Red Hat Enterprise Linux 5

Virtual Server Administration

Linux Virtual Server (LVS) for Red Hat Enterprise Linux

Edição 5

Last Updated: 2017-10-16

Red Hat Enterprise Linux 5 Virtual Server Administration

Linux Virtual Server (LVS) for Red Hat Enterprise Linux
Edição 5

Landmann
rlandmann@redhat.com

Nota Legal

Resumo

Building a Linux Virtual Server (LVS) system offers highly-available and scalable solution for production services using specialized routing and load-balancing techniques configured through the PIRANHA. This book discusses the configuration of high-performance systems and services with Red Hat Enterprise Linux and LVS for Red Hat Enterprise Linux 5.

Índice

INTRODUÇÃO

Este documento fornece informação sobre instalação, configuração e gerenciamento dos componentes do Servidor Linux Virtual da Red Hat. O LVS fornece balanceamento de carga através das técnicas de roteamento especializadas que despacham o tráfego para os servidores do pool. Este documento não inclui informação sobre instalação, configuração e gerenciamento do software de Cluster da Red Hat. Você poderá encontrar informações sobre isto num documento isolado.

O público deste documento deve ter um conhecimento de trabalho avançado sobre a Red Hat Enterprise Linux e entendimento dos conceitos dos clusters e servidor de computação.

Este documento é organizado como segue a seguir:

- Capítulo 1, *Visão Geral do Servidor Virtual Linux*
- Capítulo 2, *Configuração LVS Inicial*
- Capítulo 3, *Configurando o LVS*
- Capítulo 4, *Configurando os roteadores LVS com a**Piranha Configuration Tool***
- Apêndice A, *Usando o LVS com o Cluster da Red Hat*

Para maiores informações sobre a Red Hat Enterprise Linux 5, refira-se aos seguintes recursos:

- *Guia de Instalação da Red Hat Enterprise Linux*— Fornece informação a respeito da instalação da Red Hat Enterprise Linux 5.
- *Guia de Implantação da Red Hat Enterprise Linux*— Fornece informação sobre implantação, configuração e administração da Red Hat Enterprise Linux 5.

Para maiores informações sobre o Red Hat Cluster Suite da Red Hat Enterprise Linux 5, refira-se aos seguintes recursos:

- *Visão Geral do Red Hat Cluster Suite*— Fornece uma visão geral de alto nível do Cluster Suite da Red Hat.
- *Configurando e Gerenciando um Cluster da Red Hat*— Fornece informação sobre instalação, configuração e gerenciamento dos componentes do Cluster da Red Hat.
- *Logical Volume Manager Administration*— Provides a description of the Logical Volume Manager (LVM), including information on running LVM in a clustered environment.
- *Sistema de Arquivo Global: Configuração e Administração*— Fornece informação sobre instalação, configuração e suporte da Red Hat GFS (Sistema de Arquivo Global da Red Hat).
- *Global File System 2: Configuration and Administration*— Provides information about installing, configuring, and maintaining Red Hat GFS2 (Red Hat Global File System 2).
- *Usando Caminhos Múltiplos do Mapeador do Dispositivo*— Fornece informação sobre a utilização do recurso de Caminho Múltiplo do Mapeador de Dispositivo da Red Hat Enterprise Linux 5.

- *Usando GNBD com o Sistema de Arquivo Global* — Fornece uma visão geral de como se utilizar o Dispositivo de Bloqueio da Rede Global (GNBD) com o GFS da Red Hat.
- *Notas de Versão do Cluster Suite da Red Hat* — Fornece informação sobre a versão atual do Cluster Suite da Red Hat.

A documentação do Red Hat Cluster Suite e outros documentos da Red Hat estão disponíveis em HTML, PDF e versões RPM da Red Hat Enterprise Linux de documentação em CD e on-line em http://www.redhat.com/docs/.

1. COMENTÁRIOS

If you spot a typo, or if you have thought of a way to make this manual better, we would love to hear from you. Please submit a report in Bugzilla (http://bugzilla.redhat.com/bugzilla/) against the component **Documentation-cluster**.

Be sure to mention the manual's identifier:

```
Virtual_Server_Administration(EN)-5 (2010-02-08T16:55)
```

By mentioning this manual's identifier, we know exactly which version of the guide you have.

Caso você tenha alguma sugestão para a melhoria desta documentação, por favor tente ser o mais claro possível. E, caso você encontre um erro, por favor inclua o número da seção e algumas partes do texto para fácil localização.

CAPÍTULO 1. VISÃO GERAL DO SERVIDOR VIRTUAL LINUX

O Servidor Virtual Linux (LVS) é um conjunto integrado de componentes de software para o balanceamento de carga IP, através de um conjunto dos servidores reais. O LVS atua num par de computadores configurados igualmente: o primeiro é o *roteador LVS ativo* e o segundo é o *roteador LVS de backup*. O roteador LVS ativo serve duas funções:

- Balancear a carga através dos servidores reais.
- Para checar a integridade dos serviços em cada servidor real.

O roteador LVS de backup monitora o roteador LVS ativo e se responsabiliza por isto, em caso do roteador LVS ativo falhar.

Este capítulo fornece uma visão geral dos componentes e funções do LVS, e consiste nas seguintes seções:

1.1. A BASIC LVS CONFIGURATION

Figura 1.1, “A Basic LVS Configuration” shows a simple LVS configuration consisting of two layers. On the first layer are two LVS routers — one active and one backup. Each of the LVS routers has two network interfaces, one interface on the Internet and one on the private network, enabling them to regulate traffic between the two networks. For this example the active router is using *Network Address Translation* or *NAT* to direct traffic from the Internet to a variable number of real servers on the second layer, which in turn provide the necessary services. Therefore, the real servers in this example are connected to a dedicated private network segment and pass all public traffic back and forth through the active LVS router. To the outside world, the servers appears as one entity.

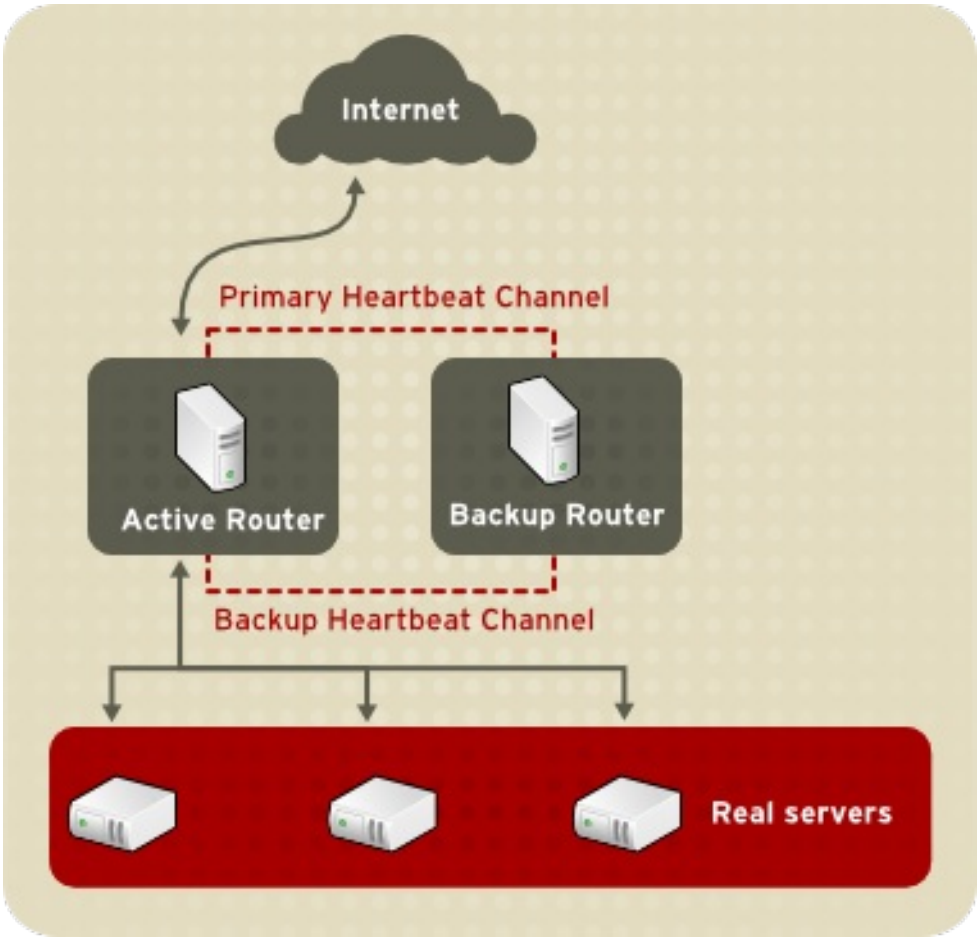


Figura 1.1. A Basic LVS Configuration

Service requests arriving at the LVS routers are addressed to a *virtual IP* address, or *VIP*. This is a publicly-routable address the administrator of the site associates with a fully-qualified domain name, such as www.example.com, and is assigned to one or more *virtual servers*. A virtual server is a service configured to listen on a specific virtual IP. Refer to Seção 4.6, "**VIRTUAL SERVERS**" for more information on configuring a virtual server using the **Piranha Configuration Tool**. A VIP address migrates from one LVS router to the other during a failover, thus maintaining a presence at that IP address (also known as *floating IP addresses*).

Os endereços IP talvez estejam com alias ao mesmo dispositivo do qual conecta o roteador LVS à Internet. Por exemplo, se o eth0 estiver conectado à Internet, então os servidores virtuais múltiplos poderão estar com alias para o **eth0:1**. Alternativamente, cada servidor virtual pode ser associado com um dispositivo separado por serviço. Por exemplo, o tráfego HTTP pode ser manuseado em **eth0:1**, e o tráfego FTP pode ser manuseado em **eth0:2**.

Only one LVS router is active at a time. The role of the active router is to redirect service requests from virtual IP addresses to the real servers. The redirection is based on one of eight supported load-balancing algorithms described further in Seção 1.3, "Visão Geral do Agendamento LVS".

O roteador ativo também monitora dinamicamente o health em geral dos serviços específicos nos servidores reais através de simples *scripts enviados/esperados*. Para ajudar na detecção do health dos serviços que requerem os dados dinâmicos, como por exemplo os HTTPS ou SSL, o administrador pode também chamar serviços externos executáveis. Caso um serviço funcionar incorretamente num servidor real, o roteador ativo interromperá o envio de trabalhos para o servidor até isto retornar à uma operação normal.

O roteador de backup atua a função de sistema Standby. Periodicamente, os roteadores LVS mudam as mensagens heartbeat através da interface pública externa primária, e numa situação de falha a

interface primária. Caso o nó de backup falhe em receber a mensagem heartbeat no intervalo esperado, ele iniciará a falha e assumirá a função de roteador ativo. Durante a falha, o roteador de backup se responsabiliza pelos endereços VIP servidos por um roteador de falha usando a técnica conhecida como *falsificação de ARP*—, onde o roteador LVS de backup se anuncia como destino dos endereçados pacotes IP ao nó de falha. Quando o nó de falha retornar ao serviço ativo, o nó de backup assumirá a função de hot-backup novamente.

The simple, two-layered configuration used in Figura 1.1, “A Basic LVS Configuration” is best for serving data which does not change very frequently — such as static webpages — because the individual real servers do not automatically sync data between each node.

1.1.1. Replicação de Dados e Compartilhamento de dados entre Servidores Reais

Uma vez que não exista componente interno no LVS para compartilhar os mesmos dados entre os servidores reais, o administrador possui duas opções básicas:

- Sincronizar os dados através do pool de servidores reais
- Adicionar a terceira camada à topologia para o acesso de dados compartilhados

A primeira opção é preferida por servidores que não permitem grande número de usuários para carregar ou mudar os dados nos servidores reais. Se a configuração permitir grande número de usuários para modificação dos dados, como por exemplo um website de comércio eletrônico, a adição da terceira camada será preferível.

1.1.1.1. Configuração de Servidores Reais para Dados Sincronizados

Existem diversas maneiras em que um administrador pode escolher para sincronizar os dados através do pool de servidores reais. Por exemplo, o shell scripts pode ser implementado em caso da web de engenheiros atualizar a página, e esta ser enviada a todos os servidores simultaneamente. Além disso, o sistema administrador pode usar programas como por exemplo o **rsync** para replicar mudanças de dados através de todos os nós num conjunto de intervalo.

No entanto, o tipo de dados sincronizados não funcionam da melhor forma se uma configuração estiver sobrecarregada com usuários carregando arquivos constantemente ou lançando transações de banco de dados. Para uma configuração com um alto valor de carga, a *topologia de três camadas*será a solução ideal.

1.2. A THREE-TIER LVS CONFIGURATION

Figura 1.2, “A Three-Tier LVS Configuration” shows a typical three-tier LVS topology. In this example, the active LVS router routes the requests from the Internet to the pool of real servers. Each of the real servers then accesses a shared data source over the network.

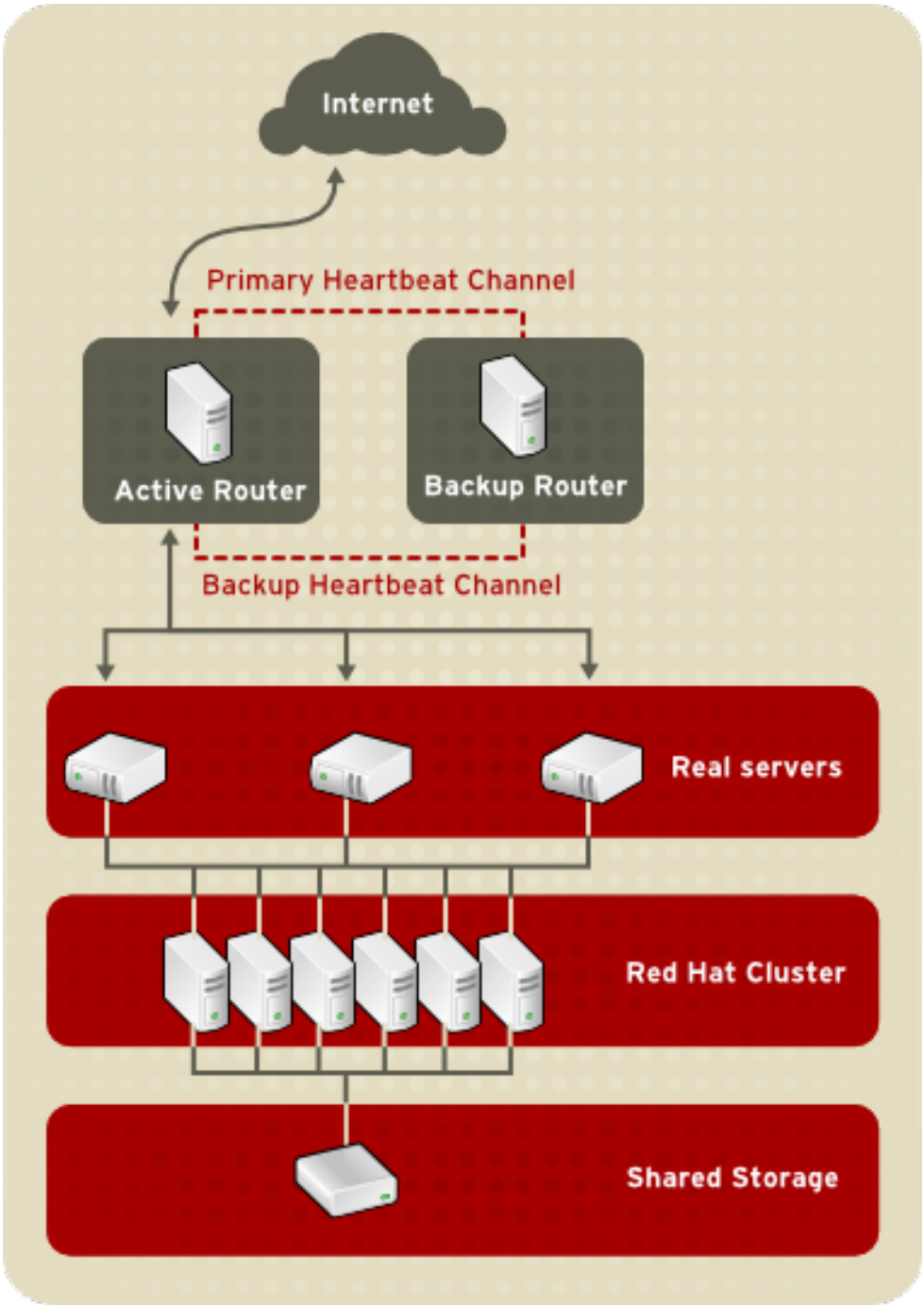


Figura 1.2. A Three-Tier LVS Configuration

Esta configuração é ideal para servidores FTP não disponíveis, onde o acesso aos dados é armazenado no servidor central de alta disponibilidade, e acessado por cada servidor real por meio do diretório NFS exportado ou Samba compartilhado. Esta topologia é também recomendada para websites que acessam o banco de dados central e de alta disponibilidade para transações. Além disso, com a utilização da configuração ativa-ativa com o Red Hat Cluster Manager, os administradores podem configurar um cluster de alta disponibilidade para servir ambas funções simultaneamente.

A terceira camada dos exemplos acima não precisa utilizar o Red Hat Cluster Manager, mas a falha em se utilizar a solução de alta disponibilidade poderá introduzir um único ponto crítico de falha.

1.3. VISÃO GERAL DO AGENDAMENTO LVS

Uma das vantagens em se utilizar o LVS é a sua habilidade de atuação flexível, IP- balanceamento da carga de nível num pool de servidor real. Esta flexibilidade é devido a variedade de algoritmos

agendados que um administrador pode escolher quando configurando o LVS. O balanceamento de carga LVS é superior aos métodos de menor flexibilidade, como por exemplo a *Repetição Alternada DNS*, onde a natureza hierárquica do DNS e a captura por máquinas de clientes pode levar ao não balanceamento de carga. Além disso, a filtração de baixo nível empregada pelo roteador LVS possui vantagens sobre a solicitação da aplicação de nível enviada. Isto é devido às cargas de balanceamento, no nível dos pacotes da rede, causarem a mínima elevação de computação e permitirem uma boa escalabilidade.

Using scheduling, the active router can take into account the real servers' activity and, optionally, an administrator-assigned *weight* factor when routing service requests. Using assigned weights gives arbitrary priorities to individual machines. Using this form of scheduling, it is possible to create a group of real servers using a variety of hardware and software combinations and the active router can evenly load each real server.

O mecanismo de agendamento para o LVS é fornecido por uma coleção de patches (remendos) de kernel chamado módulos do *Servidor Virtual IP*. Estes módulos ativam a *camada 4* (*L4*)

Para rastrear e rotear os pacotes eficientemente, o IPVS constrói a *tabela IPVS* no kernel. Esta tabela é usada por um roteador LVS ativo para redirecionar solicitações do endereço do servidor virtual para os servidores reais, e retorná-los ao pool. A tabela IPVS é constantemente atualizada por uma utilidade chamada *ipvsadm* — da qual adiciona e remove os membros do cluster, dependendo na disponibilidade que os mesmos oferecem.

1.3.1. Agendamento de Algoritmos

The structure that the IPVS table takes depends on the scheduling algorithm that the administrator chooses for any given virtual server. To allow for maximum flexibility in the types of services you can cluster and how these services are scheduled, Red Hat Enterprise Linux provides the following scheduling algorithms listed below. For instructions on how to assign scheduling algorithms refer to Seção 4.6.1, “A Subseção do `SERVIDOR VIRTUAL`”.

Round-Robin Scheduling

Distribui cada solicitação seqüencialmente em volta do pool dos servidores reais. Usando este algoritmo, todos os servidores reais são tratados igualmente sem considerar a capacidade ou carga. Este modelo de agendamento parece-se ao DNS de repetição alternativa, porém mais granular uma vez que isto é uma conexão de rede baseada e não host baseada. O agendamento de repetição alternada LVS também não sofre as instabilidades causadas pelas questões DNS em cache.

Weighted Round-Robin Scheduling

Distributes each request sequentially around the pool of real servers but gives more jobs to servers with greater capacity. Capacity is indicated by a user-assigned weight factor, which is then adjusted upward or downward by dynamic load information. Refer to Seção 1.3.2, “Agendamento e Carga do Servidor” for more on weighting real servers.

O agendamento de repetição alternado é a escolha preferida caso existam diferenças significantes na capacidade de servidores reais no pool. No entanto, se uma solicitação de carga variar dinamicamente, o servidor de carga mais pesada talvez responda mais do que suas solicitações compartilhadas.

Least-Connection

Distribui mais solicitações aos servidores reais com poucas conexões ativas. A conexão mínima é um tipo de algoritmo de agendamento dinâmico, fazendo com que isto seja a melhor opção caso haja um alto grau de variações na carga solicitada. Isto é devido à conexão mínima controlar as conexões vivas para os servidores reais através da tabela IPVS. Isto é bastante adequado para um

pool de servidores reais, onde cada nó de membro possui aproximadamente a mesma capacidade. Caso um grupo de servidores possua a mesma capacidade, o agendamento de conexão mínima sobrecarregado será uma melhor escolha.

Weighted Least-Connections (default)

Distributes more requests to servers with fewer active connections relative to their capacities. Capacity is indicated by a user-assigned weight, which is then adjusted upward or downward by dynamic load information. The addition of weighting makes this algorithm ideal when the real server pool contains hardware of varying capacity. Refer to Seção 1.3.2, “Agendamento e Carga do Servidor” for more on weighting real servers.

Locality-Based Least-Connection Scheduling

Distribui mais solicitações aos servidores com poucas conexões ativas referentes a seus IPs de destino. Este algoritmo é designado para o uso do cluster de servidor de cache proxy. Isto roteia os pacotes para um endereço IP ao servidor daquele endereço, a não ser que o servidor esteja acima da capacidade e possua um servidor com metade da carga. Neste caso, isto determinará o endereço IP para o servidor real de carga mínima.

Locality-Based Least-Connection Scheduling with Replication Scheduling

Distribui mais solicitações para servidores com poucas conexões ativas relativas às suas destinações IPs. Este algoritmo é também designado para o uso num cluster de servidor de cache proxy. Isto difere de um Agendamento de Conexão Mínima Baseada Localmente pelo mapeamento do endereço IP alvo ao subconjunto de nós do servidor real. As solicitações são então roteadas para o servidor neste subconjunto com o número mínimo de conexões. Caso todos os nós do destino IP estiverem acima da capacidade, este replicará um novo servidor para o endereço IP de destino, adicionando o servidor real com conexões mínimas. Estas abrangem todo o pool de servidores reais ao subconjunto de servidores reais para o destino IP. O nó mais carregado desprende-se do subconjunto do servidor real para prevenir um número demasiado de replicações.

Destination Hash Scheduling

Distribui solicitações ao pool de servidores reais apenas observando o destino IP numa tabela hash estática. Este algoritmo é designado para o uso no cluster de servidor cache proxy.

Source Hash Scheduling

Distribui solicitações ao pool de servidores reais apenas observando o recurso IP numa tabela hash estática. Este algoritmo é designado para os roteadores LVS com firewalls múltiplos.

1.3.2. Agendamento e Carga do Servidor

O administrador do LVS pode determinar uma *carga* para cada nó no pool de servidor real. Esta carga é um valor integral do qual é fatorado em qualquer agendamento de *carga reconhecida* de algoritmos (como por exemplo conexões mínimas sobrecarregadas), e ajuda o roteador LVS a carregar o sofware mais uniformemente com diferentes capacidades.

As cargas trabalham com uma proporção relativa de uma à outra. Por exemplo, se um servidor real possue carga 1 e outro servidor possue carga 5, então o servidor com uma carga 5 obtém 5 conexões para cada conexão que outro servidor obter. O valor do padrão para a carga do servidor real é 1.

Embora o adicionamento de carga para variação das configurações do software num pool de servidor real poderá ajudar o balanceamento de carga mais eficientemente, isto poderá causar também balanços instáveis quando o servidor real for introduzido ao pool do servidor real, e o servidor virtual for agendado usando conexões mínimas sobrecarregadas. Por exemplo, vamos supor que há três

servidores no pool de servidor real. Os servidores A e B são carregados em 1 terço, e o servidor C em 2. Se o servidor C desconectar por algum motivo, os servidores A e B igualmente distribuem a carga abandonada. No entanto, uma vez que o servidor C voltar on-line, o roteador LVS visualizará que isto possui zero conexão e inunda o servidor com todas as solicitações até que isto faça par com os servidores A e B.

Para prevenir este fenômeno, os administradores podem realizar no servidor virtual um servidor *quiesce* — a qualquer instante que o nó de servidor real aparecer on-line. Desta maneira, a tabela de conexões mínimas é restaurada para zero e o roteador roteia as solicitações como se todos os servidores reais fossem recentemente adicionados ao cluster.

1.4. MÉTODOS DE ROTEAMENTO

A Red Hat Enterprise Linux usa a *Tradução do Endereço da Rede*ou *Roteamente NAT* para o LVS, do qual permite ao administrador uma grande flexibilidade quando utilizando o software disponível e integrando o LVS numa rede existente.

1.4.1. Roteamento NAT

Figura 1.3, “LVS Implemented with NAT Routing” , illustrates LVS utilizing NAT routing to move requests between the Internet and a private network.

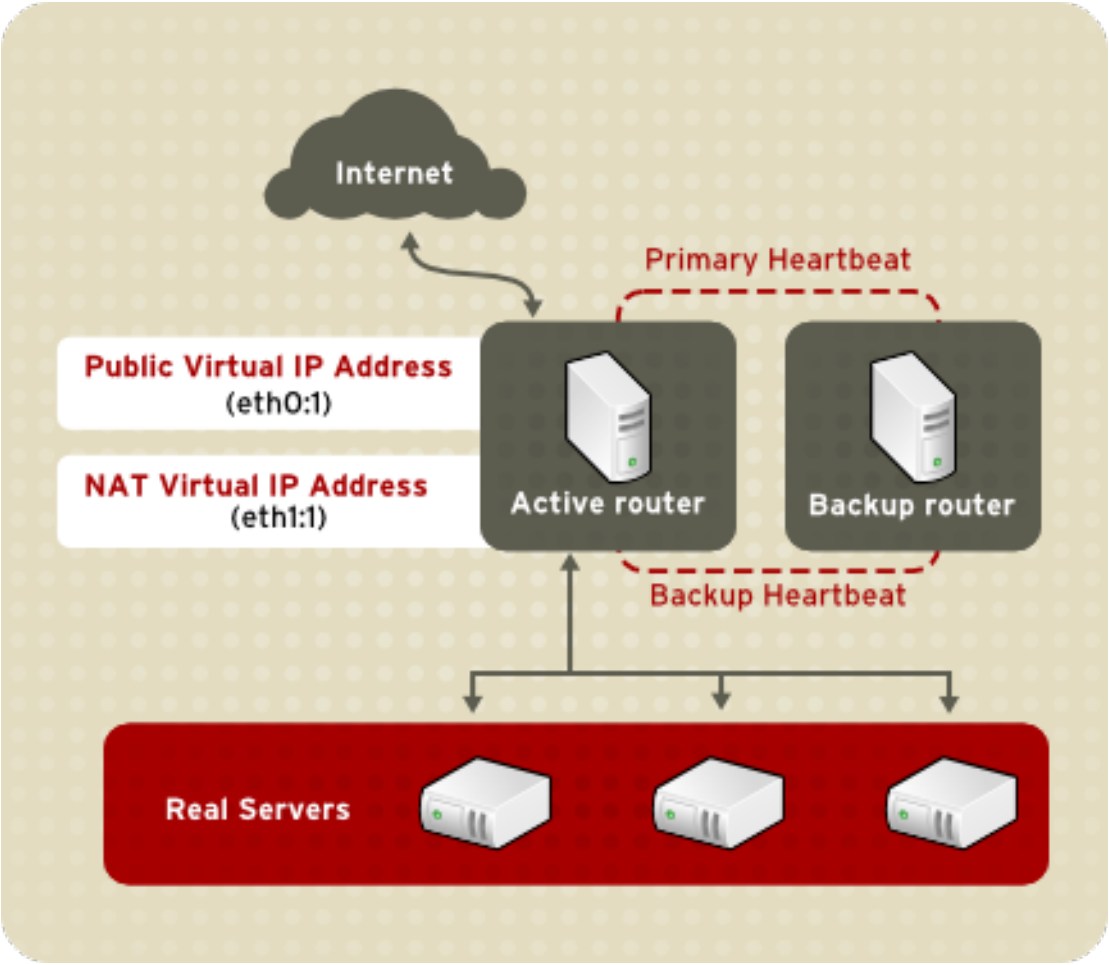


Figura 1.3. LVS Implemented with NAT Routing

Neste exemplo, existem dois NICs no roteador LVS ativo. O NIC para a Internet tem um *endereço IP real* no eth0 e endereço IP flutuante com alias para o eth0:1. O NIC para a interface da rede privada tem um endereço IP real no eth1, e possui um endereço IP flutuante com alias para o eth1:1. Num evento de falha, a interface virtual direcionada à Internet e a interface virtual direcionada à privada são

comandadas pelo roteador LVS de backup simultaneamente. Todos os demais servidores localizados na rede privada usam o IP flutuante para o roteador NAT, assim como a rota padrão para comunicar-se ao roteador LVS ativo. Desta forma, a habilidade deles de responder as solicitações da Internet não é debilitada.

In this example, the LVS router's public LVS floating IP address and private NAT floating IP address are aliased to two physical NICs. While it is possible to associate each floating IP address to its own physical device on the LVS router nodes, having more than two NICs is not a requirement.

Usando esta topologia, o roteador LVS ativo recebe a solicitação e a roteia ao servidor apropriado. O servidor real então processa a solicitação e retorna os pacotes ao roteador LVS, do qual usa a tradução do endereço da rede para substituir o endereço do servidor real nos pacotes com os endereços VIP público de roteadores LVS. Este processo é chamado *máscara IP*, pois os endereços IP atuais dos servidores reais estão escondidos dos clientes solicitantes.

Usando este roteamento NAT, os servidores reais podem ser qualquer tipo de máquina executando vários sistemas operantes. A maior desvantagem é que o roteador LVS pode começar um afunilamento em grande implantação de cluster, pois isto deve processar as solicitações de saída, como também as solicitações de entrada.

1.4.2. Roteamento Direto

Construindo uma configuração LVS, da qual usa o roteamento direto, proporciona um aumento benéfico do desempenho comparado às demais topologias da rede LVS. O roteamento direto permite os servidores reais processarem e rotearem os pacotes diretamente ao usuário solicitante, ao invés de passá-los através do roteador LVS. O roteamento direto reduz a possibilidade de problemas de desempenho da rede, removendo o trabalho do roteador LVS, para processar os pacotes de entrada apenas.

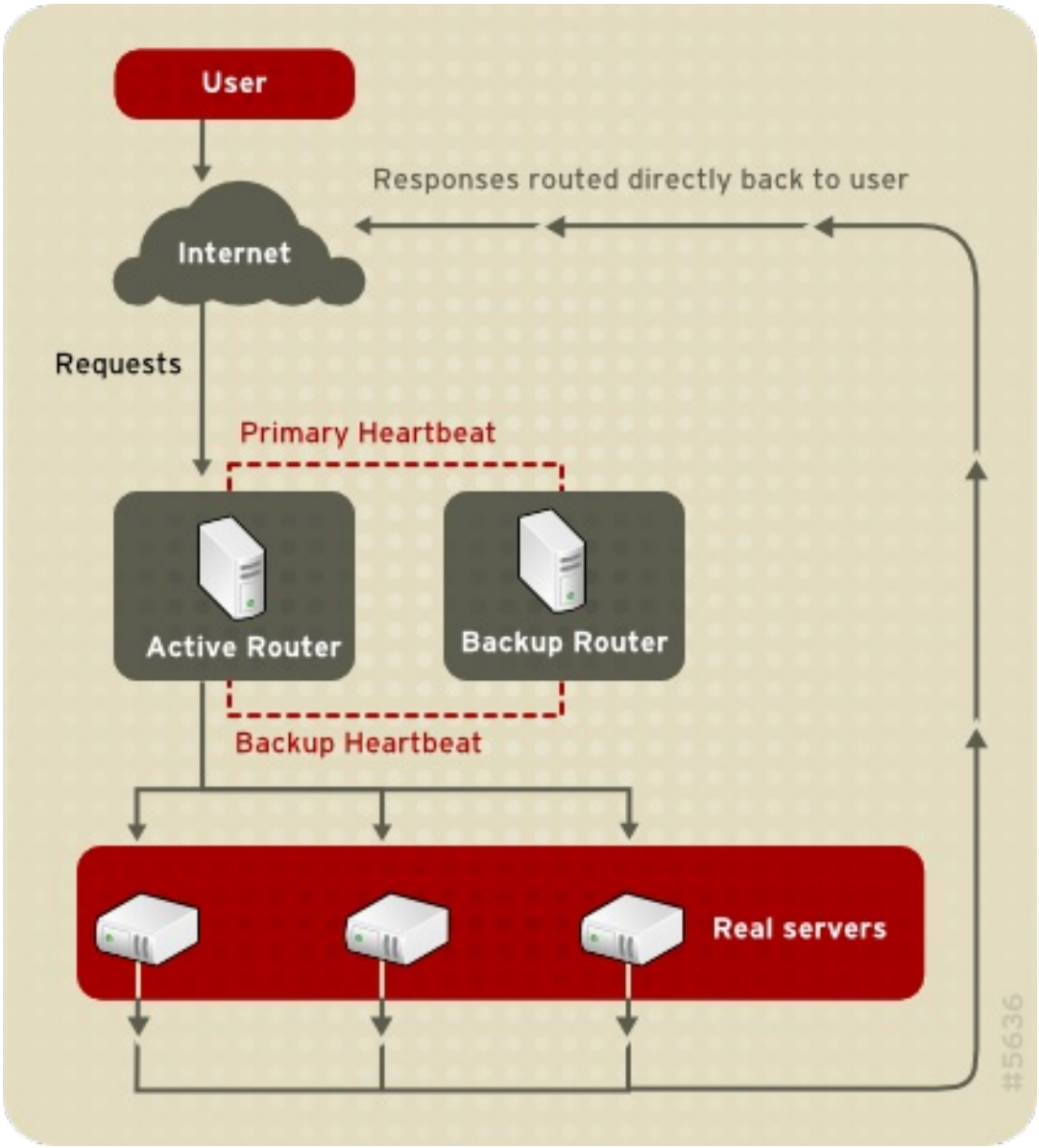


Figura 1.4. LVS Implemented with Direct Routing

Na típica configuração LVS do roteamento direto, o roteamento LVS recebe as solicitações do servidor de entrada através do IP virtual (VIP), e usa o algoritmo de agendamento para rotear a solicitação aos servidores reais. O servidor real processa a solicitação e envia a resposta diretamente ao cliente, contornando os roteadores LVS. Este método de roteamento permite que a escalabilidade daqueles servidores reais seja adicionada sem carga adicional no roteador LVS, para rotear os pacotes de saída de um servidor real ao cliente, do qual pode iniciar um afunilamento sob carga pesada da rede.

1.4.2.1. Roteamento Direto e Limitação do ARP

Enquanto existem muitas vantagens ao se utilizar o roteamento direto em LVS, existem também limitações. O problema mais comum com o LVS por meio de roteamento direto é com o *Protocolo de Resolução de Endereço* (ARP).

In typical situations, a client on the Internet sends a request to an IP address. Network routers typically send requests to their destination by relating IP addresses to a machine's MAC address with ARP. ARP requests are broadcast to all connected machines on a network, and the machine with the correct IP/MAC address combination receives the packet. The IP/MAC associations are stored in an ARP cache, which is cleared periodically (usually every 15 minutes) and refilled with IP/MAC associations.

O problema com as solicitações ARP, numa configuração LVS de roteamento direto, é o motivo pelo qual uma solicitação de um cliente a um endereço IP deve ser associado com o endereço MAC, para que a solicitação seja manuseada. Além disso, o endereço IP virtual do sistema LVS deve também ser associado ao MAC. No entanto, uma vez que o roteador LVS e todos os servidores reais possuírem o mesmo VIP, a solicitação ARP irá transmitir ed a todas as máquinas associadas com o VIP. Isto pode causar diversos problemas, como por exemplo o VIP ser associado diretamente a um dos servidores e processar solicitações diretamente, contornando o roteador LVS completamente e vencendo o propósito da configuração LVS.

Para resolver este problema, tenha certeza de que as solicitações de entrada são sempre enviadas ao roteador LVS ao invés de um dos servidores reais. Isto pode ser efetuado usando tanto o **`arptables_jf`** ou a ferramenta de filtragem do pacote **`iptables`** pelas seguintes razões:

- O **`arptables_jf`** previne o ARP de associar-se os VIPs com os servidores reais.
- O método **`iptables`** foge completamente do problema ARP, por não configurar os VIPs nos servidores reais, em primeiro lugar.

For more information on using **`arptables`** or **`iptables`** in a direct routing LVS environment, refer to Seção 3.2.1, “Roteamento Direto e **`arptables_jf`**” or Seção 3.2.2, “Roteamento Direto e **`iptables`**”.

1.5. PERSISTÊNCIA E MARCAS FIREWALL

Em algumas situações, será recomendável a um cliente conectar-se repetidamente ao mesmo servidor real, ao invés de ter um algoritmo de carga LVS enviando aquela solicitação ao melhor servidor disponível. Alguns exemplos destas situações incluem os formulários da web de página múltipla, cookies, SSL, e conexões FTP. Nestes casos, um cliente talvez não trabalhe propriamente, a não ser que a transação seja manuseada pelo mesmo servidor para reter o contexto. O LVS fornece dois recursos diferentes para cuidar disto: *persistência* e *marcas firewall*.

1.5.1. Persistência

A persistência atua como um cronômetro quando permitido. Uma vez que um cliente conecta-se a um serviço, o LVS se recorda da última conexão por um período específico de tempo. Se o endereço IP do mesmo cliente se conectar novamente naquele período, ele será enviado ao mesmo servidor que ele foi conectado previamente — contornando os mecanismos de balanceamento de carga. Quando uma conexão acontecer fora do período da janela, ela será manuseada de acordo com as regras de agendamento.

A Persistência também permite ao administrador especificar uma máscara subnet para aplicar um teste no endereço IP do cliente, como uma ferramenta para o controle dos quais os endereços possuam o nível mais alto de persistência, desta maneira agrupando as conexões à subnet.

Agrupamento de conexões destinadas a portais diferentes, pode ser importante para protocolos dos quais utilizam mais de um portal para comunicação, como por exemplo o FTP. No entanto, a persistência não é uma maneira eficiente para manusear o problema de agrupamento junto de conexões destinadas para portais diferentes. Para estas situações, é aconselhável se utilizar as *marcas firewall*.

1.5.2. Marcas Firewall

As marcas firewall são uma maneira fácil e eficiente para portais de grupo usados por um protocolo ou grupo de protocolos relacionados. Por exemplo, se o LVS é distribuído para operar num site de comércio eletrônico, as marcas firewall podem ser usadas para agrupar as conexões HTTP no portal 80

e assegurar as conexões HTTPS no portal 443. Para determinar a mesma marca firewall do servidor virtual para cada protocolo, coloque informações para que a transação possa ser preservada, uma vez que o roteador LVS envia todas as solicitações ao mesmo servidor real, após a conexão ser aberta.

Os administradores do LVS usam as marcas firewall ao invés da persistência, todas as vezes necessárias, para conexões de agrupamento. Isto é devido a sua eficiência e uso fácil. No entanto, os administradores devem continuar adicionando persistência aos servidores virtuais em conjunção às marcas firewall, para garantir que clientes sejam conectados ao mesmo servidor por um período adequado de tempo.

1.6. LVS — UM DIAGRAMA DE BLOCO

LVS routers use a collection of programs to monitor cluster members and cluster services. Figura 1.5, "LVS Components" illustrates how these various programs on both the active and backup LVS routers work together to manage the cluster.

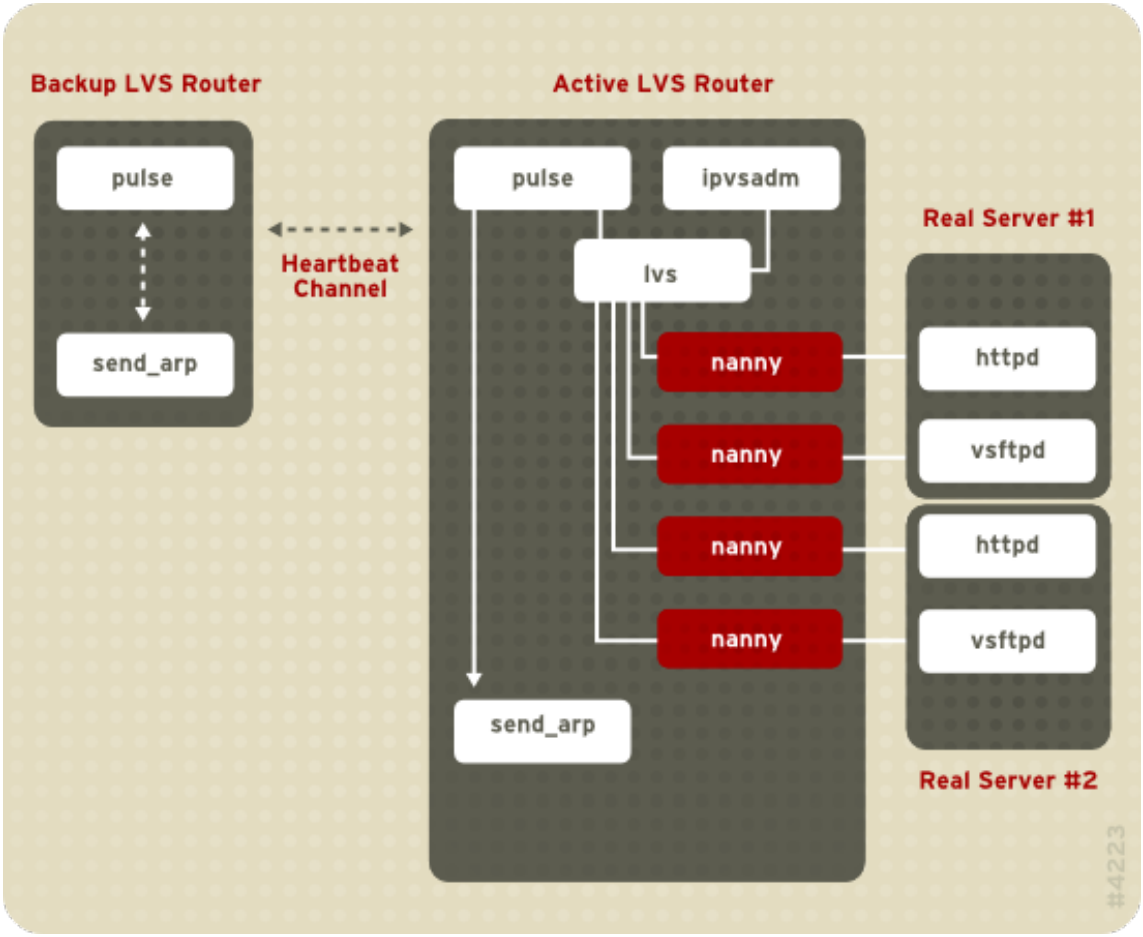


Figura 1.5. LVS Components

O daemon **pulse** atua em ambos roteadores LVS ativo e passivo. No roteador de backup, o **pulse** envia um *heartbeat* à interface pública do roteador ativo para certificar-se de que este está funcionando corretamente. No roteador ativo, o **pulse** inicia o daemon **lvs** e responde às solicitações *heartbeat* do roteador LVS de backup.

Uma vez inciado, o daemon **lvs** chama a utilidade **ipvsadm** para configurar e manter a tabela de roteamento IPVS no kernel e iniciar o processo **nanny**, para todo servidor virtual configurado em cada servidor real. Cada processo **nanny** checa o estado de um serviço configurado no servidor real, e

informa o daemon **lvs** se o serviço no servidor real possui mal funcionamento. Caso o mal funcionamento seja detectado, o daemon **lvs** instrui o **ipvsadm** a remover o servidor real da tabela de roteamento IPVS.

Caso o roteador de backup não receber uma resposta do roteador ativo, ele iniciará a falha chamando o **send_arp** para reinstalar todos os endereços IP virtuais aos endereços de software NIC (endereços *MAC*) do nó de backup. Ele então envia um comando para o roteador ativo por meio das interfaces da rede pública e privada para desligar o daemon **lvs** no roteador ativo, e iniciar o daemon **lvs** no nó de backup, para aceitar solicitações dos servidores virtuais configurados.

1.6.1. LVS Components

Seção 1.6.1.1, “**pulse**” shows a detailed list of each software component in an LVS router.

1.6.1.1. pulse

This is the controlling process which starts all other daemons related to LVS routers. At boot time, the daemon is started by the **/etc/rc.d/init.d/pulse** script. It then reads the configuration file **/etc/sysconfig/ha/lvs.cf**. On the active router, **pulse** starts the LVS daemon. On the backup router, **pulse** determines the health of the active router by executing a simple heartbeat at a user-configurable interval. If the active router fails to respond after a user-configurable interval, it initiates failover. During failover, **pulse** on the backup router instructs the **pulse** daemon on the active router to shut down all LVS services, starts the **send_arp** program to reassign the floating IP addresses to the backup router's MAC address, and starts the **lvs** daemon.

1.6.1.2. lvs

O daemon **lvs** atua no roteador LVS ativo uma vez chamado pelo **pulse**. Isto lê o arquivo de configuração **/etc/sysconfig/ha/lvs.cf**, chama a utilidade **ipvsadm** para construir e manter a tabela de roteamento IPVS, e determina um processo **nanny** para cada serviço LVS configurado. Caso o **nanny** relatar que um servidor real está fora, o **lvs** irá instruir a utilidade **ipvsadm** para remover o servidor real da tabela de roteamento IPVS.

1.6.1.3. ipvsadm

Este serviço atualiza a tabela de roteamento no kernel. O daemon **lvs** ativa e administra o LVS chamando o **ipvsadm** para adicionar, mudar ou deletar entradas na tabela de roteamento IPVS.

1.6.1.4. nanny

O monitoramento daemon **nanny** atua no roteador LVS ativo. Através deste daemon, o roteador ativo determina o health de cada servidor, e opcionalmente monitora sua carga de trabalho. Cada serviço definido no servidor real possui um processo separado.

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

Este é o arquivo de configuração LVS. Diretamente ou indiretamente, todos os daemons buscam suas informações de configuração deste arquivo.

1.6.1.6. Piranha Configuration Tool

Esta é a ferramenta baseada na Web para monitoramento, configuração e administração do LVS. Esta é a ferramenta padrão para manter o arquivo de configuração LVS `/etc/sysconfig/ha/lvs.cf`.

1.6.1.7. `send_arp`

Este programa envia a difusão ARP quando o endereço IP flutuante muda de um nó para outro durante a falha.

Capítulo 2, *Configuração LVS Inicial* reviews important post-installation configuration steps you should take before configuring Red Hat Enterprise Linux to be an LVS router.

CAPÍTULO 2. CONFIGURAÇÃO LVS INICIAL

Após a instalação do Red Hat Enterprise Linux, você deve seguir alguns passos básicos para configurar tanto os roteadores LVS quanto os servidores reais. Este capítulo abrange detalhadamente estes passos iniciais.

NOTA

O nó do roteador LVS, que torna-se o nó ativo uma vez que o LVS é iniciado, e é também referido com um *nó primário*. Quando você for configurar o LVS, utilize a **Piranha Configuration Tool** no nó primário.

2.1. SERVIÇOS DE CONFIGURAÇÃO NOS ROTEADORES LVS

O programa de instalação da Red Hat Enterprise Linux instala todos os componentes requeridos para configurar o LVS, porém os serviços apropriados devem ser ativados antes da configuração do LVS. Configure os serviços apropriados para os dois roteadores no período de inicialização. Existem três ferramentas primárias disponíveis de configuração de serviços para ativar o período de inicialização sob a Red Hat Enterprise Linux: o programa de linha de comando **chkconfig**, o programa baseado-ncurses **ntsysv** e a **Services Configuration Tool** gráfica. Todas estas ferramentas requerem o acesso ao root.

NOTA

Para alcançar o acesso ao root, abra um envelope de aviso e use o comando **su -** acompanhado da senha da root. Por exemplo:

```
$ su - root password
```

Existem três serviços, nos roteadores LVS, que precisam ser configurados para a ativação no período de inicialização:

- O serviço **piranha-gui** (apenas no nó primário)
- O serviço **pulse**
- O serviço **sshd**

Caso você esteja aplicando clustering nos serviços multi-port ou usando as marcas firewall, você deverá ativar também o serviço **iptables**.

É recomendável configurar estes serviços para ativar tanto o nível de execução 3 (runlevel 3) como também o nível de execução 5. Para efetuar isto usando o **chkconfig**, digite o seguinte comando para cada serviço:

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

No comando acima, substitua o *daemon* com o nome do serviço em que você está ativando. Para acessar a lista de serviços no sistema assim como em qual o nível de execução em que eles estão configurados, aplique o seguinte comando:

/sbin/chkconfig --list

ATENÇÃO

Turning any of the above services on using **chkconfig** does not actually start the daemon. To do this use the **/sbin/service** command. See Seção 2.3, “Iniciando o Serviço da **Piranha Configuration Tool**” for an example of how to use the **/sbin/service** command.

For more information on runlevels and configuring services with **ntsysv** and the **Services Configuration Tool**, refer to the chapter titled *"Controlling Access to Services"* in the *Red Hat Enterprise Linux System Administration Guide*.

2.2. CONFIGURANDO A SENHA PARA A PIRANHA CONFIGURATION TOOL

Antes de se utilizar a **Piranha Configuration Tool** pela primeira vez no roteador LVS primário, você deverá restringir o acesso à ela, criando uma senha. Para isto, logon como root e edite o seguinte comando:

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

Após a entrada deste comando, crie a senha administrativa quando solicitada.

ATENÇÃO

Para a senha ser mais segura, ela não poderá conter nomes próprios, comumente conhecidos como acrônimos, ou palavras de um dicionário de qualquer linguagem. Não deixe a senha codificada em qualquer lugar no sistema.

Caso a senha seja modificada durante uma seção ativa da **Piranha Configuration Tool**, será requerido ao administrador a criação de uma nova senha.

2.3. INICIANDO O SERVIÇO DA PIRANHA CONFIGURATION TOOL

Após você ter definido a senha para a **Piranha Configuration Tool**, inicie ou reinicie o serviço localizado em **/etc/rc.d/init.d/piranha-gui**. Para realizar isto, digite o seguinte comando como root:

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

or

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

Issuing this command starts a private session of the Apache HTTP Server by calling the symbolic link

/usr/sbin/piranha_gui -> /usr/sbin/httpd. For security reasons, the **piranha-gui** version of **httpd** runs as the piranha user in a separate process. The fact that **piranha-gui** leverages the **httpd** service means that:

1. O Apache HTTP Server deve ser instalado no sistema.
2. A interrupção ou reinicialização do Apache HTTP Server por meio do comando **serviço**, interromperá o serviço **piranha-gui**.

ATENÇÃO

Caso o comando **/sbin/service httpd stop** ou **/sbin/service httpd restart** for editado num roteador LVS, você deverá iniciar o serviço **piranha-gui** editando o seguinte comando:

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

The **piranha-gui** service is all that is necessary to begin configuring LVS. However, if you are configuring LVS remotely, the **sshd** service is also required. You do *not* need to start the **pulse** service until configuration using the **Piranha Configuration Tool** is complete. See Seção 4.8, “Iniciando o LVS” for information on starting the **pulse** service.

2.3.1. Configurando o Portal do Servidor da Web Piranha Configuration Tool

A **Piranha Configuration Tool** atua por padrão no portal 3636. Para a efetuação de mudança deste número do portal, mude a linha **Listen 3636** na Seção 2 do arquivo de configuração da Web **piranha-gui /etc/sysconfig/ha/conf/httpd.conf**.

Para o uso da **Piranha Configuration Tool**, você precisará no mínimo de um texto do navegador da Web apenas. Caso você inicie um navegador da Web num roteador LVS primário, abra o **http://*localhost*:3636** local. Você pode alcançar a **Piranha Configuration Tool** de qualquer lugar por meio do navegador da Web substituindo o *localhost* com o hostname (nome anfitrião) ou endereço IP do roteador LVS primário.

Quando o seu navegador conectar à **Piranha Configuration Tool**, você deverá logon ao acesso dos serviços de configuração. Entre **piranha** no campo **Nome do usuário** e a senha configurada com a **piranha-passwd** no campo **Senha**.

Agora que a **Piranha Configuration Tool** está sendo executada, você talvez queira considerar a limitação dos que têm acesso à ferramenta na rede. A próxima seção revisa as maneiras para efetuar esta tarefa.

2.4. LIMITANDO O ACESSO À PIRANHA CONFIGURATION TOOL

A **Piranha Configuration Tool** informa uma combinação válida de nome do usuário e senha. No entanto, devido a todos os dados serem passados à **Piranha Configuration Tool**, isto é um texto plano. É recomendável que você restrinja o acesso apenas às redes de confiança ou da máquina local.

The easiest way to restrict access is to use the Apache HTTP Server's built in access control

mechanisms by editing **/etc/sysconfig/ha/web/secure/.htaccess**. After altering the file you do not have to restart the **piranha-gui** service because the server checks the **.htaccess** file each time it accesses the directory.

Por padrão, o controle de acesso ao diretório permite qualquer um visualizar o conteúdo deste diretório. Segue abaixo uma amostra do acesso padrão:

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

Para limitar o acesso da **Piranha Configuration Tool** apenas ao localhost (anfitrião local), mude o arquivo **.htaccess** para permitir o acesso de apenas um disparador de auto-retorno (127.0.0.1). Para maiores informações sobre o disparador de auto-retorno, veja o capítulo titulado como *Scripts da Rede* na *Red Hat Enterprise Linux Reference Guide*

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

Você pode também permitir hosts ou subnets específicos como segue no exemplo abaixo:

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

Neste exemplo, apenas os navegadores de máquina com o endereço IP 192.168.1.100 e máquinas na rede 172.16.57/24 podem acessar a **Piranha Configuration Tool**.

ATENÇÃO

Editando o arquivo **Piranha Configuration Tool** **.htaccess** limitará o acesso às páginas configuradas no diretório **/ etc/sysconfig/ha/web/secure/**, mas não ao logon e páginas de ajuda no **/etc/sysconfig/ha/web/**. Para limitar o acesso a este diretório, crie um arquivo **.htaccess** no diretório **/etc/sysconfig/ha/web/** com **pedido**, **solicitação**, e linhas **deny** idênticas a **/etc/sysconfig/ha/web/secure/.htaccess**.

2.5. LIGANDO PACOTE DE ENCAMINHAMENTO

Para que o roteador LVS envie os pacotes da rede propriamente ao servidor real, cada nó do roteador LVS deve possuir o enviado IP ativado ao kernel. Logon como root e mude a linha que lê o **net.ipv4.ip_forward = 0** no **/etc/sysctl.conf** para o seguinte:

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

As mudanças terão efeito uma vez que você reiniciar o sistema.

Para checar se o enviado IP está ativado, edite o seguinte comando como root:

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

Caso o comando acima retornar a **1**, conseqüentemente o enviado IP será desativado. Caso isto retorne a **0**, você poderá ativá-lo manualmente usando o seguinte comando:

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

2.6. CONFIGURANDO SERVIÇOS NOS SERVIDORES REAIS

Caso os servidores reais forem sistemas da Red Hat Enterprise Linux, configure os apropriados servidores daemons para ativado no período de inicialização. Estes daemons podem incluir o **httpd** para serviços da Web ou **xinetd** para FTP ou serviços Telnet.

É recomendável também acessar os servidores reais remotamente. Desta forma, o daemon **sshd** deverá também ser instalado e ativado.

CAPÍTULO 3. CONFIGURANDO O LVS

O LVS consiste em dois grupos básicos: os roteadores LVS e os servidores reais. Para previnir um único ponto de falha, cada grupo deve conter pelo menos dois sistemas membros.

O grupo de roteador LVS deve consistir em dois sistemas idênticos ou bem similar executando a Red Hat Enterprise Linux. Um irá atuar como roteador LVS ativo enquanto que o outro permanecerá no modo standby ativo, desta forma eles precisam ter capacidades bem parecidas.

Antes de escolher e configurar o hardware para o grupo do servidor real, você deve decidir qual dos três tipos de topologia LVS a ser usado.

3.1. A REDE LVS-NAT

A topologia NAT permite uma notável latitude em se utilizar o hardware existente, porém é limitada em sua habilidade de manusear cargas volumosas, devido ao fato de que todos os pacotes que entram e saem do cluster passam pelo roteador LVS.

Layout da Rede

A topologia para o LVS utilizando o roteamento NAT é a mais fácil de ser configurada, de uma perspectiva do layout da rede, devido ao cluster precisar apenas de um ponto de acesso à rede pública. Os servidores reais passam todas as solicitações de volta através do roteador LVS, desta forma eles estarão na própria rede privada.

Hardware

A topologia NAT é a mais flexível em termos de hardware, devido aos servidores reais não precisarem estar nas máquinas Linux para funcionar corretamente. Numa topologia NAT, cada servidor real apenas precisa de um NIC uma vez que isto estará apenas respondendo ao roteador LVS. Por outro lado, os roteadores LVS precisam de dois NICs cada para rotear o tráfego entre duas redes. Devido a esta topologia criar uma rede de afunilamento no roteador LVS, o Ethernet gigabit NICs pode ser implantado em cada roteador LVS para aumentar a largura da banda que os roteadores LVS podem suportar. Caso o Ethernet gigabit seja implantado nos roteadores LVS, qualquer conexão de troca dos servidores reais aos roteadores LVS devem ter pelo menos dois portais Ethernet gigabit para identificar a carga eficientemente.

Software

Devido a topologia NAT requerer o uso de `iptables` para algumas configurações, pode existir um número regulado de configuração de software fora da **Piranha Configuration Tool**. Particularmente, os serviços FTP e o uso das marcas firewall requerem uma configuração extra manual dos roteadores LVS à apropriada solicitação de roteador.

3.1.1. Interfaces da Rede Configurada pelo LVS com NAT

To set up LVS with NAT, you must first configure the network interfaces for the public network and the private network on the LVS routers. In this example, the LVS routers' public interfaces (`eth0`) will be on the 192.168.26/24 network (I know, I know, this is not a routable IP, but let us pretend there is a firewall in front of the LVS router for good measure) and the private interfaces which link to the real servers (`eth1`) will be on the 10.11.12/24 network.

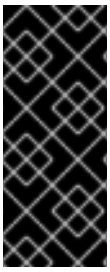
So on the active or *primary* LVS router node, the public interface's network script, `/etc/sysconfig/network-scripts/ifcfg-eth0`, could look something like this:

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

O **/etc/sysconfig/network-scripts/ifcfg-eth1** para a interface NAT privada no roteador LVS pode ser similar a:

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

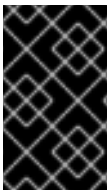
In this example, the VIP for the LVS router's public interface will be 192.168.26.10 and the VIP for the NAT or private interface will be 10.11.12.10. So, it is essential that the real servers route requests back to the VIP for the NAT interface.



IMPORTANTE

The sample Ethernet interface configuration settings in this section are for the real IP addresses of an LVS router and *not* the floating IP addresses. To configure the public and private floating IP addresses the administrator should use the **Piranha Configuration Tool**, as shown in Seção 4.4, “**GLOBAL SETTINGS**” and Seção 4.6.1, “A Subseção do **SERVIDOR VIRTUAL**”.

After configuring the primary LVS router node's network interfaces, configure the backup LVS router's real network interfaces — taking care that none of the IP address conflict with any other IP addresses on the network.

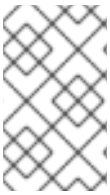


IMPORTANTE

Certifique-se que cada interface no nó de backup serve a mesma rede com a interface no nó primário. Por exemplo, se o eth0 conectar a mesma rede pública no nó primário, isto deverá também se comunicar a rede pública no nó de backup.

3.1.2. Roteadores em Servidores Reais

O mais importante é lembrar que quando configurando as interfaces da rede de servidores reais numa topologia NAT, a porta de ligação deve ser ajustada para o endereço IP flutuante do roteador LVS. Neste exemplo, o endereço será 10.11.12.10.



NOTA

Once the network interfaces are up on the real servers, the machines will be unable to ping or connect in other ways to the public network. This is normal. You will, however, be able to ping the real IP for the LVS router's private interface, in this case 10.11.12.8.

So the real server's **/etc/sysconfig/network-scripts/ifcfg-eth0** file could look similar to this:

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

ATENÇÃO

Caso um servidor real tiver mais de uma interface de rede configurada com a linha **GATEWAY=**, a primeira a aparecer chegará à saída. Portanto, caso os dois **eth0** e **eth1** sejam configurados e o **eth1** for usado para LVS, os servidores reais talvez não roteiem as solicitações apropriadamente.

É recomendável desligar as interfaces da rede externa configurando **ONBOOT=no** nos scripts da rede, com o diretório **/etc/sysconfig/network-scripts/** ou garantindo que a porta de comunicação está corretamente adaptada na rede, da qual será a primeira a aparecer.

3.1.3. Ativando os Roteadores NAT em Roteadores LVS

In a simple NAT LVS configuration where each clustered service uses only one port, like HTTP on port 80, the administrator needs only to enable packet forwarding on the LVS routers for the requests to be properly routed between the outside world and the real servers. See Seção 2.5, “Ligando Pacote de Encaminhamento” for instructions on turning on packet forwarding. However, more configuration is necessary when the clustered services require more than one port to go to the same real server during a user session. For information on creating multi-port services using firewall marks, see Seção 3.4, “Serviços de Portal Múltiplo e LVS” .

Once forwarding is enabled on the LVS routers and the real servers are set up and have the clustered services running, use the **Piranha Configuration Tool** to configure LVS as shown in Capítulo 4, *Configurando os roteadores LVS com a**Piranha Configuration Tool***.

ATENÇÃO

Do not configure the floating IP for **eth0:1** or **eth1:1** by manually editing network scripts or using a network configuration tool. Instead, use the **Piranha Configuration Tool** as shown in Seção 4.4, “**GLOBAL SETTINGS**” and Seção 4.6.1, “A Subseção do **SERVIDOR VIRTUAL**”.

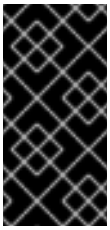
When finished, start the **pulse** service as shown in Seção 4.8, “Iniciando o LVS”. Once **pulse** is up and running, the active LVS router will begin routing requests to the pool of real servers.

3.2. ROTEAMENTO DIRETO POR MEIO DO LVS

As mentioned in Seção 1.4.2, “Roteamento Direto”, direct routing allows real servers to process and route packets directly to a requesting user rather than passing outgoing packets through the LVS router. Direct routing requires that the real servers be physically connected to a network segment with the LVS router and be able to process and direct outgoing packets as well.

Layout da Rede

Em uma configuração LVS de roteamento direto, o roteador LVS precisa receber as solicitações de entrada e roteá-las para o apropriado servidor real a ser processado. Os servidores reais então precisam rotear *diretamente* uma resposta ao cliente. Por exemplo, se um cliente estiver na Internet e enviar o pacote através do roteador LVS a um servidor real, o servidor real deve ser capaz de ir diretamente ao cliente via internet. Isto pode ser efetuado apenas configurando a entrada do servidor real para passar pacotes à Internet. Cada servidor no pool do servidor pode ter a sua própria entrada separada (e cada entrada com a sua própria conexão de Internet), permitindo o máximo rendimento e escalabilidade. No entanto, para configurações LVS típicas, os servidores reais podem se comunicar através de uma entrada (e portanto uma conexão da rede).



IMPORTANTE

Não é aconselhável usar o roteador LVS como uma saída aos servidores reais, pois isto adiciona complexidades de configurações desnecessárias como também a carga da rede no roteador LVS. Esta reintroduz o afinilamento da rede existente num roteador NAT.

Hardware

Os requerimentos do hardware de um sistema LVS usando o roteamento direto é similar às outras topologias LVS. Enquanto que o roteador precisa ser executado pela Red Hat Enterprise Linux para processar as solicitações de entrada e desempenho de balanceamento de carga para os servidores reais, onde estes não precisam ser máquinas LINUX para funcionar corretamente. Cada roteador LVS precisa de um ou dois NICs (dependendo se há um roteador de backup). Você pode usar dois NICs para fácil configuração e tráfego separado distinguível —as solicitações de entrada são manuseadas por um NIC e os pacotes roteados aos servidores reais por solicitação.

Uma ligação à Internet é requerida, uma vez que os servidores reais contornem o roteador e enviem os pacotes de saída diretamente ao cliente. Para melhor desempenho e disponibilidade, cada servidor real pode ser conectado à sua própria entrada separada, da qual possue a própria conexão dedicada à rede portadora em que o cliente é conectado (como por exemplo a Internet ou Intranet)

Software

There is some configuration outside of **Piranha Configuration Tool** that needs to be done, especially for administrators facing ARP issues when using LVS via direct routing. Refer to Seção 3.2.1, “Roteamento Direto e `arptables_jf`” or Seção 3.2.2, “Roteamento Direto e `iptables`” for more information.

3.2.1. Roteamento Direto e `arptables_jf`

In order to configure direct routing using **`arptables_jf`**, each real server must have their virtual IP address configured, so they can directly route packets. ARP requests for the VIP are ignored entirely by the real servers, and any ARP packets that might otherwise be sent containing the VIPs are mangled to contain the real server's IP instead of the VIPs.

Usando o método **arptables_jf**, os aplicativos talvez liguem-se a cada IP individual ou portal do qual o servidor real está prestando serviço. Por exemplo, o método **arptables_jf** permite instâncias múltiplas do Apache HTTP Server sejam explicitamente limitadas à execução de diferentes VIPs no sistema. Existem também vantagens significantes de desempenho para usar as **arptables_jf** sobre a opção **iptables**.

No entanto, usando o método **arptables_jf**, os VIPs não podem ser configurados para começar a inicialização usando as ferramentas de configuração do sistema da Red Hat Enterprise Linux padrão.

Para configurar cada servidor real com o intuito de ignorar as solicitações ARP de cada endereço IP virtual, utilize os seguintes passos:

1. Crie as entradas da tabela ARP para cada endereço IP virtual em cada servidor real (o real_ip é o IP que o diretor usa para se comunicar com o servidor real; freqüentemente isto é o IP vinculado ao **eth0**):

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

   Isto induzirá os servidores reais a ignorem todas as solicitações ARP para os endereços IP virtuais, e alterarem qualquer saída de respostas ARP, que de outra forma talvez possuam o IP virtual, em vez do servidor. O único nó que deve responder às solicitações ARP, para qualquer VIPs, é o atual nó LVS ativo.

2. Uma vez que isto tenha sido completado em cada servidor real, salve as entradas de tabela ARP digitando os seguintes comandos em cada servidor real:

   service arptables_jf save

   chkconfig --level 2345 arptables_jf on

   O comando **chkconfig** irá induzir o sistema a recarregar as configurações arptables na inicialização — antes da rede ser iniciada.

3. Configure o endereço IP virtual em todos os servidores usando **ifconfig** para criar um IP com alias. Por exemplo:

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

   Ou usando a utilidade **iproute2 ip**, por exemplo:

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

   Como visto anteriormente, os endereços IP não podem ser configurados para começar a inicialização usando as ferramentas de configuração do sistema da Red Hat. Uma maneira de trabalhar com este problema será colocando estes comandos em **/etc/rc.d/rc.local**.

4. Configure Piranha for Direct Routing. Refer to Capítulo 4, *Configurando os roteadores LVS com a **Piranha Configuration Tool*** for more information.

3.2.2. Roteamento Direto e iptables

Você irá também trabalhar no problema ARP usando o método do roteamento direto criando as regras

do firewall de **iptables**. Para configurar o roteamento direto usando as **iptables**, você deve adicionar regras que criam um proxy transparente. Com isto, um servidor real irá enviar os pacotes de serviços ao endereço VIP, mesmo que o endereço IP não exista no sistema.

O método das **iptables** é mais simples de se configurar do que o método **arptables_jf**. Este método também ilude inteiramente o problema ARP LVS, pois o(s) endereço (s) apenas existe no diretor LVS ativo.

No entanto, existem problemas de desempenho quando usando o método **iptables** comparado às **arptables_jf**, pois há elevação no encaminhamento/mascaramento de cada pacote.

Você não pode reutilizar os portais usando o método **iptables**. Por exemplo, não é possível executar dois serviços do Apache HTTP Server separados, com limite ao portal 80, pois ambos devem atar-se ao ***INADDR_ANY*** ao invés dos endereços IP virtuais.

Para configurar o roteamento direto no método de **iptables**, use os passos seguintes:

1. Um em cada servidor real, executa o seguinte comando para cada VIP, portal e combinação (TPC ou UDP) de protocolo, cuja intenção é de ser servido pelo servidor real:

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

   Este comando irá induzir os servidores reais a processarem os pacotes destinados pelo VIP e portal em que eles estão determinados.

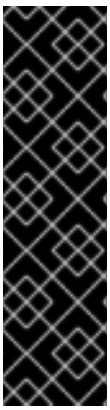
2. Salve a configuração em cada servidor real:

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

   Os comandos acima induzem o sistema a recarregar a configuração das **iptables** no bootup — antes da rede ser inicializada.

3.3. COMBINANDO A CONFIGURAÇÃO

Após determinar qual dos métodos de roteamento anteriores a ser utilizado, o hardware deve ser ligado juntamente na rede.



IMPORTANTE

Os dispositivos do adaptador nos roteadores LVS devem ser configurados para acessar as mesmas redes. Por exemplo, se o **eth0** se conectar a rede pública e **eth1** se conectar a rede privada, então estes mesmos dispositivos no roteador LVS de backup devem se conectar às mesmas redes.

Além disso, a saída listada na primeira interface a aparecer no tempo de inicialização, será adicionada à mesma tabela de roteamento, e as subseqüentes saídas listadas em outras interfaces serão ignoradas. Isto é especialmente importante em se considerar quando configurando os servidores reais.

Após a conexão física juntamente com o hardware do cluster, configure as interfaces da rede nos roteadores primários e de backup. Isto pode ser feito usando a aplicação gráfica como **system-config-network** ou editando os scripts manualmente. Para maiores informações sobre como adicionar

dispositivos usando **system-config-network**, veja o capítulo chamado *Configuração da Rede* no *Guia de Implantação da Red Hat Enterprise Linux*. O resto deste capítulo mostrará exemplos de alterações para as interfaces da rede a serem feitas tanto manualmente ou através da **Piranha Configuration Tool**.

3.3.1. Dicas Diversas de Rede LVS

Configure o endereço IP real para ambas as redes públicas e privadas nos roteadores antes de tentar configurar o cluster usando a **Piranha Configuration Tool**. As seções em cada topologia dão um exemplo dos endereços da rede, mas os endereços da rede atual são necessários. Abaixo são alguns dos programas úteis para criação das interfaces da rede ou checagem do estado delas.

Trazendo Interfaces da Rede Geral

Para criar uma interface da rede real, utilize o seguinte comando com o root, substituindo *N* com o número correspondente a interface (`eth0` e `eth1`).

```
/sbin/ifup ethN
```

ATENÇÃO

Do *not* use the `ifup` scripts to bring up any floating IP addresses you may configure using **Piranha Configuration Tool** (`eth0:1` or `eth1:1`). Use the `service` command to start `pulse` instead (see Seção 4.8, “Iniciando o LVS” for details).

Baixando as Interfaces da Rede Real

Para baixar a interface da rede real, use o seguinte comando como root, substituindo *N* com o número correspondente à interface (`eth0` e `eth1`).

```
/sbin/ifdown ethN
```

Checando o Status das Interfaces da Rede

Caso você precise checar qual das interfaces da rede estão ativas em qualquer momento solicitado, digite o seguinte:

```
/sbin/ifconfig
```

Para verificar a tabela de roteamento para a máquina, edite o seguinte comando:

```
/sbin/route
```

3.4. SERVIÇOS DE PORTAL MÚLTIPLO E LVS

LVS routers under any topology require extra configuration when creating multi-port LVS services. Multi-port services can be created artificially by using firewall marks to bundle together different, but related protocols, such as HTTP (port 80) and HTTPS (port 443), or when LVS is used with true multi-port protocols, such as FTP. In either case, the LVS router uses firewall marks to recognize that packets destined for different ports, but bearing the same firewall mark, should be handled identically.

Also, when combined with persistence, firewall marks ensure connections from the client machine are routed to the same host, as long as the connections occur within the length of time specified by the persistence parameter. For more on assigning persistence to a virtual server, see Seção 4.6.1, “A Subseção do **SERVIDOR VIRTUAL**”.

Infelizmente, o mecanismo usado para balancear as cargas nos servidores reais — IPVS — pode reconhecer as marcas firewall designadas ao pacote, mas não pode designar as marcas firewall por si mesmo. O trabalho das marcas firewall de *designação* deve ser desempenhado pelo filtro do pacote da rede, **iptables**, fora da **Piranha Configuration Tool**.

3.4.1. Designando Marcas Firewall

Para determinar as marcas firewall para o pacote destinado ao portal específico, o administrador deve usar **iptables**.

This section illustrates how to bundle HTTP and HTTPS as an example; however, FTP is another commonly clustered multi-port protocol. If an LVS is used for FTP services, refer to Seção 3.5, “Configurando o FTP” for configuration details.

A regra básica para lembrar de quando se utilizar as marcas firewall é a seguinte: cada protocolo que utiliza a marca firewall na **Piranha Configuration Tool**, possui uma regra **iptables** comensurável designando as marcas aos pacotes da rede.

Antes de criar as regras do filtro do pacote da rede, tenha certeza de que não hajam regras existentes. Para isto, abra o envelope de aviso, logon como root e digite:

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

Caso as **iptables** não estiverem sendo executadas, o aviso aparecerá instantaneamente.

Caso as **iptables** estiverem ativas, elas exibirão o conjunto de regras. Caso as regras estejam presentes, digite o seguinte comando:

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

Caso as regras já estejam colocadas, será importante checar os conteúdos do **/etc/sysconfig/iptables** e copiar qualquer regra que seja importante guardar num lugar seguro antes de prosseguir.

Segue abaixo as regras que determinam a mesma marca firewall, 80, ao tráfego de entrada destinado ao endereço IP flutuante, *n.n.n.n*, nos portais 80 e 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
```

For instructions on assigning the VIP to the public network interface, see Seção 4.6.1, “A Subseção do **SERVIDOR VIRTUAL**”. Also note that you must log in as root and load the module for **iptables** before issuing rules for the first time.

Nos comandos **iptables** acima, o *n.n.n.n* deve ser substituído com o IP flutuante para o seus servidores virtuais HTTP e HTTPS. Estes comandos têm o efeito net de designar qualquer tráfego

endereçado ao VIP nos portais apropriados à uma marca firewall de 80, que em atividade é reconhecida por IPVS e envios apropriados.

ATENÇÃO

The commands above will take effect immediately, but do not persist through a reboot of the system. To ensure network packet filter settings are restored upon reboot, refer to Seção 3.6, “Salvando as Configurações do Filtro do Pacote da Rede”

3.5. CONFIGURANDO O FTP

O Protocolo de Transporte de Arquivo (File Transport Protocol, FTP) é um antigo e complexo protocolo do portal múltiplo que apresenta um distinto conjunto de desafios a um ambiente LVS. Para entender a natureza destes desafios, você deve primeiramente entender algumas chaves principais sobre como o FTP opera.

3.5.1. O funcionamento do FTP

Com outras relações do cliente do servidor, a máquina do cliente abre uma conexão ao servidor num portal particular e o servidor então responde ao cliente daquele portal. Quando o cliente FTP conectar ao servidor FTP, este abrirá a conexão 21 do portal de controle FTP. Então o *cliente* avisa o *servidor* FTP se é para estabelecer uma conexão *ativa* ou *passiva*. O tipo de conexão escolhida escolhida por um cliente determina como o servidor responde e onde as transações dos portais irão acontecer.

Os dois tipos de conexões de dados são:

Conexões Ativas

Quando uma conexão ativa é estabelecida, o *servidor* abre a conexão de dados para o cliente do portal 20 a um portal de grande alcance na máquina do cliente. Todos os dados deste servidor são então passados a esta conexão.

Conexões Passivas

Quando uma conexão passiva é estabelecida, o *cliente* pergunta ao servidor FTP para estabelecer o portal de conexão passiva, do qual pode ser qualquer portal maior de 10,000. O servidor então obriga o portal altamente numerado para esta seção particular e transmite o número do portal de volta ao cliente. O cliente abre o portal de limite novamente para a conexão de dados. Cada solicitação de dados do cliente gera resultados na conexão de dados separados. Os clientes FTP mais modernos tentam estabelecer uma conexão passiva quando solicitando os dados de servidores.

NOTA

O *cliente* determina o tipo de conexão, não o servidor. Isto significa que para o FTP de cluster ser efetivo, você deverá configurar os roteadores LVS para acessar ambas conexões ativas e passivas.

A relação do servidor/cliente pode potencialmente abrir um número grande de portais que a **Piranha Configuration Tool** e IPVS não sabem a respeito.

3.5.2. Como isto afeta o Roteamento LVS

O pacote IPVS enviado apenas permite conexões de entrada e saída do cluster baseado na sua identificação de seu número do portal ou marca firewall. Caso um cliente de fora do cluster tente abrir um portal IPVS sem ser configurado para identificação, isto derrubará a conexão. Simultaneamente, se o servidor real tentar abrir a conexão de backup da Internet, num portal IPVS que não sabe nada a respeito, isto derrubará a conexão. Isto quer dizer que *todas* as conexões dos clientes FTP na Internet, *devem* possuir a mesma marca firewall determinada por eles e todas as conexões do servidor que *devem* ser propriamente enviadas à Internet usando as regras de filtração do pacote da rede.

3.5.3. Criando Regras do Filtro de Pacote da Rede

Before assigning any **iptables** rules for FTP service, review the information in Seção 3.4.1, “Designando Marcas Firewall ” concerning multi-port services and techniques for checking the existing network packet filtering rules.

Below are rules which assign the same firewall mark, 21, to FTP traffic. For these rules to work properly, you must also use the **VIRTUAL SERVER** subsection of **Piranha Configuration Tool** to configure a virtual server for port 21 with a value of **21** in the **Firewall Mark** field. See Seção 4.6.1, “A Subseção do SERVIDOR VIRTUAL” for details.

3.5.3.1. Regras para Conexões Ativas

As regras para conexões ativas avisam o Kernel a aceitar e enviar conexões ao endereço IP flutuante *interno* no portal 20 — o portal de dados FTP.

O seguinte comando **iptables** permite o roteador a aceitar as conexões de saída dos servidores reais, onde o IPVS não possui conhecimento a respeito:

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

In the **iptables** command, *n.n.n* should be replaced with the first three values for the floating IP for the NAT interface's internal network interface defined in the **GLOBAL SETTINGS** panel of **Piranha Configuration Tool**.

3.5.3.2. Regras para Conexões Passivas

As regras para conexões passivas determinam a marca firewall apropriada para conexões vindas da Internet ao IP flutuante do serviço de uma grande variedade de portais —10,000 a 20,000.

ATENÇÃO

Caso você esteja limitando o alcance do portal para uma conexão passiva, você deverá configurar o servidor VSFTP para usar um alcance do portal combinado. Isto pode ser perfeito adicionando as seguintes linhas ao **/etc/vsftpd.conf**:

```
pasv_min_port=10000

pasv_max_port=20000
```

Você deverá também controlar o endereço em que o servidor exibe ao cliente nas conexões FTP passivas. Num sistema LVS de roteamento NAT, adicione a seguinte linha **/etc/vsftpd.conf** para ativar o endereço IP do servidor real ao VIP, do qual é o que o cliente vê na conexão. Por exemplo:

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

Substitua o *n.n.n.n* com o endereço VIP do sistema LVS.

Para configuração de outros serviços FTP, consulte a documentação respectiva.

Este alcance deve ser grande o suficiente para a maioria das situações, no entanto você pode aumentar este número para incluir toda a disponibilidade de portais não segurados alterando **10000:20000** nos comandos abaixo para **1024:65535**.

Os comandos seguintes **iptables** possuem o efeito net de designar qualquer tráfego endereçado ao IP flutuante nos portais apropriados da marca firewall de 21, da qual é em troca reconhecida pelo IPVS e enviada apropriadamente:

```
/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
```

Nos comandos **iptables**, o *n.n.n.n* deve ser substituído pelo IP flutuante para o servidor virtual FTP na subseção do **SERVIDOR VIRTUAL** da **Piranha Configuration Tool**.

ATENÇÃO

The commands above take effect immediately, but do not persist through a reboot of the system. To ensure network packet filter settings are restored after a reboot, see Seção 3.6, “Salvando as Configurações do Filtro do Pacote da Rede”

Finally, you need to be sure that the appropriate service is set to activate on the proper runlevels. For more on this, refer to Seção 2.1, “Serviços de Configuração nos Roteadores LVS” .

3.6. SALVANDO AS CONFIGURAÇÕES DO FILTRO DO PACOTE DA REDE

Após configurar os filtros do pacote da rede apropriada para a sua situação, salve as configurações para que então elas sejam restauradas após a reinicialização. Para o **iptables**, digite o seguinte comando:

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

Isto salva as configurações em **/etc/sysconfig/iptables**, desta forma elas podem ser chamados novamente no período de inicialização.

Once this file is written, you are able to use the **/sbin/service** command to start, stop, and check the status (using the status switch) of **iptables**. The **/sbin/service** will automatically load the appropriate module for you. For an example of how to use the **/sbin/service** command, see Seção 2.3, “Iniciando o Serviço da **Piranha Configuration Tool**”.

Finally, you need to be sure the appropriate service is set to activate on the proper runlevels. For more on this, see Seção 2.1, “Serviços de Configuração nos Roteadores LVS” .

O próximo capítulo explicará como se utilizar a **Piranha Configuration Tool** para configuração do roteador LVS e descrever os passos necessários para ativar o cluster LVS.

CAPÍTULO 4. CONFIGURANDO OS ROTEADORES LVS COM A PIRANHA CONFIGURATION TOOL

A **Piranha Configuration Tool** fornece uma estrutura de aproximação para criar o arquivo de configuração necessário pelo LVS — `/etc/sysconfig/ha/lvs.cf`. Este capítulo descreve a operação básica da **Piranha Configuration Tool** e como ativar o cluster, uma vez que a configuração for completada.

IMPORTANTE

O arquivo de configuração para o cluster LVS segue regras restritas de formatação. O uso da **Piranha Configuration Tool** é a melhor maneira de se prevenir erros sintaxes no `lvs.cf`, e conseqüentemente prevenir as falhas do software.

4.1. SOFTWARE NECESSÁRIO

O serviço `piranha-gui` deve ser ativado no roteador LVS primário para o uso da **Piranha Configuration Tool**. Para configurar o LVS, você precisará no mínimo de um navegador da Web de texto apenas, como por exemplo `links`. Caso você esteja acessando o roteador LVS de uma outra máquina, você precisará também de uma conexão `ssh` para o roteador LVS primário, como o usuário de root.

É recomendável manter a conexão atual `ssh` numa janela do terminal, enquanto configurando o roteador LVS primário. Esta conexão fornece um caminho seguro para reiniciar o `pulse` e outros serviços, configurar a rede de filtros de pacotes, e monitorar o `/var/log/messages` durante a solução de problemas.

As próximas quatro seções caminham em direção a cada uma das páginas da **Piranha Configuration Tool** e dão instruções de como utilizá-la para configurar o LVS.

4.2. FAZENDO O LOGON NA PIRANHA CONFIGURATION TOOL

When configuring LVS, you should always begin by configuring the primary router with the **Piranha Configuration Tool**. To do this,verify that the `piranha-gui` service is running and an administrative password has been set, as described in Seção 2.2, “Configurando a Senha para a **Piranha Configuration Tool**”.

If you are accessing the machine locally, you can open `http://localhost:3636` in a Web browser to access the **Piranha Configuration Tool**. Otherwise, type in the hostname or real IP address for the server followed by `:3636`. Once the browser connects, you will see the screen shown in Figura 4.1, “The Welcome Panel”.

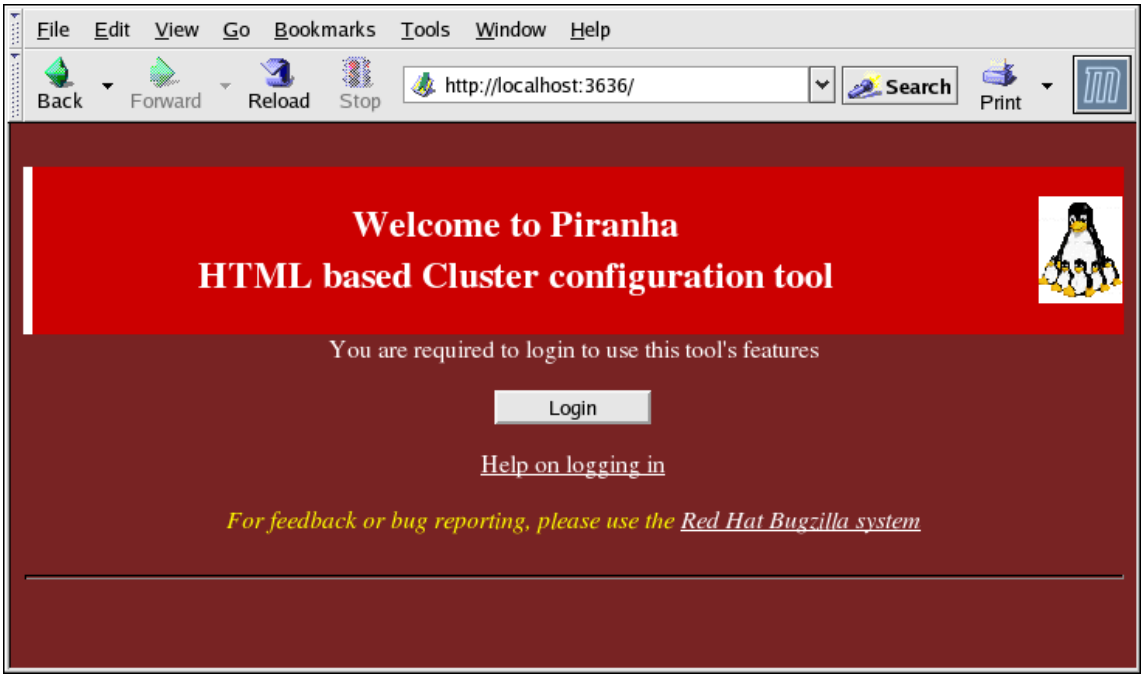


Figura 4.1. The Welcome Panel

Clique no botão **Logon** e entre **piranha** para o **Nome do usuário** e a senha administrativa criada por você no campo **Senha**.

A **Piranha Configuration Tool** é feita de quatro telas principais ou *painéis*. Além disso, o painel **Servidores Virtuais** contém quatro *subseções*. O painel **CONTROLE/MONITORAMENTO** é o primeiro painel após a tela de logon.

4.3. CONTROL/MONITORING

O Painel **CONTROLE/MONITORAMENTO** apresenta o status de tempo de execução limitado do LVS. Ele apresenta também o status do **pulse** daemon, a tabela de roteamento LVS, e o processo **nanny** do LVS gerado.

NOTA

The fields for **CURRENT LVS ROUTING TABLE** and **CURRENT LVS PROCESSES** remain blank until you actually start LVS, as shown in Seção 4.8, “Iniciando o LVS”.

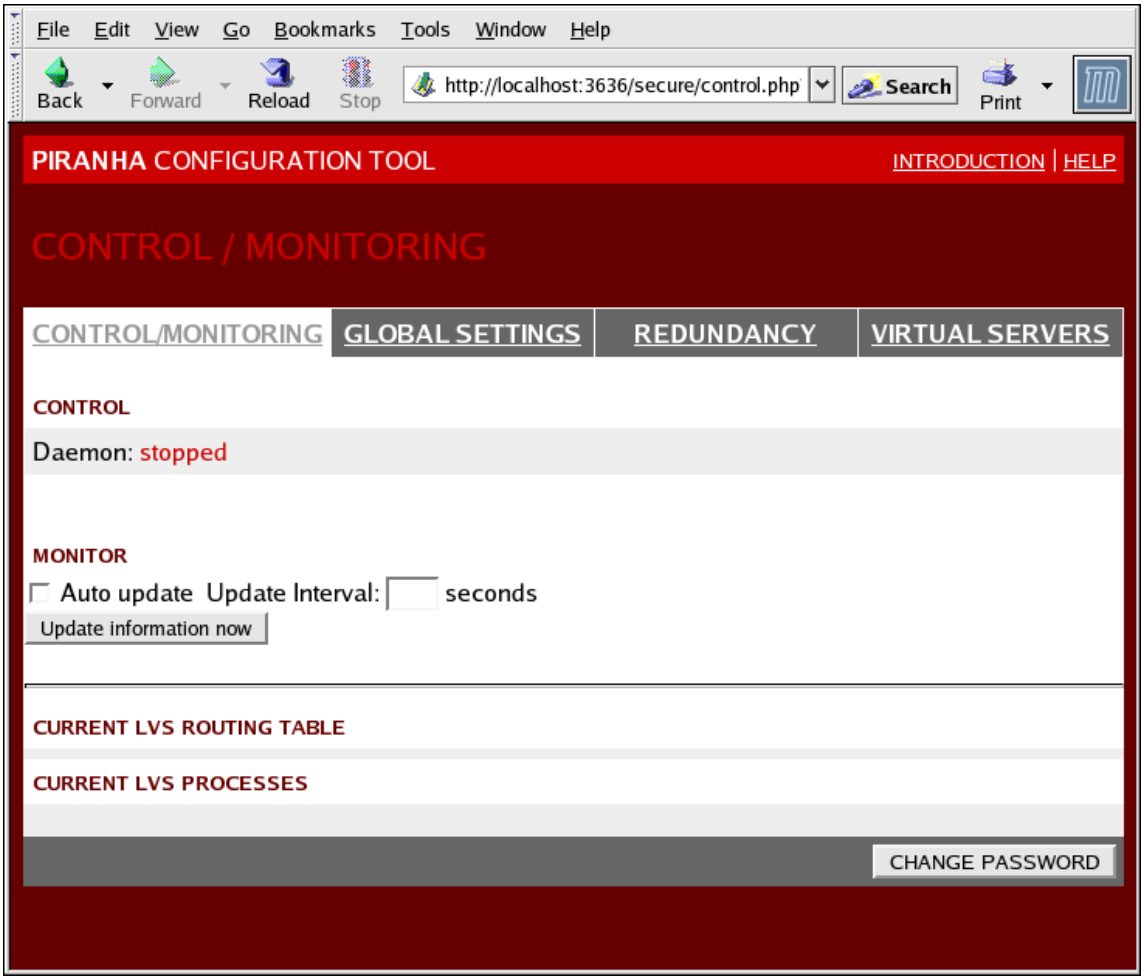


Figura 4.2. The CONTROL/MONITORING Panel

Auto update

O status demonstrado nesta página pode ser atualizado automaticamente no intervalo configurável do usuário. Para capacitar esta característica, clique na caixa de **Auto atualização** e ajuste a freqüência de atualização desejada na caixa de texto **Atualizar freqüência em segundos** (o valor do padrão é de 10 segundos)

Não é recomendável que você ajuste a configuração automática para um intervalo de 10 segundos. Caso isto ocorra, será difícil reconfigurar o intervalo **Auto atualização**, pois a página irá atualizar-se muito freqüentemente. Caso você encontre este problema, apenas clique em outro painel e então retorne ao **CONTROLE/MONITORANDO**.

A característica **Auto update** não opera em todos os navegadores, como por exemplo **Mozilla**.

Update information now

Você pode atualizar manualmente o status da informação apenas clicando neste botão.

CHANGE PASSWORD

Clicando neste botão o levará a uma tela de ajuda, com informação de como mudar a senha administrativa para a aplicação da **Piranha Configuration Tool**.

4.4. GLOBAL SETTINGS

The **GLOBAL SETTINGS** panel is where the you define the networking details for the primary LVS router's public and private network interfaces.

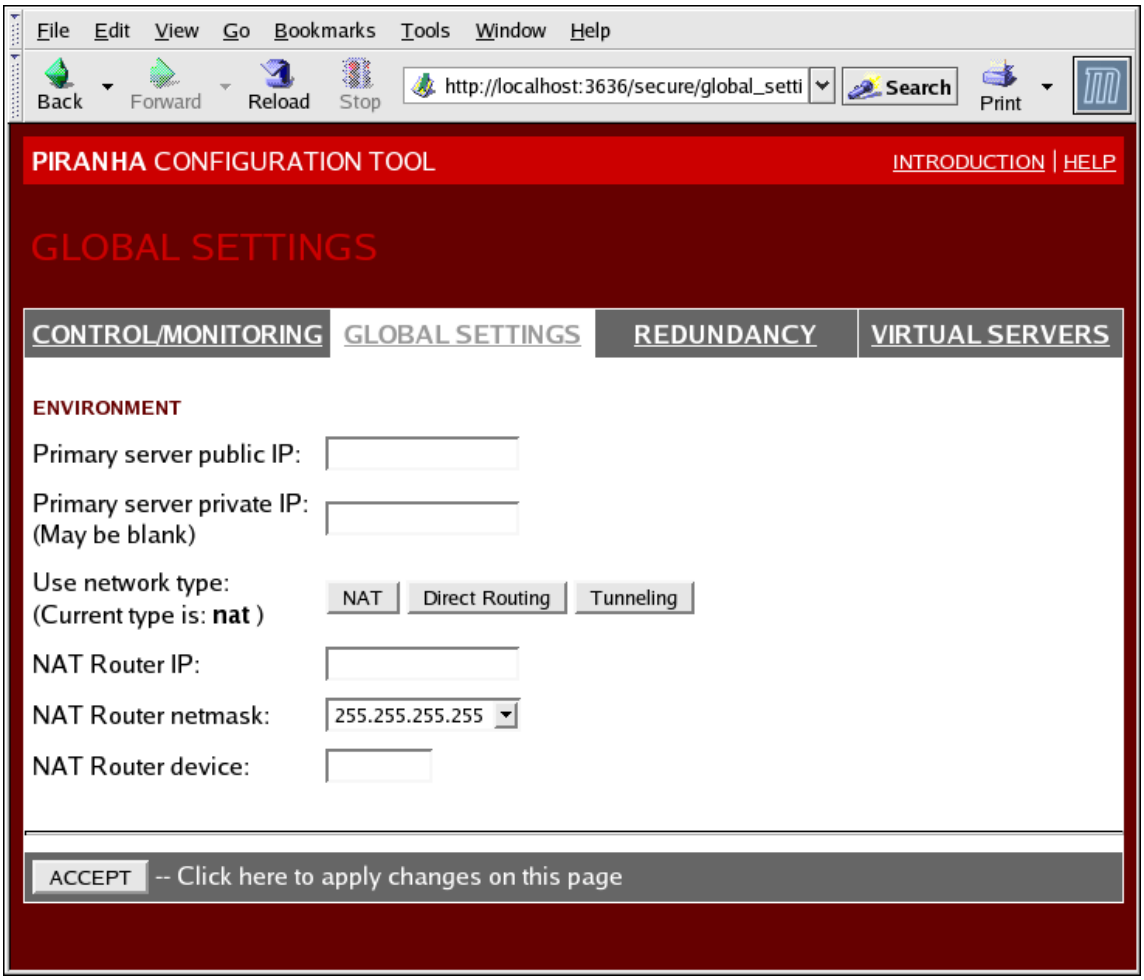


Figura 4.3. The GLOBAL SETTINGS Panel

The top half of this panel sets up the primary LVS router's public and private network interfaces. These are the interfaces already configured in Seção 3.1.1, "Interfaces da Rede Configurada pelo LVS com NAT".

Primary server public IP

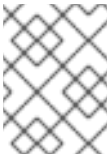
Neste campo, entre o endereço IP real que pode ser roteado para o nó LVS primário.

Primary server private IP

Enter the real IP address for an alternative network interface on the primary LVS node. This address is used solely as an alternative heartbeat channel for the backup router and does not have to correlate to the real private IP address assigned in Seção 3.1.1, "Interfaces da Rede Configurada pelo LVS com NAT". You may leave this field blank, but doing so will mean there is no alternate heartbeat channel for the backup LVS router to use and therefore will create a single point of failure.

NOTA

O endereço IP privado não é necessário para configurações de **Roteamento Direto**, assim como todos os servidores reais e os diretores LVS compartilham os mesmos endereços IP virtuais, e devem possuir a mesma configuração de rota.



NOTA

The primary LVS router's private IP can be configured on any interface that accepts TCP/IP, whether it be an Ethernet adapter or a serial port.

`Use network type`

Clique no botão **NAT** para selecionar o roteamento NAT.

Clique no botão **`Roteamento Direto`** para selecionar o roteamento direto.

The next three fields deal specifically with the NAT router's virtual network interface connecting the private network with the real servers. These fields *do not* apply to the direct routing network type.

`NAT Router IP`

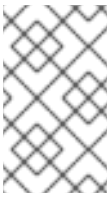
Entre o IP flutuante privado neste campo. Este IP flutuante deve ser usado como passagem para os servidores reais.

`NAT Router netmask`

If the NAT router's floating IP needs a particular netmask, select it from drop-down list.

`NAT Router device`

Utilize este campo do texto para definir o nome do dispositivo da interface da rede para o endereço IP flutuante, como por exemplo o **`eth1:1`**.



NOTA

Você deve alias o endereço IP flutuante à Interface Ethernet conectada à rede privada. Neste exemplo, a rede privada está na interface **`eth1`**, então o **`eth1:1`** é o endereço IP flutuante.

ATENÇÃO

Após completar esta página, clique no botão **ACEITAR** para ter certeza de que você não perderá qualquer mudança quando selecionando um painel novo.

4.5. REDUNDANCY

O painel de **REDUNDÂNCIA** permite você configurar o nó do roteador LVS de backup e configurar várias opções de monitoramento do heartbeat.

NOTA

The first time you visit this screen, it displays an "inactive" **Backup** status and an **ENABLE** button. To configure the backup LVS router, click on the **ENABLE** button so that the screen matches Figura 4.4, “The **REDUNDANCY** Panel”.

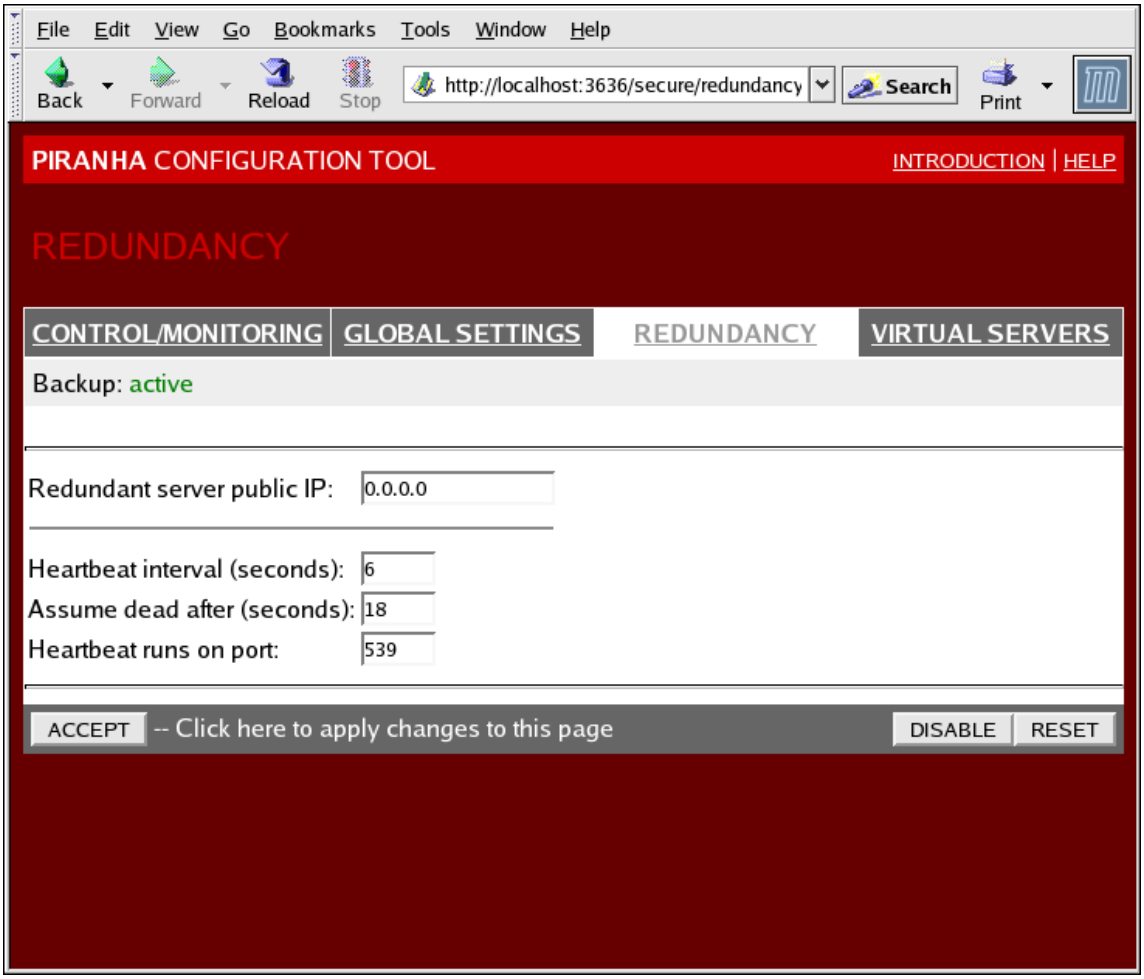


Figura 4.4. The REDUNDANCY Panel

`Redundant server public IP`

Entre o endereço IP real público para o nó do roteador LVS de backup.

`Redundant server private IP`

Enter the backup node's private real IP address in this text field.

Caso você não veja o campo chamado **`IP privado do servidor Redundante`**, retorne ao painel de **`CONFIGURAÇÃO GLOBAL`**, entre o endereço **`IP privado do servidor privado`** e clique em **`ACEITAR`**.

O resto do painel é dedicado à configuração do canal de heartbeat, do qual é usado pelo nó de backup para monitorar o nó primário durante a falha.

`Heartbeat Interval (seconds)`

Este campo determina os segundos entre heartbeats — o intervalo em que o nó de backup irá checar o status funcional do nó LVS primário.

Assume dead after (seconds)

Caso o nó LVS primário não responder após este número de segundos, o nó do roteador LVS de backup irá iniciar a falha.

Heartbeat runs on port

Este campo prepara o portal do qual o heartbeat se comunica com o nó LVS primário. O padrão é ajustado para 539, caso este campo seja deixado em branco.

ATENÇÃO

Lembre-se de clicar no botão **ACEITAR** após realizar qualquer mudança neste painel. Com isto, você poderá ter a garantia de que você não irá perder qualquer alteração, quando selecionando um novo painel.

4.6. VIRTUAL SERVERS

O painel **SERVIDORES VIRTUAIS** exibe a informação para cada servidor virtual definido corretamente. Cada entrada de tabela apresenta o status do servidor, o nome do servidor, o designado IP virtual para o servidor, o netmask do IP virtual, o número do portal do qual o serviço se comunica, o protocolo utilizado e a interface do dispositivo virtual.

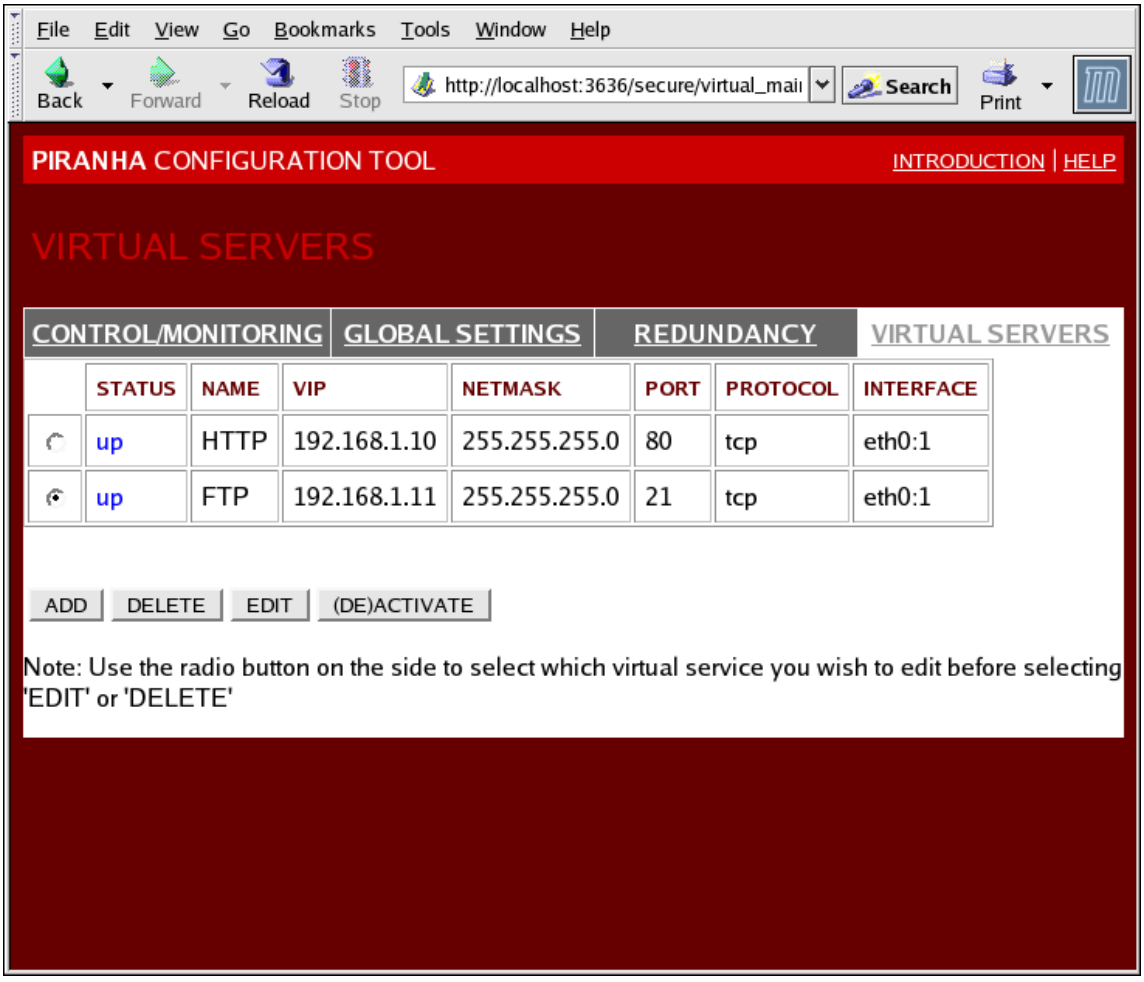


Figura 4.5. The VIRTUAL SERVERS Panel

Cada servidor apresentado no painel **SERVIDORES VIRTUAIS** pode ser configurado nas telas subseqüentes ou *subseções*.

Para adicionar o serviço, clique no botão **ADICIONAR**. Para remover o serviço, selecione o botão rádio próximo ao servidor virtual e clique no botão **DELETAR**.

Para ativar ou desativar o servidor virtual na tabela, clique no botão rádio deste servidor e clique no botão **(DES)ATIVAR**.

Após adicionar um servidor virtual, você pode configurá-lo apenas clicando no botão rádio para o lado esquerdo, e clicando no botão **EDITAR** para exibir a subseção do **SERVIDOR VIRTUAL**

4.6.1. A Subseção do SERVIDOR VIRTUAL

The **VIRTUAL SERVER** subsection panel shown in Figura 4.6, “The **VIRTUAL SERVERS** Subsection” allows you to configure an individual virtual server. Links to subsections related specifically to this virtual server are located along the top of the page. But before configuring any of the subsections related to this virtual server, complete this page and click on the **ACCEPT** button.

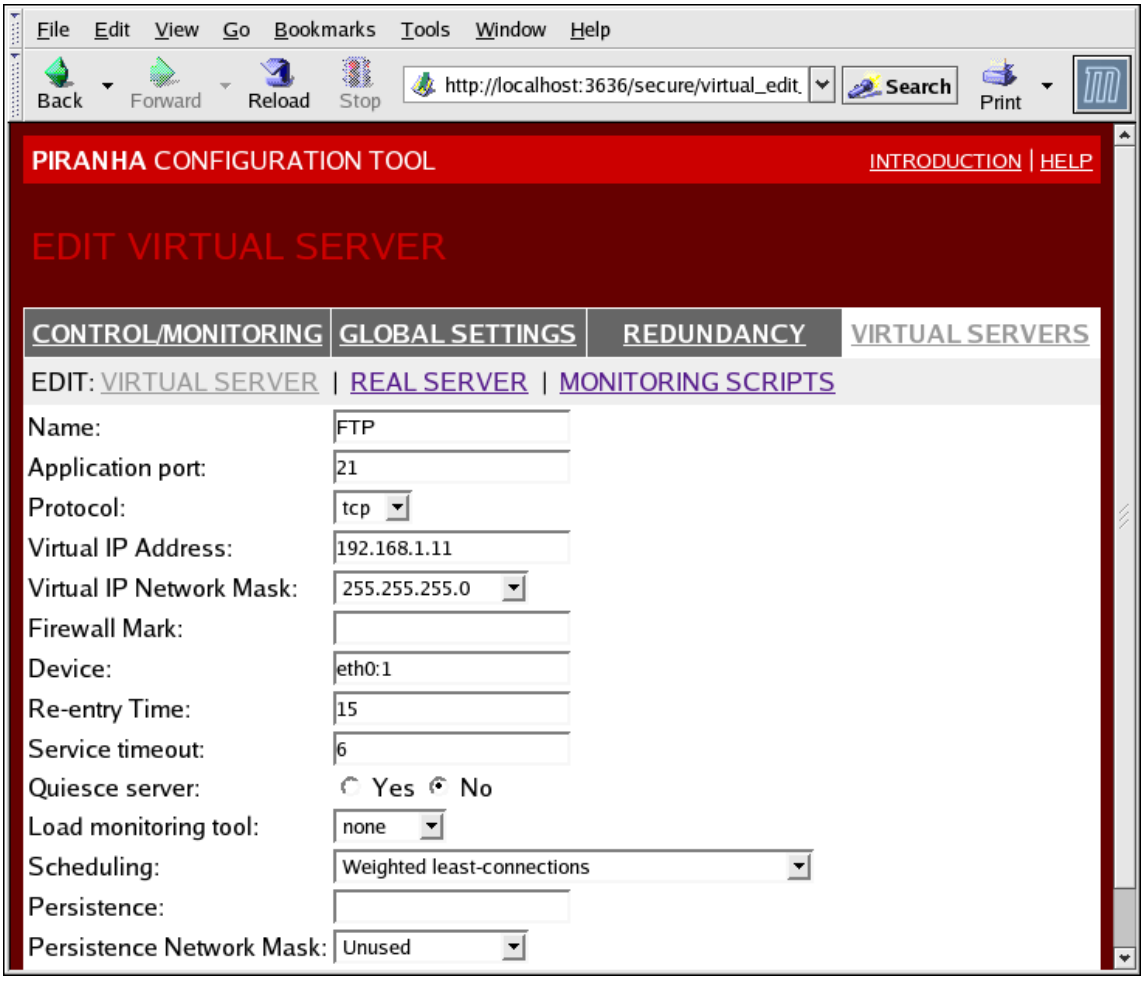


Figura 4.6. The VIRTUAL SERVERS Subsection

Name

Entre o nome descritivo à identidade do servidor virtual. Este nome *não* é o hostname para a máquina, então faça-o descritivo e de fácil identificação. Você pode ainda referenciar o protocolo usado pelo servidor virtual, como por exemplo o HTTP.

Application port

Entre o número do portal completo para que a aplicação do serviço possa escutá-lo. Uma vez que este exemplo é para os serviços HTTP, o portal 80 está sendo utilizado.

Protocol

Escolha entre o UDP e TCP no menu suspenso. Os servidores da Web tipicamente se comunicam via o protocolo TCP, então isto é selecionado como segue a seguir no exemplo acima.

Virtual IP Address

Enter the virtual server's floating IP address in this text field.

Virtual IP Network Mask

Configure a netmask para este servidor virtual com o menu suspenso.

Firewall Mark

Não entre um valor integral da marca firewall neste campo, a não ser que você esteja construindo protocolos de portal múltiplo ou criando um servidor virtual separado, mas com protocolos

relacionados. Neste exemplo, o servidor virtual acima possui uma **Marca Firewal** de 80, pois nós estamos construindo conexões para o HTTP no portal 80 e HTTPS no portal 443, usando o valor de marca firewall de 80. Uma vez combinada com a persistência, esta técnica irá garantir aos usuários acessarem as páginas da Web protegidas e não protegidas, das quais são roteadas ao mesmo servidor real, preservando o estado.

ATENÇÃO

Entering a firewall mark in this field allows IPVS to recognize that packets bearing this firewall mark are treated the same, but you must perform further configuration outside of the **Piranha Configuration Tool** to actually assign the firewall marks. See Seção 3.4, “Serviços de Portal Múltiplo e LVS” for instructions on creating multi-port services and Seção 3.5, “Configurando o FTP” for creating a highly available FTP virtual server.

Device

Entre o nome do dispositivo da rede, da qual você queira o endereço IP flutuante definido pelo campo do **Endereço IP Virtual** vincular.

Você deve alias o endereço IP flutuante à Interface Ethernet conectada à rede pública. Neste exemplo, a rede pública é uma interface **eth0**, então o **eth0:1** deve ser entrado como o nome do disparador.

Re-entry Time

Entre um valor integral que define o espaço de tempo, em segundos, antes do roteador LVS ativo tentar trazer o servidor real de volta ao pool, após a falha.

Service Timeout

Entre um valor integral que define o espaço de tempo, em segundos, antes de um servidor real ser considerado dead e ser removido do pool.

Quiesce server

Quando o botão rádio do **servidor Quiesce** for selecionado, a qualquer instante um novo nó do servidor real aparecerá on-line. A mesa de conexões mínimas é reconfigurada para zero para que o roteador LVS ativo roteie as solicitações como se todos os servidores reais fossem recentemente adicionados ao pool. Esta opção previne um novo servidor de atolar-se com o alto número de conexões por entrada no pool.

Load monitoring tool

O roteador LVS pode monitorar a carga em vários servidores reais utilizando tanto o **rup** ou o **ruptime**. Caso você selecione o **rup** do menu suspenso, cada servidor real deve executar o serviço **rstatd**. E, caso você selecione o **ruptime**, cada servidor real deverá executar o serviço **rwhod**.

ATENÇÃO

O monitoramento de carga *não* é o mesmo de que um balanceamento de carga, e pode ser difícil de se predizer o comportamento de agendamento quando combinado com os algoritmos de agendamento sobrecarregado. Além disso, caso você use o monitoramento de carga, os servidores reais deverão ser máquinas Linux.

Scheduling

Select your preferred scheduling algorithm from the drop-down menu. The default is **Weighted least-connection**. For more information on scheduling algorithms, see Seção 1.3.1, “Agendamento de Algoritmos”.

Persistence

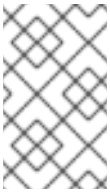
Caso um administrador precise de conexões persistentes para o servidor virtual durante as transações do cliente, entre o número de segundos da inatividade permitida para lapso, antes da conexão esgotar o tempo limite no próximo campo.

IMPORTANTE

If you entered a value in the **Firewall Mark** field above, you should enter a value for persistence as well. Also, be sure that if you use firewall marks and persistence together, that the amount of persistence is the same for each virtual server with the firewall mark. For more on persistence and firewall marks, refer to Seção 1.5, “Persistência e Marcas Firewall”.

Persistence Network Mask

Para limitar a persistência a uma subnet particular, selecione a apropriada máscara da rede do menu suspenso.



NOTA

Antes da entrada das mácaras firewall, a persistência limitada pela subnet era um caminho cru das conexões empacotadas. Agora é recomendável se utilizar a persistência em relação às máscaras firewall para atingir o mesmo resultado.

ATENÇÃO

Lembre-se de clicar no botão **ACEITAR** após realizar qualquer mudança neste painel. Com isto, você não perderá as alterações quando estiver selecionando um novo painel.

4.6.2. Subseção SERVIDOR REAL

Clicando no link da subseção do **SERVIDOR REAL** no topo do painel, exibirá a subseção **EDITAR SERVIDOR REAL**. Isto exibirá o status dos hosts de servidor físico para um serviço virtual particular.

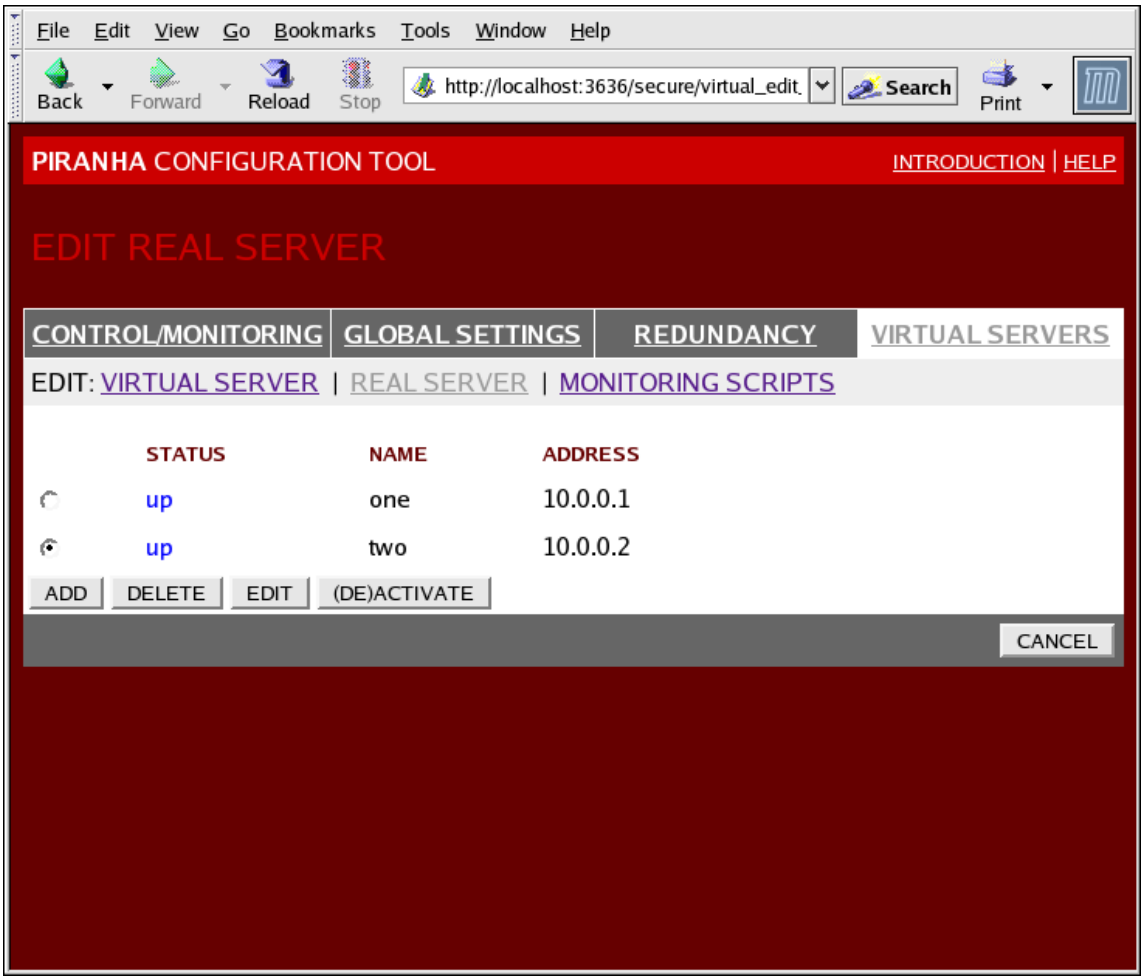


Figura 4.7. The REAL SERVER Subsection

Click the **ADD** button to add a new server. To delete an existing server, select the radio button beside it and click the **DELETE** button. Click the **EDIT** button to load the **EDIT REAL SERVER** panel, as seen in Figura 4.8, “The **REAL SERVER** Configuration Panel”.

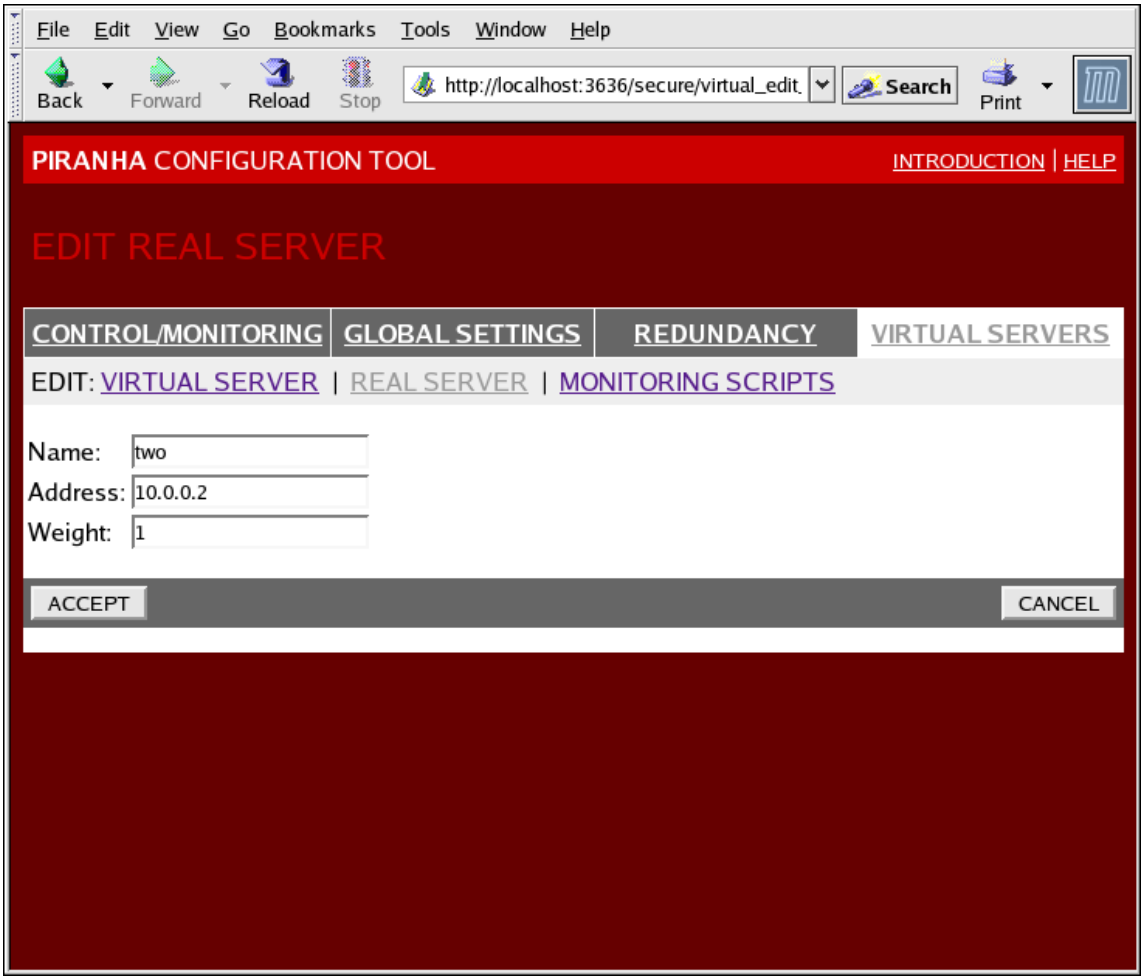
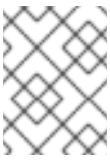


Figura 4.8. The REAL SERVER Configuration Panel

Este painel consiste em três campos de entradas:

`Name`

O nome descritivo para o servidor real.



NOTA

Este nome *não* é o hostname para a máquina, então faça isto descritivo e facilmente identificável.

`Address`

The real server's IP address. Since the listening port is already specified for the associated virtual server, do not add a port number.

`Weight`

An integer value indicating this host's capacity relative to that of other hosts in the pool. The value can be arbitrary, but treat it as a ratio in relation to other real servers in the pool. For more on server weight, see Seção 1.3.2, “Agendamento e Carga do Servidor”.

ATENÇÃO

Lembre-se de clicar no botão **ACEITAR** após realizar qualquer mudança neste painel. Com isto, você terá a garantia de que você não perderá qualquer alteração, quando estiver selecionando um novo painel.

4.6.3. `EDIT MONITORING SCRIPTS` Subsection

Clique no link **SCRIPTS DE MONITORAÇÃO** no topo da página. A subseção da **EDIÇÃO DE SCRIPTS DE MONITORAÇÃO** permite um administrador especificar uma seqüência de envio/esperado para verificar qual serviço do servidor virtual é funcional, em cada servidor real. Este é também o lugar onde o administrador pode especificar os scripts personalizados para checar os serviços requerendo os dados de mudança dinamicamente.

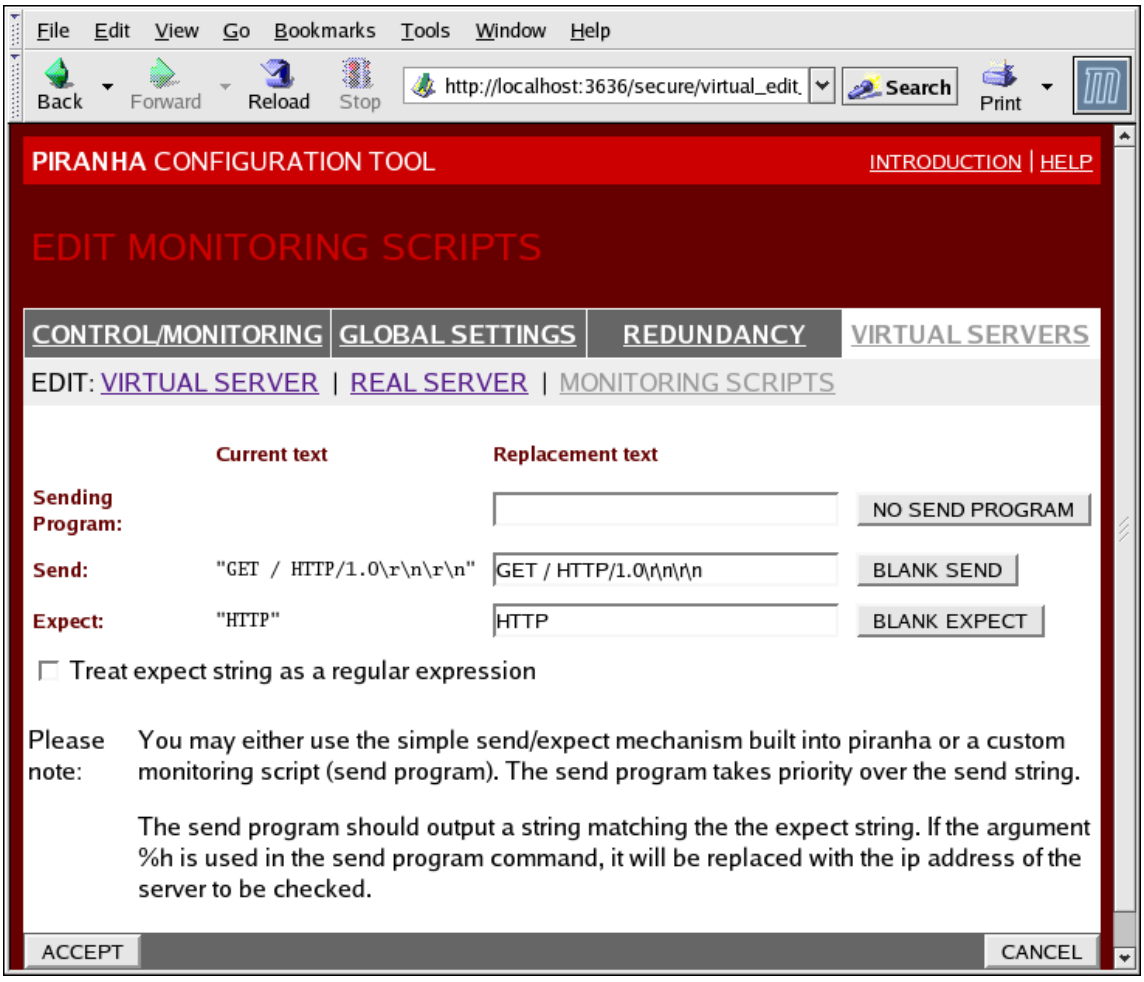
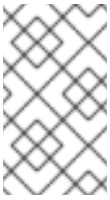


Figura 4.9. The `EDIT MONITORING SCRIPTS` Subsection

`Sending Program`

Para uma verificação mais avançada de serviço, você pode usar este campo para especificar o caminho do script de checagem de serviço. Esta funcionalidade é de grande ajuda para os serviços que requerem a mudança de dados dinamicamente, como o HTTPS ou SSL.

Para o uso desta funcionalidade, você deverá escrever um script que retorna a uma resposta textual, configurar isto para ser executável, e digitar o caminho para isto no campo **Programa Enviado**.



NOTA

To ensure that each server in the real server pool is checked, use the special token **%h** after the path to the script in the **Sending Program** field. This token is replaced with each real server's IP address as the script is called by the **nanny** daemon.

Segue a seguir um script de exemplo para ser utilizado como um guia, quando compondo um script de checagem de serviço externo:

```
#!/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

Caso um programa externo entre no campo **Programa Enviado**, o campo **Enviar** será ignorado.

Send

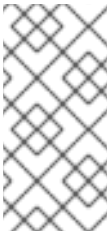
Entre uma seqüência do **nanny** daemon para envio de cada servidor real neste campo. Por padrão o campo enviado é completado para o HTTP. Você pode alterar este valor dependendo de suas necessidades. Caso você deixe este campo em branco, o **nanny** daemon tentará abrir o portal e assumirá o serviço, executando-o caso este suceda.

Apenas uma seqüência é permitida neste campo, e pode conter apenas caracteres imprimíveis, como também os seguintes caracteres de fuga:

- \n para uma nova linha.
- \r para retorno de reboque.
- \t para tabela.
- \ para pular para o próximo caracter que segue a seguir.

Expect

Entre a resposta textual da qual o servidor deve retornar, caso isto esteja funcionando propriamente. Caso você escreva o seu próprio programa enviado, entre a resposta em que você entrou para envio, no caso desta ser bem sucedida.



NOTA

Para determinar o que deve ser enviado para o serviço dado, você poderá abrir a conexão ao portal no servidor real e verificar o que foi retornado. Por exemplo, o FTP reporta 220 por conexão, podendo então entrar mais **`rápido`** no campo **Enviado** e **`220`** no campo **Esperado**.

ATENÇÃO

Lembre-se de clicar no botão **ACEITAR** após realizar qualquer mudança neste painel. Com isto, você terá a garantia de que você não perderá qualquer alteração, quando estiver selecionando um novo painel.

Once you have configured virtual servers using the **Piranha Configuration Tool**, you must copy specific configuration files to the backup LVS router. See Seção 4.7, “Arquivos de Configuração Sincronizados” for details.

4.7. ARQUIVOS DE CONFIGURAÇÃO SINCRONIZADOS

Após configurar o roteador LVS primário, existem diversos arquivos de configuração dos quais devem ser copiados ao roteador LVS de backup, antes de iniciar o LVS.

Estes arquivos incluem:

- **`/etc/sysconfig/ha/lvs.cf`** — o arquivo de configuração para os roteadores LVS.
- **`/etc/sysctl`** — o arquivo de configuração que, entre outras coisas, habilita o pacote enviado no kernel.
- **`/etc/sysconfig/iptables`** — Caso você esteja usando as marcas firewall, você deverá sincronizar um desses arquivos baseado em qual filtro do pacote da rede você estará utilizando.

IMPORTANTE

O **`/etc/sysctl.conf`** e os arquivos **`/etc/sysconfig/iptables`** *não* sofrem alteração uma vez em que você estiver utilizando a **Piranha Configuration Tool**.

4.7.1. Sincronizando `lvs.cf`

A qualquer momento em que o arquivo de configuração LVS, **`/etc/sysconfig/ha/lvs.cf`**, for criado ou atualizado, você deverá copiar isto ao nó roteador de backup.

ATENÇÃO

Os nós de roteador LVS de backup e ativo devem possuir arquivos **lvs.cf** idênticos. Os arquivos de configuração LVS, sem combinação entre os nós de roteador LVS, podem prevenir a falha.

A melhor forma de se utilizar isto será utilizando o comando **scp**.

IMPORTANTE

To use **scp** the **sshd** must be running on the backup router, see Seção 2.1, “Serviços de Configuração nos Roteadores LVS” for details on how to properly configure the necessary services on the LVS routers.

Edite o seguinte comando como o usuário do root de roteador LVS primário, para sincronizar os arquivos **lvs.cf** entre os nós roteadores:

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

Neste comando, substitua o *n.n.n.n* pelo endereço IP real de roteador LVS de backup.

4.7.2. Sincronizando o sysctl

O arquivo **sysctl** é apenas modificado uma vez, na maioria das situações. Este arquivo está preparado no tempo de inicialização e informa o kernel para desligar o pacote enviado.

IMPORTANTE

If you are not sure whether or not packet forwarding is enabled in the kernel, see Seção 2.5, “Ligando Pacote de Encaminhamento” for instructions on how to check and, if necessary, enable this key functionality.

4.7.3. Sincronizando as regras de Filtração do Pacote da Rede

Caso você esteja usando as **iptables**, você precisará sincronizar o arquivo de configuração apropriado no roteador LVS de backup.

Caso você altere alguma das regras do filtro do pacote da rede, entre o seguinte comando como root do roteador LVS primário:

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

Neste comando, substitua o *n.n.n.n* pelo endereço IP real de roteador LVS de backup.

A seguir abra uma seção **ssh** no roteador de backup ou logon na máquina com o root e digite o seguinte comando:

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

Once you have copied these files over to the backup router and started the appropriate services (see Seção 2.1, “Serviços de Configuração nos Roteadores LVS” for more on this topic) you are ready to start LVS.

4.8. INICIANDO O LVS

Para iniciar o LVS, é melhor possuir dois terminais de root abertos simultaneamente, ou dois roots abertos simultaneamente de seções **ssh** do roteador LVS primário.

Em um terminal, observe as mensagens de log do kernel com o comando:

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

Então inicie o LVS digitando o seguinte comando no outro terminal:

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

Follow the progress of the **pulse** service's startup in the terminal with the kernel log messages. When you see the following output, the pulse daemon has started properly:

```
gratuitous lvs arps finished
```

Para interromper a vigilância **/var/log/messages**, digite **Ctrl+c**.

A partir deste ponto, o roteador LVS primário é também o roteador LVS ativo. Mesmo que você possa fazer solicitações ao LVS neste instante, você deverá iniciar o roteador LVS de backup antes de colocar o cluster em serviço. Para realizar isto, apenas repita o processo descrito acima no nó do roteador LVS de backup.

Após completado o passo final, o LVS estará funcionando e operando normalmente.

APÊNDICE A. USANDO O LVS COM O CLUSTER DA RED HAT

Você pode usar roteadores LVS com um Cluster da Red Hat, para implantar a alta disponibilidade e o site de comércio eletrônico, do qual fornece balanceamento de carga, integridade de dados e disponibilidade de aplicativo.

The configuration in Figura A.1, “LVS with a Red Hat Cluster” represents an e-commerce site used for online merchandise ordering through a URL. Client requests to the URL pass through the firewall to the active LVS load-balancing router, which then forwards the requests to one of the Web servers. The Red Hat Cluster nodes serve dynamic data to the Web servers, which forward the data to the requesting client.

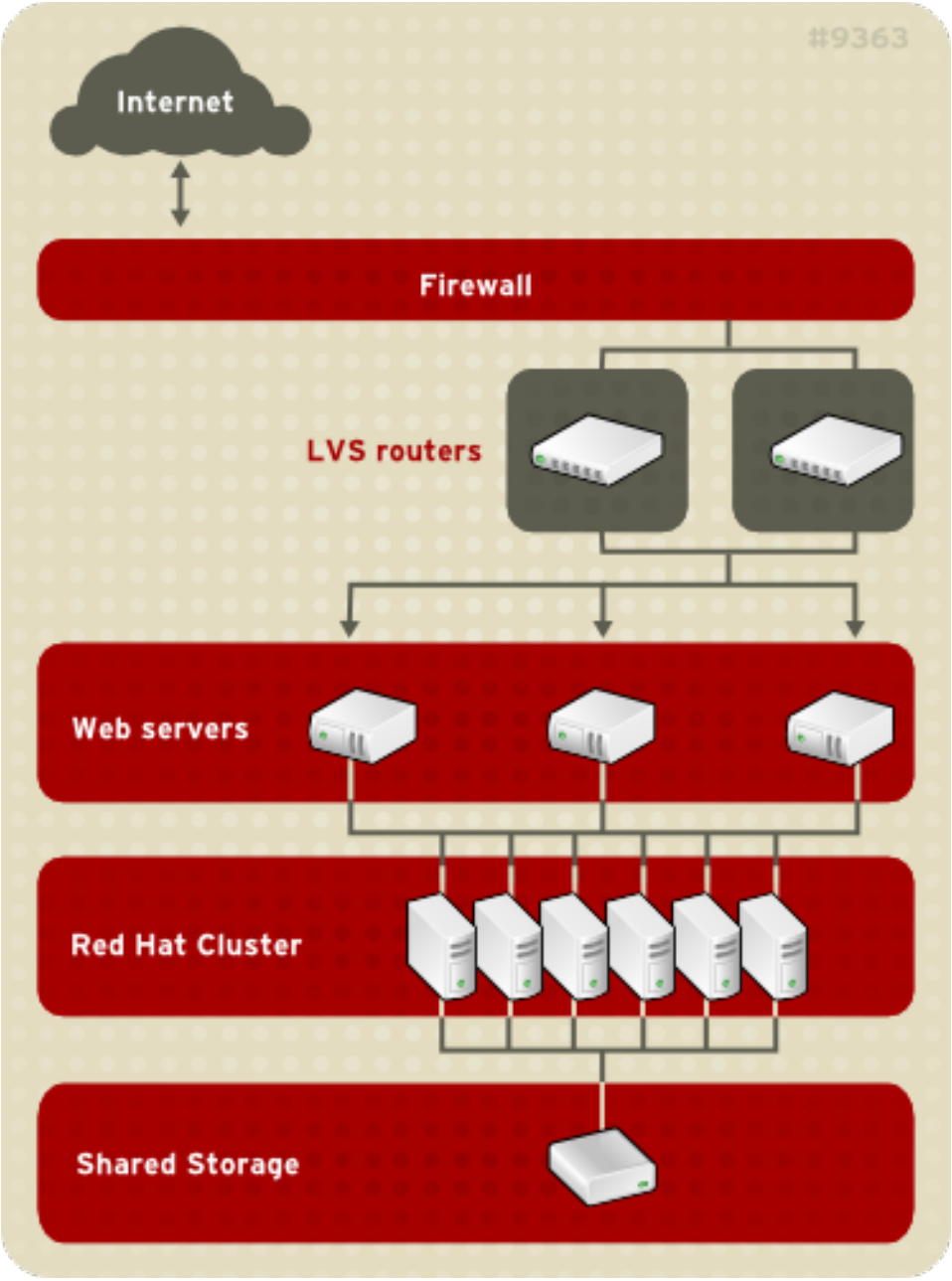


Figura A.1. LVS with a Red Hat Cluster

Serving dynamic Web content with LVS requires a three-tier configuration (as shown in Figura A.1, “LVS with a Red Hat Cluster”). This combination of LVS and Red Hat Cluster allows for the configuration of a high-integrity, no-single-point-of-failure e-commerce site. The Red Hat Cluster can run a high-availability instance of a database or a set of databases that are network-accessible to the Web servers.

Uma configuração de três camadas é requerida para providenciar um conteúdo dinâmico. Enquanto que uma configuração LVS de duas camadas é adequada, caso os servidores da Web servir apenas conteúdo da Web estático (consistindo em quantias pequenas de mudanças de dados infreqüentemente), uma configuração de duas camadas não é adequada caso os servidores da Web servirem o conteúdo dinâmico. O conteúdo dinâmico pode incluir o inventário do produto, pedido de compra ou banco de dados do consumidor, do qual deve ser consistente em todos os servidores da Web para a garantia de que todos os consumidores tenham acesso à atualização de dados e informação exata.

Cada camada fornece as seguintes funções:

- Primeira camada — roteadores LVS desempenhando o balanceamento de carga para distribuir as solicitações da Web.
- Segunda camada — Um conjunto de servidores da Web para servir as solicitações.
- Terceira camada — Um Cluster da Red Hat para servir os dados dos servidores da Web.

In an LVS configuration like the one in Figura A.1, “LVS with a Red Hat Cluster” , client systems issue requests on the World Wide Web. For security reasons, these requests enter a Web site through a firewall, which can be a Linux system serving in that capacity or a dedicated firewall device. For redundancy, you can configure firewall devices in a failover configuration. Behind the firewall are LVS load-balancing routers, which can be configured in an active-standby mode. The active load-balancing router forwards the requests to the set of Web servers.

Each Web server can independently process an HTTP request from a client and send the response back to the client. LVS enables you to expand a Web site's capacity by adding Web servers behind the LVS routers; the LVS routers perform load balancing across a wider set of Web servers. In addition, if a Web server fails, it can be removed; LVS continues to perform load balancing across a smaller set of Web servers.

APÊNDICE B. REVISION HISTORY

Revisão 5-8.400 **2013-10-31** **Rüdiger Landmann**
Rebuild with publican 4.0.0

Revisão 5-8 **2012-07-18** **Anthony Towns**
Rebuild for Publican 3.0

Revisão 2.0-0 **Mon Feb 08 2010** **Paul Kennedy**
Resolves: 492000
Changes -d to -s in arptables "OUT" directive in "Direct Routing and arptables_jf" section.

Revisão 1.0-0 **Tue Jan 20 2009** **Paul Kennedy**
Consolidation of point releases

ÍNDICE REMISSIVO

Símbolos

A

C

D

F

I

J

L

R

S

W