

Lab 3: DNS

Objective:

To help students understand how DNS works and setup a Domain Name Server.

Scenario:

- Domain name: **coyote365.net**
- IP Address Range: **192.168.1.0/24**
- Servers:
 - Firewall (hadrian.coyote365.net) : 192.168.1.1**
 - DHCP server (dhcp.coyote365.net) : 192.168.1.1**
 - DNS server (ns.coyote365.net) : 192.168.1.2**
 - email server (mail.coyote365.net) : 192.168.1.3**
 - web server (www.coyote365.net) : 192.168.1.4**
 - LDAP server (ldap.coyote365.net) : 192.168.1.6**
 - Oracle server (ora.coyote365.net) : 192.168.1.7**
 - NFS server (beehive.coyote365.net) : 192.168.1.8**
 - Secure web server (sweb.coyote365.net): 192.168.1.9**
- Workstation:
 - lin.coyote365.net : 192.168.1.100**
 - win.coyote365.net : 192.168.1.101**

Preparation:

Create a Virtual Machine name “ns” and install CentOS 5.7.
You might want to copy another VM to this VM.

[1] Installation:

1-1 Required packages:

- **bind**
- **bind-utils**
- **bind-libs**

1-2 Configuration files:

/etc/named.conf
/var/named/named.ens.hosts
/var/named/named.rev.ens.hosts

1-3 Installation:

```
[root@ns /root]# yum -y install bind bind-utils bind-libs
```

[2] Configuration:

```
[root@ns /root]# cp -apr /usr/share/doc/bind-9.3.6/sample/etc/* /etc/
[root@ns /root]# cp -apr /usr/share/doc/bind-9.3.6/sample/var/named/* /var/named/
```

Edit: /etc/named.conf

```
options
{
    query-source    port 53;
    directory "/var/named"; // the default
    dump-file       "data/cache_dump.db";
    statistics-file  "data/named_stats.txt";
    memstatistics-file "data/named_mem_stats.txt";
};

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

key ddns_key
{
    algorithm hmac-md5;

    #use /usr/sbin/dns-keygen to generate TSIG keys
    secret "eDMHhnGja0gsnlBXVmIPnb1RLWksR2mDpYnEwKMu0JdkFP4uA2JEktZgSTSK";
};

view "external"
{
    match-clients      {any;}
    match-destinations {any;}
    recursion          no;
    allow-query-cache   {none;}
    include "/etc/named.root.hints";

    zone "coyote365.net" {
        type master;
        file "named.coyote365.net.hosts";
    };

    zone "1.168.192.in-addr.arpa" {
        type master;
        file "named.rev.coyote365.net.hosts";
    };
};
```

dig ns @ 198.41.0.4 > named.root

Edit: /var/named/named.coyote365.net.hosts

\$TTL 86400

```
@      IN SOA  192.168.1.2      ns.coyote365.net. (
                                2012012401    ; serial
                                3H             ; refresh
                                15M           ; retry
                                1W            ; expire
                                1D )          ; minimum
coyote365.net.      IN      NS      ns.coyote365.net.
hadrian             IN A      192.168.1.1
dhcp                IN A      192.168.1.1
ns                  IN A      192.168.1.2
mail                IN A      192.168.1.3
www                 IN A      192.168.1.4
acme                 IN A      192.168.1.5
ldap                IN A      192.168.1.6
ora                 IN A      192.168.1.7
beehive             IN A      192.168.1.8
sweb                 IN A      192.168.1.9
lin                 IN A      192.168.1.100
win                 IN A      192.168.1.101
```

Edit: /var/named/named.rev.coyote365.net.hosts

\$TTL 86400

```
@      IN      SOA      localhost.      root.localhost. (
                                2012012401    ; Serial
                                28800          ; Refresh
                                14400          ; Retry
                                3600000        ; Expire
                                86400 )       ; Minimum
@      IN      NS      localhost.
1      IN      PTR      hadrian.coyote365.net.
2      IN      PTR      ns.coyote365.net.
3      IN      PTR      mail.coyote365.net.
4      IN      PTR      www.coyote365.net.
5      IN      PTR      acme.coyote365.net.
6      IN      PTR      ldap.coyote365.net.
7      IN      PTR      ora.coyote365.net.
8      IN      PTR      beehive.coyote365.net.
9      IN      PTR      sweb.coyote365.net.
100    IN      PTR      lin.coyote365.net.
101    IN      PTR      win.coyote365.net.
```

[3] Firewall / SELinux Settings

[root@ns ~]# setup

Select "Firewall Configuration" and Select "Disabled" on SELinux Section

```
----- Firewall Configuration -----
|
| A firewall protects against unauthorized
| network intrusions. Enabling a firewall blocks
| all incoming connections. Disabling a firewall
| allows all connections and is not recommended.
|
| Security Level: (*) Enabled ( ) Disabled
|
|           SELinux:           Enforcing
|                               Permissive
|                               Disabled
|
| -----
| | OK |   | Customize |   | Cancel |
| -----
|
```

[4] Start the services:

Start DNS:

[root@ns /root]# service named restart

Start DNS on boot time:

[root@ns /root]# chkconfig named on

[5] Set your DNS client:

Edit /etc/resolv.conf

[root@ns /root]# vi /etc/resolv.conf

search coyote365.net

nameserver 192.168.1.2

[6] Testing

Check startup log:

[root@ns ~]# tail /var/log/messages

```
Feb 7 03:45:29 ns named[21116]: starting BIND 9.3.3rc2 -u named
Feb 7 03:45:29 ns named[21116]: found 1 CPU, using 1 worker thread
Feb 7 03:45:29 ns named[21116]: loading configuration from '/etc/named.conf'
Feb 7 03:45:29 ns named[21116]: listening on IPv4 interface lo, 127.0.0.1#53
Feb 7 03:45:29 ns named[21116]: listening on IPv4 interface eth0, 192.168.1.2#53
Feb 7 03:45:29 ns named[21116]: command channel listening on 127.0.0.1#953
Feb 7 03:45:29 ns named[21116]: command channel listening on ::1#953
Feb 7 03:45:29 ns named[21116]: zone 1.168.192.in-addr.arpa/IN/external: loaded serial 2008012401
Feb 7 03:45:29 ns named[21116]: zone coyote365.net/IN/external: loaded serial 2008012402
Feb 7 03:45:29 ns named[21116]: running
Feb 7 03:45:29 ns named[21116]: zone coyote365.net/IN/external: sending notifies (serial 2008020401)
Feb 7 03:45:30 ns named[21116]: client 192.168.1.2#1092: view external: received notify for zone 'coyote365.net'
```

Forward lookup test:

```
[root@ns ~]# nslookup www.coyote365.net
```

```
Server:      192.168.1.2
```

```
Address:     192.168.1.2#53
```

```
Name: ns.coyote365.net
```

```
Address: 192.168.1.2
```

Reverse lookup test:

```
[root@ns ~]# nslookup 192.168.1.2
```

```
Server:      192.168.1.2
```

```
Address:     192.168.1.2#53
```

```
2.1.168.192.in-addr.arpa    name = ns.coyote365.net.
```

[7] Adding new DNS entry: Adding mac.coyote365.net (192.168.1.102)

Edit: /var/named/ named.coyote365.net.hosts

```
$TTL 86400
```

```
@      IN SOA  192.168.1.2 ns.coyote365.net. (
                                2012012402      ; serial
                                3H                ; refresh
                                15M               ; retry
                                1W                ; expire
                                1D )             ; minimum
                                IN NS           ns.coyote365.net.
coyote365.net.
fwall      IN A      192.168.1.1
ns          IN A      192.168.1.2
mail       IN A      192.168.1.3
www        IN A      192.168.1.4
dhcp       IN A      192.168.1.5
ldap       IN A      192.168.1.6
ora        IN A      192.168.1.7
beehive    IN A      192.168.1.8
swab       IN A      192.168.1.9
lin        IN A      192.168.1.100
win        IN A      192.168.1.101
mac        IN A      192.168.1.102
```

- Serial Number increased by 1 2012012401 → 2012012502
- Last line “mac IN A 192.168.1.102” is added

Edit: /var/named/ named.rev.coyote365.net.hosts

\$TTL 86400

```
@      IN      SOA      localhost. root.localhost. (
                                2012012402          ; Serial
                                28800                ; Refresh
                                14400                ; Retry
                                3600000              ; Expire
                                86400 )              ; Minimum
@      IN      NS      localhost.
1      IN      PTR      firewall.coyote365.net.
2      IN      PTR      ns.coyote365.net.
3      IN      PTR      mail.coyote365.net.
4      IN      PTR      www.coyote365.net.
5      IN      PTR      dhcp.coyote365.net.
6      IN      PTR      ldap.coyote365.net.
7      IN      PTR      ora.coyote365.net.
8      IN      PTR      beehive.coyote365.net.
9      IN      PTR      sweb.coyote365.net.
100    IN      PTR      lin.coyote365.net.
101    IN      PTR      win.coyote365.net.
102    IN      PTR      mac.coyote365.net.
```

- Serial Number increased by 1 2011012501 → 2011012502
- Last line “111 IN PTR host11.coyote365.net.” is added

Reload DNS databases:

[root@ns ~]# service named reload

Lab 3: DNS Report

Name: _____

Team Member: _____

[1] What is purpose of DNS Server?

[2] Draw the Network diagram for DNS server and Clients.

[3] What are the advantages of DNS?

[4] What package(s) you should install in order to setup a DNS server?

[5] What command you want to use in order to setup a DNS server?

[6] Write your own named.conf, forward lookup file, and reverse lookup file for following scenario.

Scenario:

- IP Address Range: **192.168.0.0/22**
- Gateway: **192.168.0.1**
- DNS: **192.168.0.2**
- Domain name: **mycoyote365.net**
- **10 servers**
- **10 workstations**

[7] Explain how your DNS server answer to its clients when clients query the domain name such as google.com in other domain?

[8] What did you learn from this lab?

[9] Compare following commands:

- **nslookup**
- **dig**
- **host**