RHN Proxy Server 4.0

Installation Guide

RHN Proxy Server 4.0: Installation Guide


Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

RHNproxy(EN)-4.0-RHI (2005-04-20T13:40)

The GPG fingerprint of the security@redhat.com key is:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Table of Contents

Chapter 1.

Introduction

1.1. Red Hat Network

Red Hat Network (RHN) is the environment for system-level support and management of Red Hat systems and networks of systems. Red Hat Network brings together the tools, services, and information repositories needed to maximize the reliability, security, and performance of their systems. To use RHN, system administrators register the software and hardware profiles, known as System Profiles, of their client systems with Red Hat Network. When a client system requests package updates, only the applicable packages for the client are returned (based upon the software profile stored on the RHN Servers).

Advantages of using Red Hat Network include:

- Scalability — with Red Hat Network, a single system administrator can set up and maintain hundreds or thousands of Red Hat systems more easily, accurately, and quickly than they could maintain a single system without Red Hat Network.
- Standard Protocols — standard protocols are used to maintain security and increase capability. For example, XML-RPC gives Red Hat Network the ability to do much more than merely download files.
- Security — all communication between registered systems and Red Hat Network takes place over secure Internet connections.
- View Errata Alerts — easily view Errata Alerts for all your client systems through one website.
- Scheduled Actions — use the website to schedule actions, including Errata Updates, package installs, and software profile updates.
- Simplification — maintaining Red Hat systems becomes a simple, automated process.

1.2. RHN Proxy Server

An RHN Proxy Server is a service deployed within a corporate network with advanced Red Hat Network functionality, such as a package-caching mechanism for reduced bandwidth usage and customizable channels enabling custom package deployment.

This service allows a business or corporation to cache RPM Updates on an internal, centrally located RHN Proxy Server and have the client systems download the updates from that server instead of from one of the RHN Servers [1] over the Internet. The clients' System Profiles and user information are stored on the secure, central RHN Servers, which also serve the RHN website (rhn.redhat.com). The Proxy acts as a go-between for client systems and Red Hat Network (or an RHN Satellite Server). Only the package files are stored on the RHN Proxy Server. Every transaction is authenticated, and the **Red Hat Update Agent** checks the GPG signature of each package retrieved from the local RHN Proxy Server.

In addition to storing official Red Hat packages, the RHN Proxy Server can be configured to deliver an organization's own custom packages from private RHN *channels*, using the RHN Package Manager.

1. Throughout this document, replace RHN Server with RHN Satellite Server if the RHN Proxy Server connects to a RHN Satellite Server instead.

For instance, an organization could develop its own software, package it in an RPM, sign it with its own GPG signature, and have the local RHN Proxy Server update all the individual systems in the network with the latest versions of the custom software.

Advantages of using RHN Proxy Server include:

- Scalability — there can be multiple local RHN Proxy Servers within one organization.
- Security — an end-to-end secure connection is maintained: from the client systems, to the local RHN Proxy Server, to the Red Hat Network servers.
- Saves time — packages are delivered significantly faster over a local area network than the Internet.
- Saves bandwidth — packages are downloaded from the RHN File servers only once (per local Proxy Server's caching mechanism) instead of downloading each package to each client system.
- Saves disk space on individual systems — one large disk array is required instead of extra disk space on all the client systems.
- Customized updates — create a truly automated package delivery system for custom software packages, as well as official Red Hat packages required for the client systems. Custom private RHN channels allow an organization to automate delivery of in-house packages.
- Customized configuration — restrict or grant updates to specific architectures and OS versions.
- Only one Internet connection required — the client systems connect only through the HTTP-enabled Proxy Server and therefore do not need a connection to the external network (Internet), but only require access to the Local Area Network to which the RHN Proxy Server is connected. Only the RHN Proxy Server needs an Internet connection to contact the RHN Servers, unless the RHN Proxy Server is using a RHN Satellite Server, in which case only the RHN Satellite Server requires an Internet connection.

1.3. Terms to Understand

Before understanding RHN Proxy Server, it is important to become familiar with the following Red Hat Network terms:

- *Channel* — A channel is a list of software packages. There are two types of channels: base channels and child channels. A *base channel* consists of a list of packages based on a specific architecture and Red Hat release. A *child channel* is a channel associated with a base channel but contains extra packages.
- *Organization Administrator* — Organization Administrator is a user role with the highest level of control over an organization's Red Hat Network account. Members with this role can add other users, other systems, and system groups to the organization, as well as remove them. A Red Hat Network organization must have at least one Organization Administrator.
- *Channel Administrator* — A Channel Administrator is a user role with full access to channel management capabilities. Users with this role are capable of creating channels and assigning packages to channels. This role can be assigned by an Organization Administrator through the **Users** tab of the RHN website.
-

Red Hat Update Agent — The **Red Hat Update Agent** is the Red Hat Network client application (`up2date`) that allows users to retrieve and install new or updated packages for the client system on which the application is run.

- *Traceback* — A traceback is a detailed description of "what went wrong" that is useful for troubleshooting the RHN Proxy Server. Tracebacks are automatically generated when a critical error occurs and are mailed to the individual(s) designated in the RHN Proxy Server's configuration file.

For more detailed explanations of these terms and others, refer to the *Red Hat Network Reference Guide* available at http://www.redhat.com/docs/.

1.4. How it Works

The **Red Hat Update Agent** on the client systems does not directly contact a Red Hat Network Server. Instead, the client (or clients) connects to an RHN Proxy Server that connects to the Red Hat Network Servers or to a RHN Satellite Server. Thus, the client systems do not need direct access to the Internet. They need access only to the RHN Proxy Server.

Important

Red Hat strongly recommends that clients connected to RHN Proxy Server be running the latest update of Red Hat Enterprise Linux to ensure proper connectivity.

By default, a client is authenticated directly by Red Hat Network Servers. Using an RHN Proxy Server, authentication works similarly except that the RHN Proxy Server provides route information as well. After a successful authentication, the Red Hat Network Server informs the RHN Proxy Server that it is permitted to execute a specific action for the client. The RHN Proxy Server downloads all of the updated packages (if they are not already present in its cache) and delivers them to the client system.

Requests from the **Red Hat Update Agent** on the client systems are still authenticated on the server side, but package delivery is significantly faster since the packages are cached in the HTTP Proxy Caching Server or the RHN Proxy Server (for local packages); the RHN Proxy Server and client system are connected via the LAN and are limited only by the speed of the local network.

Authentication is done in the following order:

1. The client performs a login action at the beginning of a client session. This login is passed through one or more RHN Proxy Servers until it reaches a Red Hat Network Server.
2. The Red Hat Network Server attempts to authenticate the client. If authentication is successful, the server then passes back a session token via the chain of RHN Proxy Servers. This token, which has a signature and expiration, contains user information, including subscribe-to channels, username, etc.
3. Each RHN Proxy Server caches this token on its local file system in `/var/cache/rhn/`. Caching reduces some of the overhead of authenticating with Red Hat Network Servers and greatly improves the performance of Red Hat Network.
4. This session token is passed back to the client machine and is used in subsequent actions on Red Hat Network.

From the client's point of view, there is no difference between an RHN Proxy Server and a Red Hat Network Server. From the Red Hat Network Server's point of view, an RHN Proxy Server is a special type of RHN client. Clients are thus not affected by the route a request takes to reach a Red

Hat Network Server. All the logic is implemented in the RHN Proxy Servers and Red Hat Network Servers.

Optionally the RHN Package Manager can be installed and configured to serve custom packages written specifically for the organization. These are not official Red Hat packages. After creating a private RHN channel, the custom RPM packages are associated with the private channel by uploading the package headers to the RHN Servers. Only the headers are uploaded, not the actual package files. The headers are required because they contain crucial RPM information, such as software dependencies, that allows RHN to automate package installation. The actual custom RPM packages are stored on the RHN Proxy Server and sent to the client systems from inside the organization's local area network.

Configuring a computer network to use RHN Proxy Servers is straightforward. The Red Hat Network applications on the client systems must be configured to connect to the RHN Proxy Server instead of the Red Hat Network Servers. Refer to the *RHN Client Configuration Guide* for details. On the proxy side, one has to specify the next proxy in the chain (which will eventually end with a Red Hat Network Server). If the RHN Package Manager is used, the client systems must be subscribed to the private RHN channel.

Chapter 2.

Requirements

These requirements must be met before installation. To install RHN Proxy Server version 3.6 or later from RHN Satellite Server, the Satellite itself must be version 3.6 or later.

2.1. Software Requirements

To perform an installation, the following software-related components must be available:

- Base operating system — RHN Proxy Server is supported with Red Hat Enterprise Linux AS 3 Update 5 or later, or Red Hat Enterprise Linux AS 4 only. The operating system can be installed from disc, local ISO image, kickstart, or any of the methods supported by Red Hat.

   **Important**

  If you plan to obtain Monitoring-level service, you *must* install your RHN Proxy Server on Red Hat Enterprise Linux AS 3 Update 5 or Red Hat Enterprise Linux AS 4. These are the only supported base operating systems for Proxies serving Monitoring-entitled systems.

  Each version of Red Hat Enterprise Linux AS requires a certain package set to support RHN Proxy Server. Anything more can cause errors during installation. Therefore, Red Hat recommends obtaining the desired package set in the following ways:

   **Note**

  For kickstarting either Red Hat Enterprise Linux AS 4 or Red Hat Enterprise Linux AS 3 Update 5, specify the following package group: **`@ Base`**

  For installing Red Hat Enterprise Linux AS 4 or Red Hat Enterprise Linux AS 3 Update 5 via CD or ISO image, select the following package group: **`Minimal`**

   **Warning**

  Security-enhanced Linux (SELinux) must be disabled in Red Hat Enterprise Linux AS 4 prior to installation of RHN Proxy Server. To do this during CD or ISO image installation, select **`Disabled`** when presented with options for SELinux support. To do this for kickstart installation, include the command `selinux --disabled` or wait for the install to complete, edit the `/etc/selinux/config` file to read `SELINUX=disabled` and reboot the system.

- An available RHN Proxy Server entitlement within your Red Hat Network account.
- An available Provisioning entitlement within your Red Hat Network account (which should come packaged with your RHN Proxy Server entitlement).
- Access to the Red Hat Network Tools channel for the installed version of Red Hat Enterprise Linux AS.
- All `rhncfg*` packages installed on the Proxy (from the RHN Tools channel).
- Either the `rhns-certs-tools` package installed on the Proxy (from the RHN Tools channel) or the secure sockets layer (SSL) CA certificate password used to generate the parent server certificate (such as on an RHN Satellite Server).

- Configuration of the system to accept remote commands and configuration management through Red Hat Network. Refer to Section 4.2 *RHN Proxy Server Installation Process* for instructions.

2.2. Hardware Requirements

The following hardware configuration is required for the RHN Proxy Server:

- Pentium III processor, 1.26GHz, 512K cache or equivalent
- 512 MB of memory
- 3 GB storage for base install of Red Hat Enterprise Linux AS
- 6 GB storage per distribution/channel

The load on the Apache HTTP Server is directly related to the frequency with which client systems connect to the Proxy, so if you reduce the default interval of four hours (or 240 minutes) as set in the `/etc/sysconfig/rhn/rhnsd` configuration file of the client systems, you will *increase* the load on this component significantly.

2.3. Disk Space Requirements

The caching mechanism used by RHN Proxy Server is the Squid HTTP proxy, which saves significant bandwidth for the clients. It should have a reasonable amount of space available. The cached packages are stored in `/var/spool/squid`. The required free space allotment is 6 GB storage per distribution/channel.

If the RHN Proxy Server is configured to distribute custom, or local packages, make sure that the `/var` mount point on the system storing local packages has sufficient disk space to hold all of the custom packages, which are stored in `/var/spool/rhn-proxy`. The required disk space for local packages depends on the number of custom packages served.

2.4. Additional Requirements

The following additional requirements must be met before the RHN Proxy Server installation can be considered complete:

- Full Access

  Client systems need full network access to the RHN Proxy Server services and ports.

- Firewall Rules

  The RHN Proxy Server solution can be firewalled from the Internet, but it must be able to issue outbound connections to the Internet on ports 80 and 443. In addition, if the Proxy will be connected to an RHN Satellite Server that will be configured to push actions to client systems and the Proxy, you must allow inbound connections on port 5222.

- Synchronized System Times

  There is great time sensitivity when connecting to a Web server running SSL (Secure Sockets Layer); it is imperative the time settings on the clients and server are reasonably close together so the SSL certificate does not expire before or during use. It is recommended Network Time Protocol (NTP) be used to synchronize the clocks.

- Fully Qualified Domain Name (FQDN)

  The system upon which the RHN Proxy Server will be installed must resolve its own FQDN properly.

- A Red Hat Network Account

  Customers who will be connecting to the central Red Hat Network Servers to receive incremental updates will need an account with Red Hat Network. This account should be set up at the time of purchase with the sales representative.

- Backups of Login Information

  It is imperative customers keep track of all primary login information. For RHN Proxy Server, this includes usernames and passwords for the Organization Administrator account and SSL certificate generation. Red Hat strongly recommends this information be copied onto two separate floppy disks, printed out on paper, and stored in a fireproof safe.

- Distribution Locations

  Since the Proxy forwards virtually all local HTTP requests to the central RHN Servers, you must take care to put files destined for distribution (such as in a kickstart installation tree) in the non-forwarding location on the Proxy: `/var/www/html/pub/`. Files placed in this directory can be downloaded directly from the Proxy. This can be especially useful for distributing GPG keys or establishing installation trees for kickstarts.

In addition, Red Hat recommends the system running the code not be publicly available. No users but the system administrators should have shell access to these machines. All unnecessary services should be disabled. You can use `ntsysv` or `chkconfig` to disable services.

Finally, you should have the following technical documents in hand for use in roughly this order:

1. *The RHN Proxy Server Installation Guide* — This guide, which you are now reading, provides the essential steps necessary to get an RHN Proxy Server up and running.
2. *The RHN Client Configuration Guide* — This guide explains how to configure the systems to be served by an RHN Proxy Server or RHN Satellite Server. (This will also likely require referencing *The RHN Reference Guide*, which contains steps for registering and updating systems.)
3. *The RHN Channel Management Guide* — This guide identifies in great detail the recommended methods for building custom packages, creating custom channels, and managing private Errata.
4. *The RHN Reference Guide* — This guide describes how to create RHN accounts, register and update systems, and use the RHN website to its utmost potential. This guide will probably come in handy throughout the installation and configuration process.

Chapter 3.

Example Topologies

The RHN Proxy Server can be configured in multiple ways. Select one method depending on the following factors:

1. The total number of client systems to be served by the
2. The maximum number of clients expected to connect *concurrently* to the RHN Proxy Server.
3. The number of custom packages and channels to be served by the RHN Proxy Server.
4. The number of RHN Proxy Servers being used in the customer environment.

The rest of this chapter describes possible configurations and explains their benefits.

3.1. Single Proxy Topology

The simplest configuration is to use a single RHN Proxy Server to serve your entire network. This configuration is adequate to service a small group of clients and a network that would benefit from caching Red Hat RPMs and storing custom packages on a local server.

The disadvantage of using one RHN Proxy Server is that performance will be compromised as the number of clients requesting packages grows.

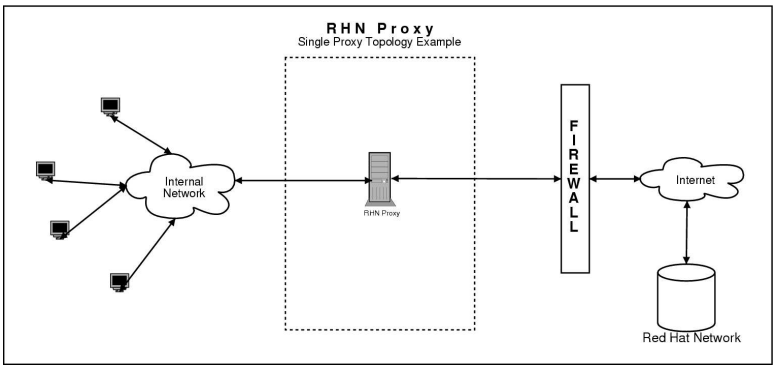

Figure 3-1. Single Proxy Topology

3.2. Multiple Proxy Horizontally Tiered Topology

For larger networks, a more distributed method may be needed, such as having multiple RHN Proxy Servers all connecting to Red Hat Network individually. This horizontally tiered configuration balances the load of client requests while enabling each Proxy to simultaneously synchronize with RHN.

A disadvantage of this horizontal structure is that custom packages loaded to an individual Proxy must be distributed to its sibling servers. This situation can be addressed in one of two ways:

- Either, the **rsync** file transfer program can be used to synchronize packages between the Proxies, or
- a Network File System (NFS) share can be established between the Proxies and the custom channel repository.

Either of these solutions will allow any client of any RHN Proxy Servers to have all custom packages delivered to them.

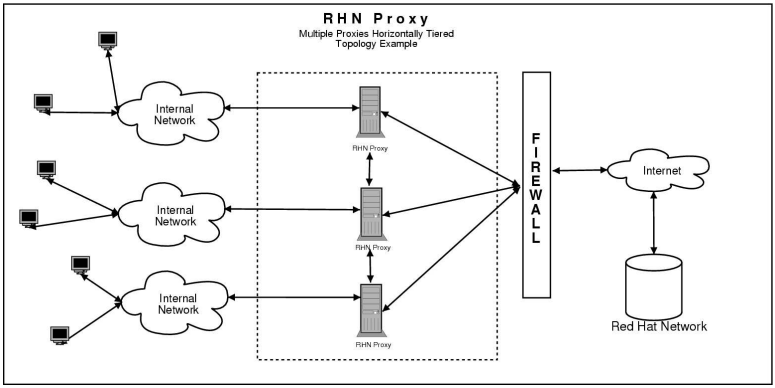

Figure 3-2. Multiple Proxy Horizontally Tiered Topology

3.3. Multiple Proxy Vertically Tiered Topology

An alternative method for multiple RHN Proxy Servers is to establish a primary Proxy that the others connect to for RPMs from Red Hat Network and custom packages created locally. In essence, the secondary Proxies act as clients of the primary. This alleviates the need to establish synchronization between the RHN Proxy Servers as they use the `up2date` functionality inherent with the product.

Like the horizontally tiered configuration, this vertical method allows any client of any RHN Proxy Servers to have all custom packages delivered to them. The Proxy merely looks in its repository to see if it can find the package on its filesystem. If not, it then makes the attempt from the next level up.

This vertically tiered configuration ensures the secondary Proxies depend upon the primary for updates from RHN, as well as for custom packages. Also, custom channels and packages must be placed on the primary Proxy only, to ensure distribution to the child Proxies. Finally, the configuration files of the secondary Proxies must point to the primary, instead of directly at Red Hat Network.

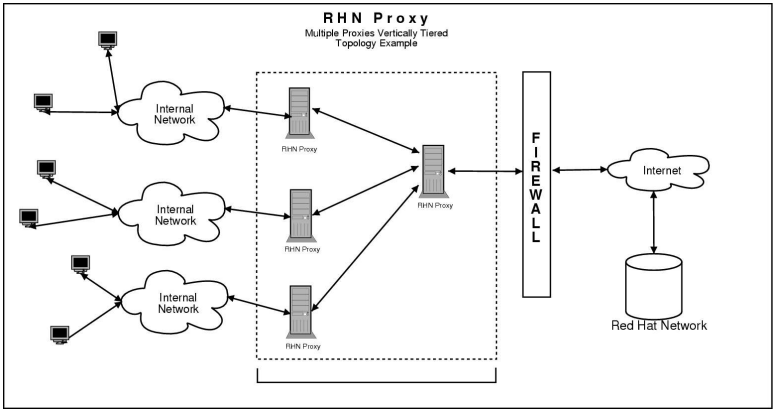

Figure 3-3. Multiple Proxy Vertically Tiered Topology

3.4. Proxies with RHN Satellite Server

In addition to the methods described in detail within this chapter, customers also have the option of using RHN Proxy Server in conjunction with RHN Satellite Server. This works similarly to the vertically tiered Proxy configuration but increases capacity significantly, as Satellites can serve a much greater number of client systems.

For a thorough description of this combination, refer to the Example Topologies chapter of the *RHN Satellite Server Installation Guide*. Linking the two products' SSL certificates is described in the *RHN Client Configuration Guide*. To find out how channels and packages are shared between them, refer to the *RHN Channel Management Guide*.

Chapter 4.

Installation

This chapter describes the initial installation of the RHN Proxy Server. It presumes the prerequisites listed in Chapter 2 *Requirements* have been met. However, if you are *upgrading* to a newer version of RHN Proxy Server, contact your Red Hat representative for assistance.

4.1. Base Install

The RHN Proxy Server is designed to run on the Red Hat Enterprise Linux AS operating system. Therefore, the first phase is to install the base operating system, either from disc, ISO image, or kickstart. During and after operating system installation, make sure you:

- Allocate plenty of space to the partition that will be used to store packages, according to the hardware requirements set forth earlier. The default location for cached Red Hat packages is `/var/spool/squid`, while custom packages are located in `/var/spool/rhn-proxy`.
- Install the packages required by RHN Proxy Server and only those packages. *You must install only the base packages as others will cause the RHN Proxy Server installation to fail* Refer to Section 2.1 *Software Requirements* for the method to obtain the correct package group needed for each version of Red Hat Enterprise Linux AS.


Important

If you plan to obtain Monitoring-level service, you *must* install your RHN Proxy Server on Red Hat Enterprise Linux AS 3 Update 5 or Red Hat Enterprise Linux AS 4. These are the only supported base operating systems for Proxies serving Monitoring-entitled systems.

- Enable Network Time Protocol (NTP) on the Proxy and select the appropriate time zone. All client systems should already be running the `ntpd` daemon and be set to the correct time zone.
- Disable the `ipchains` and `iptables` services after installation.

4.2. RHN Proxy Server Installation Process

The following instructions describe the RHN Proxy Server installation process:

1. Register the newly installed Red Hat Enterprise Linux AS system with Red Hat Network (either the central RHN Servers or your RHN Satellite Server) using the organizational account containing the RHN Proxy Server entitlement with the command: `up2date --register`.
2. Grant the system a Provisioning entitlement by visiting the RHN Website (or the fully qualified domain name of the Satellite serving the Proxy), logging in as the Organization Administrator, navigating to the **Systems** ⇒ **System Entitlements** page, checking the box of system on which the RHN Proxy Server is to be installed and clicking the **Add Provisioning** button.
3. Ensure the system is subscribed to the Red Hat Network Tools channel for its base operating system by clicking the name of the system and navigating to the **System** ⇒ **System Details** ⇒ **Channels** ⇒ **Software** subtab. If the Red Hat Network Tools channel is *not* selected, please select it and subscribe the system to this channel by clicking on the **Change Subscriptions** button.

4. Install all the `rhncfg` packages by navigating to the **System** ⇒ **System Details** ⇒ **Packages** ⇒ **Install** subtab and searching for `rhncfg` using the **Filter by Package Name** text search box. In the resulting list, select all the packages and install them.

5. If you will be enabling secure sockets layer (SSL) encryption on the Proxy and connecting to the central RHN Servers, install the `rhns-certs-tools` package from the same Red Hat Network Tools channel and use the **RHN SSL Maintenance Tool** to generate the tar file required later. Refer to the SSL Certificates chapter of the *RHN Client Configuration Guide* for instructions.

   If you will be enabling SSL encryption on the Proxy and connecting to an *RHN Satellite Server* or another *RHN Proxy Server* with SSL, you will also need the CA certificate password used for the parent system.

6. Log into the system through a terminal as root and run the `rhn_check` command to immediately initiate the scheduled package installation.

7. Once the packages have been installed, as confirmed through the **System Details** ⇒ **Events** tab, prepare the system to accept remote commands and configuration management with the following command:
   ```
   /usr/bin/rhn-actions-control --enable-all
   ```

8. Within the RHN website, navigate to the **System Details** ⇒ **Proxy** subtab.

Warning

Please note the RHN Proxy Server installation may replace the `squid.conf` and `httpd.conf` configuration files on the system to ease upgrades later. If you have edited these files and want to preserve them, they are rotated in place and can be retrieved after installation.

Figure 4-1. System Details ⇒ Proxy

9. In the **System Details** ⇒ **Proxy** subtab, the pulldown menu should indicate your ability to activate the system as an RHN Proxy Server. Ensure the version is properly selected and click the **Activate Proxy** button. The **Welcome** page of the installation appears.

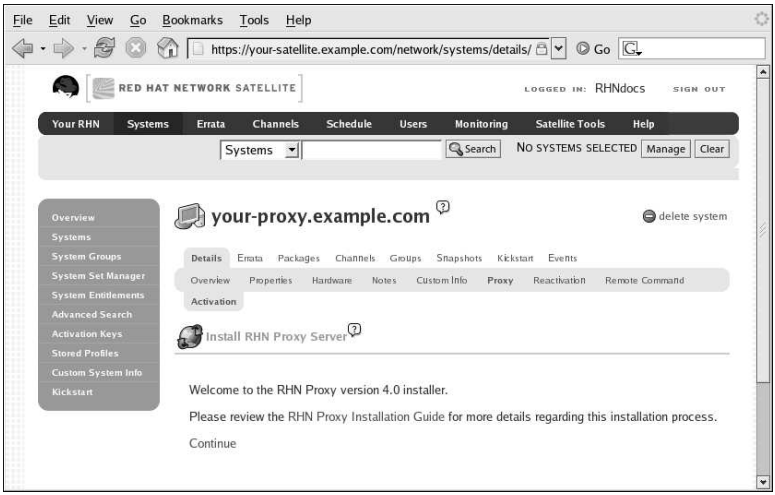

Figure 4-2. Welcome

10. In the **Welcome** page, you will find notification of any requirements not met by the system. When the system is ready, a **continue** link appears. Click it to go to the **Terms & Conditions** page.

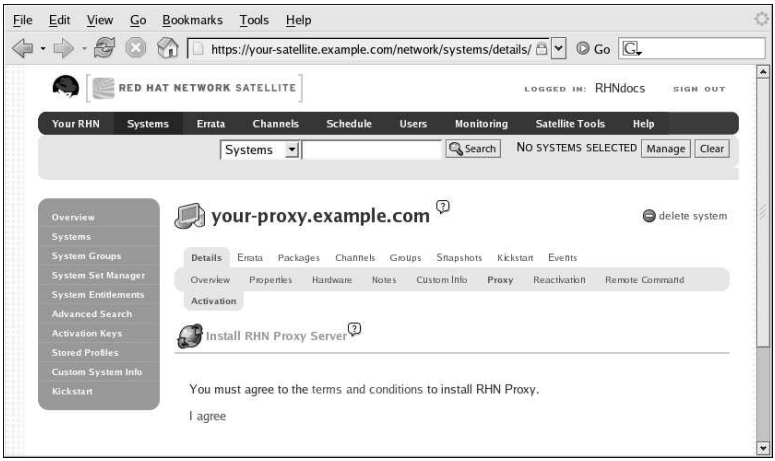

Figure 4-3. Terms & Conditions

11. In the **Terms & Conditions** page, click the **terms and conditions** link to view the licensing agreement of the RHN Proxy Server. When satisfied, click the **I agree** link. The **Enable Monitoring** page appears next.

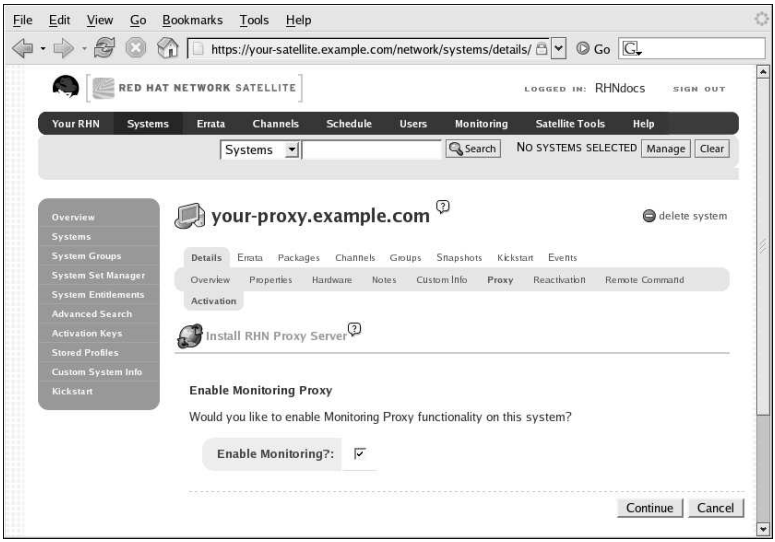

Figure 4-4. Enable Monitoring

12. In the **Enable Monitoring** page, you must decide whether the Proxy will be used to monitor systems served by it. For this to take place, the RHN Proxy Server must meet the requirements identified in Chapter 2 *Requirements* and be connected to an RHN Satellite Server (or another Proxy connected to a Satellite). To enable monitoring on the Proxy, select the checkbox and click **continue**. The **Configure RHN Proxy Server** page appears.

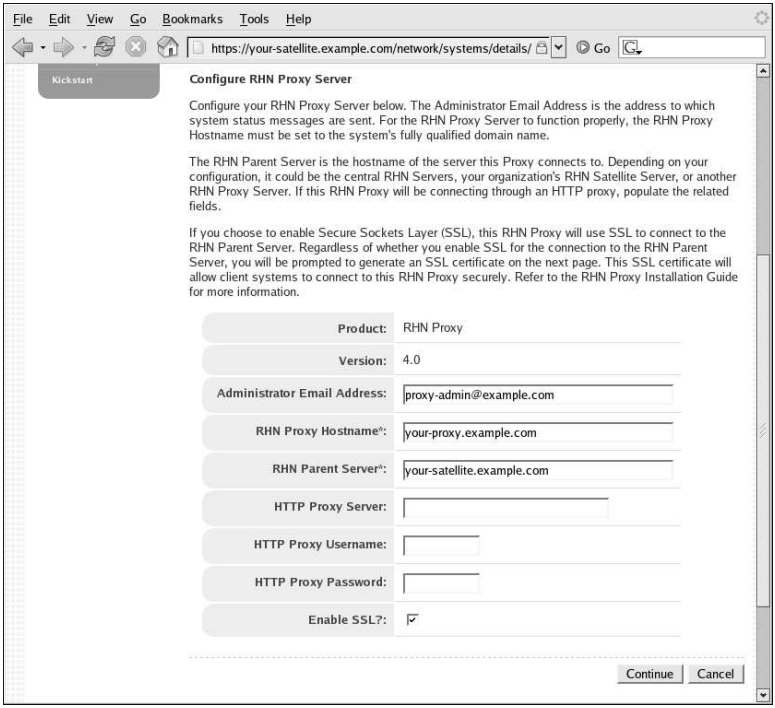

Figure 4-5. Configure RHN Proxy Server

13. In the **Configure RHN Proxy Server** page, provide or confirm the entries for all required fields. The Administrator Email Address will receive all mail generated by the Proxy, including sometimes large quantities of error-related tracebacks. To stem this flow, consider establishing mail filters that capture messages with a subject of "RHN TRACEBACK from *hostname*". To list more than one administrator, enter a comma-separated list of email addresses.

    The RHN Proxy Hostname is the fully qualified domain name (FQDN) of the RHN Proxy Server. The RHN Parent Server is the domain name of the server serving the Proxy, either the central RHN Servers, another RHN Proxy Server or an RHN Satellite Server. To connect to the central RHN Servers, include the value **`xmlrpc.rhn.redhat.com`**. To connect to a Satellite or another Proxy, enter the parent system's FQDN.

    If the RHN Proxy Server will connect through an HTTP proxy, configure it using the associated fields. Note that references to protocol, such as **`http://`** or **`https://`** should not be included in the **HTTP Proxy Server** field. Insert only the hostname and port in the form hostname:port, such as my.corporate.gateway.example.com:3128.

Tip

The installation process affects only the Proxy configuration file: `/etc/rhn/rhn.conf`. The **Red Hat Update Agent** (`up2date`) configuration file, `/etc/sysconfig/rhn/up2date`, must be updated manually to receive its updates from another server, such as an RHN Satellite Server.

Finally, you must decide whether to enable SSL using the checkbox at the bottom. Red Hat strongly recommends you employ this level of encryption for all traffic to and from the RHN Proxy Server. To select it, however, you must be connecting to the central RHN Servers (which have SSL enabled by default) or to an RHN Satellite Server or RHN Proxy Server that has SSL enabled. Connection to the central RHN Servers requires upload of the certificate tar file mentioned earlier. Connection to a Satellite or another Proxy through SSL requires the CA certificate password used in enabling SSL on the parent system.

If you will not enable SSL during installation, leave this box unchecked and refer to the SSL Certificates chapter of the *RHN Client Configuration Guide* to learn how to obtain this level of security post install. When finished, click **continue**. If you enabled SSL and are connecting to a Satellite or another Proxy, the **Configure SSL** page appears. If you enabled SSL and are connecting to the central RHN servers, the **Upload SSL** page appears. If you did not enable SSL but did enable Monitoring, skip to the description of the **Configure Monitoring** page. If you did not enable SSL or Monitoring, skip to the description of the **Install Progress** page.

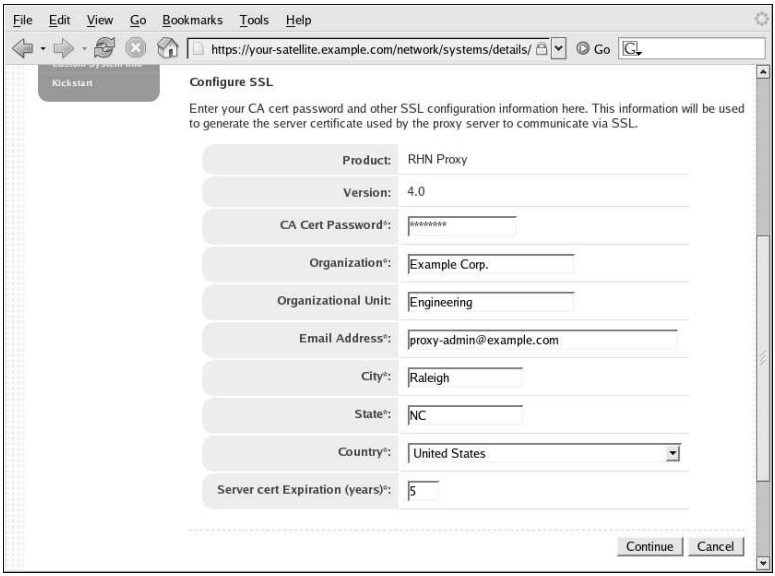

Figure 4-6. Configure SSL

14. In the **Configure SSL** page *applicable only to a Proxy connecting to an RHN Satellite Server or another RHN Proxy Server with SSL enabled*, provide the information needed to generate the server certificate. The most important item is the CA certificate password, which must match the password used while enabling SSL on the parent server. The remaining fields may match the parent server's values but can differ depending on the role of the RHN Proxy Server, for instance reflecting a different geographic location. Similarly, the email address can be the same one provided earlier for the Proxy administrator but can be directed to a particular certificate administrator. Certificate expiration is configurable. As always, ensure the values provided here exist in the backups of information described in Chapter 2 *Requirements*. Once finished, click **continue**.

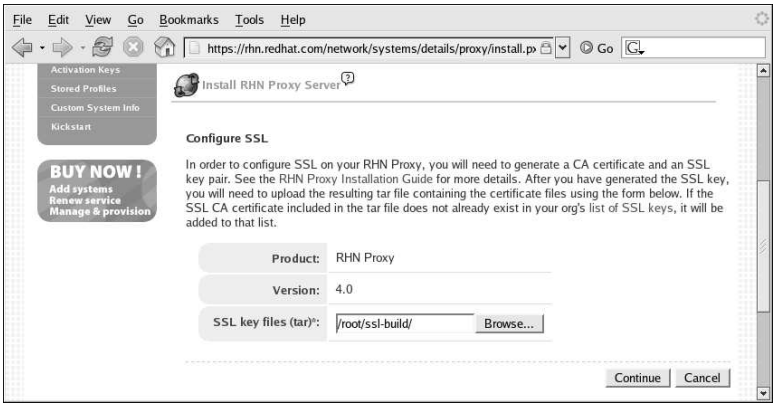

Figure 4-7. Upload SSL

In the **Upload SSL** page *applicable only to a Proxy connecting to the central RHN Servers*, locate the tar file created using the **RHN SSL Maintenance Tool** using the **Browse** button. It will be named `rhn-org-httpd-ssl-archive-`*`MACHINENAME-VERSION`*`.tar` with the machine name reflecting the Proxy's hostname. Once located, click **continue**.

Note

Since you must be root to generate the SSL key, the resulting SSL tar file will be located in `/root/ssl-build/`*`HOSTNAME/`*. This file will *not* be visible to a non-root user, therefore you must copy the file to a location visible to the user running the browser.

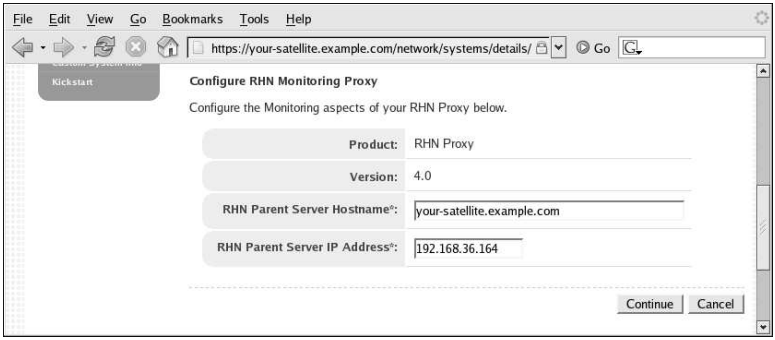

Figure 4-8. Configure Monitoring

15. In the **Configure Monitoring** page, provide or confirm the hostname and IP address of the parent server connected to by the RHN Proxy Server. This must be either an RHN Satellite Server or another Proxy which is in turn connected to a Satellite. *You cannot achieve Monitoring through the central RHN Servers.* When finished, click **continue**. The **Install Progress** page appears.

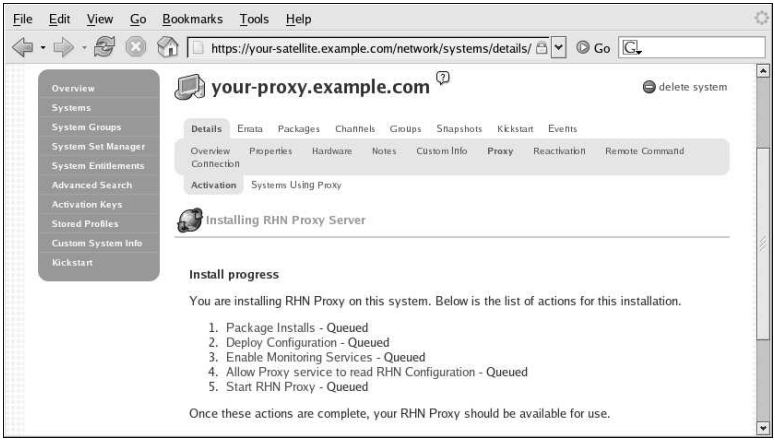

Figure 4-9. Install Progress

16. In the **Install Progress** page, you may monitor the steps of the installation as they take place. Click the link to any step to go to its **Action Details** page. When a step has been undertaken, its status goes from `Queued` to `Picked Up` and then finally to `Completed`. Like the earlier package installs, you can immediately trigger these steps by running the `rhn_check` command in a terminal on the system as root. When finished, the **Install Progress** page will display the message `The installation is complete`. You may now begin registering systems to be served by the RHN Proxy Server. Refer to the *RHN Client Configuration Guide*.

Chapter 5.

RHN Package Manager

The RHN Package Manager is a command line tool that allows an organization to serve local packages associated with a private RHN channel through the RHN Proxy Server. If you want the RHN Proxy Server to update only official Red Hat packages, you do not need to install the RHN Package Manager.

To use the RHN Package Manager, install the `rhns-proxy-package-manager` package and its dependencies.

Only the header information for packages is uploaded to the RHN Servers. The headers are required so that RHN can resolve package dependencies for the client systems. The actual package files (`*.rpm`) are stored on the RHN Proxy Server.

The RHN Package Manager uses the same settings as the Proxy, defined in the `/etc/rhn/rhn.conf` configuration file.

5.1. Creating a Private Channel

Before local packages can be provided through the RHN Proxy Server, a private channel is needed to store them. Perform the following steps to create a private channel:

1. Log in to the RHN Web interface at https://rhn.redhat.com.
2. Click **Channels** on the top navigation bar. If the **Manage Channels** option is not present in the left navigation bar, ensure this user has channel editing permissions set. Do this through the **Users** category accessible through the top navigation bar.
3. In the left navigation bar, click **Manage Software Channels** and then the **create new channel** button at the top-right corner of the page.
4. Select a parent channel and base channel architecture, then enter a name, label, summary, and description for the new private channel. The channel label must: be at least six characters long, begin with a letter, and contain only lowercase letters, digits, dashes (-), and periods(.). Also enter the URL of the channel's GPG key. Although this field isn't required, it is recommended to enhance security. For instructions on generating GPG keys, refer to the RHN Channel Management Guide.
5. Click **Create Channel**.

5.2. Uploading Packages

Note

You must be an Organization Administrator to upload packages to private RHN channels. The script will prompt you for your RHN username and password.

After creating the private channel, upload the package headers for your binary and source RPMs to the RHN Server and copy the packages to the RHN Proxy Broker Server. To upload the package headers for the binary RPMs, at the command line:

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

pkg-list is the list of packages to be uploaded. Alternatively, use the `-d` option to specify the local directory that contains the packages to add to the channel. Ensure the directory contains only the packages to be included and no other files. RHN Package Manager can also read the list of packages from standard input (using `--stdin`).

To upload the package headers for the source RPMs:

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

If you have more than one channel specified (using `-c` or `--channel`), the uploaded package headers will be linked to all the channels listed.

Note

If a channel name is not specified, the packages are not added to any channel. The packages can then be added to a channel using the Red Hat Network Web interface. The interface can also be used to modify existing private channels.

After uploading the packages, you can immediately check the RHN Web interface to verify their presence. Click **Channels** in the top navigation bar, **Manage Software Channels** in the left navigation bar, and then the name of the custom channel. Then click the **Packages** subtab. Each RPM should be listed.

You can also check to see if the local directory is in sync with the RHN Server's image of the channels at the command line:

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

This `-s` option will list all the missing packages (packages uploaded to the RHN Server not present in the local directory). You must be an Organization Administrator to use this command. The script will prompt you for your RHN username and password. Refer to Table 5-1 for additional command line options.

If you are using the RHN Package Manager to update local packages, you must go to the RHN website to subscribe the system to the private channel.

5.3. Command Line Options

A summary of all the command line options for RHN Package Manager `rhn_package_manager`:

Option	Description
`-v`, `--verbose`	Increase verbosity.
`-d`*DIR*, `--dir=`*DIR*	Process packages from directory *DIR*.
`-c`*CHANNEL*, `--channel=`*CHANNEL*	Manage this channel — may be present multiple times.
`-n`*NUMBER*, `--count=`*NUMBER*	Process this number of headers per call — the default is 32.

Option	Description
`-l`, `--list`	List each package name, version number, release number, and architecture in the specified channel(s).
`-s`, `--sync`	Check if local directory is in sync with the server.
`-p`, `--printconf`	Print the current configuration and exit.
`-X`*`PATTERN`*, `--exclude=`*`PATTERN`*	Exclude files matching this glob expression — can be present multiple times.
`--newest`	Push only the packages that are newer than packages already pushed to the server for the specified channel.
`--stdin`	Read the package names from stdin.
`--nosig`	Push unsigned packages. By default the RHN Package Manager attempts to push only signed packages.
`--username=`*`USERNAME`*	Specify your RHN username. If you do not provide one with this option, you will be prompted for it.
`--password=`*`PASSWORD`*	Specify your RHN password. If you do not provide one with this option, you will be prompted for it.
`--source`	Upload source package headers.
`--dontcopy`	In the post-upload step, do not copy the packages to their final location in the package tree.
`--test`	Only print the packages to be pushed.
`--no-ssl`	*Not recommended* — Turn off SSL.
`-?`, `--usage`	Briefly describe the options.
`--copyonly`	Copies the file listed in the argument into the specified channel. Useful when a channel on the proxy is missing a package and you don't want to reimport all of the packages in the channel. E.g., `rhn_package_manager -c`*`CHANNEL`* `--copyonly` */PATH/TO/MISSING/FILE*
`-h`, `--help`	Display the help screen with a list of options.

Table 5-1. `rhn_package_manager` options

Tip

These command line options are also described in the `rhn_package_manager` man page: `man rhn_package_manager`.

Chapter 6.

Troubleshooting

This chapter provides tips for determining the cause of and resolving the most common errors associated with RHN Proxy Server. If you need additional help, contact Red Hat Network support at https://rhn.redhat.com/help/contact.pxt. Log in using your Satellite-entitled account to see your full list of options.

6.1. Managing the Proxy Service

Since the RHN Proxy Server consists of a multitude of individual components, Red Hat provides a master service, `rhn-proxy`, that allows you to stop, start, or retrieve status from the various services in the appropriate order. This helper service accepts all of the typical commands:

```
service rhn-proxy start
service rhn-proxy stop
service rhn-proxy restart
service rhn-proxy status
```

Use the `rhn-proxy` service to shut down and bring up the entire RHN Satellite Server and retrieve status messages from all of its services at once.

6.2. Log Files

Virtually every troubleshooting step should start with a look at the associated log file or files. These files provide invaluable information about the activity that has taken place on the device or within the application and can be used to monitor performance and ensure proper configuration. See Table 6-1 for the paths to all relevant log files:

Component	Log File Location
Apache HTTP Server	`/var/log/httpd/` directory
Squid	`/var/log/squid/` directory
RHN Proxy Broker Server	`/var/log/rhn/rhn_proxy_broker.log`
RHN SSL Redirect Server	`/var/log/rhn/rhn_proxy_redirect.log`
Red Hat Update Agent	`/var/log/up2date`

Table 6-1. Log Files

6.3. Questions and Answers

This section contains the answers to the most frequently asked questions regarding installing and configuring an RHN Proxy Server solution.

1. After configuring the RHN Package Manager how can I determine if the local packages were successfully added to the private RHN channel?

Use the command `rhn_package_manager -l -c "name_of_private_channel"` to list the pri-

vate channel packages known to the RHN Servers. Or visit the RHN Web interface.

After subscribing a registered system to the private channel, you can also execute the command `up2date -l --showall` on the registered system and look for the packages from the private RHN channel.

2. How can I determine whether the clients are connecting to the Squid server?

The `/var/log/squid/access.log` file logs all connections to the Squid server.

3. The **Red Hat Update Agent** on the client systems will not connect through the RHN Proxy Server. How can I resolve this error?

Make sure the latest version of the **Red Hat Update Agent** is installed on the client systems. The latest version contains features necessary to connect through an RHN Proxy Server. The latest version can be obtained through the Red Hat Network or from http://www.redhat.com/support/errata/. Also, be advised that since the RHN Proxy Server acts as a caching mechanism for RHN, the `httpProxy` setting in `/etc/sysconfig/rhn/up2date` on client systems is redundant and probably unnecessary.

The RHN Proxy Server is an extension of Apache. See Table 6-1 for its log file location.

4. My RHN Proxy Server configuration does not work. Where do I begin troubleshooting it?

Make sure `/etc/sysconfig/rhn/systemid` is owned by root.apache with the permissions 0640.

Read the log files. A list is available at Table 6-1.

6.4. General Problems

To begin troubleshooting general problems, examine the log file or files related to the component exhibiting failures. A useful exercise is to tail all log files and then run `up2date --list`. You should then examine all new log entries for potential clues.

A common issue is full disk space. An almost sure sign of this is the appearance of halted writing in the log files. If logging stopped during a write, such as mid-word, you likely have filled disks. To confirm this, run this command and check the percentages in the Use% column:

```
df -h
```

In addition to log files, you can obtain valuable information by retrieving the status of your various components. This can be done for the Apache HTTP Server and Squid.

To obtain the status of the Apache HTTP Server, run the command:

```
service httpd status
```

To obtain the status of Squid, run the command:

```
service squid status
```

If the administrator isn't getting email from the RHN Proxy Server, confirm the correct email addresses have been set for `traceback_mail` in `/etc/rhn/rhn.conf`.

6.5. Host Not Found/Could Not Determine FQDN

Because RHN configuration files rely exclusively on fully qualified domain names (FQDN), it is imperative key applications are able to resolve the name of the RHN Proxy Server into an IP address. **Red Hat Update Agent**, **Red Hat Network Registration Client**, and the Apache HTTP Server are particularly prone to this problem with the RHN applications issuing errors of "host not found" and the Web server stating "Could not determine the server's fully qualified domain name" upon failing to start.

This problem typically originates from the `/etc/hosts` file. You may confirm this by examining `/etc/nsswitch.conf`, which defines the methods and the order by which domain names are resolved. Usually, the `/etc/hosts` file is checked first, followed by Network Information Service (NIS) if used, followed by DNS. One of these has to succeed for the Apache HTTP Server to start and the RHN client applications to work.

To resolve this problem, identify the contents of the `/etc/hosts` file. It may look like this:

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

First, in a text editor, remove the offending machine information, like so:

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

Then, save the file and attempt to re-run the RHN client applications or the Apache HTTP Server. If they still fail, explicitly identify the IP address of the Proxy in the file, such as:

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

Replace the value here with the actual IP address of the Proxy. This should resolve the problem. Keep in mind, if the specific IP address is stipulated, the file will need to be updated when the machine obtains a new address.

6.6. Connection Errors

If your are experiencing problems that you believe to be related to failed connections, follow these measures:

- Confirm the correct `rhn-org-httpd-ssl-key-pair-`*`MACHINE_NAME-VER-REL`*`.noarch.rpm` is installed on the RHN Proxy Server and the corresponding `rhn-org-trusted-ssl-cert-*.noarch.rpm` or raw CA SSL public (client) certificate is installed on all client systems.
- Verify the client systems are configured to use the appropriate certificate.
- If using one or more RHN Proxy Servers, ensure each Proxy's SSL certificate is prepared correctly. If using the RHN Proxy Server in conjunction with an RHN Satellite Server the Proxy should have both its own server SSL key-pair and CA SSL public (client) certificate installed, since it will serve in both capacities. Refer to the SSL Certificates chapter of the *RHN Client Configuration Guide* for specific instructions.
- If the RHN Proxy Server is connecting through an HTTP Proxy, make sure the URL listed is valid. For instance, the HTTP Proxy URL field should not contain references to protocols, such as http:// or https://. Only the hostname and port should be included in the form hostname:port, such as corporate_gateway.example.com:8080.
- Make sure client systems are not using firewalls of their own blocking required ports, as identified in Section 2.4 *Additional Requirements*.

6.7. Caching Issues

If package delivery fails or an object appears to be corrupt, and it isn't related to connection errors, you should consider clearing the caches. The RHN Proxy Server has two caches you should be concerned with: one for Squid and the other for authentication.

The Squid cache is located in `/var/spool/squid/`. To clear it, stop the Apache HTTP Server and Squid, delete the contents of that directory, and restart both services. Issue these commands in this order:

```
service httpd stop
service squid stop
rm -fv /var/spool/squid/*
service squid start
service httpd start
```

You may accomplish the same task more quickly by just clearing the directory and restarting squid, but you will likely receive a number of RHN traceback messages.

The internal caching mechanism used for authentication by the Proxy may also need its cache cleared. To do this, issue the following command:

```
rm -fv /var/cache/rhn/*
```

Although the RHN Authentication Daemon was deprecated with the release of RHN Proxy Server 3.2.2 and replaced with the aforementioned internal authentication caching mechanism, the daemon may still be running on your Proxy. To turn it off, issue the following individual commands in this order:

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

To clear its cache, issue:

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

If you must retain the RHN Authentication Daemon, which Red Hat recommends against and does not support, note that its performance can suffer from verbose logging. For this reason, its logging (to `/var/log/rhn/rhn_auth_cache.log`) is turned off by default. If you do run the daemon and desire logging, turn it back on by adding the following line to the Proxy's `/etc/rhn/rhn.conf` file:

```
auth_cache.debug = 2
```

6.8. Proxy Debugging by Red Hat

If you've exhausted these troubleshooting steps or want to defer them to Red Hat Network professionals, Red Hat recommends you take advantage of the strong support that comes with RHN Proxy Server. The most efficient way to do this is to aggregate your Proxy's configuration parameters, log files, and database information and send this package directly to Red Hat.

RHN provides a command line tool explicitly for this purpose: The **RHN Proxy Diagnostic Info Gatherer**, commonly known by its command `rhn-proxy-debug`. To use this tool, simply issue that command as root. You will see the pieces of information collected and the single tarball created, like so:

```
[root@rhel-4 root]# rhn-proxy-debug
Collecting and packaging relevant diagnostic information.
Warning: this may take some time...
```

```
    * copying configuration information
    * copying logs
    * querying RPM database (versioning of RHN Proxy, etc.)
    * get diskspace available
    * timestamping
    * creating tarball (may take some time): /tmp/rhn-proxy-debug.tar.bz2
    * removing temporary debug tree

Debug dump created, stored in /tmp/rhn-proxy-debug.tar.bz2
Deliver the generated tarball to your RHN contact or support channel.
```

Once finished, email the new file from the `/tmp/` directory to your Red Hat representative for immediate diagnosis.

Appendix A.

Sample RHN Proxy Server Configuration File

The `/etc/rhn/rhn.conf` configuration file for the RHN Proxy Server provides a means for you to establish key settings. Be warned, however, that errors inserted into this file may cause Proxy failures. Make configuration changes with caution.

If you are also using an RHN Satellite Server, you should be particularly concerned with the following parameters: traceback_mail and proxy.rhn_parent. Review the sample and its comments (beginning with a hash mark #), for additional details.

Note

You may add the `use_ssl` setting to `rhn.conf` for testing purposes only. Set its value to 0 to turn off SSL between the Proxy and the upstream server temporarily. Note that this greatly compromises security. Return the setting to its default value of 1 to re-enable SSL, or simply remove the line from the configuration file.

```
# 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
```

Index