Servicios de red implicados en el despliegue de una aplicación

Despliegue de aplicaciones web

DAW – Despliegue de aplicaciones web (2º - 0614)

Introducción

- Una aplicación web necesita de servicios de red para poder funcionar de forma correcta y coherente.
- Concretamente estos servicios son:
  - Servicio de nombre de dominio (DNS). Traducción nombres de dominio del protocolo Internet (IP).
  - Servicio de directorio (LDAP). Validación de usuarios de forma centralizada y controlar el acceso a cualquier aplicación instalada en el sistema operativo.

Sistema de nombre de dominio

- Es la forma que los nombres de dominio se encuentran en Internet, que se traducen en direcciones del protocolo Internet (IP).
- Permite no tener que recordar la dirección IP de cada una de las páginas web que visitamos en Internet.

nslookup <host>

- Recupera velozmente la información correspondiente (IP) para poder conectar al servidor o host remoto.
- Formas para resolución del nombre de dominio requerido:
  - Fichero “hosts” (/etc/hosts o C:\Windows\System32\drivers\etc\hosts)
  - Relacionada con los servidores DNS (configuración del interfaz de red / DHCP). Más habitual.
- Nombre de dominio. Dirección de una empresa, organización, asociación, persona o grupo de personas en Internet.
  - Fácil, rápida y práctica para encontrar un sitio en Internet
  - Identificación en Internet

Sistema de nombre de dominio

- Niveles de dominio
  - De primer nivel. Terminan en “.com”, “.gob”, “.org”, etc., designados por el ICANN.
  - De segundo nivel. Relacionados con el país donde se dan de alta (por ejemplo en España los terminados en “.es” designados por Red.es).
  - De tercer nivel. Correspondientes al tipo “.com.es”, “.nom.es”, “.org.es”, “.gob.es”, “.edu.es”, etc.

Descripción de una URL

- Cualquier cambio en la dirección IP o un nombre en cualquier dispositivo se puede replicar a todos los servidores DNS (según configuración).
- Zonas de búsqueda:
  - Zona de búsqueda directa. Traducción nombre de domino a IP.
  - Zona de búsqueda inversa. Traducción IP a nombre de domino.
- Zonas de búsqueda:
  - Master. Crea sus propios registros, no copia de los ficheros de otro servidor DNS.
  - Slave. Respaldo en caso de fallo y reducir carga de los servidores DNS principales.
  - Caché. Mantiene copias de las resoluciones de DNS que han sido buscadas en otros servidores.

Sistema de nombre de dominio

Ventajas	Desventajas
No hay duplicidad de nombres (único administrador)	En algunos casos es fácil hackear el servicio DNS
No hay carga excesiva en la red ni en los hosts	Errores en configuración (fácil)
Coherencia de la información	

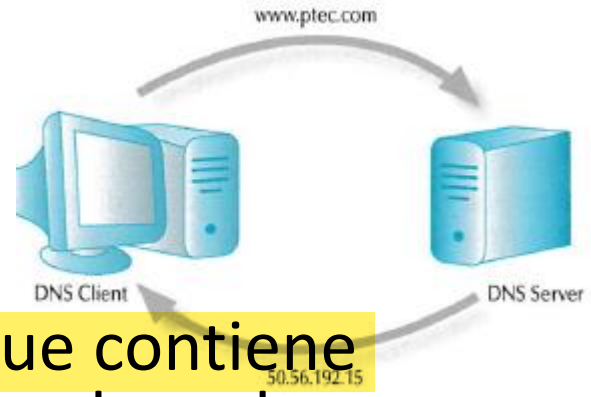
- Tipos de servidores DNS
  - Servidores **primarios** o maestros. Guardan la información relacionada con las zonas de las que son autorizados. El administrador es el encargado de añadir, modificar o eliminar los nombres de dominio.
  - Servidores **secundarios** o esclavos. No tiene archivos de zona propias, sino que están transferidos de un segundo o tercer nivel jerárquico. Servidores de backup del primario o maestro.
  - Servidores locales o **caché**. Realiza peticiones a otros servidores DNS para tener las respuestas preparadas para futuras solicitudes, sin autoridad sobre ninguna zona. Mejoran los tiempos de respuesta, la carga de los equipos y el tráfico de red.

Sistema de nombre de dominio

- Registros DNS
  - Las zonas definidas en los servidores DNS están compuesta de registros, que se definen como archivos de mapeo.
  - La cantidad total de registros DNS que se pueden definir está limitado a un total de 25.

Tipo de registro	Descripción	Sintaxis
A (Address)	Traduce nombres de dominio en direcciones IP.	`new.com A xxx.xxx.xxx.xxx`
PTR (Pointer)	Traduce direcciones IP en nombres de dominio.	`3.0.0.20.in-addr.arpa PTR host.new.om`
MX (Mail Exchanger	Asocia un nombre de dominio a un servidor de correo. El número 10 indica preferencia; a menor número, mayor preferencia.	`new.com MX 10 correo.new.com`
CNAME	Es un alias que se le asigna a un host que tiene una dirección IP.	`Alias.new.com CNAME nombre. new.com`
NS	Define los servidores principales de un dominio; al menos debe haber uno.	`new.com IN NS servidor1.new. com`
SOA	Es el primer registro de la zona; solo puede haber uno configurado. Especifica el servidor DNS primario del dominio. Pieza clave del archivo de zona.	Es un tipo de registro que especifica información del DNS. Los campos se definen más adelante.
TXT	Ofrece información adicional a un dominio. También se usa como almacenamiento en claves de cifrado.	`new.com TXT "Informacion adicional"`
SPF	Es un registro de tipo texto que se crea en la zona directa del DNS. Se usa principalmente para evitar la suplantación de identidad.	`new.com IN SPF "v=spf1 a:exchange.new.com –all"`

Sistema de nombre de dominio



- El cliente envía un mensaje de consulta al servidor DNS que contiene un nombre totalmente cualificado (FQDN), un tipo de consulta, y la clase de nombre de dominio.
- Flujo de consulta:
  1. El cliente tiene una caché que almacena lo registros que se usan habitualmente (resuelto de forma local).
  2. Consulta al servidor DNS, que puede responder desde su caché.
  3. El servidor DNS puede responder desde su zona que tiene configurada.
  4. Recursividad - El servidor DNS puede consultar a otros servidores DNS y con ello responde.
  5. Iteración - El cliente realiza la consulta a otros servidores DNS preferidos (primario y secundario)

Sistema de nombre de dominio

- Consulta recursiva. El servidor DNS da respuesta a la petición del cliente:
  - Un error NXDOMAIN (dominio o equipo no existe)
  - Un error temporal (no permite acceder al servidor DNS por problema de conectividad)
  - La respuesta a la petición con la dirección del registro A, acompañada del registro CNAME si existirá. Se indica si la respuesta es autoritaria o no (por el mismo o servidor exterior).

  Ejemplo de flujo del proceso de petición de IP
- Consulta iterativa. El servidor DNS responderá de forma parcial al cliente:
  - Las mismas respuesta de la consulta recursiva.
  - Una lista de servidores para preguntar por la petición del cliente, típica de servidores raíz o TLD (Top LevelDomain).
- ~~Consulta inversa (obsoleta). Cuando el cliente quiere conocer el nombre del dominio al que pertenece un registro.~~

Sistema de nombre de dominio

- Instalación y configuración servidor DNS en SO Linux:
  - Instalación:
    - apt-get update
    - apt-get install bind9 bind9utils
  - Arranque: service named [start | stop | status | restart | reload]
  - Monitorización:
    - ps –ef | grep named
    - netstat –ltun | grep :53
  - Resolución en linux. Fichero "/etc/resolv.conf " (nameserver, search)
  - "/etc/bind/named.conf.options "
    - Define la caché de nuestro DNS, y la configuración genérica del servidor (transferencia de zonas, forwarders, etc.)
    - Definición de forwarders (reenviadores).
  - "/etc/bind/named.conf.local". Donde se definen las zonas de búsqueda directas e inversas
  - Configuración del servidor DNS como caché (por defecto).
  - Configuración del servidor DNS para que reenvíe consultas
    - "/etc/bind/named.conf.options"
    - Parámetro forwarders

```
forwarders {
//DNS Cloudflare
        1.1.1.1;
        1.0.0.1;
//DNS Google
        8.8.8.8;
        8.8.4.4;
};
```

Sistema de nombre de dominio

```
// Zona de busqueda directa para xxxacmexxx.com
zone "xxxacmexxx.com" {
        type master;
        file "zonas/db.xxxacmexxx.com";
};
```

```
// Zona de busqueda inversa para 10.0.2.0/24
zone "2.0.10.in-addr.arpa" {
        type master;
        file "zonas/db.10.0.2";
};
```

- Instalación y configuración servidor DNS en SO Linux:
  - Configuración de un servidor DNS primario
    - "/var/cache/bind/zonas".
      - Directorio donde se definen las zonas
    - "/etc/bind/named.conf.local".
      - Definición de la zonas:
        - Resolución directa
        - Resolución inversa
    - Comprobación de zona
      - named-checkconf
      - named-checkzone
    - Creación de subdominio

- *$TTL (Time to Live):* indica la duración en segundos que se conservarán los datos en memoria caché.
- *Nombre_zona:* FQDN de la zona administrada por este archivo, los nombres de zona deben acabar en punto, de lo contrario dará error en el chequeo de los archivos. Usualmente se pone @ para no cargar demasiado al archivo. Es necesario declarar el registro NS y A para que la zona conozca tanto el dominio como la IP del servidor DNS que suministra la zona.
- *IN:* esta opción es obsoleta pero es la única que se puede usar hasta la fecha. Es la clase de Internet.
- *SOA (Start of Authority):* registro obligatorio para indicar que el servidor actual es el propietario y legítimo de esta zona.
- *Serial:* número de serie del archivo, se usa cuando la zona se replica a otros servidores.
- *Refresh:* valor numérico que se utiliza cuando la zona se replica a un servidor esclavo, y el intervalo con el que se comprueba la validez.
- *Retry:* es un valor numérico que indica el tiempo que pasa hasta que contacta el servidor esclavo con el servidor maestro.
- *Expire:* es otro valor numérico que indica cuántos segundos como máximo el servidor retendrá los registros antes de expirarlos.
- *Negative:* indica cuánto tiempo el servidor debe conservar en su caché la repuesta negativa.
- *NS:* registro que indica cuál es el servidor de nombres para esta zona.

Sistema de nombre de dominio

- Instalación y configuración servidor DNS en SO Linux:
  - Configuración de un servidor DNS secundario (esclavo)
    - “var/cache/bin/zonas”.
      - Directorio donde se replican las zonas
    - “/etc/bind/named.conf.local” (en esclavo)
      - Definición de la zona (a recibir del maestro) en el esclavo:
        - Resolución directa
        - Resolución inversa
    - “/etc/bind/named.conf.local” (en el maestro), para cada zona

```
// Zona de búsqueda directa para zeppelinux.net
zone "zeppelinux.net" {
        type slave;
        file "zonas/db.zeppelinux.net";
        masters {192.168.1.45;};
};
```

```
// Zona de búsqueda inversa para 192.168.1.0/24
zone "1.168.192.in-addr.arpa" {
        type slave;
        file "zonas/db.192.168.1";
        masters {192.168.1.45;};
};
```

```
allow-transfer {192.168.1.46;};
```

```
// Zona de búsqueda directa para viajes.zeppelinux.net
zone "viajes.zeppelinux.net" {
        type master;
        file "zonas/db.viajes.zeppelinux.net";
        allow-transfer {192.168.1.46;};
};
```

Servicio de directorio

- Un directorio en cualquier SO es una base de datos preparada para navegar, leer y buscar información almacenada en ella (encontrar información:
  - No contemplan transacciones complicadas ni opción de vuelta atrás.
  - La actualización es mediante cambios simples, siempre que se permita en la definición del directorio.
  - Dan respuesta a grandes solicitudes de búsqueda, con capacidad de incrementar la disponiblidad y la fiabilidad cuando se replica la información.
  - Funciones básicas:
    - Buscar información. Múltiples formas, ya sea por nombre o por otro campo implementado en el directorio.
    - Gestionar información. Agregar, editar o borrar usuarios por distintos campos. En caso de haber más de un directorio, habría que sincronizarlos.
    - Control de seguridad. Controlar el acceso por parte de los usuarios. Además gestiona los certificados digitales de los usuarios del directorio, cuyas funciones sería:
      - Creación
      - Distribución
      - Destrucción
      - Ubicación
- Las aplicaciones que acceden a los servicios de directorio son muy diversas: aplicaciones web, correo electrónico, acceso a edificiones, SO, etc.

Servicio de directorio

- Organización de LDAP
  - Según su diseño/implementación
    - **Centralizado**. Todas las consultas se canalizan en un único servidor, y todas son respondidas por él. No es necesario sincronizarlo / Único punto de fallo.
    - **Distribuido**. Información dividida en varios servidores que permiten responder a las consultas.
      - Información fraccionada. Cada servidor contiene sólo un subconjunto de la información.
      - Información replicada. Toda la información forma parte de todos los servidores.
  - LDAP (Lightweight Directory Acess Protocol) estándares definidos por IETF en varios RFC (https://ldap.com/ldap-related-rfcs/). Comparativa con X.500:
    - LDAP usa TCP/IP (no protocolos teóricos del modelo OSI)
    - LDAP representa la información mediante cadenas de caracteres (no estructuras ASN.1).
    - LDAP es simple e intuitivo a la hora de comprenderlo e implementarlo.
  - LDAP define un protocolo para el contenido de los mensajes entre un cliente y un servidor.

Servicio de directorio

- Organización de LDAP
  - La implementación de LDAP se realiza mediante Open LDAP (desarrollado por OpenLDAP)
    - Código de licencia libre y multiplataforma. Basado en el estándar X.500.
    - Tiene estructura de árbol denominado DIT.
    - Soporta IPv3, LDAPv3 y esquema distribuido.
    - Internacional (uso de caracteres UTF-8)
    - En Linux tiene una magnifica integración con otras aplicaciones, y mecanismos de búsqueda avanzado.
  - Modelo de información, que permite dar forma a la estructura almacenada el LDAP
    - Dato básico en el directorio es una entrada que corresponde con un objeto en el mundo real
    - Una entrada se compone de un conjunto de atributos, cada uno de ellos tiene un tipo con sus valores.
    - Todos los atributos tienen un identificador llamado OID y una sintaxis que permite definir los valores que se va a poner.

      dn: dc=ejemplo, dc=com
  - Modelo de referencia, que a la hora de nombrar los daos LDAP define cómo se organizan y referencias estos, primero se definen las estructuras de como se organizan las entradas y posteriormente se indica cómo referencias o acceder a las mismas

Servicio de directorio

```
dn: <nombre distinguido>
<nombre_atributo>: <valor>
<nombre_atributo>: <valor>
<nombre_atributo>: <valor>
```

- Archivos básicos de configuración y uso
  - El formato de intercambio de datos LDAP, llamado LDIF, es una extensión de archivo de texto sin formato usada para almacenar datos del directorio LDAP.
  - LDIF es un conjunto de registros y solicitudes de actualización de LDAP que incluye agregar, eliminar, modificar y cambier nombre.
  - Sintaxis de LDIF, que consta de dos partes
    - DN que debe figurar en la primera línea de entrada y que se compone de la cadena dn: seguida del nombre distinguido de la entrada.
    - La siguiente parte son los atributos de la entrada

Crea una unidad organizativa llamada “People” en el dominio ejemplo

```
dn: ou=People,dc=ejemplo,dc=com
objectClass: organizationalUnit
ou: People
```

Crea un empleado (“People”) con sus atributos en la ou anterior

```
dn: cn=alice,ou=People,dc=ejemplo,dc=com
objectClass: top
ObjectClass: account
objectClass: posixAccount
ObjectClass: shadowAccount
cn: alice
uid: alice
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/alice
userPassword: AlicePassword
loginShell: /bin/bash
```

Servicio de directorio

- Instalación de OpenLDAP en SO Linux
  - Ejecutar "*apt install slapd ldap-utils*" Solicita "Administrator password" con confirmación
  - Editar "/etc/hosts" Añadir "10.0.2.15 ldap.ejemplo.com ldap"
  - Ejecutar "*dpkg-reconfigure slapd*" DNS domain name: ejemplo.com, Organization name: ejemplo
  - Monitorización/arranque/parada:
    - *service slapd [start | stop | status | restart | force-reload]*
    - *ps –ef | grep slapd*
    - *Netstat –ltun | grep :389*
  - Herramientas:
    - # slapcat — Muestra la información contenida
    - # ldapadd — Permite insertar entradas en un directorio

      ldapadd -D "cn=admin,dc=ejemplo,dc=com" -W -H ldapi:/// -f /etc/ldap/users.ldif

      ldapadd -D "cn=admin,dc=ejemplo,dc=com" -W -H ldapi:/// -f /etc/ldap/alice.ldif
    - # ldapsearch — Permite seleccionar/buscar los objetos de un directorio

      ldapsearch -x -b "ou=People,dc=ejemplo,dc=com"
    - # ldapmodify — Permite modificar objetos de un directorio

      ldapmodify -D "cn=admin,dc=ejemplo,dc=com" -W -H ldapi:/// -f /etc/ldap/mod_alice.ldif
    - # ldapdelete — Permite borrar entradas en un directorio

      ldapdelete -D "cn=admin,dc=ejemplo,dc=com" -W -H ldapi:/// -f /etc/ldap/del_pepe.ldif

Servicio de directorio

- Autenticación en el servicio de directorio
  - Ejecutar "*apt install libpam-ldapd libnss-ldapd*"
    - Dirección: ldap://127.0.0.1:389
    - Base: dc=ejemplo,dc=com
    - Servicios: password y group
  - Monitorización/arranque/parada
    - *service nslcd [start | stop | status | restart | force-reload]*
    - *ps –ef | grep nslcd*
  - Herramientas: *# login*