Bind9 安装设置指南

目录

[隐藏]

- 1 HOWTO Setup BIND9 DNS Server （如何安装设置 Bind9 DNS 服务器）
  - 1.1 Repositories 软件库
  - 1.2 Installing BIND9 （安装 BIND9）
  - 1.3 BIND9 Scenarios

        - 1.3.1 Caching Server（缓冲服务器）
        - 1.3.2 Master Server（主服务器）
        - 1.3.3 Slave Server（从服务器）
        - 1.3.4 Hybrids（混和模式）
        - 1.3.5 Stealth Servers（私密服务器）
    - 1.4 DNS Record Types（DNS 记录类型）
        - 1.4.1 Address Records（地址记录）
        - 1.4.2 Alias Records（别名记录）
        - 1.4.3 Mail Exchange Records（邮件交换记录）
        - 1.4.4 Name Server Records（域名服务器记录）
    - 1.5 Configuring BIND9（配置 BIND9）
        - 1.5.1 Caching Server（缓冲服务器）
        - 1.5.2 Master Server（主服务器）
        - 1.5.3 Slave Server（从服务器）
    - 1.6 Chrooting BIND9
        - 1.6.1 The Chroot Enviroment（Chroot 环境）
        - 1.6.2 BIND9's Configuration（BIND9 的配置）
        - 1.6.3 Ubuntu's syslogd Daemon Configuration（Ubuntu 的 syslogd 守护进程配置）
        - 1.6.4 Restart the syslog server and BIND9（重启 syslog 服务及 BIND9）
    - 1.7 Starting, Stopping, and Restarting BIND9（开始、停止和重启 BIND9）
        - 1.7.1 Status（状态）
    - 1.8 Tips & Tricks（提示与技巧）
    - 1.9 Additional Possibilities（附加功能）
    - 1.10 Further Information（更多信息）
        - 1.10.1 Online Recources（在线资源）
        - 1.10.2 Printed Resources（印刷资源）

[编辑]HOWTO Setup BIND9 DNS Server （如何安装设置 Bind9 DNS 服务器）

原文出处：

原文作者：

翻译人员：FireHare

校正人员：purewind

贡献人员：

适用版本：

This HOWTO is aimed to at people looking to learn how to configure and maintain a DNS server, such as for a network or to serve DNS zones for a domain name.
本指南是写给那些想学习如何配置和维护 DNS 服务器的人，例如为某个网络或者 DNS zones(DNS 域)提供 Domain Name(域名)服务

[编辑]Repositories 软件库

BIND9 is available in the core Ubuntu repository. No additional repository needs to be enabled for BIND9.
BIND9 已经包含在 Ubuntu 核心库中，BIND9 并不需要启用其它附加库。

Before we begin, you should be familiar with RootSudo.
在我们开始之前，您应该熟悉 RootSudo。

[编辑]Installing BIND9 （安装 BIND9）

The Server
服务器

```
$ sudo apt-get install bind9
```

Useful Tools (For Testing)
有用的工具（测试用）

```
$ sudo apt-get install bind9-host dnsutils
```

Documentation (Optional)
文档（可选）

```
$ sudo apt-get install bind9-doc
```

[编辑]BIND9 Scenarios

There are many setups BIND9 may be configured.
BIND9 可以安装配置成许多类型。

The most useful setups are: 最常用的配置有：

[编辑]Caching Server（缓冲服务器）

This can be useful for a broadband connection to a host or small network. By caching DNS queries, you reduce the bandwidth used and (hopefully) reducing your bandwidth used (and hopefully even your broadband bill!).
这对于宽带连接的主机或小网络来说是有用的。通过缓冲 DNS 队列，您可以减少带宽的消耗，或者说有望减少您带宽的使用（甚至有望减少您宽带费用）。

[编辑]Master Server（主服务器）

BIND9 can be used to serve DNS records (groups of records are referred to as zones) for a registered domain name or an imaginary one (but only if used on a restricted network)
BIND9 可以用于为已注册或虚拟的（仅用于受限网络中）域名提供 DNS 记录（指向域的记录组）。

[编辑]Slave Server（从服务器）

A slave DNS server is used to complement a Master DNS server by serving a copy of the zone(s) configured on the Master server. Slave servers are recommended in larger setups (larger networks or on the internet) if you intend to power a registered domain name, since they ensure that your DNS zone is still available, even if your Master server is not online.
从服务器用于提供一个在主服务器中配置域的完整备份。如果您想要支持一个注册的域名，建议将从服务器用在较大的机构（较大的网络或在因特网上）。因为这样做可以确保您的 DNS 域甚至在您主服务器没有在线的情况下依然可用。

[编辑]Hybrids（混和模式）

You can even configure BIND9 to be a Caching and Master DNS server simultaneously, a Caching and a Slave server or even a Caching, Master and Slave server. All that is required is simply combining the differnet configuration examples from this document.
您甚至可以将 BIND9 同时配置成一个缓冲和主服务器，一个缓冲服务器和一个从服务器，甚至是一个缓冲、主、从服务器。而所有这一切只需将本文档中不同配置简单的合并在一起就可以了。 What's this?

[编辑]Stealth Servers（私密服务器）

There are also two other common DNS server setups (used when working with zones for registered domain names), Stealth Master and Stealth Slave. These are effectively the same as Master and Slave DNS servers, but with a slight organisational difference.
还有另外两种常用的 DNS 服务器的安装（使用注册域名运行）：私有主服务器和私有从服务器。它们的作用与主、从 DNS 服务是相同的，但在组织结构上有所不同。

For example, you have 3 DNS servers; A, B and C.
例如，您有 3 个 DNS 服务器：A、B 和 C。

A is the Master, B and C are slaves.
A 是主服务器，B 和 C 是从服务器。

If you configure your registered domain to use A and B as your domain's DNS servers, then C is a Stealth Slave. It's still a slave, but it's not going to be asked about the zone you are serving to the internet from A and B
如果您将 A 和 B 配置成您的域 DNS 服务器，然后 C 是一个私密从服务器。它也是个从服务器，但您为互联网提供服务的 A 和 B 不会去询问其中的域。

If you configure your registerd domain to use B and C as your domain's DNS servers, then A is a stealth master. Any additional records or edits to the zone are done on A, but computers on the internet will only ever ask B and C about the zone.
如果您将 B 和 C 配置成您的域 DNS 服务器，然后 A 是一个私密主服务器。任何附加的记录或对区域的编辑都做在 A 上，但在互联网上的计算机只会询问 B 和 C 中的域。

[编辑]DNS Record Types（DNS 记录类型）

There are lots of different DNS record types, but for a someone reading this document, you need only deal with these record types
DNS 记录类型是有很多不同的，但对于阅读本文档的人来说，您只需要处理以下这些记录类型

[编辑]Address Records（地址记录）

The most commonly used type of record.
最常用的记录类型

```
www       IN    A       1.2.3.4
```

[编辑]Alias Records（别名记录）

Used to create an alias from an existing A record. You cannot create a CNAME record pointing to another CNAME record.
常用于为一个已有的 A 记录创建别名。您不能创建一个 CNAME 记录指向另一个 CNAME 记录。

```
mail      IN    CNAME   www
www       IN    A       1.2.3.4
```

[编辑]Mail Exchange Records（邮件交换记录）

Used to define where email should be sent to. Must point to an A record, not a CNAME.
常用于定义邮件发往何处。必须指向一个 A 记录，不能是 CNAME。

```
IN    MX      mail.example.com.

[...]

mail    IN    A       1.2.3.4
```

[编辑]Name Server Records（域名服务器记录）

Used to define which servers serve copies of this zone. It must point to an A record, not a CNAME.
常用于定义哪个服务器提供该区域的拷贝。它必须指向一个 A 记录，不能是 CNAME。

This is where Master and Slave servers are definied. Stealth servers are intentionally omitted.
这是定义主、从服务器的地方。私密服务器被有意省略。

```
IN    NS      ns.example.com.

[...]

ns      IN    A       1.2.3.4
```

[编辑]Configuring BIND9（配置 BIND9）

BIND9 Configuration files are stored in
BIND9 配置文件被保存在

```
/etc/bind/
```

The main configuration is stored in the following files
主配置文件被保存在下列文件中

```
/etc/bind/named.conf
/etc/bind/named.conf.options
/etc/bind/named.conf.local
```

[编辑]Caching Server（缓冲服务器）

The default configuration is setup to act as a caching server by default.
缺省状态下默认是当作缓冲服务器来配置安装的。

All that is required is simply adding the IP numbers of your ISP's DNS servers.
所有的要求只是简单的添加您 ISP 的 DNS 服务器的 IP 而已。

Simply uncomment and edit the following:
只需反注释并编辑下列内容：

```
named.conf.options:


[...]

forwarders {
1.2.3.4;
5.6.7.8;
};

[...]
```

(where 1.2.3.4 and 5.6.7.8 are the IP numbers of your ISP's DNS servers)
（其中 1.2.3.4 和 5.6.7.8 是您 ISP 商 DNS 服务器的 IP。

[编辑]Master Server（主服务器）

To add a DNS zone to BIND9, turning BIND9 into a Master server, all you simply have to do is:
要添加 DNS 域到 BIND9，让 BIND9 成为主服务器，您只需如下所示：

```
named.conf.local:


[...]

zone "example.com" {
type master;
file "/etc/bind/db.example.com";
};

[...]
```

Now use an existing zone file as a template
现在使用一个已有域文件作为模板

```
$ sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

Now, to edit our zone
现在，编辑我们的域

```
db.example.com:



;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
1         ; Serial
604800         ; Refresh
86400         ; Retry
```

```
2419200         ; Expire
604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
```

Edit localhost. to the FQDN of your server, with an additional "." at the end.
编辑 localhost. 指向您服务器的 FQDN，在其后有一个附加的 "."。

Eg:
例如：

```
db.example.com:



;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     box.example.com. root.localhost. (
1         ; Serial
604800         ; Refresh
86400         ; Retry
2419200         ; Expire
604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
```

Edit root.localhost to be your email address, but with a "." instead of the "@", and another "." at the end.
编辑 root.localhost 指向你的邮件地址，不过要用 "." 代替 "@"，另一个 "." 放在末尾。

Eg:
例如：

johndoe@exmaple.com should be added as johndoe.example.com.
johndoe@exmaple.com 将使用 johndoe.example.com. 的形式添加。

Increment the Serial number (you must increment the serial number for every time you make any changes to the zone file and reload the zone by restarting BIND9. If you make multiple

changes before restarting BIND9, simply increment the serial once.
增加序列号（您必须在您每次对域文件做更改并通过重启 BIND9 重新引导域时增加您的序列号。如果您在重启 BIND9 之前做了多处改变，只需增加一次序列号即可）。

Tip: Many people like to use the last date edited as the serial of a zone, such as 2005010100 which is yyyymmddss (where s is serial)
技巧：许多人喜欢使用最新的日期作为域的序列号，例如以 yyyymmddss 的形式 2005010100 。

Now, you can add DNS records to the bottom of the zone. Do remember to increment the serial as you add entries though.
现在，您可以将 DNS 记录添加在域的底部。记住在您添加条目之后要增加序列号。

[编辑]Slave Server（从服务器）

First, on the master server, you have to allow the zone transfer. The sample zone definition in /etc/bind/named.conf.local should like this:
首先，在主服务器上，您必须允许域可以传输。这个在 /etc/bind/named.conf.local 中域定义的示例如下所示：

```
[...]

zone "example.com" {
type master;
file "/etc/bind/db.example.com";
allow-transfer {
@ip_slave;
};
};

[...]
```

On the slave, you have to proceed to the same installation that was done on the master. Then edit the /etc/bind/named.conf.localand add the following declaration for the zone:
在从服务器上，您还必须象主服务器上一样做同样处理。然后编辑 /etc/bind/named.conf.local 并为域添加下列声明：

```
[...]

zone "example.com" {
type slave;
file "/etc/bind/db.example.com";
```

```
masters { @ip_master; };
};

[...]
```

Restart the server, you should see in /var/log/syslog something like:
重启服务器，您将在 /var/log/syslog 类似下面的提示：

```
syslog.5.gz:May 14 23:33:53 smith named[5064]: zone example.com/IN: transferred serial
2006051401
syslog.5.gz:May 14 23:33:53 smith named[5064]: transfer of 'example.com/IN' from 10.0.0.202#53:
end of transfer
```

[编辑]Chrooting BIND9

Chrooting BIND9 is a recommended setup from a security perspective. In a chroot enviroment, BIND9 has access to all the files and hardware devices it needs, but is unable to access anything it should not need.
Chrooting BIND9 从安全角度来说是被推荐的安装。在 chroot 环境中，BIND9 可以访问所有它所需的文件和硬件，但不能访问它所不需要的。

To chroot BIND9, simply create a chroot enviroment for it and add the additional configuration below
要 chroot BIND9，只需为它创建一个 chroot 环境并在下面添加额外配置。

[编辑]The Chroot Enviroment（Chroot 环境）

Create the following directory structure
创建下面目录结构

```
$ sudo mkdir -p /chroot/named
$ cd /chroot/named
$ sudo mkdir -p dev etc/namedb/slave var/run
```

Set permissions for chroot environment
为 chroot 环境设置权限

```
$ sudo chown root:root /chroot
```

```
$ sudo chmod 700 /chroot
$ sudo chown bind:bind /chroot/named
$ sudo chmod 700 /chroot/named
```

Create or move the bind configuration file.
创建或移动 bind 配置文件。

```
$ sudo touch /chroot/named/etc/named.conf
```

or
或

```
$ sudo cp /etc/named.conf /chroot/named/etc
```

Give write permissions to the user bind for /chroot/named/etc/namedb/slave directory.
将 /chroot/named/etc/namedb/slave 目录的写权限赋予 bind 用户。

```
$sudo chown bind:bind /chroot/named/etc/namedb/slave
```

This is where the files for all slave zones will be kept. This increases security, by stopping the ability of an attacker to edit any of your master zone files if they do gain access as the bind user. Accordingly, all slave file names in the /chroot/named/etc/named.conf file will need to have directory names that designate the slave directory. An example zone definition is listed below.
所有的从域将放置在此处。这样可以增强安全性，如果攻击者得到了 bind 用户的权限，他们也没有办法修改您的主域文件。因此在 /chroot/named/etc/named.conf 文件中的所有的从文件名都必须带着指向从目录的目录名。下面列出了一个域定义的示例：

```
zone “my.zone.com.” {
type slave;
file “slaves/my.zone.com.dns”;
masters {
10.1.1.10;
};
};
```

Create the devices BIND9 requires
创建 BIND9 的环境

```
$ sudo mknod /chroot/named/dev/null c 1 3
$ sudo mknod /chroot/named/dev/random c 1 8
```

Give the user bind access to the /chroot/named/var/run directory that will be used to strore PID and statistical data.
给 bind 用户访问 /chroot/named/var/run 目录的权限，该目录用于保存 PID 和状态数据

```
$ sudo chown bind:bind /chroot/named/var/run
```

[编辑]BIND9's Configuration（BIND9 的配置）

Edit the bind startup options found in /etc/default/bind9. Change the line the reads:
在 /etc/default/bind9 中编辑 bind 启动选项。原来选项如下：

```
/etc/default/bind9:

OPTIONS=" -u bind"
```

So that it reads
现在改为

```
/etc/default/bind9:


OPTIONS="-u bind -t /var/named -t /chroot/named -c /etc/named.conf"
```

The -t option changes the root directory from which bind operates to be /chroot/named. The -c option tells Bind that the configuration file is located at /etc/named.conf. Remember that this path is relative to the root set by -t.
选项 -t 将 bind 操作的根目录改成 /chroot/named，选项 -c 则告诉 bind 配置文件在 /etc/named.conf。记住用 -t 设置的是相对路径。

The named.conf file must also recieve extra options in order to run correctly below is a minimal set of options:
named.conf 文件也必须接受额外的选项以便正常运行，下面是最小的选项集：

```
/chroot/named/etc/named.conf:
```

```
options {
directory "/etc/namedb";
pid-file "/var/run/named.pid";
statistics-file "/var/run/named.stats";
};
```

[编辑]Ubuntu's syslogd Daemon Configuration（Ubuntu 的 syslogd 守护进程配置）

```
/etc/init.d/sysklogd:


[...]

SYSLOGD="-u syslog -a /chroot/named/dev/log"

[...]
```

(Author Note: Check this config)
(注意：检查该配置）

[编辑]Restart the syslog server and BIND9（重启 syslog 服务及 BIND9）

```
$ sudo /etc/init.d/sysklogd restart
$ sudo /etc/init.d/bind9 restart
```

At this point you should check /var/log/messages for any errors that may have been thrown by bind.
这里，您要检查 /var/log/messages 是否有 bind 引起的错误。

[编辑]Starting, Stopping, and Restarting BIND9（开始、停止和重启 BIND9）

Use the following command to start BIND9 :
使用下列命令开始 BIND9：

```
$ sudo /etc/init.d/bind9 start
```

To stop it, use :
停止它，使用：

```
$ sudo /etc/init.d/bind9 stop
```

Finally, to restart it, run
最后，要重启它，运行：

```
$ sudo /etc/init.d/bind9 restart
```

[编辑]Status（状态）

To check the status of your BIND9 installation:
要检查您的 BIND9 安装状态：

```
$ host $record localhost
```

or
或

```
$ dig $record @localhost
```

(where localhost is the system you are setting BIND9 up on. If not localhost, use the appropriate IP number.) （在这里 localhost 是您安装 BIND9 的系统。如果不要 localhost，那么使用适当的 IP 地址。）

[编辑]Tips & Tricks（提示与技巧）

[编辑]Additional Possibilities（附加功能）

You can monitor your BIND9 server usage by installing the bindgraph package from the Universe (To enable Universe - see AddingRepositoriesHowto) and following configuration details as outlined in bindgraph's README documents
您可以从 Universe 库中安装 bindgraph 包（要激活 Universe 库 — 请参见 AddingRepositoriesHowto），并用它来监视您的 BIND9 服务器的使用，配置细节可以在 bindgraph README 文档中找到。

[编辑]Further Information（更多信息）

[编辑]Online Recources（在线资源）

"ISC's BIND9 Manual"

TLDP's "DNS HOWTO" (For General Overview)

"Chroot BIND Howto"

[编辑]Printed Resources（印刷资源）

"DNS & BIND" - Paul Albitz & Cricket Liu - 4th Editi