DNS & BIND

DNS(Domain Name Service) 域名解析服务，基础性服务。

域名：[www.magedu.com](http://www.magedu.com)(主机名，FQDN（Full Qualified Domain Name）完全限定域名)

DNS是用来干什么的： 名称解析，名称转换（背后有查询过程，数据库）

FQDN < ----- > IP

172.16.0.1 [www.magedu.com](http://www.magedu.com)

172.16.0.2 mail.magedu.com

nsswitch:

## hosts文件

hosts: files dns

file : /etc/hosts

dns: DNS

stub resolver:名称解析器

ping [www.magedu.com](http://www.magedu.com) 就会调用stub resolver，解析hosts文件。

报文交换网络，路由网络的发展壮大。主机越来越多。IP地址没有域名好记。人容易记住。

## hosts文件对应关系

IP FQDN Aliases

172.16.0.1 [www.magedu.com](http://www.magedu.com) www

通过名称就可以找到对应的IP，通过IP也能找到对应的名称。

## DNS诞生背景

htos文件中维护10，100条无所谓，成千上万就行不通了。所以hosts是早期计算机网络发展遗留的产物。在早期双方需要通信了，就去下载对方hots文件覆盖本地hosts文件，就是下载其他主机的信息。以便进行通信，但是随着http的到来，互联网的春天到了，互联网中的主机爆炸式增长。这种方法就行不通了于是就诞生了名称地址管理机构，IANA（美国政府主导）后来诞生了ICANN（有很多分支机构），其实就是维护互联网中主机的IP地址和这台主机的名称的对应关系的这么一个数据库。 所以发展过程如下

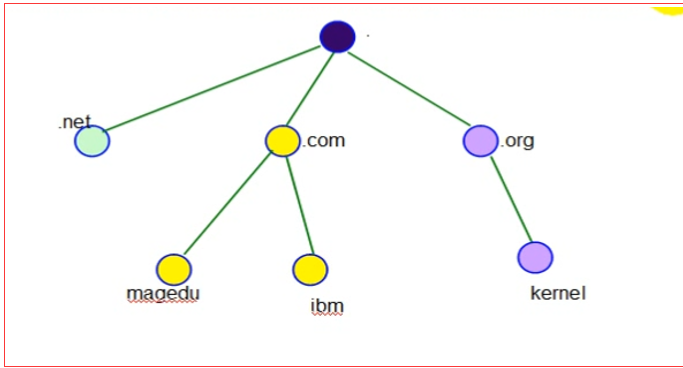
1. 周期的下载主机信息（个人）
2. INANA server 移交到专门的NS主机进行处理，
3. 一个server还不够
4. 分布式数据库，逐级授权。逐级下放。

## DNS域的层级结构

从小到大

. 是根域

.net .com .org 是组织域也称为顶级域 .gov .edu .info



TLD (TOP Layer Domain)

组织域 .com .net .org

国家域 .cn .tw .hk .iq .ir .jp

反向域 IP---> FQDN

解析：

反向：IP---> FQDN

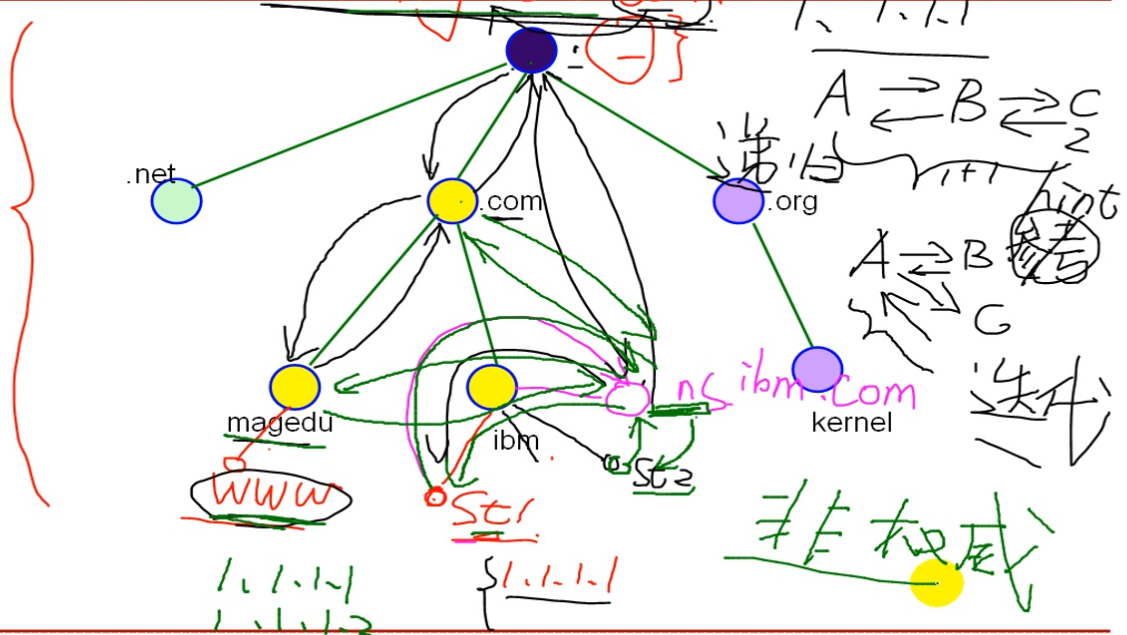
正向：FQDN----->IP

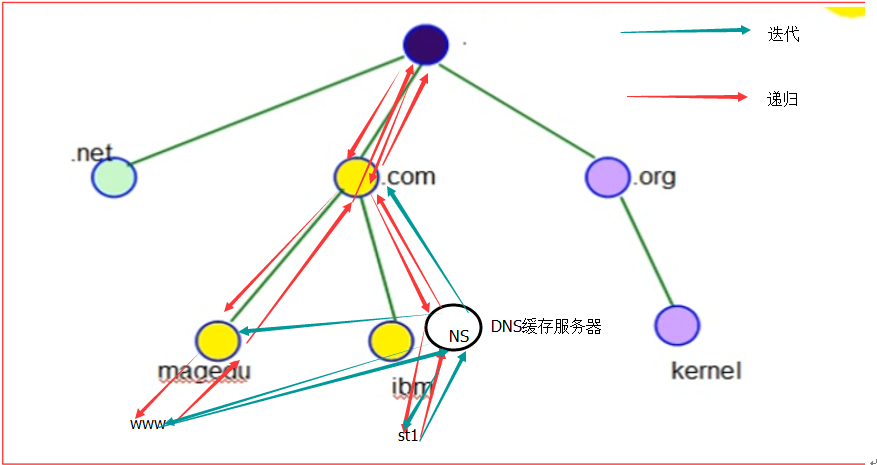
www.magedu.com.

名称是从底向上，授权是从顶到底的。

IP和域名是多对多的关系。

## 工作机制





注：NS 就是DNS缓存服务器。

两端式的查询：递归+迭代

对于st1是递归的。对于ns是迭代的。节省了带宽，根域也不会累死。

DNS分布式数据库：上级仅知道直接下级，下级只知道根的位置

DNS服务器：

接收本地客户查询（递归），肯定答案和否定答案都是有TTL

对于三级域垮域请求，不予递归。

TTL缓存时间，避免频繁的请求查询，减轻服务器压力。

内部客户端请求：权威答案 （递归）

肯定答案：TTL

否定答案：TTL

外部客户端请求：非权威答案（迭代）

所以内部NS一定要给你递归。内部NS不递归就over了。

全球有13台根域名服务器，安全级别相当高。中国没有，连个镜像都没有。

a.root-server.net – m.root-server.net 13个

## DNS服务器类型

DNS主从服务器

主服务器：数据修改

辅助服务器：请求数据同步，

需要定义：

版本号 检查时间周期 重试时间 过期时间 否定答案的缓存时间 TTL

缓存DNS服务器：只提供缓存机制。

DNS转发器： 不缓存，只负责转发。

谁负责地址解析。由直接上级指定。

## 资源记录

数据库中的每一个条目称之为一个资源记录。(Resource Record),

格式：

NAME [TTL] IN RRT(资源记录类型) VALUE

[www.mageude.com](http://www.mageude.com). 600 IN PTR www.magedu.com.

## 资源记录类型

1. SOA（Start Of Authority）: 起始授权记录，标明一个区域内部主从服务器如何同步数据，以及起始授权对象是谁的。

Zone Name TTL IN SOA FQDN serial adminMail\_Box(

serial number

refresh

retry

expire

na ttl)

时间单位：M （分钟） ，H（小时）， D(天) ，w(周) ，默认单位是秒

邮箱格式：[admin@magedu.com](mailto:admin@magedu.com) 写为 admin.magedu.com

magedu.com. 600 IN SOA ns1.magedu.com. admin.magedu.com. (

2017102401

1H

5M

1W

1D)

1. NS(name server) : Zone Name ------->FQDN 片儿长

Name Server : Domain name -------> IP 还需要一个地址 需要成组出现

magedu.com. 600 IN NS ns.magedu.com.

ns.magedu.com. 600 IN A 1.1.1.2

1. MX(mail eXchanger):Zone Name ---------> FQDN 邮件服务器 多个

Zone Name TTL IN MX PRI(优先级) VALUE

magedu.com. 600 IN MX 10 mail.magedu.com.

mail.magedu.com. 600 IN A 1.1.1.3

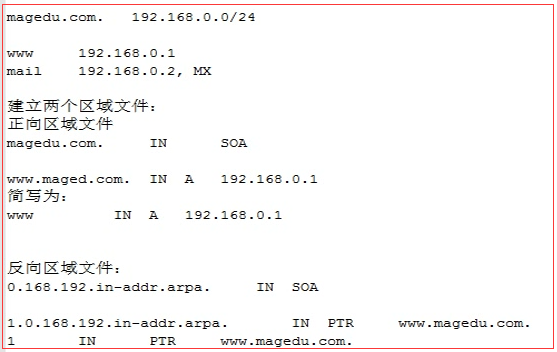
1. A(address) : FQDN ------> IPv4
2. AAAA: FQDN---------->Ipv6
3. PTR (pointer) : IP ------>FQDN
4. CNAME : FQDN-------FQDN 别名记录

[www.magedu.com](http://www.magedu.com). IN CNAME [www.magedu.com](http://www.magedu.com).

对于DNS来说

域： domain 是逻辑概念

区域：Zone 是物理概念



区域传送：

完全区域传送 AXFR

增量区域传送 IXFR

区域类型：

主区域： master

从区域： slaver

提示区域： hint 定义根在什么地方

转发区域： forward直接配置要找的服务地址。不用找根了。

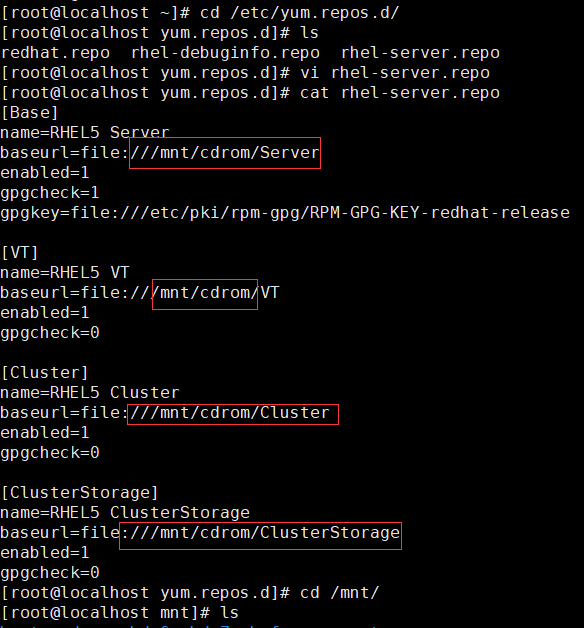
## BIND

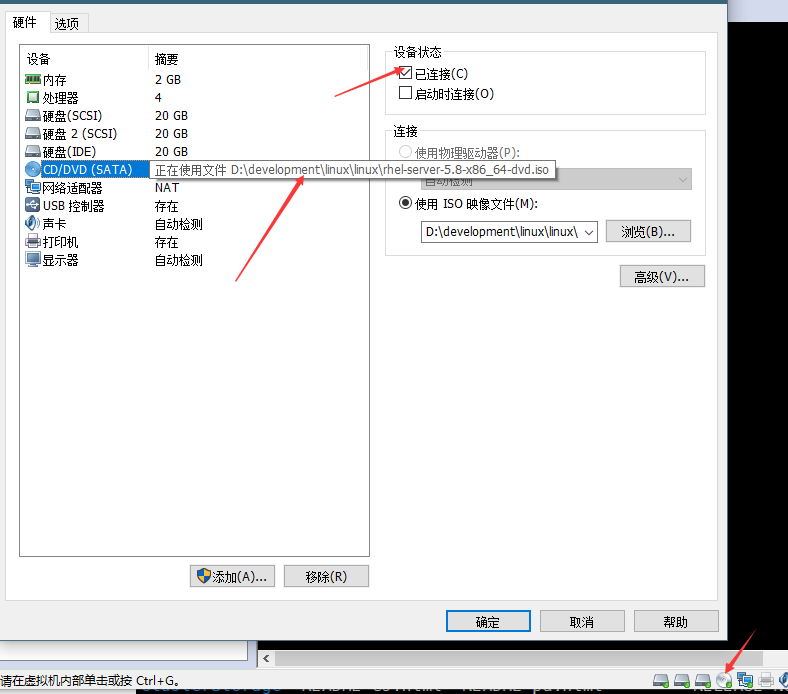
Berkeley Internete Name Domain

ISC [www.ISC.org](http://www.ISC.org)

当然红帽也提供了rpm包

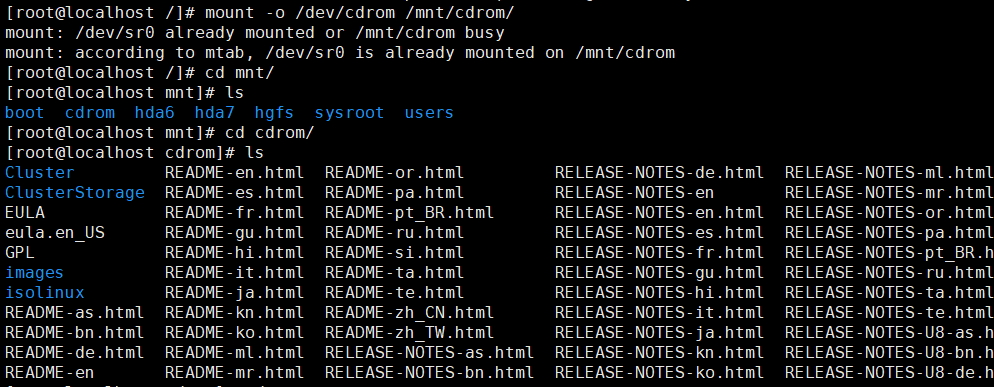
先进性挂载



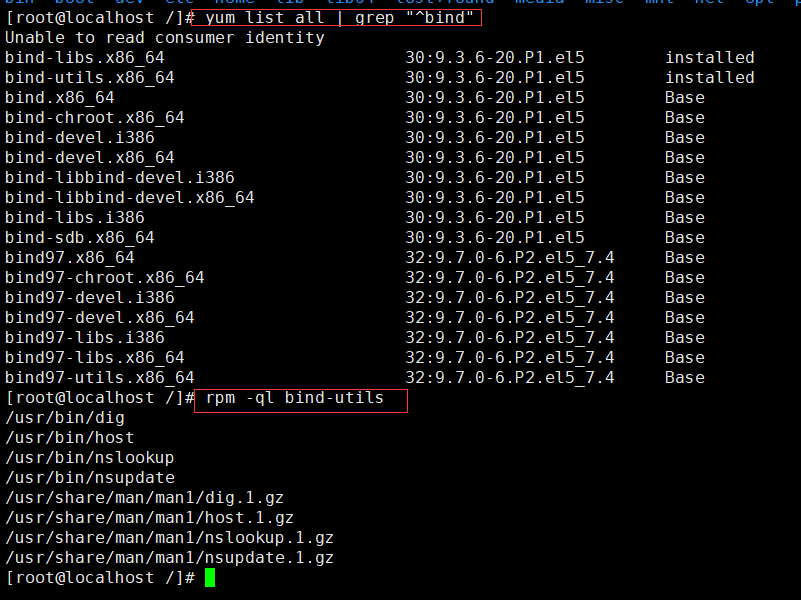


进行挂载

mount –r /dev/cdrom /mnt/cdrom/



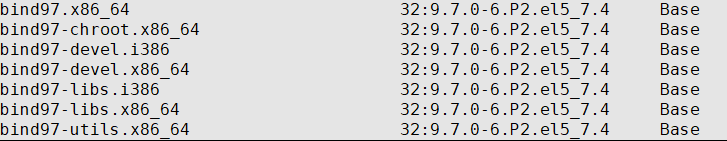
yum list all | grep “^bind”

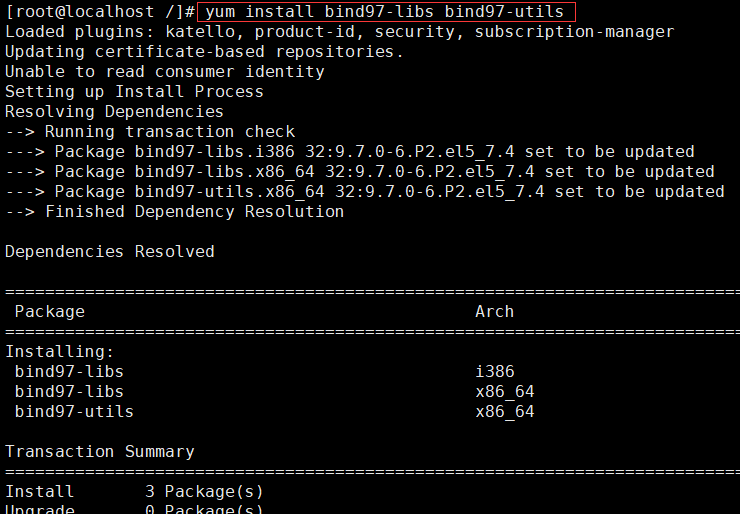


卸载已经安装的两个

[root@localhost /]# rpm -e bind-libs bind-utils

安装bind97 主流版





bind97主配置文件

/etc/named.conf

BIND进程的工作属性

区域的定义

/etc/rndc.key 远程控制工具的秘钥文件

rndc: Remote Name Domain Controller

/etc/rndc.conf 配置文件信息

/var/named/\*\* 区域数据文件

/etc/rc.d/init.d/named 脚本

{start|stop|restart|status|reload|configtest(配置测试文件)}

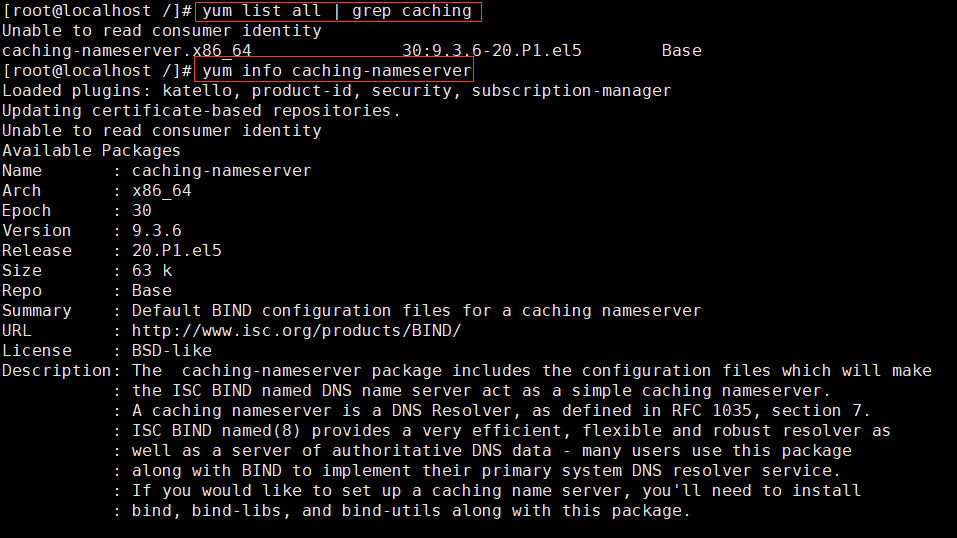
二进制程序：named

bind-chroot: 加强服务器安全的手段。

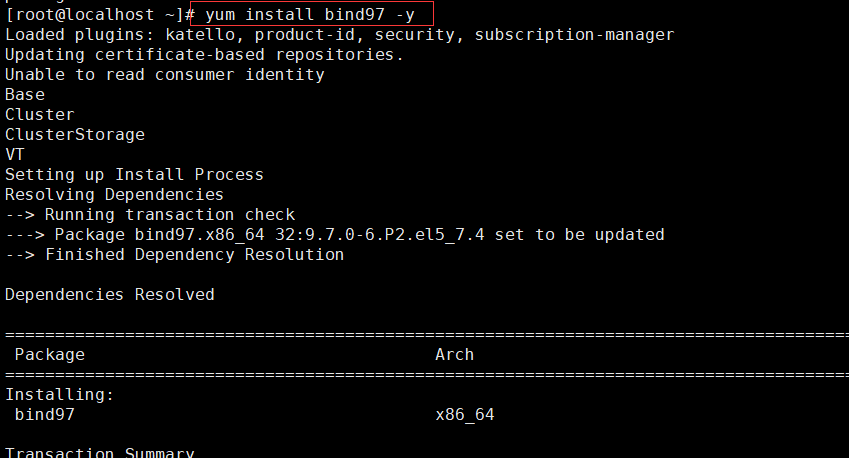
yum list all | grep caching

yum info caching-nameserver 查看软件包信息

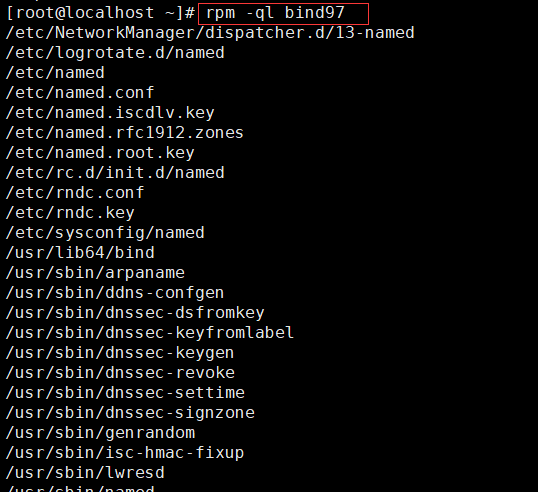
rpm –qi xxx 查看软件包信息



yum install bind97 -y



rpm –al bind97 查看生成了哪些文件



/etc/named.conf 主配置文件

常用到的命令：

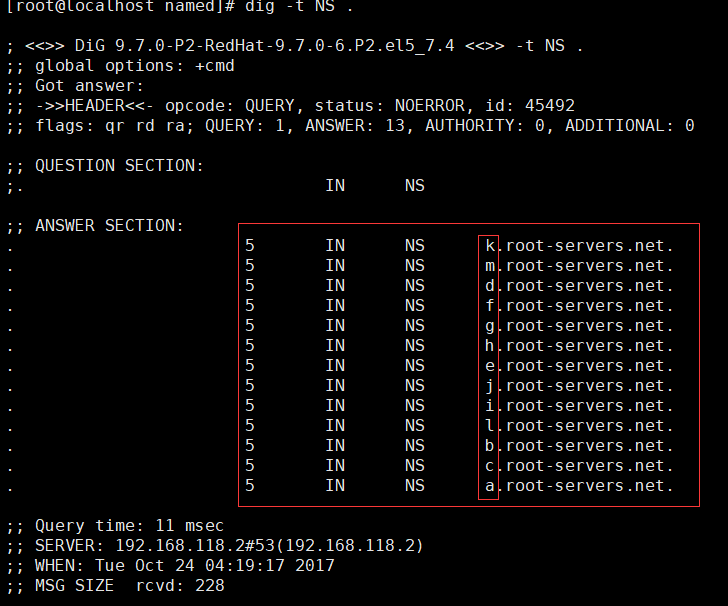
检查命令

named-checkconfig

named-checkzone

dig : Domain Information Gropher 到域名系统中去查找记录

dig –t NS .



DNS: 监听的协议及端口

53/udp 查询使用，免三次握手

53/tcp

953/rndc 远程控制的端口



listen-on port 53 ;

directory “/var/named”目录 最关键的 数据目录

recursion yes 给被人递归

allow-query {localhost；}允许谁来查询

区域：

zone “ZONE NAME” IN{

type{master|slave|hint|forward};

};

主区域：

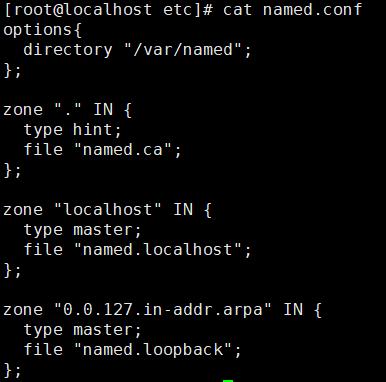
file “区域数据文件”

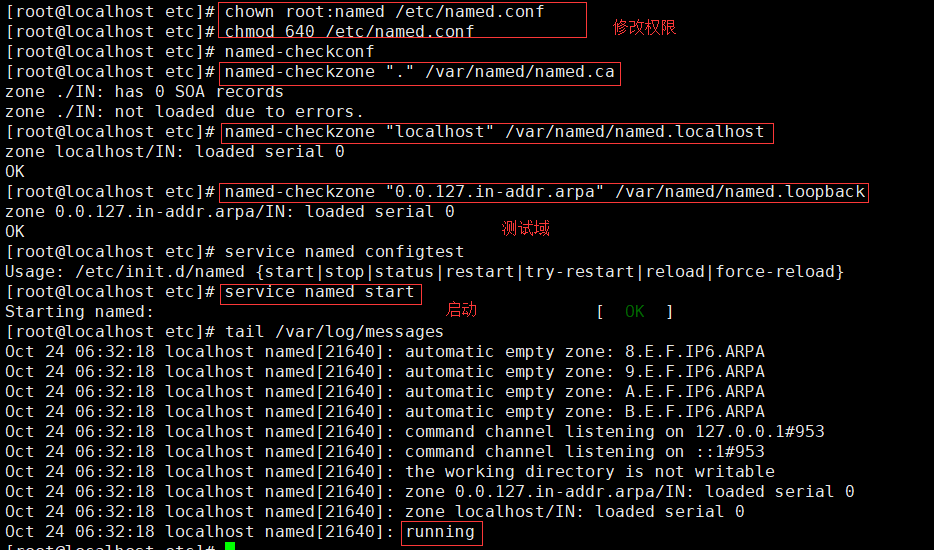
从区域：

file “区域数据文件”

masters{ master1\_ip; }

缓存DNS





不能让Selinux启动起来。

临时性关闭Selinux

命令： getenforce 查看状态

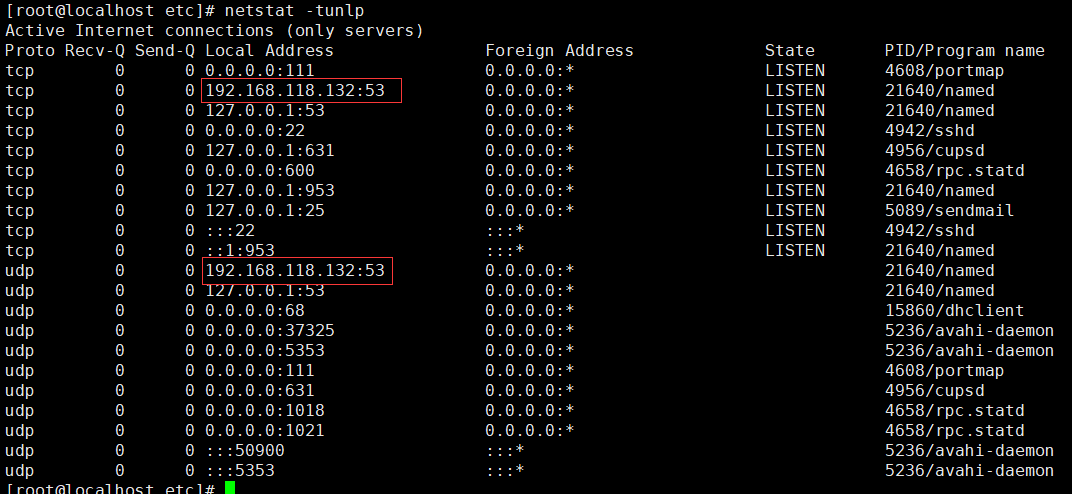
Enforcing 启动状态

setenforce 0 关闭

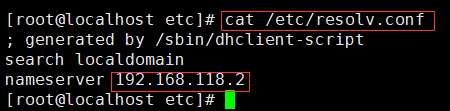
setenforce 1 开启

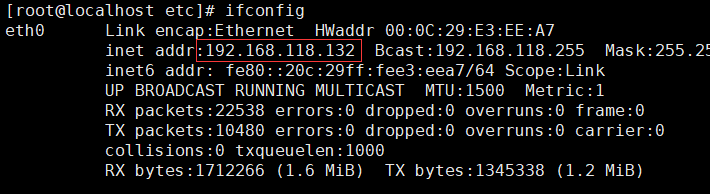
永久关闭：

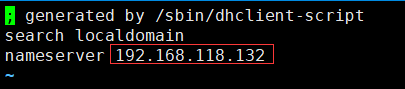
vi /etc/selinux/config 中的 selinux=disabled 或者 selinux =permissive



vi /etc/resolv.conf 将nameserver修改成本机地址

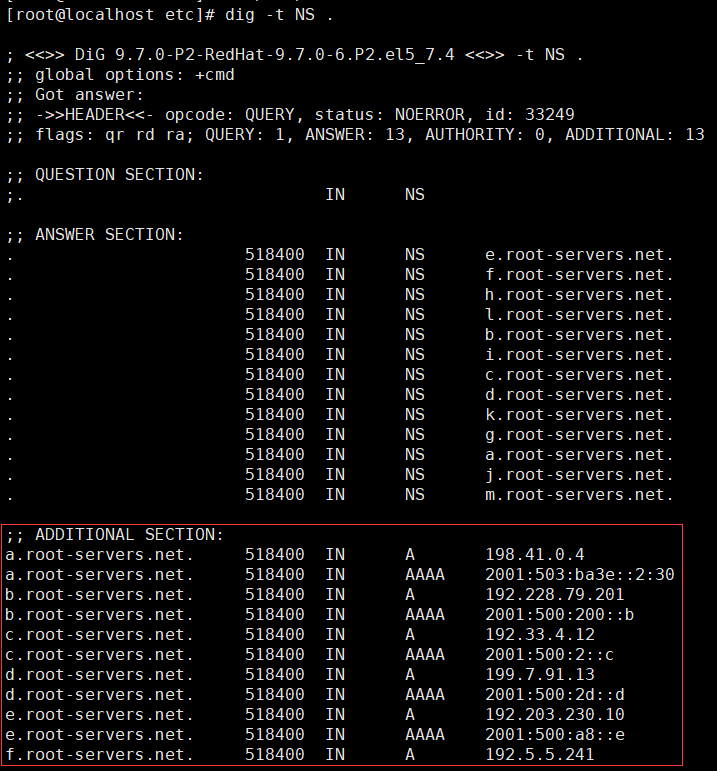


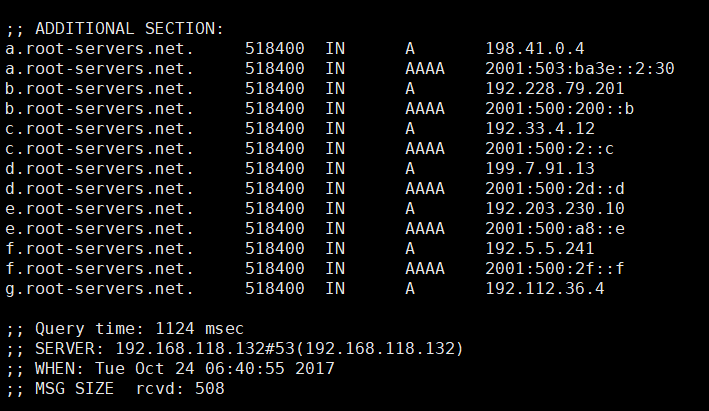




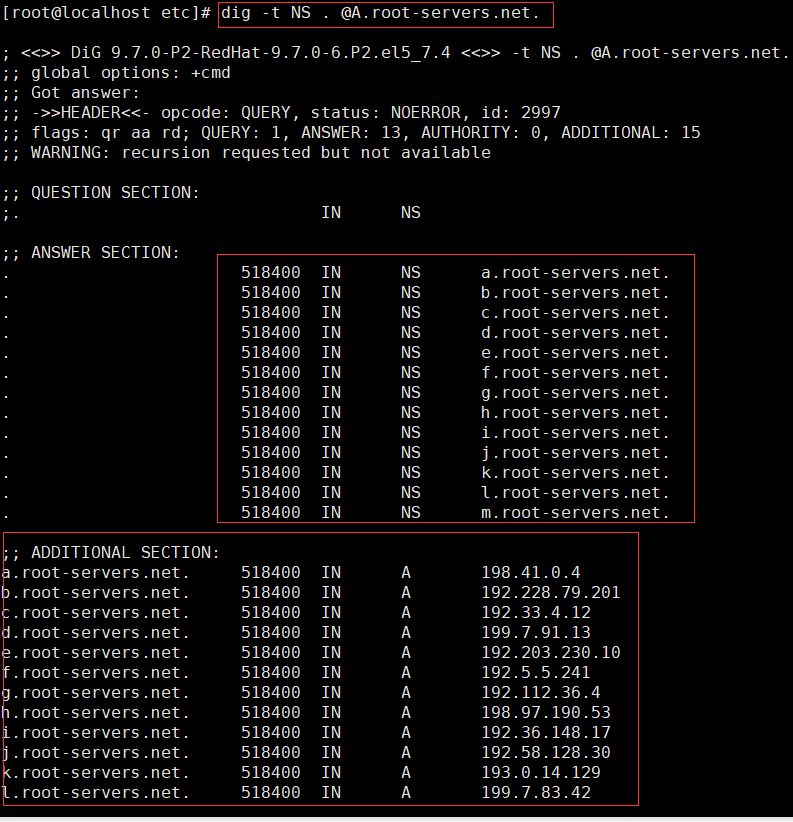
将reslov.conf的nameserver的地址修改成 192.168.118.132 本机地址

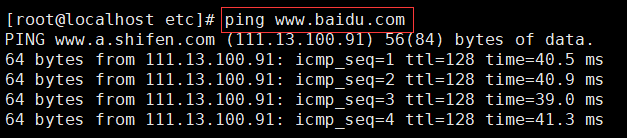
就能去解析地址了

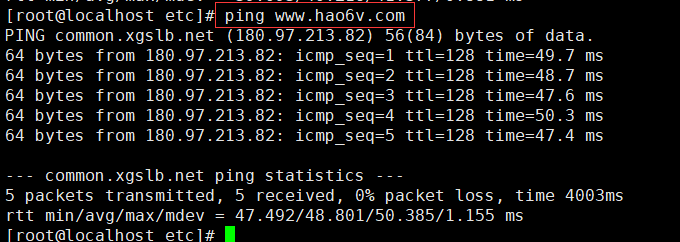




dig –t NS . @A.root-servers.net.

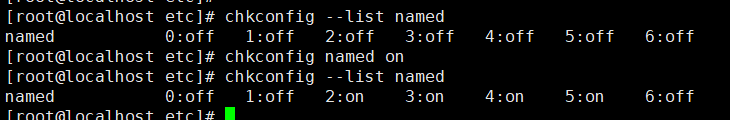




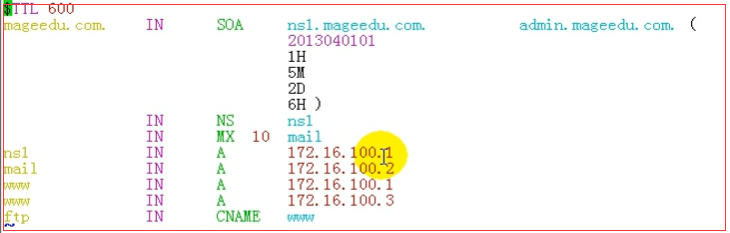


因此，这台主机就可以解析主机名了，就算他不知道也会去找根，通过迭代最终会解析出来的。一个DNS缓存服务器就配置好了，可以正常工作。

下次开机就可以启动起来了

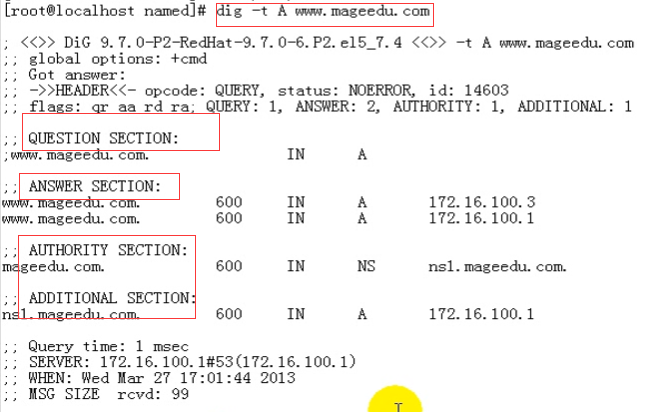


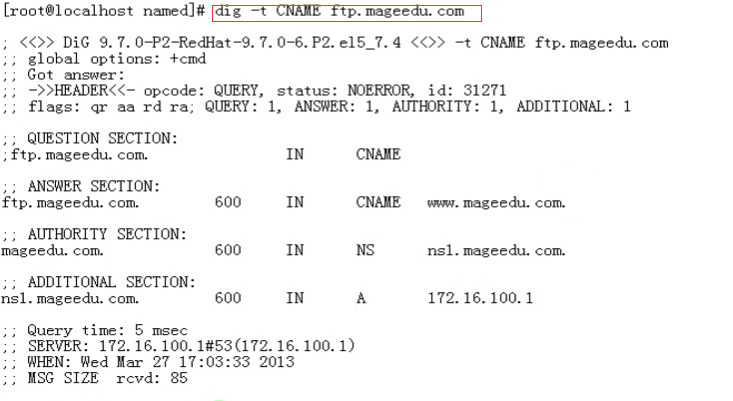


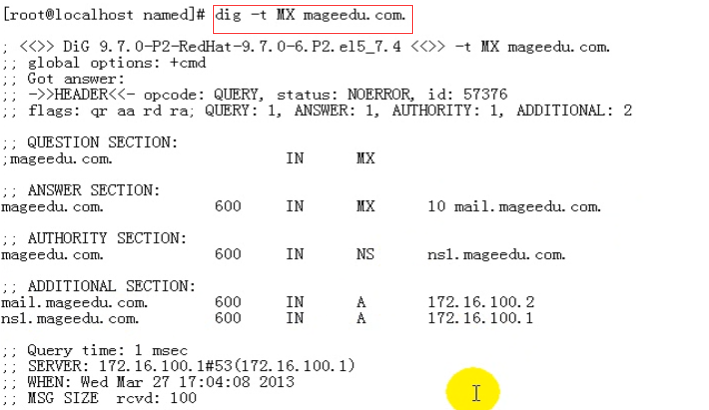


重启服务 service named restart

dig –t A [www.magedu.com](http://www.magedu.com) 查询

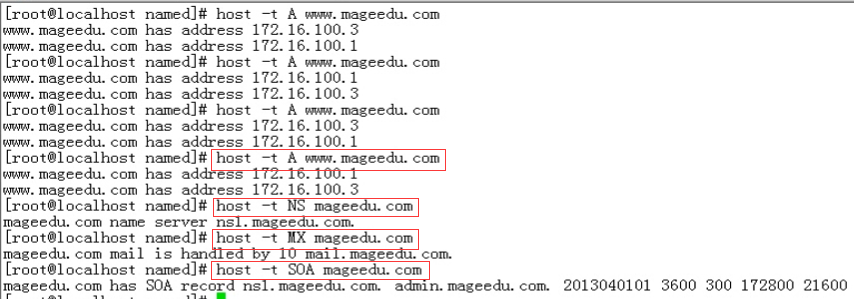






dig –x IP: 根据IP查FQDN

host –t A [www.baidu.com](http://www.baidu.com) 查询名称的解析结果



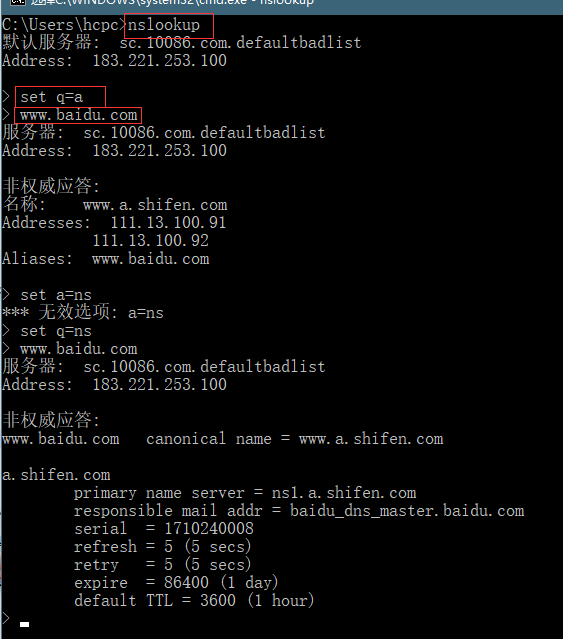
nslookup: 交互式

nslookup

server IP

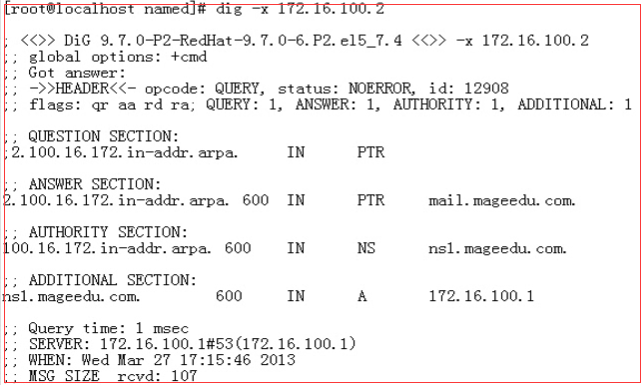
set q=rt 资源记录类型

name

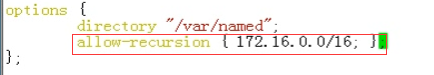








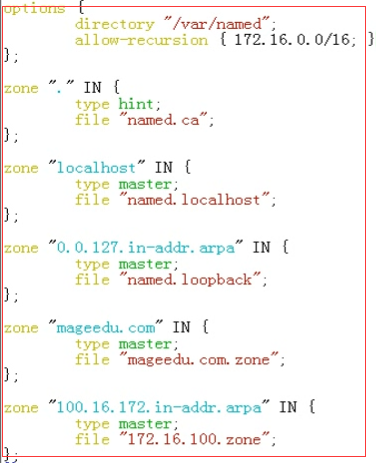
allow-recursion 允许递归的网段，一般是NS负责的内部才递归



递归查询

dig +recurse –t A [www.baidu.com](http://www.baidu.com) @172.16.100.1





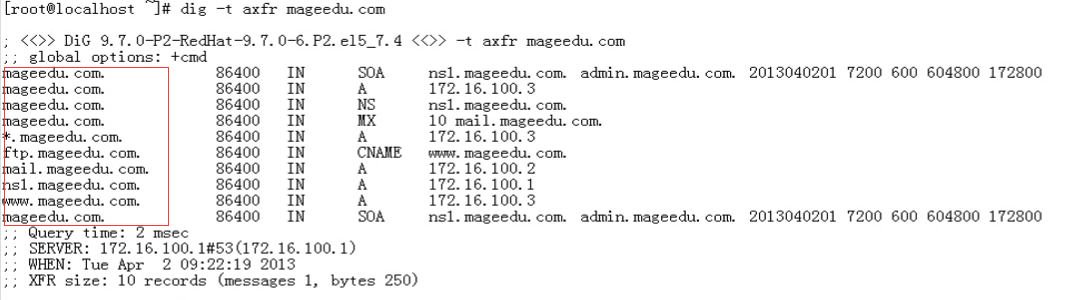
dig +recurse –t A [www.baidu.com](http://www.baidu.com) @127.0.0.1

发现连本机都递归不了，因为只为172递归了

axfr 完全区域传送 得到全部记录 只允许从服务器传送。

ixfr 增量区域传送

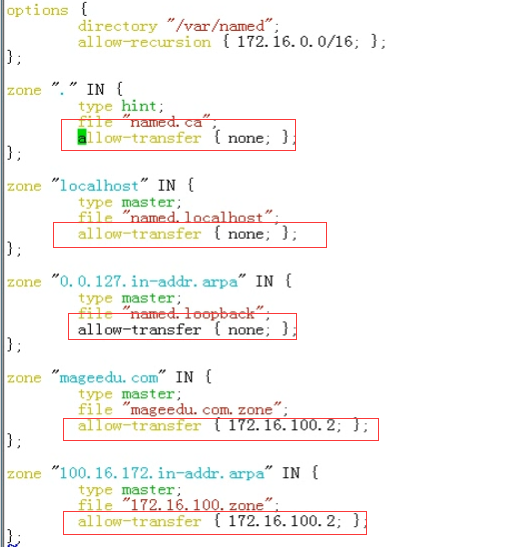
dig –t axfr magedu.com



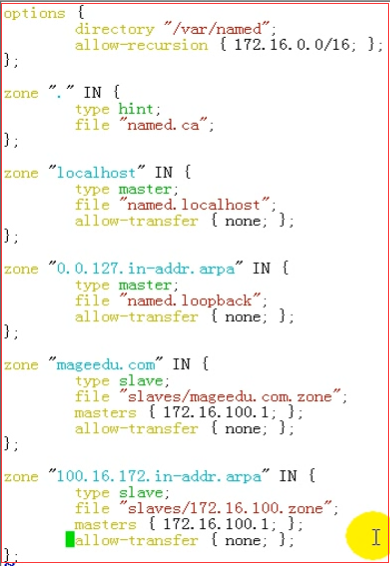
dig –t ixfr 2017040201 magedu.com 有主从结构

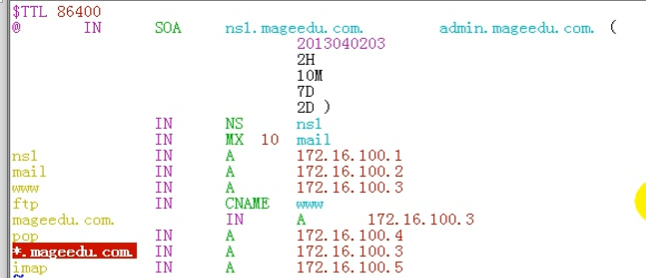


named.conf需要做如下配置：



从服务器：





rndc dns远程控制命令

rndc –h 查看帮助

rndc-confgen > /etc/rndc.conf

