BIND&DNS内部培训教程

1、域名系统

域名系统为一个分布式数据库，它使本地负责控制整个分布式数据库的部分段，每一段中的数据通过客户，服务器模式在整个网络上均可存取，通过采用复制技术和缓存技术使得整个数据库可靠的同时，又拥有良好的性能。

域名服务器包含数据库的部分段的信息，并可提供被称之为解析器的客户来访问。DNS 的数据库结构形成一个倒立的树状结构，根的名字用空字符串""来表示，但在文本中用"."来书写。树的每一个节点都表示整个分布式数据库中的一个分区（域），每个域可再进一步划分成子分区（域），每个域都有一个标签（LABEL），标明了它与父域的关系。域也有一个域名（domain name），给出它在整个分布式数据库中的位置。在DNS 中，域名全称是一个从该域到根的标签序列，以"."分隔这些标签.该标签最多可包含63 个字符。树中每一节点的完整域名为从该节点到根之间路径上的标签序列。

如果根域在节点的域名中出现，该名字看起来就象以点结尾（实际上是以点和空标签作结尾）。这些以点结尾的域名被称之为绝对域名（Absoulte Domain Name），不以点结尾的域名被称之为相对域名。域（Domains）即为树状域名空间中的一棵子树，域的域名同该子树根节点的域名一样。也就是说，域的名字就是该域中最高层节点的名字。举例来说，zhuhai.gd.cn 域的顶端就是名为zhuhai.gd.cn 的节点。

在DNS 中，每个域分别由不同的组织进行管理。每个组织都可以将它的域再分成一定数量的子域并将这些子域委托给其他组织进行管理，域既能包括主机又能包括其他域（它的子域）。域名被用做DNS 数据库中的索引.子域中任何域名被认为是域的一部分。事实上，主机即为域，域名仅是DNS 数据库中的索引，"主机"可由指向相关主机信息的域名来索引，域包含所有其域名在该域的主机。
在域名树中，叶节点的域通常代表主机，它们的域名可指向网络地址，硬件信息和邮件路由信息。在树内的节点，其域名既可命名一台主机，也可指向有关该域的子孙或子域的结构信息，在域名树中的内部域名并不受唯一性限制，它们既可表示它们所对应的域，又可代表网络中某台特定的主机。例如，sun.com 既是sun 的域，又是在sun 和internet 间转发信件的邮件服务器的域名。

网络上的每一台主机都有一个域名，域名给出有关主机的信息，该信息中包含IP 地址，MAIL 路由信息等等，主机也可以有一个或多个域名别名。

1.1 域名

判断域是否为另一域的子域的简单方法是比较它们的域名、子域名以其父域名结尾。设计域名系统的一个主要目的是让管理分散化，这是通过代理来实现的。管理域的组织将该域划分成子域，每一个子域可以由其他组织代理，这意味着那些代理组织负责维护在该子域的所有数据。他们可以自由地改变数据，甚至可以将他们管理的子域再划分成更多的子域并将它们再分配。父域中仅包含指向这些子域的指针，因而引用对那里

的查询。

1.2 域名服务器

存储有关域名空间信息的程序被称为域名服务器（name server）.通常，域名服务器拥有部分域名空间（称之为区zone）的完整信息，域名服务器可以拥有多个区的授权。

区与域的关系：

区包含了域中除了代理给别处的子域外所含有的所有域名和数据。如果域的子域没有被代理出去，则该区包含该子域名和子域中的数据。

DNS 定义了两类域名服务器：primary Master 和secondary Master.PM 域名服务器。从它所运行的主机上的文件获得它所负责的区的数据，SM 域名服务器则是从其它的具有该区授权的域名服务器上获得它的区的数据，SM 域名服务器会定期查询PM 域名服务器以保证区数据为最新版本。

一般情况下，最好设立一台PM 域名服务器和若干台SM 域名服务器，这样可以分担负载。以及确保区中所有主机都有比较靠近的域名服务器，方便访问。

1.3 解析器

运行在主机上并需要域名空间信息的重新需要解析器（Resolver），在bind 中解析器仅仅是一组库例程，并编译进象telnet 和ftp 这样的程序中，它们并非独立的进程。解析器所做的工作为：汇集查询，发送查询并等待应答，未得到应答时重发查询。

1.4 地址到域名的映射

在域名空间的数据是通过名字来进行索引的，找到一个给定域名的地址相对容易。但是要找到映射给一定地址的域名就要在树上的每一个域名空间作穷尽搜索。如果这样的话，效率将相当低，为了解决这个问题，创建一个以地址为索引的域名空间.这部分名字空间被称为in-addr.arpa 域。
in-addr.arpa 域中的节点以Doted-octet（将32bitIP 地址表示为由"."分隔开的四个8bit 的十进制形式的方法）形式表示IP 地址。IP 地址在名字空间以相反的方向表示，因为名字是从叶读到根，例如，www.zhuhai.gd.cn 的IP 地址为202.105.177.100，则相应的in-addr.arpa 子域为177.105.202.in-addr.arpa，使IP 地址中的第一个字节出现在树的最高层使的管理员有能力沿着网络联接将in-addr.arpa 域代理出去，例如177.105.202.in-addr.arpa 可以被代理给网络177.105.202 的管理员。

1.5 缓存与生存期

名字服务器在处理递归查询时，可能要进行多次查询才能得到信息，在这过程中，名字服务器可以获得很多有关域名空间的信息，名字服务器将所以这些信息都缓存起来以加速以后的查询。除了加速查询外，缓存还使得我们不必再次查询根名字服务器，这样可使得我们不必过分依赖根名字服务器而大大减轻根名字服务器的负载。

生存期（TTL）为所容许的名字服务器对数据缓存的时间长度，一旦生存期到了，名字服务器必须丢弃缓存数据并从授权的名字服务器中重新获取新的数据。这样可以确保域数据在整个网络上的一致性。

2. 安装服务器软件

2.1 取得bind 软件包（现在新的版本为8.2.2 p5）
从bind 的主页http：//www.isc.org 上取得最新stable 版的三个文件：
bind-contrib.tar.gz
bind-doc.tar.gz
bind-src.tar.gz
或者从http：//www.redhat.com 上取得三个文件：
bind-8.2.2-p5-9.i386.rpm
bind-devel-8.2.2-p5-9.i386.rpm
cache-nameserver-6.2-2.noarch.rpm

2.2 安装bind 软件包
安装tar 封装的软件包：
（1）先解压软件包
tar zxpf bind-contrib.tar.gz
tar zxpf bind-doc.tar.gz
tar zxpf bind-src.tar.gz

（2）编辑修改Makefile.set 文件，增加或修改
'DESTLIB=/usr/lib/bind/lib'
'DESTINC='/usr/lib/bind/include'

（3）编译并安装
make
make install

（4）安装rpm 封装的软件包：
rpm -Uhv bind-8.2.2-p5-9.i386.rpm
rpm -Uhv bind-devel-8.2.2-p5-9.i386.rpm
rpm -Uhv cache-nameserver-6.2-2.noarch.rpm

3.让服务器跑起来---基本篇

3.1
BIND 可被配置成几种不同的运行方式，通用的BIND 配置为纯解析器系统，纯缓存服务器，主服务器，辅服务器。
解析器是指通过域名服务器查询域信息的程序代码，在unix 系统中，它是以库例程的方式实现的，而并不是一个单独的客户程序.纯解析器系统很容易配置，只要设置一下/etc/resolv.conf 文件。这种方式通常用于由于某些限制不能在本地运行域名服务器软件的系统中。
例如：/etc/resolv.conf 内容类似为：
search jmcs.net
nameserver 202.106.0.20
当配置解析器库以使用BIND 名字服务进行主机查找，你也必须告知它使用哪个名

字服务器。对此有一个独立的文件，称为resolv.conf。如果这个文件不存在或是空的，那么解析器就假设名字服务器在你本地的主机上。如果在你的本地主机上运行一个名字服务器，你必须单独地设置它。resolv.conf 中最重要的选项是nameserver，它给出了要使用的名字服务器的IP 地址。如果你通过几次给出nameserver 选项指定了几个名字服务器，那么它们会以给出的顺序试用。因此，你应该首先给出最可靠的服务器。目前，至多支持三个名字服务器。如果没有给出nameserver 选项，那么解析器试图连接本地主机上的名字服务器。

其它两个选项，domain 和search 涉及到如果BIND 不能用第一个请求解析主机名时附加在主机名上的缺省域。search 选项指定了一个试用的域名列表。列表项是用空格或制表符分开的。

如果没有给出search 选项，就会通过使用域名本身从本地域名以及直至root 的父域中建立一个搜寻列表。本地域名可以使用domain 语句给出；如果一个也没有给出，那么解析器就通过系统调用getdomainname（2）来获取。

3.2 其它三类配置方式是用于域名服务器的纯缓存服务器纯缓存服务器运行域名服务器软件，但并没有域名服务器数据库文件，它记录下每一个从远程域名服务器获得的数据，以回答将来对同一信息的查询。

（1）纯缓存服务器所需的三个基本配置文件：

/etc/named.conf

/var/named/named.ca

/var/named/named.local

（2）创建或修改/etc/named.conf：

```
// generated by named-bootconf.pl
options
{
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to,  you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53,  but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
forwarders {202.99.8.1;202.106.0.20;};
};
//
// a caching only nameserver config
//
zone '.'
{
type hint;
file "named.ca";
```

```
};
zone '0.0.127.in-addr.arpa'
{
type master;
file "named.local";
};
```

（3）在文件中'forwarders {202.106.0.20;202.99.8.1;};'其中的IP 地址是你网络中主服
务器和辅服务器的IP 地址。

（4）创建或修改/var/named/named.local：

```
@ IN SOA localhost. root.localhost.  (
1997022700 ; Serial
28800 ; Refresh
14400 ; Retry
3600000 ; Expire
86400 ) ; Minimum
IN NS localhost.
1 IN PTR localhost.
```

（5）创建或修改/var/named/named.ca：

至于/var/named/named.ca 就要从redhat linux 光碟获得了.也用命令从互联网上获得：

```
dig @a.root-servers.net > /var/named/named.ca
```

如果是用rpm 封装的软件包安装的话，这三个文件会自动生成，我们只需要修改/etc/named.conf 。其中/var/named.ca 一般是不用修改的.

（6）主服务器：

主服务器是给定域的所有信息的授权来源。它所装载的域信息来自于由域管理员所创建并在本地维护的磁盘文件。

我们用"test.com"作为例子，我们需要五个基本配置文件：

```
/etc/named.conf
/var/named/named.ca
/var/named/named.local
/var/named/named.test.com
/var/named/named.172.16.0
```

（6.1）创建或修改/etc/named.conf：

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
```

```
// query-source address * port 53;
};
//
// a PM nameserver config
```
北京蓝色先锋软件有限公司版权所有违者必究
地址：北京市北京站东街甲10 号华安商务楼6 层
网址： www.bluepioneer.com.cn 邮编：100005 第8 页共14 页
电话：(010)65594026 传真：(010)65594064
```
//
zone '.' {
type hint;
file "named.ca";
};
zone '0.0.127.in-addr.arpa' {
type master;
file "named.local";
};
//there are our primary zone files
zone "test.com" {
type master;
file "named.test.com";
};
zone '0.16.172.in-addr.arpa' {
type master;
file 'named.172.16.0';
};
```
文件中的zone'test.com'段是声明这是用于test.com 域的主服务器，用于该域的数据从/var/named/named.test.com 文件中装载。
文件中的zone '0.16.172.in-addr.arpa'段是指向映射IP 地址172.16.0.* 到主机名的
文件。用于该域的数据从/var/named/named.172.16.0 文件中装载。
（6.2）创建或修改/var/named/named.local
```
@ IN SOA ns.test.com. root.ns.test.com. (
2000051500 ; Serial
28800 ; Refresh
14400 ; Retry
3600000 ; Expire
86400 ) ; Minimum
IN NS ns.test.com.
1 IN PTR localhost.
```
注意：在修改named.*文件时每次存盘时要注意增加Serial 值，如使用绝对域名时千万别忘了后面带的'.'。
资源记录中的@字符转变为当前的域test.com，IN 表示资源记录使用TCP/IP 地址，SOA 表示管辖开始记录.ns.test.com. 是这个域的主DNS 服务器的标准名称，在之后是联系

的
EMAIL 地址，其中@字符必须用'.'代替。

（6.3）创建或修改/var/named/named.test.com

```
@ IN SOA ns.test.com. root.ns.test.com. （
2000051500 ; Serial
28800 ; Refresh
14400 ; Retry
3600000 ; Expire
86400 ） ; Minimum
IN NS ns.test.com.
ns A 172.16.0.1
ns2 A 172.16.0.11
www A 172.16.0.2
ftp CNAME www.test.com.
mail A 172.16.0.3
MX 10 mail.test.com.
```

（6.4）创建或修改/var/named/named.172.16.0

```
@ IN SOA ns.test.com. root.ns.test.com. （
2000051500 ; Serial
28800 ; Refresh
14400 ; Retry
3600000 ; Expire
86400 ） ; Minimum
IN NS ns.test.com.
1 IN PTR ns.test.com.
11 IN PTR ns1.test.com.
2 IN PTR www.test.com.
3 IN PTR mail.test.com.
```

（7）辅服务器

辅服务器从主服务器上获取域信息的完整拷贝.也能以授权方式回答有关域的查询。我们用'test.com'作为例子，我们需要五个基本配置文件：

/etc/named.conf
/var/named/named.ca
/var/named/named.local

（7.1）创建或修改/etc/named.conf：

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
```

```
* port by default.
*/
// query-source address * port 53;
};
//
// a SM nameserver config
//
zone '.' {
type hint;
file "named.ca";
};
zone '0.0.127.in-addr.arpa' {
type master;
file "named.local";
};
//there are our slave zone files
zone "test.com" {
type slave;
file "named.test.com";
masters {172.16.0.1;};
};
zone '0.16.172.in-addr.arpa' {
type slave;
file 'named.172.16.0';
masters {172.16.0.1;};
};
```

在文件中'masters {172.16.0.1;};'其中的IP 地址是你网络中主服务器的IP 地址。从主服务器上拷贝/var/named/named.ca 和/var/named/named.local 这两个文件。实际运行的服务器可以是以上其中一种配置，也能同时包含多种配置，但所有的系统都应该运行解析器。

4.标准资源记录

资源记录文本名意义记录类型功能

Start of Authority 授权开始SOA 标记区数据的开始，定义影响整个区的参数Name Server 名字服务器
NS 标明域的名字服务器
Address 地址
A 转换主机名到地址
Pointer 指针PTR 转换地址到主机名
Mail Exchange 邮件交换MX 标明发往给定域名的邮件应传送到的位置
Canonical Name 正规名CNAME 定义主机名别名

HOST information 主机信息HINFO 描绘主机硬件和操作系统的信息
Wellknown Service 著名服务WKS 通告网络服务

DNS 使用MX 记录来实现邮件路由，它规定了域名的邮件服务器要么处理，要么向前转发有关该域名的邮件.处理邮件是指将其传送给其地址所关联的个人，向前转发邮件是指通过SMTP 协议将其传送给其最终目的地。为了防止邮递路由，MX 记录除了邮件交换器的域名外还有一个特殊参数：优先级值.优先级值是个从0 到65535 的无符号整数，它给出邮件交换器的优先级别。优先级值自身并不重要，关键在于它同其它邮件交换器的优先级值的相对大小，优先级值相对越小，优先级越高。邮件总是首先试图传递给优先级值相对最小的邮件交换器，失败后才试图传递给优先级值稍大的邮件交换器。邮件总是试遍了同一优先级的邮件交换器，失败后才试图传递给优先级稍低的邮件交换器。注意你列为邮件交换器的主机必须拥有地址记录。
例如：
mail A 172.16.0.3
MX 10 mail.test.com.

5.管理工具

5.1 dig
named.ca 文件的作用是告诉你的服务器在哪里可以找到根域的域服务器，这个文件一定要保证正确无误，一般来说，这个文件几乎不会变动，但是不能保证不会变动，最好是每一，两个月同步一下。使用下面的命令获得新的named.ca 文件：
dig @a.root-servers.net.ns >/var/named/named.ca
5.2 ndc
ndc 这个指令是由系统管理员用来管理域服务器的操作，在终端中输入ndc help 可得到帮助。
ndc restart 用来重新启动named 进程;
ndc reload 用来装入新的数据库.
5.3 nslookup
nslookup 是用来询域名信息的命令，它分交互模式和非交互模式两种方式。
非交互模式：nslookup www.zhuhai.gd.cn
交互模式：nslookup
注意，当用nslookup 查询时出现’Non-authoritative answer：’，表明这次并没有到网络外去查询，而是在缓存区中查找并找到数据。
交互模式除了能查询单个的主机，还可以查询DNS 记录的任何类型，并且传输一个域的整个区域信息。当不加参数地调用，nslookup 将显示它所用的名字服务器，并且进入交互模式。
在’>’提示符下，你可以键入任何想要查询的域名。缺省地，它请求类A 记录，这些是包含与域名相关的IP 地址的。
你可以通过发出‘set type=type’来改变这个类型，这里type 是上面描述的资源记录名，或ANY。
例如，你可以与它进行下面的对话：
$ nslookup
Default Name Server： rs10.hrz.th-darmstadt.de
Address： 130.83.56.60

```
> sunsite.unc.edu
Name Server:  rs10.hrz.th-darmstadt.de
Address:  130.83.56.60
Non-authoritative answer:
Name:  sunsite.unc.edu
Address:  152.2.22.81
```

如果你试者去查询一个没有相应IP 地址的名字，但DNS 数据库中能找到其它的记录，nslookup 将返回一个错误信息说‘No type A records found’（‘没有类型A 记录发现’）。

然而，你可以通过发出‘set type’命令来查询不是类型A 的其它记录。例如， 要得到unc.edu的SOA 记录，你要发出：

```
> unc.edu
*** No address (A) records available for unc.edu
Name Server:  rs10.hrz.th-darmstadt.de
Address:  130.83.56.60
> set type=SOA
> unc.edu
Name Server:  rs10.hrz.th-darmstadt.de
Address:  130.83.56.60
Non-authoritative answer:
unc.edu
origin = ns.unc.edu
mail addr = shava.ns.unc.edu
serial = 930408
refresh = 28800 (8 hours)
retry = 3600 (1 hour)
expire = 1209600 (14 days)
minimum ttl = 86400 (1 day)
Authoritative answers can be found from:
UNC.EDU nameserver = SAMBA.ACS.UNC.EDU
SAMBA.ACS.UNC.EDU internet address = 128.109.157.30
```

以同样的方式你可以查询MX 记录，等等。使用一个ANY 类型将返回与一个给出的名字关联的所有资源记录。

```
> set type=MX
> unc.edu
Non-authoritative answer:
unc.edu preference = 10,  mail exchanger = lambada.oit.unc.edu
lambada.oit.unc.edu internet address = 152.2.22.80
Authoritative answers can be found from:
UNC.EDU nameserver = SAMBA.ACS.UNC.EDU
SAMBA.ACS.UNC.EDU internet address = 128.109.157.30
```

除了调试，nslookup 的一个实际应用是为named.ca 文件获取根名字服务器的当前列

表。
你可以通过查询与根域相关的所有NS 类型记录来做到：

```
> set type=NS
> .
Name Server:  fb0430.mathematik.th-darmstadt.de
Address:  130.83.2.30
Non-authoritative answer:
 (root)  nameserver = NS.INTERNIC.NET
 (root)  nameserver = AOS.ARL.ARMY.MIL
 (root)  nameserver = C.NYSER.NET
 (root)  nameserver = TERP.UMD.EDU
 (root)  nameserver = NS.NASA.GOV
 (root)  nameserver = NIC.NORDU.NET
 (root)  nameserver = NS.NIC.DDN.MIL
Authoritative answers can be found from:
 (root)  nameserver = NS.INTERNIC.NET
 (root)  nameserver = AOS.ARL.ARMY.MIL
 (root)  nameserver = C.NYSER.NET
 (root)  nameserver = TERP.UMD.EDU
 (root)  nameserver = NS.NASA.GOV
 (root)  nameserver = NIC.NORDU.NET
 (root)  nameserver = NS.NIC.DDN.MIL
NS.INTERNIC.NET internet address = 198.41.0.4
AOS.ARL.ARMY.MIL internet address = 128.63.4.82
AOS.ARL.ARMY.MIL internet address = 192.5.25.82
AOS.ARL.ARMY.MIL internet address = 26.3.0.29
C.NYSER.NET internet address = 192.33.4.12
TERP.UMD.EDU internet address = 128.8.10.90
NS.NASA.GOV internet address = 128.102.16.10
NS.NASA.GOV internet address = 192.52.195.10
NS.NASA.GOV internet address = 45.13.10.121
NIC.NORDU.NET internet address = 192.36.148.17
NS.NIC.DDN.MIL internet address = 192.112.36.4
```

nslookup 完整的命令集可以通过nslookup 中的help 命令得到.