

第22章 配置Squid服务

学习Linux请加QQ群： 群1(163262181) 群2(148412746) 群3(246401509) 群4(173884211)

跟阿铭学Linux邀请函 (<http://www.aminglinux.com>)，猿课已上线，请加微信aminglinux84索要配套视频教程。

这一章，阿铭介绍一下squid，它大多用作http服务的缓存服务器，缓存图片等静态文件可以加速客户端的请求返回速度。当然squid的功能可不仅仅局限于这么一小块。

Squid是什么

Squid是比较知名的代理软件，它不仅可以在linux上还可以跑在windows以及Unix上，它的技术已经非常成熟。目前使用Squid的用户也是十分广泛的。Squid与Linux下其它的代理软件如Apache、Socks、TIS FWTk和delegate相比，下载安装简单，配置简单灵活，支持缓存和多种协议。

Squid之所以用的很多，是因为它的缓存功能，Squid缓存不仅可以节省宝贵的带宽资源，也可以大大降低服务器的I/O。从经济角度考虑，它是很多网站架构中不可或缺的角色。

Squid不仅可以做正向代理，又可以做反向代理。当作为正向代理时，Squid后面是客户端，客户端想上网不管什么网都得经过Squid。 当一个用户(客户端)想要请求一个主页时，它向Squid发出一个申请，要Squid替它请求，然后Squid 连接用户要请求的网站并请求该主页，接着把该主页传给用户同时保留一个备份，当别的用户请求同样的页面时，Squid把保存的备份立即传给用户，使用户觉得速度相当快。使用正向代理时，客户端需要做一些设置，才能实现，也就是平时我们在IE选项中设置的那个代理。而反向代理是，Squid后面为某个站点的服务器，客户端请求该站点时，会先把请求发送到Squid上，然后Squid去处理用户的请求动作。阿铭教你一个特别容易的区分：正向代理，Squid后面是客户端，客户端上网要通过Squid去上；反向代理，Squid后面是服务器，服务器返回给用户数据需要走Squid。

也许你会问，什么时候需要配置正向代理，又什么时候配置反向代理呢？阿铭的观点是，正向代理用在企业的办公环境中，员工上网需要通过Squid代理来上网，这样可以节省网络带宽资源。而反向代理用来搭建网站静态项(图片、html、流媒体、js、css等)的缓存服务器，它用于网站架构中。

搭建Squid正向代理

CentOS系统自带Squid包，但是需要安装一下：

```
[root@localhost ~]# yum install -y squid
```

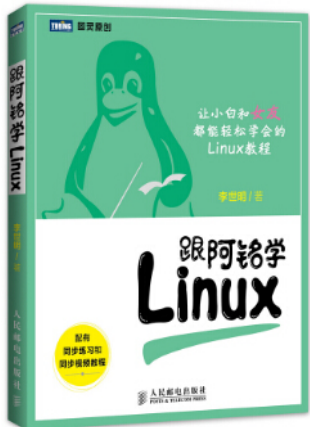
当然你也可以源码包编译安装，Squid官方网站为 <http://www.squid-cache.org/> 当前最新版本为3.3，下载3.1版本即可，因为CentOS6上提供的版本也为3.1版本。如果你想编译安装Squid， 请参考阿铭提供的编译参数吧：

```
./configure --prefix=/usr/local/squid \
--disable-dependency-tracking \
--enable-dlmalloc \
--enable-gnuregex \
--disable-carp \
--enable-async-io=240 \
--with-pthreads \
--enable-storeio=ufs,aufs,diskd,null \
--disable-wccp \
--disable-wccpv2 \
--enable-kill-parent-hack \
--enable-cachemgr-hostname=localhost \
--enable-default-err-language=Simplify_Chinese \
--with-build-environment=POSIX_V6_ILP32_OFFBIG \
--with-maxfd=65535 \
--with-aio \
--disable-poll \
--enable-epoll \
--enable-linux-netfilter \
--enable-large-cache-files \
--disable-ident-lookups \
--enable-default-hostsfile=/etc/hosts \
--with-dl \
--with-large-files \
--enable-removal-policies=heap,lru \
--enable-delay-pools \
--enable-snmp \
--disable-internal-dns
```

目录列表

第1章 前言
第2章 关于Linux的历史
第3章 对Linux系统管理员的建议
第4章 安装Linux操作系统
第5章 初步认识Linux
第6章 Linux系统的远程登陆
第7章 Linux文件与目录管理
第8章 Linux系统用户及用户组管理
第9章 Linux磁盘管理
第10章 文本编辑工具vim
第11章 文档的压缩与打包
第12章 安装RPM包或者安装源码包
第13章 学习 shell脚本之前的基础知识
第14章 正则表达式
第15章 shell脚本
第16章 linux系统日常管理
第17章 LAMP环境搭建
第18章 LNMP环境搭建
第19章 学会使用简单的MySQL操作
第20章 NFS服务配置
第21章 配置FTP服务
第22章 配置Squid服务
第23章 配置Tomcat
第24章 配置Samba服务器
第25章 MySQL replication(主从)配置
结语

阿铭著作：



微信扫码获取最新版linux电子书和视频

这些参数不见得符合你的需求，阿铭只是提供一个参考，也许你在编译的过程中会遇到诸多错误，没有关系，请google或者到阿铭论坛(<http://www.aminglinux.com/bbs/forum-40-1.html>)发帖求助。阿铭觉得使用CentOS中自带的squid已经满足需求，所以没有编译安装。

安装完后，可以查看squid版本：

```
[root@localhost ~]# squid -v
Squid Cache: Version 3.1.10
```

同时还可以看到squid的编译参数。下面阿铭需要配置一下squid，来实现正向代理：

```
[root@localhost ~]# rm -f /etc/squid/squid.conf
[root@localhost ~]# vim /etc/squid/squid.conf
```

我们不使用默认配置文件，删除，重新写入如下配置：

```
http_port 3128
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl SSL_ports port 443
acl Safe_ports port 80 8080 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localnet
http_access allow localhost
http_access allow all
cache_dir aufs /data/cache 1024 16 256
cache_mem 128 MB
hierarchy_stoplist cgi-bin ?
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern \.(jpg|png|gif|mp3|xml) 1440 50% 2880 ignore-reload
refresh_pattern . 0 20% 4320
```

配置文件中有几处阿铭要简单描述一下，第一行的“http_port 3128”这个指的是，squid服务启动后将要监听的端口，也可以是80。“cache_dir”这个用来指定本地磁盘上的缓存目录，后边的1024为大小，单位是M，具体根据你的磁盘大小决定。“cache_mem”它用来规定缓存占用内存的大小，即把缓存的东西存到内存里，具体也需要根据你的机器的内存定，如果你的机器只是跑Squid服务，那么留给系统512M内存外，其他都可以都分给squid，但阿铭做实验的虚拟机一共才300M内存，所以只分了128M。

配置文件保存好后，可以先检测一下是否有语法错误：

```
[root@localhost ~]# squid -kcheck
```

如果提示信息为：

```
squid: ERROR: No running copy
```

这是说squid还未启动，没有关系，显示成这样说明配置文件没有问题了。在启动前还得再做一件事，就是初始化缓存目录：

```
[root@localhost ~]# mkdir /data/cache
[root@localhost ~]# chown -R squid:squid /data/cache/
[root@localhost ~]# squid -z
2013/06/12 16:25:14| Creating Swap Directories
2013/06/12 16:25:14| /data/cache exists
```

好了，初始化完成后，就可以启动squid了：

```
[root@localhost ~]# /etc/init.d/squid start
正在启动 squid: . [确定]
```

查看squid是否启动：

```
[root@localhost ~]# ps aux |grep squid
root      7201  0.0  0.7 14524 2444 ?        Ss   16:25   0:00 squid -f /etc/squid/squid.conf
squid     7204  0.0  2.7 17468 9024 ?        S    16:25   0:00 (squid) -f /etc/squid/squid.conf
squid     7205  0.0  0.2 3280  916 ?        S    16:25   0:00 (unlinkd)
```

SEARCH

Go

Enter search terms or a module, class or function name.

现在你可以在你的真机上测测看squid的正向代理了，具体IE选项阿铭不再阐述，如果实在不懂请google或者求助阿铭(<http://www.aminglinux.com/bbs/forum-40-1.html>)，而阿铭懒得去设置什么IE选项，直接使用curl命令测试即可：

```
[root@localhost ~]# curl -xlocalhost:3128 http://www.baidu.com/
```

如果你看到了一大串，说明squid正向代理设置ok啦。另外我们也可以观察squid对图片的缓存：

```
[root@localhost ~]# curl -xlocalhost:3128 http://www.aminglinux.com/bbs/static/image/common/logo.png -I
HTTP/1.0 200 OK
Server: nginx/1.0.0
Date: Sat, 08 Jun 2013 04:30:17 GMT
Content-Type: image/png
Content-Length: 7785
Last-Modified: Wed, 13 Jan 2010 03:33:47 GMT
Accept-Ranges: bytes
X-Cache: HIT from dx_cache216.5d6d.com
X-Cache: MISS from localhost.localdomain
X-Cache-Lookup: MISS from localhost.localdomain:3128
Via: 1.0 dx_cache216.5d6d.com:80 (squid), 1.0 localhost.localdomain (squid/3.1.10)
Connection: keep-alive

[root@localhost ~]# curl -xlocalhost:3128 http://www.aminglinux.com/bbs/static/image/common/logo.png -I
HTTP/1.0 200 OK
Server: nginx/1.0.0
Content-Type: image/png
Content-Length: 7785
Last-Modified: Wed, 13 Jan 2010 03:33:47 GMT
Accept-Ranges: bytes
Date: Sat, 08 Jun 2013 04:30:17 GMT
X-Cache: HIT from dx_cache216.5d6d.com
Age: 360898
Warning: 113 localhost.localdomain (squid/3.1.10) This cache hit is still fresh and more than 1 day old
X-Cache: HIT from localhost.localdomain
X-Cache-Lookup: HIT from localhost.localdomain:3128
Via: 1.0 dx_cache216.5d6d.com:80 (squid), 1.0 localhost.localdomain (squid/3.1.10)
Connection: keep-alive
```

阿铭连续访问了两次阿铭论坛的logo图片，可以发现前后两次的不同，其中“X-Cache-Lookup: HIT from localhost.localdomain:3128”显示，该请求已经HIT，它直接从本地的3128端口获取了数据。

有时，我们会有这样的需求，就是想限制某些域名不能通过代理访问，或者说只想代理某几个域名，这如何做呢？在squid.conf中找到：

```
acl CONNECT method CONNECT
```

在其下面添加四行：

```
acl http proto HTTP
acl good_domain dstdomain .lishiming.net .aminglinux.com
http_access allow http good_domain
http_access deny http !good_domain
```

其中我的白名单域名为“.lishiming.net .aminglinux.com”，这里的 . 表示万能匹配，前面可以是任何字符，你只需要填写你的白名单域名即可。重启squid再来测测看：

```
[root@localhost ~]# /etc/init.d/squid restart
[root@localhost ~]# curl -xlocalhost:80 http://www.baidu.com/ -I
```

访问百度已经变为403了。如果要设置黑名单呢？道理是一样的：

```
acl http proto HTTP
acl bad_domain dstdomain .sina.com .souhu.com
http_access allow http !bad_domain
http_access deny http bad_domain
```

重启squid后，测试：

```
[root@localhost ~]# /etc/init.d/squid restart
[root@localhost ~]# curl -xlocalhost:80 http://www.sina.com/ -I
[root@localhost ~]# curl -xlocalhost:80 http://www.baidu.com/ -I
```

baidu.com可以访问，而sina.com不可以访问了。

搭建Squid反向代理

过程其实和前面的正向代理没有什么太大区别，唯一的区别是配置文件中一个地方需要改动一下。需要把：

```
http_port 3128
```

改为：

```
http_port 80 accel vhost vport
```

然后再增加你要代理的后端真实服务器信息：

```
cache_peer 123.125.119.147 parent 80 0 originserver name=a
cache_peer 61.135.169.125 parent 80 0 originserver name=b
cache_peer_domain a www.qq.com
cache_peer_domain b www.baidu.com
```

因为咱们之前没有配置网站信息，所以阿铭就拿**qq.com**和**baidu.com**来做例子吧。其中**cache_peer**为配置后端的服务器ip以及端口，**name**后边为要配置的域名，这里和后面的**cache_peer_domain**相对应。实际的应用中，ip大多为内外ip，而域名也许会有多个，如果是**squid**要代理一台web上的所有域名，那么就写成这样：

```
cache_peer 192.168.10.111 80 0 originserver
```

后面连**cache_peer_domain**也省了。

反向代理主要用于缓存静态项，因为诸多静态项目尤其是图片、流媒体等比较耗费带宽，在中国，联通网访问电信的资源本就慢，如果再去访问大流量的图片、流媒体那更会慢了，所以如果在联通网配置一个**squid**反向代理，让联通客户端直接访问这个联通**squid**，而这些静态项已经被缓存在了**squid**上，这样就大大加快了访问速度。也许你听说过**CDN**，其实它的设计原理就是这样的思路。好了，我们再测一测反向代理吧。

因为修改了配置文件，所以需要重启一下**squid**：

```
[root@localhost ~]# /etc/init.d/squid restart
[root@localhost ~]# curl -xlocalhost:80 http://www.baidu.com/
[root@localhost ~]# curl -xlocalhost:80 http://www.qq.com/
[root@localhost ~]# curl -xlocalhost:80 http://www.sina.com/
```

你会发现，**baidu.com**和**qq.com**都能正常访问，然而**sina.com**访问503了，这是因为阿铭并没有加**sina.com**的相关设置。

还有一个知识点，阿铭需要介绍给你：

```
[root@localhost ~]# squid -h
Usage: squid [-cdhvzCFNRVYX] [-s | -l facility] [-f config-file] [-[au] port] [-k signal]
    -a port    Specify HTTP port number (default: 3128).
    -d level   Write debugging to stderr also.
    -f file    Use given config-file instead of
               /etc/squid/squid.conf
    -h         Print help message.
    -k reconfigure|rotate|shutdown|interrupt|kill|debug|check|parse
               Parse configuration file, then send signal to
               running copy (except -k parse) and exit.
    -s | -l facility
               Enable logging to syslog.
    -u port    Specify ICP port number (default: 3130), disable with 0.
    -v         Print version.
    -z         Create swap directories
    -C         Do not catch fatal signals.
    -D         OBSOLETE. Scheduled for removal.
    -F         Don't serve any requests until store is rebuilt.
    -N         No daemon mode.
    -R         Do not set REUSEADDR on port.
    -S         Double-check swap during rebuild.
    -X         Force full debugging.
    -Y         Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.
```

上面阿铭把**squid**命令所用到的选项全部打印出来了，但阿铭觉得最常用的除了 `squid -k check` 外，还有一个那就是 `squid -k reconfigure` 它们俩都可以简写：

```
[root@localhost ~]# squid -kche
[root@localhost ~]# squid -krec
```

其中第二条命令表示重新加载配置文件，如果我们更改了配置文件后，不需要重启**squid**服务，直接使用该命令重新加载配置即可。

阿铭建议你最好再扩展学习一下：<http://www.aminglinux.com/bbs/thread-5446-1-1.html>

教程答疑：[请移步这里](#)。

欢迎你加入 [阿铭学院](#) 和阿铭一起学习Linux，让阿铭成为你Linux生涯中永远的朋友吧！

