Red Hat Enterprise Linux 7
Notes de version 7.1

Notes de version de Red Hat Enterprise Linux 7

Red Hat Customer Content Services

Red Hat Enterprise Linux 7 Notes de version 7.1

Notes de version de Red Hat Enterprise Linux 7

Red Hat Customer Content Services

Notice légale

Résumé

Les notes de version documentent les fonctionnalités et améliorations majeures apportées à la version Red Hat Enterprise Linux 7.1 ainsi que les problèmes connus dans cette version 7.1. Pour obtenir des informations détaillées concernant les changements entre Red Hat Enterprise Linux 6 et 7, veuillez consulter le Guide de planification de migration Remerciements Le service de support technique Red Hat Global Support Services tient à remercier Sterling Alexander et Michael Everette pour leur contribution exceptionnelle lors des tests de Red Hat Enterprise Linux 7.

Table des matières

Préface

Les versions mineures de Red Hat Enterprise Linux comprennent des améliorations individuelles, des améliorations de la sécurité, ainsi que des errata de correctifs de bogues. Les *Notes de version Red Hat Enterprise Linux 7.1* documentent les changements majeurs, les fonctionnalités et les améliorations apportées au système d'exploitation Red Hat Enterprise Linux 7 et aux applications l'accompagnant dans cette version mineure. En outre, les *Notes de version Red Hat Enterprise Linux 7.1* documentent les problèmes connus dans Red Hat Enterprise Linux 7.1.

Important

Les *Notes de version Red Hat Enterprise Linux 7.1* en ligne, qui sont disponibles ici, sont considérées comme étant la version à jour et définitive. Nos clients ayant des questions sur la mise à jour sont invités à consulter les *Notes de version* et de trouver leur version de Red Hat Enterprise Linux.

Note

Pour obtenir la description des problèmes connus, veuillez consulter la Version anglaise des Notes de version Red Hat Enterprise Linux 7.1.

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/.

Partie I. Nouvelles fonctionnalités

Cette partie décrit les nouvelles fonctionnalités et améliorations majeures offertes par Red Hat Enterprise Linux 7.1.

Chapitre 1. Architectures

Red Hat Enterprise Linux 7.1 est disponible en tant que kit 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.

1.1. Red Hat Enterprise Linux pour POWER, Little Endian

Red Hat Enterprise Linux 7.1 offre la prise en charge little endian sur les serveurs IBM Power Systems utilisant les processeurs IBM POWER8. Auparavant, avec Red Hat Enterprise Linux 7, seule la variante big endian était offerte pour IBM Power Systems. La prise en charge de little endian sur serveurs basés POWER8 vise à améliorer la portabilité des applications entre les systèmes compatibles Intel 64 bits (**x86_64**) et les systèmes IBM Power Systems.

- Des supports d'installatation séparés sont offerts pour installer Red Hat Enterprise Linux sur des serveurs IBM Power Systems en mode little endian. Ces supports sont disponibles à partir de la section Téléchargement du Portail Client Red Hat.
- Seuls les serveurs basés sur processeurs IBM POWER8 sont pris en charge avec Red Hat Enterprise Linux pour POWER, little endian.
- Actuellement, Red Hat Enterprise Linux pour POWER, little endian est uniquement pris en charge en tant qu'invité KVM sous **Red Hat Enteprise Virtualization for Power**. Les installations sur matériel bare metal ne sont pas prises en charge pour le moment.
- Le chargeur de démarrage **GRUB2** est utilisé sur le support d'installation et pour le démarrage réseau. Le Guide d'installation a été mis à jour avec des instructions pour paramétrer un serveur de démarrage réseau pour les clients IBM Power Systems utilisant **GRUB2**.
- Tous les paquets logiciels pour IBM Power Systems sont disponibles pour les variantes little endian et big endian de Red Hat Enterprise Linux pour POWER.
- Les paquets créés pour Red Hat Enterprise Linux pour POWER, little endian utilisent le code d'architecture **ppc64le** - par exemple, *gcc-4.8.3-9.ael7b.ppc64le.rpm*.

[1] Remarquez que l'installation Red Hat Enterprise Linux 7.1 est uniquement prise en charge sur du matériel 64 bits. Red Hat Enterprise Linux 7.1 est capable d'exécuter des systèmes d'exploitation 32 bits en tant que machines virtuelles, y compris des versions précédentes de Red Hat Enterprise Linux.

[2] Actuellement, Red Hat Enterprise Linux 7.1 (little endian) est uniquement pris en charge en tant qu'invité KVM sous les hyperviseurs **Red Hat Enteprise Virtualization for Power** et **PowerVM**.

[3] Remarquez que Red Hat Enterprise Linux 7.1 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 7.1.

Chapitre 2. Hardware Enablement

2.1. Intel Broadwell Processor and Graphics Support

Red Hat Enterprise Linux 7.1 adds support for all current 5th generation Intel processors (code name Broadwell). Support includes the CPUs themselves, integrated graphics in both 2D and 3D mode, and audio support (Broadwell High Definition Legacy Audio, HDMI Audio and DisplayPort Audio).

The **turbostat** tool (part of the *kernel-tools* package) has also been updated with support for the new processors.

2.2. Support for TCO Watchdog and I2C (SMBUS) on Intel Communications Chipset 89xx Series

Red Hat Enterprise Linux 7.1 adds support for TCO Watchdog and I2C (SMBUS) on the 89xx series Intel Communications Chipset (formerly Coleto Creek).

2.3. Intel Processor Microcode Update

CPU microcode for Intel processors in the *microcode_ctl* package has been updated from version **`0x17`** to version **`0x1c`** in Red Hat Enterprise Linux 7.1.

Chapitre 3. Installation et démarrage

3.1. Installateur

L'installateur Red Hat Enterprise Linux, **Anaconda**, a été amélioré afin d'obtenir un meilleur processus d'installation pour Red Hat Enterprise Linux 7.1.

Interface

- L'interface de l'installateur graphique contient désormais un écran supplémentaire qui active la configuration du mécanisme de vidage sur incident du noyau **Kdump** pendant l'installation. Précédemment, celle-ci était configurée après l'installation, à l'aide de l'utilitaire **firstboot**, qui n'était pas accessible sans une interface graphique. Désormais, vous pouvez configurer **Kdump** comme faisant partie du processus d'installation sur les systèmes sans environnement graphique. Le nouvel écran est accessible à partir du menu principal de l'installateur (**`Sommaire de l'installation`**).

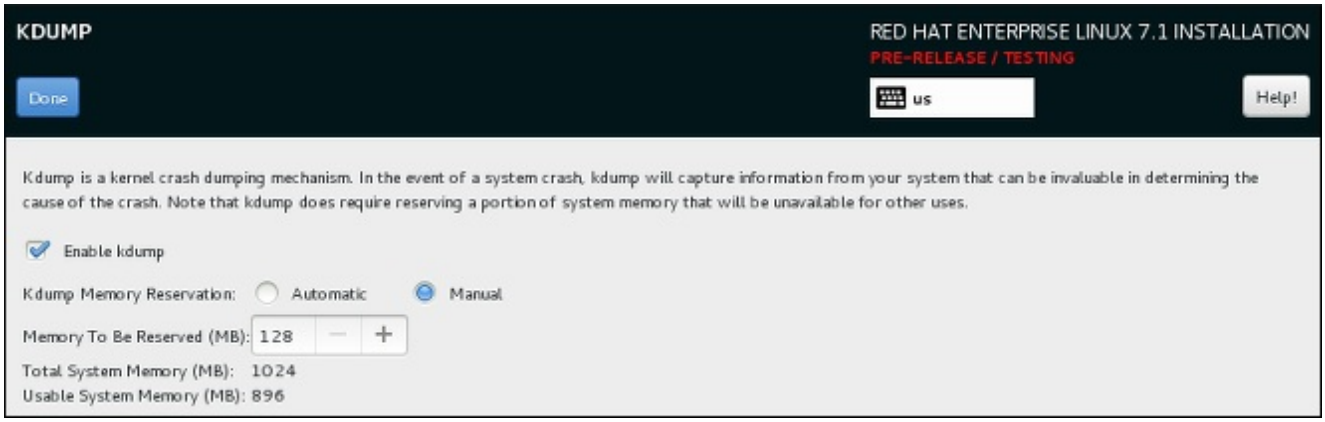

Figure 3.1. Le nouvel écran Kdump

- L'écran de partitionnement manuel a été reconçu pour améliorer l'expérience utilisateur. Certaines commandes ont été déplacées dans différents emplacements sur l'écran.

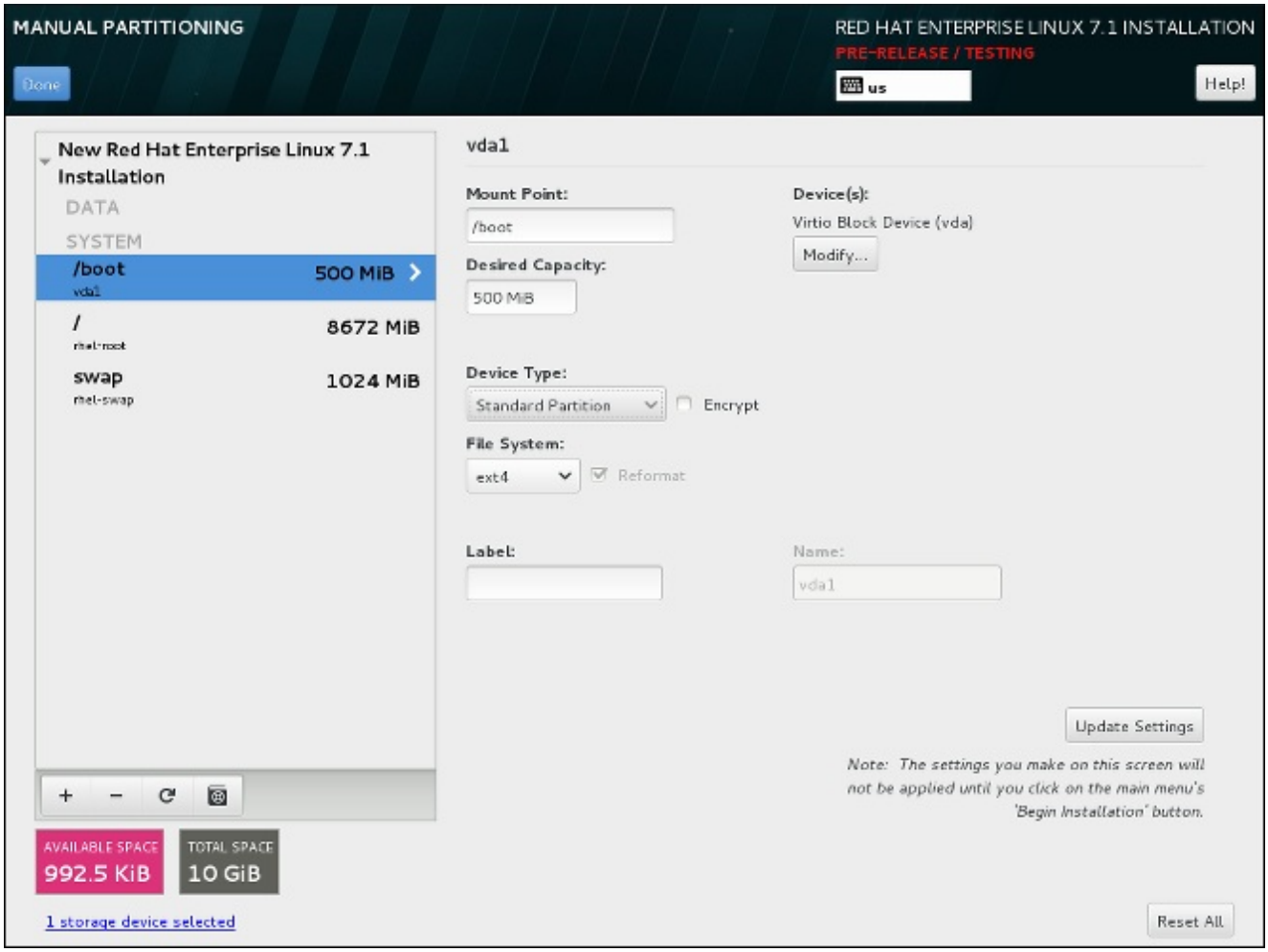

Figure 3.2. L'écran de partitionnement manuel reconçu

- Vous pouvez désormais configurer un pont réseau dans l'écran **Nom d'hôte & Réseau** de l'installateur. Pour ce faire, veuillez cliquer sur le bouton **+** en bas de la liste des interfaces, sélectionnez **Bridge** à partir du menu, et configurez le pont dans la boîte de dialogue **Modifier la connexion du pont** qui apparaît après. Cette boîte de dialogue est fournie par **NetworkManager** et est entièrement documentée dans le *Guide de mise en réseau Red Hat Enterprise Linux 7.1*.

  Plusieurs nouvelles options Kickstart ont aussi été ajoutée pour la configuration du pont. Veuillez voir ci-dessous pour les détails.

- L'installateur n'utilise plus de multiples consoles pour afficher les enregistrements. À la place, tous ces enregistrements se trouvent dans des volets **tmux** dans la console virtuelle 1 (**tty1**). Pour accéder aux enregistrements pendant l'installation, appuyez sur **Ctrl**+**Alt**+**F1** pour basculer sur **tmux**, puis utilisez **Ctrl**+**b** ***X*** pour basculer entre différentes fenêtres (remplacez *X* par le numéro d'une fenêtre en particulier comme affiché en bas de l'écran).

  Pour revenir à l'interface graphique, appuyez sur **Ctrl**+**Alt**+**F6**.

- L'interface de ligne de commande d'**Anaconda** inclut désormais une aide complète. Pour l'afficher, veuillez utiliser la commande **anaconda -h** sur un système avec le paquet *anaconda* installé. L'interface de ligne de commande vous permet d'exécuter l'installateur sur un système installé, ce qui est utile pour les installations d'images de disque.

Commandes et options Kickstart

- La commande **logvol** possède une nouvelle option : **--profile=**. Veuillez utiliser cette option pour spécifier un nom de profil de configuration à utiliser avec les volumes logiques fins. Si utilisé, le nom sera aussi inclut dans les métadonnées pour le volume logique.

  Par défaut, les profils disponibles sont **default** et **thin-performance** et sont définis dans le répertoire **/etc/lvm/profile**. Veuillez consulter la page man **lvm(8)** pour obtenir des informations supplémentaires.

- The behavior of the **--size=** and **--percent=** options of the **logvol** command has changed. Previously, the **--percent=** option was used together with **--grow** and **--size=** to specify how much a logical volume should expand after all statically-sized volumes have been created.

  Starting with Red Hat Enterprise Linux 7.1, **--size=** and **--percent=** can not be used on the same **logvol** command.

- L'option **--autoscreenshot** de la commande Kickstart **autostep** a été corrigée, et enregistre désormais correctement une capture d'écran de chaque écran dans le répertoire **/tmp/anaconda-screenshots** lors de la fermeture de celui-ci. Une fois l'installation terminée, ces captures d'écran sont déplacées dans **/root/anaconda-screenshots**.

- La commande **liveimg** prend désormais en charge les installation à partir de fichiers tar ainsi que les images de disque. L'archive tar doit contenir le système de fichier root du support d'installation, et le nom du fichier doit se terminer par **.tar**, **.tbz**, **.tgz**, **.txz**, **.tar.bz2**, **.tar.gz**, ou **.tar.xz**.

- Plusieurs nouvelles options ont été ajoutés à la commande **network** pour configurer les ponts réseau. Ces options sont :

  - **--bridgeslaves=** : Lorsque cette option est utilisée, le pont réseau avec le nom de périphérique spécifié à l'aide de l'option **--device=** sera créée et les périphériques définis dans l'option **--bridgeslaves=** seront ajoutés au pont. Par exemple :

    ```
    network --device=bridge0 --bridgeslaves=em1
    ```

  - **--bridgeopts=** : Liste des paramètres de l'interface liée par pont séparés par des virgules. Les valeurs disponibles sont **stp**, **priority**, **forward-delay**, **hello-time**, **max-age**, et **ageing-time**. Pour obtenir des informations sur ces paramètres, veuillez consulter la page man **nm-settings(5)**.

- La commande **autopart** possède une nouvelle option option, **--fstype**. Cette option vous permet de modifier le type de système de fichiers par défaut (**xfs**) lors de l'utilisation du partitionnement automatique dans un fichier Kickstart.

- Several new features were added to Kickstart for better container support. These features include:

  - **repo --install** : Cette nouvelle option enregiste la configuration du référentiel sur le système installé dans le répertoire **/etc/yum.repos.d/**. Sans utiliser cette option, un référentiel configuré dans un fichier Kickstart sera uniquement disponible pendant le processus d'installation, et non sur le système installé.

  - **bootloader --disabled** : Cette option empêchera le chargeur de démarrage d'être installé.

  - **%packages --nocore** : Une nouvelle option pour la section **%packages** d'un fichier Kickstart qui empêche le système d'installer le groupe de paquets **@core**. Ceci active l'installation extrêmement minimale de systèmes pour une utilisation avec des conteneurs.

  Please note that the described options are only useful when combined with containers, and using the options in a general-purpose installation could result in an unusable system.

Entropy Gathering for LUKS Encryption

- If you choose to encrypt one or more partitions or logical volumes during the installation (either during an interactive installation or in a Kickstart file), **Anaconda** will attempt to gather 256 bits of entropy (random data) to ensure the encryption is secure. The installation will continue after 256 bits of entropy are gathered or after 10 minutes. The attempt to gather entropy happens at the beginning of the actual installation phase when encrypted partitions or volumes are being created. A dialog window will open in the graphical interface, showing progress and remaining time.

  The entropy gathering process can not be skipped or disabled. However, there are several ways to speed the process up:

  - If you can access the system during the installation, you can supply additional entropy by pressing random keys on the keyboard and moving the mouse.
  - If the system being installed is a virtual machine, you can attach a *virtio-rng* device (a virtual random number generator) as described in the Red Hat Enterprise Linux 7.1 Virtualization Deployment and Administration Guide.

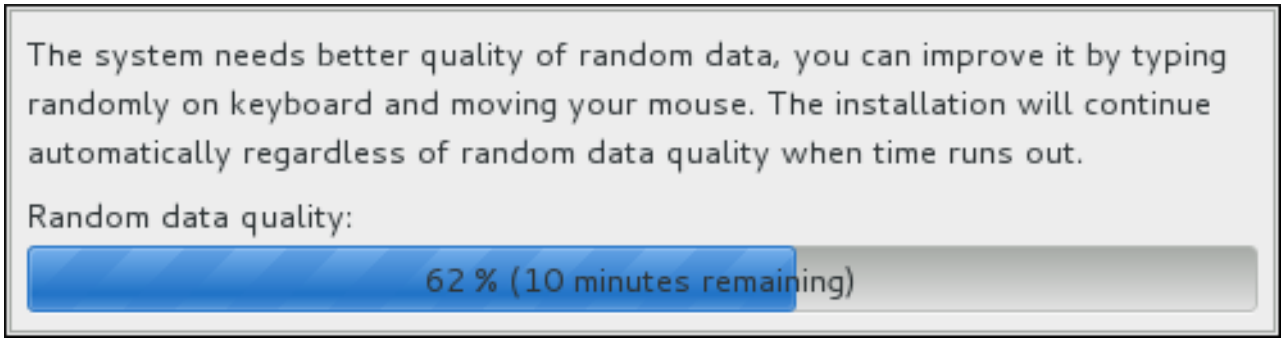

Figure 3.3. Gathering Entropy for Encryption

Aide intégrée dans l'installateur graphique

Chaque écran dans l'interface graphique de l'installateur et dans l'utilitaire **Initial Setup** possède désormais un bouton d'**Aide** dans le coin en haut à droite. Cliquer sur ce bouton ouvre une section du Guide d'installation concernant l'écran actuel en utilisant le navigateur d'aide **Yelp**.

Figure 3.4. Anaconda built-in help

3.2. Chargeur de démarrage

Le support d'installation pour IBM Power Systems utilise désormais le chargeur de démarrage **GRUB2** à la place de **yaboot**, qui était précédemment offert. Pour la variante big endian de Red Hat Enterprise Linux sur POWER, **GRUB2** est recommandé mais **yaboot** peut aussi être utilisé. La nouvelle variante, little endian, requiert le démarrage **GRUB2**.

Le Guide d'installation a été mis à jour avec des instructions pour paramétrer un serveur de démarrage réseau pour systèmes IBM Power Systems utilisant **GRUB2**.

Chapitre 4. Stockage

Cache LVM

As of Red Hat Enterprise Linux 7.1, LVM cache is fully supported. This feature allows users to create logical volumes with a small fast device performing as a cache to larger slower devices. Please refer to the **lvm(7)** manual page for information on creating cache logical volumes.

Remarquez les restrictions suivantes sur l'utilisation de volumes logiques de cache (LV) :

- Le volume logique du cache doit être un périphérique de haut niveau. Il ne peut pas être utilisé en tant que pool dynamique, image de volume logique RAID, ou comme tout autre type de sous-volume logique.
- The cache LV sub-LVs (the origin LV, metadata LV, and data LV) can only be of linear, stripe, or RAID type.
- Les propriétés du volume logique de cache ne peuvent pas être modifiées après leur création. Pour modifier les propriétés du cache, supprimez le cache puis recréez-le avec les propriétés souhaitées.

Gestion de matrices de stockage avec l'API libStorageMgmt

Avec Red Hat Enterprise Linux 7.1, la gestion de matrices de stockage avec **libStorageMgmt**, une interface de programmation indépendante des matrices de stockage, est totalement prise en charge. L'interface de programmation fournie est stable, cohérente et permet aux développeurs de gérer de manière programmatique différentes matrices de stockage et d'utiliser les fonctionnalités accélérées par le matériel fournies. Les administrateurs système peuvent également utiliser **libStorageMgmt** pour configurer le stockage manuellement et pour automatiser les tâches de gestion du stockage avec l'interface de ligne de commande incluse. Veuillez remarquer que le greffon **Targetd** n'est pas totalement pris en charge et reste un aperçu technologique.

- NetApp Filer (ontap 7-Mode)
- Nexenta (nstor 3.1.x uniquement)
- SMI-S, pour les fournisseurs suivants :
  - HP 3PAR
    - OS version 3.2.1 ou plus récente
  - EMC VMAX et VNX
    - Solutions Enabler V7.6.2.48 ou version plus récente
    - Kit de correctifs à chaud SMI-S Provider V4.6.2.18 ou version plus récente
  - Fournisseur non-intégré HDS VSP Array
    - Hitachi Command Suite v8.0 ou version plus récente

Pour obtenir des informations supplémentaires sur **libStorageMgmt**, veuillez consulter le chapitre correspondant dans le Guide d'administration du stockage.

Prise en charge de LSI Syncro

Red Hat Enterprise Linux 7.1 inclut le code dans le pilote **megaraid_sas** pour activer les adaptateurs HA-DAS (« High Availability Direct Attached Storage ») LSI Syncro CS. Malgré le fait que le pilote **megaraid_sas** est entièrement pris en charge pour les adaptateurs précédemment activés, l'utilisation de ce pilote pour Syncro CS est uniquement disponible en tant qu'aperçu technologique. La prise en charge de cet adaptateur sera fourni directement par LSI, votre intégrateur système ou votre fournisseur système. Les utilisateurs déployant Syncro CS sur Red Hat Enterprise Linux 7.1 sont encouragés à donner des commentaires et suggestions à Red Hat et LSI. Pour obtenir des informations supplémentaires sur les solutions LSI Syncro CS, veuillez vous rendre sur http://www.lsi.com/products/shared-das/pages/default.aspx.

Interface de programmation d'application LVM

Red Hat Enterprise Linux 7.1 présente la nouvelle API LVM en tant qu'aperçu technologique. Cette API est utilisée pour effectuer des requêtes et contrôler certains aspects de LVM.

Veuillez consulter le fichier d'en-tête **lvm2app.h** pour obtenir des informations supplémentaires.

Prise en charge DIF/DIX

DIF/DIX est une nouvelle addition au standard SCSI et un aperçu technologique dans Red Hat Enterprise Linux 7.1. 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.

For more information, refer to the section Block Devices with DIF/DIX Enabled in the Storage Administration Guide.

Vérification et sortie d'erreurs de syntaxe device-mapper-multipath améliorée

L'outil **device-mapper-multipath** a été amélioré pour vérifier le fichier **multipath.conf** de manière plus fiable. Par conséquent, si **multipath.conf** contient une ligne ne pouvant pas être analysée de manière syntaxique, **device-mapper-multipath** rapporte une erreur et ignore ces lignes afin d'éviter qu'une analyse syntaxique incorrecte ne soit effectuée.

En outre, les expressions génériques suivantes ont été ajoutées à la commande **multipathd show paths format** :

- %N et %n pour les noms des nœuds globaux Fibre Channel (« Fibre Channel World Wide Node Names ») de l'hôte et de la cible, respectivement.
- %R et %r pour les noms des ports globaux Fibre Channel (« Fibre Channel World Wide Port Names ») de l'hôte et de la cible, respectivement.

Il est désormais plus facile d'associer des périphériques multipaths à des hôtes et des cibles Fibre Channel et leurs ports, ce qui permet aux utilisateurs de gérer leur configuration du stockage de manière plus efficace.

Chapitre 5. Systèmes de fichiers

Prise en charge du système de fichiers Btrfs

Le système de fichiers **`Btrfs`** (B-Tree) est pris en charge en tant qu'aperçu technologique dans Red Hat Enterprise Linux 7.1. Ce système de fichier offre des fonctionnalités de gestion, fiabilité et évolutivité avancées. Il permet aux utilisateurs de créer des instantanés, et active la compression et la gestion de périphériques intégrée.

OverlayFS

The **`OverlayFS`** file system service allows the user to "overlay" one file system on top of another. Changes are recorded in the upper fil esystem, while the lower file system becomes read-only. This can be useful because it allows multiple users to share a file system image, for example containers, or when the base image is on read-only media, for example a DVD-ROM.

On Red Hat Enterprise Linux 7.1, OverlayFS is supported as a Technology Preview. There are currently two restrictions:

- It is recommended to use **`ext4`** as the lower file system; the use of **`xfs`** and **`gfs2`** file systems is not supported.
- SELinux is not supported, and to use OverlayFS, it is required to disable enforcing mode.

Prise en charge de NFS parallèle

NFS parallèle (pNFS) fait partie du standard NFS v4.1 qui permet aux clients d'accéder à des périphériques de stockage directement et en parallèle. L'architecture pNFS peut améliorer l'évolutivité et les performances des serveurs NFS pour plusieurs charges de travail communes.

pNFS defines three different storage protocols or layouts: files, objects, and blocks. The client supports the files layout, and with Red Hat Enterprise Linux 7.1, the blocks and object layouts are fully supported.

Red Hat continue à travailler avec les projets open source et de ses partenaires afin de qualifier de nouveaux types de disposition pNFS et pour fournir une prise en charge totale sur davantage de types de dispositions dans le futur.

Pour obtenir des informations supplémentaires sur pNFS, veuillez consulter http://www.pnfs.com/.

Chapitre 6. Noyau

Prise en charge des périphériques blocs Ceph

Les modules **libceph.ko** et **rbd.ko** ont été ajoutés au noyau Red Hat Enterprise Linux 7.1. Ces modules de noyau RBD permettent à un hôte Linux de voir un périphérique bloc Ceph en tant qu'entrée de périphérique de disque normale, pouvent être montée sur un répertoire et formatée avec un système de fichiers standard, tel que **XFS** ou **ext4**.

Remarquez que le module CephFS, **ceph.ko**, n'est pas actuellement pris en charge sur Red Hat Enterprise Linux 7.1.

Mises à jour concurrentes Flash MCL

Les mises à jour du niveau de microcode (MCL) sont activées dans Red Hat Enterprise Linux 7.1 sur l'architecture IBM System z. Ces mises à niveau peuvent être appliquées sans impact sur les opérations d'E/S sur le support de stockage flash et notifie les utilisateurs du niveau de service du matériel flash modifié.

Correctifs dynamiques du noyau

Red Hat Enterprise Linux 7.1 présente **kpatch**, un « utilitaire de correction du noyau » dynamique, en tant qu'aperçu technologique. L'utilitaire **kpatch** permet aux utilisateurs de gérer une collection de correctifs du noyau binaires pouvant être utilisés pour corriger le noyau dynamiquement, sans avoir à effectuer de redémarrage. Veuillez remarquer que **kpatch** est pris en charge pour une exécution sur architectures AMD64 et Intel 64 uniquement.

Crashkernel avec plus d'un CPU

Red Hat Enterprise Linux 7.1 active le démarrage de crashkernel avec plus d'un CPU. Cette fonction est prise en charge en tant qu'aperçu technologique.

Cible dm-era

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 « ère » (de l'anglais, « era »). Chaque 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.

Pilote de noyau Cisco VIC

Le pilote de noyau Infiniband Cisco VIC a été ajouté à Red Hat Enterprise Linux 7.1 en tant qu'aperçu technologique. Ce pilote permet l'utilisation de sémantiques similaires à RDMA (« Remote Directory Memory Access ») sur architectures propriétaires Cisco.

Gestion de l'entropie améliorée dans hwrng

La prise en charge RNG de matériel paravirtualisé (hwrng) pour invités Linux via virtio-rng a été améliorée dans Red Hat Enterprise Linux 7.1. Précédemment, le démon **rngd** devait être démarré à l'intérieur de l'invité et dirigé vers le pool d'entropie du noyau. À partir de Red Hat Enterprise Linux 7.1, l'étape manuelle est supprimée. Un nouveau thread **khwrngd** cherche l'entropie à partir du périphérique **virtio-rng** si

l'entropie de l'invité tombe sous un niveau spécifique. Le fait de rendre ce processus transparent aide tous les invités Red Hat Enterprise Linux à tirer profit des bénéfices de sécurité offerts par le RNG matériel paravirtualisé fournit par les hôtes KVM.

Amélioration des performances d'équilibrage des charges du planificateur

Précédemmant, le code d'équilibrage des charges du planificateur équilibrait tous les CPU inactifs. Dans Red Hat Enterprise Linux 7.1, l'équilibrage des charges pour le compte d'un CPU inactif est uniquement effectué lorsque le CPU doit effectuer l'équilibrage des charges. Ce nouveau comportement réduit le taux d'équilibrage des charges sur les CPU actifs et par conséquent la quantité de travail non nécessaire effectué par le planificateur, ce qui améliore ses performances.

Équilibrage newidle amélioré dans le planificateur

Le comportement du planificateur a été modifié pour arrêter de rechercher des tâches dans le code d'équilibrage **`newidle`** s'il y a des tâches exécutables, ce qui conduit à de meilleures performances

HugeTLB prend en charge l'allocation Huge Page 1 Go par nœud

Red Hat Enterprise Linux 7.1 a ajouté la prise en charge de l'allocation de pages gigantesque lors du runtime, ce qui permet aux utilisateurs de **`hugetlbfs`** de 1 Go de spécifier le nœud NUMA (« Non-Uniform Memory Access ») qui devrait être alloué pendant le runtime.

Nouveau mécanisme de verrouillage basé MCS

Red Hat Enterprise Linux 7.1 présente un nouveau mécanisme de verrouillage, le verrouillage MCS. Ce nouveau mécanisme de verrouillage réduit l'alourdissement **`spinlock`** dans les systèmes de grande taille, ce qui rend **`spinlocks`** plus efficace dans Red Hat Enterprise Linux 7.1.

Augmentation de la taille de la pile de processus de 8 Ko à 16 Ko

À partir de Red Hat Enterprise Linux 7.1, la taille de la pile de processus du noyau a augmenté de 8 Ko à 16 Ko afin d'aider les processus de grande taille à utiliser l'espace de la pile.

Fonctionnalités uprobe et uretprobe activées dans perf et systemtap

Avec Red Hat Enterprise Linux 7.1, les fonctionnalités **`uprobe`** et **`uretprobe`** fonctionnent correctement avec la commande **`perf`** et le script **`systemtap`**.

Vérification de la cohérence des données dun bout à l'autre

La vérification de la cohérence de données d'un bout à l'autre sur IBM System z est totalement prise en charge dans Red Hat Enterprise Linux 7.1. Ceci améliore l'intégrité des données et empêche la corruption et la perte des données de manière plus efficace.

DRBG sur systèmes 32 bits

Avec Red Hat Enterprise Linux 7.1, DRBG (« Deterministic Random Bit Generator ») a été mis à jour pour fonctionner sur des systèmes 32 bits.

Prise en charge des crashkernel de grande taille

The **Kdump** kernel crash dumping mechanism on systems with large memory, that is up to the Red Hat Enterprise Linux 7.1 maximum memory supported limit of 6TB, has become fully supported in Red Hat Enterprise Linux 7.1.

Chapitre 7. Virtualisation

Nombre maximum de vCPU dans KVM augmenté

Le nombre maximum de CPU virtuels (vCPU) dans un invité KVM a été augmenté jusqu'à 240. Ceci augmente la quantité d'unités de traitement virtuel qu'un utilisateur peut assigner à l'invité, ce qui améliore le potentiel de performance.

Prise en charge des nouvelles instructions Intel Core de 5ème génération dans QEMU, KVM, et l'API libvirt

Avec Red Hat Enterprise Linux 7.1, la prise en charge des processeurs Intel Core de 5ème génération a été ajouté à l'hyperviseur QEMU, le code du noyau KVM, et l'API **`libvirt`**. Ceci permet aux invités KVM d'utiliser les instructions et fonctionnalités suivantes : ADCX, ADOX, RDSFEED, PREFETCHW, et SMAP (« Supervisor Mode Access Prevention »).

Prise en charge USB 3.0 pour les invités KVM

Red Hat Enterprise Linux 7.1 offre une prise en charge USB améliorée grâce à l'ajout de l'émulation USB 3.0 hostadapter (xHCI) en tant qu'aperçu technologique.

Compression pour la commande dump-guest-memory

Avec Red Hat Enterprise Linux 7.1, la commande **`dump-guest-memory`** prend en charge la compression du vidage sur incident. Ceci permet aux utilisateurs qui ne peuvent pas utiliser la commande **`virsh dump`** de nécessiter moins d'espace disque pour les vidages sur incident des invités. En outre, l'enregistrement fréquent de vidages sur incident compressés d'un invité prend moins de temps que l'enregistrement d'un vidage non compressé.

Microprogramme Open Virtual Machine Firmware

OMVF (« Open Virtual Machine Firmware ») est disponible en tant qu'aperçu technologique dans Red Hat Enterprise Linux 7.1. OVMF est un environnement de démarrage sécurisé UEFI pour invités AMD64 et Intel 64.

Amélioration des performances réseau sur Hyper-V

Plusieurs nouvelles fonctionnalités du pilote réseau Hyper-V sont prises en charge pour améliorer les performances réseau. Par exemple, la mise à l'échelle côté réception, la décharge d'envois de grande taille, les E/S de ventilation/regroupement sont désormais pris en charge, et le débit réseau est augmenté.

hypervfcopyd dans hyperv-daemons

Le démon **`hypervfcopyd`** a été ajouté aux paquets *hyperv-daemons*. **`hypervfcopyd`** est une implémentation d'une fonctionnalité de service de copie de fichier pour un invité Linux exécuté sur hôte Hyper-V 2012 R2. Il permet à l'hôte de copier un fichier (sur VMBUS) dans l'invité Linux.

Nouvelles fonctionnalités dans libguestfs

Red Hat Enterprise Linux 7.1 présente un certain nombre de fonctionnalités dans **`libguestfs`**, un ensemble d'outils pour accéder et modifier des images de disque de machines virtuelles.

Nouveaux outils

- **`virt-builder`** — nouvel outil pour créer des images de machine virtuelle. Veuillez utiliser virt-builder pour créer et personnaliser des invités rapidement et de manière sécurisée.
- **`virt-customize`** — nouvel outil pour personnaliser des images de disque de machines virtuelles. Veuillez utiliser virt-customize pour installer des paquets, modifier des fichiers de configuration, exécuter des scripts et pour définir des mots de passe.
- **`virt-diff`** — nouvel outil pour afficher les différences entres systèmes de fichiers de deux machines virtuelles. Veuillez utiliser virt-diff pour découvrir facilement quels fichiers ont été modifiés entre les snapshots.
- **`virt-log`** — nouvel outil pour répertorier les fichiers journaux des invités. L'outil virt-log prend en charge toute une variété d'invités, y compris Linux traditionnell, Linux utilisant un journal, et le journal d'événements Windows.
- **`virt-v2v`** — nouvel outil pour convertir les invités d'un hyperviseur étranger pour qu'ils puissent fonctionner sur KVM, géré par libvirt, OpenStack, oVirt, Red Hat Enterprise Virtualization (RHEV), plusieurs autres cibles. Actuellement, virt-v2v peut convertir des invités Red Hat Enterprise Linux et Windows fonctionnant sur Xen et VMware ESX.

Suivi de l'enregistreur de vol

Support for flight recorder tracing has been introduced in Red Hat Enterprise Linux 7.1. Flight recorder tracing uses **`SystemTap`** to automatically capture qemu-kvm data as long as the guest machine is running. This provides an additional avenue for investigating qemu-kvm problems, more flexible than qemu-kvm core dumps.

Pour obtneir des instructions supplémentaires sur la manière de configurer et d'utiliser le suivi d'enregistreur de vol, veuillez consulter le Guide d'administration et de déploiement de la virtualisation.

RDMA-based Migration of Live Guests

The support for Remote Direct Memory Access (RDMA)-based migration has been added to **`libvirt`**. As a result, it is now possible to use the new **`rdma://`** migration URI to request migration over RDMA, which allows for significantly shorter live migration of large guests. Note that prior to using RDMA-based migration, RDMA has to be configured and **`libvirt`** has to be set up to use it.

Chapitre 8. Clustering

Délai d'expiration dynamique des jetons pour Corosync

L'option **token_coefficient** a été ajoutée à **Corosync Cluster Engine**. La valeur de **token_coefficient** est uniquement utilisée lorsque la section **nodelist** est spécifiée et contient au moins trois nœuds. Dans une telle situation, le délai d'expiration est calculé comme suit :

```
[jeton + (quantité de nœuds - 2)] * token_coefficient
```

Ceci permet au cluster de se mettre à l'échelle sans avoir à modifier le délai d'expiration du jeton à chaque fois qu'un nouveau nœud est ajouté. La valeur par défaut est de 650 millisecondes, mais peut être paramétrée sur 0, résultant ainsi par la suppression de cette fonctionnalité.

Cette fonctionnalité permet à **Corosync** de gérer l'ajout et la suppression dynamique de nœuds.

Amélioration du Tie Breaker Corosync

La fonctionnalité du quorum **auto_tie_breaker** de **Corosync** a été améliorée afin de fournir des options permettant la configuration et des modifications des nœuds tie breaker plus flexible. Les utilisateurs peuvent désormais sélectionner une liste de nœuds qui conserveront le quorum en cas de scission équitable du cluster, ou choisir qu'un quorum sera conservé par le nœud avec l'ID de nœud le plus bas ou le plus haut.

Améliorations de Red Hat High Availability

Avec Red Hat Enterprise Linux 7.1, le module complémentaire **Red Hat High Availability** prend désormais en charge les fonctionnalités suivantes. Pour obtenir des informations sur ces fonctionnalités, veuillez consulter le manuel *Référence du module complémentaire High Availability*.

- La commande **pcs resource cleanup** peut désormais réinitialiser le statut d'une ressource et **failcount** pour toutes les ressources.
- Vous pouvez spécifier un paramètre **lifetime** avec la commande **pcs resource move** afin d'indiquer la période pendant laquelle la contrainte de cette ressource restera en place.
- Vous pouvez utiliser la commande **pcs acl** pour définir les permissions des utilisateurs locaux afin qu'ils puissent avoir accès en lecture seule ou en lecture-écriture à la configuration du cluster en utilisant des listes de contrôle d'accès (ACL).
- La commande **pcs constraint** prend désormais en charge la configuration d'options de contrainte spécifiques en plus des options des ressources générales.
- La commande **pcs resource create** prend en charge le paramètre **disabled** pour indiquer que la ressources créée n'est pas lancée automatiquement.
- La commande **pcs cluster quorum unblock** empêche le cluster d'attendre tous les nœuds lors de l'établissement du quorum.
- Vous pouvez configurer l'ordre du groupe de ressources avec les paramètres **before** (« avant ») et **after** (« après ») de la commande **pcs resource create**.
- Vous pouvez sauvegarder la configuration du cluster dans un fichier tarball et restaurer les fichiers de configuration du cluster sur tous les nœuds avec les options **backup** et **restore** de la commande **pcs config**.

Chapitre 9. Compilateur et outils

Prise en charge de l'application à chaud de correctifs Linux sur binaires System z

GCC (« GNU Compiler Collection ») implémente la prise en charge de l'application en ligne de correctifs de code multithread pour sur binaires System z. La sélection de fonctions spécifiques pour l'application à chaud de correctifs est activée par l'utilisation d'un « attribut de fonction » et l'application à chaud de correctifs pour toutes les fonctions peut être activée à l'aide de l'option de ligne de commande **`-mhotpatch`**.

L'activation de l'application à chaud de correctifs a un impact négatif sur la taille et les performances des logiciels. Ainsi, il est recommandé d'utiliser l'application à chaud de correctifs pour des fonctions spécifiques plutôt que de l'activer pour toutes les fonctions.

La prise en charge de l'application à chaud de correctifs Linux sur binaires System z était un Aperçu Technologique sur Red Hat Enterprise Linux 7.0. Avec la sortie de Red Hat Enterprise Linux 7.1, celle-ci est désormais totalement prise en charge.

Amélioration de l'interface de programmation PAPI

Red Hat Enterprise Linux 7 inclut l'interface de programmation PAPI (**Performance Application Programming Interface**). PAPI est une spécification pour les compteurs d'interfaces multiplateforme et compteurs de performances du matériel sur microprocesseurs modernes. Ces compteurs existent en tant qu'ensemble de registres de petite taille comptant les événements, qui sont des occurrences de signaux spécifiques liés à la fonction d'un processeur. La surveillance de ces événements compte une variété d'usages dans l'analyse des performances et le réglages d'applications.

In Red Hat Enterprise Linux 7.1 PAPI and the related **`libpfm`** libraries have been enhanced to provide support for IBM Power8, Applied Micro X-Gene, ARM Cortex A57, and ARM Cortex A53 processors. In addition, the events sets have been updated for Intel Haswell, Ivy Bridge, and Sandy Bridge processors.

OProfile

OProfile est un profileur global pour les systèmes Linux. Le profilage est exécuté de manière transparente en arrière-plan et les données du profil peuvent être collectées à tout moment. Dans Red Hat Enterprise Linux 7.1, **OProfile** a été amélioré afin de fournir la prise en charge des familles de processeurs suivantes : Intel Atom Processor C2XXX, processeurs Intel Core de 5ème génération, IBM Power8, AppliedMicro X-Gene, et ARM Cortex A57.

OpenJDK8

En tant qu'aperçu technologique, Red Hat Enterprise Linux 7.1 offre les paquets *java-1.8.0-openjdk*, qui contiennent la dernière version du kit de développement OpenJDK (« Open Java Development Kit »), OpenJDK8. Ces paquets offrent une implémentation totalement conforme de Java SE 8 et peuvent être utilisés en parallèle avec les paquets *java-1.7.0-openjdk*, qui restent disponibles sur Red Hat Enterprise Linux 7.1.

Java 8 offre de nombreuses améliorations, comme les expressions Lambda, les méthodes par défaut, une nouvelle interface de programmation Stream pour les collections, JDBC 4.2, la prise en charge du matériel AES, et bien plus encore. En plus de améliorations, OpenJDK8 contient de nombreuses autres mises à jour de performance et correctifs de bogues.

sosreport remplace snap

L'outil **snap**, déconseillé, a été supprimé du paquet *powerpc-utils*. Sa fonctionnalité a été intégrée à l'outil **sosreport**.

Prise en charge GDB pour Little-Endian 64-bit PowerPC

Red Hat Enterprise Linux 7.1 implémente la prise en charge de l'architecture 64-bit PowerPC little-endian dans GDB (« GNU Debugger »).

Amélioration de Tuna

Tuna est un outil qui peut être utilisé pour ajuster les réglages des planificateurs, comme la politique de planificateur, la priorité RT, et les affinités du CPU. Avec Red Hat Enterprise Linux 7.1, l'interface utilisateur graphique **Tuna** a été améliorée et requiert une autorisation root lors de son lancement. Ainsi, l'utilisateur n'est pas obligé d'exécuter le bureau en tant qu'utilisateur root pour invoquer l'interface utilisateur graphique **Tuna**. Pour obtenir des informations supplémentaires sur **Tuna**, veuillez consulter le Guide de l'utilisateur Tuna.

Chapitre 10. Mise en réseau

Trusted Network Connect

Red Hat Enterprise Linux 7.1 présente la fonctionnalité Trusted Network Connect en tant qu'apeçu technologique. Trusted Network Connect est utilisé avec des solutions NAC (« Network Access Control ») actuelles, telles que TLS, 802.1X, ou IPsec pour intégrer l'évaluation de posture des points d'arrivée ; c'est-à-dire, de collecter les informations système d'un point d'arrivée (comme les paramètres de configuration du système d'exploitation, les paquets installés et autres que l'on nomme des mesures d'intégrité). Trusted Network Connect est utilisé pour vérifier ces mesures et politiques d'accès réseau avant d'autoriser le point d'arrivée à accéder au réseau.

Fonctionnalité SR-IOV dans le pilote qlcnic

La prise en charge de 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 directement fournie par QLogic et nous encourageons nos clients à faire suivre leurs commentaires à QLogic et à Red Hat. Les autres fonctionnalités du pilote qlcnic restent entièrement prises en charge.

Filtre de paquets Berkeley

La prise en charge des *traffic classifier* (classifieurs de trafic) basés BPF (« Berkeley Packet Filter ») a été ajoutée à Red Hat Enterprise Linux 7.1. BPF est utilisé lors du filtrage des paquets pour les sockets de paquets, pour la mise en bac à sable dans le *mode de traitement sécurisé* (seccomp), et dans Netfilter. BPF possède une implémentation à la volée pour les architectures les plus importantes ainsi qu'une syntaxe riche pour la création de filtres.

Amélioration de la stabilité de l'horloge

Précédemment, les résultats de tests indiquaient que la désactivation de la capacité de noyau sans tic pouvait fortement améliorer la stabilité de l'horloge du système. Le mode sans tic du noyau peut être désactivé en ajoutant **`nohz=off`** aux paramètres des options de démarrage du noyau. Cependant, de récentes améliorations appliquées au noyau dans Red Hat Enterprise Linux 7.1 ont fortement amélioré la stabilité de l'horloge du système et la différence de stabilité de l'horloge avec ou sans **`nohz=off`** devrait être bien moindre pour la plupart des utilisateurs. Ceci est utile pour les applications de synchronisation du temps utilisant **`PTP`** et **`NTP`**.

Paquets libnetfilter_queue

Le paquet *libnetfilter_queue* a été ajout à Red Hat Enterprise Linux 7.1. **`libnetfilter_queue`** est une bibliothèque de l'espace utilisateur fournissant une interface de programmation aux paquets mis en file d'attente par le filtre des paquets du noyau. Il permet la réception des paquets en attente en provenance du sous-système **`nfnetlink_queue`** du noyau, mais aussi l'analyse des paquets, la ré-écriture des en-têtes de paquets et la réinjection des paquets altérés.

Amélioration des associations (teaming)

Le paquet *libteam* a été mis à jour à la version **`1.14-1`** dans Red Hat Enterprise Linux 7.1. Il fournit un certain nombre d'améliorations et de correctifs de bogues. Plus particulièrement, **`teamd`** peut désormais être automatiquement régénéré par **`systemd`**, ce qui améliore sa stabilité générale.

Pilote Intel QuickAssist Technology

Le pilote Intel QuickAssist Technology (QAT) a été ajouté à Red Hat Enterprise Linux 7.1. Le pilote QAT active le matériel QuickAssist, qui offre des capacités hardware offload crypto à un système.

Prise en charge de LinuxPTP timemaster pour basculements entre PTP et NTP

Le paquet *linuxptp* a été mis à jour à la version **`1.4`** dans Red Hat Enterprise Linux 7.1. Il fournit un certain nombre de correctifs de bogues et d'améliorations. Particulièrement pour le basculement entre domaines **`PTP`** et sources **`NTP`** utilisant l'application **timemaster**. Lorsqu'il y a de multiples domaines **`PTP`** disponibles sur le réseau, ou lorsqu'un basculement sur **`NTP`** est nécessaire, le programme **timemaster** peut être utilisé pour synchroniser l'horloge du système avec toutes les sources horaires disponibles.

initscripts réseau

La prise en charge des noms VLAN personnalisés a été ajoutée dans Red Hat Enterprise Linux 7.1. La prise en charge améliorée d'**`IPv6`** dans les tunnels GRE a également été ajoutée ; L'adresse interne persiste désormais à travers les redémarrages.

ACK avec délai TCP

La prise en charge d'un ACK avec délai TCP configurable a été ajoutée au paquet *iproute* dans Red Hat Enterprise Linux 7.1. Celle-ci peut être activée avec la commande **`ip route quickack`**.

NetworkManager

L'option de liaison **`lacp_rate`** est désormais prise en charge dans Red Hat Enterprise Linux 7.1. **NetworkManager** a été amélioré afin de changer le nom des périphériques plus facilement lorsque les noms d'interfaces maîtres sont changés avec les noms d'interfaces esclaves.

En outre, un paramètre de priorité a été ajouté à la fonction auto-connect de **NetworkManager**. Si plus d'un candidat éligible est disponible pour auto-connect, **NetworkManager** sélectionne la connexion avec la plus haute priorité. Si toutes les connexions disponibles possèdent des valeurs de priorité égales, **NetworkManager** utilisera le comportement par défaut et sélectionnera la dernière connexion active.

Espaces de noms réseau et VTI

La prise en charge des VTI (*virtual tunnel interfaces*) avec des espaces de noms réseaua été ajoutée dans Red Hat Enterprise Linux 7.1. Ceci permet au trafic en provenance d'un VTI d'être passé entre différents espaces de noms lorsque les paquets sont encapsulés ou désencapsulés.

Stockage de configuration alternatif pour le greffon memberOf

La configuration du greffon **`MemberOf`** pour le serveur 389 Directory Server peut désormais être stocké dans un suffixe mappé à une base de données d'arrière-plan. Ceci permet à la configuration du greffon **`MemberOf`** d'être répliquée, ce qui, pour un utilisateur, facilite la tâche de maintenance d'une configuration de greffon **`MemberOf`** se trouvant dans un environnement répliqué.

Chapitre 11. Linux Containers

The **Docker** project is an open-source project that automates the deployment of applications inside Linux Containers, and provides the capability to package an application with its runtime dependencies into a container. It provides a command-line tool for the life cycle management of image-based containers. Linux containers enable rapid application deployment, simpler testing, maintenance, and troubleshooting while improving security. Using Red Hat Enterprise Linux 7 with containers allows customers to increase staff efficiency, deploy third-party applications faster, enable a more agile development environment, and manage resources more tightly.

To quickly get up-and-running with docker formatted containers, refer to Get Started with docker Formatted Containers.

Red Hat Enterprise Linux 7.1 ships with docker version 1.4.1, which includes a number of new features, security fixes, patches and changes. Highlights include:

- The ENV instruction in the Dockerfile now supports arguments in the form of ENV name=value name2=value2 ...
- An experimental overlayfs storage driver has been introduced.
- An update is included for CVE-2014-9356: Path traversal during processing of absolute symlinks. Absolute symlinks were not adequately checked for traversal which created a vulnerability via image extraction and/or volume mounts.
- An update is included for CVE-2014-9357: Escalation of privileges during decompression of LZMA (.xz) archives. Docker 1.3.2 added chroot for archive extraction. This created a vulnerability that could allow malicious images or builds to write files to the host system and escape containerization, leading to privilege escalation.
- An update is included for CVE-2014-9358: Path traversal and spoofing opportunities via image identifiers. Image IDs passed either via docker load or registry communications were not sufficiently validated. This created a vulnerability to path traversal attacks wherein malicious images or repository spoofing could lead to graph corruption and manipulation.

Red Hat provides platform container images for building applications on both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7.

Red Hat fournit également **Kubernetes** pour une utilisation lors de l'orchestration des conteneurs. Pour obtenir des informations supplémentaires sur Kubernetes, veuillez consulter Get Started Orchestrating Docker Containers with Kubernetes.

Linux containers are supported running on hosts with SELinux enabled. SELinux is not supported when the **`/var/lib/docker`** directory is located on a volume using the B-tree file system (Btrfs).

11.1. Components of docker Formatted Containers

The docker container format works with the following fundamental components:

- *Conteneur* – application bac à sable. Chaque conteneur est basés sur une *image* contenant les données de configuration nécessaires. Lorsque vous lancez un conteneur à partir d'une image, une couche inscriptible est ajoutée sur cette image. Chaque fois que vous effectuez une commande commit sur un conteneur (avec la commande **`docker commit`**), un nouvelle couche d'image est ajoutée pour stocker vos modifications.

- *Image* – instantané statique de la configuration des conteneurs. Une image est une couche en lecture seule qui n'est jamais modifiée. Tous les changements sont effectués sur la couche inscriptible la plus haute, et peuvent uniquement être enregistrés en créant une nouvelle image. Chaque image dépend d'une ou plusieurs image(s) parente(s).
- *Platform Container Image* – an image that has no parent. Platform container images define the runtime environment, packages, and utilities necessary for a containerized application to run. The platform image is read-only, so any changes are reflected in the copied images stacked on top of it. See an example of such stacking in Figure 11.1, « Mise en couche d'image à l'aide du format Docker ».
- *Registre* – référentiel d'images. Les registres sont des référentiels publiques ou privés qui contiennent des images disponibles pour téléchargement. Certains registres permettent aux utilisateurs de téléverser des images afin de les mettre à disponibilité pour d'autres utilisateurs.
- *Dockerfile* – fichier de configuration avec des instructions de création pour les images Docker. Les Dockerfiles offrent une manière d'automatiser, de réutiliser et de partager des procédures de création.

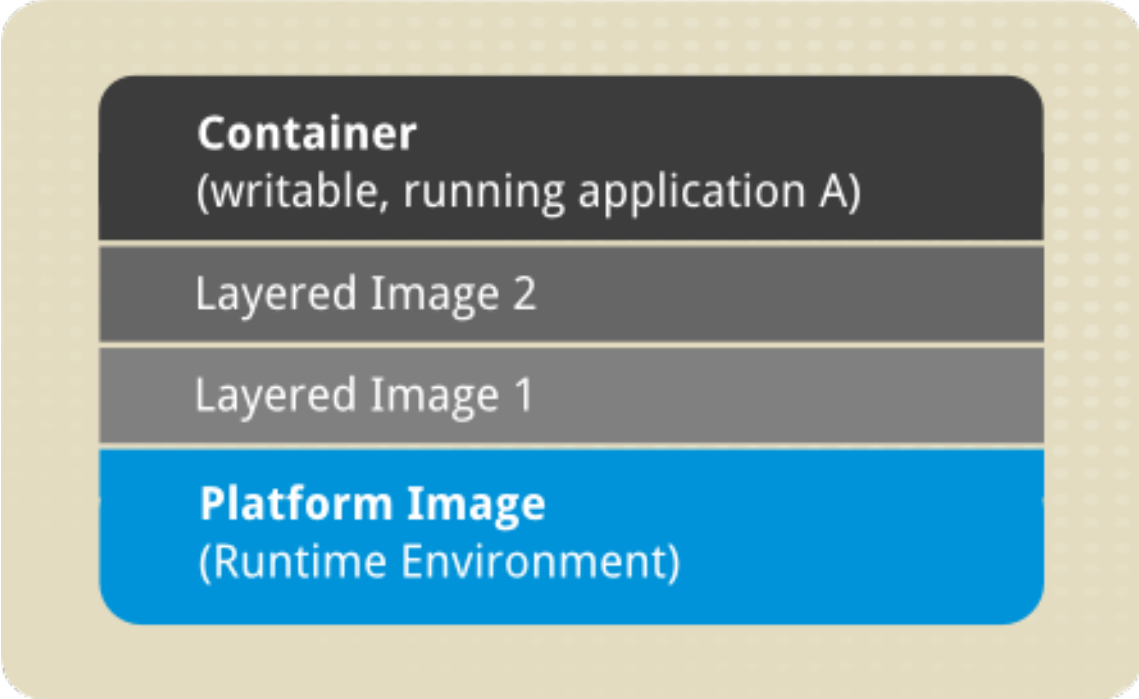

Figure 11.1. Mise en couche d'image à l'aide du format Docker

11.2. Advantages of Using Containers

The Docker project provides an API for container management, an image format, and the possibility to use a remote registry for sharing containers. This scheme benefits both developers and system administrators with advantages such as:

- *Déploiement d'applications rapide* – les conteneurs incluent les conditions nécessaires minimales à l'exécution de l'application, réduisant ainsi leurs taille et leurs permettant d'être rapidemment déployés.
- *Portabilité à travers les ordinateurs* – une application et toutes ses dépendances peuvent être regroupées en un seul conteneur indépendant de la version hôte du noyau Linux, de la plateforme de distribution, ou du modèle de déploiement. Ce conteneur peut être transféré vers un autre ordinateur qui exécute Docker, puis exécuté à partir de celui-ci sans problèmes de compatibilité

- *Contrôle des versions et réutilisation des composants* – il est désormais possible de contrôler les versions successives d'un conteneur, d'en inspecter les différences, ou de restaurer les versions précédentes. Les conteneurs réutilisent les composants des couches précédentes, ce qui les rend particulièrement léger.
- *Partage* – vous pouvez utiliser un référentiel à distance pour partager votre conteneur avec d'autres utilisateurs. Red Hat fournit un registre dans ce but, et il est également possible de configurer votre propre référentiel privé.
- *Empreinte légère et alourdissement minimal* – Les images Docker sont habituellement très petites, ce qui permet une livraison rapide et réduit le temps pris pour déployer les nouveaux conteneurs d'applications.
- *Maintenance simplifiée* – Docker réduit les efforts et éles risques de problèmes avec les dépendances d'application.

11.3. Comparaison avec des machines virtuelles

Virtual machines represent an entire server with all of the associated software and maintenance concerns. Containers provide application isolation and can be configured with minimum run-time environments. In a container, the kernel and parts of the operating system infrastructure are shared. For the virtual machine, a full operating system must be included.

- Vous pouvez créer ou détruire des conteneurs rapidement et facilement. Les machines virtuelles nécessitent une installation complète et requièrent davantage de ressources de calcul pour s'exécuter.
- Les conteneurs sont légers. Ainsi, comparé aux machines virtuelles, un plus grand nombre de conteneurs peuvent être exécutés simultanément sur un ordinateur hôte.
- Les conteneurs partagent leurs ressources de manière efficace. Les machines virtuelles sont isolées. Ainsi, de multiples variations d'une application exécutée dans des conteneurs ont aussi la capacité d'être très légères. Par exemple, les binaires partagés ne sont pas dupliqués sur le système.
- Les machines virtuelles peuvent être migrées pendant leur exécution. Cependant, les conteneurs ne peuvent pas être migrés pendant leur exécution et doivent être arrêtés avant de pouvoir être déplacés d'un ordinateur hôte à un autre.

Les conteneurs ne remplacent pas les machines virtuelles pour tous les cas d'utilisation. Une évaluation minutieuse est requise afin de déterminer ce qui est le mieux pour votre application.

To quickly get up-and-running with docker formatted containers, refer to Get Started with docker Formatted Containers.

More information about Linux Containers, the Docker project, subscriptions and support can be found in this FAQ.

11.4. Using Containers on Red Hat Enterprise Linux 7.1

Packages containing **docker**, **kubernetes**, and registry software have been released as part of the Extras channel in Red Hat Enterprise Linux. Once the Extras channel has been enabled, the packages can be installed in the usual way. For more information on installing packages or enabling channels, see the System Administrator's Guide.

Red Hat provides a registry of platform container images and Red Hat Atomic Container Images. This registry provides base images for building applications on both Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 and pre-built solutions usable on Red Hat Enterprise Linux 7.1 with Docker. For more information about the registry and a list of available packages, see Container Images.

11.5. Containers with the LXC Format Have Been Deprecated

The following LXC packages, which contain Linux resource containers, are deprecated starting with Red Hat Enterprise Linux 7.1:

- libvirt-daemon-driver-lxc
- libvirt-daemon-lxc
- libvirt-login-shell

The Linux container functionality is now focused on the docker management interface (docker command-line interface). Please note: It is possible that the listed LXC packages will not be shipped with future releases of Red Hat Enterprise Linux, as they may be considered for formal removal.

Chapitre 12. Authentification et interopérabilité

Manual Backup and Restore Functionality

This update introduces the **ipa-backup** and **ipa-restore** commands to Identity Management (IdM), which allow users to manually back up their IdM data and restore them in case of a hardware failure. For further information, see the ipa-backup(1) and ipa-restore(1) manual pages or the documentation in the Linux Domain Identity, Authentication, and Policy Guide.

Prise en charge de la migration de WinSync à Trust

This update implements the new **ID Views** mechanism of user configuration. It enables the migration of Identity Management users from a **WinSync** synchronization-based architecture used by **Active Directory** to an infrastructure based on Cross-Realm Trusts. For the details of **ID Views** and the migration procedure, see the documentation in the Windows Integration Guide.

One-Time Password Authentication

One of the best ways to increase authentication security is to require two factor authentication (2FA). A very popular option is to use one-time passwords (OTP). This technique began in the proprietary space, but over time some open standards emerged (HOTP: RFC 4226, TOTP: RFC 6238). Identity Management in Red Hat Enterprise Linux 7.1 contains the first implementation of the standard OTP mechanism. For further details, see the documentation in the System-Level Authentication Guide.

Intégration SSSD pour CIFS (« Common Internet File System »)

A plug-in interface provided by **SSSD** has been added to configure the way in which the **cifs-utils** utility conducts the ID-mapping process. As a result, an **SSSD** client can now access a CIFS share with the same functionality as a client running the **Winbind** service. For further information, see the documentation in the Windows Integration Guide.

Outil de gestion de l'autorité du certificat

The **ipa-cacert-manage renew** command has been added to the Identity management (IdM) client, which makes it possible to renew the IdM Certification Authority (CA) file. This enables users to smoothly install and set up IdM using a certificate signed by an external CA. For details on this feature, see the ipa-cacert-manage(1) manual page.

Granularité du contrôle des accès augmentée

It is now possible to regulate read permissions of specific sections in the Identity Management (IdM) server UI. This allows IdM server administrators to limit the accessibility of privileged content only to chosen users. In addition, authenticated users of the IdM server no longer have read permissions to all of its contents by default. These changes improve the overall security of the IdM server data.

Accès au domaine limité pour les utilisateurs non-privilégiés

The **domains=** option has been added to the **pam_sss** module, which overrides the **domains=** option in the **/etc/sssd/sssd.conf** file. In addition, this update adds the **pam_trusted_users** option, which allows the user to add a list of numerical UIDs or user names that are trusted by the **SSSD** daemon, and the **pam_public_domains** option and a list of domains accessible even for untrusted users. The mentioned

additions allow the configuration of systems, where regular users are allowed to access the specified applications, but do not have login rights on the system itself. For additional information on this feature, see the documentation in the Linux Domain Identity, Authentication, and Policy Guide.

Configuration du fournisseur de données automatique

Désormais, la commande **`ipa-client-install`** configure par défaut **`SSSD`** en tant que fournisseur de données du service sudo. Ce comportement peut être désactivé en utilisant l'option **`--no-sudo`**. En outre, l'option **`--nisdomain`** a été ajoutée pour spécifier le nom de domaine NIS pour l'installation du client IdM, et l'option **`--no_nisdomain`** a été ajoutée pour éviter de définir le nom de domaine NIS. Si aucune de ces options n'est utilisée, le domaine IPA sera utilisé la place.

Utilisation des fournisseurs sudo AD et LDAP

Le fournisseur AD est un backend utilisé pour connecter un serveur Active Directory. Dans Red Hat Enterprise Linux 7.1, 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 du domaine du fichier **`sssd.conf`**.

32-bit Version of krb5-server and krb5-server-ldap Deprecated

The 32-bit version of **`Kerberos 5 Server`** is no longer distributed, and the following packages are deprecated starting with Red Hat Enterprise Linux 7.1: *krb5-server.i686*, *krb5-server.s390*, *krb5-server.ppc*, *krb5-server-ldap.i686*, *krb5-server-ldap.s390*, and *krb5-server-ldap.ppc*. There is no need to distribute the 32-bit version of *krb5-server* on Red Hat Enterprise Linux 7, which is supported only on the following architectures: AMD64 and Intel 64 systems (**`x86_64`**), 64-bit IBM Power Systems servers (**`ppc64`**), and IBM System z (**`s390x`**).

Chapitre 13. Sécurité

Guide de sécurité SCAP

Le paquet *scap-security-guide* a été inclus dans Red Hat Enterprise Linux 7.1. Il fournit les lignes directrices de sécurité et les mécanismes de validation correspondants. Des conseils sont spécifiés dans le protocole SCAP (*Security Content Automation Protocol*), qui constitue un catalogue de conseils de renforcement pratique. Le guide de sécurité **SCAP Security Guide** contient les données nécessaires pour vérifier la conformité de la sécurité du système avec les normes de politique de sécurité recommandées. Une description écrite ainsi qu'un test automatisé (sonde) sont compris. En automatisant le test, **SCAP Security Guide** permet de vérifier la conformité du système de manière pratique, efficace et régulière.

The Red Hat Enterprise Linux 7.1 version of the **SCAP Security Guide** includes the *Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)*, which can be used for compliance scans of Red Hat Enterprise Linux Server 7.1 cloud systems.

Also, the Red Hat Enterprise Linux 7.1 *scap-security-guide* package contains SCAP datastream content format files for Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7, so that remote compliance scanning of both of these products is possible.

The Red Hat Enterprise Linux 7.1 system administrator can use the **oscap** command line tool from the *openscap-scanner* package to verify that the system conforms to the provided guidelines. See the scap-security-guide(8) manual page for further information.

Stratégie SELinux

Dans Red Hat Enterprise Linux 7.1, la politique SELinux a été modifiée ; des services sans leur politique SELinux qui étaient auparavant exécutés dans le domaine **init_t** sont désormais exécutés dans le nouveau domaine **unconfined_service_t**. Veuillez consulter le chapitre Processus non-confinés du Guide de l'utilisateur et de l'administrateur SELinux de Red Hat Enterprise Linux 7.1.

Nouvelles fonctionnalités dans OpenSSH

L'ensemble d'outils **OpenSSH** a été mis à jour à la version 6.6.1p1, qui offre plusieurs nouvelles fonctionnalités liées au chiffrement :

- L'échange de clé à l'aide de la courbe élliptique **Diffie-Hellman** dans **Curve25519** de Daniel Bernstein est désormais pris en charge. Cette méthode est désormais fournie par défaut et le serveur et le client la prennent en charge.
- La prise en charge de l'utilisation du schéma de signature de courbe élliptique **Ed25519** en tant que type de clé publique a été ajoutée. **Ed25519**, qui peut être utilisé pour les clés de l'utilisateur et celles de l'hôtes, offre une meilleure sécurité et de meilleures performance que **ECDSA** et **DSA**.
- Un nouveau format de clé privée a été ajouté et utilise la fonction de dérivation de clé (KDF) **bcrypt**. Par défaut, ce format est utilisé pour les clés **Ed25519** mais peut également être requis pour d'autres types de clés.
- Un nouveau chiffrement de transport, **chacha20-poly1305@openssh.com**, a été ajouté. Il combine le chiffrement de flux de Daniel Bernstein, **ChaCha20**, et le code d'authentification de message (MAC) **Poly1305**.

Nouvelles fonctionnalités dans Libreswan

L'implémentation **Libreswan** du VPN IPsec a été mise à jour à la version 3.12, qui offre plusieurs nouvelles

fonctionnalités et améliorations :

- De nouveaux chiffrements ont été ajoutés.
- **IKEv2** support has been improved.
- La prise en charge de chaînes de certificats intermédiaires a été ajoutée dans **IKEv1** et **IKEv2**.
- La gestion de connexion a été améliorée.
- L'interopérabilité a été améliorée avec les systèmes OpenBSD, Cisco, et Android.
- La prise en charge de **systemd** a été améliorée.
- La prise en charge a été ajoutée pour **CERTREQ** haché et les statistiques de trafic.

Nouvelles fonctionnalités dans TNC

The Trusted Network Connect (TNC) Architecture, provided by the *strongimcv* package, has been updated and is now based on **strongSwan 5.2.0**. The following new features and improvements have been added to the TNC:

- The **PT-EAP** transport protocol (RFC 7171) for Trusted Network Connect has been added.
- The Attestation *Integrity Measurement Collector* (IMC)/*Integrity Measurement Verifier* (IMV) pair now supports the IMA-NG measurement format.
- La prise en charge de l'IMV d'attestation a été améliorée en implémentant un nouvel élément de travail TPMRA.
- La prise en charg d'une interface de programmation REST basée JSON avec IMV SWID a été ajoutée.
- The SWID IMC can now extract all installed packages from the **dpkg**, **rpm**, or **pacman** package managers using the **swidGenerator**, which generates SWID tags according to the new ISO/IEC 19770-2:2014 standard.
- The **libtls TLS 1.2** implementation as used by **EAP-(T)TLS** and other protocols has been extended by AEAD mode support, currently limited to **AES-GCM**.
- Improved (IMV) support for sharing access requestor ID, device ID, and product information of an access requestor via a common **imv_session** object.
- Plusieurs bogues ont été corrigés dans les protocoles **IF-TNCCS** (**PB-TNC**, **IF-M** (**PA-TNC**)), ainsi que dans la paire **OS IMC/IMV**.

Nouvelles fonctionnalités dans GnuTLS

L'implémentation **GnuTLS** des protocoles **SSL**, **TLS**, et **DTLS** a été mise à jour à la version 3.3.8, qui offre un certain nombre de nouvelles fonctionnalités et améliorations :

- La prise en charge de **DTLS 1.2** a été ajoutée.
- La prise en charge ALPN (*Application Layer Protocol Negotiation*) a été ajoutée.
- Les performances des suites de chiffrement de courbe elliptique ont été améliorées.
- De nouvelles suites de chiffrement, **RSA-PSK** et **CAMELLIA-GCM**, ont été ajoutées.
- La prise en charge native du standard TPM (*Trusted Platform Module*) a été ajoutée.

- La prise en charge des cartes smart **PKCS#11** et des modules HSM (*hardware security modules*) a été améliorée de plusieurs manières.
- La conformité avec les standards de sécurité *FIPS 140* (*Federal Information Processing Standards*) a été améliorée de plusieurs manières.

Chapitre 14. Bureau

Prise en charge de Quad-buffered OpenGL Stereo Visuals

GNOME Shell et le gestionnaire de fenêtres composite **Mutter** permettent désormais d'utiliser quad-buffered OpenGL stereo visuals sur le matériel pris en charge. Vous devrez posséder le pilote NVIDIA Display Driver version 337 ou une version plus récente afin d'être en mesure d'utiliser cette fonctionnalité correctement.

Fournisseurs de compte en ligne

Une nouvelle clé **GSettings** **`org.gnome.online-accounts.whitelisted-providers`** a été ajoutée aux comptes en ligne **GNOME Online Accounts** (fournis par le paquet *gnome-online-accounts*). Cette clé vous donne une liste de fournisseurs de compte en ligne qui sont explicitement autorisés à être chargés lors du démarrage. En spécifiant cette clé, les administrateurs système peuvent activer les fournisseurs appropriés ou en désactiver d'autres de manière sélective.

Chapitre 15. Prise en charge et maintenance

Micro-rapports autorisés par ABRT

In Red Hat Enterprise Linux 7.1, the **Automatic Bug Reporting Tool** (**ABRT**) receives tighter integration with the Red Hat Customer Portal and is capable of directly sending micro-reports to the Portal. **ABRT** provides a utility, **`abrt-auto-reporting`**, to easily configure user's Portal credentials necessary to authorize micro-reports.

The integrated authorization allows **ABRT** to reply to a micro-report with a rich text which may include possible steps to fix the cause of the micro-report. For example, **ABRT** can suggest which packages are supposed to be upgraded or offer Knowledge base articles related to the issue.

Veuillez consulter le Portail Client pour obtenir davantage d'informations sur cette fonctionnalité.

Chapitre 16. 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 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.

Red Hat Software Collections utiliser un mécanisme d'empaquetage alternatif basé sur l'utilitaire **`scl`** afin de fournir un ensemble de paquets parallèles. Cet ensemble permet l'utilisation de versions de paquets alternatifs sur Red Hat Enterprise Linux. En utilisant l'utilitaire **`scl`**, les utilisateurs peuvent choisir à tout moment la version du paquet qu'ils souhaitent exécuter.

Important

Red Hat Software Collections possèdent un cycle de vie et une durée de prise en charge plus court que Red Hat Enterprise Linux. Pour obtenir des informations supplémentaires, veuillez consulter le Cycle de vie du produit Red Hat Software Collections.

Red Hat Developer Toolset fait désormais parte 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.

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.

Chapitre 17. Red Hat Enterprise Linux for Real Time

Red Hat Enterprise Linux for Real Time is a new offering in Red Hat Enterprise Linux 7.1 comprised of a special kernel build and several user space utilities. With this kernel and appropriate system configuration, Red Hat Enterprise Linux for Real Time brings deterministic workloads, which allow users to rely on consistent response times and low and predictable latency. These capabilities are critical in strategic industries such as financial service marketplaces, telecommunications, or medical research.

For instructions on how to install Red Hat Enterprise Linux for Real Time, and how to set up and tune the system so that you can take full advantage of this offering, refer to the Red Hat Enterprise Linux for Real Time 7 Installation Guide.

Partie II. Pilotes de périphériques

Ce chapitre fournit une liste complète de tous les pilotes de périphériques ayant été mis à jour dans Red Hat Enterprise Linux 7.1.

Chapitre 18. Mises à jour des pilotes de stockage

- Le pilote **hpsa** a été mis à niveau à la version 3.4.4-1-RH1.
- Le pilote **qla2xxx** a été mis à niveau à la version 8.07.00.08.07.1-k1.
- Le pilote **qla4xxx** a été mis à niveau à la version 5.04.00.04.07.01-k0.
- Le pilote **qlcnic** a été mis à niveau à la version 5.3.61.
- Le pilote **netxen_nic** a été mis à niveau à la version 4.0.82.
- Le pilote **qlge** a été mis à niveau à la version 1.00.00.34.
- Le pilote **bnx2fc** a été mis à niveau à la version 2.4.2.
- Le pilote **bnx2i** a été mis à niveau à la version 2.7.10.1.
- Le pilote **cnic** a été mis à niveau à la version 2.5.20.
- Le pilote **bnx2x** a été mis à niveau à la version 1.710.51-0.
- Le pilote **bnx2** a été mis à niveau à la version 2.2.5.
- Le pilote **megaraid_sas** a été mis à niveau à la version 06.805.06.01-rc1.
- Le pilote **mpt2sas** a été mis à niveau à la version 18.100.00.00.
- Le pilote **ipr** a été mis à niveau à la version 2.6.0.
- Les paquets *kmod-lpfc* ont été ajoutés à Red Hat Enterprise Linux 7, ce qui assure une meilleure stabilité lors de l'utilisation du pilote lpfc avec des adaptateurs FC (« Fibre Channel ») et FCoE (« Fibre Channel over Ethernet »). Le pilote **lpfc** a été mis à niveau à la version 0:10.2.8021.1.
- Le pilote **be2iscsi** a été mis à niveau à la version 10.4.74.0r.
- Le pilote **nvme** a été mis à niveau à la version 0.9.

Chapitre 19. Mises à jour des pilotes réseau

- Le pilote **bna** a été mis à niveau à la version 3.2.23.0r.
- Le pilote **cxgb3** a été mis à niveau à la version 1.1.5-ko.
- Le pilote **cxgb3i** a été mis à niveau à la version 2.0.0.
- Le pilote **iw_cxgb3** a été mis à niveau à la version 1.1.
- Le pilote **cxgb4** a été mis à niveau à la version 2.0.0-ko.
- Le pilote **cxgb4vf** a été mis à niveau à la version 2.0.0-ko.
- Le pilote **cxgb4i** a été mis à niveau à la version 0.9.4.
- Le pilote **iw_cxgb4** a été mis à niveau à la version 0.1.
- Le pilote **e1000e** a été mis à niveau à la version 2.3.2-k.
- Le pilote **igb** a été mis à niveau à la version 5.2.13-k.
- Le pilote **igbvf** a été mis à niveau à la version 2.0.2-k.
- Le pilote **ixgbe** a été mis à niveau à la version 3.19.1-k.
- Le pilote **ixgbevf** a été mis à niveau à la version 2.12.1-k.
- Le pilote **i40e** a été mis à niveau à la version 1.0.11-k.
- Le pilote **i40evf** a été mis à niveau à la version 1.0.1.
- Le pilote **e1000** a été mis à niveau à la version 7.3.21-k8-NAPI.
- Le pilote **mlx4_en** a été mis à niveau à la version 2.2-1.
- Le pilote **mlx4_ib** a été mis à niveau à la version 2.2-1.
- Le pilote **mlx5_core** a été mis à niveau à la version 2.2-1.
- Le pilote **mlx5_ib** a été mis à niveau à la version 2.2-1.
- Le pilote **ocrdma** a été mis à niveau à la version 10.2.287.0u.
- Le pilote **ib_ipoib** a été mis à niveau à la version 1.0.0.
- Le pilote **ib_qib** a été mis à niveau à la version 1.11.
- Le pilote **enic** a été mis à niveau à la version 2.1.1.67.
- Le pilote **be2net** a été mis à niveau à la version 10.4r.
- Le pilote **tg3** a été mis à niveau à la version 3.137.
- Le pilote **r8169** a été mis à niveau à la version 2.3LK-NAPI.

Chapitre 20. Mises à jour des pilotes graphiques

- Le pilote **`vmwgfx`** a été mis à niveau à la version 2.6.0.0.

Partie III. Known Issues

This part describes known issues in Red Hat Enterprise Linux 7.1.

Chapitre 21. Installation and Booting

anaconda component, BZ#1067868

Under certain circumstances, when installing the system from the boot DVD or ISO image, not all assigned IP addresses are shown in the network spoke once network connectivity is configured and enabled. To work around this problem, leave the network spoke and enter it again. After re-entering, all assigned addresses are shown correctly.

Chapitre 22. Networking

`rsync` component, BZ#1082496

The **`rsync`** utility cannot be run as a socket-activated service because the **`rsyncd@.service`** file is missing from the *rsync* package. Consequently, the **`systemctl start rsyncd.socket`** command does not work. However, running **`rsync`** as a daemon by executing the **`systemctl start rsyncd.service`** command works as expected.

Chapitre 23. Authentication and Interoperability

`bind-dyndb-ldap` component, BZ#1139776

The latest version of the **`bind-dyndb-ldap`** system plug-in offers significant improvements over the previous versions, but currently has some limitations. One of the limitations is missing support for the LDAP rename (MODRDN) operation. As a consequence, DNS records renamed in LDAP are not served correctly. To work around this problem, restart the **`named`** daemon to resynchronize data after each MODRDN operation. In an Identity Management (IdM) cluster, restart the **`named`** daemon on all IdM replicas.

`ipa` component, BZ#1186352

When you restore an Identity Management (IdM) server from backup and re-initalize the restored data to other replicas, the Schema Compatibility plug-in can still maintain a cache of the old data from before performing the restore and re-initialization. Consequently, the replicas might behave unexpectedly. For example, if you attempt to add a user that was originally added after performing the backup, and thus removed during the restore and re-initialization steps, the operation might fail with an error, because the Schema Compatibility cache contains a conflicting user entry. To work around this problem, restart the IdM replicas after re-intializing them from the master server. This clears the Schema Compatibility cache and ensures that the replicas behave as expected in the described situation.

`ipa` component, BZ#1188195

Both anonymous and authenticated users lose the default permission to read the **`facsimiletelephonenumber`** user attribute after upgrading to the Red Hat Enterprise Linux 7.1 version of Identity Management (IdM). To manually change the new default setting and make the attribute readable again, run the following command:

```
ipa permission-mod 'System: Read User Addressbook Attributes' --
includedattrs facsimiletelephonenumber
```

Chapitre 24. Desktop

`gobject-introspection` component, BZ#1076414

The **`gobject-introspection`** library is not available in a 32-bit multilib package. Users who wish to compile 32-bit applications that rely on GObject introspection or libraries that use it, such as **`GTK+`** or **`GLib`**, should use the *mock* package to set up a build environment for their applications.

Annexe A. Historique des versions

Version 1.0-9.3	**Thu Jan 29 2015**	**Sam Friedmann**

Fichiers traduits synchronisés avec les sources XML 1.0-9.1

Version 1.0-9.1	**Thu Jan 29 2015**	**Sam Friedmann**

Fichiers de traduction synchronisés avec les sources XML 1.0-9

Version 1.0-9	**Wed Jan 14 2015**	**Milan Navrátil**

Publication des notes de version de Red Hat Enterprise Linux 7.1.

Version 1.0-8	**Thu Dec 15 2014**	**Jiří Herrmann**

Publication des notes de version de Red Hat Enterprise Linux 7.1 Beta.