Domain Name System

Sistema de Nombres de Dominio

Comprendiendo la resolución de nombres DNS.

El servicio de DNS **permite que un equipo** cliente de la red r**egistre y resuelva nombres de dominio**. Estos nombres se utilizan para encontrar y acceder a recursos de otros equipos de la red o de otras redes como Internet.

La resolución de nombres es el proceso de resolver nombres DNS a direcciones IP. La resolución de nombres es similar a mirar un nombre en la guía telefónica, donde el nombre se asocia con un número de teléfono. Por ejemplo, cuando se conecta al lugar Web de Microsoft, se utiliza el nombre www.microsoft.com. El DNS resuelve www.microsoft.com y su dirección asociada 207.46.130.149.

Un servidor de nombres sólo puede resolver una consulta para una zona en la que tiene autoridad. Si un servidor de nombres no puede resolver la consulta, dicha consulta pasa a otros servidores de nombres que sean capaces de resolver la consulta. Los servidores de nombres almacenan en caché los resultados de las consultas para reducir el tráfico de DNS en la red en futuras consultas.

El servicio de DNS utiliza el modelo cliente/servidor para la resolución de nombres. Para resolver una consulta de búsqueda directa, un cliente pasa una consulta a un servidor de nombres local. El servidor de nombres local o resuelve la consulta o consulta a otro servidor de nombres para la resolución.

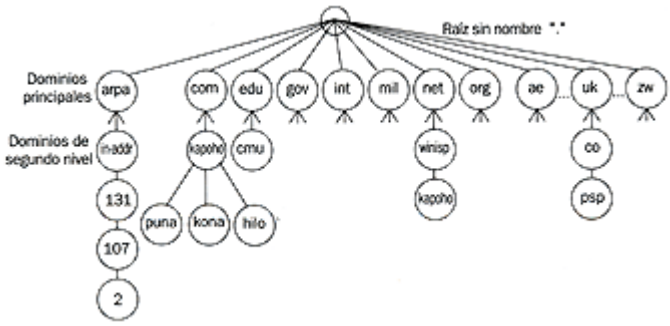
Siguiendo las prácticas del libro, vamos a instalar y configurar en vuestra máquina virtual un servidor DNS. Primero leed estos apuntes y familiarizaos con los conceptos. Os ayudará a entender qué estáis haciendo, cuando preparéis el Servidor DNS, un equipo que registra y resuelve nombres de domino (!!!vaya!!, justo lo que nos interesa)

Los tres componentes principales de DNS son los siguientes:

- Espacio de nombres de dominio.
- Registros de recursos (RR) asociados. Una base de datos distribuida de información de nombres.
- Servidores de nombre de DNS. Servidores que mantienen el espacio de nombres de dominio y los RR y responden a las peticiones de los clientes de DNS.

Espacio de nombres de dominio

El espacio de nombres de dominio está estructurado de manera jerárquica en un árbol que empieza en una raíz sin nombre para todas las operaciones de DNS. En el espacio de nombres de DNS cada nodo y cada hoja en el árbol del espacio de nombres de dominio representan un dominio con nombre. Cada dominio puede tener dominios hijos adicionales.



Cada nodo en el árbol de DNS tiene un nombre distinto llamado etiqueta (label). Cada etiqueta de DNS puede tener entre 1 y 63 caracteres y el dominio raíz no tiene caracteres.
Un nombre de dominio concreto es la lista de etiquetas en la ruta desde el nodo nombrado hasta la raíz del árbol de DNS. La convención de DNS es que las etiquetas que componen un nombre de dominio se leen de izquierda a derecha, desde lo más concreto hasta la raíz, por ejemplo, www.midominio.com. Este nombre completo también se denomina nombre de dominio completo, FQDN (Fully Qualified Domain Name).

Los nombres de dominio se puede almacenar en mayúsculas o en minúsculas, pero todas las comparaciones y funciones de dominios se definen como insensibles a mayúsculas y minúsculas. Por tanto, www.midominio.com es idéntico a WWW.MIDOMINIO.COM para las operaciones de nombrado de dominios.

Un dominio superior es un dominio de DNS directamente debajo de la raíz. Las tres categorías de dominios superiores son las siguientes:

- **<ARPA>.** Es un dominio especial, se usa en la actualidad para búsqueda inversa de nombres.
- **Dominios de 3 letras.** Existen siete dominios superiores de 3 caracteres.
- **Nombres de 2 letras para los países.** Estos dominios con código de país se basan en los nombres de país de la Organización Internacional de Normalización (ISO) y se usan, principalmente, por compañías y organizaciones fuera de los EE.UU. La excepción es UK, que utiliza .uk como dominio superior, aunque el código de país de ISO es GB.
-

Registro de recursos de DNS.

Un registro de recurso es un registro que contiene información relacionada con un dominio que puede contener la base de datos de DNS y que puede solicitar y usar un cliente de DNS. Por ejemplo, el RR de host de un dominio concreto mantiene la dirección de IP de tal dominio (host); **un cliente de DNS podrá utilizar este RR para conseguir la dirección de IP para el dominio**.

Cada servidor de DNS contiene los RR relacionados con aquellas porciones del espacio de nombre de DNS para el que es autoridad, o para el que puede responder las solicitadas por un host. Cuando un servidor de DNS es autorizado para una porción del espacio de nombres de DNS, dichos administradores del sistema son los responsables de asegurar que la información sobre esa porción del espacio de nombres de DNS es correcta. Para aumentar la eficiencia, un servidor de DNS dado puede hacer caché de los RR relativos a un dominio de cualquier parte del árbol de dominios.

Cada RR contendrá un conjunto de información común, como la siguiente:

- **Propietario.** Indica el dominio de DNS en el que se encuentra el registro de recurso.
- **TTL.** Tiempo que utilizan otros servidores de DNS para determinar durante cuanto

tiempo se hace caché de la información de un registro antes de descartarla. Para la mayoría de los RR, este campo es opcional. El valor de TTL se mide en segundos, con un valor de 0 que indica que el RR contiene datos volátiles que no se deben guardar en caché. Por ejemplo, los registros SOA tienen un valor de TTL predeterminado de 1 hora, de esta forma se evita que otros servidores mantengan en caché estos registros durante largos períodos de tiempo, lo que podría retrasar la propagación de cambios.

- **Tipo.** Este campo es requerido y mantiene un texto mnemónico estándar que indica el tipo del RR. Por ejemplo, el mnemónico A indica que el RR guarda la información de dirección (Address) del host.

Los archivos de zona de DNS estándar contienen el conjunto de RR de dicha zona en un archivo de texto. En el archivo de zona, cada RR consta de los elementos de datos anteriores, aunque diferentes registros pueden contener registros con formatos ligeramente diferentes para datos específicos.

Los RR usados más habitualmente, son:

Dirección de host (A) [Adress 32 bits]
Este RR contiene un RR dirección de host **que hace corresponder un nombre de dominio de DNS con una dirección de IPv4 de 32 bits**.

Registro host de IPv6 (AAAA) [Adress 128 bits]
Este RR contiene un RR dirección de host que h**ace corresponder un nombre de dominio de DNS a una dirección de IPv6 de 128 bits.**

Nombre canónico (CNAME) [canonical name]
El RR nombre canónico (CNAME) permite a los administradores de red crear un alias de otro nombre de dominio. El uso de RR CNAME se recomienda para su uso en los siguientes escenarios:

- Cuando un host especificado en un RR (A) de la misma necesita cambiar de nombre. Por ejemplo, si necesita cambiar el nombre de kona.midominio.com a hilo.midominio.com, crearía una entrada CNAME para kona.midominio.com que apuntase a hilo.midominio.com.
- Cuando un nombre genérico de un servicio conocido, como ftp o www, se necesita resolver a un grupo de equipos individuales, cada uno con un RR (A) individual. Por ejemplo, podría querer que www.midominio.com fuese un alias de kona.midominio.com y hilo.midominio.com. Un usuario que accediese a www.midominio.com normalmente no advertiría qué equipo realmente sirve la solicitud.

Puntero (PTR) [Pointer reverse]
Este RR que se usa para los mensajes de búsqueda inversa. Normalmente, se usa sólo el árbol de dominio in-addr.arpa para la búsqueda inversa de la correspondencia dirección-nombre. La **búsqueda DNS inversa** o la resolución DNS inversa (rDNS) es la determinación de un nombre de dominio que está asociado a una determinada dirección

IP utilizando el Sistema de nombres de dominio (DNS) de Internet.

Servidor de nombres (NS)
El registro de tipo NS indica quien es el servidor de nombres para el dominio. Es necesario que a dicho nombre se le asocie una dirección IP mediante un registro de tipo A.

Inicio de autoridad (SOA)
En primer lugar al describir un dominio siempre aparece el denominado registro SOA, **que describe una zona de autoridad,** es decir, una zona donde los datos que aparecen el fichero maestro son los que tienen prioridad y deben ser tomados como referencia.
El registro contiene distintos parámetros:

- Serie: el primer parámetro numérico conocido como número serie se debe ir incrementando cada vez que se cambia algo en el servidor de nombres, de cara a que el servidor secundario sepa que debe actualizarse.
- Refresco: indica cada cuantos segundos el servidor secundario ha de actualizarse con los datos del servidor primario.
- Reintento: indica cada cuantos segundos el servidor secundario debe intentar reconectarse al primario para actualizar los datos en caso de error.
- Expiración: indica cuanto tiempo ha de pasar para que el servidor secundario deseche toda la información que tenía del primario.
- TTL: tiempo de vida de los registros que no lo indiquen explícitamente.

Servidores de nombres de DNS.

Vale, entonces como funciona todo esto????

Un cliente efectúa una operación de solicitud a un servidor de DNS para conseguir parte o toda la información de RR relacionada con un determinado dominio, por ejemplo, para determinar qué registro o registros de hosts (A) se mantienen sobre el dominio llamado midominio.com. Si el dominio existe y también el RR solicitado, el servidor de DNS devolverá la información solicitada en un mensaje de respuesta a la solicitud. El mensaje de respuesta devolverá tanto la solicitud inicial como la respuesta con los registros relevantes, suponiendo que el servidor de DNS pueda conseguir los RR necesarios.

Solicitud inversa.
Una solicitud inversa es aquella en la que se solicita a un servidor de DNS el nombre de dominio de DNS de un host con una determinada dirección de IP. Los mensajes de Solicitud de búsqueda inversa son, realmente, solicitudes estándar, pero relacionadas con las zonas de búsqueda inversa. Las zonas de búsqueda inversa se basan en el nombre de dominio in-addr.arpa y mantiene, principalmente, los RR de PTR.

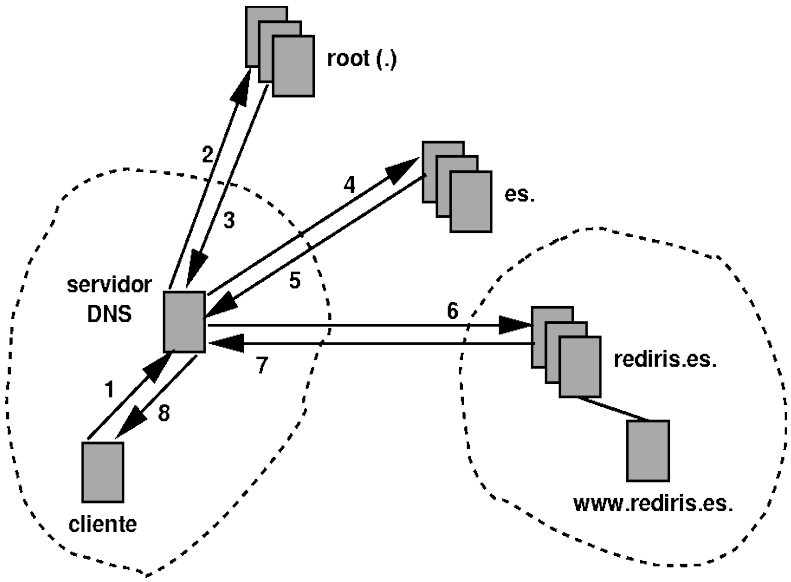
Clases de solicitudes de DNS.
Las solicitudes de DNS pueden ser de dos clases: recursivas o iterativas.

- **Una solicitud recursiva** es una solicitud de DNS que se envía a un servidor de DNS

en la que el host solicitante pregunta al servidor de DNS para que le proporcione una respuesta completa a la solicitud, aunque ello signifique que tenga que ponerse en contacto con otros servidores para obtener la respuesta. Cuando se envía una solicitud recursiva, el servidor de DNS usa un conjunto de solicitudes iterativas a otros servidores de DNS como intermediario del host solicitante para conseguir la respuesta a la solicitud.

Para resolver este tipo de solicitudes el servidor DNS dispone de los nombres y direcciones de servidores DNS del dominio raíz(.). Al conjunto de estos servidores se denominan **sugerencias raíz**.

- **Una solicitud iterativa** es una solicitud de DNS que se envía a un servidor de DNS en el que el host solicitante pide que se devuelva la mejor respuesta que el servidor de DNS pueda proporcionar sin buscar ayuda adicional de otros servidores de DNS.



Zonas.

El servicio de DNS permite dividir un espacio de nombres de DNS en zonas que almacenan información sobre uno o más dominios DNS. Las zonas se convierten en la fuente autoritaria para la información sobre nombres de dominio DNS incluidos en la zona.

El servicio de DNS proporciona la opción de dividir el espacio de nombres en una o más zonas, que pueden ser almacenadas, distribuidas y replicadas a otros servidores de DNS. El espacio de nombres DNS representa la estructura lógica de los recursos de red, y las zonas DNS proporcionan el almacenamiento físico para estos recursos.

Cuando decida dividir o no el espacio de nombres de DNS para hacer zonas adicionales, considere las siguientes razones para realizar la división:

- Necesidad de delegar la administración de parte del espacio de nombres de DNS a otra localización o departamento dentro de la organización.
- Necesidad de dividir una gran zona en zonas más pequeñas para distribuir las cargas de tráfico entre muchos servidores, mejorar el rendimiento de la resolución de

nombres DNS o crear un entorno DNS más tolerante a fallos.
- Necesidad de extender el espacio de nombres mediante la agregación de numerosos subdominios, tales como aquellos que se utilizan para acomodar la apertura de una nueva filial o sitio.
-

Hay dos tipos de zonas de búsqueda: zonas de búsqueda directa y zonas de búsqueda inversa.

Zonas de búsqueda directa.
Una zona de búsqueda directa permite consultas de búsqueda directa. En los servidores de nombres se debe configurar al menos una zona de búsqueda directa para permitir el funcionamiento del servicio de DNS. Norma, al instalar y configurar el servicio de DNS, el asistente crea automáticamente una zona de búsqueda directa basada en el nombre del DNS que se especificó para el servidor.

- **Estándar principal.** Una zona estándar principal es la copia maestra de una nueva zona almacenada en un archivo estándar de texto. Tiene que administrar y mantener una zona principal en un equipo en el que crea la zona.
- **Estándar secundaria.** Una zona estándar secundaria es una réplica de una zona existente. Las zonas secundarias son de sólo lectura y están almacenadas en archivos de texto estándar. Una zona principal debe estar configurada para crear una zona secundaria. Cuando cree una zona secundaria, debe especificar el servidor de DNS, denominado servidor maestro, que transferirá la información de zona al servidor de nombres que contiene la zona secundaria estándar. Las zonas secundarias proporcionarán redundancia y reducirán la carga en el servidor de nombres que contiene el archivo de la base de datos de la zona principal.

Zonas de búsqueda inversa.
Un zona de búsqueda inversa permite las consultas de búsqueda inversa. Las zonas de búsqueda inversa no son necesarias. Sin embargo, una zona de búsqueda inversa es necesaria para ejecutar herramientas de reparación de problemas, como NSLOOKUP.

Al igual que con las zonas de búsqueda directa, existen distintos tipos de zonas de búsqueda inversa que puede configurar:
- Estándar principal.
- Estándar secundaria.

Delegación de Zonas.
Una zona comienza como una base de datos de almacenamiento para un servidor de nombres de DNS concreto. Si se añaden otros dominios debajo del dominio utilizado para crear la zona, estos dominios pueden ser o bien parte de la misma zona o bien parte de otra zona. Una vez que un subdominio se añade, puede ser:

- Administrado o incluido como parte de la zona original de registros.
- Delegado a otra zona creada para dar soporte al subdominio.

Cuando el dominio microsoft.com se crea por primera vez como servidor único, se

configura como una zona única para todo el espacio de nombres del DNS Microsoft. Si, sin embargo, el dominio microsoft.com necesita utilizar subdominios, esos subdominios deben ser incluidos en la zona o delegados a otra zona.

Cuando se delegan zonas dentro de un espacio de nombres, debe crear también un registro de recursos SOA para apuntar al servidor autoritario de DNS para la nueva zona. Esto es necesario tanto para transferir la autoridad como para proporcionar la referencia correcta a otros servidores y clientes de DNS de los nuevos servidores hechos autoritarios para la nueva zona. El Asistente para nueva delegación está disponible para ayudar en las zonas de delegación.

Tipos de servidores DNS
Hay tres tipos de servidor de nombres:
Primario
Un servidor de nombres primario carga de disco la información de una zona, y tiene autoridad sobre ella.
Secundario
Un servidor de nombres secundario tiene autoridad sobre una zona, pero obtiene la información de esa zona de un servidor primario utilizando un proceso llamado **transferencia de zona**. Para permanecer sincronizado, los servidores de nombres secundarios consultan a los primarios regularmente y re-ejecutan la transferencia de zona si el primario ha sido actualizado. Un servidor de nombres puede operar como primario o secundario para múltiples dominios, o como primario para unos y secundario para otros. Un servidor primario o secundario realiza todas las funciones de un servidor caché.

Caché
Un servidor de nombres que no tiene autoridad para ninguna zona se denomina servidor caché.

ACLARACIÓN

DNS Dinámico (DDNS).
El servicio del DNS incluye la capacidad de realizar actualización dinámica. Esta capacidad se denomina DNS dinámico (DDNS). Con el DNS, cuando hay cambios en el dominio donde el servidor de nombres tiene autoridad, debe actualizar manualmente el archivo de la base de datos de la zona del servidor de nombres principal. Con el DDNS, los servidores de nombre y los clientes dentro de una red actualizan automáticamente los archivos de la base de datos de la zona.