

Red Hat Enterprise Linux 6

Administración del servidor virtual

Adición de equilibrador de carga para Red Hat Enterprise Linux

Edición 6



Aviso Legal

Copyright © 2010 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at <http://creativecommons.org/licenses/by-sa/3.0/>. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

1801 Varsity Drive
Raleigh, NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701

Resumen

La construcción de un sistema de adición de equilibrador de carga ofrece una solución escalable y de alta disponibilidad para servicios de producción que utilizan Servidores virtuales de Linux especializados (LVS) para técnicas de enrutamiento y balance de cargas configuradas a través de la herramienta de configuración **PIRANHA**. Este libro discute la configuración de sistemas y servicios de alto rendimiento de Red Hat Enterprise Linux y la adición de equilibrador de carga LVS para Red Hat Enterprise Linux 6.

Tabla de contenidos

Introducción

1. Convenciones del Documento
 - 1.1. Convenciones Tipográficas
 - 1.2. Convenciones del documento
 - 1.3. Notas y Advertencias

2. Comentarios

1. Visión general de la adición de equilibrador de carga

- 1.1. Configuración básica de la adición de equilibrador de carga
 - 1.1.1. Repetición y uso compartido de datos
- 1.2. Configuración de la adición de equilibrador de carga de tres partes
- 1.3. Visión general de la adición de equilibrador de carga
 - 1.3.1. Algoritmos de programación
 - 1.3.2. Peso del servidor y programación
- 1.4. Métodos de enrutamiento
 - 1.4.1. Enrutado de NAT
 - 1.4.2. Enrutado directo

1.5. Marcas de cortafuego y persistencia

- 1.5.1. Persistencia
- 1.5.2. Marcas de cortafuegos

1.6. Adición de equilibrador de carga — Diagrama de bloque

- 1.6.1. Componentes de la adición de equilibrador de carga

2. Configuración inicial de la adición de equilibrador de carga

- 2.1. Configuración de servicios en los enrutadores LVS
- 2.2. Configuración de la contraseña para la Piranha Configuration Tool
- 2.3. Inicio del servicio de la Piranha Configuration Tool
 - 2.3.1. Configuración del puerto del servidor de red de la Piranha Configuration Tool
- 2.4. Limitar el acceso a la Piranha Configuration Tool
- 2.5. Activación de reenvío de paquetes
- 2.6. Configuración de servicios en servidores reales

3. Configuración de una adición de equilibrador de carga

- 3.1. La red de adición de equilibrador de carga de NAT
 - 3.1.1. Configuración de las interfaces de red para una adición de equilibrador de carga con NAT
 - 3.1.2. Rutas en los servidores reales
 - 3.1.3. Activación de rutas NAT en enrutadores LVS
- 3.2. Adición de equilibrador de carga con enrutamiento directo
 - 3.2.1. Enrutado directo y `arpables_jf`
 - 3.2.2. Enrutado directo e `iptables`
- 3.3. Cómo armar la configuración
 - 3.3.1. Consejos generales para la red de una adición de equilibrador de carga
- 3.4. Servicios de puertos múltiples y Adición de equilibrador de carga
 - 3.4.1. Asignación de marcas de cortafuegos
- 3.5. Configuración de FTP

- 3.5.1. Cómo funciona FTP
- 3.5.2. Cómo afecta al enrutamiento de una adición de equilibrador de carga
- 3.5.3. Creación de reglas de filtro de paquetes de red

3.6. Cómo guardar los parámetros de filtro de paquetes de red

4. Configuración de la adición de equilibrador de carga con Piranha Configuration Tool

- 4.1. Software necesario
- 4.2. Inicio de sesión en la Piranha Configuration Tool
- 4.3. CONTROL/MONITORING
- 4.4. GLOBAL SETTINGS
- 4.5. REDUNDANCIA
- 4.6. SERVIDORES VIRTUALES
 - 4.6.1. Subsección SERVIDOR VIRTUAL
 - 4.6.2. Subsección SERVIDOR REAL
 - 4.6.3. Subsección EDITAR SCRIPTS DE MONITORIZACIÓN
- 4.7. Sincronización de los archivos de configuración
 - 4.7.1. Sincronización de lvs.cf
 - 4.7.2. Sincronización de sysctl
 - 4.7.3. Sincronización de las reglas de filtro de paquetes de red

4.8. Inicio de la adición de equilibrador de carga

A. Uso de la adición de Equilibrador de carga con adición de Alta disponibilidad

B. Historial de revisiones

Índice

Introducción

Este documento proporciona información sobre instalación, configuración y administración de los componentes de la adición de equilibrador de carga. La adición de equilibrador de carga proporciona balance de cargas a través de técnicas de enrutamiento especializado que despachan tráfico a un grupo de servidores.

La audiencia de este documento debe tener conocimientos avanzados de Red Hat Enterprise Linux y entender los conceptos acerca de cluster, almacenaje y servidores de informática.

Este documento está organizado de la siguiente manera:

- ▶ [Capítulo 1, *Visión general de la adición de equilibrador de carga*](#)
- ▶ [Capítulo 2, *Configuración inicial de la adición de equilibrador de carga*](#)
- ▶ [Capítulo 3, *Configuración de una adición de equilibrador de carga*](#)
- ▶ [Capítulo 4, *Configuración de la adición de equilibrador de carga con **Piranha Configuration Tool***](#)
- ▶ [Apéndice A, *Uso de la adición de Equilibrador de carga con adición de Alta disponibilidad*](#)

Para obtener mayor información sobre Red Hat Enterprise Linux 6, consulte los siguientes recursos:

- ▶ *Guía de instalación de Red Hat Enterprise Linux* — Proporciona información sobre instalación de Red Hat Enterprise Linux 6.
- ▶ *Guía de implementación de Red Hat Enterprise Linux* — Proporciona información sobre implementación, configuración y administración de Red Hat Enterprise Linux 6.

Para obtener mayor información sobre la adición del equilibrador de carga y productos relacionados para Red Hat Enterprise Linux 6, consulte los siguientes recursos:

- ▶ *Visión general* — Proporciona una visión general de alto nivel sobre la adición de alta disponibilidad, adición de almacenamiento resistente y la adición del equilibrador de carga.
- ▶ *Configuración y administración de una adición de Alta disponibilidad* — Proporciona información sobre instalación, configuración y administración de adición de Alta disponibilidad para (también conocido como Cluster de Red Hat) Red Hat Enterprise Linux 6.
- ▶ *Manejo del Administrador de volumen lógico* — Proporciona una descripción del manejo del Administrador de volumen lógico (LVM), incluyendo información sobre ejecución de LVM en un entorno de cluster.
- ▶ *Sistema de archivos global 2: Configuración y administración* — Proporciona información sobre instalación, configuración y mantenimiento de la adición de almacenamiento resistente (también conocido como Sistema de archivos global 2 de Red Hat/Red Hat Global File System 2).
- ▶ *DM Multipath* — Proporciona información sobre la función del Dispositivo- Mapeador- Multirutas de Red Hat Enterprise Linux 6.
- ▶ *Notas de lanzamiento* — Proporciona información sobre el lanzamiento actual de productos de Red Hat.

Este documento y otros documentos de Red Hat están disponibles en versiones HTML, PDF y RPM en el CD de documentación de Red Hat Enterprise Linux y en línea en <http://www.redhat.com/docs/>.

1. Convenciones del Documento

Este manual utiliza varias convenciones para resaltar algunas palabras y frases y llamar la atención sobre ciertas partes específicas de información.

En ediciones PDF y de papel, este manual utiliza tipos de letra procedentes de [Liberation Fonts](#). Liberation Fonts también se utilizan en ediciones de HTML si están instalados en su sistema. Si no, se

muestran tipografías alternativas pero equivalentes. Nota: Red Hat Enterprise Linux 5 y siguientes incluyen Liberation Fonts predeterminadas.

1.1. Convenciones Tipográficas

Se utilizan cuatro convenciones tipográficas para llamar la atención sobre palabras o frases específicas. Dichas convenciones y las circunstancias en que se aplican son las siguientes:

Negrita monoespaciado

Utilizada para resaltar la entrada del sistema, incluyendo comandos de shell, nombres de archivo y rutas. También se utiliza para resaltar teclas claves y combinaciones de teclas. Por ejemplo:

Para ver el contenido del archivo **my_next_bestselling_novel** en su directorio actual de trabajo, escriba el comando **cat my_next_bestselling_novel** en el intérprete de comandos de shell y pulse **Enter** para ejecutar el comando.

El ejemplo anterior incluye un nombre de archivo, un comando de shell y una tecla clave. Todo se presenta en negrita-monoespaciado y distinguible gracias al contexto.

Las combinaciones de teclas se pueden distinguir de las teclas claves mediante el guión que conecta cada parte de una combinación de tecla. Por ejemplo:

Pulse **Enter** para ejecutar el comando.

Press **Ctrl+Alt+F2** to switch to a virtual terminal.

La primera oración resalta la tecla clave determinada que se debe pulsar. La segunda resalta dos conjuntos de tres teclas claves que deben ser presionadas simultáneamente.

Si se discute el código fuente, los nombres de las clase, los métodos, las funciones, los nombres de variables y valores de retorno mencionados dentro de un párrafo serán presentados en **Negrita-monoespaciado**. Por ejemplo:

Las clases de archivo relacionadas incluyen **filename** para sistema de archivos, **file** para archivos y **dir** para directorios. Cada clase tiene su propio conjunto asociado de permisos.

Negrita proporcional

Esta denota palabras o frases encontradas en un sistema, incluyendo nombres de aplicación, texto de cuadro de diálogo, botones etiquetados, etiquetas de cajilla de verificación y botón de radio; títulos de menú y títulos del sub-menú. Por ejemplo:

Seleccionar **Sistema** → **Preferencias** → **Ratón** desde la barra del menú principal para lanzar **Preferencias de Ratón**. En la pestaña de **Botones**, haga clic en la cajilla **ratón de mano izquierda** y luego haga clic en **Cerrar** para cambiar el botón principal del ratón de la izquierda a la derecha (adecuando el ratón para la mano izquierda).

To insert a special character into a **gedit** file, choose **Applications** → **Accessories** → **Character Map** from the main menu bar. Next, choose **Search** → **Find...** from the **Character Map** menu bar, type the name of the character in the **Search** field and click **Next**. The character you sought will be highlighted in the **Character Table**. Double-click this highlighted character to place it in the **Text to copy** field and then click the **Copy** button. Now switch back to your document and choose **Edit** → **Paste** from the **gedit** menu bar.

El texto anterior incluye nombres de aplicación; nombres y elementos del menú de todo el sistema;

nombres de menú de aplicaciones específicas y botones y texto hallados dentro de una interfaz gráfica de usuario, todos presentados en **negrita proporcional** y distinguibles por contexto.

Itálicas-negrita monoespaciado* o *Itálicas-negrita proporcional

Ya sea **negrita monoespaciado** o **negrita proporcional**, la adición de **itálicas** indica texto reemplazable o variable. Las **itálicas** denotan texto que usted no escribe literalmente o texto mostrado que cambia dependiendo de la circunstancia. Por ejemplo:

Para conectar a una máquina remota utilizando **ssh**, teclee **ssh *nombredeusuario@dominio.nombre*** en un intérprete de comandos de shell. Si la máquina remota es **example.com** y su nombre de usuario en esa máquina es **john**, teclee **ssh john@example.com**.

El comando **mount -o remount *file-system*** remonta el sistema de archivo llamado. Por ejemplo, para volver a montar el sistema de archivo **/home**, el comando es **mount -o remount /home**.

Para ver la versión de un paquete actualmente instalado, utilice el comando **rpm -q *paquete***. Éste entregará el resultado siguiente: ***paquete-versión-lanzamiento***.

Note the words in bold italics above — username, domain.name, file-system, package, version and release. Each word is a placeholder, either for text you enter when issuing a command or for text displayed by the system.

Aparte del uso estándar para presentar el título de un trabajo, las **itálicas** denotan el primer uso de un término nuevo e importante. Por ejemplo:

Publican es un sistema de publicación de *DocBook*.

1.2. Convenciones del documento

Los mensajes de salida de la terminal o fragmentos de código fuente se distinguen visualmente del texto circundante.

Los mensajes de salida enviados a una terminal se muestran en **romano monoespaciado** y se presentan así:

```
books      Desktop  documentation  drafts  mss    photos  stuff  svn
books_tests Desktop1  downloads      images  notes  scripts svgs
```

Los listados de código fuente también se muestran en **romano monoespaciado**, pero se presentan y resaltan de la siguiente manera:

```
package org.jboss.book.jca.ex1;

import javax.naming.InitialContext;

public class ExClient
{
    public static void main(String args[])
        throws Exception
    {
        InitialContext iniCtx = new InitialContext();
        Object          ref    = iniCtx.lookup("EchoBean");
        EchoHome        home   = (EchoHome) ref;
        Echo            echo    = home.create();

        System.out.println("Created Echo");

        System.out.println("Echo.echo('Hello') = " + echo.echo("Hello"));
    }
}
```

1.3. Notas y Advertencias

Finalmente, utilizamos tres estilos visuales para llamar la atención sobre la información que de otro modo se podría pasar por alto.



Nota

Una nota es una sugerencia, atajo o enfoque alternativo para una tarea determinada. Ignorar una nota no debería tener consecuencias negativas, pero podría perderse de algunos trucos que pueden facilitarle las cosas.



Importante

Los cuadros con el título de importante dan detalles de cosas que se pueden pasar por alto fácilmente: cambios de configuración únicamente aplicables a la sesión actual, o servicios que necesitan reiniciarse antes de que se aplique una actualización. Ignorar estos cuadros no ocasionará pérdida de datos, pero puede causar enfado y frustración.



Aviso

Las advertencias no deben ignorarse. Ignorarlas muy probablemente ocasionará pérdida de datos.

2. Comentarios

Si encuentra algún error tipográfico en este manual, o si ha pensado en alguna forma de mejorarlo, nos gustaría saberlo. Por favor envíe un reporte en Bugzilla (<http://bugzilla.redhat.com/bugzilla/>) a nombre del producto **Documentation-cluster**.

Asegúrese de mencionar el identificador del manual:

Virtual_Server_Administration(EN)-6 (2010-10-14T16:28)

Al mencionar el identificador del manual, sabemos exactamente qué versión de la guía tiene usted.

Si tiene una sugerencia sobre cómo mejorar la documentación, trate de ser lo más específico posible. Si ha encontrado un error, por favor incluya el número de la sección y parte del contexto para poderlo identificar fácilmente.

Capítulo 1. Visión general de la adición de equilibrador de carga

La adición de equilibrador de carga es un conjunto de componentes de software que proporcionan Servidores virtuales de Linux (LVS) para balancear la carga IP a través de un set de servidores reales. La adición de equilibrador de cargas se ejecuta en un par de computadores configurados similarmente: uno de ellos es un *enrutador LVS activo* y el otro es un *enrutador LVS de respaldo*. El enrutador LVS activo tiene dos roles:

- ▶ Equilibrar la carga entre los servidores reales.
- ▶ Revisar la integridad de los servicios en cada servidor real.

El enrutador LVS de respaldo sondea el estado del enrutador LVS activo y toma control de sus tareas en caso de que éste falle.

Este capítulo proporciona un resumen de los componentes y funciones de la adición de equilibrador de carga y consta de las siguientes secciones:

- ▶ [Sección 1.1, “Configuración básica de la adición de equilibrador de carga”](#)
- ▶ [Sección 1.2, “Configuración de la adición de equilibrador de carga de tres partes”](#)
- ▶ [Sección 1.3, “Visión general de la adición de equilibrador de carga”](#)
- ▶ [Sección 1.4, “Métodos de enrutamiento”](#)
- ▶ [Sección 1.5, “Marcas de cortafuego y persistencia”](#)
- ▶ [Sección 1.6, “Adición de equilibrador de carga — Diagrama de bloque”](#)

1.1. Configuración básica de la adición de equilibrador de carga

[Figura 1.1, “Configuración básica de la adición de equilibrador de carga”](#) muestra una configuración de adición de equilibrador de carga sencilla que consta de dos capas. En la primera capa hay dos enrutadores LVS — uno activo y otro de respaldo. Cada uno de los enrutadores LVS tiene dos interfaces de red, una interfaz en internet y la otra en la red privada, las cuales le permiten regular el tráfico entre las dos redes. En este ejemplo, el enrutador activo utiliza *Traducción de dirección de red* (siglas en inglés de *Network Address Translation*) o NAT para dirigir el tráfico desde internet a un número variable de servidores reales en la segunda capa que, a su vez, proporciona los servicios necesarios. Por lo tanto, los servidores reales en este ejemplo se conectan al segmento de red privada dedicado y pasan todo el tráfico público entrante o saliente a través del enrutador LVS activo. Para el mundo exterior, los servidores aparecen como una sola entidad.

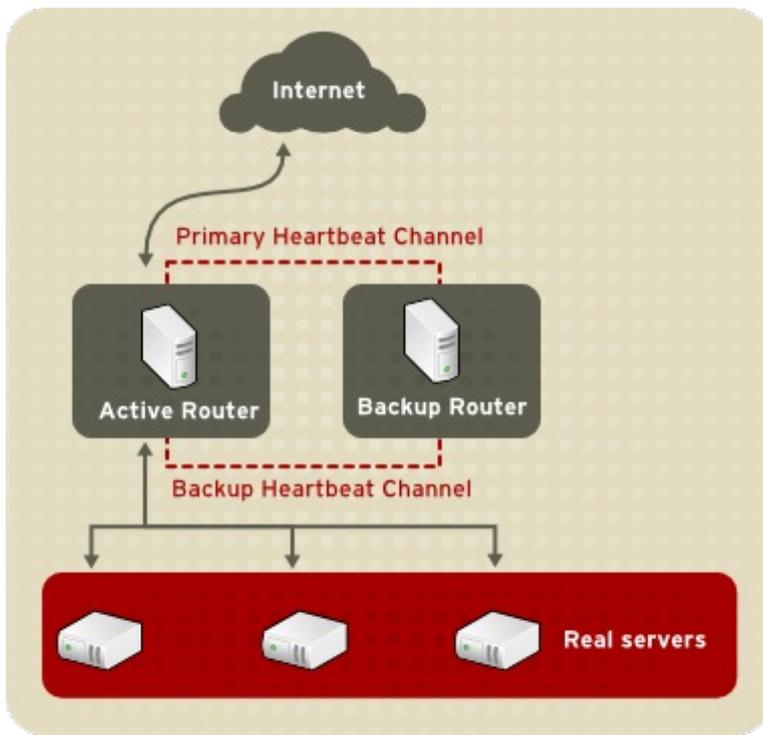


Figura 1.1. Configuración básica de la adición de equilibrador de carga

Las solicitudes de servicios que llegan al enrutador LVS son dirigidas a una *IP virtual* o *VIP*. Esta es una dirección de ruta pública que el administrador del sitio asocia con un nombre de dominio completamente calificado, como `www.ejemplo.com`, y asigna uno o más *servidores virtuales*. Un servidor virtual es un servicio configurado para escuchar en una IP virtual específica. Consulte la [Sección 4.6, “SERVIDORES VIRTUALES”](#) para obtener mayor información sobre cómo configurar un servidor virtual con la **Piranha Configuration Tool**. Una dirección VIP migra de un enrutador LVS a otro durante un proceso de recuperación contra fallos, de esta forma se mantiene una presencia en la dirección IP (también conocida como *dirección IP flotante*).

Las direcciones VIP pueden tener sobrenombres que se dirijan al mismo dispositivo que conecta al enrutador LVS con la red pública. Por ejemplo, si `eth0` está conectado a Internet, puede haber varios servidores virtuales con sobrenombres a `eth0:1`. Alternativamente, cada servidor virtual puede estar asociado con un dispositivo separado por cada servicio. Por ejemplo, el tráfico HTTP puede ser manejado en `eth0:1` y el tráfico FTP puede ser manejado en `eth0:2`.

Solamente un enrutador LVS está activo a la vez. El rol del enrutador activo es el de redirigir las solicitudes de la dirección IP virtual a los servidores reales. La redirección está basada en uno de ocho algoritmos de balance de carga descritos en la [Sección 1.3, “Visión general de la adición de equilibrador de carga”](#).

El enrutador LVS activo sondea dinámicamente la salud de los servicios especificados en los servidores reales a través de un *script de envío y espera*. Para ayudar en la detección de servicios que requieren datos dinámicos, tal como HTTPS o SSL, se puede incluso llamar a programas ejecutables externos. Si un servicio en un servidor real no funciona adecuadamente, el enrutador LVS activo no envía solicitudes a ese servidor hasta que retorne a la operación normal.

El enrutador de respaldo ejecuta el rol de sistema en espera. Periódicamente, los enrutadores LVS intercambian mensajes a través de la interfaz pública externa primaria y, en caso de fallos, a través de la interfaz privada. Si el enrutador LVS de respaldo no recibe un mensaje dentro de un intervalo de tiempo esperado, éste inicia un proceso de recuperación contra fallos y asume el rol de enrutador activo. Durante el proceso de recuperación contra fallos, el enrutador de respaldo obtiene la dirección VIP servida por el enrutador fallido utilizando una técnica conocida como *Suplantación de ARP* — en

donde el enrutador LVS de respaldo se anuncia a sí mismo como el destino de los paquetes IP dirigidos al nodo fallido. Cuando el nodo activo regrese a prestar el servicio, el nodo de respaldo asume su rol de enrutador en espera.

La configuración de dos capas que se muestra en la [Figura 1.1, “Configuración básica de la adición de equilibrador de carga”](#) es adecuada para servir datos que no cambian con mucha frecuencia — tales como páginas de web estáticas — porque los servidores reales individuales no sincronizan los datos automáticamente entre cada nodo.

1.1.1. Repetición y uso compartido de datos

Como no hay componentes internos en la adición de equilibrador de carga para compartir los mismos datos entre servidores reales, el administrador tiene dos opciones básicas:

- ▶ Sincronizar los datos entre los servidores reales.
- ▶ Añadir una tercera capa a la topología para el acceso de datos compartidos

La primera opción es la preferida para aquellos servidores que no permiten a un gran número de usuarios cargar o cambiar datos en el servidor real. Si los servidores reales permiten la modificación de datos por una gran cantidad de usuarios, como los sitios web de comercio electrónico, por ejemplo, es preferible añadir una nueva capa.

1.1.1.1. Configuración de servidores reales para sincronizar los datos

Hay muchas maneras en que el administrador puede sincronizar datos a lo largo del grupo de servidores reales. Por ejemplo, los script de shell pueden ser usados para publicar una página web que ha sido modificada en todos los servidores de forma simultánea. Asimismo, el administrador de sistemas puede usar programas como **r sync** para duplicar los cambios de datos a lo largo de todos los nodos cada determinado tiempo.

Sin embargo, este tipo de sincronización de datos no es óptimo si la configuración es utilizada por múltiples usuarios cargando archivos o ejecutando transacciones de datos constantemente. Para una configuración con alta carga, una *topología de tres capas* es la solución ideal.

1.2. Configuración de la adición de equilibrador de carga de tres partes

[Figura 1.2, “Configuración de la adición de equilibrador de carga de tres partes”](#) presenta una topología de adición de equilibrador de carga típica de tres capas. En este ejemplo, el enrutador LVS activo hace la solicitud desde Internet a un grupo de servidores reales. Cada uno de los servidores reales accede a una fuente de datos compartidos a través de la red.

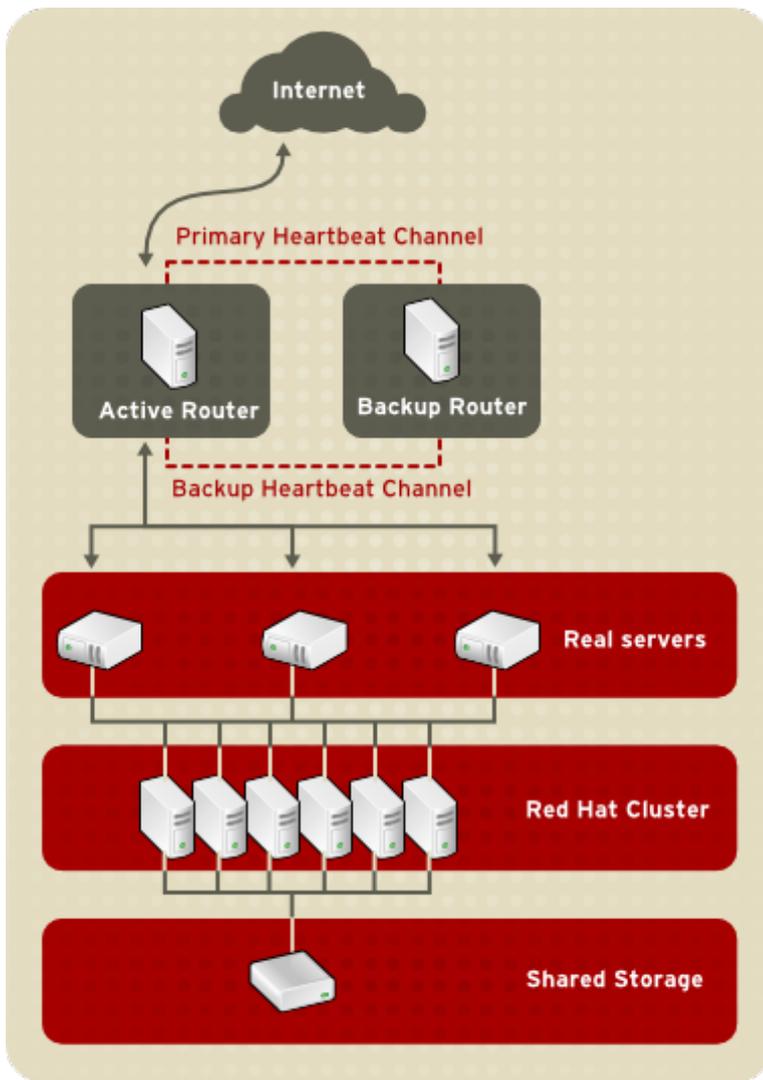


Figura 1.2. Configuración de la adición de equilibrador de carga de tres partes

Esta configuración es ideal para servidores FTP bastante usados, en donde los datos son almacenados en un servidor central de alta disponibilidad y pueden ser accedidos por cada servidor real a través de un directorio compartido NFS o un recurso Samba. Esta topología también es recomendada para sitios web que acceden a una base de datos central de alta disponibilidad para realizar transacciones. Adicionalmente, los administradores pueden configurar un cluster de alta disponibilidad para servir ambos roles simultáneamente si utilizan una configuración activo-activo con el Red Hat Cluster Manager.

La tercera capa en el ejemplo anterior no tiene que utilizar el Red Hat Cluster Manager, pero si no se utiliza una solución de alta disponibilidad podría introducir un fallo por un único elemento que podría ser crítico.

1.3. Visión general de la adición de equilibrador de carga

Una de las ventajas del uso de la adición de equilibrador de carga es la habilidad de ejecutar balance de carga de IP flexible en un grupo de servidores reales. Esta flexibilidad se debe a la variedad de algoritmos de programación que un administrador puede escoger cuando configura la adición de equilibrador de carga. La adición de equilibrador de carga es superior a métodos menos flexibles, tales como *Round-Robin DNS* en donde la naturaleza jerárquica de DNS y el proceso de cache por las máquinas clientes puede llevar a un desbalance de carga. Además, el filtro de bajo nivel empleado por el enrutador LVS tiene ventajas sobre el reenvío de solicitudes a nivel de aplicaciones porque el

balance de carga en el nivel de paquetes de red causa una sobrecarga computacional mínima y permite mayor escalabilidad.

Al usar un algoritmo de programación, el enrutador activo puede tener en cuenta la actividad de los servidores reales y, opcionalmente, un factor de *peso* asignado por los administradores cuando se envían las solicitudes de servicios. El uso de pesos asignados da prioridades arbitrarias para máquinas individuales. Al usar esta forma de programación se puede crear un grupo de servidores reales que utilizan una variedad de hardware y software y el enrutador activo puede cargar uniformemente cada servidor real.

El mecanismo de programación para la adición de equilibrador de carga es proporcionado por una colección de parches del kernel llamado *IPVS* o *Servidor virtual IP*. Estos módulos permiten interrupción de capas de transporte de *capa 4 (L4)* la cual está diseñada para funcionar bien con múltiples servidores en una dirección IP única.

Para rastrear y encaminar paquetes a los servidores reales de forma eficiente, IPVS construye una *Tabla IPVS* en el kernel. Esta tabla es utilizada por el servidor activo LVS para redirigir solicitudes desde la dirección de servidores virtuales a y desde los servidores reales en el grupo. La tabla IPVS es constantemente actualizada por un servicio llamado *ipvsadmin* — añadiendo o removiendo miembros del cluster dependiendo de su disponibilidad.

1.3.1. Algoritmos de programación

La estructura que la tabla IPVS adquiere depende del algoritmo de programación que el administrador elige para cualquier servidor virtual determinado. Para permitir mayor flexibilidad en los tipos de servicios que se pueden agrupar en cluster y para controlar la manera como se programan estos servicios, Red Hat Enterprise Linux proporciona los siguientes algoritmos de programación. Para obtener instrucciones sobre cómo asignar algoritmos de programación, consulte la [Sección 4.6.1, “Subsección SERVIDOR VIRTUAL”](#).

Programación Round-Robin

Distribuye cada solicitud secuencialmente a lo largo del grupo de servidores reales. Con este algoritmo, todos los servidores reales son tratados como iguales sin importar la capacidad o carga. Este modelo de programación se asemeja a DNS de Round-Robin, pero es más detallado porque se basa en las conexiones de red y no en el host. La programación de round-robin de la adición de equilibrador de carga tampoco sufre desbalances causados por el proceso de cache de las solicitudes de DNS.

Programación ponderada Round-Robin

Distribuye cada solicitud secuencialmente al rededor del grupo de servidores reales, pero otorga más trabajos a los servidores que tienen mayor capacidad. La capacidad es indicada por un factor de peso asignado por el usuario, el cual se ajusta hacia arriba y hacia abajo gracias a la información de carga dinámica. Consulte la [Sección 1.3.2, “Peso del servidor y programación”](#) para obtener mayor información sobre el peso de los servidores reales.

La programación Round-Robin ponderada es la preferida si hay diferencias significativas en la capacidad de los servidores reales en el grupo. Sin embargo, si la carga de solicitudes varía de forma dramática, los servidores con una capacidad mayor responderán a más solicitudes de las que deberían.

Conexión mínima

Distribuye más solicitudes a los servidores reales con menos conexiones activas. Ya que rastrea las conexiones vivas a los servidores reales a través de la tabla IPVS, la conexión

mínima es un tipo de algoritmo de programación dinámica, siendo una mejor opción si hay un alto grado de variaciones en la carga de solicitudes. Es adecuado para grupos de servidores reales en donde cada nodo miembro tiene la misma capacidad. Si un grupo de servidores tiene capacidades diferentes, la programación de conexión mínima ponderada es una mejor opción.

Conexiones ponderadas mínimas (predeterminada)

Distribuye más solicitudes a los servidores con menos conexiones activas en relación con sus capacidades. La capacidad es indicada por el usuario y es ajustada por la información de carga dinámica. La adición del parámetro de capacidad hace que este algoritmo sea ideal cuando la infraestructura tiene servidores reales con capacidades de hardware variado. Consulte la [Sección 1.3.2. "Peso del servidor y programación"](#) para obtener mayor información sobre servidores reales.

Programación de conexión mínima basada en localidad

Distribuye más solicitudes a los servidores con menos conexiones activas en relación con sus IP de destino. Este algoritmo se utiliza en cluster de servidores de cache proxy. Envía el paquete para una dirección IP al servidor con esa dirección a menos que ese servidor esté por encima de su capacidad y tenga un servidor a media carga, en dicho caso se asigna la dirección IP al servidor real con menos carga.

Programación mínima basada en localidad con programación de réplica

Distribuye más solicitudes a los servidores con menos conexiones activas de acuerdo al IP de destino. Este algoritmo es usado en servidores de cache de proxy. Se diferencia de la programación "Conexión mínima basada en localidad" al relacionar la dirección IP objetivo con un grupo de servidores reales. Las solicitudes son luego enviadas al servidor en el grupo con menos número de conexiones. Si la capacidad de todos los nodos para el IP de destino está sobre el límite, este método añade un nuevo servidor real del grupo general al grupo de servidores para el IP de destino. El nodo con mayor carga es desplazado fuera del grupo para evitar un exceso de replicación.

Programación de destino hash

Distribuye las solicitudes al grupo de servidores reales buscando el IP de destino en una tabla hash estática. Este algoritmo está diseñado para ser usado en un cluster de servidor de cache de proxy.

Programación de fuente hash

Distribuye todas las solicitudes al grupo de servidores reales, buscando el IP de origen en una tabla hash estática. Este algoritmo se utiliza en enrutadores LVS con varios cortafuegos.

1.3.2. Peso del servidor y programación

El administrador de la adición de equilibrador de carga puede asignar un *valor* a cada nodo en el grupo de servidores reales. El valor es un entero usado por los algoritmos de programación que lo *reconocen* (tal como la programación con conexiones ponderadas mínimas) y asiste al enrutador LVS en el balance de carga con hardware que tiene diferentes opciones.

Los pesos funcionan como valores relativos entre si. Por ejemplo, si un servidor real tiene un valor de 1 y otro servidor tiene un valor de 5, el servidor con peso 5 recibe 5 conexiones por cada conexión que

recibe el otro servidor. El valor de peso predeterminado es 1.

Aunque el uso de pesos para variar la configuración del hardware en un grupo de servidores reales ayuda a balancear la carga de una manera más efectiva, puede causar desbalances temporales cuando se introduce un servidor real al grupo de servidores reales y el servidor virtual está programado mediante conexiones ponderadas mínimas. Por ejemplo, supongamos que hay tres servidores en el grupo. Los servidores A y B tienen un peso de 1; el servidor C tiene un peso de 2. Si el servidor C falla, los servidores A y B se distribuyen la carga abandonada. Sin embargo, cuando el servidor C entre en línea nuevamente, no tendrá conexiones y se verá inundado de solicitudes hasta que entre en balance con A y B.

Para prevenir este fenómeno, los administradores pueden hacer que el servidor virtual se comporte como un servidor *quiesce* — cuando un servidor real entre al grupo la tabla de conexiones se inicia a cero y el enrutador LVS envía las solicitudes como si todos los servidores reales fueran nuevos en el cluster.

1.4. Métodos de enrutamiento

Red Hat Enterprise Linux utiliza *Traducción de dirección de red* o *enrutamiento de NAT* para la adición de equilibrador de carga. NAT brinda al administrador gran flexibilidad cuando se utiliza hardware disponible y se integra la adición de equilibrador de carga en la red existente.

1.4.1. Enrutado de NAT

[Figura 1.3, “La adición de equilibrador de carga implementado con enrutamiento de NAT”](#), ilustra la adición de equilibrador de carga utilizando enrutamiento de NAT para desplazar solicitudes entre Internet y la red privada.

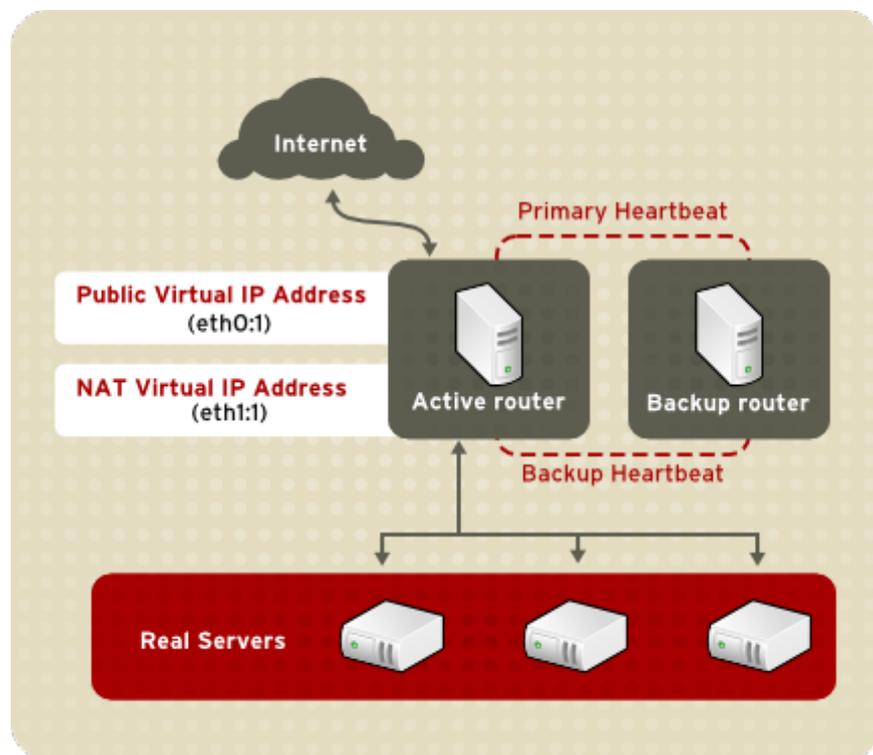


Figura 1.3. La adición de equilibrador de carga implementado con enrutamiento de NAT

En el ejemplo, hay dos NIC en el enrutador LVS activo. El NIC para Internet tiene una *dirección IP real* en eth0 y tiene una dirección IP flotante en eth0:1. El NIC para la interfaz de red privada tiene una dirección IP real en eth1 y tiene una dirección flotante en eth1:1. En el caso de fallo, la interfaz virtual que encara

el internet y la privada que encara la interfaz virtual son tomadas simultáneamente por el enrutador LVS de respaldo. Todos los servidores reales en la red privada utilizan el IP flotante para el enrutador NAT como su enrutador predeterminado para comunicarse con el enrutador LVS activo, de esta forma la habilidades para responder a solicitudes desde Internet no se ve impedida.

En el ejemplo, la dirección IP flotante pública del enrutador LVS y la dirección IP flotante NAT privada hacen referencia a los dos NIC físicos. Aunque es posible asociar cada dirección IP flotante a su dispositivo físico en el enrutador LVS, no se requiere tener más de dos NIC.

Si se utiliza esta topología, el enrutador activo LVS recibe la solicitud y la envía al servidor apropiado. El servidor real luego procesa la solicitud y retorna el paquete al enrutador LVS el cual utiliza NAT para reemplazar la dirección del servidor real en el paquete por la dirección VIP pública del enrutador LVS. Este proceso se llama *enmascaramiento de IP* porque la dirección IP de los servidores reales se oculta de las solicitudes del cliente.

Al utilizar NAT, los servidores reales pueden ser cualquier clase de máquina con cualquier sistema operativo. La desventaja principal es que el enrutador LVS puede convertirse en un cuello de botella en implementaciones grandes porque las solicitudes salientes como entrantes son procesadas.

1.4.2. Enrutado directo

La configuración de la adición de equilibrador de carga que utiliza enrutamiento directo proporciona mejor rendimiento que otras topologías de red LVS. El enrutamiento directo permite que los servidores reales procesen y encaminen los paquetes directamente al usuario que los solicitó en vez de encaminar los paquetes salientes al enrutador LVS. El enrutado directo reduce la posibilidad de problemas de rendimiento de red al relegar el trabajo de LVS al procesamiento de paquetes entrantes únicamente.

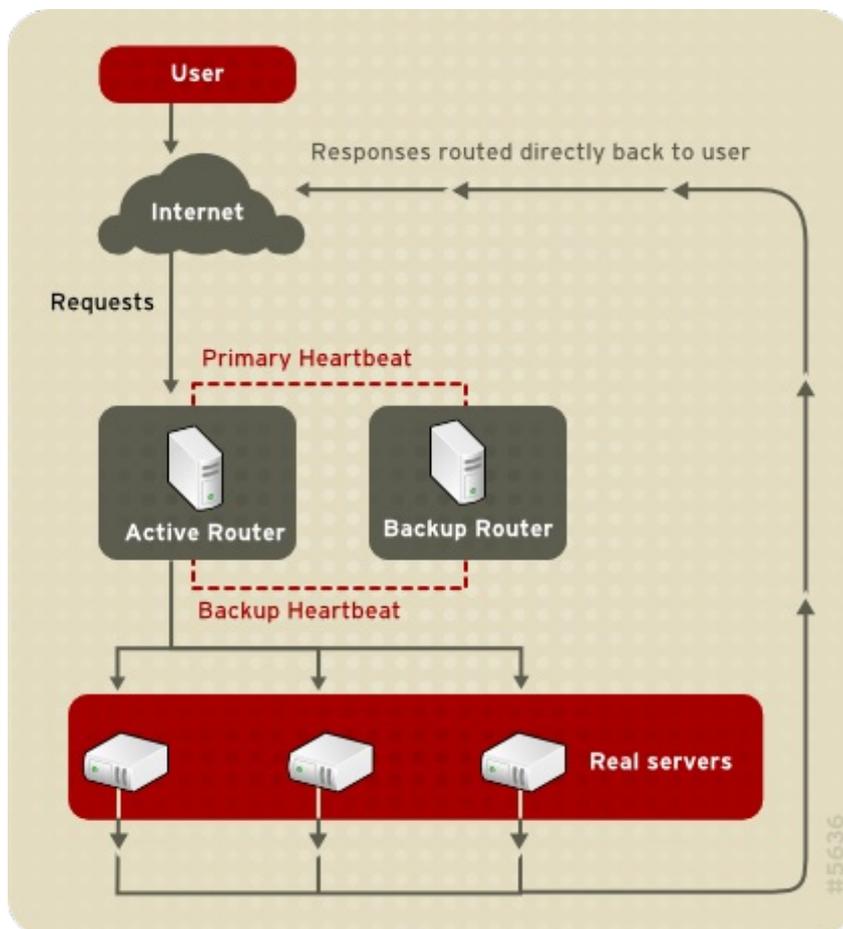


Figura 1.4. Adición de equilibrador de carga implementada con enrutamiento directo

En la configuración adición de equilibrador de carga de enrutamiento directo, el enrutador LVS recibe las solicitudes entrantes de servidores a través del IP virtual (VIP) y utiliza un algoritmo de programación para encaminar la solicitud a los servidores reales. El servidor real procesa la solicitud y envía la respuesta directamente al cliente, ignorando el enrutador LVS. Este método de enrutado permite escalabilidad ya que los servidores reales pueden ser añadidos sin el problema de que el enrutador LVS tenga que encaminar paquetes salientes desde el servidor real al cliente, lo cual puede llegar a convertirse en un cuello de botella cuando hay una carga de red pesada.

1.4.2.1. Enrutado directo y limitación ARP

Aunque hay varias ventajas al utilizar enrutamiento directo en adición de equilibrador de carga, hay también algunas limitaciones. El problema más común con LVS a través de enrutamiento directo es con el *Protocolo de resolución de direcciones* (ARP).

En situaciones típicas, un cliente en Internet envía una solicitud a una dirección IP. Los enrutadores de red envían respuestas a sus destinatarios relacionando la dirección IP con la dirección MAC de la máquina con ARP. Las solicitudes ARP son transmitidas a todas las máquinas conectadas en la red y las máquinas con la combinación IP/MAC correcta recibe el paquete. Las asociaciones IP/MAC se almacenan en una cache ARP que se limpia periódicamente (generalmente cada 15 minutos).

El problema con las solicitudes ARP en una configuración de adición de equilibrador de carga con enrutamiento directo es que una solicitud de un cliente a una dirección IP debe estar asociada con una dirección MAC para que la solicitud sea manejada, la dirección IP virtual del sistema LVS debe estar asociada con una dirección MAC. Sin embargo, como el enrutador LVS y los servidores reales todos tienen la misma VIP, el ARP será enviado a todas las máquinas asociadas con la VIP. Esto puede causar algunos problemas, tal como que el VIP sea asociado directamente con uno de los servidores reales y procesa las solicitudes directamente, dejando de lado el enrutador LVS completamente y anulando así el propósito de LVS.

Para solucionar este problema, asegúrese de que las solicitudes entrantes sean siempre enviadas al enrutador LVS y no a alguno de los servidores reales. Esto se puede realizar con las herramientas de filtro de paquetes **arptables_jf** o **iptables** por las siguientes razones:

- ▶ **arptables_jf** previene que ARP asocie las VIP con los servidores reales.
- ▶ El método **iptables** soluciona completamente el problema de ARP al no configurar las VIP en los servidores reales.

Para obtener mayor información sobre el uso de **arptables** o **iptables** en un entorno de adición de equilibrador de carga de enrutamiento directo, consulte la [Sección 3.2.1, “Enrutado directo y arptables_jf”](#) o la [Sección 3.2.2, “Enrutado directo e iptables”](#).

1.5. Marcas de cortafuego y persistencia

En algunas circunstancias, puede desearse que un cliente se conecte con el mismo servidor real varias veces en vez de tener que pasar un algoritmo de balance de adición de equilibrador de carga envíe esa solicitud al mejor servidor disponible. Ejemplos de tales situaciones incluyen los formularios web de varias páginas, las cookies, las conexiones SSL y FTP. En dichos casos, el cliente puede no funcionar adecuadamente a menos que la transacción sea procesada por el mismo servidor que retiene el contexto inicial. LVS proporciona dos funcionalidades diferentes para manejar estos casos: *persistencia* y *marcas de cortafuego*.

1.5.1. Persistencia

Cuando se activa, la persistencia actúa como un contador. Cuando un cliente se conecta a un servicio, la adición de equilibrador de carga recuerda la última conexión para el periodo de tiempo especificado. Si la misma dirección IP de cliente se conecta dentro del periodo de tiempo establecido, la solicitud se

envía al mismo servidor que estaba procesando la solicitud anteriormente — dejando de lado el mecanismo de balance de carga. Cuando ocurre una conexión fuera del tiempo límite, ésta se maneja de acuerdo a las reglas de programación en uso.

La persistencia también permite especificar una máscara de subred para aplicar a las direcciones IP del cliente como herramienta para controlar las direcciones que tienen mayor nivel de persistencia, agrupando así conexiones a esa subred.

El agrupamiento de conexiones destinadas a diferentes puertos puede ser importante para los protocolos que utilizan más de un puerto para comunicarse, tal como FTP. Sin embargo, la persistencia no es la manera más efectiva de agrupar las conexiones destinadas a diferentes puertos. Para estas situaciones, es mejor utilizar *marcas de cortafuegos*.

1.5.2. Marcas de cortafuegos

Las marcas de cortafuegos ofrecen una manera fácil y eficiente de agrupar puertos utilizados por un protocolo o grupo de protocolos relacionados. Por ejemplo, si la adición de equilibrador de carga se implementa en un sitio de comercio electrónico, las marcas de cortafuegos pueden ser usadas para agrupar conexiones HTTP en el puerto 80 y conexiones seguras en el puerto 443. Al asignar la misma marca de cortafuego al servidor virtual para cada protocolo, la información de estado para la transacción puede ser preservada porque el enrutador LVS envía todas las solicitudes al mismo servidor real después de que la conexión ha sido abierta.

Gracias a su eficiencia y facilidad de uso, los administradores de la adición de equilibrador de carga deben utilizar marcas de cortafuegos en vez de persistencia cuando sea posible agrupar conexiones. Sin embargo, se debe añadir persistencia a los servidores virtuales junto con las marcas de cortafuegos para asegurar que los clientes se reconecten al mismo servidor por un periodo de tiempo adecuado.

1.6. Adición de equilibrador de carga — Diagrama de bloque

Los enrutadores LVS utilizan un set de programas para monitorizar los miembros y los servicios del cluster. La [Figura 1.5 “Componentes de la adición de equilibrador de carga”](#) ilustra cómo trabajan estos programas tanto en los enrutadores LVS activos como en los pasivos para administrar el cluster .

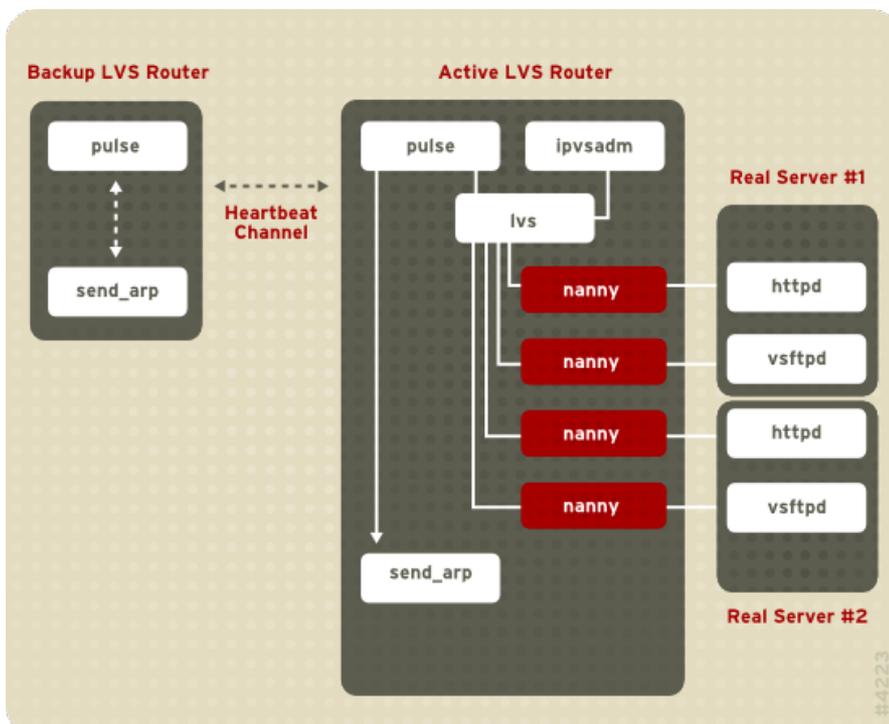


Figura 1.5. Componentes de la adición de equilibrador de carga

El demonio **pulse** se ejecuta en los enrutadores LVS activo y de respaldo. En el enrutador de respaldo, **pulse** envía un *pulso* a la interfaz pública del enrutador activo para asegurarse de que éste está funcionando apropiadamente. En el enrutador activo, **pulse** inicia el demonio **lvs** y responde a los *pulsos* enviados por el enrutador LVS de respaldo.

Una vez iniciado, el demonio **lvs** llama a la herramienta **ipvsadmin** para configurar y mantener la tabla de rutas IPVS (IP Virtual Server) en el kernel e inicia un proceso **nanny** para cada servidor virtual configurado en cada servidor real. Cada proceso **nanny** revisa el estado de cada servidor configurado en un servidor real e informa al demonio **lvs** si el servicio en el servidor real no está funcionando. Si el servicio no está funcionando, el demonio **lvs** ordena a **ipvsadm** que remueva el servidor real de la tabla de rutas IPVS.

Si el enrutador LVS de respaldo no recibe una respuesta desde el enrutador LVS activo, el primero inicia un proceso de recuperación contra fallos llamando a **send_arp** para que asigne nuevamente todas las direcciones IP virtuales a las direcciones de hardware NIC (direcciones MAC) del enrutador LVS de respaldo, envía un comando para activar el enrutador LVS activo a través de las interfaces de red pública y privada para apagar el demonio **lvs** en el enrutador LVS activo e inicia el demonio **lvs** en el enrutador LVS de respaldo para que acepte solicitudes para los servidores virtuales configurados.

1.6.1. Componentes de la adición de equilibrador de carga

[Sección 1.6.1.1, “pulse”](#) presenta una lista detallada de cada uno de los componentes de software en un enrutador LVS.

1.6.1.1. pulse

Este es el proceso que controla el inicio de los otros demonios relacionados con los enrutadores LVS. Durante el arranque, el demonio es iniciado por el script `/etc/rc.d/init.d/pulse`. Luego lee el archivo de configuración `/etc/sysconfig/ha/lvs.cf`. En el enrutador activo, **pulse** inicia el demonio LVS. En el enrutador de respaldo, **pulse** determina la salud del enrutador activo enviando un mensaje de pulso cada cierto tiempo. Si el enrutador activo no responde, el enrutador de respaldo inicia un proceso de recuperación contra fallos. Durante el proceso de recuperación contra fallos, **pulse** en el enrutador de respaldo ordena al demonio **pulse** en el enrutador activo apagar todos los servicios LVS, iniciar el programa **send_arp** para asignar la dirección IP a la dirección MAC del enrutador de respaldo e iniciar el demonio **lvs**.

1.6.1.2. lvs

El demonio **lvs** se ejecuta en el enrutador LVS activo una vez es llamado por **pulse**. Lee el archivo de configuración `/etc/sysconfig/ha/lvs.cf`, llama a la herramienta **ipvsadm** para construir y mantener la tabla de rutas IPVS y asignar un proceso **nanny** para cada servicio de adición de equilibrador de carga configurado. Si **nanny** reporta que un servidor real ha sido apagado, **lvs** ordena a la herramienta **ipvsadm** remover el servidor real de la tabla de rutas IPVS.

1.6.1.3. ipvsadm

Este servicio actualiza la tabla de rutas IPVS en el kernel. El demonio **lvs** configura y administra la adición de equilibrador de carga llamando **ipvsadm** para añadir o borrar entradas en la tabla de rutas IPVS.

1.6.1.4. nanny

El demonio de sondeo **nanny** es ejecutado en el enrutador LVS activo. A través de este demonio, el enrutador LVS activo determina el estado de cada servidor real y, opcionalmente, sondea sus cargas de trabajo. Se ejecuta un proceso separado para cada servicio definido en cada servidor real.

1.6.1.5. /etc/sysconfig/ha/lvs.cf

Este es el archivo de configuración de adición de equilibrador de carga. Directa o indirectamente, todos los demonios obtienen la información de configuración desde este archivo.

1.6.1.6. Piranha Configuration Tool

Esta es la herramienta de web para monitorizar, configurar y administrar un adición de equilibrador de carga. Es la herramienta predeterminada para mantener el archivo de configuración LVS `/etc/sysconfig/ha/lvs.cf`

1.6.1.7. send_arp

Este programa envía señales ARP cuando la dirección IP de punto flotante cambia de un nodo a otro durante el proceso de recuperación contra fallos.

[Capítulo 2. Configuración inicial de la adición de equilibrador de carga](#) revisa importantes pasos de configuración que se deben realizar después de la instalación y antes de la configuración de Red Hat Enterprise Linux para que sea un enrutador LVS.

Capítulo 2. Configuración inicial de la adición de equilibrador de carga

Después de la instalación de Red Hat Enterprise Linux, se deben ejecutar algunos pasos básicos para configurar los enrutadores LVS y los servidores reales. Este capítulo cubre estos pasos iniciales en detalle.

Nota

El enrutador LVS que se convierte en el nodo activo una vez que la adición de equilibrador de carga se inicia, se conoce también con el nombre de *nodo primario*. Cuando configure una adición de equilibrador de carga, utilice **Piranha Configuration Tool** en el nodo primario.

2.1. Configuración de servicios en los enrutadores LVS

El programa de instalación Red Hat Enterprise Linux instala todos los componentes necesarios para establecer la adición de equilibrador de carga, pero se deben activar los servicios apropiados antes de configurar la adición de equilibrador de carga. Para los dos enrutadores LVS, establezca los servicios apropiados para iniciar un tiempo de arranque. Hay tres herramientas primarias disponibles para configurar servicios para que se activen en el momento de arranque bajo Red Hat Enterprise Linux: el programa para la línea de comandos **chkconfig**, el programa basado en ncurses **ntsysv** y la **Services Configuration Tool** gráfica. Todas estas herramientas requieren acceso de root.

Nota

Para obtener los derechos de root, abra una terminal y utilice el comando **su** - seguido de la contraseña de root. Por ejemplo:

```
$ su - contraseña de root
```

En los enrutadores LVS hay tres servicios que deben ser configurados para que se activen en el tiempo de arranque:

- ▶ El servicio **piranha-gui** (nodo primario solamente)
- ▶ El servicio **pulse**
- ▶ El servicio **sshd**

Si está uniendo servicios multipuertos o utilizando marcas de cortafuegos, debe iniciar también el servicio **iptables**.

Se aconseja activar estos servicios en los niveles de ejecución 3 y 5. Utilice **chkconfig** para llevar a cabo esta tarea. Escriba el siguiente comando para cada servicio:

```
/sbin/chkconfig --level 35 daemon on
```

En el comando anterior, reemplace **daemon** por el nombre del servicio que está activando. Para obtener una lista de servicios en el sistema y ver los niveles de ejecución en los cuales cada servicio será activado, ejecute el siguiente comando:

```
/sbin/chkconfig --list
```



Advertencia

Al activar alguno de los comandos anteriores mediante **chkconfig** no se inicia el demonio. Para esto, utilice el comando **/sbin/service**. Consulte la [Sección 2.3, “Inicio del servicio de la Piranha Configuration Tool”](#) para ver un ejemplo de cómo usar el comando **/sbin/service**.

Para obtener mayor información sobre los niveles de ejecución y la configuración de servicios con **ntsysv** y **Services Configuration Tool**, consulte el capítulo titulado “Control de acceso a servicios” en la *Guía de administración del sistema de Red Hat Enterprise Linux*.

2.2. Configuración de la contraseña para la Piranha Configuration Tool

Antes de usar la **Piranha Configuration Tool** por primera vez en el enrutador LVS primario, cree una contraseña para restringir su acceso. Para ello, inicie una sesión como root y ejecute el siguiente comando:

```
/usr/sbin/piranha-passwd
```

Después de introducir el comando, cree la contraseña administrativa cuando se le indique.



Advertencia

Para que la contraseña sea más segura se deben evitar los nombres propios, acrónimos usados comúnmente o palabras de diccionario en cualquier idioma. No deje la contraseña sin encriptar en ningún lado en el sistema.

Si la contraseña cambia durante una sesión activa de la **Piranha Configuration Tool**, se le preguntará al administrador la nueva contraseña.

2.3. Inicio del servicio de la Piranha Configuration Tool

Después de establecer la contraseña para la **Piranha Configuration Tool**, inicie o reinicie el servicio **piranha-gui** ubicado en **/etc/rc.d/init.d/piranha-gui**. Escriba el siguiente comando como root:

```
/sbin/service piranha-gui start
```

```
o
```

```
/sbin/service piranha-gui restart
```

Al ejecutar este comando se inicia una sesión privada de Apache HTTP Server llamando al enlace simbólico **/usr/sbin/piranha_gui -> /usr/sbin/httpd**. Por razones de seguridad, la versión **piranha-gui** de **httpd** se ejecuta como el usuario **piranha** en un proceso independiente. El hecho de que **piranha-gui** utiliza el servicio **httpd** significa que:

1. El Apache HTTP Server debe estar instalado en el sistema.
2. Si se detiene o reinicia Apache HTTP Server a través del comando **service**, el servicio **piranha-gui** será detenido.



Advertencia

Si se ejecuta el comando `/sbin/service httpd stop` o `/sbin/service httpd restart` en un enrutador LVS, se debe iniciar el servicio **piranha-gui** ejecutando el siguiente comando:
`/sbin/service piranha-gui start`

El servicio **piranha-gui** es todo lo que se necesita para iniciar la configuración de la adición de equilibrador de cargas. Sin embargo, si está configurando la adición de equilibrador de carga en forma remota, también requerirá el servicio **sshd**. No es necesario iniciar el servicio **pulse** antes de que se haya completado la configuración con la **Piranha Configuration Tool**. Consulte la [Sección 4.8, “Inicio de la adición de equilibrador de carga.”](#) para obtener información sobre cómo iniciar el servicio **pulse**.

2.3.1. Configuración del puerto del servidor de red de la Piranha Configuration Tool

La **Piranha Configuration Tool** se ejecuta en el puerto 3636 de forma predeterminada. Para cambiar este número de puerto, cambie la línea **Listen 3636** en la sección 2 del archivo de configuración del servidor web de **piranha-gui** en `/etc/sysconfig/ha/conf/httpd.conf`.

Para utilizar la **Piranha Configuration Tool** necesitará por lo menos un navegador de web en modo texto. Abra el navegador de web del enrutador LVS primario en la URL `http://localhost:3636`. Puede utilizar la **Piranha Configuration Tool** desde cualquier sitio en la red a través de un navegador de red apuntando a la misma URL pero cambiando **localhost** con el nombre de host o dirección IP del enrutador LVS primario.

Cuando su navegador se conecte con la **Piranha Configuration Tool**, usted puede iniciar una sesión para acceder a los servicios de configuración. Introduzca **piranha** en el campo **Nombre de usuario** y la contraseña establecida con **piranha-passwd** en el campo **Contraseña**.

Ahora que la **Piranha Configuration Tool** está en ejecución, es aconsejable limitar el acceso a la herramienta a través de la red. La siguiente sección muestra varias maneras de llevar a cabo esta tarea.

2.4. Limitar el acceso a la Piranha Configuration Tool

La **Piranha Configuration Tool** solicita un nombre de usuario y una contraseña válidas. Sin embargo, ya que todos los datos pasados a la **Piranha Configuration Tool** son en texto plano, se recomienda restringir el acceso a todos aquellos que no sean parte de la red confiada o de la máquina local.

La manera más sencilla de restringir el acceso es utilizando el mecanismo de control de acceso incluido en Apache HTTP Server. Esto se logra editando el archivo `/etc/sysconfig/ha/web/secure/.htaccess`. Tras la modificación de este archivo no es necesario reiniciar el servicio **piranha-gui** porque el servidor revisa el archivo `.htaccess` cada vez que se accede al directorio.

Por defecto, el control de acceso para este directorio permite a todos ver el contenido del directorio. El acceso predeterminado es similar a:

```
Order deny,allow
Allow from all
```

Para que solo la máquina local tenga acceso a la **Piranha Configuration Tool**, cambie el archivo `.htaccess` para permitir únicamente el acceso desde el dispositivo de bucle (127.0.0.1). Para mayor información sobre *Red Hat Enterprise Linux Reference Guide* o sobre este dispositivo, vea el capítulo

titulado *Scripts de red* en *Red Hat Enterprise Linux Reference Guide*.

```
Order deny,allow
Deny from all
Allow from 127.0.0.1
```

También se puede permitir el acceso a host específicos o subredes como se muestra en este ejemplo:

```
Order deny,allow
Deny from all
Allow from 192.168.1.100
Allow from 172.16.57
```

En este ejemplo, solo los navegadores de web desde la máquina con la dirección IP de 192.168.1.100 y máquinas en la red 172.16.57/24 tienen acceso a la **Piranha Configuration Tool**.



Advertencia

La edición del archivo **.htaccess** de la **Piranha Configuration Tool** limita el acceso a las páginas de configuración en el directorio `/etc/sysconfig/ha/web/secure/` pero no la página de inicio de sesión y las páginas de ayuda en `/etc/sysconfig/ha/web/`. Para limitar el acceso a este directorio, cree un archivo **.htaccess** en el directorio `/etc/sysconfig/ha/web/` con las líneas **order**, **allow** y **deny** idénticas a `/etc/sysconfig/ha/web/secure/.htaccess`.

2.5. Activación de reenvío de paquetes

Para que el enrutador LVS reenvíe paquetes de red de forma apropiada al servidor real, cada enrutador LVS debe tener activo el reenvío de paquetes en el kernel. Inicie una sesión como root y cambie la línea que dice `net.ipv4.ip_forward = 0` en `/etc/sysctl.conf` para que lea:

```
net.ipv4.ip_forward = 1
```

Los cambios surten efecto cuando reinicie el sistema.

Para revisar si el reenvío de IP está activado, ejecute el siguiente comando como root:

```
/sbin/sysctl net.ipv4.ip_forward
```

Si el siguiente comando retorna **1**, el reenvío de IP está activo. Si retorna **0**, puede activarlo manualmente utilizando el siguiente comando:

```
/sbin/sysctl -w net.ipv4.ip_forward=1
```

2.6. Configuración de servicios en servidores reales

Si los servidores reales son sistemas Red Hat Enterprise Linux, establezca los demonios de servidores apropiados para activarlos durante el tiempo de inicio. Estos demonios incluyen **httpd** para servicios web o **xinetd** para servicios FTP o Telnet.

Podría ser útil tener acceso remoto a los servidores reales, para ello el demonio **sshd** debe estar instalado y en ejecución.

Capítulo 3. Configuración de una adición de equilibrador de carga

Una adición de equilibrador de carga consta de dos grupos básicos: el enrutador LVS y los servidores reales. Para prevenir las fallas por un único elemento, cada grupo debe tener al menos dos sistemas miembros.

El grupo de enrutadores LVS consta de dos sistemas idénticos o muy similares que ejecutan Red Hat Enterprise Linux. Uno de ellos actúa como el enrutador LVS activo y el otro permanece en espera. Por este motivo, los dos sistemas necesitan tener las mismas capacidades.

Antes de escoger y configurar el hardware para el grupo de servidores reales, se debe elegir una de las tres topologías de la adición de Equilibrador de carga que se pueden usar.

3.1. La red de adición de equilibrador de carga de NAT

La topología NAT permite gran flexibilidad en el uso de hardware existente, pero su habilidad para manejar grandes cargas es limitada debido a que todos los paquetes van y vienen a través del enrutador de adición de equilibrador de carga.

Capas de red

La topología para una adición de equilibrador de enrutamiento que utiliza NAT es la más fácil de configurar desde la perspectiva de las capas de red porque solo necesita un único acceso a la red pública. Los servidores reales pasan todas las respuestas al enrutador LVS, por lo cual, los servidores reales están en su propia red privada.

Hardware

La topología NAT es la más flexible en cuando al hardware porque los servidores reales no necesitan ser máquinas Linux para funcionar correctamente en el cluster. En un cluster NAT, cada servidor real solo necesita un NIC ya que responderá únicamente al enrutador LVS. El enrutador LVS, en cambio, necesita dos NIC para encaminar el tráfico entre las dos redes. Como esta topología crea un cuello de botella en el enrutador LVS, las NIC de ethernet con un gigabit pueden ser empleadas en cada enrutador LVS para incrementar el ancho de banda que los enrutadores LVS pueden manejar. Si Ethernet de un gigabit es utilizado en el enrutador LVS, cada interruptor que conecta los servidores reales con el enrutador LVS debe tener puertos con al menos dos gigabit de Ethernet para manejar efectivamente la carga.

Software

Ya que la topología NAT requiere el uso de **iptables** para algunas configuraciones, hay una cantidad considerable de configuración de software que debe hacerse fuera de la **Piranha Configuration Tool**. En particular, los servicios FTP y el uso de marcas de cortafuego requieren una configuración manual extra en los enrutadores LVS para que encaminen las solicitudes apropiadamente.

3.1.1. Configuración de las interfaces de red para una adición de equilibrador de carga con NAT

Para configurar una adición de equilibrador de carga LVS con NAT, el administrador debe configurar primero las interfaces de red para la red pública y la red privada en los enrutadores LVS. En este

ejemplo, la interfaz de red pública del enrutador LVS (**eth0**) estará en la red 192.168.26/24 (tenga en cuenta de que éste es solo un ejemplo, ésta no es una IP encaminable) y la interfaz privada que se conecta con los servidores reales (**eth1**) estará en la red 10.11.12/24.

Así en el enrutador LVS *primario* o activo, el script de red de la interfaz pública, `/etc/sysconfig/network-scripts/ifcfg-eth0`, se asemeja a:

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.26.9
NETMASK=255.255.255.0
GATEWAY=192.168.26.254
```

El `/etc/sysconfig/network-scripts/ifcfg-eth1` para la interfaz NAT privada en el enrutador LVS se asemeja a:

```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
IPADDR=10.11.12.9
NETMASK=255.255.255.0
```

En este ejemplo, el VIP para la interfaz pública del enrutador LVS será 192.168.26.10 y el VIP para la NAT o interfaz privada será 10.11.12.10. Por lo cual, es esencial que los servidores reales envíen la solicitud de regreso a la VIP para la interfaz NAT.



Importante

La configuración de la interfaz Ethernet de ejemplo establecida en esta sección es para las direcciones IP reales de un enrutador LVS y *no* para las direcciones IP flotantes. Para configurar las direcciones IP flotantes privada y pública, el administrador debe utilizar la **Piranha Configuration Tool** como se muestra en la [Sección 4.4, “GLOBAL SETTINGS”](#) y en la [Sección 4.6.1, “Subsección SERVIDOR VIRTUAL”](#).

Después de configurar las interfaces de red del enrutador LVS primario, configure las interfaces de red real del enrutador LVS de respaldo — se debe tener en cuenta que ninguna de las direcciones IP entren en conflicto con cualquier otra dirección IP en la red.



Importante

Asegúrese de que cada interfaz en el nodo de respaldo sirva la misma red que la interfaz en el nodo primario. Por ejemplo, si eth0 se conecta a la red pública en el nodo primario, debe conectarse a la red pública en el nodo de respaldo.

3.1.2. Rutas en los servidores reales

Es importante recordar que al configurar las interfaces de red de los servidores reales en una topología NAT, se debe establecer la puerta de enlace para la dirección IP flotante NAT del enrutador LVS. En este ejemplo, la dirección sería 10.11.12.10.



Nota

Una vez las interfaces de red están activas en los servidores reales, las máquinas no se podrán conectar de otras formas a la red pública. Esto es normal. Podrá, sin embargo, ser capaz de enviar un ping al IP real para la interfaz privada del enrutador LVS, en este caso 10.11.12.8.

El archivo `/etc/sysconfig/network-scripts/ifcfg-eth0` del servidor real podría asemejarse a:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=10.11.12.1
NETMASK=255.255.255.0
GATEWAY=10.11.12.10
```



Advertencia

Si un servidor real tiene más de una interfaz de red configurada con la línea **GATEWAY=**, la primera en activarse será la puerta de enlace. Por ello, si tanto **eth0** y **eth1** están configurados y **eth1** es utilizado por la adición de equilibrador de enrutamiento, los servidores reales no encaminarán las solicitudes apropiadamente.

Lo mejor es apagar las interfaces de red extrañas estableciendo **ONBOOT=no** en el script de red dentro del directorio `/etc/sysconfig/network-scripts/` o asegúrese de que la puerta de enlace sea establecida correctamente en la interfaz que se active de primeras.

3.1.3. Activación de rutas NAT en enrutadores LVS

En una configuración sencilla de adición de equilibrador de enrutamiento con NAT en la cual cada servicio en cluster utiliza un solo puerto, como HTTP en el puerto 80, el administrador solo necesita activar el reenvío de paquetes en los enrutadores LVS para que las solicitudes sean correctamente encaminadas entre el mundo exterior y los servidores reales. Consulte la [Sección 2.5, “Activación de reenvío de paquetes”](#) para obtener instrucciones sobre cómo activar el reenvío de paquetes. Sin embargo, una configuración más avanzada será necesaria si los servicios de cluster requieren más de un puerto para ir al mismo servidor real durante una sesión de usuario. Para obtener mayor información sobre cómo crear servicios con varios puertos, utilizando marcas de cortafuegos, consulte la [Sección 3.4, “Servicios de puertos múltiples y Adición de equilibrador de carga”](#).

Una vez el reenvío es activado en los enrutadores LVS y los servidores reales están activos y tienen los servicios de cluster en ejecución, utilice la **Piranha Configuration Tool** para configurar la adición de equilibrador de enrutado como se muestra en el [Capítulo 4, Configuración de la adición de equilibrador de carga con Piranha Configuration Tool](#).



Advertencia

No configure el IP flotante para **eth0:1** o **eth1:1** editando de forma manual los scripts de red o utilizando una herramienta de configuración de red. En su lugar, utilice la **Piranha Configuration Tool** como se muestra en la [Sección 4.4, “GLOBAL SETTINGS”](#) y en la [Sección 4.6.1, “Subsección SERVIDOR VIRTUAL”](#).

Cuando finalice, inicie el servicio **pulse** como se muestra en la [Sección 4.8, “Inicio de la adición de equilibrador de carga”](#). Una vez **pulse** esté en ejecución, el enrutador LVS activo iniciará enrutando las

solicitudes al grupo de servidores reales.

3.2. Adición de equilibrador de carga con enrutamiento directo

Como se mencionó en la [Sección 1.4.2, “Enrutado directo”](#), el enrutamiento directo permite que los servidores reales procesen y encaminen los paquetes directamente al usuario que los solicitó y no al enrutador LVS. El enrutado directo requiere que los servidores reales estén físicamente conectados al segmento de red con el enrutador LVS y que sean capaces de procesar y dirigir paquetes de salida.

Capas de red

En una configuración la adición de equilibrador de enrutamiento directo, el enrutador LVS necesita recibir las solicitudes entrantes y encaminarlas al servidor real apropiado para que sean procesadas. Los servidores reales necesitan luego encaminar *directamente* la respuesta al cliente. Por ejemplo, si el cliente está en internet y envía el paquete a través del enrutador LVS al servidor real, éste debe ser capaz de dirigirse directamente al cliente a través de Internet. Esta tarea puede llevarse a cabo configurando una puerta de enlace para que el servidor real pase paquetes a Internet. Cada servidor real en el grupo de servidores puede tener su propia puerta de enlace separada (y cada puerta de enlace con su propia conexión a Internet), permitiendo una mayor tasa de transferencia y escalabilidad. Sin embargo, para configuraciones LVS típicas, los servidores reales pueden comunicarse a través de una puerta de enlace (y una conexión de red).



Importante

No se recomienda utilizar un enrutador LVS como puerta de enlace para los servidores reales ya que esto conllevaría innecesarias complejidades de configuración y cargas de red en el enrutador LVS. Además, el cuello de botella del enrutado NAT que se trataba de evitar es introducido nuevamente.

Hardware

Los requerimientos de hardware de un sistema de adición de equilibrador de enrutamiento que utiliza enrutamiento directo es similar a otras topologías LVS. Aunque el enrutador LVS debe ejecutar Red Hat Enterprise Linux para procesar la solicitud entrante y ejecutar balance de carga para los servidores reales, los servidores reales no necesitan ser máquinas Linux para funcionar correctamente. Los enrutadores LVS necesitan uno o dos NIC cada uno (dependiendo de si hay un enrutador de respaldo). Puede utilizar dos NIC para facilitar la configuración y para separar el tráfico — las solicitudes entrantes son manejadas por un NIC y los paquetes encaminados al servidor real por el otro.

Ya que los servidores reales evitan el enrutador LVS y envían los paquetes salientes directamente al cliente, se requiere una puerta de enlace a Internet. Para alcanzar máximo rendimiento y disponibilidad, cada servidor real puede estar conectado a su propia ruta de enlace. Ésta tiene su propia conexión dedicada a la red en la cual el cliente está conectado (por ejemplo, Internet o Intranet).

Software

Hay alguna configuración fuera de la **Piranha Configuration Tool**, la cual requiere que se realice, especialmente para los administradores que afrontan problemas con ARP cuando utilizan una adición de equilibrador de carga con enrutamiento directo. Consulte la [Sección 3.2.1, “Enrutado directo y arptables_jf”](#) o la [Sección 3.2.2, “Enrutado directo e](#)

[iptables](#)” para obtener mayor información.

3.2.1. Enrutado directo y `arptables_jf`

Para configurar el enrutamiento directo con `arptables_jf`, cada servidor real debe tener su propia dirección IP virtual configurada para que puedan encaminar paquetes. Las solicitudes ARP para el VIP son ignoradas completamente por los servidores reales y cualquier paquete ARP que normalmente contendrían la VIP son transformados para que contengan el IP del servidor real en vez de la VIP.

Al usar el método `arptables_jf`, las aplicaciones podrían vincularse a cada VIP o puerto que el servidor real esté sirviendo. Por ejemplo, el método `arptables_jf` permite la ejecución de múltiples instancias de Apache HTTP Server vinculadas explícitamente a diferentes VIP del sistema. Hay también varias ventajas de rendimiento cuando se utiliza `arptables_jf` en vez de `iptables`.

Sin embargo, al utilizar el método `arptables_jf` no se puede configurar las VIP para que sean iniciadas durante el arranque con las herramientas de configuración estándar de Red Hat Enterprise Linux.

Para configurar cada servidor real para ignorar las solicitudes ARP para cada una de las direcciones IP virtuales, ejecute los siguientes pasos:

1. Cree las entradas ARP para cada dirección IP virtual en cada servidor real (el `real_ip` es el IP que el nodo director utiliza para comunicarse con el servidor real; frecuentemente es el IP vinculado a `eth0`):

```
arptables -A IN -d <virtual_ip> -j DROP
arptables -A OUT -s <virtual_ip> -j mangle --mangle-ip-s <real_ip>
```

Esto hará que los servidores reales ignoren todas las solicitudes ARP para la dirección IP virtual y cambia el IP virtual con el IP real en cualquier solicitud ARP saliente. El único servidor que debe responder a solicitudes ARP para cualquier VIP es el nodo LVS activo.

2. Una vez esta tarea ha sido completada en cada servidor real, grabe las entradas ARP escribiendo el siguiente comando en cada servidor real:

```
service arptables_jf save
chkconfig --level 2345 arptables_jf on
```

El comando `chkconfig` hará que el sistema recargue la configuración de `arptables` durante el periodo de arranque — antes de iniciar la red.

3. Configure la dirección IP Virtual en todos los servidores reales con `ifconfig` para crear un alias IP. Por ejemplo:

```
# ifconfig eth0:1 192.168.76.24 netmask 255.255.252.0 broadcast
192.168.79.255 up
```

O mediante la herramienta `iproute2 ip`, por ejemplo:

```
# ip addr add 192.168.76.24 dev eth0
```

Como se mencionó anteriormente las direcciones IP virtuales no pueden ser configuradas para ser iniciadas durante el arranque con las herramientas de configuración de Red Hat. Para solucionar este inconveniente, ubique estos comandos en `/etc/rc.d/rc.local`.

4. Configure Piranha para enrutamiento directo. Consulte el [Capítulo 4. Configuración de la adición de equilibrador de carga con Piranha Configuration Tool](#) para obtener mayor información.

3.2.2. Enrutado directo e iptables

También se puede solucionar este problema de ARP utilizando el método de enrutamiento directo a través de reglas de cortafuegos de **iptables**. Para configurar el enrutamiento directo con **iptables**, debe añadir reglas que creen un proxy transparente para que el servidor real sirva paquetes enviados a la dirección VIP aunque ésta no exista en el sistema.

El método con **iptables** es más sencillo de configurar que el método con **arptables_jf**. Este método también sorteaba el problema de ARP de LVS en su totalidad porque las direcciones IP virtuales solo existen en el nodo director LVS activo.

Sin embargo, el método con **iptables** presenta algunas desventajas de rendimiento en comparación con **arptables_jf** porque hay sobrecarga en el enmascaramiento y reenvío de cada paquete.

Tampoco se pueden reusar los puertos cuando se utiliza el método con **iptables**. Por ejemplo, no es posible ejecutar dos servicios Apache HTTP Server separados vinculados al puerto 80 porque ambos deben estar vinculados a una instancia de **INADDR_ANY** de las direcciones IP virtuales.

Para configurar el enrutamiento directo utilizando **iptables**, ejecute los siguientes pasos:

1. En cada servidor real, ejecute los siguientes comandos para cada combinación de VIP, puerto y protocolo (TCP o UDP) que será servido por el servidor real:

```
iptables -t nat -A PREROUTING -p <tcp|udp> -d <vip> --dport <port> -j REDIRECT
```

Este comando hará que el servidor real procese paquetes destinados para el VIP y puertos dados.

2. Guarde la configuración en cada servidor real:

```
# service iptables save  
# chkconfig --level 2345 iptables on
```

Los comandos anteriores hacen que el sistema recargue la configuración de **iptables** durante el arranque — antes de iniciar la red.

3.3. Cómo armar la configuración

Después de determinar cuál de los métodos de enrutamiento anteriores será usado, el hardware deberá vincularse en la red.



Importante

El adaptador en el enrutador LVS debe ser configurado para acceder a la misma red. Por ejemplo, si **eth0** se conecta a la red pública y **eth1** se conecta a la red privada, entonces los mismos dispositivos en el enrutador LVS de respaldo deben conectarse a las mismas redes. Asimismo, la puerta de enlace listada en la primera interfaz a activar durante el periodo de arranque se añade a la tabla de enrutamiento; las siguientes puertas de enlace listadas en otras interfaces se omiten. Es importante considerar este comportamiento en la configuración de los servidores reales.

Después de conectar físicamente el hardware, configure las interfaces de red en los enrutadores LVS primario y de respaldo. Esta tarea puede llevarse a cabo a través de **system-config-network** o editando los scripts manualmente. Para mayor información sobre la adición de dispositivos con **system-config-network**, consulte el capítulo titulado *Configuración de red* en la *Guía de implementación de*

Red Hat Enterprise Linux. En la parte restante de este capítulo, las alteraciones de las interfaces de red se realizan manualmente o a través de la **Piranha Configuration Tool**.

3.3.1. Consejos generales para la red de una adición de equilibrador de carga

Configure las direcciones IP reales para las redes públicas y privadas en los enrutadores LVS antes de intentar configurar una adición de equilibrador de carga mediante la **Piranha Configuration Tool**. La sección para cada topología da direcciones de red de ejemplo, pero se necesitan direcciones de red verdaderas en una configuración real. Abajo hay algunos comandos útiles para activar las interfaces de red y revisar el estado.

Activación de las interfaces de red

Para activar una interfaz de red real, utilice el siguiente comando como root, reemplazando **N** con el número correspondiente de la interfaz (**eth0** y **eth1**).

```
/sbin/ifup ethN
```



Advertencia

No utilice scripts **ifup** para activar las direcciones IP flotantes configuradas a través de la **Piranha Configuration Tool** (**eth0:1** o **eth1:1**). En su lugar, utilice el comando **service** para iniciar **pulse** (consulte la [Sección 4.8, "Inicio de la adición de equilibrador de carga"](#) para obtener mayor información).

Desactivación de las interfaces de red reales

Para desactivar una interfaz de red real, utilice el siguiente comando como root, reemplace **N** con el número correspondiente de la interfaz (**eth0** y **eth1**).

```
/sbin/ifdown ethN
```

Revisión del estado de las interfaces de red

Si necesita revisar cuáles interfaces de red están activas en un momento dado, escriba:

```
/sbin/ifconfig
```

Para ver la tabla de rutas para una máquina, ejecute el siguiente comando:

```
/sbin/route
```

3.4. Servicios de puertos múltiples y Adición de equilibrador de carga

Los enrutadores LVS bajo cualquier topología requieren configuración adicional cuando se crean servicios de adición de equilibrador de carga de múltiples puertos. Los servicios de múltiples puertos pueden ser creados artificialmente con marcas de cortafuegos para agrupar diferentes protocolos relacionados, como HTTP (puerto 80) y HTTPS (puerto 443), o cuando LVS se utiliza con protocolos de múltiples puertos tales como FTP. En cualquier caso, el enrutador LVS utiliza marcas de cortafuegos para reconocer que los paquetes destinados a diferentes puertos, pero con las mismas marcas de cortafuegos, deben ser manejados de la misma forma. Asimismo, cuando se utilizan con persistencia,

las marcas de cortafuegos garantizan que la conexión desde las máquinas clientes sean enrutadas al mismo host, siempre y cuando las conexiones se presenten dentro del tiempo especificado por el parámetro de persistencia. Para obtener mayor información sobre cómo asignar el valor de persistencia en el servidor virtual, consulte la [Sección 4.6.1, “Subsección SERVIDOR VIRTUAL”](#).

Lamentablemente, el mecanismo utilizado para balancear cargas en los servidores reales — IPVS — puede reconocer marcas de cortafuegos asignadas al paquete, pero no puede asignar marcas de cortafuegos. El trabajo de *asignar* marcas de cortafuegos debe ser llevado a cabo por el filtro de paquetes de red, **iptables** por fuera de la **Piranha Configuration Tool**.

3.4.1. Asignación de marcas de cortafuegos

Para asignar marcas de cortafuegos a un paquete destinado a un puerto particular, el administrador debe utilizar **iptables**.

Esta sección ilustra cómo agrupar, HTTP y HTTPS; sin embargo, FTP es otro protocolo común de múltiples puertos que se utiliza en agrupamientos. Si una adición de equilibrador de carga es utilizada para servicios FTP, consulte la [Sección 3.5, “Configuración de FTP”](#) para obtener más información.

La regla básica a recordar cuando se utilizan marcas de cortafuegos es que cada protocolo que utiliza una marca de cortafuego en la **Piranha Configuration Tool** debe tener una regla **iptables** proporcional para asignar las marcas de cortafuegos a los paquetes de red.

Antes de crear reglas de filtros de paquetes de red, asegúrese de que no haya aun reglas previamente establecidas. Para ello, abra una terminal, inicie una sesión de root y escriba:

```
/sbin/service iptables status
```

Si **iptables** no está en ejecución, la línea de comandos reaparecerá inmediatamente.

Si **iptables** está activo, se mostrarán las reglas que están siendo usadas. Si hay alguna regla, escriba el siguiente comando:

```
/sbin/service iptables stop
```

Si las reglas actuales son importantes, revise el contenido de **/etc/sysconfig/iptables** y guarde cualquier regla importante antes de proceder.

Abajo hay algunas reglas que asignan la misma marca de cortafuego, 80, al tráfico entrante para la dirección IP flotante **n.n.n.n** en el puerto 80 y 443.

```
/sbin/modprobe ip_tables
```

```
/sbin/iptables -t mangle -A PREROUTING -p tcp -d n.n.n.n/32 --dport 80 -j  
MARK --set-mark 80
```

```
/sbin/iptables -t mangle -A PREROUTING -p tcp -d n.n.n.n/32 --dport 443 -j  
MARK --set-mark 80
```

Para obtener instrucciones sobre cómo asignar el VIP a la interfaz de red pública, consulte la [Sección 4.6.1, “Subsección SERVIDOR VIRTUAL”](#). Note que se puede iniciar una sesión como root y cargar el módulo para **iptables** antes de establecer reglas por primera vez.

En los comandos **iptables**, reemplace **n.n.n.n** con el IP flotante para sus servidores virtuales HTTP y HTTPS. Estos comandos tienen el efecto de asignar una marca de cortafuegos 80 a cualquier tráfico dirigido a la VIP en los puertos apropiados. Esta marca es reconocida por el IPVS y enviada apropiadamente.



Advertencia

El comando tendrá efecto inmediato, pero no persistirá tras el reinicio del sistema. Para asegurarse de que los filtros de paquetes establecidos sean restaurados después del reinicio, consulte la [Sección 3.6, “Cómo guardar los parámetros de filtro de paquetes de red”](#).

3.5. Configuración de FTP

FTP (siglas en inglés de File Transport Protocol) es un protocolo de múltiples puertos que presenta un conjunto de retos para un entorno de una adición de equilibrador de carga. Para entender la naturaleza de estos retos, se debe entender primero algunos conceptos claves sobre cómo funciona FTP.

3.5.1. Cómo funciona FTP

Como en la mayoría de servicios entre cliente y servidor, el cliente abre una conexión en el servidor en un puerto particular y el servidor le responde al cliente utilizando ese mismo puerto. Cuando un cliente FTP se conecta a un servidor FTP, el primero abre una conexión FTP de control en el puerto 21. Luego el *cliente* le informa al *servidor* FTP si la conexión debe ser *activa* o *pasiva*. El tipo de conexión elegida por el cliente determina cómo responde el servidor y en qué puerto la transacción ocurre.

Los dos tipos de conexiones de datos son:

Conexiones activas

Cuando se establece una conexión activa, el *servidor* abre una conexión de datos para el cliente desde el puerto 20 a un puerto de rango más alto en la máquina cliente. Todos los datos provenientes del servidor pasan por esta conexión.

Conexiones pasivas

Cuando una conexión pasiva se establece, el *cliente* solicita al servidor FTP establecer un puerto de conexión pasiva (el cual puede ser un puerto superior a 10.000). El servidor se vincula con el puerto para esta sesión particular y envía ese número de puerto de regreso al cliente. El cliente abre el puerto para la conexión de datos. Cada solicitud de datos resulta en una conexión de datos diferente. La mayoría de clientes FTP intenta establecer una conexión pasiva cuando solicitan datos al servidor.



Nota

El *cliente* determina el tipo de conexión, no el servidor. Esto quiere decir que se debe configurar el enrutador LVS para manejar tanto conexiones pasivas como activas. La relación entre cliente y servidor en FTP puede potencialmente abrir una larga cantidad de puertos que no serán detectados por la **Piranha Configuration Tool** y IPVS.

3.5.2. Cómo afecta al enrutamiento de una adición de equilibrador de carga

El reenvío de paquetes solo permite conexiones entrantes y salientes del cluster basado en el reconocimiento del número de puerto o la marca de cortafuegos. Si un cliente externo al cluster intenta abrir un puerto IPVS que no está configurado para ser manejado, la conexión es ignorada. Asimismo, si el servidor real intenta abrir una conexión de regreso a internet en un puerto IPVS que no está

configurado, la conexión es ignorada. Esto significa que *todas* las conexiones de los clientes FTP en internet *deben* tener la misma marca de cortafuegos asignados a ellos y todas las conexiones desde el servidor *deben* ser apropiadamente reenviadas a internet usando reglas de filtros de paquetes de red.

3.5.3. Creación de reglas de filtro de paquetes de red

Antes de asignar cualquier regla de **iptables** para los servicios FTP, revise la información en la [Sección 3.4.1, “Asignación de marcas de cortafuegos”](#) concerniente a los servicios de múltiples puertos y las técnicas para revisar las reglas de filtros de paquetes de red existentes.

A continuación se muestran las reglas que asignan la misma marca de cortafuegos, 21, al tráfico FTP. Para que esas reglas funcionen apropiadamente, usted debe también utilizar la subsección **VIRTUAL SERVER** de la **Piranha Configuration Tool** para configurar un servidor virtual para el puerto 21 con un valor de **21** en el campo **Marca de cortafuegos**. Consulte la [Sección 4.6.1, “Subsección SERVIDOR VIRTUAL”](#) para obtener mayor información.

3.5.3.1. Reglas para conexiones activas

Las reglas para las conexiones activas le dicen al kernel que acepte y envíe conexiones que vienen de la dirección IP flotante *interna* en el puerto 20 — el puerto de datos FTP.

El siguiente comando de **iptables** permite que el enrutador LVS acepte conexiones salientes desde el servidor real que IPVS no conoce:

```
/sbin/iptables -t nat -A POSTROUTING -p tcp -s n.n.n.0/24 --sport 20 -j MASQUERADE
```

En el comando **iptables**, *n.n.n* debe ser remplazado con los primeros tres valores para el IP flotante para la interfaz de red interna de la interfaz NAT definida en el panel **GLOBAL SETTINGS** de la **Piranha Configuration Tool**.

3.5.3.2. Reglas para las conexiones pasivas

Las reglas para las conexiones pasivas asignan la marca d cortafuegos apropiada a conexiones entrantes desde internet al IP flotante para el servicio en una amplia gama de puertos — 10.000 a 20.000.



Advertencia

Si está limitando el rango de puertos para las conexiones pasivas, debe configurar también el servidor VSFTP para utilizar un rango de puerto coincidente. Esto puede llevarse a cabo si se añaden las siguientes líneas a **/etc/vsftpd.conf**:

```
pasv_min_port=10000
```

```
pasv_max_port=20000
```

Debe controlar también la dirección que el servidor muestra al cliente para las conexiones FTP pasivas. En un sistema de una adición de equilibrador con enrutamiento NAT, añada la siguiente línea a **/etc/vsftpd.conf** para sobrescribir la dirección IP del servidor real al VIP, la cual es la que el cliente ve tras la conexión. Por ejemplo:

```
pasv_address=n.n.n.n
```

Remplace *n.n.n.n* por la dirección VIP del sistema LVS.

Para configuraciones de otros servidores FTP, consulte la documentación respectiva.

Este rango debe ser suficiente para la mayoría de casos; sin embargo, este número puede ser incrementado para incluir todos los puertos no seguros disponibles si se cambia **10000:20000** en el

comando anterior a **1024:65535**.

El siguiente comando de **iptables** tiene el efecto de asignar una marca de cortafuegos de 21 a cualquier tráfico dirigido al IP flotante en los puertos apropiados. Esta marca es reconocida por IPVS y redirigida apropiadamente:

```
/sbin/iptables -t mangle -A PREROUTING -p tcp -d n.n.n.n/32 --dport 21 -j MARK --set-mark 21
```

```
/sbin/iptables -t mangle -A PREROUTING -p tcp -d n.n.n.n/32 --dport 10000:20000 -j MARK --set-mark 21
```

En los comandos **iptables**, *n.n.n.n* debe ser remplazado por el IP flotante para el servidor FTP virtual definido en la subsección **VIRTUAL SERVER** de la **Piranha Configuration Tool**.



Advertencia

El efecto de los comandos anteriores es inmediato, pero no persiste después de que el sistema es reiniciado. Para asegurar que los parámetros de filtro de paquetes de red sean iniciados después reiniciar el sistema, consulte la [Sección 3.6, “Cómo guardar los parámetros de filtro de paquetes de red”](#).

Finalmente, asegúrese de que los servicios apropiados están activos en los niveles de ejecución apropiados. Para mayor información sobre esto, consulte la [Sección 2.1, “Configuración de servicios en los enrutadores LVS”](#).

3.6. Cómo guardar los parámetros de filtro de paquetes de red

Después de configurar los filtros de paquetes de red apropiados para su situación, guarde la configuración para que se pueda restaurar tras el reinicio del equipo. Para **iptables**, escriba el siguiente comando:

```
/sbin/service iptables save
```

Así guarda la configuración en **/etc/sysconfig/iptables** para que sea llamada durante el periodo de arranque.

Una vez el archivo ha sido escrito, se puede usar el comando **/sbin/service** para iniciar, detener o revisar el estado de **iptables**. **/sbin/service** cargará de forma automática el módulo apropiado. Por obtener un ejemplo de cómo utilizar el comando **/sbin/service**, consulte la [Sección 2.3, “Inicio del servicio de la Piranha Configuration Tool”](#).

Finalmente, deberá asegurarse de que el servicio apropiado sea establecido a activo en los niveles de ejecución relevantes. Para mayor información consulte la [Sección 2.1, “Configuración de servicios en los enrutadores LVS”](#).

El siguiente capítulo explica cómo utilizar la **Piranha Configuration Tool** para configurar el enrutador LVS y describe los pasos necesarios para activar la Adición de equilibrador de carga.

Capítulo 4. Configuración de la adición de equilibrador de carga con Piranha Configuration Tool

La **Piranha Configuration Tool** proporciona un enfoque estructurado para crear el archivo de configuración necesario para una adición de equilibrador de carga — `/etc/sysconfig/ha/lvs.cf`. Este capítulo describe la operación básica de la **Piranha Configuration Tool** y cómo activar la adición de equilibrador de carga una vez la configuración haya sido completada.



Importante

El archivo de configuración para la adición de equilibrador de carga obedece estrictas reglas de formato. El uso de la **Piranha Configuration Tool** evita errores de sintaxis en el archivo `lvs.cf` y previene así fallas en el software.

4.1. Software necesario

El servicio **piranha-gui** debe ser ejecutado en el enrutador LVS primario para utilizar la **Piranha Configuration Tool**. Para configurar la adición de equilibrador de carga se necesita al menos un navegador de web en formato de texto (por ejemplo **links**). Si está accediendo al enrutador LVS desde otra máquina, también se necesitará una conexión **ssh** como usuario **root** al enrutador LVS primario.

Mientras se configura el enrutador LVS primario, es buena idea mantener una conexión **ssh** en una terminal. Esta conexión brinda la oportunidad de reiniciar **pulse** y otros servicios, configurar el filtro de paquetes de red y sondear `/var/log/messages` durante el periodo de solución de errores.

Las siguientes cuatro secciones presentan cada una de las páginas de configuración de la **Piranha Configuration Tool** y dan instrucciones sobre cómo utilizar la aplicación para configurar una adición de equilibrador de carga.

4.2. Inicio de sesión en la Piranha Configuration Tool

Para configurar una adición de equilibrador de carga se debe siempre iniciar la configuración del enrutador primario con la **Piranha Configuration Tool**. Para ello, verifique que el servicio **piranha-gui** está en ejecución y que se ha establecido una contraseña administrativa tal y como se describió en la [Sección 2.2, “Configuración de la contraseña para la Piranha Configuration Tool”](#).

Si está accediendo a la máquina de forma local, puede abrir `http://localhost:3636` en un navegador de web para acceder a la **Piranha Configuration Tool**. Para acceder remotamente utilice el nombre de host o la dirección IP real del servidor seguido del número de puerto `:3636`. Una vez el navegador se haya conectado, se verá la pantalla de la [Figura 4.1, “Panel de bienvenida”](#).

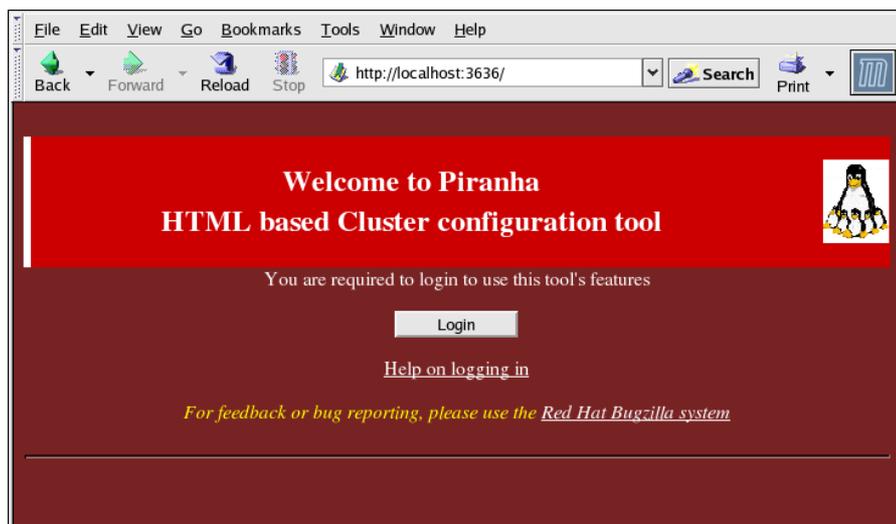


Figura 4.1. Panel de bienvenida

Haga clic en el botón **Login** e ingrese **piranha** en el campo **Username** y la contraseña administrativa previamente creada en el campo **Password**.

La **Piranha Configuration Tool** está formada de cuatro pantallas principales o *paneles*. Además, el panel **Virtual Servers** contiene cuatro *subsecciones*. El panel **CONTROL/MONITORING** es el primer panel después de la pantalla de entrada.

4.3. CONTROL/MONITORING

El panel **CONTROL/MONITORING**, presenta un estado de ejecución limitado de la adición de equilibrador de carga. Muestra el estado del demonio **pulse**, la tabla de rutas LVS y los procesos **nanny** creados por LVS.



Nota

Los campos **CURRENT LVS ROUTING TABLE** y **CURRENT LVS PROCESSES** permanecen en blanco hasta que se inicie la adición de equilibrador de carga tal y como se muestra en la [Sección 4.8, "Inicio de la adición de equilibrador de carga"](#).

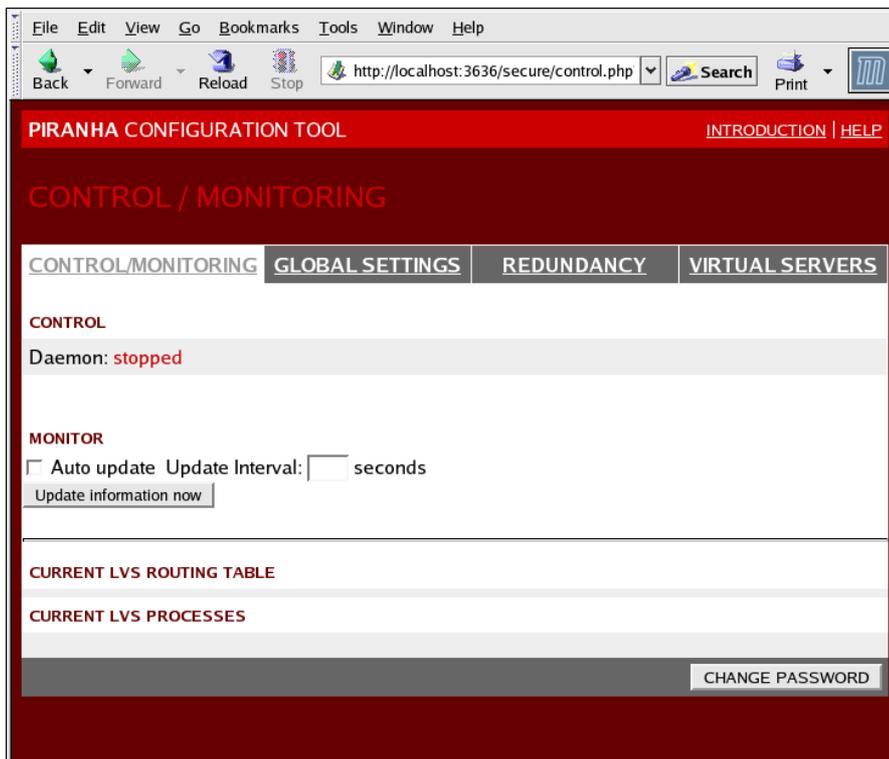


Figura 4.2. El panel CONTROL/MONITORING

Auto update

El estado que se muestra en esta página puede ser actualizado automáticamente con un intervalo configurado por el usuario. Para activar esta funcionalidad, haga clic en la casilla de verificación **Auto update** y establezca la frecuencia deseada en la caja de texto **Update frequency in seconds** (el valor predeterminado es de 10 segundos).

No se recomienda que el intervalo de tiempo sea menor de 10 segundos. Al hacerlo, puede llegar a ser difícil reconfigurar el intervalo **Auto update** porque la página se actualizará con demasiada frecuencia. Si se encuentra con este problema, simplemente haga clic en otro panel y luego regrese a **CONTROL/MONITORING**.

La funcionalidad **Auto update** no opera con todos los navegadores, por ejemplo **Mozilla**.

Update information now

Se puede actualizar la información de estado haciendo clic en este botón.

CHANGE PASSWORD

Al hacer clic en este botón se tendrá acceso a una pantalla de ayuda con información sobre cómo cambiar la contraseña administrativa para la **Piranha Configuration Tool**.

4.4. GLOBAL SETTINGS

El panel **GLOBAL SETTINGS** es donde se definen los detalles de red para las interfaces de red privada y pública del enrutador LVS primario.

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://localhost:3636/secure/global_setti Search Print

PIRANHA CONFIGURATION TOOL INTRODUCTION | HELP

GLOBAL SETTINGS

CONTROL/MONITORING GLOBAL SETTINGS REDUNDANCY VIRTUAL SERVERS

ENVIRONMENT

Primary server public IP:

Primary server private IP:
(May be blank)

Use network type:
(Current type is: nat) NAT Direct Routing Tunneling

NAT Router IP:

NAT Router netmask: 255.255.255.255

NAT Router device:

ACCEPT -- Click here to apply changes on this page

Figura 4.3. El panel de GLOBAL SETTINGS

La parte superior de este panel establece las interfaces públicas y privadas del enrutador LVS primario. Estas son las interfaces ya configuradas en la [Sección 3.1.1, “Configuración de las interfaces de red para una adición de equilibrador de carga con NAT”](#).

Primary server public IP

En este campo, introduzca la dirección IP real de ruta pública para el nodo LVS primario.

Primary server private IP

Introduzca la dirección IP real para una interfaz de red alternativa en el nodo LVS primario. Esta dirección es utilizada únicamente como un canal alternativo para los pulsos de estado para el enrutador de respaldo y no tiene ninguna relación con la dirección IP privada real asignada en la [Sección 3.1.1, “Configuración de las interfaces de red para una adición de equilibrador de carga con NAT”](#). Puede dejar este campo en blanco, pero en dicho caso no existirá un canal de pulso alternativo para el enrutador LVS de respaldo y se creará así una posibilidad de falla por un único elemento.



Nota

La dirección IP privada no es necesaria para las configuraciones de **Direct Routing**, ya que todos los servidores reales y los directores LVS comparten la misma dirección IP virtual y deben tener la misma configuración de ruta IP.

**Nota**

El IP privado del enrutador LVS primario puede ser configurado en cualquier interfaz que acepte TCP/IP, ya sea un adaptador Ethernet o un puerto serial.

Usar tipo de red

Haga clic en el botón **NAT** para seleccionar el enrutamiento NAT.

Haga clic en el botón **Direct Routing** para seleccionar el enrutamiento directo.

Los siguientes tres campos se ocupan específicamente de la interfaz de red virtual del enrutador NAT que conecta la red privada con los servidores reales. Estos campos *no* se aplican al tipo de red de enrutado directo.

IP de enrutador NAT

El IP flotante privada se define en este campo de texto. Este IP flotante debe ser usado como puerta de enlace para los servidores reales.

Netmask de enrutador NAT

Si el IP flotante del enrutador NAT necesita una máscara de red particular, selecciónela de la lista desplegable.

Dispositivo de enrutador NAT

En este campo se define el nombre del dispositivo de la interfaz de red para la dirección IP flotante, tal como **eth1:1**.

**Nota**

Debe crear un alias en la interfaz de red conectada a la red privada para la dirección IP flotante NAT. En este ejemplo, la red privada está en la interfaz **eth1** mientras que **eth1:1** está en la dirección IP flotante.

**Advertencia**

Después de completar esta página, haga clic en el botón **ACCEPT** para asegurarse de que los cambios no se pierdan al seleccionar un nuevo panel.

4.5. REDUNDANCIA

El panel **REDUNDANCIA** permite la configuración del enrutador LVS de respaldo y establece varias opciones de control de los latidos.

Nota

La primera vez que visite la pantalla se mostrará un estado de **respaldo** inactivo y un botón con la etiqueta **ENABLE**. Para configurar el enrutador LVS de respaldo, haga clic en el botón **ENABLE** para que la pantalla se asemeje a la [Figura 4.4, “El panel REDUNDANCIA”](#).

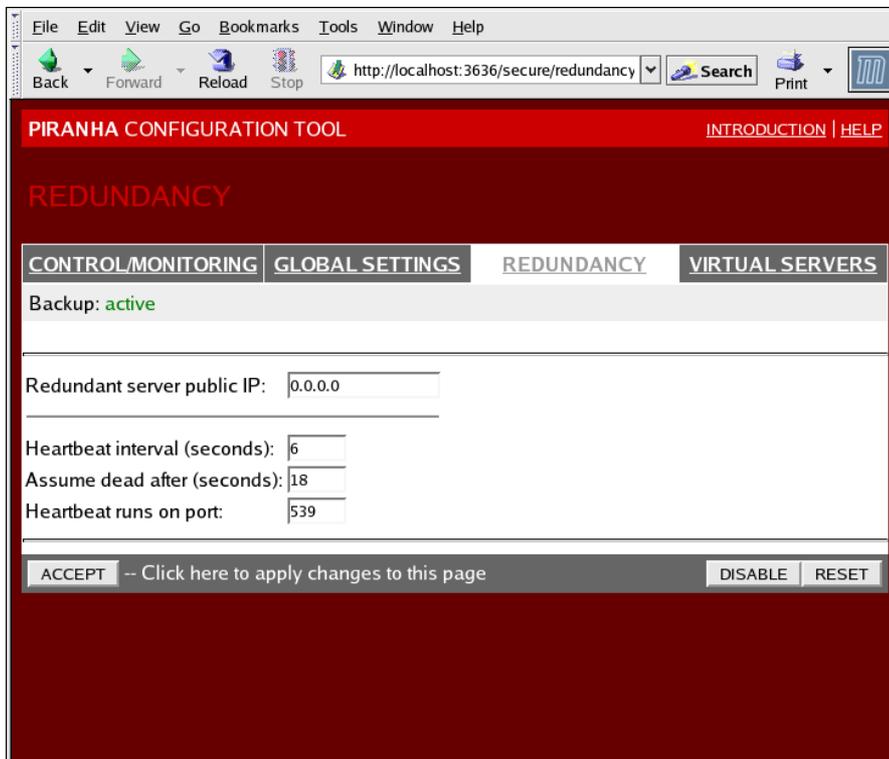


Figura 4.4. El panel REDUNDANCIA

IP pública de servidor redundante

Introduzca la dirección IP real pública para el enrutador LVS de respaldo.

IP privada de servidor redundante

Ingrese la dirección IP real privada del nodo de respaldo en este campo de texto.

Si no ve el campo llamado **panel IP privada de servidor redundante**, regrese a **Configuración GLOBAL** e ingrese una dirección en **IP privada de servidor primario** y haga clic en **ACCEPT**.

El resto del panel se utiliza para configurar el canal de pulso. El nodo de respaldo utiliza este canal para sondear la salud del nodo primario.

Intervalo de latidos (segundos)

Este campo establece el intervalo de segundos entre pulsos — el nodo de respaldo utiliza este intervalo para revisar el estado del nodo LVS primario.

Asumir como muerto después de (segundos)

Si el nodo LVS primario no responde después de este intervalo de tiempo, el enrutador LVS de respaldo inicia el procedimiento de recuperación contra fallos.

Heartbeat se ejecuta en puerto

En este campo se establece el puerto utilizado para la comunicación de pulsos con el nodo LVS primario. El valor predeterminado es 539.



Advertencia

Recuerde hacer clic en el botón **ACCEPT** después de hacer cualquier cambio en este panel para asegurarse de que las modificaciones no se pierdan al seleccionar un nuevo panel.

4.6. SERVIDORES VIRTUALES

El panel **SERVIDORES VIRTUALES** muestra la información para cada servidor virtual definido actualmente. Cada entrada en la tabla muestra el estado del servidor virtual, el nombre del servidor, el IP virtual asignado al servidor, la máscara de red del IP virtual, el número de puerto en el cual el servicio se comunica, el protocolo usado y la interfaz de dispositivo virtual.

STATUS	NAME	VIP	NETMASK	PORT	PROTOCOL	INTERFACE
up	HTTP	192.168.1.10	255.255.255.0	80	tcp	eth0:1
up	FTP	192.168.1.11	255.255.255.0	21	tcp	eth0:1

Figura 4.5. El panel **SERVIDORES VIRTUALES**

Cada servidor mostrado en el panel **SERVIDORES VIRTUALES** puede ser configurado en las pantallas o *subsecciones* siguientes.

Para añadir un servicio, haga clic en el botón **ADD**. Para remover un servicio, selecciónelo haciendo clic en el botón de radio al lado del servidor virtual y luego haga clic en **DELETE**.

Para activar o desactivar un servidor virtual en la tabla, haga clic en el botón de radio apropiado y luego en el botón **(DE)ACTIVATE**

Después de añadir un servidor virtual, éste se puede configurar al hacer clic en el botón de radio a la izquierda y luego en **EDITAR** para ir a la subsección **SERVIDOR VIRTUAL**

4.6.1. Subsección **SERVIDOR VIRTUAL**

La subsección **SERVIDOR VIRTUAL** que se muestra en la [Figura 4.6, “Subsección SERVIDORES VIRTUALES”](#) permite configurar un servidor virtual individual. Los enlaces a subsecciones relacionadas específicamente con este servidor virtual se encuentran en la parte superior de la página. Pero antes de poder configurar cualquier subsección relacionada con los servidores virtuales, se debe completar esta página y hacer clic en **ACCEPT**.

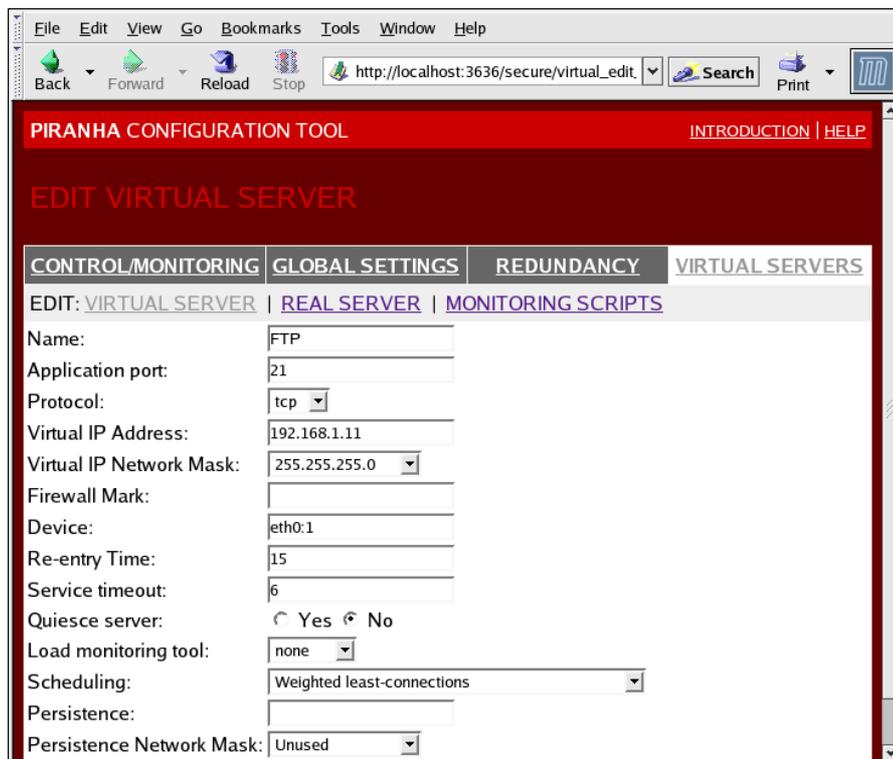


Figura 4.6. Subsección SERVIDORES VIRTUALES

Nombre

Un nombre descriptivo para identificar el servidor virtual. Este nombre *no* es el nombre de host de la máquina, debe ser descriptivo y fácilmente identificable. Puede hacer referencia al protocolo usado por el servidor virtual (como por ejemplo HTTP).

Puerto de aplicación

Introduzca el número de puerto en el cual el servicio escuchará. En este ejemplo se usa el puerto 80 para el servicio HTTP.

Protocolo

Escoja entre UDP y TCP en el menú desplegable. Como los servidores de web se comunican a través de TCP, el ejemplo muestra este protocolo.

Dirección IP virtual

Ingrese la dirección IP flotante del servidor virtual en este campo de texto.

Máscara de red IP virtual

Permite establecer la máscara de red del servidor virtual desde un menú desplegable.

Marca de cortafuegos

No ingrese un valor entero de marca de cortafuegos en este campo a menos que esté agrupando protocolos multipuertos o creando un servidor virtual de múltiples protocolos por separado, pero protocolos relacionados. En este ejemplo, el servidor virtual tiene una **Marca de cortafuegos** de 80 porque se está agrupando la conexión a HTTP en el puerto 80 y HTTPS en el puerto 443 utilizando una marca de cortafuegos de 80. Cuando se utilice la persistencia, esta técnica asegura que tanto los usuarios que utilizan las páginas web seguras como las inseguras son dirigidos al mismo servidor real, preservando así el estado.



Advertencia

Al introducir una marca de cortafuegos en este campo hace que el IPVS reconozca que paquetes con la marca de cortafuegos son tratados de la misma forma, pero se debe realizar una configuración adicional por fuera de la **Piranha Configuration Tool** para que las marcas de cortafuegos sean realmente asignadas. Consulte la [Sección 3.4, “Servicios de puertos múltiples y Adición de equilibrador de carga”](#) para obtener instrucciones en cómo crear servicios de múltiples puertos y la [Sección 3.5, “Configuración de FTP”](#) para la creación de servidores virtuales FTP de alta disponibilidad.

Dispositivo

Introduzca el nombre del dispositivo de red en el cual desea vincular la dirección flotante definida en el campo **Dirección virtual IP**.

Se debe crear un alias en la interfaz Ethernet conectada a la red pública para la dirección IP flotante pública. En este ejemplo, la red pública está en la interfaz **eth0**, por lo cual **eth0:1** debe ser introducido como el nombre del dispositivo.

Tiempo de re-entrada

Ingrese un valor entero que defina la duración en segundos antes de que el enrutador LVS activo intente añadir nuevamente un servidor real previamente fallido en el grupo de servidores.

Servicio de tiempo de espera

Introduzca un valor entero que define la duración en segundos antes de que un servidor real es considerado muerto y sea removido del grupo de servidores.

Servidor de Quiesce

Si se selecciona el botón de radio **Servidor de Quiesce**, cada vez que un nuevo servidor

entra en línea, la tabla de conexiones mínima se establece a zero para que el enrutador LVS activo encamine las solicitudes como si todos los servidores reales hubiesen sido recientemente añadidos. Esta opción previene que el nuevo servidor sea invadido por un alto número de conexiones apenas entre en el grupo de servidores.

Herramienta de control de carga

El enrutador LVS puede sondear la carga de los servidores reales con **rup** o **ruptime**. Si selecciona **rup** desde el menú desplegable, cada servidor real debe ejecutar el servicio **rstatd**. Si selecciona **ruptime**, cada servidor real debe ejecutar el servicio **rwhod**.



Advertencia

El sondeo de carga *no* es lo mismo que el balance de carga y puede resultar en comportamientos de programación difíciles de pronosticar cuando se combinan con algoritmos de programación ponderada. Asimismo, si utiliza sondeo de carga, los servidores reales deben ser máquinas Linux.

Programación

Seleccione su algoritmo de programación preferido desde el menú desplegable. **Conexión de ponderación mínima** se utiliza por defecto. Para mayor información sobre los algoritmos de programación, consulte la [Sección 1.3.1, “Algoritmos de programación”](#).

Persistencia

Utilizado si se necesitan conexiones persistentes al servidor virtual durante las transacciones del cliente. En este campo de texto se debe especificar el número de segundos de inactividad antes de que la conexión expire.



Importante

Si introdujo un entero en el campo **Marca de cortafuegos**, también debe introducir un valor de persistencia. También, asegúrese de que si se utilizan marcas de cortafuegos y persistencia, la cantidad de persistencia es la misma para cada servidor virtual con la marca de cortafuegos. Para obtener mayor información en persistencia y marcas de cortafuegos, consulte la [Sección 1.5, “Marcas de cortafuego y persistencia”](#).

Máscara de red de persistencia

Para limitar la persistencia a una subred particular, seleccione la máscara apropiada de red desde el menú desplegable.



Nota

Antes de la llegada de las marcas de cortafuegos, la persistencia limitada por una subred era la manera de agrupar conexiones. Ahora, es mejor utilizar persistencia en relación con las marcas de cortafuego para obtener el mismo resultado.



Advertencia

Recuerde hacer clic en **ACCEPT** después de realizar cualquier cambio en este panel para asegurar que los cambios no se pierdan cuando seleccione un nuevo panel.

4.6.2. Subsección **SERVIDOR REAL**

Si hace clic en el enlace de la subsección **REAL SERVER** en la parte superior del panel, llegará a la subsección **EDITAR SERVIDOR REAL**. Muestra el estado de los hosts del servidor físico para un servicio virtual particular.

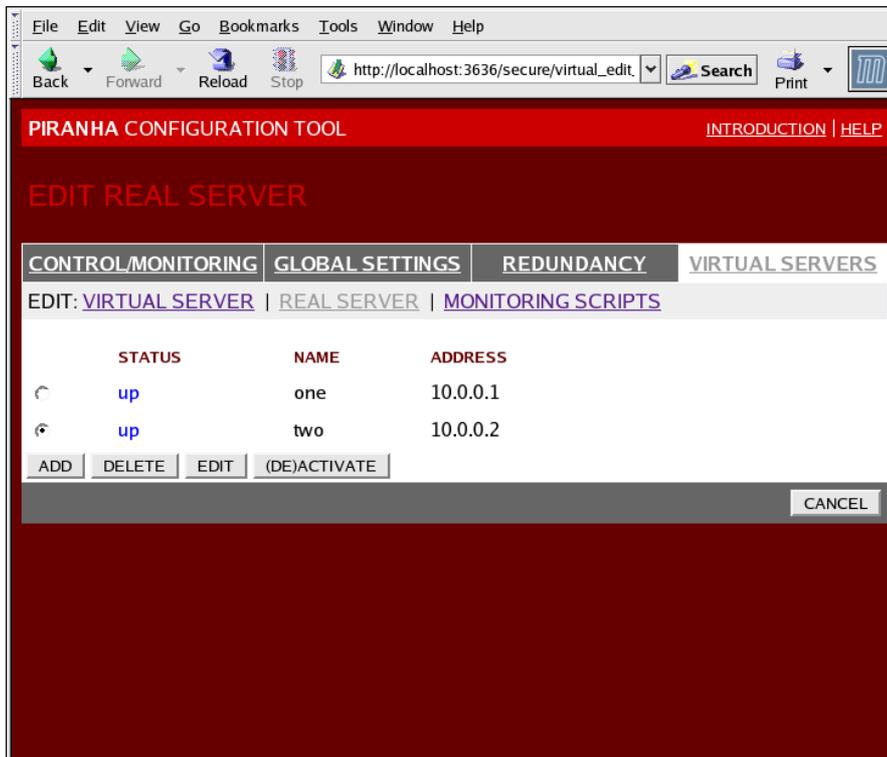


Figura 4.7. Subsección **SERVIDOR REAL**

Haga clic en **ADD** para añadir un nuevo servidor. Para borrarlo, seleccione el botón de radio al lado del servidor y haga clic en **DELETE**. Haga clic en **EDIT** para cargar el panel **EDITAR SERVIDOR REAL**, como se ve en la [Figura 4.8, “El panel de configuración **SERVIDOR REAL**”](#).

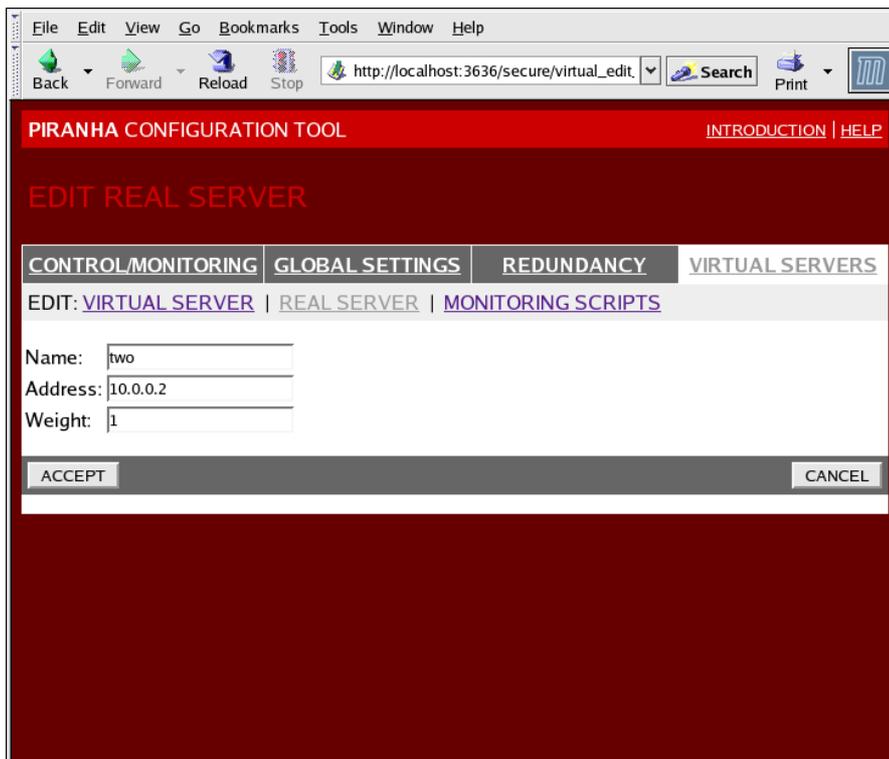


Figura 4.8. El panel de configuración SERVIDOR REAL

Este panel está constituido por tres campos:

Nombre

Un nombre descriptivo para el servidor real.



Nota

Este nombre *no* es el nombre de host de la máquina. Utilice un nombre descriptivo y fácilmente identificable.

Dirección

La dirección IP del servidor real. Ya que el puerto de escucha ya está especificado para el servidor virtual asociado, no es necesario especificar el número de puerto.

Peso

Un valor entero que indica la capacidad del host en comparación con otros servidores en el grupo de servidores. El valor puede ser arbitrario, pero debe ser tratado con relación a los otros servidores reales. Consulte la [Sección 1.3.2, “Peso del servidor y programación”](#) para obtener mayor información al respecto.



Advertencia

Recuerde hacer clic en **ACCEPT** después de realizar cualquier cambio en este panel para asegurar que los cambios no se pierdan cuando seleccione un nuevo panel.

4.6.3. Subsección EDITAR SCRIPTS DE MONITORIZACIÓN

Haga clic en el enlace **SCRIPTS DE MONITORIZACIÓN** en la parte superior de la página. La subsección **EDITAR SCRIPTS DE MONITORIZACIÓN** permite que los administradores especifiquen una secuencia de envío y expectativa para verificar que el servicio para el servidor virtual esté funcionando en cada servidor real. También es posible especificar scripts personalizados para revisar los servicios que requieren cambios de datos de forma dinámica.

Figura 4.9. Subsección EDITAR SCRIPTS DE MONITORIZACIÓN

Enviar programa

Se puede utilizar este campo para especificar la ruta a un script para una verificación de servicios más avanzada. Esta función es especialmente útil para servicios que requieren cambios de datos de forma dinámica, como HTTPS o SSL.

Para usar esta función, se debe escribir un script que retorne una respuesta textual. El script debe ser ejecutable y su ruta debe establecerse en el campo **Enviar programa**.



Nota

Para asegurarse de que cada servidor en el grupo de servidores reales sea monitorizado, utilice **%h** después de la ruta al script en el campo **Enviar programa**. Este signo se reemplaza por la dirección IP de cada servidor real cada vez que el demonio **nanny** llama al script.

El siguiente es un script de ejemplo que puede servir de guía cuando se compone un script externo para monitorizar los servicios:

```
#!/bin/sh

TEST=`dig -t soa example.com @$1 | grep -c dns.example.com`

if [ $TEST != "1" ]; then
  echo "OK"
else
  echo "FAIL"
fi
```



Nota

Si se introduce un programa externo en el campo **Enviar programa**, se ignorará el campo **Enviar**.

Enviar

Introduzca una cadena para el demonio **nanny** que será enviada a cada servidor real. Por defecto la entrada se completa para HTTP. Se puede alterar este valor dependiendo de sus necesidades. Si se deja este campo en blanco, el demonio **nanny** intentará abrir el puerto y, si lo logra, asumirá que el servicio está en ejecución.

Solo una secuencia de envío es permitida en este campo y solo puede contener caracteres ASCII y los siguientes caracteres de escape:

- ▶ \n para nueva línea.
- ▶ \r para retorno de línea.
- ▶ \t para tab.
- ▶ \ para escapar el siguiente caracter.

Esperado

Introduzca la respuesta textual que el servidor debe responder si está funcionando apropiadamente. Si escribió su propio programa de envío, introduzca la respuesta esperada.



Nota

Para determinar lo que se debe enviar para un servicio en particular, puede abrir una conexión **telnet** al puerto en el servidor real y ver lo que retorna. Por ejemplo, FTP muestra 220 tras la conexión, por lo cual puede introducir **salir** en el campo **Enviar** y **220** en el campo **Esperado**.



Advertencia

Recuerde hacer clic en **ACCEPT** después de realizar cualquier cambio en este panel para asegurar que los cambios no se pierdan cuando seleccione un nuevo panel.

Una vez haya configurado los servidores virtuales con la **Piranha Configuration Tool**, debe copiar los archivos de configuración específicos al enrutador LVS de respaldo. Consulte la [Sección 4.7, “Sincronización de los archivos de configuración”](#) para obtener mayor información.

4.7. Sincronización de los archivos de configuración

Después de configurar el enrutador LVS primario, hay varios archivos de configuración que deben ser copiados al enrutador LVS de respaldo antes de iniciar la adición de equilibrador de carga.

Entre estos archivos están:

- ▶ **/etc/sysconfig/ha/lvs.cf** — el archivo de configuración para los enrutadores LVS.
- ▶ **/etc/sysctl** — el archivo de configuración que, entre otras cosas, activa el reenvío de paquetes en el kernel.
- ▶ **/etc/sysconfig/iptables** — si está utilizando marcas de cortafuegos, debe sincronizar uno de estos archivos de acuerdo con el filtro de paquetes de red que esté utilizando.



Importante

Los archivos **/etc/sysctl.conf** y **/etc/sysconfig/iptables** *no* cambian cuando se configura la adición de equilibrador de carga con la **Piranha Configuration Tool**.

4.7.1. Sincronización de **lvs.cf**

Si se crea o se actualiza el archivo **/etc/sysconfig/ha/lvs.cf**, éste debe ser copiado al enrutador LVS de respaldo.



Advertencia

Tanto el enrutador LVS activo como el de respaldo deben tener un archivo **lvs.cf** idéntico. Si el archivo de configuración es diferente entre los enrutadores, el proceso de recuperación contra fallos podría fallar.

La mejor manera para llevar a cabo esta tarea es con el comando **scp**.



Importante

Para utilizar **scp**, **sshd** debe estar funcionando en el enrutador de respaldo. Consulte la [Sección 2.1, “Configuración de servicios en los enrutadores LVS”](#) para obtener información sobre cómo configurar apropiadamente los servicios necesarios en el enrutador LVS.

Ejecute el siguiente comando como root desde el enrutador LVS primario para sincronizar los archivos **lvs.cf** entre los nodos del enrutador:

```
scp /etc/sysconfig/ha/lvs.cf n.n.n.n:/etc/sysconfig/ha/lvs.cf
```

En el comando, reemplace *n.n.n.n* por la dirección IP real del enrutador LVS de respaldo.

4.7.2. Sincronización de `sysctl`

El archivo `sysctl` se modifica una sola vez en la mayoría de los casos. Este archivo se lee durante el periodo de arranque y le dice al kernel que active el reenvío de paquetes.



Importante

Si no está seguro si el reenvío de paquetes está o no activado en el kernel, consulte la [Sección 2.5, “Activación de reenvío de paquetes”](#) para obtener instrucciones sobre cómo revisar y, si es necesario, activar esta funcionalidad.

4.7.3. Sincronización de las reglas de filtro de paquetes de red

Si está utilizando `iptables`, podría necesitar sincronizar el archivo de configuración apropiado en el enrutador LVS de respaldo.

Si altera cualquiera de las reglas de filtro de paquetes, ingrese el siguiente comando como root en el enrutador LVS primario:

```
scp /etc/sysconfig/iptables n.n.n.n:/etc/sysconfig/
```

En el comando, reemplace *n.n.n.n* por la dirección IP real del enrutador LVS de respaldo.

Abra una sesión `ssh` en el enrutador de respaldo o inicie una sesión en la máquina y escriba el siguiente comando:

```
/sbin/service iptables restart
```

Una vez copie estos archivos al enrutador de respaldo e inicie los servicios apropiados (consulte la [Sección 2.1, “Configuración de servicios en los enrutadores LVS”](#) para obtener mayor información al respecto) estará listo para iniciar la adición de equilibrador de carga.

4.8. Inicio de la adición de equilibrador de carga

Para iniciar la adición de equilibrador de carga, es mejor tener dos terminales abiertas de forma simultánea o dos sesiones `ssh` abiertas en el enrutador LVS primario.

En una terminal, observe los mensajes de registro del kernel con el siguiente comando:

```
tail -f /var/log/messages
```

Luego inicie la adición de equilibrador de carga escribiendo el siguiente comando en la otra terminal:

```
/sbin/service pulse start
```

Siga el progreso del inicio del servicio `pulse` en la terminal que está observando los mensajes de registro del kernel. Si ve los siguientes mensajes, quiere decir que el demonio `pulse` ha sido iniciado apropiadamente:

```
gratuitous lvs arps finished
```

Para detener el sondeo de `/var/log/messages`, escriba **Ctrl+c**.

Desde ahora, el enrutador LVS primario es también el enrutador LVS activo. Aunque se pueden realizar solicitudes a la adición de equilibrador de carga en estos momentos, se debe iniciar el enrutador antes de LVS de respaldo antes de que la adición de equilibrador de carga sea puesta en servicio. Para ello, repita el proceso descrito anteriormente en el enrutador LVS de respaldo.

Una vez se complete este paso final, la adición de equilibrador de carga estará activo y en ejecución.

Uso de la adición de Equilibrador de carga con adición de Alta disponibilidad

Puede utilizar el enrutador uso de adición de Equilibrador de carga para implementar un sitio de comercio electrónico de alta disponibilidad que proporcione balance de carga, integridad de datos y disponibilidad de aplicaciones.

La configuración en la [Figura A.1, “Adición de Equilibrador de carga con adición de Alta disponibilidad”](#) representa un sitio de comercio electrónico usado para ordenar mercancía en línea a través de una URL. La solicitud del cliente pasa a través de un cortafuegos al enrutador de balance de carga LVS activo, el cual a su vez, envía la solicitud a uno de los servidores de red. Los nodos de Alta disponibilidad sirven en forma dinámica datos a los servidores de red, los cuales reenvían los datos al cliente que los solicita.

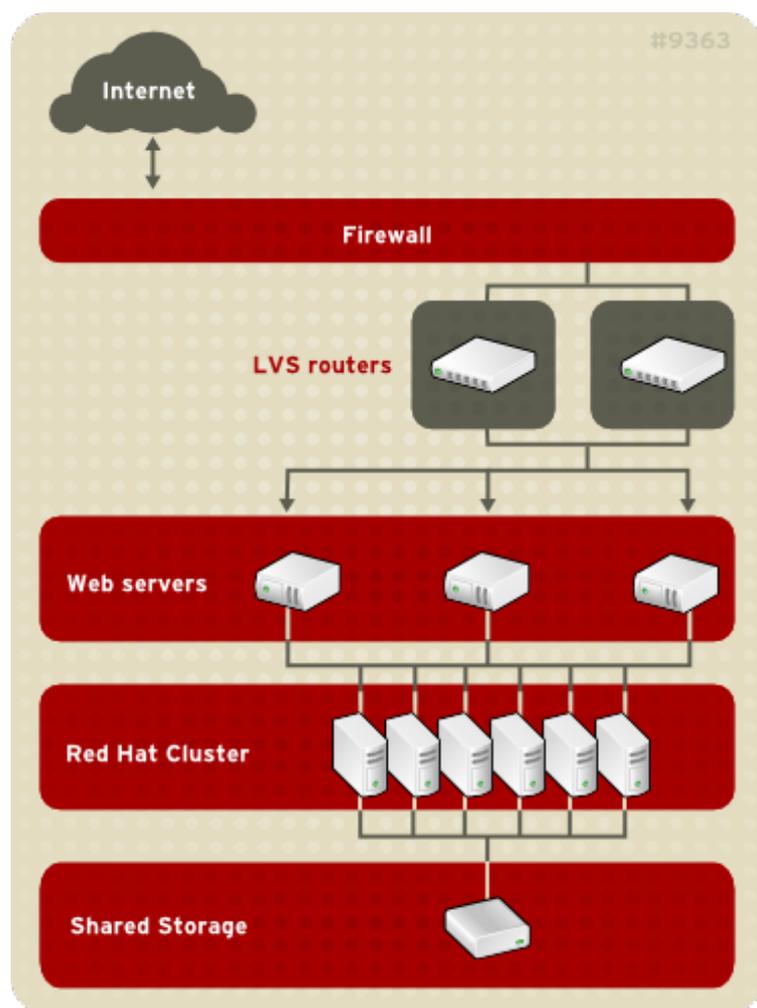


Figura A.1. Adición de Equilibrador de carga con adición de Alta disponibilidad

Para servir el contenido dinámico de red requiere una configuración de adición de Equilibrador de carga de tres capas (como se muestra en la [Figura A.1, “Adición de Equilibrador de carga con adición de Alta disponibilidad”](#)). La combinación de uso de adición de Equilibrador de carga con adición de Alta disponibilidad, permite la configuración de un sitio de comercio electrónico de alta integridad sin punto de fallo único. La adición de Alta disponibilidad puede ejecutar una instancia de alta disponibilidad de una base de datos o un conjunto de base de datos que están disponibles a través de servidores de red.

Una configuración de tres capas es requerida para proporcionar contenido dinámico. Mientras una configuración de adición de Equilibrador de carga de dos capas es apta para servidores de web que

sirven únicamente contenido estático (que consiste en cantidades pequeñas de datos que no cambian frecuentemente) pero no es apta para servidores de web que sirven contenido dinámico. El contenido dinámico puede incluir inventario de productos, ordenes de adquisición o bases de datos de clientes que deben ser consistentes en todos los servidores web para garantizar que los clientes tengan acceso actualizado y correcto a los datos.

Cada capa proporciona las siguientes funciones:

- ▶ Primera capa — los enrutadores LVS ejecutan balance de carga para distribuir solicitudes de web.
- ▶ Segunda capa — Un grupo de servidores web que procesan la solicitud.
- ▶ Tercera capa — Una adición de Equilibrador de carga para servir datos a los servidores de Web.

En una configuración una adición de Equilibrador de carga como la de la [Figura A.1, “Adición de Equilibrador de carga con adición de Alta disponibilidad”](#), los sistemas clientes envían solicitudes a la red mundial (World Wide Web). Por razones de seguridad estas solicitudes entran a un sitio web a través de un cortafuegos, el cual puede ser un sistema Linux que sirve como tal o un dispositivo de cortafuegos dedicado. Para redundancia, se puede configurar el dispositivo de cortafuegos en una configuración de recuperación contra fallos. Detrás del cortafuegos están los enrutadores LVS que proporcionan equilibrio de carga, los cuales pueden ser configurados en un modo activo-espera. El enrutador de equilibrio de carga activo reenvía la solicitud al grupo de servidores de red.

Cada servidor de web puede procesar independientemente una solicitud HTTP desde el cliente y enviar la respuesta de regreso a éste. LVS le permite expandir la capacidad de un sitio web añadiendo servidores de web tras los enrutadores LVS; los enrutadores LVS ejecutan el balance de carga a lo largo de una gran cantidad de servidores de web. Además, si un servidor web falla, puede ser removido; la adición de Equilibrador de carga continuará ejecutando el balance de carga con los demás servidores de web.

Historial de revisiones

Revisión 6-4	2012-07-18	Anthony Towns
Rebuild for Publican 3.0		
Revisión 1.0-0	Wed Nov 10 2010	Paul Kennedy
Lanzamiento inicial del libro para Red Hat Enterprise Linux 6		

Índice

A

Adición de Alta disponibilidad

- Uso de adición de Equilibrador de carga, [Uso de la adición de Equilibrador de carga con adición de Alta disponibilidad](#)
- y adición de Equilibrador de carga, [Uso de la adición de Equilibrador de carga con adición de Alta disponibilidad](#)

Adición de equilibrador de carga

- /etc/sysconfig/ha/lvs.cf archivo, [/etc/sysconfig/ha/lvs.cf](#)
- componentes de, [Componentes de la adición de equilibrador de carga](#)
- datos compartidos, [Repetición y uso compartido de datos](#)
- enrutadores LVS
 - servicios necesarios, [Configuración de servicios en los enrutadores LVS](#)
- enrutamiento directo
 - requerimientos, hardware, [Enrutado directo](#)
 - requerimientos, red, [Enrutado directo](#)
 - yarptables_jf, [Enrutado directo y arptables_jf](#)
- enrutamiento NAT
 - requerimientos, hardware, [La red de adición de equilibrador de carga de NAT](#)
 - requerimientos, red, [La red de adición de equilibrador de carga de NAT](#)
 - requerimientos, software, [La red de adición de equilibrador de carga de NAT](#)
- iniciando la adición de equilibrador de carga, [Inicio de la adición de equilibrador de carga](#)
- ipvsadm programa, [ipvsadm](#)
- nanny demonio, [nanny](#)
- Piranha Configuration Tool , [Piranha Configuration Tool](#)
- prerequisites de enrutamiento, [Configuración de las interfaces de red para una adición de equilibrador de carga con NAT](#)
- programación de tareas, [Visión general de la adición de equilibrador de carga](#)
- programación, tareas, [Visión general de la adición de equilibrador de carga](#)
- pulse demonio, [pulse](#)
- réplica de fecha, servidores reales, [Repetición y uso compartido de datos](#)
- send_arp programa, [send_arp](#)
- servicios de varios puertos, [Servicios de puertos múltiples y Adición de equilibrador de carga](#)
- servicios multi-puertos
 - FTP, [Configuración de FTP](#)

- sincronización de los archivos de configuración, [Sincronización de los archivos de configuración](#)
- tres partes
 - Red Hat Cluster Manager, [Configuración de la adición de equilibrador de carga de tres partes](#)

adición de equilibrador de carga

- reenvío de paquetes, [Activación de reenvío de paquetes](#)

Adición de Equilibrador de carga

- uso de la adición de Equilibrador de carga con adición de Alta disponibilidad, [Uso de la adición de Equilibrador de carga con adición de Alta disponibilidad](#)

Adición de equilibrador de enrutamiento

- enrutamiento directo
 - requerimientos, software, [Adición de equilibrador de carga con enrutamiento directo](#)
 - requisitos, hardware, [Adición de equilibrador de carga con enrutamiento directo](#)
 - requisitos, red, [Adición de equilibrador de carga con enrutamiento directo](#)

Adición del equilibrador de carga

- configuración inicial, [Configuración inicial de la adición de equilibrador de carga](#)
- enrutadores LVS
 - configuración de servicios, [Configuración inicial de la adición de equilibrador de carga](#)
 - nodo primario, [Configuración inicial de la adición de equilibrador de carga](#)

archivo `/etc/sysconfig/ha/lvs.cf`, [/etc/sysconfig/ha/lvs.cf](#)

`arptables_jf`, [Enrutado directo y arptables_jf](#)

C

`chkconfig`, [Configuración de servicios en los enrutadores LVS](#)

cluster

- uso de adición de Equilibrador de carga con adición de Alta disponibilidad, [Uso de la adición de Equilibrador de carga con adición de Alta disponibilidad](#)

Comentarios, [Comentarios](#)

componentes

- de adición de equilibrador de carga, [Componentes de la adición de equilibrador de carga](#)

conexiones mínimas (ver programación de tareas, Adición de equilibrador de carga)

conexiones ponderadas mínimas (ver programación de tareas, Adición de equilibrador

de carga)

D

demonio lvs, [lvs](#)

demonio nanny, [nanny](#)

demonio pulse, [pulse](#)

E

enrutamiento

- prerequisites para la adición de equilibrador de carga, [Configuración de las interfaces de red para una adición de equilibrador de carga con NAT](#)

enrutamiento directo

- y arptables_jf, [Enrutado directo y arptables_jf](#)

F

FTP, [Configuración de FTP](#)

- (ver también Adición de equilibrador de carga)

I

introducción, [Introducción](#)

Introducción

- otros documentos de Red Hat Enterprise Linux, [Introducción](#)

iptables , [Configuración de servicios en los enrutadores LVS](#)

L

La adición de equilibrador de carga

- enrutamiento directo

- requerimientos, software, [Enrutado directo](#)

- métodos de enrutamiento

- NAT, [Métodos de enrutamiento](#)

LVS

- demonio, [lvs](#)

- enrutamiento NAT

- activando, [Activación de rutas NAT en enrutadores LVS](#)

- lvs demonio, [lvs](#)

- servidores reales, [Visión general de la adición de equilibrador de carga](#)

- visión general de, [Visión general de la adición de equilibrador de carga](#)

N

NAT

- activando, [Activación de rutas NAT en enrutadores LVS](#)
- métodos de enrutamiento, adición de equilibrador de carga, [Métodos de enrutamiento](#)

P

Piranha Configuration Tool , [Piranha Configuration Tool](#)

- CONTROL/MONITORING , [CONTROL/MONITORING](#)
- EDITAR SCRIPTS DE MONITORIZACIÓN Subsección, [Subsección EDITAR SCRIPTS DE MONITORIZACIÓN](#)
- estableciendo una contraseña, [Configuración de la contraseña para la Piranha Configuration Tool](#)
- GLOBAL SETTINGS , [GLOBAL SETTINGS](#)
- limitando acceso a, [Limitar el acceso a la Piranha Configuration Tool](#)
- panel de inicio de sesión, [Inicio de sesión en la Piranha Configuration Tool](#)
- REDUNDANCIA , [REDUNDANCIA](#)
- SERVIDOR REAL subsección, [Subsección SERVIDOR REAL](#)
- SERVIDOR VIRTUAL subsección, [Subsección SERVIDOR VIRTUAL](#)
 - Dirección Ip virtual , [Subsección SERVIDOR VIRTUAL](#)
 - Marca de cortafuegos , [Subsección SERVIDOR VIRTUAL](#)
 - Persistencia , [Subsección SERVIDOR VIRTUAL](#)
 - Programación , [Subsección SERVIDOR VIRTUAL](#)
- SERVIDORES VIRTUALES , [SERVIDORES VIRTUALES](#)
- software necesario, [Software necesario](#)
- visión general de, [Configuración de la adición de equilibrador de carga con Piranha Configuration Tool](#)

piranha-passwd , [Configuración de la contraseña para la Piranha Configuration Tool](#)

programa ipvsadm, [ipvsadm](#)

programa send_arp, [send_arp](#)

programación de tareas, adición de equilibrador de carga, [Visión general de la adición de equilibrador de carga](#)

programación, tareas (Adición de equilibrador de carga), [Visión general de la adición de equilibrador de carga](#)

R

Reenvío de paquetes, [Activación de reenvío de paquetes](#)

- (ver también adición de equilibrador de carga)

round robin (ver programación de tareas, Adición de equilibrador de carga)

Round Robin ponderado (ver programación de trabajo, Adición de equilibrador de carga)

S

seguridad

- Piranha Configuration Tool , [Limitar el acceso a la Piranha Configuration Tool](#)

servicio piranha-gui, [Configuración de servicios en los enrutadores LVS](#)

servicio pulse , [Configuración de servicios en los enrutadores LVS](#)

servicio sshd, [Configuración de servicios en los enrutadores LVS](#)

servicios de varios puertos, [Servicios de puertos múltiples y Adición de equilibrador de carga](#)

- (ver también Adición de equilibrador de carga)

servidores reales

- configurando servicios, [Configuración de servicios en servidores reales](#)

sincronización de los archivos de configuración, [Sincronización de los archivos de configuración](#)

T

Traducción de dirección de red (ver NAT)