

## **Planificación:**

Durante el proyecto del Sprint 1, se ha ido consultando el manual y hemos ido realizando y analizando los archivos a manipular, directorios de importancia y configuraciones.

De forma simultánea, hemos ido variando entre buscar información y realizar acciones dentro del contenedor.

Cuando estuvimos dentro del contenedor, realizamos pasos previos (siendo superusuario):

- *apt update*
- *apt upgrade*
- *apt install bind9*
- *systemctl status bind9* (verificar si el servicio está activo)

Con esto teníamos una base sentada. Además, cada vez que manipulemos un archivo del servicio, haremos una copia original a modo de backup con “*cp archivo.conf archivo.conf.backup*”.

**IMPORTANTE:** En /etc/bind está el archivo principal de configuración de BIND9 llamado “*named.conf*”. Hay que procurar que contenga la siguiente línea (en caso contrario habrá que crearla):

```
include "/etc/bind/named.conf.local";  
include "/etc/bind/named.conf.options";
```

Después, ejecuta el siguiente comando y, si no te devuelve nada, indica que todo va bien:

```
named-checkconf /etc/bind/named.conf
```

## Actividades a realizar:

- **Configuración de un servidor primario (*master*).**

Configuramos el archivo *named.conf.local* para incluir la zona del servidor primario (1) “nexustek.asix” y la zona inversa (2):

```
//  
// Do any local configuration here  
  
//  
  
zone "nexustek.asix" { 1  
    type master;  
    file "/var/cache/bind/db.master.nexustek.asix";  
};  
  
zone "150.16.172.in-addr.arpa" { 2  
    type master;  
    file "/var/cache/bind/db.master.172.16.150";  
};
```

- **Configurar directivas globales - \*Observar Siguiente Apartado\*;**
- **Características del servidor (*named.conf.options*):**
  - **Consultas recursivas; aceptar consultas y conseguir y devolver respuestas.**  
*recursion yes;*
  - **Consultas recursivas SOLAMENTE a los equipos conectados a la misma red del servidor.**  
*allow-recursion { 172.16.150.0/24; 127.0.0.1; };*
  - **Ocultar información sobre la versión de BIND.**  
*version "no disponible";*
  - **Directorio de resolución de rutas relativas.**  
*directory "/var/cache/bind";*
  - **Servidor escucha por puerto por defecto de DNS.**  
*listen-on port 53 { any; };*
  - **Prohibir transferencias de zonas a hosts a nivel global; desde cada zona solo permitir a equipos de interés.**  
*allow-transfer { none; };*

RESULTADO FINAL DE *named.conf.options*:

```
GNU nano 8.4
options {
    // Directorio de resolucion de rutas relativas
    directory "/var/cache/bind";

    // Seguridad - verificación de autenticidad
    dnssec-validation auto;

    // Consultas recursivas
    recursion yes;
    allow-recursion { 172.16.150.0/24; 127.0.0.1; };

    // Ocultar versión BIND
    version "no disponible";

    // Permitir consultas
    allow-query { any; };

    // Escuchar por puerto por defecto DNS
    listen-on port 53 { any; };

    // Prohibir transferencias de zonas a hosts a nivel global
    allow-transfer { none; };
};
```

Después, ejecuta los siguientes comandos y, si cada uno no te devuelve nada, indica que todo va bien:

```
named-checkconf /etc/bind/named.conf.Local
named-checkconf /etc/bind/named.conf.options
```

- **Configurar servidor *master* autoritario para el dominio (incluyendo su zona inversa).**

Nos ubicamos en `/var/cache/bind` y crearemos aquí el archivo de registros llamado “`db.master.nexustek.asix`”. Dentro tendremos que poner lo siguiente: (las líneas con ‘;;’ son comentarios)

```
$TTL 2d
$ORIGIN nexustek.asix.

;; // --Registro SOA-- //
@ IN SOA ns1.master.nexustek.asix. hostmaster.master.nexustek.asix. (
    2003080800 ; serial number
    12h         ; refresh
    15m         ; update retry
    3w         ; expiry
    2h         ; minimun
)
;; IP de nexustek.asix.
@ IN A 172.16.150.203

;; // --Servidores-- //
;; Nombre del servidor "ns1"
@ IN NS ns1.nexustek.asix.
;; Nombre del servidor de correo "mail"
@ IN MX 10 mail.nexustek.asix.

;; // --IP's-- //
;; IP del servidor "ns1"
ns1 IN A 172.16.150.203
;; IP del servidor de correo "mail"
mail IN A 172.16.150.204
```

Después, se deberá de realizar los siguientes comandos (verificamos y probamos el servidor DNS):

```
systemctl restart bind9
named-checkzone [servidor] [archivo de registros]
```

```
root@vbox:/var/cache/bind# systemctl restart bind9
root@vbox:/var/cache/bind# named-checkzone nexustek.asix db.master.nexustek.asix
zone nexustek.asix/IN: loaded serial 2003080800
OK
```

Si da “OK”, eso indica que estamos yendo bien.

Ahora, creamos el archivo “*db.master.172.16.150*”. Dentro tendremos que poner lo siguiente:

```
$TTL 2d
$ORIGIN 150.16.172.in-addr.arpa.

;; // --Registro SOA-- //
@ IN SOA ns1.master.nexustek.asix. hostmaster.master.nexustek.asix. (
    2003080800 ; serial number
    12h        ; refresh
    15m        ; update retry
    3w        ; expiry
    2h        ; minimun
)
;; // --Servidores-- //
;; Nombre del servidor "ns1"
@ IN NS ns1.nexustek.asix.

;; // --PUNTEROS-- //
;; Puntero a la IP del servidor "ns1"
203 IN PTR ns1.nexustek.asix.
;; Puntero a la IP del servidor de correo "mail"
204 IN PTR mail.nexustek.asix.
```

Después, repetiremos los comandos de antes ajustando la ejecución a este archivo:

```
root@vbox:/var/cache/bind# systemctl restart bind9
root@vbox:/var/cache/bind# named-checkzone 150.16.172.in-addr.arpa db.master.172.16.150
zone 150.16.172.in-addr.arpa/IN: loaded serial 2003080800
OK
```

Si da “OK”, eso indica que estamos yendo bien.

- Configurar servidor *master* para que la zona “*intranet.nexustek.asix*” delegue gestión del subdominio en el DNS del controlador de dominio.  
Dentro del archivo “*db.master.nexustek.asix*” añadimos al final las siguientes líneas:

```
;; subdominio
$ORIGIN int.nexustek.asix.
    IN      NS      dc01
dc01    IN      A       172.16.150.220
```

Reiniciamos BIND9 el comando “*systemctl restart bind9*” y pasaremos a realizar unos comandos de comprobación:

```
dig @localhost ns1.nexustek.asix
dig @localhost mail.nexustek.asix
dig @localhost dc01.int.nexustek.asix
dig -x 172.16.150.203 @localhost
```

Al hacer los comandos, en cada uno nos tendrá que salir una parte en la que ponga “*; ; ANSWER SECTION:*”. Esta parte muestra la respuesta de la petición hecha con DIG.

- **OPCIONAL - Crear script en bash para gestionar zonas ‘A’ del DNS.**

## Dificultades:

Tuvimos dificultades menores cuya causa era el desconocimiento (dónde declarar el servidor, cómo poner los registros, etc...).

Sin embargo, tuvimos un problema grave y fue la delegación de subdominio por parte de la zona “*intranet.nexustek.asix*”, ya que, habiendo hecho varias pruebas y búsquedas, y no haber disponido del tiempo suficiente, no fuimos capaces de desarrollar este objetivo obligatorio.

## Documentación o enlaces de referencia usados:

- PDFs y enlaces aportados por el profesor correspondiente (incluyendo el manual de BIND9)
- ChatGPT - [Analizar Sprint 1](#)

*iOJO! - ChatGPT no se usó para copiarse, sino para guiarse.*