Red Hat Enterprise Linux 9

9.2 Notes de mise à jour

Notes de mise à jour pour Red Hat Enterprise Linux 9.2

Last Updated: 2023-06-12

Red Hat Enterprise Linux 9 9.2 Notes de mise à jour

Notes de mise à jour pour Red Hat Enterprise Linux 9.2

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 9.2 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 la fenêtre **Add Feedback** qui apparaît près du texte en surbrillance.
    4. Ajoutez vos commentaires et cliquez sur **Submit**.

- Soumettre un retour d'information via Bugzilla (action requise) :

    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. Cliquez sur **Submit Bug**.

CHAPITRE 1. VUE D'ENSEMBLE

1.1. PRINCIPAUX CHANGEMENTS DANS RHEL 9.2

Création d'installateurs et d'images

Principales caractéristiques du constructeur d'images :

- Image builder on-prem offre désormais une nouvelle façon améliorée de créer des plans et des images dans la console web d'Image builder.
- La création de fichiers et de répertoires personnalisés dans le répertoire **/etc** est désormais possible.
- Le type d'image RHEL for Edge Simplified Installer est désormais disponible dans la console web de création d'images.

Pour plus d'informations, voir Nouvelles fonctionnalités - Installateur et création d'images .

RHEL pour Edge

Principales caractéristiques de RHEL for Edge :

- La spécification d'un utilisateur dans un plan pour les images **simplified-installer** est désormais prise en charge.
- L'utilitaire de provisionnement Ignition est désormais pris en charge dans les images RHEL for Edge Simplified.
- Les images de l'installateur simplifié peuvent désormais être composées sans la section de personnalisation FDO dans le plan.

Pour plus d'informations, voir Nouvelles fonctionnalités - RHEL for Edge .

Sécurité

Principaux faits marquants en matière de sécurité :

- La bibliothèque de communications sécurisées **OpenSSL** est passée à la version 3.0.7.
- **SELinux user-space** ont été mis à jour vers la version 3.5.
- **Keylime** est passé à la version 6.5.2
- **OpenSCAP** est passé à la version 1.3.7.
- **SCAP Security Guide** est passé à la version 0.1.66.
- Une nouvelle règle pour la fin de session inactive a été ajoutée au guide de sécurité SCAP.
- **Clevis** accepte désormais les jetons externes.
- **Rsyslog** La journalisation cryptée TLS prend désormais en charge plusieurs fichiers d'autorité de certification.
- Les privilèges Rsyslog sont limités afin de minimiser l'exposition à la sécurité.
- Le cadre **fapolicyd** permet désormais de filtrer la base de données RPM.

Voir Nouveautés - Sécurité pour plus d'informations.

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

Des versions plus récentes des flux d'applications suivants sont désormais disponibles :

- **Python 3.11**
- **nginx 1.22**
- **PostgreSQL 15**

Les composants suivants ont été mis à jour :

- **Git** à la version 2.39.1
- **Git LFS** à la version 3.2.0

Pour plus d'informations, voir Nouveautés - Langages de programmation dynamiques, serveurs web et de base de données.

Compilateurs et outils de développement

Mise à jour de la chaîne d'outils système

Les composants suivants de la chaîne d'outils système ont été mis à jour dans RHEL 9.2 :

- **GCC 11.3.1**
- **glibc 2.34**
- **binutils 2.35.2**

Mise à jour des outils de performance et des débogueurs

Les outils de performance et les débogueurs suivants ont été mis à jour dans RHEL 9.2 :

- **GDB 10.2**
- **Valgrind 3.19**
- **SystemTap 4.8**
- **Dyninst 12.1.0**
- **elfutils 0.188**

Mise à jour des outils de contrôle des performances

Les outils de surveillance des performances suivants ont été mis à jour dans RHEL 9.2 :

- **PCP 6.0.1**
- **Grafana 9.0.9**

Mise à jour des outils de compilation

Les ensembles d'outils de compilation suivants ont été mis à jour dans RHEL 9.2 :

- **GCC Toolset 12**
- **LLVM Toolset 15.0.7**
- **Rust Toolset 1.66**

- Go Toolset 1.19.6

Pour plus de détails sur les changements, voir Nouvelles fonctionnalités - 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.

Les paquets OpenJDK de Red Hat partagent un ensemble unique de binaires entre ses versions Linux portables et RHEL 9.2 et les versions ultérieures. Avec cette mise à jour, il y a un changement dans le processus de reconstruction des paquets OpenJDK sur RHEL à partir du RPM source. Pour plus d'informations sur le nouveau processus de reconstruction, consultez le fichier README.md qui est disponible dans le paquet SRPM de la version Red Hat d'OpenJDK et qui est également installé par les paquets **java-*-openjdk-headless** sous l'arbre **/usr/share/doc**.

Pour plus d'informations, voir la documentation OpenJDK.

La console web

La console Web RHEL exécute désormais des étapes supplémentaires pour lier les volumes racine chiffrés LUKS aux déploiements **NBDE**.

Vous pouvez également appliquer les **cryptographic subpolicies** suivants par l'intermédiaire de l'interface graphique : **DEFAULT:SHA1**, **LEGACY:AD-SUPPORT**, et **FIPS:OSPP**.

Voir Nouveautés - La console web pour plus d'informations.

Conteneurs

Les changements les plus notables sont les suivants :

- Le rôle de système RHEL **podman** est désormais disponible.
- Les clients pour les signatures sigstore avec Fulcio et Rekor sont maintenant disponibles.
- Skopeo permet désormais de générer des paires de clés sigstore.
- Podman prend désormais en charge les événements pour l'audit.
- Les paquets Container Tools ont été mis à jour.
- La pile de réseaux Aardvark et Netavark prend désormais en charge la sélection de serveurs DNS personnalisés.
- La boîte à outils est désormais disponible.
- Podman Quadlet est maintenant disponible en tant qu'aperçu technologique.
- La pile réseau CNI a été supprimée.

Voir Nouveautés - Conteneurs pour plus d'informations.

1.2. MISE À NIVEAU SUR PLACE

Mise à niveau en place de RHEL 8 à RHEL 9

Les chemins de mise à niveau en place pris en charge sont actuellement les suivants :

- De RHEL 8.6 à RHEL 9.0 et de RHEL 8.8 à RHEL 9.2 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.

Parmi les améliorations notables, citons

- La stratégie de chemin de mise à niveau sur site de RHEL a changé. Pour plus d'informations, voir Chemins de mise à niveau sur site pris en charge pour Red Hat Enterprise Linux .
- Avec la sortie de RHEL 9.2, plusieurs chemins de mise à niveau sont désormais disponibles pour la mise à niveau en place de RHEL 8 vers RHEL 9. Pour la version actuelle, il est possible d'effectuer une mise à niveau en place de RHEL 8.8 vers RHEL 9.2, ou de RHEL 8.6 vers RHEL 9.0. Notez que les chemins de mise à niveau disponibles diffèrent entre les systèmes RHEL standard et les systèmes RHEL avec SAP HANA.
- Les mises à niveau sur place à l'aide d'une image ISO contenant la version cible sont désormais possibles.
- Les signatures des RPM sont désormais automatiquement vérifiées lors de la mise à niveau sur place. Pour désactiver la vérification automatique, utilisez l'option **--nogpgcheck** lors de la mise à niveau.
- Les systèmes qui sont abonnés à RHSM sont désormais automatiquement enregistrés dans Red Hat Insights. Pour désactiver l'enregistrement automatique, définissez la variable d'environnement **LEAPP_NO_INSIGHTS_REGISTER** sur **1**.
- Red Hat collecte désormais les données relatives aux mises à niveau, telles que les heures de début et de fin de la mise à niveau et la réussite ou non de la mise à niveau, pour l'analyse de l'utilisation des utilitaires. Pour désactiver la collecte de données, définissez la variable d'environnement **LEAPP_NO_RHSM_FACTS** sur **1**.

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 9.2 est distribué avec la version 5.14.0-284.11.1 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)

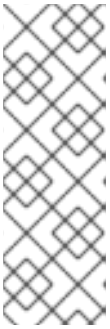
Assurez-vous d'acheter l'abonnement approprié pour chaque architecture. Pour plus d'informations, voir Démarrer avec Red Hat Enterprise Linux - architectures supplémentaires .

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 9.2.

4.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

Une nouvelle façon améliorée de créer des plans et des images dans la console web du constructeur d'images

Grâce à cette amélioration, vous avez accès à une version unifiée de l'outil de création d'images et vous bénéficiez d'une amélioration significative de votre expérience utilisateur.

Les améliorations notables apportées à l'interface graphique du tableau de bord du constructeur d'images sont les suivantes :

- Vous pouvez désormais personnaliser vos plans avec toutes les personnalisations qui n'étaient auparavant prises en charge que dans l'interface de programmation, telles que le noyau, le système de fichiers, le pare-feu, les paramètres linguistiques et d'autres personnalisations.
- Vous pouvez importer des plans en les téléchargeant ou en les faisant glisser au format **.JSON** ou **.TOML** et créer des images à partir des plans importés.
- Vous pouvez également exporter ou enregistrer vos plans au format **.JSON** ou **.TOML**.
- Accès à une liste de plans que vous pouvez trier, filtrer et qui tient compte des majuscules et des minuscules.
- Avec le tableau de bord du constructeur d'images, vous pouvez désormais accéder à vos plans, images et sources en naviguant dans les onglets suivants :
  - Blueprint - Sous l'onglet Blueprint, vous pouvez désormais importer, exporter ou supprimer vos blueprints.
  - Images - Sous l'onglet Images, vous pouvez :
    - Télécharger les images.
    - Télécharger les journaux d'images.
    - Supprimer des images.
  - Sources - Sous l'onglet Sources, vous pouvez :
    - Télécharger les images.
    - Télécharger les journaux d'images.
    - Créer des sources pour les images.
    - Supprimer des images.

Jira:RHELPLAN-139448

Possibilité de créer des fichiers et des répertoires personnalisés dans le répertoire `/etc`

Avec cette amélioration, deux nouvelles personnalisations de plans sont disponibles. Les

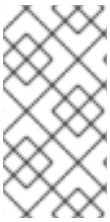
personnalisations **[[customizations.files]]** et **[[customizations.directories]]** vous permettent de créer des fichiers et des répertoires personnalisés dans le répertoire /**etc** de votre image. Actuellement, vous ne pouvez utiliser ces personnalisations que dans le répertoire /**etc**.

Le site **[[customizations.directories]]** vous permet de

- Créer de nouveaux répertoires
- Définir la propriété de l'utilisateur et du groupe pour le répertoire
- Définir l'autorisation de mode au format octal

Avec les personnalisations de **[[customizations.files]]** blueprint, vous pouvez :

- Créer de nouveaux fichiers sous le répertoire parent /
- Modifier des fichiers existants - cela remplace le contenu existant
- Définir la propriété de l'utilisateur et du groupe pour le fichier que vous créez
- Définir l'autorisation de mode au format octal



NOTE

Les nouvelles personnalisations des modèles sont prises en charge par tous les types d'images, tels que **edge-container**, **edge-commit**, entre autres. Les personnalisations ne sont pas prises en charge dans les blueprints utilisés pour créer les images Installer, telles que **edge-raw-image**, **edge-installer**, et **edge-simplified-installer**.

Jira:RHELPLAN-147428

Possibilité de spécifier l'utilisateur dans un plan pour les images simplified-installer

Auparavant, lors de la création d'un plan pour une image d'installateur simplifié, vous ne pouviez pas spécifier un utilisateur dans la personnalisation du plan, car la personnalisation n'était pas utilisée et était rejetée. Avec cette mise à jour, lorsque vous créez une image à partir d'un modèle, celui-ci crée un utilisateur dans le répertoire **/usr/lib/passwd** et un mot de passe dans le répertoire **/usr/etc/shadow** lors de l'installation. Vous pouvez vous connecter à l'appareil avec le nom d'utilisateur et le mot de passe que vous avez créés pour le projet. Notez qu'après avoir accédé au système, vous devez créer des utilisateurs, par exemple à l'aide de la commande **useradd**.

Jira:RHELPLAN-149091

Prise en charge de l'architecture ARM 64 bits pour les images .vhd créées à l'aide de l'outil de création d'images

Auparavant, les images Microsoft Azure **.vhd** créées avec l'outil de construction d'images n'étaient pas prises en charge sur les architectures ARM 64 bits. Cette mise à jour ajoute la prise en charge des images ARM 64 bits de Microsoft Azure **.vhd**. Vous pouvez désormais créer vos images **.vhd** à l'aide de l'outil de création d'images et les télécharger vers le nuage Microsoft Azure.

Jira:RHELPLAN-139424

L'installation minimale de RHEL n'installe plus que le paquet s390utils-core

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, si vous définissez l'installation RHEL sur

minimal-environment, vous n'installez que le paquet **s390utils-core** nécessaire et non le paquet auxiliaire **s390utils-base**. Si vous souhaitez utiliser le paquet **s390utils-base** avec une installation RHEL minimale, vous devez installer manuellement le paquet après avoir terminé l'installation RHEL ou installer explicitement **s390utils-base** à l'aide d'un fichier kickstart.

Bugzilla:1932480

4.2. RHEL POUR EDGE

Prise en charge d'Ignition dans RHEL pour les images simplifiées Edge

Grâce à cette amélioration, vous pouvez ajouter un fichier Ignition aux images de l'installateur simplifié en personnalisant votre plan. L'interface graphique et l'interface de commande sont toutes deux compatibles avec la personnalisation d'Ignition. RHEL for Edge utilise l'utilitaire de provisionnement Ignition pour injecter la configuration de l'utilisateur dans les images à un stade précoce du processus de démarrage. Au premier démarrage, Ignition lit sa configuration à partir d'une URL distante ou d'un fichier intégré dans l'image de l'installateur simplifié et applique cette configuration à l'image.

Jira:RHELPLAN-139659

Les images de l'installateur simplifié peuvent désormais être composées sans la section de personnalisation FDO dans le plan

Auparavant, pour créer une image RHEL for Edge Simplified Installer, vous deviez ajouter des détails à la section de personnalisation FIDO device onboarding (FDO). Dans le cas contraire, la création de l'image échouait. Avec cette mise à jour, la personnalisation FDO dans les blueprints est désormais facultative et vous pouvez créer une image RHEL for Edge Simplified Installer sans erreur.

Jira:RHELPLAN-139655

Red Hat construit l'activation de MicroShift pour les images RHEL for Edge

Avec cette amélioration, vous pouvez activer la construction Red Hat des services MicroShift dans un système RHEL for Edge. En utilisant la personnalisation du blueprint **[[customizations.firewalld.zones]]**, vous pouvez ajouter la prise en charge des sources **firewalld** dans la personnalisation du blueprint. Pour cela, spécifiez un nom pour la zone et une liste de sources dans cette zone spécifique. Les sources peuvent être de la forme **source[/mask]|MAC|ipset:ipset**.

L'exemple suivant montre comment configurer et personnaliser la prise en charge des services MicroShift pour Red Hat dans un système RHEL for Edge.

```
[[packages]]
name = "microshift"
version = "*"
[customizations.services]
enabled = ["microshift"]
[[customizations.firewall.zones]]
name = "trusted"
sources = ["10.42.0.0/16", "169.254.169.1"]
```

La version Red Hat des exigences d'installation de MicroShift, telles que les politiques de pare-feu, MicroShift RPM, **systemd** service, vous permet de créer un déploiement prêt pour la production afin de réaliser la portabilité de la charge de travail à un minimum d'appareil périphérique déployé sur le terrain et par défaut l'activation du mappeur d'appareil LVM.

Jira:RHELPLAN-136489

4.3. GESTION DES LOGICIELS

Nouvelle commande dnf offline-upgrade pour les mises à jour hors ligne sur RHEL

Grâce à cette amélioration, vous pouvez appliquer des mises à jour hors ligne à RHEL en utilisant la nouvelle commande **dnf offline-upgrade** du plug-in DNF **system-upgrade**.

IMPORTANT

La commande **dnf system-upgrade** incluse dans le plug-in **system-upgrade** n'est pas prise en charge sur RHEL.

Bugzilla:2131288

L'application de filtres de sécurité consultatifs à dnf offline-upgrade est désormais prise en charge

Avec cette amélioration, la nouvelle fonctionnalité de filtrage des avis a été ajoutée. Par conséquent, vous pouvez désormais télécharger des paquets et leurs dépendances uniquement à partir de l'avis spécifié en utilisant la commande **dnf offline-upgrade** avec les filtres de sécurité de l'avis (**--advisory**, **--security**, **--bugfix**, et d'autres filtres).

Bugzilla:2139326

La fonction unload_plugins est maintenant disponible pour l'API DNF

Avec cette amélioration, une nouvelle fonction **unload_plugins** a été ajoutée à l'API DNF pour permettre le déchargement des plug-ins.

IMPORTANT

Notez que vous devez d'abord exécuter la fonction **init_plugins**, puis la fonction **unload_plugins**.

Bugzilla:2121662

Nouvelle option --nocompression pour rpm2archive

Avec cette amélioration, l'option **--nocompression** a été ajoutée à l'utilitaire **rpm2archive**. Vous pouvez utiliser cette option pour éviter la compression lors du décompactage direct d'un paquetage RPM.

Bugzilla:2150804

4.4. SHELLS ET OUTILS DE LIGNE DE COMMANDE

ReaR est désormais entièrement pris en charge sur l'architecture IBM Z 64 bits

La fonctionnalité de base Relax and Recover (ReaR), précédemment disponible sur l'architecture IBM Z 64 bits en tant qu'aperçu technologique, est entièrement prise en charge avec le paquetage **rear** version 2.6-17.el9 ou ultérieure. Vous pouvez créer une image de secours ReaR sur l'architecture IBM Z dans l'environnement z/VM uniquement. La sauvegarde et la restauration des partitions logiques (LPAR) ne sont pas prises en charge pour le moment. ReaR prend en charge la sauvegarde et la restauration de l'agencement du disque uniquement sur les périphériques de stockage à accès direct (DASD) Extended Count Key Data (ECKD). Les DASD à accès par bloc fixe (FBA) et les disques SCSI

attachés via le protocole Fibre Channel (FCP) ne sont pas pris en charge à cette fin. La seule méthode de sortie actuellement disponible est Initial Program Load (IPL), qui produit un noyau et un ramdisk initial (initrd) compatible avec le bootloader **zIPL**.

Pour plus d'informations, voir Utilisation d'une image de secours ReaR sur l'architecture IBM Z 64 bits .

Bugzilla:2046653

4.5. SERVICES D'INFRASTRUCTURE

chrony repassé à la version 4.3

La suite **chrony** a été mise à jour à la version 4.3. Les améliorations notables par rapport à la version 4.2 sont les suivantes :

- Ajout d'un filtrage à long terme basé sur le quantile des mesures NTP (Network Time Protocol). Vous pouvez activer cette fonctionnalité en ajoutant l'option **maxdelayquant** à la directive **pool**, **server** ou **peer**.
- Ajout du journal de sélection pour fournir plus d'informations sur la sélection des sources à l'adresse **chronyd**. Vous pouvez activer le journal de sélection en ajoutant l'option **selection** à la directive **log**.
- Amélioration de la stabilité de la synchronisation lors de l'utilisation de l'horodatage matériel et des horloges de référence PHC (Pulse-Per-Second Hardware Clock).
- Ajout de la prise en charge de la stabilisation de l'horloge système à l'aide d'une horloge stable fonctionnant librement, par exemple un oscillateur à cristal compensé en température (TCXO), un oscillateur à cristal contrôlé par le four (OCXO) ou une horloge atomique.
- Augmentation du taux d'interrogation maximal à 128 messages par seconde.

Bugzilla:2133754

frr repassé à la version 8.3.1

Le paquetage **frr** pour la gestion de la pile de routage dynamique a été mis à jour à la version 8.3.1. Les changements notables par rapport à la version 8.2.2 sont les suivants :

- Ajout d'un nouvel ensemble de commandes pour interagir avec le protocole BGP (Border Gateway Protocol) :
  - la commande **set as-path replace** pour remplacer l'attribut AS path (Autonomous System) d'une route BGP par une nouvelle valeur.
  - la commande **match peer** pour faire correspondre un pair ou un groupe BGP spécifique lors de la configuration d'une feuille de route BGP.
  - la commande **ead-es-frag evi-limit** pour définir une limite sur le nombre de fragments Ethernet A-D par EVI qui peuvent être envoyés dans une période de temps donnée dans EVPN.
  - la commande **match evpn route-type** pour prendre des mesures spécifiques sur certains types de routes EVPN, telles que route-target, route-distinguisher ou routes MAC/IP.
- Ajout de la commande **show thread timers** dans l'interface de ligne de commande VTYSH pour interagir avec les démons FRR.

- Ajout de la commande **show ip ospf reachable-routers** pour afficher la liste des routeurs actuellement joignables via le protocole OSPF.
- Ajout de nouvelles commandes pour interagir avec le démon Protocol Independent Multicast (PIM) :
  - la commande **debug igmp trace detail** pour activer le débogage des messages du protocole de gestion des groupes Internet (IGMP) avec un suivi détaillé.
  - la commande **ip pim passive** pour configurer l'interface comme passive, n'envoyant pas de messages PIM.
- Ajout de nouvelles sorties pour la commande **show zebra**, telles que les statuts ECMP, EVPN, MPLS.
- Ajout de la commande **show ip nht mrib** au composant ZEBRA pour afficher les informations relatives au multicast à partir de la table **mroute** dans le noyau.

Bugzilla:2129731

vsftpd repassé à la version 3.0.5

Le démon FTP très sécurisé (**vsftpd**) fournit une méthode sécurisée de transfert de fichiers entre hôtes. Le paquetage **vsftpd** a été mis à jour à la version 3.0.5. Les changements et améliorations notables incluent les modernisations SSL suivantes :

- Par défaut, l'utilitaire **vsftpd** exige désormais l'utilisation de TLS version 1.2 ou ultérieure pour les connexions sécurisées.
- L'utilitaire **vsftpd** est désormais compatible avec la dernière version du client FileZilla.

Bugzilla:2018284

Le paquet frr contient désormais une politique SELinux ciblée

En raison du développement rapide du paquetage **frr** pour la gestion de la pile de routage dynamique, de nouvelles fonctionnalités et des problèmes de cache de vecteur d'accès (AVC) sont apparus fréquemment. Grâce à cette amélioration, les règles SELinux sont désormais intégrées au FRR afin de résoudre les problèmes plus rapidement. SELinux ajoute un niveau de protection supplémentaire au paquet en appliquant des politiques de contrôle d'accès obligatoires.

Bugzilla:2129743

powertop repassé à la version 2.15

Le paquet **powertop** pour l'amélioration de l'efficacité énergétique a été mis à jour à la version 2.15. Les changements et améliorations notables sont les suivants :

- Plusieurs erreurs Valgrind et un possible dépassement de tampon ont été corrigés pour améliorer la stabilité de l'outil **powertop**.
- Amélioration de la compatibilité avec les processeurs Ryzen et les plateformes Kaby Lake.
- Prise en charge des plates-formes Lake Field, Alder Lake N et Raptor Lake.
- Prise en charge des applications mobiles et de bureau Ice Lake NNPI et Meteor Lake.

Bugzilla:2044132

L'utilitaire systemd-sysusers est disponible dans les paquets chrony, dhcp, radvd et squid

L'utilitaire **systemd-sysusers** crée des utilisateurs et des groupes système lors de l'installation du paquet et les supprime lors de la suppression du paquet. Avec cette amélioration, les paquets suivants contiennent l'utilitaire **systemd-sysusers** dans leurs scriptlets :

- **chrony**,
- **dhcp**,
- **radvd**,
- **squid**.

Jira:RHELPLAN-136485

Le nouveau paquet synce4l pour la synchronisation des fréquences est maintenant disponible

SyncE (Synchronous Ethernet) est une fonction matérielle qui permet aux horloges PTP de réaliser une synchronisation précise de la fréquence au niveau de la couche physique. SyncE est pris en charge par certaines cartes d'interface réseau (NIC) et certains commutateurs de réseau.

Avec cette amélioration, le nouveau paquetage **synce4l** est désormais disponible et prend en charge SyncE. Par conséquent, les applications de réseau d'accès radio (RAN) des entreprises de télécommunication peuvent désormais communiquer plus efficacement grâce à une synchronisation temporelle plus précise.

Bugzilla:2143264

tuned repassé à la version 2.20.0

L'utilitaire TuneD, qui permet d'optimiser les performances des applications et des charges de travail, a été mis à jour avec la version 2.20.0. Les changements et améliorations notables par rapport à la version 2.19.0 sont les suivants :

- Une extension de l'API permet de déplacer des appareils entre les instances de plug-in au moment de l'exécution.
- Le module **plugin_cpu**, qui permet d'affiner les paramètres de performance liés au processeur, apporte les améliorations suivantes :
  - La fonction **pm_qos_resume_latency_us** vous permet de limiter le temps maximum alloué à chaque unité centrale pour passer d'un état d'inactivité à un état d'activité.
  - TuneD ajoute la prise en charge du pilote de mise à l'échelle **intel_pstate**, qui fournit des algorithmes de mise à l'échelle pour ajuster la gestion de l'énergie des systèmes en fonction de différents scénarios d'utilisation.
- L'API de socket pour contrôler TuneD à travers un socket de domaine Unix est maintenant disponible en tant qu'aperçu technologique. Voir Socket API for TuneD available as a Technology Preview pour plus d'informations.

Bugzilla:2133815, Bugzilla :2118786, Bugzilla:2095829, Bugzilla:2113925

4.6. SÉCURITÉ

Libreswan rebasé à 4,9

Les paquets **libreswan** ont été mis à jour vers la version 4.9. Les changements notables par rapport à la version précédente sont les suivants :

- Prise en charge des options **{left,right}pubkey=** des utilitaires **addconn** et **whack**
- Autotests du KDF
- Afficher la clé d'authentification de l'hôte (**showhostkey**) :
  - Prise en charge des clés publiques ECDSA
  - Nouvelle option **--pem** pour imprimer la clé publique encodée PEM
- Le protocole d'échange de clés Internet version 2 (IKEv2) :
  - Protocole d'authentification extensible - Sécurité de la couche transport (EAP-TLS)
  - Prise en charge de l'authentification EAP uniquement
- Le démon IKE de **pluto**:
  - Prise en charge des compteurs **maxbytes** et **maxpacket**

Bugzilla:2128669

OpenSSL repassé à la version 3.0.7

Les paquets OpenSSL ont été rebasés vers la version 3.0.7, qui contient plusieurs corrections de bogues et améliorations. En particulier, le fournisseur par défaut inclut désormais la fonction de hachage **RIPEMD160**.

Bugzilla:2129063

libssh prend désormais en charge les cartes à puce

Vous pouvez désormais utiliser des cartes à puce par le biais de l'identificateur de ressources uniformes (URI) #11 de la norme de cryptographie à clé publique (PKCS). Par conséquent, vous pouvez utiliser des cartes à puce avec la bibliothèque SSH **libssh** et avec les applications qui utilisent **libssh**.

Bugzilla:2026449

libssh repassé à la version 0.10.4

La bibliothèque **libssh**, qui implémente le protocole SSH pour l'accès à distance sécurisé et le transfert de fichiers entre machines, a été mise à jour à la version 0.10.4.

Nouvelles fonctionnalités :

- La prise en charge d'OpenSSL 3.0 a été ajoutée.
- La prise en charge des cartes à puce a été ajoutée.
- Deux nouvelles options de configuration **IdentityAgent** et **ModuliFile** ont été ajoutées.

D'autres changements notables sont à signaler :

- Les versions d'OpenSSL antérieures à 1.0.1 ne sont plus prises en charge

- Par défaut, la prise en charge de l'algorithme de signature numérique (DSA) a été désactivée au moment de la construction.
- L'API SCP est obsolète.
- Les API **pubkey** et **privatekey** sont obsolètes.

Bugzilla:2068475

Mise à jour des paquets SELinux pour l'espace utilisateur vers la version 3.5

Les paquets SELinux pour l'espace utilisateur **libselinux**, **libsepol**, **libsemanage**, **checkpolicy**, **mcstrans**, et **policycoreutils**, qui inclut l'utilitaire **sepolicy**, ont été mis à jour vers la version 3.5. Les améliorations notables et les corrections de bogues incluent :

- L'utilitaire **sepolicy**:
  - Ajout des booléens manquants dans les pages de manuel
  - Plusieurs mises à jour de Python et GTK
- Ajout d'une solution de contournement à **libselinux** qui réduit l'utilisation de la mémoire du tas par la bibliothèque **PCRE2**
- Le paquet **libsepol**:
  - Rejette les attributs dans les règles de type AV pour les politiques du noyau
  - N'écrit plus de définitions de classes vides, ce qui permet de simplifier les tests d'aller-retour
  - Une validation plus stricte des politiques
- Le script **fixfiles** démonte les montages bind temporaires sur le signal **SIGINT**
- Correction de nombreux bugs de code et d'orthographe
- Suppression de la dépendance au module Python obsolète **distutils** et de l'installation à l'aide de PIP
- L'option **semodule --rebuild-if-modules-changed** a été renommée en **--refresh**
- Mise à jour des traductions pour les descriptions générées et amélioration de la gestion des langues non prises en charge
- Correction de nombreux bogues d'analyse statique du code, de problèmes de fuzzer et d'avertissements du compilateur

Bugzilla:2145224, Bugzilla:2145230, Bugzilla :2145228, Bugzilla :2145229, Bugzilla :2145226, Bugzilla:2145231

OpenSCAP repassé à la version 1.3.7

Les paquets OpenSCAP ont été rebasés vers la version amont 1.3.7. Cette version apporte diverses corrections de bogues et améliorations, notamment :

- Correction d'une erreur lors du traitement des filtres OVAL(RHBZ#2126882)
- OpenSCAP n'émet plus d'éléments vides invalides sur **xmlfilecontent** si XPath ne correspond pas(RHBZ#2139060)

- Prévention des erreurs **Failed to check available memory** (RHBZ#2111040)

Bugzilla:2159286

Le guide de sécurité SCAP passe à la version 0.1.66

Les paquets du guide de sécurité SCAP (SSG) ont été rebasés vers la version amont 0.1.66. Cette version apporte diverses améliorations et corrections de bogues, notamment :

- Nouveaux profils CIS RHEL9
- Dépréciation de la règle **account_passwords_pam_faillock_audit** en faveur de **accounts_passwords_pam_faillock_audit**

Bugzilla:2158405

Nouvelle règle SCAP pour la fin de session inactive

Une nouvelle règle SCAP **logind_session_timeout** a été ajoutée au paquet **scap-security-guide** dans les profils ANSSI-BP-028 pour les niveaux Enhanced et High. Cette règle utilise une nouvelle fonctionnalité du gestionnaire de services **systemd** et met fin aux sessions utilisateur inactives après un certain temps. Cette règle fournit une configuration automatique d'un mécanisme robuste de fin de session inactive qui est requis par plusieurs politiques de sécurité. Par conséquent, OpenSCAP peut automatiquement vérifier l'exigence de sécurité liée à la fin des sessions utilisateur inactives et, si nécessaire, y remédier.

Bugzilla:2122325

scap-security-guide les règles pour les fichiers journaux Rsyslog sont compatibles avec les journaux RainerScript

Les règles de **scap-security-guide** pour la vérification et la correction de la propriété, de la propriété du groupe et des permissions des fichiers journaux Rsyslog sont désormais également compatibles avec la syntaxe RainerScript. Les systèmes modernes utilisent déjà la syntaxe RainerScript dans les fichiers de configuration Rsyslog et les règles correspondantes n'étaient pas en mesure de reconnaître cette syntaxe. Par conséquent, les règles **scap-security-guide** peuvent désormais vérifier et corriger la propriété, la propriété de groupe et les permissions des fichiers journaux Rsyslog dans les deux syntaxes disponibles.

Bugzilla:2169414

Keylime passe à la version 6.5.2

Les paquets **keylime** ont été rebasés vers la version amont - keylime-6.5.2-5.el9. Cette version contient diverses améliorations et corrections de bogues, notamment les suivantes :

- Corrige la vulnérabilité CVE-2022-3500
- L'agent Keylime n'échoue plus à l'attestation IMA lorsqu'un script est exécuté rapidement après un autre RHBZ#2138167
- Correction d'une erreur de segmentation dans le script **/usr/share/keylime/create_mb_refstate** RHBZ#2140670
- Le bureau d'enregistrement ne se bloque plus pendant la validation de l'EK lorsque l'option **require_ek_cert** est activée RHBZ#2142009

Bugzilla:2150830

Clevis accepte les jetons externes

Avec la nouvelle option **-e** introduite dans l'outil de chiffrement automatisé Clevis, vous pouvez fournir un jeton d'identification externe pour éviter d'entrer votre mot de passe pendant **cryptsetup**. Cette fonctionnalité rend le processus de configuration plus automatisé et plus pratique, et est particulièrement utile pour les paquets tels que **stratis** qui utilisent Clevis.

Bugzilla:2126533

La journalisation cryptée TLS de Rsyslog prend désormais en charge plusieurs fichiers d'autorité de certification

La nouvelle directive **NetstreamDriverCaExtraFiles** permet de spécifier une liste de fichiers d'autorité de certification (CA) supplémentaires pour la journalisation à distance cryptée par TLS. Notez que cette nouvelle directive n'est disponible que pour le pilote de flux réseau Rsyslog de **ossl** (OpenSSL).

Bugzilla:2124849

Les privilèges Rsyslog sont limités

Les privilèges du système de traitement des logs Rsyslog sont désormais limités aux seuls privilèges explicitement requis par Rsyslog. Cela minimise l'exposition à la sécurité en cas d'erreur potentielle dans les ressources d'entrée, par exemple, un plugin de réseau. Par conséquent, Rsyslog dispose des mêmes fonctionnalités, mais n'a pas de privilèges superflus.

Bugzilla:2127404

La politique SELinux permet à Rsyslog de supprimer les privilèges au démarrage

Les privilèges du système de traitement des journaux Rsyslog étant désormais plus limités afin de minimiser l'exposition à la sécurité(RHBZ#2127404), la politique SELinux a été mise à jour afin de permettre au service **rsyslog** d'abandonner ses privilèges au démarrage.

Bugzilla:2151841

Tang utilise maintenant systemd-sysusers

Le serveur de présence réseau Tang ajoute désormais les utilisateurs et les groupes du système par l'intermédiaire du service **systemd-sysusers** au lieu de scripts shell contenant des commandes **useradd**. Cela simplifie la vérification de la liste des utilisateurs du système et vous pouvez également remplacer les définitions des utilisateurs du système en fournissant des fichiers **sysuser.d** avec une priorité plus élevée.

Bugzilla:2095474

opencryptoki repassé à la version 3.19.0

Le paquet **opencryptoki** est passé à la version 3.19.0, qui apporte de nombreuses améliorations et corrections de bogues. En particulier, **opencryptoki** prend désormais en charge les fonctionnalités suivantes :

- Clés Dilithium spécifiques à IBM
- Fonctions cryptographiques à double fonction
- Annulation des opérations actives basées sur une session à l'aide de la nouvelle fonction **C_SessionCancel**, telle que décrite dans la spécification PKCS #11 Cryptographic Token Interface Base Specification v3.0

- Signatures de Schnorr à travers le mécanisme **CKM_IBM_ECDSA_OTHER**
- Dérivation de la clé Bitcoin par le mécanisme **CKM_IBM_BTC_DERIVE**
- Jetons EP11 dans les systèmes IBM z16

Bugzilla:2110314

SELinux limite désormais mptcpd et udftools

Avec cette mise à jour des paquets **selinux-policy**, SELinux restreint les services suivants :

- **mptcpd**
- **udftools**

Bugzilla:1972222

fapolicyd permet désormais de filtrer la base de données RPM

Avec le nouveau fichier de configuration **/etc/fapolicyd/rpm-filter.conf**, vous pouvez personnaliser la liste des fichiers de la base de données RPM que le cadre logiciel **fapolicyd** stocke dans la base de données de confiance. Vous pouvez ainsi bloquer certaines applications installées par RPM ou autoriser une application refusée par le filtre de configuration par défaut.

Jira:RHEL-192

GnuTLS peut ajouter et supprimer du rembourrage lors du décryptage et du cryptage

La mise en œuvre de certains protocoles nécessite un remplissage PKCS#7 lors du décryptage et du cryptage. Les fonctions de chiffrement par bloc **gnutls_cipher_encrypt3** et **gnutls_cipher_decrypt3** ont été ajoutées à GnuTLS pour gérer de manière transparente le remplissage. Par conséquent, vous pouvez désormais utiliser ces fonctions en combinaison avec le drapeau **GNUTLS_CIPHER_PADDING_PKCS7** pour ajouter ou supprimer automatiquement le remplissage si la longueur du texte clair original n'est pas un multiple de la taille du bloc.

Bugzilla:2084161

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.

Bugzilla:2091905

4.7. MISE EN RÉSEAU

NetworkManager passe à la version 1.42.2

Les paquets **NetworkManager** ont été mis à jour vers la version amont 1.42.2, qui apporte un certain nombre d'améliorations et de corrections de bogues par rapport à la version précédente :

- Les liaisons Ethernet prennent en charge l'équilibrage de la charge à la source.
- NetworkManager peut gérer les connexions sur l'appareil **loopback**.
- La prise en charge des routes IPv4 equal-cost multi-path (ECMP) a été ajoutée.
- La prise en charge de l'étiquetage **802.1ad** dans les connexions de réseaux locaux virtuels (VLAN) a été ajoutée.
- L'application **nmtui** prend en charge les profils de connexion Wi-Fi WPA-Enterprise, Ethernet avec authentification 802.1X et MACsec.
- NetworkManager rejette les baux DHCPv6 si toutes les adresses échouent à la détection des adresses dupliquées IPv6 (DAD).

Pour plus d'informations sur les changements notables, lisez les notes de version en amont .

Bugzilla:2134897

Introduction de la propriété weight dans le routage ECMP avec NetworkManager

Avec cette mise à jour, RHEL 9 prend en charge une nouvelle propriété **weight** lors de la définition des itinéraires IPv4 Equal-Cost Multi-Path (ECMP). Vous pouvez configurer le routage par trajets multiples à l'aide de NetworkManager pour équilibrer la charge et stabiliser le trafic réseau. Cela permet d'utiliser plusieurs chemins pour la transmission de données entre deux nœuds, ce qui améliore l'efficacité du réseau et fournit une redondance en cas de défaillance d'un lien. Les conditions d'utilisation de la propriété **weight** sont les suivantes

- Les valeurs valables sont 1-256.
- Définissez plusieurs itinéraires de saut suivant comme des itinéraires à saut unique à l'aide de la propriété **weight**.
- Si vous ne définissez pas **weight**, NetworkManager ne peut pas fusionner les routes en une route ECMP.

Bugzilla:2081302

La mise à jour de NetworkManager améliore la flexibilité de la configuration DNS sur plusieurs réseaux

Avec cette mise à jour, vous pouvez utiliser la section **[global-dns]** existante dans le fichier **/etc/Networkmanager/NetworkManager.conf** pour configurer les options DNS sans spécifier la valeur **nameserver** dans la section **[global-dns-domain-*]**. Cela vous permet de configurer les options DNS dans le fichier **/etc/resolv.conf** tout en continuant à vous fier aux serveurs DNS fournis par la connexion réseau pour la résolution DNS réelle. Cette fonctionnalité facilite et assouplit la gestion de vos paramètres DNS lorsque vous vous connectez à différents réseaux dotés de différents serveurs DNS. En particulier lorsque vous utilisez le fichier **/etc/resolv.conf** pour configurer les options DNS.

Bugzilla:2019306

NetworkManager supporte désormais une nouvelle propriété vlan.protocol

Avec cette mise à jour, le type d'interface **vlan** accepte désormais une nouvelle propriété **protocol**. Le type de propriété est une chaîne de caractères. Les valeurs acceptées sont soit **802.1Q** (par défaut), soit **802.1ad**. La nouvelle propriété spécifie quel protocole VLAN contrôle l'identificateur de balise pour l'encapsulation.

Bugzilla:2128809

NetworkManager permet maintenant de configurer un VLAN sur une interface non gérée

Grâce à cette amélioration, vous pouvez utiliser une interface réseau non gérée comme interface de base lors de la configuration d'un réseau local virtuel (VLAN) avec NetworkManager. Par conséquent, l'interface de base du VLAN reste intacte à moins qu'elle ne soit modifiée explicitement par le biais de la commande **nmcli device set *enp1s0* managed true** ou d'une autre API de NetworkManager.

Bugzilla:2110307

La configuration de TCP Multipath à l'aide de NetworkManager est maintenant entièrement supportée

Avec cette mise à jour, l'utilitaire NetworkManager vous offre la fonctionnalité Multipath TCP (MPTCP). Vous pouvez utiliser les commandes **nmcli** pour contrôler MPTCP et rendre ses paramètres persistants.

Pour plus d'informations, voir :

- Comprendre le TCP à trajets multiples : haute disponibilité pour les points d'extrémité et l'autoroute du réseau de l'avenir
- RFC 8684 : Extensions TCP pour l'exploitation de chemins multiples avec des adresses multiples
- Configuration permanente de chemins multiples pour les applications MPTCP

Bugzilla:2029636

L'utilitaire NetworkManager permet désormais d'activer les connexions sur l'interface loopback

Les administrateurs peuvent gérer l'interface **loopback** pour :

- Ajouter des adresses IP supplémentaires à l'interface **loopback**
- Définir la configuration DNS
- Définir une route spéciale, qui n'est pas liée à une interface
- Définir une règle d'acheminement qui n'est pas liée à l'interface
- Modifier la taille de l'unité de transmission maximale (MTU) de l'interface **loopback**

Bugzilla:2073512

Le mode de liaison balance-slb est désormais pris en charge

Le nouveau mode de liaison **balance-slb** Source load balancing ne nécessite aucune configuration du commutateur. Le **balance-slb** divise le trafic sur l'adresse Ethernet source en utilisant **xmit_hash_policy=vlan srcmac**, et NetworkManager ajoute les règles **nftables** nécessaires au filtrage du trafic. Par conséquent, vous pouvez maintenant créer des profils de liaison avec l'option **balance-slb** activée en utilisant NetworkManager.

Bugzilla:2128216

firewalld repassé à la version 1.2

Le paquetage **firewalld** a été mis à jour vers la version 1.2, qui apporte de nombreuses améliorations. Les changements notables sont les suivants :

- Prise en charge de nouveaux services (par exemple Kodi JSON-RPC, EventServer, netdata, IPFS)
- Mode de sécurité intégrée pour garantir que le système reste protégé et que la communication réseau n'est pas interrompue si le service **firewalld** rencontre une erreur lors de son démarrage
- Complétion par des tabulations dans la ligne de commande (CLI) pour certaines commandes de la politique **firewalld**

Bugzilla:2125371

Le site firewalld prend désormais en charge le mécanisme de sécurité au démarrage

Avec cette amélioration, **firewalld** revient aux valeurs par défaut de sécurité en cas d'échec du démarrage. Cette fonctionnalité protège l'hôte en cas de configurations invalides ou d'autres problèmes de démarrage. Par conséquent, même si la configuration de l'utilisateur n'est pas valide, les hôtes utilisant **firewalld** sont maintenant à l'abri des pannes au démarrage.

Bugzilla:2077512

conntrack-tools repassé à la version 1.4.7

Le paquetage **conntrack-tools** a été mis à jour vers la version 1.4.7, qui apporte de nombreuses corrections de bogues et améliorations. Les changements notables sont les suivants :

- Ajoute l'indicateur **IPS_HW_OFFLOAD**, qui spécifie le déchargement d'une entrée **conntrack** vers le matériel
- Ajoute les compteurs statistiques **clash_resolve** et **chaintoolong**
- Prise en charge du filtrage des événements par famille d'adresses IP
- Accepte oui ou non comme synonymes de on ou off dans le fichier **conntrackd.conf**
- Prise en charge du chargement automatique de l'aide de l'espace utilisateur au démarrage du démon. Les utilisateurs n'ont pas à exécuter manuellement les commandes **nfct add helper**
- Supprime l'option de commande **-o userspace** et marque toujours les événements déclenchés par l'espace utilisateur
- Les problèmes d'injection externe ne sont consignés que sous forme d'avertissement
- Ignore l'ID de la piste lors de la recherche des entrées du cache pour permettre de remplacer les anciennes entrées bloquées
- Correction de l'analyse erronée des requêtes IPv6 **M-SEARCH** dans le module **ssdp cthelper**
- Élimine la nécessité de recourir à la technique du lazy binding dans la bibliothèque **nfct**
- Assainissement de l'analyse des valeurs du protocole, détection des valeurs non valides

Bugzilla:2132398

L'API nmstate prend désormais en charge les adresses locales de liaison IPv6 en tant que serveurs DNS

Grâce à cette amélioration, vous pouvez utiliser l'API **nmstate** pour définir des adresses IPv6 link-local comme serveurs DNS. Utilisez le format **<link-local_address>%<interface>**, par exemple :

```
dns-resolver:
  config:
    server:
    - fe80::deef:1%enp1s0
```

Bugzilla:2095207

L'API nmstate prend désormais en charge les drapeaux MPTCP

Cette mise à jour améliore l'API **nmstate** avec la prise en charge des drapeaux TCP MultiPath (MPTCP). Par conséquent, vous pouvez utiliser **nmstate** pour définir les drapeaux d'adresse MPTCP sur les interfaces avec des adresses IP statiques ou dynamiques.

Bugzilla:2120473

Les propriétés min-mtu et max-mtu ont été ajoutées au MTU sur toutes les interfaces

Auparavant, un message d'exception n'était pas suffisamment clair pour comprendre les plages de MTU prises en charge. Cette mise à jour introduit les propriétés **min-mtu** et **max-mtu** dans toutes les interfaces. Par conséquent, **nmstate** indiquera la plage de MTU prise en charge lorsque le MTU souhaité n'est pas compris dans cette plage.

Bugzilla:2044150

NetworkManager permet maintenant de configurer un VLAN sur une interface non gérée

Grâce à cette amélioration, vous pouvez utiliser une interface réseau non gérée comme interface de base lors de la configuration d'un réseau local virtuel (VLAN) avec NetworkManager. Par conséquent, l'interface de base du VLAN reste intacte à moins qu'elle ne soit modifiée explicitement par le biais de la commande **nmcli device set *enp1s0* managed true** ou d'une autre API de NetworkManager.

Bugzilla:2058292

Le mode de liaison balance-slb est désormais pris en charge

Le nouveau mode de liaison **balance-slb** L'équilibrage de la charge de la source ne nécessite aucune configuration du commutateur. Le **balance-slb** divise le trafic sur l'adresse Ethernet source en utilisant **xmit_hash_policy**=**vlan srcmac**, et NetworkManager ajoute les règles **nftables** nécessaires au filtrage du trafic. Par conséquent, vous pouvez maintenant créer des profils de liaison avec l'option **balance-slb** activée en utilisant NetworkManager.

Bugzilla:2130240

Une nouvelle propriété weight à Nmstate

Cette mise à jour introduit la propriété **weight** dans l'API et la suite d'outils Nmstate. Vous pouvez utiliser **weight** pour spécifier le poids relatif de chaque chemin dans le groupe ECMP (Equal Cost Multi-Path routes). Le poids est un nombre compris entre 1 et 256. En conséquence, la propriété **weight** dans Nmstate offre une plus grande flexibilité et un meilleur contrôle sur la distribution du trafic dans un groupe ECMP.

Bugzilla:2162401

xdp-tools repassé à la version 1.3.1

Les paquets **xdp-tools** ont été mis à jour vers la version amont 1.3.1, qui apporte un certain nombre d'améliorations et de corrections de bogues par rapport à la version précédente :

- Les utilitaires suivants ont été ajoutés :
  - **xdp-bench**: Effectue des tests XDP du côté de la réception.
  - **xdp-monitor**: Surveille les erreurs et les statistiques XDP en utilisant les points de trace du noyau.
  - **xdp-trafficgen**: Génère et envoie du trafic par le biais du crochet du pilote XDP.
- Les fonctionnalités suivantes ont été ajoutées à la bibliothèque **libxdp**:
  - Les fonctions **xdp_multiprog__xdp_frags_support()**, **xdp_program__set_xdp_frags_support()** et **xdp_program__xdp_frags_support()** ont été ajoutées pour permettre le chargement de programmes avec le support XDP **frags**, une fonction également connue sous le nom de **multibuffer XDP**.
  - La bibliothèque effectue un comptage de références correct lors de l'attachement de programmes aux sockets **AF_XDP**. Par conséquent, l'application n'a plus besoin de détacher manuellement les programmes XDP lorsqu'elle utilise les sockets. La bibliothèque **libxdp** détache désormais automatiquement le programme lorsqu'il n'est plus utilisé.
  - Les fonctions suivantes ont été ajoutées à la bibliothèque :
    - **xdp_program__create()** pour créer des objets **xdp_program**
    - **xdp_program__clone()** pour le clonage d'une référence **xdp_program**
    - **xdp_program__test_run()** pour l'exécution de programmes XDP par l'intermédiaire de l'API du noyau **BPF_PROG_TEST_RUN**
  - Lorsque la variable d'environnement **LIBXDP_BPFFS_AUTOMOUNT** est définie, la bibliothèque **libxdp** prend désormais en charge le montage automatique d'un système de fichiers virtuel **bpffs** si aucun n'est trouvé. Un sous-ensemble de fonctionnalités de la bibliothèque peut désormais fonctionner lorsqu'aucun **bpffs** n'est monté.

Notez que cette version modifie également le numéro de version du programme XDP dispatcher qui est chargé sur les périphériques du réseau. Cela signifie que vous ne pouvez pas utiliser une version précédente et une nouvelle version de **libxdp** et **xdp-tools** en même temps. La bibliothèque **libxdp** 1.3 affichera les anciennes versions du répartiteur, mais ne les mettra pas automatiquement à jour. En outre, après avoir chargé un programme avec **libxdp** 1.3, les anciennes versions ne fonctionneront pas avec la nouvelle.

Bugzilla:2160066

iproute repassé à la version 6.1.0

Le paquetage **iproute** a été mis à jour vers la version 6.1.0, qui apporte de nombreuses corrections de bogues et améliorations. Les changements notables sont les suivants :

- Prise en charge de la lecture des statistiques de l'appareil **vdpa**
  - Illustration de la lecture des statistiques pour la structure de données **virtqueue** à l'index 1 :

```
# vdpa dev vstats show vdpa-a qidx 1
vdpa-a:
vdpa-a: queue_type tx received_desc 321812 completed_desc 321812
```

- Illustration de la lecture des statistiques pour la structure **virtqueue data** à l'index 16 :

```
# vdpa dev vstats show vdpa-a qidx 16
vdpa-a: queue_type control_vq received_desc 17 completed_desc 17
```

- Mise à jour des pages de manuel correspondantes

Bugzilla:2155604

Le noyau enregistre désormais l'adresse d'écoute dans les messages SYN flood

Cette amélioration ajoute l'adresse IP d'écoute aux messages d'inondation SYN :

```
Inondation SYN possible sur le port <ip_address>:<port>.
```

Par conséquent, si de nombreux processus sont liés au même port sur différentes adresses IP, les administrateurs peuvent désormais identifier clairement le socket concerné.

Bugzilla:2143850

4.8. NOYAU

Version du noyau dans RHEL 9.2

Red Hat Enterprise Linux 9.2 est distribué avec la version 5.14.0-284.11.1 du noyau.

Bugzilla:2177782

Le noyau avec une taille de page de 64k est maintenant disponible

En plus du noyau RHEL 9 for ARM qui prend en charge 4k pages, Red Hat propose désormais un paquetage de noyau optionnel qui prend en charge 64k pages : **kernel-64k**.

Le noyau de taille de page 64k est une option utile pour les grands ensembles de données sur les plates-formes ARM. Il permet d'améliorer les performances de certains types d'opérations gourmandes en mémoire et en ressources processeur.

Vous devez choisir la taille de la page sur les systèmes à architecture ARM 64 bits au moment de l'installation. Vous pouvez installer **kernel-64k** uniquement par Kickstart en ajoutant le paquet **kernel-64k** à la liste des paquets dans le fichier **Kickstart**.

Pour plus d'informations sur l'installation de **kernel-64k**, voir Effectuer une installation avancée de RHEL 9.

Bugzilla:2153073

virtiofs prise en charge de kexec-tools activée

Cette amélioration ajoute la fonction **virtiofs** à **kexec-tools** en introduisant la nouvelle option **virtiofs myfs**, où **myfs** est un nom de balise variable à définir dans la ligne de commande **qemu**, par exemple, **-device vhost-user-fs-pci,tag=myfs**

Le système de fichiers **virtiofs** implémente un pilote qui permet à un invité de monter un répertoire qui a été exporté sur l'hôte. En utilisant cette amélioration, vous pouvez sauvegarder le fichier dump **vmcore** de la machine virtuelle sur :

- Un répertoire partagé **virtiofs**.
- Le sous-répertoire, tel que /**var**/**crash**, lorsque le système de fichiers racine est un répertoire partagé **virtiofs**.
- Un répertoire partagé **virtiofs** différent, lorsque le système de fichiers racine de la machine virtuelle est un répertoire partagé **virtiofs**.

Bugzilla:2085347

Le paquet kexec-tools apporte désormais des améliorations sur les cibles kdump distantes

Avec cette amélioration, le paquet **kexec-tools** ajoute des corrections de bogues et des améliorations significatives. Les changements les plus notables sont les suivants :

- Optimisation de la consommation de mémoire pour **kdump** en n'activant que les interfaces réseau nécessaires.
- Amélioration de l'efficacité du réseau pour **kdump** en cas d'interruption de la connexion. Le temps d'attente par défaut pour l'établissement d'un réseau est de 10 minutes maximum. Il n'est donc plus nécessaire de passer les paramètres **dracut**, tels que **rd.net.timeout.carrier** ou **rd.net.timeout.dhcp**, pour identifier un transporteur.

Bugzilla:2076416

Le FBP passe à la version 6.0

Le filtre de paquets Berkeley (BPF) a été rebasé sur la version 6.0 du noyau Linux avec de nombreuses améliorations. Cette mise à jour active toutes les fonctionnalités BPF qui dépendent du format de type BPF (BTF) pour les modules du noyau. Ces fonctionnalités comprennent l'utilisation des trampolines BPF pour le traçage, la disponibilité du principe Compile Once - Run Everywhere (CO-RE), et plusieurs fonctionnalités liées au réseau. En outre, les modules du noyau contiennent désormais des informations de débogage, ce qui signifie qu'il n'est plus nécessaire d'installer les paquets **debuginfo** pour inspecter les modules en cours d'exécution.

Pour plus d'informations sur la liste complète des fonctionnalités BPF disponibles dans le noyau en cours d'exécution, utilisez la commande **bpftool feature**.

Jira:RHELPLAN-133650

Le méta-outil rtla ajoute les traceurs osnoise et timerlat pour améliorer les capacités de traçage

Real-Time Linux Analysis (**rtla**) est un méta-outil qui comprend un ensemble de commandes permettant d'analyser les propriétés en temps réel de Linux. **rtla** exploite les capacités de traçage du noyau pour fournir des informations précises sur les propriétés et les causes profondes des résultats inattendus du système. **rtla** ajoute actuellement la prise en charge des commandes de traçage **osnoise** et **timerlat**:

- Le traceur **osnoise** fournit des informations sur le bruit du système d'exploitation.
- Le traceur **timerlat** affiche périodiquement la latence de la minuterie au niveau du gestionnaire de l'IRQ de la minuterie et du gestionnaire des threads.

Notez que pour utiliser la fonctionnalité **timerlat** de **rtla**, vous devez désactiver le contrôle d'admission à l'aide du script **sysctl -w kernel.sched_rt_runtime_us=-1**.

Bugzilla:2075216

Le module argparse permet désormais de configurer les sockets de l'unité centrale

Grâce à cette amélioration, vous pouvez spécifier un socket de CPU spécifique lorsque vous en avez plusieurs. Vous pouvez visualiser l'utilisation de l'aide en utilisant **-h** sur une sous-commande, par exemple, **tuna show_threads -h**.

Pour configurer un socket de CPU spécifique, spécifiez l'option **-S** avec chaque commande **tuna** où vous devez utiliser des sockets de CPU :

```
tuna <commande> [-S CPU_SOCKET_LIST]
```

Par exemple, utilisez **tuna show_threads -S 2,3** pour afficher les threads ou **tuna show_irqs -S 2,3** pour afficher les demandes d'interruption (IRQ) attachées.

Par conséquent, cette amélioration facilite l'utilisation de l'unité centrale sur la base des sockets de l'unité centrale sans qu'il soit nécessaire de spécifier chaque unité centrale individuellement.

Bugzilla:2122781

Le format de sortie pour cgroups et irqs a été amélioré pour une meilleure lisibilité

Grâce à cette amélioration, la sortie de la commande **tuna show_threads** pour l'utilitaire **cgroup** est désormais structurée en fonction de la taille du terminal. Vous pouvez également configurer un espacement supplémentaire pour la sortie de **cgroups** en ajoutant la nouvelle option **-z** ou **--spaced** à la commande **show_threads**.

En conséquence, la sortie de **cgroups** a maintenant un format lisible amélioré qui s'adapte à la taille de votre terminal.

Bugzilla:2121517

Une nouvelle interface de ligne de commande a été ajoutée à l'outil tuna en temps réel

Cette amélioration ajoute une nouvelle interface de ligne de commande à l'outil **tuna**, qui est basé sur le module d'analyse **argparse**. Avec cette mise à jour, vous pouvez désormais effectuer les tâches suivantes :

- Modifier les attributs des threads de l'application et du noyau.
- Opérer sur les demandes d'interruption (IRQ) par nom ou par numéro.
- Opérer sur des tâches ou des fils en utilisant l'identifiant du processus.
- Spécifiez les unités centrales et les ensembles d'unités centrales avec le numéro de l'unité centrale ou le numéro de la prise.

En utilisant la commande **tuna -h**, vous pouvez imprimer les arguments de la ligne de commande et les options correspondantes. Pour chaque commande, il existe des arguments optionnels, que vous pouvez visualiser avec la commande **tuna *<command>* -h** pour afficher les arguments de la ligne de commande.

En conséquence, **tuna** fournit maintenant une interface avec un menu de commandes et d'options plus standardisé, plus facile à utiliser et à maintenir que l'interface en ligne de commande.

Bugzilla:2062865

La sortie de la commande rteval comprend maintenant les chargements de programme et les informations sur les fils de mesure

La commande **rteval** affiche désormais un résumé du rapport avec le nombre de charges de programme, les threads de mesure et le CPU correspondant qui a exécuté ces threads. Ces informations permettent d'évaluer les performances d'un noyau temps réel sous charge sur des plates-formes matérielles spécifiques.

Le rapport **rteval** est écrit dans un fichier XML avec le journal de démarrage du système et enregistré dans le fichier compressé **rteval-<date>-N-tar.bz2**. L'adresse **date** indique la date de génération du rapport et l'adresse **N** est le compteur de la Nième exécution.

Pour générer un rapport **rteval**, entrez la commande suivante :

```
# rteval --summarize rteval-<date>-N.tar.bz2
```

Bugzilla:2081325

Les options -W et --bucket-width ont été ajoutées au programme oslat pour mesurer la latence

Grâce à cette amélioration, vous pouvez spécifier une plage de latence pour un seul godet avec une précision de l'ordre de la nanoseconde. Les largeurs qui ne sont pas des multiples de 1000 nanosecondes indiquent une précision de l'ordre de la nanoseconde. En utilisant les nouvelles options, **-W** ou **--bucket-width**, vous pouvez modifier l'intervalle de latence entre les godets pour mesurer la latence avec un temps de retard inférieur à la microseconde.

Par exemple, pour définir une largeur de seau de latence de 100 nanosecondes pour 32 seaux sur une durée de 10 secondes à exécuter sur une plage de CPU de 1 à 4 et omettre la taille de seau zéro, exécutez la commande suivante :

```
# oslat -b 32 -D 10s -W 100 -z -c 1-4
```

Notez qu'avant d'utiliser l'option, vous devez déterminer quel niveau de précision est significatif par rapport à la mesure de l'erreur.

Bugzilla:2041637

Le protocole de transport NVMe/FC est activé en tant que cible de stockage kdump

Le mécanisme **kdump** prend désormais en charge le protocole Nonvolatile Memory Express (NVMe) over Fibre Channel (NVMe/FC) en tant que cible de vidage. Avec cette mise à jour, vous pouvez configurer **kdump** pour enregistrer les fichiers de vidage de crash du noyau sur des cibles de stockage NVMe/FC.

Par conséquent, **kdump** peut capturer et sauvegarder le fichier **vmcore** sur **NVMe/FC** en cas de panne du noyau sans erreur de **timeout** ou **reconnect**.

Pour plus d'informations sur la configuration NVMe/FC, voir Gestion des périphériques de stockage

Bugzilla:2080110

L'outil crash-utility est passé à la version 8.0.2

Le programme **crash-utility**, qui analyse l'état d'un système actif ou après un crash du noyau, est passé

à la version 8.0.2. Le changement le plus important est l'ajout de la prise en charge des périphériques **multiqueue(blk-mq)**. En utilisant la commande **dev -d** ou **dev -D**, vous pouvez afficher les statistiques d'entrées/sorties sur disque pour les périphériques **multiqueue(blk-mq)**.

Bugzilla:2119685

openssl-ibmca repassé à la version 2.3.1

Le moteur et le fournisseur OpenSSL dynamique pour IBMCA sur l'architecture IBM Z 64 bits ont été rebasés vers la version amont 2.3.1. Il est recommandé aux utilisateurs de RHEL 9 d'utiliser OpenSSL *provider* pour garantir la compatibilité avec les futures mises à jour d'OpenSSL. La fonctionnalité *engine* a été supprimée dans la version 3 d'OpenSSL.

Bugzilla:2110378

Cryptage de la décharge de l'invité Secure Execution avec les clés du client

Cette nouvelle fonctionnalité permet aux invités dumps for Secure Execution initiés par l'hyperviseur de collecter des informations sur les pannes du noyau à partir de KVM dans des scénarios où l'utilitaire **kdump** ne fonctionne pas. Notez que les dumps initiés par l'hyperviseur pour Secure Execution sont conçus pour le matériel IBM Z Series z16 et LinuxONE Emperor 4.

Bugzilla:2044204

Le protocole TSN pour le temps réel a été activé sur la plateforme ADL-S

Avec cette amélioration, la spécification IEEE Time Sensitive Networking (TSN) permet la synchronisation temporelle et le traitement déterministe des charges de travail en temps réel sur le réseau sur la plateforme Intel Alder Lake S (ADL-S). Elle prend en charge les périphériques réseau suivants :

- Un combo MAC-PHY discret 2.5GbE avec support TSN : Intel® i225/i226
- Un MAC 2.5GbE intégré dans le SOC avec des puces PHY tierces de Marvell, Maxlinear et TI couvrant les vitesses 1GbE et 2.5Gbe, est disponible sur certains sites **skus** et SOC.

Avec le protocole TSN, vous pouvez gérer des charges de travail de type ordonnancement d'applications déterministes, préemption et synchronisation temporelle précise dans des implémentations embarquées. Ces implémentations nécessitent des réseaux dédiés, spécialisés et propriétaires, alors que les charges de travail s'exécutent sur des réseaux Ethernet, Wi-Fi et 5G standard.

En conséquence, TSN fournit des capacités améliorées pour :

- Matériel : systèmes basés sur Intel utilisés pour la mise en œuvre de charges de travail en temps réel dans l'IdO
- Applications déterministes et sensibles au temps

Bugzilla:2100606

Le pilote Intel ice est passé à la version 6.0.0

Le pilote Intel **ice** a été mis à jour vers la version amont 6.0.0, qui apporte un certain nombre d'améliorations et de corrections de bogues par rapport aux versions précédentes. Les améliorations notables sont les suivantes :

- Protocole point à point sur Ethernet (**PPPoE**) - décharge matérielle du protocole

- Commande d'écriture du protocole du circuit intégré (**I2C**)
- VLAN Tag Protocol Identifier (**TPID**) filtres dans le modèle de pilote du commutateur Ethernet (**switchdev**)
- Double étiquetage VLAN dans **switchdev**

Bugzilla:2104468

L'option d'écriture de données pour le module gnss est maintenant disponible

Cette mise à jour offre la possibilité d'écrire des données sur le récepteur **gnss**. Auparavant, **gnss** n'était pas entièrement configurable. Avec cette amélioration, toutes les fonctions de **gnss** sont désormais disponibles.

Bugzilla:2111048

Hébergement de certificats Secure Boot pour les systèmes IBM zSystems

À partir d'IBM z16 A02/AGZ et de LinuxONE Rockhopper 4 LA2/AGL, vous pouvez gérer les certificats utilisés pour valider les noyaux Linux lors du démarrage du système avec l'option Secure Boot activée sur la console de gestion du matériel (HMC). Notamment :

- Vous pouvez charger des certificats dans un magasin de certificats système en utilisant la HMC en mode DPM et classique à partir d'un serveur FTP auquel la HMC peut accéder. Il est également possible de charger des certificats à partir d'un périphérique USB connecté à la HMC.
- Vous pouvez associer des certificats stockés dans le magasin de certificats à une partition LPAR. Plusieurs certificats peuvent être associés à une partition et un certificat peut être associé à plusieurs partitions.
- Vous pouvez dissocier les certificats du magasin de certificats d'une partition à l'aide des interfaces HMC.
- Vous pouvez supprimer des certificats de la liste de certificats.
- Vous pouvez associer jusqu'à 20 certificats à une partition.

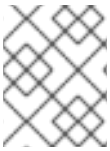
Les certificats de microprogrammes intégrés sont toujours disponibles. En particulier, dès que vous utilisez le magasin de certificats géré par l'utilisateur, les certificats intégrés ne sont plus disponibles.

Les fichiers de certificats chargés dans le magasin de certificats doivent répondre aux exigences suivantes :

- Ils ont le format **PEM-** ou **DER-encoded X.509v3** et l'une des extensions de nom de fichier suivantes : **.pem**, **.cer**, **.crt**, ou **.der**.
- Ils ne sont pas périmés.
- L'attribut d'utilisation de la clé doit être *Digital Signature*.
- L'attribut d'utilisation de la clé étendue doit contenir *Code Signing*.

Une interface micrologicielle permet à un noyau Linux fonctionnant dans une partition logique de charger les certificats associés à cette partition. Linux on IBM Z stocke ces certificats dans le trousseau **.platform**, ce qui permet au noyau Linux de vérifier les noyaux **kexec** et les modules de noyaux tiers à l'aide des certificats associés à cette partition.

Il incombe à l'opérateur de ne télécharger que des certificats vérifiés et de supprimer les certificats qui ont été révoqués.



NOTE

Le certificat **Red Hat Secure Boot CA 3** que vous devez charger dans la HMC est disponible sur Product Signing Keys.

Bugzilla:2190123

4.9. SYSTÈMES DE FICHIERS ET STOCKAGE

nvme-cli repassé à la version 2.2.1

Les paquets **nvme-cli** ont été mis à jour vers la version 2.2.1, qui apporte de nombreuses corrections de bogues et améliorations. Les changements notables sont les suivants :

- Ajout de la nouvelle commande **nvme show-topology**, qui affiche la topologie de tous les sous-systèmes NVMe.
- Suppression de la dépendance de **libuuid**.
- Les champs de données de **uint128** sont affichés correctement.
- Mise à jour de la dépendance **libnvme** à la version 1.2.

Bugzilla:2139753

libnvme repassé à la version 1.2

Les paquets **libnvme** ont été mis à jour vers la version 1.2, qui apporte de nombreuses corrections de bogues et améliorations. Le changement le plus notable est la suppression de la dépendance de la bibliothèque **libuuid**.

Bugzilla:2139752

Stratis assure la cohérence de la taille des blocs dans les pools

Stratis applique désormais une taille de bloc cohérente dans les pools afin de résoudre les problèmes potentiels qui peuvent survenir lorsque des périphériques de taille de bloc différente existent dans un pool. Grâce à cette amélioration, les utilisateurs ne peuvent plus créer un pool ou ajouter de nouveaux périphériques dont la taille de bloc est différente de celle des périphériques existants dans le pool. Par conséquent, le risque de défaillance du pool est réduit.

Bugzilla:2039957

Prise en charge de la croissance des disques existants dans le pool Stratis

Auparavant, lorsqu'un utilisateur ajoutait de nouveaux disques à la matrice RAID, la taille de la matrice RAID augmentait généralement. Cependant, dans tous les cas, Stratis ignorait l'augmentation de la taille et continuait à utiliser uniquement l'espace disponible sur la matrice RAID lors de son ajout au pool. Par conséquent, Stratis n'était pas en mesure d'identifier le nouveau périphérique et les utilisateurs ne pouvaient pas augmenter la taille du pool.

Grâce à cette amélioration, Stratis identifie désormais tous les membres du pool dont la taille a augmenté. Par conséquent, les utilisateurs peuvent maintenant lancer une commande pour étendre le pool en fonction de leurs besoins.

Stratis prend désormais en charge la croissance des disques existants au sein de son pool, en plus de la fonction existante de croissance du pool par l'ajout de nouveaux disques.

Bugzilla:2039955

Amélioration de la fonctionnalité de la commande lvreduce

Avec cette amélioration, lorsque le volume logique (LV) est actif, la commande **lvreduce** vérifie si la réduction de la taille du LV n'endommagerait pas un système de fichiers présent sur celui-ci. Si un système de fichiers sur le LV nécessite une réduction et que l'option **lvreduce resizefs** n'a pas été activée, le LV ne sera pas réduit.

En outre, de nouvelles options sont désormais disponibles pour contrôler la gestion des systèmes de fichiers lors de la réduction d'un LV. Ces options offrent aux utilisateurs une plus grande flexibilité et un meilleur contrôle lors de l'utilisation de la commande **lvreduce**.

Bugzilla:1878893

Des informations sur l'alignement des E/S directes pour statx ont été ajoutées

Cette mise à jour introduit une nouvelle valeur de masque, **"STATX_DIOALIGN"**, dans l'appel **statx(2)**. Lorsque cette valeur est définie dans le champ **stx_mask**, elle demande les valeurs **stx_dio_mem_align** et **stx_dio_offset_align**, qui indiquent respectivement l'alignement requis (en octets) pour les tampons de mémoire utilisateur, les décalages de fichiers et les longueurs de segments d'E/S pour les E/S directes (O_DIRECT) sur ce fichier. Si l'E/S directe n'est pas prise en charge sur le fichier, les deux valeurs seront 0. Cette interface est désormais mise en œuvre pour les périphériques bloc ainsi que pour les fichiers sur les systèmes de fichiers xfs et ext4 dans RHEL9.

Bugzilla:2150284

Découverte du trunking de session NFSv4.1

Avec cette mise à jour, le client peut utiliser plusieurs connexions au même serveur et à la même session, ce qui accélère le transfert des données. Lorsqu'un client NFS monte un serveur NFS multi-homé avec différentes adresses IP, une seule connexion est utilisée par défaut, ignorant les autres. Pour améliorer les performances, cette mise à jour ajoute la prise en charge des options de montage **trunkdiscovery** et **max_connect**, qui permettent au client de tester chaque connexion et d'associer plusieurs connexions au même serveur et à la même session NFSv4.1.

Bugzilla:2066372

Les tailles d'entrées-sorties de NFS peuvent désormais être définies comme des multiples de PAGE_SIZE pour TCP et RDMA

Cette mise à jour permet aux utilisateurs de définir la taille des IO de NFS comme un multiple de **PAGE_SIZE** pour les connexions TCP et RDMA. Cela offre une plus grande flexibilité dans l'optimisation des performances de NFS pour certaines architectures.

Bugzilla:2107347

nfsrahead a été ajouté à RHEL 9

Avec l'introduction de l'outil **nfsrahead**, vous pouvez l'utiliser pour modifier la valeur de **readahead** pour les montages NFS, et ainsi affecter les performances de lecture de NFS.

Bugzilla:2143747

4.10. HAUTE DISPONIBILITÉ ET CLUSTERS

Nouvelle option de configuration du stand **enable-authfile**

Lorsque vous créez une configuration Booth pour utiliser le gestionnaire de tickets Booth dans une configuration cluster, la commande **pcs booth setup** active désormais par défaut la nouvelle option de configuration Booth **enable-authfile**. Vous pouvez activer cette option sur un cluster existant avec la commande **pcs booth enable-authfile**. En outre, les commandes **pcs status** et **pcs booth status** affichent désormais des avertissements lorsqu'elles détectent une éventuelle mauvaise configuration de **enable-authfile**.

Bugzilla:2116295

pcs peut maintenant exécuter l'action **validate-all** des agents des ressources et des stoniths

Lors de la création ou de la mise à jour d'une ressource ou d'un dispositif STONITH, il est désormais possible de spécifier l'option **--agent-validation**. Avec cette option, **pcs** utilise l'action **validate-all** d'un agent, lorsqu'elle est disponible, en plus de la validation effectuée par **pcs** sur la base des métadonnées de l'agent.

Bugzilla:2112270, Bugzilla:2159454

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

Python 3.11 disponible dans RHEL 9

RHEL 9.2 introduit Python 3.11, fourni par le nouveau paquet **python3.11** et une suite de paquets construits pour lui, ainsi que l'image de conteneur **ubi9/python-311**.

Les améliorations notables par rapport à la version précédente de Python 3.9 sont les suivantes :

- Amélioration significative des performances.
- Correspondance des modèles structurels à l'aide du nouveau mot-clé **match** (similaire à **switch** dans d'autres langues).
- Amélioration des messages d'erreur, par exemple en cas de parenthèses ou de crochets non fermés.
- Numéros de ligne exacts pour le débogage et d'autres cas d'utilisation.
- Prise en charge de la définition des gestionnaires de contexte sur plusieurs lignes en mettant les définitions entre parenthèses.
- Diverses nouvelles fonctionnalités liées aux indications de type et au module **typing**, telles que le nouvel opérateur d'union de type **X | Y**, les génériques variadiques et le nouveau type **Self**.
- Emplacements précis des erreurs dans les traces de retour qui pointent vers l'expression qui a causé l'erreur.
- Un nouveau module de la bibliothèque standard **tomllib** qui prend en charge l'analyse TOML.
- Possibilité de soulever et de traiter simultanément plusieurs exceptions sans rapport entre elles grâce aux groupes d'exceptions et à la nouvelle syntaxe **except***.

Python 3.11 et les paquets construits pour lui peuvent être installés en parallèle avec Python 3.9 sur le même système.

Pour installer les paquets de la pile **python3.11**, utilisez, par exemple :

```
# dnf install python3.11
# dnf install python3.11-pip
```

Pour lancer l'interpréteur, utilisez, par exemple :

```
$ python3.11
$ python3.11 -m pip --help
```

Voir Installation et utilisation de Python pour plus d'informations.

Notez que Python 3.11 aura un cycle de vie plus court que Python 3.9, qui est l'implémentation Python par défaut dans RHEL 9 ; voir Red Hat Enterprise Linux Application Streams Life Cycle .

Bugzilla:2127923

nodejs:18 rebasé à la version 18.14 avec npm rebasé à la version 9

La mise à jour de **Node.js 18.14** inclut une mise à jour majeure SemVer de **npm** de la version 8 à la version 9. Cette mise à jour était nécessaire pour des raisons de maintenance et peut nécessiter une adaptation de la configuration de **npm**.

Notamment, les paramètres liés à l'authentification qui ne sont pas liés à un registre spécifique ne sont plus pris en charge. Cette modification a été apportée pour des raisons de sécurité. Si vous utilisiez des configurations d'authentification non délimitées, le jeton fourni était envoyé à chaque registre répertorié dans le fichier **.npmrc**.

Si vous utilisez des jetons d'authentification non codés, générez et fournissez des jetons codés dans le registre dans votre fichier **.npmrc**.

Si vous avez des lignes de configuration utilisant **_auth**, comme **//registry.npmjs.org/:_auth** dans vos fichiers **.npmrc**, remplacez-les par **//registry.npmjs.org/:_authToken=${NPM_TOKEN}** et fournissez le jeton scoped que vous avez généré.

Pour une liste complète des changements, voir le journal des changements en amont .

Bugzilla:2178088

git repassé à la version 2.39.1

Le système de contrôle de version **Git** a été mis à jour à la version 2.39.1, qui apporte des corrections de bogues, des améliorations et des gains de performance par rapport à la version 2.31 publiée précédemment.

Parmi les améliorations notables, citons

- La commande **git log** prend désormais en charge un format de remplacement pour la sortie **git describe**: **git log --format=%(describe)**
- La commande **git commit** supporte désormais l'option **--fixup<commit>** qui permet de corriger le contenu du commit sans modifier le message de log. Avec cette mise à jour, vous pouvez également utiliser :
  - L'option **--fixup=amend:<commit>** permet de modifier à la fois le message et le contenu.

    - L'option **--fixup=reword:<commit>** permet de ne mettre à jour que le message de validation.

- Vous pouvez utiliser la nouvelle option **--reject-shallow** avec la commande **git clone** pour désactiver le clonage à partir d'un référentiel peu profond.
- La commande **git branch** prend désormais en charge l'option **--recurse-submodules**.
- Vous pouvez maintenant utiliser la commande **git merge-tree** pour :
    - Tester si deux branches peuvent fusionner.
    - Calculer l'arbre qui résulterait du commit de fusion si les branches étaient fusionnées.
- Vous pouvez utiliser la nouvelle variable de configuration **safe.bareRepository** pour filtrer les dépôts nus.

Bugzilla:2139379

git-lfs repassé à la version 3.2.0

L'extension **Git Large File Storage (LFS)** a été mise à jour à la version 3.2.0, qui apporte des corrections de bogues, des améliorations et des gains de performance par rapport à la version 2.13 publiée précédemment.

Les changements les plus notables sont les suivants :

- **Git LFS** introduit un protocole de transport purement basé sur SSH.
- **Git LFS** propose désormais un pilote de fusion.
- L'utilitaire **git lfs fsck** vérifie désormais également que les pointeurs sont canoniques et que les fichiers LFS attendus ont un format correct.
- La prise en charge du protocole d'authentification NT LAN Manager (NTLM) a été supprimée. Utilisez plutôt l'authentification Kerberos ou Basic.

Bugzilla:2139383

Un nouveau flux de modules : nginx:1.22

Le serveur web et proxy **nginx 1.22** est maintenant disponible en tant que module stream **nginx:1.22**. Cette mise à jour apporte un certain nombre de corrections de bogues, de correctifs de sécurité, de nouvelles fonctionnalités et d'améliorations par rapport à la version 1.20 publiée précédemment.

Nouvelles fonctionnalités :

- **nginx** prend désormais en charge :
    - OpenSSL 3.0 et la fonction **SSL_sendfile()** lors de l'utilisation d'OpenSSL 3.0.
    - La bibliothèque PCRE2.
    - POP3 et IMAP pipelining dans le module proxy **mail**.
- **nginx** transmet maintenant les lignes d'en-tête **Auth-SSL-Protocol** et **Auth-SSL-Cipher** au serveur d'authentification du proxy de messagerie.

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.
- **nginx** supporte désormais les variables dans les directives suivantes : **proxy_ssl_certificate**, **proxy_ssl_certificate_key**, **grpc_ssl_certificate**, **grpc_ssl_certificate_key**, **uwsgi_ssl_certificate**, et **uwsgi_ssl_certificate_key**.
- La directive **listen** du module stream prend désormais en charge un nouveau paramètre **fastopen**, qui active le mode **TCP Fast Open** pour les sockets à l'écoute.
- Une nouvelle directive **max_errors** a été ajoutée au module proxy **mail**.

Autres modifications :

- **nginx** renvoie désormais toujours une erreur si :
  - La méthode **CONNECT** est utilisée.
  - Les en-têtes **Content-Length** et **Transfer-Encoding** sont spécifiés dans la demande.
  - Le nom de l'en-tête de la requête contient des espaces ou des caractères de contrôle.
  - La ligne d'en-tête de la demande **Host** contient des espaces ou des caractères de contrôle.
- **nginx** bloque désormais toutes les requêtes HTTP/1.0 qui incluent l'en-tête **Transfer-Encoding**.
- **nginx** établit désormais des connexions HTTP/2 en utilisant le protocole de négociation de la couche d'application (ALPN) et ne prend plus en charge le protocole de négociation du protocole suivant (NPN).

Pour installer le flux **nginx:1.22**, utilisez

```
# dnf module install nginx:1.22
```

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

Pour obtenir des informations sur la durée de la prise en charge des flux du module **nginx**, consultez le cycle de vie des flux d'applications de Red Hat Enterprise Linux .

Bugzilla:2096174

mod_security repassé à la version 2.9.6

Le module **mod_security** pour le serveur HTTP Apache a été mis à jour à la version 2.9.6, qui apporte de nouvelles fonctionnalités, des corrections de bogues et des correctifs de sécurité par rapport à la version 2.9.3 précédemment disponible.

Parmi les améliorations notables, citons

- Ajustement des règles d'activation de l'analyseur dans le fichier **modsecurity.conf-recommended**.
- Amélioration de la façon dont **mod_security** analyse les requêtes multipartites HTTP.
- Ajout d'une nouvelle collection **MULTIPART_PART_HEADERS**.

- Ajout d'une résolution d'horodatage en microsecondes à l'horodatage formaté du journal.
- Ajout des géo-pays manquants.

Bugzilla:2143211

Nouveaux paquets : tomcat

RHEL 9.2 introduit la version 9 du serveur Apache Tomcat. Tomcat est le conteneur de servlets utilisé dans l'implémentation de référence officielle des technologies Java Servlet et JavaServer Pages. Les spécifications de Java Servlet et JavaServer Pages sont développées par Sun dans le cadre du Java Community Process. Tomcat est développé dans un environnement ouvert et participatif et publié sous la licence Apache Software License version 2.0.

Bugzilla:2160511

Un nouveau flux de modules : postgresql:15

RHEL 9.2 introduit **PostgreSQL 15** en tant que flux de modules **postgresql:15**. **PostgreSQL 15** offre un certain nombre de nouvelles fonctionnalités et d'améliorations par rapport à la version 13. Les changements notables sont les suivants :

- Vous pouvez désormais accéder aux données JSON de **PostgreSQL** en utilisant des indices. Exemple de requête :

```
SELECT ('{ "postgres": { "release": 15 }}'::jsonb)['postgres']['release'];
```

- **PostgreSQL** prend désormais en charge les types de données à plages multiples et étend la fonction **range_agg** pour agréger les types de données à plages multiples.
- **PostgreSQL** améliore le suivi et l'observabilité :
  - Vous pouvez désormais suivre la progression des commandes **COPY** et de l'activité Write-ahead-log (WAL).
  - **PostgreSQL** fournit désormais des statistiques sur les slots de réplication.
  - En activant le paramètre **compute_query_id**, vous pouvez désormais suivre une requête de manière unique à travers plusieurs fonctionnalités **PostgreSQL**, y compris **pg_stat_activity** ou **EXPLAIN VERBOSE**.
- **PostgreSQL** améliore la prise en charge du parallélisme des requêtes de la manière suivante :
  - Amélioration des performances des analyses séquentielles parallèles.
  - La capacité du langage de procédure SQL (**PL/pgSQL**) à exécuter des requêtes parallèles lors de l'utilisation de la commande **RETURN QUERY**.
  - Activation du parallélisme dans la commande **REFRESH MATERIALIZED VIEW**.
- **PostgreSQL** inclut désormais la commande SQL standard **MERGE**. Vous pouvez utiliser **MERGE** pour écrire des instructions SQL conditionnelles qui peuvent inclure les actions **INSERT**, **UPDATE** et **DELETE** dans une seule instruction.
- **PostgreSQL** fournit les nouvelles fonctions suivantes pour l'utilisation d'expressions régulières pour inspecter les chaînes de caractères : **regexp_count()**, **regexp_instr()**, **regexp_like()**, et **regexp_substr()**.

- **PostgreSQL** ajoute le paramètre **security_invoker**, que vous pouvez utiliser pour interroger les données avec les autorisations de l'appelant de la vue, et non du créateur de la vue. Cela vous permet de vous assurer que les appelants de la vue disposent des autorisations correctes pour travailler avec les données sous-jacentes.
- **PostgreSQL** améliore les performances, notamment dans ses installations d'archivage et de sauvegarde.
- **PostgreSQL** ajoute la prise en charge des algorithmes de compression sans perte **LZ4** et **Zstandard** (**zstd**).
- **PostgreSQL** améliore ses algorithmes de tri en mémoire et sur disque.
- La mise à jour du fichier d'unité **postgresql.service** systemd garantit désormais que le service **postgresql** est démarré après la mise en route du réseau.

Les modifications suivantes sont incompatibles avec le passé :

- Les autorisations par défaut du schéma public ont été modifiées. Les utilisateurs nouvellement créés doivent obtenir une autorisation explicite en utilisant la commande **GRANT ALL ON SCHEMA public TO myuser;**. Par exemple :

```
postgres=# CREATE USER mydbuser;
postgres=# GRANT ALL ON SCHEMA public TO mydbuser;
postgres=# \c postgres mydbuser
postgres=$ CREATE TABLE mytable (id int);
```

- La fonction **libpq PQsendQuery()** n'est plus supportée en mode pipeline. Modifiez les applications concernées pour utiliser la fonction **PQsendQueryParams()** à la place.

Voir aussi Utilisation de PostgreSQL.

Pour installer le flux **postgresql:15**, utilisez

```
# dnf module install postgresql:15
```

Si vous souhaitez effectuer une mise à niveau à partir d'un flux **postgresql** antérieur dans RHEL 9, migrez vos données **PostgreSQL** comme décrit dans Migrating to a RHEL 8 version of PostgreSQL (Migration vers une version RHEL 8 de PostgreSQL).

Pour obtenir des informations sur la durée de la prise en charge des flux du module **postgresql**, consultez le cycle de vie des flux d'applications de Red Hat Enterprise Linux .

Bugzilla:2128410

4.12. COMPILATEURS ET OUTILS DE DÉVELOPPEMENT

openblas repassé à la version 0.3.21

La bibliothèque OpenBLAS a été mise à jour vers la version 0.3.21. Cette mise à jour inclut des correctifs d'optimisation des performances pour la plateforme IBM POWER10.

Bugzilla:2112099

Un nouveau flux de modules : swig:4.1

RHEL 9.2 introduit la version 4.1 de Simplified Wrapper and Interface Generator (SWIG) en tant que flux de modules **swig:4.1** disponible dans le dépôt CodeReady Linux Builder (CRB). Notez que les paquets inclus dans le dépôt CodeReady Linux Builder ne sont pas pris en charge.

Par rapport à **SWIG 4.0** publié dans RHEL 9.0, **SWIG 4.1**:

- Ajout de la prise en charge des versions 12 à 18 de **Node.js** et suppression de la prise en charge des versions antérieures à 6 de **Node.js**.
- Ajout de la prise en charge de **PHP 8**.
- Gère l'encapsulation de **PHP** entièrement via l'API C de **PHP** et ne génère plus d'encapsulation de **.php** par défaut.
- Prend en charge uniquement **Perl 5.8.0** et les versions ultérieures.
- Ajout de la prise en charge des versions 3.9 à 3.11 de **Python**.
- Seuls **Python 3.3** et les versions ultérieures de **Python 3** sont pris en charge, ainsi que **Python 2.7**.
- Correction de diverses fuites de mémoire dans le code généré par **Python**.
- Amélioration de la prise en charge des normes C99, C 11, C 14 et C 17 et début de la mise en œuvre de la norme C 20.
- Prise en charge de la classe de pointeurs C **std::unique_ptr**.
- Inclut plusieurs améliorations mineures dans la gestion des modèles C.
- Correction de l'utilisation de la déclaration C dans plusieurs cas.

Pour installer le flux du module **swig:4.1**:

1. Activer le référentiel CodeReady Linux Builder (CRB) .
2. Installer le flux de modules :

```
# dnf module install swig:4.1
```

Bugzilla:2139101

Nouveau paquet : jmc dans le référentiel CRB

RHEL 9.2 introduit le profileur JDK Mission Control (JMC) pour les JVM HotSpot version 8.2.0, disponible en tant que paquet **jmc** dans le dépôt CodeReady Linux Builder (CRB) pour les architectures AMD et Intel 64 bits.

Pour installer la JMC, vous devez d'abord activer le référentiel CodeReady Linux Builder (CRB) .

Notez que les paquets inclus dans le dépôt CRB ne sont pas pris en charge.

Bugzilla:2122401

Les attributs des services OpenJDK sont désormais disponibles en mode FIPS

Auparavant, les services et algorithmes cryptographiques disponibles pour OpenJDK en mode FIPS étaient filtrés de manière trop stricte et les attributs de service n'étaient pas disponibles. Avec cette amélioration, ces attributs de service sont désormais disponibles en mode FIPS.

Bugzilla:2186803

Performance Co-Pilot passe à la version 6.0

Performance Co-Pilot (**PCP**) a été mis à jour à la version 6.0. Les améliorations notables sont les suivantes :

1. Prise en charge de l'archive PCP de la version 3 :
   Il s'agit notamment de la prise en charge des altérations des domaines d'instance, des horodatages Y2038, des horodatages à la nanoseconde près, des fuseaux horaires arbitraires et des décalages de fichiers 64 bits utilisés pour les volumes individuels plus importants (au-delà de 2 Go).

   Cette fonction est actuellement activée par l'intermédiaire du paramètre **PCP_ARCHIVE_VERSION** dans le fichier **/etc/pcp.conf**.

   Les archives de la version 2 restent les archives par défaut.

2. Seul OpenSSL est utilisé dans l'ensemble du PCP. Mozilla NSS/NSPR n'est plus utilisé :
   Cela a un impact sur **libpcp**, **PMAPI** clients et **PMCD** l'utilisation du cryptage. Ces éléments sont maintenant configurés et utilisés de manière cohérente avec **pmproxy** HTTPS support et **redis-server**, qui utilisaient déjà OpenSSL.

3. Nouvel horodatage avec une précision de l'ordre de la nanoseconde **PMAPI** appels pour les interfaces de la bibliothèque **PCP** qui utilisent des horodatages.
   Tous ces éléments sont facultatifs et une compatibilité ascendante totale est préservée pour les outils existants.

4. Les outils et services suivants ont été mis à jour :

   pcp2elasticsearch

   Mise en place d'un support d'authentification.

   pcp-dstat

   Prise en charge des plugins **top-alike**.

   pcp-htop

   Mise à jour vers la dernière version stable en amont.

   pmseries

   Ajout des fonctions **sum**, **avg**, **stdev**, **nth_percentile**, **max_inst**, **max_sample**, **min_inst** et **min_sample**.

   pmdabpf

   Ajout de modules CO-RE (Compile Once - Run Everywhere) et prise en charge des systèmes AMD64, Intel 64 bits, ARM 64 bits et IBM Power.

   pmdabpftrace

   Les exemples de scripts de démarrage automatique ont été déplacés dans le répertoire **/usr/share**.

   pmdadenki

   Ajout de la prise en charge de plusieurs batteries actives.

   pmdalinux

Mises à jour des dernières modifications apportées à **/proc/net/netstat**.

pmdaopenvswitch

Ajout de statistiques supplémentaires sur l'interface et la couverture.

pmproxy

Les paramètres de la demande peuvent désormais être envoyés dans le corps de la demande.

pmieconf

Ajout de plusieurs règles **pmie** pour les métriques Open vSwitch.

pmlogger_farm

Ajout d'un fichier de configuration par défaut pour les enregistreurs de fermes.

pmlogger_daily_report

Quelques améliorations majeures en matière d'efficacité.

Bugzilla:2117074

grafana repassé à la version 9.0.9

Le paquet **grafana** a été rebasé à la version 9.0.9. Les changements notables sont les suivants :

- Le panneau des séries temporelles est désormais l'option de visualisation par défaut, remplaçant le panneau des graphiques
- Nouveau panneau de carte thermique
- Nouveau générateur de requêtes pour Prometheus et Loki
- Mise à jour des alertes Grafana
- Améliorations multiples de l'interface utilisateur et des performances
- La licence est passée d'Apache 2.0 à GNU Affero General Public License (AGPL)

Les fonctions suivantes sont proposées à titre expérimental et facultatif :

- Nouveau panneau de diagrammes à barres
- Nouveau groupe de travail sur la chronologie de l'État
- Nouveau panneau d'historique des statuts
- Nouveau panneau d'histogramme

Pour plus d'informations, voir : Nouveautés de Grafana v9.0 et Nouveautés de Grafana v8.0.

Bugzilla:2116847

grafana-pcp repassé à la version 5.1.1

Le paquetage **grafana-pcp** a été rebasé à la version 5.1.1. Les changements notables sont les suivants :

Éditeur de requêtes

ajout de boutons pour désactiver la conversation sur les taux et la conversation sur l'utilisation du temps.

Redis

suppression de la fonction **label_values(metric, label)** qui était obsolète.

Redis

correction de l'erreur de réseau pour les mesures comportant de nombreuses séries (nécessite Performance Co-Pilot v6).

Redis

fixer le délai d'attente de l'API **pmproxy** à 1 minute.

Bugzilla:2116848

Mise à jour du jeu d'outils GCC 12

GCC Toolset 12 est un ensemble d'outils de compilation qui fournit des versions récentes d'outils de développement. Il est disponible en tant que flux d'application sous la forme d'une collection de logiciels dans le dépôt **AppStream**.

Les changements notables introduits dans RHEL 9.2 sont les suivants :

- Le compilateur GCC a été mis à jour vers la version 12.2.1, qui apporte de nombreuses corrections de bogues et améliorations disponibles dans la version amont de GCC.
- **annobin** a été mis à jour à la version 11.08.

Les outils et versions suivants sont fournis par le Toolset 12 de GCC :

Outil	Version
CCG	12.2.1
GDB	11.2
binutils	2.38
dwz	0.14
annobin	11.08

Pour installer GCC Toolset 12, exécutez la commande suivante en tant que root :

```
# dnf install gcc-toolset-12
```

Pour exécuter un outil du GCC Toolset 12 :

```
$ scl enable gcc-toolset-12 tool
```

Pour lancer une session shell dans laquelle les versions des outils du Toolset 12 de GCC remplacent les versions système de ces outils :

```
$ scl enable gcc-toolset-12 bash
```

Pour plus d'informations, voir GCC Toolset 12.

Bugzilla:2110583

Le compilateur GCC mis à jour est désormais disponible pour RHEL 9.2

Le compilateur GCC du système, version 11.3.1, a été mis à jour pour inclure de nombreuses corrections de bogues et améliorations disponibles dans le GCC en amont.

La collection de compilateurs GNU (GCC) fournit des outils pour développer des applications avec les langages de programmation C, C , et Fortran.

Pour plus d'informations sur l'utilisation, voir Développement d'applications C et C dans RHEL 9 .

Bugzilla:2117632

Le jeu d'outils LLVM passe à la version 15.0.7

LLVM Toolset a été mis à jour à la version 15.0.7. Les changements notables sont les suivants :

- Les avertissements **-Wimplicit-function-declaration** et **-Wimplicit-int** sont activés par défaut dans C99 et les versions plus récentes. Ces avertissements deviendront des erreurs par défaut dans Clang 16 et au-delà.

Bugzilla:2118567

Rust Toolset repassé à la version 1.66.1

Rust Toolset a été mis à jour à la version 1.66.1. Les changements notables sont les suivants :

- L'API **thread::scope** crée un champ lexical dans lequel les variables locales peuvent être empruntées en toute sécurité par les threads nouvellement créés, et ces threads sont tous assurés de quitter le champ lexical avant qu'il ne se termine.
- L'API **hint::black_box** ajoute une barrière à l'optimisation du compilateur, ce qui est utile pour préserver le comportement dans les benchmarks qui pourraient autrement être optimisés.
- Le mot-clé **.await** effectue désormais des conversions avec le trait **IntoFuture**, de manière similaire à la relation entre **for** et **IntoIterator**.
- Les types génériques associés (GAT) permettent aux traits d'inclure des alias de type avec des paramètres génériques, ce qui permet de nouvelles abstractions sur les types et les durées de vie.
- Une nouvelle instruction **let-else** permet de lier des variables locales avec une correspondance conditionnelle des motifs, en exécutant un bloc divergent **else** lorsque le motif ne correspond pas.
- Les blocs étiquetés permettent aux instructions **break** de sauter à la fin du bloc, en incluant éventuellement une valeur d'expression.
- **rust-analyzer** est une nouvelle implémentation du protocole du serveur de langue, qui permet la prise en charge de Rust dans de nombreux éditeurs. Il remplace l'ancien paquetage **rls**, mais vous devrez peut-être ajuster la configuration de votre éditeur pour migrer vers **rust-analyzer**.
- Cargo dispose d'une nouvelle sous-commande **cargo remove** pour supprimer les dépendances de **Cargo.toml**.

Bugzilla:2123900

Go Toolset passe à la version 1.19.6

Go Toolset a été mis à jour à la version 1.19.6. Les changements notables sont les suivants :

- Corrections de sécurité pour les paquets suivants :
  - **crypto/tls**
  - **mime/multipart**
  - **net/http**
  - **path/filepath**
- Corrections de bugs :
  - La commande **go**
  - L'éditeur de liens
  - La durée d'exécution
  - Le paquet **crypto/x509**
  - Le paquet **net/http**
  - Le paquet **time**

Bugzilla:2175173

Le paquet tzdata comprend désormais le fichier /usr/share/zoneinfo/leap-seconds.list

Auparavant, le paquetage **tzdata** ne fournissait que le fichier **/usr/share/zoneinfo/leapseconds**. Certaines applications s'appuient sur le format alternatif fourni par le fichier **/usr/share/zoneinfo/leap-seconds.list** et, par conséquent, rencontrent des erreurs.

Avec cette mise à jour, le paquet **tzdata** comprend désormais les deux fichiers, ce qui permet de prendre en charge les applications qui reposent sur l'un ou l'autre format.

Bugzilla:2157982

4.13. GESTION DE L'IDENTITÉ

Prise en charge par SSSD de la conversion des répertoires personnels en minuscules

Avec cette amélioration, vous pouvez désormais configurer SSSD pour qu'il convertisse les répertoires personnels des utilisateurs en minuscules. Cela permet de mieux s'intégrer à la nature sensible à la casse de l'environnement RHEL. L'option **override_homedir** de la section **[nss]** du fichier **/etc/sssd/sssd.conf** reconnaît désormais la valeur du modèle **%h**. Si vous utilisez **%h** dans le cadre de la définition de **override_homedir**, SSSD remplace **%h** par le répertoire personnel de l'utilisateur en minuscules.

Jira:RHELPLAN-139430

SSSD prend désormais en charge la modification des mots de passe des utilisateurs LDAP à l'aide de la stratégie de mot de passe shadow

Avec cette amélioration, si vous définissez **ldap_pwd_policy** sur **shadow** dans le fichier

/etc/sssd/sssd.conf, les utilisateurs LDAP peuvent désormais modifier leur mot de passe stocké dans LDAP. Auparavant, les modifications de mot de passe étaient rejetées si **ldap_pwd_policy** était défini sur **shadow**, car il n'était pas clair si les attributs LDAP **shadow** correspondants étaient mis à jour.

En outre, si le serveur LDAP ne peut pas mettre à jour automatiquement les attributs **shadow**, définissez l'option **ldap_chpass_update_last_change** sur **True** dans le fichier **/etc/sssd/sssd.conf** pour indiquer à SSSD de mettre à jour l'attribut.

Bugzilla:1507035

IdM prend désormais en charge le paramètre min_lifetime

Avec cette amélioration, le paramètre **min_lifetime** a été ajouté au fichier **/etc/gssproxy/*.conf**. Le paramètre **min_lifetime** déclenche le renouvellement d'un ticket de service si sa durée de vie restante est inférieure à cette valeur.

Par défaut, sa valeur est de 15 secondes. Pour les clients de volume réseau tels que NFS, afin de réduire le risque de perte d'accès en cas d'indisponibilité momentanée du KDC, fixez cette valeur à 60 secondes.

Bugzilla:2184333

Le module ipapwpolicy ansible-freeipa prend désormais en charge de nouvelles options de politique de mot de passe

Avec cette mise à jour, le module **ipapwpolicy** inclus dans le paquetage **ansible-freeipa** prend en charge des options supplémentaires de la bibliothèque **libpwquality**:

maxrepeat
: Spécifie le nombre maximum de caractères identiques dans une séquence.

maxsequence
: Spécifie la longueur maximale des séquences de caractères monotones (**abcd**).

dictcheck
: Vérifie si le mot de passe est un mot du dictionnaire.

usercheck
: Vérifie si le mot de passe contient le nom d'utilisateur.

Si l'une des options de la nouvelle politique de mot de passe est activée, la longueur minimale des mots de passe est de 6 caractères. Les paramètres de la politique relative aux nouveaux mots de passe ne s'appliquent qu'aux nouveaux mots de passe.

Dans un environnement mixte avec des serveurs RHEL 7 et RHEL 8, les nouveaux paramètres de la politique de mot de passe ne sont appliqués que sur les serveurs fonctionnant sous RHEL 8.4 ou une version ultérieure. Si un utilisateur est connecté à un client IdM et que ce dernier communique avec un serveur IdM fonctionnant sous RHEL 8.3 ou une version antérieure, les nouvelles exigences en matière de stratégie de mot de passe définies par l'administrateur système ne s'appliquent pas. Pour garantir un comportement cohérent, mettez à niveau tous les serveurs vers RHEL 8.4 ou une version ultérieure.

Jira:RHELPLAN-137416

IdM prend désormais en charge le module de gestion Ansible ipanetgroup

En tant qu'administrateur du système de gestion des identités (IdM), vous pouvez intégrer IdM aux domaines NIS et aux groupes nets. Le module **ipanetgroup ansible-freeipa** vous permet de réaliser les opérations suivantes :

- Vous pouvez faire en sorte qu'un groupe net IdM existant contienne des utilisateurs, des groupes, des hôtes et des groupes d'hôtes IdM spécifiques, ainsi que des groupes nets IdM imbriqués.
- Vous pouvez vous assurer que des utilisateurs, des groupes, des hôtes et des groupes d'hôtes IdM spécifiques, ainsi que des groupes nets IdM imbriqués, sont absents d'un groupe net IdM existant.
- Vous pouvez vous assurer qu'un groupe de réseau spécifique est présent ou absent dans IdM.

Jira:RHELPLAN-137411

Nouvelles variables de rôle ipaclient_configure_dns_resolver et ipaclient_dns_servers Ansible ipaclient spécifiant le résolveur DNS du client

Auparavant, lors de l'utilisation du rôle **ansible-freeipa ipaclient** pour installer un client Identity Management (IdM), il n'était pas possible de spécifier le résolveur DNS pendant le processus d'installation. Vous deviez configurer le résolveur DNS avant l'installation.

Grâce à cette amélioration, vous pouvez spécifier le résolveur DNS lorsque vous utilisez le rôle **ipaclient** pour installer un client IdM avec les variables **ipaclient_configure_dns_resolver** et **ipaclient_dns_servers**. Par conséquent, le rôle **ipaclient** modifie le fichier **resolv.conf** et les utilitaires **NetworkManager** et **systemd-resolved** pour configurer le résolveur DNS sur le client de la même manière que le rôle **ansible-freeipa ipaserver** le fait sur le serveur IdM. Par conséquent, la configuration du DNS lors de l'utilisation du rôle **ipaclient** pour installer un client IdM est désormais plus efficace.

NOTE

L'utilisation du programme d'installation en ligne de commande **ipa-client-install** pour installer un client IdM nécessite toujours la configuration du résolveur DNS avant l'installation.

Jira:RHELPLAN-137406

L'utilisation du rôle ipaclient pour installer un client IdM avec un OTP ne nécessite aucune modification préalable du contrôleur Ansible

Auparavant, la commande **kinit** sur le contrôleur Ansible était une condition préalable à l'obtention d'un mot de passe à usage unique (OTP) pour le déploiement du client Identity Management (IdM). La nécessité d'obtenir l'OTP sur le contrôleur était un problème pour Red Hat Ansible Automation Platform (AAP), où le paquetage **krb5-workstation** n'était pas installé par défaut.

Avec cette mise à jour, la demande de TGT de l'administrateur est désormais déléguée au premier serveur IdM spécifié ou découvert. Par conséquent, vous pouvez désormais utiliser un OTP pour autoriser l'installation d'un client IdM sans modification supplémentaire du contrôleur Ansible. Cela simplifie l'utilisation du rôle **ipaclient** avec AAP.

Jira:RHELPLAN-137403

L'IdM impose désormais la présence de la structure MS-PAC dans les tickets Kerberos

À partir de RHEL 9.2, pour renforcer la sécurité, Identity Management (IdM) et MIT Kerberos imposent désormais la présence de la structure du certificat d'attribut de privilège (MS-PAC) dans les tickets Kerberos émis par le centre de distribution Kerberos (KDC) de RHEL IdM.

En novembre 2022, en réponse à CVE-2022-37967, Microsoft a introduit une signature étendue qui est calculée sur l'ensemble de la structure MS-PAC plutôt que sur la somme de contrôle du serveur. À partir de RHEL 9.2, les tickets Kerberos émis par IdM KDC contiennent également la signature étendue.

NOTE

La présence de la signature étendue n'est pas encore imposée dans l'IdM.

Jira:RHELPLAN-159146

Nouveau modèle de configuration de domaine pour le KDC permettant un cryptage des clés conforme à la norme FIPS 140-3

Cette mise à jour fournit un nouvel exemple de configuration du domaine (**EXAMPLE.COM**) dans le fichier **/var/kerberos/krb5kdc/kdc.conf**. Elle apporte deux changements :

- La famille **AES HMAC SHA-2**, conforme à la norme FIPS 140-3, est ajoutée à la liste des types pris en charge pour le cryptage des clés.
- Le type de cryptage de la clé principale du KDC passe de **AES 256 HMAC SHA-1** à **AES 256 HMAC SHA-384**.

AVERTISSEMENT

Cette mise à jour concerne les domaines MIT autonomes. Ne modifiez pas la configuration du centre de distribution Kerberos (KDC) dans RHEL Identity Management.

L'utilisation de ce modèle de configuration est recommandée pour les nouveaux royaumes. Le modèle n'affecte pas les royaumes déjà déployés. Si vous envisagez de mettre à jour la configuration de votre royaume conformément au modèle, tenez compte des points suivants :

Pour mettre à jour la clé principale, il ne suffit pas de modifier les paramètres de la configuration du KDC. Suivez la procédure décrite dans la documentation MIT Kerberos : https://web.mit.edu/kerberos/krb5-1.20/doc/admin/database.html#updating-the-master-key

L'ajout de la famille **AES HMAC SHA-2** aux types pris en charge pour le chiffrement des clés est sans danger à tout moment car il n'affecte pas les entrées existantes dans le KDC. Les clés ne seront générées que lors de la création de nouveaux mandants ou du renouvellement des identifiants. Notez que les clés de ce nouveau type ne peuvent pas être générées sur la base de clés existantes. Pour que ces nouveaux types de chiffrement soient disponibles pour un certain mandant, ses informations d'identification doivent être renouvelées, ce qui signifie que les keytabs des mandants de service doivent également être renouvelés.

Le seul cas où les mandants ne doivent pas comporter de clé **AES HMAC SHA-2** est celui des billets d'attribution de tickets (TGT) inter-royaumes d'Active Directory (AD). Comme AD ne met pas en œuvre la norme RFC8009, il n'utilise pas la famille de types de chiffrement **AES HMAC SHA-2**. Par conséquent, un TGS-REQ inter-royaumes utilisant un TGT inter-royaumes chiffré sur **AES HMAC SHA-2** échouerait. La meilleure façon d'empêcher le client MIT Kerberos d'utiliser **AES HMAC SHA-2** contre

AD est de ne pas fournir de clés **AES HMAC SHA-2** pour les mandants AD inter-royaumes. Pour ce faire, assurez-vous que vous créez les entrées TGT inter-royaumes avec une liste explicite de types de chiffrement de clé qui sont tous pris en charge par AD :

```
kadmin.local <<EOF
add_principal +requires_preauth -e aes256-cts-hmac-sha1-96,aes128-cts-hmac-sha1-96 -pw
[password] krbtgt/[MIT realm]@[AD realm]
add_principal +requires_preauth -e aes256-cts-hmac-sha1-96,aes128-cts-hmac-sha1-96 -pw
[password] krbtgt/[AD realm]@[MIT realm]
EOF
```

Pour que les clients MIT Kerboros utilisent les types de chiffrement **AES HMAC SHA-2**, vous devez également définir ces types de chiffrement comme **permitted** dans la configuration du client et du KDC. Sur RHEL, ce paramètre est géré par le système crypto-policy. Par exemple, sur RHEL 9, les hôtes utilisant la politique de chiffrement **DEFAULT** autorisent les tickets chiffrés **AES HMAC SHA-2** et **AES HMAC SHA-1**, tandis que les hôtes utilisant la politique de chiffrement **FIPS** n'acceptent que les tickets chiffrés **AES HMAC SHA-2**.

Bugzilla:2068535

Configurer pam_pwhistory à l'aide d'un fichier de configuration

Avec cette mise à jour, vous pouvez configurer le module **pam_pwhistory** dans le fichier de configuration **/etc/security/pwhistory.conf**. Le module **pam_pwhistory** enregistre le dernier mot de passe de chaque utilisateur afin de gérer l'historique des changements de mot de passe. Un support a également été ajouté dans **authselect** qui vous permet d'ajouter le module **pam_pwhistory** à la pile PAM.

Bugzilla:2126640, Bugzilla:2142805

samba repassé à la version 4.17.5

Les paquets **samba** ont été mis à jour vers la version amont 4.17.5, qui apporte des corrections de bogues et des améliorations par rapport à la version précédente. Les changements les plus notables :

- Les améliorations apportées à la sécurité dans les versions précédentes ont eu un impact sur les performances du serveur Server Message Block (SMB) pour les charges de travail à forte teneur en métadonnées. Cette mise à jour améliore les performances dans ce scénario.
- L'option **--json** a été ajoutée à l'utilitaire **smbstatus** pour afficher des informations d'état détaillées au format JSON.
- Les modules **samba.smb.conf** et **samba.samba3.smb.conf** ont été ajoutés à l'API Python **smbconf**. Vous pouvez les utiliser dans des programmes Python pour lire et, éventuellement, écrire la configuration Samba de manière native.

Notez que le protocole server message block version 1 (SMB1) est obsolète depuis Samba 4.11 et sera supprimé dans une prochaine version.

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**. Red Hat ne prend pas en charge la rétrogradation des fichiers de base de données **tdb**.

Après avoir mis à jour Samba, utilisez l'utilitaire **testparm** pour vérifier le fichier **/etc/samba/smb.conf**.

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

Bugzilla:2131993

ipa-client-install supporte désormais l'authentification avec PKINIT

Auparavant, le site **ipa-client-install** ne prenait en charge que l'authentification par mot de passe. Cette mise à jour permet à **ipa-client-install** de prendre en charge l'authentification par PKINIT.

Par exemple :

```
ipa-client-install --pkinit-identity=FILE:/path/to/cert.pem,/path/to/key.pem --pkinit-anchor=FILE:/path/to/cacerts.pem
```

Pour utiliser l'authentification PKINIT, vous devez établir la confiance entre IdM et la chaîne CA du certificat PKINIT. Pour plus d'informations, voir la page de manuel **ipa-cacert-manage(1)**. En outre, les règles de mappage de l'identité du certificat doivent mapper le certificat PKINIT de l'hôte à un principal qui a la permission d'ajouter ou de modifier un enregistrement d'hôte. Pour plus d'informations, voir la page de manuel **ipa certmaprule-add**.

Bugzilla:2143224

Red Hat IdM et Certificate System prennent désormais en charge le protocole EST

Enrollment over Secure Transport (EST) est une nouvelle fonctionnalité du sous-système de certification qui est spécifiée dans la RFC 7030 et qui est utilisée pour fournir des certificats à partir d'une autorité de certification (CA). EST met en œuvre le côté serveur de l'opération, comme **/getcacerts**, **/simpleenroll**, et **/simplereenroll**.

Notez que Red Hat prend en charge à la fois EST et le Simple Certificate Enrollment Protocol (SCEP) original dans le système de certificats.

Bugzilla:1849834

Purge automatique des certificats expirés

Cette mise à jour ajoute un mécanisme automatique pour purger les certificats expirés et les enregistrements de demande de la base de données. Vous pouvez activer cette fonction en fonction de certaines règles, telles que la limite de taille de la recherche, la limite de temps de la recherche et la durée de conservation.

Pour supprimer les enregistrements en toute sécurité, l'autorité de certification doit utiliser la méthode Random Certificate Serial Numbers v1 (RSNv3) pour générer les numéros de série des certificats et les identifiants des demandes d'inscription ou de renouvellement. L'AC fournit un travail d'élagage qui supprime les éléments suivants :

- Certificats expirés depuis un certain temps.
- Demandes complétées correspondant aux certificats expirés.
- Demandes incomplètes qui sont restées inactives pendant un certain temps.

Vous devez planifier l'exécution régulière de cette tâche afin de supprimer un certain nombre d'enregistrements à chaque exécution. Les enregistrements restants seront supprimés lors des exécutions suivantes. Pour les déploiements importants, vous pouvez répartir la tâche entre les serveurs du cluster.

Bugzilla:1883477

Améliorer l'utilisation du cache négatif

Cette mise à jour améliore les performances du SSSD pour les recherches par identifiant de sécurité (SID). Elle stocke désormais les SID non existants dans le cache négatif pour les domaines individuels et demande le domaine auquel le SID appartient.

Bugzilla:1766490

ACME prend désormais en charge la suppression automatique des certificats expirés

Auparavant, le service ACME (Automated Certificate Management Environment) de la gestion des identités (IdM) ne supprimait pas les certificats expirés de l'autorité de certification (AC). Comme ACME émet des certificats de courte durée (90 jours), les certificats expirés s'accumulaient dans l'autorité de certification, ce qui affectait les performances.

Grâce à cette amélioration, ACME peut désormais supprimer automatiquement les certificats expirés à des intervalles spécifiés.

La suppression des certificats expirés est désactivée par défaut. Pour l'activer, entrez :

```
# ipa-acme-manage pruning --enable --cron "0 0 1 * *"
```

Les certificats expirés sont ainsi supprimés le premier jour de chaque mois à minuit.

NOTE

Les certificats expirés sont supprimés après leur période de conservation. Par défaut, cette période est de 30 jours après l'expiration.

Pour plus de détails, voir la page de manuel **ipa-acme-manage(1)**.

Bugzilla:2162677

Le serveur d'annuaire prend désormais en charge les clés privées ECDSA pour TLS

Auparavant, vous ne pouviez pas utiliser d'algorithmes cryptographiques plus puissants que RSA pour sécuriser les connexions au serveur Directory. Avec cette amélioration, Directory Server prend désormais en charge les clés ECDSA et RSA.

Bugzilla:2096795

Directory Server prend désormais en charge la journalisation étendue des opérations de recherche

Auparavant, les enregistrements dans le journal des accès n'indiquaient pas pourquoi certaines opérations de recherche avaient une valeur **etime** très élevée. Avec cette version, vous pouvez activer l'enregistrement de statistiques telles que le nombre de consultations d'index (opérations de lecture de la base de données) et la durée totale des consultations d'index pour chaque opération de recherche. Ces enregistrements statistiques peuvent aider à analyser pourquoi la valeur **etime** peut être si coûteuse en ressources.

Bugzilla:1859271

Le niveau de journalisation des erreurs NUNC_STANS a été remplacé par le nouveau niveau de journalisation 1048576

Auparavant, vous ne pouviez pas facilement déboguer les problèmes liés à la politique de mot de passe. Avec le nouveau niveau de journalisation **1048576** pour le journal des erreurs, vous pouvez maintenant vérifier les informations suivantes sur la politique de mot de passe :

- Quelle politique locale rejette ou autorise la mise à jour d'un mot de passe.
- La violation exacte de la syntaxe.

Bugzilla:2057070

Directory Server introduit le journal de sécurité

Pour suivre correctement les problèmes au fil du temps, Directory Server dispose désormais d'un journal spécialisé qui conserve les données de sécurité. Le journal de sécurité ne tourne pas rapidement et consomme moins de ressources disque que le journal d'accès qui contient toutes les informations, mais nécessite une analyse coûteuse pour obtenir les données de sécurité.

Le nouveau journal du serveur enregistre les événements de sécurité tels que les événements d'authentification, les problèmes d'autorisation, les attaques DoS/TCP et d'autres événements.

Directory Server stocke le journal de sécurité dans le répertoire **/var/log/dirsrv/slapd-*instance_name*/** avec d'autres fichiers journaux.

Bugzilla:2093981

Directory Server peut désormais compresser les fichiers journaux archivés

Auparavant, les fichiers journaux archivés n'étaient pas compressés. Avec cette version, vous pouvez activer la compression des fichiers journaux d'accès, d'erreur, d'audit, d'échec d'audit et de sécurité afin d'économiser de l'espace disque. Notez que seule la compression des fichiers journaux de sécurité est activée par défaut.

Utilisez les nouveaux attributs de configuration suivants dans l'entrée **cn=config** pour gérer la compression :

- **nsslapd-accesslog-compress** pour le journal d'accès
- **nsslapd-errorlog-compress** pour le journal des erreurs
- **nsslapd-auditlog-compress** pour le journal d'audit
- **nsslapd-auditfaillog-compress** pour le journal des échecs d'audit
- **nsslapd-securelog-compress** pour le journal de sécurité

Bugzilla:1132524

Nouveau paramètre de configuration nsslapd-auditlog-display-attrs pour le journal d'audit du serveur d'annuaire

Auparavant, il était difficile de déterminer qui avait modifié une entrée si le nom distinctif (DN) de l'entrée ne contenait pas d'informations d'identification claires. Avec le nouveau paramètre **nsslapd-auditlog-display-attrs**, vous pouvez définir des attributs supplémentaires que Directory Server affiche dans le journal d'audit pour fournir plus de détails sur l'entrée modifiée.

Par exemple, si vous attribuez la valeur **cn** au paramètre **nsslapd-auditlog-display-attrs**, le journal d'audit affiche l'attribut **cn** dans la sortie :

```
time: 20221014125914
dn: uid=73747737483,ou=people,dc=example,dc=com
result: 0
*#cn: John Smith*
```

```
changetype: modify
replace: displayName
displayName: jsmith
-
replace: modifiersname
modifiersname: cn=dm
-
replace: modifytimestamp
modifytimestamp: 20221014165914Z
```

Si vous souhaitez que le journal d'audit inclue tous les attributs d'une entrée modifiée, vous pouvez utiliser un astérisque (*) comme valeur du paramètre.

Bugzilla:2136610

Une nouvelle option de configuration pamModuleIsThreadSafe est désormais disponible

Lorsqu'un module PAM est thread-safe, vous pouvez améliorer le débit d'authentification PAM et le temps de réponse de ce module spécifique en définissant la nouvelle option de configuration **pamModuleIsThreadSafe** sur **yes**:

```
`pamModuleIsThreadSafe: yes`
```

Cette configuration s'applique à l'entrée de configuration du module PAM (enfant de **cn=PAM Pass Through Auth,cn=plugins,cn=config**).

Utilisez l'option **pamModuleIsThreadSafe** dans le fichier de configuration **dse.ldif** ou la commande **ldapmodify**. Notez que la commande **ldapmodify** nécessite le redémarrage du serveur.

Bugzilla:2142639

Directory Server peut désormais importer un paquet de certificats

Auparavant, lorsque vous essayiez d'ajouter un paquet de certificats à l'aide de l'utilitaire **dsconf** ou **dsctl**, la procédure échouait avec une erreur et le paquet de certificats n'était pas importé. Ce comportement était dû à l'utilitaire **certutil** qui ne pouvait importer qu'un seul certificat à la fois. Avec cette mise à jour, Directory Server contourne le problème avec l'utilitaire **certutil**, et un paquet de certificats est ajouté avec succès.

Bugzilla:1878808

4.14. BUREAU

Désactiver le swipe pour changer d'espace de travail

Auparavant, le fait de balayer vers le haut ou vers le bas avec trois doigts changeait toujours l'espace de travail sur un écran tactile. Avec cette version, vous pouvez désactiver le changement d'espace de travail.

Pour plus d'informations, voir Désactiver le swipe pour changer d'espace de travail .

Bugzilla:2154358

Wayland est maintenant activé sur les GPU Aspeed

Auparavant, le pilote GPU Aspeed n'était pas suffisamment performant pour permettre l'exécution d'une session Wayland. Pour contourner ce problème, la session Wayland a été désactivée pour les GPU Aspeed.

Avec cette version, les performances du pilote ont été significativement améliorées et la session Wayland est maintenant réactive. En conséquence, la session Wayland est désormais activée par défaut sur les GPU Aspeed.

Bugzilla:2131203

Menu personnalisé de clic droit sur le bureau

Vous pouvez désormais personnaliser le menu qui s'ouvre lorsque vous cliquez avec le bouton droit de la souris sur l'arrière-plan du bureau. Vous pouvez créer des entrées personnalisées dans le menu qui exécutent des commandes arbitraires.

Pour personnaliser le menu, voir Personnaliser le menu du clic droit sur le bureau .

Bugzilla:2160553

4.15. LA CONSOLE WEB

Certaines sous-politiques cryptographiques sont désormais disponibles dans la console web

Cette mise à jour de la console web RHEL étend les options de la boîte de dialogue **Change crypto policy**. Outre les quatre politiques cryptographiques applicables à l'ensemble du système, vous pouvez désormais appliquer les sous-politiques suivantes via l'interface graphique :

- **DEFAULT:SHA1** est la politique **DEFAULT** avec l'algorithme **SHA-1** activé.
- **LEGACY:AD-SUPPORT** est la stratégie **LEGACY** avec des paramètres moins sûrs qui améliorent l'interopérabilité des services Active Directory.
- **FIPS:OSPP** est la politique **FIPS** avec des restrictions supplémentaires inspirées de la norme Critères communs pour l'évaluation de la sécurité des technologies de l'information.

Jira:RHELPLAN-137505

La console web exécute désormais des étapes supplémentaires pour lier les volumes racine chiffrés LUKS à l'EDNB

Avec cette mise à jour, la console Web RHEL exécute des étapes supplémentaires requises pour lier les volumes racine chiffrés LUKS aux déploiements NBDE (Network-Bound Disk Encryption). Après avoir sélectionné un système de fichiers racine chiffré et un serveur Tang, vous pouvez ignorer l'ajout du paramètre **rd.neednet=1** à la ligne de commande du noyau, l'installation du paquet **clevis-dracut** et la régénération d'un ramdisk initial (**initrd**). Pour les systèmes de fichiers non racine, la console web active désormais les unités **remote-cryptsetup.target** et **clevis-luks-akspass.path systemd** , installe le paquet **clevis-systemd** et ajoute le paramètre **_netdev** aux fichiers de configuration **fstab** et **crypttab**. Par conséquent, vous pouvez désormais utiliser l'interface graphique pour toutes les étapes de configuration du client Clevis lors de la création de déploiements NBDE pour le déverrouillage automatisé des volumes racine cryptés LUKS.

AVERTISSEMENT

En raison d'un bogue dans le code permettant de déterminer si l'utilisateur ajoute ou non une clé Tang au système de fichiers racine, le processus de liaison dans la console Web se bloque lorsqu'il n'y a pas de système de fichiers sur le conteneur LUKS. Comme la console Web affiche le message d'erreur **TypeError: Qe(...) is undefined** après que vous avez cliqué sur le bouton **Trust key** dans la boîte de dialogue **Verify key**, vous devez effectuer toutes les étapes requises dans l'interface de ligne de commande dans le scénario décrit.

Jira:RHELPLAN-139125

4.16. RÔLES DU SYSTÈME RED HAT ENTERPRISE LINUX

La règle de routage permet de consulter une table de routage par son nom

Avec cette mise à jour, le rôle système **rhel-system-roles.network** RHEL prend en charge la recherche d'une table de routage par son nom lorsque vous définissez une règle de routage. Cette fonctionnalité permet une navigation rapide pour les configurations réseau complexes où vous devez avoir différentes règles de routage pour différents segments du réseau.

Bugzilla:2131293

Le rôle de système network permet de définir une valeur de priorité DNS

Cette amélioration ajoute le paramètre **dns_priority** au rôle système RHEL **network**. Vous pouvez attribuer à ce paramètre une valeur comprise entre **-2147483648** et **2147483647**. La valeur par défaut est **0**. Les valeurs inférieures ont une priorité plus élevée. Notez que les valeurs négatives conduisent le rôle de système à exclure d'autres configurations ayant une valeur de priorité numérique supérieure. Par conséquent, en présence d'au moins une valeur de priorité négative, le rôle de système n'utilise que les serveurs DNS des profils de connexion ayant la valeur de priorité la plus basse.

Par conséquent, vous pouvez utiliser le rôle de système **network** pour définir l'ordre des serveurs DNS dans différents profils de connexion.

Bugzilla:2133858

Nouveaux paramètres de personnalisation IPsec pour le rôle de système vpn RHEL

Étant donné que certains périphériques réseau nécessitent une personnalisation d'IPsec pour fonctionner correctement, les paramètres suivants ont été ajoutés au rôle de système **vpn** RHEL :

IMPORTANT

Ne modifiez pas les paramètres suivants sans connaissances préalables. La plupart des scénarios ne nécessitent pas de personnalisation.

De plus, pour des raisons de sécurité, cryptez une valeur du paramètre **shared_key_content** en utilisant Ansible Vault.

- Paramètres du tunnel :

- **shared_key_content**
- **ike**
- **esp**
- **ikelifetime**
- **salifetime**
- **retransmit_timeout**
- **dpddelay**
- **dpdtimeout**
- **dpdaction**
- **leftupdown**

- Paramètres par hôte :
- **leftid**
- **rightid**

Par conséquent, vous pouvez utiliser le rôle **vpn** pour configurer la connectivité IPsec avec un large éventail de périphériques réseau.

Bugzilla:2119102

Le rôle de système selinux RHEL prend désormais en charge le paramètre local

Cette mise à jour du rôle système **selinux** RHEL introduit la prise en charge du paramètre **local**. En utilisant ce paramètre, vous pouvez supprimer uniquement les modifications de votre politique locale et préserver la politique SELinux intégrée.

Bugzilla:2128843

Le rôle de système ha_cluster prend désormais en charge l'exécution automatisée des rôles de système firewall, selinux et certificate

Le rôle de système RHEL ha_cluster prend désormais en charge les fonctionnalités suivantes :

Utilisation des rôles de système firewall et selinux pour gérer l'accès aux ports

Pour configurer les ports d'un cluster afin qu'ils exécutent les services **firewalld** et **selinux**, vous pouvez définir les nouvelles variables de rôle **ha_cluster_manage_firewall** et **ha_cluster_manage_selinux** sur **true**. Cela configure le cluster afin qu'il utilise les rôles de système **firewall** et **selinux**, en automatisant et en exécutant ces opérations dans le rôle de système **ha_cluster**. Si ces variables sont définies sur leur valeur par défaut de **false**, les rôles ne sont pas exécutés. Avec cette version, le pare-feu n'est plus configuré par défaut, car il n'est configuré que lorsque **ha_cluster_manage_firewall** est défini sur **true**.

Utilisation du rôle de système certificate pour créer une paire de clés privées et de certificats pcsd

Le rôle de système **ha_cluster** prend désormais en charge la variable de rôle **ha_cluster_pcsd_certificates**. La définition de cette variable transmet sa valeur à la variable **certificate_requests** du rôle de système **certificate**. Il s'agit d'une méthode alternative pour créer la paire clé privée/certificat pour **pcsd**.

Bugzilla:2130010

Le rôle de système RHEL **postfix** peut désormais utiliser les rôles de système RHEL **firewall** et **selinux** pour gérer l'accès aux ports

Grâce à cette amélioration, vous pouvez automatiser la gestion de l'accès aux ports en utilisant les nouvelles variables de rôle **postfix_manage_firewall** et **postfix_manage_selinux**:

- S'ils sont définis sur **true**, chaque rôle est utilisé pour gérer l'accès au port.
- S'ils sont réglés sur **false**, ce qui est la valeur par défaut, les rôles ne s'engagent pas.

Bugzilla:2130329

Le rôle de système RHEL **vpn** peut désormais utiliser les rôles **firewall** et **selinux** pour gérer l'accès aux ports

Grâce à cette amélioration, vous pouvez automatiser la gestion de l'accès aux ports dans le rôle de système RHEL **vpn** via les rôles **firewall** et **selinux**. Si vous définissez les nouvelles variables de rôle **vpn_manage_firewall** et **vpn_manage_selinux** sur **true**, les rôles gèrent l'accès aux ports.

Bugzilla:2130344

Le rôle de système **logging** RHEL prend désormais en charge l'accès aux ports et la génération des certificats

Grâce à cette amélioration, vous pouvez utiliser le rôle de journalisation pour gérer l'accès aux ports et générer des certificats à l'aide de nouvelles variables de rôle. Si vous définissez les nouvelles variables de rôle **logging_manage_firewall** et **logging_manage_selinux** sur **true**, les rôles gèrent l'accès aux ports. La nouvelle variable de rôle pour la génération de certificats est **logging_certificates**. Le type et l'utilisation sont les mêmes que pour le rôle **certificate certificate_requests** . Vous pouvez maintenant automatiser ces opérations directement en utilisant le rôle **logging**.

Bugzilla:2130357

Le rôle de système RHEL **metrics** peut désormais utiliser les rôles **firewall** et **selinux** pour gérer l'accès aux ports

Grâce à cette amélioration, vous pouvez contrôler l'accès aux ports. Si vous définissez les nouvelles variables de rôle **metrics_manage_firewall** et **metrics_manage_firewall** sur **true**, les rôles gèrent l'accès aux ports. Vous pouvez désormais automatiser et effectuer ces opérations directement en utilisant le rôle **metrics**.

Bugzilla:2133528

Le rôle de système RHEL **nbde_server** peut désormais utiliser les rôles **firewall** et **selinux** pour gérer l'accès aux ports

Avec cette amélioration, vous pouvez utiliser les rôles **firewall** et **selinux** pour gérer l'accès aux ports. Si vous définissez les nouvelles variables de rôle **nbde_server_manage_firewall** et **nbde_server_manage_selinux** sur **true**, les rôles gèrent l'accès aux ports. Vous pouvez maintenant automatiser ces opérations directement en utilisant le rôle **nbde_server**.

Bugzilla:2133930

Le fournisseur du réseau **initscripts** prend en charge la configuration de la métrique de route de la passerelle par défaut

Avec cette mise à jour, vous pouvez utiliser le fournisseur de réseau **initscripts** dans le rôle de système RHEL **rhel-system-roles.network** pour configurer la métrique de route de la passerelle par défaut.

Les raisons d'une telle configuration peuvent être les suivantes :

- Répartition de la charge de trafic sur les différents chemins
- Spécification des itinéraires primaires et des itinéraires de secours
- Exploiter les stratégies de routage pour envoyer le trafic vers des destinations spécifiques via des chemins spécifiques

Bugzilla:2134202

Intégration du rôle de système RHEL cockpit avec les rôles firewall, selinux et certificate

Cette amélioration vous permet d'intégrer le rôle **cockpit** avec les rôles **firewall** et **selinux** pour gérer l'accès aux ports et le rôle **certificate** pour générer des certificats.

Pour contrôler l'accès au port, utilisez les nouvelles variables **cockpit_manage_firewall** et **cockpit_manage_selinux**. Ces deux variables sont définies par défaut sur **false** et ne sont pas exécutées. Définissez-les à **true** pour permettre aux rôles **firewall** et **selinux** de gérer l'accès au port du service de la console web RHEL. Les opérations seront alors exécutées dans le cadre du rôle **cockpit**.

Notez que vous êtes responsable de la gestion de l'accès aux ports pour le pare-feu et SELinux.

Pour générer des certificats, utilisez la nouvelle variable **cockpit_certificates**. La variable est définie par défaut sur **false** et n'est pas exécutée. Vous pouvez utiliser cette variable de la même manière que la variable **certificate_request** dans le rôle **certificate**. Le rôle **cockpit** utilisera alors le rôle **certificate** pour gérer les certificats de la console web RHEL.

Bugzilla:2137663

Nouveau rôle de système RHEL pour une intégration directe avec Active Directory

Le nouveau rôle de système RHEL **rhel-system-roles.ad_integration** a été ajouté au package **rhel-system-roles**. Ainsi, les administrateurs peuvent désormais automatiser l'intégration directe d'un système RHEL avec un domaine Active Directory.

Bugzilla:2140795

Nouveau rôle Ansible pour Red Hat Insights et la gestion des abonnements

Le paquetage **rhel-system-roles** inclut désormais le rôle système de configuration d'hôte à distance (**rhc**). Ce rôle permet aux administrateurs d'enregistrer facilement les systèmes RHEL sur les serveurs Red Hat Subscription Management (RHSM) et Satellite. Par défaut, lorsque vous enregistrez un système en utilisant le rôle système **rhc**, le système se connecte à Red Hat Insights. Avec le nouveau rôle système **rhc**, les administrateurs peuvent désormais automatiser les tâches suivantes sur les nœuds gérés :

- Configurez la connexion à Red Hat Insights, y compris la mise à jour automatique, les remédiations et les balises pour le système.
- Activer et désactiver les référentiels.
- Configurer le proxy à utiliser pour la connexion.
- Définir le déblocage du système.

Pour plus d'informations sur l'automatisation de ces tâches, voir Utilisation du rôle système RHC pour enregistrer le système.

Bugzilla:2141330

Ajout de la prise en charge de l'adresse MAC clonée

L'adresse MAC clonée est l'adresse MAC du port WAN de l'appareil qui est la même que l'adresse MAC de la machine. Avec cette mise à jour, les utilisateurs peuvent spécifier l'interface de liaison ou de pont avec l'adresse MAC ou la stratégie telle que **random** ou **preserve** pour obtenir l'adresse MAC par défaut pour l'interface de liaison ou de pont.

Bugzilla:2143768

Le rôle Ansible de Microsoft SQL Server prend en charge les répliques asynchrones à haute disponibilité

Auparavant, le rôle Ansible de Microsoft SQL Server ne prenait en charge que les répliques primaires, synchrones et témoins de haute disponibilité. Désormais, vous pouvez définir la variable **mssql_ha_replica_type** sur **asynchronous** pour la configurer avec un type de réplique asynchrone pour une réplique nouvelle ou existante.

Bugzilla:2151282

Le rôle Ansible de Microsoft SQL Server prend en charge le type de cluster "read-scale"

Auparavant, le rôle Microsoft SQL Ansible ne prenait en charge que le type de cluster externe. Désormais, vous pouvez configurer le rôle avec une nouvelle variable **mssql_ha_ag_cluster_type**. La valeur par défaut est **external**, utilisez-la pour configurer le cluster avec Pacemaker. Pour configurer le cluster sans Pacemaker, utilisez la valeur **none** pour cette variable.

Bugzilla:2151283

Le rôle Ansible de Microsoft SQL Server peut générer des certificats TLS

Auparavant, vous deviez générer manuellement un certificat TLS et une clé privée sur les nœuds avant de configurer le rôle Microsoft SQL Ansible. Avec cette mise à jour, le rôle Microsoft SQL Server Ansible peut utiliser le rôle **redhat.rhel_system_roles.certificate** à cette fin. Désormais, vous pouvez définir la variable **mssql_tls_certificates** au format de la variable **certificate_requests** du rôle **certificate** pour générer un certificat TLS et une clé privée sur le nœud.

Bugzilla:2151284

Microsoft SQL Server Le rôle Ansible prend en charge la configuration de la version 2022 du serveur SQL

Auparavant, le rôle Microsoft SQL Ansible ne prenait en charge que la configuration de SQL Server version 2017 et version 2019. Cette mise à jour prend en charge la version 2022 de SQL Server pour le rôle Microsoft SQL Ansible. Désormais, vous pouvez définir la valeur **mssql_version** sur **2022** pour configurer un nouveau serveur SQL 2022 ou mettre à niveau un serveur SQL de la version 2019 à la version 2022. Notez que la mise à niveau d'un serveur SQL de la version 2017 à la version 2022 n'est pas disponible.

Bugzilla:2153428

Microsoft SQL Server Le rôle Ansible prend en charge la configuration de l'authentification Active Directory

Avec cette mise à jour, le rôle Microsoft SQL Ansible prend en charge la configuration de l'authentification Active Directory pour un serveur SQL. Désormais, vous pouvez configurer l'authentification Active Directory en définissant des variables avec le préfixe **mssql_ad_**.

Bugzilla:2163709

Le rôle de système journald RHEL est désormais disponible

Le service **journald** collecte et stocke les données de journalisation dans une base de données centralisée. Avec cette amélioration, vous pouvez utiliser les variables de rôle du système **journald** pour automatiser la configuration du journal **systemd** et configurer la journalisation persistante à l'aide de Red Hat Ansible Automation Platform.

Bugzilla:2165175

Le rôle de système ha_cluster prend désormais en charge la configuration des dispositifs de quorum

Un dispositif quorum fait office de dispositif d'arbitrage tiers pour une grappe. Il est recommandé d'utiliser un dispositif quorum pour les grappes comportant un nombre pair de nœuds. Dans le cas des clusters à deux nœuds, l'utilisation d'un dispositif quorum permet de mieux déterminer quel nœud survit dans une situation de cerveau divisé. Vous pouvez maintenant configurer un dispositif de quorum avec le rôle système **ha_cluster**, à la fois **qdevice** pour une grappe et **qnetd** pour un nœud d'arbitrage.

Bugzilla:2140804

4.17. VIRTUALISATION

Les dispositifs cryptographiques matériels peuvent désormais être automatiquement branchés à chaud

Auparavant, il n'était possible de définir des périphériques cryptographiques pour le passage que s'ils étaient présents sur l'hôte avant le démarrage du périphérique médiatisé. Désormais, vous pouvez définir une matrice de dispositif médiatisé qui répertorie tous les dispositifs cryptographiques que vous souhaitez transmettre à votre machine virtuelle (VM). Ainsi, les dispositifs cryptographiques spécifiés sont automatiquement transférés à la machine virtuelle en cours d'exécution s'ils deviennent disponibles ultérieurement. De même, si les périphériques deviennent indisponibles, ils sont supprimés de la machine virtuelle, mais le système d'exploitation invité continue à fonctionner normalement.

Bugzilla:1871126

Amélioration des performances des périphériques PCI passthrough sur IBM Z

Avec cette mise à jour, l'implémentation du PCI passthrough sur le matériel IBM Z a été améliorée grâce à de multiples améliorations de la gestion des E/S. Par conséquent, les périphériques PCI transmis aux machines virtuelles KVM (VM) sur les hôtes IBM Z sont désormais nettement plus performants.

En outre, les périphériques ISM peuvent désormais être attribués aux machines virtuelles sur les hôtes IBM Z.

Bugzilla:1871143

Nouveau paquet : passt

Cette mise à jour ajoute le paquetage **passt**, qui permet d'utiliser le back-end réseau en mode utilisateur **passt** pour les machines virtuelles.

Pour plus d'informations sur l'utilisation de **passt**, voir la documentation amont de libvirt .

Bugzilla:2131015

affectation des périphériques zPCI

Il est désormais possible d'attacher des périphériques zPCI en tant que périphériques pass-through à des machines virtuelles (VM) hébergées sur RHEL fonctionnant sur du matériel IBM Z. Par exemple, cela permet d'utiliser des lecteurs flash NVMe dans les machines virtuelles.

Jira:RHELPLAN-59528

4.18. CAPACITÉ DE SOUTIEN

Le service public sos passe à une cadence de mise à jour de 4 semaines

Au lieu de publier les mises à jour de **sos** avec les versions mineures de RHEL, la cadence de publication de l'utilitaire **sos** passe de 6 mois à 4 semaines. Vous pouvez trouver des détails sur les mises à jour du paquet **sos** dans le journal des modifications RPM toutes les 4 semaines ou vous pouvez lire un résumé des mises à jour **sos** dans les notes de mise à jour RHEL tous les 6 mois.

Bugzilla:2164987

La commande sos clean obscurcit désormais les adresses IPv6

Auparavant, la commande **sos clean** n'obscurcissait pas les adresses IPv6, ce qui laissait des données sensibles dans le rapport **sos**. Avec cette mise à jour, **sos clean** détecte et obscurcit les adresses IPv6 comme prévu.

Bugzilla:2134906

4.19. CONTENEURS

Le nouveau rôle de système podman RHEL est maintenant disponible

À partir de Podman 4.2, vous pouvez utiliser le rôle de système **podman** pour gérer la configuration de Podman, les conteneurs et les services **systemd** qui exécutent les conteneurs Podman.

Jira:RHELPLAN-118705

Podman prend désormais en charge les événements pour l'audit

À partir de Podman v4.4, vous pouvez rassembler toutes les informations pertinentes sur un conteneur directement à partir d'un seul événement et de l'entrée **journald**. Pour activer l'audit de Podman, modifiez le fichier de configuration **container.conf** et ajoutez l'option **events_container_create_inspect_data=true** à la section **[engine]**. Les données sont au format JSON, le même que celui de la commande **podman container inspect**. Pour plus d'informations, voir Comment utiliser les nouveaux événements de conteneurs et les fonctionnalités d'audit dans Podman 4.4.

Jira:RHELPLAN-136602

Le méta-paquet container-tools a été mis à jour

Le méta-paquet RPM **container-tools**, qui contient les outils Podman, Buildah, Skopeo, crun et runc, est désormais disponible. Cette mise à jour applique une série de corrections de bogues et d'améliorations par rapport à la version précédente.

Les changements notables dans Podman v4.4 sont les suivants :

- Présenter Quadlet, un nouveau générateur de systèmes qui permet de créer et de maintenir facilement des services systemd à l'aide de Podman.
- Une nouvelle commande, **podman network update**, a été ajoutée, qui met à jour les réseaux pour les conteneurs et les pods.
- Une nouvelle commande, **podman buildx version**, a été ajoutée, qui indique la version de buildah.
- Les conteneurs peuvent désormais avoir des contrôles de santé au démarrage, ce qui permet d'exécuter une commande pour s'assurer que le conteneur est complètement démarré avant que le contrôle de santé normal ne soit activé.
- Prise en charge de la sélection d'un serveur DNS personnalisé à l'aide de la commande **podman --dns**.
- La création et la vérification des signatures sigstore à l'aide de Fulcio et Rekor sont désormais disponibles.
- Amélioration de la compatibilité avec Docker (nouvelles options et alias).
- Amélioration de l'intégration Kubernetes de Podman - les commandes **podman kube generate** et **podman kube play** sont maintenant disponibles et remplacent les commandes **podman generate kube** et **podman play kube**. Les commandes **podman generate kube** et **podman play kube** sont toujours disponibles mais il est recommandé d'utiliser les nouvelles commandes **podman kube**.
- Les pods gérés par Systemd et créés par la commande **podman kube play** s'intègrent désormais à sd-notify, en utilisant l'annotation **io.containers.sdnotify** (ou **io.containers.sdnotify/$name** pour des conteneurs spécifiques).
- Les pods gérés par Systemd et créés par **podman kube play** peuvent maintenant être mis à jour automatiquement, en utilisant l'annotation **io.containers.auto-update** (ou **io.containers.auto-update/$name** pour des conteneurs spécifiques).

Podman a été mis à jour vers la version 4.4. Pour plus d'informations sur les changements notables, voir les notes de version en amont .

Jira:RHELPLAN-136607

Aardvark et Netavark prennent désormais en charge la sélection de serveurs DNS personnalisés

Les piles réseau Aardvark et Netavark prennent désormais en charge la sélection d'un serveur DNS personnalisé pour les conteneurs au lieu des serveurs DNS par défaut de l'hôte. Vous disposez de deux options pour spécifier le serveur DNS personnalisé :

- Ajouter le champ **dns_servers** dans le fichier de configuration **containers.conf**.
- Utilisez la nouvelle option **--dns** Podman pour spécifier l'adresse IP du serveur DNS.

L'option **--dns** remplace les valeurs du fichier **container.conf**.

Jira:RHELPLAN-138024

Skopeo permet désormais de générer des paires de clés sigstore

Vous pouvez utiliser la commande **skopeo generate-sigstore-key** pour générer une paire de clés publiques/privées Sigstore. Pour plus d'informations, voir la page de manuel **skopeo-generate-sigstore-key**.

Jira:RHELPLAN-151481

La boîte à outils est désormais disponible

Avec l'utilitaire **toolbox**, vous pouvez utiliser l'environnement de ligne de commande conteneurisé sans installer les outils de dépannage directement sur votre système. Toolbox s'appuie sur Podman et d'autres technologies de conteneurs standard de l'OCI. Pour plus d'informations, voir toolbx.

Jira:RHELPLAN-150266

Les images des conteneurs ont désormais une étiquette à deux chiffres

Dans RHEL 9.0 et RHEL 9.1, les images de conteneurs avaient une étiquette à trois chiffres. À partir de RHEL 9.2, les images de conteneurs ont désormais une étiquette à deux chiffres.

Jira:RHELPLAN-147982

Il est possible d'utiliser plusieurs clés GPG de confiance pour signer les images

Le fichier **/etc/containers/policy.json** prend en charge un nouveau champ **keyPaths** qui accepte une liste de fichiers contenant les clés de confiance. De ce fait, les images de conteneurs signées avec les clés GPG General Availability et Beta de Red Hat sont désormais acceptées dans la configuration par défaut.

Par exemple :

```
"registry.redhat.io": [
        {
            "type": "signedBy",
            "keyType": "GPGKeys",
            "keyPaths": ["/etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release", "/etc/pki/rpm-gpg/RPM-GPG-
KEY-redhat-beta"]
        }
]
```

Jira:RHELPLAN-129327

Podman prend désormais en charge les crochets de pré-exécution

Les scripts d'extension appartenant à la racine et situés dans les répertoires **/usr/libexec/podman/pre-exec-hooks** et **/etc/containers/pre-exec-hooks** définissent un contrôle fin sur les opérations du conteneur, notamment en bloquant les actions non autorisées.

Le fichier **/etc/containers/podman_preexec_hooks.txt** doit être créé par un administrateur et peut être vide. Si **/etc/containers/podman_preexec_hooks.txt** n'existe pas, les scripts d'extension ne seront pas exécutés. Si tous les scripts du plugin renvoient une valeur nulle, la commande **podman** est exécutée, sinon la commande **podman** se termine avec le code de sortie hérité.

Red Hat recommande d'utiliser la convention d'appellation suivante pour exécuter les scripts dans l'ordre correct : **DDD-*plugin_name.lang***, par exemple **010-check-group.py**. Notez que les scripts du plugin sont valides au moment de la création. Les conteneurs créés avant les scripts de plugins ne sont pas affectés.

Bugzilla:2119200

Les signatures sigstore sont maintenant disponibles

À partir de Podman 4.2, vous pouvez utiliser le format sigstore pour les signatures d'images de conteneurs. Les signatures sigstore sont stockées dans le registre des conteneurs avec l'image du conteneur, sans qu'il soit nécessaire d'avoir un serveur de signatures distinct pour stocker les signatures des images.

Jira:RHELPLAN-74672

La boîte à outils permet de créer des conteneurs RHEL 9

Auparavant, l'utilitaire Toolbox ne prenait en charge que les images RHEL UBI 8. Avec cette version, Toolbox prend désormais également en charge RHEL UBI 9. Par conséquent, vous pouvez créer un conteneur Toolbox basé sur RHEL 8 ou 9.

La commande suivante crée un conteneur RHEL basé sur la même version de RHEL que votre système hôte :

```
$ toolbox create
```

Vous pouvez également créer un conteneur avec une version spécifique de RHEL. Par exemple, pour créer un conteneur basé sur RHEL 9.2, utilisez la commande suivante :

```
$ toolbox create --distro rhel --release 9.2
```

Bugzilla:2163752

Nouveau paquet : passt

Cette mise à jour ajoute le paquet **passt**, qui permet d'utiliser le réseau sans racine **pasta** pour les conteneurs.

Par rapport à la connexion **Slirp**, qui est actuellement utilisée par défaut par Podman pour les réseaux non privilégiés, **pasta** apporte les améliorations suivantes :

- Amélioration du débit et meilleure prise en charge de l'IPv6, y compris la prise en charge du protocole NDP (Neighbor Discovery Protocol) et du protocole DHCPv6
- Possibilité de configurer le transfert de ports TCP et UDP sur IPv6

Pour utiliser **pasta** afin de connecter un conteneur Podman, utilisez l'option de ligne de commande **--network pasta**.

Bugzilla:2209419

CHAPITRE 5. CHANGEMENTS IMPORTANTS DANS LES PARAMÈTRES EXTERNES DU NOYAU

Ce chapitre fournit aux administrateurs système un résumé des changements significatifs apportés au noyau distribué avec Red Hat Enterprise Linux 9.2. Ces changements peuvent inclure, par exemple, des entrées **proc** ajoutées ou mises à jour, des valeurs par défaut **sysctl** et **sysfs**, des paramètres de démarrage, des options de configuration du noyau ou tout autre changement de comportement notable.

Nouveaux paramètres du noyau

nomodeset

Ce paramètre du noyau permet de désactiver la configuration du mode noyau. Les pilotes DRM n'effectueront pas de changement de mode d'affichage ni de rendu accéléré. Seule la mémoire tampon du système pourra être utilisée si elle a été configurée par le micrologiciel ou le chargeur de démarrage.
nomodeset est utile comme solution de repli, ou pour les tests et le débogage.

printk.console_no_auto_verbose

Avec ce paramètre du noyau, vous pouvez désactiver l'augmentation du niveau du journal de la console en cas d'oops, de panique ou de problèmes détectés par le lockdep (uniquement si le débogage du verrou est activé). À l'exception des configurations avec un faible débit en bauds sur la console série, définissez ce paramètre à **0** pour fournir plus d'informations de débogage.

- Format : **<bool>**
- La valeur par défaut est **0** (**auto_verbose** est activé)

rcupdate.rcu_exp_cpu_stall_timeout=[KNL]

Ce paramètre du noyau permet de définir le délai d'attente pour les messages d'avertissement de décrochage du CPU de l'UCR accélérée. La valeur est exprimée en millisecondes et la valeur maximale autorisée est de 21 000 millisecondes.
Notez que cette valeur est ajustée à la résolution d'un tic-tac d'arche. En mettant cette valeur à zéro, c'est la valeur de **rcupdate.rcu_cpu_stall_timeout** qui est utilisée (après conversion des secondes en millisecondes).

rcupdate.rcu_task_stall_info=[KNL]

Ce paramètre permet de définir le délai initial en jours pour les messages d'information de décrochage de tâche RCU, qui donnent une indication du problème à ceux qui n'ont pas la patience d'attendre dix minutes. Les messages d'information ne sont imprimés qu'avant le message d'avertissement de décrochage pour un délai de grâce donné. Désactiver avec une valeur inférieure ou égale à zéro.

- La valeur par défaut est **10** secondes.
- Une modification de la valeur ne prend effet qu'au début du prochain délai de grâce.

rcupdate.rcu_task_stall_info_mult=[KNL]

Ce paramètre est un multiplicateur pour l'intervalle de temps entre les messages d'information successifs sur le blocage des tâches RCU pour un délai de grâce des tâches RCU donné. Cette valeur est comprise entre un et dix, inclusivement.
La valeur par défaut est trois, de sorte que le premier message d'information est imprimé 10 secondes après le début du délai de grâce, le deuxième à 40 secondes, le troisième à 160 secondes, puis l'avertissement de décrochage à 600 secondes, ce qui empêcherait l'impression d'un quatrième

message à 640 secondes.

smp.csd_lock_timeout=[KNL]

Avec ce paramètre, vous pouvez spécifier la période de temps en millisecondes pendant laquelle **smp_call_function()** and friends attendra qu'un CPU libère le verrou CSD. Ce paramètre est utile pour diagnostiquer des bogues impliquant des processeurs qui désactivent les interruptions pendant de longues périodes.

- La valeur par défaut est **5,000** millisecondes.
- La valeur zéro désactive cette fonction.
- Cette fonction peut être désactivée plus efficacement en utilisant le paramètre du noyau **csdlock_debug-**.

srcutree.big_cpu_lim=[KNL]

Ce paramètre permet de spécifier le nombre d'unités centrales constituant un système de grande taille, de sorte que les structures **srcu_struct** doivent immédiatement allouer un tableau **srcu_node**.

- La valeur par défaut est **128**.
- ne prend effet que si les quatre bits de poids faible de **srcutree.convert_to_big** sont égaux à **3** (décision au démarrage).

srcutree.convert_to_big=[KNL]

Ce paramètre permet de spécifier les conditions dans lesquelles une structure SRCU arborescente **srcu_struct** sera convertie en grande forme, c'est-à-dire avec un arbre **rcu_node**:

- 0 : Jamais.
- 1 : A l'heure du **init_srcu_struct()**.
- 2 : Lorsque **rcutorture** décide de.
- 3 : Décider au moment du démarrage (par défaut).
- 0x1X : au-dessus de plus si contention élevée.
  Dans les deux cas, l'arbre **srcu_node** sera dimensionné en fonction du nombre réel de CPU pendant l'exécution (**nr_cpu_ids**) et non pas en fonction du nombre de CPU à la compilation **CONFIG_NR_CPUS**.

srcutree.srcu_max_nodelay=[KNL]

Ce paramètre permet de spécifier le nombre d'instances sans délai par jiffy pour lesquelles le fil de travail de la période de grâce SRCU sera réordonnancé avec un délai nul. Au-delà de cette limite, le fil de travail sera réordonnancé avec un délai de sommeil d'un jour.

srcutree.srcu_max_nodelay_phase=[KNL]

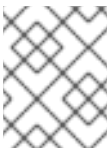
Ce paramètre permet de spécifier, pour chaque phase du délai de grâce, le nombre d'interrogations des lecteurs sans sommeil. Au-delà de cette limite, le thread de travailleur de délai de grâce sera reprogrammé avec un délai de sommeil d'un jiffy, entre chaque rescan des lecteurs, pour une phase de délai de grâce.

srcutree.srcu_retry_check_delay=[KNL]

Ce paramètre permet de spécifier le nombre de microsecondes de délai de non-sommeil entre chaque interrogation de lecteurs sans sommeil.

srcutree.small_contention_lim=[KNL]

Ce paramètre permet de spécifier le nombre d'événements de contention du côté de la mise à jour qui seront tolérés avant d'initier la conversion d'une structure **srcu_struct** en une structure de grande taille.



NOTE

La valeur de **srcutree.convert_to_big** doit avoir le bit 0x10 défini pour que les conversions basées sur la contention se produisent.

Mise à jour des paramètres du noyau

crashkernel=size[KMG][@offset[KMG]]

[KNL] En utilisant **kexec**, Linux peut basculer vers un noyau de crash en cas de panique. Ce paramètre réserve la région de mémoire physique [offset, taille de l'offset] pour cette image du noyau. Si **@offset** est omis, un offset approprié est sélectionné automatiquement.
[KNL, X86-64, ARM64] Sélectionner d'abord une région inférieure à 4G, et se rabattre sur une région de réserve supérieure à 4G lorsque **@offset** n'a pas été spécifié.

Pour plus de détails, voir **Documentation/admin-guide/kdump/kdump.rst**.

crashkernel=size[KMG],low

- [KNL, X86-64, ARM64] Avec ce paramètre, vous pouvez spécifier une mémoire basse inférieure à 4G pour le second noyau. Lorsque **crashkernel=X,high** est passé, cela nécessite une certaine quantité de mémoire basse, par exemple **swiotlb** nécessite au moins 64M 32K de mémoire basse, et suffisamment de mémoire basse supplémentaire est nécessaire pour s'assurer que les tampons DMA pour les périphériques 32 bits ne seront pas épuisés. Le noyau essaiera d'allouer automatiquement une taille de mémoire par défaut inférieure à 4G. La taille par défaut dépend de la plate-forme.
  - x86 : max(swiotlb_size_or_default() 8MiB, 256MiB)
  - arm64 : 128MiB
    0pour désactiver l'allocation faible.

    Ce paramètre sera ignoré si **crashkernel=X,high** n'est pas utilisé ou si la mémoire réservée est inférieure à 4G.
- [KNL, ARM64] Ce paramètre permet de spécifier une plage basse dans la zone DMA pour le noyau de crash dump.
  Ce paramètre est ignoré lorsque **crashkernel=X,high** n'est pas utilisé.

deferred_probe_timeout=[KNL]

Ce paramètre permet de définir un délai en secondes pour que la sonde différée cesse d'attendre les dépendances à sonder. Seules les dépendances spécifiques (sous-systèmes ou pilotes) qui ont opté pour cette option seront ignorées.
Un délai d'attente de **0** expirera à la fin des appels entrants. Si le délai n'a pas expiré, l'option sera relancée à chaque enregistrement de pilote réussi. Cette option éliminera également les périphériques qui se trouvent encore sur la liste des sondes différées après une nouvelle tentative.

driver_async_probe=[KNL]

Ce paramètre permet d'établir une liste de noms de pilotes à interroger de manière asynchrone. * (l'astérisque) correspond à tous les noms de pilotes.

- Si * est spécifié, les autres noms de pilotes listés sont ceux qui ne correspondent PAS à *. Format : **<driver_name1>,<driver_name2>…**

hugetlb_cma=[HW,CMA]

Ce paramètre permet de spécifier la taille d'une zone CMA utilisée pour l'allocation de pages gigantesques. Ou, en utilisant le format nœud, la taille d'une zone CMA par nœud.
Format : **nn[KMGTPE] or (node format) <node>:nn[KMGTPE][,<node>:nn[KMGTPE]]**

Réserver une zone CMA de taille donnée et allouer des pages gigantesques à l'aide de l'allocateur CMA. Si cette option est activée, l'allocation au démarrage de pages gigantesques est ignorée.

hugepages=[HW]

Ce paramètre permet de spécifier le nombre de pages HugeTLB à allouer au démarrage.

- Si elle suit hugepagesz, elle spécifie le nombre de pages de hugepagesz à allouer.
- S'il s'agit du premier paramètre HugeTLB de la ligne de commande, il spécifie le nombre de pages à allouer pour la taille de page énorme par défaut.
- Si l'on utilise le format nœud, le nombre de pages à allouer par nœud peut être spécifié. Voir aussi **Documentation/admin-guide/mm/hugetlbpage.rst**.

  Format : **<integer> or (node format) <node>:<integer>[,<node>:<integer>]**

hugetlb_free_vmemmap=[KNL]

This parameter requires **CONFIG_HUGETLB_PAGE_OPTIMIZE_VMEMMAP** to be enabled. Allows heavy hugetlb users to free up some more memory (7 * PAGE_SIZE for each 2MB hugetlb page).

- Format : **{ [oO][Nn]/Y/y/1 | [oO][Ff]/N/n/0 (default) }**
- [oO][Nn]/Y/y/1 : activer la fonction
- [oO][Ff]/N/n/0 : désactiver la fonction
  Construit avec **CONFIG_HUGETLB_PAGE_OPTIMIZE_VMEMMAP_DEFAULT_ON=y**,

  La valeur par défaut est *on*.

NOTE

Ce paramètre n'est pas compatible avec **memory_hotplug.memmap_on_memory**. Si les deux paramètres sont activés, **hugetlb_free_vmemmap** a la priorité sur **memory_hotplug.memmap_on_memory**.

ivrs_ioapic=[HW,X86-64]

Ce paramètre permet de remplacer la correspondance IOAPIC-ID <-> DEVICE-ID fournie dans le tableau IVRS ACPI.
Par défaut, le segment PCI est **0** et peut être omis. Il peut être omis,

- pour mapper l'IOAPIC-ID décimal 10 au périphérique PCI 00:14.0, écrire le paramètre comme suit :

```
ivrs_ioapic[10]=00:14.0
```

- pour mapper l'IOAPIC-ID décimal 10 au segment PCI 0x1 et au périphérique PCI 00:14.0, écrivez le paramètre comme suit :

```
ivrs_ioapic[10]=0001:00:14.0
```

ivrs_hpet=[HW,X86-64]

Ce paramètre permet de remplacer la correspondance HPET-ID <-> DEVICE-ID fournie dans le tableau IVRS ACPI.
Par défaut, le segment PCI est **0** et peut être omis. Il peut être omis :

- pour affecter le HPET-ID décimal 0 au périphérique PCI 00:14.0, écrivez le paramètre comme suit :

```
ivrs_hpet[0]=00:14.0
```

- pour affecter l'ID HPET décimal 10 au segment PCI 0x1 et au périphérique PCI 00:14.0, écrivez le paramètre comme suit :

```
ivrs_ioapic[10]=0001:00:14.0
```

ivrs_acpihid=[HW,X86-64]

Ce paramètre permet de remplacer la correspondance ACPI-HID:UID <-> DEVICE-ID fournie dans le tableau ACPI du SVI.
Par exemple, pour affecter *UART-HID:UID AMD0020:0* au segment PCI *0x1* et à l'ID de périphérique PCI *00:14.5*, écrivez le paramètre comme suit :

```
ivrs_acpihid[0001:00:14.5]=AMD0020:0
```

Par défaut, le segment PCI est **0** et peut être omis. Par exemple, pour le périphérique PCI *00:14.5*, écrivez le paramètre comme suit :

```
ivrs_acpihid[00:14.5]=AMD0020:0
```

kvm.eager_page_split=[KVM,X86]

Avec ce paramètre, vous pouvez contrôler si KVM essaiera ou non de diviser de manière proactive toutes les pages volumineuses pendant l'enregistrement des données sales.
Le fractionnement avide des pages réduit les interruptions de l'exécution vCPU en éliminant les défauts de protection en écriture et les conflits de verrouillage MMU qui seraient autrement nécessaires pour fractionner paresseusement les pages volumineuses. Les charges de travail VM qui effectuent rarement des écritures ou qui n'écrivent que dans une petite région de la mémoire VM peuvent bénéficier de la désactivation du découpage de page anticipé pour permettre aux pages volumineuses d'être encore utilisées pour les lectures.

Le comportement du fractionnement rapide des pages dépend de l'activation ou de la désactivation de **KVM_DIRTY_LOG_INITIALLY_SET**.

- Si cette option est désactivée, toutes les pages volumineuses d'un lot de mémoire seront scindées avec empressement lorsque la journalisation des erreurs est activée sur ce lot de mémoire.

- Si cette option est activée, le découpage des pages sera effectué lors de l'exécution de l'ioctl **KVM_CLEAR_DIRTY**, et uniquement pour les pages en cours d'effacement.
  Le fractionnement des pages n'est possible que lorsque **kvm.tdp_mmu=Y**.

  La valeur par défaut est **Y** (on).

kvm-arm.mode=[KVM,ARM]

Ce paramètre permet de sélectionner l'un des modes de fonctionnement du KVM/arm64.

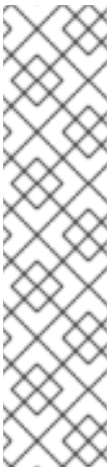
- aucun : Désactivation forcée de KVM.
- nvhe : Mode standard basé sur nVHE, sans prise en charge des invités protégés.
- protected : mode basé sur nVHE avec prise en charge des invités dont l'état est maintenu privé par rapport à l'hôte.
  La valeur par défaut est **VHE**/**nVHE** en fonction du support matériel.

nosmep=[X86,PPC64s]

Ce paramètre permet de désactiver le SMEP (Supervisor Mode Execution Prevention) même s'il est pris en charge par le processeur.
Format : **pci=option[,option…] [PCI] various_PCI_subsystem_options**

Certaines options du présent document s'appliquent à un dispositif spécifique ou à un ensemble de dispositifs (**<pci_dev>**). Elles sont spécifiées dans l'un des formats suivants :

```
[<domain>:]<bus>:<dev>.<func>[/<dev>.<func>]*
pci:<vendor>:<device>[:<subvendor>:<subdevice>]
```



NOTE

- Le premier format spécifie une adresse de bus PCI/dispositif/fonction qui peut changer si un nouveau matériel est inséré, si le micrologiciel de la carte mère change, ou en raison de changements causés par d'autres paramètres du noyau. Si le domaine n'est pas spécifié, il est considéré comme égal à zéro. En option, un chemin d'accès à un périphérique via plusieurs adresses de périphérique et de fonction peut être spécifié après l'adresse de base (ceci est plus robuste contre les problèmes de renumérotation).
- Le deuxième format sélectionne les appareils à l'aide d'identifiants de l'espace de configuration qui peuvent correspondre à plusieurs appareils dans le système.

- earlydump : vidage de l'espace de configuration PCI avant que le noyau ne change quoi que ce soit
- off : [X86] ne pas sonder le bus PCI
- bios : [X86-32] forcer l'utilisation du BIOS PCI, ne pas accéder directement au matériel. Utilisez cette option si votre machine dispose d'un pont hôte PCI non standard.
- nobios : [X86-32] interdire l'utilisation du BIOS PCI, seules les méthodes d'accès direct au matériel sont autorisées. Utilisez cette option si vous rencontrez des plantages au démarrage et que vous pensez qu'ils sont causés par le BIOS.

- conf1 : [X86] Force l'utilisation du mécanisme d'accès à la configuration PCI 1 (adresse de configuration dans le port d'E/S 0xCF8, données dans le port d'E/S 0xCFC, tous deux 32 bits).

- conf2 : [X86] Force l'utilisation du mécanisme d'accès à la configuration PCI 2 (le port d'E/S 0xCF8 est un port 8 bits pour la fonction, le port d'E/S 0xCFA, également 8 bits, définit le numéro de bus. L'espace de configuration est ensuite accessible via les ports *0xC000-0xCFFF*).

  - Voir http://wiki.osdev.org/PCI pour plus d'informations sur les mécanismes d'accès à la configuration.

- noaer : [PCIE] Si le paramètre de configuration du noyau PCIEAER est activé, cette option de démarrage du noyau peut être utilisée pour désactiver l'utilisation des rapports d'erreur avancés PCIE.

- nodomains : [PCI] Désactiver la prise en charge de plusieurs domaines racine PCI (également appelés segments PCI, dans le jargon ACPI).

- nommconf : [X86] Désactiver l'utilisation de MMCONFIG pour la configuration PCI

- check_enable_amd_mmconf [X86] : vérifie et active l'accès MMIO correctement configuré à l'espace de configuration PCI sur les processeurs AMD de la famille 10h

- nomsi : [MSI] Si le paramètre de configuration du noyau **PCI_MSI** est activé, cette option de démarrage du noyau peut être utilisée pour désactiver l'utilisation des interruptions MSI dans l'ensemble du système.

- noioapicquirk : [APIC] Désactive toutes les bizarreries d'interruption de démarrage. Option de sécurité pour garder les IRQ de démarrage activées. Cette option ne devrait jamais être nécessaire.

- ioapicreroute : [APIC] Active le reroutage des IRQ de démarrage vers l'IO-APIC primaire pour les ponts qui ne peuvent pas désactiver les IRQ de démarrage. Cela corrige une source d'IRQ parasites lorsque le système masque les IRQ.

- noioapicreroute [APIC] Désactive la solution de contournement qui utilise l'équivalent d'une IRQ de démarrage qui se connecte à un chipset où les IRQ de démarrage ne peuvent pas être désactivées. C'est le contraire de ioapicreroute.

- biosirq : [X86-32] Utiliser les appels du BIOS PCI pour obtenir la table de routage des interruptions. Ces appels sont connus pour être bogués sur plusieurs machines et ils bloquent la machine lorsqu'ils sont utilisés, mais sur d'autres ordinateurs, c'est le seul moyen d'obtenir la table d'acheminement des interruptions. Essayez cette option si le noyau est incapable d'allouer des IRQ ou de découvrir des bus PCI secondaires sur votre carte mère.

- rom : [X86] Attribue un espace d'adressage aux ROM d'extension. A utiliser avec précaution car certains périphériques partagent des décodeurs d'adresse entre les ROM et d'autres ressources.

- norom : [X86] Ne pas attribuer d'espace d'adressage aux ROM d'extension qui n'ont pas déjà des plages d'adresses attribuées par le BIOS.

- nobar : [X86] Ne pas attribuer d'espace d'adressage aux BAR qui n'ont pas été attribuées par le BIOS.

- irqmask=0xMMMM : [X86] Définit un masque de bits des IRQs autorisées à être assignées automatiquement aux périphériques PCI. Vous pouvez faire en sorte que le noyau exclue les IRQs de vos cartes ISA de cette manière.

- pirqaddr=0xAAAAA : [X86] Spécifier l'adresse physique de la table PIRQ (normalement générée par le BIOS) si elle est en dehors de la plage **F0000h-100000h**.

- lastbus=N : [X86] Analyse tous les bus à partir du bus #N. Peut être utile si le noyau n'arrive pas à trouver vos bus secondaires et que vous voulez lui indiquer explicitement lesquels.

- assign-busses : [X86] Attribue toujours nous-mêmes tous les numéros de bus PCI, sans tenir compte de ce que le microprogramme a pu faire.

- usepirqmask : [X86] Permet d'honorer le masque d'IRQ possible stocké dans la table $PIR du BIOS. Ceci est nécessaire sur certains systèmes dont le BIOS est défectueux, notamment certains ordinateurs portables HP Pavilion N5400 et Omnibook XE3. Cela n'aura aucun effet si le routage ACPI IRQ est activé.

- noacpi : [X86] Ne pas utiliser l'ACPI pour le routage des IRQ ou pour l'analyse PCI.

- use_crs : [X86] Utilise les informations de la fenêtre du pont hôte PCI de l'ACPI. Sur les BIOS de 2008 ou plus récents, cette option est activée par défaut. Si vous avez besoin de l'utiliser, veuillez rapporter un bogue.

- nocrs : [X86] Ignorer les fenêtres du pont hôte PCI de l'ACPI. Si vous avez besoin d'utiliser ceci, veuillez rapporter un bogue.

- use_e820 : [X86] Utiliser les réservations E820 pour exclure certaines parties des fenêtres du pont hôte PCI. Il s'agit d'une solution de contournement pour les défauts du BIOS dans les méthodes _CRS du pont d'hôte. Si vous avez besoin de l'utiliser, veuillez rapporter un bogue à *linux-pci@vger.kernel.org*.

- no_e820 : [X86] Ignore les réservations E820 pour les fenêtres du pont hôte PCI. C'est la valeur par défaut sur le matériel moderne. Si vous avez besoin de l'utiliser, veuillez signaler un bogue à *linux-pci@vger.kernel.org*.

- routeirq : Effectue le routage des IRQ pour tous les périphériques PCI. Cette opération est normalement effectuée à l'adresse **pci_enable_device()**, et cette option est donc une solution temporaire pour les pilotes défectueux qui ne l'appellent pas.

- skip_isa_align : [X86] ne pas aligner l'adresse de départ des entrées/sorties, afin de pouvoir gérer plus de cartes pci

- oearly : [X86] Ne pas faire d'analyse précoce de type 1. Cela peut aider sur certaines cartes cassées qui vérifient la machine lorsque l'espace de configuration de certains périphériques est lu. Mais plusieurs solutions de contournement sont désactivées et certains pilotes IOMMU ne fonctionneront pas.

- bfsort : Trie les périphériques PCI dans l'ordre "breadth-first". Ce tri est effectué pour obtenir un ordre des périphériques compatible avec les anciens noyaux (⇐ 2.4).

- nobfsort : Ne pas trier les périphériques PCI par ordre de priorité.

- pcie_bus_tune_off : Désactive l'accord PCIe MPS (Max Payload Size) et utilise les valeurs par défaut du MPS configurées par le BIOS.

- pcie_bus_safe : Fixer le MPS de chaque dispositif à la plus grande valeur supportée par tous les dispositifs situés en dessous du complexe racine.

- pcie_bus_perf Fixe le MPS du périphérique à la plus grande valeur autorisée pour son bus parent. Réglez également MRRS (Max Read Request Size) sur la plus grande valeur supportée (pas plus grande que le MPS que le périphérique ou le bus peut supporter) pour de meilleures performances.

- pcie_bus_peer2peer : Définir le MPS de chaque périphérique à 128B, ce qui est garanti pour chaque périphérique. Cette configuration permet un DMA peer-to-peer entre n'importe quelle paire d'appareils, éventuellement au prix d'une réduction des performances. Elle garantit également que les périphériques ajoutés à chaud fonctionneront.

- cbiosize=nn[KMG] : La quantité fixe d'espace bus réservée à la fenêtre IO du pont CardBus. La valeur par défaut est *256 bytes*.

- cbmemsize=nn[KMG] : La quantité fixe d'espace de bus réservée à la fenêtre de mémoire du pont CardBus. La valeur par défaut est *64 megabytes*.

- resource_alignment=

  - Format : **[<order of align>@]<pci_dev>[; …]**

  - Spécifie l'alignement et le périphérique pour réaffecter les ressources mémoire alignées. La manière de spécifier le périphérique est décrite ci-dessus. Si **<order of align>** n'est pas spécifié, **PAGE_SIZE** est utilisé comme alignement. Un pont PCI-PCI peut être spécifié si les fenêtres de ressources doivent être étendues. Pour spécifier l'alignement pour plusieurs instances d'un périphérique, le fournisseur PCI, le périphérique, le sous-fournisseur et le sous-dispositif peuvent être spécifiés, par exemple, **12@pci:8086:9c22:103c:198f** pour un alignement de 4096 octets.

- ecrc= : Activer/désactiver PCIe ECRC (vérification CRC de bout en bout de la couche transactionnelle).

  - bios : Utiliser les paramètres du BIOS/firmware. Il s'agit de la valeur par défaut.

  - off : Désactiver la CECR

  - on : Activer l'ECRC.

- hpiosize=nn[KMG] : La quantité fixe d'espace de bus réservée à la fenêtre IO du pont hotplug. La taille par défaut est *256 bytes*.

- hpmmiosize=nn[KMG] : La quantité fixe d'espace de bus réservée à la fenêtre MMIO du pont hotplug. La taille par défaut est *2 megabytes*.

- hpmmioprefsize=nn[KMG] : La quantité fixe d'espace de bus réservée à la fenêtre MMIO_PREF du pont hotplug. La taille par défaut est *2 megabytes*.

- hpmemsize=nn[KMG] : La quantité fixe d'espace de bus réservée aux fenêtres MMIO et MMIO_PREF du pont hotplug. La taille par défaut est *2 megabytes*.

- hpbussize=nn : Le nombre minimum de numéros de bus supplémentaires réservés aux bus situés en dessous d'un pont hotplug. La valeur par défaut est *1*.

- realloc= : Active/désactive la réaffectation des ressources du pont PCI si les allocations effectuées par le BIOS sont trop faibles pour accueillir les ressources requises par tous les périphériques enfants.

    - off : Désactive la fonction de réallocation
    - on : Activer la réallocation
- realloc : identique à realloc=on
- noari : ne pas utiliser PCIe ARI.
- noats : [PCIE, Intel-IOMMU, AMD-IOMMU] n'utilisent pas PCIe ATS (et IOTLB du périphérique IOMMU).
- pcie_scan_all : Analyse tous les périphériques PCIe possibles. Sinon, nous ne recherchons qu'un seul périphérique sous un port PCIe en aval.
- big_root_window : Essaie d'ajouter une grande fenêtre mémoire de 64 bits au complexe racine PCIe sur les processeurs AMD. Certains matériels GFX peuvent redimensionner une BAR pour permettre l'accès à toute la VRAM. L'ajout de la fenêtre est légèrement risqué (elle peut entrer en conflit avec des périphériques non signalés), donc cela entache le noyau.
- disable_acs_redir=<pci_dev>[; ...] : Spécifiez un ou plusieurs périphériques PCI (dans le format spécifié ci-dessus) séparés par des points-virgules. Pour chaque périphérique spécifié, les capacités de redirection PCI ACS seront désactivées, ce qui permettra au trafic P2P entre les périphériques de passer par des ponts sans être forcé en amont. Note : ceci supprime l'isolation entre les appareils et peut placer plus d'appareils dans un groupe IOMMU.
- force_floating : [S390] Force l'utilisation des interruptions flottantes.
- nomio : [S390] Ne pas utiliser les instructions MIO.
- norid : [S390] ignorer le champ RID et forcer l'utilisation d'un domaine PCI par fonction PCI

rcupdate.rcu_cpu_stall_timeout=[KNL]

Définit le délai d'attente pour les messages d'avertissement de décrochage du CPU de la RCU. La valeur est exprimée en secondes et la valeur maximale autorisée est de 300 secondes.

rcupdate.rcu_task_stall_timeout=[KNL]

Ce paramètre permet de définir le délai d'attente en jours pour les messages d'avertissement de blocage de la tâche RCU. Désactiver avec une valeur inférieure ou égale à zéro.
La valeur par défaut est **10** minutes.

Une modification de la valeur ne prend effet qu'au début du prochain délai de grâce.

retbleed=[X86]

Ce paramètre permet de contrôler l'atténuation de la vulnérabilité RETBleed (Arbitrary Speculative Code Execution with Return Instructions).
Les atténuations UNRET et IBPB basées sur AMD n'empêchent pas à elles seules les threads frères d'influencer les prédictions d'autres threads frères. C'est pourquoi STIBP est utilisé sur les processeurs qui le supportent, et l'atténuation SMT sur les processeurs qui ne le supportent pas.

- désactivé - pas d'atténuation
- auto - sélection automatique d'une migration

- auto,nosmt - sélectionne automatiquement une atténuation, en désactivant SMT si nécessaire pour l'atténuation complète (uniquement sur Zen1 et les versions antérieures sans STIBP).
- ibpb - Sur AMD, atténuer également les courtes fenêtres de spéculation sur les limites des blocs de base. Sûr, impact le plus élevé sur les performances. Il active également le STIBP s'il est présent. Ne convient pas à Intel.
- ibpb,nosmt - Comme **ibpb** ci-dessus, mais désactive SMT lorsque STIBP n'est pas disponible. C'est l'alternative pour les systèmes qui n'ont pas de STIBP.
- unret - Force l'activation des thunks de retour non formés, uniquement efficace sur les systèmes basés sur AMD f15h-f17h.
- unret,nosmt - Comme unret, mais désactive SMT lorsque STIBP n'est pas disponible. C'est l'alternative pour les systèmes qui n'ont pas de STIBP.
  La sélection de **auto** permet de choisir une méthode d'atténuation au moment de l'exécution en fonction de l'unité centrale.

  Ne pas spécifier cette option équivaut à **retbleed=auto**.

swiotlb=[ARM,IA-64,PPC,MIPS,X86]

Format : **{ <int> [,<int>] | force | noforce }**

- <int> - Nombre de blocs TLB E/S
- <int> - Deuxième nombre entier après la virgule. Nombre de zones **swiotlb** disposant de leur propre verrou. Ce nombre sera arrondi à une puissance de *2*.
- force - force l'utilisation des tampons de rebond même s'ils ne sont pas automatiquement utilisés par le noyau
- noforce - N'utilise jamais les tampons de rebond (pour le débogage)

Nouveaux paramètres sysctl

kernel.nmi_wd_lpm_factor (PPC uniquement)

Ce facteur représente le pourcentage ajouté à **watchdog_thresh** lors du calcul de la temporisation du chien de garde NMI pendant un LPM. Le délai de verrouillage progressif n'est pas affecté. Utilisez ce facteur pour l'appliquer au délai d'attente du chien de garde NMI (uniquement lorsque **nmi_watchdog** est réglé sur 1).

- Une valeur de **0** signifie qu'il n'y a pas de changement.
- La valeur par défaut est **200**, ce qui signifie que le chien de garde NMI est réglé sur *30s* (sur la base de **watchdog_thresh** égal à *10*).

net.core.txrehash

Avec ce paramètre, vous pouvez contrôler le comportement par défaut de la reconsidération du hachage sur la socket d'écoute lorsque l'option **SO_TXREHASH** est définie sur **SOCK_TXREHASH_DEFAULT** (c'est-à-dire qu'elle n'est pas remplacée par **setsockopt**).

- S'il vaut **1** (valeur par défaut), la reconsidération du hachage est effectuée sur la socket à l'écoute.

- S'il est fixé à **0**, la reconsidération du hachage n'est pas effectuée.

net.sctp.reconf_enable - BOOLEAN

Cette extension permet d'activer ou de désactiver l'extension de la fonctionnalité de reconfiguration de flux spécifiée dans la RFC6525. Cette extension permet de "réinitialiser" un flux et comprend les paramètres **Outgoing/Incoming SSN Reset**, **SSN/TSN Reset** et **Add Outgoing/Incoming Streams**.

- 1 : Activation de l'extension.
- 0 : Désactive l'extension.
- La valeur par défaut est **0**.

net.sctp.intl_enable - BOOLEAN

Cette extension permet d'activer ou de désactiver l'extension de la fonctionnalité d'entrelacement des messages utilisateur spécifiée dans la RFC8260. Cette extension permet l'entrelacement des messages d'utilisateur envoyés sur différents flux. Lorsque cette fonctionnalité est activée, le bloc I-DATA remplace le bloc DATA pour transporter les messages d'utilisateur si l'homologue le prend également en charge. Notez que pour utiliser cette fonctionnalité, vous devez définir cette option à **1** et définir également les options de socket **SCTP_FRAGMENT_INTERLEAVE** à **2** et **SCTP_INTERLEAVING_SUPPORTED** à **1**.

- 1 : Activation de l'extension.
- 0 : Désactive l'extension.
- La valeur par défaut est **0**.

net.sctp.ecn_enable - BOOLEAN

Cette extension permet de contrôler l'utilisation de la notification explicite de congestion (ECN) par le protocole SCTP. Comme pour le TCP, l'ECN n'est utilisé que lorsque les deux extrémités de la connexion SCTP indiquent qu'elles le supportent. Cette fonctionnalité est utile pour éviter les pertes dues à la congestion en permettant aux routeurs de signaler la congestion avant de devoir abandonner les paquets.

- 1 : Activation de l'ECN.
- 0 : Désactivation de l'ECN.
- La valeur par défaut est **1**.

vm.hugetlb_optimize_vmemmap

Ce bouton n'est pas disponible lorsque le paramètre du noyau **memory_hotplug.memmap_on_memory** est configuré ou que la taille de *struct page* (une structure définie dans **include/linux/mm_types.h**) n'est pas une puissance de deux (une configuration inhabituelle du système pourrait en être la cause).
Vous pouvez activer (1) ou désactiver (0) la fonction d'optimisation des pages **vmemmap** associées à chaque page HugeTLB.

- Si cette option est activée, les pages **vmemmap** de l'allocation ultérieure de pages HugeTLB par l'allocateur compagnon seront optimisées (7 pages par page HugeTLB de 2 Mo et 4095 pages par page HugeTLB de 1 Go), tandis que les pages HugeTLB déjà allouées ne seront

pas optimisées. Lorsque ces pages HugeTLB optimisées sont libérées du pool HugeTLB vers l'allocateur compagnon, les pages **vmemmap** représentant cette plage doivent être remappées et les pages **vmemmap** écartées précédemment doivent être réattribuées.

- Si votre cas d'utilisation est que les pages HugeTLB sont allouées de manière impromptue (par exemple, ne jamais allouer explicitement des pages HugeTLB avec **nr_hugepages** mais seulement définir **nr_overcommit_hugepages**, ces pages HugeTLB sur-engagées sont allouées de manière impromptue) au lieu d'être tirées du pool HugeTLB, vous devriez évaluer les avantages des économies de mémoire par rapport à la surcharge (~2x plus lente qu'avant) de l'allocation ou de la libération des pages HugeTLB entre le pool HugeTLB et l'allocateur de copains. Un autre comportement à noter est que si le système est soumis à une forte pression de mémoire, il peut empêcher l'utilisateur de libérer des pages HugeTLB entre le pool HugeTLB et l'allocateur compagnon puisque l'allocation des pages **vmemmap** peut échouer, vous devez réessayer plus tard si votre système est confronté à cette situation.

- Si cette option est désactivée, les pages **vmemmap** de l'allocation ultérieure de pages HugeTLB par l'allocateur compagnon ne seront pas optimisées, ce qui signifie que la surcharge supplémentaire au moment de l'allocation par l'allocateur compagnon disparaît, alors que les pages HugeTLB déjà optimisées ne seront pas affectées. Si vous voulez vous assurer qu'il n'y a pas de pages HugeTLB optimisées, vous pouvez d'abord définir **nr_hugepages** en **0**, puis désactiver cette fonction. Notez que l'écriture de **0** à **nr_hugepages** transformera toutes les pages HugeTLB de *in use* en pages excédentaires. Ces pages excédentaires sont donc optimisées jusqu'à ce qu'elles ne soient plus utilisées. Vous devrez attendre que ces pages excédentaires soient libérées avant qu'il n'y ait plus de pages optimisées dans le système.

net.core.rps_default_mask

Masque par défaut de l'unité centrale de RPS utilisé sur les périphériques réseau nouvellement créés. Un masque vide signifie que le RPS est désactivé par défaut.

Modification des paramètres sysctl

kernel.numa_balancing

Ce paramètre permet d'activer, de désactiver et de configurer l'équilibrage automatique de la mémoire NUMA basé sur les défauts de page. La mémoire est déplacée automatiquement vers les nœuds qui y accèdent souvent. La valeur à définir peut être le résultat de la combinaison OU des éléments suivants :

```
= ================================
0 NUMA_BALANCING_DISABLED
1 NUMA_BALANCING_NORMAL
2 NUMA_BALANCING_MEMORY_TIERING
= ================================
```

Ou **NUMA_BALANCING_NORMAL** pour optimiser le placement des pages entre les différents nœuds NUMA afin de réduire l'accès à distance. Sur les machines NUMA, l'accès à la mémoire distante par un processeur entraîne une perte de performance. Lorsque cette fonctionnalité est activée, le noyau échantillonne le thread de tâche qui accède à la mémoire en désapprouvant périodiquement les pages et en piégeant ensuite un défaut de page. Au moment du défaut de page, il est déterminé si les données accédées doivent être migrées vers un nœud de mémoire locale.

Ou **NUMA_BALANCING_MEMORY_TIERING** pour optimiser le placement des pages entre les différents types de mémoire (représentés par différents nœuds NUMA) afin de placer les pages chaudes dans la mémoire rapide. Cette méthode est également mise en œuvre sur la base du

démappage et du défaut de page.

net.ipv6.route.max_size

Cette fonction est désormais obsolète pour l'ipv6, car le ramassage des ordures gère les entrées d'itinéraires mises en cache.

net.sctp.sctp_wmem

Cette option était auparavant documentée comme n'ayant aucun effet. Désormais, seule la première valeur (**min**) est utilisée, **default** et **max** sont ignorés.

- min : taille minimale du tampon d'envoi pouvant être utilisé par les sockets SCTP. Elle est garantie à chaque socket SCTP (mais pas à l'association) même en cas de pression modérée sur la mémoire.
- La valeur par défaut est **4K**.

CHAPITRE 6. PILOTES DE PÉRIPHÉRIQUES

6.1. NOUVEAUX CONDUCTEURS

- Pilote vidéo ACPI (**video**), uniquement pour l'architecture ARM 64 bits
- Pilote CXL pour les dispositifs d'extrémité de mémoire CXL et les commutateurs pour l'expansion de la mémoire (**cxl_mem**)
- Noyau du récepteur GNSS (**gnss**)
- Module de simulation GPIO (**gpio-sim**), uniquement pour l'architecture ARM 64 bits
- Pilote GPIO VirtIO (**gpio-virtio**), uniquement pour l'architecture ARM 64 bits
- Pilote NVIDIA Tegra HTE (Hardware Timestamping Engine) (**hte-tegra194**), uniquement pour l'architecture ARM 64 bits
- Pilote d'adaptateur I2C pour le bus LPI2C (**i2c-imx-lpi2c**), uniquement dans l'architecture ARM 64 bits
- Pilote de bus Virtio i2c (**i2c-virtio**), uniquement pour l'architecture ARM 64 bits
- Prise en charge du pilote de niveau utilisateur pour le sous-système d'entrée (**uinput**), uniquement dans l'architecture ARM 64 bits
- Module qui implémente des fonctions communes qui peuvent être utilisées par l'hôte nvme ou les pilotes cibles (**nvme-common**)
- AMD PMC Driver (**amd-pmc**), uniquement pour les architectures AMD et Intel 64 bits
- Pilote de plate-forme Nvidia sn2201 (**nvsw-sn2201**), uniquement pour les architectures AMD et Intel 64 bits
- Serial multi instantiate pseudo device driver (**serial-multi-instantiate**), uniquement dans les architectures AMD et Intel 64-bit
- Pilote RTC Micro Crystal RV8803 (**rtc-rv8803**), uniquement pour les architectures ARM 64 bits et les architectures AMD et Intel 64 bits
- Pilote de contrôleur QSPI NVIDIA Tegra (**spi-tegra210-quad**), uniquement pour l'architecture ARM 64 bits
- Pilote UCSI pour le contrôleur Cypress CCGx Type-C (**ucsi_ccg**), uniquement dans l'architecture ARM 64 bits
- Calcul confidentiel Accès à la zone secrète de l'EFI (**efi_secret**), uniquement sur les architectures AMD et Intel 64 bits
- TDX Guest Driver (**tdx-guest**), uniquement pour les architectures AMD et Intel 64 bits
- Pilote de chien de garde HPE (**hpwdt**), uniquement dans l'architecture ARM 64 bits
- POWER Architecture Platform Watchdog Driver (**pseries-wdt**), uniquement dans IBM Power Systems, Little Endian

Pilotes de réseau

- Pilote pour le trafic encapsulé VXLAN (**vxlan**)
- Marvell OcteonTX2 RVU Admin Function Driver (**rvu_af**), uniquement en architecture ARM 64 bits
- Marvell RVU NIC Physical Function Driver (**rvu_nicpf**), uniquement dans l'architecture ARM 64 bits
- Pilote PTP Marvell RVU NIC (**otx2_ptp**), uniquement pour l'architecture ARM 64 bits
- Marvell RVU NIC Virtual Function Driver (**rvu_nicvf**), uniquement dans l'architecture ARM 64 bits
- Pilote NVIDIA Tegra MGBE (**dwmac-tegra**), uniquement pour l'architecture ARM 64 bits
- Interface CAN à ligne série (**slcan**), uniquement dans l'architecture ARM 64 bits
- Pilote réseau Solarflare Siena (**sfc-siena**), uniquement pour IBM Power Systems, Little Endian et les architectures AMD et Intel 64 bits

Pilotes graphiques et divers

- DRM Buddy Allocator (**drm_buddy**), uniquement dans l'architecture ARM 64 bits et IBM Power Systems, Little Endian
- DRM display adapter helper (**drm_display_helper**), uniquement dans l'architecture ARM 64 bits, IBM Power Systems, Little Endian, et les architectures AMD et Intel 64 bits
- DRM DisplayPort AUX bus (**drm_dp_aux_bus**), uniquement dans l'architecture ARM 64 bits
- Pilote Host1x pour les produits Tegra (**host1x**), uniquement en architecture ARM 64 bits
- Pilote DRM NVIDIA Tegra (**tegra-drm**), uniquement pour l'architecture ARM 64 bits
- Intel® GVT-g pour KVM (**kvmgt**), uniquement pour les architectures AMD et Intel 64 bits
- Processeur de gestion HP® iLO/iLO2 (**hpilo**), uniquement en architecture ARM 64 bits
- Pilote auxiliaire Intel® pour les périphériques GSC (**mei-gsc**), uniquement dans les architectures AMD et Intel 64 bits

6.2. PILOTES MIS À JOUR

Mises à jour des pilotes de stockage

- Le pilote pour Microchip Smart Family Controller (**smartpqi**) a été mis à jour à la version 2.1.20-035 (uniquement pour l'architecture ARM 64 bits, IBM Power Systems, Little Endian, et les architectures AMD et Intel 64 bits).
- Le pilote SCSI Emulex LightPulse Fibre Channel (**lpfc**) a été mis à jour vers la version 14.2.0.8 (uniquement pour l'architecture ARM 64 bits, IBM Power Systems, Little Endian, et les architectures AMD et Intel 64 bits).
- MPI3 Storage Controller Device Driver (**mpi3mr**) a été mis à jour à la version 8.2.0.3.0.

- Le pilote de l'adaptateur de débogage CSI (**scsi_debug**) a été mis à jour à la version 0191.
- Le pilote de périphérique LSI MPT Fusion SAS 3.0 (**mpt3sas**) a été mis à jour vers la version 43.100.00.00 (uniquement pour les architectures 64 bits ARM, IBM Power Systems, Little Endian, et les architectures 64 bits AMD et Intel).

CHAPITRE 7. CARACTÉRISTIQUES DU FBP DISPONIBLES

Ce chapitre fournit la liste complète des fonctionnalités de **Berkeley Packet Filter** (**BPF**) disponibles dans le noyau de cette version mineure de Red Hat Enterprise Linux 9. Les tableaux incluent les listes de :

- Configuration du système et autres options
- Types de programmes disponibles et aides prises en charge
- Types de cartes disponibles

Ce chapitre contient les résultats générés automatiquement par la commande **bpftool feature**.

Tableau 7.1. Configuration du système et autres options

Option	Valeur
non privilégié_bpf_désactivé	2 (bpf() syscall restreint aux utilisateurs privilégiés, l'administrateur peut le modifier)
Compilateur JIT	1 (activé)
Durcissement du compilateur JIT	1 (activé pour les utilisateurs non privilégiés)
Compilateur JIT kallsyms exports	1 (activé pour la racine)
Limite de mémoire pour JIT pour les utilisateurs non privilégiés	264241152
CONFIG_BPF	y
CONFIG_BPF_SYSCALL	y
CONFIG_HAVE_EBPF_JIT	y
CONFIG_BPF_JIT	y
CONFIG_BPF_JIT_ALWAYS_ON	y
CONFIG_DEBUG_INFO_BTF	y
CONFIG_DEBUG_INFO_BTF_MODULES	y
CONFIG_CGROUPS	y
CONFIG_CGROUP_BPF	y
CONFIG_CGROUP_NET_CLASSID	y

Option	Valeur
CONFIG_SOCK_CGROUP_DATA	y
CONFIG_BPF_EVENTS	y
CONFIG_KPROBE_EVENTS	y
CONFIG_UPROBE_EVENTS	y
CONFIG_TRACING	y
CONFIG_FTRACE_SYSCALLS	y
CONFIG_FUNCTION_ERROR_INJECTION	y
CONFIG_BPF_KPROBE_OVERRIDE	n
CONFIG_NET	y
CONFIG_XDP_SOCKETS	y
CONFIG_LWTUNNEL_BPF	y
CONFIG_NET_ACT_BPF	m
CONFIG_NET_CLS_BPF	m
CONFIG_NET_CLS_ACT	y
CONFIG_NET_SCH_INGRESS	m
CONFIG_XFRM	y
CONFIG_IP_ROUTE_CLASSID	y
CONFIG_IPV6_SEG6_BPF	n
CONFIG_BPF_LIRC_MODE2	n
CONFIG_BPF_STREAM_PARSER	y
CONFIG_NETFILTER_XT_MATCH_BPF	m
CONFIG_BPFILTER	n

Option	Valeur
CONFIG_BPFILTER_UMH	n
CONFIG_TEST_BPF	m
CONFIG_HZ	1000
bpf() syscall	disponible
Limite de taille des programmes	disponible
Support de boucle limité	disponible
Extension ISA v2	disponible
Extension ISA v3	disponible

Tableau 7.2. Types de programmes disponibles et aides prises en charge

Type de programme	Aides disponibles
filtre_socket	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_strtr, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
kprobe	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_group_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
sched_cls	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_skb_set_tstamp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6

Type de programme	Aides disponibles
sched_act	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_vlan_push, bpf_skb_vlan_pop, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_change_proto, bpf_skb_change_type, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_set_hash, bpf_skb_adjust_room, bpf_skb_get_xfrm_state, bpf_skb_load_bytes_relative, bpf_fib_lookup, bpf_skb_cgroup_id, bpf_skb_ancestor_cgroup_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_skb_cgroup_classid, bpf_redirect_neigh, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_redirect_peer, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_skb_set_tstamp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6

Type de programme	Aides disponibles
point de traçage	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_group_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
xdp	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_redirect, bpf_perf_event_output, bpf_csum_diff, bpf_get_current_task, bpf_get_numa_node_id, bpf_xdp_adjust_head, bpf_redirect_map, bpf_xdp_adjust_meta, bpf_xdp_adjust_tail, bpf_fib_lookup, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_tcp_check_syncookie, bpf_tcp_gen_syncookie, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_check_mtu, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_xdp_get_buff_len, bpf_xdp_load_bytes, bpf_xdp_store_bytes, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data, bpf_tcp_raw_gen_syncookie_ipv4, bpf_tcp_raw_gen_syncookie_ipv6, bpf_tcp_raw_check_syncookie_ipv4, bpf_tcp_raw_check_syncookie_ipv6

Type de programme	Aides disponibles
perf_event	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_perf_prog_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_read_branch_records, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_group_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_get_attach_cookie, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
cgroup_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_load_bytes_relative, bpf_skb_cgroup_id, bpf_get_local_storage, bpf_skb_ancestor_group_id, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_fullsock, bpf_tcp_sock, bpf_skb_ecn_set_ce, bpf_get_listener_sock, bpf_skc_lookup_tcp, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_sk_cgroup_id, bpf_sk_ancestor_group_id, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
cgroup_sock	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_storage_get, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
lwt_in	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_lwt_push_encap, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
lwt_out	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
lwt_xmit	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_l3_csum_replace, bpf_l4_csum_replace, bpf_tail_call, bpf_clone_redirect, bpf_get_cgroup_classid, bpf_skb_get_tunnel_key, bpf_skb_set_tunnel_key, bpf_redirect, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_get_tunnel_opt, bpf_skb_set_tunnel_opt, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_csum_update, bpf_set_hash_invalid, bpf_get_numa_node_id, bpf_skb_change_head, bpf_lwt_push_encap, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_csum_level, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
sock_ops	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_sock_map_update, bpf_getsockopt, bpf_sock_ops_cb_flags_set, bpf_sock_hash_update, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_load_hdr_opt, bpf_store_hdr_opt, bpf_reserve_hdr_opt, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
sk_skb	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_skb_store_bytes, bpf_tail_call, bpf_perf_event_output, bpf_skb_load_bytes, bpf_get_current_task, bpf_skb_change_tail, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_skb_change_head, bpf_get_socket_cookie, bpf_get_socket_uid, bpf_skb_adjust_room, bpf_sk_redirect_map, bpf_sk_redirect_hash, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
cgroup_device	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
sk_msg	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_msg_redirect_map, bpf_msg_apply_bytes, bpf_msg_cork_bytes, bpf_msg_pull_data, bpf_msg_redirect_hash, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_msg_push_data, bpf_msg_pop_data, bpf_spin_lock, bpf_spin_unlock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_group_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
raw_tracepoint	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_group_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
cgroup_sock_addr	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_get_cgroup_classid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_setsockopt, bpf_getsockopt, bpf_bind, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_sk_lookup_tcp, bpf_sk_lookup_udp, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_skc_lookup_tcp, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
lwt_seg6local	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_cgroup_classid, bpf_get_route_realm, bpf_perf_event_output, bpf_skb_load_bytes, bpf_csum_diff, bpf_skb_under_cgroup, bpf_get_hash_recalc, bpf_get_current_task, bpf_skb_pull_data, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
lirc_mode2	non pris en charge
sk_reuseport	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_socket_cookie, bpf_skb_load_bytes_relative, bpf_sk_select_reuseport, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
flow_dissector	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_skb_load_bytes, bpf_get_current_task, bpf_get_numa_node_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
cgroup_sysctl	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sysctl_get_name, bpf_sysctl_get_current_value, bpf_sysctl_get_new_value, bpf_sysctl_set_new_value, bpf_strtol, bpf_strtoul, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_strtr, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Type de programme	Aides disponibles
raw_tracepoint_writable	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_send_signal, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_get_current_ancestor_group_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_get_task_stack, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
cgroup_sockopt	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_uid_gid, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_get_current_cgroup_id, bpf_get_local_storage, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_tcp_sock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_get_netns_cookie, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_loop, bpf_strncmp, bpf_get_retval, bpf_set_retval, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
traçage	non pris en charge
struct_ops	non pris en charge
ext	non pris en charge
lsm	non pris en charge

Type de programme	Aides disponibles
sk_lookup	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_perf_event_output, bpf_get_current_task, bpf_get_numa_node_id, bpf_sk_release, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_jiffies64, bpf_sk_assign, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_get_current_task_btf, bpf_ktime_get_coarse_ns, bpf_for_each_map_elem, bpf_snprintf, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_task_pt_regs, bpf_skc_to_unix_sock, bpf_loop, bpf_strncmp, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data
syscall	bpf_map_lookup_elem, bpf_map_update_elem, bpf_map_delete_elem, bpf_probe_read, bpf_ktime_get_ns, bpf_get_prandom_u32, bpf_get_smp_processor_id, bpf_tail_call, bpf_get_current_pid_tgid, bpf_get_current_uid_gid, bpf_get_current_comm, bpf_perf_event_read, bpf_perf_event_output, bpf_get_stackid, bpf_get_current_task, bpf_current_task_under_cgroup, bpf_get_numa_node_id, bpf_probe_read_str, bpf_get_socket_cookie, bpf_perf_event_read_value, bpf_get_stack, bpf_get_current_cgroup_id, bpf_map_push_elem, bpf_map_pop_elem, bpf_map_peek_elem, bpf_spin_lock, bpf_spin_unlock, bpf_sk_storage_get, bpf_sk_storage_delete, bpf_send_signal, bpf_skb_output, bpf_probe_read_user, bpf_probe_read_kernel, bpf_probe_read_user_str, bpf_probe_read_kernel_str, bpf_send_signal_thread, bpf_jiffies64, bpf_get_ns_current_pid_tgid, bpf_xdp_output, bpf_get_current_ancestor_cgroup_id, bpf_ktime_get_boot_ns, bpf_ringbuf_output, bpf_ringbuf_reserve, bpf_ringbuf_submit, bpf_ringbuf_discard, bpf_ringbuf_query, bpf_skc_to_tcp6_sock, bpf_skc_to_tcp_sock, bpf_skc_to_tcp_timewait_sock, bpf_skc_to_tcp_request_sock, bpf_skc_to_udp6_sock, bpf_get_task_stack, bpf_d_path, bpf_copy_from_user, bpf_snprintf_btf, bpf_per_cpu_ptr, bpf_this_cpu_ptr, bpf_task_storage_get, bpf_task_storage_delete, bpf_get_current_task_btf, bpf_sock_from_file, bpf_for_each_map_elem, bpf_snprintf, bpf_sys_bpf, bpf_btf_find_by_name_kind, bpf_sys_close, bpf_timer_init, bpf_timer_set_callback, bpf_timer_start, bpf_timer_cancel, bpf_get_func_ip, bpf_task_pt_regs, bpf_get_branch_snapshot, bpf_skc_to_unix_sock, bpf_kallsyms_lookup_name, bpf_find_vma, bpf_loop, bpf_strncmp, bpf_xdp_get_buff_len, bpf_copy_from_user_task, bpf_kptr_xchg, bpf_map_lookup_percpu_elem, bpf_skc_to_mptcp_sock, bpf_dynptr_from_mem, bpf_ringbuf_reserve_dynptr, bpf_ringbuf_submit_dynptr, bpf_ringbuf_discard_dynptr, bpf_dynptr_read, bpf_dynptr_write, bpf_dynptr_data

Tableau 7.3. Types de cartes disponibles

Type de carte	Disponible
hachage	yes

Type de carte	Disponible
réseau	yes
prog_array	yes
perf_event_array	yes
percpu_hash	yes
tableau percpu_	yes
trace_de_pile	yes
cgroup_array	yes
lru_hash	yes
lru_percpu_hash	yes
lpm_trie	yes
array_of_maps	yes
hash_of_maps	yes
carte de données	yes
carte du stock	yes
cpumap	yes
xskmap	yes
sockhash	yes
cgroup_storage	yes
reuseport_sockarray	yes
percpu_cgroup_storage	yes
file d'attente	yes
pile	yes
sk_storage	yes

Type de carte	Disponible
devmap_hash	yes
struct_ops	yes
ringbuf	yes
inode_storage	yes
stockage_de_tâches	yes
bloom_filter	yes

CHAPITRE 8. BUG FIXES

Cette partie décrit les bogues corrigés dans Red Hat Enterprise Linux 9.2 qui ont un impact significatif sur les utilisateurs.

8.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

Le programme d'installation affiche désormais correctement l'espace disque total dans le cas d'un partitionnement personnalisé avec des périphériques RAID multipath ou DDF

Auparavant, lorsque le partitionnement personnalisé était sélectionné dans l'installateur sur un système doté d'un périphérique RAID multipath ou DDF, l'espace disque total n'était pas indiqué correctement et les périphériques de disque membres étaient répertoriés comme étant disponibles pour le partitionnement.

Avec cette mise à jour, le partitionnement personnalisé dans l'installateur indique une valeur correcte pour l'espace disque total et ne permet d'utiliser que le périphérique DDF RAID ou multipath dans son ensemble.

Bugzilla:2052938

L'installateur ajoute désormais correctement les options de configuration dans les fichiers yum repo

Auparavant, le programme d'installation n'ajoutait pas correctement les options de configuration dans les fichiers yum repo lors de l'inclusion et de l'exclusion de paquets provenant de dépôts d'installation supplémentaires. Avec cette mise à jour, les fichiers yum repo sont créés correctement. Par conséquent, l'utilisation des options **--excludepkgs=** ou **--includepkgs=** dans la commande **repo** kickstart exclut ou inclut les paquets spécifiés pendant l'installation, comme prévu.

Bugzilla:2158210

L'utilisation de l'option DHCP **filename** ne bloque plus le téléchargement du fichier **kickstart** pour l'installation

Auparavant, lors de la création d'un chemin d'accès pour obtenir le fichier kickstart à partir d'un serveur NFS, le programme d'installation ne prenait pas en compte l'option DHCP **filename**. Par conséquent, le programme d'installation ne téléchargeait pas le fichier kickstart et bloquait le processus d'installation. Avec cette mise à jour, l'option DHCP **filename** construit correctement un chemin vers le fichier kickstart. Par conséquent, le fichier kickstart est téléchargé correctement et le processus d'installation démarre correctement.

Bugzilla:1991843

Le programme d'installation crée désormais une nouvelle configuration de disque GPT lors du partitionnement personnalisé

Auparavant, le programme d'installation ne modifiait pas l'agencement du disque en GPT lorsque **inst.gpt** était spécifié sur la ligne de commande du noyau, et l'utilisateur supprimait toutes les partitions d'un disque avec l'agencement MBR sur le rayon de partitionnement personnalisé. Par conséquent, l'agencement du disque MBR est resté sur le disque.

Avec cette mise à jour, le programme d'installation crée une nouvelle disposition GPT sur le disque si **inst.gpt** est spécifié dans la ligne de commande du noyau, et toutes les partitions sont supprimées d'un disque sur les rayons de partitionnement personnalisé.

Bugzilla:2127100

L'installateur répertorie désormais toutes les partitions PPC PreP Boot ou BIOS Boot lors d'un partitionnement personnalisé

Auparavant, lors de l'ajout de plusieurs partitions **PPC PreP Boot** ou **BIOS Boot** pendant le partitionnement personnalisé, l'écran Partitionnement personnalisé n'affichait qu'une seule partition d'un type apparenté. Par conséquent, l'écran de partitionnement personnalisé ne reflétait pas l'état réel de la disposition de partitionnement prévue, ce qui rendait le processus de partitionnement difficile et non transparent.

Avec cette mise à jour, l'écran Partitionnement personnalisé affiche correctement toutes les partitions **PPC PreP Boot** ou **BIOS Boot** dans la liste des partitions. Les utilisateurs peuvent ainsi mieux comprendre et gérer l'agencement prévu du partitionnement.

Bugzilla:2093793

8.2. GESTION DES ABONNEMENTS

Le gestionnaire d'abonnement ne refuse plus l'enregistrement et la récupération du contenu Red Hat

Auparavant, **subscription-manager** fonctionnait en mode conteneur lorsqu'il était exécuté sous OpenShift Container Platform (OCP) en raison de l'amélioration de la logique de détection des conteneurs dans RHEL 9. Par conséquent, le système n'était pas en mesure d'utiliser les informations d'identification de l'abonnement fournies et ne récupérait donc pas le contenu Red Hat.

Cette mise à jour a corrigé la logique de détection des conteneurs de sorte que **subscription-manager** fonctionnant sous OCP ne détecte pas le système (c'est-à-dire le pod en cours d'exécution) comme un conteneur. Par conséquent, vous pouvez maintenant utiliser les identifiants d'abonnement fournis ou même vous enregistrer en utilisant vos propres identifiants pour récupérer le contenu Red Hat à partir d'un conteneur OpenShift.

Bugzilla:2108549

subscription-manager ne conserve plus le texte non essentiel dans le terminal

À partir de RHEL 9.1, **subscription-manager** affiche des informations de progression pendant le traitement de toute opération. Auparavant, pour certaines langues, généralement non latines, les messages de progression n'étaient pas nettoyés à la fin de l'opération. Avec cette mise à jour, tous les messages sont nettoyés correctement à la fin de l'opération.

Si vous avez désactivé les messages de progression, vous pouvez les réactiver en entrant la commande suivante :

```
# subscription-manager config --rhsm.progress_messages=1
```

Bugzilla:2136694

8.3. GESTION DES LOGICIELS

RPM ne se bloque plus lors d'une transaction impliquant le redémarrage du service fapolicyd

Auparavant, si vous essayiez de mettre à jour un paquet qui entraînait le redémarrage du service **fapolicyd**, par exemple **systemd**, la transaction RPM cessait de répondre parce que le plug-in **fapolicyd** ne parvenait pas à communiquer avec le démon **fapolicyd**.

Avec cette mise à jour, le plug-in **fapolicyd** communique désormais correctement avec le démon **fapolicyd**. Par conséquent, RPM ne se bloque plus lors d'une transaction impliquant le redémarrage du service **fapolicyd**.

Bugzilla:2111251

L'annulation d'une transaction de mise à niveau DNF est désormais possible pour un groupe de paquets ou un environnement

Auparavant, la commande **dnf history rollback** échouait lors d'une tentative d'annulation d'une transaction de mise à niveau pour un groupe de paquets ou un environnement.

Avec cette mise à jour, le problème a été corrigé et vous pouvez maintenant annuler la transaction de mise à niveau DNF pour un groupe de paquets ou un environnement.

Bugzilla:2122626

La mise à jour des DNF de sécurité est désormais possible pour les paquets dont l'architecture est modifiée par la mise à jour

Le correctif pour BZ#2108969 introduit avec RHBA-2022:8295 a causé une régression où la mise à niveau DNF utilisant des filtres de sécurité a ignoré les paquets qui ont changé leur architecture de ou à **noarch** à travers la mise à niveau. Par conséquent, les mises à jour de sécurité manquantes pour ces paquets pouvaient laisser le système dans un état vulnérable.

Avec cette mise à jour, le problème a été corrigé et la mise à niveau DNF de sécurité ne saute plus les paquets qui changent d'architecture de ou vers **noarch**.

Bugzilla:2124480

Les fichiers Qt message QM avec des noms de 3 lettres sont maintenant empaquetés lorsqu'un paquet RPM est construit ou reconstruit

Auparavant, le script **find-lang.sh** ne pouvait pas trouver les fichiers Qt message QM (**.qm**) dont les noms étaient composés de 3 caractères. Par conséquent, ces fichiers n'étaient pas ajoutés à un paquetage RPM.

Avec cette mise à jour, le problème a été corrigé et les fichiers QM des messages Qt à 3 lettres peuvent maintenant être empaquetés lors de la construction ou de la reconstruction d'un RPM.

Bugzilla:2144005

8.4. SHELLS ET OUTILS DE LIGNE DE COMMANDE

ReaR gère correctement les DASD exclus sur l'architecture IBM Z

Auparavant, sur l'architecture IBM Z, ReaR reformatait tous les périphériques de stockage à accès direct (DASD) connectés pendant le processus de récupération, y compris les DASD que les utilisateurs excluaient de la configuration sauvegardée et dont ils n'avaient pas l'intention de restaurer le contenu. Par conséquent, si vous excluiez certains DASD de la configuration sauvegardée, leurs données étaient perdues lors de la restauration du système. Avec cette mise à jour, ReaR ne formate plus les DASD exclus lors de la restauration du système, y compris le périphérique à partir duquel le système de secours ReaR a été démarré (à l'aide du chargeur de démarrage zIPL). Vous êtes également invité à confirmer le script de formatage du DASD avant que ReaR ne reformate les DASD. Cela permet de s'assurer que les données des DASD exclus survivent à une restauration du système.

Bugzilla:2172589

ReaR n'échoue plus à restaurer des systèmes de fichiers XFS non-LVM

Auparavant, lorsque vous utilisiez ReaR pour restaurer un système de fichiers XFS non LVM avec certains paramètres et un mappage de disque, ReaR créait le système de fichiers avec les paramètres par défaut au lieu des paramètres spécifiés. Par exemple, si vous aviez un système de fichiers avec les paramètres **sunit** et **swidth** définis sur des valeurs non nulles et que vous restauriez le système de fichiers à l'aide de ReaR avec un mappage de disque, le système de fichiers était créé avec les paramètres par défaut **sunit** et **swidth** en ignorant les valeurs spécifiées. En conséquence, ReaR échouait lors du montage du système de fichiers avec des options XFS spécifiques. Avec cette mise à jour, ReaR restaure correctement le système de fichiers avec les paramètres spécifiés.

Bugzilla:2160748

wsmancli gère correctement les statuts HTTP 401 non autorisés

L'utilitaire **wsmancli** pour la gestion des systèmes utilisant le protocole de gestion des services Web gère désormais l'authentification pour mieux se conformer à la RFC 2616.

Auparavant, lors de la connexion à un service nécessitant une authentification, la commande **wsmancli** renvoyait le message d'erreur **Authentication failed, please retry** immédiatement après avoir reçu une réponse HTTP 401 non autorisée, par exemple, en raison d'informations d'identification incomplètes. Pour continuer, **wsmancli** vous invitait à fournir à la fois le nom d'utilisateur et le mot de passe, même dans les cas où vous aviez déjà fourni une partie de vos informations d'identification.

Avec cette mise à jour, **wsmancli** ne demande que des informations d'identification qui n'ont pas été fournies précédemment. Par conséquent, la première tentative d'authentification n'affiche aucun message d'erreur. Un message d'erreur ne s'affiche qu'une fois que vous avez fourni toutes les informations d'identification et que l'authentification a échoué.

Bugzilla:2127416

8.5. SÉCURITÉ

USBGuard enregistre les règles même si RuleFile n'est pas défini

Auparavant, si la directive de configuration **RuleFile** dans USBGuard était définie mais que **RuleFolder** ne l'était pas, le jeu de règles ne pouvait pas être modifié. Avec cette mise à jour, vous pouvez désormais modifier le jeu de règles même si RuleFolder est défini mais pas RuleFile. Par conséquent, vous pouvez modifier la politique permanente dans USBGuard pour enregistrer de manière permanente les règles nouvellement ajoutées.

Bugzilla:2155910

python-sqlalchemy repassé à la version 1.4.45

Le paquetage **python-sqlalchemy** a été rebasé à la version 1.4.45, qui apporte de nombreuses corrections de bogues par rapport à la version 1.4.37. Cette version contient notamment un correctif pour un bogue de mémoire critique dans la génération de la clé de cache.

Bugzilla:2152649

crypto-policies désactive maintenant NSEC3DSA pour BIND

Auparavant, les règles cryptographiques applicables à l'ensemble du système ne contrôlaient pas l'algorithme NSEC3DSA dans la configuration de BIND. Par conséquent, NSEC3DSA, qui ne répond pas aux exigences de sécurité actuelles, n'était pas désactivé sur les serveurs DNS. Avec cette mise à jour, toutes les politiques cryptographiques désactivent par défaut NSEC3DSA dans la configuration BIND.

Bugzilla:2152635

OpenSSL dans SECLEVEL=3 fonctionne désormais avec les suites de chiffrement PSK

Auparavant, les suites de chiffrement à clé pré-partagée (PSK) n'étaient pas reconnues comme des méthodes d'échange de clés à secret parfait (PFS). Par conséquent, les suites de chiffrement **ECDHE-PSK** et **DHE-PSK** ne fonctionnaient pas avec OpenSSL configuré sur **SECLEVEL=3**, par exemple, lorsque la politique cryptographique du système était définie sur **FUTURE**. La nouvelle version du paquet **openssl** corrige ce problème.

Bugzilla:2060044

Clevis saute désormais correctement les dispositifs commentés dans les crypttab

Auparavant, Clevis essayait de déverrouiller les périphériques commentés dans le fichier **crypttab**, ce qui entraînait l'exécution du service **clevis-luks-askpass** même si le périphérique n'était pas valide. Cela entraînait des exécutions de service inutiles et rendait le dépannage difficile.

Avec cette correction, Clevis ignore les périphériques commentés. Désormais, si un périphérique non valide est commenté, Clevis n'essaie pas de le déverrouiller et **clevis-luks-askpass** se termine de manière appropriée. Cela facilite le dépannage et réduit les exécutions de service inutiles.

Bugzilla:2159728

Clevis ne demande plus trop d'entropie de la part de pwmake

Auparavant, l'utilitaire de génération de mots de passe **pwmake** affichait des avertissements indésirables lorsque Clevis utilisait **pwmake** pour créer des mots de passe destinés à stocker des données dans les métadonnées **LUKS**, ce qui amenait Clevis à utiliser une entropie plus faible. Avec cette mise à jour, Clevis est limité à 256 bits d'entropie fournis à **pwmake**, ce qui élimine l'avertissement indésirable et utilise la quantité correcte d'entropie.

Bugzilla:2159735

USBGuard ne provoque plus d'avertissement déroutant

Auparavant, une condition de course pouvait se produire dans USBGuard lorsqu'un processus parent se terminait plus tôt que le premier processus enfant. En conséquence, **systemd** signalait qu'un processus était présent avec un PID parent (PPID) mal identifié. Avec cette mise à jour, un processus parent attend que le premier processus enfant se termine en mode travail. Par conséquent, **systemd** ne signale plus ce type d'avertissement.

Bugzilla:2042345

L'OOM killer ne met plus fin prématurément à usbguard

Auparavant, le fichier **usbguard.service** ne contenait pas de définition de l'option **OOMScoreAdjust** pour le service **systemd**. Par conséquent, lorsque le système manquait de ressources, le processus **usbguard-daemon** pouvait être interrompu avant d'autres processus non privilégiés. Avec cette mise à jour, le fichier **usbguard.service** contient désormais l'option **OOMScoreAdjust**, ce qui évite que le processus **usbguard-daemon** ne soit interrompu prématurément par un tueur en mémoire (Out-of-Memory, OOM).

Bugzilla:2097419

logrotate ne signale plus incorrectement Rsyslog dans la rotation des journaux

Auparavant, l'ordre des arguments était mal défini dans le script **logrotate**, ce qui provoquait une erreur de syntaxe. De ce fait, **logrotate** ne signalait pas correctement Rsyslog lors de la rotation des journaux.

Avec cette mise à jour, l'ordre des arguments dans **logrotate** est corrigé et **logrotate** signale correctement Rsyslog après la rotation des journaux, même lorsque la variable d'environnement **POSIXLY_CORRECT** est définie.

Bugzilla:2124488

imklog ne fait plus appel à free() pour les objets manquants

Auparavant, le module **imklog** appelait une fonction **free()** sur un objet déjà libéré. Par conséquent, **imklog** pouvait provoquer une erreur de segmentation. Avec cette mise à jour, l'objet n'est plus libéré deux fois.

Bugzilla:2157659

fagenrules --load fonctionne désormais correctement

Auparavant, le service **fapolicyd** ne gérait pas correctement le signal de raccrochage (SIGHUP). Par conséquent, **fapolicyd** se terminait après avoir reçu le signal SIGHUP et la commande **fagenrules --load** ne fonctionnait pas correctement. Cette mise à jour contient un correctif pour ce problème. Par conséquent, **fagenrules --load** fonctionne désormais correctement et les mises à jour des règles ne nécessitent plus le redémarrage manuel de **fapolicyd**.

Bugzilla:2070655

Les analyses et les remédiations ignorent correctement les règles d'audit SCAP Clé d'audit

Auparavant, les règles de surveillance d'audit définies sans clé d'audit (clé**-k** ou **-F**) rencontraient les problèmes suivants :

- Les règles ont été marquées comme non conformes même si d'autres parties de la règle étaient correctes.
- La remédiation Bash a corrigé le chemin d'accès et les autorisations de la règle de surveillance, mais elle n'a pas ajouté la clé d'audit correctement.
- La remédiation n'a parfois pas corrigé la clé manquante, renvoyant une valeur **error** au lieu d'une valeur **fixed**.

Les règles suivantes sont concernées :

- **audit_rules_login_events**
- **audit_rules_login_events_faillock**
- **audit_rules_login_events_lastlog**
- **audit_rules_login_events_tallylog**
- **audit_rules_usergroup_modification**
- **audit_rules_usergroup_modification_group**
- **audit_rules_usergroup_modification_gshadow**
- **audit_rules_usergroup_modification_opasswd**
- **audit_rules_usergroup_modification_passwd**

- **audit_rules_usergroup_modification_shadow**
- **audit_rules_time_watch_localtime**
- **audit_rules_mac_modification**
- **audit_rules_networkconfig_modification**
- **audit_rules_sysadmin_actions**
- **audit_rules_session_events**
- **audit_rules_sudoers**
- **audit_rules_sudoers_d**

Avec cette mise à jour, la clé Audit a été supprimée des vérifications et des remédiations Bash et Ansible. Par conséquent, les incohérences causées par le champ de clé lors des vérifications et des remédiations ne se produisent plus, et les auditeurs peuvent choisir ces clés arbitrairement pour faciliter la recherche dans les journaux d'audit.

Bugzilla:2120978

Keylime n'échoue plus dans l'attestation des systèmes qui accèdent à plusieurs fichiers mesurés par l'IMA

Auparavant, si un système qui exécute l'agent Keylime accédait à plusieurs fichiers mesurés par l'architecture de mesure de l'intégrité (IMA) en succession rapide, le vérificateur Keylime traitait incorrectement les ajouts au journal de l'IMA. En conséquence, le hachage en cours d'exécution ne correspondait pas à l'état correct du registre de configuration de la plate-forme (PCR), et le système échouait à l'attestation. Cette mise à jour corrige le problème et les systèmes qui accèdent rapidement à plusieurs fichiers mesurés n'échouent plus à l'attestation.

Bugzilla:2138167

Le script de génération de la politique Keylime ne provoque plus d'erreur de segmentation ni de vidage du noyau

Le script **create_mb_refstate** génère des politiques pour l'attestation de démarrage mesurée dans Keylime. Auparavant, **create_mb_refstate** calculait incorrectement la longueur des données dans le champ **DevicePath**. En conséquence, le script essayait d'accéder à une mémoire invalide en utilisant la longueur incorrectement calculée, ce qui entraînait une erreur de segmentation et un vidage du noyau.

Cette mise à jour, qui a été publiée dans l'avis RHBA-2022:105318-02, empêche l'erreur de segmentation lors du traitement du journal des événements de démarrage mesuré. Par conséquent, vous pouvez générer une politique de démarrage mesurée.

Bugzilla:2140670

Les certificats TPM ne font plus planter le registraire Keylime

Auparavant, certains certificats dans le magasin de certificats de Keylime TPM étaient des certificats x509 malformés et provoquaient le plantage du registraire de Keylime. Cette mise à jour corrige le problème, et le registraire Keylime ne se bloque plus à cause de certificats malformés.

Bugzilla:2142009

8.6. MISE EN RÉSEAU

NetworkManager préserve désormais les adresses IP lors de la réapplication avant l'acquisition d'un nouveau bail DHCP

Auparavant, après avoir modifié les paramètres de connexion et utilisé la commande **nmcli device reapply**, NetworkManager n'a pas conservé le bail DHCP. Par conséquent, l'adresse IP était temporairement supprimée. Avec cette correction, NetworkManager préserve le bail DHCP et l'utilise jusqu'à ce qu'il expire ou que le client en demande un nouveau. Par conséquent, lorsque la commande **nmcli device reapply** redémarre le client DHCP, elle ne supprime pas temporairement l'adresse IP.

Bugzilla:2117352

Le service firewalld ne déclenche désormais l'avertissement de dépréciation de ipset que lors de l'utilisation de règles directes

Auparavant, le service **firewalld** utilisait le module de noyau **ipset** obsolète alors que ce n'était pas nécessaire. Par conséquent, RHEL consignait l'avertissement de dépréciation du module, ce qui pouvait être trompeur car la fonctionnalité **ipset** de **firewalld** n'est pas dépréciée. Avec cette mise à jour, **firewalld** n'utilise que le module obsolète **ipset** et enregistre l'avertissement si l'utilisateur utilise explicitement **ipsets** avec l'option **--direct**.

Bugzilla:2122678

L'interface HNV affiche désormais les options après le redémarrage

Auparavant, l'utilitaire **nmcli** a créé un lien de virtualisation de réseau hybride (HNV) à l'aide de l'API NetworkManager. Par conséquent, après un redémarrage, le lien HNV perdait le paramètre du port primaire. Avec cette correction, **nmcli** utilise désormais **hcnmgr** pour définir les options de liaison pour le port primaire. L'utilitaire **hcnmgr** prend en charge la migration des partitions actives avec la virtualisation d'entrée/sortie à racine unique (SR-IOV) pour les réseaux hybrides. Par conséquent, l'interface de liaison HNV affiche l'option **active slave/primary_reselect** après le redémarrage.

Bugzilla:2125152

8.7. NOYAU

FADump activé avec Secure Boot fonctionne correctement

Auparavant, lorsque la fonction FADump (Firmware Assisted Dump) était activée dans l'environnement Secure Boot et que l'un des composants de démarrage dépassait la zone de mémoire allouée, les redémarrages du système provoquaient un état GRUB Out of Memory (OOM). Cette mise à jour apporte une correction dans **kexec-tools** afin que Secure Boot et FADump fonctionnent correctement ensemble.

Bugzilla:2139000

8.8. CHARGEUR DE DÉMARRAGE

grubby transmet désormais correctement les arguments à un nouveau noyau

Lorsque vous ajoutez un nouveau noyau à l'aide de l'outil **grubby** et que vous ne spécifiez aucun argument, ou que vous laissez les arguments vides, **grubby** ne transmettra aucun argument au nouveau noyau et **root** ne sera pas défini. L'utilisation des options **--args** et **--copy-default** permet de s'assurer que les nouveaux arguments sont ajoutés aux arguments par défaut.

Bugzilla:2127453

8.9. SYSTÈMES DE FICHIERS ET STOCKAGE

Le programme d'installation crée des périphériques LUKSv2 avec une taille de secteur de 512 octets

Auparavant, le programme d'installation RHEL créait des périphériques LUKSv2 avec des secteurs de 4096 octets si le disque avait des secteurs physiques de 4096 octets. Avec cette mise à jour, le programme d'installation crée désormais des périphériques LUKSv2 avec une taille de secteur de 512 octets afin d'offrir une meilleure compatibilité de disque avec différentes tailles de secteur physique utilisées ensemble dans un groupe de volumes LVM, même lorsque les volumes physiques LVM sont chiffrés.

Bugzilla:2103800

supported_speeds sysfs l'attribut indique des valeurs de vitesse correctes

Auparavant, en raison d'une définition incorrecte dans le pilote **qla2xxx**, l'attribut **supported_speeds sysfs** pour le HBA indiquait une vitesse de 20 Gb/s au lieu de la vitesse attendue de 64 Gb/s. Par conséquent, si l'adaptateur de bus hôte prenait en charge une vitesse de liaison de 64 Gb/s, la valeur de **supported_speeds sysfs** était incorrecte, ce qui affectait la valeur de la vitesse signalée.

Avec cette mise à jour, l'attribut **supported_speeds sysfs** pour HBA indique les valeurs de vitesse correctes, à savoir 16 Gb/s, 32 Gb/s et 64 Gb/s. Vous pouvez visualiser les valeurs de vitesse en exécutant la commande **cat /sys/class/fc_host/host*/supported_speeds**.

Bugzilla:2069758

8.10. HAUTE DISPONIBILITÉ ET CLUSTERS

pcs ne permet plus de modifier les propriétés d'un cluster qui ne devraient pas être modifiées

Auparavant, l'interface de ligne de commande **pcs** vous permettait de modifier les propriétés de la grappe qui ne devraient pas être modifiées ou pour lesquelles la modification n'a pas d'effet. Avec cette correction, **pcs** ne vous permet plus de modifier ces propriétés de cluster : **cluster-infrastructure**, **cluster-name**, **dc-version**, **have-watchdog**, et **last-lrm-refresh**.

Bugzilla:1620043

pcs affiche désormais les propriétés du cluster qui ne sont pas explicitement configurées

Auparavant, la commande **pcs** permettant d'afficher la valeur d'une propriété de cluster spécifique ne répertoriait pas les valeurs qui n'étaient pas explicitement configurées dans la CIB. Avec cette correction, si une propriété de cluster n'est pas définie, **pcs** affiche la valeur par défaut de la propriété.

Bugzilla:1796827

Les ressources du cluster qui font appel à crm_mon s'arrêtent désormais proprement lors de la fermeture

Auparavant, l'utilitaire **crm_mon** renvoyait un état de sortie non nul alors que Pacemaker était en cours d'arrêt. Les agents de ressources qui appelaient **crm_mon** dans leur action de surveillance, tels que **ocf:heartbeat:pqsql**, pouvaient incorrectement renvoyer un échec lors de l'arrêt du cluster. Avec cette correction, **crm_mon** renvoie un succès même si le cluster est en cours d'arrêt. Les ressources qui appellent **crm_mon** s'arrêtent maintenant proprement lors de l'arrêt du cluster.

Bugzilla:2133546

Les actions de métadonnées de l'agent de ressources OCF peuvent désormais appeler crm_node sans provoquer de clôtures inattendues

Depuis RHEL 8.5, les actions de métadonnées de l'agent de ressources OCF bloquent le contrôleur et les requêtes **crm_node** exécutent les demandes du contrôleur. Par conséquent, si l'action de métadonnées d'un agent appelle **crm_node**, elle bloque le contrôleur pendant 30 secondes jusqu'à ce que l'action se termine. Cela peut entraîner l'échec d'autres actions et la clôture du nœud.

Avec cette correction, le contrôleur exécute désormais les actions de métadonnées de manière asynchrone. Une action de métadonnées de l'agent de ressources OCF peut désormais appeler **crm_node** sans problème.

Bugzilla:2125344

Pacemaker revérifie désormais les affectations de ressources immédiatement lorsque l'ordre des ressources est modifié

Depuis RHEL 8.7, Pacemaker ne revérifie pas les affectations de ressources lorsque l'ordre des ressources dans la CIB change sans que la définition des ressources ne soit modifiée. Si la réorganisation de la configuration entraînait un déplacement des ressources, celui-ci n'avait pas lieu avant la prochaine transition naturelle, jusqu'à la valeur de **cluster-recheck-interval-property**. Cela pouvait poser des problèmes si l'adhérence des ressources n'était pas configurée pour une ressource.

Avec cette modification, Pacemaker revérifie les affectations de ressources lorsque l'ordre des ressources dans la CIB change, comme c'était le cas pour les versions antérieures de Pacemaker. Le cluster répond maintenant immédiatement à ces changements, si nécessaire.

Bugzilla:2125337

L'activation d'une ressource unique et d'une opération de surveillance ne permet plus d'effectuer des opérations de surveillance pour toutes les ressources d'un groupe de ressources

Auparavant, après avoir supprimé la gestion de toutes les ressources et opérations de surveillance dans un groupe de ressources, la gestion d'une des ressources de ce groupe avec son opération de surveillance réactivait les opérations de surveillance pour toutes les ressources du groupe de ressources. Cela pouvait entraîner un comportement inattendu de la grappe.

Avec cette correction, la gestion d'une ressource et la réactivation de son opération de surveillance réactivent l'opération de surveillance pour cette ressource uniquement et non pour les autres ressources d'un groupe de ressources.

Bugzilla:2092950

8.11. COMPILATEURS ET OUTILS DE DÉVELOPPEMENT

La recherche DNS peut désormais aboutir même si certains enregistrements CNAME sont invalides

Auparavant, le résolveur de stub DNS **glibc** traitait les enregistrements CNAME avec des noms de propriétaires qui ne sont pas des noms d'hôtes comme des erreurs de paquets DNS. Par conséquent, la requête DNS échouait à cause des erreurs de paquets DNS. Avec cette mise à jour, le résolveur de stub **glibc** ignore désormais les enregistrements CNAME invalides et les informations d'alias

correspondantes ne sont pas extraites. Par conséquent, les recherches DNS peuvent maintenant réussir même si la réponse du serveur inclut une chaîne CNAME qui contient un nom de domaine qui n'est pas un nom d'hôte.

Bugzilla:2129005

golang supporte désormais les clés de 4096 bits en mode x509 FIPS

Auparavant, **golang** ne prenait pas en charge les clés de 4096 bits en mode x509 FIPS. Par conséquent, lorsque l'utilisateur utilisait des clés de 4096 bits, le programme se bloquait. Avec cette mise à jour, **golang** prend désormais en charge les clés de 4096 bits en mode x509 FIPS.

Bugzilla:2133019

Vous pouvez installer SciPy à l'aide de pip sur toutes les architectures

Auparavant, le paquetage **openblas-devel** ne contenait pas de fichier pkg-config pour la bibliothèque OpenBLAS. Par conséquent, dans certains cas, il était impossible de déterminer les drapeaux du compilateur et de l'éditeur de liens à l'aide de l'utilitaire **pkgconf** lors de la compilation avec OpenBLAS. Par exemple, cela a provoqué l'échec de la commande **pip install scipy** sur les architectures 64 bits IBM Z et IBM Power Systems, Little Endian.

Cette mise à jour ajoute le fichier **openblas.pc** au paquetage **openblas-devel** sur toutes les architectures prises en charge. Par conséquent, vous pouvez installer la bibliothèque SciPy à l'aide du programme d'installation du paquet **pip**.

Notez que dans RHEL 9, il est recommandé de construire vos applications à partir du paquetage **flexiblas-devel** et de lier vos projets à la bibliothèque FlexiBLAS.

Bugzilla:2115737

La fonction tzset de glibc attribue désormais une valeur non nulle à la variable "lumière du jour" si les données TZ contiennent une règle d'heure avancée

Auparavant, la fonction **tzset** de **glibc** définissait la variable daylight à 0 si la dernière transition DST dans le fichier de données du fuseau horaire n'entraînait pas de changement d'horloge en raison d'un changement simultané du décalage de l'heure standard. Par conséquent, lorsque les applications utilisent la variable daylight pour vérifier si l'heure d'été a été active, elles n'obtiennent pas le bon résultat et effectuent des actions incorrectes sur la base de cette information. Pour remédier à ce problème, la fonction **tzset** attribue désormais une valeur non nulle à la variable daylight s'il existe une règle DST dans les données du fuseau horaire, quel que soit le décalage. Par conséquent, les applications observent désormais la présence de règles d'heure avancée, indépendamment des changements de décalage.

Bugzilla:2155352

L'implémentation OpenJDK RSAPSSSignature valide désormais les clés RSA avant de les utiliser

Auparavant, l'implémentation de RSAPSSSignature dans OpenJDK ne vérifiait pas complètement si des clés RSA données pouvaient être utilisées par le fournisseur SunRSASign avant de tenter de les utiliser, ce qui entraînait des erreurs lors de l'utilisation de fournisseurs de sécurité personnalisés. Le bogue est maintenant corrigé et, par conséquent, l'implémentation de RSAPSSSignature valide désormais les clés RSA et permet à d'autres fournisseurs de gérer ces clés lorsqu'elle ne le peut pas.

Bugzilla:2188023

Le fournisseur de signature XML d'OpenJDK est maintenant fonctionnel en mode FIPS

Auparavant, le fournisseur de signature XML d'OpenJDK ne pouvait pas fonctionner en mode FIPS. Grâce aux améliorations apportées au support du mode FIPS, le fournisseur de signature XML d'OpenJDK est désormais activé en mode FIPS.

Bugzilla:2186810

OpenJDK en mode FIPS ne rencontre plus d'erreurs inattendues avec certains jetons PKCS#11

Auparavant, certains jetons PKCS#11 n'étaient pas complètement initialisés avant d'être utilisés par OpenJDK en mode FIPS, ce qui entraînait des erreurs inattendues. Avec cette mise à jour, ces erreurs sont désormais attendues et gérées par le code de support FIPS.

Bugzilla:2186806

8.12. GESTION DE L'IDENTITÉ

L'authentification auprès d'IdP externes nécessitant un secret client est désormais possible

Auparavant, SSSD ne transmettait pas correctement les secrets client aux fournisseurs d'identité externes (IdP). Par conséquent, l'authentification échouait contre les IdP externes que vous aviez précédemment configurés avec la commande **ipa idp-add --secret** pour exiger un secret client. Avec cette mise à jour, SSSD transmet le secret client à l'IdP et les utilisateurs peuvent s'authentifier.

Jira:RHELPLAN-148303

IdM prend désormais en charge la définition des masques d'hôtes pour les règles sudo à l'aide d'Ansible

Auparavant, la commande **ipa sudorule-add-host** permettait de définir un masque d'hôte à utiliser par la règle **sudo**, mais cette option n'était pas présente dans le paquet **ansible-freeipa**. Avec cette mise à jour, vous pouvez désormais utiliser la variable **ansible-freeipa hostmask** pour définir une liste de masques d'hôtes auxquels s'applique une règle **sudo** particulière, définie dans Identity Management (IdM).

Par conséquent, vous pouvez désormais automatiser la définition des masques d'hôtes pour les règles IdM **sudo** avec Ansible.

Bugzilla:2127913

L'utilitaire dscreate fonctionne désormais correctement lorsqu'il utilise un chemin personnalisé avec le paramètre db_dir

Auparavant, une instance qui utilisait des chemins d'accès personnalisés n'arrivait pas à démarrer parce que les répertoires personnalisés avaient une mauvaise étiquette SELinux. En conséquence, SELinux refusait l'accès à ces répertoires et l'instance n'était pas créée. Avec cette version, l'utilitaire **dscreate** définit les étiquettes SELinux correctes pour les répertoires d'instance personnalisés.

Bugzilla:1924569

Un changement de mot de passe pour le compte du gestionnaire de réplication du serveur d'annuaire fonctionne désormais correctement

Auparavant, après un changement de mot de passe, Directory Server ne mettait pas correctement à jour le cache de mot de passe pour l'accord de réplication. Par conséquent, lorsque vous changiez le mot de passe du compte du gestionnaire de réplication, la réplication échouait. Avec cette mise à jour, Directory

Server met correctement à jour le cache et, par conséquent, la réplication fonctionne comme prévu.

Bugzilla:1956987

Le programme d'installation du client IdM ne spécifie plus la configuration de l'autorité de certification TLS dans le fichier ldap.conf

Auparavant, le programme d'installation du client IdM spécifiait la configuration de l'autorité de certification TLS dans le fichier **ldap.conf**. Avec cette mise à jour, OpenLDAP utilise le magasin de confiance par défaut et le programme d'installation du client IdM ne définit pas la configuration de l'autorité de certification TLS dans le fichier **ldap.conf**.

Bugzilla:2094673

8.13. RÔLES DU SYSTÈME RED HAT ENTERPRISE LINUX

Le rôle du système nbde_client gère désormais correctement les différents noms de clevis-luks-askpass

Le rôle de système **nbde_client** a été mis à jour pour gérer les systèmes sur lesquels l'unité **clevis-luks-askpass systemd** a un nom différent. Le rôle fonctionne désormais correctement avec les différents noms de **clevis-luks-askpass** sur les nœuds gérés, ce qui nécessite de déverrouiller également les volumes cryptés LUKS qui se montent tardivement dans le processus de démarrage.

Bugzilla:2126959

Les journaux des rôles du système ha_cluster n'affichent plus les mots de passe et les secrets non chiffrés

Le rôle de système **ha_cluster** accepte des paramètres qui peuvent être des mots de passe ou d'autres secrets. Auparavant, certaines tâches consignaient leurs entrées et sorties. Par conséquent, les journaux des rôles pouvaient contenir des mots de passe non cryptés et d'autres secrets.

Avec cette mise à jour, les tâches ont été modifiées pour utiliser la directive Ansible **no_log: true** et la sortie de la tâche n'est plus affichée dans les journaux de rôle. Les journaux des rôles du système **ha_cluster** ne contiennent plus de mots de passe ni d'autres secrets. Bien que cette mise à jour protège les informations sécurisées, les journaux de rôle fournissent désormais moins d'informations que vous pouvez utiliser lors du débogage de votre configuration.

Bugzilla:2143816

Les clusters configurés avec le rôle de système ha_cluster pour utiliser le SBD et ne pas démarrer au démarrage fonctionnent désormais correctement

Auparavant, si un utilisateur configurait un cluster à l'aide du rôle système **ha_cluster** pour utiliser le SBD et ne pas démarrer au démarrage, le service SBD était désactivé et le SBD ne démarrait pas. Avec cette correction, le service SBD est toujours activé si un cluster est configuré pour utiliser le SBD, qu'il soit ou non configuré pour démarrer au démarrage.

Bugzilla:2153030

L'activation du fournisseur de fichiers implicites permet de corriger la configuration de cockpit-session-recording SSSD

Un fournisseur de fichiers implicites SSSD désactivé entraînait la création d'une configuration SSSD (System Security Services Daemon) invalide par les modules **cockpit-session-recording**. Cette mise à jour active inconditionnellement le fournisseur de fichiers et, par conséquent, la configuration SSSD

créée par **cockpit-session-recording** fonctionne désormais comme prévu.

Bugzilla:2153043

Le rôle nbde_client_clevis ne signale plus de traceback aux utilisateurs

Auparavant, le rôle **nbde_client_clevis** échouait parfois dans une exception, ce qui entraînait un retour en arrière et la communication de données sensibles, telles que le champ **encryption_password**, à l'utilisateur. Avec cette mise à jour, le rôle ne signale plus de données sensibles, mais uniquement les messages d'erreur appropriés.

Bugzilla:2162782

La définition de la propriété stonith-watchdog-timeout avec le rôle de système ha_cluster fonctionne désormais dans un cluster arrêté

Auparavant, lorsque vous définissiez la propriété **stonith-watchdog-timeout** avec le rôle système **ha_cluster** dans un cluster arrêté, la propriété reprenait sa valeur précédente et le rôle échouait. Avec cette correction, la configuration de la propriété **stonith-watchdog-timeout** à l'aide du rôle système **ha_cluster** fonctionne correctement.

Bugzilla:2167528

Le trafic réseau est désormais dirigé vers l'interface réseau prévue lors de l'utilisation de initscripts avec le rôle de système RHEL networking

Auparavant, lors de l'utilisation du fournisseur **initscripts**, la configuration du routage pour les connexions réseau ne spécifiait pas le périphérique de sortie par lequel le trafic devait passer. Par conséquent, le noyau pouvait utiliser un périphérique de sortie différent de celui prévu par l'utilisateur. Désormais, si le nom de l'interface réseau est spécifié dans le playbook pour la connexion, il est utilisé comme périphérique de sortie dans le fichier de configuration de l'itinéraire. Cela aligne le comportement avec NetworkManager, qui configure le périphérique de sortie dans les routes lors de l'activation des profils sur les périphériques. Ainsi, les utilisateurs peuvent s'assurer que le trafic est dirigé vers l'interface réseau prévue.

Bugzilla:2168735

Le rôle selinux gère désormais les modules de politique de manière idempotente

Auparavant, le rôle **selinux** copiait un module existant sur le nœud géré à chaque fois, signalant un changement même si le module était déjà présent. Avec cette mise à jour, le rôle **selinux** vérifie si le module a été installé sur le nœud géré et ne tente pas de copier et d'installer le module s'il est déjà installé.

Bugzilla:2160152

8.14. VIRTUALISATION

L'heure système sur les VM imbriquées fonctionne désormais de manière fiable

Auparavant, l'heure système des machines virtuelles (VM) imbriquées était parfois désynchronisée par rapport aux hôtes de niveau 0 et de niveau 1. Il arrivait également que la machine virtuelle imbriquée ne réponde plus ou se termine de manière inattendue.

Avec cette mise à jour, le code de gestion du temps dans le code du noyau de l'hôte KVM a été corrigé, ce qui empêche les erreurs décrites de se produire.

Bugzilla:2140899

Le démarrage des VM sur IBM Z n'échoue plus lors de l'utilisation de **memfd** memory backing

Auparavant, sur les hôtes IBM Z, les machines virtuelles (VM) ne démarraient pas si elles étaient configurées pour utiliser le type **memfd** de support de mémoire hugepage, par exemple comme suit :

```
<memoryBacking>
  <hugepages/>
  <source type='memfd'/>
</memoryBacking>
```

Avec cette mise à jour, la cause sous-jacente a été corrigée et les machines virtuelles concernées démarrent désormais correctement.

Bugzilla:2116496

VNC peut désormais se connecter de manière fiable aux machines virtuelles UEFI après migration

Auparavant, si vous activiez ou désactiviez une file d'attente de messages lors de la migration d'une machine virtuelle (VM), le client Virtual Network Computing (VNC) ne parvenait pas à se connecter à la VM une fois la migration terminée.

Ce problème ne concerne que les machines virtuelles basées sur l'UEFI qui utilisent l'Open Virtual Machine Firmware (OVMF).

Le problème a été corrigé et le client VNC se connecte désormais de manière fiable aux machines virtuelles UEFI une fois la migration terminée.

Jira:RHELPLAN-135600

Le programme d'installation affiche le disque système prévu pour l'installation de RHEL sur la VM

Auparavant, lors de l'installation de RHEL sur une VM utilisant des périphériques **virtio-scsi**, il était possible que ces périphériques n'apparaissent pas dans le programme d'installation en raison d'un bogue de **device-mapper-multipath**. Par conséquent, lors de l'installation, si certains périphériques disposaient d'un jeu de série et d'autres non, la commande **multipath** réclamait tous les périphériques disposant d'un jeu de série. De ce fait, le programme d'installation n'a pas pu trouver le disque système attendu pour installer RHEL dans la VM.

Avec cette mise à jour, **multipath** définit correctement les périphériques sans numéro de série comme n'ayant pas d'identifiant WWID (World Wide Identifier) et les ignore. Lors de l'installation, **multipath** ne réclame que les périphériques que **multipathd** utilise pour lier un périphérique multipath, et le programme d'installation affiche le disque système prévu pour installer RHEL dans la VM.

Bugzilla:1926147

CHAPITRE 9. 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 .

9.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

Les périphériques NVMe sur Fibre Channel sont désormais disponibles dans le programme d'installation RHEL en tant qu'aperçu technologique

Vous pouvez désormais ajouter des périphériques NVMe over Fibre Channel à votre installation RHEL en tant qu'aperçu technologique. Dans RHEL Installer, vous pouvez sélectionner ces périphériques dans la section NVMe Fabrics Devices lors de l'ajout de disques sur l'écran Destination de l'installation.

Bugzilla:2107346

9.2. SHELLS ET OUTILS DE LIGNE DE COMMANDE

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.

Bugzilla:2047161

9.3. SERVICES D'INFRASTRUCTURE

L'API Socket pour TuneD est disponible en avant-première technologique

L'API socket permettant de contrôler TuneD par l'intermédiaire d'un socket de domaine Unix est désormais disponible en tant qu'aperçu technologique. L'API socket correspond à l'API D-Bus et fournit une méthode de communication alternative pour les cas où D-Bus n'est pas disponible. En utilisant l'API socket, vous pouvez contrôler le démon TuneD pour optimiser les performances et modifier les valeurs de divers paramètres de réglage. L'API socket est désactivée par défaut, vous pouvez l'activer dans le fichier **tuned-main.conf**.

Bugzilla:2113900

9.4. SÉCURITÉ

gnutls utilise désormais KTLS en tant qu'avant-première technologique

Les paquets **gnutls** mis à jour peuvent utiliser Kernel TLS (KTLS) pour accélérer le transfert de données sur des canaux cryptés en tant qu'aperçu technologique. Pour activer KTLS, ajoutez le module de noyau **tls.ko** à l'aide de la commande **modprobe**, et créez un nouveau fichier de configuration **/etc/crypto-policies/local.d/gnutls-ktls.txt** pour les politiques cryptographiques du système avec le contenu suivant :

```
[global]
ktls = true
```

Notez que la version actuelle ne prend pas en charge la mise à jour des clés de trafic par le biais des messages TLS **KeyUpdate**, ce qui a une incidence sur la sécurité des suites de chiffrement AES-GCM. Voir le document RFC 7841 - TLS 1.3 pour plus d'informations.

Bugzilla:2042009

9.5. 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 .

Bugzilla: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.

Bugzilla: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 de DNS multidiffusion.

Notez que **systemd-resolved** est un aperçu technologique non pris en charge.

Bugzilla:2020529

9.6. NOYAU

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.

Bugzilla:1874182

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).

Bugzilla:2030412

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.

Bugzilla:2023416

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. La version 2 ajoute **Enclave Dynamic Memory Management** (EDMM). Les caractéristiques notables sont les suivantes

- Modification des permissions EPCM des pages régulières d'une enclave appartenant à une enclave initialisée.
- Ajout dynamique de pages régulières à une enclave initialisée.
- Extension d'une enclave initialisée pour accueillir plus de threads.
- Suppression des pages normales et des pages TCS d'une enclave initialisée.

Bugzilla:1660337

rvu_af, rvu_nicpf, et rvu_nicvf disponibles sous forme d'aperçu technologique

Les modules de noyau suivants sont disponibles en tant qu'aperçu technologique pour la famille de processeurs d'infrastructure Marvell OCTEON TX2 :

- **rvu_nicpf** - Pilote de fonction physique de la carte d'interface réseau Marvell OcteonTX2
- **rvu_nicvf** - Pilote de la fonction virtuelle de la carte d'interface réseau Marvell OcteonTX2
- **rvu_nicvf** - Pilote Marvell OcteonTX2 RVU Admin Function

Bugzilla:2040643

9.7. 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.

Bugzilla: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 .

Bugzilla: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/specifications/.

Bugzilla:2021672

nvme-stas disponible en avant-première technologique

Le paquetage **nvme-stas**, qui est un client Central Discovery Controller (CDC) pour Linux, est maintenant disponible en tant qu'aperçu technologique. Il gère les notifications d'événements asynchrones (AEN), les contrôles automatisés des connexions au sous-système NVMe, la gestion et le signalement des erreurs, ainsi que la configuration automatique (**zeroconf**) et manuelle.

Ce paquetage se compose de deux démons, Storage Appliance Finder (**stafd**) et Storage Appliance Connector (**stacd**).

Bugzilla:1893841

L'authentification en bande NVMe TP 8006 est disponible en tant qu'aperçu technologique

L'implémentation du TP 8006 de Non-Volatile Memory Express (NVMe), qui est une authentification en bande pour NVMe over Fabrics (NVMe-oF), est maintenant disponible en tant qu'aperçu technologique non pris en charge. La proposition technique NVMe 8006 définit le protocole d'authentification en bande **DH-HMAC-CHAP** pour NVMe-oF, qui est fourni avec cette amélioration.

Pour plus d'informations, voir les descriptions des options **dhchap-secret** et **dhchap-ctrl-secret** dans la page de manuel **nvme-connect(1)**.

Bugzilla:2027304

9.8. 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 Technology Preview pour les architectures AMD et Intel 64 bits.

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.

Notez que depuis RHEL 9.2, **jmc-core** et **owasp-java-encoder** sont disponibles dans le dépôt CodeReady Linux Builder (CRB), que vous devez explicitement activer. Pour plus d'informations, voir Comment activer et utiliser le contenu dans CodeReady Linux Builder .

Bugzilla:1980981

9.9. 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.

Bugzilla: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).

Bugzilla:2084166

le sous-paquet sssd-idp est disponible en tant qu'aperçu technologique

Le sous-paquet **sssd-idp** pour SSSD contient les plugins **oidc_child** et krb5 **idp**, qui sont des composants côté client qui effectuent l'authentification OAuth2 contre les serveurs de gestion d'identité (IdM). Cette fonctionnalité n'est disponible qu'avec les serveurs IdM sur RHEL 9.1 et les versions ultérieures.

Bugzilla:2065693

Le plugin idp krb5 interne de SSSD est disponible en tant qu'aperçu technologique

Le plugin SSSD krb5 **idp** vous permet de vous authentifier auprès d'un fournisseur d'identité externe (IdP) à l'aide du protocole OAuth2. Cette fonctionnalité n'est disponible qu'avec les serveurs IdM sur RHEL 9.1 et les versions ultérieures.

Bugzilla:2056482

RHEL IdM permet de déléguer l'authentification des utilisateurs à des fournisseurs d'identité externes en tant qu'aperçu technologique

Dans RHEL IdM, vous pouvez désormais associer des utilisateurs à des fournisseurs d'identité externes (IdP) qui prennent en charge le flux d'autorisation de périphérique OAuth 2. Lorsque ces utilisateurs s'authentifient avec la version SSSD disponible dans RHEL 9.1 ou une version ultérieure, ils bénéficient des fonctionnalités d'authentification unique de RHEL IdM avec des tickets Kerberos après avoir effectué l'authentification et l'autorisation auprès du fournisseur d'identité externe.

Parmi les caractéristiques notables, on peut citer

- Ajout, modification et suppression de références à des IdP externes à l'aide des commandes **ipa idp-***
- Activation de l'authentification IdP pour les utilisateurs avec la commande **ipa user-mod --user-auth-type=idp**

Pour plus d'informations, voir Utilisation de fournisseurs d'identité externes pour s'authentifier auprès de l'IdM.

Bugzilla:2069202

9.10. 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

9.11. INFRASTRUCTURES GRAPHIQUES

Les cartes graphiques Intel Arc A-Series disponibles en avant-première technologique

Les cartes graphiques Intel Arc A-Series, également connues sous le nom d'Alchemist ou DG2, sont désormais disponibles en tant qu'aperçu technologique.

Pour activer l'accélération matérielle avec les graphiques Intel Arc A-Series, ajoutez l'option suivante à la ligne de commande du noyau :

```
i915.force_probe=pci-id
```

Dans cette option, remplacez ***pci-id*** par l'un des éléments suivants :

- L'ID PCI de votre GPU Intel.
- Le caractère * pour activer le pilote i915 avec tout le matériel de qualité alpha.

Bugzilla:2041690

9.12. 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

9.13. VIRTUALISATION

Intel SGX disponible pour les machines virtuelles en tant qu'aperçu technologique

En tant qu'aperçu technologique, les Intel Software Guard Extensions (SGX) peuvent désormais être configurées pour les machines virtuelles (VM) hébergées sur RHEL 9. SGX aide à protéger l'intégrité et la confidentialité des données pour des processus spécifiques sur le matériel Intel. Après avoir configuré SGX sur votre hôte, la fonctionnalité est transmise à ses VM, de sorte que les systèmes d'exploitation invités (OS) puissent l'utiliser.

Notez que pour qu'un système d'exploitation invité puisse utiliser SGX, vous devez d'abord installer les pilotes SGX pour ce système d'exploitation spécifique. En outre, SGX sur votre hôte ne peut pas crypter la mémoire des VM.

Jira:RHELPLAN-69761

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, Intel 64 et ARM 64

En tant qu'aperçu technologique, RHEL 9 introduit la fonctionnalité **virtio-mem** sur les systèmes AMD64, Intel 64 et ARM 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.

Bugzilla:2014487, Bugzilla :2044172, Bugzilla:2044162

Intel TDX dans les hôtes RHEL

En tant qu'aperçu technologique, la fonctionnalité Intel Trust Domain Extension (TDX) peut désormais être utilisée dans les systèmes d'exploitation invités RHEL 9.2. Si le système hôte prend en charge TDX, vous pouvez déployer des machines virtuelles (VM) RHEL 9 isolées matériellement, appelées domaines de confiance (TD). Notez toutefois que TDX ne fonctionne pas actuellement avec **kdump**, et que l'activation de TDX entraînera l'échec de **kdump** sur la VM.

Bugzilla:1955275

Une image unifiée du noyau de RHEL est désormais disponible en tant qu'aperçu technologique

Dans le cadre d'un aperçu technologique, vous pouvez désormais obtenir le noyau RHEL sous forme d'image de noyau unifié (UKI) pour les machines virtuelles (VM). Une image de noyau unifiée combine le noyau, les initramfs et la ligne de commande du noyau en un seul fichier binaire signé.

Les UKI peuvent être utilisées dans des environnements virtualisés et en nuage, en particulier dans les machines virtuelles confidentielles où de solides capacités SecureBoot sont nécessaires. L'UKI est disponible sous la forme d'un paquetage **kernel-uki-virt** dans les dépôts RHEL 9.

Actuellement, l'UKI RHEL ne peut être utilisée que dans une configuration de démarrage UEFI.

Bugzilla:2142102

9.14. RHEL DANS LES ENVIRONNEMENTS EN NUAGE

RHEL est désormais disponible sur les VM confidentielles Azure en tant qu'aperçu technologique

Avec le noyau RHEL mis à jour, vous pouvez désormais créer et exécuter des machines virtuelles (VM) confidentielles RHEL sur Microsoft Azure en tant qu'aperçu technologique. L'image de noyau unifiée (UKI) récemment ajoutée permet désormais de démarrer des images de machines virtuelles confidentielles cryptées sur Azure. L'UKI est disponible sous la forme d'un paquetage **kernel-uki-virt** dans les dépôts RHEL 9.

Actuellement, l'UKI RHEL ne peut être utilisée que dans une configuration de démarrage UEFI.

Jira:RHELPLAN-139800

9.15. CONTENEURS

Quadlet dans Podman est maintenant disponible en avant-première technologique

À partir de Podman v4.4, vous pouvez utiliser Quadlet pour générer automatiquement un fichier de service **systemd** à partir de la description du conteneur en tant qu'aperçu technologique. La description du conteneur est au format de fichier unitaire **systemd**. La description se concentre sur les détails pertinents du conteneur et cache la complexité technique de l'exécution des conteneurs sous **systemd**. Les Quadlets sont plus faciles à écrire et à maintenir que les fichiers unitaires **systemd**.

Pour plus de détails, voir la documentation amont et Make systemd better for Podman with Quadlet .

Jira:RHELPLAN-148394

Les clients pour les signatures sigstore avec Fulcio et Rekor sont maintenant disponibles en tant qu'aperçu technologique

Avec les serveurs Fulcio et Rekor, vous pouvez désormais créer des signatures en utilisant des certificats à court terme basés sur l'authentification d'un serveur OpenID Connect (OIDC), au lieu de gérer manuellement une clé privée. Les clients pour les signatures sigstore avec Fulcio et Rekor sont maintenant disponibles en tant qu'aperçu technologique. Cette fonctionnalité supplémentaire ne concerne que le support côté client et n'inclut pas les serveurs Fulcio ou Rekor.

Ajoutez la section **fulcio** dans le fichier **policy.json**. Pour signer les images de conteneurs, utilisez les commandes **podman push --sign-by-sigstore=file.yml** ou **skopeo copy --sign-by-sigstore=*file.yml*** où ***file.yml*** est le fichier de paramètres de signature sigstore.

Pour vérifier les signatures, ajoutez la section **fulcio** et les champs **rekorPublicKeyPath** ou **rekorPublicKeyData** dans le fichier **policy.json**. Pour plus d'informations, voir la page de manuel **containers-policy.json**.

Jira:RHELPLAN-136611

CHAPITRE 10. 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.

L'état de la 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 .

10.1. 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.

Bugzilla:1899167

Les personnalisations d'utilisateurs et de groupes dans les blueprints **edge-commit** et **edge-container** ont été supprimées

La spécification d'une personnalisation d'utilisateur ou de groupe dans les blueprints est obsolète pour les types d'image **edge-commit** et **edge-container**, car la personnalisation de l'utilisateur disparaît lorsque vous mettez à niveau l'image et que vous ne spécifiez plus l'utilisateur dans le blueprint. Par conséquent, vous devez spécifier les utilisateurs et les groupes directement dans les blueprints pour les types d'image de bord qui sont utilisés pour déployer un commit OSTree existant, tel que **edge-raw-image**, **edge-installer**, et **edge-simplified-installer**.

Notez que la spécification d'une personnalisation d'un utilisateur ou d'un groupe dans les blueprints reste prise en charge, mais que cette prise en charge sera éventuellement supprimée.

Bugzilla:2173928

10.2. GESTION DES ABONNEMENTS

L'option --token de la commande subscription-manager est obsolète

L'option **--token=<TOKEN>** de la commande **subscription-manager register** est une méthode d'authentification qui permet d'enregistrer votre système auprès de Red Hat. Cette option dépend des capacités offertes par le serveur de droits. Le serveur de droits par défaut, **subscription.rhsm.redhat.com**, prévoit de désactiver cette fonctionnalité. Par conséquent, une tentative d'utilisation de **subscription-manager register --token=<TOKEN>** peut échouer avec le message d'erreur suivant :

```
Token authentication not supported by the entitlement server
```

Vous pouvez continuer à enregistrer votre système en utilisant d'autres méthodes d'autorisation, par exemple en incluant les options jumelées **--username** / **--password** et **--org** / **--activationkey** de la commande **subscription-manager register**.

Bugzilla:2163716

10.3. SHELLS ET OUTILS DE LIGNE DE COMMANDE

L'utilitaire dump du paquetage dump est obsolète

L'utilitaire **dump** utilisé pour la sauvegarde des systèmes de fichiers est obsolète et ne sera pas disponible dans RHEL 9.

Dans RHEL 9, Red Hat recommande d'utiliser l'utilitaire de sauvegarde **tar**, **dd**, ou **bacula**, en fonction du type d'utilisation, qui fournit des sauvegardes complètes et sûres sur les systèmes de fichiers ext2, ext3 et ext4.

Notez que l'utilitaire **restore** du paquet **dump** reste disponible et pris en charge dans RHEL 9 et est disponible en tant que paquet **restore**.

Bugzilla:1997366

Le backend de la base de données SQLite dans Bacula est obsolète

Le système de sauvegarde Bacula prend en charge plusieurs bases de données : PostgreSQL, MySQL et SQLite. Le backend SQLite a été déprécié et ne sera plus supporté dans une version ultérieure de RHEL. En remplacement, migrez vers l'un des autres backends (PostgreSQL ou MySQL) et n'utilisez pas le backend SQLite dans les nouveaux déploiements.

Bugzilla:2089395

10.4. 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

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.

Bugzilla:2054740

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.

Bugzilla:1995600

OpenSSL supprime MD2, MD4, MDC2, Whirlpool, 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, 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.

Bugzilla: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.

Bugzilla:2034569

OpenSSL requiert du padding pour le chiffrement RSA en mode FIPS

OpenSSL ne supporte plus le cryptage RSA sans padding en mode FIPS. Le chiffrement RSA sans remplissage est peu courant et rarement utilisé. Notez que l'encapsulation de clés avec RSA (RSASVE) n'utilise pas de rembourrage mais est toujours prise en charge.

Bugzilla:2168665

10.5. MISE EN RÉSEAU

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.

Bugzilla: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.

Bugzilla: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.

Bugzilla:2089200

10.6. 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 .

Bugzilla:2058153

L'appel système kexec_load pour kexec-tools a été supprimé

L'appel système **kexec_load**, qui charge le deuxième noyau, ne sera plus pris en charge dans les prochaines versions de RHEL. L'appel système **kexec_file_load** remplace **kexec_load** et est désormais l'appel système par défaut sur toutes les architectures.

Bugzilla:2113873

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.

Bugzilla:2013884

10.7. 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.

Bugzilla:2038183

10.8. 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.

Bugzilla:1927780, Jira:RHELPLAN-80695, Bugzilla:1974657

10.9. COMPILATEURS ET OUTILS DE DÉVELOPPEMENT

Les clés de taille inférieure à 2048 sont dépassées par openssl 3.0

Les tailles de clés inférieures à 2048 bits sont dépréciées par **openssl** 3.0 et ne fonctionnent plus dans le mode FIPS de Go.

Bugzilla:2111072

Certains modes de PKCS1 v1.5 sont désormais obsolètes

Certains modes de **PKCS1** v1.5 ne sont pas approuvés dans **FIPS-140-3** pour le cryptage et sont désactivés. Ils ne fonctionneront plus dans le mode FIPS de Go.

Bugzilla:2092016

10.10. 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.

Bugzilla: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

-h et -p ont été supprimées dans les utilitaires clients OpenLDAP.

Le projet OpenLDAP en amont a déprécié les options **-h** et **-p** dans ses utilitaires et recommande d'utiliser l'option **-H** pour spécifier l'URI LDAP. Par conséquent, RHEL 9 a supprimé ces deux options dans tous les utilitaires clients OpenLDAP. Les options **-h** et **-p** seront supprimées des produits RHEL dans les prochaines versions.

Jira:RHELPLAN-137660

Le fournisseur SSSD files est obsolète

Le fournisseur SSSD **files** a été supprimé dans Red Hat Enterprise Linux (RHEL) 9. Le fournisseur **files** pourrait être supprimé dans une prochaine version de RHEL.

Jira:RHELPLAN-139805

Le paramètre nsslapd-idlistscanlimit est obsolète et sa valeur par défaut a été modifiée

Avec la nouvelle optimisation de la réorganisation des filtres, l'impact de l'attribut **nsslapd-idlistscanlimit** sur les performances de recherche est plus néfaste qu'utile. Par conséquent, cet attribut est obsolète. En outre, la valeur par défaut a été remplacée par **2147483646** (illimité).

Bugzilla:1952241

10.11. BUREAU

GTK 2 est désormais obsolète

L'ancienne boîte à outils GTK 2 et les paquets suivants ont été supprimés :

- **adwaita-gtk2-theme**
- **gnome-common**
- **gtk2**
- **gtk2-immodules**
- **hexchat**

Plusieurs autres paquets dépendent actuellement de GTK 2. Ils ont été modifiés de manière à ne plus dépendre des paquets dépréciés dans une future version majeure de RHEL.

Si vous maintenez une application qui utilise GTK 2, Red Hat vous recommande de porter l'application vers GTK 4.

Jira:RHELPLAN-131882

10.12. INFRASTRUCTURES GRAPHIQUES

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

10.13. RÔLES DU SYSTÈME RED HAT ENTERPRISE LINUX

Le rôle de système **network** affiche un avertissement de dépréciation lors de la configuration des équipes sur les nœuds RHEL 9

Les capacités d'équipe réseau ont été dépréciées dans RHEL 9. Par conséquent, l'utilisation du rôle de système **network** RHEL sur un nœud de contrôle RHEL 8 pour configurer une équipe réseau sur des nœuds RHEL 9, affiche un avertissement concernant la dépréciation.

Bugzilla:1999770

10.14. 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.

Bugzilla: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, Bugzilla:1621944

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.

Bugzilla: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**.

Bugzilla:1951814

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

Les anciens modèles de CPU sont désormais obsolètes

Un nombre important de modèles de CPU sont devenus obsolètes et ne seront plus pris en charge pour une utilisation dans des machines virtuelles (VM) dans une prochaine version majeure de RHEL. Les modèles obsolètes sont les suivants :

- Pour Intel : modèles antérieurs aux familles de processeurs Intel Xeon 55xx et 75xx (également connus sous le nom de Nehalem)
- Pour AMD : modèles antérieurs à AMD Opteron G4
- Pour IBM Z : modèles antérieurs à IBM z14

Pour vérifier si votre VM utilise un modèle de processeur obsolète, utilisez l'utilitaire **virsh dominfo** et recherchez une ligne similaire à la suivante dans la section **Messages**:

```
tainted: use of deprecated configuration settings
deprecated configuration: CPU model 'i486'
```

Bugzilla:2060839

La migration en direct basée sur RDMA est obsolète

Avec cette mise à jour, la migration des machines virtuelles en cours d'exécution à l'aide de l'accès direct à la mémoire à distance (RDMA) est devenue obsolète. Par conséquent, il est toujours possible d'utiliser l'URI de migration **rdma://** pour demander une migration via RDMA, mais cette fonctionnalité ne sera plus prise en charge dans une prochaine version majeure de RHEL.

Jira:RHELPLAN-153267

10.15. 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 ou une version ultérieure doivent être redémarrés s'ils sont reliés 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.

Bugzilla:2069279

rhel9/pause a été supprimé

L'image du conteneur **rhel9/pause** a été supprimée.

Bugzilla:2106816

La pile réseau CNI est obsolète

La pile réseau Container Network Interface (CNI) a été supprimée. Auparavant, les conteneurs se connectaient au plugin Container Network Interface (CNI) uniquement via DNS. Podman v.4.0 a introduit une nouvelle pile réseau Netavark. Vous pouvez utiliser la pile réseau Netavark avec Podman et d'autres applications de gestion de conteneurs de l'Open Container Initiative (OCI). La pile réseau Netavark pour Podman est également compatible avec les fonctionnalités avancées de Docker. Les conteneurs situés sur plusieurs réseaux peuvent accéder aux conteneurs situés sur n'importe lequel de ces réseaux.

Pour plus d'informations, voir Passage de la pile réseau de CNI à Netavark .

Jira:RHELPLAN-147725

10.16. 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
- mod_auth_mellon
- motif
- motif-devel
- python3-pytz
- xorg-x11-server-Xorg

CHAPITRE 11. PROBLÈMES CONNUS

Cette partie décrit les problèmes connus dans Red Hat Enterprise Linux 9.2.

11.1. CRÉATION D'INSTALLATEURS ET D'IMAGES

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.

Bugzilla:1640697

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.

Bugzilla:1697896

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.

Bugzilla:2050140

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.

Bugzilla:1877697

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.

Bugzilla:1914955

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.

Bugzilla: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.

Bugzilla:2047713

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.

Bugzilla:1997832

L'image d'installation de RHEL for Edge ne parvient pas à créer des points de montage lors de l'installation d'une charge utile rpm-ostree

Lors du déploiement des charges utiles **rpm-ostree**, utilisées par exemple dans une image d'installation RHEL for Edge, le programme d'installation ne crée pas correctement certains points de montage pour les partitions personnalisées. En conséquence, l'installation est interrompue avec l'erreur suivante :

```
The command 'mount --bind /mnt/sysimage/data /mnt/sysroot/data' exited with the code 32.
```

Pour contourner ce problème :

- Utilisez un schéma de partitionnement automatique et n'ajoutez pas de points de montage manuellement.
- Attribuer manuellement des points de montage uniquement dans le répertoire **/var**. Par exemple, **/var/*my-mount-point***), et les répertoires standard suivants : / **/boot** , **/var**.

Le processus d'installation se termine donc avec succès.

Bugzilla:2125542

NetworkManager ne démarre pas après l'installation lorsqu'il est connecté à un réseau mais qu'il n'y a pas d'adresse DHCP ou d'adresse IP statique configurée

À partir de RHEL 9.0, Anaconda active automatiquement les périphériques réseau lorsqu'il n'y a pas de configuration réseau spécifique **ip=** ou kickstart. Anaconda crée un fichier de configuration persistant par défaut pour chaque périphérique Ethernet. Dans le profil de connexion, les valeurs **ONBOOT** et **autoconnect** sont définies sur **true**. Par conséquent, lors du démarrage du système installé, RHEL active les périphériques réseau et le service **networkManager-wait-online** échoue.

En guise de solution de contournement, procédez de l'une des manières suivantes :

- Supprimez toutes les connexions à l'aide de l'utilitaire **nmcli**, à l'exception de celle que vous souhaitez utiliser. Par exemple :
  a. Liste de tous les profils de connexion :

     ```
     # nmcli connection show
     ```

  b. Supprimez les profils de connexion dont vous n'avez pas besoin :

```
# nmcli connection delete <connection_name>
```

Remplacez <nom_de_la_connexion> par le nom de la connexion que vous souhaitez supprimer.

- Désactive la fonction de connexion automatique au réseau dans Anaconda si aucune configuration réseau spécifique **ip=** ou kickstart n'est définie.
  a. Dans l'interface graphique d'Anaconda, naviguez jusqu'à **Network & Host Name**.
  b. Sélectionnez un périphérique réseau à désactiver.
  c. Cliquez sur **Configure**.
  d. Dans l'onglet **General**, désélectionnez l'option **Connect automatically with priority**.
  e. Cliquez sur **Save**.

Bugzilla:2115783

Impossible de charger un pilote mis à jour à partir du disque de mise à jour des pilotes dans l'environnement d'installation

Une nouvelle version d'un pilote provenant du disque de mise à jour des pilotes peut ne pas se charger si le même pilote provenant du disque d'installation initial a déjà été chargé. Par conséquent, une version mise à jour du pilote ne peut pas être appliquée à l'environnement d'installation.

Pour contourner le problème, utilisez l'option de ligne de commande du noyau **modprobe.blacklist=** en même temps que l'option **inst.dd**. Par exemple, pour s'assurer qu'une version mise à jour du pilote **virtio_blk** provenant d'un disque de mise à jour des pilotes est chargée, utilisez **modprobe.blacklist=virtio_blk**, puis suivez la procédure habituelle d'application des pilotes à partir du disque de mise à jour des pilotes. Le système peut ainsi charger une version mise à jour du pilote et l'utiliser dans l'environnement d'installation.

Bugzilla:2164216

L'installateur se bloque en mode FIPS lors de la création de dispositifs LUKS avec une phrase de passe courte

La longueur minimale d'une phrase de passe utilisée pour les périphériques LUKS est de 8 octets lorsque le système fonctionne en mode FIPS. Par conséquent, lors de la création d'un périphérique LUKS avec une phrase de passe inférieure à 8 octets et d'une installation en mode FIPS, le programme d'installation se bloque. Pour contourner ce problème, utilisez une phrase de passe LUKS d'au moins 8 octets. Par conséquent, le programme d'installation ne se bloque pas lors de la création de périphériques LUKS en mode FIPS.

Certains caractères nécessitent plus d'un octet pour être codés. Par conséquent, vous pouvez utiliser moins de 8 caractères dans certains cas, en fonction des caractères utilisés. Une phrase de passe comportant au moins 8 caractères fonctionne dans tous les cas.

Bugzilla:2163497

Les installations Kickstart ne parviennent pas à configurer la connexion réseau

Anaconda effectue la configuration réseau du kickstart uniquement par le biais de l'API NetworkManager. Anaconda traite la configuration du réseau après la section **%pre** kickstart. Par conséquent, certaines tâches de la section de démarrage **%pre** sont bloquées. Par exemple, le

téléchargement de paquets à partir de la section **%pre** échoue en raison de l'indisponibilité de la configuration du réseau.

Pour contourner ce problème :

- Configurer le réseau, par exemple à l'aide de l'outil **nmcli**, dans le cadre du script **%pre**.
- Utilisez les options de démarrage du programme d'installation pour configurer le réseau pour le script **%pre**.

Par conséquent, il est possible d'utiliser le réseau pour les tâches de la section **%pre** et le processus d'installation de kickstart se termine.

Bugzilla:2173992

11.2. 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.

Bugzilla:2073510

11.3. 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**.

Bugzilla: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.

Bugzilla:2053598

11.4. 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).

Bugzilla: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.

Bugzilla:1984982

libotr n'est pas conforme à la norme FIPS

La bibliothèque **libotr** et la boîte à outils pour la messagerie off-the-record (OTR) fournissent un chiffrement de bout en bout pour les conversations de messagerie instantanée. Cependant, la bibliothèque **libotr** n'est pas conforme aux normes FIPS (Federal Information Processing Standards) en raison de son utilisation des fonctions **gcry_pk_sign()** et **gcry_pk_verify()**. Par conséquent, vous ne pouvez pas utiliser la bibliothèque **libotr** en mode FIPS.

Bugzilla:2086562

11.5. SÉCURITÉ

tangd-keygen ne gère pas correctement les umask qui ne sont pas par défaut

Le script **tangd-keygen** ne modifie pas les autorisations de fichiers pour les fichiers de clés générés. Par conséquent, sur les systèmes dotés d'un masque de mode de création de fichiers utilisateur par défaut (**umask**) qui empêche la lecture des clés par d'autres utilisateurs, la commande **tang-show-keys** renvoie le message d'erreur **Internal Error 500** au lieu d'afficher les clés.

Pour contourner le problème, utilisez la commande **chmod o r *.jwk** pour modifier les permissions sur les fichiers du répertoire **/var/db/tang**.

Bugzilla:2188743

OpenSSL ne détecte pas si un jeton PKCS #11 supporte 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.

Bugzilla: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.

Bugzilla:1685470

scp vide les fichiers copiés sur eux-mêmes lorsqu'une syntaxe spécifique est utilisée

L'utilitaire **scp** est passé du protocole de copie sécurisée (SCP) au protocole de transfert de fichiers SSH (SFTP), plus sûr. Par conséquent, la copie d'un fichier d'un emplacement vers le même emplacement efface le contenu du fichier. Le problème concerne la syntaxe suivante :

scp localhost:/myfile localhost:/myfile

Pour contourner ce problème, ne copiez pas de fichiers vers une destination identique à l'emplacement source en utilisant cette syntaxe.

Le problème a été corrigé pour les syntaxes suivantes :

- **scp /myfile localhost:/myfile**
- **scp localhost:~/myfile ~/myfile**

Bugzilla:2056884

Le module complémentaire OSCAP Anaconda ne récupère pas les profils personnalisés dans l'installation graphique

Le module complémentaire OSCAP Anaconda ne fournit pas d'option pour sélectionner ou désélectionner l'adaptation des profils de sécurité dans l'installation graphique RHEL. À partir de RHEL 8.8, le module complémentaire ne prend pas en compte l'adaptation par défaut lors de l'installation à

partir d'archives ou de paquets RPM. Par conséquent, l'installation affiche le message d'erreur suivant au lieu de récupérer un profil OSCAP adapté :

```
There was an unexpected problem with the supplied content.
```

Pour contourner ce problème, vous devez spécifier des chemins dans la section **don org_fedora_oscap** de votre fichier Kickstart, par exemple :

```
xccdf-path = /usr/share/xml/scap/sc_tailoring/ds-combined.xml
tailoring-path = /usr/share/xml/scap/sc_tailoring/tailoring-xccdf.xml
```

Par conséquent, vous ne pouvez utiliser l'installation graphique pour les profils personnalisés OSCAP qu'avec les spécifications Kickstart correspondantes.

Bugzilla:2165920

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**.

Bugzilla:2105162

oscap-anaconda-addon ne permet pas au CIS de durcir les systèmes avec le groupe de paquets Network Servers

Lors de l'installation de RHEL Network Servers avec un profil de sécurité CIS (**cis**, **cis_server_l1**, **cis_workstation_l1**, ou **cis_workstation_l2**) sur des systèmes où le groupe de paquets Network Servers est sélectionné, **oscap-anaconda-addon** envoie le message d'erreur **package tftp has been added to the list of excluded packages, but it can't be removed from the current software selection without breaking the install**. Pour poursuivre l'installation, revenez à la sélection des logiciels et décochez la case **Network Servers** additional software pour permettre à l'installation et au durcissement de se terminer. Installez ensuite les paquets requis.

Bugzilla:2172264

Keylime n'accepte pas les certificats PEM concaténés

Lorsque Keylime reçoit une chaîne de certificats sous la forme de plusieurs certificats au format PEM concaténés dans un seul fichier, le composant Keylime **keylime-agent-rust** n'utilise pas correctement tous les certificats fournis lors de la vérification de la signature, ce qui entraîne un échec de la poignée de main TLS. En conséquence, les composants clients (**keylime_verifier** et **keylime_tenant**) ne peuvent pas se connecter à l'agent Keylime. Pour contourner ce problème, utilisez un seul certificat au lieu de plusieurs.

Jira:RHELPLAN-157225

Keylime nécessite un fichier spécifique pour tls_dir = default

Lorsque la variable **tls_dir** est définie sur **default** dans la configuration du vérificateur ou du registraire Keylime, Keylime vérifie la présence du fichier **cacert.crt** dans le répertoire **/var/lib/keylime/cv_ca**. Si le fichier n'est pas présent, le service **keylime_verifier** ou **keylime_registrar** ne démarre pas et enregistre le message suivant dans un journal : **Exception: It appears that the verifier has not yet created a CA and certificates, please run the verifier first**. En conséquence, Keylime rejette les certificats d'autorité de certification (CA) personnalisés qui ont un nom de fichier différent même s'ils sont placés dans le répertoire **/var/lib/keylime/ca_cv**.

Pour contourner ce problème et utiliser des certificats d'autorité de certification personnalisés, spécifiez manuellement **tls_dir =/var/lib/keylime/ca_cv** au lieu d'utiliser **tls_dir = default**.

Jira:RHELPLAN-157337

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**.

Bugzilla: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.

Bugzilla:2038978

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.

Bugzilla:2070722

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.

Bugzilla:2073567

Problèmes de consommation de mémoire d'OpenSCAP

Sur les systèmes disposant d'une mémoire limitée, l'analyseur OpenSCAP peut se terminer prématurément ou ne pas générer les fichiers de résultats. Pour contourner ce problème, vous pouvez personnaliser le profil d'analyse afin de désélectionner les règles qui impliquent une récursivité sur l'ensemble du système de fichiers /:

- **rpm_verify_hashes**
- **rpm_verify_permissions**

- **rpm_verify_ownership**
- **file_permissions_unauthorized_world_writable**
- **no_files_unowned_by_user**
- **dir_perms_world_writable_system_owned**
- **file_permissions_unauthorized_suid**
- **file_permissions_unauthorized_sgid**
- **file_permissions_ungroupowned**
- **dir_perms_world_writable_sticky_bits**

Pour plus de détails et de solutions de contournement, voir l'article de la base de connaissances correspondant.

Bugzilla:2161499

11.6. 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.

Bugzilla:2151040

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.

Bugzilla: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**.

Bugzilla:2082303

11.7. NOYAU

Le mécanisme kdump dans le noyau provoque des erreurs OOM sur le noyau 64K

La taille de page du noyau de 64 Ko sur l'architecture ARM 64 bits utilise plus de mémoire que le noyau de 4 Ko. Par conséquent, **kdump** provoque une panique du noyau et l'allocation de mémoire échoue avec des erreurs de type "out of memory" (OOM). Pour contourner le problème, configurez manuellement la valeur de **crashkernel** à 640 Mo. Par exemple, définissez le paramètre **crashkernel=** comme **crashkernel=2G- :640M**.

Par conséquent, le mécanisme **kdump** n'échoue pas sur le noyau 64K dans le scénario décrit.

Bugzilla:2160676

Les applications clients qui dépendent de la taille de page du noyau peuvent nécessiter une mise à jour lors du passage d'un noyau de 4k à 64k pages

RHEL est compatible avec les noyaux de taille de page 4k et 64k. Les applications clients qui dépendent d'un noyau de 4k peuvent nécessiter une mise à jour lors du passage d'un noyau de 4k à un noyau de 64k. Parmi les cas connus, citons **jemalloc** et les applications dépendantes.

La bibliothèque d'allocation de mémoire **jemalloc** est sensible à la taille de page utilisée dans l'environnement d'exécution du système. La bibliothèque peut être construite pour être compatible avec des noyaux de 4k et 64k pages, par exemple, lorsqu'elle est configurée avec **--with-lg-page=16** ou **env JEMALLOC_SYS_WITH_LG_PAGE=16** (pour **jemallocator** Rust crate). Par conséquent, un décalage peut se produire entre la taille de page de l'environnement d'exécution et la taille de page qui était présente lors de la compilation des binaires qui dépendent de **jemalloc**. Par conséquent, l'utilisation d'une application basée sur **jemalloc** déclenche l'erreur suivante :

```
<jemalloc> : Taille de page système non supportée
```

Pour éviter ce problème, utilisez l'une des approches suivantes :

- Utilisez la configuration de construction ou les options d'environnement appropriées pour créer des binaires compatibles avec les tailles de page 4k et 64k.
- Construire tous les paquets de l'espace utilisateur qui utilisent **jemalloc** après avoir démarré dans le noyau final de 64k et l'environnement d'exécution.

Par exemple, vous pouvez construire l'outil **fd-find**, qui utilise également **jemalloc**, avec le gestionnaire de paquets Rust **cargo**. Dans l'environnement 64k final, déclenchez une nouvelle compilation de toutes les dépendances pour résoudre le problème de taille de page en entrant la commande **cargo**:

```
# cargo install fd-find --force
```

Bugzilla:2167783

Le service kdump ne parvient pas à créer le fichier initrd sur les systèmes IBM Z

Sur les systèmes IBM Z 64 bits, le service **kdump** ne parvient pas à charger le disque RAM initial (**initrd**) lorsque les informations de configuration liées à **znet**, telles que **s390-subchannels**, se trouvent dans un profil de connexion **NetworkManager** inactif. Par conséquent, le mécanisme **kdump** échoue avec l'erreur suivante :

```
dracut: Failed to set up znet
kdump: mkdumprd: failed to make kdump initrd
```

En guise de solution de contournement, utilisez l'une des solutions suivantes :

- Configurer un lien ou un pont réseau en réutilisant le profil de connexion qui contient les informations de configuration **znet**:

  ```
  $ nmcli connection modify enc600 master bond0 slave-type bond
  ```

- Copier les informations de configuration de **znet** du profil de connexion inactif vers le profil de connexion actif :

  a. Exécutez la commande **nmcli** pour interroger les profils de connexion **NetworkManager**:

  ```
  # nmcli connection show

  NAME                UUID              TYPE   Device

  bridge-br0          ed391a43-bdea-4170-b8a2 bridge   br0
  bridge-slave-enc600  caf7f770-1e55-4126-a2f4 ethernet enc600
  enc600              bc293b8d-ef1e-45f6-bad1 ethernet --
  ```

  b. Mettre à jour le profil actif avec les informations de configuration de la connexion inactive :

  ```
  #!/bin/bash
   inactive_connection=enc600
   active_connection=bridge-slave-enc600
   for name in nettype subchannels options; do
   field=802-3-ethernet.s390-$name
   val=$(nmcli --get-values "$field"connection show "$inactive_connection")
   nmcli connection modify "$active_connection" "$field" $val"
   done
  ```

  c. Redémarrez le service **kdump** pour que les modifications soient prises en compte :

  ```
  # kdumpctl restart
  ```

Bugzilla:2064708

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.

Bugzilla:2000616

La fonctionnalité Delay Accounting n'affiche pas par défaut les colonnes de statistiques SWAPIN et IO%

La fonctionnalité **Delayed Accounting**, contrairement aux premières versions, est désactivée par défaut. Par conséquent, l'application **iotop** n'affiche pas les colonnes de statistiques **SWAPIN** et **IO%** et affiche l'avertissement suivant :

```
CONFIG_TASK_DELAY_ACCT not enabled in kernel, cannot determine SWAPIN and IO%
```

La fonctionnalité **Delay Accounting**, qui utilise l'interface **taskstats**, fournit des statistiques sur les retards pour toutes les tâches ou threads qui appartiennent à un groupe de threads. Les retards dans l'exécution des tâches surviennent lorsqu'elles attendent qu'une ressource du noyau devienne disponible, par exemple, une tâche qui attend qu'une unité centrale soit libre pour s'exécuter. Les statistiques aident à définir la priorité de l'unité centrale d'une tâche, la priorité des entrées/sorties et les valeurs limites de **rss** de manière appropriée.

Pour contourner le problème, vous pouvez activer l'option de démarrage **delayacct** soit au moment de l'exécution, soit au moment du démarrage.

- Pour activer **delayacct** au moment de l'exécution, entrez :

  ```
  echo 1 > /proc/sys/kernel/task_delayacct
  ```

  Notez que cette commande active la fonctionnalité à l'échelle du système, mais uniquement pour les tâches que vous démarrez après avoir exécuté cette commande.

- Pour activer **delayacct** de manière permanente au démarrage, utilisez l'une des procédures suivantes :

  - Modifiez le fichier **/etc/sysctl.conf** pour remplacer les paramètres par défaut :

    a. Ajoutez l'entrée suivante au fichier **/etc/sysctl.conf**:

    ```
    kernel.task_delayacct = 1
    ```

    Pour plus d'informations, voir Comment définir les variables sysctl sur Red Hat Enterprise Linux.

    b. Redémarrez le système pour que les modifications soient prises en compte.

  - Ajouter l'option **delayacct** à la ligne de commande du noyau.
    Pour plus d'informations, voir Configuration des paramètres de la ligne de commande du noyau.

Par conséquent, l'application **iotop** affiche les colonnes de statistiques **SWAPIN** et **IO%**.

Bugzilla:2132480

Le mécanisme kdump ne parvient pas à capturer le fichier 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.

Bugzilla: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**.

Pour contourner ce problème, procédez de l'une des manières suivantes :

- Diminuez la valeur du paramètre **crashkernel** d'un minimum de 240 MB pour répondre à l'exigence de taille, par exemple **crashkernel=240M**.
- Utilisez l'option **crashkernel=x,high** pour réserver la mémoire du noyau de crash supérieure à 4 Go pour **kdump**.

Par conséquent, l'allocation de mémoire au noyau de crash pour **kdump** n'échoue pas sur les systèmes Ampere Altra.

Bugzilla:2065013

RHEL ne reconnaît pas les disques NVMe lorsque VMD est activé

Lorsque vous réinitialisez ou rattachez le pilote, le domaine Volume Management Device (VMD) ne se réinitialise pas en douceur. Par conséquent, le matériel ne peut pas détecter et énumérer correctement ses périphériques. Par conséquent, le système d'exploitation avec VMD activé ne reconnaît pas les disques NVMe, en particulier lors de la réinitialisation d'un serveur ou de l'utilisation d'une machine virtuelle.

Bugzilla:2128610

Le site iwl7260-firmware interrompt le Wi-Fi sur Intel Wi-Fi 6 AX200, AX210, et Lenovo ThinkPad P1 Gen 4

Après la mise à jour du pilote **iwl7260-firmware** ou **iwl7260-wifi** vers la version fournie par RHEL 9.1 et plus, le matériel se retrouve dans un état interne incorrect et signale son état de manière incorrecte. Par conséquent, les cartes Intel Wifi 6 peuvent ne pas fonctionner et afficher le message d'erreur :

```
kernel: iwlwifi 0000:09:00.0: Failed to start RT ucode: -110
kernel: iwlwifi 0000:09:00.0: WRT: Collecting data: ini trigger 13 fired (delay=0ms)
kernel: iwlwifi 0000:09:00.0: Failed to run INIT ucode: -110
```

Une solution non confirmée consiste à éteindre le système et à le rallumer. Ne pas redémarrer.

Bugzilla:2129288

weak-modules from kmod ne fonctionne pas avec les interdépendances de modules

Le script **weak-modules** fourni par le paquet **kmod** détermine quels modules sont compatibles avec les noyaux installés. Cependant, lors de la vérification de la compatibilité des modules avec le noyau, **weak-modules** traite les dépendances des symboles des modules de la version supérieure à la version inférieure du noyau pour lequel ils ont été construits. Par conséquent, les modules avec des interdépendances construits pour différentes versions du noyau peuvent être interprétés comme non compatibles, et le script **weak-modules** ne fonctionne donc pas dans ce cas.

Pour contourner le problème, compilez ou installez les modules supplémentaires avec le dernier noyau stocké avant d'installer le nouveau noyau.

Bugzilla:2103605

Le pilote mlx5 échoue lors de l'utilisation de l'adaptateur Mellanox ConnectX-5

En mode de pilote de commutateur Ethernet (**switchdev**), le pilote **mlx5** échoue lorsqu'il est configuré avec le paramètre DMFS (device managed flow steering) et le matériel pris en charge par l'adaptateur **ConnectX-5**. En conséquence, vous pouvez voir le message d'erreur suivant :

```
BUG: Bad page cache in process umount pfn:142b4b
```

Pour contourner ce problème, utilisez le paramètre SMFS (software managed flow steering) au lieu de DMFS.

Bugzilla:2180665

11.8. CHARGEUR DE DÉMARRAGE

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.

Bugzilla:2026579

11.9. SYSTÈMES DE FICHIERS ET STOCKAGE

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**.

Bugzilla:1983602

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.

Bugzilla:2033080

Le service **blk-availability** systemd désactive les piles de périphériques 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.

Bugzilla:2011699

La désactivation de la comptabilisation des quotas n'est plus possible pour un système de fichiers XFS monté avec des quotas activés

Depuis RHEL 9.2, il n'est plus possible de désactiver la comptabilisation des quotas sur un système de fichiers XFS qui a été monté avec des quotas activés.

Pour contourner ce problème, désactivez la comptabilisation des quotas en remontant le système de fichiers avec l'option quota supprimée.

Bugzilla:2160619

Le système ne démarre pas lors de l'ajout d'un périphérique NVMe-FC en tant que point de montage dans le fichier **/etc/fstab**

Les périphériques NVMe-FC (Non-volatile Memory Express over Fibre Channel) montés via le fichier **/etc/fstab** ne se montent pas au démarrage et le système passe en mode d'urgence. Cela est dû à un bogue connu dans les services **nvme-cli nvmf-autoconnect systemd**.

Bugzilla:2168603

Tâches LVM suspendues avec l'hôte SAN Boot après l'émission d'une restitution NetApp

Avec l'hôte RHEL 9.2 SAN Boot, l'exécution de l'opération NetApp Giveback entraîne des avertissements de tâches suspendues LVM et des E/S bloquées, même lorsque des chemins alternatifs sont disponibles dans un environnement DM-Multipath. Pour remédier à cette situation, redémarrez votre système. Il n'existe actuellement aucune solution connue ou solution de contournement pour ce problème.

Bugzilla:2173947

modification de la règle udev pour les périphériques NVMe

Il y a un changement de règle udev pour les périphériques NVMe qui ajoute le paramètre **OPTIONS="string_escape=replace"**. Cela entraîne un changement de nom du disque by-id pour certains fournisseurs, si le numéro de série de votre périphérique comporte des espaces blancs.

Bugzilla:2185048

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

python3.11-lxml ne fournit pas le sous-module lxml.isoschematron

Le paquet **python3.11-lxml** est distribué sans le sous-module **lxml.isoschematron** car il n'est pas sous licence open source. Le sous-module implémente le support ISO Schematron. Comme alternative, la validation pré-ISO-Schematron est disponible dans la classe **lxml.etree.Schematron**. Le reste du contenu du paquetage **python3.11-lxml** n'est pas affecté.

Bugzilla:2157708

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.

Bugzilla:1991500

11.11. 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.

Bugzilla:2083727

GCC dans GCC Toolset 12 : la détection du processeur peut échouer sur les processeurs Intel Sapphire Rapids

La détection du CPU sur les processeurs Intel Sapphire Rapids repose sur l'existence de la fonctionnalité **AVX512_VP2INTERSECT**. Cette fonctionnalité a été supprimée de la version 12 du GCC Toolset et, par conséquent, la détection du processeur peut échouer sur les processeurs Intel Sapphire Rapids.

Bugzilla:2141718

11.12. GESTION DE L'IDENTITÉ

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.

Bugzilla: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.

Bugzilla:2047175

MIT Kerberos ne prend pas en charge les certificats ECC pour PKINIT

MIT Kerberos n'implémente pas le document RFC5349 request for comments, qui décrit la conception de la prise en charge de la cryptographie à courbe elliptique (ECC) dans la cryptographie à clé publique pour l'authentification initiale (PKINIT). Par conséquent, le paquet MIT **krb5-pkinit**, utilisé par RHEL, ne prend pas en charge les certificats ECC. Pour plus d'informations, voir Prise en charge de la cryptographie à courbe elliptique (ECC) dans la cryptographie à clé publique pour l'authentification initiale dans Kerberos (PKINIT).

Bugzilla:2106043

La sous-politique DEFAULT:SHA1 doit être définie sur les clients RHEL 9 pour que PKINIT fonctionne contre 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.

Cependant, le centre de distribution Kerberos (KDC) d'Active Directory (AD) utilise toujours l'algorithme de condensé SHA-1 pour signer les messages CMS. Par conséquent, les clients Kerberos RHEL 9 ne parviennent pas à authentifier les utilisateurs en utilisant PKINIT contre un KDC AD.

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
```

Bugzilla:2060798

L'authentification PKINIT d'un utilisateur échoue si un agent Kerberos RHEL 9 communique avec un agent Kerberos non RHEL-9 et non AD

Si un agent Kerberos RHEL 9, qu'il s'agisse d'un client ou d'un centre de distribution Kerberos (KDC), interagit avec un agent Kerberos non RHEL-9 qui n'est pas un agent Active Directory (AD), l'authentification PKINIT de l'utilisateur 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 et non AD pour vous assurer qu'il ne signe pas les données CMS à l'aide de l'algorithme SHA-1. Pour cela, mettez à jour votre client Kerberos ou les paquets KDC avec 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

Par conséquent, l'authentification PKINIT de l'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 contre les KDC AD.

Bugzilla:2077450

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
```

Bugzilla:2057471

Le client Heimdal ne parvient pas à authentifier un utilisateur à l'aide de PKINIT contre le KDC RHEL 9

Par défaut, un client Heimdal Kerberos initie l'authentification PKINIT d'un utilisateur IdM en utilisant Modular Exponential (MODP) Diffie-Hellman Group 2 pour Internet Key Exchange (IKE). Cependant, le Centre de distribution Kerberos (KDC) du MIT sur RHEL 9 ne prend en charge que les groupes MODP 14 et 16.

Par conséquent, la demande de pré-authentification échoue avec l'erreur **krb5_get_init_creds: PREAUTH_FAILED** sur le client Heimdal et **Key parameters not accepted** sur le KDC MIT RHEL.

Pour contourner ce problème, assurez-vous que le client Heimdal utilise le groupe MODP 14. Définissez le paramètre **pkinit_dh_min_bits** dans la section **libdefaults** du fichier de configuration du client sur 1759 :

```
[libdefaults]
pkinit_dh_min_bits = 1759
```

En conséquence, le client Heimdal complète la pré-authentification PKINIT contre le KDC MIT de RHEL.

Bugzilla:2106296

IdM en mode FIPS ne prend pas en charge l'utilisation du protocole NTLMSSP pour établir une confiance bidirectionnelle entre forêts

L'établissement d'une confiance bidirectionnelle entre Active Directory (AD) et Identity Management (IdM) avec le mode FIPS activé échoue parce que l'authentification NTLMSSP (New Technology LAN Manager Security Support Provider) n'est pas conforme à la norme FIPS. IdM en mode FIPS n'accepte pas le hachage NTLM RC4 que le contrôleur de domaine AD utilise lors de la tentative d'authentification.

Bugzilla:2124243

Échec des demandes de certificats de transfert de technologie entre IdM et AD

Les informations du certificat d'attributs de privilèges (PAC) dans les tickets IdM Kerberos sont désormais signées avec le cryptage AES SHA-2 HMAC, qui n'est pas pris en charge par Active Directory (AD).

Par conséquent, les demandes de TGS entre IdM et AD, c'est-à-dire les configurations de confiance à double sens, échouent avec l'erreur suivante :

```
Erreur générique (voir texte électronique) lors de l'obtention des informations d'identification pour
<service principal>
```

Bugzilla:2060421

Le chiffrement et le déchiffrement de la chambre forte IdM échouent en mode FIPS

Le chiffrement OpenSSL RSA-PKCS1v15 est bloqué si le mode FIPS est activé. Par conséquent, les chambres fortes de gestion de l'identité (IdM) ne fonctionnent pas correctement, car IdM utilise actuellement le cryptage PKCS1v15 pour envelopper la clé de session avec le certificat de transport.

Bugzilla:2089907

Les utilisateurs qui n'ont pas de SID ne peuvent pas se connecter à IdM après une mise à jour

Après la mise à niveau de votre réplique IdM vers RHEL 9.2, le centre de distribution Kerberos (KDC) IdM peut ne pas délivrer de tickets d'attribution de tickets (TGT) aux utilisateurs qui n'ont pas d'identifiants de sécurité (SID) attribués à leurs comptes. Par conséquent, les utilisateurs ne peuvent pas se

connecter à leurs comptes.

Pour contourner le problème, générez des SID en exécutant la commande suivante en tant qu'administrateur IdM sur une autre réplique IdM dans la topologie :

```
# ipa config-mod --enable-sid --add-sids
```

Ensuite, si les utilisateurs ne peuvent toujours pas se connecter, examinez le journal des erreurs du serveur d'annuaire. Vous devrez peut-être ajuster les plages d'ID pour inclure les identités POSIX des utilisateurs.

Voir la solution de la base de connaissances When upgrading to RHEL9, IDM users are not able to login anymore pour plus d'informations.

Jira:RHELPLAN-157939

Les utilisateurs IdM migrés peuvent être incapables de se connecter en raison de la non-concordance des identifiants de domaine

Si vous avez utilisé le script **ipa migrate-ds** pour migrer des utilisateurs d'un déploiement IdM à un autre, ces utilisateurs peuvent avoir des problèmes pour utiliser les services IdM parce que leurs identifiants de sécurité (SID) n'ont pas le SID du domaine de l'environnement IdM actuel. Par exemple, ces utilisateurs peuvent récupérer un ticket Kerberos avec l'utilitaire **kinit**, mais ils ne peuvent pas se connecter. Pour résoudre ce problème, consultez l'article suivant de la base de connaissances : Migrated IdM users unable to log in due to mismatching domain SIDs (Utilisateurs IdM migrés incapables de se connecter en raison de la non-concordance des SID de domaine).

Jira:RHELPLAN-109613

MIT krb5 L'utilisateur ne parvient pas à obtenir un TGT AD en raison de l'incompatibilité des types de chiffrement générant le PAC de l'utilisateur

Dans MIT **krb5 1.20** et les paquets ultérieurs, un certificat d'attribut de privilège (PAC) est inclus par défaut dans tous les tickets Kerberos. Le Centre de distribution Kerberos (KDC) du MIT sélectionne le type de chiffrement le plus puissant disponible pour générer la somme de contrôle du KDC dans le PAC, qui est actuellement le type de chiffrement **AES HMAC-SHA2** défini dans la RFC8009. Cependant, Active Directory (AD) ne prend pas en charge cette RFC. Par conséquent, dans une configuration AD-MIT cross-realm, un utilisateur de MIT **krb5** ne parvient pas à obtenir un ticket AD (TGT) parce que le TGT cross-realm généré par MIT KDC contient un type de somme de contrôle KDC incompatible dans le PAC.

Pour contourner le problème, définissez le paramètre **disable_pac** à **true** pour le domaine MIT dans la section **[realms]** du fichier de configuration **/var/kerberos/krb5kdc/kdc.conf**. En conséquence, le KDC du MIT génère des tickets sans PAC, ce qui signifie qu'AD ne procède pas à la vérification de la somme de contrôle et qu'un utilisateur de MIT **krb5** peut obtenir un TGT AD.

Bugzilla:2016312

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

L'ajout d'une réplique RHEL 9 en mode FIPS à un déploiement IdM en mode FIPS initialisé avec RHEL 8.6 ou une version antérieure échoue

La politique cryptographique FIPS par défaut de RHEL 9 visant à se conformer à la norme FIPS 140-3 n'autorise pas l'utilisation de la fonction de dérivation de clé des types de chiffrement AES HMAC-SHA1, telle que définie par la RFC3961, section 5.1.

Cette contrainte constitue un obstacle lors de l'ajout d'une réplique Identity Management (IdM) RHEL 9 en mode FIPS à un environnement IdM RHEL 8 en mode FIPS dans lequel le premier serveur a été installé sur un système RHEL 8.6 ou antérieur. En effet, il n'existe pas de types de chiffrement communs entre RHEL 9 et les versions précédentes de RHEL, qui utilisent généralement les types de chiffrement AES HMAC-SHA1 mais pas les types de chiffrement AES HMAC-SHA2.

Vous pouvez afficher le type de cryptage de votre clé principale IdM en entrant la commande suivante sur le serveur :

```
# kadmin.local getprinc K/M | grep -E '^Key:'
```

Pour contourner le problème, activez l'utilisation de AES HMAC-SHA1 sur la réplique RHEL 9 :

```
update-crypto-policies --set FIPS:AD-SUPPORT
```

AVERTISSEMENT

Cette solution de contournement pourrait être contraire à la conformité FIPS.

Par conséquent, l'ajout de la réplique RHEL 9 au déploiement IdM se déroule correctement.

Notez que des travaux sont en cours pour fournir une procédure permettant de générer les clés Kerberos cryptées AES HMAC-SHA2 manquantes sur les serveurs RHEL 7 et RHEL 8. Cela permettra d'atteindre la conformité FIPS 140-3 sur la réplique RHEL 9. Toutefois, ce processus ne sera pas entièrement automatisé, car la conception de la cryptographie des clés Kerberos rend impossible la conversion des clés existantes en différents types de cryptage. La seule solution consiste à demander aux utilisateurs de renouveler leurs mots de passe.

Bugzilla:2103327

SSSD enregistre correctement les noms DNS

Auparavant, si le DNS était mal configuré, SSSD échouait toujours lors de la première tentative d'enregistrement du nom DNS. Pour contourner ce problème, cette mise à jour fournit un nouveau paramètre : **dns_resolver_use_search_list**. Définissez **dns_resolver_use_search_list = false** pour éviter d'utiliser la liste de recherche DNS.

Bugzilla:1608496

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.

Bugzilla:2053204

Directory Server ne peut importer des fichiers LDIF qu'à partir de /var/lib/dirsrv/slapd-*instance_name*/ldif/

Depuis RHEL 8.3, Red Hat Directory Server (RHDS) utilise ses propres répertoires privés et la directive **PrivateTmp** systemd est activée par défaut pour les services LDAP. Par conséquent, RHDS ne peut importer des fichiers LDIF qu'à partir du répertoire **/var/lib/dirsrv/slapd-*instance_name*/ldif/** . Si le fichier LDIF est stocké dans un répertoire différent, tel que **/var/tmp**, **/tmp**, ou **/root**, l'importation échoue avec une erreur similaire à la suivante :

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

Pour contourner ce problème, procédez comme suit :

1. Déplacer le fichier LDIF dans le répertoire **/var/lib/dirsrv/slapd-*instance_name*/ldif/** répertoire :

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
```

2. Définir les autorisations permettant à l'utilisateur **dirsrv** de lire le fichier :

```
# chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
```

3. Rétablir le contexte SELinux :

```
# restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
```

Pour plus d'informations, voir l'article de la solution LDAP Service cannot access files under the host's /tmp and /var/tmp directories.

Bugzilla:2075525

11.13. 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.

Bugzilla: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.

Bugzilla:2060308

11.14. INFRASTRUCTURES GRAPHIQUES

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

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.

Bugzilla: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

11.15. LA CONSOLE WEB

Les étapes de liaison NBDE de la console web ne fonctionnent pas sur les groupes de volumes avec un système de fichiers racine

En raison d'un bogue dans le code permettant de déterminer si l'utilisateur ajoute ou non une clé Tang au système de fichiers racine, le processus de liaison dans la console Web se bloque lorsqu'il n'y a pas de système de fichiers sur le conteneur LUKS. Comme la console Web affiche le message d'erreur **TypeError: Qe(...) is undefined** après que vous avez cliqué sur le bouton **Trust key** dans la boîte de dialogue **Verify key**, vous devez effectuer toutes les étapes requises dans l'interface de ligne de commande dans le scénario décrit.

Bugzilla:2203361

La console VNC fonctionne mal à certaines résolutions

Lorsque vous utilisez la console Virtual Network Computing (VNC) sous certaines résolutions d'affichage, vous pouvez rencontrer un problème de décalage de la souris ou ne voir qu'une partie de l'interface. Par conséquent, l'utilisation de la console VNC peut s'avérer impossible. Pour contourner ce problème, vous pouvez essayer d'agrandir la taille de la console VNC ou utiliser la visionneuse de bureau dans l'onglet de la console pour lancer la visionneuse à distance à la place.

Bugzilla:2030836

11.16. RÔLES DU SYSTÈME RED HAT ENTERPRISE LINUX

Le rôle du système metrics ne fonctionne pas avec la collecte de données sur les personnes handicapées

La collecte de faits Ansible peut être désactivée dans votre environnement pour des raisons de performance ou autres. Dans de telles configurations, il n'est actuellement pas possible d'utiliser le rôle système **metrics**. Pour contourner ce problème, activez la mise en cache des faits ou n'utilisez pas le rôle système **metrics** s'il n'est pas possible d'utiliser la collecte de faits.

Bugzilla:2078999

Si firewalld.service est masqué, l'utilisation du rôle de système RHEL firewall échoue

Si **firewalld.service** est masqué sur un système RHEL, le rôle de système RHEL **firewall** échoue. Pour contourner ce problème, démasquez l'adresse **firewalld.service**:

```
systemctl unmask firewalld.service
```

Bugzilla:2123859

Impossible d'enregistrer des systèmes avec des noms d'environnement

Le rôle système **rhc** ne parvient pas à enregistrer le système lorsqu'il spécifie des noms d'environnement dans **rhc_environment**. Pour contourner ce problème, utilisez les identifiants d'environnement au lieu des noms d'environnement lors de l'enregistrement.

Bugzilla:2187539

Le rôle de système rhc échoue sur les systèmes déjà enregistrés lorsque rhc_auth contient des clés d'activation

L'exécution de fichiers de livre de jeu sur des systèmes déjà enregistrés échoue si des clés d'activation sont spécifiées pour le paramètre **rhc_auth**. Pour contourner ce problème, ne spécifiez pas de clés d'activation lors de l'exécution du fichier playbook sur le système déjà enregistré.

Bugzilla:2186218

11.17. VIRTUALISATION

L'installation d'une machine virtuelle via https ou ssh échoue dans certains cas

Actuellement, l'utilitaire **virt-install** échoue lorsqu'il tente d'installer un système d'exploitation invité (OS) à partir d'une source ISO via une connexion https ou ssh - 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**.

De même, l'utilisation de la console web RHEL 9 pour installer un système d'exploitation invité échoue et affiche une erreur **Unknown driver 'https'** si vous utilisez une URL https ou ssh, ou la fonction **Download OS**.

Pour contourner ce problème, installez **qemu-kvm-block-curl** et **qemu-kvm-block-ssh** sur l'hôte pour activer la prise en charge des protocoles https et ssh, respectivement. Vous pouvez également utiliser un autre protocole de connexion ou une autre source d'installation.

Bugzilla: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.

Bugzilla:2077767

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.

Bugzilla: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.

Bugzilla:1817965

Le réseau de l'hôte ne peut pas envoyer de ping aux VMs avec VFs pendant la migration en direct

Lors de la migration en direct d'une machine virtuelle (VM) avec une fonction virtuelle (VF) configurée, telle qu'une VM qui utilise le logiciel SR-IOV virtuel, le réseau de la VM n'est pas visible pour les autres périphériques et la VM ne peut pas être atteinte par des commandes telles que **ping**. Cependant, une fois la migration terminée, le problème ne se produit plus.

Bugzilla:1789206

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.

Bugzilla:1969724

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.

Bugzilla:2005173

La VM Windows ne parvient pas à obtenir l'adresse IP après la réinitialisation de l'interface réseau

Il arrive que les machines virtuelles Windows ne parviennent pas à obtenir une adresse IP après une réinitialisation automatique de l'interface réseau. Par conséquent, la machine virtuelle ne parvient pas à se connecter au réseau. Pour résoudre ce problème, désactivez et réactivez le pilote de la carte réseau dans le gestionnaire de périphériques de Windows.

Bugzilla:2084003

Les adaptateurs réseau Broadcom ne fonctionnent pas correctement sur les machines virtuelles Windows après une migration en direct

Actuellement, les adaptateurs réseau de la famille Broadcom, tels que Broadcom, Qlogic ou Marvell, ne peuvent pas être débranchés à chaud pendant la migration en direct des machines virtuelles (VM) Windows. Par conséquent, les adaptateurs ne fonctionnent pas correctement une fois la migration terminée.

Ce problème ne concerne que les adaptateurs connectés à des machines virtuelles Windows utilisant la virtualisation d'E/S à racine unique (SR-IOV).

Bugzilla:2090712, Bugzilla :2091528, Bugzilla:2111319

Les VM Windows Server 2016 cessent parfois de fonctionner après le branchement à chaud d'une vCPU

Actuellement, l'attribution d'une vCPU à une machine virtuelle (VM) en cours d'exécution avec un système d'exploitation invité Windows Server 2016 peut entraîner divers problèmes, tels que l'arrêt inopiné de la VM, l'absence de réponse ou le redémarrage.

Bugzilla:1915715

L'utilisation d'un grand nombre de files d'attente peut entraîner l'échec des machines virtuelles Windows

Les machines virtuelles (VM) Windows peuvent échouer lorsque le périphérique virtuel Trusted Platform Module (vTPM) est activé et que la fonction *multi-queue virtio-net* est configurée pour utiliser plus de 250 files d'attente.

Ce problème est dû à une limitation du dispositif vTPM. Le périphérique vTPM a une limite codée en dur sur le nombre maximum de descripteurs de fichiers ouverts. Étant donné que plusieurs descripteurs de fichiers sont ouverts pour chaque nouvelle file d'attente, la limite interne du vTPM peut être dépassée, ce qui entraîne l'échec de la VM.

Pour contourner ce problème, choisissez l'une des deux options suivantes :

- Gardez le dispositif vTPM activé, mais utilisez moins de 250 files d'attente.
- Désactivez le dispositif vTPM pour qu'il utilise plus de 250 files d'attente.

Bugzilla:2020146

Messages d'erreur redondants sur les machines virtuelles équipées de périphériques NVIDIA passthrough

Lors de l'utilisation d'une machine hôte Intel avec un système d'exploitation RHEL 9.2, les machines virtuelles (VM) avec un périphérique GPU NVDIA transmis enregistrent fréquemment le message d'erreur suivant :

```
Spurious APIC interrupt (vector 0xFF) on CPU#2, should never happen.
```

Cependant, ce message d'erreur n'a pas d'impact sur la fonctionnalité de la VM et peut être ignoré. Pour plus de détails, consultez la base de connaissances de Red Hat .

Bugzilla:2149989

Certains invités Windows ne démarrent pas après une conversion v2v sur des hôtes équipés de processeurs AMD EPYC

Après avoir utilisé l'utilitaire **virt-v2v** pour convertir une machine virtuelle (VM) qui utilise Windows 11 ou Windows Server 2022 comme système d'exploitation invité, la VM ne parvient pas à démarrer. Cela se produit sur les hôtes qui utilisent des processeurs de la série AMD EPYC.

Bugzilla:2168082

Le redémarrage du service OVS sur un hôte peut bloquer la connectivité réseau de ses machines virtuelles en cours d'exécution

Lorsque le service Open vSwitch (OVS) redémarre ou tombe en panne sur un hôte, les machines virtuelles (VM) qui s'exécutent sur cet hôte ne peuvent pas récupérer l'état du dispositif de mise en réseau. Par conséquent, les machines virtuelles peuvent être dans l'incapacité totale de recevoir des paquets.

Ce problème n'affecte que les systèmes qui utilisent le format virtqueue emballé dans leur pile réseau **virtio**.

Pour contourner ce problème, utilisez le paramètre **packed=off** dans la définition du périphérique réseau **virtio** pour désactiver packed virtqueue. Lorsque la fonction packed virtqueue est désactivée, l'état du périphérique réseau peut, dans certaines situations, être récupéré à partir de la mémoire vive.

Bugzilla:1947422

Le pilote du GPU Nvidia cesse de fonctionner après l'arrêt de la VM

Le noyau RHEL a adopté un changement Linux en amont qui aligne les délais de transition de l'alimentation des périphériques plus étroitement sur ceux requis par la spécification PCIe. En conséquence, en raison de la fonction audio du GPU, certains GPU Nvidia peuvent s'arrêter de fonctionner après l'arrêt d'une VM.

Pour contourner le problème, désassignez la fonction audio du GPU de la VM. En outre, en raison des exigences d'isolation DMA pour l'affectation des périphériques (c'est-à-dire le regroupement IOMMU), liez la fonction audio au pilote **vfio-pci**, ce qui permet à la fonction GPU de continuer à être affectée et à fonctionner normalement.

Bugzilla:2178956

nodedev-dumpxml ne liste pas correctement les attributs pour certains dispositifs médiatisés

Actuellement, la commande **nodedev-dumpxml** ne répertorie pas correctement les attributs des dispositifs à médiation qui ont été créés à l'aide de la commande **nodedev-create**. Pour contourner ce problème, utilisez plutôt les commandes **nodedev-define** et **nodedev-start**.

Bugzilla:2143158

La récupération d'une migration de VM post-copie interrompue peut échouer

Si une migration post-copie d'une machine virtuelle (VM) est interrompue puis immédiatement reprise sur le même port entrant, la migration peut échouer avec l'erreur suivante : **Address already in use**

Pour contourner ce problème, attendez au moins 10 secondes avant de reprendre la migration post-copie ou passez à un autre port pour la récupération de la migration.

Bugzilla:2178376

virtiofs il n'est pas possible d'attacher des périphériques après avoir redémarré **virtqemud** ou **libvirtd**

Actuellement, le redémarrage des services **virtqemud** ou **libvirtd** empêche les périphériques de stockage **virtiofs** d'être attachés aux machines virtuelles sur votre hôte.

Bugzilla:2078693

virsh blkiotune --weight ne parvient pas à définir la valeur correcte du contrôleur d'E/S cgroup

Actuellement, l'utilisation de la commande **virsh blkiotune --weight** pour définir le poids de la VM ne fonctionne pas comme prévu. La commande ne parvient pas à définir la valeur **io.bfq.weight** correcte dans le fichier d'interface du contrôleur d'E/S cgroup. Il n'y a pas de solution pour le moment.

Jira:RHELPLAN-83423

Échec du branchement à chaud d'une carte Watchdog sur une machine virtuelle

Actuellement, si aucun emplacement PCI n'est disponible, l'ajout d'une carte Watchdog à une machine virtuelle (VM) en cours d'exécution se solde par l'erreur suivante :

```
Failed to configure watchdog
ERROR Error attempting device hotplug: internal error: No more available PCI slots
```

Pour contourner ce problème, arrêtez la VM avant d'ajouter la carte Watchdog.

Bugzilla:2173584

Le mappage des nœuds NUMA ne fonctionne pas correctement sur les processeurs AMD EPYC

QEMU ne gère pas correctement le mappage des nœuds NUMA sur les processeurs AMD EPYC. Par conséquent, les performances des machines virtuelles (VM) avec ces CPU peuvent être affectées négativement si elles utilisent une configuration de nœuds NUMA. En outre, les machines virtuelles affichent un avertissement similaire au suivant pendant le démarrage.

```
sched: CPU #4's llc-sibling CPU #3 is not on the same node! [node: 1 != 0]. Ignoring dependency.
WARNING: CPU: 4 PID: 0 at arch/x86/kernel/smpboot.c:415 topology_sane.isra.0+0x6b/0x80
```

Pour contourner ce problème, n'utilisez pas de CPU AMD EPYC pour les configurations de nœuds NUMA.

Bugzilla:2176010

Une défaillance de NFS pendant la migration d'une VM entraîne un échec de la migration et un coredump de la VM source

Actuellement, si le service ou le serveur NFS est arrêté pendant la migration de la machine virtuelle (VM), QEMU de la VM source ne peut pas se reconnecter au serveur NFS lorsqu'il redémarre. Par conséquent, la migration échoue et un coredump est lancé sur la VM source. Actuellement, il n'existe pas de solution de contournement.

Bugzilla:2058982

11.18. RHEL DANS LES ENVIRONNEMENTS EN NUAGE

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.

Pour éviter que ce problème ne se produise, procédez comme suit avant de cloner une VM ou de créer un instantané de VM :

1. Décommenter la ligne **use_devicesfile = 0** dans le fichier **/etc/lvm/lvm.conf**
2. Redémarrer la VM

Bugzilla:2059545

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.

Bugzilla:2037657

Les instances RHEL sur Azure ne démarrent pas si elles sont provisionnées par **cloud-init** et configurées avec une entrée de montage NFSv3

Actuellement, le démarrage d'une machine virtuelle RHEL (VM) sur la plateforme cloud Microsoft Azure échoue si la VM a été provisionnée par l'outil **cloud-init** et que le système d'exploitation invité de la VM possède une entrée de montage NFSv3 dans le fichier **/etc/fstab**.

Bugzilla:2081114

La définition d'une IP statique dans une machine virtuelle RHEL sur un hôte VMware ne fonctionne pas

Actuellement, lors de l'utilisation de RHEL en tant que système d'exploitation invité d'une machine virtuelle (VM) sur un hôte VMware, la fonction DatasourceOVF ne fonctionne pas correctement. Par conséquent, si vous utilisez l'utilitaire **cloud-init** pour configurer le réseau de la VM en IP statique et que vous redémarrez ensuite la VM, le réseau de la VM passera en DHCP.

Pour résoudre ce problème, consultez la base de connaissances VNware .

Bugzilla:1750862

11.19. 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
```

Bugzilla:1869561

11.20. CONTENEURS

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

ANNEXE A. LISTE DES TICKETS PAR COMPOSANT

Les tickets Bugzilla et JIRA sont listés dans ce document pour référence. Les liens renvoient aux notes de version de ce document qui décrivent les tickets.

Composant	Billets
389-ds-base	Bugzilla:2096795, Bugzilla:1859271, Bugzilla: 2057070, Bugzilla: 2093981, Bugzilla: 1132524, Bugzilla:2136610, Bugzilla:2142639, Bugzilla :1878808, Bugzilla: 1924569, Bugzilla:1956987, Bugzilla :1952241, Bugzilla :2063140, Bugzilla :2047175, Bugzilla:2053204
Doc-administration-guide	Bugzilla:2075525
NetworkManager	Bugzilla:2134897, Bugzilla: 2081302, Bugzilla: 2019306, Bugzilla :2128809, Bugzilla:2110307, Bugzilla :2117352, Bugzilla :2029636, Bugzilla:2073512, Bugzilla :2128216, Bugzilla:1894877, Bugzilla:2151040
aardvark-dns	Jira:RHELPLAN-138024
anaconda	Bugzilla:2052938, Bugzilla:2158210, Bugzilla: 1991843, Bugzilla :2127100, Bugzilla: 2093793, Bugzilla:2107346, Bugzilla:2050140, Bugzilla:1877697, Bugzilla: 1914955, Bugzilla :1929105, Bugzilla :1997832, Bugzilla :2125542, Bugzilla :2115783, Bugzilla :2164216, Bugzilla:2163497
ansible-collection-microsoft-sql	Bugzilla:2151282, Bugzilla :2151283, Bugzilla :2151284, Bugzilla :2153428, Bugzilla:2163709
ansible-freeipa	Bugzilla:2127913
bacula	Bugzilla:2089395
bind	Bugzilla:1984982
chrony	Bugzilla:2133754
clevis	Bugzilla:2126533, Bugzilla :2159728, Bugzilla:2159735
cloud-init	Bugzilla:1750862
cockpit	Bugzilla:2203361
cockpit-appstream	Bugzilla:2030836
cockpit-machines	Bugzilla:2173584
conntrack-tools	Bugzilla:2132398

Composant	Billets
crash	Bugzilla:2119685
crypto-policies	Bugzilla:2152635
cyrus-sasl	Bugzilla:1995600
device-mapper-multipath	Bugzilla:2033080, Bugzilla:2011699, Bugzilla:1926147
dnf	Bugzilla:2131288, Bugzilla :2121662, Bugzilla:2122626, Bugzilla:2073510
dnf-plugins-core	Bugzilla:2139326
edk2	Bugzilla:1935497
fapolicyd	Jira:RHEL-192, Bugzilla:2054740, Bugzilla:2070655
firefox	Bugzilla:2013247
firewalld	Bugzilla:2125371, Bugzilla:2077512, Bugzilla:2122678
frr	Bugzilla:2129731, Bugzilla:2129743
gcc	Bugzilla:2110583, Bugzilla:2117632, Bugzilla:2141718
gdm	Bugzilla:2131203
gimp	Bugzilla:2047161
git	Bugzilla:2139379
git-lfs	Bugzilla:2139383
glibc	Bugzilla:2129005, Bugzilla:2155352
gnome-shell-extensions	Bugzilla:2154358, Bugzilla:2160553
gnupg2	Bugzilla:2070722, Bugzilla:2073567
gnutls	Bugzilla:2084161, Bugzilla:2042009
golang	Bugzilla:2133019, Bugzilla :2175173, Bugzilla :2111072, Bugzilla:2092016
grafana	Bugzilla:2116847
grafana-pcp	Bugzilla:2116848

Composant	Billets
grub2	Bugzilla:2026579
grubby	Bugzilla:2127453
gssproxy	Bugzilla:2184333
ipa	Bugzilla:2143224, Bugzilla :2162677, Bugzilla: 2084180, Bugzilla :2084166, Bugzilla :2069202, Bugzilla:2094673, Bugzilla:2057471, Bugzilla :21243, Bugzilla:2089907
iproute	Bugzilla:2155604
java-1.8.0-openjdk	Bugzilla:2188023
java-17-openjdk	Bugzilla:2186803, Bugzilla:2186810, Bugzilla:2186806
jmc	Bugzilla:2122401
jmc-core	Bugzilla:1980981
kdump-anaconda-addon	Bugzilla:2017401
kernel	Bugzilla:2153073, Bugzilla:2143850, Bugzilla: 1871126, Bugzilla :1871143, Bugzilla: 2075216, Bugzilla:2100606, Bugzilla:2104468, Bugzilla:2111048, Bugzilla :2150284, Bugzilla :2066372, Bugzilla: 2107347, Bugzilla: 2140899, Bugzilla :2069758, Bugzilla: 1613522, Bugzilla:1874182, Bugzilla:1995338, Bugzilla :1570255, Bugzilla :2023416, Bugzilla:2021672, Bugzilla :2027304, Bugzilla :1660337, Bugzilla: 1955275, Bugzilla:2142102, Bugzilla: 2041690, Bugzilla :2040643, Bugzilla:2167783, Bugzilla :2000616, Bugzilla :2013650, Bugzilla:2132480, Bugzilla :2059545, Bugzilla :1960467, Bugzilla:2005173, Bugzilla :2128610, Bugzilla:2129288, Bugzilla:2013884, Bugzilla:2149989, Bugzilla:2168603, Bugzilla: 2173947, Bugzilla:2178956, Bugzilla:2180665
kexec-tools	Bugzilla:2085347, Bugzilla: 2076416, Bugzilla :2160676, Bugzilla: 2080110, Bugzilla :2139000, Bugzilla:2113873, Bugzilla :2064708, Bugzilla:2065013
keylime	Bugzilla:2150830, Bugzilla :2138167, Bugzilla:2140670, Bugzilla:2142009
kmod	Bugzilla:2103605
krb5	Bugzilla:2068535, Bugzilla: 2106043, Bugzilla: 2060798, Bugzilla:2077450, Bugzilla: 2106296, Bugzilla:2060421, Bugzilla :2016312, Bugzilla:2103327
libdnf	Bugzilla:2124480

Composant	Billets
libnvme	Bugzilla:2139752
libotr	Bugzilla:2086562
libreswan	Bugzilla:2128669
libsepol	Bugzilla:2145224
libssh	Bugzilla:2026449, Bugzilla:2068475
libvirt	Bugzilla:2014487, Bugzilla:2143158, Bugzilla:2078693
libxcrypt	Bugzilla:2034569
llvm-toolset	Bugzilla:2118567
lvm2	Bugzilla:1878893, Bugzilla:2038183
mod_security	Bugzilla:2143211
mysql	Bugzilla:1991500
nfs-utils	Bugzilla:2143747, Bugzilla:2081114
nginx	Bugzilla:2096174
nmstate	Bugzilla:2095207, Bugzilla: 2120473, Bugzilla :2044150, Bugzilla:2058292, Bugzilla :2130240, Bugzilla:2162401
nodejs	Bugzilla:2178088
nss	Bugzilla:2091905
nvme-cli	Bugzilla:2139753
nvme-stas	Bugzilla:1893841
open-vm-tools	Bugzilla:2037657
openblas	Bugzilla:2112099, Bugzilla:2115737
opencryptoki	Bugzilla:2110314
openscap	Bugzilla:2159286, Bugzilla:2161499

Composant	Billets
openssh	Bugzilla:2056884
openssl	Bugzilla:2129063, Bugzilla :2060044, Bugzilla :1975836, Bugzilla :2168665, Bugzilla:1681178, Bugzilla:1685470
openssl-ibmca	Bugzilla:2110378
osbuild-composer	Bugzilla:2173928
oscap-anaconda-addon	Bugzilla:2165920, Bugzilla:2172264
pacemaker	Bugzilla:2133546, Bugzilla:2125344, Bugzilla:2125337
pam	Bugzilla:2126640
passt	Bugzilla:2131015
pause-container	Bugzilla:2106816
pcp	Bugzilla:2117074
pcs	Bugzilla:2116295, Bugzilla :2112270, Bugzilla :1620043, Bugzilla:1796827, Bugzilla:2092950
pki-core	Bugzilla:1849834, Bugzilla:1883477
podman	Jira:RHELPLAN-136602, Jira:RHELPLAN-136607, Bugzilla:2119200, Jira:RHELPLAN-136611, Bugzilla:2069279
postgresql	Bugzilla:2128410
powerpc-utils	Bugzilla:2125152
powertop	Bugzilla:2044132
python-blivet	Bugzilla:2103800
python-sqlalchemy	Bugzilla:2152649
python3.11	Bugzilla:2127923
python3.11-lxml	Bugzilla:2157708

Composant	Billets
qemu-kvm	Bugzilla:2116496, Bugzilla:1965079, Bugzilla:1951814, Bugzilla: 2060839, Bugzilla: 2014229, Bugzilla:2052424, Bugzilla:1817965, Bugzilla:1789206, Bugzilla: 2090712, Bugzilla:1915715, Bugzilla :2020146, Bugzilla: 1947422, Bugzilla :2178376, Bugzilla:2176010, Bugzilla:2058982
realtime-tests	Bugzilla:2041637
rear	Bugzilla:2172589, Bugzilla:2160748
restore	Bugzilla:1997366
rhel-system-roles	Bugzilla:2131293, Bugzilla:2133858, Bugzilla: 2078999, Bugzilla:2119102, Bugzilla :2128843, Bugzilla:2130010, Bugzilla :2130329, Bugzilla:2130344, Bugzilla :2130357, Bugzilla:2133528, Bugzilla:2133930, Bugzilla: 2134202, Bugzilla :2137663, Bugzilla:2140795, Bugzilla :2141330, Bugzilla:2143768, Bugzilla :2165175, Bugzilla:2140804, Bugzilla: 2126959, Bugzilla:2143816, Bugzilla :2153030, Bugzilla :2153043, Bugzilla :2162782, Bugzilla:2167528, Bugzilla :2168735, Bugzilla: 2160152, Bugzilla: 1999770, Bugzilla:2123859, Bugzilla :2187539, Bugzilla:2186218
rpm	Bugzilla:2150804, Bugzilla:2111251, Bugzilla:2144005
rsyslog	Bugzilla:2124849, Bugzilla :2127404, Bugzilla :2124488, Bugzilla:2157659
rteval	Bugzilla:2081325
rust	Bugzilla:2123900
s390utils	Bugzilla:2044204, Bugzilla:1932480
samba	Bugzilla:2131993
scap-security-guide	Bugzilla:2158405, Bugzilla :2122325, Bugzilla :2169414, Bugzilla :2105162, Bugzilla:2120978, Bugzilla:2038978
selinux-policy	Bugzilla:2151841, Bugzilla:1972222, Bugzilla:2064274
sos	Bugzilla:2164987, Bugzilla:2134906, Bugzilla:1869561
sssd	Bugzilla:1507035, Bugzilla :1766490, Bugzilla :2065693, Bugzilla:2056482, Bugzilla:1608496
stratisd	Bugzilla:2039957, Bugzilla :2039955, Bugzilla:2041558
subscription-manager	Bugzilla:2108549, Bugzilla:2163716, Bugzilla:2136694

Composant	Billets
swig	Bugzilla:2139101
synce4l	Bugzilla:2143264
systemd	Bugzilla:2018112
systemtap	Bugzilla:2083727
tang	Bugzilla:2095474, Bugzilla:2188743
tigervnc	Bugzilla:2060308
tomcat	Bugzilla:2160511
toolbox	Bugzilla:2163752
tuna	Bugzilla:2122781, Bugzilla:2121517, Bugzilla:2062865
tuned	Bugzilla:2133815, Bugzilla:2113900
tzdata	Bugzilla:2157982
udisks2	Bugzilla:1983602
unbound	Bugzilla:2070495
usbguard	Bugzilla:2155910, Bugzilla:2042345, Bugzilla:2097419
virt-v2v	Bugzilla:2168082
virtio-win	Bugzilla:1969724, Bugzilla:2084003
vsftpd	Bugzilla:2018284
wsmancli	Bugzilla:2127416
xdp-tools	Bugzilla:2160066

Composant	Billets
autres	Bugzilla:2177782, Jira: RHELPLAN-137505, Jira:RHELPLAN-139125, Bugzilla:2046653, Jira:RHELPLAN-133650, Jira:RHELPLAN-139430, Jira:RHELPLAN-137416, Jira:RHELPLAN-137411, Jira:RHELPLAN-137406, Jira :RHELPLAN-137403, Jira: RHELPLAN-159146, Jira :RHELPLAN-139448, Jira:RHELPLAN-151481, Jira:RHELPLAN-150266, Jira:RHELPLAN-147982, Jira:RHELPLAN-147428, Jira:RHELPLAN-139659, Jira :RHELPLAN-149091, Jira: RHELPLAN-139655, Jira:RHELPLAN-139424, Jira:RHELPLAN-136489, Jira:RHELPLAN-59528, Bugzilla:2209419, Bugzilla:2190123, Jira:RHELPLAN-135600, Jira :RHELPLAN-148303, Bugzilla: 2020529, Bugzilla:2030412, Jira:RHELPLAN-103993, Jira:RHELPLAN-122345, Jira :RHELPLAN-27394, Jira:RHELPLAN-27737, Jira:RHELPLAN-148394, Bugzilla:1927780, Jira :RHELPLAN-110763, Bugzilla:1935544, Bugzilla:2089200, Jira:RHELPLAN-15509, Jira:RHELPLAN-99136, Jira:RHELPLAN-103232, Bugzilla:1899167, Bugzilla:1979521, Jira:RHELPLAN-100087, Jira :RHELPLAN-100639, Bugzilla:2058153, Jira :RHELPLAN-113995, Jira:RHELPLAN-983, Jira:RHELPLAN-131882, Jira :RHELPLAN-137660, Jira:RHELPLAN-139805, Jira:RHELPLAN-147725, Jira:RHELPLAN-153267, Jira :RHELPLAN-157225, Jira:RHELPLAN-157337, Bugzilla:1640697, Bugzilla: 1697896, Bugzilla:2047713, Jira:RHELPLAN-96940, Jira:RHELPLAN-117234, Jira:RHELPLAN-119001, Jira:RHELPLAN-119852, Bugzilla :2077767, Bugzilla:2053598, Bugzilla:2082303, Jira :RHELPLAN-121049, Jira: RHELPLAN-157939, Jira:RHELPLAN-109613, Bugzilla:2160619, Bugzilla: 2173992, Bugzilla:2185048, Jira:RHELPLAN-83423

ANNEXE B. HISTORIQUE DES RÉVISIONS

0.0.1

10 mai 2023, Gabriela Fialová(gfialova@redhat.com)

- Publication des notes de mise à jour de Red Hat Enterprise Linux 9.2.

0.0.0

29 mars 2023, Gabriela Fialová(gfialova@redhat.com)

- Publication des notes de mise à jour de Red Hat Enterprise Linux 9.2 Beta.