Red Hat Satellite 5.6

Guide de r?f?rence

Guide des fonctionnalités avancées de Red Hat Satellite

Édition 1

Last Updated: 2017-10-10

Red Hat Satellite 5.6 Guide de r�f�rence

Guide des fonctionnalités avancées de Red Hat Satellite
Édition 1

John Ha
Red Hat Engineering Content Services

Lana Brindley
Red Hat Engineering Content Services

Daniel Macpherson
Red Hat Engineering Content Services

Athene Chan
Red Hat Engineering Content Services

David O'Brien
Red Hat Engineering Content Services

Notice légale

Résumé

Bienveue sur le Guide de référence Red Hat Satellite 5.6. Le Guide de référence Red Hat Satellite vous présente les fonctionnalités avancées du serveur Satellite.

Table des matières

PRÉFACE

1. AUDIENCE

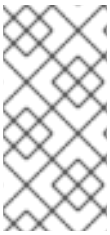
Le public cible de ce guide inclut les **administrateurs de système** qui cherchent à gérer les mises à jour de systèmes dans un réseau interne.

CHAPITRE 1. INFORMATIONS RED HAT SATELLITE

Cette section couvre divers sujets concernant la configuration avancée de Red Hat Satellite.

1.1. OUTILS DE LIGNE DE COMMANDE POUR LA GESTION DE LA CONFIGURATION

Outre les options fournies sur le site web Red Hat Satellite, il existe deux outils en ligne de commande pour gérer les fichiers de configuration d'un système : le **Red Hat Network Configuration Client** et le **Red Hat Network Configuration Manager**. Il existe un autre outil, le **Red Hat Network Actions Control**, qui est utilisé pour activer et désactiver la gestion de configuration sur les systèmes client. Si vous ne disposez pas encore de ces outils, vous pouvez les obtenir dans canal enfant **`Red Hat Network Tools`** de votre système d'exploitation.



NOTE

Lors du déploiement d'un fichier de configuration via le site web, une sauvegarde du fichier précédent, y compris son chemin complet, est effectuée dans le répertoire **`/var/lib/rhncfg/backups/`** sur le système concerné. Cette sauvegarde conserve son nom de fichier, mais une extension **`.rhn-cfg-backup`** y est ajoutée.

1.1.1. Red Hat Network Actions Control

Le **Red Hat Network Actions Control** (**`rhn-actions-control`**) est utilisé pour activer et désactiver la gestion de configuration d'un système. Les systèmes client, par défaut, ne peuvent pas être gérés de cette manière. Cet outil permet aux administrateurs système d'activer et désactiver des modes spécifiques d'actions admissibles, comme le *déploiement* d'un fichier de configuration sur le système, le *téléchargement* d'un fichier à partir du système, l'utilisation de *diff* afin de trouver ce qui est actuellement géré sur un système et ce qui est disponible, ou l'autorisation de l'exécution de *commandes à distance* arbitraires. Ces divers modes sont activés ou désactivés en plaçant ou en supprimant des fichiers et des répertoires dans le répertoire **`/etc/sysconfig/rhn/allowed-actions/`**. Vu les permissions par défaut sur le répertoire **`/etc/sysconfig/rhn/`**, le Red Hat Network Actions Control doit être exécuté par un utilisateur possédant l'accès root.

1.1.1.1. Options en ligne de commande générales

Une page **`man`** est disponible, comme pour la plupart des outils en ligne de commande. Décidez simplement quelles actions programmées de Red Hat Network devraient être activées de façon à être utilisées par les administrateurs système. Ces options activent les différents modes d'actions programmées :

Tableau 1.1. options de `rhn-actions-control`

Option	Description
--enable-deploy	Permet à rhncfg-client de déployer des fichiers.
--enable-diff	Permet à rhncfg-client de comparer des fichiers.
--enable-upload	Permet à rhncfg-client de télécharger des fichiers.

Option	Description
--enable-mtime-upload	Permet à rhncfg-client de télécharger mtime.
--enable-all	Permet à rhncfg-client de tout faire.
--enable-run	Active l'exécution d'un script.
--disable-deploy	Désactive le déploiement.
--disable-diff	Désactive la comparaison.
--disable-upload	Désactive le téléchargement.
--disable-mtime-upload	Désactive le téléchargement de mtime.
--disable-all	Désactive toutes les options.
--disable-run	Désactive l'exécution de scripts.
--report	Rapporte si les modes sont activés ou désactivés.
-f, --force	Force l'opération sans demander avant
-h, --help	Affiche le message d'aide et quitte

Une fois qu'un mode est défini, votre système sera prêt pour la gestion de configuration via Red Hat Satellite. **`rhn-actions-control --enable-all`** est une option courante.

1.1.2. Red Hat Network Configuration Client

Comme son nom l'indique, le **Red Hat Network Configuration Client** (**`rhncfg-client`**) est installé et exécuté depuis un système client individuel. Vous pouvez l'utiliser pour recueillir des informations sur la manière selon laquelle Red Hat Network déploie les fichiers de configuration sur le client.

Le **Red Hat Network Configuration Client** offre les modes primaires suivants : list, get, channels, diff et verify.

1.1.2.1. Listage des fichiers de configuration

Pour dresser la liste des fichiers de configuration pour la machine et des étiquettes (labels) s'appliquant au canaux de configuration, exécutez la commande suivante :

```
rhncfg-client list
```

La sortie ressemble à la liste suivante :

```
Config Channel      File
config-channel-17   /etc/example-config.txt
```

```
config-channel-17   /var/spool/aalib.rpm
config-channel-14   /etc/rhn/rhn.conf
```

Ces fichiers sont les fichiers de configuration qui s'appliquent à votre système. Cependant, il se peut que des fichiers dupliqués soient présents dans les autres canaux. Par exemple, exécutez la commande suivante :

```
rhncfg-manager list config-channel-14
```

et examinez la sortie suivante :

```
Files in config channel 'config-channel-14' /etc/example-config.txt
/etc/rhn/rhn.conf
```

Vous pouvez alors vous demander où est passée la seconde version de **/etc/example-config.txt**. Le niveau du fichier **/etc/example-config.txt** dans **config-channel-17** était supérieur à celui du même fichier dans **config-channel-14**. Ainsi, la version du fichier de configuration dans **config-channel-14** n'est pas déployée pour ce système, bien que le fichier réside toujours dans le canal. La commande **rhncfg-client** ne liste pas le fichier parce qu'il ne sera pas déployé sur ce système.

1.1.2.2. Obtention d'un fichier de configuration

Pour télécharger le fichier de configuration le plus approprié à votre machine, exécutez la commande suivante :

```
rhncfg-client get /etc/example-config.txt
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Deploying /etc/example-config.txt
```

Afficher le contenu du fichier avec la commande **less** ou un autre pager. Remarquez que le fichier est sélectionné comme étant le plus pertinent selon le rang du canal de configuration le contenant. Cette opération est effectuée sous l'onglet **Configuration** de la page **Détails du système**.

1.1.2.3. Affichage des canaux de configuration

Pour afficher les étiquettes et les noms de canaux de configuration s'appliquant au système, exécutez la commande suivante :

```
rhncfg-client channels
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Config channels: Label Name ----- ---- config-channel-17 config chan 2
config-channel-14 config chan 1
```

La table suivante liste les options disponibles pour **rhncfg-client get** :

Tableau 1.2. options de rhncfg-client get

Option	Description
--topdir=TOPDIR	Rend toutes les opérations de fichiers relatives à cette chaîne
--exclude=EXCLUDE	Exclut le déploiement d'un fichier avec 'get'/ Peut être utilisé de multiples fois.
-h, --help	Affiche le message d'aide et quitte

1.1.2.4. Différentiation entre les fichiers de configuration

Pour afficher les différences entre les fichiers de configuration déployés sur le système et ceux stockés par Red Hat Network, exécutez la commande suivante :

```
rhncfg-client diff
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
[root@testsatellite root]# rhncfg-client diff
--- /etc/test
+++ /etc/test 2013-08-28 00:14:49.405152824 +1000
@@ -1 +1,2 @@
 This is the first line
+This is the second line added
```

De plus, vous pouvez inclure l'option **`--topdir`** pour comparer les fichiers de configuration dans Red Hat Network avec ceux figurant sur un emplacement arbitraire (et non utilisé) sur le système client, comme ceci :

```
[root@ root]# rhncfg-client diff --topdir /home/test/blah/ /usr/bin/diff:
/home/test/blah/etc/example-config.txt: No such file or directory
/usr/bin/diff: /home/test/blah/var/spool/aalib.rpm: No such file or
directory
```

1.1.2.5. Vérification des fichiers de configuration

Pour déterminer rapidement si des fichiers de configuration client sont différents des fichiers qui lui sont associés via Red Hat Network, exécutez la commande suivante :

```
rhncfg-client verify
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
modified /etc/example-config.txt /var/spool/aalib.rpm
```

Le fichier **`example-config.txt`** est modifié localement alors que **`aalib.rpm`** lui ne l'est pas.

La table suivante liste les options disponibles pour **`rhncfg-client verify`** :

Tableau 1.3. options de `rhncfg-client verify`

Option	Description
-v, --verbose	Augmente la quantité d'informations de sortie. Affiche les différences dans le mode, le propriétaire et les permissions de groupe pour le fichier de configuration spécifié.
-o, --only	Affiche uniquement les fichiers présentant des différences.
-h, --help	Affiche le message d'aide et quitte

1.1.3. Red Hat Network Configuration Manager

Contrairement au **Red Hat Network Configuration Client**, le **Red Hat Network Configuration Manager** (**`rhncfg-manager`**) est conçu pour maintenir le référentiel central de Red Hat Network contenant les fichiers de configuration et les canaux, et non pas ceux qui figurent sur les systèmes clients. Cet outil offre une alternative en ligne de commande aux fonctionnalités de gestion de la configuration offertes par le site web Red Hat Network, ainsi que la possibilité de créer des scripts pour certaines voire pour toutes les tâches de maintenance associées.

Ce dernier est créé pour être utilisé par des administrateurs de configuration (Config Administrators) et requiert un nom d'utilisateur et un mot de passe Red Hat Network avec l'ensemble de permissions appropriées. Le nom d'utilisateur peut être spécifié dans **`/etc/sysconfig/rhn/rhncfg-manager.conf`** ou dans la section [rhncfg-manager] de **`~/.rhncfgrc`**.

Lorsque le **Red Hat Network Configuration Manager** est exécuté en tant que super-utilisateur, il tente d'obtenir les valeurs de configuration nécessaires du **Red Hat Update Agent**. S'il est exécuté en tant qu'un utilisateur autre que super-utilisateur, il sera peut-être nécessaire d'apporter des modifications de configuration dans le fichier **`~/.rhncfgrc`**. Le fichier de session est mis en cache dans **`~/.rhncfg-manager-session`** afin d'éviter de devoir se connecter à chaque commande.

Le délai d'expiration par défaut pour le **Red Hat Network Configuration Manager** est de 30 minutes. Pour modifier cette durée, ajoutez l'option **`server.session_lifetime`** ainsi qu'une nouvelle valeur dans le fichier **`/etc/rhn/rhn.conf`** présent sur le serveur exécutant le gestionnaire, comme dans l'extrait ci-dessous :

```
server.session_lifetime = 120
```

Le **Red Hat Network Configuration Manager** offre les modes primaires suivants : add, create-channel, diff, diff-revisions, download-channel, get, list, list-channels, remove, remove-channel, revisions, update et upload-channel.

Chaque mode offre son propre ensemble d'options qui peuvent être affichées en exécutant la commande suivante :

```
rhncfg-manager mode --help
```

Remplacez *mode* par le nom du mode à inspecter.

```
rhncfg-manager diff-revisions --help
```

Vous pouvez consulter une telle liste d'options pour le mode add (ajouter) dans le Tableau 1.4, « options de **`rhncfg-manager add`** ».

1.1.3.1. Création d'un canal de configuration

Pour créer un canal de configuration pour votre organisation, exécutez la commande suivante :

```
rhncfg-manager create-channel channel-label
```

Si le système demande votre nom d'utilisateur et mot de passe pour Red Hat Satellite, saisissez-les. Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Red Hat Network username: rhn-user
Password:
Creating config channel channel-label Config channel channel-label created
```

Une fois que vous avez créé un canal de configuration, utilisez les modes restants affichés ci-dessus pour peupler et maintenir ce canal.

1.1.3.2. Ajout de fichiers au canal de configuration

Pour ajouter un fichier au canal de configuration, vous devez préciser l'étiquette du canal ainsi que le fichier local à télécharger, comme le montre l'extrait ci-dessous :

```
rhncfg-manager add --channel=channel-label /path/to/file
```

Outre l'étiquette de canal et le chemin vers le fichier, vous pouvez utiliser les options disponibles pour modifier le fichier lors de son ajout. Par exemple, vous pouvez modifier le chemin d'accès et le nom du fichier en incluant l'option **`--dest-file`** dans la ligne de commande, comme dans l'extrait ci-dessous :

```
rhncfg-manager add --channel=channel-label --dest-
file=/new/path/to/file.txt/path/to/file
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Pushing to channel example-channel
Local file >/path/to/file -> remote file /new/path/to/file.txt
```

La table suivante liste les options disponibles pour **`rhncfg-manager add`** :

Tableau 1.4. options de `rhncfg-manager add`

Option	Description
-c CHANNEL --channel=CHANNEL	Télécharge des fichiers dans ce canal de configuration
-d DEST_FILE --dest-file=DEST_FILE	Télécharge le fichier comme ce chemin
--delim-start=DELIM_START	Commencer le délimiteur pour l'interpolation de variables
--delim-end=DELIM_END	Finir le délimiteur pour l'interpolation de variables
-i, --ignore-missing	Ignore les fichiers locaux manquants

Option	Description
--selinux-context=SELINUX_CONTEXT	Écrase le contexte SELinux
-h, --help	Affiche le message d'aide et quitte

NOTE

Par défaut, la taille maximale des fichiers de configuration est 128 Ko. Si vous devez changer cette valeur, recherchez ou créez la ligne suivante dans le fichier **`/etc/rhn/rhn.conf`** :

```
web.maximum_config_file_size=128
```

En outre, recherchez ou créez la ligne suivante dans le fichier **`/etc/rhn/rhn.conf`** :

```
maximum_config_file_size=128
```

Dans les deux emplacements, veuillez remplacer 128 par la valeur limite que vous souhaitez, en octets.

1.1.3.3. Différences entre les derniers fichiers de configuration

Pour afficher les différences entre les fichiers de configuration stockés sur disque et les dernières révisions sur le canal, exécutez la commande suivante :

```
rhncfg-manager diff --channel=channel-label --dest-file=/path/to/file.txt
\ /local/path/to/file
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
--- /tmp/dest_path/example-config.txt config_channel: example-channel
revision: 1
+++ /home/test/blah/hello_world.txt 2003-12-14 19:08:59.000000000 -0500
@@ -1 +1 @@
-foo
+hello, world
```

La table suivante liste les options disponibles pour **`rhncfg-manager diff`** :

Tableau 1.5. options de `rhncfg-manager diff`

Option	Description
-c CHANNEL, --channel=CHANNEL	Obtenir des fichiers de ce canal de configuration
-r REVISION, --revision=REVISION	Utiliser cette révision
-d DEST_FILE, --dest-file=DEST_FILE	Télécharge le fichier comme ce chemin

Option	Description
-t TOPDIR, --topdir=TOPDIR	Rend tous les fichiers relatifs à cette chaîne
-h, --help	Affiche le message d'aide et quitte

1.1.3.4. Différences entre différentes versions

Pour comparer différentes versions d'un fichier parmi les canaux et révisions, utilisez l'option **-r** pour indiquer la révision spécifique du fichier à laquelle le fichier même devrait être comparé et l'option **-n** pour identifier les deux canaux devant être vérifiés. Reportez-vous à la Section 1.1.3.11, « Détermination du nombre de révisions d'un fichier » pour obtenir des informations en relation avec le sujet. Spécifiez ici un seul nom de fichier dans la mesure où vous comparez le fichier à une autre version du même fichier comme le montre l'extrait ci-dessous :

```
rhncfg-manager diff-revisions -n=channel-label1 -r=1 -n=channel-label2 -
r=1 /path/to/file.txt
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
--- /tmp/dest_path/example-config.txt 2004-01-13 14:36:41 \ config
channel: example-channel2 revision: 1
--- /tmp/dest_path/example-config.txt 2004-01-13 14:42:42 \ config
channel: example-channel3 revision: 1
@@ -1 +1,20 @@
-foo
+blah
+-----BEGIN PGP SIGNATURE-----
+Version: GnuPG v1.0.6 (GNU/Linux)
+Comment: For info see http://www.gnupg.org
+
+iD8DBQA9ZY6vse4XmfJPGwgRAsHcAJ9ud9dabUcdscdcqB8AZP7e0Fua0NmKsdhQCeOWHX
+VsDTfen2NWdwwPaTM+S+Cow=
+=Ltp2
+-----END PGP SIGNATURE-----
```

La table suivante liste les options disponibles pour **rhncfg-manager diff-revisions** :

Tableau 1.6. options de `rhncfg-manager diff-revisions`

Option	Description
-c CHANNEL, --channel=CHANNEL	Utiliser ce canal de configuration
-r REVISION, --revision=REVISION	Utiliser cette révision
-h, --help	Affiche le message d'aide et quitte

1.1.3.5. Téléchargement de tous les fichiers d'un canal

Pour télécharger tous les fichiers d'un canal sur le disque, créez un répertoire et exécutez la commande suivante :

```
rhncfg-manager download-channel channel-label --topdir .
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Copying /tmp/dest_path/example-config.txt -> \
blah2/tmp/dest_path/example-config.txt
```

La table suivante liste les options disponibles pour **`rhncfg-manager download-channel`** :

Tableau 1.7. options de `rhncfg-manager download-channel`

Option	Description
-t TOPDIR, --topdir=TOPDIR	Répertoire auquel tous les chemins de fichiers sont associés. Cette option doit être définie.
-h, --help	Affiche le message d'aide et quitte

1.1.3.6. Obtention du contenu d'un fichier

Pour diriger le contenu d'un fichier spécifique vers la sortie standard (stdout), exécutez la commande suivante :

```
rhncfg-manager get --channel=channel-label \ /tmp/dest_path/example-
config.txt
```

Vous devriez voir le contenu du fichier en sortie.

1.1.3.7. Listage de tous les fichiers d'un canal

Pour dresser la liste de tous les fichiers d'un canal, exécutez la commande suivante :

```
rhncfg-manager list channel-label
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Files in config channel `example-channel3': /tmp/dest_path/example-
config.txt
```

La table suivante liste les options disponibles pour **`rhncfg-manager get`** :

Tableau 1.8. options de `rhncfg-manager get`

Option	Description
-c CHANNEL, --channel=CHANNEL	Obtenir des fichiers de ce canal de configuration

Option	Description
-t TOPDIR, --topdir=TOPDIR	Rend tous les fichiers relatifs à cette chaîne
-r REVISION, --revision=REVISION	Obtenir la révision de ce fichier
-h, --help	Affiche le message d'aide et quitte

1.1.3.8. Listage de tous les canaux de configuration

Pour dresser la liste de tous les canaux de configuration de votre organisation, exécutez la commande suivante :

```
rhncfg-manager list-channels
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Available config channels: example-channel example-channel2 example-
channel3 config-channel-14 config-channel-17
```

Notez que cette opération ne dresse pas la liste de canaux **`local_override`** ou **`server_import`**

1.1.3.9. Suppression d'un fichier dans un canal

Pour supprimer un fichier dans un canal, exécutez la commande suivante :

```
rhncfg-manager remove --channel=channel-label /tmp/dest_path/example-
config.txt
```

Si le système demande votre nom d'utilisateur et mot de passe pour Red Hat Network, saisissez-les. Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Red Hat Network username: rhn-user Password: Removing from config channel
example-channel3 /tmp/dest_path/example-config.txt removed
```

La table suivante liste les options disponibles pour **`rhncfg-manager remove`** :

Tableau 1.9. options de `rhncfg-manager remove`

Option	Description
-c CHANNEL, --channel=CHANNEL	Supprimer les fichiers dans ce canal de configuration
-t TOPDIR, --topdir=TOPDIR	Rend tous les fichiers relatifs à cette chaîne
-h, --help	Affiche le message d'aide et quitte

1.1.3.10. Suppression d'un canal de configuration

Pour supprimer un canal de configuration dans votre organisation, exécutez la commande suivante :

```
rhncfg-manager remove-channel channel-label
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Removing config channel example-channel Config channel example-channel
removed
```

1.1.3.11. Détermination du nombre de révisions d'un fichier

Pour connaître le nombre de révisions (les révisions vont de 1 à N, N représentant un nombre entier supérieur à 0) d'un fichier/chemin d'accès existant dans un canal, exécutez la commande suivante :

```
rhncfg-manager revisions channel-label /tmp/dest_path/example-config.txt
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Analyzing files in config channel example-channel \
/tmp/dest_path/example-config.txt: 1
```

1.1.3.12. Mise à jour d'un fichier dans un canal

Pour créer une nouvelle révision d'un fichier dans un canal (ou ajouter la première révision à ce canal si aucune n'existait avant le chemin d'accès spécifié), exécutez la commande suivante :

```
rhncfg-manager update \ --channel=channel-label --dest-
file=/path/to/file.txt /local/path/to/file
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Pushing to channel example-channel: Local file example-
channel/tmp/dest_path/example-config.txt -> \ remote file
/tmp/dest_path/example-config.txt
```

La table suivante liste les options disponibles pour **`rhncfg-manager update`** :

Tableau 1.10. options de `rhncfg-manager update`

Option	Description
-c CHANNEL, --channel=CHANNEL	Télécharge des fichiers dans ce canal de configuration
-d DEST_FILE, --dest-file=DEST_FILE	Télécharge le fichier comme ce chemin
-t TOPDIR, --topdir=TOPDIR	Rend tous les fichiers relatifs à cette chaîne
--delim-start=DELIM_START	Commencer le délimiteur pour l'interpolation de variables
--delim-end=DELIM_END	Finir le délimiteur pour l'interpolation de variables

Option	Description
-h, --help	Affiche le message d'aide et quitte

1.1.3.13. Téléchargement de plusieurs fichiers en même temps

Pour télécharger plusieurs fichiers dans un canal de configuration depuis un disque local et en une seule opération, exécutez la commande suivante :

```
rhncfg-manager upload-channel --topdir=topdir channel-label
```

Une sortie semblable à celle reproduite ci-dessous devrait apparaître :

```
Using config channel example-channel4 Uploading /tmp/ola_world.txt from
blah4/tmp/ola_world.txt
```

La table suivante liste les options disponibles pour **`rhncfg-manager upload-channel`** :

Tableau 1.11. options de `rhncfg-manager upload-channel`

Option	Description
-t TOPDIR, --topdir=TOPDIR	Répertoire auquel tous les chemins de fichiers sont associés
-c CHANNEL, --channel=CHANNEL	Liste des canaux dans lesquels les informations de configuration seront téléchargées. Les canaux sont délimités par ",". Par exemple : --channel=foo,bar,baz
-h, --help	Affiche le message d'aide et quitte

1.2. MONITORING

Le droit d'accès Red Hat Network Monitoring vous permet d'effectuer de nombreuses actions conçues de façon à ce que vos systèmes continuent de fonctionner correctement et efficacement. Avec ce droit, vous pouvez surveiller de près les ressources système, les services réseau, les bases de données et les applications standards et personnalisées.

Monitoring fournit des informations sur l'état en temps réel et historiquement, ainsi que des données de métriques spécifiques. Celui-ci fournit des notifications immédiates lors de défaillances et de dégradations de performance avant qu'elles ne deviennent critiques. Il fournit également les informations nécessaires pour mener la planification de capacités et la corrélation d'événements. Par exemple, les résultats d'une sonde qui enregistre l'utilisation de CPU sur les systèmes seraient de valeur inestimable pour la répartition des charges sur ces systèmes.

Il y a deux composantes au système Monitoring : le système de contrôle Monitoring, et le *Monitoring scout*. Le système de contrôle assure les fonctions principales, telles que le stockage de données de contrôle et agit dessus. Monitoring scout exécute toutes les sondes et recueille des données de contrôle. Le monitoring scout peut être activé pour s'exécuter sur un système Satellite ou Red Hat Satellite Proxy. L'utilisation de monitoring scout sur Proxy permet de décharger le travail du Satellite, fournissant une évolutivité pour les sondes.

Le niveau de service Monitoring implique la définition de méthodes de notification, l'installation de sondes sur les systèmes, la revue régulière du statut de toutes les sondes et la production de rapports affichant les données historiques pour un système ou un service. Cette section cherche à identifier les tâches communes associées au droit d'accès Monitoring. Souvenez-vous que pratiquement tous les changements qui affectent votre infrastructure Monitoring doivent être finalisés en mettant à jour votre configuration, sur la page **`Scout Config Push`**.

1.2.1. Conditions préalables

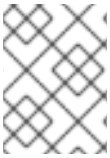
Avant d'essayer d'implémenter le droit d'accès Red Hat Network Monitoring sur votre infrastructure, assurez-vous que tous les outils nécessaires sont bien en place. Vous aurez besoin au minimum des éléments suivants :

- Droits d'accès Monitoring - Ces droits d'accès sont requis pour tous les systèmes devant être surveillés. Le Monitoring est uniquement pris en charge sur les systèmes Red Hat Enterprise Linux.
- Red Hat Satellite avec Monitoring - les systèmes Monitoring doivent être connectés à un Satellite avec un système d'exploitation de base Red Hat Enterprise Linux 5 ou une version supérieure.
- Monitoring Administrator - Ce rôle doit être donné aux utilisateurs qui installent des sondes, créent des méthodes de notification ou modifient l'infrastructure de contrôle d'une manière ou d'une autre (souvenez-vous que l'administrateur de Satellite hérite automatiquement des capacités de tous les autres rôles au sein d'une organisation et peut donc mener ces tâches). Assignez ce rôle sur la page **`Détails utilisateur`** de l'utilisateur.
- Red Hat Network monitoring daemon - Ce démon de contrôle (ou surveillance), ainsi que la clé SSH pour le scout, est requis sur les systèmes surveillés pour que les les contrôleurs de processus internes soient bien exécutés. Vous pouvez cependant exécuter ces sondes en utilisant le démon SSH existant de ces systèmes (**`sshd`**). Reportez-vous à la Section 1.2.2, « Configuration du démon Red Hat Network Monitoring Daemon (**`rhnmd`**) » pour des instructions sur l'installation et une courte liste des sondes nécessitant cette connexion sécurisée. Consultez Annexe A, *Sondes* pour une liste complète des sondes disponibles.

Activer Monitoring

Monitoring est désactivé par défaut, et devra être activé avant d'être utilisé.

1. Connectez-vous avec des privilèges d'administrateur de Satellite, et naviguez dans **Admin** → **Configuration Red Hat Satellite**. Cochez la case **`Activer le Monitoring`**, puis cliquez sur **`Mettre à jour`**pour enregistrer.
2. Redémarrez les services pour qu'ils enregistrent les changements. Rendez-vous sur l'onglet **restart** pour redémarrer le satellite. Cela va mettre le Satellite hors ligne pendant quelques minutes.
3. Vérifiez si l'onglet **Monitoring** est disponible sour **Configuration Red Hat Satellite** afin de confirmer que Monitoring est activé.
4. Rendez-vous sur **Admin** → **Configuration Red Hat Satellite** → **Monitoring**. Cochez la case **`Activer Monitoring Scout`** pour activer le scout. Puis cliquez sur**`Mettre à jour la configuration`** pour enregistrer.



NOTE

Il est recommandé de laisser les valeurs par défaut de la configuration de Monitoring. **Sendmail** doit être configuré pour utiliser les notifications.

1.2.2. Configuration du démon Red Hat Network Monitoring Daemon (`rhnmd`)

Pour profiter au maximum de vos droits Monitoring, Red Hat suggère d'installer le démon Red Hat Network Monitoring sur vos systèmes client. Basé sur **OpenSSH**, **`rhnmd`** permet au Satellite de communiquer de manière sécurisée avec le système client pour accéder aux processus internes et pour obtenir le statut des sondes.

Veuillez noter que le démon Red Hat Network Monitoring requiert que les systèmes contrôlés autorisent les connexions sur le port 4545. Vous pouvez éviter d'ouvrir ce port et d'installer le démon en utilisant à la place **`sshd`**. Reportez-vous à Section 1.2.2.2, « Configuration de SSH » pour davantage d'informations.

Certaines sondes nécessitent le démon. Une connexion chiffrée, soit par le démon Red Hat Network Monitoring, soit par **`sshd`**, est requise sur les systèmes client pour l'exécution des sondes suivantes :

- Linux::CPU Usage
- Linux::Disk IO Throughput
- Linux::Disk Usage
- Linux::Inodes
- Linux::Interface Traffic
- Linux::Load
- Linux::Memory Usage
- Linux::Process Counts by State
- Linux::Process Count Total
- Linux::Process Health
- Linux::Process Running
- Linux::Swap Usage
- Linux::TCP Connections by State
- Linux::Users
- Linux::Virtual Memory
- LogAgent::Log Pattern Match
- LogAgent::Log Size
- Network Services::Remote Ping
- Oracle::Client Connectivity

- General::Remote Program
- General::Remote Program with Data

Notez que toutes les sondes du groupe Linux exigent ce pré-requis.

1.2.2.1. Installation du démon Red Hat Network Monitoring

Installez le démon Red Hat Network Monitoring pour préparer les systèmes au contrôle en utilisant les sondes identifiées dans **rhnmd**. Remarquez que les étapes de cette section sont facultatives si vous prévoyez d'utiliser **sshd** pour autoriser des connexions sécurisées entre l'infrastructure de contrôle Red Hat Network Monitoring et les systèmes contrôlés. Consultez Section 1.2.2.2, « Configuration de SSH » pour obtenir des instructions.

Le paquetage **rhnmd** se trouve dans le canal Red Hat Network Tools (outils Red Hat Network) pour toutes les distributions Red Hat Enterprise Linux. Pour l'installer, suivez les étapes suivantes :

1. Abonnez les systèmes afin qu'ils soient contrôlés par le canal Red Hat Network Tools associé au système. Ceci peut être effectué de manière individuelle via le sous-onglet **Détails du système** → **Canaux** → **Logiciels** ou pour de multiples systèmes à la fois via l'onglet **Détails du système** → **Systèmes cibles**.

2. Une fois abonné, veuillez ouvrir l'onglet **Détails du canal** → **Paquetages** et recherchez le paquetage **rhnmd** (sous la lettre « R »).

3. Cliquez sur le nom de paquetage pour ouvrir la page **Package Details**. Passez sous l'onglet **Target Systems**, sélectionnez les systèmes souhaités et cliquez sur **Install Packages**.

4. Installez la clé publique SSH sur tous les systèmes client à contrôler, comme la Section 1.2.2.3, « Installation de la clé SSH » le décrit.

5. Lancez le démon Red Hat Network Monitoring sur tous les systèmes client à l'aide de la commande suivante :

```
service rhnmd start
```

6. Lors de l'ajout de sondes qui nécessitent le démon, acceptez les valeurs par défaut pour **RHNMD User** et **RHNMD Port** : respectivement **nocpulse** et **4545**.

1.2.2.2. Configuration de SSH

Si vous souhaitez éviter l'installation du démon Red Hat Network Monitoring et l'ouverture du port 4545 sur les systèmes client, vous pouvez configurer **sshd** de façon à fournir la connexion chiffrée nécessaire entre les systèmes et Red Hat Network. Cette option peut être hautement désirable si **sshd** est déjà en cours d'exécution. Pour configurer le démon en mode de contrôle, suivez les étapes suivantes :

1. Assurez-vous que le paquetage SSH est installé sur les systèmes à contrôler :

```
rpm -qi openssh-server
```

2. Identifiez l'utilisateur à associer au démon. Celui-ci peut être n'importe quel utilisateur sur le système, tant que la clé SSH requise peut être ajoutée dans le fichier **~/.ssh/authorized_keys** de l'utilisateur.

3. Identifiez le port utilisé par le démon, comme l'identifie son fichier de configuration **/etc/ssh/sshd_config**. La valeur par défaut est le port 22.

4. Installez la clé publique SSH sur tous les systèmes client à contrôler, comme la Section 1.2.2.3, « Installation de la clé SSH » le décrit.

5. Lancez **sshd** sur tous les systèmes client à l'aide de la commande suivante :

```
service sshd start
```

6. Lors de l'ajout de sondes qui nécessitent le démon, insérez les valeurs dérivées des étapes 2 et 3 dans les champs **RHNMD User** et **RHNMD Port**.

1.2.2.3. Installation de la clé SSH

Que vous utilisiez **rhnmd** ou **sshd**, vous devez installer la clé SSH publique du démon Red Hat Network Monitoring sur les systèmes à contrôler pour terminer la connexion sécurisée. Pour l'installer, suivez les étapes suivantes :

1. Rendez-vous sur la page **Monitoring** → **Scout Config Push** de l'interface Satellite et cliquez sur le nom du scout qui contrôlera le système client. La clé SSH **id_dsa.pub** est visible sur la page suivante.

2. Copiez la chaîne de caractères (commençant par ssh-dss et finissant par le nom d'hôte du Satellite).

3. Sélectionnez **Systèmes** depuis le menu de gauche et cliquez sur la case à cocher à côté des systèmes auxquels vous souhaitez envoyer la clé SSH. Cliquez sur le bouton **Manage** (Gérer) en haut de la page pour terminer.

4. A partir de **System Set Manager**, cliquer sur **Exécuter les commandes à distance**, puis sur la case **Script**, enfin saisir la ligne suivante :

```
#!/bin/sh
cat <<EOF >> ~nocpulse/.ssh/authorized_keys
```

   Puis, cliquez sur **Entrée** et collez la clé SSH et ajoutez EOF. Le résultat devrait ressembler à ce qui suit :

```
#!/bin/sh
cat <<EOF>> ~nocpulse/.ssh/authorized_keys
ssh-dss AABBAB3NzaC3kc3MABCCBAJ4cmyf5jt/ihdtFbNE1YHsT0np0SYJz7xk
hzoKUUWnZmOUqJ7eXoTbGEcZjZLppOZgzAepw1vUHXfa/L9XiXvsV8K5Qmcu70h0
1gohBIder/1I1QbHMCgfDVFPtfV5eedau4AAACAc99dHbWhk/dMPiWXgHxdI0vT2
SnuozIox2klmfbTeO4Ajn/Ecfxqgs5diat/NIaeoItuGUYepXFoVv8DVL3wpp45E
02hjmp4j2MYNpc6Pc3nPOVntu6YBv+whB0VrsVzeqX89u23FFjTLGbfYrmMQflNi
j8yynGRePIMFhI= root@satellite.example.com
EOF
```

5. Définissez la date et l'heure auxquelles vous souhaitez que les actions prennent place, puis cliquez sur **Schedule Remote Command**.

Une fois que la clé est en place et accessible, toutes les sondes qui en ont besoin, devraient autoriser des connexions **ssh** entre l'infrastructure de Monitoring et le système contrôlé. Vous pouvez alors

programmer des sondes qui nécessitent le démon de contrôle, à être exécutées sur les systèmes nouvellement configurés.

1.2.3. Configuration du paquetage `mysql` pour les sondes

Si Red Hat Satellite va servir des systèmes client ayant des droits d'accès au service Monitoring sur lesquels vous souhaitez exécuter des sondes **MySQL**, vous devrez configurer le paquetage **`mysql`** sur Red Hat Satellite. Consultez l'Annexe A, *Sondes* pour obtenir une liste de toutes les sondes disponibles.

Abonnez le Satellite au canal de base Red Hat Enterprise Linux et installez le paquetage **`mysql`** via **`up2date`**, **`yum`** ou Red Hat Network Hosted.

Une fois que vous aurez terminé, vous pourrez utiliser votre satellite pour programmer les sondes MySQL.

1.2.4. Activation des notifications

Outre l'affichage du statut des sondes dans l'interface Red Hat Network, vous pouvez être informé dès que l'état d'une sonde change. Ceci est particulièrement important lors du contrôle de systèmes de production à mission critique. Pour cette raison, Red Hat vous recommande de profiter de cette fonctionnalité.

Pour activer les notifications de sondes dans Red Hat Network, vous devez avoir identifié un serveur d'échange de courrier et un domaine de courrier pendant l'installation de Red Hat Satellite et configuré **sendmail** de façon à traiter correctement les courriers entrants. Consultez la section *Installation* du *Guide d'installation Red Hat Satellite* pour davantage de détails.

1.2.4.1. Création de méthodes de notification

Les notifications son envoyées via une *méthode de notification*, une adresse électronique ou de pager associée à un utilisateur Red Hat Network spécifique. Bien que l'adresse soit liée à un compte utilisateur particulier, elle peut servir à de multiples administrateurs via un alias ou une liste de diffusion. Chaque compte utilisateur peut contenir plusieurs méthodes de notification. Pour créer une méthode de notification, veuillez effectuer les étapes suivantes :

1. Connectez-vous au Satellite en tant qu'administrateur Satellite ou Monitoring.

2. Rendez-vous sur **`Utilisateurs`** et sélectionnez le nom d'utilisateur. Sur la page **`Détails de l'utilisateur`**, cliquez sur **Méthodes de notification → créer une nouvelle méthode**.

3. Saisissez une étiquette intuitive et descriptive pour le nom de la méthode, comme par exemple **`email du jour du DBA`**, puis entrez l'adresse électronique correcte. Souvenez-vous que les étiquettes pour toutes les méthodes de notification sont disponibles dans une seule liste durant la création de sondes. Elles devraient donc être uniques pour votre organisation.

4. Sélectionnez la case si vous désirez que des messages abrégés soient envoyés à l'adresse électronique. Ce format plus court contient seulement l'état de la sonde, le nom d'hôte du système, le nom de la sonde, l'heure et la date du message et l'ID d'envoi. Le format standard, plus long affiche en plus les en-têtes des messages, des détails sur le système et les sondes et des instructions pour les réponses.

5. Une fois terminé, cliquez sur **`Créer la méthode`**. La nouvelle méthode est affichée dans l'onglet **Détails de l'utilisateur → Méthodes de notification** et sur la page **`Notification`** sous la catégorie **`Monitoring`** du haut. Cliquez sur son nom pour la modifier ou la supprimer.

6. Lors de l'ajout de sondes, cochez la case **`Probe Notifications`** et sélectionnez la nouvelle méthode de notification dans le menu déroulant. Les méthodes de notification assignées aux sondes ne peuvent pas être supprimées tant que cette association n'est pas supprimée.

1.2.4.2. Réception de notifications

Si vous créez des méthodes de notification et que vous les associez avec des sondes, vous devez être prêt à les recevoir. Ces notifications arriveront sous la forme de petits messages texte envoyés à l'adresse électronique spécifiée. Voici un exemple de notification par courrier électronique :

```
Subject: CRITICAL: [hostname]: Satellite: Users at 1
From: "Monitoring Satellite Notification" (rogerthat01@redhat.com)
Date: Mon, 26 Aug 2013 13:42:28 -0800
To: user@organization.com

This is Red Hat Monitoring Satellite notification 01dc8hqw.

Time: Mon Aug 26, 21:42:25 PST
State: CRITICAL
System: [hostname] ([IP address])
Probe: Satellite: Users
Message: Users 6 (above critical threshold of 2)
Notification #116 for Users

Run from: Red Hat Monitoring Satellite
```

Comme vous pouvez le voir, les notifications par courrier électronique plus longues contiennent pratiquement tout ce que vous devriez savoir sur la sonde associée. En plus de la commande, du temps d'exécution, du système contrôlé et de l'état de la sonde, le message contient l'*ID d'envoi*, qui est une chaîne de caractères unique représentant le message précis et la sonde. Dans le message ci-dessus, l'ID d'envoi est 01dc8hqw.

NOTE

Vu que les notifications peuvent être générées dès qu'une sonde change d'état, de simples modifications dans votre réseau peuvent provoquer un déluge de notifications. Les notifications peuvent être redirigées vers une boîte de réception spécifiquement conçue pour celles-ci afin d'éviter de créer des problèmes liés aux priorités du courrier. La section suivante traite de la redirection des notifications.

1.2.4.3. Redirection de notifications

Lorsque vous recevez une notification, vous pouvez la rediriger en incluant des règles avancées de notification dans un courrier de reconnaissance. Activer les redirections de réponses courrier en ouvrant le fichier **`/etc/aliases`** et en ajoutant la ligne suivant :

```
rogerthat01:    "| /etc/smrsh/ack_queuer.pl"
```

Une fois que le paramètre est défini, répondez simplement à la notification et incluez l'option souhaitée. Parmi les options de redirection, ou *types de filtres*, possibles figurent :

- ACK METOO - Envoie la notification aux destinations de redirection *en plus de* la destination par défaut.

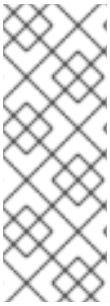
- ACK SUSPEND - Suspend la méthode de notification pour une durée spécifiée.
- ACK AUTOACK - Ne change pas la destination de la notification, mais reconnaît automatiquement les alertes correspondantes dès qu'elles sont envoyées.
- ACK REDIR - Envoie la notification aux destinations de redirection *à la place de* la destination par défaut.

Le format de la règle devrait être *type_filtre type_sonde durée adresse_électronique* où *type_filtre* est l'une des commandes avancées précédentes, *type_sonde* indique **check** ou **host**, *durée* est la durée de temps pour la redirection, et *adresse_électronique* est la destination souhaitée. Par exemple :

```
ACK METOO host 1h boss@domain.com
```

La mise en majuscules n'est pas nécessaire. La durée peut être spécifiée en minutes (m), heures (h) ou jours (d). Les adresses électroniques sont nécessaires pour les notifications de redirection (REDIR) et supplémentaires(METOO).

La description de l'action contenue dans le courrier résultant aura par défaut la valeur de la commande saisie par l'utilisateur. La raison affichée est un résumé de l'action, par exemple « email ack redirect by user@domain.com » (message ack redirigé par utilisateur@domain.com), où l'utilisateur équivaut à l'expéditeur du message.



NOTE

Vous pouvez arrêter ou rediriger pratiquement toutes les notifications de sondes en répondant aux messages électroniques de notifications avec une variante de la commande **`ack suspend host`**. Cependant, vous ne pouvez pas arrêter les notifications de sondes du Satellite en répondant à une sonde avec **`ack suspend host`** ou d'autres réponses redirigées. Ces sondes nécessitent que vous changiez les notifications sur l'interface web du Satellite.

1.2.4.4. Suppression de méthodes de notification

Les relations existantes entre méthodes et sondes peuvent compliquer le processus de suppression des méthodes de notification. Veuillez suivre ces étapes pour supprimer une méthode de notification :

1. Connectez-vous au Satellite en tant qu'administrateur Satellite ou Monitoring.
2. Rendez-vous sur la page **Monitoring** → **Notifications** et cliquez sur le nom de la méthode à supprimer.
3. Sur l'onglet **Utilisateur** → **Détails de l'utilisateur** → **Méthodes de notification**, cliquez sur **`Supprimer la méthode`**. Si la méthode n'est associée à aucune sonde, une page de confirmation vous sera présentée. Cliquez sur **`Confirmer la suppression`**. La méthode de notification est alors supprimée.

NOTE

Vu que le nom et l'adresse de la méthode de notification peuvent être édités, pensez à mettre à jour la méthode au lieu de la supprimer. Cette action redirigera les notifications depuis toutes les sondes en utilisant la méthode sans avoir à éditer chaque sonde et créer une nouvelle méthode de notification.

4. Si la méthode est associée à une ou plusieurs sondes, au lieu d'une page de confirmation, une liste des sondes qui utilisent la méthode et des systèmes auxquels sont attachées les sondes, vous sera présentée. Cliquez sur le nom de la sonde pour passer directement sur l'onglet **Détails du système → Sondes**.

5. Veuillez sélectionner une autre méthode de notification et cliquez sur **`Mettre à jour la sonde`**.

6. Retournez sur la page **Monitoring → Notifications** et supprimez la méthode de notification.

1.2.5. À propos des sondes

Maintenant que le démon Red Hat Network Monitoring a été installé et que les méthodes de notification ont été créées, vous pouvez commencer à installer les sondes sur vos systèmes ayant des droits d'accès de Monitoring. Si un système possède des droits d'accès de Monitoring, un onglet **`Sondes`** est affiché sur sa page **`Détails du système`**. Vous y effectuerez la plupart des travaux concernant les sondes.

1.2.5.1. Gestion des sondes

Les sondes sont créée via le serveur Red Hat Satellite. Une fois que les sondes ont été créées, elles sont propagées vers les systèmes ayant des droits d'accès monitoring spécifiés enregistrés sur le Satellite. Veuillez suivre les étapes ci-dessous pour ajouter une sonde au serveur Satellite :

1. Connectez-vous Satellite en tant qu'administrateur Satellite ou administrateur de groupe de systèmes du système.

2. Rendez-vous sur l'onglet **Détails du système → Sondes** et cliquez sur **`Créer un nouvelle sonde`**.

3. Sur la page **`Création de sondes système`**, remplissez tous les champs requis. Sélectionnez tout d'abord le groupe de commandes de sondes (Probe Command Group). Ceci modifie la liste des sondes disponibles et d'autres champs et conditions préalables. Consultez l'Annexe A, *Sondes* pour obtenir la liste complète des sondes par groupes de commandes. Souvenez-vous que certaines sondes requièrent que le démon Red Hat Network Monitoring soit installé sur le système client.

4. Sélectionnez la commande de sonde (Probe Command) et l'agent de contrôle Monitoring Scout souhaités, habituellement **`Red Hat Monitoring Satellite`**, mais ici, probablement Red Hat Satellite Proxy Server. Saisissez une description courte mais unique pour la sonde.

5. Sélectionnez la case **`Notifications de sonde`** pour recevoir des notifications lorsque la sonde change d'état. Utilisez le menu déroulant **`Intervalle de vérification de sonde`** pour déterminer la fréquence d'envoi des notifications. La sélection de **`1 minute`** (et de la case **`Notification de sonde`**) signifie que vous recevrez des notifications chaque minute, lorsque la sonde dépasse ses limites CRITICAL ou WARNING. Reportez-vous à la Section 1.2.4, « Activation des notifications »/> pour savoir comment créer des méthodes de notification et reconnaître leurs messages.

6. Utilisez les champs **`Utilisateur RHNMD`** et **`Port RHNMD`**, s'ils apparaissent, pour forcer la sonde à communiquer via **`sshd`**, plutôt que par le démon Red Hat Network Monitoring. Reportez-vous à la Section 1.2.2.2, « Configuration de SSH » pour davantage de détails. Sinon, acceptez les valeurs par défaut de **`nocpulse`** et **`4545`**, respectivement.

7. Si le champ **`Timeout`** est présent, modifiez sa valeur par défaut selon vos besoins. La plupart, mais pas tous les délais d'attente provoquent un état UNKNOWN (inconnu). Si les métriques de

la sonde sont basées sur le temps, assurez-vous que le délai n'est pas inférieur à la durée allouée aux limites. Sinon, les métriques ne servent à rien, vu que le délai d'attente de la sonde sera atteint avant toute autre limite.

8. Utilisez les champs restants pour établir les limites d'alerte de la sonde, dans les cas applicables. Ces valeurs CRITICAL et WARNING déterminent à quel point la sonde a changé d'état. Reportez-vous à la Section 1.2.5.2, « Définition de limites » pour obtenir les meilleures pratiques de ces limites.

9. Une fois terminé, cliquez sur **`Create Probe`**. Souvenez-vous que vous devez valider la modification de votre configuration de Monitoring sur la page **`Scout Config Push`** pour que celle-ci prenne effet.

Pour supprimer une sonde, rendez-vous sur sa page **`État actuel`** (en cliquant sur le nom de la sonde depuis l'onglet **Détails du système** → **Sondes**) et cliquez sur **`Supprimer la sonde`**. Confirmez ensuite la suppression.

1.2.5.2. Définition de limites

De nombreuses sondes offertes par Red Hat Satellite contiennent des limites d'alerte qui, lorsqu'elles sont dépassées, indiquent un changement de l'état de la sonde. Par exemple, la sonde Linux::CPU Usage vous permet de définir les limites CRITICAL et WARNING pour le pourcentage de CPU utilisé. Si le système contrôlé rapporte que 75 pour cent du CPU est utilisé et que la valeur de la limite WARNING est fixée 70 pour cent, la sonde passera dans un état WARNING. Certaines sondes offrent une multitude de telles limites.

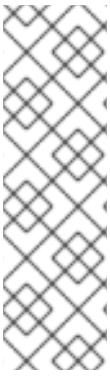
Afin de profiter au maximum de vos droits d'accès de Monitoring et d'éviter de fausses notifications, Red Hat vous recommande d'exécuter vos sondes sans notifications pendant un moment pour établir une performance de ligne de base pour chacun de vos systèmes. Bien que les valeurs par défaut fournies pour les sondes puissent vous convenir, chaque organisation a un environnement différent qui peut exiger la modification des limites.

1.2.5.3. Surveillance du serveur Satellite

En outre de la surveillance de tous vos systèmes clients, vous pouvez aussi utiliser Red Hat Network pour surveiller votre Satellite ou Proxy. Pour surveiller le Satellite ou Proxy, trouvez un système surveillé par le serveur et rendez-vous sur l'onglet **Détails du système** → **Sondes** de ce système.

Cliquez sur **`Créer une nouvelle sonde`** et sélectionnez le groupe de commandes de sondes **`Satellite`**. Remplissez ensuite les champs restants comme vous le feriez pour toute autre sonde. Reportez-vous à la Section 1.2.5.1, « Gestion des sondes » pour obtenir des instructions.

Bien que le Satellite ou Proxy semble être surveillé par le système client, la sonde est en fait exécutée depuis le serveur même. Les limites et les notifications fonctionnent normalement.



NOTE

Toutes les sondes qui nécessitent des connexions du démon Red Hat Network Monitoring ne peuvent pas être utilisées sur le Red Hat Satellite ou Red Hat Satellite Proxy Server sur lequel des logiciels de contrôle Monitoring sont en cours d'exécution. Sont incluses la plupart des sondes du groupe de commandes Linux ainsi que les sondes « Log Agent » (agent de journalisation) et les sondes « Remote Program » (programme distant). Utilisez les sondes du groupe de commandes Satellite pour contrôler les Red Hat Satellites et les Red Hat Satellite Proxy Server. Dans le cas de scouts Proxy, les sondes sont répertoriées sous le système pour lequel elles effectuent des rapports de données.

1.2.6. Monitoring

Si vous cliquez sur l'onglet **Monitoring** sur la barre de navigation du haut, la catégorie **Monitoring** et ses liens apparaissent. Ces pages, qui nécessitent des droits d'accès au service Monitoring, vous permettent de consulter les résultats des sondes que vous avez configurées pour une exécution sur les systèmes ayant des droits d'accès Monitoring et pour une gestion de la configuration de votre infrastructure de contrôle.

Initiez le contrôle d'un système via l'onglet **Sondes** de la page **Détails du système**. Consultez l'Annexe A, *Sondes* pour une liste complète des sondes disponibles.

1.2.6.1. Statut de la sonde

IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

La page **Statut de la sonde** s'affiche par défaut lorsque vous cliquez sur **Monitoring**, situé sur la barre de navigation en haut.

La page **Statut de la sonde** affiche le résumé du nombre de sondes dans les différents états et fournit une simple interface pour rapidement identifier les sondes qui posent problème. Veuillez noter que les totaux des sondes dans les onglets figurant en haut de la page ne correspondront peut-être pas aux nombres de sondes affichés dans les tableaux ci-dessous. Les comptes qui apparaissent en haut incluent les sondes pour tous les systèmes de votre organisation alors que les tableaux affichent uniquement les sondes qui se trouvent sur les systèmes auxquels vous avez accès grâce au rôle d'administrateur de groupe de systèmes. Il est aussi possible que le nombre de sondes affichées soit en retard d'un maximum d'une minute.

La liste suivante décrit chaque état et identifie les icônes qui leur sont associés :

-  - *Critical* - La sonde a atteint la limite CRITICAL.
-  - *Warning* - La sonde a atteint la limite WARNING.
-  - *Unknown* - La sonde n'est pas en mesure de rapporter de données métriques ou d'état.
-  - *Pending* - La sonde a été programmée mais n'a pas encore été exécutée ou n'est pas en mesure de pouvoir être exécutée.
-  - *OK* - La sonde est en cours d'exécution normale.

La page **Probe Status** contient des onglets pour chaque état possible, ainsi qu'un onglet qui liste toutes les sondes. Chaque table contient des colonnes indiquant le statut de la sonde, le système contrôlé, les sondes utilisées et la date et l'heure de la dernière mise à jour du statut.

Dans ces tableaux, cliquer sur le nom du système vous conduira à l'onglet **Monitoring** (contrôle) de la page **Détails du système**. Cliquer sur le nom de la sonde vous conduira à la page **État actuel**. À partir de là, vous pouvez modifier la sonde, la supprimer et générer des rapports basés sur ses résultats.

Les informations sur le statut de la sonde et les données Monitoring (ou données de contrôle ou surveillance) qui étaient auparavant disponibles uniquement à travers l'interface web du Satellite

peuvent maintenant être exportées dans un fichier CSV. Cliquez sur les liens **`Télécharger CSV`** à partir des pages Monitoring afin de télécharger des fichiers CSV avec des informations pertinentes. Les données exportées peuvent inclure, mais ne sont pas limitées à :

- Statut de la sonde
- Toutes les sondes dans un état donné (OK, MISE EN GARDE, INCONNU, CRITIQUE, EN ATTENTE)
- Historique d'événements d'une sonde

1.2.6.1.1. Statut de la sonde ⇒ Critical (critique)

IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Les sondes qui ont dépassé leurs limites CRITICAL ou qui ont atteint un statut critique par d'autres moyens. Par exemple, certaines sondes deviennent critiques (plutôt qu'inconnues) lors du dépassement de leur délai d'attente.

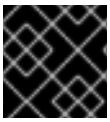
1.2.6.1.2. Statut de la sonde ⇒ Warning (Avertissement)

IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Les sondes ont dépassé leur seuil d'avertissement (WARNING).

1.2.6.1.3. Statut de la sonde ⇒ Unknown (Inconnu)



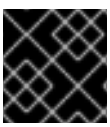
IMPORTANT

Le droit d'accès Monitoring est requis pour cette fonctionnalité.

Les sondes qui ne peuvent pas recueillir les métriques nécessaires pour définir l'état des sondes. La plupart mais pas la totalité des sondes entre dans un état Inconnu (« Unknown ») lorsque leur délai d'attente est dépassé. Cela peut signifier que ce dernier devrait être augmenté ou que la connexion ne peut pas être établie avec le système contrôlé.

Il est également possible que les paramètres de configuration des sondes ne sont pas corrects et que leurs données ne peuvent pas être trouvées. Finalement, cet état peut indiquer qu'une erreur logicielle s'est produite.

1.2.6.1.4. Statut de la sonde ⇒ Pending (En attente)



IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Sondes dont les données n'ont pas été reçues par Red Hat Network. Cet état est prévu pour une sonde qui vient d'être programmée mais qui n'a pas encore été exécutée. Si toutes les sondes passent à un état en attente (pending), votre infrastructure de contrôle peut ne pas fonctionner correctement.

1.2.6.1.5. Statut de la sonde ⇒ OK

IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Sondes ayant été exécutées avec succès sans exception. Cet état est l'état désiré pour toutes les sondes.

1.2.6.1.6. Statut de la sonde ⇒ All (Toutes)

IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Sondes programmées sur les systèmes dans votre compte, répertoriées dans l'ordre alphabétique par nom de système.

1.2.6.1.7. État actuel

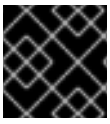
IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Identifie le statut de la sonde sélectionnée et sa dernière exécution, tout en offrant la possibilité de générer un rapport sur la sonde. Bien que cette page est intégrale au contrôle, elle se trouve sous l'onglet **`Probes`** dans la page **`System Details`** vu que sa configuration est spécifique au système contrôlé.

Pour afficher un rapport sur les résultats de la sonde, choisissez une durée appropriée à l'aide des champs **`date`** et décidez si vous souhaitez afficher des données métriques, l'historique du changement des états ou les deux. Pour obtenir des données de métriques, sélectionnez la ou les métriques sur lesquelles vous souhaitez obtenir des rapports et à l'aide des cases à cocher, décidez si les résultats devraient être affichés dans un graphe, un journal d'événements ou les deux. Cliquez ensuite sur **`Generate report`** (générer un rapport) au bas de la page. Si aucune donnée n'existe pour les métriques de la sonde, le message suivant apparaît « NO DATA SELECTED TIME PERIOD AND METRIC » (aucune donnée pour la durée de temps et la métrique spécifiées).

1.2.6.2. Notification



IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Identifie les méthodes de contact établies pour votre organisation. Ces méthodes contiennent des adresses électroniques ou de pageur conçues pour recevoir des alertes provenant de sondes.

Les diverses méthodes de notification qui sont disponibles à votre organisation sont listées sur l'écran par défaut **`Notification`**. Les méthodes sont listées selon l'utilisateur auquel elles s'appliquent.

Pour créer une nouvelle méthode de notification, cliquez sur le nom de l'utilisateur pour lequel la notification s'applique. La page Détails de l'utilisateur ⇒ Méthodes de notification de l'utilisateur apparaît. Cliquez sur le titre de la méthode de notification pour modifier les propriétés de la méthode.

1.2.6.2.1. Notification ⇒ Filters (filtres)

Les filtres de notification vous permettent de créer des règles à long terme qui suspendent, redirigent ou reconnaissent automatiquement les notifications standards ou envoient des notifications supplémentaires. Cela peut être utile dans la gestion de communications de sondes avec des commentaires ou fréquentes.

1.2.6.2.1.1. Notification ⇒ Notification Filters ⇒ Active Filters (filtres actifs)

Cet écran est l'écran par défaut pour l'onglet "Notification Filters". Il affiche tous les filtres actifs disponibles à votre organisation. Cliquez sur le nom du filtre pour éditer ses propriétés.

Pour créer un filtre de notifications, cliquez sur le lien **`create new notification filter`** (créer un nouveau filtre) en haut à droite de l'écran. Configurez chaque option listée ci-dessous et cliquez sur le bouton **`Save Filter`** (enregistrer) pour créer le filtre.

1. *Description* : Saisissez une valeur qui vous permet de distinguer ce filtre d'autres.

2. *Type* : Déterminez l'action que le filtre devrait prendre : rediriger, reconnaître, suspendre ou ajouter la notification entrante.

3. *Send to* (envoyer à) : Les options **`Redirect Notification`** (rediriger la notification) et **`Supplemental Notification`** (notification supplémentaire) dans l'étape deux requièrent une adresse électronique à laquelle envoyer les notifications. Les options restantes ne nécessitent aucune adresse électronique.

4. *Scope* (étendue) : Déterminez les composants de contrôle qui sont sujets au filtre.

5. *Organization/Scout/Probe* : Cette option vous permet de sélectionner l'organisation, les scouts ou les sondes auxquels ce filtre s'applique. Pour sélectionner plusieurs éléments de la liste, appuyez sur la touche **`Ctrl`** tout en cliquant sur les noms des éléments. Pour sélectionner une gamme d'éléments, appuyez sur la touche **`Shift`** tout en cliquant sur le premier et le dernier éléments de la gamme.

6. *Probes in State* (sondes en état) : Sélectionnez quels états de sondes correspondent au filtre. Par exemple, vous pouvez choisir de créer une notification supplémentaire uniquement pour les sondes critiques. Dé-sélectionnez la case à gauche de l'état que vous souhaitez que le filtre ignore.

7. *Notifications sent to* (notifications envoyées à) : Ceci est la méthode à laquelle la notification devrait être envoyée si aucun filtre n'est en place. Vous pouvez, par exemple, rediriger les notifications qui iraient normalement à un utilisateur si ce dernier part en vacances, laissant toutes les autres notifications de la sonde inchangées.

8. *Match Output* (sortie de la correspondance) : Sélectionnez les résultats de notifications précis en saisissant une expression régulière. Si la partie "Message:" de la notification ne correspond pas à l'expression régulière, le filtre n'est pas appliqué.

9. *Recurring* : Sélectionnez si un filtre est exécuté de manière continue ou récurrente. Un filtre

récurrent est exécuté plusieurs fois pendant une durée de temps inférieure à la durée du filtre. Par exemple, un filtre récurrent peut être exécuté pendant 10 minutes toutes les heures entre le début et la fin de l'exécution du filtre. Un filtre non-récurrent est exécuté de manière continue entre le début et la fin de l'exécution du filtre.

10. *Beginning* (début) : Saisissez une date et une heure pour le début du fonctionnement du filtre.

11. *Ending* (fin) : Saisissez une date et une heure pour la fin du filtre.

12. *Recurring Duration* (durée de récurrence) : La durée pendant laquelle un filtre récurrent est actif. Ce champ, uniquement applicable aux filtres récurrents, commence à l'heure **`Beginning`** spécifiée ci-dessus. Toute notification générée en-dehors de la durée spécifiée n'est pas filtrée.

13. *Recurring Frequency* (fréquence) : La fréquence d'activation du filtre.

Les filtres de notifications ne peuvent pas être supprimés. Cependant, un filtre peut être annulé en définissant la date et l'heure de fin dans le passé (notez que la date de fin doit être égale ou supérieure à la date de début, ou les changements échoueront). Une autre méthode est de sélectionner un ensemble de filtres sur la page **`Active`** et de cliquer sur le bouton **`Expire Notification Filters`** en bas à droite. Ces filtres sont alors annulés et apparaissent dans l'onglet **`Expired Filters`** (filtres périmés).

1.2.6.2.1.2. Notification ⇒ Notification Filters ⇒ Expired Filters (filtres périmés)

Cet onglet liste tous les filtres de notification dont la date de fin est déjà passée. Les filtres périmés sont stockés in-définitivement. Cela permet à une organisation de recycler les filtres utiles au besoin et fournit une entrée historique pour la résolution de problèmes.

1.2.6.3. Probe Suites (suites de sondes)

Les suites de sondes vous permettent de configurer et d'appliquer une ou plusieurs sondes à un ou plusieurs systèmes. Elles peuvent être configurées une fois, puis appliquées à un certain nombre de systèmes par lot. Cette opération économise du temps et offre une cohérence pour les clients de Monitoring.

Pour créer et appliquer une suite de sondes, créez tout d'abord une suite de sondes vide, puis configurez les sondes qu'elle contient, et finalement, appliquez la suite aux systèmes sélectionnés.

1. Depuis la page Monitoring ⇒ Probe Suites, sélectionnez le lien **`create probe suite`** (créer une suite de sondes). Saisissez un nom facilement distinguable pour la suite de sondes. Vous pouvez également choisir d'ajouter une courte description à la suite. Cliquez sur le bouton **`Create Probe Suite`** pour continuer.

2. Ajoutez et configurez les sondes qui composent la suite. Cliquez sur le lien **`create new probe`** (créer une nouvelle sonde) en haut à droite.

3. Configurez la sonde et cliquez sur le bouton **`Créer la sonde`** en bas à droite. Répétez ce processus jusqu'à ce que toutes les sondes désirées aient été ajoutées.

NOTE

Sendmail doit être configuré correctement sur Red Hat Satellite et sur chaque système client sur lequel la suite de sondes (« Probe Suite ») est appliquée, le démon **`rhnmd`** doit aussi être installé et en cours d'exécution. Consultez le *Guide d'installation Red Hat Satellite* pour obtenir des informations supplémentaires.

4. Dans l'onglet « Systèmes », ajoutez les systèmes sur lesquels la suite de sondes s'applique. Cliquez sur le lien **`ajouter des systèmes à la suite de sondes`** en haut à droite de l'écran pour continuer.

5. La page suivante affiche une liste de tous les systèmes ayant des droits d'accès à Monitoring. Cochez la case à gauche des systèmes auxquels vous souhaitez appliquer la suite de sondes, sélectionnez le scout que vous souhaitez utiliser et cliquez sur le bouton **`Add systems to probe suite`** pour terminer la création de la suite de sondes.

Vous pouvez soit supprimer soit détacher des sondes de la suite. Le fait de détacher une sonde désassocie les sondes de la suite et les convertit en sondes spécifiques au système pour le système donnée. Cela signifie que les changements apportés aux sondes détachées n'affecteront que ce système. Le fait de supprimer une sonde la supprime de la suite pour tous les systèmes.

Pour supprimer des sondes de la suite de sondes :

1. De la page Monitoring ⇒ Probe Suites, cliquez sur le titre de la suite de sondes que vous souhaitez modifier.

2. Sélectionnez l'onglet **`Probes`** (Sondes).

3. Cochez la case à côté de la sonde que vous souhaitez supprimer.

4. Cliquez sur le bouton **`Supprimer des sondes de la suite de sondes`**.

Vous pouvez également supprimer un système de la suite de sondes. Vous pouvez le faire de deux manières. La première méthode est de détacher le système de la suite de sondes. Ce faisant, le système a toujours les mêmes sondes qui lui sont assignées. Cependant, vous avez maintenant la possibilité de configurer ces sondes individuellement sans affecter d'autres systèmes.

Pour détacher un système de la suite :

1. De la page **`Monitoring`** ⇒ **`Probe Suites`**, cliquez sur le titre de la suite de sondes que vous souhaitez modifier.

2. Sélectionnez l'onglet **`Systémes`**.

3. Cochez la case à côté des systèmes que vous souhaitez supprimer de la suite de sondes.

4. Cliquez sur le bouton **`Détacher les systèmes de la suite de sondes`**.

La deuxième méthode est de supprimer le système de la suite. Le système est supprimé de la suite et toutes les sondes exécutées sur ce système sont supprimées.

NOTE

Cette action supprime toutes les sondes des suites de sondes du système ainsi que toutes les données historiques de série de temps et de journaux d'événements. Cette action est irréversible.

Pour supprimer un système de la suite de sondes et supprimer toutes les sondes associées du système :

1. De la page Monitoring ⇒ Probe Suites, cliquez sur le titre de la suite de sondes que vous souhaitez modifier.

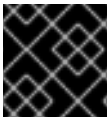
2. Sélectionnez l'onglet **`Systémes`**.

3. Cochez la case à côté des systèmes que vous souhaitez supprimer de la suite de sondes.

4. Cliquez sur le bouton **`Supprimer les systèmes de la suite de sondes`**.

Finalement, comme avec les sondes uniques, vous devriez télécharger un fichier CSV contenant des informations à propos des suites de sondes. Cliquez le lien **`Télécharger le fichier CSV`** en bas de la page **`Monitoring`** ⇒ **`Suites de sondes`** pour télécharger le fichier.

1.2.6.4. Scout Config Push



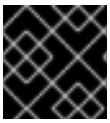
IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

Affiche le statut de votre infrastructure de contrôle (Monitoring). Dès que vous apportez une modification à votre configuration de contrôle, comme l'ajout d'une sonde à un système ou la modification des limites d'une sonde, vous devrez reconfigurer votre infrastructure de contrôle. Pour ce faire, cochez la case du Red Hat Network Server et cliquez sur **`Push Scout Configs`**. Le tableau sur cette page affiche la date et l'heure des commandes d'envoi « push » demandées et terminées.

Cliquer sur le nom du serveur ouvre sa clé publique SSH Red Hat Network Monitoring Daemon. Cela vous permet de copier et coller la clé SSH sur les systèmes qui sont contrôlés par le scout. Cette opération est requise pour que le démon Red Hat Network Monitoring Daemon puisse se connecter au Satellite.

1.2.6.5. Configuration de contrôle générale



IMPORTANT

Le droit d'accès Monitoring est requis pour afficher cet onglet.

La page « Configuration du contrôler général » se trouve sur **Admin** → **Configuration Red Hat Satellite** → **Monitoring**. Elle recueille les informations qui sont applicables de façon universelle à votre infrastructure de contrôle (« Monitoring »). Toute modification sur cette page provoquera la réinitialisation des services Monitoring sur Red Hat Satellite. Des événements de redémarrage seront aussi programmés pour les services Monitoring sur tous les Red Hat Satellite Proxy Servers qui se connectent à ce Satellite et sur lesquels Monitoring est activé. Ainsi, les services Monitoring sur ces serveurs rechargent immédiatement leur configuration.

De façon générale, les paramètres par défaut fournis dans les autres champs sont suffisants vu qu'ils dérivent de votre installation Satellite. Vous pouvez néanmoins utiliser les champs sur cette page pour modifier votre configuration du Monitoring. Par exemple, vous pouvez y changer votre serveur d'échange de courrier. Cette page vous permet également de modifier la destination de tous les messages administratifs provenant du Satellite. Lorsque vous avez terminé, cliquez sur **`Update Config`** (mettre à jour la configuration).

1.3. MULTIPLES SATELLITES

La *synchronisation inter-satellite* (ISS) permet à un Satellite de synchroniser le contenu et les permissions d'une autre instance Satellite dans une relation *pair-à-pair*. Cependant, dans la section suivante, un Satellite qui reçoit un contenu sera nommé « Satellite esclave » et un Satellite agissant comme l'emplacement source du contenu sera nommé « Satellite maître ». Lors de l'utilisation d'ISS pour synchroniser un contenu, l'instance du Satellite esclave peut posséder une installation différente de

celle du maître pour les entités qui ne sont pas un contenu, comme les utilisateurs et organisations. L'administrateur Satellite sur l'instance esclave est libre d'ajouter, supprimer et modifier les entités indépendamment de ce qui se produit sur l'instance maître.

NOTE

Maître et esclave sont des termes hérités comportant des connotations qui ne sont *pas appliquées* par le protocole ISS. Veuillez ne pas oublier la signification de ces termes, comme décrit ci-dessus, lorsque vous étudiez cette section.

La fonctionnalité ISS peut être utilisée de différentes manières selon les besoins de l'organisation. Il existe des configurations ISS dans lesquelles deux Satellites peuvent chacun agir en tant que maître et esclave de l'autre. Cette section contient une section sur des cas d'utilisation et sur la manière de paramétrer ISS pour mieux convenir à votre organisation.

Prérequis ISS

Ci-dessous figurent les conditions requises pour pouvoir utiliser ISS :

- Deux serveurs Red Hat Satellite ou plus
- Au moins un Red Hat Satellite rempli avec au moins un canal
- Privilèges d'administrateur Satellite sur tous les systèmes Satellite destinés à ISS

1.3.1. Synchronisation Inter-Satellite

ISS peut être configuré manuellement ou avec un nouvel outil nommé **`spacewalk-sync-setup`**. Ces deux méthodes sont efficaces et l'utilisateur peut choisir laquelle utiliser.

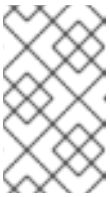
1.3.1.1. Configuration manuelle

Procédure 1.1. Configurer le serveur Satellite maître

Avec Satellite 5.6, ISS permet au Satellite esclave de dupliquer la hiérarchie de confiance organisationnelle et les permissions de canaux personnalisés à partir des paramètres configurés sur le maître. Ceci peut être effectué en exportant des informations sur des organisations spécifiques depuis le Satellite maître vers le Satellite esclave destinataire. L'administrateur Satellite sur le Satellite esclave peut ensuite choisir de mapper les organisations maîtres sur des organisations esclaves spécifiques. De futures opérations **`satellite-sync`** utiliseront ces informations pour assigner les appartenances aux canaux personnalisés à l'organisation esclave qui est mappée sur une organisation maître spécifique. Ceci peut aussi mapper les relations de confiance entre l'organisation maître exposée et les organisations esclave correspondantes, créant ainsi les relations équivalentes sur l'esclave.

1. Sur l'interface web :
    a. Connectez-vous en tant qu'administrateur Satellite.
    b. Cliquez sur **Admin** → **Configuration ISS** → **Installation du maître**.
    c. Cliquez sur le lien **`Ajouter un nouvel esclave`** situé dans le coin en haut à droite.
    d. Veuillez remplir les informations suivantes :

- Nom de domaine complet de l'esclave (FQDN)
- Allow Slave to Sync? - Choisir ce champ permettra au Satellite esclave d'accéder au Satellite maître. Sinon, le contact avec cet esclave sera refusé.
- Sync all orgs to Slave? - Cocher ce champ synchronisera toutes les organisations sur le Satellite esclave.



NOTE

Choisir l'option **`Sync All Orgs to Slave?`** sur la page « Installation du maître » écrasera toute organisation spécifiquement sélectionnée dans la table des organisations locales ci-dessous.

e. Cliquez sur **`Créer`**.

f. (Optionnel) Cliquez sur une organisation locale à exporter sur le Satellite esclave.

g. Cliquez sur **`Autoriser les organisations`**.

NOTE

Sur Satellite 5.5, le Satellite maître utilisait le paramètre ***`iss_slaves`*** du fichier **`/etc/rhn/rhn.conf`** pour identifier quels esclaves pouvaient contacter le Satellite maître. Satellite 5.6 utilise les informations de la page d'installation de maître pour déterminer ces informations.

2. Sur la ligne de commande :

   a. Activez la fonctionnalité ISS (« Inter-satellite synchronization ») dans le fichier **`/etc/rhn/rhn.conf`** :

   ```
   disable_iss=0
   ```

   b. Enregistrez le fichier de configuration, puis redémarrez le service **`httpd`** :

   ```
   service httpd restart
   ```

Procédure 1.2. Configurer les serveurs esclaves

Les serveurs Satellites esclaves sont les machines qui recevront un contenu synchronisé du serveur maître.

1. Pour transférer le contenu des serveurs esclaves de manière sécurisée, vous devrez posséder le certificat **`ORG-SSL`** du serveur maître. Celui-ci peut être téléchargé via HTTP depuis le répertoire **`/pub/`** de n'importe quel Satellite. Le fichier est nommé **`RHN-ORG-TRUSTED-SSL-CERT`**, mais il peut être renommé et placé n'importe où dans le système de fichiers local de l'esclave, par exemple dans le répertoire **`/usr/share/rhn/`**.

2. Connectez-vous au Satellite esclave en tant qu'administrateur Satellite.

3. Cliquez sur **Admin** → **Configuration ISS** → **Installation de l'esclave**.

4. Cliquez sur le lien **`Ajouter un nouveau maître`** situé dans le coin en haut à droite.
5. Veuillez remplir les informations suivantes :
   - Nom de domaine complet du maître (FQDN)
   - Maître par défaut ?
   - Nom de fichier du certificat CA de ce maître - Utilisez le nom complet du certificat CA téléchargé lors de l'étape initiale de cette procédure.
6. Cliquez sur **`Ajouter un nouveau maître`**.

Procédure 1.3. Effectuer une synchronisation Inter-Satellite Sync

Une fois que les serveurs maîtres et esclaves sont configurés, une synchronisation peut être effectuée entre eux.

- Lancez la synchronisation en exécutant la commande **`satellite-sync`** :

```
satellite-sync -c your-channel
```

NOTE

Toute option de ligne de commande fournie avec la commande **`satellite-sync`** remplacera tous les paramètres personnalisés dans le fichier **`/etc/rhn/rhn.conf`**.

Procédure 1.4. Mapper les organisations exportées du Satellite maître avec les organisations du Satellite esclave.

Conditions préalables

Après avoir effectué les procédures précédentes, le Satellite maître devrait s'afficher dans l'« Installation de l'esclave » du Satellite esclave sous **Admin → Configuration ISS → Installation de l'esclave**. Si ce n'est pas la cas, veuillez vérifier les étapes ci-dessus.

Un mappage entre les noms organisationnels sur le Satellite maître permet aux permissions d'accès aux canaux d'être définies sur le Satellite maître et propagées lorsque le contenu est synchronisé sur un Satellite esclave. Il n'est pas nécessaire de mapper tous les détails des organisations et canaux pour tous les Satellites esclaves, les administrateurs Satellite peuvent sélectionner quelles permissions et organisations peuvent être synchronisées en autorisant ou en omettant les mappages.

Pour terminer le mappage, veuillez suivre la procédure sur le Satellite esclave :

1. Connectez-vous en tant qu'administrateur Satellite.
2. Cliquez sur **Admin → Configuration ISS → Installation de l'esclave**.
3. Sélectionnez un Satellite maître en cliquant sur son nom.
4. Utilisez le menu déroulant pour mapper le nom de l'organisation maître exportée sur une organisation locale correspondante dans le Satellite esclave.
5. Cliquez sur **`Mettre à jour le mappage`**.

6. Sur la ligne de commande, exécutez **satellite-sync** sur chaque canal personnalisé pour obtenir la structure de confiance (« trust ») et les permissions de canal correctes :

```
satellite-sync -c your-channel
```

1.3.1.2. Configuration automatisée

spacewalk-sync-setup permet aux utilisateurs de spécifier une instance Satellite maître et esclave et utilise des fichiers de configuration pour définir les informations décrites dans les installations du maître et de l'esclave. Cette commande peut créer un ensemble de fichiers de configuration par défaut si cela est requis. Essentiellement, elle automatise la configuration précédemment installée et mappée pour des relations de maître à esclave.

Conditions préalables

Pour qu'une configuration automatisée fonctionne avec succès :

- Le paquetage spacewalk-util doit être installé sur le système qui exécutera la commande **spacewalk-sync-setup**.
- Les organisations existantes avec des permissions personnalisées du Satellite maître doivent être présentes.
- Les organisations existantes du le Satellite esclave doivent être présentes.

Procédure 1.5. Configurer le serveur Satellite maître

1. Activez la fonctionnalité ISS (« Inter-satellite synchronization ») dans le fichier **/etc/rhn/rhn.conf** :

```
disable_iss=0
```

2. Enregistrez le fichier de configuration, puis redémarrez le service **httpd** :

```
service httpd restart
```

Procédure 1.6. Configurer les serveurs esclaves

Les serveurs Satellites esclaves sont les machines dont le contenu sera synchronisé avec le serveur maître.

1. Pour transférer le contenu des serveurs esclaves de manière sécurisée, vous devrez posséder le certificat **ORG-SSL** du serveur maître. Celui-ci peut être téléchargé via HTTP depuis le répertoire **/pub/** de n'importe quel Satellite. Le fichier est nommé **RHN-ORG-TRUSTED-SSL-CERT**, mais il peut être renommé et placé n'importe où dans le système de fichiers local de l'esclave, par exemple dans le répertoire **/usr/share/rhn/**.
2. Connectez-vous au Satellite esclave en tant qu'administrateur Satellite.
3. Cliquez sur **Admin** → **Configuration ISS** → **Installation de l'esclave**.
4. Cliquez sur le lien **Ajouter un nouveau maître** situé dans le coin en haut à droite.
5. Veuillez remplir les informations suivantes :

- Nom de domaine complet du maître (FQDN)
- Maître par défaut ?
- Nom de fichier du certificat CA de ce maître - Utilisez le nom complet du certificat CA téléchargé lors de l'étape initiale de cette procédure.

6. Cliquez sur **`Ajouter un nouveau maître`**.

Procédure 1.7. Mapper des organisations de Satellite maître avec des organisations de Satellite(s) esclave(s) avec spacewalk-sync-setup

1. Connectez-vous à un système. Peu importe s'il s'agit d'un Satellite maître, esclave, ou même d'un autre type de système, tant que le système peut accéder à l'API XMLRPC public des Satellites maîtres et esclaves.

2. Exécutez la commande **`spacewalk-sync-setup`** sur une interface de ligne de commande :

```
spacewalk-sync-setup --ms=[Master_FQDN] \
--ml=[Master_Sat_Admin_login] \
--mp=[Master_Sat_Admin_password] \
--ss=[Slave FQDN]  --sl=[Slave_Sat_Admin_login] \
--sp=[Slave_Sat_Admin_password> \
--create-templates --apply
```

Où :

- --ms=MASTER, --master-server=MASTER est le nom de domaine complet (FQDN) du maître auquel se connecter
- --ml=MASTER_LOGIN, --master-login=MASTER_LOGIN est l'identifiant d'administrateur Satellite pour le Satellite maître
- --mp=MASTER_PASSWORD, --master-password=MASTER_PASSWORD est le mot de passe de l'identifiant d'administrateur Satellite pour le Satellite maître
- --ss=SLAVE, --slave-server=SLAVE est le nom de domaine complet (FQDN) du Satellite esclave auquel se connecter.
- --sl=SLAVE_LOGIN, --slave-login=SLAVE_LOGIN est l'identifiant d'administrateur Satellite pour le Satellite esclave
- --sp=SLAVE_PASSWORD, --slave-password=SLAVE_PASSWORD est le mot de passe de l'identifiant d'administrateur Satellite pour le Satellite esclave
- --ct, --create-templates est l'option qui crée le fichier d'installation du maître et de l'esclave pour la paire maître/esclave pointée
- --apply dit aux instances Satellite d'effectuer les modifications spécifiées par les fichiers d'installation sur les instances Satellite spécifiées

NOTE

Pour davantage d'options d'installation :

```
spacewalk-sync-setup --help
```

La sortie de cette commande sera comme suit :

```
INFO: Connecting to [admin@master-fqdn]
INFO: Connecting to [admin@slave-fqdn]
INFO: Generating master-setup file $HOME/.spacewalk-sync-
setup/master.txt
INFO: Generating slave-setup file $HOME/.spacewalk-sync-
setup/slave.txt
INFO: Applying master-setup $HOME/.spacewalk-sync-setup/master.txt
INFO: Applying slave-setup $HOME/.spacewalk-sync-setup/slave.txt
```

3. Sur la ligne de commande, exécutez la commande **`satellite-sync`** sur chaque canal personnalisé pour obtenir la structure de confiance (« trust ») et les permissions de canal correctes :

```
satellite-sync -c your-channel
```

1.3.2. Synchronisation organisationnelle

La synchronisation ISS peut aussi être utilisée pour importer un contenu vers n'importe quelle organisation spécifique. Ceci peut être effectué localement ou en utilisant une synchronisation à distance. Cette fonction est utile pour un Satellite déconnecté avec de multiples organisations, où le contenu est retrouvé via des vidages de canaux ou en l'exportant depuis des Satellites connectés, puis en l'important sur le Satellite déconnecté. La synchronisation organisationnelle peut être utilisée pour exporter des canaux personnalisés depuis des Satellite connectés. Elle peut aussi être utilisée efficacement pour déplacer un contenu entre de multiples organisations.

La synchronisation organisationnelle comprend certaines règles qui sont suivies afin de maintenir l'intégrité de l'organisation source :

- Si le contenu de la source appartient à l'organisation ***`NULL`*** (ou à tout autre contenu Red Hat), il se mettra par défaut sur l'organisation ***`NULL`*** même si une organisation destinataire est spécifiée. Ceci assure que le contenu spécifié se trouve toujours dans l'organisation privilégiée ***`NULL`***.
- Si une organisation est spécifiée dans la ligne de commande, le contenu sera importé depuis celle-ci.
- Si aucune organisation n'est spécifiée, il se mettra par défaut sur organisation 1.

Ci-dessous figurent trois scénarios-exemples où des ID organisationnels (***`orgid`***) sont utilisés pour effectuer une synchronisation entre Satellites :

Exemple 1.1. Import de contenu depuis le Satellite maître vers le Satellite esclave

Cet exemple importe le contenu depuis le Satellite maître vers le Satellite esclave :

```
satellite-sync --parent-sat=master.satellite.example.com -c channel-name
--orgid=2
```

Exemple 1.2. Import de contenu depuis le vidage exporté d'une organisation

Cet exemple importe le contenu depuis le vidage exporté d'une organisation spécifique :

```
$ satellite-sync -m /dump -c channel-name --orgid=2
```

Exemple 1.3. Importer un contenu depuis Red Hat Network Hosted

Cet exemple importe un contenu depuis Red Hat Network Hosted (en supposant que le système est enregistré et activé) :

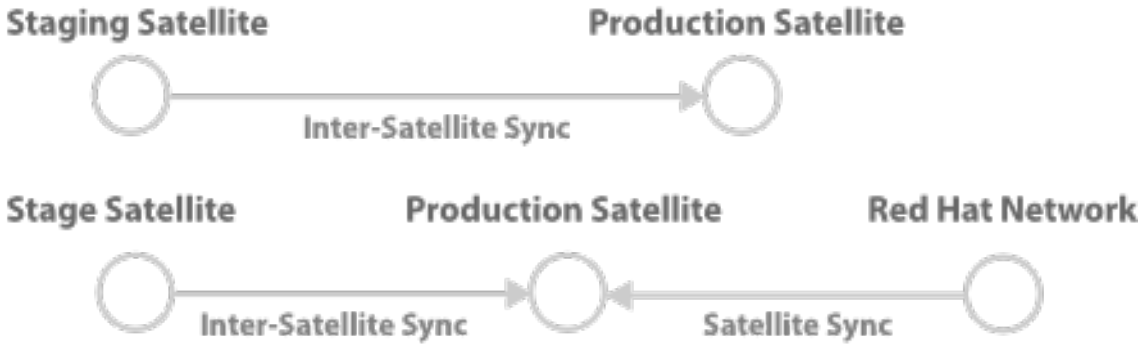
```
$ satellite-sync -c channel-name
```

1.3.3. Cas d'utilisation de la synchronisation ISS (Inter-Satellite Sync)

La synchronisation ISS (« Inter-Satellite Synchronization ») peut être utilisée de plusieurs manières en fonction des besoins de l'organisation. Cette section propose des exemples de la façon dont vous pouvez choisir d'utiliser la synchronisation ISS ainsi que des méthodes de paramétrage et d'opération.

Exemple 1.4. Satellite de pré-production (Staging Satelllite)

Dans cet exemple, un Satellite de *pré-production* (de l'anglais, « Staging Satellite ») est utilisé pour préparer le contenu et assurer le travail d'assurance qualité (QA) sur les paquetages afin de vérifier qu'ils sont corrects pour une utilisation en milieu de production. Une fois que le contenu est approuvé pour partir en production, le Satellite de production synchronisera le contenu du Satellite de pré-production.



1. Exécutez la commande **satellite-sync** pour synchroniser des données avec **rhn_parent** (habituellement Red Hat Network Hosted) :

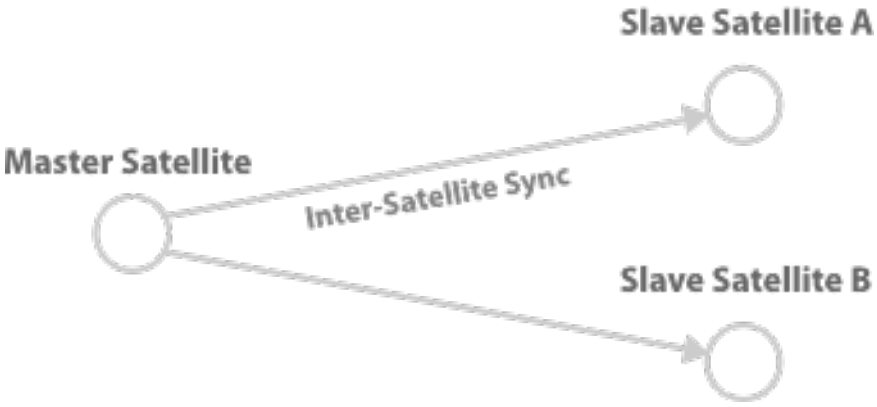
   ```
   satellite-sync -c your-channel
   ```

2. Exécutez la commande suivante pour synchroniser des données depuis le serveur de pré-production :

```
satellite-sync --iss-parent=staging-satellite.example.com -c
custom-channel
```

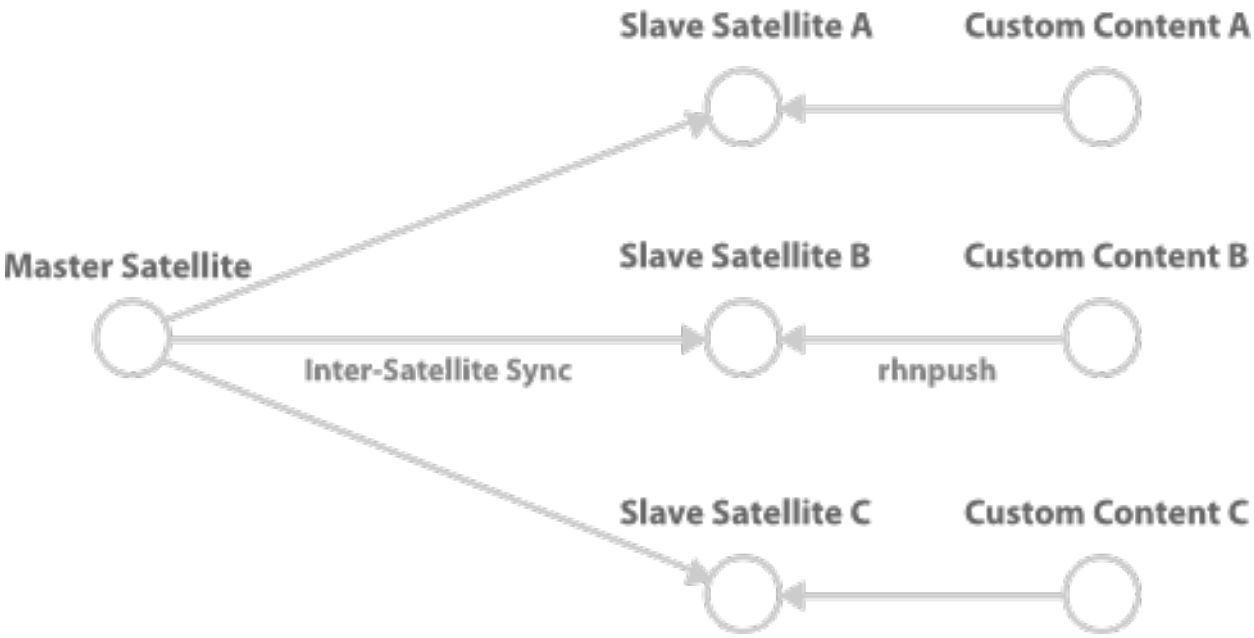
Exemple 1.5. Esclaves synchronisés

Dans cet exemple, le Satellite maître fournit des données directement à ses esclaves, ces changements sont régulièrement synchronisés.



Exemple 1.6. Contenu esclave personnalisé

Cet exemple utilise le Satellite maître comme canal de développement, à partir duquel le contenu est distribué vers tous les Satellites esclaves de production. Certains Satellites esclaves auront un contenu supplémentaire qui n'est pas présent dans les canaux Satellite maîtres. Ces paquetages sont préservés, mais tout changement dans le Satellite maître sera synchronisé avec les Satellites esclaves.



Exemple 1.7. Synchronisation bi-directionnelle

Dans cet environnement, deux serveurs Red Hat Satellite agissent en tant que maître et esclave l'un pour l'autre et peuvent synchroniser leurs contenus entre eux. Le serveur Satellite à partir duquel la

commande **satellite-sync** est exécutée va récupérer le contenu de l'autre serveur Satellite et les données synchronisées dépendront des options exécutées avec **satellite-sync**. Sans aucune option, la synchronisation tentera de mettre à jour tout ce qui a été synchronisé auparavant.

Consultez la Section 1.3.1.1, « Configuration manuelle » pour configurer un Satellite maître. La configurations de deux serveurs Satellite en tant que maître créera une synchronisation bidirectionnelle.

CHAPITRE 2. INFORMATIONS SPÉCIFIQUES À SOLARIS ET RED HAT SATELLITE

Cette section concerne l'utilisation de Red Hat Satellite avec des systèmes Solaris.

2.1. GUIDE DE SUPPORT UNIX

2.1.1. Introduction

Ce chapitre documente la procédure d'installation pour les fonctionnalités Red Hat Network et identifie ses différences lors de son utilisation pour gérer des systèmes client basés sur UNIX. Red Hat Network offre la prise en charge UNIX pour aider les clients à migrer de UNIX à Linux. Vu l'étendue limitée de cette tâche, les fonctions offertes pour la gestion de clients UNIX ne sont pas aussi complètes que celles disponibles pour la gestion de systèmes Red Hat Enterprise Linux.

Les sections suivantes spécifient les variantes UNIX supportées, les fonctionnalités Red Hat Network prises en charge par le système de gestion UNIX, les conditions préalables pour la gestion d'un système UNIX avec Red Hat Network, ainsi que la procédure d'installation pour les clients UNIX.

2.1.1.1. Variantes UNIX supportées

Les variantes, versions et architectures UNIX suivantes sont prises en charge par Red Hat Satellite :

Tableau 2.1. Architectures et versions Solaris prises en charge

Version Solaris	sun4m	sun4d	sun4u	sun4v	sun4us	x86
Solaris 8	oui	non	oui	s/o	non	non
Solaris 9	oui	s/o	oui	s/o	non	oui
Solaris 10	s/o	s/o	oui	oui	non	oui

2.1.1.2. Conditions préalables

Ces éléments sont nécessaires pour obtenir le support UNIX :

- Red Hat Satellite 5.0 ou versions supérieures
- Un certificat de Satellite avec des droits d'accès Management
- Des droits d'accès Management pour chaque client UNIX
- Paquetages Red Hat Network pour UNIX, y compris python, pyOpenSSL et les paquetages Red Hat Network Client
- Paquetages Sunfreeware fournissant des bibliothèques de prise en charge

NOTE

Certains de ces paquetages sont également disponibles via Red Hat Satellite. Consultez la Section 2.1.3.1, « Télécharger et installer des paquetages supplémentaires » pour obtenir une liste complète.

2.1.1.3. Fonctions incluses

Les fonctions suivantes sont incluses dans l'accord de niveau de service de support UNIX car elles existent dans Red Hat Network :

- Le **Démon du service Red Hat Network** (**`rhnsd`**), qui déclenche **`rhn_check`** selon un intervalle de temps configurable
- Le **Client de configuration Red Hat Network** (**`rhncfg-client`**) qui exécute toutes les actions de configuration programmées depuis le Satellite.
- Le **Gestionnaire de configuration Red Hat Network** (**`rhncfg-manager`**) qui permet l'administration en ligne de commande des canaux de configuration Red Hat Network
- Le programme **`rhn_check`** qui se connecte au Satellite et effectue toutes les actions programmées depuis le serveur
- Toutes les fonctionnalités de niveau Management, comme le groupement de systèmes, la comparaison de profils de paquetages et l'utilisation du gestionnaire "System Set Manager" pour gérer plusieurs systèmes à la fois
- Une fonction Provisioning appelée *Commandes à distance* qui permet aux utilisateurs de programmer des commandes de niveau root sur des clients gérés via le site web du Satellite, si le client autorise cette action

2.1.1.4. Différences en fonctionalités

Les fonctionnalités Red Hat Network suivantes fonctionnent différemment dans un environnement UNIX :

- L'agent de configuration pour UNIX **Red Hat Update Agent for UNIX** offre un ensemble bien plus réduit d'options que son équivalent Linux et dépend de l'ensemble d'outils natifs du système d'exploitation pour l'installation de paquetages, au lieu de **`rpm`**. Consultez la Section 2.1.4.2.4, « Mise à jour depuis la ligne de commande » pour obtenir la liste précise d'options.
- L'application **Red Hat Network Push** a été modifiée de manière similaire pour télécharger les types de fichiers UNIX natifs, y compris les paquetages, les correctifs et les clusters de correctifs.

  Éant donné que les fichiers Solaris, de paquetages et de clusters de correctifs sont différents des fichiers rpm, le mécanisme pour le téléchargement de canaux est quelque peu différent. Il existe deux applications dans le paquetage **`rhnpush`** pour Solaris :

  - La première, **`solaris2mpm`**, est un utilitaire Red Hat Network qui crée un fichier MPM pour chaque paquetage ou correctif Solaris. Le format neutre du fichier MPM permet au Satellite de comprendre et gérer les fichiers téléchargés.
  - La seconde, **`rhnpush`**, a été étendue pour qu'elle puisse traiter les fichiers MOM aussi bien que les fichiers RPM. Autrement, elle fonctionne de la même manière que la version Linux de **`rhnpush`**.

- La catégorie **`Channels`** (canaux) du site web Red Hat Network a été élargie pour accueillir le stockage et l'installation de types de fichiers UNIX natifs.

2.1.1.5. Fonctions exclues

Les fonctionnalités Red Hat Network suivantes ne sont pas disponibles avec le système de support UNIX :

- Toutes les fonctionnalités de niveau Provisioning, comme le kickstart et le retour en arrière de paquetages, à l'exception de la gestion de fichiers de configuration
- Toutes les options sur les errata, vu que le concept de mises à jour d'errata n'est pas compris dans UNIX
- Fichiers source pour les paquetages

De plus, les fichiers *Answer* ne sont pas pris en charge. La prise en charge de tels fichiers est prévue pour une prochaine version.

IPV6 n'est pas pris en charge sur les systèmes Solaris.

De plus, le déplacement de fichiers **`RHAT*.pkg`** en cours d'installation n'est pas pris en charge.

2.1.2. Préparation/Configuration du serveur Satellite

Configurez le Satellite pour prendre en charge les clients UNIX avant que les fichiers requis soient disponibles pour le déploiement sur les systèmes clients.Vous pouvez le faire de deux manières, selon si vous avez déjà installé votre serveur Satellite :

1. Durant l'installation du Satellite :

   Activez le support UNIX sur le Satellite en sélectionnant la case "Enable Solaris Support" (activer le support Solaris) durant l'installation, comme dans la figure suivante :

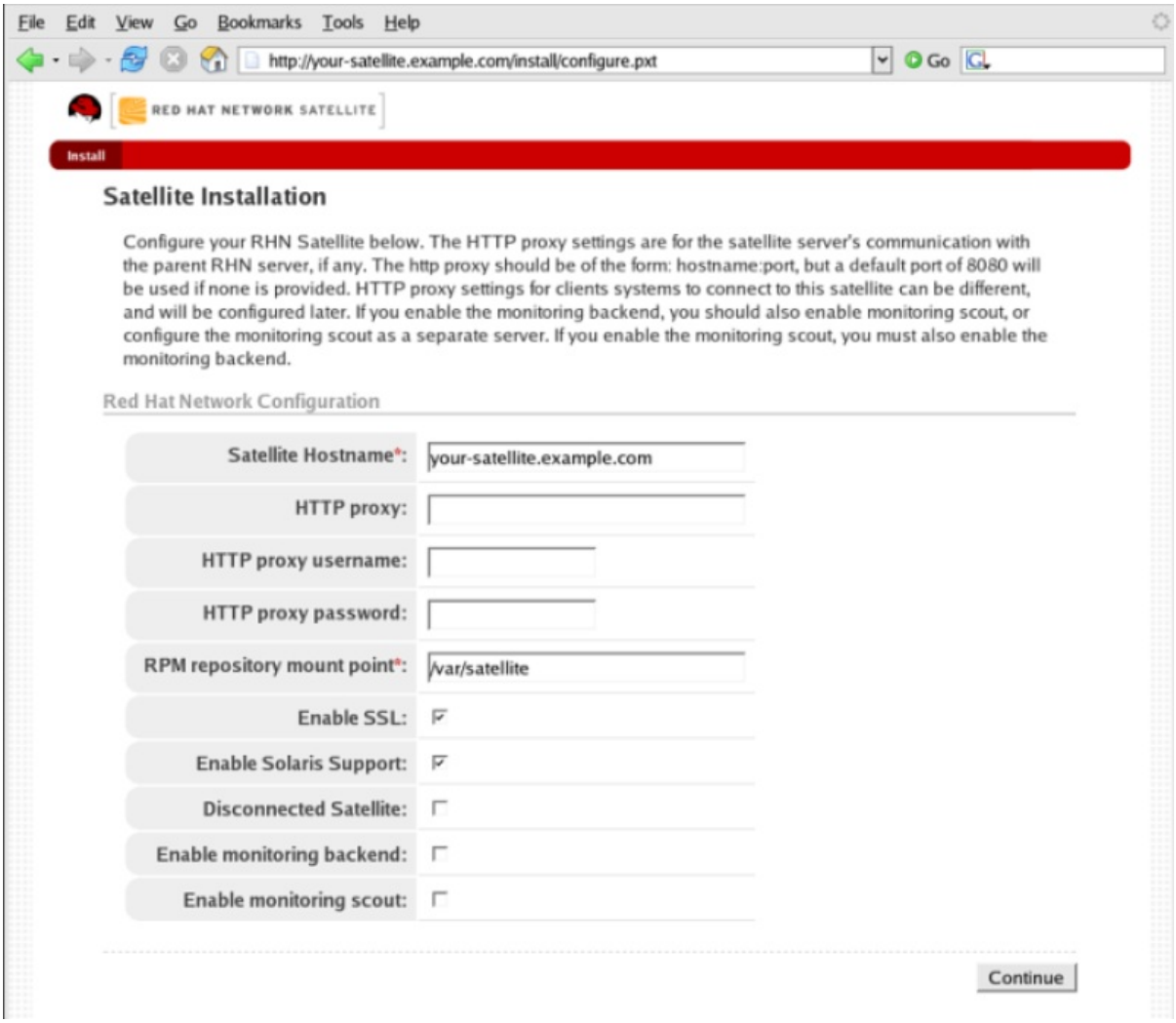


Figure 2.1. Activer le support UNIX durant l'installation du Satellite

2. Après l'installation du Satellite :

   Activez le support UNIX en configurant le Satellite après son installation. Pour ce faire, sélectionnez **Admin** dans la barre de menu du haut, puis sélectionnez **Configuration Satellite** dans la barre de navigation de gauche. Dans l'écran suivant, sélectionnez la case **`Activer le support Solaris`**, comme dans la figure suivante :

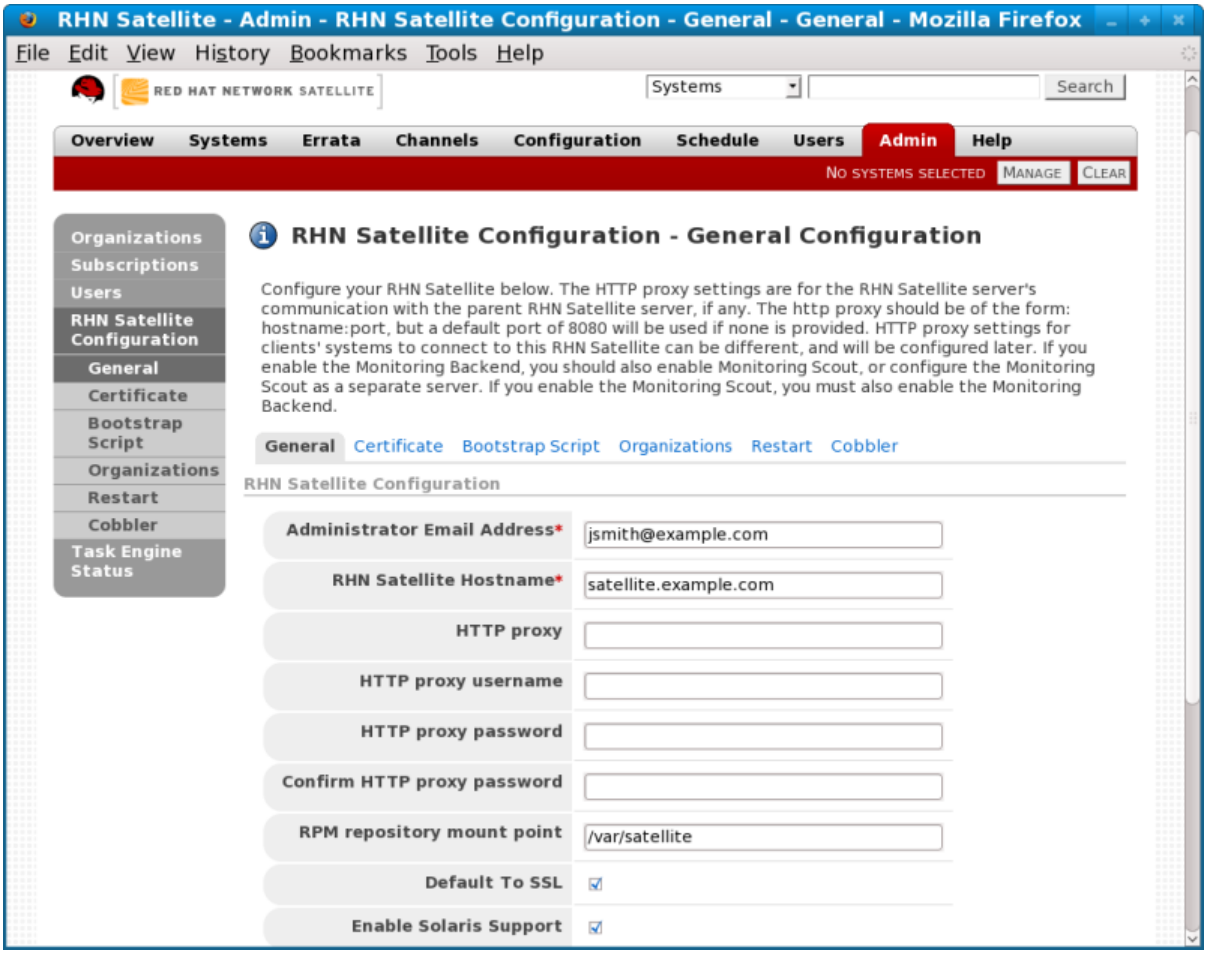


Figure 2.2. Activer le support UNIX après l'installation du Satellite

Cliquez sur le bouton **`Update Configuration`** (mettre à jour la configuration) pour enregistrer les modifications.

3. Finalement, créez un canal de base auquel vos systèmes clients peuvent s'abonner. Red Hat Network ne fournit pas de contenu UNIX, **`satellite-sync`** ne peut donc pas être utilisé pour créer le canal.

   Pour créer un canal Solaris, connectez-vous à l'interface web du Satellite en tant qu'administrateur Satellite ou autorité de certificat. Naviguez sur l'onglet **`Channel`** (Canal), suivi par **`Manage Software Channels`** (Gérer les canaux logiciels) sur la barre de navigation de gauche. Cliquez sur le lien **`create new channel`** (Créer un nouveau canal) en haut à droite de l'écran résultant. Fournissez un nom et une étiquette pour votre nouveau canal et sélectionnez l'architecture **`SPARC Solaris`** ou**`i386 Solaris`**, selon l'architecture du client.

2.1.3. Préparation de systèmes client Unix

Avant de pouvoir bénéficier de Red Hat Network, vos systèmes client basés sur UNIX doivent être préparés à la connexion :

1. Téléchargez et installez **`gzip`** ainsi que les bibliothèques tierces requises.

2. Téléchargez l'application Red Hat Network tarball à partir du Satellite vers le client et installez le contenu.

3. Vous devez ensuite déployer les certificats SSL requis pour une connexion sécurisée.

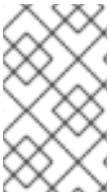
4. Configurez les applications client de façon à se connecter à Red Hat Satellite.

Une fois terminé, vos systèmes seront prêts à recevoir des mises à jour Red Hat Network. Les sections suivantes expliquent ces étapes en détails.

2.1.3.1. Télécharger et installer des paquetages supplémentaires

Cette section vous guide à travers les processus de téléchargement et d'installation d'applications tiers et d'applications Red Hat Network du Satellite au client UNIX.

L'agent **Red Hat Update Agent pour UNIX** (`up2date`) est d'une importance primordiale. Il fournit le lien entre vos systèmes client et Red Hat Network. La version spécifique à UNIX de **Red Hat Update Agent** est limitée en fonctionnalités par rapport à son équivalent pour Linux, mais permet quand même l'enregistrement de systèmes et facilite les installations et les mises à jour de paquetages. Consultez Section 2.1.4, « Enregistrement et mises à jour du client Unix » pour obtenir une description complète des options de l'outil.



NOTE

Il pourrait être utile d'entrer la commande **`bash`** lors d'une première connexion au client Solaris. Si le shell BASH est disponible, le comportement du système ressemblera à celui de Linux.

2.1.3.1.1. Installation de paquetages tiers

L'installation des applications Red Hat Network ne peut pas continuer à moins que les bibliothèques et utilitaires suivants soient présents :

- **`gzip`**
- **`libgcc`**
- **`openssl`**
- **`zlib`**

L'utilitaire **`gzip`** est fourni par le paquetage SUNW gzip et peut être téléchargé à partir de http://www.sunfreeware.com.

Sur les versions récentes de Solaris, les bibliothèques nécessaires sont fournies par les paquetages suivants installés nativement :

- **`SUNWgccruntime`**
- **`SUNWopenssl*`**
- **`SUNWzlib`**

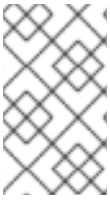
Pour des versions plus anciennes de Solaris, les paquetages suivants requis peuvent être téléchargés à partir de http://www.sunfreeware.com :

- **`SMClibgcc`** ou **`SMCgcc`**
- **`SMCossl`**

- **SMCzlib**

Pour vérifier si un paquetage est installé sur le client, utilisez la commande **pkginfo**. Par exemple, pour vérifier si un paquetage contient "zlib" dans le nom, exécutez la commande suivante :

```
# pkginfo | grep zlib
```



NOTE

Notez que les noms d'archives de paquetages Solaris sont différents des noms de paquetages installés. Par exemple, l'archive de paquetages **libgcc<version>-sol<solaris-version>-sparc-local.gz** devient SMClibgcc après l'installation

2.1.3.1.2. Configurer le chemin de recherche de bibliothèque

Afin de permettre au client Solaris d'utiliser les bibliothèques installées durant l'étape précédente, vous devez ajouter leur emplacement au chemin de recherche de bibliothèque. Pour ce faire, vérifiez d'abord le chemin de recherche de bibliothèque actuel :

```
# crle -c /var/ld/ld.config
```

Prenez note du chemin courant de la bibliothèque par défaut. Ensuite, modifiez le chemin pour inclure également les composants indiqués ci-dessous. Notez que l'option **-l** réinitialise la valeur plutôt que de la soumettre, ainsi, s'il y avait déjà des valeurs sur votre système, faites-les précéder par le paramètre -l.

Sur sparc :

```
 # crle -c /var/ld/ld.config -l
/other/existing/path:/lib:/usr/lib:/usr/local/lib
```

Sur x86 :

```
# crle -c /var/ld/ld.config -l
/other/existing/path:/lib:/usr/lib:/usr/local/lib:/usr/sfw/lib
```

2.1.3.1.3. Télécharger des paquetages client Red Hat Network

Téléchargez l'archive appropriée tarball de paquetages du répertoire **/var/www/html/pub/** de votre serveur Satellite. Si vous pouvez utiliser un navigateur web GUI tel que Mozilla, naviguez vers le répertoire **/pub** du Satellite et enregistrez l'archive tarball appropriée vers votre client :

```
http://your-satellite.example.com/pub/rhn-solaris-
bootstrap-<version>-<solaris-arch>-<solaris-version>.tar.gz
```

Si vous devez télécharger l'archive tarball à partir de la ligne de commande, il devrait être possible d'utiliser le **ftp** pour transférer le fichier du Satellite vers le client.

L'utilisation de **gzip** permet de décompresser l'archive tarball. Vous devriez avoir les paquetages suivants :

- **RHATpossl**

- **RHATrhnrcfg**
- **RHATrhnrcfga**
- **RHATrhnrcfgc**
- **RHATrhnrcfgm**
- **RHATrhnc**
- **RHATrhnl**
- **RHATrpush**
- **RHATsmart**

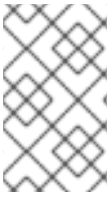
SMClibgcc et **SMCosslg** devraient aussi être inclus dans l'archive tarball.

2.1.3.1.4. Installer les paquetages Red Hat Network

Passez dans les répertoires extraits et utilisez l'outil d'installation natif de la variante UNIX pour ensuite installer chaque paquetage. Par exemple, sur les machines Solaris, utilisez la commande **pkgadd**. Répondez « yes » aux invites durant l'installation du paquetage.

Voici comment une installation typique devrait continuer :

```
# pkgadd -d RHATpossl-0.6-1.p24.6.pkg all
# pkgadd -d RHATpythn-2.4.1-2.rhn.4.sol9.pkg all
# pkgadd -d RHATrhnl-1.8-7.p23.pkg all
...
```



NOTE

Vous pouvez utiliser l'option **-n** de **pkgadd** pour exécuter la commande en mode non-interactif. Cependant, cela pourrait provoquer l'échec en silence de l'installation de certains paquetages sur Solaris 10.

Continuez jusqu'à ce que chaque paquetage soit installé dans le chemin spécifique à Red Hat Network : **/opt/redhat/rhn/solaris/**.

2.1.3.1.5. Inclure les paquetages Red Hat Network dans le chemin PATH

Afin que les paquetages Red Hat Network soient disponibles à chaque connexion, vous devriez les ajouter au chemin PATH. Pour ce faire, ajoutez ces commandes à votre script de connexion :

```
# PATH=$PATH:/opt/redhat/rhn/solaris/bin
# PATH=$PATH:/opt/redhat/rhn/solaris/usr/bin
# PATH=$PATH:/opt/redhat/rhn/solaris/usr/sbin
# export PATH
```

Pour activer l'accès aux pages man des commandes du client Red Hat Network, ajoutez-les au chemin MANPATH. Pour ce faire, ajoutez les commandes suivantes dans votre script de connexion :

```
# MANPATH=$MANPATH:/opt/redhat/rhn/solaris/man
# export MANPATH
```

Alternativement, vous pouvez aussi accéder aux pages de manuel avec la commande suivante :

```
# man -M /opt/redhat/rhn/solaris/man <man page>
```

Finalement, ajoutez les bibliothèques Red Hat à votre PATH comme vous l'avez fait avec **libgcc**, **openssl** et **zlib**.

```
crle -c /var/ld/ld.config -l <current library
paths>:/opt/redhat/rhn/solaris/lib
```

2.1.3.2. Déploiement de certificats SSL client

Pour assurer le transfert de données sécurisé, Red Hat recommande fortement d'utiliser SSL. Red Hat Satellite facilite l'implémentation de SSL en générant les certificats nécessaires durant son installation. Le certificat côté serveur est automatiquement installé sur le Satellite, alors que le certificat client est placé dans le répertoire **/pub/** du serveur web du Satellite.

Pour installer le certificat, suivez les étapes suivantes pour chaque client :

1. Téléchargez le certificat SSL depuis le répertoire **/var/www/html/pub/** de Red Hat Satellite sur le système client. Le certificat aura un nom similaire à **RHN-ORG-TRUSTED-SSL-CERT**. Il est accessible via le web à l'URL suivant :**https://your-satellite.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT**.

2. Déplacez le certificat SSL dans le répertoire spécifique à Red Hat Network pour votre variante UNIX. Pour Solaris, cette opération peut être accomplie avec une commande similaire à :

   ```
   mv /path/to/RHN-ORG-TRUSTED-SSL-CERT
   /opt/redhat/rhn/solaris/usr/share/rhn/
   ```

Une fois terminé, le nouveau certificat du client sera installé dans le répertoire approprié pour votre système UNIX. Si vous avez un nombre important de systèmes à préparer pour la gestion Red Hat Network, vous pouvez programmer ce processus entier dans un script.

Vous devez maintenant reconfigurer les applications client de Red Hat Network pour faire référence au certificat SSL nouvellement installé. Consultez la Section 2.1.3.3, « Configuration des clients » pour obtenir des instructions.

2.1.3.3. Configuration des clients

La dernière étape avant d'enregistrer vos systèmes client avec Red Hat Network est de reconfigurer leurs applications Red Hat Network de façon à utiliser le nouveau certificat SSL et obtenir des mises à jour de Red Hat Satellite. Ces changements peuvent être effectués en éditant le fichier de configuration de l'agent **Red Hat Update Agent**, qui fournit les fonctionnalités d'enregistrement et de mises à jour.

Suivez ces étapes sur chaque système client :

1. En tant que super-utilisateur, passez dans le répertoire de configuration de Red Hat Network pour le système. Pour Solaris, le chemin complet est **/opt/redhat/rhn/solaris/etc/sysconfig/rhn/**.

2. Ouvrez le fichier de configuration **up2date** dans un éditeur de texte.

3. Trouvez l'entrée ***serverURL*** et donnez-lui la valeur du nom de domaine complet (FQDN) de votre Red Hat Satellite :

```
serverURL[comment]=Remote server URL
serverURL=https://your-satellite.example.com/XMLRPC
```

4. Assurez-vous que l'application fait référence à Red Hat Satellite même lorsque SSL est désactivé en définissant également la valeur de ***noSSLServerURL*** sur le Satellite :

```
noSSLServerURL[comment]=Remote server URL without SSL
noSSLServerURL=http://your-satellite.example.com/XMLRPC
```

5. En gardant ouvert le fichier de configuration **up2date**, trouvez l'entrée ***sslCACert*** et donnez-lui la valeur du nom et de l'emplacement du certificat SSL comme décrit dans la Section 2.1.3.2, « Déploiement de certificats SSL client », par exemple :

```
sslCACert[comment]=The CA cert used to verify the ssl server
sslCACert=/opt/redhat/rhn/solaris/usr/share/rhn/RHN-ORG-TRUSTED-SSL-
CERT
```

Vos systèmes client sont maintenant prêts à l'enregistrement avec Red Hat Network et la gestion par votre Satellite.

2.1.4. Enregistrement et mises à jour du client Unix

Maintenant que vous avez installé des paquetages spécifiques à Red Hat Network, implémenté SSL et reconfiguré vos systèmes client de façon à se connecter à Red Hat Satellite, vous êtes prêt à commencer à enregistrer les systèmes et à obtenir des mises à jour.

2.1.4.1. Enregistrement de systèmes Unix

Cette section décrit le processus d'enregistrement à Red Hat Network pour les systèmes UNIX. Pour ce faire, vous devez utiliser **rhnreg_ks**. L'utilisation de clés d'activation pour enregistrer vos systèmes est optionnelle. Ces clés vous permettent de prédéterminer les paramètres au sein de Red Hat Network, comme les canaux de base et les groupes de systèmes, et de les appliquer automatiquement aux systèmes pendant leur enregistrement.

Comme la génération et l'utilisation de clés d'activation sont examinées en profondeur dans d'autres chapitres, cette section se concentre sur les différences lors de leur application aux variantes UNIX.

Pour enregistrer des systèmes UNIX avec Red Hat Satellite, veuillez effectuer les tâches suivantes dans cet ordre :

1. Connectez-vous à l'interface web du Satellite et cliquez sur l'onglet **Systems** dans la barre de navigation du haut, puis sur **Activation Keys** (clé d'activation) dans la barre de navigation de gauche. Cliquez ensuite sur le lien **create new key** (créer une nouvelle clé) en haut à droite de la page.

2. Sur la page suivante, sélectionnez le canal de base que vous avez créez à la fin de la Section 2.1.2, « Préparation/Configuration du serveur Satellite ».

3. Après la création de la clé, cliquez sur son nom dans la liste **Activation Keys** pour améliorer ses paramètres Red Hat Network en associant les canaux logiciels, de configuration et les groupes de systèmes.

4. Ouvrez un terminal sur le système client à enregistrer et devenez le super-utilisateur.

5. Utilisez **rhnreg_ks** avec l'option **--activationkey** pour enregistrer le client avec le Satellite. La chaîne de caractères de la clé, qui peut être directement copiée de la liste **Activation Keys** dans le site web. La commande devrait ressembler à l'exemple suivant :

```
rhnreg_ks --activationkey=b25fef0966659314ef9156786bd9f3af
```

6. Revenez sur le site web, cliquez sur le nom de la clé d'activation et assurez-vous que le nouveau système apparaît sous l'onglet **Activated Systems** (systèmes activés).

2.1.4.2. Mises à jour

Les mises à jour de paquetages dans UNIX sont traitées différemment comparé à Linux. Par exemple, Solaris dépend des clusters de correctifs (Clusters Patches) pour mettre à jour plusieurs paquetages à la fois, alors que les systèmes d'exploitation Red Hat utilisent les mises à jour d'errata (Errata Updates) pour associer les mises à niveau à des paquetages spécifiques. De plus, Solaris utilise des fichiers de réponses pour automatiser les installations interactives de paquetages, ce que Linux ne comprend pas, alors que Red Hat offre le concept de paquetages source. De ce fait, cette section cherche à souligner les différences dans l'utilisation des outils Red Hat Network sur les systèmes UNIX. (Remarque : Red Hat Network ne prend pas en charge les fichiers de réponses Solaris dans la version actuelle, cette prise en charge est prévue pour les prochaines versions).

Malgré les différences inhérentes, comme le manque d'errata, les interfaces de gestion de canaux et de paquetages dans le site web Red Hat Network sur le Satellite fonctionnent en majorité de la même manière pour les systèmes UNIX. Tous les canaux logiciels conçus pour servir les variantes UNIX peuvent être construits pratiquement de la même manière que les canaux personnalisés décrits dans le *Guide de démarrage Red Hat Satellite*. La différence la plus significative est l'architecture. Lors de la création d'un canal logiciel UNIX, assurez-vous de sélectionner l'architecture des canaux de base correspondante aux systèmes devant être servis.

Divisez vos paquetages en canaux de base et canaux enfants selon leur nature. Par exemple, sur Solaris, les paquetages d'installation devraient aller dans le canal de base Solaris, alors que les correctifs et les clusters de correctifs devraient aller dans un canal enfant du canal de base Solaris. Les paquetages d'installation supplémentaires peuvent aller dans un canal enfant « Extras » séparé.

Red Hat Network traite les correctifs de la même manière que les paquetages. Ils sont listés et installés de la même manière et avec la même interface que les paquetages normaux. Les correctifs sont numérotés par Solaris et auront des noms comme "patch-solaris-108434". La version d'un correctif Solaris est extraite des métadonnées Solaris originales et la publication est toujours 1.

Les clusters de correctifs sont des paquets de correctifs qui sont installés comme une unité. Red Hat Network conserve les informations de la dernière installation réussie d'un cluster de correctifs sur un système. Cependant, les clusters de correctifs ne sont pas suivis sur le client en tant qu'entités installées. Ils n'apparaissent donc pas dans la liste de paquetages ou de correctifs installés. Les noms de clusters de correctifs ressemblent à "patch-cluster-solaris-7_Recommended". La version est une chaîne de dates, comme "20040206", la publication est toujours 1 et l'époque est toujours 0.

2.1.4.2.1. Télécharger des paquetages vers le Satellite

Red Hat Network ne fournit pas de contenu UNIX ; tout paquetage Solaris, correctif ou cluster de

correctifs doit être téléchargé vers le Satellite sous un format pouvant être compris par un système client. Ce paquetage pourra ensuite être géré et distribué vers d'autres systèmes. Red Hat Network a créé **solaris2mpm** afin de traduire des paquetages Solaris, des correctifs, et des clusters de correctifs en un format que le Satellite peut comprendre.

2.1.4.2.1.1. solaris2mpm

Comme mentionné dans la Section 2.1.1.4, « Différences en fonctionalités », **solaris2mpm** fait partie de Red Hat Network Push pour Solaris. Le contenu qui est envoyé vers un canal Solaris sur le Satellite doit d'abord être sous le format .mpm.

Un fichier .mpm est une archive contenant une description des données du paquetage et le paquetage ou correctif lui-même. La commande solaris2mpm doit être exécutée sur le client, jamais sur le Satellite.

NOTE

solaris2mpm requiert de l'espace libre équivalent à trois fois la taille d'un des paquetages, correctifs ou cluster de correctifs qu'il convertit. Habituellement, l'espace dans **/tmp/** sera utilisé pour répondre à ce besoin. Cependant, l'option **--tempdir**vous permet de spécifier, si nécessaire, un autre répertoire.

Des multiples fichiers peuvent être spécifiés sur la ligne de commande de solaris2mpm. Ci-dessous, une exemple d'utilisation :

```
# solaris2mpm RHATrpush-3.1.5-21.pkg RHATrpush-3.1.5-23.pkg
Opening archive, this may take a while
Writing out RHATrpush-3.1.5-21.sparc-solaris.mpm
Opening archive, this may take a while
Writing out RHATrpush-3.1.5-23.sparc-solaris.mpm
```

Parce qu'aucun autre répertoire a été spécifié, les fichiers .mpm résultants sont écris dans le répertoire /tmp/. Remarquez que le nom des fichiers .mpm résultants inclut l'architecture du client sur lequel il a été créé. Dans ce cas, il s'agissait de SPARC Solaris. Le format général des noms de fichier mpm est :

```
name-version-release.arch.mpm
```

Les clusters de correctifs sont "élargis" - des fichiers .mpm sont générés pour chaque correctif dans le cluster, en plus d'un fichier .mpm "meta" de premier niveau contenant toutes les informations du cluster.

Ci-dessous figurent les options de solaris2mpm :

Tableau 2.2. options solaris2mpm

Option	Description
--version	Affiche le numéro de version du programme et quitte
-h, --help	Affiche cette information et quitte
-?, --usage	Imprime des informations sur l'utilisation d'un programme et quitte
--tempdir=<tempdir>	Répertoire temporaire à partir duquel travailler

Option	Description
--select-arch=<arch>	Sélectionne l'architecture (i386 ou SPARC) pour les paquetages qui en ont plusieurs.

2.1.4.2.1.2. rhnpush avec des fichiers .mpm

La version Solaris de **rhnpush** fonctionne de la même manière que l'utilitaire standard mais avec la possibilité supplémentaire de traiter des fichiers .mpm. Ci-dessous, un exemple d'utilisation.

```
% rhnpush -v --server testbox.example.com --username myuser -c solaris-8 \
RHATrpush-3.1.5-*.mpm
 Red Hat Network password:
 Connecting to http://testbox.example.com/APP
 Uploading package RHATrpush-3.1.5-21.sparc-solaris.mpm
 Uploading package RHATrpush-3.1.5-23.sparc-solaris.mpm
```

NOTE

Les fichiers .mpm du cluster de correctifs doivent être poussés de manière concurrente avec ou après, mais jamais avant, les fichiers .mpm pour les correctifs contenus dans ce cluster.

Utilisez solaris2mpm sur chacun des paquetages, correctifs ou clusters de correctifs que vous désirez gérer avec le Satellite. Ensuite, utilisez Red Hat Network Push pour les télécharger sur le canal qui leur a été créé.

2.1.4.2.2. Mise à jour via le site web

Pour installer des paquetages ou des correctifs sur un système individuel, cliquez sur le nom du système dans la catégorie **Systems**, sélectionnez les paquetages des listes "Upgrade" ou "Install" de l'onglet **Packages** ou l'onglet **Patches** et cliquez sur **Install/Upgrade Selected Packages** (installer / mettre à niveau les paquetages sélectionnés).

Pour exécuter une commande à distance tout en installant le paquetage, cliquez sur **Run Remote Command** au lieu de **Confirm**. Consultez la Section 2.1.5, « Commandes à distance » pour obtenir des instructions.

Pour installer des paquetages ou des correctifs sur plusieurs systèmes à la fois, sélectionnez les systèmes et cliquez sur **System Set Manager** dans la barre de navigation de gauche. Puis, dans l'onglet **Packages**, sélectionnez les paquetages des listes "Upgrade" ou "Install" et cliquez sur **Install/Upgrade Packages**. Pour terminer l'action, programmez les mises à jour.

2.1.4.2.3. rhnsd

Sur les systèmes Red Hat Enterprise Linux, le démon **rhnsd**, qui instruit le système client de s'enregistrer avec Red Hat Network, est lancé automatiquement lors du démarrage. Sur les systèmes Solaris, **rhnsd** *n'est pas* lancé par défaut lors du démarrage. Il peut être lancé à partir d'une ligne de commande de cette manière :

```
rhnsd --foreground --interval=240
```

L'emplacement par défaut pour **rhnsd** est **/opt/redhat/rhn/solaris/usr/sbin/rhnsd**. Voici les options disponibles pour **rhnsd** sur Solaris :

Tableau 2.3. Options rhnsd

Option	Description
-f, --foreground	Démarre en avant-plan
-i, --interval=MINS	Se connecte à Red Hat Network toutes les MINS minutes
-v, --verbose	Journalise toutes les actions dans syslog
-h, --help	Donne cette liste d'aide
-u, --usage	Donne cette liste d'aide
-V, --version	Imprime la version du programme

2.1.4.2.4. Mise à jour depuis la ligne de commande

Comme le site web, l'utilisation de l'agent **Red Hat Update Agent** en ligne de commande est affectée par les limites de la gestion de paquetages UNIX. Ceci dit, la plupart des fonctions essentielles peuvent toujours être effectuées via la commande **up2date**. La différence la plus importante est l'absence de toutes les options sur les fichiers source. Consultez le Tableau 2.4, « Arguments de l'agent de mise à jour en ligne de commande » pour une liste précise d'options disponibles aux systèmes UNIX.

La version en ligne de commande de l'agent **Red Hat Update Agent** accepte les arguments suivants sur les systèmes UNIX :

Tableau 2.4. Arguments de l'agent de mise à jour en ligne de commande

Argument	Description
--version	Affiche les informations de version du programme.
-h, **--help**	Affiche ce message d'aide et quitte.
-v, **--verbose**	Affiche des sorties supplémentaires.
-l, **--list**	Liste les dernières versions de tous les paquetages installés.
-p, **--packages**	Met à jour les paquetages associés à ce profil de système.
--hardware	Mettre à jour le profil matériel de ce système sur Red Hat Network.
--showall	Liste tous les paquetages disponibles à télécharger.

Argument	Description
--show-available	Liste tous les paquetages disponibles qui ne sont pas couramment installés.
--show-orphans	Liste tous les paquetages couramment installés qui ne sont pas dans les canaux auxquels le système est abonné.
--show-channels	Affiche les noms de canaux avec les noms de paquetages, dans les cas appropriés.
--installall	Installe tous les paquetages disponibles. Utilisez avec **--channel**.
--channel=*CHANNEL*	Spécifie les canaux à partir desquels mettre à jour à l'aide d'étiquettes de canaux.
--get	Trouve le paquetage spécifié sans résoudre les dépendances.

2.1.5. Commandes à distance

Avec le support UNIX, Red Hat Network offre la flexibilité d'exécuter des commandes à distance sur les systèmes client par le site web du Satellite. Cette fonction vous permet d'exécuter pratiquement toute application ou tout script (compatible) sur tout système de votre domaine sans jamais avoir à ouvrir un terminal.

2.1.5.1. Activation de commandes

Avec la flexibilité offerte par cet outil, existe également un risque important et la responsabilité de mitiger ce risque. Pour toutes les situations pratiques, cette fonction donne une invite BASH root à tout personne qui possède un accès administratif au système sur le site web.

Ceci peut cependant être contrôlé par le même mécanisme activé lors de la configuration utilisé pour déterminer les systèmes qui peuvent avoir leurs fichiers de configuration gérés par Red Hat Network.

En bref, vous devez créer un répertoire et un fichier sur le système UNIX qui indique à Red Hat Network qu'il est acceptable d'exécuter des commandes à distance sur la machine. Le répertoire doit s'appeler **script**, le fichier **run** et les deux doivent se trouver dans le répertoire **/etc/sysconfig/rhn/allowed-actions/** spécifique à votre variante UNIX.

Par exemple, dans Solaris, exécutez cette commande pour créer le répertoire :

```
mkdir -p /opt/redhat/rhn/solaris/etc/sysconfig/rhn/allowed-actions/script
```

Pour créer le fichier requis dans Solaris, exécutez la commande suivante :

```
touch /opt/redhat/rhn/solaris/etc/sysconfig/rhn/allowed-
actions/script/run
```

2.1.5.2. Exécution de commandes

Vous pouvez programmer une commande à distance de différentes manières : sur un système individuel, sur plusieurs systèmes à la fois et pour accompagner une action de paquetages.

Pour exécuter une commande à distance sur un système individuel, ouvrez la page **System Details**(Détails du système) et cliquez sur le sous-onglet **Remote Command** (commande à distance). (Remarquez que cet onglet apparaît seulement si le système a un droit d'accès d'approvisionnement) Sur cette page, veuillez établir les paramètres de cette commande. Vous pouvez identifier un utilisateur, un groupe et un délai d'attente spécifiques, ainsi que le script même. Sélectionnez une date et une heure pour commencer à essayer la commande et cliquez sur le lien **Schedule Remote Command** (programmer la commande à distance).

De manière similaire, vous pouvez exécuter une commande à distance sur plusieurs systèmes à la fois à l'aide de **System Set Manager**. Sélectionnez les systèmes, rendez-vous sur **System Set Manager**, cliquez sur l'onglet **Provisioning** (approvisionnement) et descendez jusqu'à la section **Remote Command** (Commande à distance). À ce niveau, vous pouvez exécuter une commande à distance sur tous les systèmes sélectionnés à la fois.

Pour exécuter une commande à distance avec une action de paquetages, programmez l'action sous l'onglet **Packages** de la page **System Details** et cliquez sur **Run Remote Command** (exécuter) tout en confirmant l'action. Utilisez les boutons radio en haut pour déterminer si la commande devrait être exécutée avant ou après l'action de paquetages, définissez les paramètres de la commande et cliquez sur **Schedule Package Install/Upgrade** (programmer l'installation / la mise à niveau de paquetages).

Notez que l'installation de plusieurs paquetages qui ont différentes commandes à distance, nécessite la programmation séparée des installations ou la combinaison des commandes dans un seul script.

CHAPITRE 3. INFORMATIONS RED HAT SATELLITE PROXY

Cette section concerne l'utilisation du proxy Red Hat Satellite Proxy avec le gestionnaire Red Hat Network Package Manager.

3.1. UTILISER LE GESTIONNAIRE DE PAQUETAGES RED HAT NETWORK PACKAGE MANAGER ET SERVIR LES PAQUETAGES LOCAUX VIA RED HAT NETWORK PROXY

Red Hat Network Package Manager est un outil de ligne de commande permettant à une organisation de servir des paquetages locaux associés à un canal Red Hat Network privé à travers le serveur Red Hat Network Proxy Server. Pour uniquement mettre à jour les paquetages Red Hat officiels pour le serveur Red Hat Network Proxy Server, veuillez ne pas installer le gestionnaire Red Hat Network Package Manager.

Pour utiliser le gestionnaire Red Hat Network Package Manager, installez le paquetage **`spacewalk-proxy-package-manager`** et ses dépendances.

Seules les informations d'en-tête pour les paquetages sont téléchargées vers les serveurs Red Hat Network. Les en-têtes sont requis afin que Red Hat Network puisse résoudre les dépendances de paquetages pour les systèmes client. Les fichiers de paquetages (**`*.rpm`**) sont stockés sur Red Hat Network Proxy Server.

Le gestionnaire Red Hat Network Package Manager utilise les mêmes paramètres que le Proxy, définis dans le fichier de configuration **`/etc/rhn/rhn.conf`**.

Voici un résumé de toutes les options en ligne de commande de Red Hat Network Package Manager **`rhn_package_manager`**:

Tableau 3.1. options de `rhn_package_manager`

Option	Description
`-v`, **`--verbose`**	Augmenter les commentaires.
`-d`*DIR*, **`--dir=`***DIR*	Traiter les paquetages du répertoire *DIR*.
`-c`*CHANNEL*, **`--channel=`***CHANNEL*	Gérer ce canal - peut être présent plusieurs fois.
`-n`*NUMBER*, **`--count=`***NUMBER*	Traite ce nombre d'en-têtes par appel - la valeur par défaut est 32.
`-l`, **`--list`**	Lister chaque nom de paquetage, numéro de version, numéro de publication et architecture dans le ou les canaux spécifiés.
`-s`, **`--sync`**	Vérifier si le répertoire local est en synchronisation avec le serveur.
`-p`, **`--printconf`**	Imprime la configuration courante et quitte.

Option	Description
-X*PATTERN*, **--exclude=***PATTERN*	Exclure les fichiers correspondant à cette expression globale - peut être présent plusieurs fois.
--newest	Pousser uniquement les paquetages qui sont plus récents que les paquetages déjà poussés sur le serveur pour le canal spécifié.
--stdin	Lire les noms de paquetages depuis stdin.
--nosig	Envoyer les paquetages non signés. Par défaut, Red Hat Network Package Manager essaie uniquement d'envoyer les paquetages signés.
--username=*USERNAME*	Spécifier votre nom d'utilisateur Red Hat Network. Si vous ne fournissez pas un nom avec cette option, le système vous le demandera.
--password=*PASSWORD*	Spécifier votre mot de passe Red Hat Network. Si vous n'en fournissez pas un avec cette option, le système vous le demandera.
--source	Télécharger les en-têtes de paquetages sources.
--dontcopy	Dans l'étape avant le téléchargement, ne pas copier les paquetages dans leur emplacement final dans l'arborescence de paquetages.
--test	Uniquement imprimer les paquetages à pousser.
--no-ssl	*Non recommandé* - Désactiver SSL.
-?, **--usage**	Décrire brièvement les options.
--copyonly	Copier le fichier listé dans l'argument dans le canal spécifié. Cette option est utile lorsqu'un paquetage manque à un canal sur le proxy et que vous ne souhaitez pas réimporter tous les paquetages dans le canal. Par exemple, **rhn_package_manager -c***CANAL* **--copyonly** */CHEMIN/AU/FICHIER/MANQUANT*
-h, **--help**	Affiche l'écran d'aide avec une liste d'options.

NOTE

Ces options en ligne de commande sont également décrites dans la page man de **rhn_package_manager** : **man rhn_package_manager**.

Pour que Red Hat Network Package Manager puisse servir les paquetages locaux, les étapes suivantes doivent être observées :

1. Créer un canal privé.
2. Télécharger les paquetages locaux dans le canal.

Les étapes seront traitées en détails dans les prochaines sections.

3.1.1. Créer un canal privé

Avant que les paquetages locaux puissent être fournis via Red Hat Network Proxy Server, un canal privé est nécessaire pour les stocker. Effectuez les étapes suivantes pour créer un canal privé :

1. Connectez-vous sur l'interface web Red Hat Network à l'adresse https://rhn.redhat.com ou au serveur Red Hat Satellite du réseau.
2. Cliquez sur **Canaux** dans la barre de navigation supérieure. Si l'option **Gérer les canaux** n'est pas présente dans la barre de navigation de gauche, assurez-vous que cet utilisateur possède les permissions d'édition de canaux. Pour ce faire, utilisez la catégorie **Utilisateurs** accessible via la barre de navigation supérieure.
3. Dans la barre de navigation de gauche, cliquez sur **Gérer les canaux logiciels**, puis sur le bouton **créer un nouveau canal** en haut à droite de la page.
4. Sélectionnez une architecture de canal parent et canal de base, puis saisissez un nom, une étiquette, un résumé et une description pour le nouveau canal privé. L'étiquette de canal doit: avoir au moins six caractères, commencer par une lettre et contenir uniquement des lettres en minuscules, des chiffres, des tirets (-) et des points (.). Saisissez également l'URL de la clé GPG du canal. Bien que ce champ ne soit pas requis, il est recommandé pour améliorer la sécurité. Pour obtenir des instructions sur la génération de clés GPG, reportez-vous au *Guide de gestion des canaux Red Hat Network*.
5. Cliquez sur **Créer un canal**.

3.1.2. Télécharger des paquetages

NOTE

Vous devez être un administrateur d'organisations pour télécharger des paquetages vers des canaux Red Hat Network privés. Le script vous invitera à saisir votre nom d'utilisateur et votre mot de passe Red Hat Network.

Après avoir créé le canal privé, téléchargez les en-têtes de paquetages pour les RPM source et binaires vers le serveur Red Hat Network et copiez les paquetages sur le serveur Red Hat Network Broker. Pour télécharger les en-têtes de paquetages pour les RPM binaires, veuillez saisir la commande suivante :

```
rhn_package_manager -c "label_of_private_channel" pkg-list
```

Cette commande téléchargera l'en-tête du paquetage sur le nom de canal spécifié et le paquetage sur **/var/spool/rhn-proxy/rhn**.

pkg-list est la liste de paquetages à télécharger. Alternativement, utilisez l'option **-d** pour spécifier le répertoire local qui contient les paquetages à ajouter au canal. Assurez-vous que le répertoire ne

contienne uniquement les paquetages à inclure et aucun autre fichier. Red Hat Network Package Manager peut également lire la liste de paquetages de l'entrée standard (à l'aide de **--stdin**).

Pour télécharger les en-têtes de paquetages pour les RPM source:

```
rhn_package_manager -c "label_of_private_channel" --source pkg-list
```

Si vous avez plusieurs canaux spécifiés (à l'aide de **-c** ou **--channel**), les en-têtes de paquetages téléchargés seront liés à tous les canaux listés.

NOTE

Si un nom de canal n'est pas spécifié, les paquetages ne sont ajoutés à aucun canal. Les paquetages peuvent alors être ajoutés à un canal à l'aide de l'interface web de Red Hat Network. L'interface peut également être utilisée pour modifier les canaux privés existants.

Après avoir téléchargé les paquetages, vous pouvez immédiatement vérifier l'interface web Red Hat Network pour vérifier leur présence. Cliquez sur **Canaux** dans la barre de navigation supérieure, **Gérer les canaux logiciels** dans la barre de navigation de gauche, puis sur le nom du canal personnalisé. Cliquez ensuite sur l'onglet **Paquetages**. Chaque RPM devrait être répertorié.

Vous pouvez également vérifier si le répertoire local est en synchronisation avec l'image des canaux du serveur Red Hat Network sur la ligne de commande :

```
rhn_package_manager -s -c "label_of_private_channel"
```

L'option **-s** va répertorier tous les paquetages manquants (paquetages téléchargés sur le serveur Red Hat Network qui ne sont pas présents dans le répertoire local). Vous devez être un administrateur d'organisations pour pouvoir utiliser cette commande. Le script vous demandera votre nom d'utilisateur et votre mot de passe Red Hat Network.

Si vous utilisez Red Hat Network Package Manager pour mettre à jour les paquetages locaux, vous devez vous rendre sur le site web Red Hat Network pour abonner le système au canal privé.

CHAPITRE 4. GESTION DE PAQUETAGES PERSONNALISÉS

Ce chapitre offre un aperçu sur la manière de créer des paquetages pour une livraison réussie via Red Hat Network. Parmi les sujets étudiés figurent pourquoi RPM devrait être utilisé, comment construire des paquetages pour Red Hat Network, et comment signer correctement des paquetages.

4.1. CONSTRUCTION DE PAQUETAGES POUR RED HAT NETWORK

Red Hat Network utilise la technologie du *Gestionnaire de paquetages RPM* (RPM, de l'anglais RPM Package Manager) pour déterminer les ajouts et les mises à jour de logiciels applicables à chaque système client. Les paquetages récupérés de Red Hat Network sont normalement sous le format RPM. Les images ISO entières sont cependant disponibles via l'onglet **Logiciels** du site web de Red Hat Network, mais elles ne sont pas disponibles dans les installations Red Hat Satellite. Si la prise en charge de Solaris est activée sur le serveur Satellite, vous pouvez utiliser l'outil Red Hat Network Push pour télécharger les paquetages Solaris vers les canaux personnalisés utilisés par les clients Solaris.

RPM est un outil qui offre aux utilisateurs une méthode simple pour installer, désinstaller, mettre à niveau et vérifier les paquetages logiciels. Il permet également aux développeurs de logiciels de mettre en paquetages le code source et les versions compilées d'un programme pour les utilisateurs et les développeurs.

4.1.1. Bénéfices de RPM

RPM offre les avantages suivants :

Mises à niveau faciles

À l'aide de RPM, vous mettez à niveau les composants individuels d'un système sans une réinstallation entière. Lorsque Red Hat publie une nouvelle version de Red Hat Enterprise Linux, les utilisateurs n'ont pas à effectuer une réinstallation pour mettre à niveau leur système. RPM permet des mises à niveau sur place, intelligentes et entièrement automatisées de votre système. Les fichiers de configuration dans les paquetages sont conservés afin que les utilisateurs ne perdent pas leurs personnalisations. Il n'existe pas de fichier spécial de mise à niveau nécessaire pour mettre à jour un paquetage vu que le même fichier RPM est utilisé pour installer et mettre à niveau le paquetage.

Interrogation de paquetages

RPM fournit des options d'interrogation qui vous permettent de rechercher dans votre base de données RPM tous les paquetages ou seulement certains fichiers. Vous pouvez également facilement trouver à quel paquetage appartient un fichier et d'où provient le paquetage. Les fichiers contenus dans le paquetage se trouvent dans une archive compressée, avec un en-tête binaire personnalisé contenant les informations utiles sur le paquetage et son contenu. RPM interroge les en-têtes d'une manière rapide et facile.

Vérification du système

Une autre fonctionnalité est la possibilité de vérifier les paquetages. Si vous pensez qu'un fichier associé à un paquetage a été supprimé, vous pouvez vérifier le paquetage pour voir le statut des fichiers qu'il fournit. La vérification vous avertit de toute anomalie. Si des erreurs existent, les fichiers peuvent facilement être réinstallés. Les fichiers de configuration modifiés sont conservés pendant la réinstallation.

Sources pristines

Un objectif crucial de la conception de RPM est de permettre l'utilisation de sources de logiciels *pristines*, comme elles sont distribuées par les auteurs des logiciels. Avec RPM, ces sources peuvent

être mises en paquetages avec tout correctif qui était utilisé, plus des instructions complètes de création. Ceci est un avantage important pour plusieurs raisons. Par exemple, si une nouvelle version d'un programme est publiée, vous n'avez pas forcément à recommencer à zéro pour qu'il compile. Vous pouvez examiner le correctif pour voir ce que vous *pourriez* avoir à faire. Toutes les valeurs par défaut compilées et les changements apportés pour faire en sorte que le logiciel soit créé correctement, sont facilement visibles en utilisant cette technique.

Garder les sources pristines peut sembler important uniquement aux développeurs, mais le résultat est un logiciel de qualité supérieure pour les utilisateurs également.

4.1.2. Directives Red Hat Network RPM

La force de RPM repose dans sa capacité de définir les dépendances et d'identifier des conflits correctement. Red Hat Network dépend de cet aspect de RPM. Red Hat Network offre un environnement automatisé, ce qui signifie qu'aucune intervention manuelle ne peut prendre place durant l'installation d'un paquetage. Ainsi, lors de la création de RPM pour la distribution via Red Hat Network, il est impératif de suivre les règles suivantes :

1. Apprendre RPM. Il est crucial de posséder une compréhension profonde des fonctions importantes de RPM pour construire correctement des paquetages. Pour obtenir davantage d'informations sur RPM, commencez par les ressources suivantes :

   - http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html
   - http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/Packagers_Guide/index.html
   - http://www.gurulabs.com/GURULABS-RPM-LAB/GURULABS-RPM-GUIDE-v1.0.PDF

2. Lors de la construction d'un RPM enfant pour un canal enfant, créez le paquetage sur une installation fraîche de Red Hat Enterprise Linux de la même version que le canal de base de l'enfant. Assurez-vous d'appliquer tout d'abord toutes les mises à jour de Red Hat Network.

3. Le paquetage RPM doit être installé sans l'utilisation des options **`--force`** ou **`--nodeps`**. Si vous ne pouvez pas installer un RPM proprement sur votre système construit, Red Hat Network ne peut pas l'installer automatiquement sur un système.

4. Le nom de fichier du paquetage RPM doit être sous le format NVR (nom, version, publication) et doit contenir l'architecture pour le paquetage. Le format correct est ***`nom-version-publication.arch`*****`.rpm`**. Par exemple, le nom de fichier d'un paquetage RPM valide est **`nompqtg-0.84-1.i386.rpm`**, où le nom est *nompqtg*, la version est *0.84*, la publication est *1* et l'architecture est *i386*.

5. Le paquetage RPM devrait être signé par le mainteneur du paquetage. Les paquetages non signés peuvent être distribués via Red Hat Network, mais **yum** doit être forcé à les accepter. Signer les paquetages est fortement recommandé et est examiné dans la Section 4.2, « Signatures numériques pour paquetages Red Hat Network ».

6. Si le paquetage est modifié d'une manière ou d'une autre, y compris changer la signature ou recompiler, la version ou la publication doit être augmentée de manière incrémentielle. En d'autres termes, le NVRA (y compris l'architecture) pour chaque RPM distribué via Red Hat Network doit correspondre à une construction unique pour éviter toute ambiguïté.

7. Un paquetage RPM ne peut pas se rendre obsolète.

8. Si un paquetage est divisé en paquetages séparés, faites extrêmement attention aux dépendances. Ne divisez pas un paquetage existant à moins d'avoir une très bonne raison de le faire.

9. Aucun paquetage ne peut dépendre de scripts interactifs avant l'installation, après l'installation, avant la désinstallation ou après la désinstallation. Si le paquetage requiert une intervention directe de l'utilisateur durant l'installation, il ne peut pas fonctionner avec Red Hat Network.

10. Tout script avant l'installation, après l'installation, avant la désinstallation et après la désinstallation ne devrait jamais écrire quoi que ce soit sur stderr ou stdout. Redirigez les messages dans **/dev/null** s'ils ne sont pas nécessaires. Sinon, écrivez les dans un fichier.

11. Lors de la création du fichier de spécification, utilisez les définitions de groupes de **/usr/share/doc/rpm-<*version*>/GROUPS**. Si vous ne trouvez pas de correspondance exacte, sélectionnez la meilleure possible.

12. Utilisez la fonction de dépendances RPM pour assurer que le programme soit exécuté après son installation.

IMPORTANT

Ne créez pas un RPM en archivant les fichiers, puis en les désarchivant dans le script après l'installation. Cette action écrase l'objectif de RPM.

Si les fichiers de l'archive ne sont pas inclus dans la liste de fichiers, ils ne peuvent pas être vérifiés ou examinés contre tout conflit. Dans la plupart des cas, RPM peut tout même empaqueter ou dés-empaqueter des archives d'une manière très efficace. Par exemple, ne créez pas de fichiers dans une section %post qui ne peut pas ou ne sera pas nettoyée dans une section %postun.

4.2. SIGNATURES NUMÉRIQUES POUR PAQUETAGES RED HAT NETWORK

Tous les paquetages distribués via Red Hat Network devraient avoir une *signature numérique*. Une signature numérique est créée avec une clé privée unique et peut être vérifiée avec la clé publique correspondante. Après la création d'un paquetage, le RPM source (SRPM) et le RPM peuvent être signés numériquement avec une clé GnuPG. Avant l'installation du paquetage, la clé publique est utilisée pour vérifier que le paquetage a été signé par un tiers de confiance et que le paquetage n'a pas changé depuis sa signature.

4.2.1. Génération d'une paire de clés GnuPG

Une paire de clés GnuPG consiste en une clé privée et une clé publique. Pour générer une paire de clés :

1. Veuillez saisir la commande suivante en tant qu'utilisateur root sur l'invite shell :

```
gpg --gen-key
```

Les paires de clés GPG ne doivent pas être créées par des utilisateurs qui ne sont pas des super-utilisateurs. Le super-utilisateur peut bloquer les pages de mémoire, ce qui signifie que les informations ne seront jamais écrites sur disque, contrairement aux utilisateurs qui sont pas des super-utilisateurs.

2. Après avoir exécuté la commande pour générer la paire de clés, vous verrez un écran de présentation contenant les options de clés similaire à l'exemple suivant :

```
gpg (GnuPG) 2.0.14; Copyright (C) 2009 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection?
```

3. Choisissez l'option : (2) DSA and ElGamal. Cette option vous permet de créer une signature numérique et de chiffrer/déchiffrer avec deux types de technologies. Saisissez **2**, puis appuyez sur **Entrée**.

4. Ensuite, choisissez la taille de la clé, qui est la longueur de la clé. Plus la clé est longue, plus vos messages seront résistants contre les attaques. Créer une clé d'au moins 2048 octets est recommandée.

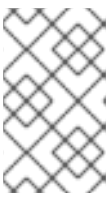
5. L'option suivante vous demande de spécifier combien de temps vous souhaitez que votre clé soit valide. Si vous choisissez une date d'expiration, souvenez-vous que toute personne qui utilise votre clé publique doit également être informée de son expiration et donnée une nouvelle clé publique. Il est recommandé de ne pas sélectionner de date d'expiration. Si vous ne choisissez pas de date, le système vous demandera de confirmer votre décision :

```
Key does not expire at all Is this correct (y/n)?
```

6. Appuyez sur **y** pour confirmer votre décision.

7. Votre prochaine tâche est de fournir un ID utilisateur contenant votre nom, votre adresse électronique et un commentaire facultatif. Chaque valeur est demandée individuellement. Lorsque vous avez terminé, le système vous présentera un résumé des informations que vous avez saisies.

8. Une fois que vous acceptez vos choix, vous saisirez une phrase-mot de passe.



NOTE

Tout comme vos mots de passe de compte, une bonne phrase-mot de passe est essentielle pour une sécurité optimale dans GnuPG. Mélangez les lettres majuscules et minuscules et/ou incluez des ponctuations.

9. Une fois que vous saisissez et vérifiez votre phrase-mot de passe, vos clés sont générées. Un message similaire à l'exemple suivant sera affiché :

```
We need to generate a lot of random bytes. It is a good idea to
perform some
other action (type on the keyboard, move the mouse, utilize the
disks)
during the prime generation; this gives the random number generator
```

```
a
better chance to gain enough entropy.

+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++ +++.
++++++++++++++++++++++++++++++++++.........................++++
```

Lorsque l'activité sur l'écran cesse, vos nouvelles clés sont placées dans le répertoire **.gnupg**, situé dans le répertoire de base root. Ceci est l'emplacement par défaut des clés générées par l'utilisateur root.

Pour répertorier les clés root, utilisez la commande :

```
gpg --list-keys
```

La sortie est similaire à l'exemple suivant :

```
gpg: key D97D1329 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   3  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 3u
gpg: next trustdb check due at 2013-08-28
pub   2048D/D97D1329 2013-08-27 [expires: 2013-08-28]
      Key fingerprint = 29C7 2D2A 5F9B 7FF7 6411  A9E7 DE3E 5D0F D97D 1329
uid                  Your Name<you@example.com>
sub   2048g/0BE0820D 2013-08-27 [expires: 2013-08-28]
```

Pour obtenir votre clé publique, utilisez la commande suivante :

```
gpg --export -a 'Your Name' > public_key.txt
```

Votre clé publique est écrite dans le fichier **public_key.txt**.

Cette clé publique est assez importante. Elle est la clé qui doit être déployée sur tous les systèmes client qui reçoivent les logiciels clients via **yum**. Les techniques pour déployer cette clé dans une organisation sont examinées dans le *Guide de configuration du client Red Hat Network*.

4.2.2. Signer des paquetages

Avant de pouvoir signer des paquetages, vous devez configurer votre fichier **~/.rpmmacros** de façon à inclure les éléments suivants :

```
%_signature gpg
%_gpg_name B7085C8A
```

Remplacez la valeur d'ID de clé **_gpg_name** *B7085C8A* par l'ID de clé de votre porte-clés GPG que vous utilisez pour signer les paquetages. Cette valeur indique à **RPM** quelle signature utiliser.

Pour signer le paquetage *package-name-1.0-1.noarch.rpm*, utilisez la commande suivante :

```
rpm --resign package-name-1.0-1.noarch.rpm
```

Saisissez votre phrase-mot de passe. Pour assurer que le paquetage est signé, utilisez la commande suivante :

```
rpm --checksig -v package-name-1.0-1.noarch.rpm
```

NOTE

Avant d'exécuter la commande **rpm --checksig -v**, importez la clé GPG. Consultez la Section 4.3, « Import de clés GPG personnalisées » dans la section suivante pour obtenir davantage d'informations.

Vous devriez voir la phrase « Good signature from "*Your Name*" » dans la sortie, où *Your Name* est remplacé par le nom associé à la clé de signature.

4.3. IMPORT DE CLÉS GPG PERSONNALISÉES

Pour les clients qui prévoient de construire et de distribuer leurs propres RPM de manière sécurisée, il est fortement recommandé que tous les RPM personnalisés soient signés à l'aide de GPG (GNU Privacy Guard). La génération de clés GPG et la construction de paquetages signés GPG sont examinées dans le Section 4.2.1, « Génération d'une paire de clés GnuPG ».

Une fois les paquetages signés, la clé publique doit être déployée sur tous les systèmes qui importent ces RPM. Cette tâche a deux étapes : créez tout d'abord un emplacement central pour la clé publique afin que les clients puissent l'obtenir, et ajoutez ensuite la clé au porte-clés GPG local pour chaque système.

La première étape est commune et peut être effectuée en utilisant l'approche du site web recommandée pour le déploiement d'applications client Red Hat Network. Pour ce faire, créez un répertoire public sur le serveur Web et placez-y la signature GPG publique :

```
cp /some/path/YOUR-RPM-GPG-KEY /var/www/html/pub/
```

La clé peut être téléchargée par les systèmes client à l'aide de **Wget** :

```
wget -O- -q http://your_proxy_or_sat.your_domain.com/pub/YOUR-RPM-GPG-KEY
```

L'option **-O-** envoie les résultats vers la sortie standard alors que l'option **-q** configure l'exécution de **Wget** en mode quiet (sortie désactivée). Souvenez-vous de remplacer la variable *YOUR-RPM-GPG-KEY* par le nom de fichier de votre clé.

Une fois que la clé est disponible sur le système de fichiers client, importez la dans le porte-clés GPG local. Différents systèmes d'exploitation requièrent différentes méthodes.

Pour Red Hat Enterprise Linux 3 ou une version supérieure, utilisez la commande suivante :

```
rpm --import /path/to/YOUR-RPM-GPG-KEY
```

Une fois que la clé GPG a bien été ajoutée au client, le système devrait pouvoir valider les RPM personnalisés signés avec la clé correspondante.

NOTE

Lors de l'utilisation de RPM et canaux personnalisés, veuillez toujours créer une clé GPG personnalisée pour ces paquetages. L'emplacement de la clé GPG doit aussi être ajouté au profil Kickstart.

La clé GPG personnalisée doit être ajoutée aux systèmes client, sinon l'installation Kickstart pourrait échouer.

CHAPITRE 5. RÉSOLUTION DE PROBLÈMES

Ce chapitre offre des conseils pour déterminer la cause d'erreurs les plus communes associées à Red Hat Satellite et pour les résoudre. Si vous avez besoin d'aide supplémentaire, contactez l'assistance Red Hat Network à l'adresse https://access.redhat.com/support/. Connectez-vous en utilisant votre compte ayant des droits d'accès au Satellite pour voir la liste complète de vos options.

Pour commencer la résolution de problèmes généraux, examinez le fichier journal ou les fichiers associés au composant présentant des échecs. Un exercice utile est d'exécuter la commande **`tail -f`** pour tous les fichiers journaux, puis d'exécuter la commande **`yum list`**. Vous devriez alors examiner toutes les nouvelles entrées de journaux pour des indices potentiels.

5.1. Espace disque

Q : Mon espace disque s'est rempli rapidement. Que s'est-il passé et que dois-je faire ?

R : Un problème commun est l'espace de disque plein. Un signe pratiquement sûr de ce problème est l'apparence d'écriture arrêtée dans les fichiers journaux. Si la journalisation s'est arrêtée durant une écriture, comme un mot à moitié écrit, il est probable que les disques soient pleins. Pour confirmer cela, exécutez la commande suivante et vérifiez les pourcentages dans la colonne **`Uti%`** :

```
# df -h
```

Outre les fichiers journaux, vous pouvez obtenir des informations de valeur en obtenant le statut de Red Hat Satellite et de ses divers composants. Pour ce faire, utilisez la commande suivante :

```
# /usr/sbin/rhn-satellite status
```

De plus, vous pouvez obtenir individuellement le statut de composants tels que le serveur web Apache et le **Red Hat Network Task Engine**. Par exemple, pour afficher le statut du serveur web Apache, exécutez la commande suivante :

```
# service httpd status
```

5.2. Installation et mise à jour

Q : SELinux me bombarde de messages pendant l'installation. Pourquoi ?

R : Si vous rencontrez des problèmes avec les messages SELinux (comme les messsages de refus AVC) pendant l'installation de Red Hat Satellite, veillez à ce que les fichiers **`audit.log`** soient bien disponibles, de façon à ce que le personnel du support technique Red Hat puisse vous assister. Vous pourrez trouver le fichier dans **`/var/log/audit/audit.log`** et vous pourrez l'attacher au ticket du support technique afin que les ingénieurs puissent vous assister.

Q : J'ai modifié `/var/satellite` en un montage NFS, maintenant SELinux l'empêche de fonctionner correctement. Que dois-je faire ?

R : Les paramètres SELinux doivent être modifiés en se basant sur le nouveau montage NFS afin que SELinux autorise ce trafic. Vous pouvez effectuer ceci avec cette commande :

```
# /usr/sbin/setsebool -P spacewalk_nfs_mountpoint on
```

Si vous utilisez Red Hat Enterprise Linux 6, vous devrez aussi exécuter la commande :

```
# /usr/sbin/setsebool -P cobbler_use_nfs on
```

Q : Mon Satellite ne fonctionne pas. Que se passe-t-il ?

R : N'enregistrez Red Hat Satellite sur aucun des canaux enfant suivants disponibles à partir des serveurs centraux de Red Hat Network :

Red Hat Developer Suite

Red Hat Application Server

Red Hat Extras

JBoss product channels

S'abonner à ces canaux et mettre à jour le Satellite peut installer de nouvelles versions de composants logiciel critiques invalides, causant ainsi l'échec du Satellite.

5.3. Services

Q : Pourquoi le serveur Web Apache n'est-il pas en cours d'exécution ?

R : Si le serveur Web Apache n'est pas en cours d'exécution, des entrées dans votre fichier **`/etc/hosts`** peuvent être incorrectes.

Q : Comment puis-je trouver le statut de Red Hat Network Task Engine ?

R : Pour obtenir le statut du **Red Hat Network Task Engine**, exécutez la commande suivante :

```
# service taskomatic status
```

Q : Comment puis-je trouver le statut de la base de données intégrée du Satellite ?

R : Pour obtenir le statut de la base de données intégrée du Satellite, si elle existe, exécutez la commande suivante :

```
# db-control status
```

Q : Que faire si la fonctionnalité push de Red Hat Satellite arrête de fonctionner ?

R : Si la fonctionalité push de Red Hat Satellite cessent de fonctionner, il est possible que d'anciens fichiers journaux en soient la cause. Arrêtez le démon jabberd avant de supprimer ces fichiers. Pour ce faire, exécutez les commandes suivantes en tant qu'utilisateur root :

```
# service jabberd stop
# rm -f /var/lib/jabberd/db/_db*
# service jabberd start
```

5.4. Connectivité

Q : Je ne parviens pas à me connecter ! Comment est-ce que je résous le problème ?

R : Les mesures suivantes peuvent être utilisées pour résoudre les problèmes d'erreurs générales de connexion :

Essayez de connecter la base de données de Red Hat Satellite en ligne de commande à l'aide de la chaîne de connexion correcte, se trouvant dans **/etc/rhn/rhn.conf** :

```
# sqlplus username/password@sid
```

Assurez-vous que Red Hat Satellite utilise le protocole de temps réseau NTP et qu'il est défini sur le bon fuseau horaire. Cela s'applique également à tous les systèmes client et à la machine séparée de la base de données dans Red Hat Satellite avec la base de données autonome.

Confirmez que le bon paquetage :

```
rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm
```

est installé sur Red Hat Satellite et que le fichier **rhn-org-trusted-ssl-cert-*.noarch.rpm** correspondant ou le certificat SSL CA (client) public brut est installé sur tous les systèmes client.

Vérifiez que les systèmes client sont configurés de façon à utiliser le certificat approprié.

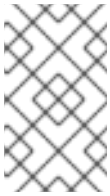
Si vous utilisez également un ou plusieurs serveurs Red Hat Satellite Proxy Servers, assurez-vous que les certificats SSL de chaque proxy sont préparés correctement. Le proxy devrait avoir sa propre paire de clés SSL de serveur et son propre certificat SSL CA public (client) installés, vu qu'il servira dans les deux fonctions. Reportez-vous au chapitre sur les certificats SSL du *Guide de configuration du client Red Hat Satellite* pour obtenir des instructions spécifiques.

Assurez-vous que les systèmes client n'utilisent pas leurs propres pare-feu bloquant ainsi les ports requis, comme l'identifie la section *Conditions supplémentaires* du *Guide d'installation Red Hat Satellite*.

Q : Que dis-je faire si l'importation ou la synchronisation d'un canal a échoué et que vous ne pouvez pas le retrouver d'une autre manière ?

R : Si l'import ou la synchronisation d'un canal a échoué et que vous ne pouvez pas le retrouver d'une autre manière, exécutez la commande suivante pour supprimer le cache :

```
# rm -rf temporary-directory
```



NOTE

La section *Préparations pour importer à partir d'un support local* du *Guide d'installation Red Hat Satellite* spécifie **/var/rhn-sat-import/** en tant que répertoire temporaire.

Relancez ensuite l'import ou la synchronisation.

Q : Je reçois des erreurs "SSL_CONNECT". Que dois-je faire ?

R : Un problème commun de connexion, indiqué par les erreurs **SSL_CONNECT**, est le résultat d'un Satellite installé sur une machine dont la date et l'heure ont été mal configurées. Durant l'installation du Satellite, les certificats SSL sont créés avec des dates et des heures qui ne sont pas exactes. Si la date et l'heure du Satellite sont alors corrigées, la date et l'heure de départ du certificat peuvent être définies dans le futur, ce qui les rendra invalides.

Pour résoudre ce problème, vérifiez la date et l'heure sur les clients et le Satellite à l'aide de la commande suivante :

```
# date
```

Les résultats devraient être pratiquement identiques pour toutes les machines et au sein des fenêtres de validité "notBefore" (pas avant) et "notAfter" (pas après) des certificats. Vérifiez les dates et les heures des certificats client à l'aide de la commande suivante :

```
# openssl x509 -dates -noout -in /usr/share/rhn/RHN-ORG-TRUSTED-SSL-
CERT
```

Vérifiez les dates et les heures des certificats du serveur du Satellite à l'aide de la commande suivante :

```
# openssl x509 -dates -noout -in /etc/httpd/conf/ssl.crt/server.crt
```

Par défaut, le certificat du serveur a une durée de vie d'un an alors que les certificats client sont bons pour dix ans. Si vous trouvez que les certificats ne sont pas corrects, vous pouvez attendre la date et l'heure de départ valides, si possible, ou créer de nouveaux certificats, préférablement avec toutes les dates et les heures système définies sur GMT.

5.5. Journalisation et rapports

Q : Quels sont les différents fichiers de journalisation ?

R : Chaque étape de résolution de problèmes devrait commencer avec l'examen des fichiers journaux associés. Ces derniers offrent des informations inestimables sur l'activité qui a pris place sur le périphérique ou au sein de l'application, ces informations peuvent être utilisées pour contrôler la performance et assurer une configuration correcte. Consultez le Tableau 5.1, « Fichiers journaux » pour les chemins aux fichiers journaux appropriés :

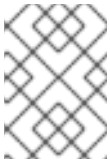
Il peut y avoir des fichiers journaux numérotés (tels que /var/log/rhn/rhn_satellite_install.log.1, /var/log/rhn/rhn_satellite_install.log.2, etc.) dans le répertoire **/var/log/rhn/**. Il s'agit de journaux *rotatifs*, des fichiers journaux créés avec une extension .<NUMBER> lorsque le fichier **rhn_satellite_install.log** actuel est rempli à la taille spécifiée par le démon **logrotate(8)** et le contenu est donc écrit sur un fichier journal rotatif. Par exemple, **rhn_satellite_install.log.1** contiendra le fichier journal rotatif le plus ancient, tandis que **rhn_satellite_install.log.4** contiendra le fichier journal rotatif le plus récent.

Tableau 5.1. Fichiers journaux

Composant/Tâche	Emplacement du fichier journal
Serveur web Apache	répertoire **`/var/log/httpd/`**
Red Hat Satellite	répertoire **`/var/log/rhn/`**
Programme d'installation Red Hat Satellite	**`/var/log/rhn/rhn_satellite_install.log`**
Installation de la base de données - *Base de données intégrée*	**`/var/log/rhn/install_db.log`**
Population de la base de données	**`/var/log/rhn/populate_db.log`**
Outil de synchronisation Red Hat Satellite	**`/var/log/rhn/rhn_server_satellite.log`**
Infrastructure du Monitoring	Répertoire **`/var/log/nocpulse/`**
Notifications du Monitoring	répertoire **`/var/log/notification/`**
Red Hat Network DB Control - *Base de données intégrée*	**`/var/log/rhn/rhn_database.log`**
Red Hat Network Task Engine (taskomatic)	**`/var/log/messages`**
yum	**`/var/log/yum.log`**
Transactions XML-RPC	**`/var/log/rhn/rhn_server_xmlrpc.log`**

Q : Comment utiliser les rapports `spacewalk-report` ?

R : Dans certaines instances, les administrateurs pourraient nécessiter un sommaire précis et formaté de leurs ressources Red Hat Satellite, que ceci soit nécessaire afin de faire un inventaire de leurs droits d'accès, des systèmes abonnés, ou des utilisateurs et organisations. Plutôt que de rassembler ce type d'informations manuellement depuis l'interface du Satellite, Red Hat Satellite inclut la commande **`spacewalk-report`** pour rassembler et afficher les informations vitales du Satellite en une seule fois.



NOTE

Le paquetage **`spacewalk-reports`** doit être installé pour pouvoir utiliser **`spacewalk-report`**.

`spacewalk-report` permet aux administrateurs d'organiser et d'afficher des rapports concernant le contenu, les errata, les systèmes, l'historique des événements système et les ressources utilisateur du Satellite. La commande **`spacewalk-report`** est utilisée pour générer des rapports sur :

System Inventory - Répertorie tous les systèmes enregistrés sur le Satellite.

Entitlements - Répertorie toutes les organisations sur le Satellite et les trie par droits d'accès système ou canal.

Errata - Répertorie tous les errata concernant les systèmes enregistrés et trie les errata en fonction de la sévérité ainsi que les systèmes s'appliquant à un erratum en particulier.

Users - Répertorie tous les utilisateurs enregistrés sur le Satellite, et répertorie tout système associé à un utilisateur en particulier.

System History - Répertorie un sous-ensemble ou tous les événements système qui se sont produits.

Pour recevoir un rapport sous le format CSV, exécutez ce qui suit à l'invite de commande de votre serveur Satellite.

```
# spacewalk-report report_name
```

Les rapports suivants sont disponibles :

Tableau 5.2. Rapports `spacewalk-report`

Rapport	Invoqué ainsi	Description
Inventaire du système	**`inventory`**	Liste des systèmes enregistrés sur le serveur avec des informations sur le matériel et les logiciels.
Droits d'accès	**`droits d'accès`**	Répertorie toutes les organisations sur le Satellite avec leurs droits d'accès système ou canaux.
Errata dans les canaux	**`errata-channels`**	Répertorie les errata dans les canaux
Tous les errata	**`errata-list-all`**	Liste complète de tous les errata
Errata de systèmes	**`errata-systems`**	Répertorie les errata applicables et tous les systèmes enregistrés qui sont affectés
Utilisateurs du système	**`users`**	Répertorie tous les utilisateurs enregistrés sur le Satellite
Systèmes administrés	**`users-systems`**	Répertorie les systèmes pouvant être administrés par des utilisateurs individuels
Arborescences kickstart	**`kickstartable-trees`**	Répertorie les arborescences pouvant être « kickstartées »
Historique du système	**`system-history`**	Répertorie l'historique des événements système

Rapport	Invoqué ainsi	Description
Canaux des historiques de systèmes	**system-history-channels**	Répertorie l'historique des événements système
Historique de la configuration du système	**system-history-configuration**	Répertorie l'historique des événements de la configuration du système
Historique des droits d'accès système	**system-history-entitlements**	Répertorie l'historique des événements des droits d'accès système
Historique d'errata système	**system-history-errata**	Répertorie l'historique des événements d'errata système
Historique Kickstart des systèmes	**system-history-kickstart**	Répertorie l'historique des événements kickstart et provisioning
Historique des paquetages système	**system-history-packages**	Répertorie l'historique des événements des paquetages système

Pour obtenir plus d'informations sur un rapport individuel, exécutez **spacewalk-report** avec l'option **--info** ou **--list-fields-info** et le nom du rapport. La description et la liste des champs possibles du rapport s'afficheront.

Pour obtenir plus d'informations, la page man **spacewalk-report(8)** ainsi que le paramètre **--help** du programme **spacewalk-report** peuvent être utilisés pour accéder à des informations supplémentaires sur les invocations du programme et ses options.

Q : Comment déterminer la version de votre schéma de bases de données ?

R : Pour déterminer la version de votre schéma de bases de données, exécutez la commande suivante :

```
# rhn-schema-version
```

Q : Comment déterminer mes types de caractères ?

R : Pour dériver les types de l'ensemble de caractères de la base de données de votre Satellite, exécutez la commande suivante :

```
# rhn-charsets
```

Q : Pourquoi l'administrateur ne reçoit-il pas d'emails ?

R : Si l'administrateur ne reçoit pas de courrier électronique provenant de Red Hat Satellite, confirmez que les bonnes adresses électroniques ont été définies pour **`traceback_mail`** dans **`/etc/rhn/rhn.conf`**.

Q : Comment changer l'expéditeur de courrier traceback ?

R : Si le courrier traceback est marqué depuis dev-null@rhn.redhat.com et que vous souhaitez que l'adresse soit valide pour votre organisation, incluez l'option **`web.default_mail_from`** et la valeur appropriée dans **`/etc/rhn/rhn.conf`**.

5.6. Erreurs

Q : J'obtiens l'erreur suivante « Error validating satellite certificate » pendant une installation de Red Hat Satellite. Comment la corriger ?

R : L'erreur « Error validating satellite certificate » qui apparaît pendant une installation de Red Hat Satellite est causée par la présence d'un proxy HTTP dans l'environnement. Cela peut être confirmé en consultant le fichier **`install.log`**, et en localisant l'erreur suivante :

```
ERROR: unhandled exception occurred:
Traceback (most recent call last):
  File "/usr/bin/rhn-satellite-activate", line 45, in ?
    sys.exit(abs(mod.main() or 0))
  File "/usr/share/rhn/satellite_tools/rhn_satellite_activate.py",
line 585, in main
    activateSatellite_remote(options)
  File "/usr/share/rhn/satellite_tools/rhn_satellite_activate.py",
line 291, in activateSatellite_remote
    ret = s.satellite.deactivate_satellite(systemid, rhn_cert)
  File "/usr/lib/python2.4/site-packages/rhn/rpclib.py", line 603, in
__call__
    return self._send(self._name, args)
  File "/usr/lib/python2.4/site-packages/rhn/rpclib.py", line 326, in
_request
    self._handler, request, verbose=self._verbose)
  File "/usr/lib/python2.4/site-packages/rhn/transports.py", line 171,
in request
    headers, fd = req.send_http(host, handler)
  File "/usr/lib/python2.4/site-packages/rhn/transports.py", line 698,
in send_http
    self._connection.connect()
  File "/usr/lib/python2.4/site-packages/rhn/connections.py", line
193, in connect
    sock.connect((self.host, self.port))
  File "<string>", line 1, in connect
socket.timeout: timed out
```

Pour résoudre le problème :

1. Exécuter le script install en mode déconnecté, et ignorer l'installation de la base de données qui a déjà été faite :

   ■

```
# ./install.pl --disconnected --skip-db-install
```

2. Ouvrir **/etc/rhn/rhn.conf** avec votre éditeur de texte préféré, et ajouter ou modifier la ligne suivante :

```
server.satellite.rhn_parent = satellite.rhn.redhat.com
```

Retirer la ligne suivante :

```
disconnected=1
```

Si vous utilisez un proxy pour la connexion à RHN, vous aurez également besoin d'ajouter ou de modifier les lignes suivantes pour refléter les paramètres du proxy.

```
server.satellite.http_proxy = <hostname>:<port>
server.satellite.http_proxy_username = <username>
server.satellite.http_proxy_password = <password>
```

3. Ré-activer le Satellite en mode connecté, en utilisant la commande **rhn-satellite-activate** en tant qu'utilisateur root, en incluant le chemin d'accès et le nom de fichier du certificat de satellite :

```
# rhn-satellite-activate --rhn-cert=/path/to/file.cert
```

Sinon, essayer d'exécuter le script **install.pl** en mode connecté, mais avec l'option **--answer-file=*answer file***. Veillez à ce que le fichier réponse possède les informations de proxy HTTP spécifiées comme suit :

```
rhn-http-proxy = <hostname>:<port>
rhn-http-proxy-username = <username>
rhn-http-proxy-password = <password>
```

Q : J'obtiens l'erreur suivante « ERROR: server.mount_point not set in the configuration file » quand j'essaie d'activer ou de synchroniser Red Hat Satellite. Comment régler ce problème ?

R : Une erreur « ERROR: server.mount_point not set in the configuration file » peut se produire au moment de l'activation ou de la synchronisation de Red Hat Satellite si le paramètre de configuration ***mount_point*** de **/etc/rhn/rhn.conf** ne pointe pas vers un chemin d'accès de répertoire, ou que le chemin d'accès vers lequel il pointe n'est pas présent ou n'a pas la permission d'accéder au répertoire.

Pour résoudre ce problème, vérifier la valeur du paramètre de configuration ***mount_point*** dans **/etc/rhn/rhn.conf**. S'il est fixé à la valeur par défaut **/var/satellite**, vérifier que les répertoires **/var/satellite** et **/var/satellite/redhat** existent. Pour toute valeur, vérifier que le chemin d'accès au fichier est précis, et que les permissions sont configurées correctement.

Q : Pourquoi est-ce que `cobbler check` produit une erreur indiquant qu'il a besoin d'une version différente de `yum-utils` ?

R : Parfois, en exécutant la commande **`cobbler check`**, vous pouvez obtenir une erreur qui ressemble à ce qui suit :

```
# cobbler check
The following potential problems were detected:
#0: yum-utils need to be at least version 1.1.17 for reposync -l,
current version is 1.1.16
```

Il s'agit d'un problème connu du paquetage **`reposync`** de Cobbler. Il s'agit d'une fausse erreur qui peut être ignorée en toute sécurité. Cette erreur sera résolue dans les versions futures de Red Hat Satellite.

Q : Je reçois l'erreur « unsupported version » quand je tente d'activer le certificat Red Hat Satellite. Comment corriger ce problème ?

R : Si votre certificat Red Hat Satellite a été corrompu, vous pourriez avoir les erreurs suivantes :

```
ERROR: <Fault -2: 'unhandled internal exception: unsupported version:
96'>
```

```
RHN_PARENT: satellite.rhn.redhat.com
     Error reported from RHN: <Fault -2: 'unhandled internal
exception: unsupported version: 115'>
     ERROR: unhandled XMLRPC fault upon remote activation: <Fault -2:
'unhandled internal exception: unsupported version: 115'>
     ERROR: <Fault -2: 'unhandled internal exception: unsupported
version: 115'>
```

```
Invalid satellite certificate
```

Pour résoudre ce problème, veuillez contacter les services de support Red Hat pour obtenir un nouveau certificat.

Q : J'obtiens une erreur "Internal Server Error" qui se plaint d'ASCII quand j'essaie de modifier le profile kickstart. Que se passe-t-il ?

R : Si vous avez ajouté quelques paramètres de noyau récemment à votre profile de kickstart, vous noterez sans doute que lorsque vous tentez d' **`Afficher une liste des profils de Kickstart`**, vous obtenez l'erreur de serveur interne suivante :

```
'ascii' codec can't encode character u'\u2013'
```

Cette erreur se produit car il y a du texte dans le profil qui n'est pas reconnu correctement.

Pour résoudre le problème :

1. Ssh directement sur le serveur du Satellite en tant qu'utilisateur root :

```
# ssh root@satellite.fqdn.com
```

2. Chercher le profil de kickstart qui cause le problème en regardant les dates des fichiers dans **/var/lib/cobbler/config/profiles.d** et en localisant celui qui a été modifié le plus récemment :

```
# ls -l /var/lib/cobbler/config/profiles.d/
```

3. Ouvrir le profile dans votre éditeur de texte préféré, et essayez de localiser le texte suivant :

```
\u2013hostname
```

Changer l'entrée ainsi :

```
--hostname
```

4. Sauvegarder les changements au profil et fermer le fichier.

5. Redémarrer les services Red Hat Satellite pour récupérer le profil mis à jour :

```
# rhn-satellite restart
Shutting down rhn-satellite...
Stopping RHN Taskomatic...
Stopped RHN Taskomatic.
Stopping cobbler daemon:                                   [
OK  ]
Stopping rhn-search...
Stopped rhn-search.
Stopping MonitoringScout ...                               [
OK  ]
Stopping Monitoring ...                                    [
OK  ]
Stopping httpd:                                            [
OK  ]
Stopping tomcat5:                                          [
OK  ]
Shutting down osa-dispatcher:                              [
OK  ]
Shutting down Oracle Net Listener ...                      [
OK  ]
Shutting down Oracle DB instance "rhnsat" ...              [
OK  ]
Shutting down Jabber router:                               [
OK  ]
Done.
Starting rhn-satellite...
Starting Jabber services                                   [
OK  ]
Starting Oracle Net Listener ...                           [
OK  ]
Starting Oracle DB instance "rhnsat" ...                   [
OK  ]
Starting osa-dispatcher:                                   [
OK  ]
Starting tomcat5:                                          [
```

```
OK  ]
Starting httpd:                                            [
OK  ]
Starting Monitoring ...                                    [
OK  ]
Starting MonitoringScout ...                               [
OK  ]
Starting rhn-search...
Starting cobbler daemon:                                   [
OK  ]
Starting RHN Taskomatic...
Done.
```

6. Retournez sur l'interface web. Notez que celle-ci peut prendre un certain temps avant de résoudre les services, mais devrait retourner à la normale après un certain temps.

Q : Je reçois le message "Host Not Found" (Impossible de trouver l'hôte) ou "Could Not Determine FQDN" (Impossible de déterminer le FQDN). Que dois-je faire maintenant ?

R : Vu que les fichiers de configuration de RHN dépendent exclusivement de noms de domaine entièrement qualifiés (ou FQDN), il est impératif que les applications clés puissent résoudre le nom de Red Hat Satellite en une adresse IP. **Red Hat Update Agent**, le **Red Hat Network Registration Client** et le serveur Web Apache sont particulièrement sujets à ce problème avec les applications Red Hat Network produisant des erreurs « host not found » (hôte introuvable) et le serveur Web indiquant « Could not determine the server's fully qualified domain name » (impossible de déterminer le nom de domaine du serveur) lors de l'échec du démarrage.

Ce problème provient en général du fichier **`/etc/hosts`**. Vous pouvez confirmer ceci en examinant le fichier **`/etc/nsswitch.conf`**, qui définit les méthodes et l'ordre dans lequel les noms de domaine sont résolus. Normalement, le fichier **`/etc/hosts`** est vérifié en premier, suivi par le NIS (Network Information Service), s'il est utilisé, puis par le DNS. L'un d'eux doit réussir pour que le serveur Web Apache démarre et que les applications client de RHN fonctionnent.

Pour résoudre ce problème, identifiez le contenu du fichier **`/etc/hosts`**. Il peut ressembler à l'exemple suivant :

```
127.0.0.1 this_machine.example.com this_machine localhost.localdomain
\ localhost
```

Tout d'abord, dans un éditeur de texte, supprimez les informations de la machine fautive comme dans l'exemple suivant :

```
127.0.0.1 localhost.localdomain.com localhost
```

Puis, enregistrez le fichier et essayez d'exécuter à nouveau les applications client de RHN ou le serveur Web Apache. Si elles échouent toujours, identifiez de manière explicite l'adresse IP du Satellite dans le fichier comme dans l'exemple suivant :

```
127.0.0.1 localhost.localdomain.com localhost
123.45.67.8 this_machine.example.com this_machine
```

Remplacez la valeur ici avec l'adresse IP actuelle du Satellite. Le problème devrait ainsi être résolu. Souvenez-vous que si l'adresse IP spécifique est stipulée, le fichier devra être mis à jour lorsque la machine obtient une nouvelle adresse.

Q : J'obtiens l'erreur « This server is not an entitled Satellite » (ce serveur n'est pas un Satellite autorisé) quand j'essaie de synchroniser le serveur Red Hat Satellite. Comment corriger ce problème ?

R : Si **satellite-sync** rapporte que le serveur n'est pas activé en tant que Red Hat Satellite, c'est qu'il n'a pas souscrit au canal Red Hat Satellite respectif. S'il s'agit d'un système récemment installé, alors il est possible que le certificat de satellite ne soit pas activé sur le système. S'il était activé, alors il est maintenant désactivé.

Vérifiez les canaux enfants du système pour déterminer s'il est souscrit à un canal Red Hat Network Red Hat Satellite. Affichez les canaux abonnés (ou souscrits) avec la commande suivante :

```
# yum repolist
```

Activez le même certificat de Satellite à nouveau sur votre Satellite en utilisant cette commande en tant qu'utilisateur root :

```
# rhn-satellite-activate -vvv --rhn-cert=/path/to/certificate
```

5.7. Interface web

Q : J'ai des problèmes avec l'interface utilisateur Red Hat Satellite. Quels fichiers de journalisation devrais-je vérifier ?

R : Si vous rencontrez des erreurs pendant la visualisation, la planification ou lorsque vous travaillez avec des kickstarts dans l'interface utilisateur Red Hat Satellite, vérifiez le fichier de journalisation **/var/log/tomcat6/catalina.out**.

Pour toutes les autres erreurs d'interface utilisateur, vérifiez le fichier de journalisation **/var/log/httpd/error_log**.

5.8. Anaconda

Q : Je rencontre une erreur disant : Erreur lors du téléchargement du fichier kickstart. Quel est le problème et comment puis-je le résoudre ?

R : Cette erreur est habituellement le résultat d'un problème réseau. Pour localiser le problème, exécutez la commande **cobbler check**, et lisez la sortie. Elle devrait ressembler à ceci :

```
# cobbler check
The following potential problems were detected:
#0: reposync is not installed, need for cobbler reposync,
install/upgrade yum-utils?
#1: yumdownloader is not installed, needed for cobbler repo add with -
-rpm-list parameter, install/upgrade yum-utils?
#2: The default password used by the sample templates for newly
installed machines (default_password_crypted in /etc/cobbler/settings)
is still set to 'cobbler' and should be changed
#3: fencing tools were not found, and are required to use the
(optional) power management features. install cman to use them
```

Si **cobbler check** ne fournit pas de réponse, vérifiez les éléments suivants :

Vérifiez que **httpd** est en cours d'exécution : **service httpd status**

Vérifiez que **cobblerd** est en cours d'exécution : **service cobblerd status**

Vérifiez qu'il est possible de récupérer le fichier kickstart à l'aide de **wget** depuis un autre hôte :

```
wget http://satellite.example.com/cblr/svc/op/ks/profile/rhel5-
i386-u3:1:Example-Org
```

Q : Je reçois une erreur d'installation de paquetage disant Le fichier *chkconfig-1.3.30.1-2.i386.rpm* ne peut pas être ouvert. Quel est le problème et comment puis-je le corriger ?

R : Les clients vont récupérer le contenu de Red Hat Satellite en se basant sur le paramètre ***--url*** dans le kickstart. Par exemple :

```
url --url http://satellite.example.com/ks/dist/ks-rhel-i386-server-5-
u3
```

Si vous recevez des erreurs d'Anaconda disant qu'il ne peut pas trouver d'image(s) ou de paquetage(s), vérifiez que l'URL du kickstart générera bien une réponse ***200 OK***. Ceci peut être effectué en tentant de récupérer le fichier se trouvant dans cet URL à l'aide de **wget** :

```
wget http://satellite.example.com/ks/dist/ks-rhel-i386-server-5-u3
--2011-08-19 15:06:55--  http://satellite.example.com/ks/dist/ks-rhel-
i386-server-5-u3
Resolving satellite.example.com... 10.10.77.131
Connecting to satellite.example.com|10.10.77.131|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0 [text/plain]
Saving to: `ks-rhel-i386-server-5-u3.1'
2011-08-19 15:06:55 (0.00 B/s) - `ks-rhel-i386-server-5-u3.1' saved
[0/0]
```

Si vous recevez une réponse différente de ***200 OK***, vérifiez les journaux de l'erreur pour découvrir le problème. Vous pouvez aussi vérifier le fichier qu'Anaconda a essayé de télécharger en cherchant dans le fichier **access_log** :

```
# grep chkconfig /var/log/httpd/access_log
10.10.77.131 - - [19/Aug/2011:15:12:36 -0400] "GET
/rhn/common/DownloadFile.do?url=/ks/dist/ks-rhel-i386-server-
5-u3/Server  /chkconfig-1.3.30.1-2.i386.rpm HTTP/1.1" 206 24744 "-"
"urlgrabber/3.1.0 yum/3.2.19"
10.10.76.143 - - [19/Aug/2011:15:12:36 -0400] "GET /ks/dist/ks-rhel-
i386-server-5-u3/Server/chkconfig-
1.3.30.1-2.i386.rpm HTTP/1.1" 206 24744 "-" "urlgrabber/3.1.0
yum/3.2.19"
10.10.76.143 - - [19/Aug/2011:15:14:20 -0400] "GET /ks/dist/ks-rhel-
i386-server-5-u3/Server/chkconfig-
1.3.30.1-2.i386.rpm HTTP/1.1" 200 162580 "-" "urlgrabber/3.1.0
```

```
yum/3.2.19"
10.10.77.131 - - [19/Aug/2011:15:14:20 -0400] "GET
/rhn/common/DownloadFile.do?url=/ks/dist/ks-rhel-i386-server-
5-u3/Server/chkconfig-1.3.30.1-2.i386.rpm HTTP/1.1" 200 162580 "-"
"urlgrabber/3.1.0 yum/3.2.19"
```

Si les requêtes n'apparaissent pas dans le fichier **access_log**, le système pourrait avoir des problèmes avec l'installation réseau. Si les erreurs apparaissent mais génèrent des erreurs, alors vérifiez les journaux des erreurs.

Vous pouvez aussi tenter de télécharger les fichiers manuellement afin de voir si le paquetage est disponible :

```
wget http://satellite.example.com/ks/dist/ks-rhel-i386-server-5-
u3/Server/chkconfig-1.3.30.1-2.i386.rpm
```

5.9. Tracebacks

Q : Je reçois des courriers électroniques avec « WEB TRACEBACK » pour sujet. Que devrais-je faire à ce propos ?

R : Typiquement, un email traceback ressemble typiquement à ceci :

```
Subject: WEB TRACEBACK from satellite.example.com
Date: Wed, 19 Aug 2011 20:28:01 -0400
From:Red Hat Satellite <dev-null@redhat.com>
To: admin@example.com

java.lang.RuntimeException: XmlRpcException calling cobbler.
 at
com.redhat.rhn.manager.kickstart.cobbler.CobblerXMLRPCHelper.invokeMet
hod(CobblerXMLRPCHelper.java:72)
 at
com.redhat.rhn.taskomatic.task.CobblerSyncTask.execute(CobblerSyncTask
.java:76)
 at
com.redhat.rhn.taskomatic.task.SingleThreadedTestableTask.execute(Sing
leThreadedTestableTask.java:54)
 at org.quartz.core.JobRunShell.run(JobRunShell.java:203)
 at
org.quartz.simpl.SimpleThreadPool$WorkerThread.run(SimpleThreadPool.ja
va:520)
Caused by: redstone.xmlrpc.XmlRpcException: The response could not be
parsed.
 at redstone.xmlrpc.XmlRpcClient.handleResponse(XmlRpcClient.java:434)
 at redstone.xmlrpc.XmlRpcClient.endCall(XmlRpcClient.java:376)
 at redstone.xmlrpc.XmlRpcClient.invoke(XmlRpcClient.java:165)
 at
com.redhat.rhn.manager.kickstart.cobbler.CobblerXMLRPCHelper.invokeMet
hod(CobblerXMLRPCHelper.java:69)
 ... 4 more
Caused by: java.io.IOException: Server returned HTTP response code:
503 for URL: http://someserver.example.com:80/cobbler_api
 at
```

```
sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConn
ection.java:1236)
 at redstone.xmlrpc.XmlRpcClient.handleResponse(XmlRpcClient.java:420)
 ... 7 more
```

Ceci indique qu'un problème s'est produit lors de la communication de Cobbler avec le service **taskomatic**. Essayez de vérifier les éléments suivants :

Vérifiez que **httpd** est en cours d'exécution : **# service httpd status**

Vérifiez que **cobblerd** est en cours d'exécution : **# service cobblerd status**

Vérifiez qu'il n'existe pas de règle de pare-feu qui pourrait prévenir les connexions **localhost**

5.10. Enregistrement

Q : La commande rhnreg_ks échoue lorsque je l'exécute, elle retourne ERROR: unable to read system id (ERREUR : lecture de l'ID du système impossible). Quel est le problème ?

R : Il existe une section **%post** qui enregistre la machine sur Red Hat Satellite à la fin du fichier kickstart :

```
# begin Red Hat management server registration
mkdir -p /usr/share/rhn/
wget http://satellite.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT -O
/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
perl -npe 's/RHNS-CA-CERT/RHN-ORG-TRUSTED-SSL-CERT/g' -i
/etc/sysconfig/rhn/*
rhnreg_ks --serverUrl=https://satellite.example.com/XMLRPC --
sslCACert=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT --activationkey=1-
c8d01e2f23c6bbaedd0f6507e9ac079d
# end Red Hat management server registration
```

En interprétant ceci dans l'ordre d'ajout, ceci va :

Créer un répertoire pour héberger le certificat SSL personnalisé utilisé par Red Hat Satellite.

Récupérer le certificat SSL à utiliser pendant l'enregistrement.

Chercher et remplacer les chaînes du certificat SSL depuis les fichiers de configuration de **rhn-register**, puis enregistrer sur Red Hat Satellite à l'aide du certificat SSL et d'une clé d'activation. Chaque profil kickstart inclut une clé d'activation qui assure que le système se voit assigné une base et des canaux enfants corrects, ainsi que les bons droits d'accès. S'il s'agit du réapprovisionnement d'un système existant, la clé d'activation assurera aussi que celui-ci soit bien associé au profil système précédent.

Si la commande **rhnreg_ks** échoue, vous pourriez voir des erreurs comme celle-ci dans le fichier de journalisation **ks-post.log** :

```
ERROR: unable to read system id.
```

Ces erreurs se produiront aussi si vous tentez d'effectuer **rhn_check** et que votre système n'a pas été enregistré sur Red Hat Satellite.

La meilleure manière de résoudre ce problème est d'afficher le fichier kickstart et de directement copier et coller les quatres étapes lors de l'invite de commande une fois que le kickstart est terminé. Cela produira des messages d'erreurs plus détaillés qui vous aideront à localiser le problème.

5.11. Kickstarts et snippets

Q : Quelle est la structure des répertoires des kickstarts ?

R : Le chemin de base où les kickstarts sont stockés est **/var/lib/rhn/kickstarts/**. Dans ce répertoire, les kickstarts bruts se trouvent dans le sous-répertoire **upload**, et les kickstarts générés par assistant se trouvent dans le répertoire **wizard** :

```
Raw Kickstarts: /var/lib/rhn/kickstarts/upload/$profile_name--
$org_id.cfg
Wizard Kickstarts: /var/lib/rhn/kickstarts/wizard/$profile_name--
$org_id.cfg
```

Q : Quelle est la structure des répertoires des snippets de Cobbler ?

R : Les snippets de Cobbler sont stockés dans **/var/lib/rhn/kickstarts/snippets**. Cobbler accède aux snippets à l'aide du lien symbolique **/var/lib/cobbler/snippets/spacewalk**.

```
Snippets:  /var/lib/rhn/kickstarts/snippets/$org_id/$snippet_name
```

IMPORTANT

Les RPM de Red Hat Satellite s'attendent à ce que les répertoires des snippets et kickstarts de Cobbler se trouvent à leurs emplacements par défaut, ne les modifiez pas.

5.12. Monitoring

Q : Existe-t-il des outils de diagnostic pouvant aider à déterminer la cause des erreurs de contrôle ?

R : Même si toutes les activités concernant le contrôle sont conduites via l'interface Satellite, Red Hat offre accès aux outils de diagnostic en ligne de commande pouvant vous aider à déterminer la cause d'erreurs. Pour utiliser ces outils, vous devez être en mesure de devenir l'utilisateur **nocpulse** sur le Satellite effectuant les contrôles.

Veuillez commencer par vous connecter au Satellite en tant que super-utilisateur. Puis basculez en utilisateur **nocpulse** à l'aude de la commande suivante :

```
su - nocpulse
```

Pour résoudre complètement les problèmes concernant une sonde, vous devez tout d'abord obtenir

son ID de sonde. Vous pouvez l'obtenir en exécutant **rhn-catalog** sur le serveur Red Hat Satellite en tant qu'utilisateur **nocpulse**. La sortie de la commande ressemblera à l'exemple suivant :

```
2 ServiceProbe on example1.redhat.com (199.168.36.245): test 2
3 ServiceProbe on example2.redhat.com (199.168.36.173): rhel2.1 test
4 ServiceProbe on example3.redhat.com (199.168.36.174): SSH
5 ServiceProbe on example4.redhat.com (199.168.36.175): HTTP
```

L'ID de sonde est le premier numéro, tandis que le nom de la sonde (comme saisi dans l'interface Satellite) est la dernière entrée sur la ligne. Dans l'exemple ci-dessus, l'ID de sonde 5 correspond à la sonde nommée HTTP.

Vous pouvez également passer les options **--commandline** (**-c**) et **--dump** (**-d**) avec un ID de sonde à la commande **rhn-catalog** pour obtenir des informations supplémentaires sur la sonde, comme dans l'exemple suivant :

```
rhn-catalog --commandline --dump 5
```

L'option **--commandline** produit les paramètres de la commande définis pour la sonde, alors que **--dump** obtient tout le reste, y compris les limites d'alerte et les intervalles et les méthodes de notification.

La commande ci-dessus produira une sortie similaire à l'exemple suivant :

```
5 ServiceProbe on example4.redhat.com (199.168.36.175  ):
linux:cpu usage
      Run as: Unix::CPU.pm --critical=90 --sshhost=199.168.36.175
--warn=70 --timeout=15 --sshuser=nocpulse
--shell=SSHRemoteCommandShell --sshport=4545
```

Maintenant que vous possédez l'ID, utilisez-le avec **rhn-runprobe** afin d'examiner la sortie de la sonde.

Q : Comment interpréter la sortie de rhn-runprobe ?

R : Maintenant que vous avez obtenu l'ID de sonde avec **rhn-catalog**, vous pouvez l'utiliser avec **rhn-runprobe** pour examiner la sortie complète de la sonde. Notez que par défaut, **rhn-runprobe** fonctionne en mode test, ce qui signifie qu'aucun résultat n'est entré dans la base de données. Voici ses options :

Tableau 5.3. Options de rhn-runprobe

Option	Description
--help	Affiche les options disponibles et quitte.
--probe=*PROBE_ID*	Exécute la sonde avec cet ID.
--prob_arg=*PARAMETER*	Écrase toutes les paramètres de la sonde de la base de données.

Option	Description
--module=*PERL_MODULE*	Nom du paquetage d'un autre code à exécuter.
--log=all=*LEVEL*	Définit le niveau de journal pour un paquetage ou un préfixe de paquetage.
--debug=*LEVEL*	Définit le niveau de débogage numérique.
--live	Exécute la sonde, met en file d'attente les données et envoie des notifications (si nécessaire).

Vous devez inclure au minimum les options et les valeurs **--probe** et **--log**. L'option **--probe** prend la valeur de l'ID de sonde probeID et l'option **--log** prend la valeur « all » (« tous », pour tous les niveaux d'exécution) et un niveau numérique de commentaires. Ci-dessous figure un exemple :

```
rhn-runprobe --probe=5 --log=all=4
```

La commande ci-dessus demande la sortie de sonde pour probeID 5, pour tous les niveaux d'exécution, avec un niveau élevé de commentaires.

Plus spécifiquement, vous pouvez donner les paramètres de commande dérivé de **rhn-catalog**, comme suit :

```
rhn-runprobe 5 --log=all=4 --sshuser=nocpulse --sshport=4545
```

Cette commande produira une sortie avec commentaires décrivant l'exécution effectuée de la sonde. Les erreurs sont clairement identifiées.

5.13. Satellites à multiples organisations et certificat Satellite

Q : Comment enregistrer mes systèmes dans un environnement à multiples organisations lorsque je ne possède pas suffisamment de droits d'accès dans mon certificat Satellite ?

R : Il existe des situations pour lesquelles vous aurez besoin de libérer des droits d'accès, avec peu de temps à votre disposition, et vous n'aurez peut-être pas accès à chaque organisation pour le faire vous-même. Il y a une option dans Multi-Org Satellites qui permet à l'administrateur Satellite de réduire le nombre de droits d'accès, en dessous de leur niveau d'utilisation. Cette méthode doit être effectuée à partir de l'organisation administrative.

Par exemple, une fois dans votre organisation administrative, si votre certificat est à court de 5 titres de gestion de système pour pouvoir couvrir tous les systèmes enregistrés sur votre Satellite, les 5 systèmes qui ont été enregistrés le plus récemment pour cette organisation, perdront leurs droits d'accès. Ce processus est décrit ci-dessous :

1. Dans le fichier **/etc/rhn/rhn.conf**, définissez ***web.force_unentitlement*** sur 1.
2. Redémarrez le Satellite.

3. Réduisez les droits d'accès alloués aux organisations souhaitées, soit par les onglets **`Subscriptions`**(abonnements) de chaque organisation, ou soit par les onglets **`Organizations`** de chaque droit d'accès individuel.

4. Un certain nombre de systèmes de l'organisation devraient maintenant être dans l'état **`unentitled`** (perte des droits d'accès). Le nombre de systèmes sans droits d'accès, dans cette organisation, doit être égal à la différence entre le nombre total de droits d'accès que vous avez supprimé pour cette organisation, et le nombre de droits d'accès qui ne s'appliquaient pas aux systèmes pour cette organisation.

   Ainsi, si vous supprimez 10 droits d'accès de l'organisation au niveau de la 3ème étape, et que l'organisation possède 4 droits d'accès qui n'étaient pas utilisés par les systèmes, alors il y aura 6 systèmes dépourvus de droits d'accès dans cette organisation.

Une fois que vous aurez le nombre de droits d'accès requis, vous serez alors en mesure d'activer votre nouveau certificat de Satellite. Remarquez bien que modifier la variable ***`web.force_unentitlement`*** est uniquement utile pour réduire les droits d'accès alloués à une organisation donnée en dessous du niveau d'utilisation. Si une organisation possède plus de droits d'accès qu'elle n'en utilise, vous n'aurez pas besoin de paramétrer cette variable pour les supprimer.

Q : Je possède des droits d'accès supplémentaires sur le certificat Satellite qui ne sont pas utilisés. Qu'arrive-t-il à ces droits d'accès ?

R : Si on vous donne un nouveau certificat de Satellite et qu'il comprend plus de droits d'accès que le nombre de droits d'accès consommé par votre Satellite, tout droit d'accès supplémentaire sera assigné à l'organisation administrative. Si vous vous connectez à l'interface web en tant qu'administrateur de Satellite, vous serez alors en mesure d'allouer ces droits d'accès à d'autres organisations. Les droits d'accès précédemment alloués à d'autres organisations ne seront pas affectés.

5.14. Installation et configuration du proxy

Q : Après avoir configuré le gestionnaire de paquetages « Red Hat Network Package Manager », comment puis-je déterminer si les paquetages locaux ont bien été ajoutés au canal Red Hat Network privé ?

R : Utilisez la commande **`rhn_package_manager -l -c "nom_du_canal_privé"`** pour répertorier les paquetages du canal privé connus par le Satellite. Vous pouvez également vous rendre sur l'interface Satellite.

Après avoir abonné un système enregistré au canal privé, vous pouvez également exécuter la commande **`yum --disablerepo="*" --enablerepo="your_repo_name" list available`** sur le système enregistré et rechercher les paquetages du canal Satellite privé.

Q : Comment puis-je déterminer si les clients se connectent au serveur Squid?

R : Le fichier **`/var/log/squid/access.log`** journalise toutes les connexions au serveur Squid.

Q : L'agent de mise à jour « Red Hat Update Agent » sur les systèmes client ne se connecte pas via Red Hat Satellite Proxy. Comment puis-je résoudre cette erreur ?

R : Assurez-vous que la dernière version de Red Hat Update Agent soit installée sur les systèmes client. La dernière version contient les fonctionnalités nécessaires pour se connecter via Red Hat Satellite Proxy. La dernière version peut être obtenue à partir de Red Hat Network en lançant la

Red Hat Satellite Proxy est une extension d'Apache. Consultez la section *Fichiers journaux* du *Guide d'installation Red Hat Satellite Proxy* pour obtenir l'emplacement de son fichier journal.

Q : La configuration de mon proxy Red Hat Satellite Proxy ne fonctionne pas. Par où dois-je commencer pour résoudre le problème ?

R : Assurez-vous que **`/etc/sysconfig/rhn/systemid`** appartient à root.apache avec les permissions 0640.

Veuillez lire les fichiers journeaux. Une liste est disponible dans la section *Fichiers journaux* du *Guide d'installation Red Hat Satellite Proxy*.

Q : Comment résoudre les problèmes généraux de Red Hat Satellite Proxy ?

R : Pour commencer la résolution de problèmes généraux, veuillez examiner le ou les fichiers journaux associés au composant présentant des échecs.

Un problème commun est l'espace de disque plein. Un signe pratiquement sûr de ce problème est l'apparence d'écriture arrêtée dans les fichiers journaux. Si la journalisation s'est arrêtée durant une écriture, comme un mot à moitié écrit, il est probable que vos disques sont pleins. Pour confirmer cela, exécutez la commande suivante et vérifiez les pourcentages dans la colonne :

```
df -h
```

En outre des fichiers journaux, vous pouvez obtenir des informations de valeur en obtenant le statut de vos divers composants. Cette opération peut être effectuée pour le serveur web Apache et Squid.

Pour obtenir le statut du serveur web Apache, exécutez la commande suivante :

```
service httpd status
```

Pour obtenir le statut de Squid, exécutez la commande suivante :

```
service squid status
```

Si l'administrateur ne reçoit pas de courrier électronique provenant du proxy Red Hat Satellite, confirmez que les bonnes adresses électroniques ont été définies pour **`traceback_mail`** dans **`/etc/rhn/rhn.conf`**.

Q : Mon proxy Red Hat Satellite Proxy a rencontré l'erreur "Host Not Found"/"Could not Determine FQDN" (hôte introuvable/Impossible de déterminer le nom de domaine complet). Que dois-je faire ?

R : Comme les fichiers de configuration de RHN dépendent exclusivement de noms de domaine entièrement qualifiés (ou FQDN), il est impératif que les applications clés puissent résoudre le nom de Red Hat Satellite Proxy en une adresse IP. L'agent Red Hat Update Agent, le client d'enregistrement Red Hat Network Registration Client et le serveur web Apache sont

particulièrement sujets à ce problème avec les applications Red Hat Network produisant des erreurs « host not found » (hôte introuvable) et le serveur Web indiquant « Could not determine the server's fully qualified domain name » (impossible de déterminer le nom de domaine complet du serveur) lors de l'échec du démarrage.

Ce problème provient du fichier **/etc/hosts**. Vous pouvez confirmer ceci en examinant le fichier **/etc/nsswitch.conf**, qui définit les méthodes et l'ordre dans lequel les noms de domaine sont résolus. Normalement, le fichier **/etc/hosts** est vérifié en premier, suivi par le NIS (Network Information Service), s'il est utilisé, puis par le DNS. L'un d'eux doit réussir pour que le serveur Web Apache démarre et que les applications client de Red Hat Network fonctionnent.

Pour résoudre ce problème, identifiez le contenu du fichier **/etc/hosts**. Il peut ressembler à l'exemple suivant :

```
127.0.0.1 this_machine.example.com this_machine localhost.localdomain
\ localhost
```

Dans un éditeur de texte, supprimez les informations de l'hôte de la machine du fichier, ceci devrait être similaire à :

```
127.0.0.1 localhost.localdomain.com localhost
```

Enregistrez le fichier et essayez d'exécuter à nouveau les applications client Red Hat Network ou le serveur Web Apache. Si elles échouent toujours, identifiez de manière explicite l'adresse IP du Proxy dans le fichier comme dans l'exemple suivant :

```
127.0.0.1 localhost.localdomain.com localhost
123.45.67.8 this_machine.example.com this_machine
```

Remplacez la valeur ici avec l'adresse IP actuelle du Proxy. Le problème devrait ainsi être résolu. Souvenez-vous que si l'adresse IP spécifique est stipulée, le fichier devra être mis à jour lorsque la machine obtient une nouvelle adresse.

Q : J'ai des problèmes avec Red Hat Satellite Proxy et des erreurs de connexion réseau. Que dois-je faire ?

R : Si vous rencontrez des problèmes et que vous pensez qu'ils sont associés aux connexions échouées, suivez les mesures suivantes :

Confirmez que le bon paquetage :

```
rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm
```

est installé sur Red Hat Satellite Proxy et le fichier **rhn-org-trusted-ssl-cert-*.noarch.rpm** correspondant ou le certificat SSL CA (client) public brut est installé sur tous les systèmes client.

Vérifiez que les systèmes client sont configurés de façon à utiliser le certificat approprié.

Si vous utilisez un ou plusieurs proxy Red Hat Satellite, assurez-vous que les certificats SSL de chaque proxy sont préparés correctement. Si vous utilisez Red Hat Satellite Proxy en conjonction avec Red Hat Satellite, le proxy devrait avoir sa propre paire de clés SSL

de serveur et son propre certificat CA SSL public (client) installés, vu qu'il servira dans les deux fonctions. Reportez-vous au chapitre sur les certificats SSL du *Guide de configuration du client Red Hat Satellite* pour obtenir des instructions spécifiques.

Si Red Hat Satellite Proxy se connecte via un proxy HTTP, assurez-vous que l'URL répertorié est valide. Par exemple, le champ URL du proxy HTTP ne devrait pas contenir de références aux protocoles, comme par exemple http:// ou https://. Seuls le nom d'hôte et le port devraient être inclus sous la forme nom d'hôte:port, par exemple **`votre-passerelle.exemple.com:8080`**.

Assurez-vous que les systèmes client n'utilisent pas leurs propres pare-feu bloquant ainsi les ports requis, comme l'identifie la section *Conditions préalables supplémentaires* du *Guide d'installation Red Hat Satellite Proxy*.

Q : J'ai des problèmes avec des erreurs de livraison de paquetages et la corruption d'objets. Que dois-je vérifier ?

R : Si la livraison de paquetages échoue ou qu'un objet semble être corrompu et que ce problème n'est pas associé aux erreurs de connexion, vous devriez penser à vider les caches. Red Hat Satellite Proxy possède deux caches que vous devriez connaître : un pour Squid et l'autre pour l'authentification.

Le cache de Squid se situe dans **`/var/spool/squid/`**. Pour le vider :

1. Arrêter le serveur web Apache : **`service httpd stop`**
2. Arrêter le serveur Squid : **`service squid stop`**
3. Supprimer le contenu de ce répertoire : **`rm -fv /var/cache/rhn/*`**
4. Redémarrer les deux services :

```
service squid start
service httpd start
```

La même tâche peut être accomplie plus rapidement en vidant le répertoire et en redémarrant Squid, mais cette méthode résultera probablement en un grand nombre de message de traceback Red Hat Network.

Le mécanisme de cache interne utilisé pour l'authentification par le Proxy peut également nécessiter le nettoyage de son cache. Pour ce faire, exécutez la commande suivante :

```
rm -fv /var/cache/rhn/*
```

NOTE

Si vous avez épuisé ces étapes de résolution de problèmes ou que vous souhaitez les remettre à des professionnels de Red Hat Network, Red Hat recommande que vous utilisiez la puissante assistance offerte avec Red Hat Satellite. La manière la plus efficace

pour ce faire est de rassembler les paramètres de configuration, les fichiers journaux et les informations de bases de données de votre Satellite et d'envoyer ce paquetage directement à Red Hat.

RHN fournit un outil en ligne de commande explicitement dans ce but : l'outil **Satellite Diagnostic Info Gatherer** (rassembleur d'informations de diagnostique du Satellite), plus couramment connu par sa commande **`satellite-debug`**. Pour utiliser cet outil, exécutez simplement cette commande en tant que super-utilisateur. Vous verrez les informations recueillies et le fichier tarball créé comme dans l'exemple suivant :

```
# satellite-debug
Collecting and packaging relevant diagnostic information.
Warning: this may take some time...
    * copying configuration information
    * copying logs
    * querying RPM database (versioning of Red Hat Satellite,
etc.)
    * querying schema version and database character sets
    * get diskspace available
    * timestamping
    * creating tarball (may take some time): /tmp/satellite-
debug.tar.bz2
    * removing temporary debug tree

Debug dump created, stored in /tmp/satellite-debug.tar.bz2
Deliver the generated tarball to your Red Hat Network contact
or support channel.
```

Une fois terminé, envoyez par courrier électronique le nouveau fichier du répertoire **`/tmp/`** à votre représentant Red Hat pour un diagnostique immédiat.

De plus, Red Hat fournit un outil de ligne de commande nommé **SoS Report**, plus couramment connu par sa commande **`sosreport`**. Cet outil réunit vos paramètres de configuration du proxy, les fichiers de journalisation et les informations des bases de données, puis les envoie directement à Red Hat.

Pour utiliser cet outil pour les informations Red Hat Satellite, le paquetage **`sos`** doit être installé. Tapez **`sosreport -o rhn`** en tant que root sur le serveur Satellite pour créer un rapport. Par exemple :

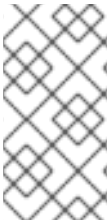
```
[root@satserver ~]# sosreport -o rhn

sosreport (version 1.7)

This utility will collect some detailed  information about the
hardware and  setup of your  Red Hat Enterprise Linux  system.
The information is collected and an archive is  packaged under
/tmp, which you can send to a support representative.
Red Hat will use this information for diagnostic purposes ONLY
and it will be considered confidential information.

This process may take a while to complete.
No changes will be made to your system.

Press ENTER to continue, or CTRL-C to quit.
```



Vous êtes alors invité à donner votre première initiale et votre nom de famille, puis le numéro du cas de support (qui s'intitule également un numéro de traçage).

Il se peut que le système mette plusieurs minutes à générer et archiver le rapport en fichier compressé. Une fois terminé, envoyez par courrier électronique le nouveau fichier du répertoire **/tmp/** à votre représentant Red Hat pour un diagnostique immédiat.

ANNEXE A. SONDES

Les systèmes ayant des droits d'accès Monitoring peuvent avoir des sondes qui leur sont appliquées pour constamment confirmer leur santé et leur efficacité opérationnelle complète. Cette section répertorie les sondes disponibles par groupes de commandes, comme Apache.

De nombreuses sondes qui contrôlent les aspects internes de vos systèmes (comme la sonde Linux::Disk Usage) au lieu des aspects externes (comme la sonde Network Services::SSH) requièrent l'installation du démon de contrôle (Monitoring) Red Hat Network (**`rhnmd`**). Ce pré-requis est noté dans la référence de la sonde individuelle.

Chaque sonde a sa propre référence dans cette section qui identifie les champs requis (marqués par un *), les valeurs par défaut et les limites qui peuvent être définies pour déclencher des alertes. De manière similaire, le début de la section de chaque groupe de commandes contient les informations applicables à toutes les sondes de ce groupe. Les directives générales sont présentées dans la Section A.1, « Directives sur les sondes ». Les autres sections examinent les sondes individuelles.

NOTE

Presque toutes les sondes utilisent le protocole TCP (*Transmission Control Protocol*) comme protocole de transport. Toute exception est notée dans les références de la sonde individuelle.

A.1. DIRECTIVES SUR LES SONDES

Les directives générales suivantes soulignent la signification de chaque état de sonde et fournissent un guide pour définir les limites de vos sondes.

La liste suivante fournit une brève description de la signification de chaque état de sonde :

Inconnu

Les sondes qui ne peuvent pas recueillir les métriques nécessaires pour déterminer l'état de sonde. La plupart des sondes (mais pas toutes) passent dans cet état lorsqu'elles dépassent leur délai de d'attente. Les sondes dans cet état peuvent également être configurées incorrectement.

Pending (en attente)

Les sondes dont les données n'ont pas été reçues par Red Hat Satellite. Il est normal que les nouvelles sondes soient dans cet état. Cependant, si toutes les sondes passent dans cet état, l'infrastructure de contrôle peut être sur le point d'échouer.

Valider

Les sondes qui ont été exécutées sans erreur. Cet état est l'état désiré pour toutes les sondes.

Avertissement

Les sondes ont dépassé leur seuil d'avertissement (WARNING).

Critique

Les sondes qui ont dépassé leurs limites CRITICAL ou qui ont atteint un statut critique par d'autres moyens (certaines sondes deviennent critiques lors du dépassement de leur délai d'attente).

Lors de l'ajout de sondes, sélectionnez des limites significatives qui, lorsqu'elles sont dépassées, vous

avertissent vous et vos administrateur de tout problème au sein de votre infrastructure. Les délais d'attente sont normalement saisis en secondes. Des exceptions à ces règles sont notées dans les références des sondes individuelles.

IMPORTANT

Certaines sondes ont des limites basées sur le temps. Afin que des limites comme CRITICAL et WARNING fonctionnent comme prévu, leurs valeurs ne peuvent pas dépasser la durée de temps allouée au délai d'attente. Sinon, un statut UNKNOWN sera renvoyé dans tous les cas de latence étendue, annulant de cette façon les limites. Pour cette raison, Red Hat recommande fortement de vous assurer que les périodes de délai dépassent toutes les limites de temps.

Exécutez vos sondes sans notifications pendant un moment pour établir la performance de base pour chacun de vos systèmes. Bien que les valeurs par défaut fournies pour les sondes peuvent convenir à vos besoins, chaque organisation possède un environnement différent pouvant nécessiter la modification des limites.

A.2. APACHE 1.3.X ET 2.0.X

Les sondes de cette section peuvent être appliquées à des instances du serveur web Apache. Bien que les valeurs par défaut supposent que vous appliquerez ces sondes utilisant HTTP standard, vous pouvez également les utiliser sur des connexions sécurisées en changeant le protocole d'application par **`https`** et le port par **443**.

A.2.1. Apache::Processes

La sonde Apache::Processes contrôle les processus exécutés sur un serveur web Apache et recueille les métriques suivantes :

- Données transférées par enfant - Enregistre les informations de transfert de données concernant les enfants individuels. Un processus enfant est un processus qui est créé à partir d'un autre processus ou du processus parent.
- Données transférées par emplacement - La quantité cumulative de données transférées par un processus enfant qui redémarre. Le nombre d'emplacements est configuré dans le fichier **`httpd.conf`** à l'aide du paramètre **`MaxRequestsPerChild`**.

La directive **`ExtendedStatus`** dans le fichier **`httpd.conf`** du serveur web doit avoir la valeur **`On`** pour que cette sonde fonctionne correctement.

Tableau A.1. Paramètres de Apache::Processes

Champ	Valeur
Application Protocol*	http
Port*	80
Pathname* (nom de chemin)	/server-status
UserAgent* (agent d'utilisateur)	NOCpulse-ApacheUptime/1.0

Champ	Valeur
Nom d'utilisateur	
Mot de passe	
Timeout* (délai d'attente)	15
Critical Maximum Megabytes Transferred Per Child (méga-octets transférés par enfant maximum pour le statut critical)	
Warning Maximum Megabytes Transferred Per Child (méga-octets transférés par enfant maximum pour le statut warning)	
Critical Maximum Megabytes Transferred Per Slot (méga-octets transférés par slot maximum pour le statut critical)	
Warning Maximum Megabytes Transferred Per Slot (méga-octets transférés par slot maximum pour le statut warning)	

A.2.2. Apache::Traffic

La sonde Apache::Traffic contrôle les requêtes exécutées sur un serveur web Apache et recueille les métriques suivantes :

- Requêtes actuelles - Nombre de requêtes traitées par le serveur lors de l'exécution de sondes.
- Taux de requêtes - Les accès au serveur par seconde depuis l'exécution de la dernière sonde.
- Traffic - Les kilooctets par seconde de trafic que le serveur a traités depuis l'exécution de la dernière sonde.

La directive **`ExtendedStatus`** dans le fichier **`httpd.conf`** du serveur web doit avoir la valeur **`On`** pour que cette sonde fonctionne correctement.

Tableau A.2. Paramètres de Apache::Traffic

Champ	Valeur
Application Protocol*	http
Port*	80
Pathname* (nom de chemin)	/server-status
UserAgent* (agent d'utilisateur)	NOCpulse-ApacheUptime/1.0
Nom d'utilisateur	

Champ	Valeur
Mot de passe	
Timeout* (délai d'attente)	15
Critical Maximum Current Requests (nombre de requêtes courantes maximum pour le statut critical)	
Warning Maximum Current Requests (nombre de requêtes courantes maximum pour le statut warning)	
Critical Maximum Request Rate (taux de requêtes maximum pour le statut critical, événements par seconde)	
Warning Maximum Request Rate (taux de requêtes maximum pour le statut warning, événements par seconde)	
Critical Maximum Traffic (trafic maximum pour le statut critical, kilo-octets par seconde)	
Warning Maximum Traffic (trafic maximum pour le statut warning, kilo-octets par seconde)	

A.2.3. Apache::Uptime

La sonde Apache::Uptime stocke les durées de temps cumulatives depuis le dernier démarrage du serveur web. Aucune métrique n'est recueillie par cette sonde, qui est conçue pour aider à suivre les contrats de niveau de services (SLA, de l'anglais service level agreements).

Tableau A.3. Paramètres de Apache::Uptime

Champ	Valeur
Application Protocol*	http
Port*	80
Pathname* (nom de chemin)	/server-status
UserAgent* (agent d'utilisateur)	NOCpulse-ApacheUptime/1.0
Nom d'utilisateur	
Mot de passe	
Timeout* (délai d'attente)	15

A.3. BEA WEBLOGIC 6.X ET VERSION SUPÉRIEURE

Les sondes de cette section (à part JDBC Connection Pool) peuvent être configurées de façon à contrôler les propriétés de tout serveur BEA WebLogic 6.x et toute version supérieure (d'administration ou géré) exécuté sur un hôte donné, même dans un environnement de clusters. Le contrôle d'un cluster est accompli en envoyant toutes les requêtes SNMP au serveur d'administration du domaine, puis en interrogeant ses serveurs gérés pour des données individuelles.

Afin d'obtenir ce niveau supérieur de granularité, le paramètre **`BEA Domain Admin Server`** (serveur d'administration du domaine BEA) doit être utilisé pour faire la différence entre le serveur d'administration qui reçoit des requêtes SNMP et le serveur géré exécutant la sonde spécifiée. Si l'hôte à sonder est le serveur d'administration, alors le paramètre **`BEA Domain Admin Server`** peut être laissé vierge et uniquement les requêtes SNMP et la sonde lui seront envoyés.

Si l'hôte à sonder est le serveur géré, alors l'adresse IP du serveur d'administration devrait être fourni dans le paramètre **`BEA Domain Admin Server`** et le nom du serveur géré devrait être inclus dans le paramètre **`BEA Server Name`** et ajouté à la fin du champ **`SNMP Community String`** (chaîne de communauté SNM). Les requêtes SNMP sont alors envoyées à l'hôte du serveur d'administration, comme requis, mais redirige la sonde spécifique sur l'hôte du serveur géré.

Vous devriez également noter que la chaîne de communauté nécessaire à l'exécution de sondes sur les hôtes de serveur géré devrait être sous la forme **`préfixe_communauté@nom_serveur_géré`** afin que la requête SNMP retourne des résultats pour le serveur géré souhaité. Finalement, SNMP doit être activé sur chaque système contrôlé. La prise en charge SNMP doit être activée et configurée via la console WebLogic.

Veuillez consulter la documentation incluse avec votre serveur BEA ou les informations sur le site web BEA pour obtenir davantage de détails sur les conventions d'attribution de noms de chaîne de la communauté BEA.

A.3.1. BEA WebLogic::Execute Queue

La sonde BEA WebLogic::Execute Queue contrôle la file d'attente d'exécution de WebLogic et fournit les métriques suivantes :

- Threads d'exécution inactifs - Nombre de threads d'exécution dans un état inactif.
- Longueur de la file d'attente - Nombre de requêtes dans la file d'attente.
- Taux de requêtes - Nombre de requêtes par seconde.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.4. Paramètres de BEA WebLogic::Execute Queue

Champ	Valeur
SNMP Community String* (chaîne de communauté SNMP)	public
SNMP Port*	161
SNMP Version*	1

Champ	Valeur
BEA Domain Admin Server (serveur d'administration de domaine BEA)	
BEA Server Name* (nom du serveur BEA)	myserver
Queue Name* (nom de file d'attente)	défaut
Critical Maximum Idle Execute Threads (threads d'exécution inactifs maximum pour le statut critical)	
Warning Maximum Idle Execute Threads (threads d'exécution inactifs maximum pour le statut warning)	
Critical Maximum Queue Length (longueur de file d'attente maximum pour le statut critical)	
Warning Maximum Queue Length (longueur de file d'attente maximum pour le statut warning)	
Critical Maximum Request Rate (taux de requêtes maximum pour le statut critical)	
Warning Maximum Request Rate (taux de requêtes maximum pour le statut warning)	

A.3.2. BEA WebLogic::Heap Free

La sonde BEA webLogic::Heap Free recueille les métriques suivantes :

- Heap Free (Tas libre) - Pourcentage d'espace de tas libre.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.5. Paramètres de BEA webLogic::Heap Free

Champ	Valeur
SNMP Community String* (chaîne de communauté SNMP)	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server (serveur d'administration de domaine BEA)	
BEA Server Name* (nom du serveur BEA)	myserver

Champ	Valeur
Critical Maximum Heap Free (tas libre maximum pour le statut critical)	
Warning Maximum Heap Free (tas libre maximum pour le statut warning)	
Warning Minimum Heap Free (tas libre minimum pour le statut warning)	
Critical Minimum Heap Free (tas libre minimum pour le statut critical)	

A.3.3. BEA webLogic::JDBC Connection Pool

La sonde BEA webLogic::JDBC Connection Pool contrôle le groupement JDBC (Java Database Connection) uniquement sur un serveur d'administration de domaine (aucun serveur géré) et recueille les métriques suivantes :

- Connections - Nombre de connexions au JDBC.
- Connection Rate - La vitesse à laquelle les connexions sont effectuées sur le JDBC, mesurée en connexions par seconde.
- Waiter - Le nombre de sessions en attente de connexions au JDBC.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.6. Paramètres de BEA webLogic::JDBC Connection Pool

Champ	Valeur
SNMP Community String* (chaîne de communauté SNMP)	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server (serveur d'administration de domaine BEA)	
BEA Server Name* (nom du serveur BEA)	myserver
JDBC Pool Name* (nom de groupement JDBC)	MyJDBC Connection Pool (groupement de connexions MyJDBC)
Critical Maximum Connections (connexions maximum pour le statut critical)	

Champ	Valeur
Warning Maximum Connections (connexions maximum pour le statut warning)	
Critical Maximum Connection Rate (taux de connexion maximum pour le statut critical)	
Warning Maximum Connection Rate (taux de connexion maximum pour le statut warning)	
Critical Maximum Waiters (sessions en attente maximum pour le statut critical)	
Warning Maximum Waiters (sessions en attente maximum pour le statut warning)	

A.3.4. BEA webLogic::Server State

La sonde BEA webLogic::Server State contrôle l'état courant d'un serveur web BEA webLogic. Si la sonde ne peut pas se connecter au serveur, un statut CRITICAL en résulte.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.7. Paramètres de BEA webLogic::Server State

Champ	Valeur
SNMP Community String* (chaîne de communauté SNMP)	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server (serveur d'administration de domaine BEA)	
BEA Server Name* (nom du serveur BEA)	

A.3.5. BEA webLogic::Servlet

La sonde BEA webLogic::Servlet contrôle la performance d'un servlet particulier déployé sur un serveur webLogic et recueille les métriques suivantes :

- High Execution Time - La plus longue durée, en millisecondes, de temps pris pour l'exécution du servlet depuis le démarrage du système.
- Low Execution Time - La plus courte durée, en millisecondes, de temps pris pour l'exécution du servlet depuis le démarrage du système.

- Execution Time Moving Average - Une moyenne changeante du temps d'exécution.
- Execution Time Average - Une moyenne standard du temps d'exécution.
- Reload Rate - Le nombre de fois que le servlet spécifié est rechargé par minute.
- Invocation Rate - Le nombre de fois que le servlet spécifié est invoqué par minute.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.8. Paramètres de BEA webLogic::Servlet

Champ	Valeur
SNMP Community String* (chaîne de communauté SNMP)	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server (serveur d'administration de domaine BEA)	
BEA Server Name* (nom du serveur BEA)	myserver
Servlet Name* (nom du servlet)	
Critical Maximum High Execution Time (temps haut d'exécution maximum pour le statut critical)	
Warning Maximum High Execution Time (temps haut d'exécution maximum pour le statut warning)	
Critical Maximum Execution Time Moving Average (moyenne changeable du temps d'exécution maximum pour le statut critical)	
Warning Maximum Execution Time Moving Average (moyenne changeable du temps d'exécution maximum pour le statut warning)	

A.4. GÉNÉRAL

Les sondes de cette section sont conçues pour contrôler les aspects de base de vos systèmes. Lorsque vous les appliquez, assurez-vous que leurs limites de temps ne dépassent pas la durée de temps allouée à la période de délai d'attente. Sinon, la sonde retourne un statut UNKNOWN dans tous les cas de latence étendue, annulant ainsi les limites.

A.4.1. General::Remote Program

La sonde General::Remote Program vous permet d'exécuter toute commande ou tout script sur votre système et d'obtenir une chaîne de statut. Notez que le message résultant sera limité à 1024 octets.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.9. Paramètres de General::Remote Program

Champ	Valeur
Command*	
OK Exit Status* (statut de sortie OK)	0
Warning Exit Status* (statut de sortie Warning)	1
Critical Exit Status* (statut de sortie Critical)	2
Timeout	15

A.4.2. General::Remote Program with Data

La sonde General::Remote Program with Data vous permet d'exécuter toute commande ou tout script sur votre système et d'obtenir une valeur, ainsi qu'une chaîne de statut. Pour utiliser cette sonde, vous devez inclure du code XML dans le corps de votre script. Cette sonde prend en charge les balises XML suivantes :

- <perldata> </perldata>
- <hash> </hash>
- <item key =" "> </item>

Le programme à distance devra envoyé des itérations du code suivant à la commande **STDOUT** :

```
<perldata> <hash> <item
key="data">10</item> <item
key="status_message">status message here</item>
</hash> </perldata>
```

La valeur requise pour **data** est le point de données à insérer dans la base de données pour la famille "time-series". L'option **status_message** est facultative et peut avoir la valeur de toute chaîne de texte désirée avec une longueur maximum de 1024 octets. Les programmes à distance qui n'incluent pas une option **status_message** rapporteront quand même la valeur et le statut retournés.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde. XML est sensible à la casse. Le nom de l'élément clé **data** ne peut pas être modifié et doit recueillir un nombre comme valeur.

Tableau A.10. Paramètres de General::Remote Program with Data

Champ	Valeur
Command*	
OK Exit Status* (statut de sortie OK)	0
Warning Exit Status* (statut de sortie Warning)	1
Critical Exit Status* (statut de sortie Critical)	2
Timeout	15

A.4.3. General::SNMP Check

La sonde General::SNMP Check teste votre serveur SNMP en spécifiant un seul identificateur d'objet (OID, de l'anglais object identifier) en notation à points (comme par exemple **`1.3.6.1.2.1.1.1.0`**) et une limite associée à la valeur renvoyée. Elle recueille les métriques suivantes :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur SNMP réponde à une requête de connexion.

Conditions préalables - SNMP doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde. Seuls les entiers peuvent être utilisés pour les valeurs de limites.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.11. Paramètres de General::SNMP Check

Champ	Valeur
SNMP OID*	
SNMP Community String* (chaîne de communauté SNMP)	public
SNMP Port*	161
SNMP Version*	2
Timeout* (délai d'attente)	15
Critical Maximum Value (valeur maximum pour le statut critical)	
Warning Maximum Value (valeur maximum pour le statut warning)	
Warning Minimum Value (valeur minimum pour le statut warning)	

Champ	Valeur
Critical Minimum Value (valeur minimum pour le statut critical)	

A.4.4. General::TCP Check

La sonde General::TCP Check teste votre serveur TCP en vérifiant qu'il peut se connecter à un système via le numéro de port spécifié. Elle recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur TCP réponde à une requête de connexion.

La sonde passe la chaîne spécifiée dans le champ **Send** lors de la connexion. La sonde anticipe une réponse du système, qui devrait inclure la sous-chaîne spécifiée dans le champ **`Expect`**. Si la chaîne attendue n'est pas trouvée, la sonde retourne un statut CRITICAL.

Tableau A.12. Paramètres de General::TCP Check

Champ	Valeur
Send	
Expect	
Port*	1
Timeout* (délai d'attente)	10
Critical Maximum Latency (latence maximum pour le statut critical)	
Warning Maximum Latency (latence maximum pour le statut warning)	

A.4.5. General::UDP Check

La sonde General::UDP Check teste votre serveur UDP en vérifiant qu'il peut se connecter à un système via le numéro de port spécifié. Elle recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur UDP réponde à une requête de connexion.

La sonde passe la chaîne spécifiée dans le champ **Send** lors de la connexion. La sonde anticipe une réponse du système, qui devrait inclure la sous-chaîne spécifiée dans le champ **`Expect`**. Si la chaîne attendue n'est pas trouvée, la sonde retourne un statut CRITICAL.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.13. Paramètres de General::UDP Check

Champ	Valeur
Port*	1
Send	
Expect	
Timeout* (délai d'attente)	10
Critical Maximum Latency (latence maximum pour le statut critical)	
Warning Maximum Latency (latence maximum pour le statut warning)	

A.4.6. General::Uptime (SNMP)

La sonde General::Uptime (SNMP) enregistre la durée de temps depuis le dernier démarrage du périphérique. Elle utilise l'identificateur d'objet (OID) SNMP pour obtenir cette valeur. Le seul statut d'erreur qu'elle retournera est UNKNOWN.

Conditions préalables - SNMP doit être en cours d'exécution sur le système contrôlé et l'accès à l'OID doit être activé pour pouvoir exécuter cette sonde.

Le protocole de transport de cette sonde est UDP (User Datagram Protocol).

Tableau A.14. Paramètres de General::Uptime (SNMP)

Champ	Valeur
SNMP Community String* (chaîne de communauté SNMP)	public
SNMP Port*	161
SNMP Version*	2
Timeout* (délai d'attente)	15

A.5. LINUX

Les sondes de cette section contrôlent les aspects essentiels de vos systèmes Linux, de l'utilisation du CPU à la mémoire virtuelle. Appliquez les aux systèmes à mission critique pour être averti avant un échec.

Contrairement aux autres groupes de sondes, qui peuvent nécessiter le démon de contrôle (Monitoring) Red Hat Network ou non, chaque sonde Linux nécessite que **`rhnmd`** soit en cours d'exécution sur le système contrôlé.

A.5.1. Linux::CPU Usage

La sonde Linux::CPU Usage contrôle l'utilisation de CPU sur un système et recueille les métriques suivantes :

- CPU Percent Used - La moyenne en cinq secondes du pourcentage de l'utilisation de CPU au moment de l'exécution de la sonde.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.15. Paramètres de Linux::CPU Usage

Champ	Valeur
Timeout* (délai d'attente)	15
Critical Maximum CPU Percent Used (pourcentage de CPU utilisé maximum pour le statut critical)	
Warning Maximum CPU Percent Used (pourcentage de CPU utilisé maximum pour le statut warning)	

A.5.2. Linux::Disk IO Throughput

La sonde Linux::Disk IO Throughput contrôle un disque donné et recueille les métriques suivantes :

- Read Rate - La quantité de données qui est lue en kilo-octets par seconde.
- Write Rate - La quantité de données qui est écrite en kilo-octets par seconde.

Pour obtenir la valeur pour le champ **Disk number or disk name** (numéro ou nom de disque), exécutez **iostat** sur le système à contrôler et regardez quel nom a été assigné au disque que vous souhaitez. La valeur par défaut de **0** vous donne normalement des statistiques du premier disque dur connecté directement au système.

Conditions préalables - Le démon de contrôle (Monitoring) Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde. Le paramètre **Disk number or disk name** (numéro ou nom du disque) doit également correspondre au format utilisé lorsque la commande **iostat** est exécutée. Si le format n'est pas identique, la sonde configurée passe dans un état UNKNOWN.

Tableau A.16. Paramètres de Linux::Disk IO Throughput

Champ	Valeur
Disk number or disk name*	0
Timeout* (délai d'attente)	15
Critical Maximum KB read/second (Ko lus par seconde maximum pour le statut critical)	

Champ	Valeur
Warning Maximum KB read/second (Ko lus par seconde maximum pour le statut warning)	
Warning Minimum KB read/second (Ko lus par seconde minimum pour le statut warning)	
Critical Minimum KB read/second (Ko lus par seconde minimum pour le statut critical)	
Critical Maximum KB written/second (Ko écrits par seconde maximum pour le statut critical)	
Warning Maximum KB written/second (Ko écrits par seconde maximum pour le statut warning)	
Warning Minimum KB written/second (Ko écrits par seconde minimum pour le statut warning)	
Critical Minimum KB written/second (Ko écrits par seconde minimum pour le statut critical)	

A.5.3. Linux::Disk Usage

La sonde Linux::Disk Usage contrôle l'espace disque sur un système de fichiers spécifique et recueille les métriques suivantes :

- File System Used - Le pourcentage de système de fichiers actuellement en utilisation.
- File System Used - La quantité du système de fichiers en méga-octets actuellement en utilisation.
- Space Available - La quantité du système de fichiers en méga-octets actuellement disponible.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.17. Paramètres de Linux::Disk Usage

Champ	Valeur
File system*	/dev/hda1
Timeout* (délai d'attente)	15
Critical Maximum File System Percent Used (pourcentage utilisé de système de fichiers maximum pour le statut critical)	

Champ	Valeur
Warning Maximum File System Percent Used (pourcentage utilisé de système de fichiers maximum pour le statut warning)	
Critical Maximum Space Used (espace utilisé maximum pour le statut critical)	
Warning Maximum Space Used (espace utilisé maximum pour le statut warning)	
Warning Minimum Space Available (espace disponible minimum pour le statut warning)	
Critical Minimum Space Available (espace disponible minimum pour le statut critical)	

A.5.4. Linux::Inodes

La sonde Linux::Inodes contrôle le système de fichiers spécifié et recueille les métriques suivantes :

- Inodes - Le pourcentage d'inodes actuellement en utilisation.

Une inode est une structure de données contenant des informations sur les fichiers dans un système de fichiers Linux. Il existe une inode pour chaque fichier et un fichier est identifié uniquement par le système de fichiers sur lequel il se trouve et son numéro d'inode sur ce système.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.18. Paramètres de Linux::Inodes

Champ	Valeur
File system*	/
Timeout* (délai d'attente)	15
Critical Maximum Inodes Percent Used (pourcentage d'inodes utilisé maximum pour le statut critical)	
Warning Maximum Inodes Percent Used (pourcentage d'inodes utilisé maximum pour le statut warning)	

A.5.5. Linux::Interface Traffic

La sonde Linux::Interface Traffic mesure la quantité de trafic entrant et sortant de l'interface spécifiée (comme eth0) et recueille les métriques suivantes :

- Input Rate - Le trafic par seconde, en octets, entrant dans l'interface spécifiée.
- Output Rate - Le trafic par seconde, en octets, sortant de l'interface spécifiée.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.19. Paramètres de Linux::Interface Traffic

Champ	Valeur
Interface*	
Timeout* (délai d'attente)	30
Critical Maximum Input Rate (taux d'entrée maximum pour le statut critical)	
Warning Maximum Input Rate (taux d'entrée maximum pour le statut warning)	
Warning Minimum Input Rate (taux d'entrée minimum pour le statut warning)	
Critical Minimum Input Rate (taux d'entrée minimum pour le statut critical)	
Critical Maximum Output Rate (taux de sortie maximum pour le statut critical)	
Warning Maximum Output Rate (taux de sortie maximum pour le statut warning)	
Warning Minimum Output Rate (taux de sortie minimum pour le statut warning)	
Critical Minimum Output Rate (taux de sortie minimum pour le statut critical)	

A.5.6. Linux::Load

La sonde Linux::Load contrôle le CPU d'un système et recueille les métriques suivantes :

- Load - La charge moyenne sur le CPU du système sur diverses périodes de temps.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.20. Paramètres de Linux::Load

Champ	Valeur
Timeout* (délai d'attente)	15
Critical CPU Load 1-minute average (moyenne en 1 minute de charge de CPU pour le statut critical)	
Warning CPU Load 1-minute average (moyenne en 1 minute de charge de CPU pour le statut warning)	
Critical CPU Load 5-minute average (moyenne en 5 minutes de charge de CPU pour le statut critical)	
Warning CPU Load 5-minute average (moyenne en 5 minutes de charge de CPU pour le statut warning)	
Critical CPU Load 15-minute average (moyenne en 15 minutes de charge de CPU pour le statut critical)	
Warning CPU Load 15-minute average (moyenne en 15 minutes de charge de CPU pour le statut warning)	

A.5.7. Linux::Memory Usage

La sonde Linux::Memory Usage contrôle la mémoire sur un système et recueille les métriques suivantes :

- RAM Free - La quantité de mémoire vive (RAM) libre en méga-octets sur un système.

Vous pouvez également inclure la mémoire récupérable dans cette métrique en saisissant **yes** ou **no** dans le champ **Include reclaimable memory** (inclure la mémoire récupérable)

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.21. Paramètres de Linux::Memory Usage

Champ	Valeur
Include reclaimable memory (inclut la mémoire recouvrable)	non
Timeout* (délai d'attente)	15
Warning Maximum RAM Free (RAM libre maximum pour le statut warning)	
Critical Maximum RAM Free (RAM libre maximum pour le statut critical)	

A.5.8. Linux::Process Counts by State

La sonde Linux::Process Counts by State identifie le nombre de processus dans les états suivants :

- Blocked - Un processus qui est passé dans la file d'attente et dont l'état est passé sur **`waiting`**.
- Defunct - Un processus qui a été terminé (parce qu'il a été tué par un signal ou parce qu'il a appelé **`exit()`**) et dont le processus parent n'a pas encore reçu de notification de son arrêt en exécutant une forme de l'appel système **`wait()`**.
- Stopped - Un processus qui a été arrêté avant la fin de son exécution.
- Sleeping - Un processus qui est dans l'état de sommeil **`Interruptible`** et qui peut être réintroduit plus tard en mémoire, son exécution étant reprise à partir de son point d'arrêt.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.22. Paramètres de Linux::Process Counts by State

Champ	Valeur
Timeout* (délai d'attente)	15
Critical Maximum Blocked Processes (processus bloqués maximum pour le statut critical)	
Warning Maximum Blocked Processes (processus bloqués maximum pour le statut warning)	
Critical Maximum Defunct Processes (processus terminés maximum pour le statut critical)	
Warning Maximum Defunct Processes (processus terminés maximum pour le statut warning)	
Critical Maximum Stopped Processes (processus arrêtés maximum pour le statut critical)	
Warning Maximum Stopped Processes (processus arrêtés maximum pour le statut warning)	
Critical Maximum Sleeping Processes (processus endormis maximum pour le statut critical)	
Warning Maximum Sleeping Processes (processus endormis maximum pour le statut warning)	
Critical Maximum Child Processes (processus enfants maximum pour le statut critical)	

Champ	Valeur
Warning Maximum Child Processes (processus enfants maximum pour le statut warning)	

A.5.9. Linux::Process Count Total

La sonde Linux::Process Count Total contrôle un système et recueille les métriques suivantes :

- Process Count - Le nombre total de processus en cours d'exécution sur le système.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.23. Paramètres de Linux::Process Count Total

Champ	Valeur
Timeout* (délai d'attente)	15
Critical Maximum Process Count (compte de processus maximum pour le statut critical)	
Warning Maximum Process Count (compte de processus maximum pour le statut warning)	

A.5.10. Linux::Process Health

La sonde Linux::Process Health contrôle les processus spécifiés par l'utilisateur et recueille les métriques suivantes :

- CPU Usage - Le taux d'utilisation du CPU pour un processus donné en millisecondes par seconde. Cette métrique rapporte la colonne « Temps » de la sortie de **ps**, qui est le temps de CPU cumulé utilisé par le processus. Cela rend la métrique indépendante des intervalles de sonde, permet la définition de limites saines et génère des graphes utilisables (c-à-d, une pointe soudaine dans l'utilisation de CPU est affichée comme une pointe dans le graphe).
- Child Process Groups - Le nombre de processus enfants créés par le processus parent spécifié. Un processus enfant hérite de la plupart de ses attributs, comme les fichiers ouverts, de son parent.
- Threads - Le nombre de threads en cours d'exécution pour un processus donné. Un thread est l'unité de base de l'utilisation de CPU et comprend un compteur de programmes, un ensemble d'enregistrement et un espace de pile. Un thread est également appelé un processus léger.
- Physical Memory Used - La quantité de mémoire physique (ou RAM) en kilo-octets utilisée par le processus spécifié.
- Virtual Memory Used - La quantité de mémoire virtuelle en kilo-octets utilisée par le processus spécifié ou la taille du processus dans la mémoire réelle plus le swap.

Spécifiez le processus par son nom de commande ou son ID de processus (PID). La saisie d'un PID écrase la saisie d'un nom de commande. Si aucun nom de commande ou aucun PID n'est saisi, l'erreur « Command not found » (commande introuvable) est affichée et l'état de la sonde deviendra CRITICAL.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.24. Paramètres de Linux::Process Health

Champ	Valeur
Command Name (nom de commande)	
Process ID (PID) file (fichier PID)	
Timeout* (délai d'attente)	15
Critical Maximum CPU Usage (utilisation du CPU maximum pour le statut critical)	
Warning Maximum CPU Usage (utilisation du CPU maximum pour le statut warning)	
Critical Maximum Child Process Groups (groupes de processus enfants maximum pour le statut critical)	
Warning Maximum Child Process Groups (groupes de processus enfants maximum pour le statut warning)	
Critical Maximum Threads (threads maximum pour le statut critical)	
Warning Maximum Threads (threads maximum pour le statut warning)	
Critical Maximum Physical Memory Used (mémoire physique utilisée maximum pour le statut critical)	
Warning Maximum Physical Memory Used (mémoire physique utilisée maximum pour le statut warning)	
Critical Maximum Virtual Memory Used (mémoire virtuelle utilisée maximum pour le statut critical)	
Warning Maximum Virtual Memory Used (mémoire virtuelle utilisée maximum pour le statut warning)	

A.5.11. Linux::Process Running

La sonde Linux::Process Running vérifie que le processus spécifié fonctionne correctement. Elle compte les processus ou les groupes de processus selon si la case **`Count process groups`** (compter les groupes de processus) est sélectionnée.

Par défaut, la case est sélectionnée, indiquant ainsi que la sonde devrait compter le nombre de parents de groupes de processus indépendamment du nombre d'enfants. Cela vous permet, par exemple, de vérifier que deux instances du serveur web Apache sont exécutées sans se soucier du nombre (dynamique) de processus enfants. Si elle n'est pas sélectionnée, la sonde effectue un compte direct du nombre de processus (enfants et parents) correspondant au processus spécifié.

Spécifiez le processus par son nom de commande ou son ID de processus (PID). La saisie d'un PID écrase la saisie d'un nom de commande. Si aucun nom de commande ou aucun PID n'est saisi, l'erreur « Command not found » (commande introuvable) est affichée et l'état de la sonde deviendra CRITICAL.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.25. Paramètres de Linux::Process Running

Champ	Valeur
Command name	
fichier PID	
Compter les groupes de processus	(sélectionné)
Timeout* (délai d'attente)	15
Critical Maximum Number Running (nombre en cours d'exécution maximum pour le statut critical)	
Critical Minimum Number Running (nombre en cours d'exécution minimum pour le statut critical)	

A.5.12. Linux::Swap Usage

La sonde Linux::Swap Usage contrôle les partitions swap en cours d'exécution sur un système et rapporte la métrique suivante :

- Swap Free - Le pourcentage de mémoire swap actuellement libre.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.26. Paramètres de Linux::Swap Usage

Champ	Valeur
Timeout* (délai d'attente)	15

Champ	Valeur
Warning Minimum Swap Free (swap libre minimum pour le statut warning)	
Critical Minimum Swap Free (swap libre minimum pour le statut critical)	

A.5.13. Linux::TCP Connections by State

La sonde Linux::TCP Connections by State identifie le nombre total de connexions TCP, ainsi que la quantité de chacune dans les états suivants :

- TIME_WAIT - Le socket attend après la fermeture par commande d'arrêt à distance afin de pouvoir traiter les paquets qui sont toujours dans le réseau.
- CLOSE_WAIT - Le côté distant a été éteint et attend maintenant la fermeture du socket.
- FIN_WAIT - Le socket est fermé et la connexion est maintenant en train de fermer.
- ESTABLISHED - La connexion du socket est établie.
- SYN_RCVD - La requête de connexion a été reçue du réseau.

Cette sonde peut être utile pour trouver et isoler le trafic réseau pour des adresses IP spécifiques ou pour examiner les connexions réseau au système contrôlé.

Les paramètres de filtre pour la sonde vous permettent de rétrécir l'étendue de la sonde. Cette sonde utilise la commande **`netstat -ant`** pour recevoir des données. Les paramètres **`Local IP address`** et **`Local port`** utilisent des valeurs de la colonne **`Local Address`** de la sortie ; les paramètres **`Remote IP address`** et **`Remote port`** utilisent les valeurs de la colonne **`Foreign Address`** de la sortie pour tout rapport.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.27. Paramètres de Linux::TCP Connections by State

Champ	Valeur
Local IP address filter pattern list (liste de modèles de filtres d'adresses IP locales)	
Local port number filter (filtre de numéros de ports locaux)	
Remote IP address filter pattern list (liste de modèles de filtres d'adresses IP à distance)	
Remote port number filter (filtre de numéros de ports à distance)	

Champ	Valeur
Timeout* (délai d'attente)	15
Critical Maximum Total Connections (connexions totales maximum pour le statut critical)	
Warning Maximum Total Connections (connexions totales maximum pour le statut warning)	
Critical Maximum TIME_WAIT Connections (connexions TIME_WAIT maximum pour le statut critical)	
Warning Maximum TIME_WAIT Connections (connexions TIME_WAIT maximum pour le statut warning)	
Critical Maximum CLOSE_WAIT Connections (connexions CLOSE_WAIT maximum pour le statut critical)	
Warning Maximum CLOSE_WAIT Connections (connexions CLOSE_WAIT maximum pour le statut warning)	
Critical Maximum FIN_WAIT Connections (connexions FIN_WAIT maximum pour le statut critical)	
Warning Maximum FIN_WAIT Connections (connexions FIN_WAIT maximum pour le statut warning)	
Critical Maximum ESTABLISHED Connections (connexions ESTABLISHED maximum pour le statut critical)	
Warning Maximum ESTABLISHED Connections (connexions ESTABLISHED maximum pour le statut warning)	
Critical Maximum SYN_RCVD Connections (connexions SYN_RCVD maximum pour le statut critical)	
Warning Maximum SYN_RCVD Connections (connexions SYN_RCVD maximum pour le statut warning)	

A.5.14. Linux::Users

La sonde Linux::Users contrôle les utilisateurs d'un système et rapporte la métrique suivante :

- Users - Le nombre d'utilisateurs actuellement connectés.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.28. Paramètres de Linux::Users

Champ	Valeur
Timeout* (délai d'attente)	15
Critical Maximum Users (utilisateurs maximum pour le statut critical)	
Warning Maximum Users (utilisateurs maximum pour le statut warning)	

A.5.15. Linux::Virtual Memory

La sonde Linux::Virtual Memory contrôle la mémoire totale du système et recueille la métrique suivante :

- Virtual Memory - Le pourcentage de la mémoire totale du système - RAM plus swap - qui est libre.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.29. Paramètres de Linux::Virtual Memory

Champ	Valeur
Timeout* (délai d'attente)	15
Warning Minimum Virtual Memory Free (mémoire virtuelle libre minimum pour le statut warning)	
Critical Minimum Virtual Memory Free (mémoire virtuelle libre minimum pour le statut critical)	

A.6. LOGAGENT

Les sondes de cette section contrôlent les fichiers journaux sur vos systèmes. Vous pouvez les utiliser pour interroger les journaux sur certaines expressions et suivre les tailles de fichiers. Pour que les sondes LogAgent soient exécutées, l'utilisateur **`nocpulse`** doit posséder l'accès lecture sur vos fichiers journaux.

Notez que les données de la première exécution de ces sondes ne seront pas mesurées par rapport aux limites pour éviter de fausses notifications causées par des données de métriques incomplètes. Les mesures commenceront sur la deuxième exécution.

A.6.1. LogAgent::Log Pattern Match

La sonde LogAgent::Log Pattern Match utilise des expressions régulières pour trouver du texte situé au sein du fichier journal contrôlé et recueille les métriques suivantes :

- Regular Expression Matches - Le nombre de correspondances qui se sont produites depuis la dernière exécution de la sonde.
- Regular Expression Match Rate - Le nombre de correspondances par minute depuis la dernière exécution de la sonde.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde. Pour que cette sonde soit exécutée, l'utilisateur **nocpulse** doit posséder l'accès lecture sur vos fichiers journaux.

Outre le nom et l'emplacement du fichier journal à contrôler, vous devez fournir une expression régulière à comparer. L'expression doit être formatée pour **egrep**, qui est équivalent à **grep -E** et supporte les expressions régulières étendues. Ci-dessous figure l'ensemble d'expressions régulières pour **egrep** :

```
^ beginning of line
$ end of line
. match one char
* match zero or more chars
[] match one character set, e.g. '[Ff]oo'
[^] match not in set '[^A-F]oo'
+ match one or more of preceding chars
? match zero or one of preceding chars
| or, e.g. a|b
() groups chars, e.g., (foo|bar) or (foo)+
```

AVERTISSEMENT

N'incluez pas de guillemets simples (') dans l'expression. Sinon **egrep**échouera en silence et la sonde arrivera au bout de son délai.

Tableau A.30. Paramètres de LogAgent::Log Pattern Match

Champ	Valeur
Log file* (fichier journal)	/var/log/messages
Basic regular expression* (expression régulière de base)	
Timeout* (délai d'attente)	45
Critical Maximum Matches (correspondances maximum pour le statut critical)	
Warning Maximum Matches (correspondances maximum pour le statut warning)	

Champ	Valeur
Warning Minimum Matches (correspondances minimum pour le statut warning)	
Critical Minimum Matches (correspondances minimum pour le statut critical)	
Critical Maximum Match Rate (taux de correspondances maximum pour le statut critical)	
Warning Maximum Match Rate (taux de correspondances maximum pour le statut warning)	
Warning Minimum Match Rate (taux de correspondances minimum pour le statut warning)	
Critical Maximum Match Rate (taux de correspondances maximum pour le statut critical)	

A.6.2. LogAgent::Log Size

La sonde LogAgent::Log Size contrôle la croissance des fichiers journaux et recueille les métriques suivantes :

- Size - La taille dont le fichier journal a grandi en octets depuis la dernière exécution de la sonde.
- Output Rate - Le nombre d'octets par minute dont le fichier journal augmenté depuis la dernière exécution de la sonde.
- Lines - Le nombre de lignes écrites dans le fichier journal depuis la dernière exécution de la sonde.
- Line Rate - Le nombre de lignes écrites par minute dans le fichier journal depuis la dernière exécution de la sonde.

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde. Pour que cette sonde soit exécutée, l'utilisateur **`nocpulse`** doit posséder l'accès lecture sur vos fichiers journaux.

Tableau A.31. Paramètres de LogAgent::Log Size

Champ	Valeur
Log file* (fichier journal)	/var/log/messages
Timeout* (délai d'attente)	20
Critical Maximum Size (taille maximum pour le statut critical)	

Champ	Valeur
Warning Maximum Size (taille maximum pour le statut warning)	
Warning Minimum Size (taille minimum pour le statut warning)	
Critical Minimum Size (taille minimum pour le statut critical)	
Critical Maximum Output Rate (taux de sortie maximum pour le statut critical)	
Warning Maximum Output Rate (taux de sortie maximum pour le statut warning)	
Warning Minimum Output Rate (taux de sortie minimum pour le statut warning)	
Critical Minimum Output Rate (taux de sortie minimum pour le statut critical)	
Critical Maximum Lines (lignes maximum pour le statut critical)	
Warning Maximum Lines (lignes maximum pour le statut warning)	
Warning Minimum Lines (lignes minimum pour le statut warning)	
Critical Minimum Lines (lignes minimum pour le statut critical)	
Critical Maximum Line Rate (taux de lignes maximum pour le statut critical)	
Warning Maximum Line Rate (taux de lignes maximum pour le statut warning)	
Warning Minimum Line Rate (taux de lignes minimum pour le statut warning)	
Critical Minimum Line Rate (taux de lignes minimum pour le statut critical)	

A.7. MYSQL 3.23 - 3.33

Les sondes de cette section contrôlent les aspects de la base de données MySQL à l'aide du binaire **`mysqladmin`**. Aucun privilège d'utilisateur spécifique n'est nécessaire pour ces sondes.

Remarquez que le paquetage **`mysql-server`** doit être installé sur le système effectuant le contrôle pour que ces sondes soient exécutées. Consultez la section sur l'installation de MySQL du *Guide d'installation Red Hat Satellite* pour obtenir des instructions.

A.7.1. MySQL::Database Accessibility

La sonde MySQL::Database Accessibility teste la connectivité via un compte de base de données qui n'a aucun privilège de base de données. Si aucune connexion n'est effectuée, un statut CRITICAL en résulte.

Tableau A.32. Paramètres de MySQL::Database Accessibility

Champ	Valeur
Username*	
Mot de passe	
MySQL Port	3306
Database* (base de données)	mysql
Timeout	15

A.7.2. MySQL::Opened Tables

La sonde MySQL::Opened Tables contrôle le serveur MySQL et recueille la métrique suivante :

- Opened Tables - Les tables qui ont été ouvertes depuis le lancement du serveur.

Tableau A.33. Paramètres de MySQL::Opened Tables

Champ	Valeur
Nom d'utilisateur	
Mot de passe	
MySQL Port*	3306
Timeout	15
Critical Maximum Opened Objects (objets ouverts maximum pour le statut critical)	
Warning Maximum Opened Objects (objets ouverts maximum pour le statut warning)	

Champ	Valeur
Warning Minimum Opened Objects (objets ouverts minimum pour le statut warning)	
Critical Minimum Opened Objects (objets ouverts minimum pour le statut critical)	

A.7.3. MySQL::Open Tables

La sonde MySQL::Open Tables contrôle le serveur MySQL et recueille la métrique suivante :

- Open Tables - Le nombre de tables ouvertes lorsque la sonde est exécutée.

Tableau A.34. Paramètres de MySQL::Open Tables

Champ	Valeur
Nom d'utilisateur	
Mot de passe	
MySQL Port*	3306
Timeout	15
Critical Maximum Open Objects (objets ouverts maximum pour le statut critical)	
Warning Maximum Open Objects (objets ouverts maximum pour le statut warning)	
Warning Minimum Open Objects (objets ouverts minimum pour le statut warning)	
Critical Minimum Open Objects (objets ouverts minimum pour le statut critical)	

A.7.4. MySQL::Query Rate

La sonde MySQL::Query contrôle le serveur MySQL et recueille la métrique suivante :

- Query Rate - Le nombre en moyenne de requêtes par seconde par serveur de bases de données.

Tableau A.35. Paramètres de MySQL::Query Rate

Champ	Valeur
Nom d'utilisateur	
Mot de passe	
MySQL Port*	3306
Timeout	15
Critical Maximum Query Rate (taux de requêtes maximum pour le statut critical)	
Warning Maximum Query Rate (taux de requêtes maximum pour le statut warning)	
Warning Minimum Query Rate (taux de requêtes minimum pour le statut warning)	
Critical Minimum Query Rate (taux de requêtes minimum pour le statut critical)	

A.7.5. MySQL::Threads Running

La sonde MySQL::Threads Running contrôle le serveur MySQL et recueille la métrique suivante :

- Threads Running - Le nombre total de threads en cours d'exécution au sein de la base de données.

Tableau A.36. Paramètres de MySQL::Threads Running

Champ	Valeur
Nom d'utilisateur	
Mot de passe	
MySQL Port*	3306
Timeout	15
Critical Maximum Threads Running (threads en cours d'exécution maximum pour le statut critical)	
Warning Maximum Threads Running (threads en cours d'exécution maximum pour le statut warning)	

Champ	Valeur
Warning Minimum Threads Running (threads en cours d'exécution minimum pour le statut warning)	
Critical Minimum Threads Running (threads en cours d'exécution minimum pour le statut critical)	

A.8. NETWORK SERVICES

Les sondes de cette section contrôlent divers services intégrés à un réseau fonctionnant. Lorsque vous les appliquez, assurez-vous que leurs limites de temps ne dépassent pas la durée de temps allouée à la période de délai d'attente. Sinon, un statut UNKNOWN est renvoyé dans tous les cas de latence étendue, annulant ainsi les limites.

A.8.1. Network Services::DNS Lookup

La sonde Network Services::DNS Lookup utilise la commande **`dig`** pour voir si elle peut résoudre le nom de système ou de domaine spécifié dans le champ **`Host or Address to look up`** (hôte ou adresse à consulter). Elle recueille la métrique suivante :

- Query Time - La durée en millisecondes requise pour exécuter la requête **`dig`**.

Cette sonde est utile pour le contrôle du statut de vos serveurs DNS. Si vous souhaitez contrôler l'un de vos serveurs DNS, fournissez un nom d'hôte ou de domaine bien connu, comme par exemple un moteur de recherche important ou un site web d'entreprise.

Tableau A.37. Paramètres de Network Services::DNS Lookup

Champ	Valeur
Host or Address to look up (hôte ou adresse à consulter)	
Timeout* (délai d'attente)	10
Critical Maximum Query Time (durée de requête maximum pour le statut critical)	
Warning Maximum Query Time (durée de requête maximum pour le statut warning)	

A.8.2. Network Services::FTP

La sonde Network Services::FTP utilise les sockets de réseau pour tester la disponibilité du port FTP. Elle recueille la métrique suivante :

- Remote Service Latency - La durée en secondes prise par le serveur FTP pour répondre à une requête de connexion.

Cette sonde prend en charge l'authentification. Donnez un nom d'utilisateur et un mot de passe dans les champs appropriés pour utiliser cette fonctionnalité. La valeur **`Expect`** optionnelle est la chaîne à

comparer après une connexion réussie au serveur FTP. Si la chaîne attendue n'est pas trouvée, la sonde retourne un état CRITICAL.

Tableau A.38. Paramètres de Network Services::FTP

Champ	Valeur
Expect	FTP
Nom d'utilisateur	
Mot de passe	
FTP Port*	21
Timeout* (délai d'attente)	10
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.8.3. Network Services::IMAP Mail

La sonde Network Services::IMAP Mail détermine si elle peut se connecter au service IMAP 4 sur le système. La spécification d'un port optionnel écrasera le port 143 par défaut. Elle recueille la métrique suivante :

- Remote Service Latency - La durée en secondes prise par le serveur IMAP pour répondre à une requête de connexion.

La valeur **`Expect`** requise est la chaîne à comparer après une connexion réussie au serveur IMAP. Si la chaîne attendue n'est pas trouvée, la sonde retourne un état CRITICAL.

Tableau A.39. Paramètres de Network Services::IMAP Mail

Champ	Valeur
IMAP Port*	143
Expect*	Valider
Timeout* (délai d'attente)	5
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.8.4. Network Services::Mail Transfer (SMTP)

La sonde Network Services::Mail Transfer (SMTP) détermine si elle peut se connecter au port SMTP sur le système. La spécification d'un port optionnel écrase le port 25 par défaut. Elle recueille la métrique suivante :

- Remote Service Latency - La durée en secondes prise par le serveur SMTP pour répondre à une requête de connexion.

Tableau A.40. Paramètres de Network Services::Mail Transfer (SMTP)

Champ	Valeur
SMTP Port*	25
Timeout* (délai d'attente)	10
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.8.5. Network Services::Ping

La sonde Network Services::Ping détermine si le serveur Red Hat Satellite peut exécuter la commande **`ping`** sur le système contrôlé ou une adresse IP spécifiée. Elle vérifie également la perte de paquets et compare la moyenne d'aller-retour aux niveaux des limites Warning et Critical. La valeur **`Packets to send`** (paquets à envoyer) requise vous permet de contrôler combien de paquets ICMP ECHO sont envoyés au système. Cette sonde recueille les métriques suivantes :

- Round-Trip Average - La durée de temps en millisecondes prise par le paquet ICMP ECHO pour aller au système contrôlé et en revenir.
- Packet Loss - Le pourcentage de données perdues en transit.

Bien qu'il soit facultatif, le champ **`IP Address`** peut être utile dans le rassemblement de métriques pour les systèmes qui ont plusieurs adresses IP. Par exemple, si le système est configuré avec plusieurs adresses IP virtuelles ou utilise la traduction d'adresses réseau NAT (de l'anglais Network Address Translation) pour prendre en charge les adresses IP internes et externes, cette option peut être utilisée pour vérifier une adresse IP secondaire, au lieu de l'adresse primaire associée au nom d'hôte.

Notez que cette sonde exécute **`ping`** depuis un serveur Red Hat Satellite et non pas le système contrôlé. Le fait de remplir le champ "IP Address"ne teste pas la connectivité entre le système et l'adresse IP spécifiée mais entre le serveur Red Hat Satellite et l'adresse IP. La saisie de la même adresse IP pour les sondes Ping sur différents systèmes effectue ainsi exactement la même tâche. Pour exécuter une commande **`ping`** depuis un système contrôlé sur une adresse IP individuelle, utilisez à la place la sonde Remote Ping. Reportez-vous à la Section A.8.7, « Network Services::Remote Ping ».

Tableau A.41. Paramètres de Network Services::Ping

Champ	Valeur
IP Address (valeur par défaut de l'adresse IP du système)	
Packets to send* (paquets à envoyer)	20
Timeout* (délai d'attente)	10
Critical Maximum Round-Trip Average (moyenne d'aller-retour maximum pour le statut critical)	
Warning Maximum Round-Trip Average (moyenne d'aller-retour maximum pour le statut warning)	
Critical Maximum Packet Loss (perte de paquets maximum pour le statut critical)	
Warning Maximum Packet Loss (perte de paquets maximum pour le statut warning)	

A.8.6. Network Services::POP Mail

La sonde Network Services::POP Mail détermine si elle peut se connecter au port POP3 du système. Un numéro de port doit être spécifié ; la spécification d'un autre numéro de port écrase le port par défaut qui est 110. Cette sonde recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur POP réponde à une requête de connexion.

La valeur **`Expect`** requise est la chaîne à comparer après une connexion réussie au serveur POP. La sonde recherche la chaîne dans la première ligne de la réponse du système. La valeur par défaut est **`+OK`**. Si la chaîne attendue n'est pas trouvée, la sonde retourne un état CRITICAL.

Tableau A.42. Paramètres de Network Services::POP Mail

Champ	Valeur
Port*	110
Expect*	+OK
Timeout* (délai d'attente)	10
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.8.7. Network Services::Remote Ping

La sonde Network Services::Remote Ping détermine si le système contrôlé peut exécuter la commande **`ping`** vers une adresse IP spécifiée. Elle contrôle également la perte de paquets et compare la moyenne d'aller-retour aux niveaux des limites Warning et Critical. La valeur **`Packets to send`** (paquets à envoyer) requise vous permet de contrôler combien de paquets ICMP ECHO sont envoyés à cette adresse. Cette sonde recueille les métriques suivantes :

- Round-Trip Average - La durée de temps en millisecondes prise par le paquet ICMP ECHO pour aller à l'adresse IP et en revenir.
- Packet Loss - Le pourcentage de données perdues en transit.

Le champ **`IP Address`** identifie l'adresse précise à laquelle envoyer un ping. Au contraire du champ optionnel semblable dans la sonde Ping standard, ce champ est requis. Le système contrôlé dirige la commande ping vers une adresse tierce, au lieu du serveur Red Hat Satellite. Vu que la sonde Remote Ping teste la connectivité depuis le système contrôlé, une autre adresse IP doit être spécifiée. Pour effectuer des commandes ping depuis le serveur Red Hat Satellite vers un système ou une adresse IP, utilisez à la place la sonde Ping standard. Reportez-vous à la Section A.8.5, « Network Services::Ping ».

Conditions préalables - Le démon de contrôle Red Hat Network (**`rhnmd`**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde.

Tableau A.43. Paramètres de Network Services::Remote Ping

Champ	Valeur
IP Address*	
Packets to send* (paquets à envoyer)	20
Timeout* (délai d'attente)	10
Critical Maximum Round-Trip Average (moyenne d'aller-retour maximum pour le statut critical)	
Warning Maximum Round-Trip Average (moyenne d'aller-retour maximum pour le statut warning)	
Critical Maximum Packet Loss (perte de paquets maximum pour le statut critical)	
Warning Maximum Packet Loss (perte de paquets maximum pour le statut warning)	

A.8.8. Network Services::RPCService

La sonde Network Services::RPCService teste la disponibilité de programmes d'appels de procédure à distance (RPC, de l'anglais, remote procedure call) sur une adresse IP donnée. Elle recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur RPC réponde à une requête de connexion.

Les programmes de serveur RPC, qui fournissent des appels de fonctions via le réseau RPC, s'enregistrent au réseau RPC en déclarant un identifiant et un nom de programme. NFS est un exemple de service qui fonctionne via le mécanisme RPC.

Les programmes client qui souhaitent utiliser les ressources des programmes de serveur RPC le peuvent en demandant à la machine sur laquelle le programme de serveur se trouve, de fournir l'accès aux fonctions RPC dans le numéro ou le nom de programme RPC. Ces conversations peuvent se produire sur TCP ou UDP (mais sont pratiquement toujours UDP).

Cette sonde vous permet de tester la disponibilité de simples programmes. Vous devez spécifier le nom ou le numéro de programme, le protocole sur lequel la conversation se produit et le délai d'attente normal.

Tableau A.44. Paramètres de Network Services::RPCService

Champ	Valeur
Protocol (TCP/UDP)	udp
Service Name* (nom de service)	nfs
Timeout* (délai d'attente)	10
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.8.9. Network Services::Secure web Server (HTTPS)

La sonde Network Services::Secure web Server (HTTPS) détermine la disponibilité du serveur web sécurisé et recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur HTTPS réponde à une requête de connexion.

Cette sonde confirme qu'elle peut se connecter au port HTTPS sur l'hôte spécifié et obtenir l'URL spécifié. Si aucun URL n'est spécifié, la sonde cherche le document root. La sonde recherche un message HTTP/1. du système, à moins que vous ne modifiez cette valeur. La spécification d'un autre numéro de port écrase le port par défaut de 443.

Cette sonde prend en charge l'authentification. Donnez un nom d'utilisateur et un mot de passe dans les champs appropriés pour utiliser cette fonctionnalité. Au contraire de la plupart des sondes, cette sonde retourne un état CRITICAL si elle ne peut pas contacter le système avant la fin de la période de délai d'attente.

Tableau A.45. Paramètres de Network Services::Secure web Server (HTTPS)

Champ	Valeur
Chemin URL	/

Champ	Valeur
Expect Header (en-tête expect)	HTTP/1
Expect Content (contenu expect)	
UserAgent* (agent d'utilisateur)	NOCpulse-check_http/1.0
Nom d'utilisateur	
Mot de passe	
Timeout* (délai d'attente)	10
HTTPS Port*	443
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.8.10. Network Services::SSH

La sonde Network Services::SSH détermine la disponibilité de SSH sur le port spécifié et recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur SSH réponde à une requête de connexion.

Au moment de contacter le serveur SSH et de recevoir une réponse valide, la sonde affiche les informations de version du protocole et du serveur. Si la sonde reçoit une réponse invalide, elle affiche le message retourné par le serveur et produit un état WARNING.

Tableau A.46. Paramètres de Network Services::SSH

Champ	Valeur
SSH Port*	22
Timeout* (délai d'attente)	5
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.8.11. Network Services::web Server (HTTP)

La sonde Network Services::web Server (HTTP) détermines la disponibilité du serveur web et recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur HTTP réponde à une requête de connexion.

Cette sonde confirme qu'elle peut se connecter au port HTTP sur l'hôte spécifié et obtenir l'URL spécifié. Si aucun URL n'est spécifié, la sonde cherchera le document root. Le sonde recherche un message HTTP/1. du système, à moins que vous ne modifiez cette valeur. La spécification d'un autre numéro de port écrasera le port par défaut de 80. Au contraire de la plupart des sondes, cette sonde retournera un état CRITICAL si elle ne peut pas contacter le système avant la fin de la période de délai d'attente.

Cette sonde prend en charge l'authentification. Donnez un nom et un mot de passe dans les champs appropriés pour utiliser cette fonctionnalité. Le champ "Virtual Host" optionnel peut être utilisé pour contrôler un ensemble de documentation séparé qui se trouve sur la même machine physique présentée comme un serveur autonome. Si votre serveur web n'est pas configure pour utiliser les hôtes virtuels (ce qui est le cas), vous devriez laisser ce champ vierge. Si vous avez des hôtes virtuels configurés, saisissez le nom de domaine du premier hôte. Ajoutez autant de sondes nécessaires pour contrôler tous les hôtes virtuels sur la machine.

Tableau A.47. Paramètres de Network Services::web Server (HTTP)

Champ	Valeur
Chemin URL	/
Hôte virtuel	
Expect Header (en-tête expect)	HTTP/1
Expect Content (contenu expect)	
UserAgent* (agent d'utilisateur)	NOCpulse-check_http/1.0
Nom d'utilisateur	
Mot de passe	
Timeout* (délai d'attente)	10
HTTP Port*	80
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.9. ORACLE 8I, 9I, 10G, AND 11G

Les sondes de cette section peuvent être appliquées aux instances de la base de données Oracle correspondant aux versions prises en charge. Les sondes Oracle requièrent la configuration de la base de données et la création d'associations en exécutant la commande suivante :

```
$ORACLE_HOME/rdbms/admin/catalog.sql
```

De plus, pour que ces sondes fonctionnent correctement, l'utilisateur Oracle configuré dans la sonde doit posséder les privilèges minimums de CONNECT et SELECT_CATALOG_ROLE.

Certaines sondes Oracle sont conçues spécifiquement pour régler des périphériques pour des gains en performance à long terme, plutôt que pour éviter des défaillances. Red Hat recommande donc de les programmer de façon à se produire moins souvent, entre toutes les heures et tous les deux jours. Cela offre une meilleure représentation statistique tout en désaccentuant les anomalies qui peuvent se produire à des intervalles de temps plus courts. Ceci s'applique aux probes suivantes : Buffer Cache, Data Dictionary Cache, Disk Sort Ratio, Library Cache et Redo Log.

Afin que les limites CRITICAL et WARNING basées sur le temps fonctionnent comme prévu, leurs valeurs ne peuvent pas dépasser la durée de temps allouée au délai d'attente. Sinon, un statut UNKNOWN est renvoyé dans tous les cas de latence étendue, annulant de cette façon les limites. Pour cette raison, Red Hat recommande fortement de vous assurer que les périodes de délai dépassent toutes les limites de temps. Dans cette section, cela concerne particulièrement la sonde TNS Ping.

Finalement, les clients qui utilisent ces sondes Oracle sur une base de données qui utilise le serveur MTS (Multi-Threaded Server) d'Oracle doivent contacter l'assistance Red Hat pour ajouter des entrées au fichier /etc/hosts du serveur Red Hat Network afin de s'assurer que le nom DNS soit résolu correctement.

A.9.1. Oracle::Active Sessions

La sonde Oracle::Active Sessions contrôle une instance d'Oracle et recueille les métriques suivantes :

- Active Sessions - Le nombre de sessions actives basé sur la valeur de **V$PARAMETER.PROCESSES**.
- Available Sessions - Le pourcentage de sessions actives disponibles basé sur la valeur de **V$PARAMETER.PROCESSES**.

Tableau A.48. Paramètres de Oracle::Active Sessions

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout* (délai d'attente)	30
Critical Maximum Active Sessions (sessions actives maximum pour le statut critical)	

Champ	Valeur
Warning Maximum Active Sessions (sessions actives maximum pour le statut warning)	
Critical Maximum Available Sessions Used (sessions disponibles utilisées maximum pour le statut critical)	
Warning Maximum Available Sessions Used (sessions disponibles utilisées maximum pour le statut warning)	

A.9.2. Oracle::Availability

La sonde Oracle::Availability détermine la disponibilité de la base de données depuis Red Hat Satellite.

Tableau A.49. Paramètres de Oracle::Availability

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout* (délai d'attente)	30

A.9.3. Oracle::Blocking Sessions

La sonde Oracle::Blocking Sessions contrôle un instance d'Oracle et recueille la métrique suivante :

- Blocking Sessions - Le nombre de sessions empêchant d'autres sessions de valider leurs changements dans la base de données Oracle, comme vous l'avez déterminé dans la valeur *Time Blocking* requise. Seules ces sessions qui ont bloqué pendant cette durée, mesurée en secondes, seront comptées comme sessions bloquantes.

Tableau A.50. Paramètres de Oracle::Blocking Sessions

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	

Champ	Valeur
Oracle Port*	1521
Time Blocking (seconds)* (temps de blocage en secondes)	20
Timeout* (délai d'attente)	30
Critical Maximum Blocking Sessions (sessions bloquantes maximum pour le statut critical)	
Warning Maximum Blocking Sessions (sessions bloquantes maximum pour le statut warning)	

A.9.4. Oracle::Buffer Cache

La sonde Oracle::Buffer Cache calcule la proportion de connexions au cache de tampon afin d'optimiser la taille du cache de tampon de base de données SGA (system global area). Elle recueille les métriques suivantes :

- Db Block Gets - Le nombre de blocs accédés via des commandes get par simple bloc (pas par le mécanisme get homogène).
- Consistent Gets - Le nombre d'accès au tampon de bloc pour obtenir des données dans un mode homogène.
- Physical Reads - Le nombre cumulé de blocs lus du disque.
- Buffer Cache Hit Ratio - Le taux auquel la base de données va dans le tampon au lieu du disque dur pour obtenir des données. Un taux faible suggère que davantage de RAM devrait être ajoutée au système.

Tableau A.51. Paramètres de Oracle::Buffer Cache

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port	1521
Timeout* (délai d'attente)	30
Warning Minimum Buffer Cache Hit Ratio (proportion de connexions au cache de tampon minimum pour le statut warning)	

Champ	Valeur
Critical Minimum Buffer Cache Hit Ratio (proportion de connexions au cache de tampon minimum pour le statut critical)	

A.9.5. Oracle::Client Connectivity

La sonde Oracle::Client Connectivity détermine si la base de données est activée et capable de recevoir des connexions du système contrôlé. Cette sonde ouvre une connexion **rhnmd** vers le système et crée une commande **sqlplus connect** à exécuter sur le système contrôlé.

Le paramètre **Expected DB name** est la valeur attendue de **V$DATABASE.NAME**. Cette valeur est insensible à la casse. Un statut CRITICAL est retourné si cette valeur n'est pas trouvée.

Conditions préalables - Le démon de contrôle Red Hat Network (**rhnmd**) doit être en cours d'exécution sur le système contrôlé pour pouvoir exécuter cette sonde. Pour que cette sonde soit exécutée, l'utilisateur **nocpulse** doit posséder l'accès lecture sur vos fichiers journaux.

Tableau A.52. Paramètres de Oracle::Client Connectivity

Champ	Valeur
Oracle Hostname or IP address* (nom d'hôte ou adresse IP Oracle)	
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
ORACLE_HOME*	/opt/oracle
Expected DB Name* (nom de base de données attendu)	
Timeout* (délai d'attente)	30

A.9.6. Oracle::Data Dictionary Cache

La sonde Oracle::Data Dictionary Cache calcule la proportion de connexions au cache du dictionnaire de la base de données (Data Dictionary Cache Hit Ratio) afin d'optimiser la taille SHARED_POOL_SIZE dans **init.ora**. Elle recueille les métriques suivantes :

- Data Dictionary Hit Ratio - Proportion des tentatives réussies ou non de recherche du cache du dictionnaire de la base de données. En d'autres termes, le taux auquel la base de données va dans le dictionnaire au lieu du disque dur pour obtenir des données. Un taux faible suggère que davantage de RAM devrait être ajoutée au système.

- Gets - Le nombre de blocs accédés via des commandes get par simple bloc (pas par le mécanisme get homogène).
- Cache Misses - Le nombre d'accès au tampon de bloc pour obtenir des données dans un mode homogène.

Tableau A.53. Paramètres de Oracle::Data Dictionary Cache

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout* (délai d'attente)	30
Warning Minimum Data Dictionary Hit Ratio (proportion de connexions au dictionnaire de la base de données minimum pour le statut warning)	
Critical Minimum Data Dictionary Hit Ratio (proportion de connexions au dictionnaire de la base de données minimum pour le statut critical)	

A.9.7. Oracle::Disk Sort Ratio

La sonde Oracle::Disk Sort Ratio contrôle une instance de base de données Oracle et recueille la métrique suivante :

- Disk Sort Ratio - Le taux de tris Oracle qui étaient trop grands pour être terminés en mémoire et qui ont été en fait triés à l'aide d'un segment temporaire.

Tableau A.54. Paramètres de Oracle::Disk Sort Ratio

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout* (délai d'attente)	30

Champ	Valeur
Critical Maximum Disk Sort Ratio (proportion de tris de disque maximum pour le statut critical)	
Warning Maximum Disk Sort Ratio (proportion de tris de disque maximum pour le statut warning)	

A.9.8. Oracle::Idle Sessions

La sonde Oracle::Idle Sessions contrôle une instance d'Oracle et recueille la métrique suivante :

- Idle Sessions - Le nombre de sessions Oracle qui sont inactives, comme vous l'avez déterminé dans la valeur *Time Idle* requise. Seules ces sessions qui ont été inactives pendant cette durée, mesurée en secondes, sont comptées comme sessions inactives.

Tableau A.55. Paramètres de Oracle::Idle Sessions

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Time Idle (seconds)* (temps inactif en secondes)	20
Timeout* (délai d'attente)	30
Critical Maximum Idle Sessions (sessions inactives maximum pour le statut critical)	
Warning Maximum Idle Sessions (sessions inactives maximum pour le statut warning)	

A.9.9. Oracle::Index Extents

La sonde Oracle::Index Extents contrôle une instance d'Oracle et recueille la métrique suivante :

- Allocated Extents - Le nombre d'étendues allouées pour tout index.
- Available Extents - Le pourcentage d'étendues disponibles pour tout index.

Le champ **`Index Name`** (nom d'index) requis contient la valeur par défaut `%` qui correspond à tout nom d'index.

Tableau A.56. Parmètres de Oracle::Index Extents

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Index Owner* (propriétaire de l'index)	%
Index Name* (nom d'index)	%
Timeout* (délai d'attente)	30
Critical Maximum of Allocated Extents (étendues allouées maximum pour le statut critical)	
Warning Maximum of Allocated Extents (étendues allouées maximum pour le statut warning)	
Critical Maximum of Available Extents (étendues disponibles maximum pour le statut critical)	
Warning Maximum of Available Extents (étendues disponibles maximum pour le statut warning)	

A.9.10. Oracle::Library Cache

La sonde Oracle::Library Cache calcule le taux d'échec dans le cache de la bibliothèque (Library Cache Miss Ratio) afin d'optimiser la taille SHARED_POOL_SIZE dans **`init.ora`**. Elle recueille les métriques suivantes :

- Library Cache Miss Ratio - Le taux d'échec de pin dans le cache de la bibliothèque. Cela se produit lorsqu'une session exécute une instruction qui a déjà été analysée mais trouve que l'instruction ne se trouve plus dans le groupe partagé.
- Executions - Le nombre de fois qu'un pin a été demandé pour des objets de cet espace de noms.
- Cache Misses - Le nombre de pins devant maintenant récupérer l'objet du disque. Ces pins sont composés d'objets avec des pins précédents datant du moment où l'identificateur de l'objet a été créé.

Tableau A.57. Paramètres de Oracle::Library Cache

Champ	Valeur
Oracle SID*	

Champ	Valeur
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout* (délai d'attente)	30
Critical Maximum Library Cache Miss Ratio	
Warning Maximum Library Cache Miss Ratio	

A.9.11. Oracle::Locks

La sonde Oracle::Locks contrôle une base de données Oracle et recueille la métrique suivante :

- Active Locks - Le nombre courant de verrous actifs comme la valeur dans la table v$locks le détermine. Les administrateurs de bases de données devraient faire attention à des nombres élevés de verrous présents dans une base de données.

Les verrous sont utilisés afin que plusieurs utilisateurs ou processus qui mettent à jour les mêmes données dans la base de données ne provoquent pas de conflit. Cette sonde est utile pour avertir les administrateurs de bases de données lorsque un nombre élevé de verrous sont présents dans une base de données spécifique.

Tableau A.58. Paramètres de Oracle::Locks

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout* (délai d'attente)	30
Critical Maximum Active Locks (verrous actifs maximum pour le statut critical)	
Warning Maximum Active Locks (verrous actifs maximum pour le statut warning)	

A.9.12. Oracle::Redo Log

La sonde Oracle::Redo Log contrôle une base de données Oracle et recueille les métriques suivantes :

- Redo Log Space Request Rate - Le nombre moyen de requêtes d'espace de fichiers Redo Log par minute depuis le démarrage du serveur.
- Redo Buffer Allocation Retry Rate - Le nombre moyen de nouvelles tentatives d'allocation de tampon par minute depuis le démarrage du serveur.

Les métriques retournées et les limites auxquelles elles sont comparées sont des nombres représentant le taux de changement en événements par minute. Le taux de changement pour ces métriques devrait être contrôlé vu qu'une croissance rapide peut indiquer des problèmes demandant une enquête.

Tableau A.59. Paramètres de Oracle::Redo Log

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout* (délai d'attente)	30
Critical Maximum Redo Log Space Request Rate	
Warning Maximum Redo Log Space Request Rate	
Critical Maximum Redo Buffer Allocation Retry Rate	
Warning Maximum Redo Buffer Allocation Retry Rate	

A.9.13. Oracle::Table Extents

La sonde Oracle::Table Extents contrôle une base de données Oracle et recueille les métriques suivantes :

- Allocated Extents-Any Table - Le nombre total d'étendues pour toute table.
- Available Extents-Any Table - Le pourcentage d'étendues disponibles pour toute table.

Dans Oracle, les étendues de tables permettent à une table de grandir. Lorsqu'une table est pleine, elle est *étendue* d'une quantité d'espace configurée lorsque la table est créée. Les étendues sont configurées selon chaque table, avec une taille d'étendue et un nombre maximum d'étendues.

Par exemple, une table qui commence avec 10 Mo d'espace et qui est configurée avec une taille d'étendue de 1 Mo et un maximum de 10 étendues peut grandir jusqu'à un maximum de 20 Mo (en étant étendue de 1Mo dix fois). Cette sonde peut être configurée de façon à avertir par (1) le nombre

d'étendues allouées (par exemple, "devenir critical lorsque la table a été étendue 5 ou plusieurs fois") ou (2) la table est étendue au-delà d'un certain pourcentage de son maximum d'étendues (par exemple, "devenir critical lorsque la table a dépassé 80% ou plus de son maximum d'étendues").

Les champs requis **`Table Owner`** et **`Table Name`** contiennent la valeur par défaut `%` qui correspond à tout propriétaire ou nom de table.

Tableau A.60. Paramètres de Oracle::Table Extents

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Table Owner*	%
Table Name*	%
Timeout* (délai d'attente)	30
Critical Maximum Allocated Extents (étendues allouées maximum pour le statut critical)	
Warning Maximum Allocated Extents (étendues allouées maximum pour le statut warning)	
Critical Maximum Available Extents (étendues disponibles maximum pour le statut critical)	
Warning Maximum Available Extents (étendues disponibles maximum pour le statut warning)	

A.9.14. Oracle::Tablespace Usage

La sonde Oracle::Tablespace Usage contrôle une base de données Oracle et recueille la métrique suivante :

- Available Space Used - Le pourcentage d'espace disponible dans chaque espace de table qui a été utilisé.

L'espace de table est le groupe partagé d'espace dans lequel un ensemble de tables se trouve. Cette sonde avertit l'utilisateur lorsque la quantité totale d'espace disponible passe en-dessous de la limite. L'espace de table est mesurée en octets. Les étendues ne l'affectent donc pas directement (bien que chaque étendue supprime de l'espace disponible du groupe partagé).

Le champ requis **`Tablespace Name`** (nom d'espace de table) est sensible à la casse et contient une valeur par défaut de `%` qui correspond à tout nom de table.

Tableau A.61. Paramètres de Oracle::Tablespace Usage

Champ	Valeur
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Tablespace Name*	%
Timeout* (délai d'attente)	30
Critical Maximum Available Space Used (espace disponible utilisé maximum pour le statut critical)	
Warning Maximum Available Space Used (espace disponible utilisé maximum pour le statut warning)	

A.9.15. Oracle::TNS Ping

La sonde Oracle::TNS Ping détermine si un écouteur Oracle est vivant et recueille la métrique suivante :

- Remote Service Latency - Le temps nécessaire en secondes pour que le serveur Oracle réponde à une requête de connexion.

Tableau A.62. Paramètres de Oracle::TNS Ping

Champ	Valeur
TNS Listener Port* (port d'écoute TNS)	1521
Timeout* (délai d'attente)	15
Critical Maximum Remote Service Latency (latence de services à distance maximum pour le statut critical)	
Warning Maximum Remote Service Latency (latence de services à distance maximum pour le statut warning)	

A.10. RED HAT SATELLITE

Les sondes de cette section peuvent être appliquées sur Red Hat Satellite pour contrôler sa santé et ses performances. Comme ces sondes sont exécutées localement, aucune application spécifique ou aucun protocole de transport n'est requis.

A.10.1. Red Hat Satellite::Disk Space

La sonde Red Hat Satellite::Disk Space contrôle l'espace de disque libre sur un Satellite et recueille les métriques suivantes :

- File System Used - Le pourcentage du système de fichiers actuellement utilisé.
- Space Used - La taille de fichier utilisée par le système de fichiers actuel.
- Space Available - La taille de fichier disponible au système de fichiers actuel.

Tableau A.63. Paramètres Red Hat Satellite::Disk Space

Champ	Valeur
Device Pathname* (nom de chemin du périphérique)	/dev/hda1
Critical Maximum File System Used (système de fichiers utilisé maximum pour le statut critical)	
Warning Maximum File System Used (système de fichiers utilisé maximum pour le statut warning)	
Critical Maximum Space Used (espace utilisé maximum pour le statut critical)	
Warning Maximum Space Used (espace utilisé maximum pour le statut warning)	
Critical Maximum Space Available (espace disponible maximum pour le statut critical)	
Warning Maximum Space Available (espace disponible maximum pour le statut warning)	

A.10.2. Red Hat Satellite::Execution Time

La sonde Red Hat Satellite::Execution Time contrôle le temps d'exécution pour les sondes exécutée depuis un Satellite et recueille la métrique suivante :

- Probe Execution Time Average - Les secondes prises pour exécuter entièrement une sonde.

Tableau A.64. Paramètres Red Hat Satellite::Execution Time

Champ	Valeur
Critical Maximum Probe Execution Time Average (moyenne de temps d'exécution d'une sonde maximum pour le statut critical)	
Warning Maximum Probe Execution Time Average (moyenne de temps d'exécution d'une sonde maximum pour le statut warning)	

A.10.3. Red Hat Satellite::Interface Traffic

La sonde Red Hat Satellite::Interface Traffic contrôle le trafic d'interface sur un Satellite et recueille les métriques suivantes :

- Input Rate - La quantité de trafic en octets par seconde reçue par le périphérique.
- Output Rate - La quantité de trafic en octets par seconde envoyée par le périphérique.

Tableau A.65. Paramètres Red Hat Satellite::Interface Traffic

Champ	Valeur
Interface*	eth0
Timeout (seconds)*	30
Critical Maximum Input Rate (taux d'entrée maximum pour le statut critical)	
Critical Maximum Output Rate (taux de sortie maximum pour le statut critical)	

A.10.4. Red Hat Satellite::Latency

La sonde Red Hat Satellite::Latency contrôle la latence de sondes sur un Satellite et recueille la métrique suivante :

- Probe Latency Average - Le délai en secondes entre le moment où une sonde devient prête à être exécutée et le moment où elle est exécutée. Sous des conditions normales, cette durée est généralement inférieure à une seconde. Lorsqu'un Satellite est surchargé (parce qu'il a trop de sondes par rapport à leur temps d'exécution moyen), le nombre augmente.

Tableau A.66. Paramètres Red Hat Satellite::Latency

Champ	Valeur
Critical Maximum Probe Latency Average	
Warning Maximum Probe Latency Average	

A.10.5. Red Hat Satellite::Load

La sonde Red Hat Satellite::Load contrôle la charge CPU sur un Satellite et recueille la métrique suivante :

- Load - La charge moyenne sur le CPU pour une durée de 1-, 5- et 15-minutes.

Tableau A.67. Paramètres Red Hat Satellite::Load

Champ	Valeur
Critical Maximum 1-minute Average (moyenne d'1 minute maximum pour le statut critical)	
Warning Maximum 1-minute Average (moyenne d'1 minute maximum pour le statut warning)	
Critical Maximum 5-minute Average (moyenne de 5 minutes maximum pour le statut critical)	
Warning Maximum 5-minute Average (moyenne de 5 minutes maximum pour le statut warning)	
Critical Maximum 15-minute Average (moyenne de 15 minutes maximum pour le statut critical)	
Warning Maximum 15-minute Average (moyenne de 15 minutes maximum pour le statut warning)	

A.10.6. Red Hat Satellite::Probe Count

La sonde Red Hat Satellite::Probe Count contrôle le nombre de sondes sur un Satellite et recueille la métrique suivante :

- Probes - Le nombre de sondes individuelles en cours d'exécution sur un Satellite.

Tableau A.68. Paramètres Red Hat Satellite::Probe Count

Champ	Valeur
Critical Maximum Probe Count (nombre de sondes maximum pour le statut critical)	
Warning Maximum Probe Count (nombre de sondes maximum pour le statut warning)	

A.10.7. Red Hat Satellite::Process Counts

La sonde Red Hat Satellite::Process Counts contrôle le nombre de processus sur un Satellite et recueille les métriques suivantes :

- Blocked - Le nombre de processus qui ont été placés dans la file d'attente et dans l'état d'attente.
- Child - Le nombre de processus créés par un autre processus qui est déjà en cours d'exécution sur la machine.
- Defunct - Le nombre de processus qui ont été terminés (parce qu'ils ont été tués par un signal ou parce qu'ils ont appelé **`exit()`**) et dont les processus parents n'ont pas encore reçu de notification de leur arrêt en exécutant une forme de l'appel système **`wait()`**.
- Stopped - Le nombre de processus qui ont été arrêtés avant la fin de leur exécution.
- Sleeping - Un processus qui est dans l'état de sommeil **`Interruptible`** et qui peut être réintroduit plus tard en mémoire, son exécution étant reprise à partir de son point d'arrêt.

Tableau A.69. Paramètres Red Hat Satellite::Process Counts

Champ	Valeur
Critical Maximum Blocked Processes (processus bloqués maximum pour le statut critical)	
Warning Maximum Blocked Processes (processus bloqués maximum pour le statut warning)	
Critical Maximum Child Processes (processus enfants maximum pour le statut critical)	
Warning Maximum Child Processes (processus enfants maximum pour le statut warning)	
Critical Maximum Defunct Processes (processus terminés maximum pour le statut critical)	
Warning Maximum Defunct Processes (processus terminés maximum pour le statut warning)	
Critical Maximum Stopped Processes (processus arrêtés maximum pour le statut critical)	
Warning Maximum Stopped Processes (processus arrêtés maximum pour le statut warning)	
Critical Maximum Sleeping Processes (processus endormis maximum pour le statut critical)	
Warning Maximum Sleeping Processes (processus endormis maximum pour le statut warning)	

A.10.8. Red Hat Satellite::Processes

La sonde Red Hat Satellite::Processes contrôle le nombre de processus sur un Satellite et recueille la métrique suivante :

- Processes - Le nombre de processus exécutés simultanément sur la machine.

Tableau A.70. Paramètres Red Hat Satellite::Processes

Champ	Valeur
Critical Maximum Processes	
Warning Maximum Processes	

A.10.9. Red Hat Satellite::Process Health

La sonde Red Hat Satellite::Process Health contrôle les processus spécifiés par le client et recueille les métriques suivantes :

- CPU Usage - Le pourcentage d'utilisation du CPU pour un processus donné.
- Child Process Groups - Le nombre de processus enfants créés par le processus parent spécifié. Un processus enfant hérite de la plupart de ses attributs, comme les fichiers ouverts, de son parent.
- Threads - Le nombre de threads en cours d'exécution pour un processus donné. Un thread est l'unité de base de l'utilisation de CPU et comprend un compteur de programmes, un ensemble d'enregistrement et un espace de pile. Un thread est également appelé un processus léger.
- Physical Memory Used - La quantité de mémoire physique en kilo-octets utilisée par le processus spécifié.
- Virtual Memory Used - La quantité de mémoire virtuelle en kilo-octets utilisée par le processus spécifié ou la taille du processus dans la mémoire réelle plus le swap.

Spécifiez le processus par son nom de commande ou son ID de processus (PID). La saisie d'un PID écrase la saisie d'un nom de commande. Si aucun nom de commande ou aucun PID n'est saisi, l'erreur « Command not found » (commande introuvable) est affichée et l'état de la sonde deviendra CRITICAL.

Tableau A.71. Paramètres Red Hat Satellite::Process Health

Champ	Valeur
Command Name (nom de commande)	
Process ID (PID) file (fichier PID)	
Timeout* (délai d'attente)	15
Critical Maximum CPU Usage (utilisation du CPU maximum pour le statut critical)	

Champ	Valeur
Warning Maximum CPU Usage (utilisation du CPU maximum pour le statut warning)	
Critical Maximum Child Process Groups (groupes de processus enfants maximum pour le statut critical)	
Warning Maximum Child Process Groups (groupes de processus enfants maximum pour le statut warning)	
Critical Maximum Threads (threads maximum pour le statut critical)	
Warning Maximum Threads (threads maximum pour le statut warning)	
Critical Maximum Physical Memory Used (mémoire physique utilisée maximum pour le statut critical)	
Warning Maximum Physical Memory Used (mémoire physique utilisée maximum pour le statut warning)	
Critical Maximum Virtual Memory Used (mémoire virtuelle utilisée maximum pour le statut critical)	
Warning Maximum Virtual Memory Used (mémoire virtuelle utilisée maximum pour le statut warning)	

A.10.10. Red Hat Satellite::Process Running

La sonde Red Hat Satellite::Process Running vérifie que le processus spécifié est en cours d'exécution. Spécifiez le processus par son nom de commande ou son ID de processus (PID). La saisie d'un PID écrase la saisie d'un nom de commande. Un statut Critical résulte si la sonde ne peut pas vérifier la commande ou le PID.

Tableau A.72. Paramètres Red Hat Satellite::Process Running

Champ	Valeur
Command Name (nom de commande)	
Process ID (PID) file (fichier PID)	
Critical Number Running Maximum (nombre en cours d'exécution maximum pour le statut critical)	
Critical Number Running Minimum (nombre en cours d'exécution minimum pour le statut critical)	

A.10.11. Red Hat Satellite::Swap

La sonde Red Hat Satellite::Swap contrôle le pourcentage d'espace swap libre disponible sur un Satellite. Un statut CRITICAL résulte si la valeur passe en-dessous de la limite Critical. Un statut WARNING résulte si la valeur passe en-dessous de la limite Warning.

Tableau A.73. Paramètres Red Hat Satellite::Swap

Champ	Valeur
Critical Minimum Swap Percent Free (pourcentage de swap libre minimum pour le statut critical)	
Warning Minimum Swap Percent Free (pourcentage de swap libre minimum pour le statut warning)	

A.10.12. Red Hat Satellite::Users

La sonde Red Hat Satellite::Users contrôle le nombre d'utilisateurs actuellement connectés sur un Satellite. Un statut CRITICAL résulte si la valeur passe en-dessous de la limite Critical. Un statut WARNING résulte si la valeur passe en-dessous de la limite Warning.

Tableau A.74. Paramètres Red Hat Satellite::Users

Champ	Valeur
Critical Maximum Users (utilisateurs maximum pour le statut critical)	
Warning Maximum Users (utilisateurs maximum pour le statut warning)	

ANNEXE B. HISTORIQUE DES VERSIONS

Version 4-32.2.400 **2013-10-31** **Rüdiger Landmann**
Rebuild with publican 4.0.0

Version 4-32.2 **Fri Aug 30 2013** **Sam Friedmann**
Brewed for fr-FR

Version 4-32.1 **Fri Aug 30 2013** **Terry Chuang**
Fichiers de traduction synchronisés avec les sources XML 4-32

Version 4-32 **Thu Aug 29 2013** **Dan Macpherson**
Première implémentation des commentaires de la révision QE

Version 4-31 **Tue Aug 27 2013** **Dan Macpherson**
Modifications mineures

Version 4-30 **Tue Aug 27 2013** **Dan Macpherson**
Implémentation QE Finale

Version 4-29 **Tue Aug 27 2013** **Dan Macpherson**
Correction du texte de l'écran

Version 4-28 **Tue Aug 27 2013** **Dan Macpherson**
Suppression des balises computeroutput

Version 4-27 **Tue Aug 27 2013** **Dan Macpherson**
Implémentation des commentaires de BZ#1001385

Version 4-26 **Tue Aug 27 2013** **Dan Macpherson**
Implémentation des commentaires QE de BZ#1001385

Version 4-25 **Tue Aug 27 2013** **Dan Macpherson**
Correction typographique mineure pour BZ#1001378

Version 4-24 **Tue Aug 27 2013** **Dan Macpherson**
Implémentation des commentaires QE basés sur BZ#1001378 et BZ#1001379

Version 4-23 **Tue Aug 27 2013** **Dan Macpherson**
Implémentation des commentaires QE pour BZ#1001376

Version 4-22 **Thu Aug 15 2013** **Dan Macpherson**
Correction d'erreurs typographiques pour la révision QE

Version 4-21 **Sun Jul 28 2013** **Dan Macpherson**
Seconde implémentation des commentaires de la révision technique

Version 4-20 **Wed Jul 24 2013** **Dan Macpherson**
Corrections pour BZ#987245

Version 4-19 **Tue Jul 23 2013** **Dan Macpherson**
Première implémentation des commentaires de la révision technique

Version 4-18 **Thu Jul 12 2013** **Dan Macpherson**
Mises à jour Bêta finales

Version 4-17 **Thu Jul 12 2013** **Dan Macpherson**

Mise à jour Bêta

Version 4-16 **Thu Jul 11 2013** **Athene Chan**

Modification de la section Splice.

Ajout de contenu supplémentaire sur ISS.

Version 4-15 **Fri Jul 5 2013** **Athene Chan**

BZ#906577 Modifications ISS après révision des développeurs.

Version 4-14 **Fri Jul 5 2013** **Athene Chan**

BZ#906577 Informations supplémentaires sur les nouvelles fonctionnalités ISS incluses.

Version 4-13 **Fri June 28 2013** **Athene Chan**

Mise à jour de toutes les sections basée sur les modifications de l'interface utilisateur.

Modification de toutes les occurrences de "Red Hat Proxy" en "Red Hat Satellite Proxy" basé sur le changement du nom de la marque.

BZ#906577 Ajout d'informations sur Intersatellite-sync.

Version 4-12 **Tue June 4 2013** **Athene Chan**

BZ#969091 Modification du nom de fichier obsolète /etc/rhn/rhn_web.conf en /etc/rhn/rhn.conf.

Version 4-11 **Fri May 17 2013** **Athene Chan**

Modification des procédures en se basant sur l'interface utilisateur.

Préparation pour révision.

Version 4-10 **Thu Apr 25 2013** **Athene Chan**

BZ#908911 Toutes les références à up2date ont été modifiées pour les versions actuelles.

BZ#927113, 950295 Le résumé de l'ouvrage a été mis à jour

BZ#927546, 924221 Modifications mineures des termes standardisés

Modification du contenu pour la prochaine version.

Version 4-9 **Thu Feb 28 2013** **Athene Chan**

Table des matières modifiée en préparation de la prochaine version.

Version 4-8 **Wed Jan 2 2013** **Athene Chan**

BZ#862950 Espace entre « (pup) » et « that » (cela) inclus.

Version 4-7 **Wed Sept 19 2012** **Dan Macpherson**

Mise en paquetage finale pour 5.5

Version 4-6 **Thu Aug 16 2012** **Athene Chan**

BZ#847993 Nom de fichier modifié dans l'exemple de la section 5.2.4

Version 4-5 **Thu Aug 16 2012** **Athene Chan**

BZ#773647 Mise à jour des paragraphes concernant la capture d'écran « Créer un nouveau compte »

BZ#846691 Mise à jour du lien « buy » (achat) dans la section 1.1

Version 4-4 **Wed Aug 15 2012** **Athene Chan**

BZ#773647 Mise à jour de la capture d'écran « Créer un nouveau compte »

Version 4-3 **Thu Aug 9 2012** **Athene Chan**

Mise en pré-production des documents pour révision

Version 3-2 **Fri Aug 3 2012** **Athene Chan**

BZ#844849 Paragraphe restructuré.

Version 3-1 **Tue Jun 17 2012** **Athene Chan**

Contenu déprécié supprimé. Préparé pour la version 5.5
BZ#837703 Ajout d'une note sur les clés GPG personnalisées

Version 3-0 **Thurs May 24 2012** **Athene Chan**
BZ#783340 - Mise à jour de "s390x" vers "IBM System z"

Version 2-6 **Mon Jan 9 2012** **Lana Brindley**
BZ#707591 - Chapitre sur la virtualisation - mise à jour des instructions
BZ#746640 - Chapitre sur la virtualisation - ajout d'informations kickstart

Version 2-5 **Wed Jan 4 2012** **Lana Brindley**
BZ#707568 & BZ#707570 - Chapitre sur la virtualisation - noms des canaux
BZ#744653 - Chapitre sur la virtualisation - erreurs typographiques
BZ#744656 - Chapitre sur la virtualisation - mise à jour des instructions RHEL 6
BZ#750481 - Mise à jour de la méthode pour changer la taille de fichier maximale
BZ#766424 - Chapitre Kickstart - mise à jour du texte

Version 2-4 **Fri Sep 23 2011** **Lana Brindley**
BZ#702516 - Manuel Unix
BZ#703605 - Chapitre Monitoring (contrôle)
BZ#706868 & BZ#707169 - Chapitre Cobbler
BZ#707591 - Chapitre sur la virtualisation
BZ#707602 - Chapitre sur la virtualisation
BZ#715267 - Erreurs typographiques

Version 2-3 **Mon Aug 15 2011** **Lana Brindley**
Version du flux z plié dans le flux y

Version 2-2 **Wed Jun 15 2011** **Lana Brindley**
Préparé pour traduction

Version 2-1 **Fri May 27 2011** **Lana Brindley**
Mises à jour de la part des traducteurs

Version 2-0 **Fri May 6 2011** **Lana Brindley**
Préparé pour traduction

Version 1-29 **Fri March 25 2011** **Lana Brindley**
Entités corrigées pour la traduction
BZ#683466 - Monitoring

Version 1-28 **Thu March 24 2011** **Lana Brindley**
BZ#679621 - Entités corrigées pour la traduction
BZ#681788 - Notifications

Version 1-27 **Mon Feb 14 2011** **Lana Brindley**
BZ#658127 - API Access

Version 1-26 **Wed Feb 9 2011** **Lana Brindley**
BZ#658120 - Remove RHEL 2.1 references
BZ#658131 - API Access
BZ#669166 - Virtualization

Version 1-25 **Mon Jan 31 2011** **Lana Brindley**
BZ#443630 - Kickstart
BZ#559515 - Cobbler