简单 CDN-----智能 DNS 的部署 view、运行和实现

http://alvin1.blog.51cto.com

简单 CDN 其实就是实现智能 DNS+缓存代理（Squid）+Web 后台主机的实现，智能的对 IP 地址进行解析，然后按地区的划分进行访问

下面来记录下智能 DNS 的部署和运行的一些步骤和配置文档，以记录自己的实验实现的效果：

一、智能 DNS 的部署和运行分为：收集 IP、部署 DNS 以及运行等几部分

（1）收集 IP 我们可以在网上找到一些比较齐全的 DNS 服务器 ip 段，或者进行购买

（2）DNS 服务器部署选择操作系统 Centos，DNS 软件选择 Bind9.4 以上的版本，9.4 以下版本不支持 view 功能

（3）产生从 DNS 同步所需要的 TSIG KEY，我们可以使用 dnssec-keygen -a hmac-md5 -b 128 -h HOST 视图名称（自行定义）生成

二、DNS 原理及安装安装

域名服务器解析原理及过程：

<1>当 tom 用户查询 www.fb.com 这台主机的相关记录，它首先去本地(/etc/hosts)查询有没有相关

的记录，有则返回结果，没有则去本地 DNS 服务器(ns.fb.com)发送请求。

<2>本地域名服务器(ns.fb.com)查询缓存发现没 tom 用户查询的相关记录，所以它去根服务器查询

www.fb.com 的相关记录，并得到一个推荐的 DNS 服务器的地址(.com)

<3>然后本地域名服务去 com 域名服务器查询(www.fb.com)的相关记录，并得到了关于 exampl.com 域服务器地址，

然后本地域名服务向 example.com 发送查询请求，example.com 域名服务器查询缓存没有相应的答案，则推荐到

www.fb.com 域名服务器去查询，对于查询域名信息来说，www.fb.com 的域名则是权威的，它在自己的管辖

内找到 www 这台主机，然后用 www 这台主机的地址回复本地域名服务器(ns.fb.com)。

<4>本地域名服务器(ns.fb.com)得到了关于 www.fb.com 的主机记录，并将记录到缓存区域，然后

发送给 sandy 用户。

<5>下次再有用户查询 www.fb.com 主机信息时，本地域名服务器直接从缓存中调用此记录即可。

DNS 服务器的分类:

主域名服务器(Primary Name Server)

主域名服务器是特定域所有信息的权威来源，主域名服务器是特定域所有信息的权威来源，它从域管理员构造本地文件中加载域信息，

该文件包含服务器具有管理权的部分域结果的最权威信息。主域名服务器需要配置一组完整的文件，即主机配置文件(named.conf),

正向区域文件、反向区域文件、高速缓存初始化文件(named.ca),回送文件(named.local) 辅助 DNS 服务器(Second Name Server)

辅助 DNS 服务器

用来从主域名服务器同步区域数据文件，作为磁盘文件保存在辅助域名服务器相对应的目录，辅助 DNS 服务器只需要配置主配置文件即可，

不需要配置区域数据文件。 唯高速缓存域名服务器(Cache-only Server)

唯高速缓存域名服务器不包含域名数据库文件，它每次将从域名服务器得到的查询结果返回给客户端，并在本地将以缓存，供下次查询使用。

DNS 层次结构中资源记录介绍：

[ttl]字段 TTL(time to live (存活时间)),默认字段以秒为单位指定时间长度，在指定的时间内，数据项可被缓存并且仍被认为是有效的。

TTL 必须位于该区域数据文件的第一行，来进行标识

class:class 指定网络类型：默认类型为 IN IN(指 Internet)、HS(Hesiod:本地使用的目录服务)、CH(供域名服务器内部用来标示自己)

type 类型 A(Address):记录 FQDN-IP 转换

MX(Mail eXchanger):记录邮件交换记录

CNAME(Canonical NAME):记录别名，允许将多个名字映射到一个主机，通常 CNAME 主要用于 WEB 和邮件服务器。

SOA:(Start Of Authority):一个授权区的开始。每个配置文件必须包含 SOA 记录，以标志服务器所管理的起始处。

PTR(domain name PonitTeR):记录 IP-FQDN HINFO(Host INFOrmation):记录一组描述主机的信息文件组成，

例如：一些硬件名称及操作系统名称等信息。

rdata: A：记录主机 IP 地址

HINFO：记录 Hardware 和 OS 相关记录

MX：记录提供收发电子邮件相关信息，一般包含两个部分(preference-value)

Bind 常用的资源记录语法：

1、SOA 资源记录 $TTL 86400 区域名称(Name) 记录类型(type) SOA 主域名服务器(FQDN) 管理员邮箱地址(mail) (

serial ##number 序列号,每次更改配置值是都要在原来的基础上加上 1，表示以更新。

refresh ##刷新时间(间隔)

retry ##重试时间(间隔)

expire ##过期时间(间隔) na ttl) ##否定答案缓存 TTL 值

时间单位：M（分钟）、H（小时）、D（天）、W（周），默认单位是秒

安装：

第一步：

1.wget ftp://ftp.isc.org/isc/bind9/9.8.1-P1/bind-9.8.1-P1.tar.gz

2.tar xzf bind-9.8.1-P1.tar.gz

3.cd bind-9.8.1-P1

4../configure --prefix=/usr/local/bind --enable-threads

5.make && make install

第二步：

创建 DNS 所需文件（ named.ca、localhost.zone、named.local)

（也可以选择 yum 安装方式安装，不过必须要选择版本高于 9.4 以上的才能支持 view 功能， yum install bind97 bind97-utils .....)

```
# /usr/local/named/bin/dig > named.ca(生成named.ca文件)
# vim localhost.zone
    $TTL    86400
    $ORIGIN localhost.
    @       1D  IN  SOA @ root (
                        42
                        3H
                        15M
                        1W
                        1D)
            1D  IN  NS  @
            1D  IN  A   127.0.0.1

# vim named.local
    $TTL    86400
    @   IN  SOA localhost.  root.localhost. (
                        1997022700
                        28800
                        14400
                        3600000
                        86400 )
            IN  NS  localhost.
        1 IN  PTR localhost.

# /usr/local/named/sbin/rndc-confgen >rndc.conf (生成rndc文件，里面自动生成rndc.l
```

第三步：创建 named.conf 主配置文件

```
options {    ##定义全局选项，在所有区域中均有效，如果区域中对某一项有定义，则使用区域中定义的，否则
好的
    directory "/usr/local/named/etc";       #指定区域配置文件所保存的路径
    version "9.6.0";    #显示版本
    allow-query-cache { any; };      #指定接受DNS查询请求缓存的客户端
    allow-query { any; };             #指定接受DNS查询请求的客户端
    pid-file "/var/run/named/named.pid";   #指定DNS运行的pid文件
    };
controls {
    inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};
    # controls语句限定了rndc和正在运行的named进程之间如何进行交互，系统管理员可以用rndc向
信号并控制它。
    rndc可以连接并控制启动和停止named进程、转储named状态、将named转入调试模式。rndc是一个
置不当或不正确，来自互联网上的用
    都可以连接并控制DNS服务，rndc用来于named通信的端口默认为953 （通过rndc-confgen命令生
named之间使用验证配置rndc，实现远程控制DNS服务）
logging {      #指定BIND服务的日志参数
    channel warning { file "/var/log/named/dns_warnings" versions 3 size 124
```

道，用于指定警告日志发送的目标，把警告的信息保存在指定目录下的文件
```
    severity warning;
        print-category yes;
        print-severity yes;
        print-time yes;
  };
```
#在 日志中主要有两个概念：通道（channel）和类别（category）。通道指定了应该向哪里发送日志数据：
是发送给 syslog，还是写在一个文件里，或是发送给 named 的标准错误输出，还是发送到位存储桶（bit buc
类别则规定了哪些数据需要记录

```
 channel general_dns { file "/var/log/named/dns_logs" versions 3 size 1240k;
```
道，用于指定访问日志发送的目标，把访问的信息日志保存在指定目录下的文件
```
    severity info;
```
#version 是指定允许同时存在多少个版本的该文件，比如指定 3 个版本（version 3），
```
    print-category yes;
```
会保存 query.log、query.log0、query.log1 和 query.log2。
```
    print-severity yes;
    print-time yes;
  };
  category default { warning; };
  category queries { general_dns; };
};
```
#在定义通道的语句中，severity 是指定记录消息的级别。在 bind 中主要有以下几个级别（按照严重性递减的顺
```
# critical、error、warning、notice、info、debug [ level ]、dynamic
```
#定义了某个级别后，系统会记录包括该级别以及比该级别更严重的级别的所有消息。比如定义级别为 error，
#则会记录 critical 和 error 两个级别 的信息。一般情况下，我们记录到 info 级别就可以了。print-tim
是否需要写入时间，
#print-severity 是设定在日志 中是否需要写入消息级别，print-category 是设定在日志中是否需要写入
```
// key config
include "china.key"; #/usr/local/named/sbin/dnssec-keygen -a hmac-md5 -b 12
```
china 生成的 key
```
include "hk.key";
include "rndc.key";
include "tw.key";
//add ip acl
include "ip.china";  # 把预先定义好的访问控制列表文件包含进来，里面都是分类的各个地区的 dns 域名
include "ip.hk";
include "TW.acl";
view "view_china" { # 定义一个视图，名称自定义
    match-clients { key chinakey; CHINA; };  # key 为 include "china.key"里面包
```
用 dnssec-keygen -a hmac-md5 -b 128 -n HOST 视图名称 生成
```
    allow-transfer { key chinakey; };
    server 172.28.10.12 { keys chinakey; };  # 从 DNS 服务器的 IP 地址

zone "." IN {
    type hint;
    file "named.ca"; #根服务器的区域文件
    file "named.ca"; #根服务器的区域文件
```

正向解析配置文件：

```
  # vim test.com.cn    （从 DNS 会自动同步这个文件，无需自己创建）
1 $TTL 60 #全局定义 TTL 值，存活时间
2 $ORIGIN test.com.
3 @   IN  SOA ns1.test.com.(主 DNS 服务器的 FQDN,需注册) root.test.com. (
4                   2013051915; Serial   #序列号，修改主 DNS 时要让从同步需要把这个
5 值改比从的大+1
6                   60 ;Refresh         # 多少秒刷新一次
7                   900 ;Retry           # 同步失败多久再重试一次
8                   3600000 ;Expire      # 过期时间
9                   3600 );Minimum
10 ns1 60 IN A    172.28.10.11
11 ns2 60 IN A    172.28.10.12
12 www             IN CNAME    ua1.asd.com.
13 ua1.asd.com     IN  A   110.110.110.110
```

第四步：创建从 DNS named.conf 主配置文件

```
options {   #定义全局配置
    directory "/usr/local/named/etc";  #指定区域配置文件所指定的路径
    version "9.6.0";
    allow-query-cache { any; };
    allow-query { any; };
    pid-file "/var/run/named/named.pid";
    };
controls {
    inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};
logging {
    channel warning { file "/var/log/named/dns_warnings" versions 3
size 1240k;
    severity warning;
        print-category yes;
        print-severity yes;
        print-time yes;
  };

  channel general_dns { file "/var/log/named/dns_logs" versions 3 size
1240k;
    severity info;
    print-category yes;
    print-severity yes;
    print-time yes;
  };
  category default { warning; };
  category queries { general_dns; };
};
// key config
include "china.key";
include "hk.key";
include "rndc.key";
include "tw.key";
//add ip acl
include "ip.china";
include "ip.hk";
include "TW.acl";
view "view_china" {
    match-clients { key chinakey; CHINA; };
    allow-transfer { key chinakey; };
    server 172.28.10.11 { keys chinakey; }; #主DNS服务器IP，与主DNS服务器
进行key的校队

zone "." IN {
    type hint;
    file "named.ca";
};
zone "localhost" IN {
```

第五步：检查配置文件是否有错误

/usr/local/named/sbin/named-checkconf /usr/local/named/etc/named.conf

调试命令: /usr/local/named/sbin/named -gc /usr/local/named/etc/named.conf (会输出日志，可以进行错误调试)

检查 zone 文件是否有错误： /usr/local/named/sbin/named-checkzone

第六步：查看日志、进程和端口，看是否成功启动

 # tail -f /var/log/message (查看日志是否有报错)

 # ps -ef|grep named (查看进程是否正常启动)

 # netstat -antp|grep named

tcp 0 0 10.146.70.199:53 0.0.0.0:* LISTEN 1539/named

tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN 1539/named

tcp 0 0 127.0.0.1:953 0.0.0.0:* LISTEN 1539/named

第 7 步:测试

由 于我们做的是 CDN，就是把某个地区的 ip 解析到哪个 ip 地址，进行区域的划分，本案例是划分为中国、香港、台湾，所以我们可以用 vpn 来拨号测试，我们 可以使用 vpn 拨号到香港、台湾、中国进行测试，看是否访问同一个域名时是否 ip 是不一样的，如果测试出来是我们设置的 IP 那说明我们的实验成功了

测试命令： dig +trace www.test.com (域名)

dig www.test.com

nslookup www.test.com