校园双出口 DNS 负载均衡的应用研究①

Application and Research of DNS Load Balance of Dual – link Access in Campus Network

葛　昕　岳敏楠　(上海理工大学 网络管理中心 上海 200093)

摘　要：为了提高访问速度和避免过多的国际流量费用,很多高校都实现了 CERNET 和 CHINANET 双链路接入,但是外部网络对于校内服务器的访问速度并没有提高。本文介绍了 DNS 负载均衡服务器的建立方法,实现了根据用户线路自动选择访问线路,从而很大程度的提高了服务器的访问速度。

关键词：负载均衡 DNS cache

1　引言

网络为教学和科研所作贡献日益突出的今天,各个高校都接入了 CERNET(教科网),而教科网访问 CHINANET(中国公用 INTERNET 骨干网)存在两个明显的问题,一是和 CHINANET 接口存在带宽瓶颈,访问 CHINANET 站点速度较慢,另一是 CERNET 免费地址列表数量较小。因此很多高校在接入 CERNET 的同时,增加了 CHINANET 的访问线路。双线路使得访问外部资源更加通畅,但是外部网络访问校园内部资源时,不论身处何种网络,通常都是经过 CERNET 来访问,这就一定程度上影响了访问速度。而如果能根据用户所使用的网络不同来自动选择对应的访问线路,就可以很大程度的提高访问速度。我校就是使用双 DNS 解析来实现访问线路的负载均衡。

2　双链路负载均衡的实现

使用多个路由器分别接在不同的线路出口,配置相应的策略可以实现访问者自动选择线路来访问内部资源[1],但是配置起来比较烦琐,维护更新也比较麻烦。而使用负载均衡设备则是个更为有效的解决办法,主要思路就是根据访问者的 IP 地址来自动选择接入使用的线路。这里结合负载均衡设备 Array,以我校一个服务器的设置过程为例,来分析整个应用的实现过程。我校一台网站服务器,域名为 net. usst. edu. cn,其在教育网有一个独立地址 202. 120. 223. 147,另我校在申请 CHINANET 线路时,得到多个 CHINANET 地址,现使用其中一个 218. 1. 68. 71 做为该服务器的电信地址。传统访问时,不论用户使用什么网络,他们看到的我校 net 的地址都是 202. 120. 223. 147,也就是都通过 CERNET 访问。现在我们希望:如果是 CERNET 的用户,访问 net 时看到的地址是 202. 120. 223. 147,也就是从 CERNET 接入,如果是电信用户,看到的 net 的地址是 218. 1. 68. 71,也就是从 CHINANET 接入。整个系统是将策略和算法的应用结合在一起。其具体实现过程分为四个部分,如图 1。

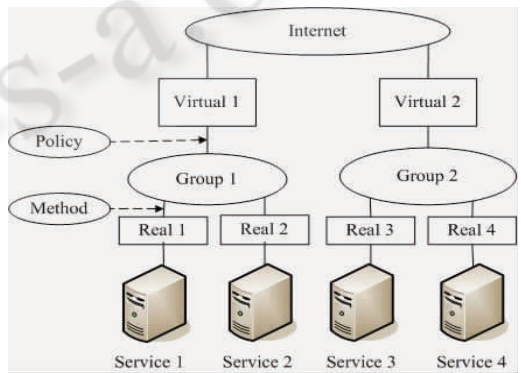

图 1　负载均衡实现关系图

2.1　定义 Real Serivce

Real Service 是提供服务的服务器的 IP 地址和端口的集合。在进行服务器负载均衡功能实现时,首先需要定义 Real Service。在定义 RealService 的同时,需

① 基金项目:浙江省教育厅高校科研计划项目(20061290)

要指定后台提供服务的服务器的 IP 地址和端口,还可以个性化的指定每个 Real Service 能够处理的并发连接数、对 Real Service 进行的健康检查方式等。

步骤 1:slb real <protocol> <real_name> <real_ip> [real_port] [max_conn] [hc_type] [hc_up] [hc_down] [timeout]

本例:slb real http "net" 202.120.223.147 80 10000 tcp 3 3 。/* 服务器的真实地址为 202.120.223.147,服务端口为 web 的 80,最大连接数目 1000,使用 tcp 协议。hc_up 和 hc_down 分别为协议健康检查的通过和失败的次数。

2.2 定义 Real Serivce Group

Real Service 组是提供相同服务的 Real Service 的集合。同一台服务器,由于其可能同时提供多个服务,可以同时属于多个 Real Service Group。在创建 Group 的同时,就需要定义 Group 中的 Real Service 处理用户访问请求的方式(Method),且可以通过加权的方式来分担不同比重的负载到相应的 Real Service 上。

步骤 2:slb group method <group_name> [method [other_parms]]

Method 为负载均衡算法,用来指定在同一组中的 RealService 的工作方式。包括:rr(round robin),pc(persistent cookie),pi(persistent IP),hi(hash IP)等等。

步骤 3:slb group member <group_name> <real_name> [<weight> | <param_string>]

定义 group member,将 Real Service 加入到 Group 中。weight 为权重。param_string 为 cookie 值。

本例:slb group method "net_g" rr /* 建立一个组,名字为 net_g,采用 rr 算法。

slb group member net_g net /* 将 net 服务器加入到组里。

2.3 定义 Policy

步骤 4:slb policy <policy_type> <virtual_name> <group or real name> <param_args *> <precedence>

本例:slb policy default vip net

slb policy qos hostname "net" "vip_net" "net_g" "net.usst.edu.cn" 1 /* 建立一个策略 net,并将其服务和组绑定。

其中 Policy 用来定义 Virtual 和 Group 之间的关系,Method 用来定义 Real 和 Group 之间的关系。

通过 Real Service 、Real Service Group 和 Policy、Method 的应用就方便的实现了服务器负载均衡功能。

2.4 定义对内对外 DNS 解析地址

步骤 5:域名对内解析地址

本例:llb dns host "net.sdns.usst.edu.cn" 202.120.223.147 1

llb dns host "net.sdns.usst.edu.cn" 218.1.68.71 1

步骤 6:域名对外解析地址

sdns host method "net.sdns.usst.edu.cn" region /* 域名 net.sdns.usst.edu.cn 解析算法为 region。

sdns pool method "net.sdns.usst.edu.cn" ct rr 1 /* 对电信站点解析算法为 rr。

sdns pool ip "net.sdns.usst.edu.cn" ct 218.1.68.71 50 /* 电信站点解析成 218.1.68.71。

sdns pool method "net.sdns.usst.edu.cn" cernet rr 1 /* 对教育站点解析算法为 rr。

sdns pool ip "net.sdns.usst.edu.cn" cernet 202.120.223.147 50 /* 教育站点解析成 202.120.223.147。

3 校内 DNS 的实现

负载均衡的实现需要校内 DNS 的支持,我校使用的是 linux+bind9,正向解析的文件中相关部分的设置如下:

@ IN NS dns1.usst.edu.cn. /* dns1 为域名解析服务器。

sdns IN NS ns.sdns.usst.edu.cn. /* sdns 为负载均衡服务器。

abc IN A 202.120.222.3 /* 不走双向线路的服务器的 A 纪录设置方法。

ns.sdns IN A 218.1.68.70 /* ns.sdns 为负载均衡服务器。

net CNAME net.sdns.usst.edu.cn. /* 进行接入路径选择的 net 服务器。

就是说,不进行路径选择的就不用在负载均衡服务器上设置,只需要在 DNS 服务器中做普通的设置就可以了。而进行路径选择的服务器在正向解析文件中,也只需要一条语句,其作用是将解析交给上一级的 SDNS 来做解析。而 SDNS 则根据算法给出合适的路径选择。

在客户端进行 nslookup 解析,测试实现效果。

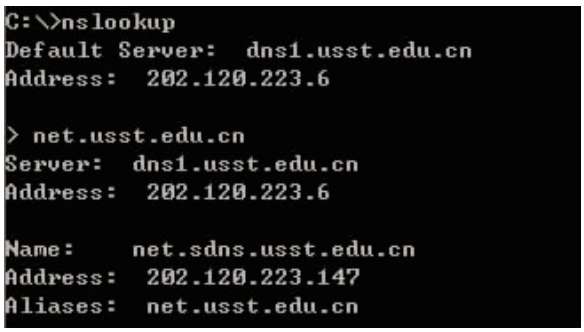

图 2　从 CERNET 访问 net 的 Nslookup 结果

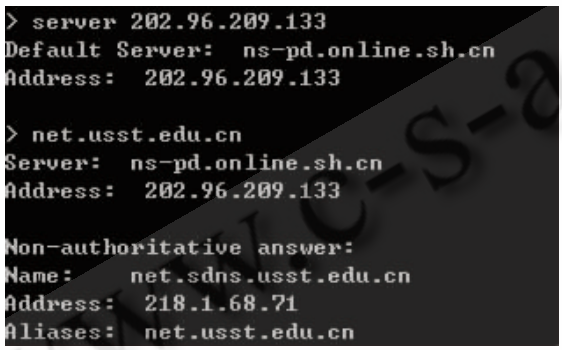

图 3　从 CHINANET 访问 net 的 Nslookup 结果

比较图 2 和图 3，得知使用 CERNET 时，访问的主页地址为 202.120.223.147，而使用 CHINANET 访问主页时，访问的地址为 218.1.68.71，这样就实现了根据用户使用的网络自动选择访问线路，从而很大程度的提高了访问速度。

4　提高性能与安全防护

为了提高内部服务器的 DNS 解析性能。可以采用在 DNS 服务器前增加一个缓存服务器的方法来进一步提升 DNS 的效率。因为高校的访问者相对比较固定，访问的站点多是重复访问，这样通过缓存服务器来实现本地查询，就避免了递归查询的时间，也大大减轻了 DNS 服务器的负载。其实现方法有多种，比较常用的一种方法是是直接安装 BIND，然后编辑配置文件 /var/named/chroot/etc/named.conf，不需要建立域，正向解析部分修改为如下形式。

```
zone "0.0.127.IN-ADDR.ARPA" {
type master;
file "master/localhost.rev";
};
```

也可以使用其他开源软件，dnsmas 和 djbdns[2] 都可以帮助实现 DNS 的缓存功能。

另外对于 DNS 服务器本身的安全，可以使用防火墙来过滤非法访问。如果网络入口处有防火墙，可以建立规则只允许访问 DNS 服务器的 53 端口。如果没有，可以使用 Linux 自带的防火强来保护服务器，通过如下规则来实现保护。

```
Iptables -A OUTPUT -p udp -dport 53 -j ACCEPT
Iptables -A INPUT -p udp -sport 53 -j ACCEPT
Iptables -A INPUT -p udp -sport 53 -m state -state ESTABLISHED -j ACCEPT
```

编辑后，需要保存修改 /etc/sysconfig/iptables 。重启动后，可以安装 dnstop 来查询 DNS 服务器的状态[3]，包括 dns 查询的目的服务器的 ip 地址表，查询的顶级域名，二级域名等。比如 dnstop - s eth0 可以列出所有排名前 20 的请求查询的客户的 IP 地址，这样就可以做到心中有数。防止有人滥用 DNS 服务，同时，可以通过安装流量统计软件 mrtg 来观察 DNS 服务器的流量情况[4]，以便在第一时间发现 DNS 攻击等问题。

5　小结

通过判断访问者的访问线路，在负载均衡服务器上实现线路自动选择，结合内部 DNS 的解析，很好的解决了高校普遍存在的外部访问内部资源速度慢的问题。这里只给出了网站的访问示例，还可以进一步应用于其他服务，如 FTP、MAIL、视频等。本文最后给出了内部 DNS 服务器的安全维护和日常管理的一些意见，希望可以帮助管理员更好的掌控您的服务器。

参考文献

1　韩钰，侯晶净. 策略路由与动态 DNS 技术在校园网中的应用研究. 教育信息化. 2006，7：31－33.
2　HOWTO Setup a DNS Server with DJBDNS，http://gentoo－wiki.com/HOWTO_Setup_a_DNS_Server_with_DJBDNS.
3　DNSTOP：STAY ON TOP OF YOUR DNS TRAFFIC，http://dns.measurement－factory.com/tools/dnstop/.
4　Tobi Oetiker's MRTG － The Multi Router Traffic Grapher，http://www.mrtg.org.