LPI 109.1 - Configure client side DNS

Curs 2021 - 2022

ASIX M01-ISO 109 Networking Fundamentals

Configure client side DNS

Description

Key concepts:

- ❏ Query remote DNS servers.
- ❏ Configure local name resolution and use remote DNS servers.
- ❏ Modify the order in which name resolution is done.
- ❏ Debug errors related to name resolution.
- ❏ Awareness of systemd-resolved.

Commands and files:

- ❏ /etc/hosts
- ❏ /etc/resolv.conf
- ❏ /etc/nsswitch.conf
- ❏ host
- ❏ dig
- ❏ getent

Configuring DNS

- static (files) : /etc/hosts
- dinàmic (dns): /etc/resolv.conf
- /etc/nsswitch

The DNS (Domain Name System) is the mapping table for the internet, allowing any computer or device to access by using a name instead of an IP address. The DNS implementation is based on a distributed database of network names and IP addresses and query interfaces to retrieve information.

/etc/hosts

- static hostnames resolution

```
$ cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.122.28  centos20
172.17.0.1      ldap.edt.org
```

/etc/resolv.conf

- The /etc/resolv.conf file is the configuration file for DNS resolvers (the client DNS part). The information in this file is normally set up by network initialization scripts.

- The configuration directives used in this file are:
    - nameserver
        - IP address of the name server that the resolver will use
        - Maximum of 3 servers can be listed
    - domain
        - Domain name to be used locally
    - search
        - Search list to be used for hostname lookup
    - sortlist
        - Allow addresses to be sorted
        - The list is specified by IP addresses and optionally the netmask
    - options
        - Used to modify the resolver's internal variables using certain keywords E.g. attempts: 3 will set the retry count for querying the name servers to 3

```
$ cat /etc/resolv.conf
# Generated by NetworkManager
search Home edt.org
nameserver 80.58.61.250
nameserver 80.58.61.254
```

/etc/nsswitch

The Name Service Switch (NSS) is used by the system administrator to specify which name information source (i.e., local files, LDAP, etc.) to use for different categories (i.e., passwd, shadow, hosts, etc.), and in which order the sources are searched.

The /etc/nsswitch.conf file is used to store the information used for name service switching. It is a text file with columns that contain the following information:

- Database name
- Lookup order of sources
- Actions permitted for the lookup result

Example fragment of /etc/nsswitch

```
passwd:     sss files systemd
shadow:     files sss
group:      sss files systemd

#hosts:     db files nisplus nis dns
hosts:      files mdns4_minimal [NOTFOUND=return] dns myhostname
```

By changing the order of the name services listed for a particular database, like hosts, the administrator could change whether the local /etc/hosts file is consulted before or after the DNS servers listed in /etc/resolv.conf.

```
hosts:        files dns
```

```
hosts:        dns files
```

```
hosts: dns [NOTFOUND=return] files
```

Querying DNS servers

The host and dig commands are used for DNS (Domain Name System) lookups, as is the nslookup command (deprecated but…). Also the getent command can be used.

Resource records types:

- A hosts
- MX mail
- NS name servers
- SOA Start of authority

The host command is used to resolve hostnames to IP addresses and IP addresses to hostnames. The utility uses UDP for transport of queries to the servers listed in the /etc/resolv.conf file.

```
$ host www.pue.es
www.pue.es is an alias for pue-app-srv.pue.es.
pue-app-srv.pue.es has address 176.34.150.171

$ host pue.es
pue.es has address 176.34.150.171
pue.es mail is handled by 10 aspmx2.googlemail.com.
pue.es mail is handled by 10 aspmx3.googlemail.com.
pue.es mail is handled by 5 alt1.aspmx.l.google.com.
pue.es mail is handled by 5 alt2.aspmx.l.google.com.
pue.es mail is handled by 1 aspmx.l.google.com.

$ host www.escoladeltreball.org
www.escoladeltreball.org is an alias for fo1.escoladeltreball.org.
fo1.escoladeltreball.org is an alias for fibra1-tel.dynalias.org.
fibra1-tel.dynalias.org has address 81.40.3.148

$ host 176.34.150.171
171.150.34.176.in-addr.arpa domain name pointer
ec2-176-34-150-171.eu-west-1.compute.amazonaws.com.

$ host -t MX gencat.cat
gencat.cat mail is handled by 5 mx1.hc489-80.eu.iphmx.com.
gencat.cat mail is handled by 20 smtp2.gencat.cat.
gencat.cat mail is handled by 10 smtp1.gencat.cat.
gencat.cat mail is handled by 5 mx2.hc489-80.eu.iphmx.com.
gencat.cat mail is handled by 30 smtp3.gencat.cat.

$ host -t NS .
. name server f.root-servers.net.
. name server b.root-servers.net.
. name server e.root-servers.net.
```

```
. name server c.root-servers.net.
. name server d.root-servers.net.
. name server i.root-servers.net.
. name server j.root-servers.net.
. name server g.root-servers.net.
. name server a.root-servers.net.
. name server h.root-servers.net.
. name server m.root-servers.net.
. name server k.root-servers.net.
. name server l.root-servers.net.
```

The dig (Domain Information Groper) command is used for troubleshooting the configuration of DNS servers. DNS server administrators like the output of the dig command because it is in the same format that the information is entered into a DNS server configuration file.

```
$ dig pue.es

; <<>> DiG 9.11.28-RedHat-9.11.28-1.fc32 <<>> pue.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7626
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1460
;; QUESTION SECTION:
;pue.es.                        IN      A

;; ANSWER SECTION:
pue.es.                 3600    IN      A       176.34.150.171

;; AUTHORITY SECTION:
pue.es.                 172800  IN      NS      ns-224.awsdns-28.com.
pue.es.                 172800  IN      NS      ns-769.awsdns-32.net.
pue.es.                 172800  IN      NS      ns-1113.awsdns-11.org.
pue.es.                 172800  IN      NS      ns-1988.awsdns-56.co.uk.

;; Query time: 274 msec
;; SERVER: 80.58.61.250#53(80.58.61.250)
;; WHEN: Wed Nov 10 21:05:27 CET 2021
;; MSG SIZE  rcvd: 191
```

```
$ dig -t NS .

; <<>> DiG 9.11.28-RedHat-9.11.28-1.fc32 <<>> -t NS .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60595
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1460
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       479194  IN      NS      j.root-servers.net.
.                       479194  IN      NS      e.root-servers.net.
.                       479194  IN      NS      d.root-servers.net.
.                       479194  IN      NS      c.root-servers.net.
.                       479194  IN      NS      m.root-servers.net.
.                       479194  IN      NS      f.root-servers.net.
.                       479194  IN      NS      k.root-servers.net.
.                       479194  IN      NS      a.root-servers.net.
.                       479194  IN      NS      l.root-servers.net.
.                       479194  IN      NS      h.root-servers.net.
.                       479194  IN      NS      g.root-servers.net.
```

```
.                       479194  IN      NS      b.root-servers.net.
.                       479194  IN      NS      i.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3560794 IN      A       198.41.0.4
b.root-servers.net.     3560794 IN      A       199.9.14.201
c.root-servers.net.     3560794 IN      A       192.33.4.12
d.root-servers.net.     3560794 IN      A       199.7.91.13
e.root-servers.net.     3560794 IN      A       192.203.230.10
f.root-servers.net.     3560794 IN      A       192.5.5.241
g.root-servers.net.     3560794 IN      A       192.112.36.4
h.root-servers.net.     3560794 IN      A       198.97.190.53
i.root-servers.net.     3560794 IN      A       192.36.148.17
j.root-servers.net.     3560794 IN      A       192.58.128.30
k.root-servers.net.     3560794 IN      A       193.0.14.129
l.root-servers.net.     3560794 IN      A       199.7.83.42
m.root-servers.net.     3560794 IN      A       202.12.27.33
a.root-servers.net.     3560794 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3560794 IN      AAAA    2001:500:200::b
c.root-servers.net.     3560794 IN      AAAA    2001:500:2::c
d.root-servers.net.     3560794 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3560794 IN      AAAA    2001:500:a8::e
f.root-servers.net.     3560794 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3560794 IN      AAAA    2001:500:12::d0d
h.root-servers.net.     3560794 IN      AAAA    2001:500:1::53
i.root-servers.net.     3560794 IN      AAAA    2001:7fe::53
j.root-servers.net.     3560794 IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     3560794 IN      AAAA    2001:7fd::1
l.root-servers.net.     3560794 IN      AAAA    2001:500:9f::42
m.root-servers.net.     3560794 IN      AAAA    2001:dc3::35

;; Query time: 7 msec
;; SERVER: 80.58.61.250#53(80.58.61.250)
;; WHEN: Wed Nov 10 21:04:35 CET 2021
;; MSG SIZE  rcvd: 811
```

```
$ dig +trace lms.pue.es
```

```
$ dig -t SOA pue.es

; <<>> DiG 9.11.28-RedHat-9.11.28-1.fc32 <<>> -t SOA pue.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32416
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;pue.es.                        IN      SOA

;; ANSWER SECTION:
pue.es.                 900     IN      SOA     ns-1113.awsdns-11.org.
awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

;; Query time: 35 msec
;; SERVER: 80.58.61.250#53(80.58.61.250)
;; WHEN: Tue Nov 16 17:25:34 CET 2021
;; MSG SIZE  rcvd: 120
```

The getent utility is used to display entries from name service databases. It can retrieve records from any source configurable by /etc/nsswitch.conf.

```
$ getent hosts
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain4
127.0.0.1       localhost localhost.localdomain localhost6 localhost6.localdomain6
```

```
192.168.122.28  centos20
```

System-resolved

Systemd provides a service called systemd-resolved. It provides mDNS, DNS, and LLMNR. When it is running, it listens for DNS requests on 127.0.0.53. It does not provide a full fledged DNS server. Any DNS requests it receives are looked up by querying servers configured in /etc/systemd/resolv.conf or /etc/resolv.conf. If you wish to use this, use resolve for hosts in /etc/nsswitch.conf. Keep in mind that the OS package that has the systemd-resolved library may not be installed by default.

Example Exercises

1. Which file is the main switch configuration file for the name resolution?
2. Which file contains the local hostnames definitions?
3. Which file contains the client DNS configuration, the resolver?
4. Show the name servers of the domain pue.es.
5. Show all the information of the FQDN lms.pue.es.

6. Realitza els exercicis indicats a: 109.4 Configure client side DNS
7. Realitza els exercicis del Question-Topics 109.4