实训第二天

1. DNS安装与环境

ps：跟陈总的文档完全不同

```
#安装bind
yum install bind bind-utils -y
```

关于环境：

不先处理一些环境问题，后面处理起来，人要疯

环境：必要两台centos7，复数其它任意网段主机（可有可无）

首先是固定自己的ip（是啊，教室到宿舍，在到教室，网络一断，又得重新配）

```
#主NDS服务器
vim /etc/sysconfig/network-scripts/ifcfg-eno16777736
TYPE=Ethernet
BOOTPROTO=static    #改为static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777736
UUID=118af5e5-92de-42b0-a1c6-619c8d9d6c81   #可删
ONBOOT=yes      #改为yes
IPADDR=192.168.241.129    #本地ip
PREFIX=24
GATEWAY=192.168.241.2
DNS1=192.168.241.129      #本地ip
```

```
#容灾所使用的服务器（由于是主服务器克隆而来，网卡一摸一样）
vim /etc/sysconfig/network-scripts/ifcfg-eno16777736
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777736
```

```
IPADDR=192.168.241.134      #自己的ip，注意区分
PREFIX=24
GATEWAY=192.168.241.2
ONBOOT=yes
DNS1=192.168.241.134       #自己的ip，注意区分
```

```
#记得更新网络配置
service network restart
```

其次是关闭防火墙和SELinux

```
#控制变量，人人有责
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]# setenforce 0
```

2. DNS的配置和部署

```
#尝试启动DNS
[root@localhost ~]# systemctl status named
named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled)
   Active: inactive (dead)
```

没有配置文件，无法启动很正常

主配置文件修改

```
[root@localhost ~]# vim /etc/named.conf

options {
        listen-on port 53 { any; };          #ip地址修改成any
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        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";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { any; };         #一样改成any
```

配置正向解析与反向解析

后面的容灾也需要以下配置

```
vim /etc/named.rfc1912.zones

#在末尾增加以下

#正向解析
zone "qiye.com" IN {
        type master;
        file "qiye.com.zone";                          #正向解析文件路径
        allow-transfer { 192.168.241.134; };       #允许转移数据（容灾）
```

```
        allow-update { 192.168.241.134; };        #允许这个ip更新数据（容灾）
};

#反向解析
zone "241.168.192.in-addr.arpa" IN {
        type master;
        file "qiye.com.local";                          #反向解析文件路径
        allow-transfer { 192.168.241.134; };      #允许转移数据（容灾）
        allow-update { 192.168.241.134; };       #允许这个ip更新数据（容灾）
};
```

```
#cd到正向解析和反向解析文件所在的文件夹
cd /var/named/
```

```
#创建正向解析文件和反向解析文件：
[root@localhost named]# ls
data  dynamic  named.ca  named.empty  named.localhost  named.loopback  slaves
#将模板复制过来，即：
[root@localhost named]# cp -p named.localhost qiye.com.zone
[root@localhost named]# cp -p named.loopback qiye.com.local
ps：假如他们的所属组是root，那么请将他们所属组改成named（我这里不用）
[root@localhost named]# ll
total 24      #所有者 所属组
drwxrwx---. 2 named named    6 Aug 31 07:53 data
drwxrwx---. 2 named named    6 Aug 31 07:53 dynamic
-rw-r-----. 1 root  named 2253 Apr  5  2018 named.ca
-rw-r-----. 1 root  named  152 Dec 15  2009 named.empty
-rw-r-----. 1 root  named  152 Jun 21  2007 named.localhost
-rw-r-----. 1 root  named  168 Dec 15  2009 named.loopback
-rw-r-----. 1 root  named  168 Dec 15  2009 qiye.com.local
-rw-r-----. 1 root  named  152 Jun 21  2007 qiye.com.zone
drwxrwx---. 2 named named    6 Aug 31 07:53 slaves
#修改所属组语句：
[root@localhost named]# chown -R named:named qiye.com.local
[root@localhost named]# chown -R named:named qiye.com.zone
```

对两个文件进行DNS域名解析编辑

```
[root@localhost named]# vim qiye.com.zone
[root@localhost named]# vim qiye.com.local
```

```
#正向解析文件
$TTL 1D
@       IN SOA  qiye.com. rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
        NS      ns.qiye.com.
ns      IN A    192.168.241.129
www     IN A    192.168.241.129
```

```
email   IN A    192.168.241.129
c2      IN A    192.168.241.134
```

```
#反向解析文件
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
        PTR     localhost.
        NS      ns.qiye.com.

ns      A       192.168.241.129
129     PTR     www.qiye.com.
129     PTR     email.qiye.com.
134     PTR     c2.qiye.com.
```

修改DNS配置

```
[root@localhost named]# vim /etc/resolv.conf
nameserver 192.168.241.129
nameserver 114.114.114.114  #可有可无，防止断网
```

再次启动DNS服务

```
#没任何返回，则正常运行
[root@localhost named]# systemctl start named
#53端口检查状态
[root@localhost named]#  lsof -i :53
COMMAND   PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
named   43300 named   21u  IPv4  91166      0t0  TCP localhost:domain (LISTEN)
named   43300 named   22u  IPv4  91168      0t0  TCP www.qiye.com:domain
(LISTEN)
named   43300 named   23u  IPv6  91170      0t0  TCP localhost:domain (LISTEN)
named   43300 named   26u  IPv4  91426      0t0  TCP 192.168.241.147:domain
(LISTEN)
named   43300 named  512u  IPv4  91164      0t0  UDP localhost:domain
named   43300 named  513u  IPv4  91167      0t0  UDP www.qiye.com:domain
named   43300 named  514u  IPv6  91169      0t0  UDP localhost:domain
named   43300 named  515u  IPv4  91425      0t0  UDP 192.168.241.147:domain
```

3.实现DNS域名解析

```
#成功正反向解析域名和ip，ya*da*ze!
[root@localhost named]# nslookup 192.168.241.129
129.241.168.192.in-addr.arpa    name = email.qiye.com.
129.241.168.192.in-addr.arpa    name = www.qiye.com.

[root@localhost named]# nslookup www.qiye.com
```

```
Server:     192.168.241.129
Address:    192.168.241.129#53

Name:   www.qiye.com
Address: 192.168.241.129

[root@localhost named]# nslookup c2.qiye.com
Server:     192.168.241.129
Address:    192.168.241.129#53

Name:   c2.qiye.com
Address: 192.168.241.134
```

截图为证!

4.容灾处理

在克隆的centos7上的操作（192.168.241.134）

无非是对配置文件的处理

```
#与前面一样
vim /etc/named.conf

options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        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";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { any; };
```

```
#注意！！！！！这里变了
[root@localhost ~]# vim /etc/named.rfc1912.zones

zone "qiye.com" IN {
        type slave;    #改成slave
        file "slave/qiye.com.zone";    #路径可以变
        masters { 192.168.241.129; };  #主DNS服务器的ip地址
```

```
};

zone "241.168.192.in-addr.arpa" IN {
        type slave;    #改成slave
        file "slave/qiye.com.local";   #路径变了
        masters { 192.168.241.129; };  #主DNS服务器ip地址
};
```

```
#DNS修改
[root@localhost ~]# vim /etc/resolv.conf

#domain localdomain
search localdomain
#nameserver 192.168.241.2
nameserver 192.168.241.129    #主DNS服务器ip地址
```

```
#查看有无正反向解析文件存在
[root@localhost ~]# ls /var/named/slaves/   #如果不存在，则把主DNS服务器的两个正反解析文件拷过来到slaves文件夹里（我的是这两个文件 qiye.com.zone，qiye.com.local）

[root@localhost ~]# cd /var/named/slaves/
```

```
#更新DNS服务
[root@localhost ~]# systemctl restart named
```

```
#验证是否成功

[root@localhost ~]# ifconfig
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.241.134  netmask 255.255.255.0  broadcast 192.168.241.255

[root@localhost ~]# nslookup www.qiye.com
Server:     192.168.241.129
Address:    192.168.241.129#53

Name:   www.qiye.com
Address: 192.168.241.129

#ping一下，发现解析成功!
[root@localhost ~]# ping www.qiye.com
PING www.qiye.com (192.168.241.129) 56(84) bytes of data.
64 bytes from www.qiye.com (192.168.241.129): icmp_seq=1 ttl=64 time=0.782 ms
64 bytes from email.qiye.com (192.168.241.129): icmp_seq=2 ttl=64 time=0.419 ms
64 bytes from email.qiye.com (192.168.241.129): icmp_seq=3 ttl=64 time=0.711 ms
^C
--- www.qiye.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.419/0.637/0.782/0.158 ms
```

```
[root@localhost ~]# host www.qiye.com
www.qiye.com has address 192.168.241.129
[root@localhost ~]# host www.qiye.com
www.qiye.com has address 192.168.241.129
^C[root@localhost ~]# vim /etc/resolv.conf
[root@localhost ~]# host www.qiye.com
www.qiye.com has address 192.168.241.129
[root@localhost ~]# host c2.qiye.com
c2.qiye.com has address 192.168.241.134
[root@localhost ~]# host 192.168.241.129
129.241.168.192.in-addr.arpa domain name pointer email.qiye.com.
129.241.168.192.in-addr.arpa domain name pointer www.qiye.com.
[root@localhost ~]# host 192.168.241.134
134.241.168.192.in-addr.arpa domain name pointer c2.qiye.com.241.168.192.in-addr
.arpa.
[root@localhost ~]#
```

完成，www.qiye.com正是主DNS服务器的域名，ip地址192.168.241.129

yadaze!

5.智能解析

部署一台DNS智能解析服务器，对 qiye.com 域名做如下智能解析：

广州用户解析 IP 为 1.1.1.1

深圳用户解析 IP 为 2.2.2.2

其他用户解析为 3.3.3.3

```
#修改主配置文件
vim /etc/named.conf
#新增以下
acl gz {               #规则：这个网段ip，返回gz文件的DNS的ip
    192.168.247.0/24;
};
acl sz {             #规则：这个网段ip，返回sz文件的DNS的ip
    192.168.100.0/24;
};
acl ot {         #规则：除上述网段ip，返回ot文件的DNS的ip
    any;
};

#并且注释zone "."
/*
zone "." IN {
        type hint;
        file "named.ca";
};
*/

view guangzhou{
match-clients { gz; };
zone "." IN {
        type hint;
        file "named.ca";
};
zone "qiye.com" IN {
        type master;
```

```
        file "qiye.com.zone.gz";
};
};

view shenzhen {
match-clients { sz; };
zone "." IN {
        type hint;
        file "named.ca";
};
zone "qiye.com" IN {
        type master;
        file "qiye.com.zone.gz";
};
};

view other {
match-clients { any; };
zone "." IN {
        type hint;
        file "named.ca";

};
zone "qiye.com" IN {
        type master;
        file "qiye.com.zone.ot";
};
};
#还有注释了下面这个
#include "/etc/named.rfc1912.zones";
```

验证可能

```
#可以发现我的ip为192.168.241.129的时候，根据上述增加的acl规则，DNS服务器给我返回了other的
3.3.3.3
[root@localhost named]# ifconfig
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.241.129  netmask 255.255.255.0  broadcast 192.168.241.255

[root@localhost named]# host www.qiye.com
www.qiye.com has address 3.3.3.3
```

ya✧da✧ze!