Servidor Proxy RHN 4.0

Manual de instalación



Servidor Proxy RHN 4.0: Manual de instalación

Copyright © 2001 - 2005 por Red Hat, Inc.



Red Hat, Inc.

1801 Varsity Drive Raleigh NC 27606-2072 USA Teléfono: +1 919 754 3700 Teléfono: 888 733 4281 Fax: +1 919 754 3701 PO B
search Triangle Park NC 27709 USA

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

Copyright © 2005 por Red Hat, Inc. Este material solamente se distribuye bajo los términos y condiciones establecidas en la Open Publication License, V1.0 o versiones posteriores (la última versión está disponible en http://www.opencontent.org/openpub/).

Los derechos de autor del propietario prohiben la distribución de versiones de este documento sustancialmente modificadas sin un permiso explícito.

La distribución del producto o una copia del mismo en forma de libro con fines comerciales está prohibida a menos que se obtenga permiso previo del propietario de los derechos de autor.

Red Hat y el logo "Shadow Man" de Red Hat, son marcas registradas de Red Hat, Inc. en los Estados Unidos y otros países.

Todas las demás marcas referenciadas aquí son propiedad de sus respectivos dueños.

La marca de GPG de la clave security@redhat.com es:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Tabla de contenidos

1. Introducción 1
1.1. Red Hat Network 1
1.2. Servidor Proxy RHN 1
1.3. Terminología básica 3
1.4. Cómo funciona 4
2. Requerimientos 7
2.1. Requerimientos de software 7
2.2. Requerimientos de hardware 8
2.3. Requerimientos de espacio de disco 8
2.4. Requerimientos adicionales 9
3. Topologías de ejemplo 11
3.1. Topología con un único Proxy 11
3.2. Topología de múltiples Proxies enlazados horizontalmente 12
3.3. Topología de múltiples Proxies ordenados verticalmente 13
3.4. Proxies con un Servidor Satellite RHN 14
4. Instalación 15
4.1. Instalación base 15
4.2. Proceso de instalación del Servidor Proxy RHN 15
5. Gestor de paquetes de RHN 27
5.1. Creando un canal privado 27
5.2. Actualizando los paquetes 27
5.3. Opciones para la línea de comandos 29
6. Localización de errores 31
6.1. Administrando el servicio Proxy 31
6.2. Archivos de registro 31
6.3. Preguntas y respuestas 32
6.4. Problemas generales 33
6.5. Host Not Found/Could Not Determine FQDN 33
6.6. Errores de conexión 34
6.7. Problemas relacionados con el caché 35
6.8. Depuración del Proxy por Red Hat 36
A. Ejemplo del archivo de configuración del Servidor Proxy RHN 37
Índice 39

Capítulo 1.

Introducción

1.1. Red Hat Network

Red Hat Network (RHN) es el entorno para la asistencia al nivel del sistema y la administración de sistemas y redes de sistemas Red Hat. Red Hat Network reune las herramientas, servicios y los depósitos de información necesarios para maximizar la fiabilidad, seguridad y rendimiento de sus sistemas. Para poder utilizar RHN, los administradores del sistema registran los perfiles de software y hardware de sus sistemas clientes, conocidos como perfiles del sistema, en Red Hat Network. Cuando un sistema solicita una actualización de paquetes, se retornarán tan sólo los paquetes aplicables para el cliente (en base a los perfiles de software almacenados en el servidor RHN).

Entre las ventajas de usar Red Hat Network se incluyen:

- Escalabilidad — con Red Hat Network, un sólo administrador del sistema puede configurar y mantener cientos o miles de sistemas Red Hat con una facilidad, certeza y rapidez mayor de la que tendría al mantener un sistema individual sin Red Hat Network.
- Protocolos estándar — los protocolos estándar son usados para mantener la seguridad e incrementar la capacidad. Por ejemplo, XML-RPC le permite a Red Hat Network realizar muchas más operaciones además de la descarga de archivos.
- Seguridad — todas las comunicaciones entre los sistemas registrados y Red Hat Network son realizadas a través de conexiones seguras de Internet.
- Vista de las alertas de erratas — las alertas de erratas para todos sus sistemas cliente son fácilmente visibles a través de un sitio web.
- Acciones programadas — utilice el sitio web para programar acciones, incluyendo actualizaciones de erratas, instalación de paquetes y actualizaciones del perfil de software.
- Simplificación — el mantenimiento de un sistema Red Hat se convierte en un sencillo proceso automatizado.

1.2. Servidor Proxy RHN

Un Servidor Proxy RHN es un servicio implementado dentro de una red corporativa con funciones Red Hat Network avanzadas, tales como el mecanismo de paquetes en caché para reducir el ancho de banda y la personalización de paquetes para permitir la implementación de paquetes personalizados.

Este servicio le permite a las empresas y corporaciones guardar en caché las actualizaciones de RPM en un Servidor Proxy RHN interno y centralizado, y permite que los sistemas clientes descarguen las actualizaciones desde ese servidor en vez de uno de los servidores de RHN [1] a través de Internet. Los perfiles del sistema de los clientes y la información del usuario están almacenadas de forma segura en los servidores centrales de RHN, los cuales hospedan también el sitio web de RHN (rhn.redhat.com). El Proxy actúa como un intermediario entre los sistemas cliente y Red Hat Network (o un Servidor Satellite RHN). Sólo los archivos de paquetes están almacenados en el Servidor Proxy RHN. Cada transacción está autenticada y el **Agente de actualización de Red Hat** revisa la firma GPG de cada paquete recibido desde el Servidor Proxy RHN local.

Además de almacenar paquetes oficiales de Red Hat, el Servidor Proxy RHN puede ser configurado para repartir los paquetes personalizados de la propia organización desde un *canal* RHN privado, usando el Gestor de paquetes de RHN. Por ejemplo, una organización puede desarrollar su propio software, empaquetarlo en un RPM, firmarlo con su propia firma GPG y usar el Servidor Proxy RHN local para actualizar todos los sistemas individuales en la red con las últimas versiones del software personalizado.

Entre las ventajas de usar el Servidor Proxy RHN se incluyen:

- Escalabilidad — puede haber más de un Servidor Proxy RHN dentro de una organización.
- Seguridad — Se mantiene una conexión segura de punta a punta: desde el sistema cliente al Servidor Proxy RHN local a los servidores Red Hat Network.
- Velocidad — los paquetes son entregados más rápidamente a través de una red de área local que a través de Internet.
- Ahorro de ancho de banda — los paquetes son descargados desde el servidor de archivos de RHN solamente una vez (mediante el mecanismo de cacheo de cada servidor Proxy) en vez de descargar cada paquete a cada sistema cliente.
- Ahorro de espacio de disco en sistemas individuales — se requiere un arreglo grande de disco en vez de espacio de disco extra en todos los sistemas cliente.
- Actualizaciones personalizadas — crea un sistema de entrega de paquetes automatizado para paquetes de software personalizado, así como de los paquetes oficiales de Red Hat requeridos por el sistema cliente. Los canales de RHN personalizados y privados le permiten a una organización la entrega automatizada de paquetes internos a ésta.
- Configuración personalizada — la habilidad de restringir o conceder actualizaciones a arquitecturas específicas o diferentes versiones de sistema operativo.
- Sólo una conexión a Internet requerida — el sistema cliente se conecta a través del servidor Proxy con HTTP activado, por lo cual no necesita una conexión a la red externa

1. A través de todo este documento, reemplace el servidor RHN por Servidor Satellite RHN, si el Servidor Proxy RHN está conectado a un Servidor Satellite RHN

(Internet), pero sólo requiere acceso a la red de área local (LAN) a la cual el Servidor Proxy RHN está conectado. Sólo el Servidor Proxy RHN necesita una conexión a Internet para contactar los servidores RHN, a menos que el Servidor Proxy RHN esté utilizando un Servidor Satellite RHN, en dicho caso, sólo el Servidor Satellite RHN requerirá una conexión a Internet.

1.3. Terminología básica

Antes de entender el funcionamiento del Servidor Proxy RHN, es importante familiarizarse con los siguientes términos usados en Red Hat Network:

- *Canal* — un canal es una lista de paquetes de software. Hay dos clase de canal: canales base y canales hijo. Un *canal base* está conformado por una lista de paquetes basada en una arquitectura específica y una versión de Red Hat. Un *canal hijo* es un canal que está asociado a un canal base y que contiene paquetes adicionales.
- *Administrador de la organización* — el Administrador de la organización es un rol de usuario que goza del más alto nivel de control sobre la cuenta Red Hat Network de una organización. Los miembros de este rol pueden añadir otros usuarios, otros sistemas y grupos de sistemas a la organización, así como removerlos. Una cuenta Red Hat Network de una organización debe al menos tener un Administrador de la organización.
- *El administrador de canales* — un administrador de canales es un rol de usuario que tiene acceso total a las funciones de administración de los canales. Los usuarios con este rol tienen la capacidad de crear canales y asignar paquetes a éstos. Este rol puede ser asignado por un Administrador de la organización a través de la pestaña **Usuarios** del sitio web de RHN.
- *Agente de actualización de Red Hat* — El **Agente de actualización de Red Hat** es la aplicación cliente de Red Hat Network (`up2date`) que permite a los usuarios recibir e instalar paquetes actualizados para el sistema cliente en el cual la aplicación está siendo ejecutada.
- *Seguimiento* — Un seguimiento es una descripción detallada de "qué estuvo mal"; esta descripción puede ser usada para la localización de errores del Servidor Proxy RHN. Los seguimientos son generados automáticamente cuando ocurre un error crítico y son enviados por correo a la persona designada en el archivo de configuración del Servidor Proxy RHN.

Para una explicación más detallada de estos y otros términos, consulte el *Manual de Referencia de Red Hat Network* disponible en http://www.redhat.com/docs/.

1.4. Cómo funciona

El **Agente de actualización de Red Hat** en el sistema cliente no contacta directamente un servidor Red Hat Network. En cambio, el cliente (o los clientes) se conectan a un Servidor Proxy RHN que se conecta a un servidor Red Hat Network o a un Servidor Satellite RHN. Así, el sistema cliente no necesita acceso directo a Internet. Éstos necesitan tan sólo tener acceso al Servidor Proxy RHN.



Importante

Red Hat recomienda encarecidamente que los clientes que se conectan con un Servidor Proxy RHN ejecuten la versión más reciente de Red Hat Enterprise Linux para asegurar una conectividad apropiada.

Por defecto, un cliente es autenticado directamente por los servidores de Red Hat Network. La autenticación trabaja de una forma similar cuando se utiliza un Servidor Proxy RHN, con la excepción de que el Servidor Proxy RHN proporciona también la información de ruta. Después de una autenticación exitosa, el servidor Red Hat Network informa al Servidor Proxy RHN que la ejecución de una acción para el cliente es permitida. El Servidor Proxy RHN descarga todas los paquetes actualizados (si éstos aun no están en el caché) y los entrega a los sistemas cliente.

Solicitudes desde el **Agente de actualización de Red Hat** en los sistemas cliente son aún autenticadas en el lado del servidor, pero la entrega de paquetes es significativamente más rápida ya que los paquetes están almacenados en el Servidor Proxy-Caché HTTP o el Servidor Proxy RHN (para paquetes locales); el Servidor Proxy RHN y el sistema cliente están conectados a través del LAN y su limitación depende de la velocidad de la red local.

La autenticación se realiza en el siguiente orden:

1. El cliente realiza una acción de login al inicio de la sesión del cliente. Este login es pasado a través de un Servidor Proxy RHN o más hasta que llega a un servidor Red Hat Network.
2. El servidor Red Hat Network intenta autenticar el cliente. Si la autenticación es satisfactoria, el servidor envía de regreso una señal de sesión a través del Servidor Proxy RHN. Esta señal, la cual tiene una firma y fecha de vencimiento, contiene la información del usuario, incluyendo el nombre de usuario, la suscripción a canales, etc.
3. Cada Servidor Proxy RHN guarda esta señal en su sistema de archivo local en `/var/cache/rhn/`. Al guardarlo se reduce el gasto de autenticación con el servidor Red Hat Network y mejora en gran medida el rendimiento de Red Hat Network.

4. Esta señal de sesión es pasada de regreso a la máquina cliente y es usada en acciones subsecuentes en Red Hat Network.

Desde el punto de vista del cliente, no hay diferencia entre un Servidor Proxy RHN y un servidor Red Hat Network. Desde el punto de vista del servidor Red Hat Network, un Servidor Proxy RHN es una clase especial de clientes de Red Hat Network. Así, los clientes no se ven afectados por la ruta que toma la petición para llegar al servidor Red Hat Network. Toda la lógica se implementa en el Servidor Proxy RHN y el servidor Red Hat Network.

Opcionalmente, el Gestor de paquetes de RHN puede ser instalado y configurado para servir paquetes personalizados escritos especialmente para la organización. Estos no son paquetes oficiales de Red Hat. Después de crear un canal privado de RHN, el paquete RPM personalizado es asociado con el canal privado descargando el encabezado del paquete al servidor RHN. Sólo el encabezado es cargado, no los archivos del paquete. Los encabezados son requeridos ya que éstos contienen información importante sobre el RPM, tal como las dependencias de software, que permiten a RHN automatizar la instalación de paquetes. Los paquetes RPM personalizados son almacenados en el Servidor Proxy RHN y enviados al sistema cliente desde el interior de la red de área local de la organización.

La configuración de una red de computadores para la utilización de un Servidor Proxy RHN es fácil. Las aplicaciones de Red Hat Network en el sistema cliente deben ser configuradas para conectarse al Servidor Proxy RHN en vez de a los servidores Red Hat Network. Consulte el *Manual de configuración de sistemas cliente de RHN* para mayor información. Del lado del proxy, se debe especificar el siguiente proxy en la cadena (la cual terminará eventualmente en un servidor Red Hat Network). Si el Gestor de paquetes de RHN es usado, el sistema cliente debe estar suscrito al canal privado de RHN.

Capítulo 2.

Requerimientos

Estos requerimientos deben cumplirse antes de la instalación. Para instalar la versión 3.6 o posterior del Servidor Proxy RHN desde un Servidor Satellite RHN, la versión del Satellite mismo debe ser 3.6 o superior.

2.1. Requerimientos de software

Para realizar una instalación, los siguientes componentes relacionados con el software deben estar disponibles:

- Sistema operativo base — el Servidor Proxy RHN es soportado únicamente bajo Red Hat Enterprise Linux AS 3 Update 5 o superior o Red Hat Enterprise Linux AS 4. El sistema operativo puede ser instalado desde el disco, imagen ISO local, kickstart o cualquier otro método soportado por Red Hat.



Importante

Si planea utilizar el nivel de servicios Monitoring, usted *debe* instalar el Servidor Proxy RHN en Red Hat Enterprise Linux AS 3 Update 5 o Red Hat Enterprise Linux AS 4. Estos son los únicos sistemas operativos base soportados por Proxies que sirven sistemas con derechos Monitoring.

Cada versión de Red Hat Enterprise Linux AS requiere ciertos juegos de paquetes para soportar el Servidor Proxy RHN. Cualquier otra cosa puede causar errores durante la instalación. Por lo cual, Red Hat le recomienda obtener el juego de paquetes deseado de las siguientes maneras:



Nota

Para instalaciones kickstart de Red Hat Enterprise Linux AS 4 o de Red Hat Enterprise Linux AS 3 Update 5, especifique el siguiente grupo de paquetes: **`@ Base`**

Para instalar Red Hat Enterprise Linux AS 4 o Red Hat Enterprise Linux AS 3 Update 5 mediante CDs o imágenes ISO, seleccione el siguiente grupo de paquetes: **`Mínima`**



Advertencia

SELinux (Security-enhanced Linux) debe ser desactivado en Red Hat Enterprise Linux AS 4 antes de la instalación del Servidor Proxy RHN. Para desactivarlo durante el proceso de instalación mediante CD o imagen ISO, seleccione **`Disabled`** cuando las opciones de soporte SELinux sean presentadas. Para desactivar SELinux durante una instalación kickstart, incluya el comando `selinux --disabled` o espere que la instalación sea completada, edite el archivo `/etc/selinux/config` para que diga `SELINUX=disabled` y reinicie el sistema.

- Un derecho disponible para el Servidor Proxy RHN en su cuenta de Red Hat Network.
- Un derecho Provisioning disponible en su cuenta de Red Hat Network (este debe venir incluido con el derecho del Servidor Proxy RHN).
- Acceso al canal de herramientas en Red Hat Network para la versión Red Hat Enterprise Linux AS instalada.
- Todos los paquetes `rhncfg*` instalados en el Proxy (desde el canal de herramientas de RHN).
- Ya sea el paquete `rhns-certs-tools` instalado en el Proxy (desde el canal Herramientas de RHN) o la contraseña del certificado SSL (secure sockets layer) CA usada para generar el certificado del servidor del nivel superior (por ejemplo, un Servidor Satellite RHN).
- El sistema debe estar configurado para aceptar comandos remotos y la administración de la configuración a través de Red Hat Network. Consulte la Sección 4.2 para obtener mayores instrucciones.

2.2. Requerimientos de hardware

La siguiente configuración de hardware es requerida por el Servidor Proxy RHN:

- Procesador Pentium III, 1.26GHz, 512K de caché o equivalente
- 512 MB de memoria
- 3 GB de almacenamiento para la instalación base de Red Hat Enterprise Linux AS
- 6 GB de almacenamiento por distribución/canal

La carga del Servidor Apache HTTP está directamente relacionada con la frecuencia con la cual los sistemas clientes se conectan con el Proxy; así, si reduce el intervalo predeterminado de cuatro horas (o 240 minutos) como se establece en el archivo de configuración `/etc/sysconfig/rhn/rhnsd` de los sistemas cliente, usted *incrementará* significativamente la carga en este componente.

2.3. Requerimientos de espacio de disco

El mecanismo de cacheo usado por el Servidor Proxy RHN es el Squid HTTP proxy, el cual economiza significativamente el ancho de banda para los clientes. Debe tener una cantidad razonable de espacio disponible. Los paquetes cacheados se almacenan en `/var/spool/squid`. La asignación de espacio libre requerido es de 6 GB de almacenamiento por distribución/canal.

Si el Servidor Proxy RHN está configurado para distribuir paquetes locales o personalizados, asegúrese que el punto de montaje `/var` en el sistema que almacena los paquetes locales tenga suficiente espacio de disco para guardar todos los paquetes personalizados, los cuales son almacenados en `/var/spool/rhn-proxy`. El espacio de disco requerido para los paquetes locales depende del número de paquetes personalizados servidos.

2.4. Requerimientos adicionales

Los siguientes requerimientos adicionales deben cumplirse antes de considerar la instalación del Servidor Proxy RHN completa:

- Acceso total

  Los sistemas cliente necesitan acceso total de red a los servicios y puertos del Servidor Proxy RHN.

- Reglas de cortafuegos

  El Servidor Proxy RHN puede estar protegido en Internet con un cortafuegos, pero debe ser posible ejecutar conexiones salientes a Internet a través de los puertos 80 y 443. Además, si el Proxy va a estar conectado a un Servidor Satellite RHN que será configurado para implementar acciones inmediatas (mediante la funcionalidad "push") a los sistemas clientes y al Proxy, usted debe permitir conexiones entrantes a través del puerto 5222.

- Tiempos del sistema sincronizados

  Hay una gran susceptibilidad relacionada con el tiempo cuando se realizan conexiones a un servidor Web ejecutando SSL (Secure Sockets Layer); es importante que la configuración de tiempo de los clientes y el servidor sea razonablemente similar para evitar que el certificado SSL expire antes o durante su uso. Se recomienda el uso de NTP (Network Time Protocol) para sincronizar los relojes.

- Nombres de dominios completamente calificados (FQDN)

  El sistema tras el cual el Servidor Proxy RHN será instalado debe resolver apropiadamente sus propios FQDN.

- Una cuenta en Red Hat Network

Los usuarios que se conectarán a los servidores centrales de Red Hat Network para recibir actualizaciones incrementales necesitarán una cuenta en Red Hat Network. Esta cuenta debe establecerse al momento de adquisición con el representante de ventas.

- Copias de seguridad de la información de inicio de sesión

  Es importante que los usuarios guarden registro de toda la información primaria de login. Para el Servidor Proxy RHN, esto incluye los nombres de usuarios y contraseñas para la cuenta del Administrador de la organización y la generación del certificado SSL. Red Hat recomienda encarecidamente que esta información sea copiada en dos disquetes separados, impresa en papel y almacenada en una caja de seguridad.

- Localización de las distribuciones

  Ya que el Proxy reenvía virtualmente todas las peticiones HTTP locales a los servidores centrales de RHN, debe tener cuidado en poner los archivos destinados para cada distribución (tal como en los árboles de instalación kickstart) en la localización no reenviable del Proxy: `/var/www/html/pub/`. Los archivos ubicados en este directorio pueden ser descargados directamente del Proxy. Esto puede ser util para distribuir llaves GPG o establecer árboles de instalación kickstart.

Además, Red Hat recomienda que el sistema ejecutando el código no sea públicamente disponible. Ningún usuario a excepción del administrador del sistema debe tener acceso de shell a estas máquinas. Todos los servicios innecesarios deben ser desactivados. Usted puede usar `ntsysv` o `chkconfig` para desactivar servicios.

Finalmente, debería tener la siguiente documentación técnica a mano para usar, aproximadamente, en el orden dado:

1. *El manual de instalación del Servidor Proxy RHN* — Es la guía que está leyendo en estos momentos. Proporciona los pasos necesarios para tener su Servidor Proxy RHN instalado y en ejecución.
2. *El manual de configuración de sistemas cliente de RHN* — Esta guía explica cómo se debe configurar los sistemas que van a ser servidos por un Servidor Proxy RHN o un Servidor Satellite RHN. (Esto requerirá asimismo consultar *El manual de referencia de RHN*, el cual contiene los pasos para registrar y actualizar los sistemas).
3. *Manual de administración de canales de RHN* — Este manual describe con gran detalle los métodos recomendados para construir paquetes personalizados, crear canales personalizados y manejar erratas privadas.
4. *El manual de referencia de RHN* — Este manual describe la manera de crear cuentas RHN, registrar y actualizar los sistemas y el uso del sitio web de RHN. Este manual es bastante útil durante el proceso de instalación y configuración.

Capítulo 3.

Topologías de ejemplo

El Servidor Proxy RHN puede ser configurado de diferentes maneras. Seleccione un método dependiendo de los siguientes factores:

1. El número total de sistemas cliente a ser servidos por el
2. El número máximo de clientes que se espera se conecten *concurrentemente* al Servidor Proxy RHN.
3. El número de canales y paquetes personalizados a ser servidos por el Servidor Proxy RHN
4. El número de Proxies a ser usados en el entorno del usuario.

El resto de este capítulo describe las posibles configuraciones y explica sus beneficios.

3.1. Topología con un único Proxy

La configuración más sencilla es la utilización de un único Servidor Proxy RHN para servir toda su red. Esta configuración es adecuada para servir un grupo pequeño de clientes y una red que se beneficiará del cacheo de RPMs de Red Hat y del almacenamiento de paquetes personalizados en el servidor local.

La desventaja de usar un único Servidor Proxy RHN es que el rendimiento se verá afectado cuando el número de clientes solicitando paquetes crezca.

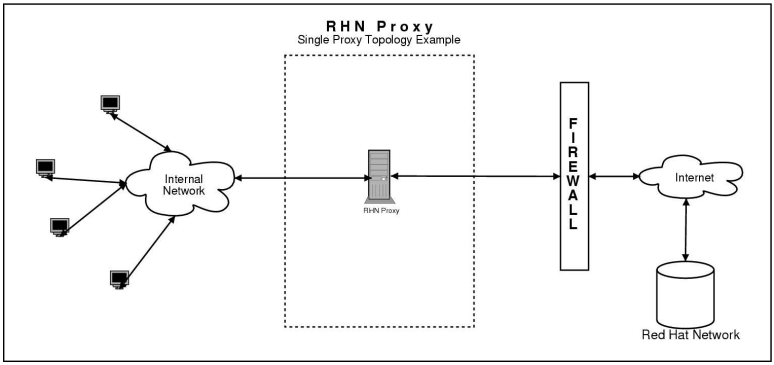


Figura 3-1. Topología con un único Proxy

3.2. Topología de múltiples Proxies enlazados horizontalmente

Para redes grandes, se necesitará un método más distribuido, tal como el ofrecido por múltiples Proxies conectados individualmente a Red Hat Network. Esta configuración de ordenamiento horizontal balancea la carga de las solicitudes de los clientes y permite a cada Proxy sincronizarse simultáneamente con RHN.

Una desventaja de esta estructura horizontal es que los paquetes personalizados cargados a un Proxy individual deben ser distribuidos a todos los demás Proxies. Esta situación puede solucionarse de dos formas:

- o bien, el programa de transferencia de archivo **rsync** puede ser usado para sincronizar paquetes entre los Proxies,
- o bien, una compartición NFS (Network File System) puede ser establecida entre los Proxies y el repositorio de canal personalizado.

Cualquiera de estas dos soluciones le permitirá a cualquier cliente de cualquier Servidor Proxy RHN tener todos los paquetes personalizados entregados a éstos.

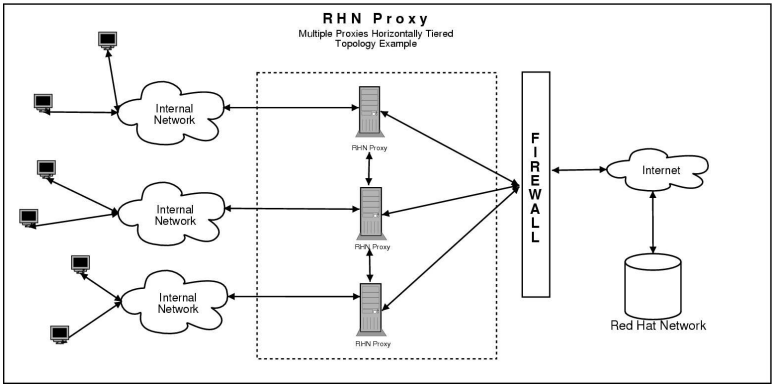


Figura 3-2. Topología de múltiples Proxies enlazados horizontalmente

3.3. Topología de múltiples Proxies ordenados verticalmente

Un método alternativo para múltiples Proxies es ordenar un Servidor Proxy RHN primario al cual se conectarán los otros para obtener RPMs desde Red Hat Network y paquetes personalizados creados localmente. En esencia, Los Proxies secundarios actuarán como clientes de los Proxies primarios. Esto solucionará la necesidad de establecer un mecanismo de sincronización entre los Proxies ya que éstos usan la función `up2date` inherente al producto.

Como la configuración de ordenamiento horizontal, este método vertical permite a cualquier cliente de cualquier Servidor Proxy RHN tener todos los paquetes personalizados entregados a éstos. El Proxy revisará en su repositario para ver si el paquete está en su sistema de archivos. Si no está, intentará solicitarlo al nivel superior

Esta configuración de ordenamiento vertical asegura que el Proxy secundario dependa del Proxy primario para las actualizaciones desde RHN y paquetes personalizados. Los canales y paquetes personalizados deben estar en el Proxy primario solamente, para asegurar la distribución de los Proxies hijos. Finalmente, los archivos de configuración de los Proxies secundarios deben apuntar al primario y no a Red Hat Network directamente.

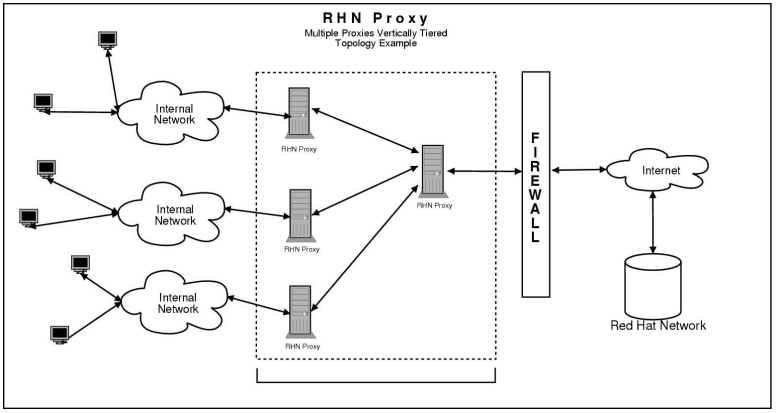


Figura 3-3. Topología de múltiples Proxies ordenados verticalmente

3.4. Proxies con un Servidor Satellite RHN

Además de los métodos descritos en este capítulo, los usuario tienen la opción de usar el Servidor Proxy RHN junto con el Servidor Satellite RHN. Esta estructura funciona de un modo similar a la configuración de proxies ordenados verticalmente pero la capacidad se ve incrementada significativamente, ya que el Satellite puede servir un número mayor de sistemas cliente.

Para una descripción más detallada de esta combinación, consulte el capítulo de topologías de ejemplo del *Manual de instalación del Servidor Satellite RHN*. La forma de enlazar los certificados SSL de ambos productos se describe en el *Manual de configuración de sistemas cliente de RHN*. Para entender como los paquetes y canales son compartidos entre éstos, consulte el *Manual de administración de canales de RHN*.

Capítulo 4.

Instalación

Este capítulo describe la instalación inicial del Servidor Proxy RHN. Presupone que los requisitos listados en el Capítulo 2 han sido cumplidos. Sin embargo, si usted está *actualizando* su versión del Servidor Proxy RHN, contacte su representante Red Hat para obtener asistencia.

4.1. Instalación base

El Servidor Proxy RHN está diseñado para ser ejecutado en el sistema operativo Red Hat Enterprise Linux AS. Así, el primer paso es instalar el sistema operativo, ya sea desde un disco, una imagen ISO o mediante la función kickstart. Durante y después de la instalación del sistema operativo, asegúrese de:

- Alocar suficiente espacio a la partición que va a ser usada para almacenar paquetes, de acuerdo a los requisitos de hardware establecidos anteriormente. La ubicación por defecto para guardar paquetes Red Hat es `/var/spool/squid`, mientras que los paquetes personalizados están ubicados en `/var/spool/rhn-proxy`.
- Instalar únicamente los paquetes requeridos por el Servidor Proxy RHN. *Usted debe instalar tan solo los paquetes base ya que la instalación de otros paquetes causará el fallo de la instalación del Servidor Proxy RHN*. Consulte en la Sección 2.1 el método para obtener el grupo de paquetes correcto necesario para cada versión de Red Hat Enterprise Linux AS.



Importante

Si planea implementar el nivel de servicios Monitoring, usted *debe* instalar su Servidor Proxy RHN en Red Hat Enterprise Linux AS 3 Update 5 o Red Hat Enterprise Linux AS 4. Estos son los únicos sistemas operativos base soportados por Proxies que sirven sistemas con derechos Monitoring.

- Active NTP (Network Time Protocol) en el Proxy y seleccione el huso horario apropiado. El demonio `ntpd` debería ya estar en ejecución en todos los sistemas clientes y el huso horario en éstos debería ya estar establecido.
- Desactive los servicios `ipchains` y `iptables` después de la instalación.

4.2. Proceso de instalación del Servidor Proxy RHN

Las siguientes instrucciones describen el proceso de instalación del Servidor Proxy RHN:

1. Registre el sistema Red Hat Enterprise Linux AS recién instalado en Red Hat Network (ya sea en los servidores centrales de RHN o en su Servidor Satellite RHN) usando la cuenta corporativa que contiene los derechos del Servidor Proxy RHN. Utilice el comando `up2date --register`.
2. Concédale al sistema los derechos Provisioning, visitando el sitio web de RHN (o el nombre de dominio completamente calificado del Satellite que sirve el Proxy), inicie una sesión como Administrador de la organización, vaya a la página **Sistemas ⇒ Derechos del sistema**, seleccionando la caja de sistemas en la cual el Servidor Proxy RHN va a ser instalado y haga clic en el botón **Añadir Provisioning**.
3. Asegúrese que el sistema esté suscrito al canal de Herramientas de Red Hat Network para su sistema operativo base, haciendo click en el nombre del sistema y dirigiéndose a la subpestaña **Sistemas ⇒ Información del sistema ⇒ Canales ⇒ Software**. Si el canal de herramientas de Red Hat Network *no* está seleccionado, por favor selecciónelo y suscriba el sistema a este canal haciendo click en el botón **Cambiar suscripción**.
4. Instalar todos los paquetes `rhncfg`. Vaya a la subpestaña **Sistema ⇒ Información del sistema ⇒ Paquetes ⇒ Instalar** y busque `rhncfg` utilizando la caja de entrada de texto del **Filtrar según nombre de paquetes**. En la lista resultante, seleccione todos los paquetes e instálelos.
5. Si va a activar la encriptación SSL (secure sockets layer) en el Proxy y conectarlo a los servidores centrales de RHN, instale el paquete `rhns-certs-tools` desde el mismo canal de herramientas de Red Hat Network y utilice **Herramienta de mantenimiento RHN SSL** para generar el archivo tar requerido posteriormente. Consulte el capítulo sobre los certificados SSL en el *Manual de configuración de sistemas cliente de RHN* para obtener instrucciones.

   Si va a activar la encriptación SSL en el Proxy y conectarlo a un *Servidor Satellite RHN* u otro *Servidor Proxy RHN* con SSL, necesitará también la contraseña de certificado CA usado por el sistema del nivel superior.
6. Entre al sistema como root a través de una terminal y ejecute el comando `rhn_check` para iniciar inmediatamente la instalación programada de paquetes.
7. Una vez que los paquetes hayan sido instalados, como se confirma en la pestaña **Información del sistema ⇒ Eventos**, prepare el sistema para aceptar comandos remotos y la administración de configuración con el siguiente comando:
   ```
   /usr/bin/rhn-actions-control --enable-all
   ```
8. Dentro del sitio web de RHN, vaya a la subpestaña **Información del sistema ⇒ Proxy**.

Advertencia

Por favor note que la instalación del Servidor Proxy RHN podría reemplazar los archivos de configuración `squid.conf` y `httpd.conf` en el sistema para facilitar las actualizaciones posteriores. Si ha editado estos archivos y desea preservarlos, estos son alternados de lugar y pueden ser recuperados después de la instalación.

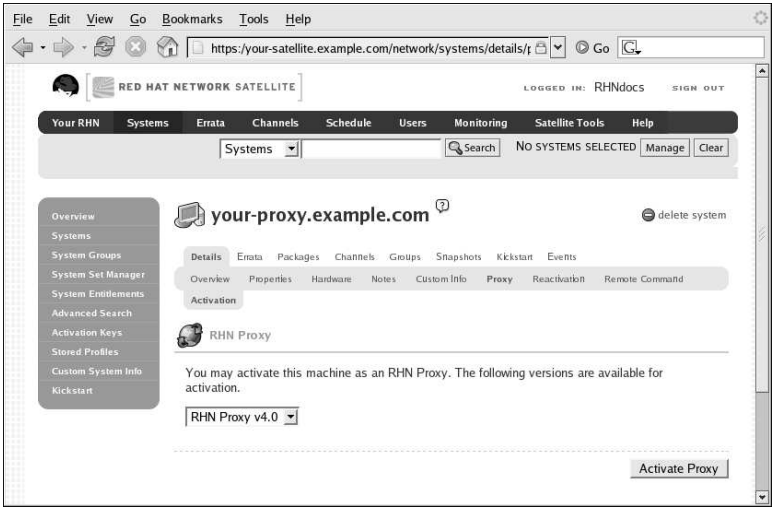


Figura 4-1. Información del sistema ⇒ Proxy

9. En la subpestaña **Información del sistema ⇒ Proxy**, el menú desplegable debe indicar la capacidad de activar un sistema como Servidor Proxy RHN. Asegúrese que la versión sea seleccionada apropiadamente y haga clic en el botón **Activar Proxy**. La página de **Bienvenida** de la instalación aparecerá.



Figura 4-2. Bienvenida

10. En la página de **Bienvenida** encontrará una notificación de cualquier requerimiento que no haya sido cumplido por el sistema. Cuando el sistema está listo, el enlace **continuar** aparecerá. Haga clic en él para ir a la página **Términos y condiciones**

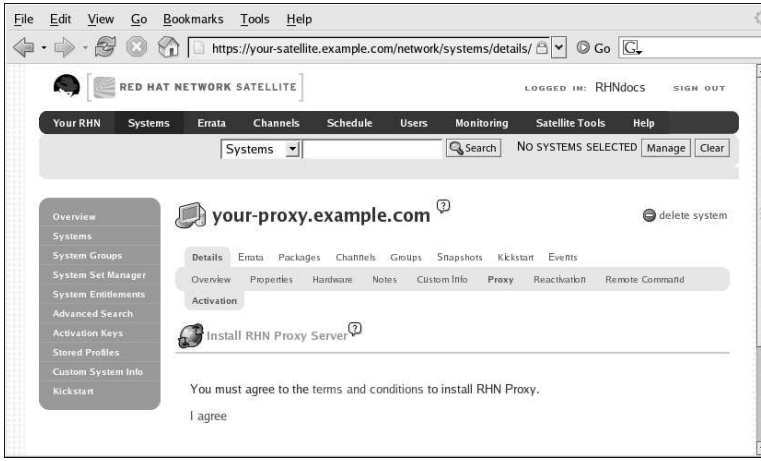


Figura 4-3. Términos y condiciones

11. En la página **Términos y condiciones**, haga clic en el enlace **Términos y condiciones** para ver el acuerdo de licencia del Servidor Proxy RHN. Una vez satisfecho, haga clic en **Aceptar**. La siguiente página, **Activar Monitoring**, aparecerá.

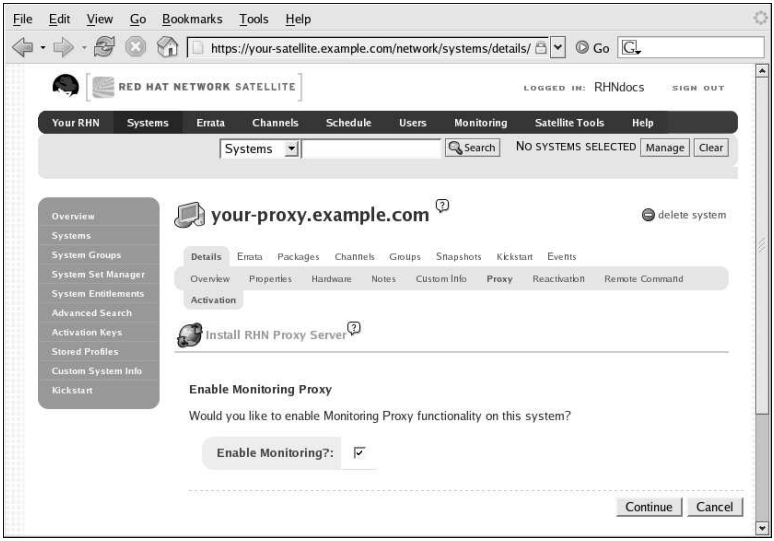


Figura 4-4. Activar Monitoring

12. En la página **Activar Monitoring**, usted debe decidir si el Proxy será usado para monitorizar sistemas servidos por él. Para activar esta función, el Servidor Proxy RHN debe cumplir los requerimientos descritos en el Capítulo 2 y estar activado a un Servidor Satellite RHN (o a otro Proxy conectado a un Satellite). Para activar el servicio de monitoreo en el Proxy, seleccione la casilla de verificación y haga clic en **continuar**. La página **Configurar Servidor Proxy RHN** aparecerá.

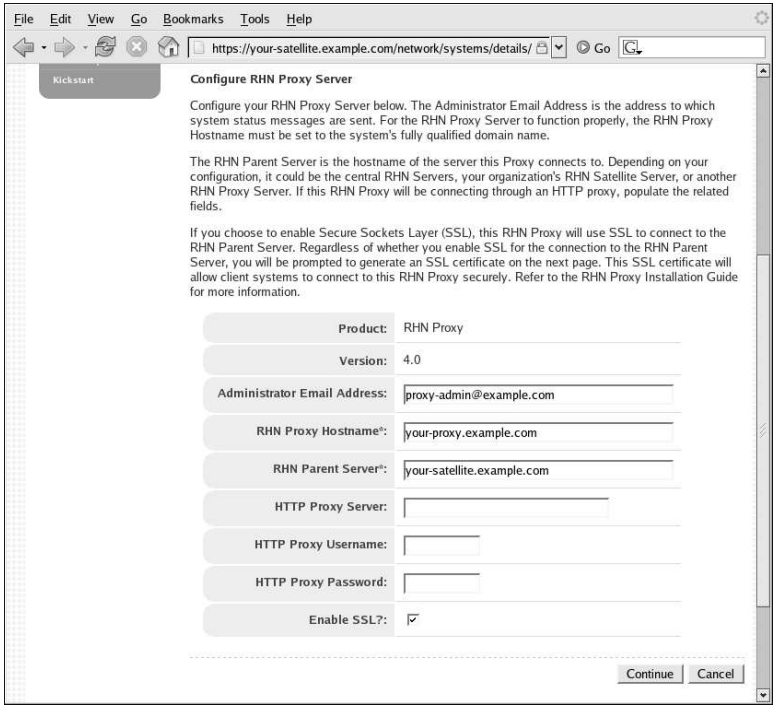


Figura 4-5. Configurar del Servidor Proxy RHN

13. En la página **Configurar Servidor Proxy RHN**, proporcione o confirme las entradas para todos los campos requeridos. La dirección electronica del administrador recibirá todos los correos generados por el Proxy, incluyendo algunas veces cantidades considerables de seguimientos de errores. Para seleccionar estos mensajes, considere el uso de un filtro de correo que capture los mensajes con el asunto "RHN TRACEBACK from `hostname`". Para listar más de un administrador, introduzca una lista de correos-e separados por comas

    El nombre de Host del RHN Proxy es el nombre de dominio completamente calificado (FQDN) del Servidor Proxy RHN. El "RHN Parent Server" es el nombre de dominio del servidor que sirve al Proxy, ya sea un servidor central de RHN, otro Servidor Proxy RHN o un Servidor Satellite RHN. Para conectarse a los servidores

centrales de RHN, incluya el valor **`xmlrpc.rhn.redhat.com`**. Para conectarse al Satellite o a otro Proxy, introduzca el FQDN del sistema de nivel superior.

Si el Servidor Proxy RHN va a ser conectado a través de un HTTP proxy, configúrelo usando los campos asociados. Note que las referencias a protocolos, como **`http://`** o **`https://`**, no deben ser incluidas en el campo **HTTP Proxy Server**. Introduzca solamente el nombre de host y el puerto de la forma hostname:port, por ejemplo: mi.corporacion.gateway.ejemplo.com:3128.



Consejo

El proceso de instalación afecta únicamente el archivo de configuración del Proxy: `/etc/rhn/rhn.conf`. El archivo de configuración del **Agente de actualización de Red Hat** (`up2date`), `/etc/sysconfig/rhn/up2date`, debe ser actualizado manualmente para recibir sus actualizaciones desde otro servidor, por ejemplo desde un Servidor Satellite RHN.

Finalmente, usted debe decidir si activar o no SSL utilizando para ello la casilla de verificación en la parte inferior. Red Hat recomienda encarecidamente que emplee este nivel de encriptación para cualquier tráfico desde o para el Servidor Proxy RHN. Para seleccionarlo, sin embargo, usted debe conectarse a los servidores centrales de RHN (los cuales tiene activado SSL por defecto) o a un Servidor Satellite RHN o a un Servidor Proxy RHN que tenga activado SSL. Las conexiones a los servidores centrales de RHN requieren la carga del archivo tar del certificado mencionado anteriormente. Las conexiones a un Satellite u otro Proxy a través de SSL requieren la contraseña del certificado CA usado en la activación de SSL en el sistema del nivel superior.

Si no desea activar SSL durante la instalación, deje sin seleccionar esta casilla y consulte el capítulo sobre certificados SSL en el *Manual de configuración de sistemas cliente de RHN* para conocer cómo se puede obtener este nivel de seguridad después de la instalación. Al finalizar, haga clic en **continuar**. Si esta activando SSL y está conectándose a un Satellite u otro Proxy, la página **Configurando SSL** aparecerá. Si usted activa SSL y está conectándose a los servidores centrales de RHN, la página **Cargando SSL** aparecerá. Si usted no activó SSL pero activó Monitoring, vaya a la descripción de la página **Configurando Monitoring**. Si usted no activo SSL o Monitoring, vaya a la descripción de la página **Progreso de la instalación**.

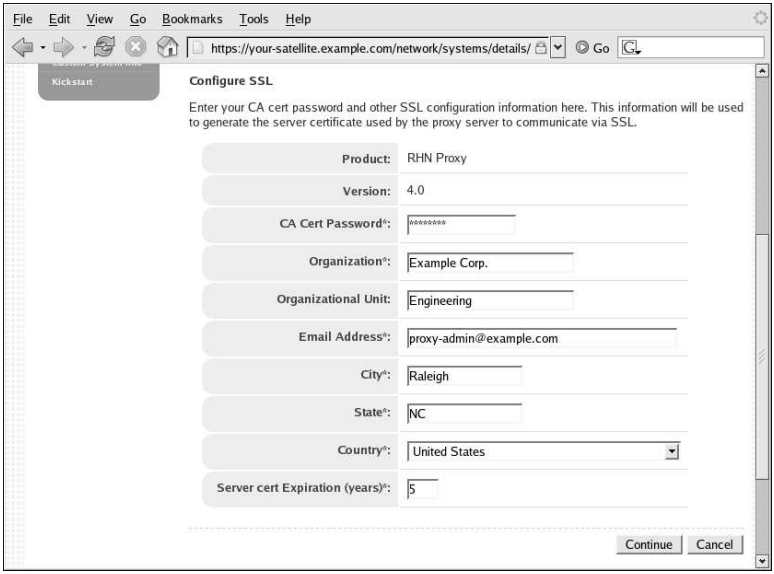


Figura 4-6. Configuración de SSL

14. En la página **Configurando SSL**, *aplicable únicamente a un Proxy que se está conectando con un Servidor Satellite RHN u otro Servidor Proxy RHN con SSL activado*, proporcione la información necesaria para generar el certificado del servidor. El elemento más importante es la contraseña de certificado CA, la cual debe coincidir con la contraseña usada al activar SSL en el servidor del nivel superior. Los campos restantes pueden coincidir con los valores del servidor del nivel superior pero pueden ser distintos dependiendo del rol del Servidor Proxy RHN, por ejemplo para reflejar una ubicación geográfica diferente. Igualmente, la dirección de correo puede ser la misma que se especificó para el administrador del Proxy pero puede ser dirigida a un administrador certificado particular. La fecha de vencimiento del certificado puede ser configurada. Como siempre, asegúrese de que los valores proporcionados aquí estén en la copia de seguridad descrita en el Capítulo 2. Una vez finalizado, haga clic en **continuar**.

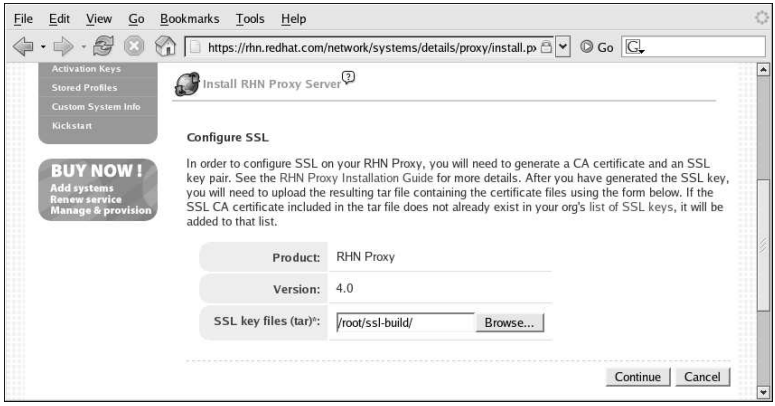


Figura 4-7. Cargar SSL

En la página **Cargando SSL**, *aplicable únicamente a un Proxy que se está conectando a los servidores centrales de RHN*, ubique el archivo tar creado con **Herramienta de mantenimiento RHN SSL**, usando el botón **Browse**. Será llamado `rhn-org-httpd-ssl-archive-`*`MACHINENAME-VERSION`*`.tar` con el nombre de la máquina haciendo referencia al nombre de host del Proxy. Una vez ubicado, haga clic en **continuar**.



Nota

Ya que usted debe ser root para generar una llave SSL, el archivo tar resultante será ubicado en `/root/ssl-build/`*`HOSTNAME/`*. Este archivo *no* será visible a un usuario sin privilegios, por lo cual usted debe ubicar el archivo a un lugar visible por el usuario que está ejecutando el navegador.

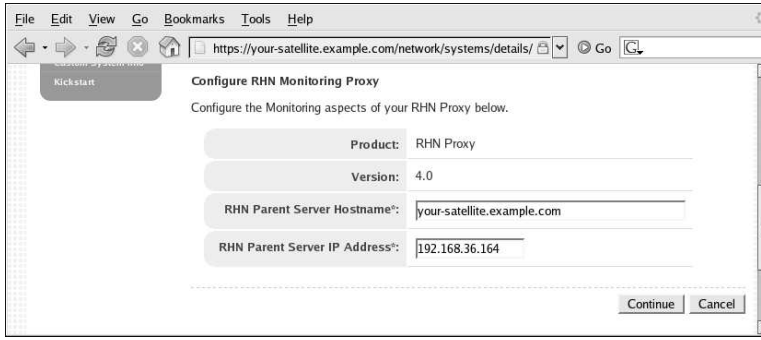


Figura 4-8. Configuración del Monitoring

15. En la página **Configurando Monitoring**, proporcione o confirme el nombre de host y dirección IP del servidor del nivel superior al cual se está conectando el Servidor Proxy RHN. Este debe ser un Servidor Satellite RHN u otro Proxy que está a su vez conectándose con un Satellite. *Usted no puede ejecutar el Monitoring a través de los servidores centrales de RHN*. Al finalizar, haga clic en **continuar**. La página **Progreso de la instalación** aparecerá.

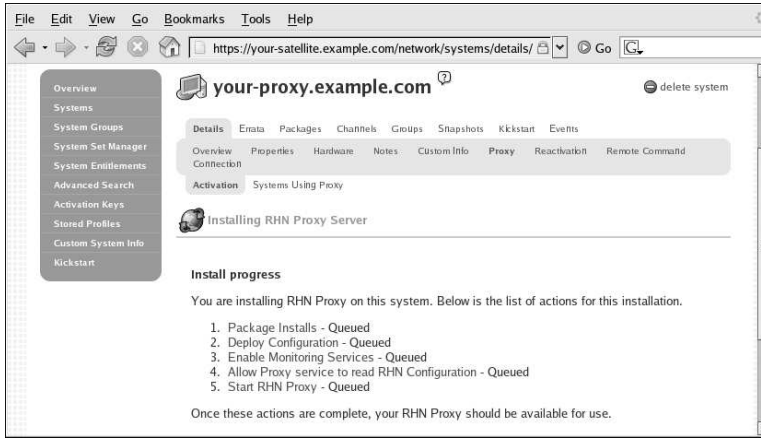


Figura 4-9. Progreso de la instalación

16. En la página **Progreso de la instalación**, usted puede monitorizar los pasos de la instalación mientras estos están siendo ejecutados. Haga clic en cualquiera de los pasos para ir a la página **Información de la acción**. Cuando un paso está siendo llevado a cabo, su estado pasa de `Queued` (en espera) a `Picked Up` (en ejecución) y finalmente a `Completed` (finalizado). Como la instalación de paquetes anterior, usted puede ejecutar estos pasos de inmediato con el comando `rhn_check` en una terminal del sistema como usuario root. Al finalizar, la página **Progreso de la instalación** mostrará el mensaje `La instalación ha sido completada`. Usted puede ahora iniciar el registro de sistemas a ser servidos por el Servidor Proxy RHN. Consulte el *Manual de configuración de sistemas clientes de RHN*.

Capítulo 5.

Gestor de paquetes de RHN

El Gestor de paquetes de RHN es una herramienta para la línea de comandos que le permite a una organización servir paquetes locales asociados con un canal RHN privado a través del Servidor Proxy RHN. Si desea que el Servidor Proxy RHN actualice únicamente paquetes oficiales de Red Hat, usted no necesita instalar el Gestor de paquetes de RHN.

Para usar el Gestor de paquetes de RHN, instale el paquete `rhns-proxy-package-manager` y sus dependencias.

Solamente la información de los encabezados para los paquetes es cargada a los servidores de RHN. Los encabezados son requeridos para que RHN pueda resolver las dependencias de los paquetes para los sistemas cliente. Los archivos de paquetes completos (`*.rpm`) son almacenados en el Servidor Proxy RHN.

El Gestor de paquetes de RHN utiliza la misma configuración que el Proxy, tal y como se define en el archivo de configuración `/etc/rhn/rhn.conf`.

5.1. Creando un canal privado

Antes de que los paquetes locales sean proporcionados por el Servidor Proxy RHN, se necesita un canal privado para almacenarlos. Ejecute los siguientes pasos para crear una canal privado:

1. Inicie una sesión en la interfaz web de RHN en https://rhn.redhat.com.
2. Haga clic en **Canales** en la barra de navegación superior. Si la opción **Administrar canales** no está presente en la barra de navegación izquierda, asegúrese de que el usuario tiene el conjunto de permisos de edición de canal. Realice esto a través de la categoría **Usuarios** accesible a través de la barra de navegación superior.
3. En la barra de navegación izquierda, haga clic en **Administrar canales de Software** y luego en el botón **crear nuevo canal** en la esquina superior izquierda de la página.
4. Seleccione un canal padre y una arquitectura de canal base, luego introduzca un nombre, una etiqueta, un resumen y una descripción para el nuevo canal privado. La etiqueta del canal debe: tener al menos seis caracteres, iniciar con una letra y tener sólo letras minúsculas, dígitos, guiones (-) y puntos (.). Introduzca también la URL de la llave GPG del canal. Aunque este campo no es requerido, se recomienda para reforzar la seguridad. Para obtener instrucciones en como generar las llaves GPG, consulte el Manual de administración de canales de RHN.
5. Haga clic en **Crear canal**

5.2. Actualizando los paquetes



Nota

Usted debe ser un Administrador de la organización para cargar paquetes a canales privados de RHN. El script le preguntará su nombre de usuario y contraseña.

Después de crear el canal privado, cargue los encabezados del paquete de sus RPMs binarios y códigos fuente a los servidores centrales de RHN y copie los paquetes al Broker del servidor Proxy RHN. Para cargar los encabezados del paquete de los RPM binarios a través de la línea de comandos:

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

pkg-list es la lista de paquetes a ser cargados. Alternativamente, utilice la opción `-d` para especificar el directorio local que contiene los paquetes a añadir al canal. Asegúrese de que el directorio contiene únicamente los paquetes a ser añadidos. El Gestor de paquetes de RHN también puede leer la lista de paquetes desde la entrada estándar (utilizando `--stdin`).

Para cargar los encabezados de los paquetes de los RPMs de código fuente:

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

Si tiene más de un canal especificado (usando la opción `-c` o `--channel`), los encabezados de paquetes cargados serán enlazados a todos los canales listados.



Nota

Si no se especifica un nombre de canal, el paquete no se añade a ningún canal. El paquete puede ser luego añadido a algún canal usando la interfaz de web de Red Hat Network. La interfaz puede también ser usada para modificar canales privados existentes.

Después de cargar los paquetes, puede revisar inmediatamente la interfaz web de RHN para verificar su presencia. Haga clic en **Canales** en la barra de navegación superior, luego en **Administrar canales de Software** en la barra de navegación izquierda y posteriormente en el nombre del canal personalizado. Luego haga clic en la subpestaña **Paquetes**. Cada RPM debe ser listado.

Usted puede también revisar si el directorio local está sincronizado con la imagen del canal en el servidor de RHN a través de la línea de comandos:

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

La opción `-s` listará todos los paquetes faltantes (los paquetes cargados en el servidor de RHN que no están presentes en el directorio local). Usted debe ser un Administrador de la organización para utilizar este comando. El script le preguntará su nombre de usuario y contraseña. Consulte la Tabla 5-1 para obtener opciones adicionales para la línea de comandos.

Si está utilizando el Gestor de paquetes de RHN para actualizar los paquetes locales, usted debe ir al sitio web de RHN para suscribir el sistema al canal privado.

5.3. Opciones para la línea de comandos

Un resumen de todas las opciones para la línea de comandos para el Gestor de paquetes de RHN `rhn_package_manager`:

Opción	Descripción
`-v`, `--verbose`	Aumentar verbosidad.
`-d`*`DIR`*, `--dir=`*`DIR`*	Procesar paquetes desde el directorio *`DIR`*.
`-c`*`CHANNEL`*, `--channel=`*`CHANNEL`*	Administrar este canal — puede estar presente varias veces.
`-n`*`NUMBER`*, `--count=`*`NUMBER`*	Procese este número de encabezados por llamada — por defecto son 32
`-l`, `--list`	Crear una lista con el nombre del paquete, el número de versión, el número de lanzamiento y la arquitectura, del canal(es) especificado.
`-s`, `--sync`	Revisar si el directorio local está sincronizado con el servidor.
`-p`, `--printconf`	Imprimir la configuración actual y salir.
`-X`*`PATTERN`*, `--exclude=`*`PATTERN`*	Excluir los archivos que coincidan con esta expresión global — puede estar presente varias veces.
`--newest`	Enviar únicamente los paquetes que son más nuevos que los paquetes ya enviados al servidor para el canal especificado.
`--stdin`	Leer el nombre del paquete desde stdin.

Opción	Descripción
`--nosig`	Enviar canales sin firma. Por defecto, el Gestor de paquetes de RHN intenta enviar únicamente los paquetes firmados.
`--username=`*`USERNAME`*	Especificar nombre de usuario de RHN. Si usted no proporciona uno con esta opción, se le preguntará por él.
`--password=`*`PASSWORD`*	Especificar contraseña de RHN. Si no proporciona una con esta opción, se le preguntará luego.
`--source`	Cargar fuente de encabezadosdel paquete.
`--dontcopy`	En el paso posterior a la carga, no copie los paquetes a su ubicación final en el árbol de paquetes.
`--test`	Únicamente imprime los paquetes a ser enviados.
`--no-ssl`	*No recomendada* — Desactivar SSL.
`-?`, `--usage`	Describir brevemente las opciones.
`--copyonly`	Copiar los archivos listados en el argumento en el canal especificado. Es útil cuando a un canal en el Proxy le falta un paquete y usted no desea importar de nuevo todos los paquetes en el canal. P.ej. `rhn_package_manager -c`*`CHANNEL`* `--copyonly` */PATH/TO/MISSING/FILE*
`-h`, `--help`	Mostrar la pantalla de ayuda con una lista de las opciones.

Tabla 5-1. Opciones de `rhn_package_manager`



Consejo

Estas opciones para la línea de comando se describen también en la página de manual de `rhn_package_manager`: `man rhn_package_manager`.

Capítulo 6.

Localización de errores

Este capítulo proporciona consejos para determinar las causas y resolver los errores más comunes asociados con el Servidor Proxy RHN. Si necesita ayuda adicional, contacte el equipo de asistencia de Red Hat Network en https://rhn.redhat.com/help/contact.pxt. Inicie la sesión con su cuenta de derechos Satellite para ver la lista completa de opciones.

6.1. Administrando el servicio Proxy

Ya que el Servidor Proxy RHN está constituido por varios componentes individuales, Red Hat proporciona un servicio maestro, `rhn-proxy`, que le permitirá detener, iniciar u obtener el estado de los diferentes servicios en el orden apropiado. Este servicio de ayuda acepta todos los comandos típicos:

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

Utilice `rhn-proxy` para apagar o iniciar todo el Servidor Satellite RHN y para obtener inmediatamente los mensajes de estado de todos sus servicios.

6.2. Archivos de registro

Virtualmente, todo proceso de localización y solución de errores debe comenzar con la revisión de los archivos de registro asociados. Estos archivos proporcionan información fundamental sobre la actividad que se ha llevado a cabo en el dispositivo o la aplicación y puede ser usado para monitorizar el rendimiento y para asegurar una apropiada configuración. Vea la Tabla 6-1 para obtener las rutas de todos los archivos de registro relevantes:

Componentes	**Ubicación de los archivos de registro**
Servidor Apache HTTP	Directorio `/var/log/httpd/`
Squid	Directorio `/var/log/squid/`
Broker del servidor Proxy RHN	`/var/log/rhn/rhn_proxy_broker.log`

Componentes	Ubicación de los archivos de registro
Servidor de redirección SSL de RHN	`/var/log/rhn/rhn_proxy_redirect.log`
Agente de actualización de Red Hat	`/var/log/up2date`

Tabla 6-1. Archivos de registro

6.3. Preguntas y respuestas

Esta sección contiene las respuestas a las preguntas más frecuentes relacionadas con la instalación y configuración de la solución Servidor Proxy RHN.

1. Después de la configuración del Gestor de paquetes de RHN, ¿cómo puedo determinar si el paquete local ha sido añadido exitosamente al canal privado de RHN?

Utilice el comando `rhn_package_manager -l -c "name_of_private_channel"` para listar los paquetes del canal privado conocidos por los servidores de RHN. También puede utilizar la interfaz del sitio web de RHN.

Después de suscribir un sistema registrado al canal privado, usted también puede ejecutar el comando `up2date -l --showall` en el sistema registrado y buscar los paquetes del canal privado de RHN.

2. ¿Cómo puede determinar si los clientes están conectados al servidor Squid?

Los archivos `/var/log/squid/access.log` registran todas las conexiones al servidor Squid.

3. El **Agente de actualización de Red Hat** en el sistema cliente no se conecta con el Servidor Proxy RHN. ¿Cómo puedo solucionar este error?

Asegúrese de que la última versión del **Agente de actualización de Red Hat** está instalada en el sistema cliente. La última versión tiene funciones necesarias para conectarse a través del Servidor Proxy RHN. Ésta versión puede obtenerse con Red Hat Network o desde http://www.redhat.com/support/errata/. Tenga en cuenta que el Servidor Proxy RHN actúa como un mecanismo de cacheo de RHN, la configuración de `httpProxy` en `/etc/sysconfig/rhn/up2date` en los sistemas cliente es redundante y probablemente innecesaria.

El Servidor Proxy RHN es una extensión de Apache. Vea la Tabla 6-1 para obtener la localización de los archivos de registro.

4. Mi configuración del Servidor Proxy RHN no está funcionando. ¿Dónde puedo iniciar el proceso de solución de errores?

Asegúrese de que `/etc/sysconfig/rhn/systemid` es propiedad del usuario root.apache y que tenga los permisos 0640.

Lea los archivos de registro. Una lista de éstos esta disponible en la Tabla 6-1.

6.4. Problemas generales

Para iniciar la solución de errores generales, examine los archivos de registro relacionados con el componente que está mostrando la falla. Un ejercicio útil es utilizar "tail" en todos los archivos de registro y luego ejecutar el comando `up2date --list`. Puede examinar luego las nuevas entradas en los archivos de registro para obtener posibles claves.

Un fallo común es el espacio de disco lleno. Un signo casi irrefutable de éste fallo es la detención de la escritura en los archivos de registro. Si la escritura de un registro se detiene antes de finalizar, en la mitad de una palabra por ejemplo, es probable que el disco esté lleno. Para confirmarlo, ejecute este comando y revise el porcentaje en la columna Uso%.

```
df -h
```

Además de los archivos de registro, usted puede obtener valiosa información solicitando el estado de los diferentes componentes. Esto puede realizarse para el Servidor Apache HTTP y Squid.

Para obtener el estado del Servidor Apache HTTP ejecute el comando:

```
service httpd status
```

Para obtener el estado de Squid, ejecute el comando:

```
service squid status
```

Si el administrador no está obteniendo ningún correo del Servidor Proxy RHN, confirme que la dirección de correo-e apropiada ha sido establecida para la opción `traceback_mail` en `/etc/rhn/rhn.conf`.

6.5. Host Not Found/Could Not Determine FQDN

Ya que los archivos de configuración de RHN dependen exclusivamente de los nombres de dominios completamente calificados (FQDN), es importante que las aplicaciones claves sean capaces de resolver el nombre del Servidor Proxy RHN en una dirección IP. El **Agente**

de actualización de Red Hat, el **Cliente de registro de Red Hat Network**, y el Servidor Apache HTTP son particularmente propensos a este problema con las aplicaciones de RHN, las cuales muestran los errores "host not found" y el estado del servidor web como "Could not determine the server's fully qualified domain name" (No se pudo determinar el nombre de dominio completamente cualificado del servidor), tras una falla de inicio.

Este problema se origina generalmente en el archivo `/etc/hosts`. Puede confirmarlo examinando `/etc/nsswitch.conf`, el cual define los métodos y el orden bajo los cuales los nombres de dominios son resueltos. Generalmente, el archivo `/etc/hosts` es el primero en ser revisado, seguido por el NIS (Servicio de información de red) si se está usando, seguido por DNS. Uno de estos debe ser exitoso para que el Servidor Apache HTTP pueda ser iniciado y para que las aplicaciones cliente de RHN funcionen.

Para resolver este problema, identifique el contenido de el archivo `/etc/hosts`. Debe ser similar a:

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

Primero, en un editor de texto, remueva la información de la máquina ofendida, como por ejemplo:

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

Luego guarde el archivo y intente ejecutar nuevamente las aplicaciones cliente de RHN o el Servidor Apache HTTP. Si éstos aun fallan, identifique explícitamente la dirección IP del Proxy en el archivo, por ejemplo:

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

Remplace aquí el valor con la dirección IP real del Proxy. Esto debería resolver el problema. Recuerde, si la dirección IP específica es estipulada, el archivo debe ser actualizado cuando la máquina obtiene una nueva dirección.

6.6. Errores de conexión

Si usted cree estar experimentando problemas relacionados con fallas de conexión, siga los pasos siguientes:

- Confirme que el paquete correcto:
  `rhn-org-httpd-ssl-key-pair-`*`MACHINE_NAME-VER-REL`*`.noarch.rpm`

  está instalado en el Servidor Proxy RHN y el `rhn-org-trusted-ssl-cert-*.noarch.rpm` correspondiente o certificado crudo CA SSL público (cliente) está instalado en todos los sistemas cliente.

- Verifique que los sistemas cliente están configurados para utilizar el certificado apropiado.
- Si está utilizando un Servidor Proxy RHN o más, asegúrese de que cada certificado SSL del Proxy está preparado correctamente. Si está utilizando el Servidor Proxy RHN junto con un Servidor Satellite RHN, el Proxy debe tener tanto su propio par de llaves SSL como el certificado CA SSL público (cliente) instalados, ya que tendrá ambas funciones. Consulte el capítulo sobre certificados SSL en el *Manual de configuración de sistemas cliente de RHN* para obtener instrucciones específicas.
- Si el Servidor Proxy RHN se está conectando a través de un Proxy HTTP, asegúrese de que la URL listada sea válida. Por ejemplo, el campo URL del Proxy HTTP no debe contener referencias al protocolo, http:// o https://. Sólo el nombre de host y el puerto deben ser incluidos en la forma hostname:port, tal como corporate_gateway. example.com:8080.
- Asegúrese que los sistemas cliente no están usando cortafuegos sobre sus propios puertos requeridos, tal y como se identifican en la Sección 2.4.

6.7. Problemas relacionados con el caché

Si una entrega de paquetes falla o un objeto parece incompleto, y el problema no está relacionado con errores de conexión, debería considerar la limpieza del caché. El Servidor Proxy RHN tiene dos caches importantes en estos casos: uno para Squid y el otro para autenticación.

El caché de Squid está ubicado en `/var/spool/squid/`. Para limpiarlo, detenga el Servidor Apache HTTP y Squid, borre el contenido de ese directorio y reinicie ambos servicios. Ejecute los siguientes comandos en el orden dado:

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

Usted podría ejecutar la misma tarea de una forma más rápida si sólo borra el contenido del directorio y reinicia squid, pero es posible que reciba un sin número de mensajes de seguimiento de RHN.

El mecanismo de cacheo interno usado para autenticación por el Proxy podría necesitar asimismo limpieza. Para hacerlo, ejecute el siguiente comando:

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

Aunque el Demonio de autenticación de RHN fue deprecado con el lanzamiento del Servidor Proxy RHN 3.2.2 y reemplazado con el mecanismo de cacheo de autenticación interna,

el demonio podría estar aun en ejecución en su Proxy. Para apagarlo, ejecute los siguientes comandos en el orden dado:

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

Para limpiar el caché, ejecute:

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

Si desea conservar el Demonio de autenticación de RHN, lo cual no es recomendado ni soportado por Red Hat, note que su rendimiento puede sufrir de registros verbosos. Por esta razón, el registro (a `/var/log/rhn/rhn_auth_cache.log`) está, por defecto, apagado. Si el demonio está en ejecución y usted desea que los registros sean grabados, añada la siguiente línea al archivo `/etc/rhn/rhn.conf` del Proxy:

```
auth_cache.debug = 2
```

6.8. Depuración del Proxy por Red Hat

Si ya ha agotado todos estos pasos para localizar y corregir errores o si desea ayuda de los profesionales de Red Hat Network, Red Hat le recomienda sacar provecho de la excelente asistencia que viene con el Servidor Proxy RHN. La forma más eficiente de realizarlo es agrupando los parámetros de configuración del Proxy, los archivos de registro y la información de la base de datos y enviando este paquete directamente a Red Hat.

RHN proporciona una herramienta explícitamente para este propósito. El **RHN Proxy Diagnostic Info Gatherer** comúnmente conocido por su comando `rhn-proxy-debug`. Para usar esta herramienta, ejecute éste comando como root. Usted verá la información recogida y el archivo tarball creado, por ejemplo:

```
[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.
```

Una vez finalizado, envíe por correo-e el archivo recién creado en el directorio `/tmp/` a su representante Red Hat para un diagnóstico inmediato.

Apéndice A.

Ejemplo del archivo de configuración del Servidor Proxy RHN

El archivo de configuración `/etc/rhn/rhn.conf` para el Servidor Proxy RHN proporciona un medio para establecer parámetros claves. Tenga en cuenta, sin embargo, que los errores introducidos en este archivo pueden causar fallos en el Proxy. Realice los cambios de configuración con cuidado.

Si usted está usando también un Servidor Satellite RHN, debe tener particular cuidado con los siguientes parámetros: traceback_mail y proxy.rhn_parent. Revise el ejemplo y sus comentarios (los cuales inician con #), para una mayor información.



Nota

Usted puede añadir el parámetro `use_ssl` a `rhn.conf` bajo motivos de prueba. Establezca el valor a 0 para apagar temporalmente SSL entre el Proxy y el servidor del nivel superior. Note que esta acción compromete en gran medida la seguridad. Establezca el parámetro al su valor predeterminado (1) para reactivar SSL, o simplemente remueva la linea del archivo de configuración.

```
# 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
```

Índice

A

administrador de canales, 3
administrador de la organización, 3
Agente de actualización de Red Hat, 3, 4
archivos de registro, 31
autenticación, 4
authentication caching
  limpieza, 35

C

canal, 3
  creando un canal privado, 27
canal privado, 27
configuración del cliente
  suscribiéndose a un canal privado, 29
cómo funciona, 4

D

Desactivando Demonio de autenticación de RHN
  rhn_auth_cache, stopping, 35

E

error host now found
  no se pudo determinar el FQDN, 33
errores de conexión, 34

G

Gestor de paquetes de RHN, 5, 27
  archivo de configuración, 27
  canales, especificando, 28
  cargando los encabezados de los paquetes, 28
  configuración, 27
  creando un canal privado, 27
  instalación, 27
  opciones para la línea de comandos, 29
  verificando lista de paquetes local, 28

I

instalación
  base, 15
  del Servidor Proxy RHN, 16

L

localización de errores, 31

P

preguntas y respuestas, 32
problemas generales, 33
problemas relacionados con el caché, 35

R

Red Hat Network
  introducción, 1
requerimientos, 7
  adicionales, 9
  espacio de disco, 9
  hardware, 8
  software, 7
requerimientos adicionales, 9
requerimientos de espacio de disco, 9
requerimientos de hardware, 8
requerimientos de software, 7
rhn-proxy
  servicio, 31
rhn.conf
  archivo de ejemplo, 37
rhn_package_manager, 28
  (Ver Gestor de paquetes de RHN)

S

satellite-debug, 36
seguimiento (traceback), 3
Servidor Proxy-Caché HTTP
    requerimientos de espacio de disco, 9
squid caching, 35

T

terminología básica, 3
topologías, 11
    múltiples proxies ordenados verticalmente, 13
    múltiples proxies organizados horizontalmente, 12
    proxies con un servidor Satellite RHN, 14
    único proxy, 11

V

ventajas, 2