

Langkah Konfigurasi DNS pada CentOS 7 tanpa Cpanel

DNS atau Domain Name System dapat diartikan sebagai: menerjemahkan nama host atau URL ke alamat IP. Misalnya, jika kita mengetik **domainanda.com** di browser, server DNS menerjemahkan nama domain ke alamat IP yang terkait. Karena alamat IP sulit diingat sepanjang waktu, server DNS digunakan untuk menerjemahkan nama host seperti **domainanda.com** ke 103.xxx.xx.xxx (**IP Server yang dimiliki**). Mengingat nama domain akan lebih mudah dibanding harus mengingat alamat IP.

Pada tutorial kali ini, Anda akan dibantu melakukan pengaturan DNS pada server CentOS 7. Berikut langkah-langkah yang harus dilakukan untuk melakukan konfigurasi DNS pada server dengan CentOS 7:

1. Silahkan melakukan login SSH server yang anda miliki, bisa menggunakan aplikasi putty atau aplikasi remote SSH yang biasa Anda gunakan.
2. Melakukan instalasi bind9 di server Anda dengan perintah sebagai berikut:

```
yum install bind-utils -y
```

3. Setelah melakukan instalasi bind9 silahkan melakukan edit pada file /etc/named.conf

Warning : sebelum melakukan edit file /etc/named.conf sebaiknya melakukan backup file asli /etc/named.conf dengan cara menjalankan perintah :

```
cp /etc/named.conf /etc/named.conf-backup
```

Selanjutnya, setelah melakukan backup silakan melakukan edit

file /etc/named.conf dengan menjalankan perintah:

```
vi /etc/named.conf
```

Tambahkan script seperti yang ditunjukkan dalam huruf tebal:

```
[root@server ~]# vi /etc/named.conf
```

```
dump-file "/var/named/data/cache_dump.db";  
statistics-file "/var/named/data/named_stats.txt";  
memstatistics-file "/var/named/data/named_mem_stats.txt";  
allow-query { localhost; 103.28.13.71; any; };
```

```
/*
```

```
– If you are building an AUTHORITATIVE DNS server, do NOT  
enable recursion.
```

```
– If you are building a RECURSIVE (caching) DNS server, you  
need to enable  
recursion.
```

```
– If your recursive DNS server has a public IP address, you  
MUST enable access
```

```
control to limit queries to your legitimate users. Failing to  
do so will
```

```
cause your server to become part of large scale DNS  
amplification
```

```
attacks. Implementing BCP38 within your network would greatly  
reduce such attack surface
```

```
*/
```

```
recursion yes;
```

```
dnssec-enable yes;
```

```
dnssec-validation yes;
```

```
/* Path to ISC DLV key */
```

```
bindkeys-file "/etc/named.iscdlv.key";
```

```
managed-keys-directory "/var/named/dynamic";
```

```
pid-file "/run/named/named.pid";
```

```

session-keyfile "/run/named/session.key";
};

logging {
channel default_debug {
file "data/named.run";
severity dynamic;
};
};

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

zone "domainanda.com" IN {
type master;
file "domainanda.ca";
allow-update { none;};
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

```

4. Membuat file DNS ZONE

Penambahan file DNS ZONE silahkan dilakukan pada directory /var/named/, langkah melakukan penambahan silahkan jalankan perintah :

```
vi /var/named/domainanda.ca
```

kemudian tambahkan script:

```

$ORIGIN domainanda.com.
$TTL 86400
@ IN SOA ns1.domainanda.com. root.domainanda.com. (
2001062501 ; serial

```

```
21600 ; refres
3600 ; retry
604800 ; expire
86400) ; minimum TTL
```

```
IN NS ns1.domainanda.com.
IN NS ns2.domainanda.com.
ns1 IN A 192.168.1.101
ns2 IN A 192.168.1.101
IN A 192.168.1.101
www IN A 192.168.1.101
mail IN A 192.168.1.101
```

Note: Langkah ini kami contohkan dengan nama file **domainanda.ca** sesuai dengan penambahan script pada langkah ke 2 dan untuk IP silakan ubah sesuai IP server yang anda miliki.

4. Jika sudah selesai membuat DNS ZONE silahkan lakukan perintah:

```
systemctl enable named
systemctl start named
```

5. Jika tahapan point 1-4 sudah dilakukan tinggal melakukan setting domain mengarah ke ip server dan silahkan menunggu resolved antara 1x24jam