Índice

Actividad 1 – Uso de herramientas dig, host y nslookup

1. Introducción

Las herramientas *dig, host o nslookup* son utilizadas para comprobar las **configuraciones DNS** establecidas sobre un **determinado dominio** de forma que podemos llevar a cabo el diagnóstico de posibles problemas que puedan ocurrir. A lo largo de la práctica identificaremos las principales opciones y funcionalidades de las herramientas y nos familiarizaremos con los diferentes **registros de recursos** del protocolo DNS.

2. Herramientas de diagnóstico para DNS

2.1 Dig

La orden `dig` (Domain information group) permite hacer consultas desde la línea de comandos o a través de un archivo mediante la opción `dig -f <nombre-archivo>`. Si no indicamos el servidor sobre el que se van a llevar a cabo las consultas, se asume que será el configurado en `/etc/resolv.conf`. La sintaxis del comando es la siguiente:

```
$ dig @servidor [opciones] [nombre] [tipo]

$ dig @8.8.8.8 +nostats cipfpbatoi.es SOA
```

- **servidor**: nombre o dirección IP del servidor DNS a consultar
- **nombre:** FQDN del dominio del que queremos consultar la información
- **tipo:** tipo de registro por el que se consulta (ANY, NS, SOA, MX, A, etc). Si no se indica se toma A por defecto.

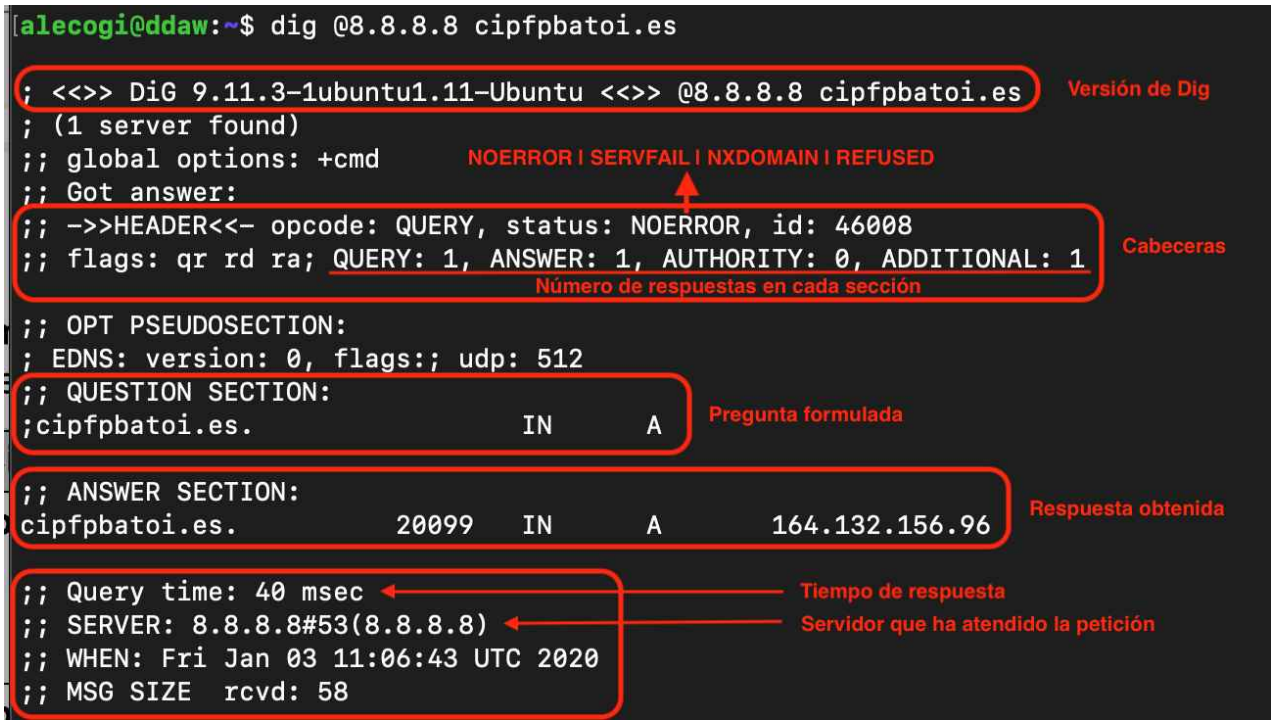
  Además, **podemos** especificar una serie de **opciones** sobre la consulta que

influirán tanto en los resultados obtenidos como en su visualización:

Opción	Descripción
+[no]trace	Indica si se muestra o no el rastro de todo el proceso de resolución. **[Por defecto no]** `$ dig @8.8.8.8 cipfpbatoi.es +trace`
+[no]short	Proporciona una respuesta concisa. **[Por defecto +]** `$ dig @8.8.8.8 cipfpbatoi.es +noshort`
+[no]stats	Habilita o no que se muestren estadísticas de la respuesta (tiempo, tamaño de la respuesta,… **[Por defecto +]** `$ dig @8.8.8.8 cipfpbatoi.es +nostats`
+[no]comments	Habilita o no que se muestren comentarios en la respuesta. **[Por defecto +]** `$ dig @8.8.8.8 cipfpbatoi.es +nocomments`

Una lista más completa de todos los comandos disponibles, puedes obtenerla en la **documentación oficial**.

A continuación se presenta la interpretación de una consulta simple con el comando del dig:



Si queremos obtener una **respuesta autoritativa**, podemos preguntar por el **registro SOA** y hacer una nueva petición poniendo como **servidor DNS** el obtenido en la respuesta anterior.

En las cabeceras de la respuesta, podemos observar una línea con los indicadores **flags:**

```
->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9464;; flags: qr rd ra; QUERY:1, ANSWER:1, AUTHORITY:0, ADDITIONAL: 1
```

El significado de cada **indicador**, viene especificado en la RFC1035 y podemos consultarlos, a modo de resumen, en la página de IANA. En caso de obtener una **respuesta autoritativa** se indicará mediante el **flag** aa (autoritative answer)

```
flags: aa qr ...
```

2.2 host

Al igual que el anterior comando, nos permite **convertir** nombres de **dominio** en **direcciones IP** y viceversa. La sintaxis del comando host es la siguiente:

```
$ host [opciones] dominio [servidor-de-nombres]

$ host -t SOA cipfpbatoi.es 8.8.8.8
```

Algunas opciones son:

Opción	Descripción

`-t <tipo>`
 	
`host -t SOA cipfpbatoi.es 8.8.8.8`
	Indica el tipo de recurso que queremos obtener

`-R <n>`
 	
`host -R 2 cipfpbatoi.es 8.8.8.8`
	Establece el número de intentos que se hacen para obtener la respuesta. Por defecto se establece a 1.

`-a`
 	
`host -a cipfpbatoi.es 8.8.8.8`
	Muestra todos los registros de recursos (RR) asociados al dominio y de la petición.
	(Obtendríamos una salida similar a la de la **herramienta dig**)

Puedes obtener una lista completa de las opciones y modificadores en la documentación oficial.

2.3. nslookup

Se trata de una alternativa a las 2 anteriores disponible tanto en sistemas operativos Linux/Unix como sistemas operativos windows. La denominación del término nslookup deriva de "**name server look up**", traducido al español como "búsqueda de servidores de nombres". La herramienta presenta 2 modos de funcionamiento:

- **Modo interactivo:** Permite llevar a cabo un número ilimitado de consultas; sobre distintas máquinas y dominios. Para ello se cuenta con un **prompt (>)** sobre el que ejecutaremos las consultas. El modo interactivo se inicia ejecutando la orden `nslookup` sin parámetros.

- **Modo no interactivo:** se introducen directamente tanto el comando **nslookup** como los parámetros, dominio y servidor de consulta. (Se trata de un modo de ejecución igual a los 2 anteriores). La sintaxis en modo interactivo viene dada por:

```
$ nslookup [-opciones] dominio [ip-servidor-dns]
```

Las opciones o modificadores de la consulta se llevan a cabo mediante la especificación de un par `clave=valor`. (Si lo ejecutamos en modo interactivo, utilizaremos la orden `set clave=valor` de forma previa a la consulta)

Opción	Descripción

`type=A|AAAA|MX|NS|SOA|ANY|PTR...`
 	
`nslookup -type=MX cipfpbatoi.es`
	Permite especificar el tipo de recurso que queremos obtener

`a`
 	
`nslookup -a cipfpbatoi.es 8.8.8.8`
	Obtiene los nombres canónicos del dominio (Registros CNAME)

`timeout=10`
 	
`nslookup -timeout=10 cipfpbatoi.es`
	Especifica el tiempo máximo en segundos por el cual se estará esperando la respuesta del servidor DNS

`[no]recurse`
 	
`nslookup -recurse cipfpbatoi.es`
	Especifica si el servidor debe preguntar a otros servidores de forma recursiva si no posee la información solicitada

Podemos consultar todas las opciones en la documentación oficial.

3. Trabajo a Realizar

Utiliza las herramientas **dig, host** y/o **nslookup** para realizar las siguientes consultas a los servidores de nombres.

1. Realiza una consulta DNS para mostrar el registro SOA relacionado con el dominio **cipfpbatoi.es**. Muestra la instrucción que has ejecutado y sus resultados utilizando las 3 herramientas disponibles (dig, host, nslookup). (**0.6 puntos**)

2. ¿Cuáles son los servidores de nombres responsables del dominio anterior que pueden responder con autoridad? ¿Hay más de uno? Muestra la instrucción que has ejecutado y sus resultados utilizando una de las 3 herramientas disponibles. (**0.6 puntos**)

3. ¿Cuáles son los servidores de correo del dominio? Hay más de uno? ¿Cuál tiene más prioridad? Muestra la instrucción que has ejecutado y sus resultados. (**0.5 puntos**)

4. Realiza un seguimiento de las consultas DNS que se realizan para resolver el dominio "**gva.es**" utilizando la herramienta **dig** y la opción **trace**. Muestra los nombres de los diferentes servidores de nombres que han consultado hasta llegar al servidor que contiene la información del dominio a buscar. (**0.8 puntos**)

> Los sistemas operativos que tienen funcionando **systemd** como es el caso de ubuntu 20.04, se utiliza un "**servidor dns** de caché local", por lo que para llevar a cabo esta tarea, especifica en el comando dig el **servidor dns** externo que se esté utilizando. Puedes averiguarlo utilizando el comando
>
> ```
> $ systemd-resolve --status
> ```

5. Realiza una consulta DNS para mostrar todos los registros tipo A de la zona **cipfpbatoi.es**. La respuesta debe ser de un servidor con autoridad. Muestra la instrucción que has ejecutado y sus resultados. (**0.5 puntos**)

6. Encuentra el nombre canónico (principal) de los siguientes dominios: www.google.es , www.upc.edu , www.uoc.es. Debes consultar los registros de tipo CNAME. Muestra la instrucción que has ejecutado y sus resultados. (**0.5 puntos**)

7. Contesta brevemente las siguientes preguntas: (**0.5 puntos**)
   - ¿Qué significa que una consulta DNS responde con autoridad.
   - ¿Qué es un TLD (Top Level Domain)?