



# **Red Hat Enterprise Linux 7 Notes de version 7.2**

---

Notes de version de Red Hat Enterprise Linux 7.2

Red Hat Customer Content  
Services



Red Hat Enterprise Linux 7 Notes de version 7.2

---

Notes de version de Red Hat Enterprise Linux 7.2

Red Hat Customer Content Services

## Notice légale

Copyright © 2015 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Résumé

Les notes de version couvrent les améliorations et des additions implémentées sur Red Hat Enterprise Linux 7.2 et documentent les problèmes connus de cette version. Pour obtenir une documentation détaillée de toutes les modifications apportées à Red Hat Enterprise Linux lors de la mise à jour 7.2, veuillez consulter les Notes techniques.

## Table des matières

<b>Préface</b> .....	<b>6</b>
<b>Chapitre 1. Architectures</b> .....	<b>7</b>
<b>Partie I. Nouvelles fonctionnalités</b> .....	<b>8</b>
<b>Chapitre 2. Authentification</b> .....	<b>9</b>
ca-certificate rebasé sur la version 2.4	9
Prise en charge des confiances à sens unique	9
openldap rebasé sur la version 2.4.40	9
Authentification du cache sur SSSD	9
SSSD autorise le mappage d'UID et de GID sur des clients individuels	9
SSSD peut désormais refuser l'accès SSH aux comptes verrouillés	9
L'utilitaire sudo est désormais capable de vérifier le checksum des commandes	10
Prise en charge smart card SSSD	10
Prise en charge de multiples profils de certificats	10
Password Vault	10
Prise en charge DNSSEC sur Identity Management	10
Proxy HTTPS Kerberos dans Identity Management	11
Réactualisation en arrière-plan des entrées mises en cache	11
Mise en cache des opérations initgroups	11
Négociation d'authentification rationalisée avec mod_auth_gssapi	11
Capacités de gestion de cycle de vie d'utilisateur	11
Prise en charge SCEP sur certmonger	11
Nouveaux paquets : ippsilon	12
NSS augmente les valeurs minimum acceptées de la puissance des clés	12
nss et nss-util rebasés à la version 3.19.1	12
Prise en charge complète des modules Apache pour IdM	12
<b>Chapitre 3. Clustering</b> .....	<b>13</b>
systemd et pacemaker sont désormais coordonnés correctement pendant les fermetures système	13
Les commandes pcs resource move et pcs resource ban affichent désormais un message d'avertissement pour clarifier le comportement des commandes	13
Nouvelle commande pour déplacer une ressource Pacemaker sur son nœud préféré	13
Prise en charge de la commande clufter pour transformer et analyser les formats de configuration de clusters	13
<b>Chapitre 4. Compilateur et outils</b> .....	<b>14</b>
tail --follow fonctionne désormais correctement sur les fichiers sur VXFS (« Veritas Clustered File System »)	14
La commande dd est maintenant capable d'afficher la progression des transferts	14
Temps d'attente amélioré sur libcurl	14
La bibliothèque libcurl implémente désormais une poignée de mains SSL non bloquante	14
GDB sur systèmes IBM Power Systems n'échoue plus lors de l'accession à la table des symboles	14
nscd mis à jour pour recharger les données de configuration automatiquement	14
La fonction bibliothèque dlopen ne tombe plus en panne lors des appels récursifs	15
L'outil opperf reconnaît désormais les identifiants huge page statiques	15
La commande rsync -X fonctionne désormais correctement	15
Les exécutable Subversion sont maintenant créés avec des données RELRO complètes	15
L'extension de fils d'exécution dans TCL fonctionne désormais correctement	15
<b>Chapitre 5. Bureau</b> .....	<b>16</b>
GNOME 3.14	16
Désormais, le paquet ibus-gtk2 met à jour le fichier immodules.cache	16

<b>Chapitre 6. Systèmes de fichiers</b> .....	<b>18</b>
gfs2-utils rebasé sur la version 3.1.8	18
GFS2 empêche désormais les utilisateurs de dépasser leurs quotas	18
XFS rebasé sur la version 4.1	18
Mises à niveau d'ext4 et jbd2	18
cifs rebasé sur la version 3.17	18
<b>Chapitre 7. Mises à jour générales</b> .....	<b>19</b>
Désormais lftp gère la redirection 302 correctement	19
Davantage d'informations de diagnostic et un greffon renommé pour sosreport	19
<b>Chapitre 8. Installation et démarrage</b> .....	<b>20</b>
Installation réseau corrigée dans initrd si la configuration réseau est fournie dans Kickstart	20
Anaconda prend désormais en charge la création de volumes logiques dans le cache	20
Amélioration du tri du menu de démarrage GRUB2	20
Désormais, Anaconda restaure correctement les actions de disque lorsqu'il se produit des changements de sélection de disque	20
Amélioration de la détection des noms de disques device-mapper	20
Gestion de PReP Boot pendant le partitionnement corrigée	20
Partitions EFI sur périphériques RAID1	21
L'installation en mode texte ne tombe plus en panne pendant la configuration réseau	21
Les écrans du mode de secours sur IBM System z ne sont plus coupés	21
Module complémentaire OpenSCAP dans Anaconda	21
Anaconda n'expire plus lorsqu'il attend un fichier Kickstart sur un CD ou DVD	22
<b>Chapitre 9. Noyau</b> .....	<b>23</b>
Les paramètres de noyau SHMMAX et SHMALL retrouvent leurs valeurs par défaut	23
Les « Transparent huge pages » ne causent plus de corruption de mémoire	23
Rebasement SCSI LIO	23
makedumpfile prend désormais en charge le nouveau format sadump représentant jusqu'à 16 To de mémoire physique	23
Supprimer ou mettre à niveau le noyau n'affichera plus d'avertissement	23
Nouveau paquet : libevdev	23
Tuned peut désormais être exécuté en mode no-daemon	23
Nouveau paquet : tuned-profiles-realtime	24
Planification d'E/S à multiples files d'attente (« Multiqueue I/O scheduling ») avec blk-mq	24
Les messages d'erreur SCSI peuvent désormais être interprétés confortablement	24
Mise à jour du sous-système et des pilotes libATA	25
FCoE et DCB ont été mis à niveau	25
perf rebasé sur la version 4.1	25
Prise en charge de TPM 2.0	25
Désormais, Turbostat fournit une sortie correcte	25
Prise en charge du processeur Intel Xeon v5	25
l'outil zswap utilise l'API zpool	25
La longueur du fichier /proc/pid/cmdline est désormais illimitée	25
La prise en charge de dma_rmb et dma_wmb est désormais offerte	26
<b>Chapitre 10. Mise en réseau</b> .....	<b>27</b>
Désormais, SNMP obéit correctement à la directive clientaddr sur IPv6	27
tcpdump prend en charge les options -J, -j, et --time-stamp-precision	27
Mise à niveau TCP/IP	27
<b>Chapitre 11. Serveurs et services</b> .....	<b>28</b>
La directive ErrorPolicy est désormais validée	28
Désormais, CUPS désactive le chiffrement SSLv3 par défaut	28

-----	----
Cups autorise désormais le trait de soulignement dans les noms d'imprimante	28
Dépendance inutile supprimée du paquet tftp-server	28
Le fichier déconseillé /etc/sysconfig/conman a été supprimé	28
<b>Chapitre 12. Stockage</b>	<b>29</b>
Nouvelles options delay_watch_checks et delay_wait_checks dans le fichier multipath.conf	29
Nouvelle option config_dir dans le fichier multipath.conf	29
Mise à niveau DM	29
Nouvelle commande dmstats pour afficher et gérer des statistiques d'E/S pour des régions de périphériques, définies par utilisateurs, qui utilisent le pilote device-mapper	29
Prise en charge DIX sur matériel spécifié	29
Cache LVM	30
Nouvelle politique du cache LVM/DM	30
ID système de LVM	31
<b>Chapitre 13. Gestion du système et des abonnements</b>	<b>32</b>
Désormais, PowerTOP respecte les noms de fichier des rapports définis par les utilisateurs	32
Commandes yum-config-manager modifiées	32
Nouveau greffon search-disabled-repos pour yum	32
<b>Chapitre 14. Virtualisation</b>	<b>33</b>
Des bus PCI supplémentaires sont désormais pris en charge en utilisant les périphériques de pont PCI expande	33
qemu-kvm prend en charge les événements de trace de fermeture de machine virtuelle (« virtual machine shutdown trace events »)	33
Intel MPX exposé à l'invité	33
Extraction du vidage de mémoire de l'invité à partir du cœur qemu-kvm	33
Prise en charge complète de virt-v2v	33
Virtualisation sur IBM Power Systems	33
Prise en charge VirtIO-1	33
Prise en charge Hyper-V TRIM	34
<b>Chapitre 15. Red Hat Software Collections</b>	<b>35</b>
<b>Partie II. Aperçus technologiques</b>	<b>36</b>
<b>Chapitre 16. Authentification</b>	<b>37</b>
Utilisation des fournisseurs sudo AD et LDAP	37
<b>Chapitre 17. Systèmes de fichiers</b>	<b>38</b>
OverlayFS	38
Prise en charge des clients NFSv4 avec structure de fichier flexible	38
NFS sur RDMA	38
Système de fichier Btrfs	39
<b>Chapitre 18. Activation du matériel</b>	<b>40</b>
Prise en charge des cartes OSA-Express5s sur qethqoat	40
Instrumentation du runtime pour IBM System z	40
Adaptateurs HA-DAS LSI Syncro CS	40
<b>Chapitre 19. Noyau</b>	<b>41</b>
Prise en charge de multiples CPU dans kdump sur systèmes AMD64 et Intel 64	41
L'outil criu	41
Espace de noms de l'utilisateur	41
Chien de garde LPAR pour IBM System z	41
Mises à jour dynamiques du noyau avec kpatch	41

i40evf gère les réinitialisations de grande envergure	41
<b>Chapitre 20. Mise en réseau</b>	<b>43</b>
Mise à jour du pilote de l'adaptateur de serveur ethernet Intel X710/XL710	43
Sortie ethtool précise	43
Pilote Cisco usNIC	43
Pilote du noyau Cisco VIC	43
Trusted Network Connect	43
Fonctionnalité SR-IOV dans le pilote qlcnic	43
<b>Chapitre 21. Stockage</b>	<b>44</b>
Planification d'E/S à files multiples pour SCSI	44
Amélioration de l'infrastructure de verrouillage LVM	44
Greffon Targetd de l'API libStorageMgmt	44
DIF/DIX	44
Cible dm-era device-mapper	44
<b>Chapitre 22. Virtualisation</b>	<b>45</b>
Virtualisation imbriquée	45
L'outil virt-p2v	45
Prise en charge d'USB 3.0 pour les invités KVM	45
<b>Partie III. Pilotes de périphériques</b>	<b>46</b>
<b>Chapitre 23. Mise à jour des pilotes de stockage</b>	<b>47</b>
<b>Chapitre 24. Mise à jour des pilotes réseau</b>	<b>48</b>
<b>Chapitre 25. Mises à jour des pilotes graphiques et de pilotes divers</b>	<b>49</b>
<b>Partie IV. Problèmes connus</b>	<b>50</b>
<b>Chapitre 26. Compilateur et outils</b>	<b>51</b>
Multiple bogues pendant les démarrages à partir de SAN sur FCoE	51
Valgrind ne peut pas exécuter de programmes créés sur une version antérieure d'Open MPI	51
<b>Chapitre 27. Bureau</b>	<b>52</b>
Des dépendances manquantes du paquet pygobject3 empêchent la mise à niveau de Red Hat Enterprise Linux 7.1	52
<b>Chapitre 28. Mises à jour générales</b>	<b>53</b>
Les noms des nouveaux périphériques assignés peuvent perturber les connexions réseau	53
<b>Chapitre 29. Installation et démarrage</b>	<b>54</b>
L'installation en mode texte ne tombe plus en panne pendant la configuration réseau	54
Possible message d'erreur de NetworkManager pendant l'installation	54
L'installation Atomic Host offre cryptsetup même s'il n'est pas disponible	54
L'installateur peut uniquement ajouter un stockage avancé la première fois que le rayon du stockage est saisi	54
<b>Chapitre 30. Noyau</b>	<b>55</b>
Certains systèmes de fichiers ext4 ne peuvent pas être redimensionnés	55
Perte de connexion répétée avec des cibles iSCSI activées iSER	55
Commande d'E/S d'appels mid-layer SCSI jusqu'à ce que la fermeture forcée du système	55
Le certificat de la clé publique Red Hat Beta doit être chargé manuellement	55
<b>Chapitre 31. Mise en réseau</b>	<b>56</b>
La politique de délai d'expiration n'est pas activée sur le noyau Red Hat Enterprise Linux 7.2	56



---

<b>Chapitre 32. Gestion du système et des abonnements</b> .....	<b>57</b>
Enregistrement incomplet en cas d'erreur	57
Le bouton Précédent (« Back ») du module complémentaire « Subscription Manager » de « Initial Setup » ne fonctionne pas	57
<b>Chapitre 33. Virtualisation</b> .....	<b>58</b>
Parcourir GRUB 2 avec KVM est problématique	58
Le redimensionnement de disques GPT (« GUID Partition Table ») sur invités Hyper-V provoque des erreurs de table de partition	58
<b>Annexe A. Versions des composants</b> .....	<b>59</b>
<b>Annexe B. Historique des versions</b> .....	<b>60</b>

## Préface

Les mises à jour mineures de Red Hat Enterprise Linux comprennent des améliorations individuelles, des améliorations de la sécurité, ainsi que des correctifs de bogues. Les *Notes de version Red Hat Enterprise Linux 7.2* documentent les changements majeurs apportés au système d'exploitation Red Hat Enterprise Linux 7 et les applications qui accompagnent cette version mineure, ainsi que les problèmes connus et une liste complète de tous les aperçus technologiques actuellement disponibles.

Les capacités et limites de Red Hat Enterprise Linux 7 par rapport aux autres versions du système sont disponibles dans l'article de la base de connaissances disponible sur <https://access.redhat.com/articles/rhel-limits>.

Pour obtenir des informations concernant le cycle de vie de Red Hat Enterprise Linux, veuillez consulter <https://access.redhat.com/support/policy/updates/errata/>.

## Chapitre 1. Architectures

Red Hat Enterprise Linux 7.2 est disponible en tant qu'ensemble unique sur les architectures suivantes : [1]

- ✦ AMD 64 bits
- ✦ Intel 64 bits
- ✦ IBM POWER7+ et POWER8 (big endian)
- ✦ IBM POWER8 (little endian) [2]
- ✦ IBM System z [3]

Dans cette version, Red Hat offre des améliorations pour les serveurs et les systèmes, ainsi qu'une amélioration de l'expérience du logiciel libre de Red Hat dans son ensemble.

---

[1] Remarquez que l'installation Red Hat Enterprise Linux 7.2 est uniquement prise en charge sur le matériel 64 bits. Red Hat Enterprise Linux 7.2 est capable d'exécuter des systèmes d'exploitation 32 bits, y compris des anciennes versions de Red Hat Enterprise Linux, en tant que machines virtuelles.

[2] Actuellement, Red Hat Enterprise Linux 7.2 (little endian) est uniquement pris en charge en tant qu'invité KVM sous les hyperviseurs **Red Hat Enterprise Virtualization for Power** et **PowerVM**.

[3] Remarquez que Red Hat Enterprise Linux 7.2 prend en charge le matériel IBM zEnterprise 196 ou ses versions plus récentes ; les systèmes mainframe IBM System z10 ne sont plus pris en charge et ne démarreront pas Red Hat Enterprise Linux 7.2.

## **Partie I. Nouvelles fonctionnalités**

Cette partie décrit les nouvelles fonctionnalités et améliorations majeures présentées dans Red Hat Enterprise Linux 7.2.

## Chapitre 2. Authentification

### ca-certificate rebasé sur la version 2.4

Le paquet `ca-certificate` a été mis à niveau à la version en amont 2.4, qui fournit un certain nombre de correctifs de bogues et d'améliorations par rapport à la version précédente. Plus particulièrement, `ca-certificate` contient désormais les modifications suivantes :

Mozilla a précédemment supprimé sa confiance de plusieurs certificats CA hérités contenant des clés RSA 1024 bits. Cette version du paquet `ca-certificate` modifie la liste Mozilla de manière à continuer à faire confiance à ces certificats CA hérités par défaut. Ces modifications ont été effectuées pour s'assurer de la compatibilité avec des déploiements PKI existants et avec des logiciels basés sur OpenSSL ou GnuTLS.

Le paquet `ca-certificate` inclut désormais la commande **ca-legacy**, qui peut être utilisée pour désactiver les modifications de compatibilité mentionnées. Veuillez consulter la page de manuel `ca-legacy(8)` pour obtenir davantage d'informations sur la manière d'utiliser la commande.

Il est également recommandé aux utilisateurs qui souhaitent désactiver les modifications héritées de se référer à l'article de la base des connaissances 1413643, qui fournit des détails sur ces modifications et les conséquences potentielles de leur désactivation.

Remarquez que l'utilisation du stockage CA unifié est requise pour être en mesure d'utiliser la commande **ca-legacy**. Veuillez consulter la page de manuel `update-ca-trust(8)` pour apprendre comment activer le stockage CA unifié.

### Prise en charge des confiances à sens unique

Identity Management autorise désormais l'utilisateur à configurer une confiance à sens unique en exécutant la commande `ipa trust-add`.

### openldap rebasé sur la version 2.4.40

Les paquets `openldap` ont été mis à niveau à la version en amont 2.4.40, qui fournit un certain nombre de correctifs de bogues ainsi qu'une amélioration par rapport à la version précédente. Plus particulièrement, des règles de correspondance ORDERING ont été ajoutées aux descriptions de type d'attribut **ppolicy**. Parmi les bogues corrigés figure : Le serveur ne se termine plus de manière inattendue lors du traitement des archives SRV, et des informations **objectClass** manquantes ont été ajoutées, celles-ci autorisent l'utilisateur à modifier la configuration frontale par le biais de moyens standards.

### Authentification du cache sur SSSD

L'authentification du cache sans tentative de reconnexion est désormais disponible sur SSSD même en mode en ligne. Une authentification directe sur le serveur réseau de manière répétitive pourrait causer une latence d'application excessive, qui pourrait rendre le processus assez long.

### SSSD autorise le mappage d'UID et de GID sur des clients individuels

Il est désormais possible de mapper des utilisateurs avec un UID et un GID différent sur des clients Red Hat Enterprise Linux spécifiques à travers une configuration du côté client en utilisant SSSD. Cette possibilité d'outrepasser le côté client peut résoudre des problèmes causés par les duplications d'UID et de GID.

### SSSD peut désormais refuser l'accès SSH aux comptes verrouillés

Auparavant, lorsque SSSD utilisait OpenLDAP comme base de données d'authentification, les utilisateurs

pouvaient s'authentifier sur le système avec succès en utilisant une clé SSH même après le verrouillage du compte utilisateur. Le paramètre `ldap_access_order` accepte désormais la valeur `ppolicy`, qui peut refuser l'accès SSH à un utilisateur se trouvant dans la situation décrite. Pour obtenir davantage d'informations sur l'utilisation de `ppolicy`, veuillez consulter la description `ldap_access_order` sur la page de manuel `sssd-ldap(5)`.

## L'utilitaire sudo est désormais capable de vérifier le checksum des commandes

La configuration de l'utilitaire sudo peut désormais stocker le checksum d'une commande ou d'un script autorisé. Lorsque la commande ou le script est exécuté à nouveau, le checksum est comparé au checksum stocké pour vérifier si quelque chose a changé. Si la commande ou le binaire a été modifié, l'utilitaire sudo refusera d'exécuter la commande ou journalisera un avertissement. Cette fonctionnalité permet de déléguer les responsabilités et les activités de résolution de problèmes correctement dans le cas où un incident se produirait.

## Prise en charge smart card SSSD

Désormais, SSSD prend en charge les smart cards pour une authentification locale. Avec cette fonctionnalité, l'utilisateur peut utiliser une smart card pour journaliser sur le système à l'aide d'une console basée texte ou graphique, ainsi qu'en utilisant des services locaux, comme le service sudo. L'utilisateur place la smart card dans le lecteur et fournit le nom d'utilisateur et le code PIN de la smart card à l'invite de connexion. Si le certificat de la smart card est vérifié, l'utilisateur est alors authentifié avec succès.

Remarquez qu'actuellement, SSSD n'autorise pas à l'utilisateur d'acquiescer un ticket Kerberos en utilisant une smart card. Pour obtenir un ticket Kerberos, l'utilisateur doit s'authentifier en utilisant l'utilitaire kinit.

## Prise en charge de multiples profils de certificats

Désormais, Identity Management prend en charge les profils multiples pour délivrer des certificats de serveur et autres, au lieu de ne prendre en charge qu'un profil de certificat à serveur unique. Les profils sont stockés dans le système Certificate.

## Password Vault

Une nouvelle fonctionnalité autorisant le stockage central sécurisé des informations privées d'utilisateur, comme les mots de passe et les clés, a été ajoutée à Identity Management. Password Vault est créé au-dessus du sous-système KRA (« Key Recovery Authority ») de PKI (« Public Key Infrastructure »).

## Prise en charge DNSSEC sur Identity Management

Les serveurs Identity Management avec DNS intégré prennent désormais en charge DNSSEC (« DNS Security Extensions »), qui est un ensemble d'extensions de DNS améliorant la sécurité du protocole DNS. Des zones DNS hébergées sur serveurs Identity Management peuvent être automatiquement signées en utilisant DNSSEC. Les clés de chiffrement sont automatiquement générées et pivotées.

Il est recommandé aux utilisateurs qui décident de sécuriser leurs zones DNS avec DNSSEC de lire et suivre ces documents :

DNSSEC Operational Practices, Version 2 : <http://tools.ietf.org/html/rfc6781#section-2>

Secure Domain Name System (DNS) Deployment Guide : <http://dx.doi.org/10.6028/NIST.SP.800-81-2>

Remarquez que les serveurs Identity Management servers avec DNS intégré utilisent DNSSEC pour valider les réponses DNS obtenues des autres serveurs DNS. Ceci peut affecter la disponibilité des zones DNS qui ne sont pas configurées conformément aux pratiques de dénomination recommandées décrites dans le Guide de mise en réseau Red Hat Enterprise Linux : [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/7/html/Networking\\_Guide/ch-Configure\\_Host\\_Names.html#sec-Recommended\\_Naming\\_Practices](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices)

## Proxy HTTPS Kerberos dans Identity Management

Une fonction proxy KDC (« Key Distribution Center »), interopérable avec l'implémentation MS-KKDCP (« Microsoft Kerberos KDC Proxy Protocol »), est désormais disponible sur Identity Management et autorise aux clients d'accéder aux services KDC et **kpasswd** en utilisant HTTPS. Les administrateurs système peuvent désormais exposer le proxy sur le bord de leur réseau en implémentant un simple proxy HTTPS inversé sans avoir besoin de paramétrer et gérer une application dédiée.

## Réactualisation en arrière-plan des entrées mises en cache

Désormais, SSSD autorise aux entrées du cache d'être mises à jour hors-bande en arrière-plan. Avant cette mise à jour, lorsque la validité des entrées mises en cache expirait, SSSD les récupérait du serveur distant et les stockait à nouveau dans la base de données, ce qui prenait assez longtemps. Avec cette mise à jour, les entrées sont retournées instantanément car le serveur principal les conserve à jour à tout moment. Remarquez que ceci cause une charge plus importante sur le serveur car SSSD télécharge les entrées de manière périodique plutôt qu'à la demande.

## Mise en cache des opérations **initgroups**

Le cache mémoire rapide SSSD prend désormais en charge les opérations **initgroups**, qui améliore la vitesse de traitement des **initgroups** et augmente les performances de certaines applications, par exemple GlusterFS et **slapi-nis**.

## Négociation d'authentification rationalisée avec **mod\_auth\_gssapi**

Identity Management utilise désormais le module **mod\_auth\_gssapi**, qui utilise les appels GSSAPI au lieu des appels Kerberos directs utilisés par l'ancien module **mod\_auth\_kerb** utilisé.

## Capacités de gestion de cycle de vie d'utilisateur

La gestion des cycles de vie des utilisateurs donne à l'administrateur un plus grand degré de contrôle sur l'activation et la désactivation des comptes utilisateurs. L'administrateur peut désormais provisionner des nouveaux comptes utilisateurs en les ajoutant à une zone de production sans les activer totalement, il peut activer des comptes utilisateurs désactivés pour les rendre totalement opérationnels, ou désactiver les comptes utilisateurs sans totalement les supprimer de la base de données.

Les capacités de gestion de cycle de vie des utilisateurs apportent d'importants bénéfices à des déploiements IdM de grande taille. Remarquez que des utilisateurs peuvent également être ajoutés à la zone de production directement depuis un client LDAP standard, en utilisant des opérations LDAP directes. Précédemment, IdM prenait uniquement en charge la gestion des utilisateurs utilisant des outils de ligne de commande IdM ou l'interface utilisateur web IdM.

## Prise en charge SCEP sur **certmonger**

Le service **certmonger** a été mis à jour pour prendre en charge le protocole SCEP (« Simple Certificate Enrollment Protocol »). Il est désormais possible de délivrer un nouveau certificat et de renouveler ou remplacer des certificats existants via SCEP.

## Nouveaux paquets : **epsilon**

Les paquets *epsilon* offrent le service de fournisseur d'identité pour les SSO (« Single sign-on ») fédérés. *epsilon* lie les fournisseurs d'authentification et les applications ou utilitaires pour qu'ils autorisent SSO. Cela inclut un serveur et des utilitaires pour configurer les fournisseurs de service basés Apache.

L'authentification utilisateur pour le SSO fourni par *Ipsilon* est effectuée avec un système de gestion des identités séparé, comme un serveur Identity Management. *Ipsilon* communique avec diverses applications et utilitaires à travers des protocoles de fédération, tels que SAML ou OpenID.

## NSS augmente les valeurs minimum acceptées de la puissance des clés

La bibliothèque NSS (« Network Security Services ») sur Red Hat Enterprise Linux 7.2 n'accepte plus les paramètres d'échange de clés DH (« Diffie-Hellman ») de moins de 768 bits, ni les certificats RSA et DSA avec des tailles de clé de moins de 1023 bits. Le renforcement de la valeur minimum acceptée des clés permet d'empêcher les attaques exploitant les vulnérabilités de sécurité connues, telles que Logjam (CVE-2015-4000) et FREAK (CVE-2015-0204).

Remarquez désormais que les tentatives de connexion à un serveur en utilisant des clés plus faibles que les nouvelles valeurs minimums échoueront, même si de telles connexions ont fonctionné dans les versions précédentes de Red Hat Enterprise Linux.

## nss et nss-util rebasés à la version 3.19.1

Les paquets *nss* et *nss-util* ont été mis à niveau à la version en amont 3.19.1, qui offre un certain nombre de correctifs de bogues et améliorations comparé à la version précédente. Plus particulièrement, la mise à jour permet aux utilisateurs de mettre à niveau à la version Mozilla Firefox 38 Extended Support et empêche aux personnes malveillantes d'exploiter la vulnérabilité de sécurité Logjam CVE-2015-4000.

## Prise en charge complète des modules Apache pour IdM

Les modules Apache suivants pour IdM (« Identity Management »), ajoutés en tant qu'aperçu technologique sur Red Hat Enterprise Linux 7.1, sont désormais complètement pris en charge : **mod\_authnz\_pam**, **mod\_lookup\_identity**, et **mod\_intercept\_form\_submit**. Les modules Apache peuvent être utilisés par des applications externes pour effectuer des interactions plus serrées avec IdM, au-delà d'une simple authentification.



## Chapitre 3. Clustering

### systemd et pacemaker sont désormais coordonnés correctement pendant les fermetures système

Auparavant, systemd et pacemaker n'étaient pas correctement coordonnés pendant les fermetures système, ce qui causait aux ressources pacemaker de ne pas quitter correctement. Avec cette mise à jour, pacemaker reçoit l'ordre de s'arrêter avant dbus et les autres services systemd que pacemaker a lancé. Ceci permet à pacemaker et aux ressources que pacemaker gère de se fermer correctement.

### Les commandes `pcs resource move` et `pcs resource ban` affichent désormais un message d'avertissement pour clarifier le comportement des commandes

La commande `pcs resource move` et les commandes `pcs resource ban` créent des contraintes d'emplacement qui bannissent de manière effective la ressource d'une exécution sur le nœud actuel jusqu'à ce que la contrainte soit supprimée ou que son cycle de vie expire. Jusqu'ici, ce comportement n'était pas clair pour les utilisateurs. Ces commandes affichent désormais un message d'avertissement expliquant ce comportement, leurs écrans d'aide et leur documentation ont également été clarifiés.

### Nouvelle commande pour déplacer une ressource Pacemaker sur son nœud préféré

Une fois qu'une ressource Pacemaker est déplacée, que ce soit dû à un basculement, ou à un administrateur déplaçant le nœud manuellement, celle-ci ne sera pas nécessairement replacée sur son nœud d'origine même si les circonstances ayant causé le basculement ont été corrigées. Vous pouvez désormais utiliser la commande `pcs resource relocate run` pour déplacer une ressource sur son nœud préféré, comme déterminé par le statut actuel du cluster, les contraintes, l'emplacement des ressources, ainsi que par d'autres paramètres. Vous pouvez également utiliser la commande `pcs resource relocate show` pour afficher les ressources ayant migré. Pour obtenir davantage d'informations sur ces commandes, veuillez consulter la référence du module complémentaire High Availability, « High Availability Add-On Reference ».

### Prise en charge de la commande `clufte` pour transformer et analyser les formats de configuration de clusters

La commande `clufte` fournit un outil pour transformer et analyser les formats de configuration de clusters. La commande `clufte` peut être utilisée pour assister lors des migrations depuis une ancienne configuration de pile à une nouvelle configuration qui tire profit de Pacemaker. Pour obtenir davantage d'informations sur les capacités de la commande `clufte`, veuillez consulter la page `man clufte(1)` ou la sortie de la commande `clufte -h`.

## Chapitre 4. Compilateur et outils

### **tail --follow fonctionne désormais correctement sur les fichiers sur VXFS (« Veritas Clustered File System »)**

VXFS (« Veritas Clustered File System ») est un système de fichiers distant, et pour les systèmes de fichiers distants, **tail** ne peut pas utiliser la fonctionnalité « inotify » pour le mode « --follow ». Le système de fichiers VXFS a désormais été ajouté à la liste des systèmes de fichiers distants, pour lesquels le mode d'interrogation a été utilisé au lieu de « inotify ». **tail --follow** peut maintenant fonctionner correctement même lorsqu'utilisé sur des fichiers sur VXFS.

### **La commande dd est maintenant capable d'afficher la progression des transferts**

La commande **dd**, qui est utilisée pour copier les fichiers octet par octet, offre maintenant l'option « status=progress » pour afficher la progression du transfert. Ceci est particulièrement utile pour les transferts de fichiers de grande taille car l'utilisateur peut estimer le temps restant et détecter les problèmes potentiels du transfert.

### **Temps d'attente amélioré sur libcurl**

La bibliothèque **libcurl** utilisait un délai de blocage inutilement long pour des actions ne contenant aucun descripteur de fichier actif, même pour les opérations de courte durée. Cela signifie que certaines actions, comme la résolution de nom d'hôte en utilisant **/etc/hosts**, prenaient un temps artificiellement long pour se terminer. Le code de blocage dans **libcurl** a donc été modifié de manière à ce que le délai initial soit court et augmente graduellement jusqu'à ce qu'un événement se produise. Maintenant, les opérations **libcurl** rapides se terminent plus rapidement.

### **La bibliothèque libcurl implémente désormais une poignée de mains SSL non bloquante**

Auparavant, la bibliothèque **libcurl** n'avait pas implémenté de poignée de mains SSL non bloquante, ce qui affectait négativement les performances des applications basées sur les multiples API **libcurl**. Pour résoudre ce problème, une poignée de mains SSL non bloquante a été implémentée sur **libcurl**, et désormais les multiples API **libcurl** rendent immédiatement le contrôle à l'application lorsqu'il ne peut pas lire ou écrire de données à partir du socket du réseau sous-jacent.

### **GDB sur systèmes IBM Power Systems n'échoue plus lors de l'accession à la table des symboles**

Auparavant, GDB sur systèmes 64 bits IBM Power Systems désallouait incorrectement une variable importante qui retenait la table des symboles du binaire en cours de débogage, ce qui provoquait une faute de segmentation lorsque GDB tentait d'accéder à cette table de symboles. Pour résoudre ce problème, cette variable spécifique a été rendue persistante et GDB peut désormais accéder aux informations plus tard pendant la session de débogage, sans lire une région de la mémoire invalide.

### **nscd mis à jour pour recharger les données de configuration automatiquement**

Cette mise à jour du démon **nscd** (« Name Server Caching Daemon ») ajoute un système de surveillance basé inotify et de surveillance de sauvegarde basé stat pour les fichiers de configuration **nscd**, de manière à ce que **nscd** puisse désormais détecter correctement les changements apportés à sa configuration et recharger les données. Ceci empêche **nscd** de retourner des données obsolètes.

## La fonction bibliothèque `dlopen` ne tombe plus en panne lors des appels récursifs

Auparavant, un défaut dans la fonction bibliothèque `dlopen` pouvait causer aux appels récursifs de cette fonction de tomber en panne ou d'être annulés avec une assertion de bibliothèque. Les appels récursifs sont possibles si une implémentation `malloc` fournie par l'utilisateur appelle `dlopen`.

L'implémentation est maintenant ré-entrante, et les appels récursifs ne tombent plus en panne et ne sont plus annulés avec une assertion.

## L'outil `operf` reconnaît désormais les identifiants huge page statiques

Auparavant, pendant les analyses d'exécution des performances du code compilé JIT (« Java just-in-time ») avec des huge pages statiques activées, la commande `operf` de OProfile enregistrait un grand nombre d'échantillons d'événements sur une mémoire anonyme (dans `anon_hugepage`) au lieu de la méthode Java appropriée. Avec cette mise à jour, `operf` reconnaît les identifiants des huge pages statiques et fait correspondre correctement les échantillons avec les méthodes Java lors de l'utilisation de huge pages allouées statiquement.

## La commande `rsync -X` fonctionne désormais correctement

Auparavant, l'outil `rsync` modifiait les appartenances de fichiers après, et non pas avant, avoir défini les attributs de sécurité. Par conséquent, les attributs de sécurité sur la cible étaient manquants, et l'exécution de la commande `rsync -X` ne fonctionnait pas correctement sous certaines circonstances. Avec cette mise à jour, l'ordre des opérations a été échangé, et `rsync` change désormais les appartenances avant de définir les attributs de sécurité. Ainsi, les attributs de sécurité sont présent dans la situation décrite comme prévu.

## Les exécutables Subversion sont maintenant créés avec des données RELRO complètes

Les exécutables fournis avec le paquet `subversion` sont désormais créés avec des données de relocation en lecture seule (RELRO) complètes, ce qui protège contre certains types d'attaques de corruption de mémoire. Par conséquent, il sera plus difficile d'exploiter Subversion avec succès si de futures vulnérabilités sont découvertes.

## L'extension de fils d'exécution dans TCL fonctionne désormais correctement

Auparavant, la prise en charge des fils d'exécution dans TCL (« Tool Command Language ») n'était pas implémentée de manière optimale. Si l'appel `fork()` était utilisé avec l'extension des fils d'exécution activée dans l'interprète TCL, le processus pouvait ne plus répondre. À cause de cela, l'interprète TCL et l'application TK étaient envoyés avec l'extension de fils d'exécution désactivée. Par conséquent, des applications de tierce-partie dépendantes des fils d'exécution TCL ou TK ne fonctionnaient pas correctement. Un patch a été implémenté pour corriger ce bogue, et l'extension des fils d'exécution est désormais activée par défaut sur TCL et TK.

## Chapitre 5. Bureau

### GNOME 3.14

Le **Bureau GNOME** a été mis à niveau à la version en amont 3.14, qui inclut de nouvelles fonctionnalités et un certain nombre d'améliorations, à savoir :

Un certain nombre de fonctionnalités ont été ajoutées au protocole de mise en fenêtre **Wayland**, y compris la configuration du clavier, la prise en charge d'écrans tactiles, la prise en charge du glisser-déposer, des menus de contexte fonctionnels, des infobulles et des boîtes combinées, de l'affichage de haute résolution, et du déplacement et du redimensionnement de fenêtres.

Les interactions tactile multipoint (« **Multitouch gestures** ») peuvent désormais être utilisées sur les écrans tactiles pour la navigation système, ainsi que sur les applications. Des gestes peuvent être utilisés pour ouvrir la vue d'ensemble des activités, la vue des Applications et l'espace de notification de messages, ou peuvent être utilisés pour basculer entre applications et espaces de travail.

GNOME 3.14 offre une prise en charge améliorée des points d'accès Wi-Fi. Lors de la connexion à un portail Wi-Fi qui requiert une authentification, GNOME affiche désormais automatiquement la page de connexion comme faisant partie du processus de connexion.

Les partages personnels de **fichiers (WebDAV)**, de **médias (DLNA)**, et d'**écrans (VNC)** peuvent désormais se rappeler sur quel réseau l'utilisateur souhaite les voir actifs. Les Paramètres fournissent également la possibilité de contrôler sur quels réseaux les partager. Cette fonctionnalité empêche le partage de contenu et de services dans des lieux publics.

Lorsque plusieurs moniteurs sont utilisés, GNOME 3.14 restaure désormais la positions d'origine des affichages si les moniteurs sont déconnectés puis reconnectés.

L'application GNOME pour les machines distantes et les machines virtuelles, **Boxes** introduit les instantanés. Désormais, **Boxes** fournit également le téléchargement automatique, l'exécution de multiples boîtes sur différentes fenêtres, et des améliorations de l'interface utilisateur, y compris un comportement plein écran amélioré et des vignettes.

**GTK+** 3.14 inclut un certain nombre de correctifs de bogues et d'améliorations, tels que le chargement automatique des menus à partir des ressources, la prise en charge de sélections multiples sur **GtkListBox**, sur les interfaces des propriétés des fichiers **GtkBuilder**, la prise en charge de dessins hors de l'allocation d'un widget (`gtk_widget_set_clip()`), de nouveaux types de transition dans **GtkStack**, et le chargement et enregistrement de fichiers avec **GtkSourceView**. En outre, **GTK+** offre désormais la prise en charge des gestes d'interaction tactile multipoint disponible sur les applications GTK+, comme taper, tirer, glisser, pincer et pivoter. Les gestes peuvent être ajoutés aux applications GTK+ existantes en utilisant **GtkGesture**.

**Glib** 3.14 offre désormais la prise en charge de la spécification des associations d'applications MIME, la prise en charge SHA-512 sur GHmac, la prise en charge d'Implements dans les fichiers de bureau, et la prise en charge d'unicode 7.0.

Le navigateur de la documentation d'**Aide** de GNOME a été reconçu pour être cohérent avec les autres applications GNOME 3. La documentation d'Aide utilise désormais une barre d'en-tête, possède une fonction de recherche intégrée, et une interface d'insertion de signets.

Une extension du shell GNOME, **Looking Glass Inspector**, offre un certain nombre de fonctionnalités pour développeurs : affichant toutes les méthodes, classes, etc. , dans un espace de noms après l'inspection, l'expansion de l'historique de l'inspecteur d'objets, ou copiant les résultats « Looking Glass » en tant que chaînes, et transférant les événements sur `gnome-shell`.

**Désormais, le paquet `ibus-gtk2` met à jour le fichier `immodules.cache`**

Auparavant, le script **update-gtk-immodules** recherchait un répertoire **/etc/gtk-2.0/\$host**, qui n'existait plus. Par conséquent, le script de post-installation du paquet *ibus-gtk2* échouait et quittait sans créer ni mettre à jour le cache. Le script de post-installation a été modifié pour remplacer **update-gtk-immodules** par **gtk-query-immodules-2.0-BITS**, et le problème ne se produit plus.

## Chapitre 6. Systèmes de fichiers

### **gfs2-utils rebasé sur la version 3.1.8**

Le paquet *gfs2-utils* a été rebasé sur la version 3.1.8, qui fournit des correctifs importants et un certain nombre d'améliorations :

- \* Les performances des utilitaires **fsck.gfs2**, **mkfs.gfs2**, et **gfs2\_edit** ont été améliorées.
- \* L'utilitaire **fsck.gfs2** effectue désormais de meilleures vérifications des journaux, de jindex, des inodes du système, et des valeurs « goal » de l'inode.
- \* Les utilitaires **gfs2\_jadd** et **gfs2\_grow** sont désormais des programmes séparés, au lieu d'être des liens symboliques vers **mkfs.gfs2**.
- \* La suite test et la documentation la concernant ont été améliorées.
- \* Le paquet ne dépend plus de Perl.

### **GFS2 empêche désormais les utilisateurs de dépasser leurs quotas**

Auparavant, GFS2 vérifiait uniquement les violations de quota une fois les opérations terminées, ce qui pouvait résulter en utilisateurs ou groupes excédant les quotas qui leur étaient alloués. Ce comportement a été corrigé, et GFS2 prédit désormais combien de blocs une opération allouerait et vérifie si leur allocation viole les quotas. Les opérations qui provoqueraient une violation de quota sont interdites. Ainsi, les utilisateurs ne dépassent jamais leurs quotas alloués.

### **XFS rebasé sur la version 4.1**

XFS a été mis à niveau à la version en amont 4.1, et comprend des correctifs de bogues mineurs, des refactorisations, et le retravail de certains mécanismes internes, comme la journalisation, la comptabilité pcpu, et un nouveau verrouillage mmap. En plus des modifications en amont, cette mise à jour étend la fonction `rename()` pour ajouter `cross-rename` (une variante symétrique de `rename()`), ainsi que la gestion `whiteout`.

### **Mises à niveau d'ext4 et jbd2**

Les périphériques `ext4` et `jbd2` ont été mis à niveau à la version en amont la plus récente, qui fournit un certain nombre de correctifs de bogues et d'améliorations comparé à la dernière version.

### **cifs rebasé sur la version 3.17**

Le module CIFS a été mis à niveau à la version en amont 3.17, qui fournit divers correctifs mineurs, ainsi que de nouvelles fonctionnalités pour « Server Message Block » 2 et 3 (SMB2 et SMB3).

## Chapitre 7. Mises à jour générales

### Désormais lftp gère la redirection 302 correctement

lftp a été mis à jour afin de gérer correctement les redirections 302 lors d'une exécution en mode miroir. Auparavant, lftp s'arrêtait avec une erreur.

### Davantage d'informations de diagnostic et un greffon renommé pour sosreport

L'outil sosreport a été amélioré pour collecter les informations liées au processus à partir de diverses applications, y compris ptp, lastlog, et ethtool. Le greffon **startup**, qui fait partie de ce changement, a été renommé **services** afin de mieux communiquer sa fonction.

## Chapitre 8. Installation et démarrage

### Installation réseau corrigée dans `initrd` si la configuration réseau est fournie dans Kickstart

Auparavant, l'installateur échouait à paramétrer ou à reconfigurer les interfaces réseau dans `initrd` si celles-ci étaient définies dans les fichiers Kickstart. Cela pouvait entraîner l'échec de l'installation et celle-ci pouvait entrer en mode de secours si l'accès réseau était requis par d'autres commandes du fichier Kickstart.

Ce problème est désormais résolu et Anaconda gère correctement la configuration réseau à partir des fichiers Kickstart dans `initrd` assez tôt pendant le processus de démarrage.

### Anaconda prend désormais en charge la création de volumes logiques dans le cache

L'installateur prend désormais en charge la création de volumes logiques LVM dans le cache et l'installation du système sur ces volumes.

Actuellement cette approche est uniquement prise en charge dans Kickstart. Pour créer un volume logique dans le cache, veuillez utiliser les nouvelles options `--cachevps=`, `--cachesize=`, et `--cachemode=` de la commande Kickstart `logvol`.

Veuillez consulter le Guide d'installation Red Hat Enterprise Linux 7 pour obtenir des informations détaillées sur ces nouvelles options.

### Amélioration du tri du menu de démarrage GRUB2

Un problème avec le mécanisme de tri utilisé par la commande `grub2-mkconfig` peut causer au fichier de configuration `grub.cfg` d'être généré avec les noyaux disponibles triés incorrectement.

GRUB2 utilise désormais le paquet `rpmdevtools` pour trier les noyaux disponibles et le fichier de configuration est généré correctement avec la version du noyau la plus récente, qui est répertoriée tout en haut.

### Désormais, Anaconda restaure correctement les actions de disque lorsqu'il se produit des changements de sélection de disque

Auparavant, Anaconda et Blivet ne restauraient pas correctement les actions planifiées sur les disques lorsque les sélections de disques changeaient, causant ainsi divers problèmes. Avec cette mise à jour, Anaconda a été corrigé et crée un instantané de la configuration du stockage initiale et y retourne lorsque les sélections de disques changent, restaurant ainsi totalement toutes les actions planifiées pour les disques.

### Amélioration de la détection des noms de disques `device-mapper`

Dans la version précédente de Red Hat Enterprise Linux 7, l'installateur pouvait tomber en panne lors d'une installation sur des disques qui contenaient auparavant des volumes logiques et que les métadonnées de ces volumes étaient toujours présentes. L'installateur ne pouvait pas reconnaître les noms `device-mapper` corrects et le processus de création de nouveaux volumes logiques LVM échouait.

La méthode utilisée pour obtenir des noms de périphérique `device-mapper` a été mise à jour et l'installation sur disques qui contenaient des métadonnées LVM existantes est désormais plus fiable.

### Gestion de PReP Boot pendant le partitionnement corrigée



Sous certaines circonstances, la partition **PreP Boot** sur IBM Power Systems pouvait être paramétrée avec une taille invalide pendant un partitionnement personnalisé. Dans cette situation, la suppression de toute partition provoquait une panne de l'installateur.

Des vérifications sont maintenant implémentées dans *anaconda* afin de s'assurer que la partition est toujours correctement dimensionnée, entre **4096 Kio** et **10 Mio**. En outre, il n'est plus nécessaire de modifier le format de la partition **PreP Boot** pour changer sa taille.

## Partitions EFI sur périphériques RAID1

Des partitions système EFI peuvent maintenant être créées sur un périphérique RAID1, ceci sert à permettre une récupération système lorsqu'un disque de démarrage échoue. Cependant, dans le cas où **Boot####** et **BootOrder**, et le volume d'ESP découvert par le microprogramme soient corrompus, mais qu'ils apparaissent toujours comme un ESP valide, alors l'ordre de démarrage ne sera pas reconstruit automatiquement. Cependant, le système devrait toujours pouvoir démarrer manuellement à partir du second disque.

## L'installation en mode texte ne tombe plus en panne pendant la configuration réseau

Auparavant, dans l'écran de configuration réseau de l'installateur en mode texte interactif, l'utilisation d'un espace lors de la spécification des serveurs de noms provoquait la panne de l'installateur.

Désormais, Anaconda gère correctement les espaces dans les définitions de serveurs de noms en mode texte, et l'installateur ne tombe plus en panne si un espace est utilisé pour séparer les adresses des serveurs de noms.

## Les écrans du mode de secours sur IBM System z ne sont plus coupés

Auparavant, le second et le troisième écran du mode de secours sur serveurs IBM System z étaient affichés incorrectement et certaines parties de l'interface étaient coupées. Le mode de secours sur cette architecture a été amélioré et tous les écrans fonctionnent désormais correctement.

## Module complémentaire OpenSCAP dans Anaconda

Il est désormais possible d'appliquer le contenu SCAP (« Security Content Automation Protocol ») pendant le processus d'installation. Ce nouveau module complémentaire de l'installateur offre une manière fiable et facile de configurer une politique de sécurité sans avoir à utiliser de scripts personnalisés.

Ce module complémentaire fournit une nouvelle section Kickstart (« %addon org\_fedora\_oscaps ») ainsi qu'un nouvel écran dans l'interface utilisateur graphique pendant une installation interactive. Ces trois parties sont documentées dans le Guide d'installation Red Hat Enterprise Linux 7.

L'application d'une politique de sécurité pendant l'installation effectuera divers changements pendant et immédiatement après l'installation, selon la politique activée. Si un profil est sélectionné, le paquet *openscap-scanner* (un outil de vérification de conformité OpenSCAP) est ajouté à votre sélection de paquets et un scan de conformité initial sera effectué une fois l'installation terminée. Les résultats de ce scan seront enregistrés sur **/root/openscap\_data**.

Plusieurs profils sont fournis sur le support d'installation par le paquet *scap-security-guide*. Vous pouvez également charger d'autres contenus en tant que flux de données, archives, ou en tant que paquets RPM à partir d'un serveur HTTP, HTTPS ou FTP si nécessaire.

Remarquez que l'application d'une politique de sécurité n'est pas nécessaire sur tous les systèmes. Ce module complémentaire doit être utilisé uniquement lorsqu'une politique spécifique est mandatée par les règles de votre organisation ou par des réglementations gouvernementales, sinon le module complémentaire peut rester dans son état par défaut, qui n'applique aucune politique de sécurité.

### **Anaconda n'expirés plus lorsqu'il attend un fichier Kickstart sur un CD ou DVD**

Auparavant, si Anaconda était configuré pour charger un fichier Kickstart à partir d'un support optique utilisant la commande `inst.ks=cdrom:/ks.cfg` et que le système était également démarré à partir d'un CD ou DVD, l'installateur attendait un court moment que le disque soit échangé. Cette fenêtre était assez courte par défaut, 30 secondes uniquement. Une fois ce délai expiré, le système entrait en mode de secours.

Anaconda a été modifié pour ne jamais expirer en attendant d'un utilisateur qu'il fournisse un fichier Kickstart sur CD ou DVD. Si les options de démarrage `inst.ks=cdrom` sont utilisées et que le fichier Kickstart n'est pas détecté, Anaconda affichera une invite et attendra que le fichier soit fourni ou qu'un redémarrage soit effectué.

## Chapitre 9. Noyau

### Les paramètres de noyau SHMMAX et SHMALL retrouvent leurs valeurs par défaut

Auparavant, les valeurs des paramètres `kernel.shmmax` et `kernel.shmall`, qui étaient définies dans le fichier `/usr/lib/sysctl.d/00-system.conf`, étaient trop basses. Par conséquent, certaines applications, comme SAP, ne pouvaient pas fonctionner correctement. Les remplacements inconvenables ont été supprimés et des valeurs de noyau par défaut suffisamment hautes sont maintenant utilisées.

### Les « Transparent huge pages » ne causent plus de corruption de mémoire

Les « Transparent huge pages » n'étaient pas synchronisées correctement pendant les opérations de lecture et d'écriture. Sous certaines circonstances, ceci causait une corruption de la mémoire lorsque les « Transparent huge pages » étaient activées. Des barrière de mémoire ont été ajoutés à la gestion « Transparent huge page » afin que ces corruptions de mémoire ne se produisent plus.

### Rebasement SCSI LIO

La cible du noyau SCSI, LIO, a été rebasée à partir de Linux-4.0.stable. Ceci inclut de nombreux correctifs de bogues, critiques à iSER, mais inclut également l'ajout de la prise en charge des commandes XCOPY, WRITE SAME, et ATS, ainsi que la prise en charge de l'intégrité des données DIF.

### makedumpfile prend désormais en charge le nouveau format sadump représentant jusqu'à 16 To de mémoire physique

La commande `makedumpfile` prend désormais en charge le nouveau format `sadump` qui peut représenter plus de 16 To d'espace de mémoire physique. Ceci permet aux utilisateurs de `makedumpfile` de lire des fichiers de vidage de plus de 16 To, générés par `sadump` sur certains nouveaux modèles de serveur.

### Supprimer ou mettre à niveau le noyau n'affichera plus d'avertissement

Auparavant, le script `weak-modules`, qui était utilisé par `kmod` pour gérer des liens symboliques de modules compatibles KABI, supprimait le répertoire `/lib/modules/<version>/weak-updates` lors de la suppression des fichiers associés à un noyau. Ce répertoire appartient au paquet `kernel` et sa suppression causait une incohérence entre le système de fichiers et l'état auquel `rpm` s'attendait. Cela entraînait l'affichage d'un avertissement chaque fois qu'un noyau était mis à niveau ou supprimé.

Le script a été mis à jour pour supprimer le contenu du répertoire `weak-updates` mais laisse le répertoire, et les avertissements ne sont plus affichés.

### Nouveau paquet : libevdev

`libevdev` est une bibliothèque de bas niveau pour l'interface du périphérique d'événements d'entrées du noyau Linux. Celle-ci fournit des interfaces sûres pour interroger les capacités de périphérique et les événements de processus des périphériques. Les versions actuelles de `xorg-x11-drv-evdev` et `xorg-x11-drv-synaptics` requièrent cette bibliothèque en tant que dépendance.

### Tuned peut désormais être exécuté en mode no-daemon

Auparavant, Tuned pouvait uniquement être exécuté en tant que démon, ce qui pouvait affecter les performances des systèmes de petite taille, à cause de l'empreinte mémoire du démon Tuned. Avec cette mise à jour, un mode no-daemon (« one shot »), qui ne requiert pas de mémoire résidente, a été ajouté à Tuned. Le mode no-daemon est désactivé car de nombreuses fonctionnalités de Tuned ne sont pas incluses dans ce mode.

## Nouveau paquet : tuned-profiles-realtime

Le paquet *tuned-profiles-realtime* a été ajouté à Red Hat Enterprise Linux Server et à Red Hat Enterprise Linux pour Real Time. Il contient un profil realtime utilisé par l'utilitaire **tuned** pour effectuer une isolation CPU et des réglages IRQ. Lorsque le profil est activé, il lit une section variable, qui spécifie les CPU devant être isolés et déplace tous les fils d'exécution qui pourraient être retirés de ces cœurs de CPU.

## Planification d'E/S à multiples files d'attente (« Multiqueue I/O scheduling ») avec blk-mq

Red Hat Enterprise Linux 7.2 inclut un nouveau mécanisme de planification des E/S à multiples files d'attente pour les périphériques bloc, appelés blk-mq. Ce mécanisme améliore les performances en autorisant certains pilotes de périphérique à mapper les requêtes d'E/S avec de multiples files d'attente de matériel ou de logiciel. L'amélioration des performances vient de la réduction de la contention de verrouillage présente lorsque de multiples fils d'exécution effectuent des E/S sur un seul périphérique. De plus récents périphériques, comme NVMe (« Non-Volatile Memory Express »), sont mieux positionnés pour tirer profit de cette fonctionnalité grâce à leur prise en charge des multiples files d'attente de soumission de matériel et d'achèvement, et à leurs performances à basse latence. Comme toujours, les améliorations des performances dépendront du matériel utilisé et de la charge de travail.

La fonctionnalité blk-mq est actuellement implémentée et est activée par défaut sur les pilotes suivants : virtio-blk, mtip32xx, nvme, et rbd.

Une fonctionnalité liée, scsi-mq, permet aux pilotes de périphérique SCSI (« Small Computer System Interface ») d'utiliser une infrastructure blk-mq. La fonctionnalité scsi-mq est offerte en tant qu'aperçu technologique sur Red Hat Enterprise Linux 7.2. Pour activer scsi-mq, veuillez spécifier **scsi\_mod.use\_blk\_mq=y** sur la ligne de commande du noyau. La valeur par défaut est **n** (désactivé).

La cible multivoies du mappeur de périphériques (« DM »), qui utilise un DM basé sur requêtes, peut également être configuré pour utiliser l'infrastructure blk-mq si l'option du noyau **dm\_mod.use\_blk\_mq=y** est spécifiée. La valeur par défaut est **n** (désactivé).

Il pourrait être bénéfique de paramétrer **dm\_mod.use\_blk\_mq=y** si les périphériques SCSI sous-jacents utilisent également blk-mq, car cela réduira la charge de verrouillage sur la couche DM.

Pour déterminer si DM multipath utilise blk-mq sur un système, affichez le fichier **/sys/block/dm-X/dm/use\_blk\_mq** avec `cat`, où **dm-X** est remplacé par le périphérique DM multipath en question. Ce fichier est uniquement accessible en lecture et reflète ce que la valeur globale dans **/sys/module/dm\_mod/parameters/use\_blk\_mq** était au moment où le périphérique DM multipathe basé requête a été créé.

## Les messages d'erreur SCSI peuvent désormais être interprétés confortablement

De précédents changements apportés à la fonction `printk()` ont provoqué la journalisation des messages d'erreur SCSI (« Small Computer System Interface ») à travers de multiples lignes. Par conséquent, si de multiples erreurs se produisent à travers différents périphériques, il peut être difficile d'interpréter ces messages d'erreur correctement. Cette mise à jour change le code de journalisation d'erreurs SCSI de manière à journaliser les messages d'erreur à l'aide de l'option `dev_printk()`, qui associe chaque message d'erreur avec le périphérique qui a généré l'erreur.

## Mise à jour du sous-système et des pilotes libATA

Cette mise à jour d'amélioration fournit de nombreux correctifs de bogues et améliorations du sous-système et des pilotes libATA.

### FCoE et DCB ont été mis à niveau

Les composants de noyau FCoE (« Fibre Channel over Ethernet ») et DCB (« Data Center Bridging ») ont été mis à niveau avec leurs versions en amont les plus récentes, fournissant ainsi de nombreux correctifs de bogues et de nombreuses améliorations comparé à leurs versions précédentes.

### perf rebasé sur la version 4.1

Les paquets perf ont été mis à niveau à la version 4.1, qui fournit de nombreux correctifs de performance et de stabilité et d'améliorations comparé à la version précédente. Plus particulièrement, ce rebasement ajoute les fonctionnalités Intel Cache QoS Monitoring et AMD IBS Ops et fournit la prise en charge d'Intel Xeon v4, mais aussi la prise en charge des modules de noyau compressé, d'événements paramétrisés et de la spécification de la longueur des points d'arrêt. En outre, un certain nombre d'options ont été ajoutées à l'outil perf, comme les options `--system-wide`, `top -z`, `top -w`, `trace --filter-pids`, et `trace --event`.

### Prise en charge de TPM 2.0

Cette mise à jour ajoute la prise en charge niveau pilote des périphériques TPM (« Trusted Platform Module ») conforme à la version 2.0.

### Désormais, Turbostat fournit une sortie correcte

Auparavant, l'outil turbostat détectait si le système offrait la prise en charge de périphériques MSR en lisant le fichier `/dev/cpu/0/msr` pour le `cpu0` au lieu du `cpu`. Par conséquent, la désactivation d'un CPU causait aux CPU d'être supprimés de la sortie de turbostat. Ce bogue a été corrigé, et l'exécution de la commande `turbostat ls` retourne désormais une sortie correcte.

### Prise en charge du processeur Intel Xeon v5

Cette amélioration ajoute la prise en charge du processeur Intel Xeon v5 à l'outil turbostat.

### l'outil zswap utilise l'API zpool

Auparavant, l'outil zswap utilisait directement zbud, un pool de stockage qui stocke des pages compressées à un niveau de 2:1 (lorsque plein). Cette mise à jour présente l'API zpool qui fournit accès aux pools zbud ou zsmalloc : zsmalloc stocke les pages compressées à une densité potentiellement plus élevée, résultant ainsi en davantage de mémoire réclamée pour des pages hautement compressibles. Avec cette mise à jour, zsmalloc a été promu aux pilotes /mm afin que zpool puisse fonctionner comme prévu.

### La longueur du fichier /proc/pid/cmdline est désormais illimitée

La limite de longueur du fichier `/proc/pid/cmdline` pour la commande `ps` était auparavant codée de manière permanente dans le noyau avec un maximum de 4096 caractères. Cette mise à jour rend la longueur de `/proc/pid/cmdline` illimitée, ce qui est particulièrement utile pour répertorier les processus avec de longs arguments de ligne de commande.

## **La prise en charge de dma\_rmb et dma\_wmb est désormais offerte**

Cette mise à jour présente deux nouvelles primitives pour synchroniser les écritures et lectures cohérentes de mémoire du cache, dma\_wmb() et dma\_rmb(). Cette fonctionnalité sera disponible pour une utilisation appropriée dans les pilotes.

## Chapitre 10. Mise en réseau

### Désormais, SNMP obéit correctement à la directive `clientaddr` sur IPv6

Auparavant, l'option `clientaddr` du fichier `snmp.conf` affectait uniquement les messages sortants envoyés via IPv4. Avec cette version, les messages IPv6 sortants sont correctement envoyés à partir de l'interface spécifiée par `clientaddr`.

### `tcpdump` prend en charge les options `-J`, `-j`, et `--time-stamp-precision`

Comme kernel, glibc, et libpcap fournissent désormais des API pour obtenir des horodatages avec une résolution à la nanoseconde, `tcpdump` a été mis à jour pour tirer profit de cette fonctionnalité. Les utilisateurs peuvent maintenant demander quelles sources d'horodatage sont disponibles (`-J`), définir une source d'horodatage spécifique (`-j`), et demander que l'horodatage utilise une résolution particulière (`--time-stamp-precision`).

### Mise à niveau TCP/IP

La pile TCP/IP a été mise à niveau à la version 3.18, qui fournit de nombreux correctifs de bogues et améliorations comparé à la version précédente. Plus particulièrement, cette mise à jour corrige l'extension d'ouverture rapide TCP, qui fonctionne désormais comme prévu lors de l'utilisation d'IPv6. En outre, cette mise à jour inclut la prise en charge de l'autocorking TCP optionnel et implémente DCTCP (« Data Center TCP »).

## Chapitre 11. Serveurs et services

### La directive `ErrorPolicy` est désormais validée

La directive de configuration `ErrorPolicy` n'était pas validée pendant le démarrage, et une politique d'erreur par défaut non-intentionnelle pouvait être utilisée sans avertissement. La directive est désormais validée lors du démarrage et réinitialisée si la valeur configurée par défaut est incorrecte. La politique envisagée est utilisée, ou un message d'avertissement est journalisé.

### Désormais, CUPS désactive le chiffrement SSLv3 par défaut

Auparavant, il n'était pas possible de désactiver le chiffrement SSLv3 dans le planificateur CUPS, ce qui le laissait vulnérable à des attaques contre SSLv3. Pour résoudre ce problème, le mot-clé `cupsd.conf` **SSLOptions** a été étendu pour inclure deux nouvelles options, **AllowRC4** et **AllowSSL3**, qui autorisent toutes deux la fonctionnalité nommée dans `cupsd`. Les nouvelles options sont également prises en charge dans le fichier `/etc/cups/client.conf`. Le comportement par défaut désactive désormais RC4 et SSL3 pour `cupsd`.

### Cups autorise désormais le trait de soulignement dans les noms d'imprimante

Le service `cups` autorise désormais les utilisateurs à inclure le trait de soulignement () dans les noms d'imprimantes locales.

### Dépendance inutile supprimée du paquet `tftp-server`

Auparavant, un paquet supplémentaire était installé par défaut lors de l'installation du paquet `tftp-server`. Avec cette mise à jour, la dépendance superflue du paquet a été supprimée, et le paquet inutile n'est plus installé par défaut lors de l'installation de `tftp-server`.

### Le fichier déconseillé `/etc/sysconfig/conman` a été supprimé

Avant de présenter le gestionnaire `systemd`, diverses limites pour les services pouvaient être configurées dans le fichier `/etc/sysconfig/conman`. Après la migration vers `systemd`, `/etc/sysconfig/conman` n'est plus utilisé et a donc été supprimé. Pour définir des limites et d'autres paramètres du démon, comme `LimitCPU=`, `LimitDATA=`, ou `LimitCORE=`, modifiez le fichier `conman.service`. Pour obtenir davantage d'informations, veuillez consulter la page de manuel `systemd.exec(5)`. En outre une nouvelle variable, `LimitNOFILE=10000`, a été ajoutée au fichier `systemd.service`. Cette variable est un commentaire par défaut. Remarquez qu'après avoir effectué tout changement à la configuration `systemd`, la commande `systemctl daemon-reload` doit être exécutée pour que ces changements puissent prendre effet.



## Chapitre 12. Stockage

### Nouvelles options `delay_watch_checks` et `delay_wait_checks` dans le fichier `multipath.conf`

Si un chemin n'est pas fiable, comme lorsqu'une connexion est fréquemment coupée, `multipathd` tentera continuellement d'utiliser ce chemin. Le délai d'attente avant que `multipathd` réalise que le chemin n'est plus accessible est réglé sur 300 secondes, ce qui peut donner l'impression que `multipathd` est tombé en panne.

Pour corriger cela, deux nouvelles options de configuration ont été ajoutées : `delay_watch_checks` et `delay_wait_checks`. Paramétrez `delay_watch_checks` sur le nombre de cycles pendant lesquels `multipathd` doit observer le chemin après avoir été mis en ligne. Si le chemin échoue avant la valeur assignée, `multipathd` ne l'utilisera pas. `Multipathd` se fiera ensuite à l'option `delay_wait_checks` pour lui faire savoir combien de cycles consécutifs doivent s'écouler avant que le chemin ne redevienne valide. Ceci empêche l'utilisation de chemins non fiables immédiatement après leur remise en ligne.

### Nouvelle option `config_dir` dans le fichier `multipath.conf`

Les utilisateurs ne pouvaient pas diviser leur configuration entre le fichier `/etc/multipath.conf` et d'autres fichiers de configuration. Ceci empêchait les utilisateurs de paramétrer un fichier de configuration principal pour leurs ordinateurs et de garder des informations sur la configuration spécifique à l'ordinateur dans des fichiers de configuration séparés pour chaque machine.

Pour répondre à ce problème, une nouvelle option `config_dir` a été ajoutée au fichier de configuration `multipath.conf`. Les utilisateurs doivent changer l'option `config_dir` soit sur une chaîne vide ou sur un nom de chemin d'accès de répertoire complet. Lorsque défini sur autre chose qu'une chaîne vide, `multipath` lira tous les fichiers `.conf` par ordre alphabétique. Les configurations seront ensuite appliquées exactement comme si elles avaient été ajoutées au fichier `/etc/multipath.conf`. Si ce changement n'est pas effectué, la valeur par défaut de `config_dir` sera `/etc/multipath/conf.d`.

### Mise à niveau DM

DM (« Device Mapper ») a été mis à niveau à la version en amont 4.0, qui fournit un certain nombre d'améliorations et de correctifs de bogues comparé à la version précédente, y compris une mise à jour des performances DM crypt et une mise à jour du cœur DM pour prendre en charge le mécanisme « Multi-Queue Block I/O Queueing Mechanism » (`blk-mq`).

### Nouvelle commande `dmstats` pour afficher et gérer des statistiques d'E/S pour des régions de périphériques, définies par utilisateurs, qui utilisent le pilote `device-mapper`

La commande `dmstats` fournit la prise en charge de l'espace utilisateur pour les statistiques d'E/S `device-mapper`. Ceci permet à un utilisateur de créer, gérer, et rapporter des compteurs d'E/S, des métriques et des données d'histogrammes de latence pour des régions arbitraires de périphériques `device-mapper`. Des champs de statistiques sont désormais disponibles dans les rapports `dmsetup` et la commande `dmstats` ajoute des modes de rapport spécialisés conçus pour une utilisation avec des informations statistiques. Pour obtenir des informations sur la commande `dmstats`, veuillez consulter la page `man dmstats(8)`.

### Prise en charge DIX sur matériel spécifié

SCSI T10 DIX est totalement pris en charge sur Red Hat Enterprise Linux 7.2 uniquement pour les HBA et matrices de stockage suivants, et non sur les LUN utilisés pour démarrer à partir d'un environnement SAN. En outre, T10 DIX est pris en charge sur RHEL 7 uniquement sur le matériel natif, et non lors d'une exécution sur des invités virtualisés.

\* EMULEX LPe16000/LPe16002

\* QLOGIC QLE2670/QLE2672

\* FUJITSU ETERNUS DX100 S3

\* FUJITSU ETERNUS DX200 S3

\* FUJITSU ETERNUS DX500 S3

\* FUJITSU ETERNUS DX600 S3

\* FUJITSU ETERNUS DX8100 S3

\* FUJITSU ETERNUS DX8700 S3

\* FUJITSU ETERNUS DX8900 S3

\* FUJITSU ETERNUS DX200F

\* FUJITSU ETERNUS DX60 S3

La prise en charge de DIX continue de faire partie des aperçus technologique pour les autres HBA et matrices de stockage.

Remarquez que T10 DIX requiert une base de données ou un autre logiciel permettant de générer et vérifier des checksums sur blocs de disque. Aucun système de fichiers Linux actuellement pris en charge n'offre cette capacité.

## Cache LVM

Le cache LVM est totalement pris en charge depuis Red Hat Enterprise Linux 7.1. Cette fonctionnalité permet aux utilisateurs de créer des volumes logique (VL) avec un périphérique rapide et de petite taille utilisé en tant que cache pour des périphériques plus lents et de plus grande taille. Veuillez consulter la page de manuel `lvmcache(7)` pour obtenir des informations sur la création de volumes logiques cache.

Veuillez remarquer les restrictions suivantes lors de l'utilisation de VL de caches :

\* Le VL du cache doit être un périphérique du niveau le plus haut niveau. Il ne peut pas être utilisé en tant que VL de pool fin, image de VL RAID, ou comme tout autre type de sous-volume logique.

\* Les sous-volumes logiques du VL du cache (le VL d'origine, le VL des métadonnées, et le VL des données) peut être de type linéaire, par bandes, ou RAID.

\* Les propriétés du VL du cache ne peuvent pas être modifiées après leur création. Pour modifier les propriétés du cache, supprimez le cache comme décrit dans `lvmcache(7)` puis recréez-le avec les propriétés souhaitées.

## Nouvelle politique du cache LVM/DM

Une nouvelle politique `dm-cache smq` a été écrite , elle réduit la consommation de mémoire et améliore les performances dans la plupart des cas d'utilisation. Celle-ci est désormais la politique par défaut du cache pour les nouveaux volumes logiques de cache LVM. Les utilisateurs préférant utiliser la politique héritée `mq` peuvent le faire en fournissant l'argument `-cachepolicy` lors de la création du volume logique du cache.

## ID système de LVM

Les groupes de volumes LVM peuvent désormais se voir assigner un propriétaire. Le propriétaire du groupe de volumes est l'ID système d'un hôte. Seul l'hôte avec l'ID système donné peut utiliser le groupe de volumes. Ceci est bénéfique aux groupes de volumes existants sur des périphériques partagés, visibles à de multiples hôtes, qui autrement ne seraient pas protégés d'une utilisation en conjonction à partir de multiples hôtes. Les groupes de volumes LVM sur périphériques partagés avec un ID système assigné sont détenus par un hôte et protégés des autres hôtes.

## Chapitre 13. Gestion du système et des abonnements

### Désormais, PowerTOP respecte les noms de fichier des rapports définis par les utilisateurs

Auparavant, les noms de fichier des rapports PowerTOP étaient générés d'une manière peu claire et non documentée. Avec cette mise à jour, l'implémentation a été améliorée, et les noms de fichier générés respectent désormais les noms requis par l'utilisateur. Ceci s'applique aux rapports CSV et HTML.

### Commandes yum-config-manager modifiées

Auparavant, l'exécution de la commande **yum-config-manager --disable** désactivait tous les référentiels configurés, tandis que la commande **yum-config-manager --enable** n'en activait aucun. Cette incohérence a été corrigée. Les commandes **--disable** et **--enable** requièrent désormais l'utilisation de « \\* » dans la syntaxe, et **yum-config-manager --enable \\*** active les référentiels. L'exécution des commandes sans ajouter « \\* » imprime un message demandant à l'utilisateur d'exécuter **yum-config-manager --disable \\*** ou **yum-config-manager --enable \\*** s'il souhaite activer ou désactiver des référentiels.

### Nouveau greffon search-disabled-repos pour yum

Le greffon `search-disabled-repos` pour yum a été ajouté aux paquets `subscription-manager`. Ce greffon permet aux utilisateurs d'effectuer avec succès des opérations yum complètes qui échouaient dû au fait que le référentiel source est dépendant d'un référentiel désactivé. Lorsque `search-disabled-repos` est installé dans le scénario décrit, yum affiche des instructions pour activer temporairement des référentiels désactivés et rechercher des dépendances manquantes. Une fois les modifications nécessaires au fichier `/etc/yum/pluginconf.d/search-disabled-repos.conf` effectuées, l'opération yum peut être reprise, avec les référentiels désactivés utilisés comme s'ils avaient été activés.

## Chapitre 14. Virtualisation

### Des bus root PCI supplémentaires sont désormais pris en charge en utilisant les périphériques de pont PCI expander

Contrairement aux ponts PCI-PCI, un bus sur un pont PCI expander peut être associé à un nœud NUMA, permettant au système d'exploitation invité de reconnaître la proximité d'un périphérique avec la RAM et les CPU. Avec cette mise à jour, les périphériques assignés peuvent être associés à leur nœud NUMA correspondant, se traduisant ainsi par des performances optimales.

### qemu-kvm prend en charge les événements de trace de fermeture de machine virtuelle (« virtual machine shutdown trace events »)

La prise en charge des événements de trace qemu-kvm pendant le processus de fermeture des systèmes de machines virtuelles a été ajoutée, ce qui permet aux utilisateurs d'obtenir le diagnostic détaillé des requêtes de fermeture d'un système invité ordonnées par la commande **virsh shutdown** ou par l'application virt-manager. Cela fournit aux utilisateurs des capacités améliorées pour isoler et déboguer les problèmes des invités KVM pendant la fermeture.

### Intel MPX exposé à l'invité

Avec cette mise à jour, qemu-kvm permet à la fonctionnalité MPX (« Intel Memory Protection Extensions ») d'être exposée à l'invité. Sur les systèmes hôtes Intel 64 qui prennent en charge MPX, ceci permet d'utiliser un ensemble d'extensions qui fournissent la prise en charge du matériel pour la protection de bornes sur les références de pointeurs.

### Extraction du vidage de mémoire de l'invité à partir du cœur qemu-kvm

Le script `dump-guest-memory.py` a été introduit dans QEMU, ce qui rend possible l'analyse d'un vidage mémoire d'un invité à partir d'un cœur de qemu-kvm en cas d'échec du noyau d'un invité. Pour obtenir davantage d'informations, veuillez consulter le texte d'aide en utilisant la commande **help dump-guest-memory**.

### Prise en charge complète de virt-v2v

Avec Red Hat Enterprise Linux 7.2, l'outil de ligne de commande virt-v2v est complètement pris en charge. Cet outil convertit les machines virtuelles exécutées sur des hyperviseurs étrangers pour les exécuter sur KVM. Actuellement, virt-v2v peut convertir des invités Red Hat Enterprise Linux et Windows exécutés sur Red Hat Enterprise Linux 5 Xen et VMware vCenter.

### Virtualisation sur IBM Power Systems

Red Hat Enterprise Linux avec KVM est pris en charge sur les systèmes AMD64 et Intel 64, mais pas sur IBM Power Systems. Red Hat offre actuellement une solution basée POWER8 avec Red Hat Enterprise Virtualization pour IBM Power Systems.

Davantage d'informations sur la prise en charge des versions et sur les procédures d'installation se trouvent dans l'article de base des connaissances suivant : <https://access.redhat.com/articles/1247773>

### Prise en charge VirtIO-1

Les pilotes Virtio ont été mis à jour avec le noyau 4.1 pour offrir la prise en charge de périphériques VirtIO 1.0.

### **Prise en charge Hyper-V TRIM**

Il est désormais possible d'utiliser des VHDX d'allocation fine et dynamique (« Thin Provisioned Hyper-V virtual hard disk »). La mise à jour ajoute la prise en charge pour réduire la taille des fichiers VHDX sous-jacents pour les machines virtuelles Microsoft Hyper-V à la taille réellement utilisée.

## Chapitre 15. Red Hat Software Collections

Red Hat Software Collections est un ensemble de contenus Red Hat fournissant des langages de programmation dynamiques, des serveurs de base de données et des paquets liés pouvant être installés et utilisés sur toutes les versions prises en charge de Red Hat Enterprise Linux 6 et Red Hat Enterprise Linux 7 sur architectures AMD64 et Intel 64.

Les langages dynamiques, serveurs de bases de données, et autres outils distribués avec les Red Hat Software Collections ne remplacent pas les outils système par défaut fournis avec Red Hat Enterprise Linux, et ne sont pas utilisés de manière préférentielle à ces outils. Les Red Hat Software Collections utilisent un mécanisme d'empaquetage alternatif basé sur l'utilitaire **sc1** pour fournir un ensemble parallèle de paquets. Cet ensemble permet l'utilisation optionnelle de versions de paquets alternatives sur Red Hat Enterprise Linux. En utilisant l'utilitaire **sc1**, les utilisateurs peuvent sélectionner la version du paquet qu'ils souhaitent exécuter à tout moment.

Red Hat Developer Toolset fait désormais partie de Red Hat Software Collections, et est inclus en tant que collection de logiciels (« Software Collection ») séparée. Red Hat Developer Toolset est conçu pour les développeurs travaillant sur la plateforme Red Hat Enterprise Linux. Cet ensemble fournit les versions actuelles de GNU Compiler Collection, GNU Debugger, la plateforme de développement Eclipse, ainsi que d'autres outils de développement, de débogage et de surveillance des performances.



### Important

Les logiciels des « Red Hat Software Collections » possèdent un cycle de vie et une durée de prise en charge plus courts que Red Hat Enterprise Linux. Pour obtenir des informations supplémentaires, veuillez consulter le [Cycle de vie du produit Red Hat Software Collections](#).

Voir la [Documentation Red Hat Software Collections](#) pour les composants inclus dans l'ensemble, les conditions nécessaires du système, problèmes connus, utilisation et les particularités de chaque collection de logiciels.

Voir la [Documentation Red Hat Developer Toolset](#) pour obtenir davantage d'informations sur les composants inclus dans cette collection de logiciels, l'installation, l'utilisation, les problèmes connus, et plus encore.

## Partie II. Aperçus technologiques

Cette partie offre une vue d'ensemble des aperçus technologiques présentés ou mis à jour sur Red Hat Enterprise Linux 7.2.

Pour obtenir davantage d'informations sur les aperçus technologiques Red Hat, veuillez consulter <https://access.redhat.com/support/offerings/techpreview/>.



## Chapitre 16. Authentification

### Utilisation des fournisseurs sudo AD et LDAP

Le fournisseur « Active Directory » (AD) est un backend utilisé pour se connecter à un serveur AD. Dans Red Hat Enterprise Linux 7.2, l'utilisation du fournisseur sudo AD en conjonction avec le fournisseur LDAP est prise en charge en tant qu'aperçu technologique. Pour activer le fournisseur sudo AD, veuillez ajouter le paramètre **sudo\_provider=ad** dans la section [domain] du fichier **sssd.conf**.

## Chapitre 17. Systèmes de fichiers

### OverlayFS

OverlayFS est un type de système de fichiers d'union. Il permet à l'utilisateur de couvrir (« **overlay** ») un système de fichiers par un autre. Les changements sont enregistrés sur le système de fichiers du haut, tandis que le celui du bas reste inchangé. Ceci permet à de multiples utilisateurs de partager une image système de fichiers, comme un conteneur ou un DVD-ROM, où l'image de base est un support de lecture seule. Veuillez consulter le fichier du noyau Documentation/filesystems/overlayfs.txt pour obtenir des informations supplémentaires.

OverlayFS reste un aperçu technologique sur Red Hat Enterprise Linux 7.2 dans la plupart des cas. Ainsi, le noyau journalisera des avertissements lorsque cette technologie est activée.

Une prise en charge complète est disponibles pour OverlayFS lorsqu'utilisé avec Docker avec les restrictions suivantes :

- \* OverlayFS est uniquement pris en charge pour une utilisation en tant que pilote de graphe Docker. Son utilisation peut uniquement être prise en charge pour les contenus COW de conteneur, et non pour le stockage persistant. Pour être pris en charge, tout stockage persistant doit être placé sur des volumes non OverlayFS. Seule la configuration Docker par défaut peut être utilisée, c'est-à-dire un niveau de couverture overlay, un lowerdir, et les niveaux inférieurs et supérieurs se trouvent sur le même système de fichiers.
- \* Seul XFS est actuellement pris en charge pour une utilisation en tant que système de fichiers de la couche inférieure.
- \* SELinux doit être activé et en mode enforcing sur la machine physique, mais doit être désactivé dans le conteneur lorsque la séparation des conteneurs est en cours. Autrement dit, /etc/sysconfig/docker ne doit pas contenir --selinux-enabled. La prise en charge SELinux de OverlayFS est en cours de développement en amont, et devrait être incluse dans une future version.
- \* L'ABI du noyau OverlayFS et le comportement de l'espace utilisateur ne sont pas considérés comme étant stables, et observeront des changements dans de futures mises à jour.

Remarquez qu'OverlayFS fournit un ensemble restreint de standards POSIX. Testez minutieusement votre application avant de la déployer avec OverlayFS.

Il existe également plusieurs problèmes connus associés à OverlayFS depuis la sortie de Red Hat Enterprise Linux 7.2. Pour obtenir des détails, veuillez consulter **Non-standard behavior** (« Comportement non standard ») dans le fichier Documentation/filesystems/overlayfs.txt.

### Prise en charge des clients NFSv4 avec structure de fichier flexible

Red Hat Enterprise Linux 7.2 ajoute la prise en charge de structures de fichiers flexible sur clients NFSv4. Cette technologie active des fonctionnalités avancées comme la mobilité de fichiers non perturbatrice, la mise en miroir côté client, fournissant une convivialité améliorée dans des domaines tels que les bases de données, le Big Data, ou la virtualisation.

Veuillez consulter <https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/> pour obtenir des informations détaillées sur la structure de fichiers flexible NFS.

### NFS sur RDMA

Le service NFSoRDMA est fourni en tant qu'aperçu technologique pour Red Hat Enterprise Linux 7.2. Ceci fait que le module svcrdma est disponible pour les utilisateurs qui comptent utiliser le transport RDMA (« Remote Direct Memory Access ») avec le serveur NFS Red Hat Enterprise Linux 7.

## Système de fichier Btrfs

Le système de fichiers Btrfs (B-Tree) est pris en charge en tant qu'aperçu technologique sur Red Hat Enterprise Linux 7.2. Ce système de fichiers offre des fonctionnalités de gestion, de fiabilité et d'évolutivité avancées. Il permet aux utilisateurs de créer des instantanés et autorise la compression et une gestion des périphériques intégrée.

## Chapitre 18. Activation du matériel

### Prise en charge des cartes OSA-Express5s sur qethqoat

La prise en charge des cartes OSA-Express5s a été ajoutée à l'outil qethqoat, qui fait partie du paquet s390utils. Cette amélioration étend l'entretien des installations de réseaux et de cartes pour des cartes OSA-Express5s, et est incluse en tant qu'aperçu technologique dans Red Hat Enterprise Linux 7.2 sur IBM System z.

### Instrumentation du runtime pour IBM System z

La prise en charge de la fonctionnalité d'instrumentation du runtime est disponible en tant qu'aperçu technologique dans Red Hat Enterprise Linux 7.2 sur IBM System z. L'instrumentation du runtime permet l'analyse et l'exécution avancée d'un certain nombre d'application de l'espace utilisateur disponibles avec le système IBM zEnterprise EC12.

### Adaptateurs HA-DAS LSI Syncro CS

Red Hat Enterprise Linux 7.1 inclut un code dans le pilote megaraid\_sas pour activer les adaptateurs haute disponibilité de stockage attaché directement (HA-DAS) LSI Syncro CS. Malgré que le pilote megaraid\_sas soit complètement pris en charge pour les adaptateurs précédemment activés, l'utilisation de ce pilote pour Syncro CS est disponible en tant qu'aperçu technologique. La prise en charge de cet adaptateur est directement offerte par LSI, votre intégrateur système ou fournisseur système. Les utilisateurs déployant Syncro CS sur Red Hat Enterprise Linux 7.2 sont encouragés à donner leur avis à Red Hat et LSI. Pour obtenir davantage d'informations sur les solutions LSI Syncro CS, veuillez visiter <http://www.lsi.com/products/shared-das/pages/default.aspx>.

## Chapitre 19. Noyau

### Prise en charge de multiples CPU dans kdump sur systèmes AMD64 et Intel 64

Sur les systèmes AMD64 et Intel 64, le mécanisme de vidage sur incident du noyau **kdump** peut désormais démarrer avec plus d'un CPU activé. Cela permet de résoudre un problème sur les systèmes à grande mémoire où, à cause du grand nombre d'entrées et sorties lors de la création d'un vidage sur incident noyau, Linux pour échouer lors de l'allocation d'interruptions de périphériques lorsqu'un seul CPU était activé (« `maxcpus=1` » ou `nr_cpus=1`).

Pour activer de multiples CPU dans le noyau des incidents, veuillez fournir les options `nr_cpus=X` (où **X** est le nombre de processeurs) et `disable_cpu_apicid=0` sur la ligne de commande du noyau.

### L'outil criu

Red Hat Enterprise Linux 7.2 présente l'outil **criu** en tant qu'aperçu technologique. Cet outil implémente **Checkpoint/Restore in User-space**, qui peut être utilisé pour geler une application en cours d'exécution et la stocker en tant que collection de fichiers. L'application peut être restaurée de son état gelé ultérieurement.

L'outil **criu** dépend des **Protocol Buffers**, un mécanisme extensible neutre quant aux langues et plateformes servant à sérialiser des données structurées. Les paquets *protobuf* et *protobuf-c*, qui fournissent cette dépendance, sont également ajoutés à Red Hat Enterprise Linux 7.2 en tant qu'aperçu technologique.

### Espace de noms de l'utilisateur

Cette fonctionnalité offre une sécurité supplémentaire aux serveurs exécutant des conteneurs Linux en fournissant une meilleure isolation entre l'hôte et les conteneurs. Les administrateurs d'un conteneur ne sont plus en mesure d'effectuer des opérations administratives sur l'hôte, ce qui améliore la sécurité.

### Chien de garde LPAR pour IBM System z

Un pilote chien de garde amélioré pour IBM System z est disponible en tant qu'aperçu technologique. Ce pilote prend en charge les partitions logiques Linux (LPAR) ainsi que les invités Linux dans l'hyperviseur z/VM, et offre des capacités de redémarrage automatique et de vidage automatique si un système Linux ne répond plus.

### Mises à jour dynamiques du noyau avec kpatch

L'utilitaire **kpatch** permet aux utilisateurs de gérer une collection de correctifs de noyau binaires qui peuvent être utilisés pour corriger le noyau dynamiquement sans avoir à redémarrer. **kpatch** est pris en charge en tant qu'aperçu technologique et est uniquement disponible sur les architectures AMD64 et Intel 64.

### i40evf gère les réinitialisations de grande envergure

Le type de réinitialisation le plus commun rencontré par une Virtual Function (VF) est la réinitialisation d'une Physical Function (PF) qui provoque à son tour une réinitialisation de VF pour chaque VF. Cependant, pour les réinitialisations de plus grande envergure, comme les réinitialisations Core ou EMP, lorsque le périphérique est réinitialisé, la VF n'obtenait pas le même VSI. Ainsi la VF ne pouvait pas récupérer car elle continuait à requérir des ressources pour son VSI d'origine. En tant qu'aperçu technologique, cette mise à

jour ajoute un état supplémentaire à la machine d'états de file d'administration, de manière à ce que le pilote puisse requérir à nouveau ses informations de configuration pendant l'exécution. Pendant la récupération de la réinitialisation, cette partie est définie dans le champ `aq_required`, et les informations de configuration sont récupérées avant de tenter de réactiver le pilote.

## Chapitre 20. Mise en réseau

### Mise à jour du pilote de l'adaptateur de serveur ethernet Intel X710/XL710

Les pilotes de noyau i40e et i40evf ont été mis à jour à la version 1.3.4-k. Ces pilotes mis à jour sont inclus en tant qu'aperçu technologique dans Red Hat Enterprise Linux 7.2.

### Sortie ethtool précise

Les capacités de requête réseau de l'utilitaire ethtool ont été améliorées dans un aperçu technologique pour Red Hat Enterprise Linux 7.2 sur IBM System z. Par conséquent, lors de l'utilisation de matériel compatible avec les requêtes améliorées, ethtool offre des options de surveillance améliorées et affiche les paramètres de la carte réseau et les valeurs de manière plus précise.

### Pilote Cisco usNIC

Les serveurs Cisco UCM (« Unified Communication Manager ») possèdent une fonctionnalité optionnelle pour fournir un contrôleur d'interface réseau d'espace utilisateur Cisco (usNIC), qui permet d'effectuer des opérations de type RDMA (« Remote Direct Memory Access ») pour des applications de l'espace utilisateur. Le pilote libusnic\_verbs, qui est pris en charge en tant qu'aperçu technologique, permet d'utiliser des périphériques usNIC vis une programmation RDMA InfiniBand standard basées sur l'API Verbs.

### Pilote du noyau Cisco VIC

Le pilote du noyau Infiniband VIC de Cisco, pris en charge en tant qu'aperçu technologique, permet d'utiliser des sémantiques de type RDMA (« Remote Directory Memory Access ») sur des architectures Cisco.

### Trusted Network Connect

Trusted Network Connect, pris en charge en tant qu'aperçu technologique, est utilisé avec des solutions NAC (« Network Access Control »), telles que TLS, 802.1X, ou IPsec pour intégrer une évaluation de posture de point d'extrémité ; c'est-à-dire la collection des informations système d'un point d'extrémité (comme les paramètres de configuration du système d'exploitation, les paquets installés, et autres termes de mesure d'intégrité). Trusted Network Connect est utilisé pour vérifier ces mesures avec les politiques d'accès avant d'autoriser le point d'extrémité à accéder au réseau.

### Fonctionnalité SR-IOV dans le pilote qlcnic

La prise en charge SR-IOV (« Single-Root I/O virtualization ») a été ajoutée au pilote qlcnic en tant qu'aperçu technologique. La prise en charge de cette fonctionnalité sera fournie directement par QLogic, et les clients sont encouragés à donner leur avis à QLogic et Red Hat. Les autres fonctionnalités du pilote qlcnic restent complètement prises en charge.

## Chapitre 21. Stockage

### Planification d'E/S à files multiples pour SCSI

Red Hat Enterprise Linux 7.2 inclut un nouveau mécanisme de planification d'E/S à files multiples pour les périphériques bloc appelés blk-mq. Le paquet scsi-mq permet au sous-système SCSI (« Small Computer System Interface ») d'utiliser ce nouveau mécanisme de mise en file d'attente. Cette fonctionnalité est offerte en tant qu'aperçu technologique et n'est pas activée par défaut. Pour l'activer, veuillez ajouter `scsi_mod.use_blk_mq=Y` à la ligne de commande du noyau.

### Amélioration de l'infrastructure de verrouillage LVM

`lvmlockd` est une infrastructure de verrouillage de nouvelle génération pour LVM. Celle-ci permet à LVM de gérer le stockage partagé par de multiples hôtes en toute sécurité, en utilisant le gestionnaire de verrous `d1m` ou `sanlock`. `sanlock` permet à `lvmlockd` de coordonner des hôtes à travers un verrouillage basé stockage, sans avoir besoin d'une infrastructure de cluster complète. Pour obtenir davantage d'informations, veuillez consulter la page man ``lvmlockd``(8).

### Greffon Targetd de l'API libStorageMgmt

À partir de Red Hat Enterprise Linux 7.1, la gestion de matrices de stockage avec libStorageMgmt, une APO indépendant des matrices de stockage, est complètement prise en charge. L'API fournie est stable, cohérente, et permet aux développeurs de gérer par programmation différentes matrices de stockage et d'utiliser les fonctionnalités d'accélération matérielle fournies. Les administrateurs systèmes peuvent également utiliser libStorageMgmt pour configurer manuellement le stockage et pour automatiser les tâches de gestion du stockage avec l'interface de ligne de commande incluse.

Le greffon Targetd n'est pas totalement prise en charge et reste un aperçu technologique.

### DIF/DIX

DIF/DIX est un nouvel ajout au standard SCSI. Il est complètement pris en charge dans Red Hat Enterprise Linux 7.2 pour les HBA et les matrices de stockage spécifiés dans le chapitre Fonctionnalités, mais DIF/DIX reste un aperçu technologique pour tous les autres HBA et matrices de stockage.

DIF/DIX augmente la taille de bloc de disque habituelle de 512 octets à 520 octets, ajoutant le DIF (« Data Integrity Field »). Le DIF stocke une valeur de checksum pour le bloc de données qui est calculé par l'adaptateur de bus hôte (HBA, de l'anglais « Host Bus Adapter ») lorsqu'une opération d'écriture se produit. Puis, le périphérique de stockage confirme le checksum à la réception et stocke les données et le checksum. Similairement, lorsqu'une opération d'écriture se produit, le checksum peut être vérifié par le périphérique de stockage et par le HBA de réception.

### Cible dm-era device-mapper

Red Hat Enterprise Linux 7.1 présente la cible du mappeur de périphériques dm-era en tant qu'aperçu technologique. dm-era conserve une trace des blocs écrits pendant une période définie par l'utilisateur, nommée une **era** (une « ère »). Chaque instance d'ère cible maintient l'ère actuelle comme compteur 32 bits augmentant de manière monotone. Cette cible permet au logiciel de sauvegarde de vérifier quels blocs ont été modifiés depuis la dernière sauvegarde. Elle permet aussi d'effectuer une invalidation partielle du contenu d'un cache pour restaurer la cohérence du cache après avoir restauré selon l'instantané du revendeur. Il est principalement prévu que la cible dm-era soit couplée avec la cible dm-cache.



## Chapitre 22. Virtualisation

### Virtualisation imbriquée

Red Hat Enterprise Linux 7.2 offre la fonctionnalité de virtualisation imbriquée en tant qu'aperçu technologique. Celle-ci permet l'utilisation d'invités KVM-QEMU en tant qu'hôtes, permettant ainsi à l'utilisateur de créer des invités dans ces invités.

### L'outil virt-p2v

Red Hat Enterprise Linux 7.2 offre l'outil virt-p2v en tant qu'aperçu technologique. Virt-p2v (physique à virtuel) est un CD-ROM, une image ISO ou PXE que l'utilisateur peut lancer sur une machine physique, et qui convertit la machine physique en machine virtuelle exécutée sur KVM.

### Prise en charge d'USB 3.0 pour les invités KVM

L'émulation d'un adaptateur hôte USB 3.0 (xHCI) pour les invités KVM reste un aperçu technologique sur Red Hat Enterprise Linux 7.2.

## Partie III. Pilotes de périphériques

Ce chapitre offre la liste complète de tous les pilotes de périphériques qui ont été mis à jour dans Red Hat Enterprise Linux 7.2.

## Chapitre 23. Mise à jour des pilotes de stockage

- ✧ Le pilote hpsa a été mis à jour à la version 3.4.4-1-RH4.
- ✧ Le pilote qla2xxx a été mis à jour à la version 8.07.00.18.07.2-k.
- ✧ Le pilote lpfc a été mis à jour à la version 10.7.0.1.
- ✧ Le pilote megaraid\_sas a été mis à jour à la version 06.807.10.00.
- ✧ Le pilote fnic a été mis à jour à la version 1.6.0.17
- ✧ Le pilote mpt2sas a été mis à jour à la version 20.100.00.00.
- ✧ Le pilote mpt3sas a été mis à jour à la version 9.100.00.00.
- ✧ Le pilote Emulex be2iscsi a été mis à jour à la version 10.6.0.0r.
- ✧ Le pilote aacraid a été mis à jour à la version 1.2.
- ✧ Le pilote bnx2i a été mis à jour à la version 2.7.10.1.
- ✧ Le pilote bnx2fc a été mis à jour à la version 2.4.2.

## Chapitre 24. Mise à jour des pilotes réseau

- ✦ Le pilote tg3 a été mis à jour à la version 3.137.
- ✦ Le pilote e1000 a été mis à jour à la version 7.3.21-k8-NAPI, qui fournit la prise en charge du délai de mise à jour txtd lors de l'utilisation de la variable booléenne xmit\_more.
- ✦ Le pilote e1000e a été mis à jour à la version 2.3.2-k.
- ✦ Le pilote igb a été mis à jour à la version 5.2.15-k.
- ✦ Le pilote igbvf a été mis à jour à la version 2.0.2-k.
- ✦ Le pilote ixgbev f a été mis à jour à la version 2.12.1-k.
- ✦ Le pilote ixgbe a été mis à jour à la version 4.0.1-k.
- ✦ Le pilote et le microprogramme bna ont été mis à jour à la version 3.2.23.0r.
- ✦ Le pilote bnx2 a été mis à jour à la version 2.4.2.
- ✦ Le pilote CNIC a été mis à jour à la version 2.5.21.
- ✦ Le pilote bnx2x a été mis à jour à la version 1.710.51-0, qui ajoute également la prise en charge qlogic NPAR des adaptateurs qlogic-nx2.
- ✦ Le pilote be2net a été mis à jour à la version 10.6.0.2.
- ✦ Le pilote bna a été mis à jour à la version 3.2.23.0r.
- ✦ Le pilote qlcnic a été mis à jour à la version 5.3.62.
- ✦ Le pilote qlge a été mis à jour à la version 1.00.00.34, qui corrige également une condition de race entre l'enregistrement NAPI (« New API ») et le désenregistrement qui entraînait auparavant des pannes système, cela se produisait si certains paramètres étaient modifiés pendant que la carte de l'interface réseau (NIC) était paramétrée sur « down ».
- ✦ Le pilote r8169 a été mis à jour à la version 2.3LK-NAPI.
- ✦ Les pilotes i40e et i40evf ont été mis à jour à la version 1.3.4-k.
- ✦ Le pilote netxen\_nic a été mis à jour à la version 4.0.82.
- ✦ Le pilote sfc a été mis à jour à la version en amont la plus récente.
- ✦ Cette mise à jour ajoute le pilote fm10k version 0.15.2-k.
- ✦ Cette mise à jour ajoute la prise en charge VT16 y compris des capacités netns.
- ✦ Le pilote de liaison a été mis à jour à la version 3.7.1.
- ✦ Le pilote iwlwifi a été mis à jour à la version en amont la plus récente.
- ✦ Le pilote vxlan a été mis à jour à la version 0.1.

## Chapitre 25. Mises à jour des pilotes graphiques et de pilotes divers

- ✦ Le pilote HDA a été mis à jour à la version en amont la plus récente afin de permettre l'utilisation de la nouvelle méthode jack kctls.
- ✦ Le pilote HPI a été mis à jour à la version 4.14.
- ✦ Le pilote Realtek HD-audio codec a été mis à jour afin d'inclure la mise à jour des codes init EAPD.
- ✦ Le pilote IPMI a été mis à jour pour remplacer l'utilisation de timespec par timespec64.
- ✦ Le pilote i915 a été mis à jour pour inclure le rebaselement du pilote d'extensions ACPI Video sur Red Hat Enterprise Linux 7.2.
- ✦ Le pilote ACPI Fan a été mis à jour à la version 0.25.
- ✦ Le pilote Update NVM-Express a été mis à jour à la version 3.19.
- ✦ Le pilote rtsx a été mis à jour à la version 4.0 pour prendre en charge les puces rtl8402, rts524A, rts525A.
- ✦ Le pilote de périphérique Generic WorkQueue Engine a été mis à jour à la version en amont la plus récente.
- ✦ Le pilote PCI a été mis à jour à la version 3.16.
- ✦ Le module du noyau EDACa été mis à jour afin de fournir la prise en charge des processeurs Intel Xeon v4.
- ✦ Le pilote pstate a été mis à jour pour prendre en charge les processeurs Intel Core 6th Generation.
- ✦ Le pilote intel\_idle a été mis à jour pour prendre en charge les processeurs Intel Core 6th Generation.

## **Partie IV. Problèmes connus**

Cette partie offre documente les problèmes connus sur Red Hat Enterprise Linux 7.2.

## Chapitre 26. Compilateur et outils

### Multiple bogues pendant les démarrages à partir de SAN sur FCoE

De multiples bogues se sont produits dans l'implémentation actuelle du démarrage à partir du SAN (« Storage Area Network ») utilisant FCoE (« Fibre Channel over Ethernet »). Red Hat cible une future version de Red Hat Enterprise Linux 7 pour les correctifs de ces bogues. Pour une liste des bogues affectés et des solutions de contournement (lorsque disponible), veuillez contacter votre représentant du support technique de Red Hat.

### Valgrind ne peut pas exécuter de programmes créés sur une version antérieure d'Open MPI

Red Hat Enterprise Linux 7.2 prend uniquement en charge la version 1.10 de l'interface binaire d'application (« application binary interface », ou ABI) Open MPI, qui est incompatible avec la version précédemment fournie de l'ABI Open MPI 1.6. Par conséquent, les programmes créés avec l'ancienne version d'Open MPI ne peuvent pas être exécutés sous Valgrind, y compris sur Red Hat Enterprise Linux 7.2. Pour contourner ce problème, veuillez utiliser la version Red Hat Developer Toolset de Valgrind pour les programmes liés à Open MPI version 1.6.

## Chapitre 27. Bureau

### Des dépendances manquantes du paquet `pygobject3` empêchent la mise à niveau de Red Hat Enterprise Linux 7.1

Le paquet `pygobject3-devel.i686` 32 bits a été supprimé de Red Hat Enterprise Linux 7.2 et remplacé par une version multilib. Si vous avez la version 32 bits du paquet installée sur un système Red Hat Enterprise Linux 7.1, vous rencontrerez une erreur `yum` lorsque vous tenterez de mettre à niveau vers Red Hat Enterprise Linux 7.2.

Pour contourner ce problème, veuillez utiliser la commande `yum remove pygobject3-devel.i686` en tant qu'utilisateur `root` pour désinstaller la version 32 bits du paquet avant de mettre à niveau votre système.



## Chapitre 28. Mises à jour générales

### Les noms des nouveaux périphériques assignés peuvent perturber les connexions réseau

Auparavant, assigner des noms d'interfaces réseau stables à des périphériques virtio était impossible car l'ordre d'énumération de ces périphériques était imprévisible. Avec ce correctif, il n'existe qu'un seul périphérique PCI parent par bus virtio, et les périphériques réseau virtio possèdent maintenant des noms de périphérique persistants dans les machines virtuelles (selon <http://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>).

Veillez remarquer qu'après avoir mis à jour systemd et redémarré la machine virtuelle, dont les noms d'interface provenaient auparavant d'un espace de nom de noyau (eth0, eth1,...), de nouveaux noms de périphériques seront assignés lors du démarrage, ce qui peut perturber la connexion réseau à la machine virtuelle.

## Chapitre 29. Installation et démarrage

### L'installation en mode texte ne tombe plus en panne pendant la configuration réseau

Auparavant, dans l'écran de configuration réseau de l'installateur en mode texte interactif, l'utilisation d'un espace lors de la spécification des serveurs de noms provoquait la panne de l'installateur.

Désormais, Anaconda gère correctement les espaces dans les définitions de serveurs de noms en mode texte, et l'installateur ne tombe plus en panne si un espace est utilisé pour séparer les adresses des serveurs de noms.

### Possible message d'erreur de NetworkManager pendant l'installation

Pendant une installation, le message d'erreur suivant peut s'afficher :

```
ERR NetworkManager: <error> [devices/nm-device.c:2590] activation_source_schedule(): (eth0): activation stage already scheduled
```

À l'heure actuelle, aucune solution de contournement n'existe pour ce bogue.

### L'installation Atomic Host offre cryptsetup même s'il n'est pas disponible

Pendant l'installation de Red Hat Enterprise Linux 7 Atomic Host, l'installateur offre l'option de chiffrer les partitions en utilisant **cryptsetup** dans l'écran de partitionnement manuel, de la même manière que cela est offert pendant une installation Red Hat Enterprise Linux 7.2.

Cependant, les partitions chiffrées ne sont pas prises en charge sur Atomic Host. Si vous chiffrez une partition pendant l'installation, vous ne pourrez pas la déverrouiller.

Pour contourner ce problème, veuillez ne pas chiffrer de partition ou de volume logique pendant une installation Red Hat Enterprise Linux Atomic Host, même si l'installateur vous présente cette option.

### L'installateur peut uniquement ajouter un stockage avancé la première fois que le rayon du stockage est saisi

Pendant une installation interactive utilisant l'interface graphique Anaconda, l'ajout de stockage avancé (iSCSI, zFCP, FCoE) à votre sélection de disque ne fonctionnera pas si vous avez déjà saisi et quitté le rayon du stockage (« storage spoke »). Pour contourner le problème, veuillez vous assurer que le réseau, si nécessaire, est actif puis saisissez le rayon du stockage et ajoutez tous les périphériques de stockage avancé.

## Chapitre 30. Noyau

### Certains systèmes de fichiers ext4 ne peuvent pas être redimensionnés

À cause d'un bogue dans le code ext4, il est actuellement impossible de redimensionner les systèmes de fichiers ext4 dont la taille de bloc est de 1 kilo-octet et qui font moins de 32 méga-octets.

### Perte de connexion répétée avec des cibles iSCSI activées iSER

Lors de l'utilisation du serveur en tant que cible iSCSI activée iSER, des pertes de connexion se produisent de manière répétée, la cible peut arrêter de répondre et le noyau ne réagit plus. Pour contourner ce problème, minimiser les pertes de connexion iSER ou rétablir le mode iSCSI sans iSER.

### Commande d'E/S d'appels mid-layer SCSI jusqu'à ce que la fermeture forcée du système

Lorsqu'une matrice de stockage retourne un statut CHECK CONDITION mais que les données sense sont invalides, le code mid-layer iSCSI (« Small Computer Systems Interface ») tentera à nouveau d'effectuer l'opération d'E/S. Si les opérations d'E/S consécutives reçoivent le même résultat, SCSI continuera de tenter d'effectuer l'opération d'E/S indéfiniment. Aucune solution de contournement n'est actuellement disponible pour ce bogue.

### Le certificat de la clé publique Red Hat Beta doit être chargé manuellement

L'administrateur système peut utiliser le mécanisme MOK (« Machine Owner Key ») pour charger le certificat correspondant de la clé publique Red Hat Beta, qui est nécessaire pour authentifier le noyau inclut dans une version Red Hat Enterprise Linux Beta. L'inscription de la clé publique Beta de Red Hat CA (« Certificate Authority ») est une procédure unique pour tout système sur lequel Red Hat Enterprise Linux 7.2 Beta sera exécuté avec le démarrage sécurisé UEFI (« UEFI Secure Boot ») activé :

1. Éteignez UEFI Secure Boot et installez Red Hat Enterprise Linux 7.2 Beta.
2. Installez le paquet kernel-doc s'il n'est pas déjà installé. Il fournit un fichier de certificat qui contient la clé publique Beta de Red Hat CA dans le fichier : `/usr/share/doc/kernel-keys/<kernel-ver>/kernel-signing-ca.cer`, où `<kernel-ver>` est la chaîne de version du noyau sans le suffixe de l'architecture de la plateforme. Par exemple, `3.10.0-314.el7`.
3. Faites une requête manuelle d'inscription de la clé publique sur la liste MOK (« Machine Owner Key ») sur le système en utilisant l'utilitaire mokutil. Veuillez exécuter la commande suivante en tant qu'utilisateur root :

```
mokutil --import /usr/share/doc/kernel-keys/<kernel-ver>/kernel-signing-ca.cer
```

Il vous sera demandé de fournir un mot de passe pour la requête d'inscription.

4. Lors du prochain redémarrage du système, il vous sera demandé de terminer l'inscription de la requête MOK sur la console système. Vous devrez répondre aux invites et fournir le mot de passe fourni à mokutil dans l'étape 3.
5. Lorsque l'inscription MOK est terminée, le système sera réinitialisé et redémarrera. Vous pouvez réactiver le démarrage sécurisé « UEFI Secure Boot » lors de ce redémarrage, ou lors de tout autre redémarrage du système.

## Chapitre 31. Mise en réseau

### La politique de délai d'expiration n'est pas activée sur le noyau Red Hat Enterprise Linux 7.2

La commande `nfct timeout` n'est pas prise en charge sur Red Hat Enterprise Linux 7.2. Pour une solution de contournement, veuillez utiliser les valeurs d'expiration globales disponibles sur `/proc/sys/net/netfilter/nf_conntrack_*_timeout_*` pour définir les valeurs de délai d'expiration.

## Chapitre 32. Gestion du système et des abonnements

### Enregistrement incomplet en cas d'erreur

Lors de l'enregistrement d'un système dans l'interface utilisateur du gestionnaire des abonnements « Subscription Manager », si l'enregistrement échoue, la fenêtre principale de l'enregistrement ne se ferme pas lorsque l'utilisateur clique sur **Valider** dans la boîte de dialogue de l'erreur. Par conséquent, la fenêtre principale de l'enregistrement reste ouverte dans un état où la tâche ne peut pas être menée à bien. Ce problème se produit, par exemple, lorsque l'utilisateur fournit des informations d'identification invalides, ou lorsque « Auto-attach » est utilisé pour l'enregistrement. Pour contourner ce problème, veuillez cliquer sur le bouton **Annuler** dans la fenêtre principale de l'enregistrement si une erreur se produit pendant le processus.

### Le bouton Précédent (« Back ») du module complémentaire « Subscription Manager » de « Initial Setup » ne fonctionne pas

Le bouton **Précédent** du premier panneau du module complémentaire « Subscription Manager » de l'utilitaire « Initial Setup » ne fonctionne pas. Pour contourner ce problème, veuillez cliquer sur **Terminé** (« Done ») en haut de « Initial Setup » pour quitter le flux de travail de l'enregistrement.

## Chapitre 33. Virtualisation

### Parcourir GRUB 2 avec KVM est problématique

Lors de l'utilisation de la console série via KVM, maintenez une touche flèche enfoncée pendant un certain temps pour parcourir les résultats du menu GRUB 2 de manière erratique. Pour contourner ce problème, évitez une saisie trop rapide en maintenant une touche flèche enfoncée pendant plus longtemps.

### Le redimensionnement de disques GPT (« GUID Partition Table ») sur invités Hyper-V provoque des erreurs de table de partition

Le gestionnaire Hyper-V prend en charge la réduction d'un disque partitionné avec GPT sur un invité s'il existe suffisamment d'espace libre après la dernière partition, en permettant à l'utilisateur d'abandonner la dernière partie inutilisée du disque. Cependant, cette opération supprimera silencieusement l'en-tête GPT secondaire, ce qui peut déclencher des messages d'erreur lorsque l'invité examine la table de partition (par exemple avec `parted(8)`). Ceci est une limite connue de Hyper-V.

Pour contourner ceci, il est possible de restaurer manuellement l'en-tête GPT secondaire avec la commande expert `gdisk(8) e`, après avoir réduit le disque GPT. Ceci se produit également lors de l'utilisation de l'option Hyper-V Expand, mais peut aussi être corrigé avec l'outil `parted(8)`.

## Annexe A. Versions des composants

Cet annexe est une liste des composants et de leurs version dans Red Hat Enterprise Linux 7.2.

**Tableau A.1. Versions des composants**

Composant	Version
Noyau	3.10.0-306.0.1
Pilote QLogic <b>qla2xxx</b>	8.07.00.08.07.1-k1
Pilote QLogic <b>qla4xxx</b>	5.04.00.04.07.01-k0
Pilote Emulex <b>lpfc</b>	10.2.8021.1
iSCSI initiator utils	<i>iscsi-initiator-utils-6.2.0.873-32</i>
DM-Multipath	<i>device-mapper-multipath-0.4.9-82</i>
LVM	<i>lvm2-2.02.128-1</i>

## Annexe B. Historique des versions

<b>Version 0.0-1.16.1</b>	<b>Mon Oct 26 2015</b>	<b>Sam Friedmann</b>
Fichiers de traduction synchronisés avec les sources XML 0.0-1.16		
<b>Version 0.0-1.16</b>	<b>Mon Oct 12 2015</b>	<b>Lenka Špačková</b>
Ajout de nouvelles fonctionnalités et de problèmes connus.		
<b>Version 0.0-1.15</b>	<b>Thu Oct 8 2015</b>	<b>Lenka Špačková</b>
Restructuration des problèmes connus et ajout de plusieurs éléments à ce chapitre. Ajout d'architectures, mise à jour d'aperçus technologiques.		
<b>Version 0.0-1.14</b>	<b>Thu Oct 1 2015</b>	<b>Lenka Špačková</b>
Mise à jour des pilotes de périphérique, ajout de plusieurs problèmes connus.		
<b>Version 0.0-1.13</b>	<b>Wed Sep 16 2015</b>	<b>Lenka Špačková</b>
Ajout de descriptions de multiples fonctionnalités et de problèmes connus.		
<b>Version 0.0-1.10</b>	<b>Wed Sep 09 2015</b>	<b>Laura Bailey</b>
Ajout des mises à jour de pilotes de 7.2 Beta.		
<b>Version 0.0-1.9</b>	<b>Wed Sep 09 2015</b>	<b>Laura Bailey</b>
Ajout des problèmes connus liés à l'aperçu technologique OverlayFS.		
<b>Version 0.0-1.8</b>	<b>Mon Sep 07 2015</b>	<b>Laura Bailey</b>
Réécriture des notes de version basée sur documents des fonctionnalités et bénéfices, sur les changements des paramètres de noyau, problèmes connus, mises à jour des pilotes, et aperçus technologique.		
<b>Version 0.0-1.7</b>	<b>Fri Sep 04 2015</b>	<b>Laura Bailey</b>
Ajout d'éléments d'aperçus technologiques aux notes de version.		
<b>Version 0.0-1.4</b>	<b>Mon Aug 31 2015</b>	<b>Laura Bailey</b>
Publication des notes de version de Red Hat Enterprise Linux 7.2 Beta.		