

北京网关服务器配置信息

安装所需要的服务

- yum -y install dhcp bind* squid nscd

配置dhcp

1. path:/etc/dhcp/dhcpd.conf

2. 配置内容

- option domain-name-servers 192.168.88.254;
- allow booting;
- allow bootp;
- default-lease-time 86400;
- max-lease-time 172800;
- ddns-update-style none;
- log-facility local7;
- subnet 192.168.88.0 netmask 255.255.254.0 {
- option domain-name-servers 192.168.88.254;
- option routers 192.168.88.254;
- option broadcast-address 192.168.88.255;
- default-lease-time 86400;
- max-lease-time 172800;
- range 192.168.88.32 192.168.88.200;
- range 192.168.89.32 192.168.89.200;}

3.备注

- 目前的dhcp, 花费了2个网段, ip范围为32-200,两头剩余的ip为保留ip
- dhcpd.conf是dhcp的核心配置文件, 如果要增加网段, 绑定固定ip, 均在这个文件里面

配置squid

1.path: /etc/squid/squid.conf

2.配置内容

- 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 192.168.0.0/23 # RFC1918 possible internal network
- acl not_download urlpath_regex -i .exe\$.msi\$.scr\$.mp3\$.flv\$.swf\$.wmv\$.mp4\$.zip\$.tar\$.rar\$.gz\$.bz2\$.7z\$.rm\$.rmb\$.avi\$.rmvb\$.iso\$
- acl not_allow_url_regex -i kaixin001.com kaixin.com
- acl english_allow url_regex -i 61.152.221.169 218.1.73.24 218.1.69.123 123.103.15.222
- acl SSL_ports port 443
- 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 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 english_allow
- http_access allow localnet
- http_access allow localhost
- http_access deny all
- http_port 192.168.88.254:8090 intercept
- hierarchy_stoplist cgi-bin ?
- cache_mem 512 MB
- maximum_object_size_in_memory 512 KB
- cache_dir aufs /cache/squid/cache 10240 16 256
- maximum_object_size 65536 KB
- cache_swap_low 30
- cache_swap_high 40
- access_log none
- cache_swap_state /cache/squid/cache/swap.state

- buffered_logs on
- cache_log **/cache/squid/var/logs/cache.log**
- coredump_dir **/cache/squid/var/logs**
- refresh_pattern ^ftp: 1440 20% 10080
- refresh_pattern ^gopher: 1440 0% 1440
- refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
- refresh_pattern . 0 20% 4320
- request_body_max_size 0 KB
- client_request_buffer_max_size 512 KB

3.备注

- 代理端口8090
- 查询了解squid缓存的设置

配置DNS

1.path:/etc/named.conf

2:配置内容

- options {
- notify-source 127.0.0.1;
- transfer-source 127.0.0.1;
- port 53;
- rrset-order {order cyclic};
- directory **"/var/named/chroot/";**
- pid-file **"/var/named/chroot/var/run/named.pid";**
- listen-on { 192.168.88.254; };
- listen-on-v6 { none; };
- forwarders { 127.0.0.1; };
- notify yes;
- };
- key rndc_key {
- secret "21tbcdnsdhcpPASS";
- algorithm hmac-md5;
- };
- controls {
- inet 127.0.0.1 port 953 allow { any; } keys { rndc_key; };
- };
- zone "." IN {
- type hint;
- file "db/named.ca";
- };
- zone "localdomain" IN {
- type master;
- file "db/localdomain.db";
- allow-update { none; };
- };
- zone "localhost" IN {
- type master;
- file "db/localhost.db";
- allow-update { none; };
- };
- zone "0.168.192.in-addr.arpa" IN {
- type master;
- file "192.db";
- check-integrity no;
- allow-update { 127.0.0.1; 192.168.0.1; };
- allow-transfer { 127.0.0.1; 192.168.0.1; };
- };

3.备注：需了解dns的chroot

配置nscd

1.path:/etc/nscd.conf

2.配置内容

- server-user nscd
- debug-level 0
- paranoia no
- **enable-cache hosts yes**
- positive-time-to-live hosts 3600

- negative-time-to-live hosts 20
- suggested-size hosts 211
- check-files hosts yes
- persistent hosts yes
- shared hosts yes
- max-db-size hosts 33554432

说明

- 1.网关服务器主要配置了NAT转发，squid做代理上网
- 2.脚本统一放在/data/shell下面
- 3.p4p1做IN口配置内网IP192.168.88.254,p1p1做OUT口配置外网ip：218.241.220.44
- 4.本机额外装了nload，iftop监控工具，使用源码包编译安装，可监控网络带宽的使用情况