

การติดตั้งปรับแต่งระบบปฏิบัติการ FreeBSD 8.1 ให้เป็น Caching DNS & intra-net DNS server นั้นจะมีขั้นตอนคล้ายกับเอกสาร <http://freebsd.aru.ac.th/FreeBSD80/f80dns.pdf> แต่บน FreeBSD8.1 นั้นจะเพิ่มด้านความปลอดภัยมากขึ้น โดยตัดและเติมบางส่วนจนทำให้วิธีการแบบเดิมไม่สามารถทำงานได้ ลองมาดูกัน

ติดตั้ง Domain Name server บน FreeBSD 8.1

#### ผลลัพธ์ที่ต้องการ

1. สมมุติว่าเราจะตั้ง Domain ของเราภายในหน่วยงานเป็น intra.net ซึ่งเราจะสามารถมี server ต่าง ๆ เช่น www.intra.net , ftp.intra.net , mail.intra.net ได้เป็นต้น
2. ให้ DNS ที่เราจะติดตั้งนี้ทำหน้าที่เป็น Caching DNS ด้วย ดังนั้นเครื่อง Client ในเครือข่าย LAN ของเราก็สามารถชี้ DNS มาที่ Server ตัวนี้ (ไม่ต้องตั้ง (ชี้) dns ข้างนอก) มันก็ใช้เรียกเว็บได้ทั่วโลก

เริ่มกันเลย

```
#cd /etc/namedb/master
#cp empty.db intra.net-for.db
```

แก้ไขไฟล์ intra.net-for.db

```
#ee intra.net-for.db
```

```
$TTL 3600
@      IN      SOA      ns.intra.net.  noc.intra.net.(
                          2010100601 ;serial
                          3600 ;refresh
                          900 ;retry
                          3600000 ;expire
                          3600) ;minimum

      IN      NS       ns.intra.net.
      IN      MX       10 mail.intra.net.
ns     IN      A        192.168.119.130
www    IN      A        192.168.119.130
ftp    IN      A        192.168.119.130
mail   IN      A        192.168.119.130
```

```
#cp intra.net-for.db intra.net-rev.db
```

แก้ไขไฟล์ intra.net-rev.db

```
#ee intra.net-rev.db
```

```
$TTL 3600
@      IN      SOA      ns.intra.net.  noc.intra.net.(
                          2010100601 ;serial
                          3600 ;refresh
                          900 ;retry
                          3600000 ;expire
                          3600) ;minimum

      IN      NS       ns.intra.net.
      IN      MX       10 mail.intra.net.
130    IN      PTR     ns.intra.net.
130    IN      PTR     www.intra.net.
130    IN      PTR     ftp.intra.net.
130    IN      PTR     mail.intra.net.
```

```

เปลี่ยน Directory เพื่อแก้ไข config
#cd /etc/namedb/
สำรองไฟล์ named.conf (กันพลาด)
#cp named.conf named.conf.org
สร้างไฟล์ rndc.conf
#rndc-confgen > rndc.conf
นำเอา rndc.conf ไปต่อท้ายไฟล์ named.conf
#cat rndc.conf >> named.conf
แก้ไข config
#ee named.conf
เพิ่มส่วน hightlight สีเหลือง ลบ hightlight สีแดง ตามบรรทัดที่ปรากฏในไฟล์ (192.168.119.130 คือ ip ของเครื่อง DNS)
listen-on { 127.0.0.1; 192.168.119.130; };
allow-query { any; };
allow-recursion { any; };
allow-transfer { none; };

/*
forwarders {
    127.0.0.1; 8.8.8.8; 8.8.4.4;
};
*/
หมายเหตุ : ip 8.8.8.8 และ 8.8.4.4 เป็น public dns ของ google

```

ในส่วน Private Use Networks ให้เพิ่ม comment ตามสีเหลือง (ถ้าทำ Authoritative DNS ไม่ต้องทำอันนี้ เพื่อความปลอดภัย)

```

// Private Use Networks (RFC 1918)
/*
zone "10.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "16.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "17.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "18.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "19.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "20.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "21.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "22.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "23.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "24.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "25.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "26.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "27.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "28.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "29.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "30.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "31.172.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
zone "168.192.in-addr.arpa" { type master; file "/etc/namedb/master/empty.db"; };
*/

```

เพิ่ม zone intra.net ทั้ง forward และ reverse ก่อน บรรทัด # Start of rndc.conf

```
zone "intra.net" {
    type master;
    file "/etc/namedb/master/intra.net-for.db";
};
zone "119.168.192.in-addr.arpa" {
    type master;
    file "/etc/namedb/master/intra.net-rev.db";
};
```

หมายเหตุ : 119.168.192.in-addr.arpa ให้เปลี่ยนตาม ip ที่ท่านใช้ในเครือข่ายของท่าน

ลบ highlight สีแดง ที่ท้ายไฟล์

```
# Start of rndc.conf
key "rndc-key" {
    algorithm hmac-md5;
    secret "5gwcAsd9GVe9hBpLATf06A==";
};
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 needed:
# key "rndc-key" {
#     algorithm hmac-md5;
#     secret "5gwcAsd9GVe9hBpLATf06A==";
# };
# controls {
#     inet 127.0.0.1 port 953
#     allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
```

บันทึกไฟล์ named.conf

คัดลอก rndc.conf เป็น rndc.key

```
#cp rndc.conf rndc.key
```

แล้วแก้ไข rndc.key โดยลบส่วนที่ highlight สีแดงออก

```
#ee rndc.key
```

```
# Start of rndc.conf
key "rndc-key" {
    algorithm hmac-md5;
    secret "5gwcAsd9GVe9hBpLATf06A==";
};
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 needed:
# key "rndc-key" {
#     algorithm hmac-md5;
#     secret "9skc0Ajm3qca+hZbvlfFyA==";
# };
#
# controls {
#     inet 127.0.0.1 port 953
#         allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf

```

```

แก้ไข /etc/resolv.conf
search intra.net
nameserver 127.0.0.1

```

```

แก้ไข /etc/rc.conf
เพิ่มบรรทัด named_enable="YES"
สั่งให้ named ทำงาน
#/etc/rc.d/named start

```

Tip: หากต้องการดู error ให้ run คำสั่ง tail -f /var/log/message เพื่อดูว่า config ของเราทำงานถูกต้องหรือ error ที่บรรทัดไหน