

DRMSD部署手册

贺伟伟, 杨正伟

Version 0.0.5, 7/15/2019

目录

- Bind配置文件的修改..... 1
- drmsd的安装..... 5
- drmsd的配置..... 5
- 系统运行..... 7

Bind配置文件的修改

在迭代服务器上的部署

创建一个标准的根域配置文件（/etc/std-rootzone）和存根的根域配置文件（/etc/local-rootzone），其内容如下：

```
$ cat /etc/std-rootzone

zone "." IN {
    type hint;
    file "named.ca";
};

$ cat /etc/local-rootzone

zone "." IN {
    type static-stub;
    server-address {
        ip1;
        ip2;
        ...
    };
};
```

在Bind的配置文件 /etc/named.conf 中删除关于根域的配置，然后替换成如下这行配置：

```
$ cat /etc/name.conf

options {

    ...

    dnstap { all; };
    dnstap-output unix "/var/run/named/dnstap.sock";

    ...

};

...

include /etc/named.conf.rootzone;

...
```

文件 /etc/named.conf.rootzone 是一个连接文件，初始值指向标准的根域配置文件，例如：

```
$ ln -s /etc/std-rootzone /etc/named.conf.rootzone
$ ls -l /etc/named.conf.rootzone

drwxrwxrwx  1 named named   18  May 30 17:17 /etc/named.conf.rootzone ->
/etc/std-rootzone
```

在根区副本上的部署

配置常态数据源

```
$ cat /etc/standard_root.zone

zone "." IN {
    type slave;
    masters {
        ip1;
        ip2;

        ...

    };
    file "slaves/standard_root.ca";
};
```

配置紧急数据源

```
$ cat /etc/exigency_root.zone

zone "." IN {
    type slave;
    masters {
        ip1;
        ip2;

        ...
    };
    file "slaves/exigency_root.ca";
};
```

创建软连接，并更改权限

```
$ ln -f -s /etc/standard_root.zone /etc/switch_root.zone
$ chown -R named:named /etc/switch_root.zone
$ ls -l /etc/*.zone

...

-rw-r--r-- named named 112 Jul 2 17:03 /etc/exigency_root.zone
-rw-r--r-- named named 112 Jul 2 17:03 /etc/standard_root.zone
lrwxrwxrwx named named 18 Jul 2 17:03 /etc/switch_root.zone ->
standard_root.zone

...
```

在Bind的配置文件 `/etc/named.conf` 中删除关于根域的配置，然后替换成如下这行配置：

```
$ cat /etc/name.conf

...

options {

    ...

    dnstap { all; };
    dnstap-output unix "/var/run/named/dnstap.sock";

    ...

};

include /etc/switch_root.zone;

...
```

配置rndc，运行rndc-confgen，根据命令结果写入配置文件 /etc/rndc.conf 和 /etc/named.conf

```
$ rndc-confgen

# Start of rndc.conf
key "rndc-key" {
    algorithm hmac-md5;
    secret "S/atGf79010VKJm0hDUJGQ==";
};

options {
    default-key "rndc-key";
    default-server 127.0.0.1;
    default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as need:
# key "rndc-key" {
#     algorithm hmac-md5;
#     secret "S/atGf79010VKJm0hDUJGQ==";
# };
#
# controls {
#     inet 127.0.0.1 port 953
#         allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
```

drmsd的安装

安装**drmsd**主要通过rpm包的格式，示例：

```
$ rpm -ivh drmsd-${DRMSD_VERSION}.el6.x86_64.rpm

...
```

drmsd的配置

drmsd的配置文件默认为 /etc/drmsd.ini，内容有：

```
$ cat /etc/drmsd.ini
```

```
[network]
port = 1024      # drmsd 监听端口号
ackhost = 127.0.0.1 # DRSS 提供 dns_commandack() 远程过程调用的ip地址
ackport = 1912    # DRSS 提供 dns_commandack() 远程过程调用的端口号
```

```
[security]
secret = 1234567890abcDEF # 用户口令
aes_key = 1234567890abcDEF # AES 密钥
aes_iv = 1234567890abcDEF # AES 加密偏移向量
```

```
[named-conf]
home = /etc          # drmsd 配置文件根目录
rndc = rndc          # Bind管理工具
```

```
switch = named.conf.rootzone # drmsd
用于在国际根和根区副本间切换的链接文件，这和 Bind 配置文件中的内容一致
```

```
std = std-rootzone      # 国际根的配置文件
local = local-rootzone  # 根区副本配置文件
stat_file = /var/named/data/named_stats.txt # Bind统计文件路径
run_file = /var/named/data/named.run        # Bind运行日志路径
dnstap_file = /var/named/data/zone.dnstap    # dnstap文件路径
```

```
[source]
root_source = switch_root.zone # drmsd
在常态数据源和紧急数据源之间切换的链接文件，这和 Bind 配置文件中的内容一致
```

```
exigency_source = exigency_root.zone # 紧急数据源
standard_source = standard_root.zone # 常态数据源
```

```
[ftp]
ip = 192.168.65.122
port = 22
user = shanghi
pwd = test123
dir = upload
```

```
[server]
operator = ct          # 运营商名称
vendor = yamu          # 企业名称
server_type = root_copy # 服务器类型(root_copy, recursion)
node_id = ct0001       # 节点ID
server_id = rs0001     # 服务器ID
upload_delay = 300     # 数据上报间隔时间
```


系统运行

```
$ /usr/bin/start_fstrm_capture -u /var/run/named/dnstap.sock -w  
/var/named/data/zone.dnstap -s 300 ①
```

```
$ service named start
```

```
$ service drmsd start
```

- ① **start_fstrm_capture** 应该在 **Bind** 之前运行，其中的 **-u** 参数与 **Bind** 配置文件中的 **dnstap-output** 配置项一致，**-w** 参数与 **/etc/drmsd.ini** 中的 **named-conf.dnstap_file** 配置项一致，**-s** 选项与 **/etc/drmsd.init** 中的 **server.upload_delay** 一致。