Red Hat Enterprise Linux 6

Notes de mise jour 6.4

Notes de mise à jour de Red Hat Enterprise Linux 6.4

Édition 4

Last Updated: 2017-10-24

Red Hat Enterprise Linux 6 Notes de mise jour 6.4

Notes de mise à jour de Red Hat Enterprise Linux 6.4
Édition 4

Landmann
rlandmann@redhat.com

Notice légale

Résumé

Les notes de mise à jour couvrent les améliorations et les ajouts apportés à Red Hat Enterprise Linux 6.4. Pour une documentation détaillée sur tous les changements apportés à Red Hat Enterprise Linux avec la mise à jour 6.4, veuillez vous reporter aux Notes techniques.

Table des matières

PRÉFACE 3

CHAPITRE 1. INSTALLATION 4
Prise en charge FCoE dans le fichier Kickstart 4
Installation via un VLAN 4
Configuration de liaisons (« Bonding ») 4

CHAPITRE 2. NOYAU 5
Protocole Fibre Channel : vérification E2E (« End-To-End », de bout en bout) de la consistance des données 5
Prise en charge Flash Express pour IBM System z 5
Module noyau Open vSwitch 5
Comparaison entre un système « Booted » (démarré) et un système « Dumped » (vidé) 5
Outil Perf mis à jour 5
Prise en charge de PMU Uncore 5
Réduction de la surcharge de temps mémoire memcg 6
« Reclaim » (réclamation) et « compaction » de mémoire 6
Prise en charge de l'aménagement d'exécution de transactions (« Transactional Execution Facility ») et de l'aménagement d'instrumentation du runtime (« Runtime Instrumentation Facility ») 6
Mode Fail-open 6
Mécanisme de vidage du noyau kdump et kexec pour IBM System z totalement pris en charge 6
Prise en charge TSC Deadline pour KVM 6
Dénomination de périphériques persistants 6
Nouveau paquetage linuxptp 7
Documentation Transparent Hugepages 7
État de la prise en charge des cibles de vidage 7

CHAPITRE 3. PILOTES DE PÉRIPHÉRIQUES 8
Pilotes de stockage 8
Pilotes de réseau 9
Pilotes divers 10

CHAPITRE 4. MISE EN RÉSEAU 12
HAProxy 12

CHAPITRE 5. AUTHENTIFICATION ET INTEROPÉRABILITÉ 13
Fonctionnalités SSSD totalement prises en charge 13
Nouveau type de stockage de cache SSSD 13
Ajout de domaines de confiance basés AD aux groupes externes 13
Renouveller automatiquement (« Auto-renew ») les certificats des sous-systèmes d'Identity Management 13
Configuration automatique des outils OpenLDAP Client pour les clients inscrits sur Identity Management 13
Prise en charge PKCS#12 pour python-nss 13
Recherche DNS complète persistante 14
Nouvelle opération CLEANALLRUV 14
Bibliothèques samba4 mises à jour 14
La fonctionnalité Cross Realm Kerberos Trust dans Identity Management 15
Prise en charge des schémas Posix pour 389 Directory Server 15

CHAPITRE 6. SÉCURITÉ 17
Traitement autoritaire des correspondances lors des recherches d'entrée d'utilisateurs sudo 17
Vérifications supplémentaires de mot de passe pour pam_cracklib 17
Option « Size » (de taille) pour Polyinstantiation tmpfs 17
Verrouillage de comptes inactifs 17
Nouveaux modes d'opération pour libica 17

Optimisation et prise en charge de la bibliothèque Compression zlib pour System z 18
Configuration du pare-feu de secours 18

CHAPITRE 7. DROITS D'ACCÈS 19
Mises à jour de chaînes 19
Test de la connexion Proxy 19
Abonner ou désabonner de multiples droits d'accès 19
Prise en charge des clés d'activation dans l'interface utilisateur graphique 19
Enregistrement sur des serveurs externes 19
Modifications de la convivialité de l'interface utilisateur graphique 19

CHAPITRE 8. VIRTUALISATION 20
8.1. KVM 20
virtio-SCSI 20
Prise en charge des processeurs d'Intel Core Next-generation 20
Prise en charge du processeur AMD Opteron 4xxx Series 20
Migration live d'invités à l'aide du transfert USB (« USB Forwarding ») via SPICE 20
Migration live d'invités utilisant des périphériques USB 20
Mise à jour de l'agent de l'invité QEMU 20
PV-EOI (« Paravirtualized End-of-Interrupt Indication ») 21
Relais son configurable (« Configurable Sound Pass-through ») 21
8.2. HYPER-V 21
Inclusion et prise en charge de l'installation d'invités pour pilotes Microsoft Hyper-V 21
8.3. ESX VMWARE 22
Pilotes PV VMware 22

CHAPITRE 9. CLUSTERING 23
Prise en charge du périphérique Fence IBM iPDU 23
Prise en charge du périphérique Fence Eaton Network Power Controller 23
Nouveau paquetage keepalived 23
Récupération Watchdog 23
Prise en charge du stockage basé VMDK 23

CHAPITRE 10. STOCKAGE 24
Prise en charge complète de Parallel NFS 24
Prise en charge XFS Online Discard 24
Prise en charge LVM pour Micron PCIe SSD 24
Prise en charge LVM pour RAID10 miroir bi-directionnel 24
Paramétrer et gérer des réservations persistantes SCSI via des périphériques Device-Mapper 24

CHAPITRE 11. COMPILATEUR ET OUTILS 25
SystemTap mis à jour à la version 1.8 25
Utilitaires lscpu et chcpu 25

CHAPITRE 12. MISES À JOUR GÉNÉRALES 26
Paquetages samba mis à jour 26
Nouveau paquetage SciPy 26
Prise en charge TLS v1.1 dans NSS 26
gdbserver Valgrind intégré 27
Nouveaux paquetages libjpeg-turbo 27
Nouveau paquetage redhat-lsb-core 27
Utilitaire createrepo mis à jour 27

ANNEXE A. HISTORIQUE DE RÉVISION 28

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 mise à jour Red Hat Enterprise Linux 6.4* documentent les changements majeurs apportés au système d'exploitation Red Hat Enterprise Linux 6, ainsi que les applications qui accompagnent cette version mineure. Des notes détaillées sur tous les changements dans cette version mineure (c'est-à-dire les bogues corrigés, les améliorations ajoutées et les problèmes trouvés) sont disponibles dans les Notes techniques. Le document Notes techniques contient aussi une liste complète des tous les aperçus technologiques actuellement disponibles avec les paquetages les fournissant.

IMPORTANT

Les *Notes de mise à jour 6.4 Red Hat Enterprise Linux* en ligne, qui sont disponibles en ligne ici, sont considérées comme étant la version mise à jour et définitive. Nos clients ayant des questions sur cette version sont invités à consulter la *Release* et les *Notes techniques* en ligne de leur version de Red Hat Enterprise Linux.

Si vous nécessitez des informations concernant le cycle de vie de Red Hat Enterprise Linux, veuillez vous reporter à https://access.redhat.com/support/policy/updates/errata/.

CHAPITRE 1. INSTALLATION

Prise en charge FCoE dans le fichier Kickstart

Lors de l'utilisation d'un fichier kickstart pour installer Red Hat Enterprise Linux 6.4, la nouvelle option kickstart ***fcoe*** vous permet de spécifier quels périphériques FCoE (« Fibre Channel over Ethernet ») doivent être automatiquement activés en plus de ceux découverts par les services EDD (« Enhanced Disk Drive »). Pour obtenir plus d'informations, veuillez vous reporter à la section *Options Kickstart* du *Guide d'installation* Red Hat Enterprise Linux 6.

Installation via un VLAN

Dans Red Hat Enterprise Linux 6.4, l'option de démarrage **vlanid=** et l'option kickstart **--vlanid=** vous permettent de définir un ID LAN virtuel (802.1q tag) pour un périphérique réseau spécifié. En spécifiant l'une de ces options, l'installation du système peut être effectuée via un VLAN.

Configuration de liaisons (« Bonding »)

L'option de démarrage **bond** et les options kickstart **--bondslaves** et **--bondopts** peuvent maintenant être utilisées pour configurer les liaisons comme faisant partie du processus d'installation. Pour obtenir plus d'informations sur la manière de configurer les liaisons, veuilelz vous reporter aux parties suivantes du *Guide d'installation* Red Hat Enterprise Linux 6 : section *Options Kickstart* et chapitre *Options de démarrage*.

CHAPITRE 2. NOYAU

Protocole Fibre Channel : vérification E2E (« End-To-End », de bout en bout) de la consistance des données

L'intégrité des données entre un adaptateur hôte et un serveur de stockage a été améliorée sur Red Hat Enterprise Linux 6.4 en implémentant la partie spécifique zFCP du standard amélioré SCSI T10 DIF pour vérification de consistance de données E2E (« End-To-End »).

Prise en charge Flash Express pour IBM System z

SCM (« Storage-Class Memory ») pour IBM System z est une classe de périphériques de stockage de données combinant à la fois des propriétés de stockage et de mémoire. SCM pour System z prend maintenant en charge la mémoire Flash Express. Les incrémentations SCM peuvent être accédées via les sous-canaux EADM (« Extended Asynchronous Data Mover »). Chaque incrémentation est représentée par un périphérique bloc. Cette fonctionnalité améliore la taux de pagination et la performance d'accès au stockage temporaire, par exemple avec l'entreposage de données.

Module noyau Open vSwitch

Red Hat Enterprise Linux 6.4 inclut le module de noyau Open vSwitch comme activateur pour les offre de produits en couche Red Hat. Open vSwitch est uniquement pris en charge en conjonction avec les produits accompagnant les utilitaires d'espace utilisateur. Veuillez remarquer que sans ces utilitaires d'espace utilisateur, Open vSwitch ne fonctionnera pas et ne pourra pas être activé pour être utilisé. Pour obtenir plus d'informations, veuillez vous reporter à l'article de la base des connaissances suivant : https://access.redhat.com/knowledge/articles/270223.

Comparaison entre un système « Booted » (démarré) et un système « Dumped » (vidé)

Cette fonctionnalité vous permet de comparer un système démarré (« booted ») avec un système vidé (« dumped ») afin d'analyser efficacement les changements pouvant être introduits suite à la migration d'image. Pour identifier un invité, des données **`stsi`** et **`stfle`** sont utilisées. Une nouvelle fonction, **`lgr_info_log()`** compare les données actuelles (***`lgr_info_cur`***) avec les dernières données enregistrées (***`lgr_info_last`***).

Outil Perf mis à jour

L'outil **perf** a été mis à jour à la version en amont 3.6-rc7, qui fournit un grand nombre de correctifs de bogues et améliorations. Ci-dessous figure une liste des améliorations les plus notables :

- La prise en charge des événements Kprobe a été ajoutée.
- Un nouveau moteur de syntaxe de ligne de commande d'événement **perf** a été inclus, celui-ci autorise l'utilisation d'accolades (**`{`** et **`}`**) pour la définition de groupes d'événements, par exemple : **`{cycles,cache-misses}`**.
- **perf** annote que le navigateur a été amélioré afin de permettre la navigation via des appels ASM et des sauts (« jumps »).
- L'outil **perf** a été mis à jour afin de fournir un affichage par utilisateur avec la nouvelle option de ligne de commande **`--uid`**. Lorsqu'utilisé, **perf** affiche uniquement les tâches d'un utilisateur spécifié.
- L'outil **perf** fournit maintenant une plus grande variété de tests automatisés.

Prise en charge de PMU Uncore

Le noyau envoyé avec Red Hat Enterprise Linux 6.4 fournit la prise en charge PMU (« Performance Monitoring Unit ») « Uncore » au sous-système de l'événement perf pour la famille de processeurs Intel Xeon Processor X55xx et Intel Xeon Processor X56xx. « Uncore » fait référence aux sous-systèmes

dans le paquetage du processeur physique qui sont partagés par de multiples cœurs de processeurs, par exemple dans le cache L3. Avec la prise en charge PMU «Uncore », les données sur la performance peuvent facilement être collectées au niveau du paquetage.

L'analyse des événements PMU a aussi été activée pour autoriser le débogage via perf.

Réduction de la surcharge de temps mémoire `memcg`

Les groupes de contrôle de mémoire maintiennent leur propre liste LRU (« Least Recently Used », éléments les moins récemment utilisés) pour réclamer, par exemple, de la mémoire. Cette liste se trouve en haut de la liste globale des LRU par zone. Dans Red Hat Enterprise Linux 6.4, la surcharge de temps mémoire de **`memcg`** a été réduite en désactivant la liste globale des LRU par zone et en convertissant ses utilisateurs pour qu'ils opèrent plutôt sur les listes cgroups par mémoire.

« Reclaim » (réclamation) et « compaction » de mémoire

Le noyau envoyé avec Red Hat Enterprise Linux 6.4 utilise « reclaim » et « compaction » pour les requêtes d'allocation d'ordre élevé ou lorsque la mémoire est sous pression.

Prise en charge de l'aménagement d'exécution de transactions (« Transactional Execution Facility ») et de l'aménagement d'instrumentation du runtime (« Runtime Instrumentation Facility »)

La prise en charge de Transactional-Execution Facility (disponible avec IBM zEnterprise EC12) dans le noyau Linuxaide à éliminer la surcharge de temps du verrouillage du logiciel qui peut avoir un impact sur la performance et offrir une évolutivité améliorée et un parallélisme pour avoir un plus haut débit de transactions. La prise en charge de Runtime Instrumentation Facility (disponible avec IBM zEnterprise EC12) fournit un mécanisme avancé de profilage de code de programme pour une analyse et optimisation améliorée du code généré par le nouveau JVM d'IBM.

Mode Fail-open

Red Hat Enterprise Linux 6.4 ajoute la prise en charge d'un nouveau mode fail-openlors de l'utilisation de la cible NFQUEUE de netfilter. ce mode permet aux utilisateurs de désactiver l'inspection des paquets temporairement et de maintenir une connectivité meme lors d'un trafic réseau important.

Mécanisme de vidage du noyau kdump et kexec pour IBM System z totalement pris en charge

Sous Red Hat Enterprise Linux 6.4, le mécanisme de vidage kdump/kexec est activé pour les systèmes IBM System z en tant que fonctionnalité totalement prise en charge. Ce, en plus du mécanisme de vidage de l'hyperviseur et du mécanisme autonome IBM System z. La limite auto-reserve est définie sur 4 Go ; ainsi, tout système IBM System z possédant plus de 4 Go de mémoire aura le mécanisme kdump/kexec activé.

Suffisamment de mémoire doit être disponible car kdump réserve par défaut environ 128 Mo. Ceci est particulièrement important lors d'une opération de mise à niveau de Red Hat Enterprise Linux 6.4. Suffisamment d'espace disque doit aussi être disponible pour stocker le vidage en cas d'incident système.

Vous pouvez configurer ou désactiver kdump via **`/etc/kdump.conf`**, **system-config-kdump**, ou **firstboot**.

Prise en charge TSC Deadline pour KVM

Le minuteur TSC deadline est un nouveau mode dans le minuteur LAPIC (« Local APIC »), qui génère des interruptions de minuteur basées sur TSC deadline, au lieu de l'intervalle du compteur de l'horloge APIC actuel. TSC deadline fournit des interruptions de minuteur plus précises (moins d'un tic), et ce pour le bénéfice du planificateur du système d'exploitation. KVM expose cette fonctionnalité aux invités.

Dénomination de périphériques persistants

Cette fonctionnalité stocke le mappage des noms de périphériques (par exemple **sda**, **sdb** et autres), ainsi que des noms de périphériques persistants (fournis par **udev** dans **/dev/disk/by-*/**) sur les messages du noyau. Ceci permet aux utilisateurs d'identifier un périphérique à partir des messages noyau. Le journal du noyau **/dev/kmsg**, qui peut être affiché avec la commande **dmesg**, affiche maintenant les messages pour les liens symboliques, qu'**udev** a créé pour les périphériques du noyau. Ces messages sont affichés sous le format suivant :

```
udev-alias: <device_name> (<symbolic_link> <symbolic link> …)
```

N'importe quel analyseur de journaux peut afficher ces messages, qui sont aussi enregistrés dans **/var/log/messages** via **syslog**.

Nouveau paquetage linuxptp

Le paquetage linuxptp, inclut dans Red Hat Enterprise Linux 6.4 en tant qu'aperçu technologique, est une implémentation de PTP (« Precision Time Protocol ») selon le standard IEEE 1588 pour Linux. Les buts du double design sont de fournir une implémentation robuste du standard et d'utiliser les API correspondants le mieux et les API plus modernes possibles offerts par le noyau Linux. La prise en charge des API et autres plateformes héritées n'est pas un but.

Documentation Transparent Hugepages

La documentation de transparent hugepages a été ajoutée au fichier suivant :

```
/usr/share/doc/kernel-doc-<version>/Documentation/vm/transhuge.txt
```

État de la prise en charge des cibles de vidage

Dans Red Hat Enterprise Linux 6.4, le fichier **/usr/share/doc/kexec-tools-2.0.0/kexec-kdump-howto.txt** fournit une liste complète des cibles de vidage prises en charge, non-prises en charge, et inconnues sous la section « Statut de la prise en charge de cibles de vidage ».

CHAPITRE 3. PILOTES DE PÉRIPHÉRIQUES

Pilotes de stockage

- Le pilote de périphérique « Direct Access Storage Devices » (ou **DASD**) a été mis à jour pour détecter les erreurs de configuration de chemin qui ne peuvent pas être détectées par le matériel ou le microcode. Lorsque la détection est réussie, le pilote de périphérique n'utilise pas de tel chemin. Par exemple, avec cette fonctionnalité, le pilote de périphérique DASD détecte les chemins qui sont assignés à un sous-canal spécifique, mais qui conduisent à différents serveurs de stockage.

- Le pilote de périphérique **zfcp** a été mis à jour pour ajouter la gestion d'erreurs et de structures de données afin de prendre en charge le mode amélioré de la carte d'adaptateur FCP (« Fibre Channel Protocol ») System z. Dans ce mode, l'adaptateur passe les données directement de la mémoire au SAN (routeur de données) lorsque la mémoire de la carte de l'adaptateur est bloquée par de grandes et lentes requêtes d'E/S.

- Le pilote **mtip32xx** a été mis à jour pour ajouter la prise en charge des derniers disques PCIe SSD.

- Le pilote **lpfc** pour adaptateursde bus hôte Fibre Channel Emulex a été mis à jour à la version 8.3.5.82.1p.

- Le pilote **qla2xxx** des QLogic Fibre Channel HBA a été mis à jour à la version 8.04.00.04.06.4-k, qui fournit la prise en charge de l'adaptateur CNA (« Converged Network Adapter ») QLogic 83XX, la prise en charge 16GBps FC pour adaptateurs QLogic et nouveaux Form Factor CNA pour serveurs HP ProLiant.

- Le pilote **qla4xxxx** a été mis à jour à la version v5.03.00.00.06.04-k0, qui ajoute la prise en charge de l'API ***change_queue_depth***, corrige un certain nombre de bogues et présente diverses améliorations.

- Le microprogramme **ql2400-firmware** pour HBA fibre channel QLogic 4Gbps a été mis à jour à la version 5.08.00.

- Le microprogramme **ql2500-firmware** pour HBA fibre channel QLogic 4Gbps a été mis à jour à la version 5.08.00.

- Le pilote **ipr** pour HBA RAID IBM Power Linux a été mis à jour à la version 2.5.4, qui ajoute la prise en charge des adaptateurs SAS Power7 6Gb et active les capacités VRAID SAS sur ces adaptateurs.

- Le pilote **hpsa** a été mis à jour à la version 2.0.2-4-RH1 afin de fournir des PCI-IDs pour la gamme contrôleurs HP Smart Array Generation 8.

- Le pilote **bnx2i** pour iSCSI Broadcom NetXtreme II a été mis à jour vers la version 2.7.2.2 avec l'activation de la prise en charge générale du matériel.

  Le support des démarrages iSCSI et FCoE sur périphériques Broadcom est maintenant totalement prise en charge sur Red Hat Enterprise Linux 6.4. Ces deux fonctionnalités sont fournies par les pilotes Broadcom bnx2i et bnx2fc.

- Le pilote **bnx2fc** pour le processeur Broadcom NetXtreme II 57712 a été mis à jour à la version 1.0.12.

Le support des démarrages iSCSI et FCoE sur périphériques Broadcom est maintenant totalement prise en charge sur Red Hat Enterprise Linux 6.4. Ces deux fonctionnalités sont fournies par les pilotes Broadcom bnx2i et bnx2fc.

- Le pilote **mpt2sas** a été mis à jour à la version 13.101.00.00, qui ajoute la prise en charge du mode multi-segment pour le pilote Linux BSG Driver.

- Le pilote Fibre Channel et FCoE Brocade **bfa** a été mis à jour à la version 3.0.23.0 qui inclut la prise en charge d'adaptateur Fibre Channel Brocade 1860 16Gbps, la prise en charge de nouveau matériel dans les serveurs Dell PowerEdge 12ème Génération, ainsi que la prise en charge d'**issue_lip**. Le microprogramme **bfa** a été mis à jour à la version 3.0.3.1.

- Le pilote **be2iscsi** pour périphériques Open iSCSI ServerEngines BladeEngine 2 a été mis à jour vers la version 4.4.58.0r afin d'ajouter la prise en charge VLAN netlink iSCSI.

- Le pilote **qib** pour HCA TrueScale a été mis à jour à la dernière version et comprend les améliorations suivantes :

  - Reconnaissance NUMA améliorée

  - Agent CCA (« Congestion Control Agent ») pour fabriques PSM (« Performance Scale Messaging »)

  - Dual Rail pour fabriques PSM

  - Améliorations de la performance et correctifs de bogues

- Les pilotes suivants ont été mis à jour afin d'inclure les fonctionnalités et correctifs de bogues les plus récents disponibles en amont : **ahci**, **md**/**bitmap**, **raid0**, **raid1**, **raid10** et **raid456**.

Pilotes de réseau

- Le pilote **netxen_nic** pour NetXen Multi port (1/10) Gigabit Network a été mis à jour à la version 4.0.80, qui ajoute la prise en charge miniDIMM. Le microprogramme **netxen_nic** a été mis à jour à la version 4.0.588.

- Le pilote **bnx2x** a été mis à jour à la version 1.72.51-0 pour inclure la prise en charge des puces Broadcom 57800/57810/57811/57840, de correctifs de bogues et du microprogramme pour les puces Broadcom 57710/57711/57712. Cette mise à jour inclut aussi les améliorations suivantes :

  - Prise en charge du déchargement iSCSI et de DCB/FCoE (« Data Center Bridging/Fibre Channel over Ethernet ») sur les puces Broadcom 57712/578xx. La puce Broadcom 57840 est uniquement prise en charge sous une configuration 4x10Get ne prend pas en charge le déchargement iSCSI et FCoE. Les versions futures prendront en charge des configurations supplémentaires ainsi que le déchargement iSCSI et FCoE.

  - Prise en charge d'une couche physique supplémentaire, y compris EEE (« Energy Efficient Ethernet »)

  - Améliorations du déchargement iSCSI

  - Fonctionalités spécifiques OEM

- Le pilote **be2net** des périphériques réseau ServerEngines BladeEngine2 10Gbps a été mis à jour à la version 4.4.31.0r pour ajouter la prise en charge RoCE (« RDMA over Converged Ethernet »).

Enoutre, la fonctionnalité SR-IOV du pilote Emulex **be2net** est maintenant totalement prise en charge par Red Hat Enterprise Linux 6.4. SR-IOV peut être exécuté sur toutes les variantes OEM et Emulex de matériel basé BE3, qui requièrent le logiciel du pilote **be2net**.

- Le pilote **ixgbevf** a été mis à jour à la version 2.6.0-k afin d'inclure les prise en charge du matériel, améliorations et correctifs de bogues les plus récents.
- Le pilote **cxgb4** pour contrôleurs réseau Chelsio Terminator4 10G Unified Wire a été mis à jour pour ajouter la prise en charge des adaptateurs Chelsio T480-CR et T440-LP-CR.
- Le pilote **cxgb3** de la famille de périphériques de réseau Chelsio T3 a été mis à jour à la dernière version 1.1.5-ko.
- Le pilote **ixgbe** pour périphériques réseau Intel 10 Gigabit PCI Express a été mis à jour à la version 3.9.15-k pour inclure la prise en charge de SR-IOV avec DCB (« Data Center Bridging ») ou RSS (« Receive-Side Scaling »), la prise en charge PTP en tant qu'aperçu technologique, la prise en charge du matériel le plus récent, les améliorations et les correctifs de bogues.
- Le pilote **iw_cxgb3** a été mis à jour.
- Le pilote **iw_cxgb4** a été mis à jour.
- Le pilote **e1000e** des périphériques réseau Intel PRO/1000 a été mis à jour afin d'ajouter la prise en charge du matériel et des fonctionnalités les plus récents et pour fournir un certain nombre de correctifs de bogues.
- Le pilote **enic** pour périphériques Ethernet Cisco 10G a été mis à jour vers la version 2.1.1.39.
- Le pilote **igbvf** (pilote réseau Intel Gigabit Virtual Function) a été mis à jour à la version en amont la plus récente.
- Le pilote **igb** pour adaptateurs Ethernet Intel Gigabit a été mis à jour à la version 4.0.1 pour ajouter la prise en charge du matériel le plus récent. La prise en charge PTP a aussi été ajoutée au pilote **igb** en tant qu'aperçu technologique.
- Le pilote **tg3** pour périphériques Ethernet Broadcom Tigon3 a été mis à jour à la version 3.124 afin d'inclure la prise en charge de nouveau matériel. La prise en charge PTP a aussi été ajoutée au pilote **tg3** en tant qu'aperçu technologique.
- Le pilote **qlcnic** pour adaptateurs de serveurs HP NC-Series QLogic 10 Gigabit a été mis à jour vers la version 5.0.29.
- Le pilote Brocade **bna** du pilote de contrôleurs Ethernet PCIe Brocade 10Gb a été mis à jour à la version 3.0.23.0 afin d'inclure la prise en charge de nouveau matériel pour les serveurs Dell PowerEdge 12ème Génération et d'activer l'utilisation de cables non-Brocade Twinax Copper. Le microprogramme **bna** a été mis à jour à la version 3.0.3.1.
- Le pilote Broadcom NetXtreme II **cnic** a été mis à jour à la version 2.5.13 afin d'inclure de nouvelles fonctionnalités, des correctifs de bogues et la prise en charge pour de nouvelles plateformes OEM.

Pilotes divers

- Le pilote **intel_idle** cpuidle pour processeurs Intel a été mis à jour pour ajouter la prise en charge de la gamme de processeurs Intel Xeon E5-XXX V2.

- Le pilote **wacom** a été mis à jour pour ajouter la prise en charge de CTL-460 Wacom Bamboo Pen, de la tablette Wacom Intuos5 Tablet, et de l'affichage Wacom Cintiq 22HD Pen Display.
- Le pilote audio HDA ALSA aété mis à jour pour activer ou améliorer la prise en charge de nouveau matériel et pour corriger un certain nombre de bogues.
- Le pilote **mlx4_en** a été mis à jour à la dernière version en amont.
- Le pilote **mlx4_ib** a été mis à jour à la dernière version en amont.
- Le pilote **mlx4_core** a été mis à jour à la dernière version en amont.
- Le pilote de périphérique **z90crypt** a été mis à jour pour prendre en charge la nouvelle carte d'adaptateur Crypto Express 4 (CEX4).

CHAPITRE 4. MISE EN RÉSEAU

HAProxy

HAProxy est un équilibreur de charges réseau de haute performance autonome, Layer 7, pour applications basées TCP et HTTP pouvant effectuer divers types de planification basées sur le contenu des requêtes HTTP. Red Hat Enterprise Linux 6.4 présente le paquetage haproxy en tant qu'aperçu technologique.

CHAPITRE 5. AUTHENTIFICATION ET INTEROPÉRABILITÉ

Fonctionnalités SSSD totalement prises en charge

Un certain nombre de fonctionnalités présentées dans Red Hat Enterprise Linux 6.3 sont maintenent totalement prises en charge dans Red Hat Enterprise Linux 6.4. Particulièrement :

- prise en charge de la gestion centrale des clés SSH,
- mappage de l'utilisateur SELinux,
- et la prise en charge de la mise en cache de mappages automount.

Nouveau type de stockage de cache SSSD

Kerberos version 1.10 offre un nouveau type de stockage de cache, **`DIR:`**, qui permet à Kerberos de maintenir des TGT (« Ticket Granting Tickets », tickets fournissant des tickets) pour de multiples KDC (« Key Distribution Centers », centres de distribution de clés) simultanément et d'effectuer une sélection automatique (« auto-select ») entre eux lors de négociations avec des ressources reconnaissant Kerberos. Dans Red Hat Enterprise Linux 6.4, SSSD a été amélioré afin de vous permettre de sélectionner le cache **`DIR:`** pour les utilisateurs se connectant via SSSD. Cette fonctionnalité est présentée comme un aperçu technologique.

Ajout de domaines de confiance basés AD aux groupes `externes`

Dans Red Hat Enterprise Linux 6.4, la commande **`ipa group-add-member`** vous permet d'ajouter des membres de domaines basés Active Directory à des groupes marqués comme **`externes`** dans Identity Management (gestion des identités). Ces membres peuvent être spécifiés par leurs noms en utilisant une syntaxe basée sur UPN ou sur domaine, par exemple **`AD\UserName`** ou **`AD\GroupName`** ou **`User@AD.Domain`**. Lorsque spécifié sous cette forme, les membres sont résolus sur le catalogue global du domaine de confiance basé Active Directory pour obtenir une valeur SID (identifiant de sécurité).

De manière alternative, une valeur SID peut être spécifiée directement. Dans ce cas, la commande **`ipa group-add-member`** vérifiera uniquement que le domaine faisant partie de la valeur SID est l'un des domaines de confiance Active Directory. Aucune tentative ne sera entreprise pour vérifier la validité de la valeur SID dans le domaine.

Il est recommandé d'utiliser la syntaxe de nom d'utilisateur ou de groupe pour spécifier les membres externes plutôt que de directement fournir leurs valeurs SID.

Renouveller automatiquement (« Auto-renew ») les certificats des sous-systèmes d'Identity Management

La période de validité d'une nouvelle autorité de certificats (ou CA, de l'anglais « Certificate Authority ») est de 10 ans. Le CA fournit un certain nombre de certificats pour ses sous-systèmes (OCSP, journaux d'audit et autres). Les certificats de sous-systèmes sont normalement valides pour 2 ans. Si le certificat expire, le CA ne démarrera pas ou ne fonctionnera pas correctement. Ainsi, dans Red Hat Enterprise Linux 6.4, les serveurs Identity Management sont capables de renouveller les certificats de leurs sous-systèmes. Les certificats des sous-systèmes sont suivis par **certmonger**, qui tentera automatiquement de renouveller les certificats avant qu'ils n'expirent.

Configuration automatique des outils OpenLDAP Client pour les clients inscrits sur Identity Management

Dans Red Hat Enterprise Linux 6.4, OpenLDAP est automatiquement configuré avec un URI LDAP, un DN de base et un certificat TLS pendant l'installation du client Identity Management. Ceci améliore l'expérience utilisateur lorsque des recherches LDAP sont effectuées sur le serveur Identity Management Directory Server.

Prise en charge PKCS#12 pour python-nss

Le paquetage python-nss, qui fournit des liaisons Python pour NSS (« Network Security Services ») et NSPR (« Netscape Portable Runtime »), a été mis à jour pour ajouter la prise en charge de PKCS #12.

Recherche DNS complète persistante

LDAP sur Red Hat Enterprise Linux 6.4 inclut la prise en charge des recherches persistantes des zones et des enregistrements de leurs ressources. La recherche persistante permet au plugin **bind-dyndb-ldap** d'être immédiatement informé sur tout changement apporté à une base de données LDAP. Elle réduit aussi l'utilisation de bande passante du réseau requise par les analyses répétées.

Nouvelle opération CLEANALLRUV

Des éléments obsolètes de la base de données RUV (« Replica Update Vector ») peuvent être supprimés avec l'opération **`CLEANRUV`**, qui les supprime d'un seul fournisseur ou maître. Red Hat Enterprise Linux 6.4 ajoute une nouvelle opération **`CLEANALLRUV`** , qui peut supprimer des données RUV obsolètes de toutes les répliques et qui doit uniquement être exécutée sur un seul maître/fournisseur.

Bibliothèques samba4 mises à jour

Les bibliothèques **samba4** (fournies par le paquetage samba4-libs) ont été mises à niveau à la dernière version en amont pour améliorer l'interopérabilité avec les domaines Active Directory (AD). SSSD utilise maintenant la bibliothèque **`libndr-krb5pac`** pour analyser le PAC (« Privilege Attribute Certificate ») fournit par un KDC (« Key Distribution Center ») AD. En outre, diverses améliorations ont été apportées aux services LSA (« Local Security Authority ») et Net Logon afin de permettre la vérification de confiance à partir d'un système Windows. Pour obtenir des informations sur l'introduction de la fonctionnalité Cross Realm Kerberos Trust, qui dépend des paquetages samba4, reportez-vous à la section intitulée « La fonctionnalité Cross Realm Kerberos Trust dans Identity Management ».

AVERTISSEMENT

Si vous effectuez une mise à niveau de Red Hat Enterprise Linux 6.3 à Red Hat Enterprise Linux 6.4 et que Samba est en cours d'utilisation, assurez-vous de désinstaller le paquetage samba4 afin d'éviter des conflits pendant la mise à niveau.

Comme la fonctionnalité Cross Realm Kerberos Trust est considérée comme un Aperçu technologique, les composants **samba4** sélectionnés sont considérés comme un Aperçu technologique aussi. Pour plus d'informations sur quels paquetages Samba sont considérés comme aperçus technologiques, veuillez vous reporter au Tableau 5.1, « Prise en charge du paquetage Samba4 ».

Tableau 5.1. Prise en charge du paquetage Samba4

Nom du paquetage	Nouveau paquetage dans 6.4 ?	Statut de la prise en charge
samba4-libs	Non	Aperçu technologique, à l'exception de la fonctionnalité requise par OpenChange
samba4-pidl	Non	Aperçu technologique, à l'exception de la fonctionnalité requise par OpenChange

Nom du paquetage	Nouveau paquetage dans 6.4 ?	Statut de la prise en charge
samba4	Non	Aperçu technologique
samba4-client	Oui	Aperçu technologique
samba4-common	Oui	Aperçu technologique
samba4-python	Oui	Aperçu technologique
samba4-winbind	Oui	Aperçu technologique
samba4-dc	Oui	Aperçu technologique
samba4-dc-libs	Oui	Aperçu technologique
samba4-swat	Oui	Aperçu technologique
samba4-test	Oui	Aperçu technologique
samba4-winbind-clients	Oui	Aperçu technologique
samba4-winbind-krb5-locator	Oui	Aperçu technologique

La fonctionnalité Cross Realm Kerberos Trust dans Identity Management

La fonctionnalité Cross Realm Kerberos Trust fournie par Identity Management est incluse en tant qu'aperçu technologique. Cette fonctionnalité permet de créer une relation de confiance entre Identity Management et un domaine Active Directory. Ceci signifie que les utilisateurs du domaine AD peuvent accéder aux ressources et services du domaine Identity Management avec leurs informations d'identification AD. Aucune donnée ne nécessite d'être synchronisée entre les contrôleurs d'Identity Management et d'Active Directory. Les utilisateurs AD s'authentifient toujours sur le contrôleur du domaine AD et les informations sur les utilisateurs sont recherchées sans avoir besoin d'effectuer une synchronisation.

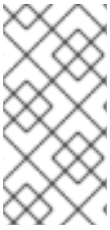
Cette fonctionnalité est fournie par le paquetage optionnel ipa-server-trust-ad. Ce paquetage dépend de fonctionnalités qui sont uniquement disponibles dans **samba4**. Comme les paquetages samba4-* sont en conflit avec les paquetages samba-*, tous les paquetages samba-* doivent être supprimés avant que ipa-server-trust-ad puisse être installés.

Lorsque le paquetage ipa-server-trust-ad est installé, la commande **`ipa-adtrust-install`** doit être exécutée sur tous les serveurs et répliques d'Identity Management afin d'activer Identity Management pour gérer les confiances. Lorsque ceci est effectué, une confiance peut être établie sur la ligne de commande à l'aide de **`ipa trust-add`** ou de l'interface utilisateur web. Pour plus d'informations, veuillez vous reporter à la section *Intégration avec Active Directory via les confiances Cross-Realm Kerberos Trusts* dans le *Guide d'Identity Management* sur https://access.redhat.com/knowledge/docs/Red_Hat_Enterprise_Linux/.

Prise en charge des schémas Posix pour 389 Directory Server

Windows Active Directory (AD) prend en charge les schémas POSIX (RFC 2307 et 2307bis) pour les

entrées d'utilisateurs et de groupes. Dans de nombreux cas, AD est utilisé en tant que source autorisée des données d'utilisateurs et de groupes, y compris les attributs POSIX. Avec Red Hat Enterprise Linux 6.4, Directory Server Windows Sync n'ignore plus ces attributs. Les utilisateurs peuvent maintenant synchroniser des attributs POSIX avec Windows Sync entre AD et 389 Directory Server.



NOTE

Lors de l'ajout de nouvelles entrées d'utilisateurs et de groupes sur Directory Server, les attributs POSIX ne sont plus synchronisés sur AD. L'ajout de nouvelles entrées d'utilisateurs et de groupes sur AD se synchronisera sur Directory Server, et la modification d'attributs sera synchronisée dans les deux sens.

CHAPITRE 6. SÉCURITÉ

Traitement autoritaire des correspondances lors des recherches d'entrée d'utilisateurs sudo

L'utilitaire **sudo** est en mesure de consulter le fichier **/etc/nsswitch.conf** en recherchant des entrées sudo et de les rechercher dans des fichiers ou en utilisant LDAP. Auparavant, lorsqu'une correspondance était trouvée dans la première base de données des entrées sudo, l'opération continuait toujours dans d'autres bases de données (y compris dans des fichiers). Dans Red Hat Enterprise Linux 6.4, une option a été ajoutée au fichier **/etc/nsswitch.conf** qui permet aux utilisateurs de spécifier une base de données à partir de laquelle une correspondance d'entrées sudo sera suffisante. Ceci élimine le besoin de rechercher toute autre base de données, améliorant ainsi la performance des recherches d'entrées sudo dans des environnements de grande taille. Ce comportement n'est pas activé par défaut et doit être configuré en ajoutant la chaîne ***[SUCCESS=return]*** après la base de données sélectionnée. Lorsqu'une corresondance est trouvée dans une base de données qui précede directement cette chaîne, la recherche ne d'effectuera dans aucune autre base de données.

Vérifications supplémentaires de mot de passe pour `pam_cracklib`

Le module **pam_cracklib** a été mis à jour afin d'ajouter de multiples vérifications de la sécurité des mots de passe :

- Certaines stratégies d'authentification n'autorisent pas les mots de passe contenant de longues séquences continues, comme « abcd » ou « 98765 ». Cette mise à jour offre la possibilité de limiter la longueur maximum de ces séquences, grâce à l'utilisation de la nouvelle option **maxsequence**.

- Le module **pam_cracklib** permet maintenant de vérifier si un nouveau mot de passe contient des mots du champ GECOS provenant d'entrées dans le fichier **/etc/passwd**. Le champ GECOS est utilisé pour stocker des informations supplémentaires sur l'utilisateur, comme le nom et nom de famille de l'utilisateur ou un numéro de téléphone, qui pourraient être utilisés par une personne malveillante dans le but de craquer le mot de passe.

- Le module **pam_cracklib** permet maintenant de spécifier le nombre maximum autorisé de caractères consécutifs de la même classe (minuscules, majuscules, chiffres et caractères spéciaux) dans un mot de passe grâce à l'option **maxrepeatclass**.

- Le module **pam_cracklib** prend maintenant en charge l'option **enforce_for_root**, qui applique des restrictions de complexité sur les nouveaux mots de passe du compte root.

Option « Size » (de taille) pour Polyinstantiation tmpfs

Sur un système avec de multiple montages tmpfs, il est nécessaire de limiter leur taille afin de les empêcher d'occuper toute la mémoire système. PAM a été mis à jour pour permettre aux utilisateurs de spécifier la taille maximum du montage du système de fichiers tmpfs lors de l'utilisation de la polyinstantiation tmpfs avec l'option **mntopts=size=<*size*>** dans le fichier de configuration **/etc/namespace.conf**.

Verrouillage de comptes inactifs

Certaines stratégies d'authentification requièrent la prise en charge du verrouillage d'un compte qui n'a pas été utilisé depuis un certain moment. Red Hat Enterprise Linux 6.4 présente une fonction supplémentaire au module **pam_lastlog**, qui permet aux utilisateurs de verrouiller les comptes après un nombre de jours configurable.

Nouveaux modes d'opération pour `libica`

La bibliothèque **libica**, qui contient un ensemble de fonctions et utilitaires pour accéder au matériel ICA (« IBM eServer Cryptographic Accelerator ») sur IBM System z, a été modifiée pour autoriser

l'utilisation de nouveaux algorithmes qui prennent en charge les instructions Message Security Assist Extension 4 dans le CPACF (« Central Processor Assist for Cryptographic Function »). Pour les chiffrements par bloca DES et 3DES, les modes d'opération suivants sont maintenant pris en charge :

- Chaînage de chiffrement de blocs (CBC, « Cipher Block Chaining ») avec vol de texte chiffré (CS, « Ciphertext Stealing »)
- Code d'authentification de messages basé sur chiffrement (CMAC, « Cipher-based Message Authentication Code »)

Pour le chiffrement de blocs AES, les modes d'opération suivants sont maintenant pris en charge :

- Chaînage de chiffrement de blocs (CBC, « Cipher Block Chaining ») avec vol de texte chiffré (CS, « Ciphertext Stealing »)
- « Counter » (contrer) avec le code d'authentification des messages du chaînage de chiffrement de blocs (CCM, « Cipher Block Chaining Message Authentication Code »)
- Galois/Counter (GCM)

Cette accélération d'algorithmes de chiffrement complexe améliore la performance des machines IBM System z de manière significative.

Optimisation et prise en charge de la bibliothèque Compression `zlib` pour System z

La bibliothèque zlib, une bibliothèque de compression de données sans perte a utilisation générale, a été mise à jour afin d'améliorer la performance de la compression sur IBM System z.

Configuration du pare-feu de secours

Les services **`iptables`** et **`ip6tables`** offrent maintenant la possibilité d'assigner une configuration de pare-feu de secours si les configurations par défaut ne peuvent pas être appliquées. Si l'application des règles de pare-feu de **`/etc/sysconfig/iptables`** échoue, le fichier de secours est appliqué, s'il existe. Le fichier de secours est nommé **`/etc/sysconfig/iptables.fallback`** et utilise le format de fichier **`iptables-save`** (comme **`/etc/sysconfig/iptables`**). Si l'application du fichier de secours échoue aussi, alors il n'y aura pas de fichier de secours supplémentaire. Pour créer un fichier de secours, veuillez utiliser les outils de configuration de pare-feu standard et copier ou renommer le fichier sur le fichier de secours. Veuillez utiliser le même processus pour le service **`ip6tables`**, remplacez toutes les occurrences de « iptables » par « ip6tables » uniquement.

CHAPITRE 7. DROITS D'ACCÈS

Mises à jour de chaînes

Dans Red Hat Enterprise Linux 6.4, plusieurs chaînes ont été renommées dans Subscription Manager :

- *abonner* a été renommé *attacher*
- *auto-subscribe* (abonnement automatique) a été renommé *auto-attach* (attacher automatiquement)
- *désabonner* a été renommé *supprimer*
- *consommateur* a été renommé *système* ou *unité*

Test de la connexion Proxy

La boîte de dialogue de la configuration du Proxy permet maintenant aux utilisateurs de tester une connexion à un proxy après avoir saisi une valeur.

Abonner ou désabonner de multiples droits d'accès

Subscription Manager est maintenant en mesure d'abonner (ou attacher) et de désabonner (ou supprimer) de multiples droits d'accès sur le champ, et ce en utilisant leurs numéros de série.

Prise en charge des clés d'activation dans l'interface utilisateur graphique

L'interface utilisateur graphique Subscription Manager vous permet maintenant d'enregistrer un système en utilisant une *clé d'activation*. Les clés d'activation permettent aux utilisateurs de préconfigurer les abonnements pour un système avant qu'il ne soit enregistré.

Enregistrement sur des serveurs externes

La prise en charge de la sélection d'un serveur distant pendant l'enregistrement d'un système est maintenant supportée dans le gestionnaire SAM. Son interface utilisateur présente une option pour choisir l'URL d'un serveur sur lequel s'enregistrer ainsi qu'un port et un préfixe pendant le processus d'enregistrement. En outre, lors d'un enregistrement avec la ligne de commande, l'option **`--serverurl`** peut être utilisée pour spécifier le serveur sur lequel s'enregistrer. Pour obtenir des informations supplémentaires sur cette fonctionnalité, reportez-vous au *Enregistrer, désenregistrer et ré-enregistrer un système* dans le *Guide de gestion des abonnements*.

Modifications de la convivialité de l'interface utilisateur graphique

L'interface utilisateur graphique du gestionnaire des abonnements a été améliorée avec diverses modifications basées sur les commentaires de nos clients.

CHAPITRE 8. VIRTUALISATION

8.1. KVM

virtio-SCSI

La pile de stockage de KVM Virtualization a été améliorée avec l'ajout de capacités virtio-SCSI (une architecture de stockage pour KVM basée sur SCSI). Virtio-SCSI fournit la capacité de se connecter directement à des LUN SCSI et améliore de manière significative l'évolutivité, comparé à virtio-blk. L'avantage de virtio-SCSI réside dans sa capacité à gérer des centaines de périphériques comparé à virtio-blk, qui peut uniquement gérer environ 25 périphériques et épuise les emplacements PCI.

Virtio-SCSI est maintenant capable d'hériter l'ensemble de fonctionnalités du périphérique cible avec la capacité de :

- attacher un disque dur virtuel ou un CD via le contrôleur virtio-SCSI,
- passer à travers un périphérique SCSI physique depuis l'hôte vers l'invité via le périphérique bloc SCSI QEMU,
- et permettre l'utilisation de centaines de périphériques par invité ; une amélioration par rapport à la limite de ~25 périphériques de virtio-blk.

virtio-scsi fut présenté dans Red Hat Enterprise Linux 6.3 en tant qu'aperçu technologique, sur Red Hat Enterprise Linux 6.4, virtio-scsi est totalement pris en charge. Les invités Windows guests (à l'exception de Windows XP) sont aussi pris en charge avec les pilotes virtio-win les plus récents.

Prise en charge des processeurs d'Intel Core Next-generation

Red Hat Enterprise Linux 6.4 offre la prise en charge des processeurs Intel Core next-generation pour **qemu-kvm** afin que les invités KVM puissent utiliser les nouvelles fonctionnalités fournies par ce processeur, les plus notables sont : Advanced Vector Extensions 2 (AVX2), Bit-Manipulation Instructions 1 (BMI1), Bit-Manipulation Instructions 2 (BMI2), Hardware Lock Elision (HLE), Restricted Transactional Memory (RTM), Process-Context Identifier (PCID), Invalidate Process-Context Identifier (INVPCID), Fused Multiply-Add (FMA), Big-Endian Move instruction (MOVBE), F Segment et G Segment BASE instruction (FSGSBASE), Supervisor Mode Execution Prevention (SMEP), Enhanced REP MOVSB/STOSB (ERMS).

Prise en charge du processeur AMD Opteron 4xxx Series

Le processeur AMD Opteron 4xxx series est maintenant pris en charge par **qemu-kvm**. Ceci permet aux nouvelles fonctionnalités de cette série de processeurs d'être exposées à des invités KVM tels que : l'ensemble d'instructions F16C, Trailing Bit Manipulation, les fonctions « decimate » de BMI1 (« Bit-Manipulation Instructions 1 ») et l'ensemble d'instructions FMA (« Fused Multiply-Add »).

Migration live d'invités à l'aide du transfert USB (« USB Forwarding ») via SPICE

Dans Red Hat Enterprise Linux 6.4, KVM prend en charge la migration live d'invités à l'aide du transfert USB via SPICE, tout en maintenant les redirections USB existantes des périphériques configurés.

Migration live d'invités utilisant des périphériques USB

Dans Red Hat Enterprise Linux 6.4, KVM prend en charge la migration live d'invités avec des périphériques USB. Les périphériques suivants sont pris en charge : les relais locaux UHCI (« Enhanced Host Controller Interface ») et UHCI (« Universal Host Controller Interface »), mais aussi des périphériques émulés, tels que périphériques de stockage, souris, claviers, hubs et autres.

Mise à jour de l'agent de l'invité QEMU

L'agent de l'invité QEMU (fournit par le paquetage qemu-guest-agent) est maintenant totalement pris en charge dans Red Hat Enterprise Linux 6.4. Il a été mis à jour à la version en amont 1.1 et inclut les améliorations et correctifs de bogues notables suivants :

- Les commandes **`guest-suspend-disk`** et **`guest-suspend-ram`** peuvent maintenant être utilisées pour suspendre sur RAM ou sur disque sur un système Windows.
- La commande **`guest-network-get-interfaces`** peut maintenant être utilisée pour acquérir des informations d'interface réseau dans Linux.
- Cette mise à jour fournit des améliorations et correctifs de la prise en charge des gels de systèmes de fichiers.
- Cette mise à jour inclut diverses corrections de la documentation ainsi que de petites améliorations.

PV-EOI (« Paravirtualized End-of-Interrupt Indication »)

Les hôtes et invités exécutant Red Hat Enterprise Linux 6.3 et autres versions plus anciennes requièrent deux sorties de machine virtuelle (basculements de contexte d'une MV à un hyperviseur) pour chaque interruption : une pour injecter l'interruption et une autre pour signaler la fin de l'interruption. Lorsque les systèmes hôte et invité sont tous deux mis à jour avec Red Hat Enterprise Linux 6.4 ou autre version plus récente, ils peuvent négocier une fonctionnalité de fin d'interruption paravirtualisée et ne requièrent qu'un basculement par interruption. Par conséquent, avec l'utilisation de Red Hat Enterprise Linux 6.4, ou d'une autre version plus récente, comme hôte et comme invité, le nombre de sorties est réduit par deux pour les charges de travail intensives en interruptions, comme le trafic réseau entrant avec un périphérique réseau virtio. Ceci amène à réduire l'utilisation CPU de manière significative pour de telles charges de travail. Remarquez que seules les interruptions de contour sont améliorées : par exemple, e1000 utilise des interruptions de niveau et n'a pas été amélioré.

Relais son configurable (« Configurable Sound Pass-through »)

Un périphérique son peut maintenant être détecté en tant que **`microphone`** ou **`speaker`** (enceinte) dans le système invité (en plus d'être détecté comme **`line-in`** et **`line-out`**). Les périphériques son peuvent maintenant fonctionner correctement avec les applications d'invités qui n'acceptent que certains types d'entrées pour l'enregistrement de voix et l'audio.

8.2. HYPER-V

Inclusion et prise en charge de l'installation d'invités pour pilotes Microsoft Hyper-V

L'installation intégrée de l'invité Red Hat Enterprise Linux et la prise en charge de périphériques paravirtualisés Hyper-V dans Red Hat Enterprise Linux 6.4 sur Microsoft Hyper-V permet aux utilisateurs d'exécuter Red Hat Enterprise Linux 6.4 en tant qu'invité sur des hyperviseurs Microsoft Hyper-V. Les pilotes Hyper-V suivants et une source d'horloge ont été ajoutés au noyau envoyé dans Red Hat Enterprise Linux 6.4 :

- un pilote réseau (**`hv_netvsc`**)
- un pilote de stockage (**`hv_storvsc`**)
- un pilote de souris conforme HID (**`hid_hyperv`**)
- un pilote VMbus (**`hv_vmbus`**)
- un pilote util (**`hv_util`**)

- un pilote de disque IDE (**ata_piix**)
- une source d'horloge (i386, AMD64/Intel 64 : **hyperv_clocksource**)

Red Hat Enterprise Linux 6.4 inclut aussi la prise en charge d'« Hyper-V » en tant que source d'horloge et un démon invité KVP (« Key-Value Pair ») Hyper-V (**hypervkvpd**) qui passe les informations de base, comme l'IP de l'invité, le FQDN, le nom du système d'exploitation et son numéro de version à l'hôte via VMbus.

8.3. ESX VMWARE

Pilotes PV VMware

Les pilotes para-virtualisés VMware ont été mis à jour pour fournir une expérience parfaite de prêt à l'emploi lors de l'exécution de Red Hat Enterprise Linux 6.4 dans VMware ESX. L'installateur Anaconda a aussi été mis à jour pour répertorier les pilotes pendant le processus d'installation. Les pilotes suivants ont été mis à jour :

- pilote réseau (**vmxnet3**)
- pilote de stockage (**vmw_pvscsi**)
- pilote de gonflage mémoire (**vmware_balloon**)
- pilote de souris (**vmmouse_drv**)
- pilote vidéo (**vmware_drv**)

CHAPITRE 9. CLUSTERING

Prise en charge du périphérique Fence IBM iPDU

Red Hat Enterprise Linux 6.4 ajoute la prise en charge du périphérique fence IBM iPDU. Pour obtenir des informations sur les paramètres de ce périphérique fence, reportez-vous à l'annexe *Paramètres de périphériques fence* dans le guide d'*Administration de clusters* de Red Hat Enterprise Linux 6.

Prise en charge du périphérique Fence Eaton Network Power Controller

Red Hat Enterprise Linux 6.4 ajoute la prise en charge de **`fence_eaton_snmp`**, l'agent fence de l'interrupteur d'alimentation réseau Eaton sur SNMP. Pour plus d'informations sur les paramètres de cet agent fence, reportez-vous à l'annexe *Paramètres des périphériques Fence* dans le guide d'*Administration de clusters* de Red Hat Enterprise Linux 6.

Nouveau paquetage keepalived

Red Hat Enterprise Linux 6.4 inclut le paquetage keepalived en tant qu'aperçu technologique. Le paquetage keepalived fournit des aménagements simples et robustes pour l'équilibrage des charges et la haute disponibilité. Le framework d'équilibrage des charges repose sur le module de noyau Linux Virtual Server fournissant un équilibrage des charges réseau Layer 4. Le démon **`keepalived`** implémente un ensemble de vérificateurs de santé pour les pools de serveurs dont les charges ont été équilibrées en fonction de leurs états. Le démon keepalived implémente aussi le protocole VRRP (« Virtual Router Redundancy Protocol »), permettant le basculement de routeur ou de directeur dans le but d'obtenir une haute disponibilité.

Récupération Watchdog

Les nouveaux agents fence **`fence_sanlock`** et **`checkquorum.wdmd`**, inclus dans Red Hat Enterprise Linux 6.4 en tant qu'aperçu technologique fournissent de nouveaux mécanismes pour déclencher la récupération d'un nœud via un périphérique de surveillance (périphérique « watchdog »). Des tutoriaux sur comment activer cet aperçu technologique ŝont disponibles sur https://fedorahosted.org/cluster/wiki/HomePage.

Prise en charge du stockage basé VMDK

Red Hat Enterprise Linux 6.4 ajoute la prise en charge des clusters utilisant la technologie d'image disque de VMware VMDK (« Virtual Machine Disk ») avec l'option « multi-writer ». Ceci vous permet, par exemple, d'utiliser le stockage basé VMDK avec l'option multi-writer pour des systèmes de fichiers clusterisés, comme GFS2.

CHAPITRE 10. STOCKAGE

Prise en charge complète de Parallel NFS

pNFS (Parallel NFS) fait partie du standard NFS v4.1 qui permet aux clients d'accéder directement aux périphériques de stockage en parallèle. L'architecture pNFS peut améliorer l'évolutivité et la performance des serveurs NFS pour des charges de travail communes. Dans Red Hat Enterprise Linux 6.4, pNFS est totalement pris en charge.

pNFS prend en charge 3 types de protocoles ou structures de stockage : les fichiers, objets et blocs. Le client NFS Red Hat Enterprise Linux 6.4 prend en charge le protocole de structure des fichiers.

Pour activer cette nouvelle fonctionnalité, veuillez utiliser l'une des options de montage suivantes sur les montages d'un serveur activé pNFS : **`-o minorversion=1`** ou **`-o v4.1`**.

Lorsque le serveur est activé pNFS-enabled, le module du noyau **`nfs_layout_nfsv41_files`** est automatiquement chargé sur le premier montage. Utilisez la commande suivante pour vérifier que ce module a été chargé :

```
~]$ lsmod | grep nfs_layout_nfsv41_files
```

Pour obtenir plus d'informations sur pNFS, veuillez vous reporter à http://www.pnfs.com/.

Prise en charge XFS Online Discard

Une opération d'abandon en ligne (« Online discard ») effectuée sur un système de fichiers monté abandonne les blocs qui ne sont pas utilisés par le système de fichiers. Les opérations d'abandon en ligne sont maintenant prises en charge sur les systèmes de fichiers XFS. Pour obtenir plus d'informations, veuillez vous reporter à la section *Abandonner les blocs inutilisés* dans le *Guide d'administration du stockage* Red Hat Enterprise Linux 6.

Prise en charge LVM pour Micron PCIe SSD

Dans Red Hat Enterprise Linux 6.4, LVM offre la prise en charge des SSD (« Solid State Drives ») Micron PCIe en tant que périphériques pouvant former une partie d'un groupe de volumes.

Prise en charge LVM pour RAID10 miroir bi-directionnel

LVM est maintenant en mesure de créer, supprimer et redimensionner des volumes logiques RAID10. Pour créer un volume logique RAID10 logical, comme pour les autres types RAID, spécifiez le type de segment comme suit :

```
~]# lvcreate --type raid10 -m 1 -i 2 -L 1G -n lv vg
```

Remarquez que les arguments **`-m`** et **`-i`** se comportent de la même manière qu'ils le feraient avec d'autres types de segments. C'est-à-dire, **`-i`** est le nombre total de bandes, alors que **`-m`** est le nombre de copies (supplémentaires) copies (c'est-à-dire **`-m 1 -i 2`** donne 2 bandes sur des miroirs bi-directionnels).

Paramétrer et gérer des réservations persistantes SCSI via des périphériques Device-Mapper

Auparavant, pour paramétrer des réservations persistantes sur des périphériques à chemins multiples, il était nécessaire de les paramétrer sur tous les périphériques du chemin. Si un périphérique était ajouté au chemin ultérieurement, il était nécessaire d'ajouter manuellement des réservations à ce chemin. Red Hat Enterprise Linux 6.4 offre la possibilité de paramétrer et gérer des réservations SCSI persistantes via les périphériques du mappeur de périphériques avec la commande **`mpathpersist`**. Lorsque des périphériques sont ajoutés au chemin, les réservations persistantes sont aussi paramétrées sur ces périphériques.

CHAPITRE 11. COMPILATEUR ET OUTILS

SystemTap mis à jour à la version 1.8

SystemTap est un outil de traçage et de vérification qui permet aux utilisateurs d'étudier et de suivre minutieusement les activités du système d'exploitation (notamment le noyau). Il fournit des informations similaires à la sortie d'outils comme **netstat**, **ps**, **top**, et **iostat** ; cependant, SystemTap est conçu pour fournir davantage d'options de filtrage et d'analyse sur les informations collectées.

Le paquetage systemtap dans Red Hat Enterprise Linux 6.4 a été mis à niveau à la version en amont 1.8, qui fournit un certain nombre de correctifs de bogues et d'améliorations :

- La syntaxe **`@var`** est maintenant une syntaxe de language alternatif pour accéder aux variables DWARF dans des handlers **`uprobe`** et **`kprobe`** (processus, noyau, module).
- Dorénavant, SystemTap décompose les variables locales pour éviter des collisions avec les en-têtes C (« C headers ») inclus par les tapsets.
- Dorénavant, le serveur de compilation et le client SystemTap prennent en charge les réseaux IPv6.
- L'exécution de SystemTap (**staprun**) permet maintenant l'utilisation de l'option de délai d'expiration **`-T`** afin d'autoriser des réveils moins fréquents pour les sondages des sorties de scripts à bas-débit.
- Le pilote de traduction de script SystemTap (**`stap`**) fournit maintenant les options de limite de ressources suivantes :

```
--rlimit-as=NUM
--rlimit-cpu=NUM
--rlimit-nproc=NUM
--rlimit-stack=NUM
--rlimit-fsize=NUM
```

- Les modules SystemTap sont maintenant plus petits et compilent plus rapidement. Dorénavant, le « debuginfo » des modules est supprimé par défaut.
- Le bogue CVE-2012-0875 (panique noyau lors du traitement de données unwind DWARF malformées) est maintenant corrigé.

Utilitaires lscpu et chcpu

L'utilitaire **lscpu**, qui affiche des informations détaillées sur les CPU disponibles, a été mis à jour afin d'inclure de nombreuses nouvelles fonctionnalités. Ainsi, un nouvel utilitaire, **chcpu**, a été ajouté, celui-ci vous permet de modifier l'état CPU (online/offline, standby/active, et autres états), de désactiver et d'activer les CPU et de configurer des CPU spécifiés.

Pour obtenir davantage d'informations sur ces utilitaires, veuillez vous reporter aux pages man **lscpu(1)** et **chcpu(8)**.

CHAPITRE 12. MISES À JOUR GÉNÉRALES

Paquetages samba mis à jour

Red Hat Enterprise Linux 6.4 inclut des paquetages samba refondus, ceux-ci présentent plusieurs correctifs de bogues et améliorations, dont la plus notable est l'ajout de la prise en charge du protocole SMB2. La prise en charge SMB2 peut être activée à l'aide du paramètre suivant dans la section **[global]** du fichier **/etc/samba/smb.conf** :

```
max protocol = SMB2
```

En outre, Samba prend maintenant en charge le chiffrement AES Kerberos. La prise en charge AES est disponible sur les systèmes d'exploitation Windows Microsoft depuis Windows Vista et Windows Server 2008. Il s'agirait du nouveau type de chiffrement Kerberos par défaut depuis Windows 7. Samba ajoute maintenant des clés Kerberos AES aux fichiers keytab qu'il contrôle. Cela signifie que les autres services Kerberos utilisant les keytabs samba et sont exécutés sur la même machine peuvent bénéficier du chiffrement AES. Afin d'utiliser des clés sessions AES (et non seulement des tickets chiffrés AES fournissant des tickets), le compte de la machine samba dans le serveur LDAP d'Active Directory doit être modifié manuellement. Pour plus d'informations, veuillez vous reporter au Blog de l'équipe Microsoft Open Specifications Support.

AVERTISSEMENT

Les paquetages samba mis à jour modifient aussi la manière dont le mappage d'ID est configurée. Il est recommandé aux utilisateurs de modifier leurs fichiers de configuration Samba existants.

Remarquez que plusieurs fichiers TDB (« Trivial Database ») ont été mis à jour et la prise en charge de l'impression a été ré-écrite afin d'utiliser l'implémentation du registre. Ceci signifie que tous les fichiers TDB sont mis à niveau dès lors que vous démarrez la nouvelle version de **smbd**. Vous ne pouvez pas mettre à niveau vers une version antérieure Samba 3.x à moins que vous ne possédiez des sauvegardes des fichiers TDB.

Pour obtenir plus d'informations sur ces modifications, reportez-vous aux Notes de mise à jour Samba 3.6.0.

Nouveau paquetage SciPy

Red Hat Enterprise Linux 6.4 inclut un nouveau paquetage scipy. Le paquetage SciPy fournit un logiciel pour les mathématiques, sciences et ingénierie. Le paquetage NumPy, qui est conçu pour manipuler de grandes matrices multi-dimensionnelles d'enregistrements arbitraires, est la bibliothèque principale de SciPy. La bibliothèque SciPy est conçue pour fonctionner avec les matrices NumPy et pour fournir diverses routines numériques efficaces, par exemple des routines pour effetuer une intégration et optimisation numérique.

Prise en charge TLS v1.1 dans NSS

Les paquetages nss et nss-util ont été mis à niveau vers la version en amont 3.14, ce afin de fournir, entre autres, la prise en charge de TLS version 1.1. Le paquetage nspr a aussi été rebasé pour la version 4.9.2. Pour obtenir des informations supplémentaires, veuillez vous reporter aux Notes de mise à jour NSS 3.14.

`gdbserver` Valgrind intégré

Le paquetage valgrind a été mis à niveau à la version en amont 3.8.1. Cette version mise à jour contient, entre autres améliorations et correctifs de bogues, un **`gdbserver`** intégré. Pour obtenir plus d'informations, veuillez vous reporter au chapitre *Valgrind* et à l'annexe *Changements dans Valgrind 3.8.1* du *Guide d'utilisation Red Hat Developer Toolset 1.1*.

Nouveaux paquetages libjpeg-turbo

Red Hat Enterprise Linux 6.4 inclut un nouvel ensemble de paquetages : libjpeg-turbo. Ces paquetages remplacent les paquetages libjpeg traditionnels, ils fournissent les mêmes fonctionnalités et API que libjpeg, mais délivrent une meilleure performance.

Nouveau paquetage redhat-lsb-core

Lors de l'installation du paquetage redhat-lsb, le système doit recevoir un grand nombre de dépendances afin de correspondre au standard LSB. Red Hat Enterprise Linux 6.4 fournit un nouveau sous-paquetage redhat-lsb-core permettant de facilement récupérer l'ensemble minimum des paquetages requis en installant le paquetage redhat-lsb-core package.

Utilitaire createrepo mis à jour

L'utilitaire **createrepo** a été mis à jour à la dernière version en amont, ce qui réduit l'utilisation de mémoire de manière significative et ajoute la prise en charge de multiples tâches (« multitasking ») via l'option **`--workers`**.

ANNEXE A. HISTORIQUE DE RÉVISION

Version 1.1-12.1.400 **2013-10-31** **Rüdiger Landmann**

Rebuild with publican 4.0.0

Version 1.1-12.1 **Mon Jan 21 2013** **Sam Friedmann**

Translation files synchronised with XML sources 1.1-12

Version 1.1-12 **Wed Dec 4 2012** **Martin Prpič**

Publication des notes de mise à jour de Red Hat Enterprise Linux 6.4 Beta.