

# Tarea 1.1



## Index

1. ¿Qué directivas son las más utilizadas en el cliente DNS?.....	3
2. Observa la siguiente imagen y contesta a las preguntas:.....	4
3. Crea el archivo para la zona inversa a partir de la siguiente imagen:.....	5
4. Averigua qué es DDNS y para qué sirve.....	5
5. Averigua qué diferencia existe entre la utilidad named-checkconf y la utilidad named-checkzone, y cómo has de ejecutarlas para verificar que todas las modificaciones hechas sobre el archivo named.conf han sido correctas.....	5
6. En un registro SOA, ¿qué significa el refresh interval? ¿Y expire?.....	5
7. Investiga la sintaxis de las órdenes más utilizadas desde el terminal para realizar consultas DNS:.....	6

## 1. ¿Qué directivas son las más utilizadas en el cliente DNS?

- **Administración de tráfico basada a nivel geográfico:** Es tener en referencia el servidor más cercano a ti que te pueda dar los datos que busques en una petición, (*Entiendo que el propósito a través de esto es optimizar envíos de información y demás*).
- **Equilibrio de carga:** Esta directiva hace que, para resumir, las peticiones recibidas se distribuyan de manera óptima en una aplicación, (*A mi entender, un método de para que la aplicación sea más óptima a la hora de trabajar*).
- **Split Brain DNS:** Es básicamente, tener dos versiones de una zona DNS, una a nivel interno y otra a nivel externo, (*por lo que he entendido, básicamente esto se utiliza a nivel de depuramiento y control de errores de una zona DNS, una zona de pruebas y otra ya arreglada para recibir peticiones y ser en general, funcional*).
- **Filtrado de consultas:** A mi entender, este método funciona para que a la hora de que se envíen consultas DNS, se puedan filtrar para evitar entiendo yo, que sean modificadas esas peticiones para reducir el riesgo de que tus usuarios les envíen URIs chungas, eso o en si mismo que tus usuarios te envíen basura que tu no quieres.
- **Redireccionamiento según la hora del día:** Entiendo que es agarrar y reducir la escalabilidad de tu red y demás según la hora del día basándose en que horas tus clientes están activos o no.
- **Análisis forense:** A mi entender, se refiere a que agarra y el servidor hace análisis de las peticiones para poder actuar en consecuencia, sea para proteger al servidor, sea para que nadie se envíe en la petición de un cliente y le envíen.

## 2. Observa la siguiente imagen y contesta a las preguntas:

```
mcgrawSRI.lan. IN SOA servidor1.mcgrawSRI.lan. admin.mcgrawSRI.lan (1242759044 10800
3600 604800 38400 )
mcgrawSRI.lan.      IN  NS servidor1.mcgrawSRI.lan.
mcgrawSRI.lan.      IN  NS servidor2.mcgrawSRI.lan.
mcgrawSRI.lan.      IN  MX 10 192.168.123.123
servidor1.mcgrawSRI.lan. IN A      192.168.123.123
servidor2.mcgrawSRI.lan. IN A      192.168.123.123
pc1.mcgrawSRI.lan.  IN  A      192.168.123.101
pc2.mcgrawSRI.lan.  IN  A      192.168.123.102
www.mcgrawSRI.lan.  IN  CNAME  servidor1.mcgrawSRI.lan.
ftp.mcgrawSRI.lan.  IN  CNAME  servidor1.mcgrawSRI.lan.
smtp.mcgrawSRI.lan. IN  CNAME  servidor1.mcgrawSRI.lan.
```

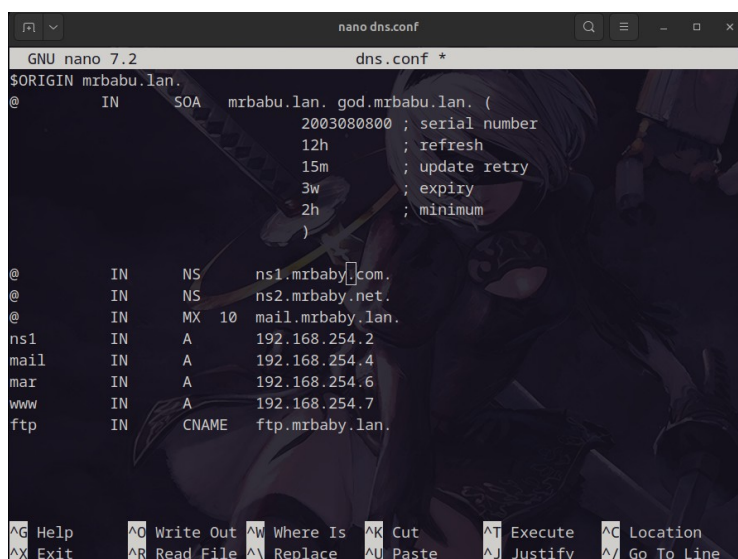
- ¿Qué tipo de zona tenemos creada? zona directa
- ¿Cómo se llama el nombre de dominio? mcgrawSRI.lan
- ¿Cuál es el correo de contacto? admin.mcgrawSRI.lan
- ¿Cuántos tipos de registros hemos creado? 5 (entendiendo que se refiere individualmente a SOA, NS, A...)

¿Qué hace cada uno de ellos?

1. **SOA:** Es el registro de una zona DNS en general, sirve para almacenar todo por lo que he entendido.
2. **NS:** Sirve para guardar el nombre de dominio
3. **MX:** Sirve para dirigir la dirección donde va el correo.
4. **A:** Registro que se usa para almacenar la IP de un dominio.
5. **CNAME:** Entiendo que esto es rollo agarrar, y sustituir un nombre por la URI cuando se busca para que pongan en el sitio deseado (*para que se entienda, rollo cuando buscar en el navegador twitter.com, y ahora que cambiaron el nombre, te redirigen a x.com*)

### 3. Crea el archivo para la zona inversa a partir de la siguiente imagen:

```
$ORIGIN mcgrawSRI.lan.  
@ IN SOA servidor1 admin (1242759044 10800 3600 604800 38400)  
@ IN NS servidor1  
@ IN NS servidor2  
@ IN MX 10 192.168.123.123  
servidor1 IN A 192.168.123.123  
servidor2 IN A 192.168.123.124  
Pc1 IN A 192.168.123.101  
Pc2 IN A 192.168.123.102  
www IN CNAME servidor1  
ftp IN CNAME servidor1  
smtp IN CNAME servidor1
```



```
GNU nano 7.2 dns.conf *  
$ORIGIN mrbabu.lan.  
@ IN SOA mrbabu.lan. god.mrbabu.lan. (  
    2003080800 ; serial number  
    12h ; refresh  
    15m ; update retry  
    3w ; expiry  
    2h ; minimum  
)  
@ IN NS ns1.mrbabu.com.  
@ IN NS ns2.mrbabu.net.  
@ IN MX 10 mail.mrbabu.lan.  
ns1 IN A 192.168.254.2  
mail IN A 192.168.254.4  
mar IN A 192.168.254.6  
www IN A 192.168.254.7  
ftp IN CNAME ftp.mrbabu.lan.
```

### 4. Averigua qué es DDNS y para qué sirve

Es el DNS dinámico, entiendo que su uso es, tanto facilitar y arreglar problemas con el DHCP como hacer más cómodo el acceso a los registros a través de peticiones aunque estes utilizando diferentes Ips (*entiendo que cuando haces login, capaz y según la IP podría haber conflictos raros*).

### 5. Averigua qué diferencia existe entre la utilidad named-checkconf y la utilidad named-checkzone, y cómo has de ejecutarlas para verificar que todas las modificaciones hechas sobre el archivo named.conf han sido correctas.

- **named-checkconf:** Se centra en ver que el archivo named.conf funcione bien en su sintaxis y no tenga problemas
- **named-checkzone:** Se centra en comprobar que en la zona DNS, los archivos estén bien, ver si dan algún error o algo.

### 6. En un registro SOA, ¿qué significa el refresh interval? ¿Y expire?

- **refresh interval:** Es un tiempo en segundos en el que actualiza si han habido cambios en el server dns, y eso lo utiliza para enviarle al dns secundario los cambios.
- **Expire:** Entiendo que se refiere al tiempo en segundos en el que el dns esta en disposición de recibir cambios, y si en un rato pasado el tiempo la zona secundaria no recibe nada, se carga la zona secundaria actual (*capaz y me he colado un poco*)

## 7. Investiga la sintaxis de las órdenes más utilizadas desde el terminal para realizar consultas DNS:

- **Ping:** Sirve para comprobar la conectividad y latencia de una IP existente, y para ver si en si mismo, esta en la red.
- **Host:** En ámbito DNS, entiendo que se refiere que el lugar donde se guardan los registros de los nombres de dominio.
- **Dig:** Sirve para hacer búsquedas de registros DNS.
- **Nslookup:** Por lo visto también se usa para sacar búsquedas de registros DNS, pero un poco menos amplio.
- **whois:** Entiendo que, es un comando que se utiliza para sacar información de un dominio o host a través de una IP.
- **Fping:** Sirve para agarrar y listar los dispositivos conectados a la red