.0 est basé sur la version amont 2.0.14

Directory Server 12.0 est basé sur la version amont 2.0.14 qui apporte un certain nombre de corrections de bogues et d'améliorations par rapport à la version précédente. Pour une liste complète des changements notables, lisez les notes de mise à jour de la version amont avant de procéder à la mise à jour :

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-14.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-13.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-12.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-11.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-10.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-9.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-8.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-7.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-6.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-5.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-4.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-3.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-2.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-1.html

(BZ#2024693)

Directory Server stocke désormais les fichiers de bases de données mappés en mémoire sur un système de fichiers tmpfs

Dans Directory Server, le paramètre **nsslapd-db-home-directory** définit l'emplacement des fichiers en mémoire des bases de données. Cette amélioration modifie la valeur par défaut du paramètre, qui passe de **/var/lib/dirsrv/slapd-*instance_name*/db/** à **/dev/shm/**. Par conséquent, lorsque les bases de données internes sont stockées sur un système de fichiers **tmpfs**, les performances de Directory Server augmentent.

(BZ#2088414)

4.16. BUREAU

GNOME mis à jour à la version 40

L'environnement GNOME a été mis à jour de GNOME 3.28 à GNOME 40 avec de nombreuses nouvelles fonctionnalités.

GNOME 40 inclut une nouvelle conception améliorée de **Activities Overview**. Cela donne à la vue d'ensemble un aspect plus cohérent et améliore la navigation dans le système et le lancement des applications. Les espaces de travail sont désormais disposés horizontalement, et la vue d'ensemble des fenêtres et la grille des applications sont accessibles verticalement.

Parmi les autres améliorations apportées à GNOME, citons

- Les performances et l'utilisation des ressources de GNOME ont été considérablement améliorées.
- Le style visuel, y compris l'interface utilisateur, les icônes et le bureau, a été rafraîchi.
- Les applications GNOME n'utilisent plus le menu d'application, qui était disponible dans le panneau supérieur. La fonctionnalité est désormais située dans un menu primaire à l'intérieur de la fenêtre d'application.
- L'application **Settings** a été remaniée.
- Le partage d'écran et les sessions de bureau à distance ont été améliorés.
- Si vous utilisez les pilotes NVIDIA propriétaires, vous pouvez désormais lancer des applications en utilisant le GPU discret :
    a. Ouvrir la vue d'ensemble.
    b. Cliquez avec le bouton droit de la souris sur l'icône de l'application dans le tableau de bord.
    c. Sélectionnez l'élément **Launch on Discrete GPU** dans le menu.
- Le menu **Power Off / Log Out** comprend désormais l'option **Suspend** et une nouvelle option **Restart**, qui permet de redémarrer le système vers le menu du chargeur de démarrage lorsque vous maintenez la **touche Alt** enfoncée.
- Les applications Flatpak sont désormais mises à jour automatiquement.
- Vous pouvez désormais regrouper les icônes d'application dans la vue d'ensemble dans des dossiers en utilisant la fonction glisser-déposer.

- L'application **Terminal** prend désormais en charge le texte de droite à gauche et le texte bidirectionnel.
- La fonction d'accessibilité **Pointer Location** fonctionne désormais dans la session Wayland. Lorsque la fonctionnalité est activée, appuyer sur **Ctrl** met en évidence l'emplacement du pointeur sur l'écran.
- Les extensions du shell GNOME sont désormais gérées par l'application **Extensions**, plutôt que par **Software**. L'application **Extensions** gère la mise à jour des extensions, la configuration des préférences d'extension, ainsi que la suppression ou la désactivation des extensions.
- Le popover des notifications comprend désormais un bouton **Do Not Disturb**. Lorsque le bouton est activé, les notifications n'apparaissent pas à l'écran.
- Les boîtes de dialogue du système qui requièrent un mot de passe ont désormais la possibilité de révéler le texte du mot de passe en cliquant sur l'icône de l'œil (▮).
- L'application **Software** détecte désormais automatiquement les réseaux avec compteur, tels que les réseaux de données mobiles. Lorsque le réseau actuel est équipé de compteurs, **Software** interrompt les mises à jour afin de réduire l'utilisation des données.
- Chaque écran connecté peut désormais utiliser un taux de rafraîchissement différent dans la session Wayland.
- La mise à l'échelle de l'affichage fractionnaire est disponible en tant qu'option expérimentale. Elle comprend plusieurs rapports fractionnaires préconfigurés.
  Pour activer la mise à l'échelle fractionnaire expérimentale, ajoutez la valeur **scale-monitor-framebuffer** à la liste des fonctions expérimentales activées :

  ```
  $ dconf write \
        /org/gnome/mutter/experimental-features \
        "['scale-monitor-framebuffer']"
  ```

  Par conséquent, les options de mise à l'échelle fractionnaire sont accessibles sur le panneau **Display** dans **Settings**.

Pour plus de détails sur les changements apportés à GNOME, voir les versions 3.30 à 40.0 dans les notes de mise à jour .

(JIRA:RHELPLAN-101240)

PipeWire est désormais le service audio par défaut

Le service **Pipewire** gère désormais toutes les sorties et entrées audio. **Pipewire** remplace le service **PulseAudio** dans les cas d'utilisation générale et le service **JACK** dans les cas d'utilisation professionnelle. Le système redirige désormais l'audio des applications qui utilisent **PulseAudio**, **JACK** ou le cadre **ALSA** vers **Pipewire**.

Les avantages de **Pipewire** par rapport aux solutions précédentes sont les suivants

- Une solution unifiée pour les utilisateurs grand public et professionnels
- Une architecture flexible et modulaire
- Haute performance et faible latence, similaire au service **JACK**
- Isolation entre les clients audio pour une meilleure sécurité

Vous ne devez plus configurer le service **JACK** pour les applications qui l'utilisent. Toutes les applications **JACK** fonctionnent désormais dans la configuration RHEL par défaut.

PulseAudio est toujours disponible dans RHEL, et vous pouvez l'activer à la place de **PipeWire**. Pour plus de détails, voir Passer de PipeWire à PulseAudio .

(JIRA:RHELPLAN-101241)

Les profils d'alimentation sont disponibles dans GNOME

Vous pouvez désormais basculer entre plusieurs profils d'alimentation dans le panneau **Power** de **Settings** dans l'environnement GNOME. Les profils d'alimentation optimisent différents paramètres du système en fonction de l'objectif sélectionné.

Les profils de puissance suivants sont disponibles :

Performances
: Optimise les performances du système et réduit l'autonomie de la batterie. Ce profil n'est disponible que sur certaines configurations de système sélectionnées.

Équilibré
: Fournit des performances système et une consommation d'énergie standard. Il s'agit du profil par défaut.

Économiseur d'énergie
: Augmente l'autonomie de la batterie et réduit les performances du système. Ce profil s'active automatiquement lorsque la batterie est faible.

La configuration de votre profil d'alimentation persiste lors des redémarrages du système.

La fonctionnalité des profils de puissance est disponible à partir du paquetage **power-profiles-daemon**, qui est installé par défaut.

(JIRA:RHELPLAN-101242)

Le soutien linguistique est désormais assuré par langpacks

La prise en charge de plusieurs langues est désormais disponible à partir des paquets **langpacks**. Vous pouvez personnaliser le niveau de prise en charge des langues que vous souhaitez installer en utilisant les noms de paquets suivants, où ***code*** est le code ISO abrégé de la langue, par exemple **es** pour l'espagnol :

langpacks-core-*code*
: Fournit un support linguistique de base, y compris

- Le site **glibc**
- La police par défaut
- La méthode de saisie par défaut si la langue l'exige

langpacks-core-font-*code*
: Fournit uniquement la police par défaut pour la langue.

langpacks-*code*
: Fournit un support linguistique complet, comprenant les éléments suivants en plus du support linguistique de base :

- Traductions
- Dictionnaires correcteurs d'orthographe
- Polices supplémentaires

(JIRA:RHELPLAN-101247)

Environnement léger à application unique

Pour les cas d'utilisation graphique qui ne présentent qu'une seule application, une interface utilisateur légère est désormais disponible.

Vous pouvez démarrer GNOME dans une session à application unique, également connue sous le nom de mode kiosque. Dans cette session, GNOME n'affiche qu'une fenêtre plein écran d'une application que vous avez configurée.

La session à application unique est nettement moins gourmande en ressources que la session GNOME standard.

Pour plus d'informations, voir Limiter la session à une seule application .

(JIRA:RHELPLAN-102552)

Bannières de classification de sécurité à l'ouverture de session et dans la session de bureau

Vous pouvez désormais configurer des bannières de classification indiquant le niveau global de classification de sécurité du système. Cette fonction est utile pour les déploiements dans lesquels l'utilisateur doit connaître le niveau de classification de sécurité du système sur lequel il est connecté.

Les bannières de classification peuvent apparaître dans les contextes suivants, en fonction de votre configuration :

- Dans le cadre de la session en cours
- Sur l'écran de verrouillage
- Sur l'écran de connexion

Les bannières de classification peuvent prendre la forme d'une notification que vous pouvez supprimer ou d'une bannière permanente.

Pour plus d'informations, voir Affichage de la classification de sécurité du système .

(BZ#2031186)

Le fond d'écran par défaut ajoute un logo Red Hat

Le fond d'écran par défaut de RHEL affiche désormais un logo Red Hat. Le logo est situé dans le coin supérieur gauche de l'écran.

Pour désactiver le logo, désactivez l'extension **Background Logo** GNOME Shell.

(BZ#2057150)

Firefox utilise désormais un cryptage plus fort dans les fichiers PKCS#12

Le navigateur web Firefox utilise des fichiers PKCS#12 pour établir des certificats d'authentification client. Auparavant, Firefox chiffrait ces fichiers à l'aide d'algorithmes anciens :

- PBE-SHA1-RC2-40 pour crypter le certificat dans le fichier PKCS#12
- PBE-SHA1-3DES pour crypter la clé dans le fichier PKCS#12

Avec cette version, Firefox chiffre par défaut les fichiers à l'aide d'algorithmes plus puissants :

- AES-256-CBC avec PBKDF2 pour crypter le certificat dans le fichier PKCS#12
- AES-128-CBC avec PBKDF2 pour crypter la clé dans le fichier PKCS#12

Grâce à cette modification, les fichiers PKCS#12 sont désormais compatibles avec la norme FIPS (Federal Information Processing Standard).

Les anciens algorithmes de chiffrement restent pris en charge dans Firefox en tant qu'option non par défaut.

(BZ#1764205)

4.17. INFRASTRUCTURES GRAPHIQUES

La session Wayland est désormais la session par défaut avec les pilotes NVIDIA

Lors de l'utilisation des pilotes NVIDIA, la session de bureau sélectionne désormais le protocole d'affichage Wayland par défaut, si la configuration du pilote prend en charge Wayland. Dans les versions précédentes de RHEL, les pilotes NVIDIA désactivaient toujours Wayland.

Pour activer Wayland avec les pilotes NVIDIA sur votre système, ajoutez les options suivantes à la ligne de commande du noyau :

- **nvidia-drm.modeset=1**
- **NVreg_PreserveVideoMemoryAllocations=1**

Notez que Wayland est le protocole d'affichage par défaut avec d'autres pilotes graphiques depuis RHEL 8.0.

Actuellement, la session Wayland avec les pilotes NVIDIA est encore incomplète et présente certains problèmes connus. Red Hat travaille activement avec NVIDIA pour combler ces lacunes et résoudre ces problèmes dans l'ensemble de la pile GPU.

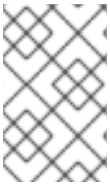
Pour connaître les limites de Wayland avec les pilotes NVIDIA, voir la section *Known issues*.

(JIRA:RHELPLAN-119000)

4.18. LA CONSOLE WEB

Authentification par carte à puce pour sudo et SSH depuis la console web

Auparavant, il n'était pas possible d'utiliser l'authentification par carte à puce pour obtenir les privilèges sudo ou utiliser SSH dans la console web. Avec cette mise à jour, les utilisateurs de la gestion des identités peuvent utiliser une carte à puce pour obtenir les privilèges sudo ou pour se connecter à un hôte différent avec SSH.



NOTE

Il n'est possible d'utiliser qu'une seule carte à puce pour s'authentifier et obtenir les privilèges sudo. L'utilisation d'une carte à puce distincte pour sudo n'est pas prise en charge.

(JIRA:RHELPLAN-95126)

Corrections de sécurité du noyau sans redémarrage dans la console web

Cette mise à jour de la console web permet aux utilisateurs d'appliquer les correctifs de sécurité du noyau sans forcer les redémarrages en utilisant le cadre **kpatch**. Les administrateurs peuvent également abonner automatiquement tout futur noyau au flux de correctifs en direct.

(JIRA:RHELPLAN-95056)

La console web RHEL fournit l'enregistrement Insights par défaut

Avec cette mise à jour, lorsque vous utilisez la console Web de Red Hat Enterprise Linux pour enregistrer un système RHEL, la case **Connect this system to Red Hat Insights.**est cochée par défaut. Si vous ne souhaitez pas vous connecter au service Insights, décochez la case.

(BZ#2049441)

Cockpit supporte désormais l'utilisation d'un certificat TLS existant

Grâce à cette amélioration, le certificat n'est plus soumis à des exigences strictes en matière d'autorisation de fichiers (comme **root:cockpit-ws 0640**) et peut donc être partagé avec d'autres services.

(JIRA:RHELPLAN-103855)

4.19. RÔLES DU SYSTÈME RED HAT ENTERPRISE LINUX

Le rôle de système de mise en réseau prend désormais en charge le SAE

Dans les réseaux Wi-Fi protected access version 3 (WPA3), la méthode d'authentification simultanée des égaux (SAE) garantit que la clé de chiffrement n'est pas transmise. Avec cette amélioration, le rôle de système RHEL de mise en réseau prend en charge la méthode SAE. Par conséquent, les administrateurs peuvent désormais utiliser le rôle de système de mise en réseau pour configurer les connexions aux réseaux Wi-Fi qui utilisent WPA-SAE.

(BZ#1993304)

Le rôle de système de mise en réseau prend désormais en charge owe

Le rôle de système RHEL de mise en réseau prend désormais en charge le chiffrement sans fil opportuniste (owe). **owe** est un type de gestion de clé d'authentification sans fil qui utilise le chiffrement entre les clients Wi-Fi et les points d'accès, et protège les clients Wi-Fi contre les attaques de reniflage. Pour utiliser owe, définissez le champ Type de gestion de clé d'authentification sans fil,**key_mgmt**, sur **owe**.

(BZ#1993377)

Le rôle de système de pare-feu permet désormais de définir la zone par défaut du pare-feu

Les zones représentent un concept permettant de gérer le trafic entrant de manière plus transparente. Les zones sont connectées à des interfaces de réseau ou se voient attribuer une série d'adresses

sources. Les règles de pare-feu pour chaque zone sont gérées indépendamment, ce qui permet à l'administrateur de définir des paramètres de pare-feu complexes et de les appliquer au trafic. Cette fonctionnalité permet de définir la zone par défaut utilisée comme zone par défaut pour l'attribution des interfaces, comme sur **firewall-cmd --set-default-zone zone-name**.

(BZ#2022461)

Le rôle de système RHEL de stockage prend désormais en charge les volumes LVM VDO

Avec cette amélioration, vous pouvez utiliser le rôle de système de stockage pour gérer les volumes LVM (Logical Manager Volumes) Virtual Data Optimizer (VDO). Le système de fichiers LVM gère les volumes VDO et, grâce à cette fonctionnalité, il est désormais possible de compresser et de dédupliquer sur les volumes LVM. Ainsi, VDO permet d'optimiser l'utilisation des volumes de stockage.

(BZ#1978488)

La prise en charge des tailles de volume exprimées en pourcentage est disponible dans le rôle de système de stockage

Cette amélioration ajoute au rôle de système RHEL de stockage la prise en charge de l'expression de la taille des volumes LVM en tant que pourcentage de la taille totale du pool. Vous pouvez spécifier la taille des volumes LVM en pourcentage de la taille du pool/VG, par exemple : 50 % en plus de la taille lisible par l'homme du système de fichiers, par exemple, 10g, 50 GiB.

(BZ#1984583)

La prise en charge des volumes mis en cache est disponible dans le rôle de système de stockage

Cette amélioration ajoute la prise en charge du rôle de système RHEL de stockage pour créer et gérer des volumes logiques LVM mis en cache. Le cache LVM peut être utilisé pour améliorer les performances des volumes logiques plus lents, en stockant temporairement des sous-ensembles de données d'un LV sur un périphérique plus petit et plus rapide, par exemple un SSD.

(BZ#2016517)

Possibilité d'ajouter ou de supprimer des sources au rôle de pare-feu

Cette mise à jour permet d'ajouter ou de supprimer des sources dans la configuration des paramètres du pare-feu à l'aide du paramètre **source**.

(BZ#2021667)

Nouveau rôle Ansible pour la gestion de Microsoft SQL Server

Le nouveau rôle **microsoft.sql.server** est conçu pour aider les administrateurs informatiques et de bases de données à automatiser les processus d'installation, de configuration et d'optimisation des performances de SQL Server sur Red Hat Enterprise Linux.

(BZ#2013853)

Microsoft SQL System Role prend désormais en charge le dépôt personnalisé pour les abonnements déconnectés ou satellites

Auparavant, les utilisateurs d'environnements déconnectés qui devaient télécharger des paquets à partir d'un serveur personnalisé ou les utilisateurs de Satellite qui devaient pointer vers Satellite ou Capsule n'étaient pas pris en charge par le rôle **microsoft.sql.server**. Cette mise à jour corrige ce problème en fournissant les variables **mssql_rpm_key**, **mssql_server_repository**, et **mssql_client_repository** que

vous pouvez utiliser pour personnaliser les référentiels à partir desquels télécharger les paquets. Si aucune URL n'est fournie, le rôle **mssql** utilise les serveurs officiels de Microsoft pour télécharger les RPM.

(BZ#2064648)

Le rôle MSSQL utilise systématiquement le commentaire "Ansible_managed" dans ses fichiers de configuration gérés

Le rôle MSSQL génère le fichier de configuration **/var/opt/mssql/mssql.conf**. Avec cette mise à jour, le rôle MSSQL insère le commentaire "Ansible managed" dans les fichiers de configuration, en utilisant la variable standard Ansible **ansible_managed**. Le commentaire indique que les fichiers de configuration ne doivent pas être modifiés directement car le rôle MSSQL peut écraser le fichier. Par conséquent, les fichiers de configuration contiennent une déclaration indiquant que les fichiers de configuration sont gérés par Ansible.

(BZ#2064690)

Prise en charge par Ansible Core des rôles système RHEL

À partir de la version RHEL 9 GA, Ansible Core est fourni, avec une portée de support limitée, pour permettre les cas d'utilisation d'automatisation pris en charge par RHEL. Ansible Core remplace Ansible Engine qui était fourni sur les versions précédentes de RHEL dans un dépôt séparé. Ansible Core est disponible dans le dépôt AppStream pour RHEL. Pour plus de détails sur les cas d'utilisation pris en charge, voir Scope of support for the Ansible Core package included in the RHEL 9 AppStream .

Si vous avez besoin d'une assistance pour Ansible Engine, ou si vous avez besoin d'une assistance pour des cas d'utilisation d'automatisation non RHEL, créez un cas sur Red Hat Support.

(JIRA:RHELPLAN-103540)

Prise en charge de la configuration de plusieurs hôtes elasticsearch dans un dictionnaire de sortie elasticsearch

Auparavant, le paramètre **server_host** prenait une valeur de chaîne pour un seul hôte. Cette amélioration l'adapte à la spécification sous-jacente **rsyslog omelasticsearch's**, de sorte qu'il accepte désormais également une liste de chaînes de caractères pour prendre en charge plusieurs hôtes. Par conséquent, il est adapté aux hôtes, conformément à la spécification sous-jacente **rsyslog omelasticsearch's**. Par conséquent, les utilisateurs peuvent configurer plusieurs hôtes **elasticsearch** dans un seul dictionnaire de sortie **elasticsearch**.

(BZ#1986460)

Les rôles système RHEL prennent désormais en charge la gestion des VPN

Auparavant, il était difficile de mettre en place des solutions sécurisées et correctement configurées de tunneling IPsec et de réseau privé virtuel (VPN) sur Linux. Grâce à cette amélioration, vous pouvez utiliser le rôle système VPN RHEL pour mettre en place et configurer plus facilement des tunnels VPN pour les connexions d'hôte à hôte et les connexions maillées sur un grand nombre d'hôtes. Vous disposez ainsi d'une interface de configuration cohérente et stable pour la configuration des tunnels VPN et IPsec dans le cadre du projet RHEL System Roles.

(BZ#2019341)

Le rôle de système SSHD RHEL prend désormais en charge les extraits de configuration non exclusifs

Grâce à cette fonctionnalité, vous pouvez configurer SSHD à travers différents rôles et playbooks sans

réécrire les configurations précédentes en utilisant des espaces de noms. Les espaces de noms sont similaires à un répertoire de dépôt et définissent des extraits de configuration non exclusifs pour SSHD. Par conséquent, vous pouvez utiliser le rôle de système SSHD RHEL à partir d'un rôle différent, si vous avez besoin de configurer seulement une petite partie de la configuration et non pas le fichier de configuration entier.

(BZ#1978752)

Ajout de l'option Network Time Security (NTS) au rôle de système timesync RHEL

L'option **NTS** a été ajoutée au rôle système de Timesync RHEL pour activer **NTS** sur les serveurs clients. NTS est un nouveau mécanisme de sécurité spécifié pour le protocole NTP (Network Time Protocol). NTS peut sécuriser la synchronisation des clients NTP sans configuration spécifique au client et peut s'adapter à un grand nombre de clients. L'option **NTS** n'est prise en charge qu'avec le fournisseur NTP **chrony** à partir de la version 4.0.

(BZ#1978753)

Prise en charge du rôle de système RHEL pour les clusters HA

Le rôle de cluster de haute disponibilité (HA Cluster) est désormais entièrement pris en charge. Les configurations suivantes sont disponibles :

- Configuration des périphériques, des ressources, des groupes de ressources et des clones de ressources de la clôture, y compris les métaattributs et les opérations sur les ressources
- Configuration des contraintes de localisation des ressources, des contraintes de colocation des ressources, des contraintes d'ordre des ressources et des contraintes de ticket des ressources
- Configuration des propriétés du cluster
- Configuration des nœuds de cluster, des noms de cluster personnalisés et des noms de nœuds
- Configuration des clusters multi-link
- Configurer le démarrage automatique des clusters au démarrage

L'exécution du rôle supprime toute configuration non prise en charge par le rôle ou non spécifiée lors de l'exécution du rôle.

Le rôle de système de cluster HA ne prend pas actuellement en charge les SBD.

(BZ#2054401)

Prise en charge de l'authentification par nom d'utilisateur et mot de passe Rsyslog pour Elasticsearch

Cette mise à jour ajoute les paramètres de nom d'utilisateur et de mot de passe Elasticsearch au rôle de système de journalisation. Par conséquent, vous pouvez permettre à Rsyslog de s'authentifier auprès d'Elasticsearch à l'aide d'un nom d'utilisateur et d'un mot de passe.

(BZ#1990490)

Le rôle du système client de l'EDNB prend en charge les adresses IP statiques

Dans les versions précédentes de RHEL, le redémarrage d'un système doté d'une adresse IP statique et configuré avec le rôle de système client NBDE (Network Bound Disk Encryption) modifiait l'adresse IP du système. Avec cette modification, les systèmes avec des adresses IP statiques sont pris en charge par le rôle de système client NBDE et leurs adresses IP ne changent pas après un redémarrage.

Notez que par défaut, le rôle d'EDNB utilise DHCP au démarrage, et bascule sur l'IP statique configurée lorsque le système est démarré.

(BZ#2031555)

La prise en charge de la spécification de raid_level pour LVM a été ajoutée

RHEL 9.0 prend en charge le regroupement des volumes LVM (Logical Volume Management) en RAID à l'aide de la fonctionnalité **lvmraid**.

(BZ#2016518)

Le rôle Certificat utilise systématiquement le commentaire "Ansible_managed" dans ses scripts d'accroche

Avec cette amélioration, le rôle de certificat génère des pré-scripts et des post-scripts pour soutenir les fournisseurs, auxquels le rôle insère le commentaire "Ansible managed" à l'aide de la variable standard Ansible "ansible_managed" :

- **/etc/certmonger/pre-scripts/script_name.sh**
- **/etc/certmonger/post-scripts/script_name.sh**

Le commentaire indique que les fichiers de script ne doivent pas être modifiés directement car le rôle de certificat peut écraser le fichier. Par conséquent, les fichiers de configuration contiennent une déclaration indiquant que les fichiers de configuration sont gérés par Ansible.

(BZ#2054364)

Une nouvelle option auto_gateway permet de contrôler le comportement de l'itinéraire par défaut

Auparavant, le paramètre **DEFROUTE** n'était pas configurable à l'aide de fichiers de configuration, mais uniquement manuellement en nommant chaque itinéraire. Cette mise à jour ajoute une nouvelle option **auto_gateway** dans la section de configuration **ip** pour les connexions, avec laquelle vous pouvez contrôler le comportement de l'itinéraire par défaut. Vous pouvez configurer **auto_gateway** de la manière suivante :

- S'il est défini sur **true**, les paramètres de la passerelle par défaut s'appliquent à une route par défaut.
- S'il est défini sur **false**, l'itinéraire par défaut est supprimé.
- S'il n'est pas spécifié, le rôle **network** utilise le comportement par défaut du rôle **network_provider** sélectionné.

(BZ#1978773)

Prise en charge de toutes les options de collage ajoutées au rôle du système network

Cette mise à jour prend en charge toutes les options de liaison pour le rôle de système RHEL **network**. Par conséquent, elle vous permet de contrôler de manière flexible la transmission du réseau sur l'interface liée. Par conséquent, vous pouvez contrôler la transmission du réseau sur l'interface liée en spécifiant plusieurs options pour cette interface.

(BZ#2054435)

NetworkManager permet de spécifier une carte réseau à l'aide de son adresse PCI

Auparavant, lors de l'établissement d'un profil de connexion, NetworkManager ne pouvait spécifier une carte réseau qu'en utilisant son nom ou son adresse MAC. Dans ce cas, le nom de l'appareil n'est pas stable et l'adresse MAC nécessite un inventaire pour maintenir l'enregistrement des adresses MAC utilisées. Désormais, vous pouvez spécifier une carte réseau en fonction de son adresse PCI dans un profil de connexion.

(BZ#1999162)

Le rôle Network System gère désormais directement les fichiers de configuration d'Ansible

Avec cette amélioration, le rôle **network** génère des fichiers **ifcfg** dans **/etc/sysconfig/network-scripts**. Il insère ensuite le commentaire "Ansible managed", en utilisant la variable standard **ansible_managed**. Ce commentaire indique que les fichiers **ifcfg** ne sont pas directement modifiables car le rôle **network** peut les écraser. La différence importante dans le traitement du fichier **ifcfg** pour ajouter le commentaire "Ansible managed" est que le rôle **network** utilise le paquetage **initscripts** alors que le NetworkManager utilise le paquetage **nm**.

(BZ#2057657)

Prise en charge par Ansible Core des rôles système RHEL

Dans RHEL 9.0, Ansible Core est fourni, avec une portée de support limitée, pour permettre les cas d'utilisation d'automatisation pris en charge par RHEL. Ansible Core remplace Ansible Engine qui était précédemment fourni dans un dépôt séparé. Ansible Core est disponible dans le dépôt AppStream pour RHEL. Pour plus de détails sur les cas d'utilisation pris en charge, voir Scope of support for the Ansible Core package included in the RHEL 9 and RHEL 8.6 and later AppStream repositories. Les utilisateurs doivent migrer manuellement leurs systèmes d'Ansible Engine vers Ansible Core.

(BZ#2012298)

Le rôle de système de cockpit est désormais pris en charge

Grâce à cette amélioration, vous pouvez installer et configurer la console web dans votre système. Par conséquent, vous pouvez gérer la console web de manière automatisée.

(BZ#2021028)

Le rôle de système d'enregistrement de la session Terminal utilise le commentaire "Ansible managed" dans ses fichiers de configuration gérés

Le rôle d'enregistrement de session terminal génère 2 fichiers de configuration :

- **/etc/sssd/conf.d/sssd-session-recording.conf**
- **/etc/tlog/tlog-rec-session.conf**

Avec cette mise à jour, le rôle d'enregistrement de session Terminal insère le commentaire "Ansible managed" dans les fichiers de configuration, en utilisant la variable Ansible standard **ansible_managed**. Le commentaire indique que les fichiers de configuration ne doivent pas être modifiés directement, car le rôle d'enregistrement de la session Terminal peut écraser le fichier. Par conséquent, les fichiers de configuration contiennent une déclaration indiquant que les fichiers de configuration sont gérés par Ansible.

(BZ#2054367)

Le rôle VPN utilise systématiquement le commentaire "Ansible_managed" dans ses fichiers de configuration gérés

Le rôle VPN génère le fichier de configuration suivant :

- **/etc/ipsec.d/mesh.conf**
- **/etc/ipsec.d/policies/clear**
- **/etc/ipsec.d/policies/private**
- **/etc/ipsec.d/policies/private-or-clear**

Avec cette mise à jour, le rôle VPN insère le commentaire "Ansible managed" dans les fichiers de configuration, en utilisant la variable standard Ansible **ansible_managed**. Le commentaire indique que les fichiers de configuration ne doivent pas être modifiés directement car le rôle VPN peut écraser le fichier. Par conséquent, les fichiers de configuration contiennent une déclaration indiquant que les fichiers de configuration sont gérés par Ansible.

(BZ#2054369)

Le rôle Postfix utilise systématiquement le commentaire "Ansible_managed" dans ses fichiers de configuration gérés

Le rôle Postfix génère le fichier de configuration **/etc/postfix/main.cf**. Avec cette mise à jour, le rôle Postfix insère le commentaire "Ansible managed" dans les fichiers de configuration, en utilisant la variable standard Ansible **ansible_managed**. Le commentaire indique que les fichiers de configuration ne doivent pas être modifiés directement car le rôle Postfix peut écraser le fichier. En conséquence, les fichiers de configuration contiennent une déclaration indiquant que les fichiers de configuration sont gérés par Ansible.

(BZ#2057662)

Le rôle de système RHEL de pare-feu a été ajouté dans RHEL 9

Avec cette amélioration, le rôle de système RHEL **rhel-system-roles.firewall** a été ajouté au paquetage **rhel-system-roles**. Les administrateurs peuvent ainsi automatiser leurs paramètres de pare-feu pour les nœuds gérés.

(BZ#2021665)

Le client SSH RHEL System Role prend désormais en charge les nouvelles options de configuration d'OpenSSH 8.7

Avec cette amélioration, OpenSSH a été mis à jour vers la dernière version, qui fournit de nouvelles options de configuration disponibles dans le rôle de client SSH pour configurer de nouveaux hôtes.

(BZ#2029427)

4.20. VIRTUALISATION

Nouvelles fonctionnalités de virtualisation de la console web RHEL

Avec cette mise à jour, la console web RHEL inclut de nouvelles fonctionnalités dans la page Machines virtuelles. Vous pouvez désormais :

- Renommer une VM
- Créer une VM avec l'authentification de l'image du nuage
- Ajouter et supprimer des périphériques USB et PCI à la VM
- Spécifier le modèle d'interface réseau

- Partager et annuler le partage de fichiers entre un hôte et sa VM

(JIRA:RHELPLAN-102009)

QEMU utilise Clang

L'émulateur QEMU est désormais construit à l'aide du compilateur Clang. Cela permet à l'hyperviseur KVM de RHEL 9 d'utiliser un certain nombre de fonctions de sécurité et de débogage avancées, et rend le développement de futures fonctions plus efficace.

(BZ#1940132)

SafeStack pour les machines virtuelles

Dans RHEL 9 sur du matériel AMD64 et Intel 64 (x86_64), l'émulateur QEMU peut utiliser SafeStack, une fonction améliorée de protection de la pile basée sur le compilateur. SafeStack réduit la capacité d'un attaquant à exploiter un débordement de mémoire tampon basé sur la pile pour modifier les pointeurs de retour dans la pile et créer des attaques de programmation orientée retour (Return-Oriented Programming, ROP). Par conséquent, les machines virtuelles hébergées sur RHEL 9 sont nettement plus sûres contre les vulnérabilités basées sur la programmation orientée retour.

(BZ#1939509)

prise en charge complète des virus sur Intel 64, AMD64 et IBM Z

Le système de fichiers virtio (**virtiofs**) est désormais entièrement pris en charge sur les architectures Intel 64, AMD64 et IBM Z. En utilisant **virtiofs**, vous pouvez partager efficacement des fichiers entre votre système hôte et ses machines virtuelles.

(JIRA:RHELPLAN-64576)

Processeurs AMD EPYC 7003 pris en charge par les invités KVM

La prise en charge des processeurs AMD EPYC de la série 7003 (également connus sous le nom de **AMD Milan**) a été ajoutée au code de l'hyperviseur et du noyau KVM, ainsi qu'à l'API libvirt. Cela permet aux machines virtuelles KVM d'utiliser les processeurs AMD EPYC de la série 7003.

(JIRA:RHELPLAN-65223)

qemu-kvm prend désormais en charge d'autres types de machines

Un ensemble de nouveaux types de machines, basés sur RHEL 9, a été ajouté pour être utilisé par les machines virtuelles (VM). Pour obtenir tous les types de machines actuellement pris en charge sur votre hôte, utilisez la commande **/usr/libexec/qemu-kvm -M help**.

En outre, tous les types de machines basés sur RHEL 7.5.0 ou une version antérieure ne sont plus pris en charge. Il s'agit également des types de machines **pc-i440fx-rhel7.5.0** et antérieures, qui étaient par défaut dans les versions majeures précédentes de RHEL. Par conséquent, toute tentative de démarrage d'une VM avec de tels types de machines sur RHEL 9 échoue avec une erreur **unsupported configuration**. Si vous rencontrez ce problème après avoir mis à niveau votre hôte vers RHEL 9, consultez la base de connaissances de Red Hat .

(JIRA:RHELPLAN-75866)

Les périphériques médiatisés sont désormais pris en charge par les CLI de virtualisation sur IBM Z

En utilisant **virt-install** ou **virt-xml**, vous pouvez désormais attacher des périphériques à médiation à vos machines virtuelles, tels que vfio-ap et vfio-ccw. Cela permet par exemple une gestion plus souple des

périphériques de stockage DASD et des coprocesseurs cryptographiques sur les hôtes IBM Z. En outre, à l'aide de **virt-install**, vous pouvez créer une VM qui utilise un périphérique DASD existant comme disque principal. Pour obtenir des instructions à ce sujet, consultez le guide Configurer et gérer la virtualisation dans RHEL 9.

(BZ#1995131)

Démons modulaires libvirt

Dans RHEL 9, la bibliothèque **libvirt** utilise des démons modulaires qui gèrent des ensembles de pilotes de virtualisation individuels sur votre hôte. Par exemple, le démon **virtqemud** gère les pilotes QEMU. Il est ainsi possible d'affiner une série de tâches impliquant des pilotes de virtualisation, telles que l'optimisation de la charge des ressources et la surveillance.

De plus, le démon monolithique libvirt, **libvirtd**, est devenu obsolète. Cependant, si vous passez de RHEL 8 à RHEL 9, votre hôte utilisera toujours **libvirtd**, que vous pouvez continuer à utiliser dans RHEL 9. Néanmoins, Red Hat recommande de passer aux démons modulaires **libvirt** à la place.

(JIRA:RHELPLAN-113994)

Les invités Windows 11 et Windows Server 2022 sont pris en charge

RHEL 9 prend en charge l'utilisation de Windows 11 et Windows Server 2022 en tant que systèmes d'exploitation invités sur les machines virtuelles KVM.

(BZ#2036856, BZ#2004161)

ksmtuned est désormais distribué séparément de qemu-kvm

Afin de réduire l'empreinte de l'hyperviseur KVM, l'utilitaire **ksmtuned** ne dépend plus de **qemu-kvm**. Par conséquent, si vous souhaitez configurer la fusion des pages identiques du noyau (KSM), vous devez installer manuellement le paquetage **ksmtuned**.

(BZ#2069501, BZ#1971678, BZ#1972158)

Nouvelle fonctionnalité : vTPM

Le module de plateforme virtuelle de confiance (vTPM) est entièrement pris en charge dans RHEL 9. vTPM permet d'ajouter un crypto-processeur virtuel TPM à une machine virtuelle (VM) exécutée dans l'hyperviseur KVM de RHEL 9. Il est ainsi possible d'utiliser la VM pour générer, stocker et gérer des clés cryptographiques.

(JIRA:RHELPLAN-98617)

Prise en charge de la virtualisation pour les processeurs Intel Atom de la série P59

Avec cette mise à jour, la virtualisation sur RHEL 9 ajoute la prise en charge des processeurs Intel Atom de la série P59, anciennement connus sous le nom de Snow Ridge. Par conséquent, les machines virtuelles hébergées sur RHEL 9 peuvent désormais utiliser le modèle de CPU **Snowridge** et profiter des nouvelles fonctionnalités offertes par ces processeurs.

(BZ#1874187)

4.21. RHEL DANS LES ENVIRONNEMENTS EN NUAGE

RHEL 9 fournit WALinuxAgent 2.3.0.2

RHEL 9 est distribué avec le paquetage Windows Azure Linux Agent (**WALinuxAgent**) version 2.3.0.2. Les corrections de bogues et améliorations notables par rapport à la version 2.2.49 sont les suivantes :

- La prise en charge des API RequiredFeatures et GoalStateAggregateStatus a été ajoutée.
- Des emplacements de repli pour les manifestes d'extension ont été ajoutés.
- Les appels manquants à str.format() ont été ajoutés lors de la création d'exceptions.

(BZ#1972101)

RHEL on Azure prend désormais en charge MANA

Les machines virtuelles RHEL 9 fonctionnant sur Microsoft Azure peuvent désormais utiliser l'adaptateur réseau Microsoft Azure (MANA).

(BZ#1957818)

cloud-init prend en charge la source de données VMware GuestInfo

Avec cette mise à jour, l'utilitaire **cloud-init** est en mesure de lire la source de données pour les données VMware guestinfo. Par conséquent, l'utilisation de **cloud-init** pour configurer des machines virtuelles RHEL 9 sur VMware vSphere est désormais plus efficace et plus fiable.

(BZ#2040090)

Les machines virtuelles RHEL 9 sont désormais prises en charge sur certains hôtes ARM64 sur Azure

Les machines virtuelles utilisant RHEL 9 comme système d'exploitation invité sont désormais prises en charge sur les hyperviseurs Microsoft Azure fonctionnant sur des processeurs Ampere Altra ARM.

(BZ#1949613)

cloud-init prend en charge les données des utilisateurs sur Microsoft Azure

L'option **--user-data** a été introduite pour l'utilitaire **cloud-init**. Cette option permet de transmettre des scripts et des métadonnées du service de métadonnées d'instance Azure (IMDS) lors de la configuration d'une machine virtuelle RHEL 9 sur Azure.

(BZ#2042351)

Nouveau module SSH pour cloud-init

Avec cette mise à jour, un module SSH a été ajouté à l'utilitaire **cloud-init**, qui génère automatiquement des clés d'hôte lors de la création d'une instance.

Notez qu'avec ce changement, la configuration par défaut de **cloud-init** a été mise à jour. Par conséquent, si vous avez effectué une modification locale, assurez-vous que le fichier /etc/cloud/cloud.cfg contient la ligne "ssh_genkeytypes : ['rsa', 'ecdsa', 'ed25519']\N" ligne.

Sinon, **cloud-init** crée une image qui ne démarre pas le service **sshd**. Dans ce cas, procédez comme suit pour contourner le problème :

1. Assurez-vous que le fichier **/etc/cloud/cloud.cfg** contient la ligne suivante :

```
ssh_genkeytypes:  ['rsa', 'ecdsa', 'ed25519']
```

2. Vérifiez si les fichiers **/etc/ssh/ssh_host_*** existent dans l'instance.

3. Si les fichiers **/etc/ssh/ssh_host_*** n'existent pas, utilisez la commande suivante pour générer des clés d'hôte :

```
cloud-init single --name cc_ssh
```

4. Redémarrez le service sshd :

```
systemctl restart sshd
```

(BZ#2115791)

4.22. CAPACITÉ DE SOUTIEN

sos report propose désormais un mode d'estimation

Cette mise à jour de **sos report** ajoute l'option **--estimate-only** qui permet d'évaluer l'espace disque nécessaire à la collecte d'un rapport **sos** à partir d'un serveur RHEL. Exécution de la commande **sos report --estimate-only**:

- exécute un test à blanc de **sos report**
- imite tous les plugins consécutivement et estime leur taille sur le disque.

Notez que l'estimation finale de l'espace disque est très approximative. Il est donc recommandé de doubler la valeur estimée.

(BZ#2011537)

4.23. CONTENEURS

Podman prend désormais en charge les noms courts sécurisés

Les alias de noms courts pour les images peuvent désormais être configurés dans le fichier **registries.conf**, dans la table **[aliases]**. Les modes de noms courts sont les suivants :

- Mise en application : Si aucun alias correspondant n'est trouvé lors de l'extraction de l'image, Podman invite l'utilisateur à choisir l'un des registres de recherche non qualifiée. Si l'image sélectionnée est extraite avec succès, Podman enregistre automatiquement un nouvel alias de nom court dans le fichier **$HOME/.cache/containers/short-name-aliases.conf** (utilisateur sans racine) et dans le fichier **/var/cache/containers/short-name-aliases.conf** (utilisateur racine). Si l'utilisateur ne peut pas être invité (par exemple, stdin ou stdout n'est pas un TTY), Podman échoue. Notez que le fichier **short-name-aliases.conf** a la priorité sur le fichier **registries.conf** si les deux spécifient le même alias.
- Permissif : Semblable au mode d'exécution, mais Podman n'échoue pas si l'utilisateur ne peut pas être invité à le faire. Au lieu de cela, Podman effectue une recherche dans tous les registres de recherche non qualifiés dans l'ordre donné. Notez qu'aucun alias n'est enregistré.

Exemple :

```
unqualified-search-registries=["registry.fedoraproject.org", "quay.io"]

[aliases]

"fedora"="registry.fedoraproject.org/fedora"
```

-

(JIRA:RHELPLAN-74542)

Changements dans le module container-tools

Le module **container-tools** contient les outils Podman, Buildah, Skopeo et runc. Le flux roulant, représenté par le flux **container-tools:rhel8** dans RHEL 8, est nommé **container-tools:latest** dans RHEL 9. Comme dans RHEL 8, les versions stables des outils de conteneur seront disponibles dans des flux numérotés (par exemple, 3.0).

Pour plus d'informations sur le flux d'applications des outils de conteneurisation, voir Container Tools AppStream - Content Availability.

(JIRA:RHELPLAN-73678)

Le paquet containers-common est maintenant disponible

Le paquet **containers-common** a été ajouté au module **container-tools:latest**. Le paquet **containers-common** contient des fichiers de configuration communs et de la documentation pour l'écosystème des outils de conteneurs, tels que Podman, Buildah et Skopeo.

(JIRA:RHELPLAN-77549)

Mise à jour des images de conteneurs avec de nouveaux paquets

Par exemple, pour mettre à jour l'image du conteneur **registry.access.redhat.com/rhel9** avec les derniers paquets, utilisez les commandes suivantes :

```
# podman run -it registry.access.redhat.com/rhel9
# dnf update -y && rm -rf /var/cache/dnf
```

Pour installer un élément particulier ***<package>*** entrer :

```
# dnf install <package>
```

Pour plus d'informations, voir Ajouter un logiciel à un conteneur UBI en cours d'exécution .

Notez que pour RHEL 9, la mise à jour ou l'installation de nouveaux paquets dans l'image nécessite que vous fonctionniez sur un hôte autorisé. Vous pouvez utiliser l'abonnement Red Hat Enterprise Linux Developer Subscription for Individuals pour accéder gratuitement aux référentiels autorisés.

Pour plus d'informations, voir Abonnement individuel gratuit pour développeur Red Hat Enterprise Linux : FAQ.

(JIRA:RHELPLAN-84168)

Le méta-paquet container-tools a été mis à jour

Le méta-paquet RPM **container-tools**, qui contient les outils Podman, Buildah, Skopeo et runc, est désormais disponible. Cette mise à jour fournit une liste de corrections de bogues et d'améliorations par rapport à la version précédente.

(JIRA:RHELPLAN-118914)

Le paquet podman-py est maintenant disponible

Le paquet **podman-py** a été ajouté au flux de modules stables **container-tools:3.0** et au module **container-tools:latest**. Le paquet **podman-py** est une bibliothèque de liens permettant d'utiliser l'API RESTful de Podman.

(BZ#1975462)

La version 2 des groupes de contrôle est maintenant disponible

La version précédente des groupes de contrôle, cgroups version 1 (cgroups v1), entraînait des problèmes de performance avec diverses applications. La dernière version des groupes de contrôle, cgroups version 2 (cgroups v2), permet aux administrateurs système de limiter les ressources pour n'importe quelle application sans causer de problèmes de performance.

Cette nouvelle version des groupes de contrôle, cgroups v2, peut être activée dans RHEL 8 et l'est par défaut dans RHEL 9.

(JIRA:RHELPLAN-73697)

Le méta-paquet container-tools est maintenant disponible

Le méta-paquet RPM **container-tools**, qui comprend Podman, Buildah, Skopeo, CRIU, Udica et toutes les bibliothèques requises, est disponible dans RHEL 9. Les flux stables ne sont pas disponibles sur RHEL 9. Pour bénéficier d'un accès stable à Podman, Buildah, Skopeo et autres, utilisez l'abonnement RHEL EUS.

Pour installer le méta-paquet **container-tools**, entrez :

```
# dnf install container-tools
```

(BZ#2000871)

La prise en charge native des systèmes de fichiers superposés dans le noyau est désormais disponible

La prise en charge des systèmes de fichiers superposés est désormais disponible à partir du noyau 5.11. Les utilisateurs non rootés bénéficieront des performances natives du système de fichiers overlayfs même lorsqu'ils fonctionnent sans root (en tant qu'utilisateur). Ainsi, cette amélioration fournit de meilleures performances aux utilisateurs non root qui souhaitent utiliser overlayfs sans avoir besoin de bind mounting.

(JIRA:RHELPLAN-99892)

Le stockage NFS est maintenant disponible

Vous pouvez désormais utiliser le système de fichiers NFS comme support de stockage pour les conteneurs et les images si votre système de fichiers prend en charge les xattr.

(JIRA:RHELPLAN-74543)

Le méta-paquet container-tools a été mis à jour

Le méta-paquet **container-tools** comprend Podman, Buildah, Skopeo, CRIU, Udica et toutes les bibliothèques nécessaires. Cette mise à jour fournit une liste de corrections de bogues et d'améliorations par rapport à la version précédente.

Les changements les plus notables sont les suivants :

- En raison des changements apportés à la pile réseau, les conteneurs créés par Podman v3 et les versions antérieures ne sont pas utilisables dans Podman v4.0
- Le système de fichiers superposé natif est utilisable en tant qu'utilisateur sans racine
- Le stockage NFS est désormais pris en charge dans un conteneur
- Les groupes de contrôle version 2 (cgroup v2) sont activés par défaut
- La rétrogradation de Podman v4 vers Podman v3 n'est pas possible à moins que tous les conteneurs ne soient détruits et recréés

Pour plus d'informations sur les changements notables dans Podman, voir les notes de version en amont.

(JIRA:RHELPLAN-99889)

Le conteneur d'exécution crun est maintenant utilisé par défaut

L'exécution du conteneur **crun** est désormais l'exécution par défaut. L'exécution du conteneur **crun** prend en charge une annotation qui permet au conteneur d'accéder aux groupes supplémentaires de l'utilisateur sans racine. Ceci est utile pour le montage de volumes dans un répertoire où setgid est défini, ou lorsque l'utilisateur n'a qu'un accès de groupe. Les moteurs d'exécution **crun** et **runc** supportent entièrement **cgroup v2**.

(JIRA:RHELPLAN-99890)

La version 2 du groupe de contrôle est maintenant disponible

La version précédente des groupes de contrôle, cgroup version 1 (cgroup v1), entraînait des problèmes de performance avec diverses applications. La dernière version des groupes de contrôle, cgroup version 2 (cgroup v2), permet aux administrateurs système de limiter les ressources pour n'importe quelle application sans causer de problèmes de performance.

Dans RHEL 9, cgroup v2 est activé par défaut.

(JIRA:RHELPLAN-75322)

Les images de base universelles sont désormais disponibles sur Docker Hub

Auparavant, les images de base universelles n'étaient disponibles qu'à partir du catalogue de conteneurs Red Hat. Avec cette amélioration, les images de base universelles sont également disponibles à partir de Docker Hub en tant qu'image Verified Publisher .

(JIRA:RHELPLAN-100032)

L'image du conteneur openssl est maintenant disponible

L'image **openssl** fournit un outil de ligne de commande **openssl** permettant d'utiliser les différentes fonctions de la bibliothèque cryptographique OpenSSL. La bibliothèque OpenSSL permet de générer des clés privées, de créer des demandes de signature de certificat (CSR) et d'afficher des informations sur les certificats.

L'image du conteneur **openssl** est disponible dans ces dépôts :

- registry.redhat.io/rhel9/openssl
- registry.access.redhat.com/ubi9/openssl

(JIRA:RHELPLAN-100034)

La pile réseau Netavark est désormais disponible

La pile Netavark est un outil de configuration réseau pour les conteneurs. Dans RHEL 9, la pile Netavark est entièrement prise en charge et activée par défaut.

Cette pile de réseau possède les capacités suivantes :

- Création, gestion et suppression d'interfaces réseau, y compris les interfaces de pont et MACVLAN
- Configuration des paramètres du pare-feu, tels que la traduction d'adresses réseau (NAT) et les règles de mappage des ports
- IPv4 et IPv6
- Capacité améliorée pour les conteneurs dans plusieurs réseaux

(JIRA:RHELPLAN-101141)

Podman supporte maintenant l'auto-construction et l'auto-exécution de pods à l'aide d'un fichier YAML

La commande **podman play kube** construit et exécute automatiquement plusieurs pods avec plusieurs conteneurs dans les pods à l'aide d'un fichier YAML.

(JIRA:RHELPLAN-108830)

Podman a désormais la possibilité de trouver des plages de subUID et de subGID à partir d'IdM

Les plages de sous-UID et de sous-GID peuvent désormais être gérées par IdM. Au lieu de déployer les mêmes fichiers **/etc/subuid** et **/etc/subgid** sur chaque hôte, vous pouvez maintenant définir les plages dans un seul stockage central. Vous devez modifier le fichier **/etc/nsswitch.conf** et ajouter **sss** à la ligne services map : **services: files sss**.

Pour plus de détails, voir la section sur la gestion manuelle des plages de sous-ID dans la documentation IdM.

(JIRA:RHELPLAN-100020)

CHAPITRE 5. BUG FIXES

Cette partie décrit les bogues corrigés dans Red Hat Enterprise Linux 9.0 qui ont un impact significatif sur les utilisateurs.

5.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

--leavebootorder ne modifie plus l'ordre de démarrage

Auparavant, l'utilisation de **--leavebootorder** pour la commande bootloader kickstart ne fonctionnait pas correctement sur les systèmes UEFI et modifiait l'ordre de démarrage. Le programme d'installation ajoutait alors RHEL en tête de la liste des systèmes installés dans le menu de démarrage UEFI.

Cette mise à jour corrige le problème et l'utilisation de **--leavebootorder** ne modifie plus l'ordre de démarrage dans le chargeur de démarrage. **--leavebootorder** est désormais pris en charge sur RHEL pour les systèmes UEFI.

(BZ#2025953)

Anaconda définit un nom d'hôte statique avant d'exécuter les scripts %post

Auparavant, lorsqu'Anaconda définissait le nom d'hôte de l'environnement d'installation à la valeur de la configuration de démarrage (**network --hostname**), il définissait un nom d'hôte transitoire. Certaines des actions effectuées pendant l'exécution du script **%post**, par exemple l'activation de périphériques réseau, entraînaient la réinitialisation du nom d'hôte à une valeur obtenue par l'opération inverse **dns**.

Avec cette mise à jour, Anaconda définit désormais un nom d'hôte statique de l'environnement d'installation pour qu'il soit stable pendant l'exécution des scripts kickstart **%post**.

(BZ#2009403)

Les utilisateurs peuvent désormais spécifier des comptes d'utilisateurs dans le plan d'installation de RHEL for Edge

Auparavant, l'exécution d'une mise à jour sur votre blueprint sans compte utilisateur défini dans l'edge commit pour la mise à niveau, comme l'ajout d'un package rpm, entraînait le verrouillage des utilisateurs d'un système, après l'application d'une mise à niveau. Ce problème a été résolu pour permettre aux utilisateurs de spécifier des comptes d'utilisateur dans le Blueprint RHEL for Edge Installer, qui crée un utilisateur sur le système au moment de l'installation, plutôt que d'avoir l'utilisateur dans le cadre du commit **ostree**.

(BZ#2060575)

Le mode basic graphics a été supprimé du menu de démarrage

Auparavant, le mode **basic graphics** était utilisé pour installer RHEL sur du matériel doté d'une carte graphique non prise en charge ou pour contourner des problèmes liés aux pilotes graphiques qui empêchaient le démarrage de l'interface graphique. Avec cette mise à jour, l'option d'installation en mode **basic graphics** a été supprimée du menu de démarrage du programme d'installation. Utilisez les options d'installation VNC pour les installations graphiques sur du matériel non pris en charge ou pour contourner les bogues des pilotes.

Pour plus d'informations sur les installations utilisant VNC, voir la section Effectuer une installation RHEL à distance à l'aide de VNC.

(BZ#1961092)

5.2. GESTION DES ABONNEMENTS

virt-who fonctionne désormais correctement avec les hôtes Hyper-V

Auparavant, lors de l'utilisation de **virt-who** pour configurer des machines virtuelles (VM) RHEL 9 sur un hyperviseur Hyper-V, **virt-who** ne communiquait pas correctement avec l'hyperviseur et la configuration échouait. Cela était dû à une méthode de cryptage obsolète dans le paquet **openssl**.

Avec cette mise à jour, le mode d'authentification **virt-who** pour Hyper-V a été modifié, et la configuration des VM RHEL 9 sur Hyper-V à l'aide de **virt-who** fonctionne désormais correctement. Notez que cela nécessite également que l'hyperviseur utilise le mode d'authentification de base. Pour activer ce mode, utilisez les commandes suivantes :

```
winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

(BZ#2008215)

5.3. GESTION DES LOGICIELS

L'exécution de createrepo_c --update sur un référentiel modulaire préserve désormais les métadonnées modulaires qui s'y trouvent

Auparavant, lors de l'exécution de la commande **createrepo_c --update** sur un référentiel modulaire existant sans la source originale des métadonnées modulaires, la politique par défaut était de supprimer toutes les métadonnées supplémentaires, y compris les métadonnées modulaires, de ce référentiel, ce qui, par conséquent, le cassait. Pour préserver les métadonnées, il fallait exécuter la commande **createrepo_c --update** avec l'option supplémentaire **--keep-all-metadata**.

Avec cette mise à jour, vous pouvez préserver les métadonnées modulaires sur un référentiel modulaire en exécutant **createrepo_c --update** sans option supplémentaire.

Pour supprimer des métadonnées supplémentaires, vous pouvez utiliser l'option new **--discard-additional-metadata**.

(BZ#2055032)

5.4. SHELLS ET OUTILS DE LIGNE DE COMMANDE

RHEL 9 fournit libservicelog 1.1.19

RHEL 9 est distribué avec **libservicelog** version 1.1.19. Les corrections de bogues notables incluent :

- Correction d'un problème d'alignement de la sortie.
- Correction de **segfault** en cas d'échec de **servicelog_open()**.

(BZ#1869568)

5.5. SÉCURITÉ

Optimisation matérielle activée sur libgcrypt en mode FIPS

Auparavant, la norme FIPS 140-2 (Federal Information Processing Standard) n'autorisait pas l'utilisation de l'optimisation matérielle. Par conséquent, dans les versions précédentes de RHEL, l'opération était

désactivée dans le paquet **libgcrypt** en mode FIPS. RHEL 9 permet l'optimisation matérielle en mode FIPS et, par conséquent, toutes les opérations cryptographiques sont exécutées plus rapidement.

(BZ#1990059)

crypto-policies il est désormais possible de désactiver l'utilisation du cryptogramme ChaCha20

Auparavant, le paquet **crypto-policies** utilisait un mot-clé erroné pour désactiver le chiffrement **ChaCha20** dans OpenSSL. Par conséquent, vous ne pouviez pas désactiver **ChaCha20** pour le protocole TLS 1.2 dans OpenSSL via **crypto-policies**. Avec cette mise à jour, le mot-clé **-CHACHA20** est utilisé à la place de **-CHACHA20-POLY1305**. Par conséquent, vous pouvez maintenant utiliser les politiques cryptographiques pour désactiver l'utilisation du chiffrement **ChaCha20** dans OpenSSL pour TLS 1.2 et TLS 1.3.

(BZ#2004207)

les systèmes IBM Z 64 bits ne deviennent plus non amorçables lors de l'installation en mode FIPS

Auparavant, la commande **fips-mode-setup** avec l'option **--no-bootcfg** n'exécutait pas l'outil **zipl**. Comme **fips-mode-setup** régénère le disque RAM initial (**initrd**) et que le système résultant a besoin d'une mise à jour de l'état interne de **zipl** pour démarrer, les systèmes IBM Z 64 bits se retrouvaient dans un état non amorçable après une installation en mode FIPS. Avec cette mise à jour, **fips-mode-setup** exécute désormais **zipl** sur les systèmes IBM Z 64 bits, même s'il est invoqué avec **--no-bootcfg**, ce qui permet au système nouvellement installé de démarrer avec succès.

(BZ#2013195)

GNUTLS_NO_EXPLICIT_INIT ne désactive plus l'initialisation implicite de la bibliothèque

Auparavant, la variable d'environnement **GNUTLS_NO_EXPLICIT_INIT** désactivait l'initialisation implicite de la bibliothèque. Dans RHEL 9, la variable **GNUTLS_NO_IMPLICIT_INIT** désactive l'initialisation implicite des bibliothèques.

(BZ#1999639)

Les applications basées sur OpenSSL fonctionnent désormais correctement avec les paramètres linguistiques turcs

La bibliothèque **OpenSSL** utilisant des fonctions de comparaison de chaînes insensibles à la casse, les applications basées sur OpenSSL ne fonctionnaient pas correctement avec les paramètres linguistiques turcs, et les vérifications omises provoquaient le plantage des applications utilisant ces paramètres. Cette mise à jour fournit un correctif permettant d'utiliser les paramètres régionaux POSIX (Portable Operating System Interface) pour la comparaison de chaînes insensibles à la casse. Par conséquent, les applications basées sur OpenSSL telles que curl fonctionnent correctement avec les paramètres linguistiques turcs.

(BZ#2071631)

kdump ne plante plus à cause des permissions SELinux

Le service de récupération en cas de panne **kdump** nécessite des autorisations SELinux supplémentaires pour démarrer correctement. Par conséquent, dans les versions précédentes, SELinux empêchait **kdump** de fonctionner, **kdump** signalait qu'il n'était pas opérationnel et des refus d'accès au cache vectoriel (AVC) étaient audités. Dans cette version, les autorisations requises ont été ajoutées à **selinux-policy** et, par conséquent, **kdump** fonctionne correctement et aucun déni d'AVC n'est audité.

(BZ#1932752)

Le paquet usbguard-selinux ne dépend plus de usbguard

Auparavant, le paquet **usbguard-selinux** dépendait du paquet **usbguard**. Cette dépendance, combinée à d'autres dépendances de ces paquets, entraînait des conflits de fichiers lors de l'installation de **usbguard**. Par conséquent, cela empêchait l'installation de **usbguard** sur certains systèmes. Avec cette version, **usbguard-selinux** ne dépend plus de **usbguard**, et par conséquent, **dnf** peut installer **usbguard** correctement.

(BZ#1986785)

dnf install et dnf update fonctionnent désormais avec fapolicyd dans SELinux

Le paquet **fapolicyd-selinux**, qui contient les règles SELinux pour fapolicyd, ne contenait pas les autorisations nécessaires pour surveiller tous les fichiers et répertoires. Par conséquent, le paquet **fapolicyd-dnf-plugin** ne fonctionnait pas correctement, ce qui faisait que les commandes **dnf install** et **dnf update** empêchaient le système de répondre indéfiniment. Dans cette version, les autorisations de surveiller tout type de fichier ont été ajoutées à **fapolicyd-selinux**. En conséquence, **fapolicyd-dnf-plugin** fonctionne correctement et les commandes **dnf install** et **dnf update** sont opérationnelles.

(BZ#1932225)

Les capacités ambiantes sont désormais appliquées correctement aux utilisateurs non root

Par mesure de sécurité, le passage d'un UID (User Identifier) de root à non-root annule les ensembles de capacités autorisées, efficaces et ambiantes.

Cependant, le module **pam_cap.so** n'est pas en mesure de définir les capacités ambiantes, car une capacité doit figurer à la fois dans l'ensemble autorisé et dans l'ensemble héritable pour faire partie de l'ensemble ambiant. En outre, l'ensemble autorisé est annulé après un changement d'UID (par exemple en utilisant l'utilitaire **setuid**), de sorte que la capacité ambiante ne peut pas être définie.

Pour résoudre ce problème, le module **pam_cap.so** prend désormais en charge l'option **keepcaps**, qui permet à un processus de conserver ses capacités autorisées après le passage de l'UID "root" à "non-root". Le module **pam_cap.so** prend également en charge l'option **defer**, qui permet à **pam_cap.so** de réappliquer les capacités ambiantes dans un rappel à **pam_end()**. Ce rappel peut être utilisé par d'autres applications après un changement d'UID.

Par conséquent, si les utilitaires **su** et **login** sont mis à jour et compatibles avec PAM, vous pouvez désormais utiliser **pam_cap.so** avec les options **keepcaps** et **defer** pour définir les capacités ambiantes pour les utilisateurs non root.

(BZ#2037215)

usbguard-notifier n'enregistre plus trop de messages d'erreur dans le journal

Auparavant, le service **usbguard-notifier** ne disposait pas des autorisations de communication interprocessus (IPC) pour se connecter à l'interface IPC **usbguard-daemon**. Par conséquent, **usbguard-notifier** n'a pas réussi à se connecter à l'interface et a écrit un message d'erreur correspondant dans le Journal. Comme **usbguard-notifier** a démarré avec l'option **--wait**, qui garantit que **usbguard-notifier** tente de se connecter à l'interface IPC chaque seconde après un échec de connexion, par défaut, le journal contient bientôt un nombre excessif de ces messages.

Avec cette mise à jour, **usbguard-notifier** ne démarre pas avec **--wait** par défaut. Le service tente de se connecter au démon seulement trois fois dans les intervalles d'une seconde. Par conséquent, le journal contient au maximum trois messages d'erreur de ce type.

(BZ#2009226)

5.6. MISE EN RÉSEAU

Les profils de connexion Wifi et Ethernet 802.1x se connectent désormais correctement

Auparavant, de nombreux profils de connexions Wifi et Ethernet 802.1x ne pouvaient pas se connecter. Ce bogue est maintenant corrigé. Tous les profils se connectent désormais correctement. Les profils qui utilisent des algorithmes cryptographiques anciens fonctionnent toujours, mais vous devez activer manuellement le fournisseur OpenSSL ancien. Cela est nécessaire, par exemple, lorsque vous utilisez DES avec MS-CHAPv2 et RC4 avec TKIP.

(BZ#1975718)

Afterburn ne met plus en place un nom d'hôte trop long en /etc/hostname

La longueur maximale d'un nom d'hôte RHEL est de 64 caractères. Cependant, certains fournisseurs de services en nuage utilisent le nom de domaine entièrement qualifié (FQDN) comme nom d'hôte, qui peut comporter jusqu'à 255 caractères. Auparavant, le service **afterburn-hostname** écrivait un tel nom d'hôte trop long directement dans le fichier **/etc/hostname**. Le service **systemd** tronquait le nom d'hôte à 64 caractères, et NetworkManager dérivait un domaine de recherche DNS incorrect à partir de la valeur tronquée. Avec cette correction, **afterburn-hostname** tronque les noms d'hôtes au premier point ou à 64 caractères, selon ce qui vient en premier. Par conséquent, NetworkManager ne définit plus de domaines de recherche DNS invalides dans **/etc/resolv.conf**.

(BZ#2008521)

5.7. NOYAU

modprobe charge les modules du noyau hors de l'arborescence comme prévu

Le fichier de configuration **/etc/depmod.d/dist.conf** fournit un ordre de recherche pour l'utilitaire **depmod**. En fonction de l'ordre de recherche, **depmod** crée le fichier **modules.dep.bin**. Ce fichier répertorie les dépendances des modules, que l'utilitaire **modprobe** utilise pour charger et décharger les modules du noyau et résoudre les dépendances des modules en même temps. Auparavant, le fichier **/etc/depmod.d/dist.conf** était manquant. Par conséquent, **modprobe** ne pouvait pas charger certains modules du noyau hors-arbre. Cette mise à jour inclut le fichier de configuration **/etc/depmod.d/dist.conf**, qui corrige l'ordre de recherche. Par conséquent, **modprobe** charge les modules de noyau hors-arbre comme prévu.

(BZ#1985100)

alsa-lib gère désormais correctement les périphériques audio qui utilisent UCM

Un bogue dans le paquetage **alsa-lib** a provoqué une analyse incorrecte de l'identifiant interne du Use Case Manager (UCM). Par conséquent, certains périphériques audio utilisant la configuration UCM n'ont pas été détectés ou n'ont pas fonctionné correctement. Le problème se produisait plus souvent lorsque le système utilisait le service audio **pipewire**. Avec la nouvelle version de RHEL 9, le problème a été corrigé en mettant à jour la bibliothèque **alsa-lib**.

(BZ#2015863)

5.8. SYSTÈMES DE FICHIERS ET STOCKAGE

Les événements de protection n'entraînent plus l'échec du rechargement des dispositifs à chemins multiples

Auparavant, lorsqu'un périphérique de chemin d'accès **read-only** était réanalysé, le noyau envoyait deux uevents de protection en écriture - l'un avec le périphérique défini sur **read**/**write**, et le suivant avec le périphérique défini sur **read-only**. Par conséquent, lors de la détection de l'événement **read**/**write** sur un périphérique de chemin d'accès, **multipathd** a essayé de recharger le périphérique à chemins multiples, ce qui a provoqué un message d'erreur de rechargement. Avec cette mise à jour, **multipathd** vérifie désormais que tous les chemins d'accès sont définis sur **read**/**write** avant de recharger un périphérique en lecture/écriture. Par conséquent, **multipathd** n'essaie plus de recharger **read**/**write** chaque fois qu'un périphérique **read-only** est analysé à nouveau.

(BZ#2017979)

device-mapper-multipath repassé à la version 0.8.7

Le paquet **device-mapper-multipath** a été mis à jour vers la version 0.8.7, qui apporte de nombreuses corrections de bogues et améliorations. Les changements notables sont les suivants :

- Correction des fuites de mémoire dans les commandes **multipath** et **kpartx**.
- Correction des erreurs de déclenchement répétées dans le fichier d'unité **multipathd.socket**.
- Amélioration de l'autoconfiguration d'un plus grand nombre de périphériques, tels que les baies DELL SC Series, les baies EMC Invista et Symmetrix (entre autres).

(BZ#2017592)

5.9. HAUTE DISPONIBILITÉ ET CLUSTERS

Le gestionnaire d'attributs de Pacemaker détermine correctement les attributs des nœuds distants, ce qui permet d'éviter les boucles de désencombrement

Auparavant, le contrôleur de Pacemaker sur un nœud pouvait être élu contrôleur désigné (DC) avant que son gestionnaire d'attributs n'apprenne qu'un nœud distant déjà actif était distant. Dans ce cas, le planificateur du nœud ne voyait aucun des attributs du nœud distant. Si le cluster utilisait l'unfencing, cela pouvait entraîner une boucle d'unfencing. Avec la correction, le gestionnaire d'attributs peut maintenant apprendre qu'un nœud distant est distant au moyen d'événements supplémentaires, y compris la synchronisation initiale des attributs au démarrage. Par conséquent, aucune boucle d'inféodation ne se produit, quel que soit le nœud élu DC.

(BZ#1975388)

5.10. COMPILATEURS ET OUTILS DE DÉVELOPPEMENT

-Wsequence-point correction du comportement de l'avertissement

Auparavant, lors de la compilation de programmes C avec GCC, l'option d'avertissement **-Wsequence-point** essayait d'avertir des expressions très longues, ce qui pouvait entraîner un comportement quadratique et donc un temps de compilation significativement plus long. Avec cette mise à jour, **-Wsequence-point** n'essaie pas d'avertir des expressions extrêmement longues et, par conséquent, n'augmente pas le temps de compilation.

(BZ#1481850)

5.11. GESTION DE L'IDENTITÉ

Authentification MS-CHAP avec le fournisseur historique OpenSSL

Auparavant, les mécanismes d'authentification FreeRADIUS qui utilisaient MS-CHAP échouaient car ils dépendaient des fonctions de hachage MD4, et MD4 a été déprécié dans RHEL 9. Avec cette mise à jour, vous pouvez authentifier les utilisateurs FreeRADIUS avec MS-CHAP ou MS-CHAPv2 si vous activez le fournisseur OpenSSL hérité.

Si vous utilisez le fournisseur OpenSSL par défaut, l'authentification MS-CHAP et MS-CHAPv2 échoue et le message d'erreur suivant s'affiche, indiquant la correction à apporter :

```
Couldn't init MD4 algorithm. Enable OpenSSL legacy provider.
```

(BZ#1978216)

L'exécution de commandes sudo n'exporte plus la variable d'environnement KRB5CCNAME

Auparavant, après l'exécution des commandes **sudo**, la variable d'environnement **KRB5CCNAME** pointait vers le cache d'informations d'identification Kerberos de l'utilisateur d'origine, qui pouvait ne pas être accessible à l'utilisateur cible. Par conséquent, les opérations liées à Kerberos pouvaient échouer car ce cache n'était pas accessible. Avec cette mise à jour, l'exécution des commandes **sudo** ne définit plus la variable d'environnement **KRB5CCNAME** et l'utilisateur cible peut utiliser son cache d'informations d'identification Kerberos par défaut.

(BZ#1879869)

SSSD évalue correctement le paramètre par défaut pour le nom du keytab Kerberos dans le fichier /etc/krb5.conf

Auparavant, si vous définissiez un emplacement non standard pour votre fichier **krb5.keytab**, SSSD n'utilisait pas cet emplacement et utilisait à la place l'emplacement par défaut **/etc/krb5.keytab**. Par conséquent, lorsque vous essayiez de vous connecter au système, la connexion échouait car le fichier **/etc/krb5.keytab** ne contenait aucune entrée.

Avec cette mise à jour, SSSD évalue désormais la variable **default_keytab_name** dans **/etc/krb5.conf** et utilise l'emplacement spécifié par cette variable. SSSD utilise uniquement l'emplacement par défaut **/etc/krb5.keytab** si la variable **default_keytab_name** n'est pas définie.

(BZ#1737489)

L'authentification au serveur d'annuaire en mode FIPS avec des mots de passe hachés avec l'algorithme PBKDF2 fonctionne désormais comme prévu

Lorsque Directory Server fonctionne en mode FIPS (Federal Information Processing Standard), la fonction **PK11_ExtractKeyValue()** n'est pas disponible. Par conséquent, avant cette mise à jour, les utilisateurs dont le mot de passe était haché à l'aide de l'algorithme PBKDF2 (password-based key derivation function 2) ne pouvaient pas s'authentifier auprès du serveur lorsque le mode FIPS était activé. Avec cette mise à jour, Directory Server utilise désormais la fonction **PK11_Decrypt()** pour obtenir les données de hachage du mot de passe. Par conséquent, l'authentification avec des mots de passe hachés avec l'algorithme PBKDF2 fonctionne maintenant comme prévu.

(BZ#1779685)

5.12. RÔLES DU SYSTÈME RED HAT ENTERPRISE LINUX

Le rôle de système de mise en réseau n'échoue plus à définir un domaine de recherche DNS si IPv6 est désactivé

Auparavant, la fonction **nm_connection_verify()** de la bibliothèque **libnm** n'ignorait pas le domaine de recherche DNS si le protocole IPv6 était désactivé. Par conséquent, lorsque vous utilisiez le rôle de système RHEL de mise en réseau et que vous définissiez **dns_search** avec **ipv6_disabled: true**, le rôle de système échouait avec l'erreur suivante :

```
nm-connection-error-quark: ipv6.dns-search: this property is not allowed for 'method=ignore' (7)
```

Avec cette mise à jour, la fonction **nm_connection_verify()** ignore le domaine de recherche DNS si IPv6 est désactivé. Par conséquent, vous pouvez utiliser **dns_search** comme prévu, même si IPv6 est désactivé.

(BZ#2004899)

Postfix role README n'utilise plus de nom de rôle simple

Auparavant, les exemples fournis dans le site **/usr/share/ansible/roles/rhel-system-roles.postfix/README.md** utilisaient la version simple du nom de rôle, **postfix**, au lieu de **rhel-system-roles.postfix**. Par conséquent, les utilisateurs consultaient la documentation et utilisaient à tort le nom de rôle ordinaire au lieu du nom de rôle qualifié complet (FQRN). Cette mise à jour corrige le problème et la documentation contient des exemples avec le FQRN, **rhel-system-roles.postfix**, ce qui permet aux utilisateurs d'écrire correctement les playbooks.

(BZ#1958964)

Le fichier README.md de Postfix RHEL System Role ne manque plus de variables dans la section "Role Variables"

Auparavant, les variables de rôle du système Postfix RHEL, telles que **postfix_check**, **postfix_backup**, **postfix_backup_multiple**, n'étaient pas disponibles dans la section "Variables de rôle". Par conséquent, les utilisateurs ne pouvaient pas consulter la documentation sur les rôles de Postfix. Cette mise à jour ajoute la documentation des variables de rôle à la section README de Postfix. Les variables de rôle sont documentées et disponibles pour les utilisateurs dans la documentation **doc/usr/share/doc/rhel-system-roles/postfix/README.md** fournie par **rhel-system-roles**.

(BZ#1978734)

Les tâches de rôle ne changent plus lors de l'exécution de la même sortie

Auparavant, plusieurs tâches du rôle étaient signalées comme étant **CHANGED** lorsque la même entrée était exécutée une nouvelle fois, même s'il n'y avait pas de changement. Par conséquent, le rôle n'agissait pas de manière idempotente. Pour résoudre ce problème, effectuez les actions suivantes :

- Vérifiez si les variables de configuration changent avant de les appliquer. Vous pouvez utiliser l'option **--check** pour cette vérification.
- N'ajoutez pas d'en-tête **Last Modified: $date** au fichier de configuration.

Par conséquent, les tâches de rôle sont idempotentes.

(BZ#1978760)

L'option logging_purge_confs supprime correctement les fichiers de configuration inutiles

Lorsque l'option **logging_purge_confs** est définie sur **true**, elle devrait supprimer les fichiers de configuration de journalisation inutiles. Auparavant, cependant, les fichiers de configuration inutiles n'étaient pas supprimés du répertoire de configuration, même si **logging_purge_confs** était défini sur **true**. Ce problème est désormais résolu et l'option a été redéfinie comme suit : si **logging_purge_confs**

est défini sur **true**, Rsyslog supprime les fichiers du répertoire **rsyslog.d** qui n'appartiennent à aucun paquetage rpm. Cela inclut les fichiers de configuration générés par les exécutions précédentes du rôle Logging. La valeur par défaut de **logging_purge_confs** est **false**.

(BZ#2039106)

Un playbook utilisant le rôle Metrics se termine avec succès sur plusieurs exécutions même si le mot de passe de Grafana admin est changé

Auparavant, les modifications apportées au mot de passe de l'utilisateur Grafana **admin** après l'exécution du rôle Metrics avec le booléen **metrics_graph_service: yes** entraînaient l'échec des exécutions ultérieures du rôle Metrics. Cela entraînait l'échec des playbooks utilisant le rôle Metrics, et les systèmes concernés n'étaient que partiellement configurés pour l'analyse des performances. Désormais, le rôle Metrics utilise l'API Grafana **deployment** lorsqu'elle est disponible et ne nécessite plus la connaissance du nom d'utilisateur ou du mot de passe pour effectuer les actions de configuration nécessaires. Par conséquent, un playbook utilisant le rôle Metrics se termine avec succès lors de plusieurs exécutions, même si l'administrateur modifie le mot de passe Grafana **admin**.

(BZ#2041632)

La configuration par le rôle Metrics suit désormais correctement les liens symboliques

Lorsque le paquet **mssql pcp** est installé, le fichier **mssql.conf** est situé dans **/etc/pcp/mssql/** et est ciblé par le lien symbolique **/var/lib/pcp/pmdas/mssql/mssql.conf**. Auparavant, cependant, le rôle Metrics écrasait le lien symbolique au lieu de le suivre et de configurer **mssql.conf**. Par conséquent, l'exécution du rôle Metrics a transformé le lien symbolique en un fichier normal et la configuration n'a donc affecté que le fichier **/var/lib/pcp/pmdas/mssql/mssql.conf**. Le lien symbolique a donc échoué et le fichier de configuration principal **/etc/pcp/mssql/mssql.conf** n'a pas été affecté par la configuration. Le problème est maintenant résolu et l'option **follow: yes** pour suivre le lien symbolique a été ajoutée au rôle Metrics. Par conséquent, le rôle Metrics préserve les liens symboliques et configure correctement le fichier de configuration principal.

(BZ#2058777)

Le rôle timesync n'échoue plus à trouver le service demandé ptp4l

Auparavant, sur certaines versions de RHEL, le module Ansible **service_facts** signalait les faits de service de manière incorrecte. Par conséquent, le rôle **timesync** signalait une erreur lors de la tentative d'arrêt du service **ptp4l**. Avec cette correction, le module Ansible **service_facts** vérifie la valeur de retour des tâches pour arrêter les services **timesync**. Si la valeur renvoyée est **failed**, mais que le message d'erreur est **Could not find the requested service NAME:**, le module suppose que l'opération a réussi. Par conséquent, le rôle **timesync** s'exécute maintenant sans erreurs comme **Could not find the requested service ptp4l**.

(BZ#2058645)

Le site kernel_settings configobj est disponible sur les hôtes gérés

Auparavant, le rôle **kernel_settings** n'installait pas le paquetage **python3-configobj** sur les hôtes gérés. Par conséquent, le rôle renvoyait une erreur indiquant que le module Python **configobj** était introuvable. Avec cette correction, le rôle s'assure que le paquetage **python3-configobj** est présent sur les hôtes gérés et le rôle **kernel_settings** fonctionne comme prévu.

(BZ#2058756)

Le rôle d'enregistrement de session de terminal tlog-rec-session est désormais correctement superposé à SSSD

Auparavant, le rôle de système RHEL d'enregistrement de session de terminal s'appuyait sur le fournisseur de fichiers SSSD (System Security Services Daemon) et sur l'option **authselect with-files-domain** activée pour configurer les entrées **passwd** correctes dans le fichier **nsswitch.conf**. Dans RHEL 9.0, SSSD n'activait pas implicitement le fournisseur de fichiers par défaut et, par conséquent, la superposition du shell **tlog-rec-session** par SSSD ne fonctionnait pas. Avec cette correction, le rôle d'enregistrement de session de terminal met désormais à jour le fichier **nsswitch.conf** pour s'assurer que **tlog-rec-session** est correctement superposé par SSSD.

(BZ#2071804)

Le rôle de système SSHD peut gérer des systèmes en mode FIPS

Auparavant, le rôle de système SSHD ne pouvait pas créer le type de clé d'hôte **not allowed** lorsqu'il était appelé. Par conséquent, le rôle de système SSHD ne pouvait pas gérer les systèmes RHEL 8 et antérieurs en mode FIPS (Federal Information Processing Standard). Avec cette mise à jour, le rôle système SSHD détecte le mode FIPS et ajuste correctement la liste des clés d'hôte par défaut. Par conséquent, le rôle système peut gérer les systèmes RHEL en mode FIPS avec la configuration HostKey par défaut.

(BZ#2029634)

Le rôle de système SSHD utilise le bon fichier de modèle

Auparavant, le rôle de système SSHD utilisait un mauvais fichier modèle. Par conséquent, le fichier **sshd_config** généré ne contenait pas le commentaire **ansible_managed**. Avec cette mise à jour, le rôle système utilise le bon fichier modèle et **sshd_config** contient le bon commentaire **ansible_managed**.

(BZ#2044408)

Le rôle de système Kdump RHEL est capable de redémarrer ou d'indiquer qu'un redémarrage est nécessaire

Auparavant, le rôle de système Kdump RHEL ignorait les nœuds gérés sans mémoire réservée pour le noyau de crash. Par conséquent, le rôle se terminait avec l'état "Success", même s'il ne configurait pas le système correctement. Avec cette mise à jour de RHEL 9, le problème a été corrigé. Dans les cas où les nœuds gérés n'ont pas de mémoire réservée pour le noyau de crash, le rôle Kdump RHEL System échoue et suggère aux utilisateurs de définir la variable **kdump_reboot_ok** sur **true** pour configurer correctement le service **kdump** sur les nœuds gérés.

(BZ#2029602)

Le fournisseur nm dans le rôle de système de mise en réseau gère désormais correctement les ponts

Auparavant, si vous utilisiez le fournisseur **initscripts**, le rôle de système de mise en réseau créait un fichier **ifcfg** qui configurait NetworkManager pour marquer les interfaces de pont comme non gérées. De plus, NetworkManager ne détectait pas les actions de suivi **initscript**. Par exemple, les actions **down** et **absent** du fournisseur initscript ne changeront pas la compréhension du NetworkManager sur l'état non géré de cette interface si la connexion n'est pas rechargée après les actions **down** et **absent**. Avec ce correctif, le rôle de système de réseau utilise la fonction **NM.Client.reload_connections_async()** pour recharger NetworkManager sur les hôtes gérés avec NetworkManager 1.18. Par conséquent, NetworkManager gère l'interface de pont lors de la commutation du fournisseur de **initscript** à **nm**.

(BZ#2038957)

Correction d'une erreur de typographie pour la prise en charge de active-backup pour le mode de liaison correct

Auparavant, il y avait une faute de frappe,**active_backup**, dans la prise en charge du port InfiniBand tout en spécifiant le mode de liaison **active-backup**. En raison de cette faute de frappe, la connexion ne prenait pas en charge le mode de liaison correct pour le port de liaison InfiniBand. Cette mise à jour corrige la faute de frappe en remplaçant le mode de liaison par **active-backup**. La connexion prend désormais en charge avec succès le port de liaison InfiniBand.

(BZ#2064391)

Le rôle de système d'enregistrement n'appelle plus les tâches plusieurs fois

Auparavant, le rôle Logging appelait plusieurs fois des tâches qui n'auraient dû être appelées qu'une seule fois. En conséquence, les appels de tâches supplémentaires ralentissaient l'exécution du rôle. Avec cette correction, le rôle d'enregistrement a été modifié pour n'appeler les tâches qu'une seule fois, améliorant ainsi les performances du rôle d'enregistrement.

(BZ#2004303)

Les rôles système RHEL gèrent désormais les commentaires ansible_managed sur plusieurs lignes dans les fichiers générés

Auparavant, certains rôles système RHEL utilisaient **# {{ ansible_managed }}** pour générer certains fichiers. Par conséquent, si un client avait un paramètre personnalisé de plusieurs lignes pour **ansible_managed**, les fichiers étaient générés de manière incorrecte. Avec cette correction, tous les rôles système utilisent l'équivalent de **{{ ansible_managed | comment }}** lors de la génération de fichiers, de sorte que la chaîne **ansible_managed** est toujours correctement commentée, y compris les valeurs multilignes **ansible_managed**. Par conséquent, les fichiers générés ont la valeur multiligne **ansible_managed** correcte.

(BZ#2006230)

Le rôle de système de pare-feu recharge désormais immédiatement le pare-feu lorsque target est modifié

Auparavant, le rôle de système de pare-feu ne rechargeait pas le pare-feu lorsque le paramètre **target** était modifié. Avec cette correction, le rôle de pare-feu recharge le pare-feu lorsque le paramètre **target** est modifié et, par conséquent, la modification de **target** est immédiate et disponible pour les opérations suivantes.

(BZ#2057164)

L'option group dans le rôle de système de certificats ne permet plus de maintenir les certificats inaccessibles au groupe

Auparavant, lors de la définition du groupe pour un certificat, le site **mode** n'était pas configuré pour autoriser la lecture par le groupe. Par conséquent, les membres du groupe ne pouvaient pas lire les certificats émis par le rôle Certificat. Avec cette correction, la configuration du groupe garantit maintenant que le mode de fichier inclut l'autorisation de lecture de groupe. Par conséquent, les certificats émis par le rôle Certificat pour les groupes sont accessibles aux membres du groupe.

(BZ#2021025)

Le rôle Logging ne manque plus de citations pour la valeur d'intervalle du module immark

Auparavant, la valeur du champ **interval** pour le module **immark** n'était pas correctement citée, car le module **immark** n'était pas correctement configuré. Cette correction permet de s'assurer que la valeur du champ **interval** est correctement citée. Le module **immark** fonctionne désormais comme prévu.

(BZ#2021676)

Le fichier /etc/tuned/kernel_settings/tuned.conf comporte un en-tête ansible_managed approprié

Auparavant, le rôle de système RHEL **kernel_settings** avait une valeur codée en dur pour l'en-tête **ansible_managed** dans le fichier **/etc/tuned/kernel_settings/tuned.conf**. Par conséquent, les utilisateurs ne pouvaient pas fournir leur propre en-tête **ansible_managed**. Dans cette mise à jour, le problème a été résolu de sorte que **kernel_settings** mette à jour l'en-tête de **/etc/tuned/kernel_settings/tuned.conf** avec le paramètre **ansible_managed** de l'utilisateur. En conséquence, **/etc/tuned/kernel_settings/tuned.conf** a un en-tête **ansible_managed** correct.

(BZ#2047506)

Le plugin de filtrage VPN System Role vpn_ipaddr convertit désormais en FQCN (Fully Qualified Collection Name)

Auparavant, la conversion de l'ancien format de rôle au format de collection ne convertissait pas le plugin de filtre **vpn_ipaddr** en FQCN (Fully Qualified Collection Name) **redhat.rhel_system_roles.vpn_ipaddr**. Par conséquent, le rôle VPN ne pouvait pas trouver le plugin par son nom court et signalait une erreur. Avec cette correction, le script de conversion a été modifié pour que le filtre soit converti au format FQCN dans la collection. Désormais, le rôle VPN s'exécute sans émettre d'erreur.

(BZ#2050341)

L'emploi pour kdump.service n'échoue plus

Auparavant, le code du rôle Kdump pour la configuration de la taille du crash du noyau n'a pas été mis à jour pour RHEL9, qui nécessite l'utilisation de **kdumpctl reset-crashkernel**. En conséquence, le rôle **kdump.service** ne pouvait pas démarrer et émettait une erreur. Avec cette mise à jour, le rôle **kdump.service** utilise **kdumpctl reset-crashkernel** pour configurer la taille du crash du noyau. Maintenant, le rôle **kdump.service** démarre avec succès le service kdump et la taille de crash du noyau est configurée correctement.

(BZ#2050419)

5.13. VIRTUALISATION

Le débranchement à chaud d'un disque virtuel monté ne provoque plus le plantage du noyau invité sur IBM Z

Auparavant, lors du détachement d'un disque monté d'une machine virtuelle (VM) en cours d'exécution sur du matériel IBM Z, le noyau de la VM se bloquait dans les conditions suivantes :

- Le disque a été attaché avec un bus cible de type **scsi** et monté à l'intérieur de l'invité.
- Après avoir débranché à chaud le disque, le contrôleur SCSI correspondant a également été débranché à chaud.

Avec cette mise à jour, le code sous-jacent a été corrigé et la panne décrite ne se produit plus.

(BZ#1997541)

5.14. CONTENEURS

Les conteneurs UBI 9-Beta peuvent fonctionner sur les hôtes RHEL 7 et 8

Auparavant, les images de conteneurs UBI 9-Beta avaient un profil seccomp incorrect dans le

paquetage **containers-common**. En conséquence, les conteneurs n'étaient pas en mesure de traiter certains appels système, ce qui entraînait une défaillance. Avec cette mise à jour, le problème a été corrigé.

(BZ#2019901)

CHAPITRE 6. APERÇUS TECHNOLOGIQUES

Cette partie fournit une liste de tous les aperçus technologiques disponibles dans Red Hat Enterprise Linux 9.

Pour plus d'informations sur l'étendue de l'assistance de Red Hat pour les fonctionnalités de l'aperçu technologique, voir l'étendue de l'assistance pour les fonctionnalités de l'aperçu technologique .

6.1. RHEL POUR EDGE

Le processus FDO est disponible en avant-première technologique

Le processus FDO pour le provisionnement automatique et l'onboarding des images RHEL for Edge est disponible en tant qu'aperçu technologique. Vous pouvez ainsi créer une image RHEL for Edge Simplified Installer, l'intégrer à une image RHEL for Edge et utiliser le processus FDO (FIDO device onboarding) pour approvisionner et intégrer automatiquement vos périphériques Edge et échanger des données avec d'autres périphériques et systèmes connectés sur les réseaux. Par conséquent, le protocole FIDO d'accueil des appareils effectue l'initialisation de l'appareil au stade de la fabrication, puis la liaison tardive pour l'utilisation effective de l'appareil.

(BZ#1989930)

6.2. SHELLS ET OUTILS DE LIGNE DE COMMANDE

ReaR disponible sur l'architecture IBM Z 64 bits en tant qu'aperçu technologique

La fonctionnalité de base Relax and Recover (ReaR) est désormais disponible sur l'architecture IBM Z 64 bits en tant qu'aperçu technologique. Vous pouvez créer une image de secours ReaR sur IBM Z uniquement dans l'environnement z/VM. La sauvegarde et la récupération des partitions logiques (LPAR) n'ont pas été testées.

La seule méthode de sortie actuellement disponible est l'Initial Program Load (IPL). L'IPL produit un noyau et un ramdisk initial (initrd) qui peut être utilisé avec le bootloader **zIPL**.

AVERTISSEMENT

Actuellement, le processus de récupération reformate tous les DASD (Direct Attached Storage Devices) connectés au système. Ne tentez pas de récupérer le système si des données de valeur se trouvent sur les périphériques de stockage du système. Cela inclut également le périphérique préparé avec le chargeur de démarrage **zIPL**, le noyau ReaR et l'initrd qui ont été utilisés pour démarrer dans l'environnement de secours. Veillez à en conserver une copie.

Pour plus d'informations, voir Utilisation d'une image de secours ReaR sur l'architecture IBM Z 64 bits .

(BZ#2046653)

GIMP disponible en avant-première technologique dans RHEL 9

GNU Image Manipulation Program (GIMP) 2.99.8 est maintenant disponible dans RHEL 9 en tant

qu'aperçu technologique. La version 2.99.8 du paquet **gimp** est une pré-version avec un ensemble d'améliorations, mais un ensemble limité de fonctionnalités et aucune garantie de stabilité. Dès que la version officielle de GIMP 3 sera publiée, elle sera introduite dans RHEL 9 en tant que mise à jour de cette version préliminaire.

Dans RHEL 9, vous pouvez facilement installer **gimp** en tant que paquetage RPM.

(BZ#2047161)

6.3. MISE EN RÉSEAU

WireGuard VPN est disponible en avant-première technologique

WireGuard, que Red Hat fournit en tant qu'aperçu technologique non pris en charge, est une solution VPN de haute performance qui fonctionne dans le noyau Linux. Elle utilise une cryptographie moderne et est plus facile à configurer que d'autres solutions VPN. En outre, la petite base de code de WireGuard réduit la surface d'attaque et, par conséquent, améliore la sécurité.

Pour plus de détails, voir Configuration d'un VPN WireGuard .

(BZ#1613522)

KTLS disponible en avant-première technologique

RHEL fournit Kernel Transport Layer Security (KTLS) en tant qu'aperçu technologique. KTLS traite les enregistrements TLS à l'aide des algorithmes de chiffrement ou de déchiffrement symétriques du noyau pour le chiffrement AES-GCM. KTLS inclut également l'interface permettant de décharger le chiffrement des enregistrements TLS sur les contrôleurs d'interface réseau (NIC) qui fournissent cette fonctionnalité.

(BZ#1570255)

Le service **systemd-resolved** est disponible en tant qu'aperçu technologique

Le service **systemd-resolved** fournit la résolution de noms aux applications locales. Le service met en œuvre un résolveur de stub DNS avec mise en cache et validation, un résolveur et un répondeur de DNS multidiffusion (Link-Local Multicast Name Resolution - LLMNR) et multidiffusion.

Notez que **systemd-resolved** est un aperçu technologique non pris en charge.

(BZ#2020529)

6.4. NOYAU

Le pilote Intel data streaming accelerator pour le noyau est disponible en tant qu'aperçu technologique

Le pilote de l'accélérateur de flux de données Intel (IDXD) pour le noyau est actuellement disponible en tant qu'aperçu technologique. Il s'agit d'un accélérateur intégré au processeur Intel qui comprend la file d'attente partagée avec la soumission de l'espace d'adressage du processus (pasid) et la mémoire virtuelle partagée (SVM).

(BZ#2030412)

SGX disponible en avant-première technologique

Software Guard Extensions(SGX) est une technologie Intel® destinée à protéger le code et les

données des logiciels contre la divulgation et la modification. Le noyau RHEL fournit partiellement les fonctionnalités SGX v1 et v1.5. La version 1 permet aux plateformes utilisant le mécanisme **Flexible Launch Control** d'utiliser la technologie SGX.

(BZ#1874182)

Le pilote Soft-iWARP est disponible en tant qu'aperçu technologique

Soft-iWARP (siw) est un logiciel, Internet Wide-area RDMA Protocol (iWARP), pilote de noyau pour Linux. Soft-iWARP met en œuvre la suite de protocoles iWARP sur la pile réseau TCP/IP. Cette suite de protocoles est entièrement mise en œuvre dans le logiciel et ne nécessite pas de matériel RDMA (Remote Direct Memory Access) spécifique. Soft-iWARP permet à un système doté d'un adaptateur Ethernet standard de se connecter à un adaptateur iWARP ou à un autre système sur lequel Soft-iWARP est déjà installé.

(BZ#2023416)

6.5. SYSTÈMES DE FICHIERS ET STOCKAGE

DAX est maintenant disponible pour ext4 et XFS en tant qu'aperçu technologique

Dans RHEL 9, le système de fichiers DAX est disponible en tant qu'aperçu technologique. DAX permet à une application de mapper directement la mémoire persistante dans son espace d'adressage. Pour utiliser DAX, un système doit disposer d'une certaine forme de mémoire persistante, généralement sous la forme d'un ou plusieurs modules de mémoire double en ligne non volatile (NVDIMM), et un système de fichiers compatible DAX doit être créé sur le(s) module(s) NVDIMM. Le système de fichiers doit également être monté avec l'option de montage **dax**. Ensuite, **mmap** d'un fichier sur le système de fichiers monté sur dax entraîne un mappage direct du stockage dans l'espace d'adressage de l'application.

(BZ#1995338)

Stratis est disponible en avant-première technologique

Stratis est un gestionnaire de stockage local. Il fournit des systèmes de fichiers gérés au-dessus des pools de stockage avec des fonctionnalités supplémentaires pour l'utilisateur :

- Gérer les snapshots et le thin provisioning
- Augmentation automatique de la taille du système de fichiers en fonction des besoins
- Maintenir les systèmes de fichiers

Pour administrer le stockage Stratis, utilisez l'utilitaire **stratis**, qui communique avec le service d'arrière-plan **stratisd**.

Stratis est fourni en tant qu'aperçu technologique.

Pour plus d'informations, voir la documentation Stratis : Configuration des systèmes de fichiers Stratis .

(BZ#2041558)

Fonctionnalités du service de découverte NVMe-oF disponibles en tant qu'aperçu technologique

Les fonctions du service de découverte NVMe-oF, définies dans les propositions techniques (TP) 8013 et 8014 de NVMexpress.org, sont disponibles en tant qu'aperçu technologique. Pour obtenir un aperçu de ces fonctionnalités, utilisez le paquetage **nvme-cli 2.0** et attachez l'hôte à un périphérique cible

NVMe-oF qui implémente le TP-8013 ou le TP-8014. Pour plus d'informations sur les TP-8013 et TP-8014, voir les TPs NVM Express 2.0 Ratifiés sur le site web https://nvmexpress.org/developers/nvme-specification/.

(BZ#2021672)

6.6. COMPILATEURS ET OUTILS DE DÉVELOPPEMENT

jmc-core et owasp-java-encoder disponible en avant-première technologique

RHEL 9 est distribué avec les paquets **jmc-core** et **owasp-java-encoder** en tant que fonctionnalités d'aperçu technologique.

jmc-core est une bibliothèque fournissant des API de base pour le contrôle de mission du kit de développement Java (JDK), y compris des bibliothèques pour l'analyse et l'écriture de fichiers d'enregistrement de vol JDK, ainsi que des bibliothèques pour la découverte de la machine virtuelle Java (JVM) par le biais du protocole de découverte Java (JDP).

Le paquetage **owasp-java-encoder** fournit une collection d'encodeurs contextuels à haute performance et à faible surcharge pour Java.

(BZ#1980981)

6.7. GESTION DE L'IDENTITÉ

DNSSEC disponible en tant qu'aperçu technologique dans IdM

Les serveurs de gestion de l'identité (IdM) avec DNS intégré mettent désormais en œuvre les extensions de sécurité DNS (DNSSEC), un ensemble d'extensions du DNS qui renforcent la sécurité du protocole DNS. Les zones DNS hébergées sur les serveurs IdM peuvent être automatiquement signées à l'aide de DNSSEC. Les clés cryptographiques sont générées automatiquement et font l'objet d'une rotation.

Il est conseillé aux utilisateurs qui décident de sécuriser leurs zones DNS avec DNSSEC de lire et de suivre ces documents :

- Pratiques opérationnelles DNSSEC, version 2
- Guide de déploiement du système de noms de domaine sécurisé (DNS)
- Considérations sur le calendrier de renouvellement des clés DNSSEC

Notez que les serveurs IdM avec DNS intégré utilisent DNSSEC pour valider les réponses DNS obtenues d'autres serveurs DNS. Cela peut affecter la disponibilité des zones DNS qui ne sont pas configurées conformément aux pratiques recommandées en matière de dénomination.

(BZ#2084180)

L'API JSON-RPC de gestion des identités est disponible en avant-première technologique

Une API est disponible pour la gestion des identités (IdM). Pour visualiser l'API, IdM fournit également un navigateur API en tant qu'aperçu technologique.

Auparavant, l'API IdM était améliorée pour permettre plusieurs versions des commandes de l'API. Ces améliorations pouvaient modifier le comportement d'une commande de manière incompatible. Les utilisateurs peuvent désormais continuer à utiliser les outils et les scripts existants même si l'API IdM change. Cela permet :

- Aux administrateurs d'utiliser des versions antérieures ou postérieures d'IdM sur le serveur par rapport au client de gestion.
- Les développeurs peuvent utiliser une version spécifique d'un appel IdM, même si la version IdM change sur le serveur.

Dans tous les cas, la communication avec le serveur est possible, même si l'une des parties utilise, par exemple, une version plus récente qui introduit de nouvelles options pour une fonctionnalité.

Pour plus de détails sur l'utilisation de l'API, voir Utilisation de l'API de gestion des identités pour communiquer avec le serveur IdM (AVANT-PROPOS TECHNOLOGIQUE).

(BZ#2084166)

ACME disponible en avant-première technologique

Le service Automated Certificate Management Environment (ACME) est désormais disponible dans Identity Management (IdM) en tant qu'aperçu technologique. ACME est un protocole de validation automatisée des identifiants et d'émission de certificats. Son objectif est d'améliorer la sécurité en réduisant la durée de vie des certificats et en évitant les processus manuels de gestion du cycle de vie des certificats.

Dans RHEL, le service ACME utilise le répondeur ACME PKI de Red Hat Certificate System (RHCS). Le sous-système RHCS ACME est automatiquement déployé sur chaque serveur d'autorité de certification (CA) dans le déploiement IdM, mais il ne traite pas les demandes jusqu'à ce que l'administrateur l'active. RHCS utilise le profil **acmeIPAServerCert** lors de l'émission de certificats ACME. La période de validité des certificats émis est de 90 jours. L'activation ou la désactivation du service ACME affecte l'ensemble du déploiement IdM.

IMPORTANT

Il est recommandé d'activer ACME uniquement dans un déploiement IdM où tous les serveurs utilisent RHEL 8.4 ou une version ultérieure. Les versions antérieures de RHEL n'incluent pas le service ACME, ce qui peut entraîner des problèmes dans les déploiements de versions mixtes. Par exemple, un serveur CA sans ACME peut faire échouer les connexions des clients, car il utilise un Subject Alternative Name (SAN) DNS différent.

AVERTISSEMENT

Actuellement, le RHCS ne supprime pas les certificats expirés. Comme les certificats ACME expirent après 90 jours, les certificats expirés peuvent s'accumuler, ce qui peut affecter les performances.

- Pour activer l'ACME dans l'ensemble du déploiement IdM, utilisez la commande **ipa-acme-manage enable**:

```
# ipa-acme-manage enable
The ipa-acme-manage command was successful
```

- Pour désactiver ACME dans l'ensemble du déploiement IdM, utilisez la commande **ipa-acme-manage disable**:

```
# ipa-acme-manage disable
The ipa-acme-manage command was successful
```

- Pour vérifier si le service ACME est installé et s'il est activé ou désactivé, utilisez la commande **ipa-acme-manage status**:

```
# ipa-acme-manage status
ACME is enabled
The ipa-acme-manage command was successful
```

(BZ#2084181)

6.8. BUREAU

GNOME pour l'architecture ARM 64 bits disponible en tant qu'aperçu technologique

L'environnement de bureau GNOME est disponible pour l'architecture ARM 64 bits en tant qu'aperçu technologique.

Vous pouvez désormais vous connecter à la session de bureau d'un serveur ARM 64 bits à l'aide de VNC. Vous pouvez ainsi gérer le serveur à l'aide d'applications graphiques.

Un ensemble limité d'applications graphiques est disponible sur ARM 64 bits. Par exemple :

- Le navigateur web Firefox
- Red Hat Subscription Manager (**subscription-manager-cockpit**)
- Configuration du pare-feu (**firewall-config**)
- Analyseur d'utilisation du disque (**baobab**)

Avec Firefox, vous pouvez vous connecter au service Cockpit sur le serveur.

Certaines applications, comme LibreOffice, ne fournissent qu'une interface en ligne de commande, et leur interface graphique est désactivée.

(JIRA:RHELPLAN-27394)

GNOME pour l'architecture IBM Z disponible en avant-première technologique

L'environnement de bureau GNOME est disponible pour l'architecture IBM Z en tant qu'aperçu technologique.

Vous pouvez désormais vous connecter à la session de bureau d'un serveur IBM Z à l'aide de VNC. Vous pouvez ainsi gérer le serveur à l'aide d'applications graphiques.

Un ensemble limité d'applications graphiques est disponible sur IBM Z. Par exemple :

- Le navigateur web Firefox
- Red Hat Subscription Manager (**subscription-manager-cockpit**)
- Configuration du pare-feu (**firewall-config**)

- Analyseur d'utilisation du disque (**baobab**)

Avec Firefox, vous pouvez vous connecter au service Cockpit sur le serveur.

Certaines applications, comme LibreOffice, ne fournissent qu'une interface en ligne de commande, et leur interface graphique est désactivée.

(JIRA:RHELPLAN-27737)

6.9. LA CONSOLE WEB

Stratis disponible en tant qu'aperçu technologique dans la console web RHEL

Avec cette mise à jour, la console web de Red Hat Enterprise Linux permet de gérer le stockage Stratis en tant qu'aperçu technologique.

Pour en savoir plus sur Stratis, voir Qu'est-ce que Stratis ?

(JIRA:RHELPLAN-122345)

6.10. VIRTUALISATION

AMD SEV et SEV-ES pour les machines virtuelles KVM

En tant qu'aperçu technologique, RHEL 9 fournit la fonction Secure Encrypted Virtualization (SEV) pour les machines hôtes AMD EPYC qui utilisent l'hyperviseur KVM. Si elle est activée sur une machine virtuelle (VM), SEV crypte la mémoire de la VM pour la protéger contre l'accès de l'hôte. La sécurité de la VM s'en trouve renforcée.

En outre, la version améliorée Encrypted State de SEV (SEV-ES) est également fournie en tant qu'aperçu technologique. SEV-ES crypte tous les contenus des registres de l'unité centrale lorsqu'une machine virtuelle cesse de fonctionner. Cela empêche l'hôte de modifier les registres de l'unité centrale de la machine virtuelle ou de lire les informations qu'ils contiennent.

Notez que SEV et SEV-ES ne fonctionnent que sur la deuxième génération de processeurs AMD EPYC (nom de code Rome) ou plus récents. Notez également que RHEL 9 inclut le chiffrement SEV et SEV-ES, mais pas l'attestation de sécurité SEV et SEV-ES.

(JIRA:RHELPLAN-65217)

La virtualisation est désormais disponible sur ARM 64

En tant qu'aperçu technologique, il est désormais possible de créer des machines virtuelles KVM sur des systèmes utilisant des processeurs ARM 64.

(JIRA:RHELPLAN-103993)

virtio-mem est désormais disponible sur AMD64 et Intel 64

En tant qu'aperçu technologique, RHEL 9 introduit la fonctionnalité **virtio-mem** sur les systèmes AMD64 et Intel 64. L'utilisation de **virtio-mem** permet d'ajouter ou de supprimer dynamiquement de la mémoire hôte dans les machines virtuelles (VM).

Pour utiliser **virtio-mem**, définissez les périphériques de mémoire **virtio-mem** dans la configuration XML d'une VM et utilisez la commande **virsh update-memory-device** pour demander des modifications de la taille des périphériques de mémoire lorsque la VM est en cours d'exécution. Pour connaître la taille

actuelle de la mémoire exposée par ces dispositifs de mémoire à une VM en cours d'exécution, consultez la configuration XML de la VM.

(BZ#2014487)

CHAPITRE 7. FONCTIONNALITÉ OBSOLÈTE

Cette partie fournit une vue d'ensemble des fonctionnalités qui ont été *deprecated* dans Red Hat Enterprise Linux 9.

Les fonctionnalités obsolètes ne seront probablement plus prises en charge dans les prochaines versions majeures de ce produit et ne sont pas recommandées pour les nouveaux déploiements. Pour obtenir la liste la plus récente des fonctionnalités obsolètes dans une version majeure particulière, consultez la dernière version de la documentation.

Le statut de prise en charge des fonctionnalités dépréciées reste inchangé dans Red Hat Enterprise Linux 9. Pour plus d'informations sur la durée de la prise en charge, voir Red Hat Enterprise Linux Life Cycle et Red Hat Enterprise Linux Application Streams Life Cycle .

Les composants matériels obsolètes ne sont pas recommandés pour les nouveaux déploiements sur les versions majeures actuelles ou futures. Les mises à jour des pilotes de matériel sont limitées aux correctifs de sécurité et aux correctifs critiques. Red Hat recommande de remplacer ce matériel dès que possible.

Un paquet peut être déprécié et son utilisation déconseillée. Dans certaines circonstances, un paquetage peut être retiré d'un produit. La documentation du produit identifie alors les paquets plus récents qui offrent des fonctionnalités similaires, identiques ou plus avancées que celles du paquet supprimé, et fournit d'autres recommandations.

Pour plus d'informations sur les fonctionnalités présentes dans RHEL 8, mais qui ont été *removed* dans RHEL 9, voir les considérations relatives à l'adoption de RHEL 9 .

7.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

Commandes Kickstart obsolètes

Les commandes Kickstart suivantes sont obsolètes :

- **timezone --ntpservers**
- **timezone --nontp**
- **logging --level**
- **%packages --excludeWeakdeps**
- **%packages --instLangs**
- **aconda**
- **pwpolicy**

Notez que lorsque seules des options spécifiques sont listées, la commande de base et ses autres options sont toujours disponibles et ne sont pas dépréciées. L'utilisation des commandes obsolètes dans les fichiers Kickstart entraîne l'affichage d'un avertissement dans les journaux. Vous pouvez transformer les avertissements des commandes obsolètes en erreurs avec l'option **inst.ksstrict** boot.

(BZ#1899167)

7.2. SÉCURITÉ

SHA-1 est déprécié à des fins cryptographiques

L'utilisation du condensé de message SHA-1 à des fins cryptographiques a été supprimée dans RHEL 9. Le condensé produit par SHA-1 n'est pas considéré comme sûr en raison des nombreuses attaques réussies documentées basées sur la recherche de collisions de hachage. Les composants cryptographiques de base de RHEL ne créent plus de signatures à l'aide de SHA-1 par défaut. Les applications de RHEL 9 ont été mises à jour pour éviter d'utiliser SHA-1 dans les cas d'utilisation liés à la sécurité.

Parmi les exceptions, le code d'authentification des messages HMAC-SHA1 et les valeurs UUID (Universal Unique Identifier) peuvent encore être créés à l'aide de SHA-1, car ces cas d'utilisation ne présentent actuellement aucun risque pour la sécurité. SHA-1 peut également être utilisé dans des cas limités liés à d'importants problèmes d'interopérabilité et de compatibilité, tels que Kerberos et WPA-2. Pour plus de détails, consultez la section Liste des applications RHEL utilisant une cryptographie non conforme à la norme FIPS 140-3 dans le document de renforcement de la sécurité de RHEL 9 .

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**. Notez que **LEGACY** active également de nombreux autres algorithmes qui ne sont pas sécurisés.

(JIRA:RHELPLAN-110763)

SCP est obsolète dans RHEL 9

Le protocole de copie sécurisée (SCP) est obsolète car il présente des failles de sécurité connues. L'API SCP reste disponible pour le cycle de vie de RHEL 9, mais son utilisation réduit la sécurité du système.

- Dans l'utilitaire **scp**, SCP est remplacé par défaut par le protocole de transfert de fichiers SSH (SFTP).
- La suite OpenSSH n'utilise pas SCP dans RHEL 9.
- SCP est obsolète dans la bibliothèque **libssh**.

(JIRA:RHELPLAN-99136)

Digest-MD5 dans SASL est obsolète

Le mécanisme d'authentification Digest-MD5 du cadre Simple Authentication Security Layer (SASL) est obsolète et pourrait être supprimé des paquets **cyrus-sasl** dans une prochaine version majeure.

(BZ#1995600)

OpenSSL supprime MD2, MD4, MDC2, Whirlpool, RIPEMD160, Blowfish, CAST, DES, IDEA, RC2, RC4, RC5, SEED et PBKDF1

Le projet OpenSSL a déprécié un ensemble d'algorithmes cryptographiques parce qu'ils ne sont pas sûrs, qu'ils sont peu utilisés, ou les deux. Red Hat déconseille également l'utilisation de ces algorithmes, et RHEL 9 les fournit pour migrer les données chiffrées afin d'utiliser de nouveaux algorithmes. Les utilisateurs ne doivent pas dépendre de ces algorithmes pour la sécurité de leurs systèmes.

Les implémentations des algorithmes suivants ont été déplacées vers l'ancien fournisseur d'OpenSSL : MD2, MD4, MDC2, Whirlpool, RIPEMD160, Blowfish, CAST, DES, IDEA, RC2, RC4, RC5, SEED et PBKDF1.

Consultez le fichier de configuration **/etc/pki/tls/openssl.cnf** pour savoir comment charger l'ancien fournisseur et activer la prise en charge des algorithmes obsolètes.

(BZ#1975836)

/etc/system-fips est désormais obsolète

La prise en charge de l'indication du mode FIPS par le fichier **/etc/system-fips** a été supprimée et le fichier ne sera pas inclus dans les versions futures de RHEL. Pour installer RHEL en mode FIPS, ajoutez le paramètre **fips=1** à la ligne de commande du noyau lors de l'installation du système. Vous pouvez vérifier si RHEL fonctionne en mode FIPS à l'aide de la commande **fips-mode-setup --check**.

(JIRA:RHELPLAN-103232)

libcrypt.so.1 est désormais obsolète

La bibliothèque **libcrypt.so.1** est désormais obsolète et pourrait être supprimée dans une prochaine version de RHEL.

(BZ#2034569)

fapolicyd.rules est obsolète

Le répertoire **/etc/fapolicyd/rules.d/**, qui contient les fichiers contenant les règles d'exécution d'autorisation et de refus, remplace le fichier **/etc/fapolicyd/fapolicyd.rules**. Le script **fagenrules** fusionne désormais tous les fichiers de règles de ce répertoire dans le fichier **/etc/fapolicyd/compiled.rules**. Les règles contenues dans **/etc/fapolicyd/fapolicyd.trust** sont toujours traitées par le cadre **fapolicyd**, mais uniquement dans un souci de compatibilité ascendante.

(BZ#2054740)

7.3. MISE EN RÉSEAU

ipset et iptables-nft sont obsolètes

Les paquets **ipset** et **iptables-nft** sont obsolètes dans RHEL. Le paquet **iptables-nft** contient différents outils tels que **iptables**, **ip6tables**, **ebtables** et **arptables**. Ces outils ne recevront plus de nouvelles fonctionnalités et leur utilisation pour les nouveaux déploiements n'est pas recommandée. En remplacement, préférez l'outil en ligne de commande **nft** fourni par le paquet **nftables**. Les installations existantes devraient migrer vers **nft** si possible.

Lorsque vous chargez le module **iptables**, **ip6tables**, **ebtables**, **arptables**, **nft_compat**, ou **ipset**, le module enregistre l'avertissement suivant dans le fichier **/var/log/messages**:

> Avertissement : <module_name> - ce pilote n'est pas recommandé pour les nouveaux déploiements. Il continue d'être pris en charge dans cette version de RHEL, mais il est probable qu'il soit supprimé dans la prochaine version majeure. Les mises à jour et les corrections de pilotes seront limitées aux problèmes critiques. Veuillez contacter l'assistance Red Hat pour de plus amples informations.

Pour plus d'informations sur la migration vers nftables, voir Migrating from iptables to nftables , ainsi que les pages de manuel **iptables-translate(8)** et **ip6tables-translate(8)**.

(BZ#1945151)

Les équipes réseau sont obsolètes dans RHEL 9

Le service **teamd** et la bibliothèque **libteam** sont obsolètes dans Red Hat Enterprise Linux 9 et seront supprimés dans la prochaine version majeure. En remplacement, configurez un lien au lieu d'une équipe réseau.

Red Hat concentre ses efforts sur le bonding basé sur le noyau afin d'éviter de maintenir deux fonctionnalités, les bonds et les teams, qui ont des fonctions similaires. Le code de bonding a été adopté par un grand nombre de clients, est robuste et est développé par une communauté active. Par conséquent, le code de bonding reçoit des améliorations et des mises à jour.

Pour plus d'informations sur la migration d'une équipe vers un lien, voir Migration d'une configuration d'équipe réseau vers un lien réseau.

(BZ#1935544)

NetworkManager stocke les nouvelles configurations de réseau sur /etc/NetworkManager/system-connections/ dans un fichier clé

Auparavant, NetworkManager stockait les nouvelles configurations réseau à l'adresse **/etc/sysconfig/network-scripts/** au format **ifcfg**. À partir de RHEL 9.0, RHEL stocke les nouvelles configurations réseau à l'adresse **/etc/NetworkManager/system-connections/** dans un format de fichier clé. Les connexions pour lesquelles les configurations sont stockées sur **/etc/sysconfig/network-scripts/** dans l'ancien format continuent de fonctionner sans interruption. Les modifications apportées aux profils existants continuent de mettre à jour les anciens fichiers.

(BZ#1894877)

Le back-end iptables dans firewalld est obsolète

Dans RHEL 9, le cadre **iptables** est obsolète. Par conséquent, le backend **iptables** et le **direct interface** dans **firewalld** sont également obsolètes. Au lieu de **direct interface**, vous pouvez utiliser les fonctionnalités natives de **firewalld** pour configurer les règles requises.

(BZ#2089200)

7.4. NOYAU

L'encapsulation ATM est obsolète dans RHEL 9

L'encapsulation du mode de transfert asynchrone (ATM) permet une connectivité de couche 2 (protocole point à point, Ethernet) ou de couche 3 (IP) pour la couche d'adaptation ATM 5 (AAL-5). Red Hat ne fournit plus de support pour les pilotes ATM NIC depuis RHEL 7. La prise en charge de l'implémentation ATM est abandonnée dans RHEL 9. Ces protocoles ne sont actuellement utilisés que dans les chipsets, qui prennent en charge la technologie ADSL et sont progressivement abandonnés par les fabricants. Par conséquent, l'encapsulation ATM est dépréciée dans Red Hat Enterprise Linux 9.

Pour plus d'informations, voir PPP Over AAL5, Multiprotocol Encapsulation over ATM Adaptation Layer 5, et Classical IP and ARP over ATM .

(BZ#2058153)

v4l/dvb les appareils de télévision et de capture vidéo ne sont plus pris en charge

Avec RHEL 9, Red Hat ne prend plus en charge les périphériques **Video4Linux** (**v4l**) et **Linux DVB** (**DVB**) qui consistent en diverses cartes de tuner de télévision et diverses cartes de capture vidéo et Red Hat ne fournit plus leurs pilotes associés.

(BZ#2074598)

7.5. SYSTÈMES DE FICHIERS ET STOCKAGE

lvm2-activation-generator et ses services générés sont supprimés dans RHEL 9.0

Le programme **lvm2-activation-generator** et ses services générés **lvm2-activation**, **lvm2-activation-early**, et **lvm2-activation-net** sont supprimés dans RHEL 9.0. Le paramètre **lvm.conf event_activation**, utilisé pour activer les services, n'est plus fonctionnel. La seule méthode d'activation automatique des groupes de volumes est l'activation basée sur les événements.

(BZ#2038183)

7.6. LANGAGES DE PROGRAMMATION DYNAMIQUES, SERVEURS WEB ET DE BASE DE DONNÉES

libdb a été supprimé

RHEL 8 et RHEL 9 fournissent actuellement la version 5.3.28 de Berkeley DB (**libdb**), qui est distribuée sous la licence LGPLv2. La version 6 de Berkeley DB en amont est disponible sous la licence AGPLv3, qui est plus restrictive.

Le paquet **libdb** est obsolète depuis RHEL 9 et pourrait ne plus être disponible dans les prochaines versions majeures de RHEL.

En outre, les algorithmes cryptographiques ont été retirés de **libdb** dans RHEL 9 et plusieurs dépendances de **libdb** ont été supprimées de RHEL 9.

Il est conseillé aux utilisateurs de **libdb** de migrer vers une autre base de données clé-valeur. Pour plus d'informations, voir l'article de la base de connaissances Remplacements disponibles pour Berkeley DB (libdb) dans RHEL.

(BZ#1927780, BZ#1974657, JIRA:RHELPLAN-80695)

7.7. GESTION DE L'IDENTITÉ

SHA-1 dans OpenDNSSec est maintenant obsolète

OpenDNSSec prend en charge l'exportation de signatures numériques et d'enregistrements d'authentification à l'aide de l'algorithme **SHA-1**. L'utilisation de l'algorithme **SHA-1** n'est plus prise en charge. Avec la version RHEL 9, **SHA-1** dans OpenDNSSec est déprécié et pourrait être supprimé dans une future version mineure. En outre, la prise en charge d'OpenDNSSec est limitée à son intégration avec Red Hat Identity Management. OpenDNSSec n'est pas pris en charge de manière autonome.

(BZ#1979521)

Le domaine du fournisseur de fichiers implicites SSSD est désactivé par défaut

Le domaine fournisseur implicite SSSD **files**, qui récupère les informations sur les utilisateurs à partir de fichiers locaux tels que **/etc/shadow** et les informations sur les groupes à partir de **/etc/groups**, est désormais désactivé par défaut.

Pour récupérer des informations sur les utilisateurs et les groupes à partir de fichiers locaux avec SSSD :

1. Configurer SSSD. Choisissez l'une des options suivantes :

a. Configurez explicitement un domaine local avec l'option **id_provider=files** dans le fichier de configuration **sssd.conf**.

```
[domain/local]
id_provider=files
...
```

b. Activez le fournisseur **files** en définissant **enable_files_domain=true** dans le fichier de configuration **sssd.conf**.

```
[sssd]
enable_files_domain = true
```

2. Configurer le commutateur des services de noms.

```
# authselect enable-feature with-files-provider
```

(JIRA:RHELPLAN-100639)

7.8. INFRASTRUCTURES GRAPHIQUES

Le serveur X.org est désormais obsolète

Le serveur d'affichage **X.org** est obsolète et sera supprimé dans une prochaine version majeure de RHEL. La session de bureau par défaut est désormais la session **Wayland** dans la plupart des cas.

Le protocole **X11** reste entièrement supporté par le back-end **XWayland**. Par conséquent, les applications qui nécessitent **X11** peuvent fonctionner dans la session **Wayland**.

Red Hat travaille à la résolution des problèmes et des lacunes restants dans la session **Wayland**. Pour les problèmes en suspens dans **Wayland**, voir la section Problèmes connus.

Vous pouvez basculer votre session utilisateur vers le back-end **X.org**. Pour plus d'informations, voir Sélection de l'environnement GNOME et du protocole d'affichage .

(JIRA:RHELPLAN-121048)

Motif a été supprimé

La boîte à outils Motif a été supprimée dans RHEL, car le développement de la communauté Motif en amont est inactif.

Les paquets Motif suivants ont été supprimés, y compris leurs variantes de développement et de débogage :

- **motif**
- **openmotif**
- **openmotif21**
- **openmotif22**

En outre, le paquet **motif-static** a été supprimé.

Red Hat recommande d'utiliser la boîte à outils GTK en remplacement. GTK est plus facile à entretenir et offre de nouvelles fonctionnalités par rapport à Motif.

(JIRA:RHELPLAN-98983)

7.9. RÔLES DU SYSTÈME RED HAT ENTERPRISE LINUX

Le rôle de système **networking** affiche un avertissement de dépréciation lors de la configuration des équipes sur les nœuds RHEL 9

Par conséquent, l'utilisation du rôle de système **networking** RHEL sur un contrôleur RHEL 8 pour configurer une équipe réseau sur des nœuds RHEL 9 affiche un avertissement concernant son obsolescence.

(BZ#1999770)

7.10. VIRTUALISATION

La vérification de l'image SecureBoot à l'aide de signatures basées sur SHA1 est obsolète

La vérification de l'image SecureBoot à l'aide de signatures basées sur l'algorithme SHA1 sur les exécutables UEFI (PE/COFF) est devenue obsolète. Red Hat recommande plutôt d'utiliser des signatures basées sur l'algorithme SHA2 ou plus récent.

(BZ#1935497)

Prise en charge limitée des instantanés de machines virtuelles

La création d'instantanés de machines virtuelles (VM) n'est actuellement prise en charge que pour les VM n'utilisant pas le micrologiciel UEFI. En outre, pendant l'opération de snapshot, le moniteur QEMU peut se bloquer, ce qui a un impact négatif sur les performances de l'hyperviseur pour certaines charges de travail.

Notez également que le mécanisme actuel de création d'instantanés de VM est obsolète et que Red Hat ne recommande pas l'utilisation d'instantanés de VM dans un environnement de production. Cependant, un nouveau mécanisme d'instantané de VM est en cours de développement et devrait être entièrement mis en œuvre dans une prochaine version mineure de RHEL 9.

(JIRA:RHELPLAN-15509, BZ#1621944)

virt-manager a été supprimé

L'application Virtual Machine Manager, également connue sous le nom de **virt-manager**, a été supprimée. La console web RHEL, également connue sous le nom de **Cockpit**, est destinée à la remplacer dans une version ultérieure. Il est donc recommandé d'utiliser la console web pour gérer la virtualisation dans une interface graphique. Notez toutefois que certaines fonctionnalités disponibles sur **virt-manager** peuvent ne pas être encore disponibles dans la console web RHEL.

(JIRA:RHELPLAN-10304)

libvirtd est devenu obsolète

Le démon monolithique **libvirt**, **libvirtd**, a été abandonné dans RHEL 9 et sera supprimé dans une prochaine version majeure de RHEL. Notez que vous pouvez toujours utiliser **libvirtd** pour gérer la virtualisation sur votre hyperviseur, mais Red Hat recommande de passer aux démons modulaires **libvirt** récemment introduits. Pour obtenir des instructions et des détails, consultez le document RHEL 9 Configuring and Managing Virtualization (Configuration et gestion de la virtualisation).

(JIRA:RHELPLAN-113995)

Le pilote de disquette virtuelle est devenu obsolète

Le pilote **isa-fdc**, qui contrôle les périphériques de disquette virtuels, est désormais obsolète et ne sera plus pris en charge dans une prochaine version de RHEL. Par conséquent, pour assurer la compatibilité avec les machines virtuelles (VM) migrées, Red Hat déconseille l'utilisation de périphériques à disquette dans les VM hébergées sur RHEL 9.

(BZ#1965079)

le format d'image qcow2-v2 est obsolète

Avec RHEL 9, le format qcow2-v2 pour les images de disques virtuels est devenu obsolète et ne sera plus pris en charge dans une prochaine version majeure de RHEL. En outre, RHEL 9 Image Builder ne peut pas créer d'images de disque au format qcow2-v2.

Au lieu de qcow2-v2, Red Hat recommande fortement d'utiliser qcow2-v3. Pour convertir une image qcow2-v2 en une version de format plus récente, utilisez la commande **qemu-img amend**.

(BZ#1951814)

7.11. CONTENEURS

L'exécution de conteneurs RHEL 9 sur un hôte RHEL 7 n'est pas prise en charge

L'exécution de conteneurs RHEL 9 sur un hôte RHEL 7 n'est pas prise en charge. Cela peut fonctionner, mais ce n'est pas garanti.

Pour plus d'informations, voir la Matrice de compatibilité des conteneurs Red Hat Enterprise Linux .

(JIRA:RHELPLAN-100087)

L'algorithme de hachage SHA1 utilisé dans Podman est obsolète

L'algorithme SHA1 utilisé pour générer le nom de fichier de l'espace de noms du réseau sans racine n'est plus pris en charge dans Podman. Par conséquent, les conteneurs sans racine démarrés avant la mise à jour vers Podman 4.1.1 à partir de l'avis RHBA-2022:5951 doivent être redémarrés s'ils sont connectés à un réseau (et pas seulement en utilisant **slirp4netns**) pour s'assurer qu'ils peuvent se connecter aux conteneurs démarrés après la mise à jour.

(BZ#2069279)

rhel9/pause a été supprimé

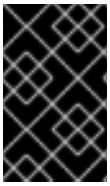
L'image du conteneur **rhel9/pause** a été supprimée.

(BZ#2106816)

7.12. PAQUETS OBSOLÈTES

Cette section répertorie les paquetages qui ont été dépréciés et qui ne seront probablement pas inclus dans une prochaine version majeure de Red Hat Enterprise Linux.

Pour les modifications apportées aux paquets entre RHEL 8 et RHEL 9, voir Changements apportés aux paquets dans le document *Considerations in adopting RHEL 9* .



IMPORTANT

Le statut de support des paquetages dépréciés reste inchangé dans RHEL 9. Pour plus d'informations sur la durée du support, voir Red Hat Enterprise Linux Life Cycle et Red Hat Enterprise Linux Application Streams Life Cycle.

Les paquets suivants sont obsolètes dans RHEL 9 :

- iptables-devel
- iptables-libs
- iptables-nft
- iptables-nft-services
- iptables-utils
- libdb
- mcpp
- python3-pytz

CHAPITRE 8. PROBLÈMES CONNUS

Cette partie décrit les problèmes connus dans Red Hat Enterprise Linux 9.0.

8.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

Les commandes reboot --kexec et inst.kexec ne fournissent pas un état prévisible du système

L'installation de RHEL à l'aide de la commande **reboot --kexec** Kickstart ou des paramètres de démarrage du noyau **inst.kexec** n'offre pas le même état prévisible du système qu'un redémarrage complet. Par conséquent, le passage au système installé sans redémarrage peut produire des résultats imprévisibles.

Notez que la fonctionnalité **kexec** est obsolète et sera supprimée dans une prochaine version de Red Hat Enterprise Linux.

(BZ#1697896)

Local Media la source d'installation n'est pas détectée lors du démarrage de l'installation à partir d'une clé USB créée à l'aide d'un outil tiers

Lors du démarrage de l'installation RHEL à partir d'une clé USB créée à l'aide d'un outil tiers, le programme d'installation ne détecte pas la source d'installation **Local Media** (seule *Red Hat CDN* est détectée).

Ce problème survient parce que l'option de démarrage par défaut **int.stage2=** tente de rechercher le format d'image **iso9660**. Cependant, un outil tiers peut créer une image ISO avec un format différent.

En guise de solution de contournement, utilisez l'une ou l'autre des solutions suivantes :

- Lors du démarrage de l'installation, cliquez sur la touche **Tab** pour modifier la ligne de commande du noyau et remplacez l'option de démarrage **inst.stage2=** par **inst.repo=**.
- Pour créer un périphérique USB amorçable sous Windows, utilisez Fedora Media Writer.
- Si vous utilisez un outil tiers tel que Rufus pour créer un périphérique USB amorçable, régénérez d'abord l'image ISO RHEL sur un système Linux, puis utilisez l'outil tiers pour créer un périphérique USB amorçable.

Pour plus d'informations sur les étapes à suivre pour exécuter l'une des solutions de contournement spécifiées, voir, Le support d'installation n'est pas détecté automatiquement lors de l'installation de RHEL 8.3.

(BZ#1877697)

Les commandes auth et authconfig Kickstart nécessitent le dépôt AppStream

Le paquetage **authselect-compat** est requis par les commandes Kickstart **auth** et **authconfig** lors de l'installation. Sans ce paquet, l'installation échoue si **auth** ou **authconfig** est utilisé. Cependant, par conception, le paquet **authselect-compat** n'est disponible que dans le dépôt AppStream.

Pour contourner ce problème, vérifiez que les dépôts BaseOS et AppStream sont disponibles pour le programme d'installation ou utilisez la commande **authselect** Kickstart pendant l'installation.

(BZ#1640697)

Politiques SELinux inattendues sur les systèmes où Anaconda s'exécute en tant qu'application

Lorsqu'Anaconda est exécuté en tant qu'application sur un système déjà installé (par exemple pour effectuer une autre installation sur un fichier image à l'aide de l'option **–image** anaconda), il n'est pas interdit au système de modifier les types et attributs SELinux au cours de l'installation. Par conséquent, certains éléments de la politique SELinux peuvent changer sur le système où Anaconda est exécuté. Pour contourner ce problème, n'exécutez pas Anaconda sur le système de production et exécutez-le dans une machine virtuelle temporaire. Ainsi, la politique SELinux sur un système de production n'est pas modifiée. L'exécution d'Anaconda dans le cadre du processus d'installation du système, tel que l'installation à partir de **boot.iso** ou **dvd.iso**, n'est pas concernée par ce problème.

(BZ#2050140)

Le lecteur de CD-ROM USB n'est pas disponible comme source d'installation dans Anaconda

L'installation échoue lorsque le lecteur de CD-ROM USB en est la source et que la commande Kickstart **ignoredisk --only-use=** est spécifiée. Dans ce cas, Anaconda ne peut pas trouver et utiliser ce disque source.

Pour contourner ce problème, utilisez la commande **harddrive --partition=sdX --dir=**/ pour effectuer l'installation à partir d'un lecteur de CD-ROM USB. L'installation n'échoue alors pas.

(BZ#1914955)

L'installation minimale de RHEL ne comprend plus le paquetage s390utils-base

Dans RHEL 8.4 et les versions ultérieures, le paquet **s390utils-base** est divisé en un paquet **s390utils-core** et un paquet auxiliaire **s390utils-base**. Par conséquent, le fait de définir l'installation RHEL sur **minimal-environment** n'installe que le paquet **s390utils-core** nécessaire et non le paquet auxiliaire **s390utils-base**. Pour contourner ce problème, installez manuellement le paquet **s390utils-base** après avoir terminé l'installation RHEL ou installez explicitement **s390utils-base** à l'aide d'un fichier kickstart.

(BZ#1932480)

Échec des installations de disques durs partitionnés avec le système de fichiers iso9660

Vous ne pouvez pas installer RHEL sur des systèmes dont le disque dur est partitionné avec le système de fichiers **iso9660**. Cela est dû à la mise à jour du code d'installation qui est configuré pour ignorer tout disque dur contenant une partition du système de fichiers **iso9660**. Cela se produit même lorsque RHEL est installé sans utiliser de DVD.

Pour contourner ce problème, ajoutez le script suivant dans le fichier kickstart pour formater le disque avant le début de l'installation.

Remarque : avant d'exécuter la solution de contournement, sauvegardez les données disponibles sur le disque. La commande **wipefs** formate toutes les données existantes sur le disque.

```
%pre
wipefs -a /dev/sda
%end
```

Par conséquent, les installations fonctionnent comme prévu, sans aucune erreur.

(BZ#1929105)

Anaconda ne parvient pas à vérifier l'existence d'un compte d'utilisateur administrateur

Lors de l'installation de RHEL à l'aide d'une interface graphique, Anaconda ne vérifie pas si le compte administrateur a été créé. En conséquence, les utilisateurs peuvent installer un système sans aucun compte d'utilisateur administrateur.

Pour contourner ce problème, veillez à configurer un compte d'utilisateur administrateur ou à définir le mot de passe root et à déverrouiller le compte root. Ainsi, les utilisateurs peuvent effectuer des tâches administratives sur le système installé.

(BZ#2047713)

Anaconda ne parvient pas à se connecter au serveur iSCSI à l'aide de la méthode **no authentication** après une tentative d'authentification CHAP infructueuse

Lorsque vous ajoutez des disques iSCSI à l'aide de l'authentification CHAP et que la tentative de connexion échoue en raison d'informations d'identification incorrectes, une nouvelle tentative de connexion aux disques à l'aide de la méthode **no authentication** échoue. Pour contourner ce problème, fermez la session en cours et connectez-vous à l'aide de la méthode **no authentication**.

(BZ#1983602)

De nouvelles fonctionnalités XFS empêchent le démarrage des systèmes PowerNV IBM POWER dont le microprogramme est antérieur à la version 5.10

Les systèmes PowerNV IBM POWER utilisent un noyau Linux pour le micrologiciel et Petitboot en remplacement de GRUB. Ainsi, le noyau du microprogramme monte **/boot** et Petitboot lit la configuration de GRUB et démarre RHEL.

Le noyau RHEL 9 introduit les fonctionnalités **bigtime=1** et **inobtcount=1** dans le système de fichiers XFS, que les noyaux dotés d'un microprogramme antérieur à la version 5.10 ne comprennent pas.

Pour contourner ce problème, vous pouvez utiliser un autre système de fichiers pour **/boot**, par exemple ext4.

(BZ#1997832)

Impossible d'installer RHEL lorsque la taille du PReP n'est pas de 4 ou 8 MiB

Le programme d'installation RHEL ne peut pas installer le chargeur de démarrage si la partition PowerPC Reference Platform (PReP) est d'une taille différente de 4 MiB ou 8 MiB sur un disque qui utilise des secteurs de 4 kiB. Par conséquent, vous ne pouvez pas installer RHEL sur le disque.

Pour contourner le problème, assurez-vous que la taille de la partition PReP est exactement de 4 ou 8 Mo et qu'elle n'est pas arrondie à une autre valeur. En conséquence, le programme d'installation peut maintenant installer RHEL sur le disque.

(BZ#2026579)

De nouvelles fonctionnalités XFS empêchent le démarrage des systèmes PowerNV IBM POWER dont le noyau du micrologiciel est antérieur à la version 5.10

Les systèmes PowerNV IBM POWER utilisent un noyau Linux pour le micrologiciel et Petitboot en remplacement de GRUB. Ainsi, le noyau du microprogramme monte **/boot** et Petitboot lit la configuration de GRUB et démarre RHEL.

Le noyau RHEL 9 introduit les fonctionnalités **bigtime=1** et **inobtcount=1** dans le système de fichiers XFS, que les microprogrammes dotés d'un noyau antérieur à la version 5.10 ne comprennent pas. En conséquence, Anaconda empêche l'installation en affichant le message d'erreur suivant :

Votre micrologiciel ne prend pas en charge les fonctions du système de fichiers XFS sur le système de fichiers **/boot**. Le système ne sera pas amorçable. Veuillez mettre à jour le micrologiciel ou changer le type de système de fichiers.

Pour contourner le problème, utilisez un autre système de fichiers pour **/boot**, par exemple **ext4**.

(BZ#2008792)

8.2. GESTION DES ABONNEMENTS

virt-who ne peut pas se connecter aux serveurs ESX en mode FIPS

Lors de l'utilisation de l'utilitaire **virt-who** sur un système RHEL 9 en mode FIPS, **virt-who** ne peut pas se connecter aux serveurs ESX. Par conséquent, **virt-who** ne signale aucun serveur ESX, même s'il est configuré pour cela, et affiche le message d'erreur suivant :

```
ValueError: [digital envelope routines] unsupported
```

Pour contourner ce problème, procédez de l'une des manières suivantes :

- Ne configurez pas le système RHEL 9 que vous utilisez pour exécuter **virt-who** en mode FIPS.
- Ne mettez pas à niveau le système RHEL que vous utilisez pour exécuter **virt-who** vers la version 9.0.

(BZ#2054504)

8.3. GESTION DES LOGICIELS

Le processus d'installation ne répond parfois plus

Lorsque vous installez RHEL, le processus d'installation ne répond parfois plus. Le fichier **/tmp/packaging.log** affiche le message suivant à la fin :

```
10:20:56,416 DDEBUG dnf: RPM transaction over.
```

Pour contourner ce problème, redémarrez le processus d'installation.

(BZ#2073510)

8.4. SHELLS ET OUTILS DE LIGNE DE COMMANDE

Le renommage des interfaces réseau à l'aide des fichiers ifcfg échoue

Sur RHEL 9, le paquetage **initscripts** n'est pas installé par défaut. Par conséquent, le renommage des interfaces réseau à l'aide des fichiers **ifcfg** échoue. Pour résoudre ce problème, Red Hat vous recommande d'utiliser les règles **udev** ou les fichiers de liens pour renommer les interfaces. Pour plus de détails, reportez-vous à Nommage cohérent des périphériques d'interface réseau et à la page de manuel **systemd.link(5)**.

Si vous ne pouvez pas utiliser l'une des solutions recommandées, installez le paquetage **initscripts**.

(BZ#2018112)

Le paquet chkconfig n'est pas installé par défaut dans RHEL 9

Le paquet **chkconfig**, qui met à jour et interroge les informations de niveau d'exécution des services système, n'est pas installé par défaut dans RHEL 9.

Pour gérer les services, utilisez les commandes **systemctl** ou installez manuellement le paquet **chkconfig**.

Pour plus d'informations sur **systemd**, voir Introduction à systemd. Pour savoir comment utiliser l'utilitaire **systemctl**, voir Gérer les services système avec systemctl.

(BZ#2053598)

8.5. SERVICES D'INFRASTRUCTURE

Les deux sites bind et unbound désactivent la validation des signatures basées sur SHA-1

Les composants **bind** et **unbound** désactivent la prise en charge de la validation de toutes les signatures RSA/SHA1 (algorithme numéro 5) et RSASHA1-NSEC3-SHA1 (algorithme numéro 7), et l'utilisation de SHA-1 pour les signatures est restreinte dans la politique cryptographique DEFAULT applicable à l'ensemble du système.

Par conséquent, certains enregistrements DNSSEC signés avec les algorithmes SHA-1, RSA/SHA1 et RSASHA1-NSEC3-SHA1 ne sont pas vérifiés dans Red Hat Enterprise Linux 9 et les noms de domaine concernés deviennent vulnérables.

Pour contourner ce problème, passez à un algorithme de signature différent, tel que RSA/SHA-256 ou des clés à courbe elliptique.

Pour plus d'informations et une liste des domaines de premier niveau concernés et vulnérables, voir la solution " DNSSEC records signed with RSASHA1 fail to verify" (enregistrements DNSSEC signés avec RSASHA1 sans vérification).

(BZ#2070495)

named ne démarre pas si le même fichier de zone inscriptible est utilisé dans plusieurs zones

BIND n'autorise pas l'utilisation du même fichier de zone inscriptible dans plusieurs zones. Par conséquent, si une configuration comprend plusieurs zones qui partagent un chemin d'accès à un fichier qui peut être modifié par le service **named**, **named** ne démarre pas. Pour contourner ce problème, utilisez la clause **in-view** pour partager une zone entre plusieurs vues et veillez à utiliser des chemins différents pour les différentes zones. Par exemple, incluez les noms des vues dans le chemin d'accès.

Notez que les fichiers de zone inscriptibles sont généralement utilisés dans les zones où les mises à jour dynamiques sont autorisées, dans les zones esclaves ou dans les zones gérées par DNSSEC.

(BZ#1984982)

8.6. SÉCURITÉ

OpenSSL ne détecte pas si un jeton PKCS #11 prend en charge la création de signatures RSA ou RSA-PSS brutes

Le protocole TLS 1.3 nécessite la prise en charge des signatures RSA-PSS. Si un jeton PKCS #11 ne prend pas en charge les signatures RSA ou RSA-PSS brutes, les applications serveur qui utilisent la bibliothèque **OpenSSL** ne fonctionnent pas avec une clé **RSA** si la clé est détenue par le jeton **PKCS #11**. Par conséquent, la communication TLS échoue dans le scénario décrit.

Pour contourner ce problème, configurez les serveurs et les clients de manière à ce qu'ils utilisent la version 1.2 du protocole TLS, qui est la version la plus élevée disponible.

(BZ#1681178)

OpenSSL traite incorrectement les jetons PKCS #11 qui ne prennent pas en charge les signatures RSA ou RSA-PSS brutes

La bibliothèque **OpenSSL** ne détecte pas les capacités liées aux clés des jetons PKCS #11. Par conséquent, l'établissement d'une connexion TLS échoue lorsqu'une signature est créée avec un jeton qui ne prend pas en charge les signatures RSA ou RSA-PSS brutes.

Pour contourner le problème, ajoutez les lignes suivantes après la ligne **.include** à la fin de la section **crypto_policy** dans le fichier **/etc/pki/tls/openssl.cnf**:

```
SignatureAlgorithms =
RSA+SHA256:RSA+SHA512:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA512:ECDSA+SHA384
MaxProtocol = TLSv1.2
```

Par conséquent, une connexion TLS peut être établie dans le scénario décrit.

(BZ#1685470)

La cryptographie non approuvée par la FIPS fonctionne dans OpenSSL en mode FIPS

La cryptographie qui n'est pas approuvée par le FIPS fonctionne dans la boîte à outils OpenSSL, quels que soient les paramètres du système. Par conséquent, vous pouvez utiliser des algorithmes cryptographiques qui devraient être désactivés lorsque le système fonctionne en mode FIPS, par exemple :

- Les suites de chiffrement TLS utilisant l'échange de clés RSA fonctionnent.
- Les algorithmes de cryptage et de décryptage à clé publique basés sur la technologie RSA fonctionnent malgré l'utilisation des blocs PKCS #1 et SSLv23 ou l'utilisation de clés de moins de 2048 bits.

(BZ#2053289)

OpenSSL ne peut pas utiliser de moteurs en mode FIPS

L'API Engine est obsolète dans OpenSSL 3.0 et est incompatible avec l'implémentation FIPS (Federal Information Processing Standards) d'OpenSSL et d'autres implémentations compatibles FIPS. Par conséquent, OpenSSL ne peut pas exécuter les moteurs en mode FIPS. Il n'existe pas de solution à ce problème.

(BZ#2087253)

Les suites de chiffrement PSK ne fonctionnent pas avec la politique cryptographique FUTURE

Les suites de chiffrement à clé pré-partagée (PSK) ne sont pas reconnues comme des méthodes d'échange de clés à secret parfait (PFS). Par conséquent, les ciphersuites **ECDHE-PSK** et **DHE-PSK** ne fonctionnent pas avec OpenSSL configuré à **SECLEVEL=3**, par exemple avec la politique cryptographique **FUTURE**. Comme solution de contournement, vous pouvez définir une politique cryptographique moins restrictive ou un niveau de sécurité inférieur (**SECLEVEL**) pour les applications qui utilisent des suites de chiffrement PSK.

(BZ#2060044)

GnuPG permet incorrectement d'utiliser des signatures SHA-1 même si cela est interdit par la norme crypto-policies

Le logiciel cryptographique GNU Privacy Guard (GnuPG) peut créer et vérifier des signatures qui utilisent l'algorithme SHA-1 indépendamment des paramètres définis par les politiques cryptographiques du système. Par conséquent, vous pouvez utiliser SHA-1 à des fins cryptographiques dans la politique cryptographique **DEFAULT**, ce qui n'est pas cohérent avec la dépréciation de cet algorithme peu sûr pour les signatures à l'échelle du système.

Pour contourner ce problème, n'utilisez pas les options de GnuPG qui impliquent SHA-1. Vous empêcherez ainsi GnuPG d'abaisser la sécurité du système par défaut en utilisant les signatures SHA-1 non sécurisées.

(BZ#2070722)

Certaines opérations d'OpenSSH n'utilisent pas les interfaces approuvées par le FIPS

La bibliothèque cryptographique OpenSSL, utilisée par OpenSSH, fournit deux interfaces : l'ancienne et la nouvelle. En raison des modifications apportées aux composants internes d'OpenSSL, seules les interfaces modernes utilisent des implémentations d'algorithmes cryptographiques certifiées FIPS. Comme OpenSSH utilise des interfaces anciennes pour certaines opérations, il n'est pas conforme aux exigences de la FIPS.

(BZ#2087121)

gpg-agent ne fonctionne pas comme agent SSH en mode FIPS

L'outil **gpg-agent** crée des empreintes MD5 lors de l'ajout de clés au programme **ssh-agent**, même si le mode FIPS désactive le condensé MD5. Par conséquent, l'utilitaire **ssh-add** ne parvient pas à ajouter les clés à l'agent d'authentification.

Pour contourner le problème, créez le fichier **~/.gnupg/sshcontrol** sans utiliser la commande **gpg-agent --daemon --enable-ssh-support**. Par exemple, vous pouvez coller la sortie de la commande **gpg --list-keys** au format **<FINGERPRINT> 0** dans **~/.gnupg/sshcontrol**. Ainsi, **gpg-agent** fonctionne comme agent d'authentification SSH.

(BZ#2073567)

SELinux staff_u Les utilisateurs peuvent passer à tort à l'option unconfined_r

Lorsque le booléen **secure_mode** est activé, les utilisateurs de **staff_u** peuvent passer par erreur au rôle **unconfined_r**. En conséquence, les utilisateurs de **staff_u** peuvent effectuer des opérations privilégiées affectant la sécurité du système.

(BZ#2021529)

La politique SELinux par défaut autorise les exécutables non confinés à rendre leur pile exécutable

L'état par défaut du booléen **selinuxuser_execstack** dans la politique SELinux est activé, ce qui signifie que les exécutables non confinés peuvent rendre leur pile exécutable. Les exécutables ne devraient pas utiliser cette option, qui pourrait indiquer des exécutables mal codés ou une attaque possible. Cependant, en raison de la compatibilité avec d'autres outils, paquetages et produits tiers, Red Hat ne peut pas modifier la valeur du booléen dans la stratégie par défaut. Si votre scénario ne dépend pas de ces aspects de compatibilité, vous pouvez désactiver l'option booléenne dans votre politique locale en entrant la commande **setsebool -P selinuxuser_execstack off**.

(BZ#2064274)

Les règles de délai SSH dans les profils STIG configurent des options incorrectes

Une mise à jour d'OpenSSH a affecté les règles des profils suivants du Guide de mise en œuvre technique de la sécurité de l'Agence des systèmes d'information de la défense (DISA STIG) :

- DISA STIG pour RHEL 9 (**xccdf_org.ssgproject.content_profile_stig**)
- DISA STIG avec GUI pour RHEL 9 (**xccdf_org.ssgproject.content_profile_stig_gui**)

Dans chacun de ces profils, les deux règles suivantes sont affectées :

```
Title: Set SSH Client Alive Count Max to zero
CCE Identifier: CCE-90271-8
Rule ID: xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0

Title: Set SSH Idle Timeout Interval
CCE Identifier: CCE-90811-1
Rule ID: xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout
```

Lorsqu'elles sont appliquées aux serveurs SSH, chacune de ces règles configure une option (**ClientAliveCountMax** et **ClientAliveInterval**) qui ne se comporte plus comme auparavant. En conséquence, OpenSSH ne déconnecte plus les utilisateurs SSH inactifs lorsqu'il atteint le délai configuré par ces règles. Comme solution de contournement, ces règles ont été temporairement supprimées des profils DISA STIG pour RHEL 9 et DISA STIG avec GUI pour RHEL 9 jusqu'à ce qu'une solution soit développée.

(BZ#2038978)

fagenrules --load ne fonctionne pas correctement

Le service **fapolicyd** ne gère pas correctement le signal de raccrochage (SIGHUP). Par conséquent, **fapolicyd** se termine après avoir reçu le signal SIGHUP. Par conséquent, la commande **fagenrules --load** ne fonctionne pas correctement et les mises à jour des règles nécessitent un redémarrage manuel de **fapolicyd**. Pour contourner ce problème, redémarrez le service **fapolicyd** après toute modification des règles, ce qui permettra à **fagenrules --load** de fonctionner correctement.

(BZ#2070655)

Les remédiations Ansible nécessitent des collectes supplémentaires

Avec le remplacement d'Ansible Engine par le paquetage **ansible-core**, la liste des modules Ansible fournis avec l'abonnement RHEL est réduite. Par conséquent, l'exécution de remédiations qui utilisent le contenu Ansible inclus dans le paquetage **scap-security-guide** nécessite des collections du paquetage **rhc-worker-playbook**.

Pour une remédiation Ansible, effectuez les étapes suivantes :

1. Installez les paquets nécessaires :

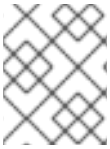
```
# dnf install -y ansible-core scap-security-guide rhc-worker-playbook
```

2. Naviguez jusqu'au répertoire **/usr/share/scap-security-guide/ansible**: # cd /usr/share/scap-security-guide/ansible
3. Exécutez le playbook Ansible approprié en utilisant les variables d'environnement qui définissent le chemin d'accès aux collections Ansible supplémentaires :

```
# ANSIBLE_COLLECTIONS_PATH=/usr/share/rhc-worker-playbook/ansible/collections/ansible_collections/ ansible-playbook -c local -i localhost, rhel9-playbook-cis_server_l1.yml
```

Remplacer ***cis_server_l1*** par l'ID du profil par rapport auquel vous souhaitez remédier au système.

Par conséquent, le contenu Ansible est traité correctement.



NOTE

La prise en charge des collections fournies dans **rhc-worker-playbook** est limitée à l'activation du contenu Ansible fourni dans **scap-security-guide**.

(BZ#2105162)

8.7. MISE EN RÉSEAU

Le service nm-cloud-setup supprime les adresses IP secondaires configurées manuellement sur les interfaces

Sur la base des informations reçues de l'environnement cloud, le service **nm-cloud-setup** configure les interfaces réseau. Désactivez **nm-cloud-setup** pour configurer manuellement les interfaces. Cependant, dans certains cas, d'autres services sur l'hôte peuvent également configurer les interfaces. Par exemple, ces services peuvent ajouter des adresses IP secondaires. Pour éviter cela, **nm-cloud-setup** supprime les adresses IP secondaires :

1. Arrêtez et désactivez le service et la minuterie **nm-cloud-setup**:

```
# systemctl disable --now nm-cloud-setup.service nm-cloud-setup.timer
```

2. Affiche les profils de connexion disponibles :

```
# nmcli connection show
```

3. Réactive les profils de connexion concernés :

```
# nmcli connection up "<profile_name>"
```

Par conséquent, le service ne supprime plus les adresses IP secondaires configurées manuellement sur les interfaces.

(BZ#2151040)

Une option rd.znet vide dans la ligne de commande du noyau entraîne l'échec de la configuration du réseau

Une option **rd.znet** sans arguments, tels que les types de réseau ou les sous-canaux, dans le noyau ne configure pas la mise en réseau. Pour contourner ce problème, supprimez complètement l'option **rd.znet** de la ligne de commande ou spécifiez les types de réseau, les sous-canaux et les autres options pertinentes. Pour plus d'informations sur ces options, consultez la page de manuel **dracut.cmdline(7)**.

(BZ#1931284)

L'absence de mise à jour de la clé de session entraîne l'interruption de la connexion

Le protocole Kernel Transport Layer Security (kTLS) ne prend pas en charge la mise à jour de la clé de session, qui est utilisée par le chiffrement symétrique. Par conséquent, l'utilisateur ne peut pas mettre à jour la clé, ce qui entraîne une interruption de la connexion. Pour contourner ce problème, il faut désactiver le protocole kTLS. Par conséquent, avec la solution de contournement, il est possible de mettre à jour la clé de session avec succès.

(BZ#2013650)

Le paquet **initscripts** n'est pas installé par défaut

Par défaut, le paquetage **initscripts** n'est pas installé. Par conséquent, les utilitaires **ifup** et **ifdown** ne sont pas disponibles. Vous pouvez utiliser les commandes **nmcli connection up** et **nmcli connection down** pour activer et désactiver les connexions. Si l'alternative proposée ne fonctionne pas, signalez le problème et installez le paquetage **NetworkManager-initscripts-updown**, qui fournit une solution NetworkManager pour les utilitaires **ifup** et **ifdown**.

(BZ#2082303)

L'adresse IP principale d'une instance change après le lancement du service nm-cloud-setup dans Alibaba Cloud

Après le lancement d'une instance dans le nuage Alibaba, le service **nm-cloud-setup** attribue l'adresse IP principale à une instance. Toutefois, si vous attribuez plusieurs adresses IP secondaires à une instance et que vous lancez le service **nm-cloud-setup**, l'ancienne adresse IP primaire est remplacée par l'une des adresses IP secondaires déjà attribuées. La liste des métadonnées renvoyée le confirme. Pour contourner le problème, configurez les adresses IP secondaires manuellement afin d'éviter que l'adresse IP primaire ne change. Ainsi, une instance conserve les deux adresses IP et l'adresse IP principale ne change pas.

(BZ#2079849)

8.8. NOYAU

kdump ne démarre pas sur le noyau RHEL 9

Le paramètre **crashkernel=auto** n'est pas configuré par défaut dans le noyau RHEL 9. Par conséquent, le service **kdump** ne démarre pas par défaut.

Pour contourner ce problème, configurez l'option **crashkernel=** avec la valeur requise.

Par exemple, pour réserver 256 Mo de mémoire à l'aide de l'utilitaire **grubby**, entrez la commande suivante :

```
# grubby --args crashkernel=256M --update-kernel ALL
```

En conséquence, le noyau RHEL 9 démarre **kdump** et utilise la valeur de la taille de la mémoire configurée pour vider le fichier **vmcore**.

(BZ#1894783)

Le mécanisme kdump ne parvient pas à capturer vmcore sur les cibles chiffrées par LUKS

Lors de l'exécution de **kdump** sur des systèmes dotés de partitions chiffrées Linux Unified Key Setup (LUKS), les systèmes requièrent une certaine quantité de mémoire disponible. Lorsque la mémoire disponible est inférieure à la quantité de mémoire requise, le service **systemd-cryptsetup** ne parvient

pas à monter la partition. Par conséquent, le second noyau ne parvient pas à capturer le fichier de vidage d'urgence (**vmcore**) sur les cibles chiffrées LUKS.

La commande **kdumpctl estimate** vous permet d'interroger **Recommended crashkernel value**, qui est la taille de mémoire recommandée pour **kdump**.

Pour contourner ce problème, procédez comme suit pour configurer la mémoire requise pour **kdump** sur les cibles cryptées LUKS :

1. Imprimer la valeur estimée de **crashkernel**:

```
# kdumpctl estimate
```

2. Configurez la quantité de mémoire requise en augmentant la valeur de **crashkernel**:

```
# grubby --args=crashkernel=652M --update-kernel=ALL
```

3. Redémarrez le système pour que les modifications soient prises en compte.

```
# reboot
```

Par conséquent, **kdump** fonctionne correctement sur les systèmes dotés de partitions chiffrées par LUKS.

(BZ#2017401)

L'allocation de la mémoire du noyau de crash échoue au démarrage

Sur certains systèmes Ampere Altra, l'allocation de la mémoire du noyau de crash pour l'utilisation de **kdump** échoue au démarrage lorsque la mémoire disponible est inférieure à 1 Go. Par conséquent, la commande **kdumpctl** ne parvient pas à démarrer le service **kdump** car la mémoire requise est supérieure à la taille de la mémoire disponible.

Pour contourner le problème, diminuez la valeur du paramètre **crashkernel** d'au moins 240 Mo afin de respecter la taille requise, par exemple **crashkernel=240M**. Par conséquent, l'allocation de mémoire au noyau de crash pour **kdump** n'échoue pas sur les systèmes Ampere Altra.

(BZ#2065013)

kTLS ne prend pas en charge le délestage de TLS 1.3 vers les cartes réseau

Kernel Transport Layer Security (kTLS) ne prend pas en charge le délestage de TLS 1.3 vers les cartes réseau. Par conséquent, le chiffrement logiciel est utilisé avec TLS 1.3 même lorsque les cartes réseau prennent en charge le délestage TLS. Pour contourner ce problème, désactivez TLS 1.3 si le délestage est nécessaire. Par conséquent, vous ne pouvez décharger que TLS 1.2. Lorsque TLS 1.3 est utilisé, les performances sont moindres, car TLS 1.3 ne peut pas être déchargé.

(BZ#2000616)

L'activation de FADump avec Secure Boot peut entraîner une perte de mémoire (OOM) dans GRUB

Dans l'environnement Secure Boot, GRUB et PowerVM allouent ensemble une zone de mémoire de 512 Mo, connue sous le nom de Real Mode Area (RMA), pour la mémoire de démarrage. La région est divisée entre les composants de démarrage et, si l'un d'entre eux dépasse son allocation, des pannes de mémoire se produisent.

En général, le système de fichiers **initramfs** installé par défaut et la table de symboles **vmlinux** sont dans les limites permettant d'éviter de telles défaillances. Toutefois, si la fonction Firmware Assisted Dump (FADump) est activée dans le système, la taille par défaut de **initramfs** peut augmenter et dépasser 95 Mo. Par conséquent, chaque redémarrage du système entraîne un état GRUB OOM.

Pour éviter ce problème, n'utilisez pas Secure Boot et FADump en même temps. Pour plus d'informations et de méthodes sur la manière de contourner ce problème, voir le lien:https://www.ibm.com/support/pages/node/6846531.

(BZ#2149172)

Les systèmes en mode Secure Boot ne peuvent pas exécuter d'opérations dynamiques sur les LPAR

Les utilisateurs ne peuvent pas exécuter d'opérations de partition logique dynamique (DLPAR) à partir de la console de gestion du matériel (HMC) si l'une ou l'autre de ces conditions est remplie :

- La fonction Secure Boot est activée, ce qui permet d'activer implicitement le mécanisme du noyau **lockdown** en mode intégrité.
- Le mécanisme du noyau **lockdown** est activé manuellement en mode intégrité ou confidentialité.

Dans RHEL 9, le noyau **lockdown** bloque complètement l'accès des Run Time Abstraction Services (RTAS) à la mémoire système accessible via le fichier de périphérique de caractères /**dev**/**mem**. Plusieurs appels RTAS nécessitent un accès en écriture à /**dev**/**mem** pour fonctionner correctement. Par conséquent, les appels RTAS ne s'exécutent pas correctement et les utilisateurs voient le message d'erreur suivant :

> HSCL2957 Il n'y a actuellement aucune connexion RMC entre la console de gestion et la partition <LPAR name> ou la partition ne prend pas en charge les opérations de partitionnement dynamique. Vérifiez la configuration du réseau sur la console de gestion et la partition et assurez-vous que l'authentification du pare-feu entre la console de gestion et la partition a eu lieu. Exécutez la commande diagrmc de la console de gestion pour identifier les problèmes qui pourraient être à l'origine de l'absence de connexion RMC.

(BZ#2083106)

8.9. CHARGEUR DE DÉMARRAGE

Les nouveaux noyaux perdent les options de ligne de commande précédentes

Le chargeur d'amorçage GRUB n'applique pas aux nouveaux noyaux les options de ligne de commande personnalisées et configurées précédemment. Par conséquent, lorsque vous mettez à jour le paquetage du noyau, le comportement du système peut changer après le redémarrage en raison des options manquantes.

Pour contourner le problème, ajoutez manuellement toutes les options personnalisées de la ligne de commande du noyau après chaque mise à jour du noyau. Ainsi, le noyau applique les options personnalisées comme prévu, jusqu'à la prochaine mise à jour du noyau.

(BZ#1969362)

8.10. SYSTÈMES DE FICHIERS ET STOCKAGE

Device Mapper Multipath n'est pas pris en charge avec NVMe/TCP

L'utilisation de Device Mapper Multipath avec le pilote **nvme-tcp** peut entraîner des avertissements Call Trace et une instabilité du système. Pour contourner ce problème, les utilisateurs de NVMe/TCP doivent activer le multipathing NVMe natif et ne pas utiliser les outils **device-mapper-multipath** avec NVMe.

Par défaut, le multipathing NVMe natif est activé dans RHEL 9. Pour plus d'informations, voir Activation du multipathing sur les périphériques NVMe.

(BZ#2033080)

Le service blk-availability systemd désactive les piles de dispositifs complexes

Dans **systemd**, le code de désactivation des blocs par défaut ne gère pas toujours correctement les piles complexes de blocs virtuels. Dans certaines configurations, les périphériques virtuels peuvent ne pas être supprimés lors de l'arrêt, ce qui entraîne l'enregistrement de messages d'erreur. Pour contourner ce problème, désactivez les piles de blocs complexes en exécutant la commande suivante :

```
# systemctl enable --now blk-availability.service
```

Par conséquent, les piles de dispositifs virtuels complexes sont correctement désactivées lors de l'arrêt et ne produisent pas de messages d'erreur.

(BZ#2011699)

Valeur invalide de sysfs pour supported_speeds

Le pilote **qla2xxx** indique 20Gb/s au lieu des 64Gb/s prévus comme l'une des vitesses de port prises en charge dans l'attribut **sysfs supported_speeds**:

```
$ cat /sys/class/fc_host/host12/supported_speeds
16 Gbit, 32 Gbit, 20 Gbit
```

Par conséquent, si l'adaptateur de bus hôte prend en charge une vitesse de liaison de 64 Gb/s, la valeur de **sysfs supported_speeds** est incorrecte. Cela n'affecte que la valeur **supported_speeds** de **sysfs** et le port fonctionne à la vitesse de liaison négociée prévue.

(BZ#2069758)

Impossible de se connecter aux espaces de noms NVMe à partir d'un initiateur Broadcom sur les systèmes AMD EPYC

Par défaut, le noyau RHEL active l'IOMMU sur les plateformes basées sur AMD. Par conséquent, lorsque vous utilisez des plates-formes activées par IOMMU sur des serveurs équipés de processeurs AMD, vous pouvez rencontrer des problèmes d'E/S NVMe, tels que l'échec des E/S en raison de la non-concordance des longueurs de transfert.

Pour contourner ce problème, ajoutez l'IOMMU en mode passthrough en utilisant l'option de ligne de commande du noyau, **iommu=pt**. Par conséquent, vous pouvez désormais vous connecter aux espaces de noms NVMe à partir de l'initiateur Broadcom sur les systèmes AMD EPYC.

(BZ#2073541)

8.11. LANGAGES DE PROGRAMMATION DYNAMIQUES, SERVEURS WEB ET DE BASE DE DONNÉES

L'option --ssl-fips-mode dans MySQL et MariaDB ne modifie pas le mode FIPS

L'option **--ssl-fips-mode** dans **MySQL** et **MariaDB** dans RHEL fonctionne différemment que dans upstream.

Dans RHEL 9, si vous utilisez **--ssl-fips-mode** comme argument pour le démon **mysqld** ou **mariadbd**, ou si vous utilisez **ssl-fips-mode** dans les fichiers de configuration des serveurs **MySQL** ou **MariaDB**, **--ssl-fips-mode** ne modifie pas le mode FIPS pour ces serveurs de base de données.

Au lieu de cela :

- Si vous attribuez la valeur **ON** à **--ssl-fips-mode**, le démon du serveur **mysqld** ou **mariadbd** ne démarre pas.
- Si vous remplacez **--ssl-fips-mode** par **OFF** sur un système compatible FIPS, les démons de serveur **mysqld** ou **mariadbd** s'exécutent toujours en mode FIPS.

Cela est normal car le mode FIPS doit être activé ou désactivé pour l'ensemble du système RHEL, et non pour des composants spécifiques.

Par conséquent, n'utilisez pas l'option **--ssl-fips-mode** dans **MySQL** ou **MariaDB** dans RHEL. Assurez-vous plutôt que le mode FIPS est activé sur l'ensemble du système RHEL :

- De préférence, installez RHEL avec le mode FIPS activé. L'activation du mode FIPS pendant l'installation garantit que le système génère toutes les clés à l'aide d'algorithmes approuvés par le FIPS et de tests de surveillance continue en place. Pour plus d'informations sur l'installation de RHEL en mode FIPS, voir Installation du système en mode FIPS.
- Vous pouvez également passer en mode FIPS pour l'ensemble du système RHEL en suivant la procédure décrite à la section Passage du système en mode FIPS.

(BZ#1991500)

8.12. COMPILATEURS ET OUTILS DE DÉVELOPPEMENT

Certaines sondes basées sur des symboles ne fonctionnent pas dans SystemTap sur l'architecture ARM 64 bits

La configuration du noyau désactive certaines fonctionnalités nécessaires à **SystemTap**. Par conséquent, certaines sondes basées sur des symboles ne fonctionnent pas sur l'architecture ARM 64 bits. Par conséquent, les scripts **SystemTap** concernés peuvent ne pas s'exécuter ou ne pas recueillir de résultats sur les points de sonde souhaités.

Ce bogue a été corrigé pour les autres architectures avec la publication de l'avis RHBA-2022:5259.

(BZ#2083727)

8.13. GESTION DE L'IDENTITÉ

Le client RHEL 9 Kerberos ne parvient pas à authentifier un utilisateur à l'aide de PKINIT contre Heimdal KDC

Lors de l'authentification PKINIT d'un utilisateur IdM sur un client Kerberos RHEL 9, le Centre de distribution Heimdal Kerberos (KDC) sur RHEL 9 ou antérieur utilise l'algorithme de signature de sauvegarde SHA-1 car le client Kerberos ne prend pas en charge le champ **supportedCMSTypes**. Cependant, l'algorithme SHA-1 a été déprécié dans RHEL 9 et l'authentification de l'utilisateur échoue.

Pour contourner ce problème, activez la prise en charge de l'algorithme SHA-1 sur vos clients RHEL 9 à l'aide de la commande suivante :

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

Par conséquent, l'authentification PKINIT fonctionne entre le client Kerberos et le KDC Heimdal.

Pour plus de détails sur les algorithmes de signature de sauvegarde pris en charge, voir Types de chiffrement Kerberos définis pour les identifiants d'algorithmes CMS.

Voir aussi L'authentification PKINIT d'un utilisateur échoue si un agent Kerberos RHEL 9 communique avec un agent Kerberos non RHEL 9.

(BZ#2068935)

L'authentification PKINIT d'un utilisateur échoue si un agent Kerberos RHEL 9 communique avec un agent Kerberos non RHEL 9

Si un agent Kerberos RHEL 9 interagit avec un autre agent Kerberos non RHEL 9 dans votre environnement, l'authentification d'un utilisateur par cryptographie à clé publique pour l'authentification initiale (PKINIT) échoue. Pour contourner le problème, effectuez l'une des actions suivantes :

- Définissez la politique cryptographique de l'agent RHEL 9 sur **DEFAULT:SHA1** pour autoriser la vérification des signatures SHA-1 :

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

- Mettez à jour l'agent non RHEL 9 pour vous assurer qu'il ne signe pas les données CMS à l'aide de l'algorithme SHA-1. Pour cela, mettez à jour vos paquets Kerberos vers les versions qui utilisent SHA-256 au lieu de SHA-1 :
  - CentOS 9 Stream : krb5-1.19.1-15
  - RHEL 8.7 : krb5-1.18.2-17
  - RHEL 7.9 : krb5-1.15.1-53
  - Fedora Rawhide/36 : krb5-1.19.2-7
  - Fedora 35/34 : krb5-1.19.2-3

Vous devez effectuer l'une de ces actions, que l'agent non corrigé soit un client Kerberos ou le Centre de distribution Kerberos (KDC).

Par conséquent, l'authentification PKINIT d'un utilisateur fonctionne correctement.

Notez que pour les autres systèmes d'exploitation, c'est la version krb5-1.20 qui garantit que l'agent signe les données du CMS avec SHA-256 au lieu de SHA-1.

Voir aussi La sous-politique DEFAULT:SHA1 doit être définie sur les clients RHEL 9 pour que PKINIT fonctionne avec les anciens KDC RHEL et les KDC AD.

(BZ#2077450)

La sous-politique DEFAULT:SHA1 doit être définie sur les clients RHEL 9 pour que PKINIT fonctionne avec les anciens KDC RHEL et les KDC AD

L'algorithme de condensé SHA-1 a été supprimé dans RHEL 9, et les messages CMS pour la cryptographie à clé publique pour l'authentification initiale (PKINIT) sont désormais signés avec l'algorithme SHA-256, plus puissant.

Alors que SHA-256 est utilisé par défaut à partir de RHEL 7.9 et RHEL 8.7, les anciens centres de distribution de clés (KDC) Kerberos sur RHEL 7.8 et RHEL 8.6 et antérieurs utilisent toujours l'algorithme de condensé SHA-1 pour signer les messages CMS. Il en va de même pour le centre de distribution de clés Active Directory (AD).

Par conséquent, les clients Kerberos de RHEL 9 ne parviennent pas à authentifier les utilisateurs à l'aide de PKINIT contre les éléments suivants :

- KDC fonctionnant sous RHEL 7.8 et antérieur
- KDC fonctionnant sous RHEL 8.6 et antérieur
- AD KDCs

Pour contourner le problème, activez la prise en charge de l'algorithme SHA-1 sur vos systèmes RHEL 9 à l'aide de la commande suivante :

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

Voir aussi Le client RHEL 9 Kerberos ne parvient pas à authentifier un utilisateur à l'aide de PKINIT contre Heimdal KDC.

(BZ#2060798)

La prise en charge FIPS de la confiance AD nécessite la sous-politique cryptographique AD-SUPPORT

Active Directory (AD) utilise des types de chiffrement AES SHA-1 HMAC, qui ne sont pas autorisés par défaut en mode FIPS sur RHEL 9. Si vous souhaitez utiliser des hôtes IdM RHEL 9 avec une confiance AD, activez la prise en charge des types de chiffrement AES SHA-1 HMAC avant d'installer le logiciel IdM.

La conformité FIPS étant un processus qui implique des accords techniques et organisationnels, consultez votre auditeur FIPS avant d'activer la sous-politique **AD-SUPPORT** pour permettre aux mesures techniques de prendre en charge les types de chiffrement AES SHA-1 HMAC, puis installez RHEL IdM :

```
# update-crypto-policies --set FIPS:AD-SUPPORT
```

(BZ#2057471)

Directory Server se termine de manière inattendue lorsqu'il est démarré en mode de référence

En raison d'un bogue, le mode de renvoi global ne fonctionne pas dans Directory Server. Si vous démarrez le processus **ns-slapd** avec l'option **refer** en tant qu'utilisateur **dirsrv**, Directory Server ignore les paramètres du port et se termine de manière inattendue. Essayer d'exécuter le processus en tant qu'utilisateur **root** modifie les étiquettes SELinux et empêche le service de démarrer à l'avenir en mode normal. Il n'y a pas de solution de rechange disponible.

(BZ#2053204)

La configuration d'un renvoi pour un suffixe échoue dans Directory Server

Si vous définissez une référence de back-end dans Directory Server, la définition de l'état du back-end à l'aide de la commande **dsconf <instance_name> backend suffix set --state referral** échoue avec l'erreur suivante :

```
Error: 103 - 9 - 53 - Server is unwilling to perform - [] - need to set nsslapd-referral before moving to referral state
```

Par conséquent, la configuration d'un renvoi pour les suffixes échoue. Pour contourner le problème :

1. Réglez manuellement le paramètre **nsslapd-referral**:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com

dn: cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
changetype: modify
add: nsslapd-referral
nsslapd-referral: ldap://remote_server:389/dc=example,dc=com
```

2. Définir l'état du back-end :

```
# dsconf <instance_name> backend suffix set --state referral
```

Par conséquent, avec la solution de contournement, vous pouvez configurer un renvoi pour un suffixe.

(BZ#2063140)

L'utilitaire dsconf n'a pas d'option pour créer des tâches de correction pour le plug-in entryUUID

L'utilitaire **dsconf** ne propose pas d'option permettant de créer des tâches de correction pour le plug-in **entryUUID**. Par conséquent, les administrateurs ne peuvent pas utiliser **dsconf** pour créer une tâche permettant d'ajouter automatiquement des attributs **entryUUID** aux entrées existantes. Une solution de contournement consiste à créer une tâche manuellement :

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: cn=entryuuid_fixup___<time_stamp__,cn=entryuuid task,cn=tasks,cn=config
objectClass: top
objectClass: extensibleObject
basedn: __<fixup base tree>__
cn: entryuuid_fixup___<time_stamp>__
filter: __<filtered_entry>__
```

Une fois la tâche créée, Directory Server corrige les entrées dont les attributs **entryUUID** sont manquants ou invalides.

(BZ#2047175)

Risque potentiel lié à l'utilisation de la valeur par défaut de l'option ldap_id_use_start_tls

L'utilisation de **ldap://** sans TLS pour les recherches d'identité peut constituer un risque pour un vecteur d'attaque. En particulier une attaque de type "man-in-the-middle" (MITM) qui pourrait permettre à un pirate d'usurper l'identité d'un utilisateur en modifiant, par exemple, l'UID ou le GID d'un objet renvoyé lors d'une recherche LDAP.

Actuellement, l'option de configuration SSSD pour appliquer TLS, **ldap_id_use_start_tls**, est par défaut **false**. Assurez-vous que votre installation fonctionne dans un environnement de confiance et décidez s'il est sûr d'utiliser une communication non chiffrée pour **id_provider = ldap**. Notez que **id_provider = ad** et **id_provider = ipa** ne sont pas concernés car ils utilisent des connexions cryptées protégées par SASL et GSSAPI.

S'il n'est pas sûr d'utiliser des communications non chiffrées, appliquez le protocole TLS en définissant l'option **ldap_id_use_start_tls** sur **true** dans le fichier **/etc/sssd/sssd.conf**. Il est prévu de modifier le comportement par défaut dans une prochaine version de RHEL.

(JIRA:RHELPLAN-155168)

8.14. BUREAU

Les modules complémentaires de Firefox sont désactivés après la mise à niveau vers RHEL 9

Si vous passez de RHEL 8 à RHEL 9, tous les modules complémentaires que vous avez précédemment activés dans Firefox sont désactivés.

Pour contourner le problème, réinstallez ou mettez à jour manuellement les modules complémentaires. Les modules complémentaires sont alors activés comme prévu.

(BZ#2013247)

VNC ne fonctionne pas après la mise à niveau vers RHEL 9

Après une mise à niveau de RHEL 8 vers RHEL 9, le serveur VNC ne démarre pas, même s'il était activé auparavant.

Pour contourner le problème, activez manuellement le service **vncserver** après la mise à niveau du système :

```
# systemctl enable --now vncserver@ :port-number
```

En conséquence, VNC est maintenant activé et démarre après chaque démarrage du système, comme prévu.

(BZ#2060308)

8.15. INFRASTRUCTURES GRAPHIQUES

Matrox G200e n'affiche aucune sortie sur un écran VGA

Il se peut que votre écran n'affiche aucune sortie graphique si vous utilisez la configuration suivante :

- Le GPU Matrox G200e
- Un écran connecté au contrôleur VGA

Par conséquent, vous ne pouvez pas utiliser ou installer RHEL sur cette configuration.

Pour contourner le problème, suivez la procédure suivante :

1. Amorcez le système dans le menu du chargeur de démarrage.

2. Ajouter l'option **module_blacklist=mgag200** à la ligne de commande du noyau.

Par conséquent, RHEL démarre et affiche la sortie graphique comme prévu, mais la résolution maximale est limitée à 1024x768 avec une profondeur de couleur de 16 bits.

(BZ#1960467)

Les utilitaires de configuration X.org ne fonctionnent pas sous Wayland

Les utilitaires X.org permettant de manipuler l'écran ne fonctionnent pas dans la session Wayland. En particulier, l'utilitaire **xrandr** ne fonctionne pas sous Wayland en raison de son approche différente de la gestion, des résolutions, des rotations et de la mise en page.

(JIRA:RHELPLAN-121049)

Les pilotes NVIDIA pourraient revenir à X.org

Dans certaines conditions, les pilotes propriétaires de NVIDIA désactivent le protocole d'affichage Wayland et reviennent au serveur d'affichage X.org :

- Si la version du pilote NVIDIA est inférieure à 470.
- Si le système est un ordinateur portable qui utilise des graphiques hybrides.
- Si vous n'avez pas activé les options requises du pilote NVIDIA.

En outre, Wayland est activé mais la session de bureau utilise X.org par défaut si la version du pilote NVIDIA est inférieure à 510.

(JIRA:RHELPLAN-119001)

Night Light n'est pas disponible sur Wayland avec NVIDIA

Lorsque les pilotes NVIDIA propriétaires sont activés sur votre système, la fonction **Night Light** de GNOME n'est pas disponible dans les sessions Wayland. Les pilotes NVIDIA ne prennent pas actuellement en charge **Night Light**.

(JIRA:RHELPLAN-119852)

8.16. LA CONSOLE WEB

La suppression de périphériques hôtes USB à l'aide de la console web ne fonctionne pas comme prévu

Lorsque vous attachez un périphérique USB à une machine virtuelle (VM), le numéro de périphérique et le numéro de bus du périphérique USB peuvent changer après avoir été transmis à la VM. Par conséquent, l'utilisation de la console web pour supprimer ces périphériques échoue en raison de la corrélation incorrecte des numéros de périphérique et de bus. Pour contourner ce problème, supprimez la partie **<hostdev>** du périphérique USB de la configuration XML de la VM.

(JIRA:RHELPLAN-109067)

L'attachement de plusieurs périphériques hôtes à l'aide de la console web ne fonctionne pas

Lorsque vous sélectionnez plusieurs périphériques à attacher à une machine virtuelle (VM) à l'aide de la console web, seul un périphérique est attaché et les autres sont ignorés. Pour contourner ce problème, attachez un seul périphérique à la fois.

(JIRA:RHELPLAN-115603)

8.17. VIRTUALISATION

L'installation d'une machine virtuelle via https échoue dans certains cas

Actuellement, l'utilitaire **virt-install** échoue lorsqu'il tente d'installer un système d'exploitation invité à partir d'une source ISO via une connexion https - par exemple en utilisant **virt-install --cdrom https://example/path/to/image.iso**. Au lieu de créer une machine virtuelle (VM), l'opération décrite se termine de manière inattendue par un message **internal error: process exited while connecting to monitor**.

Pour contourner ce problème, installez **qemu-kvm-block-curl** sur l'hôte pour activer la prise en charge du protocole https. Vous pouvez également utiliser un autre protocole de connexion ou une autre source d'installation.

(BZ#2014229)

L'utilisation des pilotes NVIDIA dans les machines virtuelles désactive Wayland

Actuellement, les pilotes NVIDIA ne sont pas compatibles avec la session graphique Wayland. Par conséquent, les systèmes d'exploitation invités RHEL qui utilisent des pilotes NVIDIA désactivent automatiquement Wayland et chargent une session Xorg à la place. Cela se produit principalement dans les scénarios suivants :

- Lorsque vous faites passer un périphérique GPU NVIDIA dans une machine virtuelle RHEL (VM)
- Lorsque vous affectez un périphérique NVIDIA vGPU à une VM RHEL

(JIRA:RHELPLAN-117234)

Le type de CPU Milan VM n'est parfois pas disponible sur les systèmes AMD Milan

Sur certains systèmes AMD Milan, les options Enhanced REP MOVSB (**erms**) et Fast Short REP MOVSB (**fsrm**) sont désactivées par défaut dans le BIOS. Par conséquent, le type de CPU "Milan" peut ne pas être disponible sur ces systèmes. En outre, la migration en direct de VM entre des hôtes Milan avec des paramètres de drapeaux de fonctionnalités différents peut échouer. Pour résoudre ces problèmes, activez manuellement **erms** et **fsrm** dans le BIOS de votre hôte.

(BZ#2077767)

Les performances du trafic réseau dans les machines virtuelles peuvent être réduites

Dans certains cas, les machines virtuelles invitées (VM) RHEL 9.0 ont des performances quelque peu réduites lorsqu'elles gèrent des niveaux élevés de trafic réseau.

(BZ#1945040)

La désactivation d'AVX rend les machines virtuelles non amorçables

Sur une machine hôte qui utilise un processeur avec support Advanced Vector Extensions (AVX), la tentative de démarrage d'une VM avec AVX explicitement désactivé échoue actuellement et déclenche une panique du noyau dans la VM.

(BZ#2005173)

Les cartes réseau virtio de basculement ne reçoivent pas d'adresse IP sur les machines virtuelles Windows

Actuellement, lors du démarrage d'une machine virtuelle (VM) Windows avec seulement une carte d'interface réseau virtio de basculement, la VM ne parvient pas à attribuer une adresse IP à la carte d'interface réseau. Par conséquent, la carte d'interface réseau n'est pas en mesure d'établir une connexion réseau. Il n'existe actuellement aucune solution de contournement.

(BZ#1969724)

Une interface **hostdev** avec des paramètres de basculement ne peut pas être branchée à chaud après avoir été débranchée à chaud

Après avoir supprimé une interface réseau **hostdev** avec une configuration de basculement d'une machine virtuelle (VM) en cours d'exécution, l'interface ne peut actuellement pas être réattachée à la même VM en cours d'exécution.

(BZ#2052424)

Échec de la migration post-copie en direct de VM avec des VF de basculement

Actuellement, la tentative de migration post-copie d'une machine virtuelle (VM) en cours d'exécution échoue si la VM utilise un périphérique dont la capacité de basculement de la fonction virtuelle (VF) est activée. Pour contourner le problème, utilisez le type de migration standard plutôt que la migration post-copie.

(BZ#1817965, BZ#1789206)

8.18. RHEL DANS LES ENVIRONNEMENTS EN NUAGE

SR-IOV fonctionne de manière sous-optimale dans les machines virtuelles ARM 64 RHEL 9 sur Azure

Actuellement, les dispositifs de mise en réseau SR-IOV ont un rendement nettement plus faible et une latence plus élevée que prévu dans les machines virtuelles ARM 64 RHEL 9 fonctionnant sur une plateforme Microsoft Azure.

(BZ#2068432)

La souris n'est pas utilisable dans les machines virtuelles RHEL 9 sur XenServer 7 avec un proxy de console

Lors de l'exécution d'une machine virtuelle (VM) RHEL 9 sur une plateforme XenServer 7 avec un proxy de console, il n'est pas possible d'utiliser la souris dans l'interface graphique de la VM. Pour contourner ce problème, désactivez le protocole compositeur Wayland dans la VM comme suit :

1. Ouvrez le fichier **/etc/gdm/custom.conf**.
2. Décommentez la ligne **WaylandEnable=false**.
3. Enregistrer le fichier.

En outre, notez que Red Hat ne prend pas en charge XenServer en tant que plate-forme pour l'exécution de VM RHEL et déconseille l'utilisation de XenServer avec RHEL dans les environnements de production.

(BZ#2019593)

Le clonage ou la restauration de machines virtuelles RHEL 9 utilisant LVM sur Nutanix AHV entraîne la disparition des partitions non root

Lors de l'exécution d'un système d'exploitation invité RHEL 9 sur une machine virtuelle (VM) hébergée sur l'hyperviseur Nutanix AHV, la restauration de la VM à partir d'un snapshot ou le clonage de la VM provoque actuellement la disparition des partitions non racine dans la VM si l'invité utilise Logical Volume Management (LVM). En conséquence, les problèmes suivants se produisent :

- Après avoir restauré la VM à partir d'un instantané, la VM ne peut pas démarrer et passe en mode d'urgence.
- Une VM créée par clonage ne peut pas démarrer et passe en mode d'urgence.

Pour contourner ces problèmes, procédez comme suit en mode d'urgence de la VM :

1. Supprimez le fichier des périphériques du système LVM : **rm /etc/lvm/devices/system.devices**
2. Recréer les paramètres du périphérique LVM : **vgimportdevices -a**
3. Redémarrer la VM

Cela permet à la VM clonée ou restaurée de démarrer correctement.

(BZ#2059545)

La fonctionnalité SR-IOV d'une carte réseau connectée à une machine virtuelle Hyper-V peut ne pas fonctionner

Actuellement, lors de la connexion d'un adaptateur réseau avec la virtualisation d'E/S à racine unique (SR-IOV) activée à une machine virtuelle RHEL 9 fonctionnant sur l'hyperviseur Microsoft Hyper-V, la fonctionnalité SR-IOV ne fonctionne pas correctement dans certains cas.

Pour contourner ce problème, désactivez SR-IOV dans la configuration de la VM, puis réactivez-le.

1. Dans la fenêtre Hyper-V Manager, cliquez avec le bouton droit de la souris sur la VM.
2. Dans le menu contextuel, naviguez jusqu'à **Settings/Network Adapter/Hardware Acceleration**.
3. Décochez la case **Activer SR-IOV**.
4. Cliquez sur **Appliquer**.
5. Répétez les étapes 1 et 2 pour accéder de nouveau à l'option **Activer SR-IOV.**
6. Cochez **Activer SR-IOV**.
7. Cliquez sur **Appliquer**.

(BZ#2030922)

La personnalisation des invités RHEL 9 sur ESXi entraîne parfois des problèmes de réseau

Actuellement, la personnalisation d'un système d'exploitation invité RHEL 9 dans l'hyperviseur VMware ESXi ne fonctionne pas correctement avec les fichiers clés NetworkManager. Par conséquent, si l'invité utilise un tel fichier clé, il aura des paramètres réseau incorrects, tels que l'adresse IP ou la passerelle.

Pour plus d'informations et des instructions de contournement, consultez la base de connaissances VMware.

(BZ#2037657)

8.19. CAPACITÉ DE SOUTIEN

Délai d'attente lors de l'exécution de sos report sur IBM Power Systems, Little Endian

Lors de l'exécution de la commande **sos report** sur des systèmes IBM Power, Little Endian avec des centaines ou des milliers de CPU, le plugin processeur atteint son délai d'attente par défaut de 300 secondes lors de la collecte de l'énorme contenu du répertoire **/sys/devices/system/cpu**. Pour contourner ce problème, augmentez le délai d'attente du plugin en conséquence :

- Pour un réglage unique, exécuter :

```
# sos report -k processor.timeout=1800
```

- Pour une modification permanente, modifiez la section **[plugin_options]** du fichier **/etc/sos/sos.conf**:

```
[plugin_options]
# Specify any plugin options and their values here. These options take the form
# plugin_name.option_name = value
#rpm.rpmva = off
processor.timeout = 1800
```

La valeur de l'exemple est fixée à 1800. La valeur particulière du délai d'attente dépend fortement d'un système spécifique. Pour définir le délai d'attente du plugin de manière appropriée, vous pouvez d'abord estimer le temps nécessaire pour collecter le plugin sans délai d'attente en exécutant la commande suivante :

```
# time sos report -o processor -k processor.timeout=0 --batch --build
```

(BZ#1869561)

8.20. CONTENEURS

Les images de conteneurs signées avec une clé Beta GPG ne peuvent pas être extraites

Actuellement, lorsque vous essayez d'extraire des images de conteneurs RHEL 9 Beta, **podman** s'arrête avec le message d'erreur : **Error: Source image rejected: None of the signatures were accepted**. Les images ne peuvent pas être extraites car les versions actuelles sont configurées pour ne pas faire confiance aux clés GPG de RHEL Beta par défaut.

Comme solution de contournement, assurez-vous que la clé GPG Red Hat Beta est stockée sur votre système local et mettez à jour l'étendue de confiance existante avec la commande **podman image trust set** pour l'espace de noms beta approprié.

Si vous n'avez pas la clé GPG Beta stockée localement, vous pouvez l'obtenir en exécutant la commande suivante :

```
sudo wget -O /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-beta
https://www.redhat.com/security/data/f21541eb.txt
```

Pour ajouter la clé GPG Beta en tant que clé de confiance à votre espace de noms, utilisez l'une des commandes suivantes :

```
sudo podman image trust set -f /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-beta
registry.access.redhat.com/namespace
```

et

```
sudo podman image trust set -f /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-beta
registry.redhat.io/namespace
```

Remplacer *namespace* par *ubi9-beta* ou *rhel9-beta*.

(BZ#2020026)

Podman ne parvient pas à extraire un conteneur "X509 : certificat signé par une autorité inconnue"

Si vous disposez de votre propre registre interne signé par notre propre certificat d'autorité de certification, vous devez importer le certificat sur votre machine hôte. Sinon, une erreur se produit :

```
x509: certificate signed by unknown authority
```

Importez les certificats d'autorité de certification sur votre hôte :

```
# cd /etc/pki/ca-trust/source/anchors/
[anchors]# curl -O <your_certificate>.crt

[anchors]# update-ca-trust
```

Vous pouvez ensuite extraire des images de conteneurs du registre interne.

(BZ#2027576)

L'exécution de systemd dans une ancienne image de conteneur ne fonctionne pas

L'exécution de systemd dans une ancienne image de conteneur, par exemple, **centos:7**, ne fonctionne pas :

```
$ podman run --rm -ti centos:7 /usr/lib/systemd/systemd
 Storing signatures
 Failed to mount cgroup at /sys/fs/cgroup/systemd: Operation not permitted
 [!!!!!!] Failed to mount API filesystems, freezing.
```

Pour contourner ce problème, utilisez les commandes suivantes :

```
# mkdir /sys/fs/cgroup/systemd
# mount none -t cgroup -o none,name=systemd /sys/fs/cgroup/systemd
# podman run --runtime /usr/bin/crun --annotation=run.oci.systemd.force_cgroup_v1=/sys/fs/cgroup -
-rm -ti centos:7 /usr/lib/systemd/systemd
```

(JIRA:RHELPLAN-96940)

podman system connection add et **podman image scp** échoue

Podman utilise des hachages SHA-1 pour l'échange de clés RSA. La connexion SSH normale entre les machines utilisant des clés RSA fonctionne, mais les commandes **podman system connection add** et **podman image scp** ne fonctionnent pas avec les mêmes clés RSA, car les hachages SHA-1 ne sont pas

acceptés pour l'échange de clés sur RHEL 9 :

```
$ podman system connection add --identity ~/.ssh/id_rsa test_connection
$REMOTE_SSH_MACHINE
Error: failed to connect: ssh: handshake failed: ssh: unable to authenticate, attempted methods [none
publickey], no supported methods remain
```

Pour contourner ce problème, utilisez les clés ED25519 :

1. Se connecter à la machine distante :

```
$ ssh -i ~/.ssh/id_ed25519 $REMOTE_SSH_MACHINE
```

2. Enregistrement de la destination ssh pour le service Podman :

```
$ podman system connection add --identity ~/.ssh/id_ed25519 test_connection
$REMOTE_SSH_MACHINE
```

3. Vérifiez que la destination ssh a été enregistrée :

```
$ podman system connection list
```

Notez qu'avec la publication de l'avis RHBA-2022:5951, le problème a été corrigé.

(JIRA:RHELPLAN-121180)

ANNEXE A. LISTE DES TICKETS PAR COMPOSANT

Les identifiants Bugzilla et JIRA sont listés dans ce document à titre de référence. Les bugs Bugzilla qui sont accessibles au public incluent un lien vers le ticket.

Composant	Billets
389-ds-base	BZ#2024693, BZ#1805717, BZ#1779685, BZ#2053204, BZ#2063140, BZ#2047175
ModemManager	BZ#1996716
NetworkManager	BZ#1980387, BZ#1949127, BZ#2060013, BZ#1931284, BZ#1894877, BZ#2079849
RHCOS	BZ#2008521
WALinuxAgent	BZ#1972101
alsa-lib	BZ#2015863
anaconda	BZ#1951709, BZ#1978264, BZ#2025953, BZ#2009403, BZ#2050140, BZ#1877697, BZ#1914955, BZ#1929105, BZ#1983602, BZ#1997832, BZ#2008792
ansible-collection-microsoft-sql	BZ#2064648, BZ#2064690
ansible-collection-redhat-rhel_mgmt	BZ#2023381
ansible-pcp	BZ#1957566
bash	BZ#2079078
bind	BZ#1984982
binutils	BZ#2030554
boost	BZ#1957950
chrony	BZ#1961131
clevis	BZ#1956760
cloud-init	BZ#2040090, BZ#2042351
cmake	BZ#1957948

Composant	Billets
container-tools	BZ#2000871
containers-common	BZ#2019901
crash	BZ#1896647
createrepo_c	BZ#2055032
crypto-policies	BZ#2004207, BZ#2013195
cyrus-sasl	BZ#1947971, BZ#1995600
device-mapper-multipath	BZ#2017979, BZ#2017592, BZ#2011699
distribution	BZ#1878583
dnf	BZ#2005305, BZ#2073510
dotnet6.0	BZ#1986211
edk2	BZ#1935497
eigen3	BZ#2032423
fapolicyd	BZ#2032408, BZ#1932225, BZ#2054740, BZ#2070655
fence-agents	BZ#1977588
fetchmail	BZ#1999276
fido-device-onboard	BZ#1989930
firefox	BZ#1764205, BZ#2013247
firewalld	BZ#2029211
freeradius	BZ#1978216
gcc	BZ#1986836, BZ#1481850
gdb	BZ#1870029, BZ#1870031
gfs2-utils	BZ#1616432
gimp	BZ#2047161

Composant	Billets
git	BZ#1956345
glibc	BZ#2023422, BZ#2024347
gnome-shell-extension-background-logo	BZ#2057150
gnome-shell-extensions	BZ#2031186
gnupg2	BZ#2070722, BZ#2073567
gnutls	BZ#2033220, BZ#1999639
golang	BZ#2014087, BZ#1984110
grafana-pcp	BZ#1993156, BZ#1845592
grafana	BZ#1993215
grub2	BZ#2026579
grubby	BZ#1969362
hostapd	BZ#2019830
ipa	BZ#1952028, BZ#1957736, BZ#1966101, BZ#1988383, BZ#2084180, BZ#2084166, BZ#2057471
iptables	BZ#1945151
javapackages-tools	BZ#1951482
jigawatts	BZ#1972029
jmc-core	BZ#1980981
kdump-anaconda-addon	BZ#1894783, BZ#2017401
kernel-rt	BZ#2002474

Composant	Billets
kernel	BZ#1844416, BZ#1851933, BZ#1780258, BZ#1874195, BZ#1953515, BZ#1960556, BZ#1948340, BZ#1952863, BZ#1978382, BZ#1957818, BZ#2002499, BZ#2050415, BZ#1951951, BZ#1949613, BZ#2036856, BZ#2034490, BZ#1943423, BZ#2054441, BZ#2046472, BZ#2068432, BZ#1997541, BZ#1613522, BZ#1874182, BZ#1995338, BZ#1570255, BZ#2023416, BZ#2021672, BZ#2019593, BZ#2000616, BZ#2013650, BZ#2033080, BZ#2069758, BZ#2059545, BZ#2030922, BZ#1945040, BZ#2073541, BZ#1960467, BZ#2005173
kexec-tools	BZ#1988894, BZ#1895232, BZ#1958452, BZ#2065013
kmod	BZ#1985100
krb5	BZ#2060798, BZ#2068935, BZ#2077450
libburn	BZ#2015861
libcap	BZ#2037215
libgcrypt	BZ#1990059
libmodulemd	BZ#1984403
libreswan	BZ#2017355, BZ#2039877
libseccomp	BZ#2019887
libservicelog	BZ#1869568
libvirt	BZ#2014487
libxcrypt	BZ#2034569
llvm-toolset	BZ#2001107
lorax-templates-rhel	BZ#1961092
lsvpd	BZ#1869564
lvm2	BZ#1899214, BZ#1749513, BZ#2038183
mariadb	BZ#1971248
mod_security_crs	BZ#1947962

Composant	Billets
nettle	BZ#1986712
nfs-utils	BZ#2059245
nginx	BZ#1953639
nmstate	BZ#1969941
nodejs	BZ#1953491
nss	BZ#2008320, BZ#2099438
numatop	BZ#1874125
nvml	BZ#1874208
opal-prd	BZ#1869560
open-vm-tools	BZ#2037657
opencryptoki	BZ#1869533
openscap	BZ#2041782
openssh	BZ#1952957, BZ#2002734, BZ#1821501, BZ#2087121
openssl	BZ#1990814, BZ#1871147, BZ#1970388, BZ#1975836, BZ#1681178, BZ#1685470, BZ#2053289, BZ#2087253, BZ#2060044, BZ#2071631
osbuild-composer	BZ#2060575
oscap-anaconda-addon	BZ#1893753
ostree	BZ#1961254
p11-kit	BZ#1966680
pacemaker	BZ#1850145, BZ#1443666, BZ#1470834, BZ#1082146, BZ#1376538, BZ#1975388
pcp	BZ#1991764, BZ#1847808, BZ#1981223
pcs	BZ#1290830, BZ#1909901, BZ#1872378, BZ#2018969, BZ#1996067

Composant	Billets
perl-Module-Signature	BZ#2039361
php	BZ#1949319
pki-core	BZ#2084181
podman	JIRA:RHELPLAN-77549, JIRA:RHELPLAN-75322, JIRA:RHELPLAN-108830, BZ#2027576
powerpc-utils	BZ#1873868
ppc64-diag	BZ#1869567
python-jsonpointer	BZ#1980256
python-podman	BZ#1975462
qemu-kvm	BZ#1940132, BZ#1939509, JIRA:RHELPLAN-75866, BZ#1874187, BZ#1965079, BZ#1951814, BZ#2014229, BZ#2052424, BZ#1817965
redis	BZ#1959756
rhel-system-roles	BZ#1993304, BZ#1993377, BZ#2022461, BZ#1978488, BZ#1984583, BZ#2016517, BZ#2021667, BZ#1986460, BZ#1978752, BZ#1978753, BZ#1990490, BZ#2031555, BZ#2016518, BZ#2054364, BZ#1978773, BZ#2054435, BZ#1999162, BZ#2057657, BZ#2012298, BZ#2021028, BZ#2054367, BZ#2054369, BZ#2057662, BZ#2021665, BZ#2029427, BZ#2004899, BZ#1958964, BZ#1978734, BZ#1978760, BZ#2039106, BZ#2041632, BZ#2058777, BZ#2058645, BZ#2058756, BZ#2071804, BZ#2029634, BZ#2044408, BZ#2029602, BZ#2038957, BZ#2064391, BZ#2004303, BZ#2006230, BZ#2057164, BZ#2021025, BZ#2021676, BZ#2047506, BZ#2050341, BZ#2050419, BZ#1999770
rpm-ostree	BZ#1961324
rpm	BZ#1942549, BZ#1962234
rsyslog	BZ#2027971, BZ#1992155
rust-toolset	BZ#2002885
s390utils	BZ#1932480
samba	BZ#2013578
scap-security-guide	BZ#2028435, BZ#2014561, BZ#2045341, BZ#2038978

Composant	Billets
selinux-policy	BZ#2055822, BZ#1932752, BZ#2021529, BZ#2064274
shadow-utils	BZ#1859252
sos	BZ#2011537, BZ#1869561
squid	BZ#1990517
sssd	BZ#1949149, BZ#2014249, BZ#1879869, BZ#1737489
strace	BZ#2038965
stratisd	BZ#2041558
stunnel	BZ#2039299
subscription-manager	BZ#1898563, BZ#2049441
sudo	BZ#1981278
swig	BZ#1943580
systemd	BZ#2018112
systemtap	BZ#2083727
tigervnc	BZ#2060308
trace-cmd	BZ#1933980
tuned	BZ#2003838
unbound	BZ#2070495
usbguard	BZ#1986785, BZ#2009226
varnish	BZ#1984185
virt-manager	BZ#1995131
virt-who	BZ#2008215, BZ#2054504
virtio-win	BZ#1969724
wpa_supplicant	BZ#1975718

Composant	Billets
autres	BZ#2077836, BZ#2019806, BZ#1937651,BZ#2010291, BZ#1941810, BZ#2091643, BZ#1941595, JIRA:RHELPLAN-80758, JIRA :RHELPLAN-80759, JIRA:RHELPLAN-82578, JIRA:RHELPLAN-68364, JIRA:RHELPLAN-78673, JIRA:RHELPLAN-78675, BZ#1940863, BZ#2079313, JIRA :RHELPLAN-100497, BZ#2068532,BZ#2089193, JIRA:RHELPLAN-102009, BZ#2065646, BZ#2088414, JIRA:RHELPLAN-80734, BZ#2013853, JIRA :RHELPLAN-103540, BZ#2019341, BZ#2008558, BZ#2008575, BZ#2009455, JIRA:RHELPLAN-74542, JIRA:RHELPLAN-73678, JIRA :RHELPLAN-84168, JIRA:RHELPLAN-73697, JIRA:RHELPLAN-95126, BZ#2080875, JIRA:RHELPLAN-97899, JIRA:RHELPLAN-100359, JIRA:RHELPLAN-103147, JIRA:RHELPLAN-103146, JIRA:RHELPLAN-79161, BZ#2046325, BZ#2021262, JIRA:RHELPLAN-64576, JIRA :RHELPLAN-65223, BZ#2083036, BZ#2011448, BZ#2019318, JIRA:RHELPLAN-101240, JIRA:RHELPLAN-101241, JIRA:RHELPLAN-101242, JIRA :RHELPLAN-101246, JIRA:RHELPLAN-101247, JIRA:RHELPLAN-102552, JIRA:RHELPLAN-99892, BZ#2027596, JIRA:RHELPLAN-119000, BZ#1940653, JIRA :RHELPLAN-95056, BZ#2054401, JIRA:RHELPLAN-113994, BZ#2059183, JIRA:RHELPLAN-74543, JIRA:RHELPLAN-99889, JIRA:RHELPLAN-99890, JIRA:RHELPLAN-100032, JIRA:RHELPLAN-100034, JIRA:RHELPLAN-101141, JIRA:RHELPLAN-100020, BZ#2069501, BZ#2070506, JIRA :RHELPLAN-117903, JIRA:RHELPLAN-98617, JIRA:RHELPLAN-103855, BZ#2091653, BZ#2082306, JIRA:RHELPLAN-65217, BZ#2020529, BZ#2030412, BZ#2046653, JIRA :RHELPLAN-103993, JIRA:RHELPLAN-122345, BZ#1927780, JIRA:RHELPLAN-110763, BZ#1935544, BZ#2089200, JIRA :RHELPLAN-15509, JIRA:RHELPLAN-99136, JIRA:RHELPLAN-103232, BZ#1899167, BZ#1979521, JIRA:RHELPLAN-100087, JIRA:RHELPLAN-100639, JIRA:RHELPLAN-10304, BZ#2058153, JIRA:RHELPLAN-113995, JIRA:RHELPLAN-121048, JIRA :RHELPLAN-98983, BZ#1640697, BZ#1697896, BZ#2020026, BZ#2047713, JIRA:RHELPLAN-109067, JIRA:RHELPLAN-115603, JIRA:RHELPLAN-96940, JIRA :RHELPLAN-117234, JIRA:RHELPLAN-119001, JIRA:RHELPLAN-119852, BZ#2077767, BZ#2053598, JIRA:RHELPLAN-121180, BZ#2082303, JIRA:RHELPLAN-121049

ANNEXE B. REMERCIEMENTS

Nous remercions les Associés Red Hat ci-dessous qui ont fourni des commentaires dans le cadre du défi de préparation à RHEL 9 :

- Buland Singh
- Pradeep Jagtap
- Omkar Andhekar
- Ju Ke
- Suresh Jagtap
- Prijesh Patel
- Nikhil Suryawanshi
- Amit Yadav
- Pranav Lawate
- John Pittman

ANNEXE C. HISTORIQUE DES RÉVISIONS

0.1-16

Jeu. 18 mai 2023, Gabi Fialova(gfialova@redhat.com)

- Ajout d'une amélioration BZ#2053642 (Système de fichiers et stockage).

0.1-15

Mercredi 17 mai 2023, Gabi Fialova(gfialova@redhat.com)

- Mise à jour du fichier deprecated-packages.adoc avec des informations sur la fin de vie.

0.1-14

Jeu. 11 mai 2023, Gabi Fialova(gfialova@redhat.com)

- Ajout d'une amélioration BZ#2190045 (Installer).

0.1-13

Jeu. 27 avril 2023, Gabi Fialova(gfialova@redhat.com)

- Ajout d'un problème connu JIRA:RHELPLAN-155168 (Identity Management).

0.1-12

Jeu. 13 avril 2023, Gabi Fialova(gfialova@redhat.com)

- Corriger un lien brisé dans une nouvelle fonctionnalité JIRA:RHELPLAN-84168 (Conteneurs).

0.1-11

Mercredi 1er mars 2023, Gabi Fialova(gfialova@redhat.com)

- Modification du texte de la documentation pour BZ#2091643 (Kernel).

0.1-10

Lun Fév 20, 2023, Gabi Fialova(gfialova@redhat.com)

- Ajout d'informations dans "Mise à niveau en place de RHEL 8 à RHEL 9" à propos des environnements SAP.

0.1-9

Mer Jan 18, 2023, Gabi Fialova(gfialova@redhat.com)

- Ajout d'un document sur les problèmes connus BZ#2083106 (Kernel).

0.1-8

Mar Jan 17, 2023, Gabi Fialova(gfialova@redhat.com)

- Mise à jour d'un texte de Tech Preview BZ#2084181 (Identity Management).

0.1-7

Lun Jan 16, 2023, Gabi Fialova(gfialova@redhat.com)

- Ajout d'un document sur les problèmes connus BZ#2149172 (Kernel).

0.1-6

Jeu. 22 déc. 2022, Gabi Fialova(gfialova@redhat.com)

- Mise à jour du texte d'un problème connu BZ#1960467 (Infrastructures graphiques).

0.1-5

Jeu. 08 Déc. 2022, Marc Muehlfeld(mmuehlfeld@redhat.com)

- Ajout d'un problème connu BZ#2151040 (réseau).

0.1-4

Mar. 15 nov. 2022, Gabriela Fialová(gfialova@redhat.com)

- Mise à jour de la section " Mise à niveau en place" .

0.1-3

Ven Sep 23, 2022, Gabriela Fialová(gfialova@redhat.com)

- Ajout d'une fonctionnalité obsolète BZ#2074598 (Kernel).

0.1-2

Mercredi 21 septembre 2022, Gabriela Fialová(gfialova@redhat.com)

- Suppression d'un problème connu BZ#2060798 (gestion des identités).
- Ajout d'une correction de bug BZ#2060798 (Identity Management).

0.1-1

Lun. 12 Sep. 2022, Gabriela Fialová(gfialova@redhat.com)

- Mise à jour de proc_providing-feedback-on-red-hat-documentation.adoc.
- Ajout d'une amélioration BZ#2119694 (Sécurité).

0.1-0

Lun Août 22, 2022, Lenka Špačková(lspackova@redhat.com)

- Ajout des fonctionnalités obsolètes BZ#2069279 et BZ#2106816 (conteneurs).
- Mise à jour de JIRA-RHELPLAN-121180 avec des informations sur une correction de z-stream (Conteneurs).

0.0-9

Mer Août 10, 2022, Lenka Špačková(lspackova@redhat.com)

- Ajout d'un problème connu BZ#1991500 (Langages de programmation dynamiques, serveurs web et de base de données).

0.0-8

Jeu. Août 4, 2022, Gabriela Fialová(gfialova@redhat.com)

- Ajout d'une amélioration JIRA-RHELPLAN-118914 (Conteneurs).
- Ajout d'un problème connu BZ#2105162 (Sécurité).
- Ajout d'un problème connu BZ#1960467 (Infrastructures graphiques).

0.0-7

Jeu. 28 Juil. 2022, Lenka Špačková(lspackova@redhat.com)

- Ajout d'une amélioration BZ#2099438 (Sécurité).
- Ajout d'un problème connu BZ#2087253 (Sécurité).
- Informations complémentaires sur les flux d'applications dans Distribution.

0.0-6

Lun Juil 11, 2022, Lenka Špačková(lspackova@redhat.com)

- Ajout d'un problème connu BZ#2077450.
- Ajout d'une amélioration BZ#2091653.
- Ajout d'une correction de bug BZ#2006230.

0.0-5

Mer Juin 29, 2022, Lenka Špačková(lspackova@redhat.com)

- Ajout des problèmes connus BZ#2087121, BZ#2073567, BZ#2083727, et BZ#2005173.
- Ajout d'une amélioration BZ#2091643.

0.0-4

Wed Jun 1, 2022, Gabriela Fialová(gfialova@redhat.com)

- Ajout d'un problème connu BZ#2027576.

0.0-3

Mar. 24 mai 2022, Gabriela Fialová(gfialova@redhat.com)

- Mise à jour de la liste des dix laboratoires de portail client les plus populaires.
- Ajout et republication d'une fonctionnalité obsolète BZ#2089200 (réseau).

0.0-2

Mercredi 18 mai 2022, Gabriela Fialová(gfialova@redhat.com)

- Publication des notes de mise à jour de Red Hat Enterprise Linux 9.0.

0.0-1

Mer. 03 nov. 2021, Lenka Špačková(lspackova@redhat.com)

- Publication des notes de mise à jour de Red Hat Enterprise Linux 9.0 Beta.