UD 1. Instalación y administración de servicios de nombres de dominio.

- - Sistemas de nombres planos y jerárquicos.
- - Resolutores de nombres. Proceso de resolución de un nombre de dominio.
- - Servidores raíz y dominios de primer nivel y sucesivos.
- - Zonas primarias y secundarias. Transferencias de zona.
- - Delegación.
- - Tipos de registros.
- - Servidores de nombres en direcciones “ip” dinámicas.
- - Utilización de reenviadores.
- - Resolución inversa.
- - Comandos relativos a la resolución de nombres.
- - El cliente del servicio de nombres de dominio. Configuración.
- - El servidor de nombres de dominio. Configuración.
- - Herramientas gráficas de configuración.
- - Documentación de las configuraciones establecidas.

DNS (Domain Name System)

Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la

mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable.La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos. El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo hosts no resultara práctico y en 1983, Paul V. Mockapetris publicó los RFC 882 y RFC 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno (estos RFC han quedado obsoletos por la publicación en 1987 de los RFC 1034 y 1035).

Sistemas de nombres planos y jerárquicos.

Sistema de nombres planos:

Cada nombre es independiente de los demás. No existe ninguna jerarquía ni relación entre ellos, de manera que el nombre no aporta otra información que la identificación del host.

Ejemplo:
El DNI es un sistema de nombres planos
12345678X -> Juan Salvador Pérez

Sistema de nombres jerárquicos:

Existe una jerarquía de nombres que establece la manera de construir el nombre de un host. El propio nombre aporta información de la pertenencia del host a determinada categoría. Ejemplo:

La dirección postal es un sistema de nombres jerárquico:
Juan Salvador Pérez
Av Camp de Morvedre, 233
Puerto de Sagunto
Valencia

Un nombre de dominio usualmente consiste en dos o más partes (técnicamente «etiquetas»), separadas por puntos cuando se las escribe en forma de texto. Por ejemplo,

www.example.com o es.wikipedia.org

- A la etiqueta ubicada más a la derecha se le llama dominio de nivel superior (en inglés

top level domain). Como com en www.ejemplo.com o org en es.wikipedia.org

- Cada etiqueta a la izquierda especifica una subdivisión o subdominio. Nótese que "subdominio" expresa dependencia relativa, no dependencia absoluta. En teoría, esta subdivisión puede tener hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres, pero restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos.
- Finalmente, la parte más a la izquierda del dominio suele expresar el nombre de la máquina (en inglés hostname). El resto del nombre de dominio simplemente especifica la manera de crear una ruta lógica a la información requerida. Por ejemplo, el dominio es.wikipedia.org tendría el nombre de la máquina "es", aunque en este caso no se refiere a una máquina física en particular.

El DNS consiste en un conjunto jerárquico de servidores DNS. Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. Al inicio de esa jerarquía se encuentra los servidores raíz: los servidores que responden cuando se busca resolver un dominio de primer y segundo nivel.

Resolutores de nombres. Proceso de resolución de un nombre de dominio.

Existen dos tipos de consultas que un cliente puede hacer a un servidor DNS, la iterativa y la recursiva.

Resolución recursiva

Las resoluciones recursivas consisten en la respuesta completa que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. El servidor encargado de hacer la resolución realiza iterativamente preguntas a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver.

Resolución iterativa

En las resoluciones iterativas, el servidor no tiene la información en sus datos locales, por lo

que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta.

Cuando existe más de un servidor autoritario para una zona, Bind utiliza el menor valor en la métrica RTT (round-trip time) para seleccionar el servidor. El RTT es una medida para determinar cuánto tarda un servidor en responder una consulta.

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer alguna comunicación, comprueba si la respuesta se encuentra en la memoria caché. En el caso de que no se encuentre, la petición se enviará a uno o más servidores DNS.

La mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el proveedor de servicios de Internet. La dirección de estos servidores puede ser configurada de forma manual o automática mediante DHCP. En otros casos, los administradores de red tienen configurados sus propios servidores DNS. El proceso de resolución normal se da de la siguiente manera:

1. El servidor A recibe una consulta iterativa desde el cliente DNS.
2. El servidor A envía una consulta iterativa a B.
3. El servidor B refiere a A otro servidor de nombres, incluyendo a C.
4. El servidor A envía una consulta iterativa a C.
5. El servidor C refiere a A otro servidor de nombres, incluyendo a D.
6. El servidor A envía una consulta iterativa a D.
7. El servidor D responde.
8. El servidor A regresa la respuesta al resolver.
9. El servidor entrega la resolución al programa que solicitó la información.

Servidores raíz y dominios de primer nivel y sucesivos.

El espacio de nombres de dominio tiene una estructura arborescente. Las hojas y los nodos del árbol se utilizan como etiquetas de los medios. Un nombre de dominio completo de un objeto consiste en la concatenación de todas las etiquetas de un camino.

Las etiquetas son cadenas alfanuméricas (con '-' como único símbolo permitido), deben contar con al menos un carácter y un máximo de 63 caracteres de longitud, y deberá comenzar con una letra (y no con '-') (ver la RFC 1035, sección "2.3.1. Preferencia nombre de la sintaxis ").

Las etiquetas individuales están separadas por puntos. Un nombre de dominio termina con un punto (aunque este último punto generalmente se omite, ya que es puramente formal).

Un FQDN correcto (también llamado Fully Qualified Domain Name), es por ejemplo este:

www.example.com. (incluyendo el punto al final).

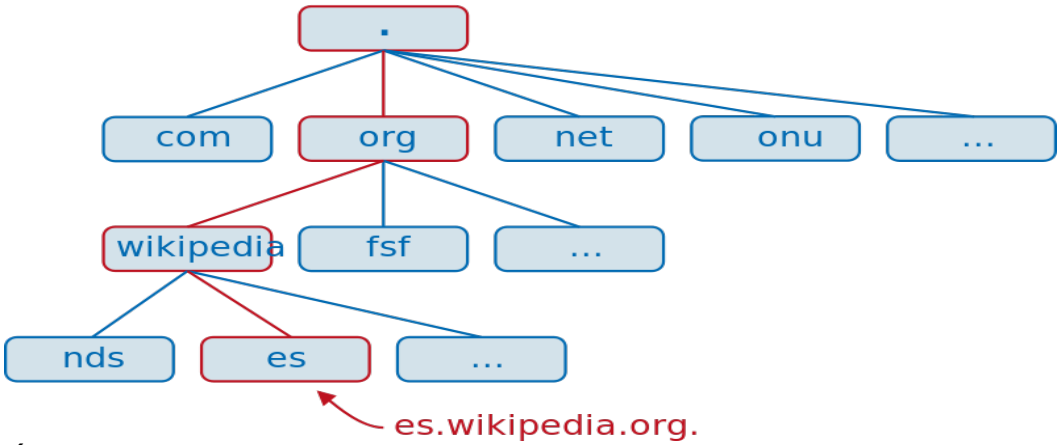
Un nombre de dominio debe incluir todos los puntos y tiene una longitud máxima de 255 caracteres.

Un nombre de dominio se escribe siempre de derecha a izquierda. El punto en el extremo derecho de un nombre de dominio separa la etiqueta de la raíz de la jerarquía (en inglés, root). Este primer nivel es también conocido como dominio de nivel superior (TLD - Top Level Domain).

Los objetos de un dominio DNS (por ejemplo, el nombre del equipo) se registran en un archivo de zona, ubicado en uno o más servidores de nombres.

Tipos de servidores DNS

- Primarios o maestros: Guardan los datos de un espacio de nombres en sus ficheros.
- Secundarios o esclavos: Obtienen los datos de los servidores primarios a través de una transferencia de zona.
- Locales o caché: Funcionan con el mismo software, pero no contienen la base de datos para la resolución de nombres. Cuando se les realiza una consulta, estos a su vez consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre.



Árbol DNS

Zonas primarias y secundarias. Transferencias de zona.

Zona de autoridad, es una parte del espacio de nombres de dominio sobre la que es responsable un servidor DNS. **E**l RFC 1035 define la zona como u*na base de datos completa para un subarbol podado del espacio de nombres de dominio.*

- Zona primaria: Es la que esta ubicada en el servidor primario. Los datos de la zona primaria se encuentran almacenados en un conjunto de ficheros ubicados en el servidor principal, estos ficheros permanecen aunque se reinicie el servidor principal.
- Zona secundaria: Están ubicados en servidores secundarios, puede haber tantas zonas secundarias como servidores secundarios exista. Los datos se obtienen de una zona primaria y permanece almacenada temporalmente en el servidor secundario. Si el servidor secundario se reinicia se tendrá que copiar nuevamente la zona. Las copias de la zona deben estar actualizadas y cada cierto tiempo contactarán con el servidor principal y descargarán una nueva copia de la zona.

Transferencias de zona.

Las Transferencias de zona DNS, es un tipo de transacción de DNS. Es uno de varios mecanismos disponibles para administradores para replicar bases de datos DNS a través de un conjunto de servidores DNS.

Se producirá una transferencia de zona durante cualquiera de los siguientes escenarios:

Al iniciar el servicio DNS en el servidor DNS secundario.

- Cuando caduca el tiempo de actualización.
- Cuando se guardan los cambios en el archivo de zona principal y hay una notificación lista.

Si llegara a existir algún problema de configuración o actualización del software de cualquiera de estos servidores se podrían explotar una serie de vulnerabilidades como por ejemplo envenenamiento de la base de datos y la integridad y confidencialidad de la base de datos del DNS primario se verían comprometidas.

Una transferencia de zona utiliza el Protocolo de Control de Transmisión (TCP) para el transporte, y toma la forma de una transacción de cliente-servidor. El cliente que solicita una transferencia de zona puede ser un servidor esclavo o servidor secundario, que solicita datos de un servidor maestro, a veces llamado un servidor primario. La parte de la base de datos que se replica es una zona.

La transferencia de zona comprende un preámbulo seguido de la transferencia de datos misma. El preámbulo comprende una búsqueda de la SOA (Start of Authority) registro de recursos para la "zona ápice", el nodo del espacio de nombres DNS que se encuentra en la parte superior de la "zona". Los campos de este registro de recursos SOA, en particular, el "número de serie", determinan si la transferencia de datos necesita ocurrir o no. El cliente compara el número de serie del registro de recursos SOA con el número de serie en la última copia de ese registro de recursos que tiene. Si el número de serie del registro que está siendo transferido es mayor, los datos en la zona se considera que han "cambiado" (de alguna manera) y el esclavo procede a solicitar la transferencia real de datos de zona. Si los números de serie son idénticos, los datos en la zona se considerará que no ha "cambiado", y el cliente puede seguir utilizando la copia de la base de datos que ya tiene, si tiene una.6

El proceso de transferencia de datos real comienza por el cliente de enviar una consulta (opcode 0) con el QTYPE especial (tipo de consulta) AXFR (valor 252) a través de la conexión TCP con el servidor.4 El servidor responde con una serie de mensajes de respuesta, que comprende todos los registros de recursos para cada nombre de dominio en la "zona". La primera respuesta comprende el registro de recursos SOA de la zona ápice. Los otros datos siguen sin un orden determinado. El final de los datos es señalado por el servidor de repitiendo la respuesta que contiene el registro de recursos SOA para la zona de ápice.

Algunos clientes de transferencia de zona realizan la búsqueda de SOA de el preámbulo utilizando el mecanismo normal de resolución de consultas DNS de su sistema. Estos clientes no abren una conexión TCP con el servidor hasta que hayan determinado que ellos

necesitan llevar a cabo la transferencia de datos. Sin embargo, ya que TCP puede ser utilizado para las transacciones de DNS normales, así como para la transferencia de zona, otros clientes de transferencia de zona realizan la búsqueda preámbulo SOA sobre la misma conexión TCP, ya que a continuación (pueden) realizar la transferencia de datos real. Estos clientes abren la conexión TCP con el servidor antes de que incluso realizan el preámbulo.

Delegación.

El Sistema de nombres de dominio (DNS) ofrece la posibilidad de dividir el espacio de nombres en una o más zonas, las cuales se pueden almacenar, distribuir y replicar en otros servidores DNS. Al estudiar si va a dividir el espacio de nombres DNS para disponer de zonas adicionales, consideraremos los siguientes motivos para usar zonas adicionales:

- Se desea delegar la administración de parte del espacio de nombres DNS en otra ubicación o departamento de la organización.
- Se desea dividir una zona de gran tamaño en zonas más pequeñas para distribuir las cargas de tráfico entre varios servidores, mejorar el rendimiento de la resolución de nombres DNS o crear un entorno DNS con mayor tolerancia a errores.
- Se desea ampliar el espacio de nombres al agregar varios subdominios a la vez, por ejemplo, para admitir la apertura de una sucursal o sitio nuevos.

Si, por alguno de estos motivos, se puede beneficiar de la delegación de zonas, quizás tenga sentido reestructurar el espacio de nombres al agregar zonas adicionales. Si se plantea cómo estructurar las zonas, use un plan que refleje la estructura de la organización.

Cuando se crea una zona principal estándar, toda la información de registro de recursos se almacena como un archivo de texto en un servidor DNS único. Este servidor actúa como el maestro principal de la zona. La información de la zona se puede replicar en otros servidores DNS para aumentar la tolerancia a errores y el rendimiento de los servidores.

Tipos de registros.

Un archivo de base de datos del servidor de nombres, (archivo DNS), es un **archivo de zona**. Contiene los registros de los dominios de la que es autoridad esa zona. Es decir es el archivo en el cual se encuentran los datos que resuelven las peticiones de nombres asociadas en direcciones IP. Se compone de una serie de registros que se verán a continuación.

Tipos de registro principales:

Registro SOA

Se forma con una serie de parámetros a tener en cuenta

- **Host Origen:** Host donde se mantiene el archivo.
- **Correo electrónico:** Del responsable de la BD. La arroba (@) se sustituye por un punto (.), debido a que @ representa el dominio raiz de la zona.
- **Numero de serie:** La versión de ese archivo. Aumenta cada vez que el archivo cambia.
- **Tiempo de actualización:** Tiempo que espera un servidor de nombres secundario para ver si el archivo ha cambiado, y por lo tanto pedir una **transferencia de zona**.
- **Tiempo de reintento:** Tiempo que espera un servidor de nombres secundario para iniciar una nueva transferencia de zona en el caso de que falle este procedimiento.
- **Tiempo de caducidad:** Tiempo que el servidor de nombres secundario intentará descargar una zona. Cuando pase, se rechaza la información antigua.
- **Tiempo de vida:** Tiempo en el que el servidor de nombres mantiene la caché cualquier registro del recurso de este archivo en base de datos.

Registro NS

El Registro NS. (siglas de **Name Server**), contiene los servidores de nombre de ese dominio, lo que permite que otros servidores de nombres vean los nombres de su dominio.

Registro MX

El registro MX es el registro de Intercambio de correo (**Mail eXchange**). Indica que host se encarga del procesamiento del correo electrónico de ese dominio.

Registro A

Los registros de dirección A, (**Adress**) asocian nombres de host a direcciones IP dentro de una zona.

Registro CNAME

Estos registros son llamados también **alias**, si bien son conocidos como entradas de *nombre canónico* (**CNAME, Canonical Name**). Su uso más común es utilizar para apuntar a un

único host más de un nombre, asi se simplifican procesos como albergar simultaneamente un servidor web y otro FTP en un mismo equipo.

Más tipos de registro:
A = Address – (dirección) Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.

- AAAA = Address – (dirección) Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.
- NS = Name Server – (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.
- MX = Mail Exchange – (registro de intercambio de correo) Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
- PTR = Pointer – (indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración de la zona DNS inversa.
- SOA = Start of authority – (Autoridad de la zona) Proporciona información sobre el servidor DNS primario de la zona.
- HINFO = Host INFOrmation – (información del sistema informático) Descripción del host, permite que la gente conozca el tipo de máquina y sistema operativo al que corresponde un dominio.
- TXT = TeXT - (Información textual) Permite a los dominios identificarse de modos arbitrarios.
- LOC = LOCalización - Permite indicar las coordenadas del dominio.
- WKS - Generalización del registro MX para indicar los servicios que ofrece el dominio. Obsoleto en favor de SRV.
- CNAME = Canonical Name – (nombre canónico) Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). Esto también es usado cuando corres múltiples servidores HTTP, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real. Ej. Ejemplo1 IN CNAME

ejemplo2

- SRV = SeRVicios - Permite indicar los servicios que ofrece el dominio. RFC 2782. Excepto MX y NS. Hay que incorporar el nombre del servicio, protocolo, dominio completo, prioridad del servicio, peso, puerto y el equipo completo. Esta es la sintaxis correspondiente: Servicio.Protocolo.Dominio-completo IN SRV Prioridad.Peso.Puerto.Equipo-Completo
- SPF = Sender Policy Framework - Ayuda a combatir el spam. En este registro se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe, consulta el SPF para comparar la IP desde la cual le llega con los datos de este registro.
- ANY = Toda la información de todos los tipos que exista.

Servidores de nombres en direcciones “ip” dinámicas.

El DNS dinámico (DDNS) es un servicio que permite la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres. El uso más común que se le da es permitir la asignación de un nombre de dominio de Internet a un dispositivo con dirección IP variable (dinámica). Esto permite conectarse con la máquina en cuestión sin necesidad de tener conocimiento de que dirección IP posee en ese momento.

El DNS dinámico hace posible utilizar un software de servidor en un dispositivo con dirección IP dinámica (como la suelen facilitar muchos ISP) para, por ejemplo, alojar un sitio web en la PC de nuestra casa, sin necesidad de contratar un hosting de terceros; pero hay que tener en cuenta que las PC caseras posiblemente no estén tan bien dotadas como los servidores de un Datacenter, ni tengan toda la infraestructura que poseen estos lugares.

Utilización de reenviadores.

Un reenviador es un servidor de Sistema de nombres de dominio (DNS) de una red que reenvía consultas DNS para nombres DNS externos a servidores DNS que están fuera de esa red. Además, puede reenviar consultas en función de los nombres de dominio específicos mediante reenviadores condicionales.

Puede designar un servidor DNS en una red como un reenviador al configurar el resto de los servidores DNS de la red para que reenvíen las consultas que no se pueden resolver de

forma local en ese servidor DNS. Al usar un reenviador, puede administrar la resolución de nombres para los nombres que están fuera de la red, como los nombres que están en Internet, y aumentar la eficacia de la resolución de nombres para los equipos de la red.

Resolución inversa.

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.

Las redes de ordenadores utilizan el Sistema de Nombres de Dominio para determinar la dirección IP asociada a un nombre de dominio. Este proceso también se conoce como la resolución de DNS hacia adelante. La búsqueda de DNS inversa es el proceso inverso, la resolución de una dirección IP a su nombre de dominio designado.

La base de datos de DNS inversa de la Internet tiene sus raíces en la dirección y el área de enrutamiento de parámetros (.arpa) del dominio de nivel superior de Internet. IPv4 utiliza el dominio in-addr.arpa y el dominio ip6.arpa se delega para IPv6. El proceso de la resolución inversa de una dirección IP utiliza el tipo de registro DNS puntero (registro PTR).

Los documentos oficiales de Internet (RFC 1033, RFC 1912 sección 2.1) especifican que "Cada host accesible en Internet debe tener un nombre" y que estos nombres coinciden con un registro de puntero inverso.

Los usos más comunes de la DNS inversa incluyen:

- El uso original de los rDNS: solucionar problemas de red a través de herramientas como traceroute, Ping, y el campo de encabezado para seguimiento "Recibido:" para el protocolo de e-mail SMTP, los sitios web de seguimiento de los usuarios (especialmente en foros de Internet), etc.
- Una técnica de antispam: la comprobación de los nombres de dominio en los rDNS para ver si los usuarios pueden ser de redes de acceso telefónico, direcciones asignadas dinámicamente, u otros servicios de bajo costo de Internet. Los propietarios de este tipo de direcciones IP suelen asignarles nombres rDNS genéricos como 1-2-3-4-dinámica-ip.example.com. Dado que la gran mayoría, pero no todos, de los e-mail que se origina en estos equipos es spam, muchos filtros de spam rechazan e-mail con estos nombres rDNS.3 4

- Una verificación forward-confirmed reverse DNS (FCrDNS) puede crear una forma de autenticación que muestra una relación válida entre el titular de un nombre de dominio y el propietario del servidor que se ha dado una dirección IP. Aunque no es muy completo, esta validación es lo suficientemente fuerte como para ser utilizado a menudo para propósitos de crear listas blancas, sobre todo porque los spammers y phishers por lo general no pueden pasar esta verificación cuando se utilizan ordenadores zombies que falsifican dominios.
- Registro del sistema o herramientas de monitoreo a menudo reciben las entradas con los dispositivos pertinentes especificados solamente por direcciones IP. Para proporcionar datos más utilizables por humanos, estos programas suelen realizar una búsqueda inversa antes de escribir el registro, escribiendo así un nombre en lugar de la dirección IP.

Comandos relativos a la resolución de nombres.

Nslookup

No obstante su desaparición en recientes versiones de BIND, es conveniente conocer las posibilidades de nslookup para realizar diversas consultas DNS. Este comando posee dos modos de comportamiento:

* Interactivo: permite realizar un número ilimitado de consultas diversas acerca de distintos hosts y dominios utilizando a varios servidores de DNS. Provee un prompt en el cual se podrán ejecutar distintos comandos en correspondencia con las acciones a realizar. Para terminarlo se podrá presionar Ctrl-D o utilizar el comando exit.
* No interactivo: se utiliza para realizar una única consulta o sea, para devolver sólo la información exacta de un host o un dominio a partir de un servidor.

El primer modo se obtiene cuando se invoca nslookup sin argumentos o cuando el primer argumento es ``-" y el segundo, un nombre de dominio o una dirección IP de un servidor de DNS. En cambio el modo no interactivo se alcanza dado que se indica como primer argumento el nombre o dirección IP del host buscado y como segundo, opcionalmente, el nombre o la dirección del servidor a consultar.

Host

El comando host es un utilitario que permite hacer búsquedas en el DNS. Se utiliza básicamente para convertir nombres en direcciones IP y viceversa.

Sintaxis: host [opciones] <dominio> [servidor]

dig

El comando dig (Domain informatiol Groper) constituye una herramienta para realizar consultas de diverso tipo a un servidor de DNS. Este muestra las respuestas recibidas de acuerdo a su solicitud. Es muy útil para detectar problemas en la configuración de los servidores de DNS debido a su flexibilidad, facilidad de uso y claridad en su salida.

Aunque normalmente las consultas que permite dig se definen en la línea de comando también se puede hacer en un fichero y pasárselo como argumento (opción -f). En el caso de que no se indique el servidor a consultar se asumirán los especificados en /etc/resolv.conf. Cuando no se añade ninguna opción o argumento en la línea de comando se consultan los servidores de nombres del dominio raíz (NS query).

La forma básica de invocar a dig es:

dig <@servidor> <nombre> [tipo]

donde:

* @servidor - es el nombre o la dirección IP del servidor a consultar.
* nombre - es el nombre de dominio del record por el cual se quiere preguntar.
* tipo - es el tipo del record por el que se consulta (ANY, NS, SOA, MX, etc.). De no indicarse se asumirá A.

Sintaxis: dig [@servidor] [opciones] [nombre] [tipo] [clase] [opciones de consulta]

El cliente del servicio de nombres de dominio. Configuración.

(depende de la distribución)

Configuración de cliente DNS en UNIX-Linux.

Se utilizan los archivos resolv.conf y host.conf

En el archivo /etc/host.conf se debe de establecer el orden de búsqueda al resolver nombres a direcciones IP. La instrucción order tal como se ve más abajo dice que primero resuelva el nombre-IP mirando en el archivo /etc/hosts (hosts) y si así no puede resolverlo que pregunte al servidor de DNS (bind).

```
[root@mi_host /etc]# cat /etc/host.conf
order hosts,bind
multi on
```

En el archivo /etc/hosts configurar la información relativa a nuestra máquina: dirección IP y dirección de 'loopback'.

```
[root@mi_host /etc]# cat /etc/hosts
127.0.0.1 localhost.localdomain localhost
10.194.2.114 mi_host.uned.es mi_host
```

La dirección IP 10.194.2.114 es sólo de ejemplo. Cada ordenador tendrá la suya propia y que tendrá que consignar aquí, así como el nombre del equipo en lugar de mi_host

En el archivo /etc/resolv.conf configuramos las direcciones IP de los servidores DNS. además del sufijo de búsqueda del dominio 'uned.es'.

```
[root@mi_host /etc]# cat /etc/resolv.conf
search uned.es
nameserver 62.204.192.21
nameserver 62.204.192.20
```

El servidor de nombres de dominio. Configuración.

Servidor sencillo con DNSmasq.

http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns_y_dhcp_sencillo_con_dnsmasq.html

Herramientas gráficas de configuración.

La principal herramienta gráfica para configurar los distintos servicios en linux es webmin.

http://usuariodebian.blogspot.com.es/2012/10/instalar-y-configurar-un-servidor-dns.html

Documentación de las configuraciones establecidas.

En los ficheros de configuración es muy recomendable añadir los comentarios necesarios para facilitar la correcta interpretación del mismo.

Cuando finalicemos la instalación y configuración de cualquier servicio, debemos dejar nuestras actuaciones perfectamente documentadas, de tal forma que sea posible restaurar la configuración en caso de fallo.

Debemos hacer constar:

- Instalación efectuada indicando el tipo de servicio y programa utilizado.
- Ficheros de configuración.
- Decisiones tomadas y justificación de las mismas. (en su caso)

- Fecha de la intervención.
- Procedimiento estándar de mantenimiento. (en su caso).