DNS i LDAP

Autors: Joan Manuel Marquès, René Serral Gracià i Leandro Navarro.

Introducció

Aquesta sessió de problemes ens ajudarà a entendre el funcionament de DNS i el LDAP.

Objectius

- Entendre per a què funciona el servei de noms DNS
- Entendre per a què serveix LDAP
- Aprendre a distingir DNS i LDAP

Tasques

1. DNS

Per a veure el funcionament del DNS utilitzarem una comanda del Linux que ens permet fer consultes a un DNS. La comanda és **`host`**.
Aquesta comanda té molts paràmetres, aquesta pràctica només n'il·lustrarà els més importants.

1.- Resolució directa de noms

Donada l'adreça d'un lloc a Internet expressada en un nom, ens retorna l'adreça IP d'aquest lloc.

```
~$ host www.fib.upc.edu
www.fib.upc.edu has address 147.83.41.7
```

```
~$ host -v www.upc.edu
Trying "www.upc.edu"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15534
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.upc.edu.                   IN      A

;; ANSWER SECTION:
www.upc.edu.            1195    IN      CNAME   www.upc.es.
www.upc.es.             59601   IN      A       147.83.20.2

;; AUTHORITY SECTION:
upc.es.                 167539  IN      NS      euler.upc.es.
upc.es.                 167539  IN      NS      backus.upc.es.

;; ADDITIONAL SECTION:
euler.upc.es.           106034  IN      A       147.83.2.10
backus.upc.es.          106034  IN      A       147.83.2.3

Received 142 bytes from 147.83.32.3#53 in 3 ms
```

Estat de la petició

2.- Resolució inversa

Donada l'adreça IP d'un lloc, ens retorna l'adreça expressada com a nom

```
~$ host 147.83.41.11
11.41.83.147.in-addr.arpa domain name pointer xino.fib.upc.es.
```

```
~$ host -v 216.239.53.101
Trying "101.53.239.216.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9170
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;101.53.239.216.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
101.53.239.216.in-addr.arpa. 86400 IN   PTR     www.google.com.

;; AUTHORITY SECTION:
53.239.216.in-addr.arpa. 86400  IN      NS      ns1.google.com.
53.239.216.in-addr.arpa. 86400  IN      NS      ns2.google.com.
53.239.216.in-addr.arpa. 86400  IN      NS      ns3.google.com.
53.239.216.in-addr.arpa. 86400  IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         101339  IN      A       216.239.32.10
ns2.google.com.         101339  IN      A       216.239.34.10
ns3.google.com.         101339  IN      A       216.239.36.10
ns4.google.com.         101339  IN      A       216.239.38.10

Received 209 bytes from 147.83.32.3#53 in 277 ms
```

3.- Localització de servidors de correu

Activarem el flag per a fer preguntes sobre correu electrònic

```
~$ host -tMX fib.upc.edu
fib.upc.edu mail is handled by 20* mail.fib.upc.es.
fib.upc.edu mail is handled by 30 relay.upc.es.
fib.upc.edu mail is handled by 40 mail.rediris.es.
```

* Indica la prioritat del servidor.

```
~$ host -v -tMX upc.edu
Trying "upc.edu"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18802
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;upc.edu.                       IN      MX

;; ANSWER SECTION:
upc.edu.                1688    IN      MX*      10 dukas.upc.es.
upc.edu.                1688    IN      MX      20 moneo.upc.es.

;; AUTHORITY SECTION:
upc.edu.                1335    IN      NS      euler.upc.edu.
upc.edu.                1335    IN      NS      backus.upc.edu.
```

```
;; ADDITIONAL SECTION:
dukas.upc.es.           109859  IN      A       147.83.2.62
moneo.upc.es.           108001  IN      A       147.83.2.91
euler.upc.edu.          1335    IN      A       147.83.2.10
backus.upc.edu.         1335    IN      A       147.83.2.3

Received 180 bytes from 147.83.32.3#53 in 6 ms
```

*Indica registre de servidor de correu

Qüestió 1: Té sentit demanar MX d'un domini però no d'un lloc (host). Perquè?

4.- "Autoritat" dels servidors

Si consultem l'adreça d'un lloc que no està en l'àmbit d'autoritat del DNS al que demanem resoldre el nom, ens respon amb l'adreça IP del lloc amb un avís que indica que ell no és "l'autoritat" d'aquest lloc. (Això vol dir que ha tret l'adreça d'alguna *caché* i que la informació possiblement és certa, però no ens ho pot garantir en un 100%). La forma que té el sistema d'avisar-nos d'això és a través dels flags que es troben a la capçalera de la resposta:

```
~$ host -v www.ccaba.upc.edu
Trying "www.ccaba.upc.edu"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49744
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.ccaba.upc.edu.              IN      A

;; ANSWER SECTION:
www.ccaba.upc.edu.      84905   IN      CNAME   xardonay.ccaba.upc.edu.
xardonay.ccaba.upc.edu. 52141   IN      A       147.83.130.130

;; AUTHORITY SECTION:
ccaba.upc.edu.          52141   IN      NS      sert.ac.upc.edu.
ccaba.upc.edu.          52141   IN      NS      backus.upc.edu.
ccaba.upc.edu.          52141   IN      NS      xardonay.ccaba.upc.edu.

;; ADDITIONAL SECTION:
sert.ac.upc.edu.        86400   IN      A       147.83.30.70
backus.upc.edu.         305     IN      A       147.83.2.3
xardonay.ccaba.upc.edu. 52141   IN      AAAA    2001:720:810:1100:204:75ff:fe97:7bd7

Received 191 bytes from 147.83.32.3#53 in 3 ms
```

Llista de servidors autoritatius

Servidor amb IPv6

Ara veurem com podem fer per a fer la consulta directament al servidors de noms que té "autoritat" sobre el lloc web que volem consultar.

```
~$ host -v www.ccaba.upc.edu 147.83.2.3
Trying "www.ccaba.upc.edu"
Using domain server:
Name: 147.83.2.3
Address: 147.83.2.3#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65014
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3
```

Servidor on realitzem la consulta

Flag que indica resposta autoritativa

```
;; QUESTION SECTION:
;www.ccaba.upc.edu.              IN      A

;; ANSWER SECTION:
www.ccaba.upc.edu.       86400   IN      CNAME   xardonay.ccaba.upc.edu.
xardonay.ccaba.upc.edu.  86400   IN      A       147.83.130.130

;; AUTHORITY SECTION:
ccaba.upc.edu.           86400   IN      NS      xardonay.ccaba.upc.edu.
ccaba.upc.edu.           86400   IN      NS      sert.ac.upc.edu.
ccaba.upc.edu.           86400   IN      NS      backus.upc.edu.

;; ADDITIONAL SECTION:
sert.ac.upc.edu.         86400   IN      A       147.83.30.70
backus.upc.edu.          1800    IN      A       147.83.2.3
xardonay.ccaba.upc.edu.  86400   IN   AAAA    2001:720:810:1100:204:75ff:fe97:7bd7

Received 191 bytes from 147.83.2.3#53 in 8 ms
```

Qüestió 2: En quines situacions dona un resultat diferent la petició de resolució al DNS autoritatiu o a un altre diferent.

5.- Àlies

És molt habitual que a una mateixa adreça IP li corresponguin diferents noms. Un d'aquests noms és el nom principal (l'anomenen canonical). Per a que en les nostres consultes ens indiqui quin és el nom canònic del lloc que consultem, activem l'opció `CNAME` abans de demanar la resolució.

```
~$ host -tCNAME www.uoc.edu
www.uoc.edu is an alias for uoc.es.edgesuite.net.
```

Per més informació, com ja és habitual només cal activar el flag "verbose":

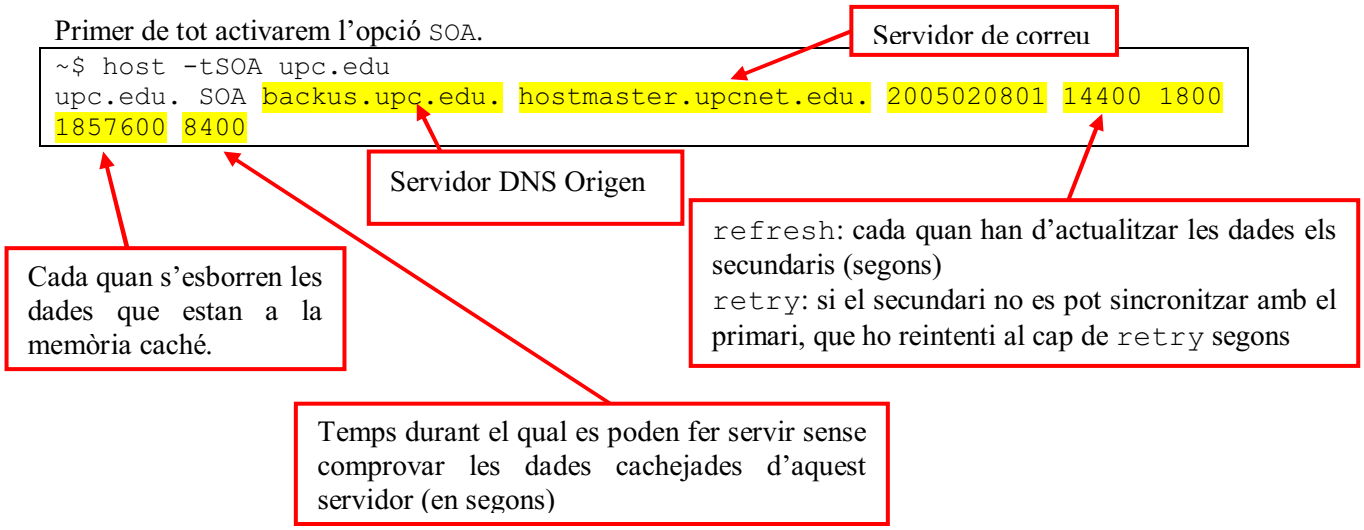
```
~$ host -v -tCNAME www.uoc.edu
Trying "www.uoc.edu"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13289
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.uoc.edu.                    IN      CNAME

;; ANSWER SECTION:
www.uoc.edu.             481     IN      CNAME   uoc.es.edgesuite.net.

;; AUTHORITY SECTION:
uoc.edu.                 33937   IN      NS      nepal.uoc.es.
uoc.edu.                 33937   IN      NS      tibet.uoc.es.

;; ADDITIONAL SECTION:
nepal.uoc.es.            33937   IN      A       213.73.40.47
tibet.uoc.es.            33937   IN      A       213.73.40.45

Received 141 bytes from 147.83.32.3#53 in 2 ms
```

6.- Informació sobre els servidors DNS (SOA)

A continuació veurem la forma d'obtenir informació sobre els servidors DNS.

Primer de tot activarem l'opció `SOA`.

```
~$ host -tSOA upc.edu
upc.edu. SOA backus.upc.edu. hostmaster.upcnet.edu. 2005020801 14400 1800
1857600 8400
```




```
~$ host -v -tSOA ibm.com
Trying "ibm.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17426
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;ibm.com.                       IN      SOA

;; ANSWER SECTION:
ibm.com.                    600     IN      SOA     ns.watson.ibm.com.
nrt.watson.ibm.com. 2005021200 3600 1800 604800 600

;; AUTHORITY SECTION:
ibm.com.                600     IN      NS      ns.austin.ibm.com.
ibm.com.                600     IN      NS      ns.watson.ibm.com.
ibm.com.                600     IN      NS      ns.almaden.ibm.com.
ibm.com.                600     IN      NS internet-server.zurich.ibm.com.

;; ADDITIONAL SECTION:
ns.austin.ibm.com.      156263  IN      A       192.35.232.34
ns.watson.ibm.com.      156263  IN      A       129.34.20.80
ns.almaden.ibm.com.     69589   IN      A       198.4.83.35
internet-server.zurich.ibm.com. 107463 IN A     195.176.20.204

Received 239 bytes from 147.83.32.3#53 in 166 ms
```

7.- Noms amb més d'una adreça IP

Hi ha llocs web que associen més d'un nom a una adreça IP. Quan es demana la resolució d'aquest nom, es rep el conjunt d'adreces IP associades.

Això s'usa per a tenir més d'una màquina que atengui un servei (p.ex. un lloc web). El receptor de les adreces, agafa la primera de la llista.

```
~$ host www.ibm.com
www.ibm.com has address 129.42.16.99
www.ibm.com has address 129.42.17.99
www.ibm.com has address 129.42.18.99
www.ibm.com has address 129.42.19.99
www.ibm.com has address 129.42.20.99
www.ibm.com has address 129.42.21.99
```

Si fem més d'una consulta al mateix lloc, ens adonarem que l'ordre de les adreces que rebem va rotant (Round Robin). Es fa així per a balancejar la càrrega. Tot i que de cops, si hi ha hagut alguna petició entre mig de les nostres podem notar que han saltat més d'una posició les IP.

```
~$ host www.cnn.com
www.cnn.com is an alias for cnn.com.
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.4
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com has address 64.236.24.28
cnn.com has address 64.236.16.20
```

Això no sempre és possible, ja que hi ha servidors que cachegen la llista d'IP i sempre retornen el mateix ordre.

```
~$ host www.cnn.com
www.cnn.com is an alias for cnn.com.
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com has address 64.236.24.28
cnn.com has address 64.236.16.20
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.4
```

(Hi ha altres tècniques per a tenir més d'un ordinador atenent un servei (p.ex. tenir un encaminador que distribueixi internament la càrrega d'atendre el servei entre diferents màquines. Externament, totes les peticions van adreçades a la mateixa adreça IP).

Qüestió 3: Quins inconvenients pot tenir el Round Robin?.

8.- Llistat de zones

Fins ara només hem fet consultes individuals de màquines, de tota manera el DNS ens permet fer consultes a zones complertes, això s'aconsegueix amb el flag –l.
El problema que té aquesta instrucció és que és necessari accedir directament a un servidor autoritatiu de la zona per motius de seguretat.

```
~$ host -l lsi.upc.edu 147.83.20.5
Using domain server:
Name: 147.83.20.5
Address: 147.83.20.5#53
```

```
Aliases:

lsi.upc.edu name server backus.upc.edu.
lsi.upc.edu name server rachael.lsi.upc.edu.
a01.lsi.upc.edu has address 147.83.200.111
.
.
.
```

Qüestió 4: Indica quins creus que són els forats de seguretat que pot provocar el fet de tenir el llistat d'una zona.

9.- Noms relatius i noms absoluts

Fins ara tots els noms que hem resolt eren relatius.

En aquest apartat farem dues consultes que no tenen solució. D'aquesta manera veurem en quins dominis fa la pregunta per a intentar resoldre el nom que li demanem.

El primer cas és un nom relatiu:

```
~$ host -v test
Trying "test.fib.upc.edu"
Trying "test"
Host test not found: 3(NXDOMAIN)
Received 97 bytes from 147.83.32.3#53 in 188 ms
```

Primer el sistema intenta resoldre el nom amb el nostre domini (ja que era un nom relatiu), tot seguit intenta la resolució com si el nom fos absolut, finalment ens informa que no existeix a la base de dades.

En aquest cas, provem amb un nom absolut:

```
~$ host -v test.
Trying "test"
Host test not found: 3(NXDOMAIN)
Received 97 bytes from 147.83.32.3#53 in 1 ms
```

Aquesta funcionalitat ens permet fer coses com:

```
~$ host www
www.fib.upc.edu has address 147.83.41.7
```

LDAP

Per a veure el funcionament del LDAP utilitzarem una comanda del Linux que ens permet fer consultes a una base de dades LDAP. La comanda és **ldapsearch**.

ldapsearch -h xano.fib.upc.es -p 9389 -b o=fib.upc.es uid=username

```
[a5s111pc32-pr_pxc]~>ldapsearch -h xano.fib.upc.es -p 9389 –b o=fib.upc.es uid=pr_pxc
dn: uid=pr_pxc, ou=PROF, o=fib.upc.es
description: Professor
gecos: Professor
gidnumber: 1032
grouprid: pxc
```

Nom únic que distingeix aquesta entrada

```
homedirectory: /home2/users/professors/pr_pxc
loginshell: /usr/local/bin/tcsh
nickname: pr_pxc
ntuid: 1007
uidnumber: 1007
uid: pr_pxc
rid: 1007
cn: pr_pxc
objectclass: top
objectclass: sambaaccount
objectclass: account
objectclass: posixaccount
objectclass: shadowaccount
objectclass: fibaccount
maquinas: fissio,fusio
uid_web: pxc
disuser: no
num_disuser: 0
```

```
[a5s111pc32-pr_pxc]~>ldapsearch -h xano.fib.upc.es -p 9389 –b o=fib.upc.es uid=pr_pxc o description
dn: uid=pr_pxc, ou=PROF, o=fib.upc.es
description: Professor
```

Enviament solució

Envieu la resposta a les qüestions plantejades al professor (en un missatge de text per grup indicant a més els noms dels membres del grup). CAL QUE EL TEMA DEL MISSATGE SIGUI: PXC-problemes sessió DNS i LDAP.

Bibliografia

- Introducció al LDAP sobre linux: http://es.tldp.org/LinuxFocus/pub/mirror/LinuxFocus/Castellano/July2000/article159.shtml
- ldapsearch man: http://www.travellingkiwi.com/docs/ldap_api/ldapsearch.htm
- ldapsearch man: http://sysadmin.cs.caltech.edu/docs/help/ldap/ldapsearch