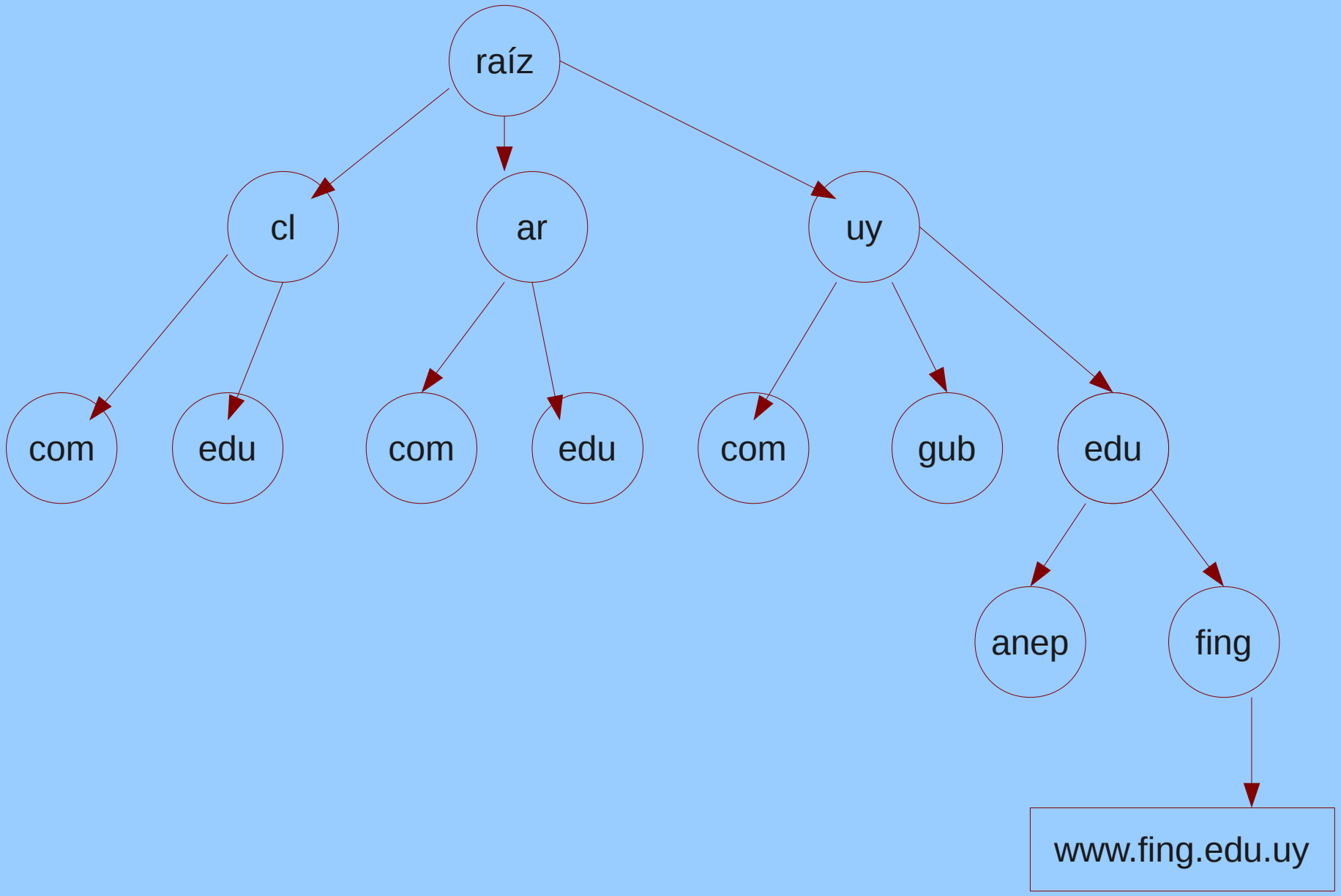
DNS

- Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usado por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet.
- Esta organizado en un órden jerarquico.


raíz
cl
ar
uy
com
edu
com
edu
com
gub
edu
anep
fing
www.fing.edu.uy

DNS

- En una organización que tenga uno o mas servidores web, o servidor de correo, debe tener funcionando un servidor DNS.
- Con un servidor DNS correctamente funcionando el resto del mundo podrá acceder a los servicios ofrecidos por la organización.

INSTALACIÓN

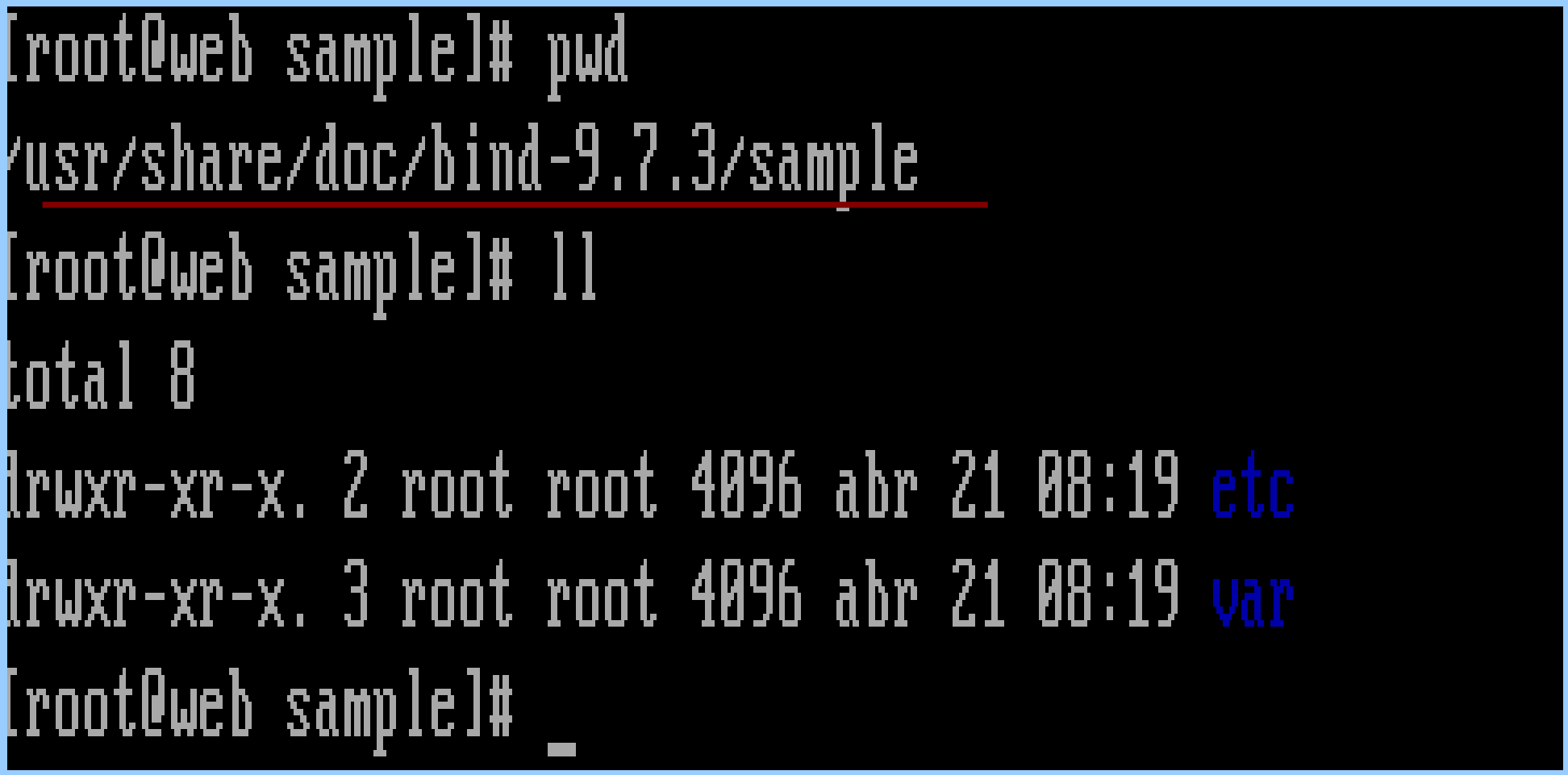
SERVIDOR DNS EN CENTOS 6
BIND9

Paquetes de bind

```
[root@www ~]# yum -y install bind-chroot bind-libs bind bind-utils_
```

```
[root@web ~]# rpm -qa |grep ^bind-
bind-chroot-9.7.3-2.el6.i686
bind-libs-9.7.3-2.el6.i686
bind-9.7.3-2.el6.i686
bind-utils-9.7.3-2.el6.i686
[root@web ~]# _
```

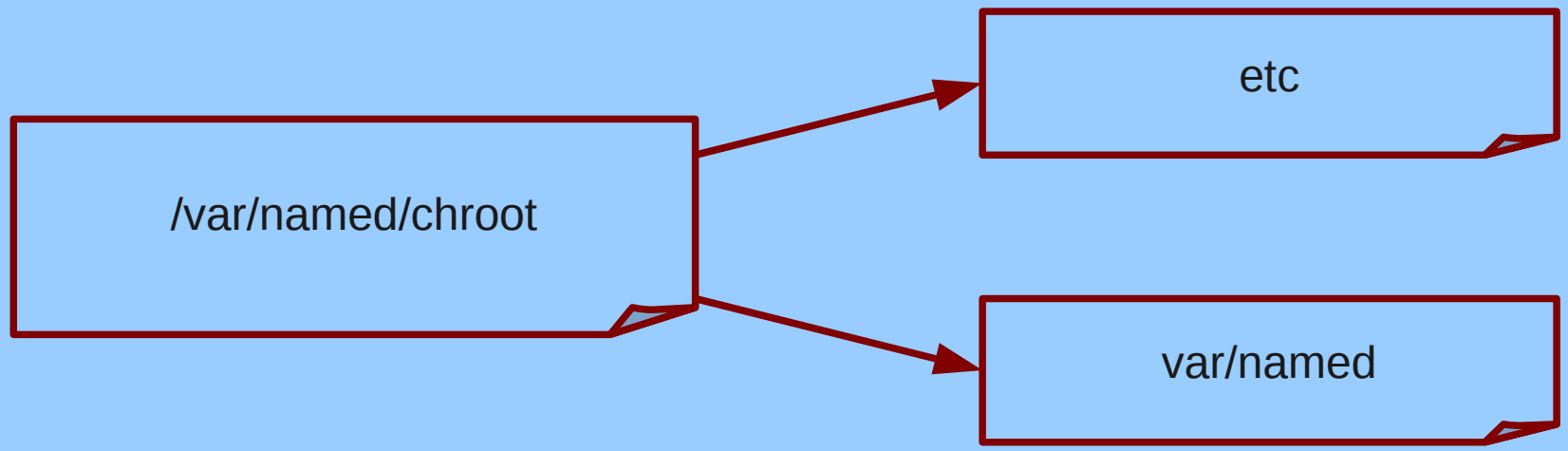
Archivos


[root@web sample]# pwd
/usr/share/doc/bind-9.7.3/sample
[root@web sample]# ll
total 8
drwxr-xr-x. 2 root root 4096 abr 21 08:19 etc
drwxr-xr-x. 3 root root 4096 abr 21 08:19 var
[root@web sample]# _

Copiar los archivos

```
[root@web sample]# ls etc/
named.conf  named.rfc1912.zones
[root@web sample]# cp etc/* /var/named/chroot/etc/
[root@web sample]# ls var/named/
data                my.internal.zone.db  named.empty     named.loopback
my.external.zone.db  named.ca            named.localhost  slaves
[root@web sample]# cp -r var/named/* /var/named/chroot/var/named/
[root@web sample]# _
```

Directorio de configuración



Directorio de configuración /var/named/chroot/etc

```
[root@web sample]# cd /var/named/chroot/etc/
[root@web etc]# ll
total 24
-rw-r--r--. 1 root root  3519 abr 21 08:22 localtime
drwxr-x---. 2 root named 4096 jul 19  2011 named
-rw-r--r--. 1 root root  7687 abr 21 08:46 named.conf
-rw-r--r--. 1 root root   931 abr 21 08:46 named.rfc1912.zones
drwxr-xr-x. 3 root root  4096 abr 21 08:22 pki
[root@web etc]# _
```

Creación de las zonas

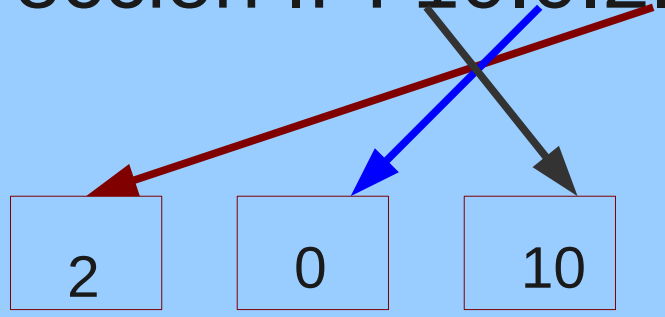
- En el archivo named.conf se configuran el comportamiento general del DNS. Este incluye el archivo named.rfc1912.zones, en el cual se definen las zonas de autoridad.
- Se define la zona de autoridad con el nombre, el tipo y el pais: solange.edu.uy
- Luego la zona inversa, donde se define la dirección IP.

named.rfc1912.zones

- **zone** “solange.edu.uy” - nombre de la zona.
- **type** “master” - tipo, puede ser master o slave.
- **file** “named.solange” - archivo donde estarán los datos de los hosts.
- **allow-update** – si se actualiza o no, en el caso de un master nunca se actualiza.

named.rfc1912.zones

- **zone “2.0.10.in-addr.arpa”**
- Esta configuración se realiza descartando el último valor de la dirección IP, y dando vuelta el valor.
- Dirección IP: 10.0.2.15



named.rfc1912.zones

```
zone "solange.edu.uy" IN {
        type master;
        file "named.solange";
        allow-update { none; };
};

zone "2.0.10.in-addr.arpa" IN {
        type master;
        file "named.solange.rev";
        allow-update { none; };
};
```

Archivo named.conf

Modificaciones a realizar:

- En la configuración predeterminada solo está habilitada la consulta local.
- Incluir en las consultas externas la configuración de la zona.
- Generar e incluir la clave.
- Comentar las zonas no utilizadas.

named.conf
Habilitar las consultas

```
 //listen-on port 53     { any; };
 listen-on port 53       { 127.0.0.1; };

*/
listen-on port 53        { any; };
listen-on port 53        { 127.0.0.1; };
```

named.conf
Habilitar las consultas

```
//allow-query          { localhost; };
allow-query            { localhost; any; };
allow-query-cache      { localhost; any; };
```

named.conf
Incluir zona externa

```
view "external"
{
/* This view will contain zones you want to serve only to "external" clients
 * that have addresses that are not match any above view:
 */
        include "/etc/named.rfc1912.zones";
```

Generar la clave

```
[root@web etc]# dnssec-keygen -a hmac-md5 -b 128 -n HOST host1
```

```
[root@web etc]# ls
Khost1.+157+63863.key       localtime  named.conf           pki
Khost1.+157+63863.private   named      named.rfc1912.zones
```

```
[root@web etc]# cat Khost1.+157+63863.private
Private-key-format: v1.3
Algorithm: 157 (HMAC_MD5)
Key: l6mQeY9EDkWkkO0akx4JZA==
Bits: AAA=
Created: 20120421123252
Publish: 20120421123252
Activate: 20120421123252
[root@web etc]#
```

Incluir la clave en named.conf

```
Key: l6mQeY9EDkWkk00akx4JZA==
```

```
key ddns_key
{
        algorithm hmac-md5;
        secret "l6mQeY9EDkWkk00akx4JZA==";
};
```

named.conf
Comentar las zonas

```
//      zone "my.internal.zone" {
//              type master;
//              file "my.internal.zone.db";
//      };
//      zone "my.slave.internal.zone" {
//              type slave;
//              file "slaves/my.slave.internal.zone.db";
//              masters { /* put master nameserver IPs here */ 127.0.0.1; } ;
//              // put slave zones in the slaves/ directory so named can update
them
//      };
//      zone "my.ddns.internal.zone" {
//              type master;
//              allow-update { key ddns_key; };
//              file "dynamic/my.ddns.internal.zone.db";
//              // put dynamically updateable zones in the slaves/ directory so
named can update them
//      };
```

```
//      zone "my.external.zone" {
//              type master;
//              file "my.external.zone.db";
//      };
```

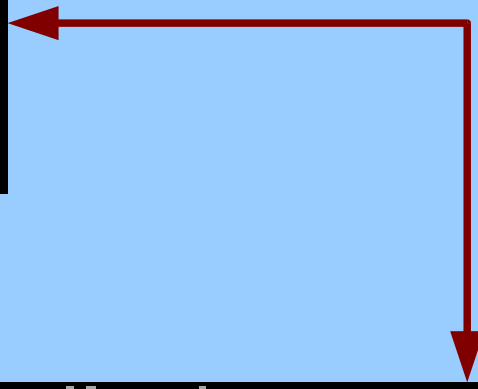
Archivos de zona

- Se deben crear los dos archivos de zona definidos en el archivo named.rfc1912.zones
- Directorio: /var/named/chroot/var/named

Archivo de zona

/var/named/chroot/etc/named.rfc1912.zones

```
zone "solange.edu.uy" IN {
        type master;
        file "named.solange";
        allow-update { none; };
};
```



```
[root@web named]# pwd
/var/named/chroot/var/named
[root@web named]# ls
data                named.ca          named.loopback    slaves
my.external.zone.db  named.empty       named.solange
my.internal.zone.db  named.localhost   named.solange.rev
[root@web named]# _
```

Tipos de registros

	Tipo	Nombre	Función
Zona	SOA	Start Of Authority	Define una zona representativa del DNS
	NS	Name Server	Identifica los servidores de zona.
Básicos	A	Dirección IPv4	Traducción de nombre a dirección
	PTR	Puntero	Traducción de dirección a nombre
	MX	Mail eXchanger	Controla el enrutado del correo
Opcional	LOC	Localización	Localización geográfica y extensión
	RP	Persona responsable	Especifica la persona de contacto de cada host
	SRV	Servicios	Proporciona la localización de servicios conocidos
	TXT	Texto	Comentarios o información sin cifrar

named.solange
archivo de zona

```
$TTL 1D
@       IN SOA  solange.edu.uy. root.local (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns1.solange.edu.uy.
web     IN      A       10.0.2.15
ns1     IN      A       10.0.2.15
```

named.solange.rev
archivo de zona

```
$TTL 1D
@       IN SOA  2.0.10.in-addr.arpa. root.local (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      ns1.solange.edu.uy.
15      PTR     ns1.solange.edu.uy.
```

Propietario

- El servicio named se ejecuta con el usuario del sistema named.
- Se debe modificar los archivos para que le pertenezcan a este usuario y su grupo.

/var/named/chroot

```
[root@web chroot]# pwd
/var/named/chroot
[root@web chroot]# ll
total 16
drwxr-x---. 2 root named 4096 abr 21 08:22 dev
drwxr-x---. 4 root named 4096 abr 21 09:06 etc
drwxr-xr-x. 3 root root  4096 abr 21 08:22 usr
drwxr-x---. 6 root named 4096 abr 21 08:22 var
[root@web chroot]# chown -R named.named etc/  var/
[root@web chroot]# _
```

Pasos finales

- Crear el archivo /var/named/chroot/etc/rndc.key con la misma clave de named.conf. Este archivo habilita la utilización del front-end **rndc**.
- Crear los enlaces simbólicos.
- Chequear la configuración.
- Iniciar el servicio.
- Configurar los clientes.

Crear el archivo rndc.key

```
[root@web etc]# pwd
/var/named/chroot/etc
[root@web etc]# cat rndc.key
key "dnsadmin" {
        algorithm hmac-md5;
        secret "l6mQeY9EDkWkkO0akx4JZA==";
};

[root@web etc]# _
```

Enlaces simbólicos

```
ln -s /var/named/chroot/etc/named.conf          /etc/named.conf
ln -s /var/named/chroot/etc/named.rfc1912.zones /etc/named.rfc1912.zones
ln -s /var/named/chroot/etc/rndc.key            /etc/rndc.key
```

Chequear la configuración

```
[root@web named]# cd /var/named/chroot/var/named/
[root@web named]# pwd
/var/named/chroot/var/named
[root@web named]# ls
data                    named.ca          named.loopback     slaves
my.external.zone.db     named.empty       named.solange
my.internal.zone.db     named.localhost   named.solange.rev
[root@web named]# named-checkzone solange.edu.uy named.solange
zone solange.edu.uy/IN: loaded serial 0
OK
[root@web named]# named-checkzone 2.0.10.in-addr.arpa named.solange.rev
zone 2.0.10.in-addr.arpa/IN: loaded serial 0
OK
[root@web named]# named-checkconf
[root@web named]# _
```

Levantar el servicio

```
[root@web named]# service named start
Iniciando named:                                           [  OK  ]
[root@web named]# rndc status
version: 9.7.3-RedHat-9.7.3-2.el6
CPUs found: 1
worker threads: 1
number of zones: 50
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/0/1000
tcp clients: 0/100
server is up and running
[root@web named]# chkconfig named on
[root@web named]# _
```

Configurar los clientes

```
[root@web etc]# cat /etc/resolv.conf
nameserver 10.0.2.15
[root@web etc]# _
```

Consultas al DNS

```
[root@web etc]# host -a solange.edu.uy
Trying "solange.edu.uy"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56075
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;solange.edu.uy.                        IN      ANY

;; ANSWER SECTION:
solange.edu.uy.         86400   IN      SOA     solange.edu.uy. root.local.solan
ge.edu.uy. 0 86400 3600 604800 10800
solange.edu.uy.         86400   IN      NS      ns1.solange.edu.uy.

;; ADDITIONAL SECTION:
ns1.solange.edu.uy.     86400   IN      A       10.0.2.15

Received 113 bytes from 10.0.2.15#53 in 8 ms
[root@web etc]# host ns1.solange.edu.uy
ns1.solange.edu.uy has address 10.0.2.15
[root@web etc]# host 10.0.2.15
15.2.0.10.in-addr.arpa domain name pointer ns1.solange.edu.uy.
[root@web etc]# _
```

Agregar el servidor de correo

- El servidor de correo se especifica con el registro **MX.**
- Una vez funcionando el DNS, se pueden agregar nuevos hosts modificando los archivos de zona.
- Luego con el comando **rndc reload** se actualiza el servidor sin tener que reiniciarlo.

Archivos de zona

```
$TTL 1D
@       IN SOA  solange.edu.uy. root.local (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns1.solange.edu.uy.
web     IN      A       10.0.2.15
ns1     IN      A       10.0.2.15
www     IN      A       10.0.2.16
@               IN      MX      10      correo
correo  IN      A 10.0.2.17
```

```
$TTL 1D
@       IN SOA  2.0.10.in-addr.arpa. root.local (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      ns1.solange.edu.uy.
15      PTR     ns1.solange.edu.uy.
16      PTR     www.solange.edu.uy.
17      PTR     correo.solange.edu.uy.
```

rndc reload

```
[root@web named]# rndc reload
server reload successful
[root@web named]# host -a solange.edu.uy
Trying "solange.edu.uy"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58880
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;solange.edu.uy.                        IN      ANY

;; ANSWER SECTION:
solange.edu.uy.         86400   IN      MX      10 correo.solange.edu.uy.
solange.edu.uy.         86400   IN      SOA     solange.edu.uy. root.local.solan
ge.edu.uy. 0 86400 3600 604800 10800
solange.edu.uy.         86400   IN      NS      ns1.solange.edu.uy.

;; ADDITIONAL SECTION:
correo.solange.edu.uy.  86400   IN      A       10.0.2.17
ns1.solange.edu.uy.     86400   IN      A       10.0.2.15

Received 152 bytes from 10.0.2.15#53 in 11 ms
[root@web named]# host -t MX solange.edu.uy
solange.edu.uy mail is handled by 10 correo.solange.edu.uy.
[root@web named]# _
```

DNS SECUNDARIO

DNS SECUNDARIO (SLAVE)

- Un servidor DNS puede tener muchas consultas o fallar.
- Por este motivo es conveniente tener un servidor secundario con la misma información del master.
- De esta forma se reparte la carga de las consultas, cuando el master no responde los clientes consultan al slave.

Configuración

- El Slave obtendrá los registros de zona del Master. Si luego modifica el Master solo debe actualizar el Slave para que esten sincronizados.
- Se debe modificar el Master para que envie los datos al Slave.
- Al Slave se debe configurar para que pida los registros del Master.

Configuración

- El Slave tendrá los mismos archivos del directorio: /var/named/chroot/etc
- Se pueden copiar los archivos de forma segura utilizando: **scp origen destino**
- Solo se modificará el archivo: **named.rfc1912.zones** una vez copiado.

Copiar los archivos

- Para copiar los archivos necesitamos el servicio sshd levantado en los dos hosts.
- service sshd start

```
[root@web etc]# scp named.* rndc.key  10.0.2.27:/var/named/chroot/etc/
```

named.rfc1912.zones

```
zone "solange.edu.uy" IN {
        type slave;
        file "named.solange";
        masters {10.0.2.15;  };
};

zone "2.0.10.in-addr.arpa" IN {
        type slave;
        file "named.solange.rev";
        masters { 10.0.2.15; };
};
```

Configuración Slave

- Hay que recordar los pasos realizados en la configuración del master.
- Links simbólicos
- Propietario.

Master named.rfc1912.zones

- Habilitar la transferencia al Slave

```
zone "solange.edu.uy" IN {
        type master;
        file "named.solange";
        allow-update { none; };
        allow-transfer { 10.0.2.77; };
};

zone "2.0.10.in-addr.arpa" IN {
        type master;
        file "named.solange.rev";
        allow-transfer { 10.0.2.77; };
        allow-update { none; };
};
```

Paso final

- Reinciar el Master
- Iniciar el Slave
- Si todo funciono bien en el directorio /var/named/chroot/var/named deben aparecer los archivos de zona.
- Comprobar la configuración con un cliente incluyendo en el archivo /etc/resolv.conf la dirección del Slave.


DNS
Domain Name System