AAD
Sessió de problemes: DNS i LDAP
(Laboratori. 1hora)

Autors: Joan Manuel Marquès 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

DNS

Per a veure el funcionament del DNS utilitzarem una comanda del Linux que ens permet fer consultes a un DNS. La comanda és **`nslookup`**.

```
 [a5s103pc25-pr_aad]~>nslookup
Default Server:  lasole.fib.upc.es   ← Servidor DNS al que estem connectats
Address:  147.83.41.104              ← adreça del servidor DNS al que estem connectats
>
```

La comanda **`help`** us donarà més informació sobre les comandes del **`nslookup`**.

```
> help
#pragma ident   "@(#)nslookup.help      1.6     96/09/12 SMI"
Commands:       (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands; see nslookup(1) for details
set OPTION      - set an option
    all         - print options, current server and host
    [no]debug   - print debugging information
    [no]d2      - print exhaustive debugging information
    [no]defname - append domain name to each query
    [no]recurse - ask for recursive answer to query
    [no]vc      - always use a virtual circuit
    domain=NAME - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME   - set root server to NAME
    retry=X     - set number of retries to X
    timeout=X   - set initial time-out interval to X seconds
    querytype=X - set query type, e.g., A,ANY,CNAME,HINFO,MX,PX,NS,PTR,SOA,TXT,W
KS
    port=X      - set port number to send query on
    type=X      - synonym for querytype
    class=X     - set query class to one of IN (Internet), CHAOS, HESIOD or ANY
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
finger [USER]   - finger the optional USER at the current default host
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -h          -  list HINFO (CPU type and operating system)
    -s          -  list well-known services
    -d          -  list all records
    -t TYPE     -  list records of the given type (e.g., A,CNAME,MX, etc.)
view FILE       - sort an 'ls' output file and view it with more
exit            - exit the program, ^D also exits
```

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.

```
> www.fib.upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Name:    xino.fib.upc.es
Address:  147.83.41.11
Aliases:  www.fib.upc.es
```

```
> www.upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Name:    www.upc.es
Address:  147.83.20.2
```

2.- Resolució inversa

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

```
> 147.83.41.11
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Name:    xino.fib.upc.es
Address:  147.83.41.11
```

```
> 216.239.53.101
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Name:    www.google.com
Address:  216.239.53.101
```

3.- Localització de servidors de correu

Activarem l'opció per a fer preguntes sobre correu electrònic

```
> set type=MX
```

Preguntem pels servidors de correu electronic d'un domini

```
> fib.upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

fib.upc.es      preference = 20, mail exchanger = dukas.upc.es
fib.upc.es      preference = 30, mail exchanger = belcebu.upc.es
fib.upc.es      preference = 40, mail exchanger = mail.rediris.es
fib.upc.es      nameserver = lasole.fib.upc.es
fib.upc.es      nameserver = ada.fib.upc.es
fib.upc.es      nameserver = backus.upc.es
fib.upc.es      nameserver = khachaturian.upc.es
fib.upc.es      nameserver = gaudi.ac.upc.es
dukas.upc.es    internet address = 147.83.2.62
belcebu.upc.es  internet address = 147.83.2.63
```

Prioritat en l'ús del servidor de correu (com més petit el número, més prioritari)

Servidors correu de la FIB

Servidors DNS de la FIB

```
mail.rediris.es internet address = 130.206.1.2
lasole.fib.upc.es       internet address = 147.83.41.104
ada.fib.upc.es  internet address = 147.83.41.6
backus.upc.es   internet address = 147.83.2.3
khachaturian.upc.es     internet address = 147.83.2.206
gaudi.ac.upc.es internet address = 147.83.32.3
```

```
> upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

upc.es  preference = 30, mail exchanger = mail.rediris.es
upc.es  preference = 10, mail exchanger = dimoni.upc.es
upc.es  preference = 10, mail exchanger = belcebu.upc.es
upc.es  nameserver = euler.upc.es
upc.es  nameserver = ineco.nic.es
upc.es  nameserver = backus.upc.es
mail.rediris.es internet address = 130.206.1.2
belcebu.upc.es  internet address = 147.83.2.63
euler.upc.es    internet address = 147.83.2.10
ineco.nic.es    internet address = 194.69.254.2
backus.upc.es   internet address = 147.83.2.3
```

Tornem al mode “normal” de consulta

```
> set type=A
```

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%)

```
> www.google.com
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Non-authoritative answer:
Name:    www.google.com
Address:  216.239.53.101
```

```
> www.uoc.edu
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Non-authoritative answer:
Name:    campus.uoc.es
Address:  213.73.40.217
Aliases:  www.uoc.edu
```

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.

Primer de tot, activarem el mode `debug` per a el resultat de la consulta ens doni més informació.

```
> set debug
```

```
> www.uoc.edu
Server:  lasole.fib.upc.es
Address:  147.83.41.104

;; res_nmkquery(QUERY, www.uoc.edu, IN, A)
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2442, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 2,  additional
= 3

    QUESTIONS:
        www.uoc.edu, type = A, class = IN
    ANSWERS:
    ->  www.uoc.edu
        canonical name = campus.uoc.es
        ttl = 67762 (18h49m22s)
    ->  campus.uoc.es
        internet address = 213.73.40.217
        ttl = 51156 (14h12m36s)
    AUTHORITY RECORDS:
    ->  uoc.es
        nameserver = NEPAL.uoc.es
        ttl = 3051 (50m51s)
    ->  uoc.es
        nameserver = tibet.uoc.es
        ttl = 3051 (50m51s)
    ADDITIONAL RECORDS:
    ->  NEPAL.uoc.es
        internet address = 213.73.40.10
        ttl = 3051 (50m51s)
    ->  NEPAL.uoc.es
        internet address = 193.146.196.6
        ttl = 3051 (50m51s)
    ->  tibet.uoc.es
        internet address = 213.73.40.9
        ttl = 77481 (21h31m21s)

------------
Non-authoritative answer:
Name:    campus.uoc.es
Address:  213.73.40.217
Aliases:  www.uoc.edu
```

DNS amb autoritat sobre www.uoc.edu

Ara que ja sabem el DNS que té autoritat sobre el lloc web `www.uoc.edu`, tornarem a demanar que ens resolguin el nom, però fent la consulta a un dels DNS que tenen autoritat sobre `www.uoc.edu`.

Primer de tot, i per a que la resposta sigui més curta ja que no ens interessen certs detalls, desactivem el mode `debug`.

```
>set nodebug
```

```
> www.uoc.edu tibet.uoc.es
Server:  tibet.uoc.es
Address:  213.73.40.9

Name:    campus.uoc.es
Address:  213.73.40.217
Aliases:  www.uoc.edu
```

Servidor DNS al que preguntem (diferent del que tenim configurat com "per defecte")

Ja no ens apareix: `Non-authoritative answer:`

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.

```
> set type=CNAME
```

```
> www.fib.upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

www.fib.upc.es  canonical name = xino.fib.upc.es
fib.upc.es      nameserver = lasole.fib.upc.es
fib.upc.es      nameserver = ada.fib.upc.es
fib.upc.es      nameserver = backus.upc.es
fib.upc.es      nameserver = khachaturian.upc.es
fib.upc.es      nameserver = gaudi.ac.upc.es
lasole.fib.upc.es       internet address = 147.83.41.104
ada.fib.upc.es  internet address = 147.83.41.6
backus.upc.es   internet address = 147.83.2.3
khachaturian.upc.es     internet address = 147.83.2.206
gaudi.ac.upc.es internet address = 147.83.32.3
```

Tornem al mode "normal" de consulta

```
> set type=A
```

Ara veurem en el mode `debug` també ens informa del nom canònic del lloc que consultem.

```
> set debug
```

```
> www.fib.upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

;; res_nmkquery(QUERY, www.fib.upc.es, IN, A)
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2449, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion
avail.
        questions = 1,  answers = 2,  authority records = 5,  additional
= 5
```

```
    QUESTIONS:
        www.fib.upc.es, type = A, class = IN
    ANSWERS:
    ->  www.fib.upc.es
        canonical name = xino.fib.upc.es
        ttl = 172800 (2D)
    ->  xino.fib.upc.es
        internet address = 147.83.41.11
        ttl = 172800 (2D)
    AUTHORITY RECORDS:
    ->  fib.upc.es
        nameserver = lasole.fib.upc.es
        ttl = 172800 (2D)
    ->  fib.upc.es
        nameserver = ada.fib.upc.es
        ttl = 172800 (2D)
    ->  fib.upc.es
        nameserver = backus.upc.es
        ttl = 172800 (2D)
    ->  fib.upc.es
        nameserver = khachaturian.upc.es
        ttl = 172800 (2D)
    ->  fib.upc.es
        nameserver = gaudi.ac.upc.es
        ttl = 172800 (2D)
    ADDITIONAL RECORDS:
    ->  lasole.fib.upc.es
        internet address = 147.83.41.104
        ttl = 172800 (2D)
    ->  ada.fib.upc.es
        internet address = 147.83.41.6
        ttl = 172800 (2D)
    ->  backus.upc.es
        internet address = 147.83.2.3
        ttl = 172800 (2D)
    ->  khachaturian.upc.es
        internet address = 147.83.2.206
        ttl = 172800 (2D)
    ->  gaudi.ac.upc.es
        internet address = 147.83.32.3
        ttl = 3681 (1h1m21s)

------------
Name:    xino.fib.upc.es
Address:  147.83.41.11
Aliases:  www.fib.upc.es
```

```
> set nodebug
```

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`.

```
> set type=SOA
```

```
> upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

upc.es
        origin = backus.upc.es
        mail addr = hostmaster.upcnet.es
        serial = 2002101511
        refresh = 86400 (1D)
        retry   = 7200 (2H)
        expire  = 2592000 (4w2d)
        minimum ttl = 172800 (2D)
upc.es  nameserver = euler.upc.es
upc.es  nameserver = ineco.nic.es
upc.es  nameserver = backus.upc.es
euler.upc.es    internet address = 147.83.2.10
ineco.nic.es    internet address = 194.69.254.2
backus.upc.es   internet address = 147.83.2.3
```

`refresh`: cada quan han d'actualitzar les dades els secundaris (segons)
`retry`: si el secundari no es pot sincronitzar amb el primari, que ho reintenti al cap de `retry` segons

← servidor de correu

Cada quan s'esborren les dades que estan a la memòria cau (cachejades)

temps durant el qual es poden fer servir sense comprovar les dades cachejades d'aquest servidor (en segons)

```
> ibm.com
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Non-authoritative answer:
ibm.com
        origin = ns.watson.ibm.com
        mail addr = nrt.watson.ibm.com
        serial = 2002101500
        refresh = 3600 (1H)
        retry   = 1800 (30M)
        expire  = 604800 (1W)
        minimum ttl = 600 (10M)

Authoritative answers can be found from:
ibm.com nameserver = ns.watson.ibm.com
ibm.com nameserver = ns.austin.ibm.com
ibm.com nameserver = ns.almaden.ibm.com
ibm.com nameserver = internet-server.zurich.ibm.com
ns.watson.ibm.com       internet address = 198.81.209.2
ns.austin.ibm.com       internet address = 192.35.232.34
ns.almaden.ibm.com      internet address = 198.4.83.35
internet-server.zurich.ibm.com  internet address = 195.176.20.204
```

Tornem al mode "normal" de consulta

```
> set type=A
```

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.

```
> www.ibm.com
Server:  lasole.fib.upc.es
Address:  147.83.41.104
```

```
Non-authoritative answer:
Name:    www.ibm.com
Addresses:  129.42.19.99, 129.42.16.99, 129.42.17.99, 129.42.18.99
```

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.

```
> www.cnn.com
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Non-authoritative answer:
Name:    cnn.com
Name:    cnn.com
Addresses:  64.236.24.28, 64.236.16.20, 64.236.16.52, 64.236.16.84
          64.236.16.116, 64.236.24.4, 64.236.24.12, 64.236.24.20
Aliases:  www.cnn.com
```

```
> www.cnn.com
Server:  lasole.fib.upc.es
Address:  147.83.41.104

Non-authoritative answer:
Name:    cnn.com
Addresses:  64.236.24.12, 64.236.24.20, 64.236.24.28, 64.236.16.20
          64.236.16.52, 64.236.16.84, 64.236.16.116, 64.236.24.4
Aliases:  www.cnn.com
```

(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.- set d2

Ara veurem que hi ha un mode que ens dóna molta informació sobre les consultes que realitzem. És un nivel de depuració més alt.

```
> set d2
```

```
> www.ac.upc.es
Server:  lasole.fib.upc.es
Address:  147.83.41.104

;; res_nmkquery(QUERY, www.ac.upc.es, IN, A)
------------
SendRequest(), len 31
    HEADER:
        opcode = QUERY, id = 47616, rcode = NOERROR
        header flags:  query, want recursion
        questions = 1,  answers = 0,  authority records = 0,  additional
= 0

    QUESTIONS:
        www.ac.upc.es, type = A, class = IN
```

```
------------
------------
Got answer (107 bytes):
    HEADER:
        opcode = QUERY, id = 47616, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 1,  additional
= 1

    QUESTIONS:
        www.ac.upc.es, type = A, class = IN
    ANSWERS:
    ->  www.ac.upc.es
        type = CNAME, class = IN, dlen = 13
        canonical name = bautravers.ac.upc.es
        ttl = 3101 (51m41s)
    ->  bautravers.ac.upc.es
        type = A, class = IN, dlen = 4
        internet address = 147.83.30.80
        ttl = 3101 (51m41s)
    AUTHORITY RECORDS:
    ->  ac.upc.es
        type = NS, class = IN, dlen = 7
        nameserver = sert.ac.upc.es
        ttl = 172800 (2D)
    ADDITIONAL RECORDS:
    ->  sert.ac.upc.es
        type = A, class = IN, dlen = 4
        internet address = 147.83.30.70
        ttl = 172800 (2D)

------------
Non-authoritative answer:
Name:    bautravers.ac.upc.es
Address:  147.83.30.80
Aliases:  www.ac.upc.es
```

9.- Noms relatius i noms absoluts

Ara que ja tenim activat el mode de depuració més alt, provarem la diferència entre 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:

```
> www.ft.fr
Server:  lasole.fib.upc.es
Address:  147.83.41.104

;; res_nmkquery(QUERY, www.ft.fr, IN, A)
------------
SendRequest(), len 27
    HEADER:
        opcode = QUERY, id = 47617, rcode = NOERROR
```

Intenta resoldre suposant que hem proporcionat un nom complet

```
        header flags:  query, want recursion
        questions = 1,  answers = 0,  authority records = 0,  additional
= 0

    QUESTIONS:
        www.ft.fr, type = A, class = IN

------------
------------
Got answer (75 bytes):
    HEADER:
        opcode = QUERY, id = 47617, rcode = NXDOMAIN
        header flags:  response, auth. answer, want recursion, recursion
avail.
        questions = 1,  answers = 0,  authority records = 1,  additional
= 0

    QUESTIONS:
        www.ft.fr, type = A, class = IN
    AUTHORITY RECORDS:
    ->  fr
        type = SOA, class = IN, dlen = 36
        ttl = 86400 (1D)
        origin = ns1.nic.fr
        mail addr = nic.nic.fr
        serial = 2002101600
        refresh = 21600 (6H)
        retry   = 3600 (1H)
        expire  = 3600000 (5w6d16h)
        minimum ttl = 86400 (1D)

------------
;; res_nmkquery(QUERY, www.ft.fr.fib.upc.es, IN, A)
------------
SendRequest(), len 38
    HEADER:
        opcode = QUERY, id = 47618, rcode = NOERROR
        header flags:  query, want recursion
        questions = 1,  answers = 0,  authority records = 0,  additional
= 0

    QUESTIONS:
        www.ft.fr.fib.upc.es, type = A, class = IN

------------
------------
Got answer (87 bytes):
    HEADER:
        opcode = QUERY, id = 47618, rcode = NXDOMAIN
        header flags:  response, auth. answer, want recursion, recursion
avail.
        questions = 1,  answers = 0,  authority records = 1,  additional
= 0

    QUESTIONS:
        www.ft.fr.fib.upc.es, type = A, class = IN
    AUTHORITY RECORDS:
```

Intenta resoldre suposant que ens haviem descuidat del domini. Afegeix el nostre domini per defecte: `fib.upc.es`

```
    ->  fib.upc.es
        type = SOA, class = IN, dlen = 37
        ttl = 86400 (1D)
        origin = lasole.fib.upc.es
        mail addr = xarxa.fib.upc.es
        serial = 2002101011
        refresh = 10800 (3H)
        retry   = 3600 (1H)
        expire  = 172800 (2D)
        minimum ttl = 86400 (1D)

------------
*** lasole.fib.upc.es can't find www.ft.fr: Non-existent host/domain
```

Ens informa que no l'ha trobat

En aquest cas, provem amb un nom absolut:

```
> www.ft.fr.
Server:  lasole.fib.upc.es
Address:  147.83.41.104

;; res_nmkquery(QUERY, www.ft.fr, IN, A)
------------
SendRequest(), len 27
    HEADER:
        opcode = QUERY, id = 47619, rcode = NOERROR
        header flags:  query, want recursion
        questions = 1,  answers = 0,  authority records = 0,  additional
= 0

    QUESTIONS:
        www.ft.fr, type = A, class = IN

------------
------------
Got answer (75 bytes):
    HEADER:
        opcode = QUERY, id = 47619, rcode = NXDOMAIN
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional
= 0

    QUESTIONS:
        www.ft.fr, type = A, class = IN
    AUTHORITY RECORDS:
    ->  fr
        type = SOA, class = IN, dlen = 36
        ttl = 10735 (2h58m55s)
        origin = ns1.nic.fr
        mail addr = nic.nic.fr
        serial = 2002101600
        refresh = 21600 (6H)
        retry   = 3600 (1H)
        expire  = 3600000 (5w6d16h)
        minimum ttl = 86400 (1D)

------------
*** lasole.fib.upc.es can't find www.ft.fr.: Non-existent host/domain
```

Intenta resoldre el nom absolut

Ens informa que no l'ha trobat

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_aad]~>ldapsearch -h xano.fib.upc.es -p 9389 -b
o=fib.upc.es uid=pr_aad
dn: uid=pr_aad, ou=PROF, o=fib.upc.es
description: Professor
gecos: Professor
gidnumber: 1032
grouprid: aad
homedirectory: /home2/users/professors/pr_aad
loginshell: /usr/local/bin/tcsh
nickname: pr_aad
ntuid: 1007
uidnumber: 1007
uid: pr_aad
rid: 1007
cn: pr_aad
objectclass: top
objectclass: sambaaccount
objectclass: account
objectclass: posixaccount
objectclass: shadowaccount
objectclass: fibaccount
maquinas: fissio,fusio
uid_web: aad
disuser: no
num_disuser: 0
```

Nom únic que distingeix aquesta entrada

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

Enviament solució

Envieu la resposta a les qüestions plantejades a: aad@ac.upc.es (en un missatge de text per grup indicant a més els noms dels membres del grup). CAL QUE EL **TEMA** DEL MISSATGE SIGUI: **AAD-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