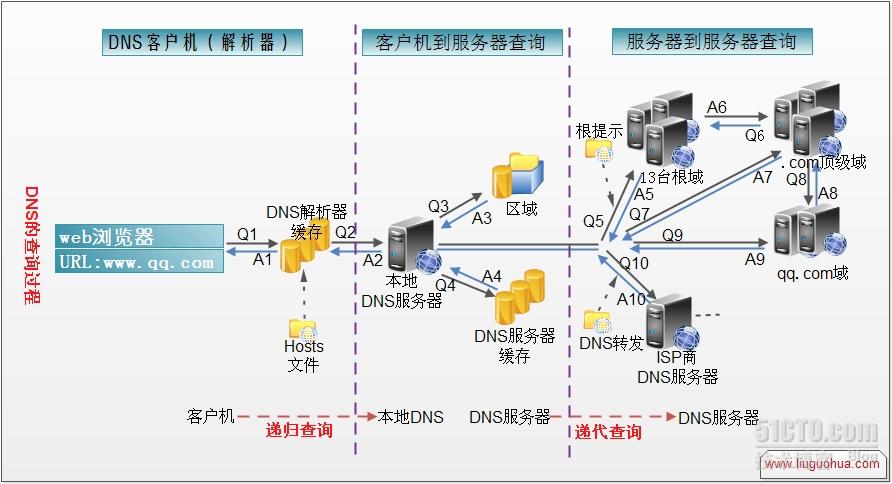
DNS服务器配置和管理

# DNS服务器概述



从客户端到本地DNS服务器是属于递归查询(一直往下查找)，而DNS服务器之间就是的交互查询就是迭代查询(客户机发送请求给dns1，dns1不能解析，则dns1把dns2的ip给客户机，客户机自动跳转到dns2，直到查询到为止)。

## 实现域名解析的方式

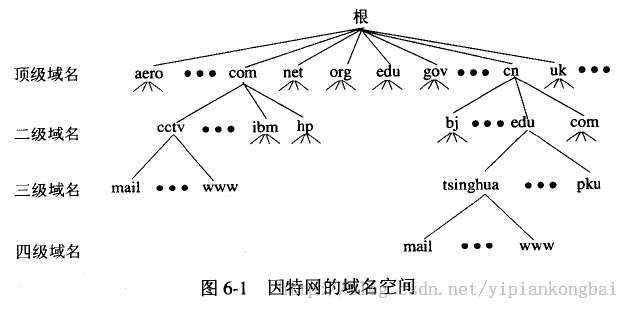
### 使用/etc/hosts文件

文件中每行是一个域名和一个ip对应的记录。更新困难，维护难。

### 域名系统DNS

域名系统的全称是Domain Name system,最常用的版本是bind。它是由域名解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。其中域名必须对应一个IP地址，一个域名可以有多个IP地址，而IP地址不一定有域名。域名系统采用类似目录树的等级结构。域名服务器为客户机/服务器模式中的服务器方，它主要有两种形式：主服务器和转发服务器。将域名映射为IP地址的过程就称为“域名解析”。

## DNS的组成



DNS规定，域名中的标号都有英文和数字组成，每一个标号不超过63个字符(为了记忆方便，一般不会超过12个字符)，也不区分大小写字母。标号中除连字符(-)外不能使用其他的标点符号。级别最低的域名写在最左边，而级别最高的字符写在最右边。由多个标号组成的完整域名总共不超过255个字符。DNS既不规定一个域名需要包含多少个下级域名，也不规定每一级域名代表什么意思。各级域名由其上一级的域名管理机构管理，而最高的顶级域名则由ICANN进行管理。用这种方法可使每一个域名在整个互联网范围内是唯一的，并且也容易设计出一种查找域名的机制。

## DNS服务器的类别

根域名服务器：所有根域名服务器都由美国政府授权的互联网域名与号码分配机构统一管理，在linux中使用“.”表示。

主域名服务器：是特定域中所有信息的授权来源，其他辅助DNS都从主域名服务器上获取信息，master表示。

辅助域名服务器：主域名服务器的备份，可充当主域名服务器的大部分功能，用slave表示。

专用缓存域名服务器：缓存从远程服务器上传递的域名查询结果。

转发域名服务器：本身不提供域名查询服务，它将要解析青葱发送到网外的Q其他DNS服务器上。

# DNS服务器的安装和启动

#第一步DNS的安装

yum -y install bind bind-chroot bind-utils

#DNS的启动

service named start/stop/restart/status

#第二步修改配置文件

vi /etc/named.conf

|  |
| --- |
| //  // named.conf  //  // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS  // server as a caching only nameserver (as a localhost DNS resolver only).  //  // See /usr/share/doc/bind\*/sample/ for example named configuration files.  //    options {  listen-on port 53 { any; }; //开启监听端口53，接受任意IP连接  listen-on-v6 port 53 { ::1; }; //支持IP V6  directory "/var/named"; //所有的正向反向区域文件都在这个目录下创建  dump-file "/var/named/data/cache\_dump.db";  statistics-file "/var/named/data/named\_stats.txt";  memstatistics-file "/var/named/data/named\_mem\_stats.txt";  allow-query { 0.0.0.0/0; }; //允许任意IP查询  recursion yes;    dnssec-enable yes;  dnssec-validation yes;  dnssec-lookaside auto;    /\* Path to ISC DLV key \*/  bindkeys-file "/etc/named.iscdlv.key";    managed-keys-directory "/var/named/dynamic";  };    logging {  channel default\_debug {  file "data/named.run";  severity dynamic;  };  };    zone "." IN {  type hint;  file "named.ca";  };    include "/etc/named.rfc1912.zones"; //主要配置文件  include "/etc/named.root.key"; |

#第三步修改/etc/named.rfc1912.zones文件，添加abc.com正向和反向区域

|  |
| --- |
| // abc.com的正向区域  zone "abc.com" IN {  type master;  file "abc.com";  allow-update { none; };  };  // abc.com的反向区域  zone "1.16.172.in-addr.arpa" IN {  type master;  file "172.16.1.arpa";  allow-update { none; };  }; |

#第四步创建正向和反向区域资源文件

在配置named.conf时，指明的资源文件目录是/var/named，故先进入该目录。 vi /var/named/abc.com

|  |
| --- |
| $TTL 1D  @ IN SOA abc.com. root.www.abc.com. (  0 ; serial  1D ; refresh  1H ; retry  1W ; expire  3H ) ; minimum  NS @  A 127.0.0.1  AAAA ::1  www IN A 10.20.28.10  ftp IN A 10.20.28.9 |

vi /var/named/com.abc

|  |
| --- |
| $TTL 1D  @ IN SOA abc.com. root.www.abc.com. (  0 ; serial  1D ; refresh  1H ; retry  1W ; expire  3H ) ; minimum  NS @  AAAA ::1  10 PTR www.abc.com.  9 PTR ftp.abc.com. |

#第五步启动DNS服务

service named start

# DNS客户端使用

## Linux客户端机器

#安装客户端

yum install bind-utils

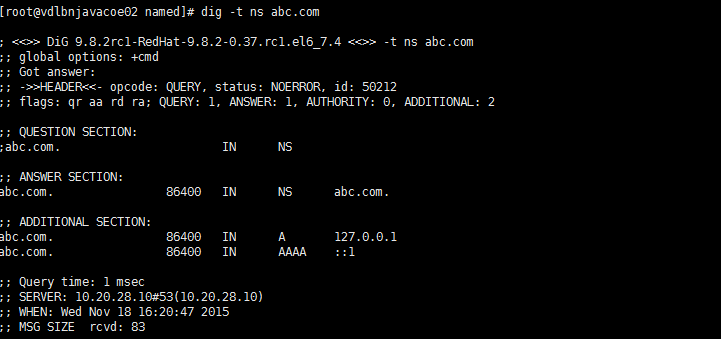
#修改DNS配置使用我们的DNS服务器

vi /etc/resolv.conf

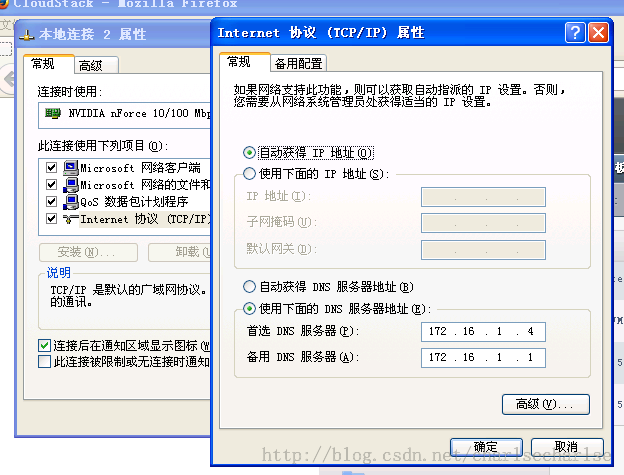
nameserver 10.20.28.10

#使用nslookup/dig用来正反向解析





## Windows客户端机器



# DNS配置文件解析

## DNS主配置文件named.conf

|  |
| --- |
| ###bind预设定了一些主机访问控制列表  ###any代表匹配任意的ip，localhost代表匹配本机所有的ip地址，none不匹配###任意ip地址  acl black{  Ip(黑名单ip)  }  acl white{  ip(白名单ip)  }  options {  ###监听的端口  listen-on port 53 { any; };  listen-on-v6 port 53 { any; };  ###定义区域配置文件的地址  directory "/var/named";  ###备份rndc dumpdb备份缓存资料后保存的文件路径和名称  dump-file "/var/named/data/cache\_dump.db";  ###运行rndc stats 后，统计信息的保存路径和名称  statistics-file "/var/named/data/named\_stats.txt";  memstatistics-file "/var/named/data/named\_mem\_stats.txt";  ###指定哪些主机可以查询服务器的权威解析数据  allow-query {any; };  ###拒绝哪些主机的查询请求  blackhole{black;};  ###允许递归查询  recursion yes;  dnssec-enable yes;  dnssec-validation yes;  dnssec-lookaside auto;  /\* Path to ISC DLV key \*/  bindkeys-file "/etc/named.iscdlv.key";  managed-keys-directory "/var/named/dynamic";  };  ###定义DNS域名解析区域  zone "." IN {  type hint;  file "named.ca";  };  ###定义正向区域  zone "abc.com" IN {  type master;  file "abc.com";  };  ###定义反向区域  zone "28.20.10.in-addr.arpa" IN {  type master;  file "com.abc";  }; |

## DNS的区域配置文件

DNS中named.conf是主配置文件，在文件中可以配置多个区域，每个区域都有自己对应的区域文件。包括正向 区域文件和反向区域文件，每一个zone(区域)中有很多资源。DNS工作过程是：

DNS服务器

Client

name.conf

域n

反向解析文件

正向解析文件

在name.conf的directory中指明的区域配置文件在/var/named中，但是这个目录的保存相应文件的链接符号，区域文件实际存放位置为/var/named/chroot/var/named目录下。

### 正向区域文件

|  |
| --- |
| $TTL 86400 //DNS生效时间, 其中第一行不能有注释  @ IN SOA www.abc.com. root.www.abc.com. (  20150915; // 系列号，其值通常设置为日期。  28800; //刷新时间  7200; //重试  604800; //过期  86400; //生存时间  )  IN NS www.abc.com.  IN MX 1 mail.abc.com.  www IN A 172.16.129.232  mail IN A 172.16.129.102  ftp IN A 172.16.129.32  www\_alias IN CNAME www.abc.com   1. SOA记录（授权记录开始）   [//@代表named.conf文件中zone](mailto://@代表named.conf文件中zone)语句定义的域名，此代表abc.com  //IN代表internet，DNS主机名用完全合格的域名系统FQDN  //以.结尾的表示绝对域名  域名 IN SOA DNS主机名 管理员邮件地址 (  20150915; // 系列号，其值通常设置为日期。  28800; //刷新时间  7200; //重试  604800; //过期  86400; //生存时间  )   1. NS记录（域名服务器Name Server）   用来指定该域名由那个服务器来进行解析。   1. MX记录（mail Exchange）   指定本区域的邮件服务器主机名。表示abc.com有一个邮件服务器，完全合格域名系统为mail.abc.com。优先级为1   1. A记录   指明域中主机域名与ip地址的对应关系。表示www.abc.com对应的ip是172.16.129.232 。其中www是相对的域名 。www后面没有“.”相当于：  [www.abc.com](http://www.abc.com).表示绝对域名，用.结尾。   1. CNAME记录   CNAME是别名记录，www1.abc.com等效于[www.abc.com](http://www.abc.com)  VI．AAAA记录  AAAA记录(AAAA record)是用来将域名解析到IPv6地址的DNS记录。 |

### 反向区域文件

|  |
| --- |
| $TTL 86400 //DNS生效时间  @ IN SOA www.abc.com. root.www.abc.com. (  20150915; // 系列号，其值通常设置为日期。  28800; //刷新时间  7200; //重试  604800; //过期  86400; //生存时间  )  IN NS [www.abc.com](http://www.abc.com).  232.129 IN PTR www.abc.com.  IN PTR www1.abc.com.  102.129 IN PTR mail.abc.com.  32.129 IN PTR [ftp.abc.com](ftp://ftp.abc.com).  //ip地址172.16.129.232对应的域名是[www.abc.com](http://www.abc.com)（.代表绝对路径） |

## 辅助DNS服务器的配置

辅助DNS服务器有两个用途：一是作为主DNS服务器的备份，第二是分担主DNS服务器的负载。当主服务器出现故障的时候，辅服务器立即承担解析任务。

辅助服务器从主DNS复制数据的过程叫做区域传输。

②DNS数据传递

辅助DNS服务器

主DNS服务器

1. 请求传输

客户机

|  |
| --- |
| zone "abc.com" IN {  type slave;  masters{主DNS的ip;}  file "abc.com";  };  zone "129.16.172.in-addr.arpa" IN {  type slave;  masters{主DNS的ip;}  file "com.abc";  }; |

# 区域委派与子域配置

|  |
| --- |
| 父域服务器添加：  #添加子域名服务器记录  子域 IN NS 子域的FQND(完全合格的域名系统)  子域名的FQDN IN A 子域名的ip  例如：  xy IN NS www.xy.abc.com  [www.xy](http://www.xy) IN A 172.16.129.82  子域服务器添加：   1. Options中添加forwarders子句，使子域不能转发的查询转发到父域。 2. 配置子域服务器   ###例如xy.abc.com  zone “子域名”IN{    } |