中标麒麟可信操作系统 V6.0

集群管理套件用户手册

中标软件有限公司

上海市徐汇区番禺路 1028 号数娱大厦 10 层（200030）

北京市海淀区北四环西路 9 号银谷大厦 20 层（100190）

广州市天河北路 898 号信源大厦 16 层 1604 室（510898）

目 录

中标麒麟软件使用许可协议

尊敬的中标麒麟用户：

首先感谢您选用由中标软件有限公司开发并制作发行的中标麒麟产品。

请在打开本软件介质包之前，仔细阅读本协议条款以及所提供的所有补充许可条款（统称“协议”）。一旦您打开本软件介质包，即表明您已接受本协议的条款，本协议将立即生效，对您和本公司双方具有法律约束力。

1. 使用许可

按照已为之支付费用的用户数目及计算机硬件类型，中标软件有限公司（下称“中标软件”） 向您授予非排他、不可转让的许可，仅允许内部使用由中标软件提供的随附软件和文档以及任何错误纠正（统称“本软件”）。

— 软件使用许可

在遵守本协议的条款和条件的情况下，中标软件给予贵机构非独占、不可转让、有限的许可，允许贵机构至多使用软件的五（5）份完整及未经修改的二进制格式副本，而此种软件副本仅可安装于贵机构操作的电脑中。

— 教育机构使用许可

在遵守本协议的条款和条件的情况下，如果贵机构是教育机构，中标软件给予贵机构非独占、不可转让的许可，允许贵机构仅在内部使用随附的未经修改的二进制格式的软件。此处的“在内部使用”是指由在贵机构入学的学生、贵机构教员和员工使用软件。

— 字型软件使用

软件中包含生成字体样式的软件（“字型软件”）。贵机构不可从软件中分离字型软件。贵机构不可改动字型软件，以新增此等字型软件被作为软件的一部

分交付予贵机构时所不具备的任何功能。贵机构不可将字型软件嵌入作为商业产品提供以换取收费或其他报酬的文件。

2. 限制

本软件受到版权（著作权）法、商标法和其他法律及国际知识产权公约的保护。中标软件和/或其许可方保留对本软件的所有权及所有相关的知识产权。对于中标软件或其许可方的任何商标、服务标记、标识或商号的任何权利、所有权或利益，本协议均不作任何授权。

3. 关于复制、修改及分发

如果在所有复制品中维持本协议书不变，您可以且必须根据《GNU GPL-GNU 通用公共许可证》复制、修改及分发中标麒麟产品中遵守《GNU GPL-GNU 通用公共许可证》协议的软件，其他不遵守《GNU GPL-GNU 通用公共许可证》协议的中标麒麟产品必须根据符合相关法律之其他许可协议进行复制、修改及分发，但任何以中标麒麟产品为基础的衍生发行版未经中标软件有限公司的书面授权不能使用任何中标软件有限公司的商标或其他任何标志。

特别注意：该复制、修改及分发不包括本产品中包含的任何不适用《GNU GPL-GNU 通用公共许可证》的软件，如中标麒麟产品中包含的输入法软件、字库软件、第三方应用软件等。除非适用法律禁止实施，否则您不得对上述软件进行复制、修改（包括反编译或反向工程）、分发。

4. 有限担保

中标软件向您担保，自购买之日起九十（90）天内（以收据副本为凭证），本软件的存储介质（如果有的话）在正常使用的情况下无材料和工艺方面的缺陷。除上述内容外，本软件按“原样”提供。在本有限担保项下，您的所有补偿及中标软件的全部责任为由中标软件选择更换本软件介质或退还本软件的购买费用。

5. 担保的免责声明

除非在本协议中有明确规定，否则对于任何明示或默示的条件、陈述及担保，包括对适销性、对特定用途的适用性或非侵权性的任何默示的担保，均不予负责，但上述免责声明被认定为法律上无效的情况除外。

6. 责任限制

在法律允许范围内，无论在何种情况下，无论采用何种有关责任的理论，无论因何种方式导致，对于因使用或无法使用本软件引起的或与之相关的任何收益损失、利润或数据损失，或者对于特殊的、间接的、后果性的、偶发的或惩罚性的损害赔偿，中标软件或其许可方均不承担任何责任（即使中标软件已被告知可能出现上述损害赔偿）。根据本协议，在任何情况下，无论是在合同、侵权行为（包括过失）方面，还是在其他方面，中标软件对您的责任将不超过您就本软件所支付的金额。即使上述担保未能达到其基本目的，上文所述的限制仍然适用。

7. 终止

本协议在终止之前有效。您可以随时终止本协议，但必须销毁本软件的全部正本和副本。如果您未遵守本协议的任何规定，则本协议将不经中标软件发出通知立即终止。终止时，您必须销毁本软件的全部正本和副本。

8. 管辖法律

与本协议相关的任何诉讼均受适用的中华人民共和国法律管辖。任何其它国家和地区的选择法律的规则不予适用。

9. 可分割性

如果本协议中有任何规定被认定为无法执行，则删除相应规定，本协议仍然有效，除非删除防碍各方愿望的实现（在这种情况下，本协议将立即终止）

10. 完整性

本协议是您与中标软件就其标的达成的完整协议。它取代此前或同期的所有口头或书面往来信息、建议、陈述和担保。在本协议期间，有关报价、订单、回

执或各方之间就本协议标的进行的其他往来通信中的任何冲突条款或附加条款，均以本协议为准。对本协议的任何修改均无约束力，除非通过书面进行修改并由每一方的授权代表签字。

11. 商标和标识

贵机构承认并与中标软件有着以下共识，即中标软件拥有中标软件、中标麒麟商标，以及所有与中标软件、中标麒麟相关的商标、服务标记、标识及其他品牌标识（“中标软件标记”）。贵机构对中标软件标记的任何使用都应有利于中标软件。

12. 源代码

本软件可能包含源代码，其提供之唯一目的是在符合本协议条款之规定时供参考之用。源代码不可再分发，除非在本协议中有明确规定。

13. 因侵权而终止

如果本软件成为或在任一方看来可能成为任何知识产权侵权索赔之标的，则任一方可立即终止本协议。

14. Java 技术限制

贵机构不可更改“Java 平台界面”（简称“JPI”，即指明为“java”包或“java”包的任何子包中的类），无论通过在 JPI 中创建额外的类，还是通过其他方式导致对 JPI 中的类进行增添或更动，均为不可。如果贵机构创建一个额外的类以及一个或多个相关的 API，而它们（i）扩展 Java 平台的功能；并且（ii）可供第三方软件开发者用于开发可调用上述额外 API 的额外软件，则贵机构必须迅即广泛公布对此种 API 的准确说明，以供所有开发者免费使用。贵机构不可创建、或授权贵机构的被许可人创建以任何方式标示为“java”、“javax”、“sun”的额外的类、界面、子包或 Sun 在任何命名约定中指明的类似约定。参见 Java 运行时环境二进制代码许可的适当版本（目前位于 http://www.java.sun.com/jdk/index.html），以了解可与 Java 小程序和应用程序共同分发的运行时代码的可供情况。

中标麒麟可信操作系统 V6.0 产品介绍

为满足政府、国防、金融、电力、机要、保密等领域对操作系统的高安全性需求，中标软件有限公司（以下简称“中标软件”）基于多年来在操作系统安全和可信计算方面的技术积累，研制推出了国内首款自主可控、高安全等级的可信操作系统软件产品-中标麒麟可信操作系统 V6.0。

结合可信计算技术和操作系统安全技术，中标麒麟可信操作系统 V6.0 通过信任链的建立及传递实现对平台软硬件的完整性度量；提供基于三权分立机制的多项安全功能（身份鉴别、访问控制、数据保护、安全标记、可信路径、安全审计等）和统一的安全控制中心；全面支持国内外可信计算规范（TCM/TPCM、TPM2.0）；兼容主流的软硬件和自主 CPU 平台；提供可持续性的安全保障，防止软硬件被篡改和信息被窃取，系统免受攻击；为业务应用平台提供全方位的安全保护，保障关键应用安全、可信和稳定的对外提供服务。

中标软件还提供基于 Linux 操作系统的安全评估、安全优化、安全加固等安全服务和系统安全定制开发业务。

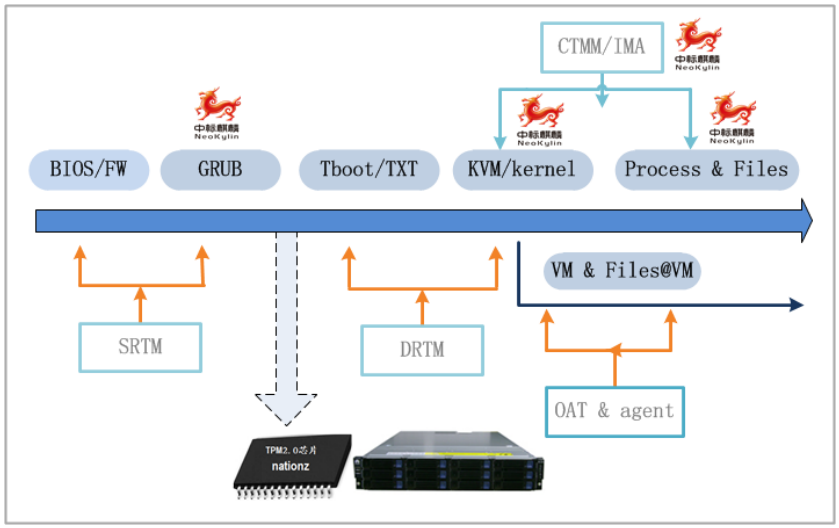
主要特性

■ 操作系统高安全等级

中标麒麟可信操作系统 V6.0 严格遵照可信计算技术规范（TCM/TPCM、TPM2.0）、GB/T 20272-2006 技术要求和国际 CC 标准等进行研制开发。通过操作系统安全的国家标准 GB/T 20272-2006 第四级（结构化保护级）测评认证并获得销售许可。

■ 可信计算实现内核级

国内首款全面支持 TCM/TPCM 和 TPM2.0 可信计算规范的可信操作系统，支持通用和专用可信密码芯片/模块；基于中标软件可信度量模块 CTMM（CS2C Trusted Measure Module）提供可信引导、可信启动和可信运行控制等功能；通过信任链的创建传递过程，实现对平台软硬件的完整性度量；提供基于可信芯片的上层可信功能和图形化的可信管理中心；并实现信任链从物理主机到虚拟化平台的拓展，提供对虚拟机的完整性度量。



■ 安全功能和机制全面

基于 LSM 的安全子系统框架，提供基于三权分立机制的多项安全功能，包括身份鉴别、自主访问控制、强制访问控制、数据机密性和完整性保护、安全标记、可信路径、安全审计等。针对不同的应用场景，系统支持细粒度的强制访问控制 SELinux 和轻量级强制访问控制 SMACK。

■ 系统管理配置灵活

内置主流数据库、中间件和应用服务器的安全策略，同时提供多种图形化安全策略配置和管理工具；基于图形化的安全控制中心实现系统安全可信功能模块化的集中配置和管理，界面友好，简洁易用；用户可以方便快捷完成系统的安全管理。

■ 良好的兼容性

中标麒麟可信操作系统 V6.0 适用于从服务器应用到桌面办公等各种环境，支持各类通用和专业应用；并内置默认的安全策略，实现系统安全和易用的结合，具有良好的软、硬件兼容性。系统支持 64 位应用程序，提供丰富的硬件驱动程序，中标软件有限公司还可协助第三方硬件厂商完成驱动程序的研发和移植，实现专用和特定硬件设备的支持。

系统要求

512MB 物理 RAM（推荐使用 1G 以上 RAM）

5G 以上可用磁盘空间

800x600 以上显示分辨率（推荐采用 1024x768 或更高分辨率）

硬件平台

Intel x86-64（AMD64）

自主 CPU 平台（龙芯、申威、兆芯、众志、Arm64 等）

获得更多的信息

如果出现了本手册不能解决的问题，可以通过如下的方式获得帮助：

阅读和打印 man 页以及 info 页。（man 页和 info 页是系统文档，可以帮助您了解系统提供了哪些可用命令以及如何使用它们）；

- 使用 GNOME 帮助浏览器；
- 登录 www.cs2c.com.cn 网站，查阅相关资料。

技术支持

请您按照中标麒麟可信操作系统 V6.0 产品包装或以下联系方式获取中标软件提供的技术支持服务，包括：

- 所有服务均以远程方式执行；
- 产品安装支持；
- 5＊8 小时电话，邮件，网站、传真等支持；
- 同版本补丁升级服务；
- 远程电话、邮件、网站、传真等支持服务只针对中标麒麟相关产品的安装、使用的问题提供支持，不包含对第三方软硬件的支持服务；
- 服务期按照合同规定起止日期内提供服务。

如果您有其它额外的技术支持需求，请致电中标软件有限公司，我们承诺为您提供优质的服务。

公司网址：www.cs2c.com.cn

客户热线：400-706-1825

电子邮件：support@cs2c.com.cn

公司电话：上海（021）51098866　北京（010）51659955　广州（020）38182526

公司传真：上海（021）51062866　北京（010）62800607　广州（020）38182529

1 LVS 配置和使用

1.1 初始 LVS 配置

1.1.1 配置 LVS 路由器上的服务

设置服务在中标麒麟可信操作系统 V6.0 引导时激活的主要工具有三个：命令行程序 chkconfig；基于 ncurses 的 ntsysv 程序；以及图形化的服务配置工具。

在主 LVS 路由器上第一次使用 Piranha 负载均衡配置工具之前，你必须创建一个口令来限制对它的使用。登录为 root 用户，使用以下命令：

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

输入该命令后，会提示创建管理口令。

警告：要使口令更安全，它不应该包含专用名词、常用简写、或任何语言的词典中的现成词汇。不要把未加密的口令留在系统的任何地方。

如果口令在某次活跃的 Piranha 负载均衡配置工具会话中被改变了，管理员会被提示提供新口令。

1.1.2 启动 PIRANHA 负载均衡配置工具服务

当你为 Piranha 负载均衡配置工具设置了口令后，启动或重新启动位于 /etc/rc.d/init.d/piranha-gui 的 piranha-gui 服务。以 root 用户身份键入以下命令：/sbin/service piranha-gui start 或 /sbin/service piranha-gui restart。

使用该命令会调用符号链接 /usr/sbin/piranha_gui -> /usr/sbin/httpd，从而启动 Apache HTTP 服务器的专有会话。出于安全考虑，httpd 的 piranha-gui 版本在另外一个进程中作为用户 piranha 来运行。piranha-gui 对 httpd 服务的影响意味着：

1） 系统上必须安装了 Apache HTTP 服务器。

2） 通过 service 命令来启动或重新启动 Apache HTTP ，服务器会停止 piranha-gui 服务。

警告：如果 /sbin/service httpd stop 或 /sbin/service httpd restart 命令在 LVS 路由器

上被使用，你必须使用以下命令来启动 piranha-gui 服务：

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

piranha-gui 服务是开始配置 LVS 集群所唯一必需的部件，然而，如果你要远程地配置集群，你还需要 sshd 服务。

1.1.2.1 配置 Piranha 负载均衡配置工具的万维网服务器端口

Piranha 负载均衡配置工具默认在端口 3636 上运行。要改变这个端口号码，改变 piranha-gui 万维网服务器配置文件 /etc/sysconfig/ha/conf/httpd.conf 的第二部分的 Listen 3636 这一行。

要使用 Piranha 负载均衡配置工具，你至少需要一个仅文本的万维网浏览器。如果你在主 LVS 路由器上启动了一个万维网浏览器，打开 http://localhost:3636。若把 localhost 换成主 LVS 路由器的主机名或 IP 地址，你就可以从任何地方都可以通过万维网浏览器来使用 Piranha 负载均衡配置工具。

当你的浏览器连接到 Piranha 负载均衡配置工具时，你必须登录才能使用集群配置服务。在 Username 字段内输入 piranha，在 Password 字段内输入 piranha-passwd 中设置的口令。

Piranha 负载均衡配置工具就开始运行了。

1.1.3 限制对 PIRANHA 负载均衡配置工具的使用

Piranha 负载均衡配置工具提示你输入有效的用户名和口令组合。然而，由于所有传递给 Piranha 负载均衡配置工具的数据都是纯明文的，推荐你把对该工具的使用限制在可信任的网络内或本地机器上。

限制使用的最简单方法是通过编辑 /etc/sysconfig/ha/web/secure/.htaccess 文件来使用 Apache HTTP 服务器内建的访问控制机制。该文件编辑完毕后，你不必重新启动 piranha-gui 服务，因为服务器在每次进入该目录时都会检查 .htaccess 这个文件。

按照默认设置，该目录的存取控制允许每个人查看目录的内容。默认的存取控制类似于：

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

要把对 Piranha 负载均衡配置工具的使用仅局限于本地主机（localhost），改变 .htaccess 文件来只允许环回设备（127.0.0.1）。

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

你还可以允许指定的主机或子网，如：

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

 注意：编辑 Piranha 负载均衡配置工具的 .htaccess 文件会限制对 /etc/sysconfig/ha/web/secure/ 目录中的配置页的使用，但并不限制 /etc/sysconfig/ha/web/ 中的登录和帮助页。要限制对这个目录的访问，在 /etc/sysconfig/ha/web/ 目录中创建一个 .htaccess 文件，其中的 order、allow、和 deny 行与 /etc/sysconfig/ha/web/secure/.htaccess 文件中的完全相同。

1.1.4 启用分组转发

为了使 LVS 路由器能够把网络分组正确地转发到实体服务器上，每个 LVS 路由器节点都必须在内核中启用 IP 转发。登录为 root 用户，把/etc/sysctl.conf 中的 net.ipv4.ip_forward = 0 这一行改为：

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

重新引导系统后改变就会生效。

要查看 IP 转发是否被启用了，以 root 用户身份使用以下命令：

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

如果以上命令返回了 1，那么 IP 转发就被启用了。如果它返回了 0，那么你需要使用以下命令来手工启用它：

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

1.1.5 配置实体服务器上的服务

如果集群中的实体服务器是中标麒麟可信操作系统 V6.0，设置相应的服务器守护进程来在引导时被激活。这些守护进程包括用于万维网服务的 httpd 和用于 FTP 或 Telnet 服务的 xinetd。

远程访问实体服务器可能会很有用，因此你还应该安装并运行 sshd 守护进程 。

1.2 设置服务器 LVS 集群

服务器 LVS 集群包括两个基本组群：LVS 路由器和实体服务器。要防止单一失效点，每组都应该至少包含两个成员系统。

LVS 路由器组应该包括两个完全相同或非常相似的运行中标麒麟可信操作系统 V6.0 的系统。一个系统充当活跃 LVS 路由器，另一个处于热备份状态，因此它们需要在能力方面尽可能地相近。

在选择和配置实体服务器组的硬件之前，你必须决定要使用三种 LVS 拓扑中的哪一种。

1.2.1 NAT LVS 集群

NAT 拓扑在利用已有硬件方面提供了较大的回旋余地，但是它在处理较大载量方面的能力却很有限。这是因为所有出入集群的分组都经过 LVS 路由器。

1） 网络布局：

从网络布局角度而言，利用 NAT 选路的 LVS 集群拓扑是最简单的一种形式。这是因为集群只需要一个到公共网络的出入口。实体服务器通过 LVS 路由器来答复所有请求，因此它们都位于自己的专用网络。

2） 硬件：

从集群硬件角度而言，NAT 拓扑是最灵活的一种，因为实体服务器不必是 Linux 机器就能够在集群中正确运行。在 NAT 集群中，每个实体服务器只需要一个 NIC，因为它只会答复 LVS 路由器。而 LVS 路由器则需要两个 NIC 才能在两个网络间为交通选路。由于这种拓扑在 LVS 路由器方面制造了一个瓶

颈，你可以在每个 LVS 路由器上使用吉位以太网网卡来增加 LVS 路由器能够处理的带宽。

若使用了吉位以太网，任何连接实体服务器和 LVS 路由器的转换器就必须至少有两个吉位以太网端口来有效地处理载量。

3） 软件

因为 NAT 拓扑需要在某些配置中使用 iptables，Piranha 配置工具之外你可能还需要进行不少的软件配置。特别是 FTP 服务和对防火墙标记的使用，你需要对 LVS 路由器进行额外的手工配置才能正确地为请求选路。

1.2.1.1 为 NAT LVS 集群配置网络接口

要设置 NAT LVS 集群，管理员必须首先配置 LVS 路由器上的用于公共网络和专用网络的网络接口。在这个例子中，LVS 路由器的公共接口（eth0）将会在 192.168.26/24 网络上（这不是一个可选路发送的 IP，但是让我们假设 LVS 路由器前面有一个防火墙），连接到实体服务器的专用接口（eth1）将会在 10.11.12/24 网络上。

因此，在活跃的或主（primary）LVS 路由器节点上，公共接口的网络脚本 /etc/sysconfig/network-scripts/ifcfg-eth0 可能和以下相似：

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

LVS 路由器上的专用 NAT 接口的 /etc/sysconfig/network-scripts/ifcfg-eth1 文件可能和以下相似：

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

在这个例子中，LVS 路由器的公共接口的 VIP 将会是 192.168.26.10，NAT

或专用接口的 VIP 将会是 10.11.12.10。因此，实体服务器把请求送回 NAT 接口的 VIP 这一点就是一个必需步骤。

 重要：本节中的以太网接口配置范例是用于 LVS 路由器的真正 IP 地址，不是浮动 IP 地址。

配置了主 LVS 路由器节点的网络接口后，你需要配置备份 LVS 路由器的真正网络接口 — 注意不要让 IP 地址和网络上的其它 IP 地址发生冲突。

 重要：确定备份节点服务上的每个接口所服务的网络都和主节点上的接口所服务的网络相同。例如，如果主节点上的 eth0 连接公共网络，备份节点上的 eth0 就必须也连接到公共网络。

1.2.1.2 在正在运行服务器上的选路

配置 NAT 集群中的实体服务器网络接口时要记住的最重要事情是把 NAT 的网关设置成 LVS 路由器的浮动 IP 地址。在这个例子中，该地址为 10.11.12.10。

 注记：一旦实体服务器上的网络接口被启用了，这些机器将无法使用其它方法来连接公共网络。这种情况是正常的。不过，你将能够联系 LVS 路由器的专用接口的真正 IP 地址，在这个例子中是 10.11.12.8。

因此实体服务器的 /etc/sysconfig/network-scripts/ifcfg-eth0 文件可能会和以下相似：

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

 警告：如果实体服务器上不止有一个网络接口配置了 GATEWAY= 行，第一个被启用的接口就会成为网关。因此，如果 eth0 和 eth1 被配置了，而 eth1 被用于 LVS 集群，实体服务器可能就不能正确为请求选路。

最好是关闭无关网络接口。这可以通过在 /etc/sysconfig/network-scripts/ 目

录中用于这些接口的网络脚本中设置 ONBOOT=no，或确保网关在第一个被启用的网络接口中被正确设置来达到。

1.2.1.3 启用 LVS 路由器上的 NAT 选路

在一个简单的 NAT LVS 集群中，每个集群只使用一个端口，如端口 80 上的 HTTP，管理员只需要在 LVS 路由器上启用分组转发就可以使请求被正确地在实体服务器和外界之间传递。决定了要使用哪一种选路方法后，LVS 集群的硬件就应该在网络上被连接在一起。把集群硬件物理连接到一起后，配置主 LVS 路由器和备份 LVS 路由器上的网络接口。

 重要：LVS 路由器上的适配器设备必须被配置进入同一个网络。例如，如果 eth0 连接公共网络，eth1 连接专用网络，那么备份 LVS 路由器上的同一设备就必须连接与此相同的网络。还有，在引导时启用的第一个接口中列举的网关被添加到选路表中，在其它接口中列举的后续网关会被忽略。在配置实体服务器时，这一点不容忽略。

1.2.1.4 LVS 联网的一般技巧

在试图使用 Piranha 配置工具配置集群之前，你需要首先配置 LVS 路由器上公共和专用网络的真正 IP 地址。前面各节关于拓扑的说明使用了网络地址的例子，但是你需要使用实际的网络地址。以下是一些有用的命令，可以用来启动网络接口或检查接口的状态。

1） 启动真正网络接口

启动真正网络接口的最佳办法是以根用户身份使用以下命令（把 N 替换成和接口 eth0 及 eth1 相对应的数字）：

```
/sbin/ifup ethN
```

 警告：不要使用 ifup 脚本来启动你可能使用 Piranha 配置工具配置了的任何浮动 IP 地址（eth0:1 或 eth1:1）。相反，使用 service 命令来启动 pulse。

2） 要关闭网络接口，键入以下命令：

```
/sbin/ifdown ethN
```

把以上命令中的 N 替换成和你想关闭的接口相对应的数字。

3） 检查网络接口的状态

如果你需要检查在某一给定时间哪些网络接口被启用，键入以下命令：

```
/sbin/ifconfig
```

4） 要查看某机器的选路表，使用以下命令：

```
/sbin/route
```

1.2.2 组装集群

决定了要使用哪一种选路方法后，LVS 集群的硬件就应该在网络上被连接在一起。

 重要：LVS 路由器上的适配器设备必须被配置进入同一个网络。例如，如果 eth0 连接公共网络，eth1 连接专用网络，那么备份 LVS 路由器上的同一设备就必须连接与此相同的网络。 还有，在引导时启用的第一个接口中列举的网关被添加到选路表中，在其它接口中列举的后续网关会被忽略。在配置实体服务器时，这一点不容忽略。

把集群硬件物理连接到一起后，配置主 LVS 路由器和备份 LVS 路由器上的网络接口。

1.2.2.1 LVS 联网的一般技巧

在试图使用 Piranha 负载均衡配置工具配置集群之前，你需要首先配置 LVS 路由器上公共和专用网络的真正 IP 地址。前面各节关于拓扑的说明使用了网络地址的例子，但是你需要使用实际的网络地址。以下是一些有用的命令，可以用来启动网络接口或检查接口的状态。

1） 启动真正网络接口

启动真正网络接口的最佳办法是以根用户身份使用以下命令（把 N 替换成和接口 eth0 及 eth1 相对应的数字）

```
/sbin/ifup ethN
```

 警告：不要使用 ifup 脚本来启动你可能使用 Piranha 负载均衡配置工具配置了的

任何浮动 IP 地址（eth0:1 或 eth1:1）。相反，使用 service 命令来启动 pulse。

2） 要关闭网络接口，键入以下命令：

```
/sbin/ifdown ethN
```

把以上命令中的 N 替换成和你想关闭的接口相对应的数字。

3） 检查网络接口的状态

如果你需要检查在某一给定时间哪些网络接口被启用，键入以下命令：

```
/sbin/ifconfig
```

4） 要查看某机器的选路表，使用以下命令：

```
/sbin/route
```

1.2.3 多端口服务和 LVS 集群

任何拓扑下的 LVS 路由器在创建多端口 LVS 服务时都需要额外的配置。多端口服务可以使用防火墙标记来把不同但却相关的协议（如 HTTP 端口 80 和 HTTPS 端口 443）捆绑在一起，或者当 LVS 被用来集群真正的多端口协议如 FTP 时被人工创建。在以上两种情况下，LVS 路由器都使用防火墙标记来识别带有相同标记却到不同端口的分组应该使用同样方法处理。还有，当和持续性综合使用时，防火墙标记会确保只要来自客户机器的连接发生在持续性参数所指定时间段内，它们会被选路发送到同一主机。

不幸的是，用来平衡真正服务的载量的机制 — IPVS — 能够识别被分配给分组的防火墙标记，但自己却不能分配防火墙标记。分配防火墙标记的任务必须被网络分组过滤器 iptables 在 Piranha 负载均衡配置工具之外执行。

1.2.3.1 LVS 分配防火墙标记

要给目标为某个特定端口的分组分配防火墙标记，管理员必须使用 iptables。

本节举例说明了如何捆绑 HTTP 和 HTTPS，但是 FTP 是另一个比较常用的集群多端口协议。

使用防火墙标记的基本规则是，对于 Piranha 负载均衡配置工具中的每一个使用防火墙标记的协议，你一定要有一个同量的 iptables 规则来给网络分组分配标记。

创建网络分组过滤规则之前，请确定目前尚没有任何规则。要确定，在 shell 提示下登录为根用户，键入：

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

如果 iptables 没有在运行，该提示会立即重新出现。

如果 iptables 处于活跃状态，它会显示一组规则集合。如果集合非空，键入以下命令：

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

如果已有的规则非常重要，检查一下 /etc/sysconfig/iptables 的内容，把要保留的规则复制到另一个地方再继续。

以下的规则给目标为浮动 IP 地址（n.n.n.n）的端口 80 和 443 的进入交通分配了同样的防火墙标记 80。在首次使用规则之前，你必须登录为根用户并载入 iptables 模块。

```
/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
```

在上面的 iptables 命令中，n.n.n.n 应该用你的 HTTP 和 HTTPS 虚拟服务器的浮动 IP 地址替换。这些命令的总体效应是给所有目标为 VIP 上的恰当端口的交通分配防火墙标记 80，随后，它就会被 IPVS 识别，并被恰当转发。

警告：以上的命令会立即生效，但是重新启动后就无效了。

1.2.4 组 LVS 集群中的 FTP

文件传输协议（FTP）是一个较老的复杂的多端口协议。它给集群环境带来了一组特殊挑战。要理解这些挑战的性质，你必须首先理解 FTP 工作原理的一

些关键所在。

1.2.4.1 FTP 的工作原理

在多数服务器客户关系中，客户机器打开到服务器的特定端口的连接。当 FTP 客户试图连接 FTP 服务器时，它会打开到 FTP 控制端口 21 的连接。然后，客户告诉 FTP 服务器要建立积极（active）还是消极（passive）连接。客户所选的连接类型决定服务器的响应方式以及传输端口。

两类数据连接为：

1） 积极连接

当建立了积极连接时，服务器从端口 20 打开到客户机器的高位端口的连接。然后，服务器上的所有数据都通过这个连接来传递。

2） 消极连接

当建立了消极连接时，客户要求 FTP 服务器建立消极连接端口，它可以是 10000 以上的任何端口。然后，服务器会把这次特定对话绑定到这个高位端口，并把端口号码转发给客户。客户会打开这个新绑定的端口进行数据连接。客户随后进行的每个数据请求都会导致单独的数据连接。多数现代 FTP 客户试图建立到 FTP 服务器的消极连接。

以上内容和集群相关的两个要点是：

1） 客户决定连接类型，而不是服务器。这意味着，要有效地集群 FTP，你必须配置 LVS 路由器来处理积极和消极连接。

2） FTP 客户/服务器关系具备潜在的打开大量 Piranha 负载均衡配置工具和 IPVS 不知道的端口的可能性。

1.2.4.2 对 LVS 选路的影响

IPVS 分组转发只有在出入集群连接的端口号码或防火墙标记被识别时才被允许。如果集群之外的客户试图打开 IPVS 没有配置处理的端口，连接就会被放弃。同理，如果实体服务器试图在一个 IPVS 不知道的端口上打开到互联网的连接，该连接也会被放弃。这意味着所有从 FTP 客户到互联网的连接都必须被分配了同样的防火墙标记，所有从 FTP 服务器的连接都必须使用网络分组过滤规则被正确地转发到互联网中。

1.2.4.3 创建网络分组过滤器规则

以下是给 FTP 交通分配相同的防火墙标记 21 的规则。要使这些规则正确运行，你必须使用 Piranha 负载均衡配置工具的 虚拟服务器 子节来给端口 21 配置一个虚拟服务器，其中的 防火墙标记 字段被设置为 21。

1） 积极连接的规则

积极连接的规则告诉内核接受和转发到内部浮动 IP 地址的端口 20 的连接。端口 20 是 FTP 数据端口。

iptables

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

在上面的 iptables 命令中，n.n.n 应该被替换成 NAT 接口的内部网络接口的浮动 IP 地址的前三个值，它在 Piranha 负载均衡配置工具的 全局设置 面板上被定义。该命令允许 LVS 路由器接受 IPVS 不知道的实体服务器的输出连接。

2） 消极连接的规则

消极连接的规则给从互联网到服务的浮动 IP 地址的连接在大范围的端口内（从 10000 到 20000）分配恰当的防火墙标记。

警告：如果你要限定消极连接的端口范围，你还必须配置 VSFTP 服务器使用匹配的端口范围。这可以通过在 /etc/vsftpd.conf 文件中添加以下行来达到：

```
pasv_min_port=10000
pasv_max_port=20000
```

你还必须控制服务器显示给客户的消极 FTP 连接的地址。在 NAT 选路的 LVS 系统中，给 /etc/vsftpd.conf 添加以下行来超越到 VIP 的实体服务器 IP 地址，这才是客户在连接时所看到的地址。例如：

```
pasv_address=X.X.X.X
```

把 *X.X.X.X* 替换成 LVS 系统的 VIP 地址。

关于其它 FTP 服务器的配置，请参考相应的文档。

这个范围应该足以满足多种情况；然而，你可以增加这个数量来包括所有可用的非安全端口，只需把以下命令中的 10000:20000 改成 1024:65535 即可。

iptables

```
/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
```

在上面的 iptables 命令中，*n.n.n.n* 应该被替换成 FTP 虚拟服务器的浮动 IP 地址，它在 Piranha 负载均衡配置工具的 虚拟服务器 子节中被定义。这些命令的总体效应是给所有要到浮动 IP 上的相应端口的交通分配防火墙标记 21，然后它会被 IPVS 识别并正确转发。

警告：以上的命令会立即生效，但是重新启动后就无效了。

最后，你需要确定恰当的服务在恰当的运行级别中被激活。

1.2.5 组保存网络分组过滤器设置

恢复。对于 iptables，键入以下命令：

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

这会把设置保存到 /etc/sysconfig/iptables 文件中，因此它们可以在引导使被重新调用。

一旦这个文件被写入，你就能够使用 /sbin/service 命令来启动、停止 iptables，以及检查它的状态（使用 status 选项）。/sbin/service 将会自动为你载入恰当的模块。

最后，你需要确定恰当的服务在恰当的运行级别中被设置为活跃。

下一章解释了如何使用 Piranha 负载均衡配置工具来配置 LVS 路由器，同时还描述了激活 LVS 集群所必需的步骤。

1.3 使用 PIRANHA 负载均衡配置工具配置 LVS 路由器

Piranha 负载均衡配置工具为 Piranha 集群创建必要的配置文件 — /etc/sysconfig/ha/lvs.cf — 提供了一种比较有结构的方法。本章描述了 Piranha 负载均衡配置工具的基本操作，以及配置结束后该如何激活集群。

重要：LVS 集群的配置文件遵循非常严格的格式规则。使用 Piranha 负载均衡配置工具是防止 lvs.cf 中的语法错误（以及由此导致的软件失败）的最佳方法。

1.3.1 必要软件

要使用 Piranha 负载均衡配置工具，主 LVS 路由器上必须运行 piranha-gui 服务，你至少需要一个仅文本的万维网浏览器，如 links。如果你要从另一个机器进入 LVS 路由器，你还需要根用户身份到主 LVS 路由器的 ssh 连接。

在配置主 LVS 路由器时，在终端窗口中保持一个并行的 ssh 连接是一个好办法。该连接会为重启 pulse 和其它服务、配置网络分组过滤器、以及故障排除期间监视 /var/log/messages 等提供一种安全方法。

以下四节概述了 Piranha 负载均衡配置工具的每个配置页，还提供了使用它来设置 LVS 集群的说明。

1.3.2 登录 PIRANHA 负载均衡配置工具

在配置 LVS 集群时，你总是应该从使用 Piranha 负载均衡配置工具配置主路由器着手。

如果你从本地进入机器，你可以在一个万维网浏览器中打开 http://localhost:3636 来使用 Piranha 负载均衡配置工具。否则，键入服务器的真正 IP 地址或主机名再跟随 :3636。浏览器连接后，你就会看到如**图 1-1** 所示的屏幕。

图 1-1 用户登录

点击【**登陆**】按钮，在 用户名中输入 piranha，在【**密码**】字段中输入你创建的管理口令。

Piranha 配置工具有四个主要面板。此外，虚拟服务器 面板包含四个子面板。【**控制/监视**】面板是登录屏幕后的第一个面板。

1.3.3 控制/监视

【**控制/监视**】面板向集群管理员显示了一个有限的集群运行时间状态。它显示了 pulse 守护进程的状态、LVS 选路表、以及 LVS 生出的 nanny 进程。

注记：在你实际启动集群之前，当前 LVS 路由表 和 当前 LVS 进程 一直会是空白。

图 1-2 控制/监视面板

1） 自动更新

在这一页上显示的状态可以按照用户配置的间隔被自动更新。要启用这项功能，点击 自动更新 ，在 更新间隔 内输入想要的更新频率（默认为 10 秒）。

推荐你不要把自动更新间隔设置为小于 10 秒的值。这么做会使你很难重新配置 自动更新 间隔，因为页面会过分频繁地被更新。如果你碰到了这个问题，只需点击另一个面板，然后再回到 控制/监视 即可。

自动更新 功能不能在所有浏览器上（如 Mozilla）运行。

2） 立即更新

你可以点击这个按钮来手工更新状态信息。

3） 修改密码

点击这个按钮把你带到帮助屏幕，该屏幕包括如何改变 Piranha 负载均衡配置工具的管理口令的信息。

1.3.4 全局设置

【全局设置】是集群管理员为主 LVS 路由器的公共和专用网络接口定义联网细节的地方。

图 1-3 全局设置面板

面板的上半部设置主 LVS 路由器的公共和专用网络接口。

1） 主服务器公共 IP

在这个字段中，输入主 LVS 节点的可公开选路的真正 IP 地址。

2） 主服务器私有 IP

输入主 LVS 节点上的另一个网络接口的真正 IP 地址。该地址仅被用作备份路由器的另一个心跳频道，它不必和真正专用 IP 地址互连。你可以把这个字段留为空白，但是这就意味着备份 LVS 路由器无法使用另外的心跳频道，从而造成单一失效点。

窍门：主 LVS 路由器的专用 IP 地址可以在任何一个接受 TCP/IP 的接口上配置，

不管它是以太网适配器还是串口。

3） 使用的网络结构类型

点击 NAT 按钮来选择 NAT 选路。

随后的三个字段是 NAT 路由器的虚拟网络接口特有的。这些网络接口连接专用网络和实体服务器。

4） NAT 路由 IP

在这个文本字段中输入专用浮动 IP 地址。该 IP 地址应该被用作实体服务器的网关。

5） NAT 路由掩码

如果 NAT 路由器的浮动 IP 地址需要一个特殊的子网掩码，从拉下菜单中选择它。

6） NAT 路由设备

使用这个文本字段来定义浮动 IP 地址的网络接口的设备名称，如 eth1:1。

窍门：你应该把 NAT 浮动 IP 地址的别名定为连接专用网络的以太网接口。在这个例子中，专用网络位于 eth1 接口，因此 **eth1:1** 是浮动 IP 地址。

警告：完成了这一页后，点击 提交 按钮来确定选择新面板时不会丢失所做的任何改变。

1.3.5 冗余

【冗余】面板允许你配置备份 LVS 路由器节点，以及设置各类心跳监视选项。

窍门：你第一次访问该屏幕时，它会显示一个“不活跃”的备份状态和**【起效】**按钮。要配置备份 LVS 路由器，点击**【起效】**按钮，这样该屏幕就会和图 1-4 所示相同。

图 1-4 冗余面板

1） 冗余服务器公共 IP

输入备份 LVS 路由器节点的公共真正 IP 地址。

2） 心跳间隔 (秒)

该字段被设置为心跳之间的秒数 — 备份节点检查主 LVS 节点的功能状态的间隔。

3） 探测死机时间（秒）

如果主 LVS 节点在几秒钟后没有答复，那么备份 LVS 路由器节点就会发起失效转移。

4） 心跳端口号

该字段设置到主 LVS 节点的心跳通信端口。若留为空白，默认值就会被设为 539。

⚠警告：在这个面板上进行了改变后，请记住点击 提交 按钮来确保改变不会丢失。

1.3.6 虚拟服务器

【虚拟服务器】面板为每个当前定义的虚拟服务器显示信息。每个表格项目

都显示了虚拟服务器的状态、服务器名称、给服务器分配的虚拟 IP 地址、虚拟 IP 的子网掩码、服务通信所用的端口号码、所用协议、以及虚拟设备接口。

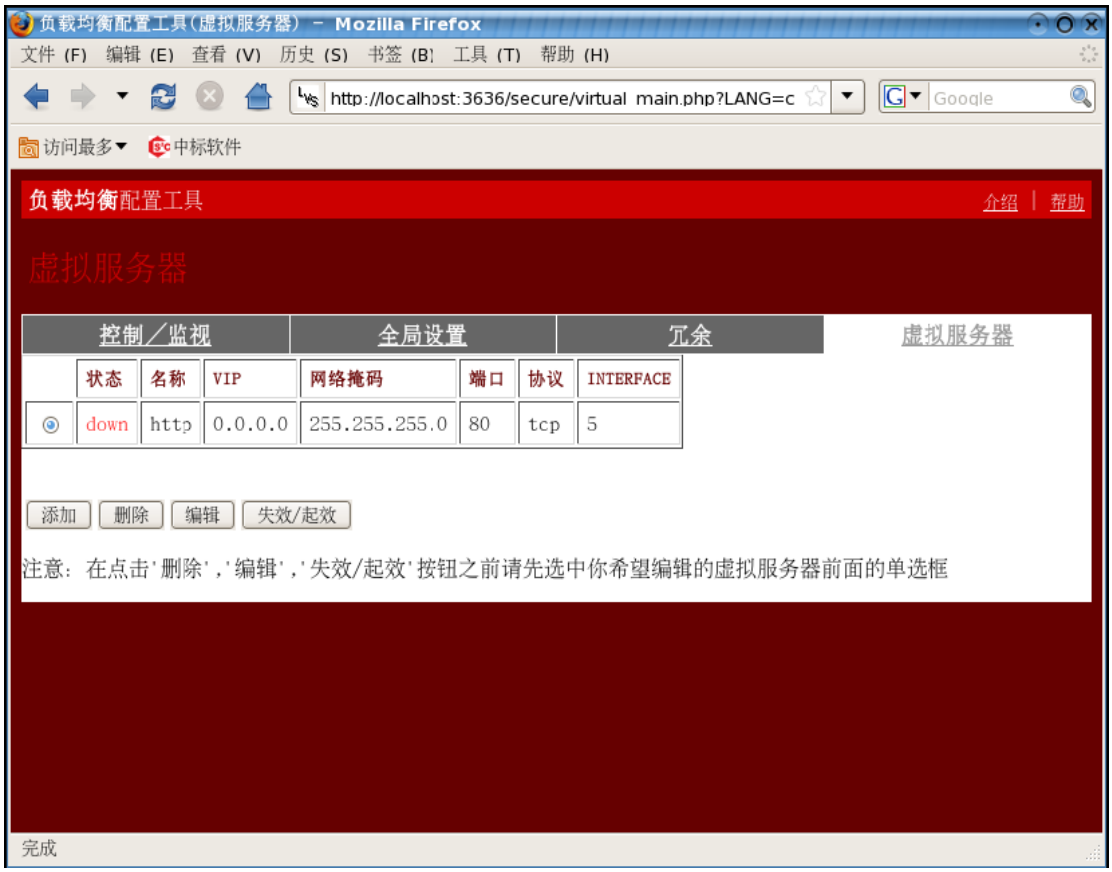


图 1-5 虚拟服务器面板

【虚拟服务器】面板中显示的每个服务器都可以在随后的屏幕或子面板中被配置。

要添加服务，点击**【添加】**按钮。要删除服务，选择该服务，点击它旁边的单选按钮，然后点击**【删除】**按钮。

要启用或禁用表中的虚拟服务器，点击它的单选按钮，然后点击**【失效/起效】**按钮。

添加了虚拟服务器后，你可以配置它。点击它旁边的单选按钮然后点击**【编辑】**按钮来显示**【编辑虚拟服务器】**子面板。

1.3.6.1 虚拟服务器子面板

如**图 1-6** 所示的 虚拟服务器 子面板允许你配置个别虚拟服务器。到相关子节的链接位于页面顶端。在配置任何与这个虚拟服务器相关的子节时，请首先完

成这一页并点击【**提交**】按钮。

图 1-6 虚拟服务器子面板

1） 名称

输入识别虚拟服务器的描述性名称。这个名称不是机器的主机名，因此请尽可能地使用描述性的可识别名称。你甚至可以引用虚拟服务器使用的协议，如 HTTP。

2） 申请端口

输入服务程序将会监听的端口号码。因为我们使用 HTTP 服务为例，端口被设为 80。

3） 协议

在拉下菜单中选择 UDP 或 TCP。万维网服务器通常通过 TCP 协议通信，因此在上面的例子中选择了 TCP。

4） 虚拟 IP 地址

在这个文本字段中输入虚拟服务器的浮动 IP 地址。

5） 虚拟 IP 网络掩码

使用拉下菜单为虚拟服务器设置子网掩码。

6） 防火墙标记

不要在这个字段中输入防火墙标记号码，除非你要捆绑多端口协议或为分开的却又相关的协议创建一个多端口虚拟服务器。以上服务器的 防火墙标记 是 80，这是因为我们把到端口 80 的 HTTP 连接和到端口 443 的 HTTPS 连接都捆绑在一起使用防火墙标记 80。当和持续性综合使用时，这种技术会确保获取不安全或安全网页的用户都会被选路发送到同一真正主机，从而保留状态。

警告：在这个字段中输入一个防火墙标记会使 IPVS 认识到带有这个防火墙标记的分组都应该被相同对待，但是你必须在 Piranha 负载均衡配置工具之外进行进一步配置来实际分配防火墙标记。

7） 设备

输入你想让在 虚拟 IP 地址 字段中定义的浮动 IP 地址绑定的网络设备的名称。

你应该把公共浮动 IP 地址的别名定为连接公共网络的以太网接口。在这个例子中，公共网络位于 eth0 接口，因此 eth0:1 就应该是设备名称。

8） 重新登陆时间

输入以秒为单位的时间，必须是整数值。这个时间是活跃 LVS 路由器试图把某个失效的实体服务器重新加入集群之前必须经过的时间。

9） 服务超时

输入以秒为单位的时间，必须是整数值。这个时间是实体服务器被认为已失效并从集群中删除之前所必须经过的时间。

10） 停止服务器

当选择了 停止服务器 单选按钮时，无论何时某个新的实体服务器节点联机，最少连接表都会被重设为零，因此活跃 LVS 路由器就会选路发送所有请求，如同所有实体服务器都被重新加入集群一样。这个选项防止了新服务器在进入集群时对大量连接应接不暇。

11） 载入监控工具

LVS 路由器能够使用 rup 或 ruptime 来监视各个实体服务器的载量。如果

你从拉下菜单中选择了 rup，每个实体服务器就必须运行 rstatd 服务。如果选择了 ruptime，每个实体服务器就必须运行 rwhod 服务。

 小心：载量监视和负载均衡不同。当与加权的调度算式综合使用时，能够导致难以预测的调度行为。还有，如果你要使用载量监视，集群中的实体服务器就必须是 Linux 机器。

12） 调度

从拉下菜单中选择优选的调度算式。默认为 Weighted least-connections

13） 持续

如果管理员需要在客户传输事务期间具备到虚拟服务器的持续性连接，在这个文本字段中输入连接超时前所允许经过的不活跃期间的秒数。

 重要：如果你在上面的**【防火墙标记】**字段中输入了一个值，你就还应该输入一个持续性值。如果你一起使用防火墙标记和持续性，请确定每个带有防火墙标记的虚拟服务器的持续性值都一致。

14） 持续网络掩码

要限制某个特定子网的持续性，从拉下菜单中选择相应的子网掩码。

 注记：在防火墙标记出现之前，按子网限制的持续性是捆绑连接的粗糙方法。现在最好是一起使用持续性和防火墙标记来达到相同的效果。

 警告：在这个面板上进行了改变后，请记住点击 提交 按钮来确保改变不会丢失。

1.3.6.2 实体服务器子面板

点击面板顶端的**【实体服务器】**子面板显示**【编辑实体服务器】**子节。它显示了某个特定虚拟服务的物理服务器主机的状态。

图 1-7 实体服务器面板

点击【**添加**】按钮来添加一个新服务器。要删除一个现存服务器，选择它旁边的单选按钮，然后点击【**删除**】按钮。点击【**编辑**】按钮来载入【**配置工具**】面板，如**图 1-8** 所示。

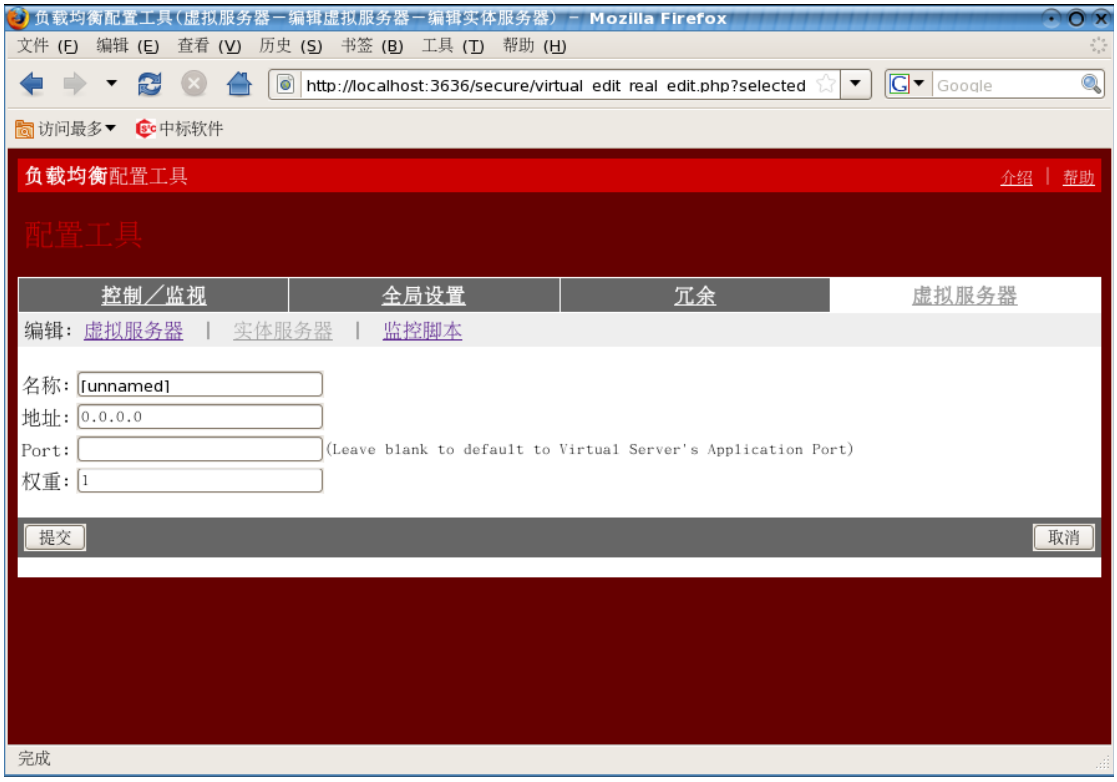


图 1-8 配置工具面板

该面板上有四个项目字段：

1） 名称

一个用于实体服务器的描述性名称。

窍门：该名称不是机器的主机名，因此请尽可能使用带有描述性和识别性的名称。

2） 地址

实体服务器的 IP 地址。由于相关虚拟服务器的监听端口已经被指定，你不必添加端口号码。

3） Port

如果为空，则默认为虚拟服务器应用的端口。

4） 权重

一个表明和集合内其它主机相比而言的主机能力的整数值。这个值可以是任意的，但是请把它当作和集群中其它实体服务器的比例对待。

警告：在这个面板上进行了改变后，请记住点击【**提交**】按钮来确保改变不会丢失。

1.3.6.3 监控脚本子面板

点击面板顶端的【**监控脚本**】链接。【**编辑监控脚本**】子面板允许管理员指定【**传送/预期**】字符串序列来校验每个实体服务器上的虚拟服务器都能正常运行。在这里，管理员还可以指定定制脚本来检查需要动态改变数据的服务。

图 1-9 编辑监控脚本

1） 传送程序

关于更高级的服务校验信息，你需要使用这个字段来指定到服务检查脚本的路径。该功能对于需要动态改变数据的服务（如 HTTPS 或 SSL）特别有用。

要使用该功能，你必须编写一个能够返回文本答复的脚本，把它设置为可执行，然后在 传送程序 字段中键入该脚本的路径。

窍门：要确保实体服务器集合中的每个服务器都被检查了，请在【**传送程序**】字段的脚本路径后使用特殊的 %h 符号。该符号会在脚本被 nanny 守护进程调用时被每个实体服务器的 IP 地址所替换。

在编写外部服务检查脚本时，你可以参照以下脚本范例：

```
#!/bin/sh
TEST=`dig -t soa example.com @$1 | grep -c dns.example.com
if [ $TEST != "1" ]; then
echo "OK
else
echo "FAIL"
fi
```

 注记：如果【**传送程序**】字段中输入了一个外部程序，那么【**传送**】字段就会被忽略。

2） 传送

在这个字段中输入 nanny 守护进程发送给每个实体服务器的字符串。按照默认设置，该字段会为 HTTP 填充。你可以根据需要来改变这个值。如果你把这个字段留为空白，nanny 守护进程会试图打开端口，若成功则假定该服务正在运行。

这个字段中只允许一个 传送 序列，而且它只能包含可打印的、ASCII 字符以及下列转义序列：

\n 代表新行。

\r 代表换行。

\t 代表制表符。

\ 转义跟随其后的字符。

3） 预期

输入服务器正常运行时应该返回的文本答复。如果你自行编写了发送程序，输入发送成功后的答复。

 窍门：要判定对某个给定服务要发送什么，你可以打开一个到实体服务器端口的 telnet 连接，看一看返回了什么。例如，FTP 在连接时返回了 220，因此你可以在【**传送**】字段中输入 quit，在【**预期**】字段中输入 220。

 警告：在这个面板上进行了改变后，请记住点击【**提交**】按钮来确保改变不会丢失。

使用 Piranha 配置工具配置了虚拟服务器后，你必须把指定的配置文件复制

到备份 LVS 路由器上。

1.3.7 同步配置文件

配置了主 LVS 路由器后，在启动集群前，你必须把几个配置文件复制到备份 LVS 路由器上。

这些文件包括：

/etc/sysconfig/ha/lvs.cf — LVS 路由器的配置文件。

/etc/sysctl — 在内核中启用分组转发的配置文件。

/etc/sysconfig/iptables — 如果你使用了防火墙标记，你应该根据所使用的网络分组过滤器来同步其中的一个文件。

 重要：当你使用 Piranha 负载均衡配置工具来配置集群时，/etc/sysctl.conf 和 /etc/sysconfig/iptables 文件不会改变。

1.3.7.1 同步 lvs.cf

无论何时 LVS 配置文件 /etc/sysconfig/ha/lvs.cf 被创建或更新，你都必须把它复制到备份 LVS 路由器节点上。

 警告：活跃和备份 LVS 路由器节点都必须有完全相同的 lvs.cf 文件。LVS 路由器节点间的错配的 LVS 配置文件会阻止失效转移的发生。

做到它的最佳途径是使用 scp 命令。

 重要：要使用 scp 命令，你必须在备份路由器上运行 sshd。

以根用户身份从主 LVS 路由器启用以下命令来同步路由器之间的 lvs.cf 文件：

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

在以上的命令中，把 *n.n.n.n* 替换成备份 LVS 路由器的真正 IP 地址。

1.3.7.2 同步 sysctl

在多数情况下，sysctl 文件只被修改了一次。该文件在引导时被读取，告诉内核启用分组转发。

1.3.7.3 同步网络分组过滤规则

如果你在使用 iptables，你将需要同步备份 LVS 路由器上的恰当配置文件。

如果你改变了任何网络分组过滤规则，以根用户身份从主 LVS 路由器输入以下命令：

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

在以上的命令中，把 *n.n.n.n* 替换成备份 LVS 路由器的真正 IP 地址。

下一步，打开到备份路由器的 ssh 会话，或以根用户身份登录到机器上，键入以下命令：

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

把这些文件复制到备份路由器并启动了恰当的服务后，你就做好了启动集群的准备了。

1.3.8 虚拟服务器启动集群

要启动 LVS 集群，最好是同时打开两个根终端，或两个到主 LVS 路由器的 ssh 会话。

在一个终端里，使用以下命令来观察内核日志消息：

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

在另一个终端里，键入以下命令来启动集群：

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

观察终端上的内核日志消息来跟踪 pulse 服务器的启动进度。该守护进程被正确启动，如果你看到了以下输出：

```
gratuitous lvs arps finished
```

要停止观察 /var/log/messages，按 [Ctrl]-[c]。

从现在起，主 LVS 路由器也是活跃 LVS 路由器。虽然你可以从此向集群

发出请求，你应该在使用集群前启动备份 LVS 路由器。要做到它，只需重复以上关于备份 LVS 路由器节点的过程即可。

完成了最后一步后，集群就开始运行了。