



Red Hat Network Satellite 5.5

Guide d'installation du proxy

Red Hat Network Satellite

Édition 3

Red Hat Network Satellite 5.5 Guide d'installation du proxy

Red Hat Network Satellite
Édition 3

Red Hat Équipe de documentation

Notice légale

Copyright © 2010 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Résumé

Bienvenue sur le guide d'installation du proxy RHN

Table des matières

CHAPITRE 1. INTRODUCTION	3
1.1. RED HAT NETWORK	3
1.2. TERMINOLOGIE FRÉQUEMMENT UTILISÉE	3
1.3. RHN PROXY SERVER	4
1.4. FONCTIONNEMENT DU PROXY	5
CHAPITRE 2. BESOINS	7
2.1. BESOINS LOGICIELS	7
2.2. BESOINS MATÉRIELS	8
2.3. BESOINS D'ESPACE DISQUE	8
2.4. BESOINS SUPPLÉMENTAIRES	8
CHAPITRE 3. EXEMPLE DE TOPOLOGIES	11
3.1. TOPOLOGIE D'UN PROXY UNIQUE	11
3.2. TOPOLOGIE DE PLUSIEURS PROXYS EN PLUSIEURS NIVEAUX HORIZONTAUX	11
3.3. TOPOLOGIE DE PLUSIEURS PROXYS EN PLUSIEURS NIVEAUX VERTICAUX	12
3.4. PROXYS AVEC SERVEUR RHN SATELLITE	13
CHAPITRE 4. INSTALLATION	14
4.1. INSTALLATION DE BASE	14
4.2. PROCESSUS D'INSTALLATION DE RHN PROXY SERVER	14
4.2.1. Le fichier Answer (réponse)	18
CHAPITRE 5. RHN PACKAGE MANAGER ET LA DESSERTE DE PAQUETAGES LOCAUX	19
5.1. CRÉER UN CANAL PRIVÉ	20
5.2. TÉLÉCHARGER DES PAQUETAGES	21
CHAPITRE 6. MISE À NIVEAU DE L'INSTALLATION	23
6.1. PRÉREQUIS	23
6.2. PROCESSUS DE MISE À NIVEAU DE L'INSTALLATION	23
CHAPITRE 7. RÉOLUTION DE PROBLÈMES	25
7.1. GÉRER LE SERVICE PROXY	25
7.2. FICHIERS JOURNAUX	25
7.3. QUESTIONS ET RÉPONSES	26
7.4. PROBLÈMES GÉNÉRAUX	27
7.5. IMPOSSIBLE DE TROUVER L'HÔTE / IMPOSSIBLE DE DÉTERMINER LE FQDN (NOMS DE DOMAINE ENTièrement QUALIFIÉS)	27
7.6. ERREURS DE CONNEXION	28
7.7. PROBLÈMES DE CACHE	28
7.8. DÉBOGAGE DU PROXY PAR RED HAT	29
ANNEXE A. EXEMPLE DE FICHIER DE CONFIGURATION DE RHN PROXY SERVER	31
ANNEXE B. HISTORIQUE DES VERSIONS	32
INDEX	33

CHAPITRE 1. INTRODUCTION

1.1. RED HAT NETWORK

Red Hat Network (RHN) est l'environnement pour l'assistance au niveau du système et la gestion de systèmes et de réseaux de systèmes Red Hat. Red Hat Network rassemble les outils, les services et les référentiels d'informations nécessaires pour maximiser la fiabilité, la sécurité et la performance des systèmes. Pour utiliser RHN, les administrateurs système enregistrent les profils logiciels et matériels, appelés Profils de système, de leurs systèmes client avec Red Hat Network. Lorsqu'un système client requiert des mises à jour de paquetages, seuls les paquetages disponibles pour le client sont retournés (selon le profil logiciel stocké sur les serveurs RHN).

Avantages de l'utilisation de Red Hat Network :

- **Évolutivité** — avec Red Hat Network, un seul administrateur système peut installer et maintenir des centaines ou des milliers de systèmes Red Hat plus facilement, plus exactement et plus rapidement que ce même administrateur pourrait maintenir un seul système sans Red Hat Network.
- **Protocoles standards** — des protocoles standards sont utilisés pour maintenir la sécurité et augmenter les capacités. Par exemple, XML-RPC permet à Red Hat Network d'effectuer bien plus que le simple téléchargement des fichiers.
- **Sécurité** — toutes les communications entre les systèmes enregistrés et Red Hat Network se produisent sur des connexions internet sécurisées.
- **Affichage des alertes d'errata** — vous pouvez facilement afficher les alertes d'errata pour tous vos systèmes client grâce à un seul site web.
- **Actions programmées** — utilisez le site web pour programmer des actions, y compris des mises à jour d'errata, des installations de paquetages et des mises à jour de profils logiciels.
- **Simplification** — la maintenance de systèmes Red Hat devient un processus plus simple et automatisé.

1.2. TERMINOLOGIE FRÉQUEMMENT UTILISÉE

Avant de comprendre RHN Proxy Server, il est important de se familiariser avec les termes de Red Hat Network suivants :

Voie/canal

Un canal est une liste de paquetages de logiciels. Il existe deux types de canaux : les canaux de base et les canaux enfant. Un *canal de base* consiste en une liste de paquetages basée sur une architecture spécifique et une version de Red Hat. Un *canal enfant* est un canal associé à un canal de base qui contient des paquetages supplémentaires.

Administrateur d'organisations

Administrateur d'organisations est un rôle d'utilisateur qui comporte le plus haut niveau de contrôle sur le compte Red Hat Network d'une organisation. Les détenteurs de tels rôles peuvent ajouter d'autres utilisateurs, d'autres systèmes et d'autres groupes de systèmes à une organisation, ainsi que les supprimer. Une organisation Red Hat Network doit comporter au moins un administrateur d'organisations.

Administrateur de canaux

Administrateur de canaux est un rôle d'utilisateur qui détient un accès complet aux capacités de gestion des canaux. Les détenteurs de tels rôles peuvent créer des canaux et assigner des paquetages à ces canaux. Ce rôle peut être assigné par un administrateur d'organisations via l'onglet **Utilisateurs** sur le site web RHN.

Agent de mise à jour « Red Hat Update Agent »

L'agent de mise à jour « Red Hat Update Agent » est une application client Red Hat Network (**up2date** ou **yum**) qui permet aux utilisateurs d'extraire et d'installer les paquetages nouveaux ou mis à jour pour le système client sur lequel l'application est exécutée.

Traçage « Traceback »

Un traceback est une description en détail de « ce qui n'a pas fonctionné » utile pour les résolutions de problèmes de RHN Proxy Server. Les traceback sont automatiquement générés lorsqu'une erreur critique se produit et sont envoyés par courriel aux individus désignés dans le fichier de configuration de RHN Proxy Server.

Pour davantage d'explications sur ces termes et sur d'autres, voir le *Guide de référence Red Hat Network*, disponible à <http://www.redhat.com/docs/manuals/satellite/> et sur la page **Help** de l'interface utilisateur web de Satellite.

1.3. RHN PROXY SERVER

RHN Proxy Server est un mécanisme de mise en cache de paquetages qui réduit les besoins en bande passante de RHN et permet le déploiement de paquetages personnalisés. Les utilisateurs de Proxy mettent en cache des RPM, comme Errata Updates de Red Hat ou des RPM personnalisés et générés par leur organisation, sur un serveur interne situé centralement. Les systèmes clients reçoivent ces mises à jour du Proxy plutôt qu'en accédant à l'internet individuellement.

Malgré que les paquetages soient desservis par le Proxy, les profils systèmes des clients et les informations d'utilisateur sont stockés sur les serveurs centraux de RHN sécurisés^[1], qui desservent également le site RHN (rhn.redhat.com). Le Proxy agit comme navette entre les systèmes des clients et Red Hat Network (ou RHN Satellite Server). Seuls les fichiers de paquetages sont stockés sur RHN Proxy Server. Chaque transaction est authentifiée, et l'agent de mise à jour Red Hat Update Agent vérifie les signatures GPG de chaque paquetage récupéré du serveur RHN Proxy Server local.

En plus de stocker les paquetages Red Hat officiels, RHN Proxy Server peut être configuré pour fournir les paquetages personnalisés d'une organisation à partir de *canaux* RHN privés, en utilisant le gestionnaire de paquetages « RHN Package Manager ». Par exemple, une organisation pourrait développer son propre logiciel, le mettre en paquetage dans un RPM, y apposer sa propre signature GPG, et soumettre tous les systèmes individuels du réseau à toutes les dernières mises à jour du logiciel personnalisé par le serveur RHN Proxy Server local.

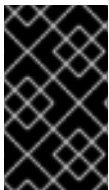
Les avantages liés à l'utilisation de RHN Proxy Server incluent :

- Évolutivité — plusieurs RHN Proxy Server locaux peuvent exister au sein d'une même organisation.
- Sécurité — une connexion sécurisée de bout en bout est maintenue : depuis les systèmes client au serveur RHN Proxy Server local, et jusqu'aux serveurs Red Hat Network.
- Temps économisé — les paquetages sont fournis bien plus rapidement sur un réseau local que par l'internet.

- Économie de bande — les paquetages sont téléchargés du RHN en une seule fois (grâce au mécanisme cache du serveur proxy) au lieu d'être téléchargés individuellement pour chaque client.
- Mises à jour personnalisées — pour créer un système de livraison de paquetages véritablement automatisé pour les paquetages logiciels personnalisés, ainsi que les paquetages officiels de Red Hat requis pour les systèmes client. Les canaux RHN privés personnalisés permettent à une organisation d'automatiser la livraison de paquetages internes.
- Configuration personnalisée — restreindre et donner des mises à jour à des architectures et des versions SO (source ouverte) spécifiques.
- Une seule connexion internet nécessaire — car les clients se connectent à RHN Proxy Server et non pas à l'internet, ils ont uniquement besoin d'une connexion LAN (réseau local) vers le serveur proxy. Seul RHN Proxy Server a besoin d'une connexion internet afin de pouvoir contacter les serveurs RHN, à moins que RHN Proxy Server utilise RHN Satellite Server, dans quel cas seul RHN Satellite Server nécessite une connexion internet.

1.4. FONCTIONNEMENT DU PROXY

L'agent Red Hat Update Agent, ou **Package Updater** des systèmes client ne contacte pas directement un serveur Red Hat Network. A la place, le client (ou les clients) se connectent à un serveur RHN Proxy Server qui se connecte à son tour à des serveurs Red Hat Network ou à RHN Satellite Server. Ainsi, les systèmes client n'ont pas besoin d'un accès direct à l'internet. Ils ont uniquement besoin d'accéder à RHN Proxy Server.



IMPORTANT

Red Hat recommande fortement que les clients qui se connectent à RHN Proxy Server appliquent les dernières mises à jour de Red Hat Enterprise Linux afin d'assurer une bonne connectivité.

Les clients qui accèdent directement à RHN sont authentifiés par les serveurs RHN. Les clients qui accèdent à RHN Proxy Server sont toujours authentifiés par RHN ; cependant, dans ce cas précis, le Proxy offre les informations sur l'authentification et le chemin d'accès à RHN. Après une authentification réussie, le serveur Red Hat Network informe RHN Proxy Server qu'il a le droit d'exécuter certaines actions pour le client. RHN Proxy Server télécharge alors tous les paquetages mis à jour (s'ils ne sont pas déjà présents en cache) et les livre au système client.

Les demandes de l'agent Red Hat Update Agent ou de Package Updater sur les systèmes client sont toujours authentifiées du côté du serveur, mais la remise des paquetages est bien plus rapide puisque les paquetages sont mis en cache dans le serveur HTTP Proxy Caching Server ou RHN Proxy Server (pour les paquetages locaux) ; RHN Proxy Server et le système client sont connectés par LAN et ne sont limités que par la vitesse du réseau local.

L'authentification est effectuée dans l'ordre suivant :

1. Le client effectue une action de connexion au début d'une session client. Cette connexion est transmise à travers un ou plusieurs RHN Proxy Server jusqu'à atteindre un serveur Red Hat Network.
2. Le serveur Red Hat Network tente d'authentifier le client. Si l'authentification réussit, le serveur passe alors un jeton de session par la chaîne de serveurs RHN Proxy Server. Ce jeton, qui porte une signature et une date d'expiration, contient les informations utilisateur, les abonnements aux canaux, les noms d'utilisateur, etc.

3. Chaque RHN Proxy Server met en cache ce jeton sur le système de fichiers local dans `/var/cache/rhn/`. La mise en cache réduit une partie du temps système de l'authentification avec les serveurs Red Hat Network et améliore considérablement la performance de Red Hat Network.
4. Ce jeton de session est renvoyé à la machine client et est utilisé dans les actions suivantes sur Red Hat Network.

Du point de vue du client, il n'y a pas de différence entre RHN Proxy Server et un serveur Red Hat Network. Du point de vue du serveur Red Hat Network, RHN Proxy Server est un type de client RHN spécial. Les clients ne sont donc pas affectés par le chemin pris par une requête pour atteindre un serveur Red Hat Network. Toute la logique est implémentée dans les serveurs RHN Proxy Server et Red Hat Network.

Optionnellement, le gestionnaire de paquetages RHN (« RHN Package Manager ») peut être installé et configuré pour desservir des paquetages personnalisés. Tout paquetage qui n'est pas un paquetage officiel de Red Hat, y compris les paquetages personnalisés spécifiquement écrits pour une organisation, peuvent uniquement être desservis à partir d'un canal logiciel privé (aussi appelé canal logiciel personnalisé). Après avoir créé un canal privé RHN, les paquetages RPM personnalisés lui sont associés en téléchargeant les en-têtes des paquetages sur les serveurs RHN. Seuls les en-têtes sont téléchargés, et non pas les fichiers des paquetages. Les en-têtes sont requis car ils contiennent des informations RPM cruciales, comme les dépendances de logiciels, ce qui permet à RHN d'automatiser l'installation du paquetage. Les paquetages RPM personnalisés sont stockés sur le serveur RHN Proxy Server et envoyés aux systèmes client à partir du réseau local de l'organisation.

Il est simple de configurer un réseau informatique en utilisant des serveurs RHN Proxy Servers. Les applications Red Hat Network des systèmes client doivent être configurées de façon à se connecter sur RHN Proxy Server à la place des serveurs Red Hat Network. Reportez-vous au *Guide de configuration du client RHN* pour davantage de détails. Du côté du Proxy, il faut spécifier le proxy suivant dans la chaîne (qui se termine finalement par un serveur Red Hat Network). Si le gestionnaire de paquetages RHN (« RHN Package Manager ») est utilisé, les systèmes client doivent être abonnés à un canal RHN privé.

[1] Tout au long de ce document, « RHN » fera soit référence au site hébergé de RHN (<http://rhn.redhat.com>) ou à RHN Satellite Server.

CHAPITRE 2. BESOINS

Ce chapitre se concentre sur les conditions devant être remplies avant de pouvoir installer RHN Proxy Server. Souvenez-vous que le Satellite doit être d'une version supérieure ou égale à la version du Proxy que vous essayez d'installer. Par exemple, pour installer RHN Proxy Server 5.4, la version de Satellite devrait être 5.4 ou une version supérieure et ne peut pas être 5.3 ou une version antérieure.

2.1. BESOINS LOGICIELS

Pour effectuer une installation, les composants logiciels suivants doivent être disponibles :

- Système d'exploitation de base — RHN Proxy Server est pris en charge sur Red Hat Enterprise Linux 5 et 6. Le système d'exploitation peut être installé depuis un disque, une image ISO locale, avec kickstart ou toute autre méthode prise en charge par Red Hat.

RHN Proxy Server peut être installé sur Red Hat Enterprise Linux 5 et 6 dans n'importe quel environnement virtualisé pris en charge par Red Hat, y compris Xen, KVM et VMware.

Notez que pour les déploiements de production, nous vous conseillons de déployer RHN Proxy Server comme seule application exécutée sur le matériel physique sous-jacent pour éviter les problèmes de contention. Aussi, réalisez bien que le support fonctionnel d'environnement virtualisé n'est pas toujours équivalent à la performance de l'exécution sur du matériel physique, vous devrez considérer avec soin votre environnement virtualisé de choix et les réglages recommandés.



NOTE

Chaque produit RHN Proxy acheté inclut une instance prise en charge de Red Hat Enterprise Linux Server. Le Proxy RHN doit être installé sur une nouvelle installation de Red Hat Enterprise Linux pour laquelle le Proxy RHN est la seule application ou service fourni par le SE. L'utilisation du SE Red Hat Enterprise Linux inclus avec RHN Proxy pour exécuter d'autres démons, applications, ou services dans votre environnement n'est pas prise en charge.

Chaque version de Red Hat Enterprise Linux requiert un certain ensemble de paquetages pour prendre en charge RHN Proxy Server. L'ajout de tout autre paquetage peut provoquer des erreurs durant l'installation. Red Hat recommande donc d'obtenir l'ensemble de paquetages désirés de la manière suivante :



NOTE

Pour le kickstart, spécifier le groupe de paquetages suivant : @ **Base**

Pour l'installation de Red Hat Enterprise Linux via CD ou image ISO, veuillez sélectionner le groupe de paquetages suivant : **Minimal**

- Un droit d'accès RHN Proxy Server disponible dans le compte RHN Satellite Server.
- Un droit d'accès Provisioning dans le compte RHN Satellite Server (qui devrait être dans un paquetage avec le droit d'accès RHN Proxy Server).

- Accès au canal Red Hat Network Tools pour la version installée de Red Hat Enterprise Linux. Ce canal inclut le paquetage **spacewalk-proxy-installer** qui contient le programme d'installation **configure-proxy.sh** requis pour installer RHN Proxy Server.
- Tous les paquetages **rhncfg*** installés sur le Proxy (du canal "RHN Tools").
- Le paquetage **spacewalk-certs-tools** installé sur le Proxy (du canal « RHN Tools ») pour les utilisateurs RHN Hosted, ou le mot de passe du certificat CA (SSL) utilisé pour générer le certificat de serveur parent pour les utilisateurs de RHN Satellite Server.
- Configuration du système pour accepter les commandes à distance et la gestion de configuration via Red Hat Network si vous utilisez la méthode d'installation dépréciée de l'interface utilisateur web. Consultez [Section 4.2, « Processus d'installation de RHN Proxy Server »](#) pour obtenir des instructions.

2.2. BESOINS MATÉRIELS

La configuration matérielle suivante est requise pour RHN Proxy Server :

- Processeur Pentium IV ou équivalent
- 512 Mo de mémoire
- Au moins 5 Go de stockage pour l'installation de base de Red Hat Enterprise Linux
- 6 Go de stockage par distribution ou canal

La charge sur le serveur web Apache est directement liée à la fréquence à laquelle les systèmes client se connectent au Proxy. Si vous réduisez donc l'intervalle par défaut de quatre heures (ou 240 minutes) définie dans le fichier de configuration **/etc/sysconfig/rhn/rhnsd** des systèmes client, vous *augmenterez* considérablement la charge sur ce composant.

2.3. BESOINS D'ESPACE DISQUE

Le mécanisme de mise en cache utilisé par RHN Proxy Server est le proxy HTTP Squid, qui économise une quantité de bande importante pour les clients. Une quantité raisonnable d'espace devrait être disponible. Les paquetages mis en cache sont stockés dans **/var/spool/squid**. L'allocation d'espace libre requise est de 6 Go de stockage par distribution ou par canal.

Si RHN Proxy Server est configuré pour distribuer des paquetages personnalisés ou locaux, assurez-vous que le point de montage **/var** sur le système stockant les paquetages locaux, possède suffisamment d'espace disque pour contenir tous les paquetages personnalisés, qui sont stockés dans **/var/spool/rhn-proxy**. L'espace disque requis pour les paquetages locaux dépend du nombre de paquetages personnalisés servis.

2.4. BESOINS SUPPLÉMENTAIRES

Les besoins supplémentaires suivants doivent être satisfaits pour que l'installation de RHN Proxy Server puisse être considérée comme terminée :

Accès total

Les systèmes client ont besoin d'un accès réseau total sur les services et les ports RHN Proxy Server.

Règles de pare-feu

RHN recommande fortement de dresser un pare-feu (firewall) entre la solution RHN Proxy Server et l'internet. Malgré tout, plusieurs ports TCP doivent être ouvert sur le proxy, selon votre implémentation de RHN Proxy Server :

Tableau 2.1. Ports à ouvrir sur le proxy

Port	Direction	Raison
80	Sortie	Le proxy utilise ce port pour atteindre rhn.redhat.com , xmlrpc.rhn.redhat.com , ainsi que l'URL de votre Satellite (suivant si RHN Proxy s'adresse à RHN Hosted ou à un serveur Satellite).
80	Entrée	Les demandes client arrivent soit par http ou par https
443	Entrée	Les demandes client arrivent soit par http ou par https
443	Sortie	Le proxy utilise ce port pour atteindre rhn.redhat.com , xmlrpc.rhn.redhat.com , ainsi que l'URL de votre Satellite (suivant si le RHN Proxy s'adresse à RHN Hosted ou à un serveur Satellite).
4545	Sortie	Si votre proxy est connecté à un serveur RHN Satellite, le Monitoring établit des connexions sur rhnmmd en cours d'exécution sur les systèmes client via le port TCP, si le contrôle Monitoring est activé et si les sondes ou vérifications sont configurées dans les systèmes enregistrés.
5222	Entrée	L'ouverture de ce port permet osad d'établir des connexions client au démon du proxy en cas d'utilisation de la technologie RHN Push.
5269	Sortie	Si votre proxy est connecté à un serveur RHN Satellite, ce port doit être ouvert pour permettre des connexions de serveur-à-serveur via jabberd pour la technologie RHN Push.

Temps de système synchronisés

Les paramètres de temps sont très importants lors d'une connexion sur un serveur web qui exécute SSL (Secure Sockets Layer, couche de sockets sécurisés). Il est impératif que les paramètres de temps sur les clients et le serveur soient raisonnablement proches pour que le certificat SSL n'expire pas avant ou pendant son utilisation. Il est recommandé que le protocole de temps réseau NTP (Network Time Protocol) soit utilisé afin de synchroniser les horloges.

Nom de domaine complet (FQDN)

Le système sur lequel RHN Proxy Server sera installé doit résoudre son propre nom de domaine complet (FQDN) correctement.

Un compte Red Hat Network

Les clients qui se connectent aux serveurs centraux Red Hat Network pour recevoir des mises à jour incrémentielles doivent posséder un compte Red Hat Network. Ce compte devrait être défini au moment de l'achat avec le représentant des ventes.

Sauvegardes des informations de connexion

Il est impératif que les clients conservent toutes les informations de connexion primaires. Pour RHN Proxy Server, celles-ci incluent les noms d'utilisateur et les mots de passe pour le compte d'administrateur d'organisation, la génération du certificat SSL. Red Hat recommande fortement que ces informations soient copiées sur deux différents disques (CD, DVD, ou disques durs amovibles), imprimées sur papier et stockées dans un coffre-fort.

Emplacements de distribution

Vu que le proxy transmet virtuellement toutes les requêtes HTTP locales aux serveurs RHN centraux, vous devez faire attention à mettre les fichiers destinés à la distribution (comme dans une arborescence d'installation kickstart) dans l'emplacement de non-transmission du proxy : **/var/www/html/pub/**. Les fichiers placés dans ce répertoire peuvent être directement téléchargés du Proxy. Ceci peut être particulièrement utile pour la distribution des clés GPG ou lors de l'établissement d'arborescences d'installation pour des kickstarts.

De plus, Red Hat recommande que le système qui exécute le code ne soit pas disponible publiquement. Seuls les administrateurs système devraient avoir l'accès shell à ces machines. Tous les services non nécessaires devraient être désactivés. Vous pouvez utiliser **ntsysv** ou **chkconfig** pour désactiver les services.

Finalement, vous devriez avoir à votre disposition les documents techniques suivants et dans l'ordre suivant :

1. Le *Guide d'installation RHN Proxy Server* — Ce guide, que vous êtes en train de lire, fournit les étapes essentielles nécessaires à la configuration et au fonctionnement d'un serveur RHN Proxy.
2. Le *Guide de configuration du client RHN* — Ce guide explique comment configurer les systèmes qui seront servis par RHN Proxy Server ou par RHN Satellite Server. (ce qui nécessitera aussi probablement d'obtenir des références au *Guide de référence RHN*, qui contient des étapes pour enregistrer et mettre à jour les systèmes.)
3. Le *Guide de gestion de canaux de RHN* — Ce guide identifie précisément les méthodes recommandées pour construire des paquetages personnalisés, créer des canaux personnalisés et gérer des errata privés.
4. Le *Guide de référence de RHN* — Ce guide décrit comment créer des comptes RHN, enregistrer et mettre à jour des systèmes et utiliser le site Web de RHN à son maximum. Ce guide sera utile durant l'installation et le processus de configuration.

CHAPITRE 3. EXEMPLE DE TOPOLOGIES

RHN Proxy Server peut être configuré de plusieurs manières. Sélectionnez une méthode selon l'un des facteurs suivants :

1. Le nombre total de systèmes client devant être servis par RHN Proxy Server
2. Le nombre maximum de clients censés se connecter *simultanément* à RHN Proxy Server.
3. Le nombre de paquets et de canaux personnalisés devant être servis par RHN Proxy Server.
4. Le nombre de serveurs RHN Proxy Server utilisés dans l'environnement du client.

Le reste de ce chapitre décrit des configurations possibles et explique leurs avantages.

3.1. TOPOLOGIE D'UN PROXY UNIQUE

La configuration la plus simple est d'utiliser un seul serveur proxy RHN pour servir votre réseau entier. Cette configuration est adéquate pour le service d'un petit groupe de clients et un réseau qui bénéficierait de la mise en cache des RPM de Red Hat et du stockage de paquets personnalisés sur un serveur local.

L'inconvénient de l'utilisation d'un serveur proxy RHN unique est que la performance sera compromise lors de l'augmentation du nombre de clients demandant des paquets.

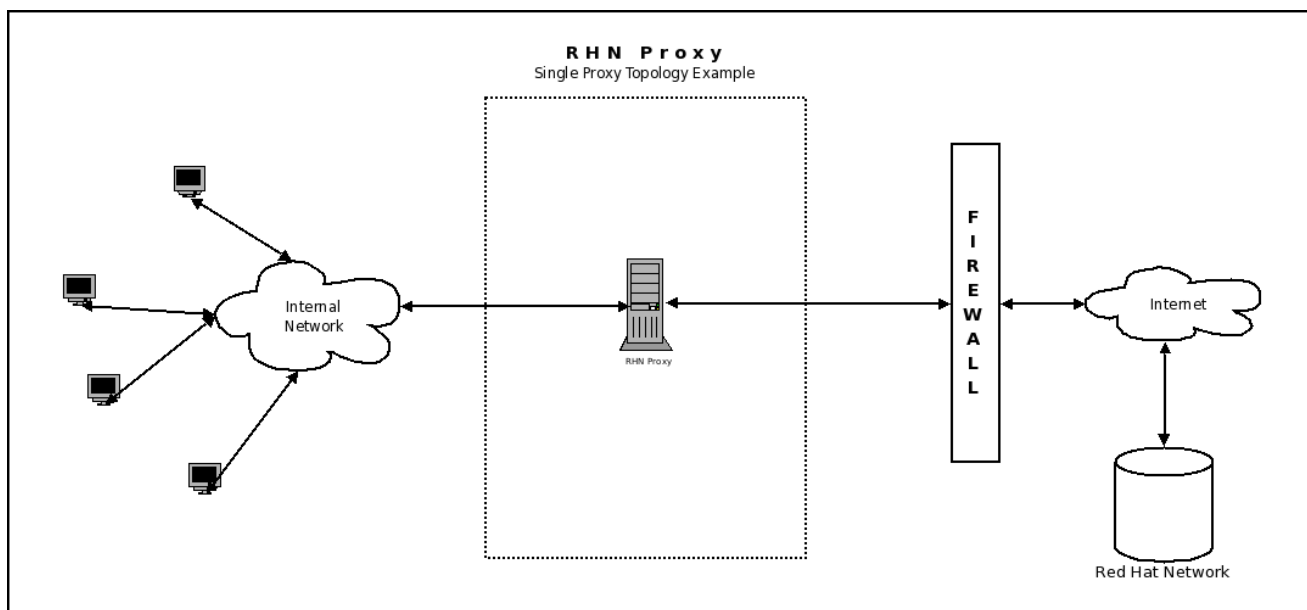


Figure 3.1. Topologie d'un proxy unique

3.2. TOPOLOGIE DE PLUSIEURS PROXYS EN PLUSIEURS NIVEAUX HORIZONTAUX

Pour des réseaux plus grands, une méthode plus distribuée peut être nécessaire, comme le fait d'avoir plusieurs serveurs proxy RHN tous connectés à Red Hat Network de manière individuelle. Cette configuration en plusieurs niveaux horizontaux répartit la charge des requêtes des clients tout en permettant à chaque proxy de se synchroniser simultanément avec RHN.

Un inconvénient de cette structure est que les paquetages personnalisés chargés sur un proxy individuel doivent être distribués sur ses serveurs apparentés (sibling). Cette situation peut être traitée de l'une des deux manières suivantes :

- Le programme de transfert de fichiers **rsync** peut être utilisé pour synchroniser les paquetages entre les proxys
- Un partage NFS (Network File System) peut être établi entre les proxys et le dépôt de canaux personnalisés.

Ces deux solutions permettront à tout client de tout serveur proxy RHN d'avoir tous les paquetages personnalisés livrés.

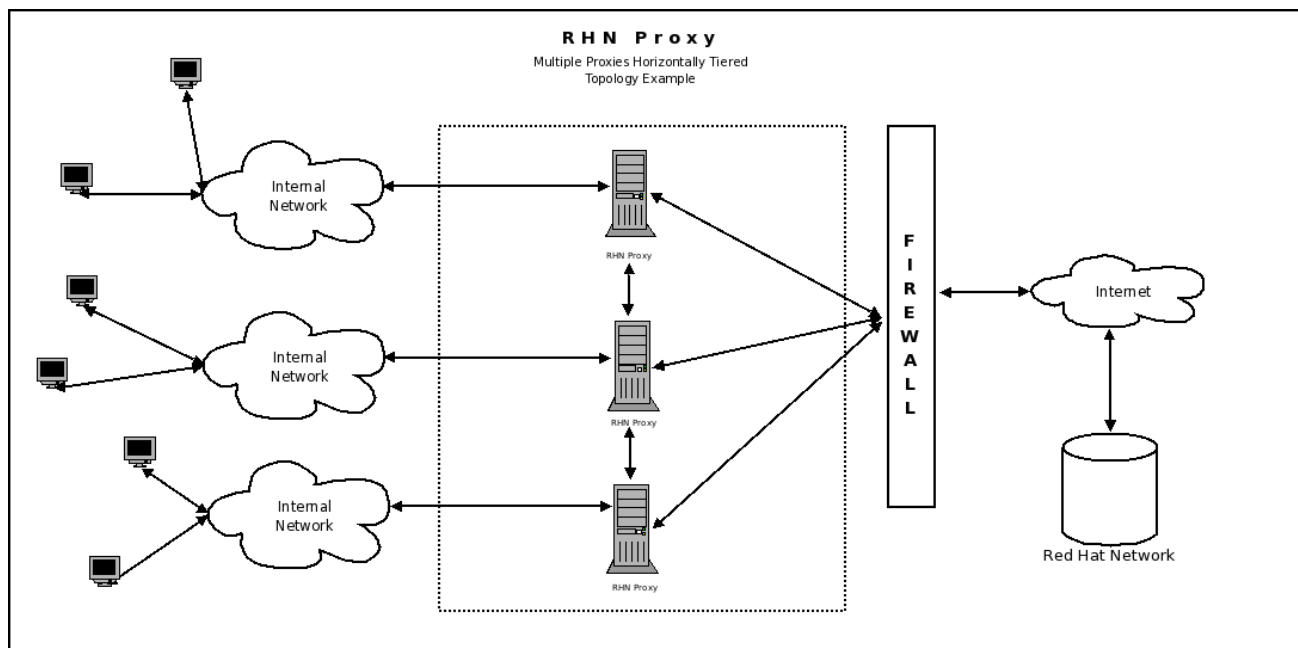


Figure 3.2. Topologie de plusieurs proxys en plusieurs niveaux horizontaux

3.3. TOPOLOGIE DE PLUSIEURS PROXYS EN PLUSIEURS NIVEAUX VERTICAUX

Une autre méthode pour plusieurs serveurs proxy RHN est d'établir un proxy primaire auquel les autres se connectent pour les RPM de Red Hat Network et les paquetages personnalisés créés localement. En essence, les proxys secondaires agissent en tant que clients du primaire. Cela supprime le besoin d'établir une synchronisation entre les serveurs proxy RHN vu qu'ils utilisent la fonction **up2date** inhérente au produit.

Tout comme la configuration horizontale, cette méthode verticale permet à tout client de tout serveurs proxy RHN d'avoir tous les paquetages personnalisés livrés. Le Proxy regarde simplement dans le dépôt s'il trouve le paquetage sur son système de fichiers. Dans le cas contraire, il essaie alors depuis le niveau supérieur.

Cette configuration verticale assure que les proxys secondaires dépendent du primaire pour les mises à jour de RHN, ainsi que pour les paquetages personnalisés. Les canaux et les paquetages personnalisés doivent également être placés uniquement sur le proxy primaire pour assurer la distribution aux proxys enfants. Finalement, les fichiers de configuration des proxys secondaires doivent pointer sur le primaire, et non pas directement sur Red Hat Network.

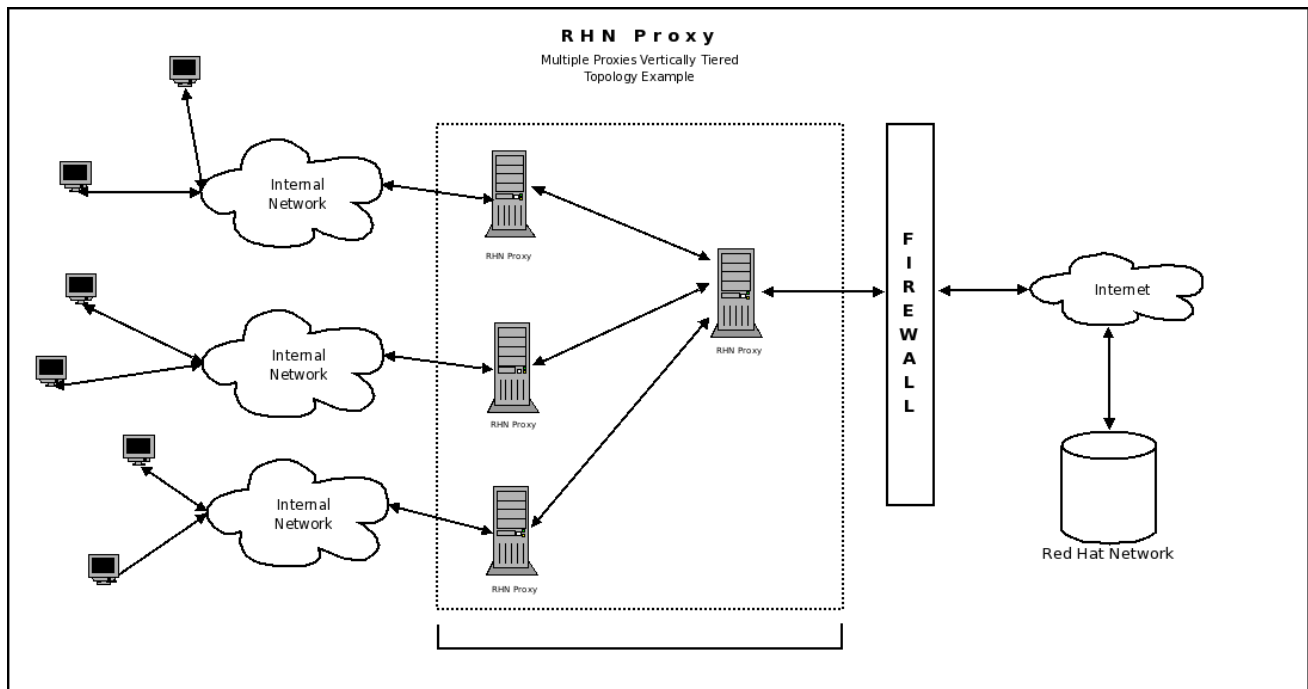


Figure 3.3. Topologie de plusieurs proxys en plusieurs niveaux verticaux

3.4. PROXYS AVEC SERVEUR RHN SATELLITE

En plus des méthodes décrites en détails dans ce chapitre, les clients ont également l'option d'utiliser le serveur proxy RHN en conjonction avec le serveur Satellite RHN. Cela fonctionne de manière similaire à la configuration verticale de Proxy, mais augmente considérablement la capacité, vu que les Satellites peuvent servir un nombre bien plus grand de systèmes client.

Pour une description complète de cette combinaison, consultez le chapitre Exemples de topologies du *Guide d'installation RHN Satellite Server*. La liaison des certificats SSL de deux produits est décrite dans le *Guide de configuration du client de RHN*. Pour savoir comment les canaux et les paquetages sont partagés entre eux, consultez le *Guide de gestion de canaux RHN*.

CHAPITRE 4. INSTALLATION

Ce chapitre décrit l'installation initiale de RHN Proxy Server. Il est présumé que les pré-requis énumérés dans [Chapitre 2, Besoins](#) ont bien été respectés. Cependant, si vous *mettez à niveau* une nouvelle version de RHN Proxy Server, veuillez contacter votre représentant Red Hat pour toute assistance requise.

4.1. INSTALLATION DE BASE

RHN Proxy Server est conçu de façon à fonctionner sur le système d'exploitation Red Hat Enterprise Linux. La première étape est donc d'installer le système d'exploitation de base, depuis un disque, une image ISO ou avec un kickstart. Pendant et après l'installation du système d'exploitation, veuillez vous assurer de bien :

- Allouer suffisamment d'espace aux partitions qui seront utilisées pour stocker les paquets, selon les besoins matériels définis auparavant. L'emplacement par défaut pour les paquets Red Hat en cache est `/var/spool/squid`, alors que les paquets personnalisés se trouvent dans `/var/spool/rhn-proxy`.



NOTE

Le programme d'installation calcule automatiquement l'espace disponible sur la partition où `/var/spool/squid` est monté, il alloue aussi jusqu'à 60 pour cent de l'espace libre pour l'utilisation RHN Proxy Server.

- Installer les paquets requis par RHN Proxy Server.



NOTE

Installez les paquets de base uniquement, car les autres entraîneront l'échec de l'installation RHN Proxy Server.

Consultez [Section 2.1, « Besoins logiciels »](#) pour la méthode d'obtention du bon groupe de paquets, qui est nécessaire pour chaque version de Red Hat Enterprise Linux.

- Activer le protocole de temps réseau NTP (Network Time Protocol) sur le proxy et sélectionner le fuseau horaire approprié. Tous les systèmes client devraient déjà exécuter le démon `ntpd` et avoir le bon fuseau horaire défini.
- Désactiver les services `ipchains` et `iptables` après l'installation.

4.2. PROCESSUS D'INSTALLATION DE RHN PROXY SERVER

Les instructions suivantes décrivent le processus d'installation de RHN Proxy Server :

1. Connectez-vous en tant qu'utilisateur root sur le système RHN Proxy Server souhaité.
2. Enregistrez le système Red Hat Enterprise Linux nouvellement installé avec Red Hat Network (soit les serveurs centraux RHN ou bien votre RHN Satellite Server) en utilisant le compte organisationnel comprenant le droit d'accès RHN Proxy Server à l'aide de la commande : `rhn_register`.
3. Abonnez le client au canal RHN Tools.

4. Installez l'installateur Proxy :

```
yum install spacewalk-proxy-installer
```

5. Effectuez l'installation :

```
configure-proxy.sh
```

**NOTE**

Afin d'effectuer cette étape avec succès, l'accès root au serveur Satellite est requis. Alternativement, veuillez ajouter l'option **--force-own-ca** à la commande.

Le programme d'installation en ligne de commande dirige les utilisateurs vers une série d'invites concernant l'installation de RHN Proxy Server et des détails de configuration initiale, comme des options d'installation et la génération de certificats SSL. Les instructions suivantes décrivent le processus d'installation :

**NOTE**

Si vous appuyez sur la touche **Entrée** sur une invite, au lieu de saisir une entrée, le programme d'installation en ligne de commande RHN Proxy Server utilisera la réponse par défaut à l'intérieur des accolades.

Sinon, pour obtenir des réponses par défaut *sans* aucune interaction avec l'utilisateur, utiliser l'option **--non-interactive**, qui utilisera toutes les réponses par défaut.

6. La première série d'invites portent sur des informations liées au site spécifiquement pour l'installation.

```
Proxy version to activate [5.4]:
```

Proxy version vous invite à confirmer quelle version de RHN Proxy Server vous souhaitez installer.

```
RHN Parent [satserver.example.com]:
```

RHN Parent est le nom de domaine ou l'adresse du système qui dessert le Proxy, qui pourraient bien être les serveurs RHN Hosted (xmlrpc.rhn.redhat.com), ou bien un serveur Satellite.

```
Traceback email []:
```

Traceback email est l'adresse email à laquelle des messages de traçage d'erreurs sont envoyés, et qui correspond le plus souvent à l'adresse email de l'administrateur du Proxy. Utiliser les virgules pour séparer les adresses s'il y en a plusieurs.

7. La série d'invites suivante est liée à la configuration des informations qui servent à générer un certificat SSL, ce qui est conseillé pour sécuriser le trafic en provenance et à destination de RHN Proxy Server.

```
Use SSL [Y/n]: y
```

À l'invite **Use SSL**, saisissez **y** pour configurer RHN Proxy Server pour supporter SSL.

```
CA Chain [/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT]:
```

Quand vous apercevez **CA Chain**, appuyez sur la touche **Enter** pour utiliser le chemin par défaut pour la Certificate Authority (CA) Chain qui a normalement pour valeur **/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT** quand le Proxy RHN communique avec un Satellite RHN. S'il communique avec RHN Hosted, c'est normalement le fichier **/usr/share/rhn/RHNS-CA-CERT**. Les certificats SSL personnalisés doivent se situer dans le répertoire **/usr/share/rhn/**.

```
HTTP Proxy []:
```

Si RHN Proxy Server connecte par un proxy HTTP, saisir le nom d'hôte et le numéro de port du proxy, par exemple **corporate.proxy.example.com:3128**

Saisir les informations nécessaires pour générer un certificat de serveur SSL qui convient, et qui comprend le nom de **Organization**, **Organization Unit** (comme **Ingénierie**), le **Common Name** (nom de domaine), ainsi que les informations sur la Ville, l'État, ou la Région. Enfin, saisir l'adresse email de l'administrateur ou d'un contact technique chargé des certificats SSL.

```
Regardless of whether you enabled SSL for the connection to the
Proxy Parent
Server, you will be prompted to generate an SSL certificate.
This SSL certificate will allow client systems to connect to this
Spacewalk Proxy
securely. Refer to the Spacewalk Proxy Installation Guide for more
information.
Organization: Example Company
Organization Unit [proxy1.example.com]:
Common Name: proxy1.example.com
City: New York
State: New York
Country code: US
Email [admin@example.com]:
```

8. À la suite de l'exécution du programme d'installation de RHN Proxy Server, le programme d'installation en ligne de commande :
 - Demande l'installation du contrôle de la prise en charge de RHN Proxy Server.
 - Autorise l'organisation à créer et remplir un canal de configuration pour de futures installations RHN Proxy Server.
 - Finalise la configuration SSL.
 - Redémarre tous les démons de service dont la configuration a été modifiée.

```
You do not have monitoring installed. Do you want to install it?
Will run 'yum install spacewalk-proxy-monitoring'. [Y/n]:n
```

Confirmer si oui ou non vous souhaitez installer le support Monitoring sur le serveur du Proxy.

```
Generating CA key and public certificate:
CA password:
CA password confirmation:
Copying CA public certificate to /var/www/html/pub for distribution
to clients:
Generating SSL key and public certificate:
CA password:
Backup made: 'rhncacert.pem' --> 'rhncacert.pem.1'
Rotated: rhncacert.pem --> rhncacert.pem.1
Installing SSL certificate for Apache and Jabberd:
Preparing packages for installation...
rhncacert.pem
```

Le programme **configure-proxy.sh** configure alors SSL, en vous invitant à créer un mot de passe de certificat d'autorité (Certificate Authority password) et de le confirmer avant de générer les clés SSL et le certificat public.

```
Create and populate configuration channel
rhncacert.pem [Y]:
Using server name satserver.example.com
Red Hat Network username: admin
Password:
Creating config channel rhncacert.pem
Config channel rhncacert.pem created
using server name satserver.example.com
Pushing to channel rhncacert.pem:
Local file /etc/httpd/conf.d/ssl.conf -> remote file
/etc/httpd/conf.d/ssl.conf
Local file /etc/rhn/rhn.conf -> remote file /etc/rhn/rhn.conf
Local file /etc/rhn/cluster.ini -> remote file /etc/rhn/cluster.ini
Local file /etc/squid/squid.conf -> remote file
/etc/squid/squid.conf
Local file /etc/httpd/conf.d/cobbler-proxy.conf -> remote file
/etc/httpd/conf.d/cobbler-proxy.conf
Local file /etc/httpd/conf.d/rhn_proxy.conf -> remote file
/etc/httpd/conf.d/rhn_proxy.conf
Local file /etc/httpd/conf.d/rhn_broker.conf -> remote file
/etc/httpd/conf.d/rhn_broker.conf
Local file /etc/httpd/conf.d/rhn_redirect.conf -> remote file
/etc/httpd/conf.d/rhn_redirect.conf
Local file /etc/jabberd/c2s.xml -> remote file /etc/jabberd/c2s.xml
Local file /etc/jabberd/sm.xml -> remote file /etc/jabberd/sm.xml
```

Le programme d'installation vous demande alors si vous souhaitez créer un canal de configuration basé sur les fichiers de configuration créés au cours de l'exécution de **configure-proxy.sh**. L'installateur va alors créer un canal de configuration RHN Satellite Server basé sur le nom du système du client sur lequel RHN Proxy Server est installé (dans l'exemple ci-dessus, le sysID est 1000010000), puis il ira collecter les divers fichiers de serveur **httpd**, **SSL**, **squid**, and **jabberd** qui comprendront le canal de configuration du serveur Proxy.

9. Enfin, l'installateur démarre et redémarre tous les services liés à RHN Proxy Server et se fermera une fois cela terminé.

```

Enabling Satellite Proxy
Shutting down rhn-proxy...
Shutting down Jabber router:                [ OK
]
Stopping httpd:                             [ OK
]
Stopping squid:                             [ OK
]
Done.
Starting rhn-proxy...
init_cache_dir /var/spool/squid... Starting squid: .    [ OK ]
Starting httpd:                               [ OK
]
Starting Jabber services                     [ OK
]
Done.

```

4.2.1. Le fichier Answer (réponse)

Si vous souhaitez automatiser certains des processus d'installation de RHN Proxy Server sur vos systèmes, le programme **configure-proxy.sh** permet aux administrateurs de créer des *fichiers de réponses* qui contiennent des réponses déjà remplies aux invites du programme d'installation.

Voici un exemple de fichier réponse qui contient de réponses anticipées concernant le numéro de version, le serveur RHN Satellite Server qui sert en tant que serveur parent, SSL, et d'autres paramètres de configuration. Pour plus d'informations sur la création et l'utilisation des fichiers réponse, voir la page de manuel **configure-proxy.sh** en saisissant **man configure-proxy.sh** à l'invite de commande shell.

```

# example of answer file for configure-proxy.sh
# for full list of possible option see
# man configure-proxy.sh

VERSION=5.4
RHN_PARENT=rhn-satellite.example.com
TRACEBACK_EMAIL=jsmith@example.com
USE_SSL=1
SSL_ORG="Red Hat"
SSL_ORGUNIT="Spacewalk"
SSL_CITY=Raleigh
SSL_STATE=NC
SSL_COUNTRY=US
INSTALL_MONITORING=N
ENABLE_SCOUT=N
CA_CHAIN=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
POPULATE_CONFIG_CHANNEL=Y

```

Pour utiliser un fichier réponse (intitulé **answers.txt** par exemple) avec **configure-proxy.sh**, saisir ce qui suit :

```
configure-proxy.sh --answer-file=answers.txt
```

CHAPITRE 5. RHN PACKAGE MANAGER ET LA DESSERTE DE PAQUETAGES LOCAUX

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

Pour utiliser le gestionnaire RHN 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 RHN. Les en-têtes sont requis afin que RHN puisse résoudre les dépendances de paquetages pour les systèmes client. Les fichiers de paquetages (***.rpm**) sont stockés sur RHN Proxy Server.

RHN Package Manager utilise les mêmes paramètres que le Proxy, définis dans le fichier de configuration **/etc/rhn/rhn.conf**.

Un résumé de toutes les options en ligne de commande de RHN Package Manager **rhn_package_manager**:

Tableau 5.1. options de rhn_package_manager

Option	Description
-v, --verbose	Augmenter les commentaires.
-dDIR, --dir=DIR	Traiter les paquetages du répertoire <i>DIR</i> .
-cCHANNEL, --channel=CHANNEL	Gérer ce canal — peut être présente plusieurs fois.
-nNUMBER, --count=NUMBER	Traiter 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	Imprimer la configuration courante et quitter.
-XPATTERN, --exclude=PATTERN	Exclure les fichiers correspondant à cette expression globale — peut être présente 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.

Option	Description
--nosig	Envoyer les paquetages non signés. Par défaut, RHN Package Manager essaie uniquement d'envoyer les paquetages signés.
--username=USERNAME	Spécifier votre nom d'utilisateur RHN. Si vous ne fournissez pas un nom avec cette option, le système vous le demandera.
--password=PASSWORD	Spécifier votre mot de passe RHN. 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	<i>Non recommandé</i> — 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, rhnpkgmgr -cCANAL --copyonly /CHEMIN/AU/FICHER/MANQUANT
-h, --help	Afficher l'écran d'aide avec une liste d'options.



NOTE

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

Pour que RHN 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.

5.1. CRÉER UN CANAL PRIVÉ

Avant que les paquetages locaux puissent être fournis via RHN 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 de RHN à l'adresse suivante : <https://rhn.redhat.com>.
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 de canaux de RHN*.
5. Cliquez sur **Créer un canal**.

5.2. TÉLÉCHARGER DES PAQUETAGES



NOTE

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

Après avoir créé le canal privé, téléchargez les en-têtes de paquets pour votre binaire et les RPM source vers le serveur RHN et copiez les paquets sur le serveur RHN Proxy Broker. Pour télécharger les en-têtes de paquets 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 paquets à télécharger. Alternativement, utilisez l'option **-d** pour spécifier le répertoire local qui contient les paquets à ajouter au canal. Assurez-vous que le répertoire ne contienne uniquement les paquets à inclure et aucun autre fichier. RHN Package Manager peut également lire la liste de paquets de l'entrée standard (à l'aide de **--stdin**).

Pour télécharger les en-têtes de paquets 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 paquets téléchargés seront liés à tous les canaux listés.

**NOTE**

Si un nom de canal n'est pas spécifié, les paquets ne sont ajoutés à aucun canal. Les paquets 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 paquets, vous pouvez immédiatement vérifier l'interface Web de RHN 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 **Paquets**. Chaque RPM devrait être listé.

Vous pouvez également vérifier si le répertoire local est en synchronisation avec l'image du serveur RHN des canaux en ligne de commande :

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

L'option **-s** va répertorier tous les paquets manquants (paquets téléchargés sur le serveur RHN 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 RHN.

Si vous utilisez RHN Package Manager pour mettre à jour les paquets locaux, vous devez vous rendre sur le site web de RHN pour abonner le système au canal privé.

CHAPITRE 6. MISE À NIVEAU DE L'INSTALLATION

Ce chapitre décrit comment mettre à niveau votre installation de RHN Proxy Server. Il est présumé que vous possédez un serveur RHN Proxy Server totalement fonctionnel ainsi que les droits d'accès qui lui sont nécessaires.

6.1. PRÉREQUIS

Pour la version la plus récente de RHN Proxy Server, vous aurez besoin de :

- Red Hat Enterprise Linux 5 (32-bit ou 64-bit) ou Red Hat Enterprise Linux 6 (64-bit uniquement).
- La suppression du profil système de l'ancien serveur Proxy de Red Hat Network Classic ou du serveur Satellite parent (si applicable)

6.2. PROCESSUS DE MISE À NIVEAU DE L'INSTALLATION

1. Effectuez une copie de sauvegarde de votre serveur Proxy. Si applicable, restaurez la direction du build SSL de la copie de sauvegarde sur le répertoire **/root/ssl-build**.
2. Enregistrez Proxy Server sur Red Hat Network Classic ou sur le serveur Satellite parent (si applicable). Assurez-vous que le serveur Proxy soit bien abonné au canal de base Red Hat Enterprise Linux Server et au canal enfant Red Hat Network Tools.
3. Installez le paquetage **spacewalk-proxy-installer** à partir du canal enfant Red Hat Network Tools :

```
# yum install spacewalk-proxy-installer
```

4. installez la version la plus récente de proxy, comme documenté dans la [Section 4.2](#), « [Processus d'installation de RHN Proxy Server](#) ».

NOTE

Si le serveur Proxy est enregistré sur Red Hat Network Classic et qu'il gère auparavant des canaux personnalisés, vous devrez restaurer le référentiel des paquetages personnalisés de la copie de sauvegarde « pré-mise à niveau ». Les permissions et appartenances devront aussi être paramétrées correctement.

```
# chmod 0750 /var/spool/rhn-proxy
# chown apache:apache /var/spool/rhn-proxy
# mkdir -m 0750 -p /var/spool/rhn-proxy/list
# chown apache:apache /var/spool/rhn-proxy/list
```

Le référentiel des paquetages personnalisés par défaut est habituellement **/var/spool/rhn-proxy**.

5. Après l'installation, mettez à jour le serveur avec les dernières mises à jour d'errata :

```
# yum update
```

6. Redémarrez les services RHN Proxy Server et testez ses fonctionnalités :

```
# /usr/sbin/rhn-proxy restart
```

CHAPITRE 7. RÉSOLUTION DE PROBLÈMES

Ce chapitre offre des conseils pour déterminer les causes des erreurs les plus communes associées à RHN Proxy Server et pour les résoudre. Si vous avez besoin d'aide supplémentaire, veuillez contacter l'assistance de Red Hat Network à l'adresse <https://rhn.redhat.com/help/contact.pxt>. Connectez-vous en utilisant votre compte ayant des droits d'accès au Satellite pour voir la liste complète de vos options.

7.1. GÉRER LE SERVICE PROXY

Vu que RHN Proxy Server consiste en une multitude de composants individuels, Red Hat fournit un script intitulé **rhn-proxy**, qui permet aux administrateurs d'arrêter, de démarrer, de redémarrer, ou d'obtenir le statut de divers services sur le Proxy.

Tableau 7.1. Commandes rhn-proxy

Commande	Fonction
/usr/sbin/rhn-proxy start	Cette commande démarre RHN Proxy Server s'il n'est pas déjà lancé.
/usr/sbin/rhn-proxy stop	Cette commande arrête RHN Proxy Server s'il n'est pas déjà arrêté.
/usr/sbin/rhn-proxy restart	Cette commande arrête le serveur RHN Proxy Server en cours d'exécution et le redémarre. Si RHN Proxy Server est arrêté, il sera lancé.
/usr/sbin/rhn-proxy status	Cette commande affiche le statut actuel de RHN Proxy Server.

7.2. FICHIERS JOURNAUX

Chaque étape de résolution de problèmes devrait virtuellement commencer par l'examen des fichiers journaux associés. Ces derniers offrent des informations de valeur sur l'activité qui a pris place sur le périphérique ou au sein de l'application et qui peuvent être utilisées pour contrôler la performance et assurer une configuration correcte. Consultez le [Tableau 7.2, « Fichiers journaux »](#) pour les chemins d'accès à tous les fichiers journaux appropriés :

Tableau 7.2. Fichiers journaux

Composant	Emplacement du fichier journal
Serveur web Apache	répertoire /var/log/httpd/
Fiche double (squid)	répertoire /var/log/squid/
Serveur RHN Proxy Broker	/var/log/rhn/rhn_proxy_broker.log
Serveur RHN SSL Redirect	/var/log/rhn/rhn_proxy_redirect.log

Composant	Emplacement du fichier journal
Agent de mise à jour « Red Hat Update Agent »	<code>/var/log/yum.log</code>

7.3. QUESTIONS ET RÉPONSES

Cette section contient les réponses aux questions les plus fréquemment posées sur l'installation et la configuration d'une solution RHN Proxy Server.

Q : Après avoir configuré le gestionnaire de paquetages RHN « RHN Package Manager », comment puis-je déterminer si les paquetages locaux ont bien été ajoutés au canal RHN privé ?

R : Utilisez la commande `rhn_package_manager -l -c "nom_du_canal_privé"` pour lister les paquetages du canal privé connus par les serveurs RHN. Vous pouvez également vous rendre sur l'interface Web de RHN.

Après avoir abonné un système enregistré au canal privé, vous pouvez également exécuter la commande `up2date -l --showall` sur le système enregistré et rechercher les paquetages du canal RHN privé.

Q : J'ai changé la configuration du nom du DNS de mon serveur Proxy, et maintenant, les systèmes de mes clients ne peuvent plus être mis à jour. Comment puis-je régler ce problème ?

R : Exécutez la commande `up2date -u` sur le système du client pour que le changement de nom prenne effet.

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 RHN Proxy Server. 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 des fonctionnalités nécessaires pour se connecter à travers RHN Proxy Server. La dernière version peut être obtenue via Red Hat Network en lançant la commande `yum update yum` en tant que superutilisateur ou bien en allant sur <http://www.redhat.com/support/errata/>.

RHN Proxy Server est une extension d'Apache. Consultez le [Tableau 7.2, « Fichiers journaux »](#) pour les emplacements de ses fichiers journaux.

Q : La configuration de mon proxy RHN Proxy Server 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.

Lisez les fichiers journaux. Une liste est disponible dans le [Tableau 7.2, « Fichiers journaux »](#).

7.4. PROBLÈMES GÉNÉRAUX

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** pour tous les fichiers journaux, puis d'exécuter la commande **up2date --list**. Vous devriez alors examiner toutes les nouvelles entrées de journaux pour des indices potentiels.

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 courriels de RHN Proxy Server, confirmez que les bonnes adresses électroniques ont été définies pour **traceback_mail** dans **/etc/rhn/rhn.conf**.

7.5. IMPOSSIBLE DE TROUVER L'HÔTE / IMPOSSIBLE DE DÉTERMINER LE FQDN (NOMS DE DOMAINE ENTièrement QUALIFIÉS)

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 RHN Proxy Server en une adresse IP. Red Hat Update Agent, Red Hat Network Registration Client et le serveur web Apache sont particulièrement sujets à ce problème avec les applications RHN produisant des erreurs de type « hôte non trouvé » et le serveur web indiquant « Impossible de déterminer le nom de domaine complet 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, suivi 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
```

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
```

Puis, enregistrez le fichier et essayez d'exécuter à nouveau les applications client de RHN ou le serveur web Apache. S'ils 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.

7.6. ERREURS DE CONNEXION

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 :

```
rhncertutils-MACHINE_NAME-VER-REL.noarch.rpm
```

est installé sur RHN Proxy Server et que le fichier **rhncertutils-*MACHINE_NAME*-*VER-REL*.noarch.rpm** correspondant au certificat CA SSL (client) brut public 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 serveurs proxy RHN, assurez-vous que les certificats SSL de chaque proxy sont préparés correctement. Si vous utilisez le serveur proxy RHN avec un serveur RHN 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 RHN* pour obtenir des instructions spécifiques.
- Si RHN Proxy Server 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 les ports requis, comme la [Section 2.4, « Besoins supplémentaires »](#) l'identifie.

7.7. PROBLÈMES DE CACHE

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. RHN Proxy Server 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 RHN.

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/*
```

Bien que le démon d'authentification RHN était déprécié avec la sortie de la version 3.2.2 de RHN Proxy Server et remplacé par le mécanisme de cache d'authentification interne mentionné auparavant, le démon peut toujours être en cours d'exécution sur votre proxy. Pour le désactiver, exécutez les commandes suivantes dans l'ordre suivant :

```
chkconfig --level 2345 rhn_auth_cache off service rhn_auth_cache stop
```

Pour vider son cache, exécutez :

```
rm /var/up2date/rhn_auth_cache
```

Si vous devez garder le démon d'authentification RHN, ce que Red Hat ne recommande pas et ne prendra pas en charge, notez que sa performance peut souffrir de la journalisation avec commentaires. Pour cette raison, sa journalisation (dans `/var/log/rhn/rhn_auth_cache.log`) est désactivée par défaut. Si vous exécutez le démon et souhaitez la journalisation, activez-le en ajoutant la ligne suivante dans le fichier `/etc/rhn/rhn.conf` du Proxy :

```
auth_cache.debug = 2
```

7.8. DÉBOGAGE DU PROXY PAR RED HAT

Si toutes ces étapes de résolution de problèmes ont été utilisées ou si vous souhaitez les remettre à des professionnels de Red Hat Network, Red Hat vous recommande de tirer profit de la prise en charge de haut niveau qui est offerte avec RHN Proxy Server.

Pour accéder à cette expertise, consultez la base de connaissance Red Hat (« Red Hat Knowledgebase ») qui procure des solutions aux problèmes les plus communs rencontrés par les

utilisateurs et qui est équipée d'une interface de recherche et de navigation robuste pour trouver les bonnes réponses à vos problèmes de proxy. Vous pouvez accéder la base de connaissance Red Hat à l'adresse suivante <http://kbase.redhat.com>.

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 RHN Satellite Server, le paquetage **sos** doit être installé. Tapez **sosreport -o rhn** en tant que root sur le serveur Satellite pour créer un rapport. Ainsi :

```
[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 diagnostic immédiat.

ANNEXE A. EXEMPLE DE FICHIER DE CONFIGURATION DE RHN PROXY SERVER

Le fichier de configuration `/etc/rhn/rhn.conf` pour RHN Proxy Server permet aux administrateurs d'établir les paramètres clés. Sachez cependant que toute erreur insérée dans ce fichier peut provoquer des défaillances du proxy. Apportez donc des modifications de configuration avec attention.

Si vous utilisez également un serveur RHN Satellite, vous devriez faire particulièrement attention aux paramètres suivants : `traceback_mail` et `proxy.rhn_parent`. Examinez l'exemple et ses commentaires, qui commencent par un signe dièse (`#`), pour toute information supplémentaire.



NOTE

Vous pouvez uniquement ajouter le paramètre **`use_ssl`** à **`rhn.conf`** pour des tests. Donnez-lui la valeur 0 pour temporairement désactiver SSL entre le Proxy et le serveur supérieur. Notez que cela compromet considérablement la sécurité. Redonnez au paramètre sa valeur par défaut de 1 pour réactiver SSL, ou supprimez simplement la ligne du fichier de configuration.

```
# Automatically generated RHN Management Proxy Server configuration file.
# -----
# -----

# SSL CA certificate location
proxy.ca_chain = /usr/share/rhn/RHNS-CA-CERT

# Corporate HTTP proxy, format: corp_gateway.example.com:8080
proxy.http_proxy =

# Password for that corporate HTTP proxy
proxy.http_proxy_password =

# Username for that corporate HTTP proxy
proxy.http_proxy_username =

# Location of locally built, custom packages
proxy.pkg_dir = /var/spool/rhn-proxy

# Hostname of RHN Server or RHN Satellite
proxy.rhn_parent = rhn.redhat.com

# Destination of all tracebacks, etc.
traceback_mail = user0@domain.com, user1@domain.com
```

ANNEXE B. HISTORIQUE DES VERSIONS

Version 3-5.2.400 Rebuild with publican 4.0.0	2013-10-31	Rüdiger Landmann
Version 3-5.2 Fichiers de traduction synchronisés avec les sources XML 3-5.2	Mon Apr 22 2013	Sam Friedmann
Version 3-5.1 Fichiers de traduction synchronisés avec les sources XML 3-5	Thu Mar 21 2013	Corina Roe
Version 3-5 Mise en paquetage finale pour 5.5	Wed Sept 19 2012	Dan Macpherson
Version 3-4 Préparé pour la version 5.5 Incorporation des modifications de la révision technique BZ#491007 Ajout d'un chapitre sur l'installation de mises à niveau	Wed Jul 4 2012	Athene Chan
Version 3-0 Préparé pour la version 5.5 Incorporation des modifications de la révision technique BZ#491007 Ajout d'un chapitre sur l'installation de mises à niveau	Wed Jul 4 2012	Athene Chan
Version 2-5 BZ#682996 - Chapitre d'installation - Instructions de mise à jour BZ#705755 - Chapitre du gestionnaire de paquetages - Informations supplémentaires BZ#722193 - Chapitre des pré-requis - Erreur corrigée BZ#729617 - Chapitre d'installation - Erreur corrigée BZ#729663 - Chapitre d'installation - Ajout d'un avertissement	Thu Jan 5 2012	Lana Brindley
Version 2-4 Version du flux z plié dans le flux y	Mon Aug 15 2011	Lana Brindley
Version 2-3 BZ#713527 - Ajout de références à RHEL 6	Wed Jun 22 2011	Lana Brindley
Version 2-2 Préparé pour publication	Wed Jun 15 2011	Lana Brindley
Version 2-1 Mises à jour de la part des traducteurs	Fri May 27 2011	Lana Brindley
Version 2-0 Préparé pour traduction	Fri May 6 2011	Lana Brindley
Version 1-9 BZ#653844 - Révision QE	Wed April 27 2011	Lana Brindley
Version 1-8 BZ#646176 - Installation	Mon Feb 7 2011	Lana Brindley

INDEX

A

Administrateur d'organisations, [Terminologie fréquemment utilisée](#)

Administrateur de canaux, [Terminologie fréquemment utilisée](#)

Agent de mise à jour « Red Hat Update Agent », [Terminologie fréquemment utilisée](#), [Fonctionnement du Proxy](#)

authentification, [Fonctionnement du Proxy](#)

avantages, [RHN Proxy Server](#)

B

besoins

espace disque, [Besoins d'espace disque](#)

logiciel, [Besoins logiciels](#)

matériel, [Besoins matériels](#)

supplémentaires, [Besoins supplémentaires](#)

besoins d'espace disque, [Besoins d'espace disque](#)

besoins en matériel, [Besoins matériels](#)

besoins logiciel, [Besoins logiciels](#)

besoins supplémentaires, [Besoins supplémentaires](#)

C

canal, [Terminologie fréquemment utilisée](#)

créer un canal privé, [Créer un canal privé](#)

canal privé, [Créer un canal privé](#)

configuration du client

s'abonner à un canal privé, [Télécharger des paquetages](#)

D

Démon d'authentification RHN, désactivation

rh_n_auth_cache, arrêt, [Problèmes de cache](#)

E

erreurs de connexion, [Erreurs de connexion](#)

F

fichiers journaux, [Fichiers journaux](#)

G

Gestionnaire de paquetages « RHN Package Manager », [Fonctionnement du Proxy](#)

H

HTTP Proxy Caching Server

besoins en espace disque, [Besoins d'espace disque](#)

I

Impossible de trouver l'hôte

Impossible de déterminer le FQDN, [Impossible de trouver l'hôte / Impossible de déterminer le FQDN \(noms de domaine entièrement qualifiés\)](#)

installation

base, [Installation de base](#)

de RHN Proxy Server, [Processus d'installation de RHN Proxy Server](#)

L

le fonctionnement du Proxy, [Fonctionnement du Proxy](#)

M

mise en cache de l'authentification

supprimer, [Problèmes de cache](#)

mise en cache de Squid, [Problèmes de cache](#)

P

port

443, [Besoins supplémentaires](#)

5222, [Besoins supplémentaires](#)

80, [Besoins supplémentaires](#)

port 443, [Besoins supplémentaires](#)

port 4545, [Besoins supplémentaires](#)

port 80, [Besoins supplémentaires](#)

ports entrant, satellite

5222, [Besoins supplémentaires](#)

Ports Proxy, [Besoins supplémentaires](#)

ports sortant

80, 443, [Besoins supplémentaires](#)

pré-requis, [Besoins](#)

Problèmes de cache, [Problèmes de cache](#)

problèmes généraux, [Problèmes généraux](#)

Q

questions et réponses, [Questions et réponses](#)

R

Red Hat Network

introduction, [Red Hat Network](#)

résolution de problèmes, [Résolution de problèmes](#)

RHN Package Manager, [RHN Package Manager et la desserte de paquets locaux](#)

canaux, spécifier, [Télécharger des paquets](#)

configurer, [Créer un canal privé](#)

créer un canal privé, [Créer un canal privé](#)

fichier de configuration, [RHN Package Manager et la desserte de paquets locaux](#)

installer, [RHN Package Manager et la desserte de paquets locaux](#)

options de ligne de commande, [RHN Package Manager et la desserte de paquets locaux](#)

télécharger les en-têtes de paquetage, [Télécharger des paquets](#)

vérifier la liste de paquets locaux, [Télécharger des paquets](#)

rhn-proxy

service, [Gérer le service Proxy](#)

rhn.conf

échantillon de fichier, [Exemple de fichier de configuration de RHN Proxy Server](#)

rhn_package_manager , [Télécharger des paquets](#) (voir RHN Package Manager)

S

satellite-debug, [Débogage du proxy par Red Hat](#)

T

Terminologie fréquemment utilisée, [Terminologie fréquemment utilisée](#)

topologies, [Exemple de topologies](#)

plusieurs proxys hiérarchisés horizontalement, [Topologie de plusieurs proxys en plusieurs niveaux horizontaux](#)

plusieurs proxys hiérarchisés verticalement, [Topologie de plusieurs proxys en plusieurs niveaux verticaux](#)

proxy unique, [Topologie d'un proxy unique](#)

proxys et serveur Satellite RHN, [Proxys avec serveur RHN Satellite](#)

traçage, [Terminologie fréquemment utilisée](#)