Tedu.cn
达内教育

构建 CDN 分发网络架构

达内·Linux 云计算学院

2016 年 3 月

目 录

一、问题

达内集团为企业网站注册了域名 www.tarena.com，部署了 2 台 Nginx 网站服务器。为了提高此站点服务不同地区用户时的响应速度，达内集团向蓝讯公司购买了 CDN 缓存服务。根据缓存分发需要，达内集团向域名注册商新网申请更改解析记录，以 CNAME 别名的方式转交给蓝讯的 DNS 服务器处理。而蓝讯公司负责识别 Web 用户的来源地址，并通过最近的 CDN 缓存节点向用户分发网页内容。

为了提高 Web 站点的访问速度，要求实现以下目标：

- 通过本地 cache 缓存，提高用户访问 Web 的速度及稳定性
- 消除地域及运营商之间的网络互连影响，客户端永远选择离自己最近的服务器获取资源
- 减轻后端源站点 Web 服务器的负载压力
- 有效预防和降低 DDOS 攻击

二、方案

根据需求中描述的网络结构，可以采用 Squid 反向代理、DNS 智能解析相结合的方式来实现 CDN 内容分发网络，如图-1 所示。

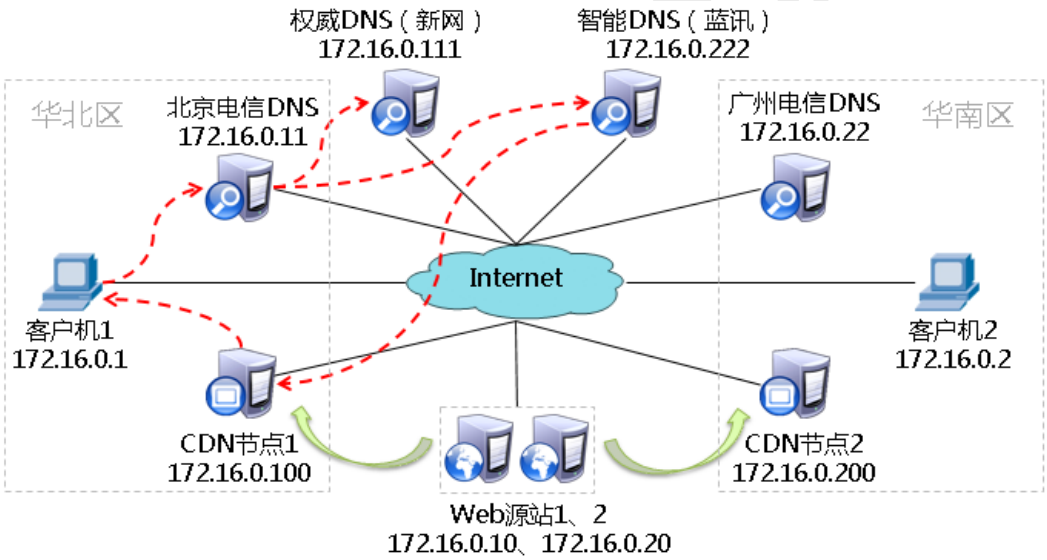

图-1

其中涉及到 10 台服务器：

- DNS 服务器-域名注册商（新网）：172.16.0.111/24，dns111.xinnet.com
- DNS 服务器-CDN 服务商（蓝讯）：172.16.0.222/24，dns222.lxcdn.net
- DNS 服务器-地区电信服务商（北京）：172.16.0.11/24，bjdns
- DNS 服务器-地区电信服务商（广州）：172.16.0.22/24，gzdns
- 反向代理服务器 1--北京 CDN 节点（蓝讯）：172.16.0.100/24，squid100.lxcdn.net
- 反向代理服务器 2--深圳 CDN 节点（蓝讯）：172.16.0.200/24，squid200.lxcdn.net
- Web 源服务器 1--达内集团：172.16.0.10/24，web10
- Web 源服务器 2--达内集团：172.16.0.20/24，web20
- 测试客户机 1--北京地区：172.16.0.1/24，pc01
- 测试客户机 2--广州地区：172.16.0.2/24，pc02

为了降低模拟实现的复杂度，本次案例中可以将这 10 个角色分配到 4 台 RHEL6 虚拟机上来实现，每

个虚拟机分别承担多个角色，如表-1 所示。

表一1 模拟 CDN 架构的虚拟机及角色

虚拟机编号	承担角色	主机名	IP 地址/掩码
host1	客户机 1 北京电信 DNS	pc01 bjdns	172.16.0.1/24 172.16.0.11/24
host2	客户机 2 广州电信 DNS	pc02 gzdns	172.16.0.2/24 172.16.0.22/24
host3	Web 源站 1 CDN 缓存节点 1 新网 DNS	web10 squid100.lxcdn.net dns111.xinnet.com	172.16.0.10/24 172.16.0.100/24 172.16.0.111/24
host4	Web 源站 2 CDN 缓存节点 2 蓝讯 DNS	web20 squid200.lxcdn.net dns222.xinnet.com	172.16.0.20/24 172.16.0.200/24 172.16.0.222/24

完成此架构后，当客户机首次解析域名 www.tarena.com 时，大致过程是：客户机-->本地区 DNS-->新网 DNS-->CDN 服务商的 DNS。解析结果是由 CDN 服务商提供的离用户最近的 CDN 缓存节点的 IP 地址。

最终测试结果应该是：

- ✧ 当从 pc01 访问 http://www.tarena.com 时，由 squid100.lxcdn.net 响应
- ✧ 当从 pc02 访问 http://www.tarena.com 时，由 squid200.lxcdn.net 响应

三、步骤

实现此案例需要按照如下步骤进行。

步骤一：为 4 台虚拟机配好地址、yum 仓库

1. 配置第一台虚拟机 host1

1）设置好主机名，方便区分

```
[root@host1 ~]# vim /etc/sysconfig/network          //固定配置
NETWORKING=yes
HOSTNAME=host1
[root@host1 ~]# hostname host1                      //临时、即时配置
[root@host1 ~]# hostname
host1
```

2）设置 IP 地址、掩码

如果是克隆的虚拟机，建议清空对应 udev 配置文件，以恢复正常的 eth0 网卡名：

```
[root@host1 ~]# > /etc/udev/rules.d/70-persistent-net.rules
[root@host1 ~]# reboot
```

网卡名无误后，修改接口配置文件：

```
[root@host1 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
IPADDR1=172.16.0.1                                  //第一个 IP 地址
PREFIX1=24                                          //第一个 IP 地址的子网掩码
IPADDR2=172.16.0.11                                 //第二个 IP 地址
PREFIX2=24                                          //第二个 IP 地址的子网掩码
DEFROUTE=yes
```

```
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth0"
```

重新启动 network 服务：

```
[root@host1 ~]# service network restart
正在关闭接口 eth0：                                        [确定]
关闭环回接口：                                             [确定]
弹出环回接口：                                             [确定]
弹出界面 eth0： Determining if ip address 172.16.0.1 is already in use for device eth0...
Determining if ip address 172.16.0.11 is already in use for device eth0...
                                                           [确定]
```

确认配好的 IP 地址信息：

```
[root@host1 ~]# ip add list eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:2c:7d:6a brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.1/24 brd 172.16.0.255 scope global eth0
    inet 172.16.0.11/24 brd 172.16.0.255 scope global secondary eth0
    .. ..
```

3）设置好/etc/hosts 映射文件，方便服务器互访

```
[root@host1 ~]# vim /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
172.16.0.1      pc01
172.16.0.2      pc02
172.16.0.11     bjdns
172.16.0.22     gzdns
172.16.0.111    dns111  dns111.xinnet.com
172.16.0.222    dns222  dns222.lxcdn.net
172.16.0.100    squid100  squid100.lxcdn.net
172.16.0.200    squid200  squid200.lxcdn.net
172.16.0.10     web10
172.16.0.20     web20
```

4）设置要使用的 DNS 服务器

各客户机 pc01、pc02 使用本地区 ISP 服务商的开放式 DNS 服务器，其他主机可以使用 CDN 服务商提供的 DNS 服务器。

```
[root@host1 ~]# vim /etc/resolv.conf
search tarena.com
nameserver 172.16.0.11
```

5）配好 yum 仓库

将虚拟机的光盘设置为 RHEL6 的光盘镜像，比如 E:\IsoFiles\RHEL_DVD\rhel-server-6.5-x86_64-dvd.iso，然后建立 yum 客户端文件。

```
[root@host1 ~]# vim /etc/yum.repos.d/rhel-source.repo
[rhel-packages]
name=Red Hat Enterprise Linux $releasever - $basearch - Source
baseurl=file:///misc/cd
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[root@host1 ~]# yum repolist
rhel-packages      | 3.9 kB     00:00 ...
repo id              repo name                                          status
rhel-packages        Red Hat Enterprise Linux 6Server - x86_64 - Source     3,690
repolist: 3,690
```

2. 配置第二台虚拟机 host2

1）设置好主机名，方便区分

```
[root@host2 ~]# vim /etc/sysconfig/network          //固定配置
NETWORKING=yes
HOSTNAME=host2
```

2）设置 IP 地址、掩码

如果是克隆的虚拟机，建议清空对应 udev 配置文件，以恢复正常的 eth0 网卡名：

```
[root@host2 ~]# > /etc/udev/rules.d/70-persistent-net.rules
[root@host2 ~]# reboot
```

网卡名无误后，修改接口配置文件：

```
[root@host2 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
.. ..
IPADDR1=172.16.0.2
PREFIX1=24
IPADDR2=172.16.0.22
REFIX2=24
.. ..
```

重新启动 network 服务，确认配好的 IP 地址信息：

```
[root@host2 ~]# service network restart
.. ..
[root@host2 ~]# ip add list eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:85:46:fb brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.2/24 brd 172.16.0.255 scope global eth0
    inet 172.16.0.22/24 brd 172.16.0.255 scope global secondary eth0
    .. ..
```

3）设置好/etc/hosts 映射文件，方便服务器互访

—— 与 host1 的配置操作相同。

4）设置要使用的 DNS 服务器

各客户机 pc01、pc02 使用本地区 ISP 服务商的开放式 DNS 服务器，其他主机可以使用 CDN 服务商提供的 DNS 服务器。

```
[root@host2 ~]# vim /etc/resolv.conf
search tarena.com
nameserver 172.16.0.22
```

5）配好 yum 仓库

—— 与 host1 的配置操作相同。

3. 配置第三台虚拟机 host3

1）设置好主机名，方便区分

```
[root@host3 ~]# vim /etc/sysconfig/network          //固定配置
NETWORKING=yes
HOSTNAME=host3
```

2）设置 IP 地址、掩码

如果是克隆的虚拟机，建议清空对应 udev 配置文件，以恢复正常的 eth0 网卡名：

```
[root@host3 ~]# > /etc/udev/rules.d/70-persistent-net.rules
[root@host3 ~]# reboot
```

网卡名无误后，修改接口配置文件：

```
[root@host3 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
.. ..
IPADDR1=172.16.0.10
PREFIX1=24
IPADDR2=172.16.0.100
PREFIX2=24
IPADDR3=172.16.0.111
PREFIX3=24
.. ..
```

重新启动 network 服务，确认配好的 IP 地址信息：

```
[root@host3 ~]# service network restart
.. ..
[root@host3 ~]# ip add list eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:84:d4:96 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.10/24 brd 172.16.0.255 scope global eth0
    inet 172.16.0.100/24 brd 172.16.0.255 scope global secondary eth0
    inet 172.16.0.111/24 brd 172.16.0.255 scope global secondary eth0
    .. ..
```

3）设置好/etc/hosts 映射文件，方便服务器互访

—— 与 host1 的配置操作相同。

4）设置要使用的 DNS 服务器

各客户机 pc01、pc02 使用本地区 ISP 服务商的开放式 DNS 服务器，其他主机可以使用 CDN 服务商提供的 DNS 服务器。

```
[root@host3 ~]# vim /etc/resolv.conf
search tarena.com
nameserver 172.16.0.222
```

5）配好 yum 仓库

—— 与 host1 的配置操作相同。

4. 配置第四台虚拟机 host4

1）设置好主机名，方便区分

```
[root@host4 ~]# vim /etc/sysconfig/network          //固定配置
NETWORKING=yes
HOSTNAME=host4
```

2）设置 IP 地址、掩码

如果是克隆的虚拟机，建议清空对应 udev 配置文件，以恢复正常的 eth0 网卡名：

```
[root@host4 ~]# > /etc/udev/rules.d/70-persistent-net.rules
[root@host4 ~]# reboot
```

网卡名无误后，修改接口配置文件：

```
[root@host4 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
.. ..
IPADDR1=172.16.0.20
PREFIX1=24
IPADDR2=172.16.0.200
PREFIX2=24
IPADDR3=172.16.0.222
PREFIX3=24
.. ..
```

重新启动 network 服务，确认配好的 IP 地址信息：

```
[root@host4 ~]# service network restart
.. ..
[root@host4 ~]# ip add list eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:5f:0b:ef brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.20/24 brd 172.16.0.255 scope global eth0
    inet 172.16.0.200/24 brd 172.16.0.255 scope global secondary eth0
    inet 172.16.0.222/24 brd 172.16.0.255 scope global secondary eth0
    .. ..
```

3）设置好/etc/hosts 映射文件，方便服务器互访

—— 与 host1 的配置操作相同。

4）设置要使用的 DNS 服务器

各客户机 pc01、pc02 使用本地区 ISP 服务商的开放式 DNS 服务器，其他主机可以使用 CDN 服务商提供的 DNS 服务器。

```
[root@host4 ~]# vim /etc/resolv.conf
search tarena.com
nameserver 172.16.0.222
```

5）配好 yum 仓库

—— 与 host1 的配置操作相同。

步骤二：搭建两个 Web 源站点

1. 部署 web10 站点（host3）

1）添加用户、安装依赖包

```
[root@host3 ~]# useradd nginx
[root@host3 ~]# yum -y install pcre-devel openssl-devel
```

2）编译安装 nginx 包

```
[root@host3 ~]# cd /var/ftp/pub/
[root@host3 pub]# tar zxf nginx-1.8.0.tar.gz -C /usr/src/
[root@host3 pub]# cd /usr/src/nginx-1.8.0/
[root@host3 nginx-1.8.0]# ./configure --prefix=/usr/local/nginx --user=nginx --group=nginx --
with-http_stub_status_module --with-http_ssl_module
[root@host3 nginx-1.8.0]# make
[root@host3 nginx-1.8.0]# make install
```

3）调整 nginx 服务配置

因为在本练习中 host3 上后面还要跑 Squid 反向代理，为了避免 80 端口冲突，需要把监听的 IP 地址也限制一下。

```
[root@host3 ~]# vim /usr/local/nginx/conf/nginx.conf
.. ..
http {
    .. ..
    server {
        listen       172.16.0.10:80;                //指定监听地址、端口
        server_name  www.tarena.com;                //指定网站域名
        .. ..
    }
}
```

简化一下测试首页：

```
[root@host3 ~]# vim /usr/local/nginx/html/index.html
Tarena IT Group.
```

4）启动 nginx 服务、确保可访问

```
[root@host3 ~]# /usr/local/nginx/sbin/nginx
[root@host3 ~]# netstat -anpt | grep :80
tcp        0      0 172.16.0.20:80    0.0.0.0:*     LISTEN      8950/nginx

[root@host3 ~]# elinks -dump http://172.16.0.10/   //访问站点 web10 成功
   Tarena IT Group.
```

2. 部署 web20 站点（host4）

1）添加用户、安装依赖包

```
[root@host4 ~]# useradd nginx
[root@host4 ~]# yum -y install pcre-devel openssl-devel
```

2）编译安装 nginx 包

这里可以跳过源码编译过程，直接拷贝 web10 已经装好的 nginx 目录：

```
[root@host4 ~]# scp -r 172.16.0.10:/usr/local/nginx  /usr/local/
root@172.16.0.10's password:      //验证对方的密码
.. ..
[root@host4 ~]# ls /usr/local/nginx/           //确认拷贝结果
client_body_temp  fastcgi_temp  logs        sbin       uwsgi_temp
conf              html          proxy_temp  scgi_temp
```

3）调整 nginx 服务配置

因为在本练习中 host4 上后面也要跑 Squid 反向代理，为了避免 80 端口冲突，需要把监听的 IP 地址也限制一下。

```
[root@host4 ~]# vim /usr/local/nginx/conf/nginx.conf
.. ..
http {
    .. ..
    server {
        listen       172.16.0.20:80;                //指定监听地址、端口
        server_name  www.tarena.com;                //指定网站域名
        .. ..
    }
}
```

简化一下测试首页：

```
[root@host4 ~]# vim /usr/local/nginx/html/index.html
Tarena IT Group.
```

4）启动 nginx 服务、确保可访问

```
[root@host4 ~]# /usr/local/nginx/sbin/nginx
[root@host4 ~]# netstat -anpt | grep :80
tcp        0      0 172.16.0.20:80    0.0.0.0:*     LISTEN      3942/nginx

[root@host4 ~]# elinks -dump http://172.16.0.20/   //访问站点 web20 成功
   Tarena IT Group.
```

步骤三：搭建 2 个 CDN 缓存节点

1. 部署北京 CDN 节点——squid100.lxcdn.net 服务器（host3）

1）安装 squid 代理软件包

```
[root@host3 ~]# yum -y install squid
```

2）修改 squid 服务配置

```
[root@host3 ~]# vim /etc/squid/squid.conf
.. ..
http_access allow all                       //将默认策略由 deny 改为 allow
visible_hostname squid100.lxcdn.net
http_port 172.16.0.100:80 vhost             //限定 IP 地址，避免与本机 nginx 冲突
cache_peer  172.16.0.10 parent 80 0 originserver
cache_peer  172.16.0.20 parent 80 0 originserver
.. ..
```

3）启动 squid 服务、确认监听结果

```
[root@host3 ~]# service squid restart
.. ..
[root@host3 ~]# netstat -anpt | grep :80
tcp        0      0 172.16.0.100:80       0.0.0.0:*      LISTEN    11313/(squid)
tcp        0      0 172.16.0.10:80        0.0.0.0:*      LISTEN    11136/nginx
```

4）测试反向代理 squid100，确保可用

从客户机 pc01 访问反向代理的 80 端口，可获得目标网页内容：

```
[root@host1 ~]# elinks -dump http://172.16.0.100/
   Tarena IT Group.
```

检查 squid 服务的访问日志，其中记录了 pc01 通过代理访问上游 Web 站点的事件：

```
[root@host3 ~]# tail -1 /var/log/squid/access.log
1437051206.927       29    172.16.0.1    TCP_MISS/200    387    GET    http://172.16.0.100/    -
FIRST_UP_PARENT/172.16.0.10 text/html
```

2. 部署广州 CDN 节点——squid200.lxcdn.net 服务器（host4）

1）安装 squid 代理软件包

```
[root@host4 ~]# yum -y install squid
```

2）修改 squid 服务配置

```
[root@host4 ~]# vim /etc/squid/squid.conf
.. ..
http_access allow all                       //将默认策略由 deny 改为 allow
visible_hostname squid200.lxcdn.net
http_port 172.16.0.200:80 vhost             //限定 IP 地址，避免与本机 nginx 冲突
cache_peer  172.16.0.20 parent 80 0 originserver
cache_peer  172.16.0.10 parent 80 0 originserver
.. ..
```

3）启动 squid 服务、确认监听结果

```
[root@host4 ~]# service squid restart
.. ..
[root@host4 ~]# netstat -anpt | grep :80
tcp        0      0 172.16.0.200:80       0.0.0.0:*      LISTEN    8996/(squid)
tcp        0      0 172.16.0.20:80        0.0.0.0:*      LISTEN    7960/nginx
```

4）测试反向代理 squid200，确保可用

从客户机 pc02 访问反向代理的 80 端口，可获得目标网页内容：

```
[root@host2 ~]# elinks -dump http://172.16.0.200/
   Tarena IT Group.
```

检查 squid 服务的访问日志，其中记录了 pc01 通过代理访问上游 Web 站点的事件：

```
[root@host4 ~]# tail -1 /var/log/squid/access.log
1437051663.406              2   172.16.0.2   TCP_MISS/200   384   GET   http://172.16.0.200/   -
FIRST_UP_PARENT/172.16.0.10 text/html
```

步骤四：构建 DNS 域名分发体系

1. 部署北京 DNS——bjdns 服务器（host1）

1）安装 bind、bind-chroot 软件包

```
[root@host1 ~]# yum -y install bind bind-chroot
```

2）建立/etc/named.conf 配置文件

备份默认配置，建立新配置，将此服务器作为缓存 DNS，无需区域数据文件。为简化域名层级，此例中的转发器可以指向新网 DNS 服务器。

```
[root@host1 ~]# mv /etc/named.conf /etc/named.conf.origin       //备份旧配置
[root@host1 ~]# vim /etc/named.conf                             //建立新配置
options {
        directory "/var/named";
        forwarders { 172.16.0.111; };
};
```

3）启动 named 服务

首次启动 named 服务时，可通过 rndc-confgen 工具生成密钥，以加快启动速度。

```
[root@host1 ~]# rndc-confgen -r /dev/urandom -a    //后续重启可跳过此操作
wrote key file "/etc/rndc.key"
[root@host1 ~]# service named restart              //确保启动服务
[root@host1 ~]# chkconfig named on                 //设为开机自运行
```

2. 部署广州 DNS——gzdns 服务器（host2）

—— 与 bjdns 的配置操作相同。

3. 部署新网 DNS——dns111.xinnet.com 服务器（host3），模拟权威 DNS

1）安装 bind、bind-chroot 软件包

```
[root@host3 ~]# yum -y install bind bind-chroot
```

2）建立/etc/named.conf 配置文件

添加二级域 xinnet.com、tarena.com，添加一级域 net，全局不允许递归。

```
[root@host3 ~]# mv /etc/named.conf /etc/named.conf.origin       //备份旧配置
[root@host3 ~]# vim /etc/named.conf                             //建立新配置
options {
        listen-on port 53 { 172.16.0.111; };
        directory "/var/named";
        recursion no;
};
zone "xinnet.com" {
        type master;
        file "xinnet.com.zone";
};
zone "net" IN {
        type master;
        file "net.zone";
};
zone "tarena.com"{
        type master;
        file "tarena.com.zone";
};
```

3）为上述区域建立解析记录文件

在 xinnet.com 域的解析记录文件中，设置好到新网 DNS 服务器的 A 记录：

```
[root@host3 ~]# vim /var/named/xinnet.com.zone
$TTL 1D
@ IN SOA @ admin.xinnet.com. (
        2015071501
        1D
        1H
        1W
        3H )
@       NS      dns111.xinnet.com.
dns111  A       172.16.0.111
```

在 net 域的解析记录文件中，设置好子域授权，将 lxcdn.net 域授权给蓝讯 DNS 服务器进行解析：

```
[root@host3 ~]# vim /var/named/net.zone
$TTL 1D
@ IN SOA @ admin.lxcdn.net. (
        2015071501
        1D
        1H
        1W
        3H )
@               NS      dns111.xinnet.com.
lxcdn.net.      NS      dns222.lxcdn.net.               ;指定子域及 DNS 服务器
dns222.lxcdn.net.       A       172.16.0.222            ;指定子 DNS 服务器地址
```

在 tarena.com 域的解析记录文件中，将客户公司的网站域名 www.tarena.com 设置为 CNAME 别名，实际站点为 www.tarena.com.lxcdn.net，从而转到蓝讯 DNS 处理：

```
[root@host3 ~]# vim /var/named/tarena.com.zone
$TTL 1D
@ IN SOA @ admin.xinnet.com. (
        2015071501
        1D
        1H
        1W
        3H )
@       NS      dns111.xinnet.com.
www     CNAME   www.tarena.com.lxcdn.net.
```

4）启动 named 服务

首次启动 named 服务时，可通过 rndc-confgen 工具生成密钥，以加快启动速度。

```
[root@host3 ~]# rndc-confgen -r /dev/urandom -a     //后续重启可跳过此操作
wrote key file "/etc/rndc.key"
[root@host3 ~]# service named restart               //确保启动服务
[root@host3 ~]# chkconfig named on                  //设为开机自运行
```

4. 部署蓝讯 DNS——dns222.lxcdn.net 服务器（host4），实现智能分离解析

1）安装 bind、bind-chroot 软件包

```
[root@host4 ~]# yum -y install bind bind-chroot
```

2）建立/etc/named.conf 配置文件

将北京、广州地区的客户机地址分为两类（每一类包括直接查询的客户机、也包括转发查询的其他 DNS 服务器），通过 view 视图实现智能分离解析。

```
[root@host4 ~]# mv /etc/named.conf /etc/named.conf.origin       //备份旧配置
[root@host4 ~]# vim /etc/named.conf                             //建立新配置
options {
```

```
        listen-on port 53 { 172.16.0.222; };
        directory "/var/named";
        forwarders { 172.16.0.111; };
};
acl client1 {
        172.16.0.1; 172.16.0.11;            #//第一类地址，北京地区的 DNS 及客户机
};
acl client2 {
        172.16.0.2; 172.16.0.22;            #//第二类地址，广州周边的 DNS 及客户机
};
view "zone1" {
        match-clients { client1; };         #//服务第一类地址
        zone "tarena.com.lxcdn.net" IN {    #//特定企业的 CDN 服务区域
                type master;
                file "tarena.com.lxcdn.net.zone1";
        };
        zone "lxcdn.net" IN {                    #//定义二级权威域 lxcdn.net
               type master;
               file "lxcdn.net.zone";
        };
};
view "zone2" {
        match-clients { client2; any; };    #//服务第二类地址及其他任意客户机
        zone "tarena.com.lxcdn.net" IN {
                type master;
                file "tarena.com.lxcdn.net.zone2";
        };
        zone "lxcdn.net" IN {
                type master;
                file "lxcdn.net.zone";
        };
};
```

3）为上述区域建立解析记录文件

在 lxcdn.net 域的解析记录文件中，添加到蓝讯 DNS 服务器及两个 CDN 缓存节点服务器的 A 记录：

```
[root@host4 ~]# vim /var/named/lxcdn.net.zone
$TTL 1D
@ IN SOA @ admin.lxcdn.net. (
        2015071501
        1D
        1H
        1W
        3H )
@       NS      dns222.lxcdn.net.
        A       172.16.0.222
dns222  A       172.16.0.222
squid100        A       172.16.0.100
squid200        A       172.16.0.200
```

针对 CDN 缓存服务域 tarena.com.lxcdn.net 建立两份解析记录文件，分别对应两类客户机地址。在视图 1 中，将 www.tarena.com 解析为 CDN 节点 1 即 squid100.lxcdn.net 的 IP 地址；而在视图 2 中，将其解析为 CDN 节点 2 即 squid200.lxcdn.net 的 IP 地址：

```
[root@host4 ~]# vim /var/named/tarena.com.lxcdn.net.zone1
$TTL 1D
@ IN SOA @ admin.lxcdn.net. (
        2015071501
        1D
        1H
        1W
        3H )
@       NS      dns222.lxcdn.net.
www     A       172.16.0.100                    //对应北京的 CDN 节点 1
```

```
[root@host4 ~]# vim /var/named/tarena.com.lxcdn.net.zone2
$TTL 1D
@ IN SOA @ admin.lxcdn.net. (
        2015071501
        1D
        1H
        1W
        3H )
@       NS      dns222.lxcdn.net.
www     A       172.16.0.200                    //对应广州的 CDN 节点 2
```

4）启动 named 服务

首次启动 named 服务时，可通过 rndc-confgen 工具生成密钥，以加快启动速度。

```
[root@host4 ~]# rndc-confgen -r /dev/urandom -a     //后续重启可跳过此操作
wrote key file "/etc/rndc.key"
[root@host4 ~]# service named restart               //确保启动服务
[root@host4 ~]# chkconfig named on                  //设为开机自运行
```

5. 域名解析测试

1）确保新网 DNS（dns111）可用

```
[root@host1 ~]# nslookup dns111.xinnet.com 172.16.0.111             //查权威域
Server:         172.16.0.111
Address:        172.16.0.111#53

Name:   dns111.xinnet.com
Address: 172.16.0.111
```

2）确保蓝讯 DNS（dns222）可用

```
[root@host1 ~]# nslookup squid100.lxcdn.net 172.16.0.222            //查权威域
Server:         172.16.0.222
Address:        172.16.0.222#53

Name:   squid100.lxcdn.net
Address: 172.16.0.100
```

3）确保蓝讯 DNS（dns222）的分离解析可用

从客户机 pc01（第一类地址）查询：

```
[root@host1 ~]# nslookup www.tarena.com.lxcdn.net 172.16.0.222      //查 CDN 子域
Server:         172.16.0.222
Address:        172.16.0.222#53

Name:   www.tarena.com.lxcdn.net
Address: 172.16.0.100
```

从客户机 pc02（第二类地址）查询：

```
[root@host2 ~]# nslookup www.tarena.com.lxcdn.net 172.16.0.222
Server:         172.16.0.222
Address:        172.16.0.222#53

Name:   www.tarena.com.lxcdn.net
Address: 172.16.0.200
```

4）确保地区 DNS（bjdns、gzdns）可用

向服务器 bjdns 查询：

```
[root@host1 ~]# nslookup dns111.xinnet.com 172.16.0.11
Server:         172.16.0.11
```

```
Address:       172.16.0.11#53

Non-authoritative answer:
Name:   dns111.xinnet.com
Address: 172.16.0.111
```

向服务器 gzdns 查询：

```
[root@host1 ~]# nslookup dns111.xinnet.com 172.16.0.22
Server:        172.16.0.22
Address:       172.16.0.22#53

Non-authoritative answer:
Name:   dns111.xinnet.com
Address: 172.16.0.111
```

5）确保子域授权（dns111-->dns222）可用

测试子域授权时，客户端正常应是其他 DNS 服务器，因此用 nslookup 会看不出结果，改用 dig 工具即可。因为新网 DNS 不提供递归，所以查子域 FQDN 的时候，如果授权可用，则会告知可用的子域名称、子域 DNS 的域名及 IP 地址信息。

```
[root@host1 ~]# dig @172.16.0.111 squid100.lxcdn.net
.. ..
;; QUESTION SECTION:
;squid100.lxcdn.net.           IN      A

;; AUTHORITY SECTION:
lxcdn.net.              86400   IN      NS      dns222.lxcdn.net.

;; ADDITIONAL SECTION:
dns222.lxcdn.net.       86400   IN      A       172.16.0.222
.. ..
```

6）确保“客户机-->地区 DNS-->权威 DNS-->CDN 的 DNS”的分离解析可用

在客户机 pc01 上：

```
[root@host1 ~]# cat /etc/resolv.conf
search tarena.com
nameserver 172.16.0.11

[root@host1 ~]# nslookup www.tarena.com
Server:        172.16.0.11
Address:       172.16.0.11#53

Non-authoritative answer:
www.tarena.com  canonical name = www.tarena.com.lxcdn.net.
Name:   www.tarena.com.lxcdn.net
Address: 172.16.0.100
```

在客户机 pc02 上：

```
[root@host2 ~]# cat /etc/resolv.conf
search tarena.com
nameserver 172.16.0.22

[root@host2 ~]# nslookup www.tarena.com
Server:        172.16.0.22
Address:       172.16.0.22#53

Non-authoritative answer:
www.tarena.com  canonical name = www.tarena.com.lxcdn.net.
Name:   www.tarena.com.lxcdn.net
Address: 172.16.0.200
```

步骤五：客户机访问测试

1. 从北京客户机 pc01 上访问 www.tarena.com

1）访问目标网站

```
[root@host1 ~]# elinks -dump http://www.tarena.com/
   Tarena IT Group.
```

2）查看 squid100 的代理日志

```
[root@host3 ~]# tail -1 /var/log/squid/access.log
1437055965.965              6  172.16.0.1  TCP_MISS/200  384  GET  http://www.tarena.com/  -
FIRST_UP_PARENT/172.16.0.10  text/html
```

2. 从广州客户机 pc02 上访问 www.tarena.com

1）访问目标网站

```
[root@host2 ~]# elinks -dump http://www.tarena.com/
   Tarena IT Group.
```

2）查看 squid100 的代理日志

```
[root@host4 ~]# tail -1 /var/log/squid/access.log
1437056077.838              1  172.16.0.2  TCP_MISS/200  384  GET  http://www.tarena.com/  -
FIRST_UP_PARENT/172.16.0.10 text/html
```