

LPIC2 2021 Sesión 9 (2021-03-02)

Documentación relacionada:

- Manual Certificación LPIC-2.pdf, pag XX
- Material Practicas LPIC-2/LPIC-202/
- Presentaciones/2020/202/
- gdrive://

Clase

DNS

DNS: Laboratorio

continuación de [dnslaboratorio](#)

- ficheros de configuración para el master del servidor DNS

[named.conf](#)

```
options {
    directory "/var/named"; %//% aunque esté enjaulado, no lo sabe...
    forwarders{
        8.8.8.8;
        8.8.4.4;
    };
    allow-transfer{
        192.168.2.152;
    };
    allow-notify {192.168.2.152;};
};

zone "." {
    type hint;
    file "named.ca";
};

zone "curso.esp"{
    type master;
    allow-update {
        192.168.2.0/24;
    };
    file "db.curso";
};

zone "2.168.192.IN-ADDR.ARPA"{
    type master;
    allow-update {
        192.168.2.0/24;
```

```
};  
file "db.192.168.2";  
};
```

db.curso

```
$ORIGIN .  
$TTL 259200 ; 3 days  
curso.esp      IN SOA      sercentos7.curso.esp. root.curso.esp. (  
                2021022502 ; serial  
                86400      ; refresh (1 day)  
                7200       ; retry (2 hours)  
                2592000    ; expire (4 weeks 2 days)  
                172800    ; minimum (2 days)  
                )  
                NS       orion.curso.esp.  
                NS       sercentos7.curso.esp.  
                MX       3 trasgu.curso.esp.  
$ORIGIN curso.esp.  
agendapc5      CNAME     pc5  
curso          A       192.168.2.3  
fresnosa       CNAME     trasgu  
localhost      A       127.0.0.1  
pc2            A       192.168.2.8  
pc3            A       192.168.2.10  
portalpc12     CNAME     pc12  
portatil       A       192.168.2.2  
trasgu         A       192.168.2.150  
orion          A       192.168.2.152  
webalizerpc12 CNAME     pc12  
sercentos7     A       192.168.2.5
```

db.192.168.2

```
$TTL 259200 ; 3 days  
2.168.192.IN-ADDR.ARPA. IN SOA      sercentos7.curso.esp. root.curso.esp. (  
                2021022501 ; serial  
                86400      ; refresh (1 day)  
                7200       ; retry (2 hours)  
                2592000    ; expire (4 weeks 2 days)  
                172800    ; minimum (2 days)  
                )  
2.168.192.IN-ADDR.ARPA. NS       orion.curso.esp.  
2.168.192.IN-ADDR.ARPA. NS       sercentos7.curso.esp.  
2.168.192.IN-ADDR.ARPA. MX       3 sercentos7.curso.esp.  
  
150            IN       PTR       trasgu.curso.esp.  
5              IN       PTR       sercentos7.curso.esp.  
152           IN       PTR       orion.curso.esp.  
8             IN       PTR       pc2.curso.esp.
```

named.ca

```

; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>"
; configuration file of BIND domain name servers).
;
; This file is made available by InterNIC
; under anonymous FTP as
; file /domain/named.cache
; on server FTP.INTERNIC.NET
; -OR- RS.INTERNIC.NET
;
; last update: Jan 29, 2004
; related version of root zone: 2004012900
;
;
; formerly NS.INTERNIC.NET
;
. 3600000 IN NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4
;
; formerly NS1.ISI.EDU
;
. 3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A 192.228.79.201
;
; formerly C.PSI.NET
;
. 3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
;
; formerly TERP.UMD.EDU
;
. 3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 A 128.8.10.90
;
; formerly NS.NASA.GOV
;
. 3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A 192.203.230.10
;
; formerly NS.ISC.ORG
;
. 3600000 NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000 A 192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
. 3600000 NS G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET. 3600000 A 192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
. 3600000 NS H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET. 3600000 A 128.63.2.53
;
; formerly NIC.NORDU.NET

```

```
;
.           3600000      NS      I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET. 3600000      A       192.36.148.17
;
; operated by VeriSign, Inc.
;
.           3600000      NS      J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET. 3600000      A       192.58.128.30
;
; operated by RIPE NCC
;
.           3600000      NS      K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET. 3600000      A       193.0.14.129
;
; operated by ICANN
;
.           3600000      NS      L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET. 3600000      A       198.32.64.12
;
; operated by WIDE
;
.           3600000      NS      M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET. 3600000      A       202.12.27.33
; End of File
```

[/etc/resolv.conf](#)

```
nameserver 192.168.2.5
nameserver 192.168.2.152
search curso.esp
domain curso.esp
```

- **/etc/sysconfig/network-scripts/icfg-enp0s3:**

```
PEERDNS=No
DNS1=<IP_DNS>
DNS2=<IP_DNS>
```

- para que no sobrescriba el **resolv.conf** (el DHCP o Vagrant) y mantenga los DNS que yo le diga
- dig

DNS: Laboratorio

- DOC: Material Practicas LPIC-2/LPIC-202/1-Domain Name Server/2-Laboratorio DNS RedHat7.pdf

- ```
options {
 directory "/var/named";
 forwarders{
 8.8.8.8;
 192.168.2.1;
 };
 // allow-transfer{
 // 192.168.2.5;
```

```
// 192.168.2.3;
// };
//
};

zone "." {
 type hint;
 file "named.ca";
};
zone "curso.esp"{
 type slave;
 file "slaves/db.curso";
 masters { 192.168.2.5; };
};

zone "2.168.192.IN-ADDR.ARPA"{
 type slave;
 file "slaves/db.192.168.2";
 masters { 192.168.2.5; };
};

};
```

- [/etc/resolv.conf](#)

```
nameserver 192.168.2.5
search curso.esp
domain curso.esp
```

- cp named.ca /var/named/chroot/var/named/
- cp named.conf /var/named/chroot/etc/
- mkdir /var/named/chroot/var/named/slaves
- chmod -R 770 /var/named/chroot/var/named/slaves
- chown -R named:named /var/named/chroot/var/named/slaves
- service named restart ← centos6 sin systemctl

## DNS (continuación)

- masterfile-format:
  - indica en que formato se transfieren las zonas desde el master: text,raw,map
  - [https://fpngenred.es/DNS/estamento\\_masterfileformat.html](https://fpngenred.es/DNS/estamento_masterfileformat.html)
- dig (pag.262),nslookup,host
  - host -t NS curso.esp
- DOC: Manual Certificacion LPIC-2.pdf, pag. 254
- añadir nueva zona esclava en el master:

```
zone "nombrezona" {
 type slave;
 masters { 192.168.x.x; };
 file "db.miempresa.com";
 masterfile-format text;
};
```

- añadir a **named.conf** para que escuche en un puerto/ip determinados:

```
options {
 directory "/var/named";
 listen-on port 53 { IP_escucha; };
 forwarders{
 8.8.8.8;
 8.8.4.4;
 };
};
```

## DNSSEC

- DOC: (pag. 267), (pag. 17 - laboratorio dns)
- **allow-transfer { acl };**
- **allow-query { acl };**
- **listen-on { acl };**
- **blackhole { acl };**
- **allow-notify { acl };**
- acl:

```
acl redlocal {
 192.168.0.150;
 127.0.0.1;
 192.168.2.0/24;
};
```

- valores predefinidos en la sección acl:
  - any
  - localhost
  - localnets
  - none
- ejemplo parcial **named.conf**:

```
acl redlocal {
 localnets;
};

acl yomismo {
 localhost;
};

acl parias {
 192.168.2.152;
};

options {
 directory "/var/named";
 forwarders{
 8.8.8.8;
 8.8.4.4;
 };
 allow-transfer{
 192.168.2.152;
 };
 allow-notify {192.168.2.152;};
};
```

```
//allow-query { redlocal; };
allow-query { yomismo; };
//blackhole { parias; };

};
```

- yomismo: no permite a un cliente resolver, con un mensaje de **REFUSED**
- parias: no responde (ni se logea) a una petición de un cliente
- redlocal: funciona correctamente
- cuenta de servicio:
  - usuario propio
  - sin shell → /sbin/nologin
  - enjaular el proceso
  - intercambio seguro entre servidores
- TSIG (Transaction SIGnature)
  - DOC: (pag. 270) (pag.9)
  - dnssec-keygen
    - **-a HMAC-MD5**: único algoritmo de cifrado soportado
    - **-b <tamaño>**: (1-512), 128 suficiente
    - **-n <propiedad>**: **HOST** para indicar que la seguridad va máquina a máquina
    - <nombreclave>

## laboratorio TSIG

- en el master:

```
dnssec-keygen -r /dev/random -a HMAC-MD5 -b 128 -n HOST curso.esp # genera
.key y .private
chmod 400 Kcurso.esp*
chown named.named Kcurso.esp*
cat Kcurso*.key # llave pública
```

- editar **named.conf** y añadir:

```
key curso.esp {
algorithm HMAC-MD5;
secret "8WaWHvdoCSNH/ZhBFWbP9w==";
};
```

- y modificar:

```
allow-transfer { key curso.esp; };
```

- systemctl restart named-chroot
- en el esclavo, **named.conf**:

```
key curso.esp {
algorithm HMAC-MD5;
secret "8WaWHvdoCSNH/ZhBFWbP9w==";
};
server 192.168.1.150 {
keys { curso.esp; };
};
```

- eliminamos las zonas transferidas (para ver que funciona) en el esclavo
- service named restart

```
Mar 2 20:26:41 sercentos7 systemd: Started Berkeley Internet Name Domain (DNS).
Mar 2 20:26:41 sercentos7 named[5154]: zone curso.esp/IN: sending notifies (serial 2021022502)
Mar 2 20:26:41 sercentos7 named[5154]: zone 2.168.192.IN-ADDR.ARPA/IN: sending notifies (serial 2021022501)
Mar 2 20:26:52 sercentos7 named[5154]: client @0x7f90240f7cb0 192.168.2.152#47935/key curso.esp (2.168.192.IN-ADDR.ARPA): transfer of '2.168.192.IN-ADDR.ARPA/IN': AXFR started: TSIG curso.esp (serial 2021022501)
Mar 2 20:26:52 sercentos7 named[5154]: client @0x7f90240f7cb0 192.168.2.152#47935/key curso.esp (2.168.192.IN-ADDR.ARPA): transfer of '2.168.192.IN-ADDR.ARPA/IN': AXFR ended
Mar 2 20:26:53 sercentos7 named[5154]: client @0x7f9026ee0d00 192.168.2.152#40125/key curso.esp (curso.esp): transfer of 'curso.esp/IN': AXFR started: TSIG curso.esp (serial 2021022502)
Mar 2 20:26:53 sercentos7 named[5154]: client @0x7f9026ee0d00 192.168.2.152#40125/key curso.esp (curso.esp): transfer of 'curso.esp/IN': AXFR ended
```

## MIRAR

- laboratorio DDNS
- DDoS (pag. 20)
  - consultas recursivas: [https://fpngenred.es/DNS/consulta\\_recursiva.html](https://fpngenred.es/DNS/consulta_recursiva.html)
  - **allow-recursions**

From:  
<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:  
<https://miguelangel.torresegea.es/wiki/info: cursos: pue: lpic2-2021:s9?rev=1614715332>

Last update: **02/03/2021 12:02**

