1.113.5
Setup and configure basic DNS services
Weight 4

Linux Professional Institute Certification — 102

Andrew Eager andrew.eager@aes-pl.com.au

Geoffrey Robertson ge@ffrey.com

Nick Urbanik nicku@nicku.org

2005 July

Outline

Contents

1 Context

Topic 113 Networking Services [24]

1.113.1 Configure and manage inetd, xinetd, and related services [4]

1.113.2 Operate and perform basic configuration of sendmail [4]

1.113.3 Operate and perform basic configuration of Apache [4]

1.113.4 Properly manage the NFS, smb, and nmb daemons [4]

1.113.5 Setup and configure basic DNS services [4]

1.113.7 Set up secure shell (OpenSSH) [4]

2 Objective

Description of Objective

Candidate should be able to configure hostname lookups and troubleshoot problems with local caching-only name server. Requires an understanding of the domain registration and DNS translation process. Requires understanding key differences in configuration files for bind 4 and bind 8.

Key files, terms, and utilities include:

/etc/hosts — file that maps host names ↔ IP addresses

/etc/resolv.conf — configuration file used to determine which name server(s) to consult

`/etc/nsswitch.conf` — tells system which order to consult various sources of naming information

`/etc/named.boot` (v.4) or `/etc/named.conf` (v.8) — configuration file for `named`.

`named` — the name server executable

3 DNS — Domain Name Service

DNS - Domain Name Service

- The internet works with numbers not names.
  `www.abc.gov.au` is really 203.2.218.61
- DNS namespace is made up of a tree of domain names.
- At the top is root (.)
- Below this is the Top Level Domain (TLD)
- Below the TLD is the Second Level Domain.
- The Second level domain is handled by whoever 'owns' that domain
- Third & lower level domains are handled by the domain owner.

DNS - Domain Name Service

- Example:

```
node1.office.my-domain.com
^       ^       ^       ^
|       |       |       |
|       |       |       -- Top level domain
|       |       -- Second level domain
|       - Subdomain
-- Hostname
```

- Domain names are fully qualified (FQDN) when a name is specified all the way down to the hostname.

4 Resolving a Name

Resolving A Name

- A name is resolved using the following steps:
  - `/etc/nsswitch.conf` is checked to see what resolution method to use (eg: read `/etc/hosts`, use dns, use nis...)
  - `nsswitch` says "use dns":
    - Read `resolv.conf` to see what name server to use
    - Send request to name server and wait for response
  - `nsswitch` says "use hosts"
    - Lookup `/etc/hosts` for a matching hostname

5 `/etc/nsswitch.conf`

The `nsswitch.conf` file

- This is a file that determines what mechanisms are used by the hostname library calls to resolve names.
- The file contains lines with an identifier followed by a list of methods to use for name lookups.
- An example:

  passwd: files nisplus nis

  shadow: files nisplus nis

  group: files nisplus nis

  hosts: db files dns

- Note that the other entries like `passwd`, `shadow` and `group` are used for other applications like `login` and have nothing to do with DNS.

The `nsswitch.conf` file

- In the hosts line, we see that any hostname to be looked up will be done in the following order:
  1. Use local databases file (.db files in `/var/db`)
  2. Read `/etc/hosts`

3. Search DNS

- The Search options can be one of:

`nisplus (or nis+)`	—	Consult NIS+ (Yellow Pages)
`nis (or yp)`	—	Consult NIS
`dns`	—	Use a DNS server
`files`	—	Use local files like `/etc/hosts`
`db`	—	Use local database files
`compat`	—	Use NIS in compat mode
`[NOTFOUND=return]`	—	Stop searching and return host notfound

An example `nsswitch` file:

```
passwd:     db files nisplus nis
shadow:     nisplus
group       db files nisplus nis

hosts:      db files nis dns

# Example - obey only what nisplus tells us...
#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files nis
protocols:  files nisplus
rpc:        files
services:   files nisplus

netgroup:   files nisplus

publickey:  nisplus
```



```
automount:  files nisplus
aliases:    files nisplus
```

6 /etc/resolv.conf

The `/etc/resolv.conf` file

- This file configures how the system uses DNS. An example:

```
search aes
nameserver 10.27.1.10
nameserver 10.27.1.254
```

- The 'search' line says what to append to a non-fully qualified name: eg: `ping node10` → `ping node10.aes`
- The `nameserver` lines tell the hostname routines which dns server to send requests to. (If first lookup fails, use the second, third)

7 BIND

BIND - Berkley Internet Name Domain

- Bind is just one implementation of a DNS. Bind is to DNS what Apache is to http.
- Bind is configured with:

  `/etc/named.conf` — For BIND V8
  `/etc/named.boot` — For BIND V4
- Know that there is a difference between V4 & V8.
- Know how to configure V8 but not V4. (Different syntax)

8 BIND configuration

BIND Configuration

- The configuration file contains subsections as follows:
  - Options → How `named` will operate
  - logging → What/how `named` will log information
  - Access Lists → Who can use `named` & what they can do
  - Remote Servers → Characteristics of remote servers
  - zones → Information about our defined domains

An Example Config file:

```
options {
        directory "/var/named/";
        forward only;
        forwarders {
            203.2.75.132;
            203.2.75.108;
        };
        query-source address * port 53;
        listen-on {
            10.27.1.10;
            127.0.0.1;
        };
        notify no;
};

#### The root zone ###
zone  "." {
        type hint;
        file  "named.ca";
};
```

An Example Config file — continued

```
#### A zone for localhost ###
zone  "0.0.127.in-addr.arpa" {
        type master;
        file  "0.0.127.in-addr.arpa.zone";
};

zone  "localhost" {
        type master;
        file  "localhost.zone";
};

### A local domain ###
zone  "1.27.10.in-addr.arpa" {
        type master;
        file  "1.27.10.in-addr.arpa.zone";
};

zone  "aes" {
        type master;
        file  "aes.zone";
};


key "key" {
        algorithm hmac-md5;
        secret "JoqlFqtncqurkhMOrrbQLYRcxSYXoNROvNTZBqWJFumleNkzOv
};
```


9 Zone Files

Zone files:

- Each zone uses a file for:
  - Hostname to IP address translations (Forward lookups)
  - IP to Hostname translatoins (Reverse lookups)
- The names can be anything, but usually:
  - Forward file → ⟨*domain*⟩.zone
  - Reverse file → ⟨*Net-IP*⟩`.in-addr.arpa`
- … where the ⟨*Net-IP*⟩ is the network part of the IP address.

9.1 Zone Records

Zone Records:

SOA record Marks the start of a zone, indicating which name server is the primary name server

NS record Defines the name server for a zone or subdomain

MX record Define mail servers for domain

CNAME record Defines an alias for a hostname

LOC record Defines the physical location of the server

SRV record Defines what services are found where (eg ftp, http etc)

A record Defines hostname to IP address translations (forward file)

PTR record Defines IP address to hostname translations (reverse file)

9.2 Example forward zone

Example Forward file `/var/named/aes.zone`

```
@       IN      SOA     node10.aes.  root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )

@       IN      NS      node10.aes.

node5   IN      MX      10      mail
node6   IN      MX      10      mail
node4   IN      MX      10      mail
node2   IN      MX      10      mail
node10  IN      MX      10      mail
gw      IN      MX      10      mail

node10  IN      A       10.27.1.10
node2   IN      A       10.27.1.2
node4   IN      A       10.27.1.4
node5   IN      A       10.27.1.5
node6   IN      A       10.27.1.6
cds     IN      A       10.27.1.99
gw      IN      A       10.27.1.254

ns      IN      CNAME   node10
mail    IN      CNAME   node10
node-4  IN      CNAME   node4
```

9.3 Example reverse zone

Example reverse file `/var/named/1.27.10.in-addr.arpa.zone`

```
@       IN      SOA     @       root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )


@       IN      NS      ns.aes.

2       IN      PTR     node2.aes.
4       IN      PTR     node4.aes.
5       IN      PTR     node5.aes.
6       IN      PTR     node6.aes.
10      IN      PTR     node10.aes.
```



```
99      IN      PTR     cds.aes.
254     IN      PTR     gw.aes.
```

10 Caching Only name server

Configuring a Caching only Nameserver

- A caching only nameserver is simple to setup. The first time a name is needed, a normal lookup occurs (Authorative) The next time that name is needed, it is returned from cache (Non-authoritative)
- Under /etc/named.conf in the options section, just make sure you have the following directives set:

```
options {
        directory "/var/named/";
        forward only;
        forwarders {
            ⟨First DNS to query⟩;
            ⟨Second DNS to query⟩;
        };
        listen-on {    ⟨Your local IP address⟩;
            127.0.0.1;
        };
```

- Leave the root zone (`.`) and localhost entries as they are.

11 Testing DNS

Testing DNS

- To test DNS, use one of the following tools:
  - `nslookup` (deprecated)
  - `dig`
  - `host`
- To use in their simplest form, just add the hostname you wish to query as the first option to the command:

```
$ nslookup node16.c223 ↩
$ dig node16.c223 ↩
$ host node16.c223 ↩
```

11.1 nslookup

nslookup

- Usage: `nslookup [option] host-to-find [-name-server]`
  Example:

  `$` **`nslookup node2.aes -10.27.1.10`** ↩

- Note: `nslookup` is deprecated and may be removed from future releases. Consider using the '`dig`' or '`host`' programs instead. Run `nslookup` with the `-sil[ent]` option to prevent this message from appearing.

```
Server:         10.27.1.10
Address:        10.27.1.10#53

Name:   node2.aes
Address: 10.27.1.2
```

11.2 dig

dig

- Usage: `dig [@name-server] host-to-find [query-type]`
- Example:

  `$` **`dig @10.27.1.10 node2.aes`** ↩

```
; «» DiG 9.2.0 «» @10.27.1.10 node2.aes
;; global options:  printcmd
;; Got answer:
;; -»HEADER«- opcode: QUERY, status: NOERROR, id: 43860
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDI

;; QUESTION SECTION:
;node2.aes.                     IN      A

;; ANSWER SECTION:
node2.aes.              86400   IN      A       10.27.1.2

;; AUTHORITY SECTION:
aes.                    86400   IN      NS      node10.aes.

;; ADDITIONAL SECTION:
```



```
node10.aes.             86400   IN      A       10.27.1.10

;; Query time: 5 msec
;; SERVER: 10.27.1.10#53(10.27.1.10)
;; WHEN: Mon Sep  2 13:48:38 2002
;; MSG SIZE  rcvd: 80
```

11.3 host

host

- Usage: `host [option] host-to-find [name-server]`
- Example:

  `$` **`host node2.aes`** ↩

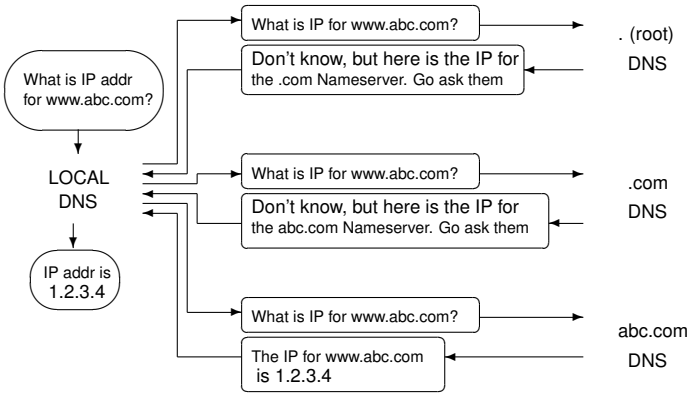
```
node2.aes has address 10.27.1.2
```

Exercise:

1. Install bind on your machine: `$` **`sudo rpm -Uvh bind-9*.rpm`** ↩
2. Configure a Caching only nameserver on your machine. (Make all queries forward to 192.168.223.254)
3. Make changes to resolv.conf & nsswitch.conf as required (Default domain to use is c223)
4. Start the named.

   `$` **`sudo service named start`** ↩
5. Test it out with the host node16.c223 using:
   - nslookup
   - dig
   - host
6. Test again this time with the host box16
7. (For those who want a DNS challenge)
   (a) Setup a set of zones for the .c223 domain.
   (b) Insert the new zone into the main configuration file
   (c) Restart the named and test it.

DNS Name Lookup Procedure



12 License Of This Document

License Of This Document