# 目的

* 熟悉linux环境以及CDN相关的软件，如apache、bind和squid
* 了解基本的CDN架构，加深对CDN原理的认识
* 了解bind的分区域加速
* 了解动态静态数据各自的设置
* 初步了解缓存规则的设置（cache的设置以及源的影响）

# 系统架构图



## 系统逻辑结构

逻辑上分成以下3个部分

1. 最终用户（包括最终用户与运营商提供的local dns）
2. CDN子系统（包括若干cache与内部dns、外部dns）
3. 源服务器系统（包括web server和客户dns）

## 实际测试物理结构

由于实验环境有限，图中的两个local dns由两台虚拟机完成（后面简称local dns1、local dns2）；cdn外部dns、客户dns和web server将采用一个虚拟机完成，后面简称wd（web & dns），而cdn内部dns和cache则是另外一台虚拟机，后面简称cid（cache & inner dns）

## 小任务

整个环境搭建完成之后，需要以上图为基础，画出<http://www.abc.com/a.jpg>的实际访问过程，主要是dns以及http的请求以及cache和web server的响应。并写出各个部件所起的作用

|  |  |
| --- | --- |
| 名称 | 具体作用 |
| Local DNS |  |
| 外部DNS |  |
| 内部DNS |  |
| 客户DNS |  |
| Cache |  |
| Web Server |  |

# 虚拟机基本安装与配置

## 安装vmware

略。

## 安装as 4 32位

略。

## 修改系统启动level

为避免窗口界面占用系统太多资源，需要修改文件/etc/inittab

id:5:initdefault:修改为

id:3:initdefault:

保存文件

## 关闭iptables，允许内网访问

命令：service iptables stop

修改/etc/rc.d/rc.local

在文件后面增加一行service iptables stop

保存，目的在于启动之后关闭iptables

## 修改网络设置

编辑文件/etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0

BOOTPROTO=static

IPADDR=192.168.30.XX

NETMASK=255.255.255.0

GATEWAY=192.168.30.52

HWADDR=00:0C:29:83:D9:AE

ONBOOT=yes

TYPE=Ethernet

保存文件

运行命令：service network restart

修改红色字体部分

建议启动之后，使用xshell登录，这样操作会方便些。

# Local dns1/2的配置

两台Local dns实现本地DNS服务器的功能。

## 安装必要的服务软件

需要安装**bind**，可以使用

rpm –qa|grep bind

as4默认安装会附带装上上述软件。

## 配置bind

修改/var/named/named.ca

只需保留以下三行即可

. 3600000 IN NS A.ROOT-SERVERS.NET.

A.ROOT-SERVERS.NET. 3600000 A **192.168.30.11**

;

修改红底IP，指定根解析DNS服务器。即为WD机器地址。

# wd的配置（web server+DNS）

## 安装必要的服务软件

需要安装**bind和apache**，可以使用

rpm –qa|grep bind

rpm –qa|grep httpd

as4默认安装会附带装上上述软件

其中bind用于搭建DNS服务、apache用于搭建web服务器。

## 配置

### Bind

#### 基本情况

* 服务允许相关
  + service named start/stop/restart/status
  + rndc reload(配置修改重新引导)
* 配置文件
  + named.conf：/etc/named.conf
  + zone相关：/var/named/

/var/named/chroot/var/named

* 配置文件检查
  + named-checkconf /etc/named.conf
  + named-checkzone zoneName zoneFile

#### 配置网站dns（负责[abc.com](http://www.abc.com)的解析）

##### 修改/etc/named.conf

增加以下部分

zone "abc.com" IN {

type master;

file "abc.com.zone";

allow-update { none ; };

};

##### 新增zone配置文件

增加/var/named/chroot/var/named/abc.com.zone

内容如下

$TTL 60

$ORIGIN abc.com.

@ IN SOA ns.abc.com. admin.abc.com. (

20090218 ; serial (d. adams)

3H ; refresh

15M ; retry

1W ; expiry

1D) ; minimum

@ IN NS ns.abc.com.

ns IN A 192.168.10.87

www IN CNAME www.abc.com.cdn.com.

mail IN CNAME www.abc.com.

@ IN MX 5 mail.abc.com.

红色部分IP地址需要修改成本机地址

设置链接

ln -s /var/named/chroot/var/named/abc.com.zone /var/named/abc.com.zone

运行命令：rndc reload 重新引导。

#### 配置不分区域的CDN dns（负责cdn.com的简单解析）

##### 修改/etc/named.conf

增加以下部分

zone "cdn.com" IN {

type master;

file "cdn.com.zone";

allow-update { none ; };

};

##### 新增zone配置文件

增加/var/named/chroot/var/named/cdn.com.zone

内容如下

$TTL 60

$ORIGIN cdn.com.

@ IN SOA ns.cdn.com. admin.cdn.com. (

20090219 ; serial (d. adams)

3H ; refresh

15M ; retry

1W ; expiry

1D) ; minimum

@ IN NS ns.cdn.com.

ns IN A 192.168.10.87

www.abc.com IN A 192.168.10.88

mail IN CNAME ns.cdn.com.

@ IN MX 5 mail.cdn.com.

ns的 A记录IP地址需要修改成本机地址

www.abc.com的 A记录要修改成cid地址(cache)

新增链接

ln -s /var/named/chroot/var/named/cdn.com.zone /var/named/cdn.com.zone

运行命令：rndc reload 重新引导。

#### 配置分区域的CDN dns（负责cdn.com的智能解析）

说明：4.2.1.3为简单的CDN解析，不分区域。而本节则配置分区域（按Local DNS）的CDN智能解析。主要是通过Bind自带的view功能来实现的。

本例中实现三个区域（Local DNS）不同解析结果的功能。

##### 修改/etc/named.conf

在controls {

inet 127.0.0.1 allow { localhost; } keys { rndckey; };

};

代码后，第一个zone定义前增加view匹配头。如下：

view "dx" {

match-clients { 192.168.30.13; }; //区配的IP，修改为Local dns1地址。

recursion no;

zone "." IN {

type hint;

file "named.ca";

};

zone "localdomain" IN {

type master;

file "localdomain.zone";

allow-update { none; };

};

zone "localhost" IN {

type master;

file "localhost.zone";

allow-update { none; };

};

.......

zone "abc.com" IN {

type master;

file "abc.com.zone";

allow-update { none ; };

};//网站DNS

zone "cdn.com" IN {

type master;

file "cdn.com.zone.dx";

allow-update { none ; };

}; //当匹配这个view时，查询cdn.com.zone.dx

……

}; //在最后一个zone定义后增加大括号

注意大括号的位置

同理，增加两个view区配，分别为命名为“wt”和“other”。如下：

view "wt" {

match-clients { 192.168.30.14; }; //区配的IP，修改为Local dns2地址。

recursion yes;

…..

zone "cdn.com" IN {

type master;

file "cdn.com.zone.dx";

allow-update { none ; };

};

….

}

view "other" {

match-clients { any; }; //不匹配前面view时则查询到此。

recursion yes;

…..

…..

zone "cdn.com" IN {

type master;

file "cdn.com.zone.other";

allow-update { none ; };

};

….

}

##### 新增zone配置文件

需要配置三个不同的cdn.com.zone.x文件来指定不同的解析。

1. 新增cdn.com.zone.dx文件

增加/var/named/chroot/var/named/cdn.com.zone.dx

内容如下

$TTL 60

$ORIGIN cdn.com.

@ IN SOA ns.cdn.com. admin.cdn.com. (

20090219 ; serial (d. adams)

3H ; refresh

15M ; retry

1W ; expiry

1D) ; minimum

@ IN NS ns.cdn.com.

ns IN A 192.168.10.87

www.abc.com IN A 192.168.10.88

mail IN CNAME ns.cdn.com.

@ IN MX 5 mail.cdn.com.

ns的 A记录IP地址需要修改成本机地址

www.abc.com的 A记录要修改成cid地址(cache)

新增链接

ln -s /var/named/chroot/var/named/cdn.com.zone /var/named/cdn.com.zone.dx

1. 新增cdn.com.zone.wt文件

增加/var/named/chroot/var/named/cdn.com.zone.wt

内容如下

$TTL 60

$ORIGIN cdn.com.

@ IN SOA ns.cdn.com. admin.cdn.com. (

20090219 ; serial (d. adams)

3H ; refresh

15M ; retry

1W ; expiry

1D) ; minimum

@ IN NS ns.cdn.com.

ns IN A 192.168.10.87

www.abc.com IN A 192.168.10.87

mail IN CNAME ns.cdn.com.

@ IN MX 5 mail.cdn.com.

ns的 A记录IP地址需要修改成本机地址

www.abc.com的 A记录要修改成wd地址(web)，即回源。

新增链接

ln -s /var/named/chroot/var/named/cdn.com.zone /var/named/cdn.com.zone.wt

1. 新增cdn.com.zone.other文件

增加/var/named/chroot/var/named/cdn.com.zone.other

内容如下

$TTL 60

$ORIGIN cdn.com.

@ IN SOA ns.cdn.com. admin.cdn.com. (

20090219 ; serial (d. adams)

3H ; refresh

15M ; retry

1W ; expiry

1D) ; minimum

@ IN NS ns.cdn.com.

ns IN A 192.168.10.87

www.abc.com IN A 192.168.10.87

mail IN CNAME ns.cdn.com.

@ IN MX 5 mail.cdn.com.

ns的 A记录IP地址需要修改成本机地址

www.abc.com的 A记录要修改成wd地址(web)，即回源。

新增链接

ln -s /var/named/chroot/var/named/cdn.com.zone /var/named/cdn.com.zone.other

运行命令：rndc reload 重新引导。

### 检查配置是否正确

named-checkconf /etc/named.conf

named-checkzone abc.com /var/named/abc.com.zone

named-checkzone cdn.com /var/named/cdn.com.zone

bind正常启动

dig @本机IP [www.abc.com](http://www.abc.com)

dig @本机IP [www.abc.com](http://www.abc.com).cdn.com

是否能出来正常结果

#### 设置开机启动

修改/etc/rc.d/rc.local

在文件后面增加一行service named start

保存退出

### Apache

使用Apache安装web服务器

#### 基本情况

服务运行相关：service httpd start/stop/restart/status

配置文件：/etc/httpd/conf/httpd.conf

日志文件：/var/log/httpd/access\_log

#### 新建访问目录

mkdir –p /var/www/abc

#### 新建virtual Host：[www.abc.com](http://www.abc.com)

修改配置文件/etc/httpd/conf/httpd.conf

//虚拟主机设置

Listen 80 //开启80端口侦听

ServerName IP:80 //输入本机IP

NameVirtualHost \*:80 //设置虚拟主机名，这里使用\*,匹配所有IP，也可以使用本机IP

<VirtualHost \*:80> //禁止直接IP访问，empty为空目录

ServerName 192.168.10.87

DocumentRoot /var/www/empty

</VirtualHost>

<VirtualHost \*:80> //我们的所要使用的域名，配置到先前创建的目录上

ServerName **www.abc.com**

DocumentRoot /var/www/abc

</VirtualHost>

#### 缓存时间设置参考

ExpiresActive On  
#启用过期header功能。  
ExpiresDefault A604800  
#缺省过期时间为“访问后的604800秒”  
ExpiresByType text/html A300  
#text/html类型文件的过期设置为“访问后的300秒”  
ExpiresByType text/css A259200  
#text/css类型文件的过期设置为“访问后的259200秒”

#### 创建静态文件

静态文件较为简单，可以在/var/www/abc/目录下，创建一些文本文件。或放入一些图片文件。

#### 创建动态文件

由于使用php等方式比较麻烦，这边使用一种简单方式替代，主要通过crontab来定时修改文件内容，以达到“动态”的效果，操作方式如下作为参考

1. 目标文件是/var/www/abc/time.txt
2. 创建脚本gettime.sh（注意chmod +x gettime.sh）,内容如下

#!/bin/bash

date > /var/www/abc/time.txt

1. 创建crontab

运行命令：crontab –e，新增如下语句，一分钟改变一次

\*/1 \* \* \* \* /var/www/abc/gettime.sh > /dev/null 2>&1

#### 设置开机启动

修改/etc/rc.d/rc.local

在文件后面增加一行service httpd start

保存退出

# cid的配置（cache+inner DNS）

## 安装必要的服务软件

需要安装**squid和bind**，可以使用

rpm –qa|grep bind

rpm –qa|grep squid

as4默认安装会附带装上上述软件

## 配置

### Bind

#### 基本情况

* 服务运行相关
  + service named start/stop/restart/status
  + rndc reload(配置修改重新引导)
* 配置文件
  + named.conf：/etc/named.conf
  + zone相关：/var/named/
    - * + /var/named/chroot/var/named
* 配置文件检查
  + named-checkconf /etc/named.conf
  + named-checkzone zoneName zoneFile

#### 配置内部DNS

##### 修改/etc/named.conf

在options里头增加一行，防止递归查询，只作内部使用，解析有限的域名

recursion no;

增加abc.com

zone "abc.com" IN {

type master;

file "abc.com.zone";

allow-update { none ; };

};

##### 新增zone配置文件

增加/var/named/chroot/var/named/abc.com.zone

内容如下

$TTL 60

$ORIGIN abc.com.

@ IN SOA ns.abc.com. admin.abc.com. (

20090218 ; serial (d. adams)

3H ; refresh

15M ; retry

1W ; expiry

1D) ; minimum

@ IN NS ns.abc.com.

ns IN A 192.168.10.88

www IN A 192.168.10.87

mail IN CNAME www.abc.com.

@ IN MX 5 mail.abc.com.

ns的 A记录IP地址需要修改成本机地址

www的 A记录要修改成wd地址，即源服务器地址

新增链接

ln -s /var/named/chroot/var/named/abc.com.zone /var/named/abc.com.zone

##### 检查配置是否正确

named-checkconf /etc/named.conf

named-checkzone abc.com /var/named/abc.com.zone

bind正常启动

dig @本机IP [www.abc.com](http://www.abc.com)

是否能出来正常结果

##### 配置resolv.conf

修改/etc/resolv.conf，确保squid使用内部dns

在最前面增加一行

nameserver 本机IP

保存

要使squid启用新的dns，上述修改完成之后，必须重启squid

##### 设置开机启动

修改/etc/rc.d/rc.local

在文件后面增加一行service named start

保存

确保bind先于squid启动

### Squid

#### 基本情况

服务运行相关：service squid start/stop/restart/status

配置文件：/etc/squid/squid.conf

访问日志：/var/log/squid/access.log

#### 配置成允许abc.com加速

增加以下内容到/etc/squid/squid.conf

http\_port 80

acl abc dstdomain .abc.com

http\_access allow abc

http\_access deny !abc //不允许非abc.com的域访问

visible\_hostname cache88 //squid机器名

httpd\_accel\_host virtual

httpd\_accel\_with\_proxy on

httpd\_accel\_uses\_host\_header on

acl txturl url\_regex -i ^http://www\.abc\.com/.\*\.txt$

no\_cache deny txturl

//该域名下txt类型的url不缓存

acl nocacheurl url\_regex -i ^http://www\.abc\.com/nocache.jpg$

no\_cache deny nocacheurl

//http://www.abc.com/nocache.jpg不缓存

refresh\_pattern -i ^http://www\.abc\.com/.\*\.jpg$ 2 100% 2 override-lastmod

//jpg缓存2分钟

acl purge method PURGE

http\_access allow purge

//允许purge

#### 设置开机启动

修改/etc/rc.d/rc.local

在文件后面增加一行service squid start

保存

# 测试结果

测试1：

* PC机设置dns为wd的IP（外部dns）
* nslookup [www.abc.com](http://www.abc.com)的结果，是否到正常的别名，然后再A记录到cid的IP
* 开启IE，启动httpwatch

测试2：

* wd机器，tail －f /var/log/httpd/access.log，准备观察输出
* cid机器，tail –f /var/log/squid/access.log，准备观察输出
* 访问<http://www.abc.com/a.jpg>，多次刷新或者访问，看看上面两个的输出是否不同

测试3：若配置分区域解析，则测试

* 通过两台locale dns，dig [www.abc.com](http://www.abc.com) 查看结果，是否返回不同的解析结果。

# 基本环境及要求

## 基本环境介绍

每台机器上有四个虚拟机器，基本配置与网络已经完成，四台机器描述如下

http+DNS

该机器装有apache以及bind，主要用做以下功能

源服务器：通过apache提供web服务，数据文件位于/var/www/abc底下，其中time.txt为动态文件，每分钟变化一次，其他为静态的图片，该webserver只提供[www.abc.com的访问。其他的域名或者IP](http://www.abc.com的访问。其他的域名或者IP)访问均拒绝。

网站DNS：将[www.abc.com](http://www.abc.com)别名到[www.abc.com.cdn.com](http://www.abc.com.cdn.com)

CDN DNS ：负责将[www.abc.com.cdn.com的解析](http://www.abc.com.cdn.com的解析) （包括分区域解析和不分区域解析）

Cache+innerDNS

该机器装有squid和bind，主要用作以下功能

Cache：作为缓存服务器，只为[www.abc.com](http://www.abc.com)提供加速服务

innerDNS：内部DNS，负责将[www.abc.com解析出源服务器IP](http://www.abc.com解析出源服务器IP)

两台localDNS

该机器装有bind，各配置1个IP，对应localDNS1和localDNS2。实现本地dns的功能。

## CDN基本环境搭建

* 配置web server，实现[www.abc.com](http://www.abc.com)的访问
* 配置cache，实现代理访问，只允许[www.abc.com](http://www.abc.com)的访问
* 配置DNS（内部DNS、网站DNS和CDN的DNS），实现通过域名进行[www.abc.com的CDN](http://www.abc.com的CDN)访问

## 区域加速与缓存规则测试

* 通过CDN DNS的设置，实现localDNS1的访问到达cache，localDNS2以及其他的访问到达源web的功能
* 源服务器不设置任何缓存过期，通过cache的设置实现以下目标
  + 动态数据不缓存直接回源，静态数据缓存一定时间
  + 静态数据设置不同的缓存时间，观察其情况的差异
* 源服务器设置一定的缓存策略，观察其对cache的影响