**Squid3服务配置安装文档**

创想空间（北京）有限公司

目录

[**1.** **Squid服务文档说明** 3](#_Toc374607574)

[**2.** **Squid服务使用范围** 3](#_Toc374607575)

[**3.** **Squid服务器拓扑图** 3](#_Toc374607576)

[**4.** **Squid安装环境及服务版本** 4](#_Toc374607577)

[**5.** **Squid服务器基础环境** 4](#_Toc374607578)

[**5.1. 启用root帐号权限** 4](#_Toc374607579)

[**5.2. 设置服务器IP地址** 4](#_Toc374607580)

[**5.3. 配置apt-get源** 5](#_Toc374607581)

[**5.4. 安装启用ssh服务** 6](#_Toc374607582)

[**5.5. 更改主机名** 6](#_Toc374607583)

[**5.6. 本地dns解析** 6](#_Toc374607584)

[**5.7. dns文件配置** 6](#_Toc374607585)

[**5.8.更改系统时间** 6](#_Toc374607586)

[**同步服务器时间** 6](#_Toc374607587)

[**6.** **安装Squid服务** 6](#_Toc374607588)

[**6.1. 安装Squid服务** 7](#_Toc374607589)

[**6.2.配置squid主配置文件** 7](#_Toc374607590)

[**6.3. 配置squid缓存文件和log** 7](#_Toc374607591)

[**6.4. 定义dns服务器地址** 7](#_Toc374607592)

[**6.5. 访问控制ACL列表** 8](#_Toc374607593)

[**6.6. 控制某个客户端访问某个域名** 9](#_Toc374607594)

[**6.7. 禁止在线看视频和听歌曲** 9](#_Toc374607595)

[**6.8. 禁止下载歌曲和视频** 10](#_Toc374607596)

[**6.9. 禁止访问部分网站** 11](#_Toc374607597)

[**6.10. 配置客户端访问错误通知** 11](#_Toc374607598)

[**7.** **安装apache支持squid脚本方式访问** 13](#_Toc374607599)

[**7.1. 安装apache2** 13](#_Toc374607600)

[**7.2. 编写squid访问脚本** 13](#_Toc374607601)

[**7.3. 重新启动apache服务和squid服务** 16](#_Toc374607602)

[**8.** **总结squid代理服务的配置文件格式** 17](#_Toc374607603)

[**9.** **客户端设置** 19](#_Toc374607604)

[**10.** **配置主代理服务器HA** 20](#_Toc374607605)

[**10.1. 安装HA服务** 21](#_Toc374607606)

[**10.2. 生成heartbeat主配置文件** 21](#_Toc374607607)

[**10.3. 配置heartbeat监听的服务文件** 21](#_Toc374607608)

[**10.4. 配置heartbeat主备服务器验证文件** 21](#_Toc374607609)

[**10.5. 启动并设置开机启动heartbeat服务** 22](#_Toc374607610)

[**10.6. 在代理squid中添加ha地址** 22](#_Toc374607611)

[**11.** **配置备份代理服务器HA** 22](#_Toc374607612)

[**11.1. 配置备份服务基础环境** 22](#_Toc374607613)

[**11.2. 安装HA服务** 22](#_Toc374607614)

[**11.3. 生成heartbeat主配置文件** 22](#_Toc374607615)

[**11.4. 配置主配置文件 ha.cf** 23](#_Toc374607616)

[**11.5. 配置heartbeat监听的服务文件** 23](#_Toc374607617)

[**11.6. 配置heartbeat主备服务器验证文件** 23](#_Toc374607618)

[**11.7. 启动并设置开机启动heartbeat服务** 23](#_Toc374607619)

[**11.8. 在代理squid中添加ha地址** 23](#_Toc374607620)

1. **Squid服务文档说明**

本文档主要介绍了安装Squid的安装环境，如何安装Squid服务，如何设置代理局域网访问Internet,如何限制网络访问，如何设置各个客户端访问Internet权限

如何监控各个服务器的硬件使用量，接如何监控不同的系统，软硬件环境。Squid互备等环境搭建。

1. **Squid服务使用范围**

Squid主要应用于公司局域网访问Internet的代理服务，针对公司全体人员及办公终端，访问internet权限设置。

1. **Squid服务器拓扑图**



1. **安装搭载squid服务ubuntu系统**

请参考ubuntu 安装文档

1. **Squid安装环境及服务版本**

|  |  |  |
| --- | --- | --- |
| Squid服务器系统 | ubuntu | 12.4 |
| Squid服务软件 | Squid | 2.7 |

1. **Squid服务器基础环境**

**5.1. 启用root帐号权限**

使用系统安装是的帐号登录

Login zss

Password：(输入实际帐号密码)

更改root密码

sudo passwd

输入root的密码

退出使用root帐号登录。

**5.2. 设置服务器IP地址**

vim /etc/network/interfacese

# The primary network interface

auto eth0

iface eth0 inet static

address 192.168.11.198

netmask 255.255.255.0

network 192.168.11.0

broadcast 192.168.11.255

gateway 192.168.11.254

# dns-\* options are implemented by the resolvconf package, if installed

dns-nameservers 192.168.240.236 192.168.240.217

**5.3. 配置apt-get源**

将原有的数据全部删除或进行备份

vi /etc/apt/sources.list(使用本地源也可使用其他网络源)

deb http://mirrors.gnetis.com/ubuntu/ precise main restricted universe multiverse

deb http://mirrors.gnetis.com/ubuntu/ precise-security main restricted universe multiverse

deb http://mirrors.gnetis.com/ubuntu/ precise-updates main restricted universe multiverse

deb http://mirrors.gnetis.com/ubuntu/ precise-proposed main restricted universe multiverse

deb http://mirrors.gnetis.com/ubuntu/ precise-backports main restricted universe multiverse

deb-src http://mirrors.gnetis.com/ubuntu/ precise main restricted universe multiverse

deb-src http://mirrors.gnetis.com/ubuntu/ precise-security main restricted universe multiverse

deb-src http://mirrors.gnetis.com/ubuntu/ precise-updates main restricted universe multiverse

deb-src http://mirrors.gnetis.com/ubuntu/ precise-proposed main restricted universe multiverse

deb-src http://mirrors.gnetis.com/ubuntu/ precise-backports main restricted universe multiverse

更新apt-get源

apt-get update

**5.4. 安装启用ssh服务**

提示：（若在ubuntu安装时未安装ssh服务，请安装ssh安装）

apt-get install ssh

启动ssh服务

/etc/init.d/ssh start

**5.5. 更改主机名**

vim /etc/hostname

proxy01.gnetis.com

**5.6. 本地dns解析**

vi /etc/hosts

192.168.11.198 proxy01.gnetis.com

无需重启系统更改主机名

hostname proxy.gnetis.com

**5.7. dns文件配置**

vim /etc/resolv.conf

search gnetis.com

nameserver 192.168.240.217

**5.8.更改系统时间**

提示：（若在ubuntu系统安装过程中没有选择时区，请按此方式更改时区。）

执行tzselect命令

选择，区域-国家-时区

将时区文件复制到当前的本机系统时间文件中

cp /usr/share/zoneinfo/Asia/Shanghai /etc/localtime

**同步服务器时间**

提示：（时间同步需要脚本运行每隔1小时进行一次同部分，所以写成脚本。）

cat <<EOF > /etc/cron.hourly/ntp.sh

#!/bin/sh

ntpdate ntp.gnetis.com

EOF

给予相应的执行权限

chmod +x /etc/cron.hourly/ntp.sh

可命令行直接运行

ntpdate ntp.gnetis.com

1. **安装Squid服务**

**6.1. 安装Squid服务**

* **使用apt-get安装**

apt-get install squid3

**6.2.配置squid主配置文件**

* **将目前squid的服务配置文件进行备份**

cp /etc/squid3/squid.conf /etc/squid3/squid.conf.bak

* **重新生成squid配置文件**

(因配置文件内容较多，所以我们将注释和空行去除)

cd /etc/squid3/

cat squid.conf.bak |grep -v "^$" |grep -v "^#" >squid.conf

* **配置squid主机名和监听端口**

vim /etc/squid/squid.conf

visible\_hostname proxy.gnetis.com

http\_port 192.168.11.198:3128

* **配置squid 访问缓存目录**
* **配置squid 日志存放目录**
* **重新启动squid服务**

**未完待续……**

/etc/init.d/squid restart

**6.3. 配置squid缓存文件和log**

vim /etc/squid/squid.conf

#cache file

cache\_dir ufs /var/spool/squid 2000 16 256

cache\_mem 64MB

cache\_swap\_low 90

cache\_swap\_high 95

maximum\_object\_size\_in\_memory 1024 KB

cache\_dir null /tmp

cache\_access\_log /var/squid/access.log

cache\_log /var/squid/cache.log

cache\_store\_log /var/squid/store.log

**6.4. 定义dns服务器地址**

#dns service

dns\_nameservers 192.168.240.217

**6.5. 访问控制ACL列表**

* **acl控制列表简介**

**加入客户端控制文件**

* 创建允许client列表存放目录

mkdir -p /etc/squid/allow/client

* 创建访问不受限制客户端文件

vim /etc/squid/allow/client/allow\_access

* 创建访问不受限制以mac方式记录的客户端

vim /etc/squid/allow/client/allow\_mac

* 创建访问网络允许使用代理的网段

vim /etc/squid/allow/client/allow\_segment

* 创建允许service列表存放目录

mkdir -p /etc/squid/allow/server/

* 创建允许目标地址列表

vim /etc/squid/allow/server/allow\_target\_ip

* 创建拒绝client列表存放目录

mkdir -p /etc/squid/deny/client

* 创建拒客户端使用代理文件

vim /etc/squid/deny/client/deny\_access

* 创建拒绝service列表存放目录

mkdir -p /etc/squid/deny/server

* 创建拒绝通过代理访问的域名列表

vim /etc/squid/deny/server/deny\_domin

* 创建拒绝使用代理的ip地址段列表

vim /etc/squid/deny/server/deny\_target\_ip

* **配置squid.conf写入acl策略**

**允许客户端访问squid代理**

#acl list

#allow acl

#client

acl allow\_access src "/etc/squid/allow/client/allow\_access"

acl allow\_mac arp "/etc/squid/allow/client/allow\_mac"

acl allow\_segment src "/etc/squid/allow/client/allow\_segment"

#server

acl allow\_target\_ip dst "/etc/squid/allow/server/allow\_target\_ip"

#all

acl all src all

acl manager proto cache\_object

acl localhost src 127.0.0.1/32

#deny acl

#client

acl deny\_access src "/etc/squid/deny/client/deny\_access"

#server

acl deny\_domin dstdomain "/etc/squid/deny/server/deny\_domin"

acl deny\_target\_ip dst "/etc/squid/deny/server/deny\_target\_ip"

* **添加控制acl列表**

acl 控制列表是按照从上至下的顺序进行匹配的

#acl control allow and deny

http\_access allow allow\_access

http\_access allow allow\_mac

http\_access allow allow\_target\_ip

http\_access deny deny\_domin

http\_access deny deny\_target\_ip

http\_access allow allow\_segment

http\_access deny all

**6.6. 控制某个客户端访问某个域名**

* 创建ip控制列表：

vim /etc/squid/taobao\_allow

加入需要访问淘宝的ip地址即可

vim /etc/squid/allow/taobao\_allow

#taobao allow

acl taobao\_allow src "/etc/squid/taobao\_allow"

#acl taobao\_acl dstdomain -i www.taobao.com

acl taobao\_acl1 url\_regex -i taobao.com

http\_access allow taobao\_allow taobao\_acl1(注意acl的位置)

**6.7. 禁止在线看视频和听歌曲**

加入视频音频格式

vim /etc/squid/squid.conf

#allow downloads

acl deny\_format urlpath\_regex -i \.exe$\.zip$\.rar$\.mp3$\.iso$ \.mtv$ \.flash$ \.mov$ \.wmp$ \.wmv$ \.rm$ \.3gp$ \.mv$ \.mpg$ \.mpeg$ \.flv$ \.mpga$ \.torrent$ \.wma$ \.avi$ \.rmvb$ \.mp4$\.swf$\.asf$\.wav$\.gif$\.ra$\.ram$.\asf$.\mid$

http\_access deny deny\_format (注意acl的顺序)

**6.8. 禁止下载歌曲和视频**

* 加入视频音频格式

vim /etc/squid/squid.conf

#deny downloads

acl no\_down url\_regex -i .exe$ .zip$ .rar$ .mp3$ .iso$ .mtv$ .flash$ .mov$ .wmp$ .wmv$ .rm$ .3gp$ .mv$ .mpg$ .mpeg$ .flv$ .mpga$ .torrent$ .wma$ .avi$ .rmvb$ .mp4$ .swf$ .asf$ .wav$ .gif$ .ra$ .ram$ .asf$ .mid$

http\_access deny no\_down(注意acl的顺序)

* 加入禁止下载脚本(当客户端访问时，若出现squid.conf中禁止下载的格式，则将跳转，调用iptables的input规则禁止访问。)

vim /etc/squid/redirectory.pl

#!/usr/bin/perl -wl

$|=1; # don't buffer the output

$DENIED = "http://wqy.gnetis.com/";

&load\_word\_list( );

my $uri;

while (my $line=<>) {

$uri=$line;

if (&word\_match($uri)) {

my ($a, $ip, $b, $c) = split(/ /,$uri);

$ip =~ s/\/.\*$//;

system("iptables -I INPUT -s $ip -j DROP");

$uri = "302:$DENIED";

} else {

$uri="";

}

} continue {

print "$uri";

}

sub load\_word\_list {

@words = qw(thunder verycd torrent NetAnts FlashGet);

}

sub word\_match {

my $uri = shift;

foreach $w (@words) { return 1 if ($uri =~ /$w/); }

return 0;

}

将跳转脚本加入squid配置文件中

vim /etc/squid/squid.conf

#url\_rewrite

url\_rewrite\_program /etc/squid/redirectory.pl

url\_rewrite\_access allow all

location\_rewrite\_program /etc/squid/redirectory.pl

location\_rewrite\_access allow all

redirector\_bypass off

**6.9. 禁止访问部分网站**

vim /etc/squid/deny/server/deny\_domin

请参考deny\_domain表(可根据实际情况添加想禁止访问的网站)



**6.10. 配置客户端访问错误通知**

Squid访问错误通知脚本默认在/usr/share/squid/errors/Simplify\_Chinese目录中。

**更改被禁止访问的网页通知**

vim /usr/share/squid/errors/Simplify\_Chinese/ERR\_ACCESS\_DENIED

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />

<title>URL过滤</title>

<style type="text/css">

\* {

padding: 0;

margin: 0;

}

body {

background: #e7e8e9;

}

#content {

width: 900px;

background: #fff;

border: 1px solid #dcdde2;

padding: 30px;

margin: 20px auto;

}

#content h1 {

padding-bottom: 5px;

font: bold 28px/40px "微软雅黑";

color: #333;

}

.partition {

height: 3px;

overflow: hidden;

background: #00aeef;

}

.partition\_left {

height: 3px;

display: block;

float: left;

background: #005aab;

}

#content p {

font: 14px/24px "微软雅黑";

margin-top: 2em;

color: #333;

}

</style>

</head>

<body>

<div id="content">

<h1 class="warning">访问被拒绝</h1>

<div class="partition"> <span class="partition\_left" style="width:150px;"></span> </div>

<p class="b\_distance">依据公司上网权限策略，您尝试访问的网站已经被拒绝。如果有疑问，请联系信息系统部。</p>

<p class="b\_distance">我们的联系电话：010-5993 3599-6666<br>

我们的统一服务邮箱：ithelp@quanshi.com</p>

</div>

</body>

</html>

**将脚本路径加入squid配置文件中**

vim /etc/squid/squid.conf

#Report the account

error\_directory /usr/share/squid/errors/Simplify\_Chinese

cache\_mgr ithelp@quanshi.com

visible\_hostname proxy.gnetis.com

1. **安装apache支持squid脚本方式访问**

**7.1. 安装apache2**

apt-get install apache2

进入网页脚本默认存放位置

cd /var/www/

**7.2. 编写squid访问脚本**

function FindProxyForURL(url, host)

{

if (isPlainHostName(host) ||

dnsDomainIs(host, ".gnetis.com") ||

dnsDomainIs(host, ".siemens.com") ||

dnsDomainIs(host, ".renhe.cn") ||

dnsDomainIs(host, ".quanshihuiyi.com") ||

dnsDomainIs(host, ".iflytek.com") ||

dnsDomainIs(host, ".soluxeint.com") ||

dnsDomainIs(host, ".quanshi.com") ||

dnsDomainIs(host, ".quanshievent.com") ||

dnsDomainIs(host, ".supersales.com") ||

dnsDomainIs(host, ".imsupersales.com") ||

dnsDomainIs(host, ".imsupersales.com.cn") ||

dnsDomainIs(host, ".imsupersales.cn") ||

dnsDomainIs(host, ".quanshimeeting.com") ||

dnsDomainIs(host, ".gnetvmeeting.com") ||

dnsDomainIs(host, ".gnet.com") ||

dnsDomainIs(host, ".gnetcenter.cn") ||

dnsDomainIs(host, ".meetingoffice.com") ||

dnsDomainIs(host, ".gnetspace.com") ||

dnsDomainIs(host, ".gnetis.net") ||

dnsDomainIs(host, ".econference.com.cn") ||

dnsDomainIs(host, ".conferencing.com") ||

dnsDomainIs(host, ".gnetconferencing.com") ||

dnsDomainIs(host, ".collabway.com") ||

dnsDomainIs(host, ".meetmeplus.com") ||

isInNet(host, "10.10.10.0", "255.255.255.0") ||

isInNet(host, "203.174.0.0", "255.255.0.0") ||

isInNet(host, "204.174.0.0", "255.255.0.0") ||

isInNet(host, "61.147.84.45", "255.255.255.255") ||

isInNet(host, "119.161.160.133", "255.255.255.255") ||

isInNet(host, "59.108.5.64", "255.255.255.192") ||

isInNet(host, "127.0.0.1", "255.255.255.255") ||

isInNet(host, "172.16.0.0", "255.255.0.0") ||

isInNet(host, "172.0.0.0", "255.0.0.0") ||

isInNet(host, "172.31.0.0", "255.255.0.0") ||

isInNet(host, "10.156.0.0", "255.255.0.0") ||

isInNet(host, "10.155.0.0", "255.255.0.0") ||

isInNet(host, "222.186.35.204", "255.255.255.255") ||

isInNet(host, "222.73.177.252", "255.255.255.255") ||

isInNet(host, "60.5.252.229", "255.255.255.255") ||

isInNet(host, "123.125.163.40", "255.255.255.255") ||

isInNet(host, "125.64.148.131", "255.255.255.255") ||

isInNet(host, "220.165.14.38", "255.255.255.255") ||

isInNet(host, "202.120.161.74", "255.255.255.255") ||

isInNet(host, "59.39.31.164", "255.255.255.255") ||

isInNet(host, "59.39.31.168", "255.255.255.255") ||

isInNet(host, "218.25.17.194", "255.255.255.255") ||

isInNet(host, "60.210.16.41", "255.255.255.255") ||

isInNet(host, "116.114.19.15", "255.255.255.255") ||

isInNet(host, "116.114.19.19", "255.255.255.255") ||

isInNet(host, "61.158.128.168", "255.255.255.255") ||

isInNet(host, "58.221.247.111", "255.255.255.255") ||

isInNet(host, "183.60.0.0", "255.255.0.0") ||

isInNet(host, "192.168.0.0", "255.255.0.0"))

return "DIRECT";

else if(isInNet(myIpAddress(),"192.168.240.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.29.0","255.255.255.0"))

{

return "PROXY 192.168.40.240:3128";

}

else if(isInNet(myIpAddress(),"192.168.40.0","255.255.255.0"))

{

return "PROXY 192.168.40.240:3128";

}

else if(isInNet(myIpAddress(),"192.168.30.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.20.0","255.255.255.0"))

{

return "PROXY 192.168.20.248:3128";

}

else if(isInNet(myIpAddress(),"192.168.18.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.17.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.15.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.13.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.12.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.11.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.25.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.101.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

else if(isInNet(myIpAddress(),"192.168.10.0","255.255.255.0"))

{

return "PROXY 192.168.11.195:3128";

}

}

**7.3. 重新启动apache服务和squid服务**

/etc/init.d/squid restart

update-rc.d squid enable on

/etc/init.d/apache2

update-rc.d apache2 enable on

1. **总结squid代理服务的配置文件格式**

#acl list

#allow acl

#client

acl allow\_access src "/etc/squid/allow/client/allow\_access"

acl allow\_mac arp "/etc/squid/allow/client/allow\_mac"

acl allow\_segment src "/etc/squid/allow/client/allow\_segment"

#server

acl allow\_target\_ip dst "/etc/squid/allow/server/allow\_target\_ip"

#all

acl all src all

acl manager proto cache\_object

acl localhost src 127.0.0.1/32

#deny acl

#client

acl deny\_access src "/etc/squid/deny/client/deny\_access"

#server

acl deny\_domin dstdomain "/etc/squid/deny/server/deny\_domin"

acl deny\_target\_ip dst "/etc/squid/deny/server/deny\_target\_ip"

#localhost

acl to\_localhost dst 127.0.0.0/8 0.0.0.0/32

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 SSL\_ports port 563 # snews

acl SSL\_ports port 873 # rsync

acl Safe\_ports port 80 # http

acl Safe\_ports port 21 # ftp

acl Safe\_ports port 443 # https

acl Safe\_ports port 70 # gopher

acl Safe\_ports port 210 # wais

acl Safe\_ports port 1025-65535 # unregistered ports

acl Safe\_ports port 280 # http-mgmt

acl Safe\_ports port 488 # gss-http

acl Safe\_ports port 591 # filemaker

acl Safe\_ports port 777 # multiling http

acl Safe\_ports port 631 # cups

acl Safe\_ports port 873 # rsync

acl Safe\_ports port 901 # SWAT

acl purge method PURGE

acl CONNECT method CONNECT

#taobao allow

acl taobao\_allow src "/etc/squid/taobao\_allow"

acl taobao\_acl url\_regex -i taobao.com

#allow downloads

#acl control allow and deny

http\_access allow allow\_access

http\_access allow allow\_mac

http\_access allow allow\_target\_ip

http\_access allow taobao\_allow taobao\_acl

http\_access deny deny\_target\_ip

http\_access deny audio

http\_access deny no\_down

http\_access deny deny\_domin

http\_access allow allow\_segment

http\_access allow manager localhost

http\_access deny manager

http\_access allow purge localhost

http\_access deny purge

http\_access deny !Safe\_ports

http\_access deny CONNECT !SSL\_ports

http\_access allow localhost

http\_access deny all

icp\_access allow localnet

icp\_access deny all

hierarchy\_stoplist cgi-bin ?

access\_log /var/log/squid/access.log squid

refresh\_pattern ^ftp: 1440 20% 10080

refresh\_pattern ^gopher: 1440 0% 1440

refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

refresh\_pattern (Release|Package(.gz)\*)$ 0 20% 2880

refresh\_pattern . 0 20% 4320

acl shoutcast rep\_header X-HTTP09-First-Line ^ICY.[0-9]

upgrade\_http0.9 deny shoutcast

acl apache rep\_header Server ^Apache

broken\_vary\_encoding allow apache

extension\_methods REPORT MERGE MKACTIVITY CHECKOUT

hosts\_file /etc/hosts

coredump\_dir /var/spool/squid

#name-port

visible\_hostname proxy.gnetis.com

http\_port 192.168.11.195:3128 transparent

http\_port 127.0.0.1:8080

#cache file

cache\_dir ufs /var/spool/squid 2000 16 256

cache\_mem 64.000000 bytes

cache\_swap\_low 90

cache\_swap\_high 95

maximum\_object\_size\_in\_memory 1024 KB

cache\_dir null /tmp

cache\_access\_log /var/log/squid/access.log

cache\_log /var/log/squid/cache.log

cache\_store\_log /var/log/squid/store.log

#Report the account

error\_directory /usr/share/squid/errors/Simplify\_Chinese

cache\_mgr ithelp@quanshi.com

visible\_hostname proxy.gnetis.com

#dns service

dns\_nameservers 192.168.240.217

#url\_rewrite

url\_rewrite\_program /etc/squid/redirectory.pl

url\_rewrite\_access allow all

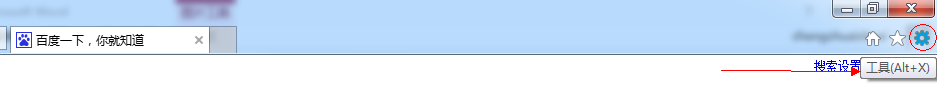
location\_rewrite\_program /etc/squid/redirectory.pl

location\_rewrite\_access allow all

redirector\_bypass off

1. **客户端设置**

* **第一步：选择ie浏览器**

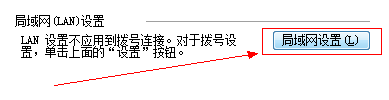


* **第二步：选择internet选项**

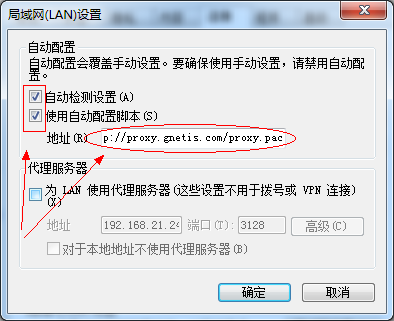
选择连接



* **第三步：选择局域网设置**



选择响应的代理配置，并填入相应的代理地址



* **完成：确定保存即可**

1. **配置主代理服务器HA**

**10.1. 安装HA服务**

apt-get install heartbeat

**10.2. 生成heartbeat主配置文件**

进入heartbeat目录

cd /etc/heartbeat/

将文件配置文件包复制到heartbeat主目录中并解压

cp /usr/share/doc/heartbeat/ha.cf.gz ./

cp /usr/share/doc/heartbeat/haresources.gz ./

cp /usr/share/doc/heartbeat/authkeys ./

gunzip ha.cf.gz

gunzip haresources.gz

配置主配置文件 ha.cf

debugfile /var/log/ha-debug

logfile /var/log/ha-log

logfacility local0

keepalive 1

deadtime 10

warntime 5

initdead 20

udpport 694

ucast eth0 192.168.21.250

auto\_failback on

node proxy001

node proxy002

ping\_group group1 192.168.21.250

respawn hacluster /usr/lib/heartbeat/ipfail

apiauth ipfail gid=root uid=root

**10.3. 配置heartbeat监听的服务文件**

vim /etc/ha.d/haresources

proxy01 IPaddr::192.168.21.248 apache2

**10.4. 配置heartbeat主备服务器验证文件**

vim /etc/ha.d/authkeys

auth 2

2 sha1 HI!

更改authkeys文件权限(否则会造成启动失败)

chmod 700 authkeys

**10.5. 启动并设置开机启动heartbeat服务**

/etc/ini.d/heartbeat start

update-rc.d heartbeat enable on

**10.6. 在代理squid中添加ha地址**

vim /etc/squid/squid.conf

http\_port 192.168.11.248:3128 transparent

重启squid服务

/etc/init.d/squid restart

1. **配置备份代理服务器HA**

**11.1. 配置备份服务基础环境**

* **更改hosts文件**

vim /etc/hosts

192.168.21.250 proxy002

192.168.11.195 proxy001

192.168.11.170 proxy001

* **更改主机名**

vim /etc/hostname

proxy002

**11.2. 安装HA服务**

apt-get install heartbeat

**11.3. 生成heartbeat主配置文件**

进入heartbeat目录

cd /etc/heartbeat/

将文件配置文件包复制到heartbeat主目录中并解压

cp /usr/share/doc/heartbeat/ha.cf.gz ./

cp /usr/share/doc/heartbeat/haresources.gz ./

cp /usr/share/doc/heartbeat/authkeys ./

gunzip ha.cf.gz

gunzip haresources.gz

**11.4. 配置主配置文件 ha.cf**

debugfile /var/log/ha-debug

logfile /var/log/ha-log

logfacility local0

keepalive 1

deadtime 10

warntime 5

initdead 20

udpport 694

ucast eth0 192.168.21.249

auto\_failback on

node proxy001

node proxy002

ping\_group group1 192.168.21.249

respawn hacluster /usr/lib/heartbeat/ipfail

apiauth ipfail gid=root uid=root

**11.5. 配置heartbeat监听的服务文件**

vim /etc/ha.d/haresources

proxy001 IPaddr::192.168.21.248 apache2

**11.6. 配置heartbeat主备服务器验证文件**

vim /etc/ha.d/authkeys

auth 2

2 sha1 HI!

更改authkeys文件权限(否则会造成启动失败)

chmod 700 authkeys

**11.7. 启动并设置开机启动heartbeat服务**

/etc/ini.d/heartbeat start

update-rc.d heartbeat enable on

**11.8. 在代理squid中添加ha地址**

vim /etc/squid/squid.conf

http\_port 192.168.11.248:3128 transparent

重启squid服务

/etc/init.d/squid restart