Linux DNS 服务器配置指南

目录

一、 域名系统介绍

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，别名仅是一些指向正式域名的另

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。

1.6 BIND：LINUX 名字服务

linux和其他的unix一样，都是用BIND来实现名字服务。BIND的服务端的软件是被称为named的守护进程。bind的主页是http://www.isc.org

二、 创建一个域名服务器

1 安装服务器软件

1.1 取得 bind 软件包

本配置指南是基于 Redhat 9 自带的 bind-9.2.1-16，更新的版本可以参照此指南。

从http://ftp.redhat.com上取得bind系统的rpm包文件：

bind-9.2.1-16.i386.rpm

1.2 安装 bind 软件包

安装 rpm 封装的软件包：

```
[root@localhost root]# rpm -Uhv bind-9.2.1-16.i386.rpm
```

2 让服务器跑起来---基本篇

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 test.com

nameserver 127.0.0.1

nameserver 172.16.0.1

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。

2.1 其它三类配置方式是用于域名服务器的

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。

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：

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。

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。

由于我们这里探讨的是主服务器,所以我们将多主服务器的配置情况进行详细的举例说明。

我们用"test.com"作为例子，我们需要四个基本配置文件：

/etc/named.conf （Bind 系统配置文件）

/var/named/named.ca（域名根服务器列表）

/var/named/test.com.zone（test.com 域配置文件）

/var/named/0.16.172.in-addr.arpa.zone（反相解析配置文件）

2.1.1 获得 named.ca 文件

在上节提到的四个文件中，除了 named.ca 文件外，都是需要我们自己去写入文件内容。named.ca 文件里面存放的是互联网上那 13 个根域名服务器的地址列表。这 13 个根服务器的地址一般情况下是不会有所改变的（截至 2005 年 11 月 2 日，上次对该文件进行修改的日期是 2002 年的 9 月份），推荐每隔 3 个月左右对该文件进行一次更新。那么 named.ca 文件如何获得呢？我们可以用 dig 命令获得：

```
[root@localhost root]# mkdir /var/named
[root@localhost root]# dig @.aroot-servers.net.ns > /var/named/named.ca
```

2.1.2 创建 named.conf 文件

由于 rpm 包安装的 Bind 系统缺省并没有生成 named.conf 这个配置文件，那么就需要我们来手动创建该文件：

```
[root@localhost root]# vi /etc/named.conf
options {
       directory "/var/named/";
};
//根域名服务器列表
zone  "." {
   type hint;
   file  "named.ca";
};
//这里是服务器的主域配置文件
zone "0.16.172.in-addr.arpa" {
   type master;
   file "0.16.172.in-addr.arpa.zone"; //域名反相解析配置文件
};

zone "test.com" {
   type master;
   file "test.com.zone";//test.com 域的域名配置文件
   allow-update { 172.16.0.1;127.0.0.1; };    // IP 地址
};
```

文件中的 zone "test.com"段定义了该域的类型为主域，该域的数据从/var/named/test.com.zone 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 211.156.33.* 到主机

名的文件。该域的数据从/var/named/0.16.172.in-addr.arpa.zone 文件中装载。

2.1.3 创建 test.com.zone 文件

```
[root@localhost root]# vi /var/named/test.com.zone
$ORIGIN test.com.
$TTL 86400    ; 1 day
test.com      IN SOA ns1.test.com. root.test.com. (
              2005103124 ; serial
              28800      ; refresh (8 hours)
              7200       ; retry (2 hours)
              604800     ; expire (1 week)
              86400      ; minimum (1 day)
              )
              NS  ns1.test.com.
              A   172.16.0.1
              MX  10 www.test.com.
ns1.test.com. A   172.16.0.1
www.test.com. A   172.16.0.1
oa.test.com.  A   172.16.0.1
mail.test.com.    A   172.16.0.1
```

注意：在修改 named.*文件时每次存盘时要注意增加 Serial 值，这么虽不是必须的，但是为了便于日后的管理，建议及时将该值修改为当前时间。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。ns1.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。

2.1.4 创建/var/named/0.16.172.in-addr.arpa.zone 文件

```
[root@localhost root]# vi /var/named/0.16.172.zone
$TTL 86400     ; 1 day
@ IN SOA ns1.test.com. root.test.com. (
       2000051500 ; Serial
       28800 ; Refresh
       14400 ; Retry
       3600000 ; Expire
       86400 ) ; Minimum
    IN NS ns1.test.com.
1   IN PTR ns1.test.com.
2   IN PTR www.test.com.
3   IN PTR oa.test.com.
4   IN PTR mail.test.com.
```

3 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：

```
                MX 10 mail.test.com.

mail.test.com.  A   172.16.0.1
```

4 管理工具

4.1 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 @.aroot-servers.net.ns >/var/named/named.ca
```

4.2 named

named 这个指令是由系统管理员用来管理域服务器的操作。

/etc/init.d/named restart 用来重新启动 named 进程;

/etc/init.d/named reload 用来装入新的数据库。

4.3 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.test.com

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: test.com

Address: 172.16.0.1

> www.test.com

Name Server: test.com

Address: 172.16.0.1

Non-authoritative answer:

Name: www. test.com

Address: 172.16.0.1

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：

> set type=SOA

> test.com

```
Name Server: test.com

Address: 172.16.0.1

Non-authoritative answer:

test.com

        origin = ns1.test.com

        mail addr = root.test.com

        serial = 2005103124

        refresh = 28800

        retry = 7200

        expire = 604800

        minimum = 86400


Authoritative answers can be found from:

test.com        nameserver = ns1.test.com.
```

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

> test.com

Non-authoritative answer:

test.com        mail exchanger = 10 www.test.com.


Authoritative answers can be found from:

test.com        nameserver = ns1.test.com.

www.test.com    internet address = 172.16.0.1
```

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

> .

Server:         218.16.120.163

Address:        218.16.120.163#53
```

```
Non-authoritative answer:
.       nameserver = G.ROOT-SERVERS.NET.
.       nameserver = H.ROOT-SERVERS.NET.
.       nameserver = I.ROOT-SERVERS.NET.
.       nameserver = J.ROOT-SERVERS.NET.
.       nameserver = K.ROOT-SERVERS.NET.
.       nameserver = L.ROOT-SERVERS.NET.
.       nameserver = M.ROOT-SERVERS.NET.
.       nameserver = A.ROOT-SERVERS.NET.
.       nameserver = B.ROOT-SERVERS.NET.
.       nameserver = C.ROOT-SERVERS.NET.
.       nameserver = D.ROOT-SERVERS.NET.
.       nameserver = E.ROOT-SERVERS.NET.
.       nameserver = F.ROOT-SERVERS.NET.

Authoritative answers can be found from:
A.ROOT-SERVERS.NET      internet address = 198.41.0.4
J.ROOT-SERVERS.NET      internet address = 192.58.128.30
```

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

5 与 Microsoft dns 的集成

Microsoft dns 定义了一个新的类型 WINS 的资源记录，它附属在域的根区。这个记录告诉 Microsoft 的 DNS 服务器如何与 WINS 服务器取得联系，解决对没有静态 DNS 记录的主机的名称查询问题。

示例，一个 WINS 资源记录如下：

```
@ IN WINS 192.168.1.100
```

为了使 DNS 和 WINS 合作，在 Microsoft 的 DNS 服务器配置中选择相应域的 properties 记录，并且在 WINS LOOKUP 标签中启用 WINS 解决。

由于采用了非标准的资源记录，大多数其他 DNS 并不支持这种资源记录，如非 Microsoft dns 的计算机企图从有 DNS-WINS 资源记录的 microsoft 的 DNS 服务器中进行区传送时，那

么，该计算机就很可能出错。

6 DNS 故障诊断

大多数 DNS 故障的原因是配置文件的语法错误，或者是对错误的计算机分配了错误的地址。当进行 DNS 故障诊断时，参照下面的指导方针。

6.1

对全部记录，检查和确认主机名称的拼写。记住绝对地址是以″.″结尾.

6.2

如果在区文件中作了任何修改，务必修改 SOA 记录中的序列号。这将保证服务器正确地重新上载文件。

6.3

确定输入到主区的名称和 IP 地址匹配反向指针文件中的反向指针信息。

6.4

Microsoft 的 DNS 服务器采用了非标准的资源记录，可能会导致问题。