TEMA 3 – Servicio de nombres (resumen)

SERVICIO DE NOMBRES

Implementa un servicio de red para proveer respuestas a las consultas en un servicio de directorio. Traduce un identificador basado en texto a una identificación numérica o componente de direccionamiento interno de sistema. Este servicio es realizado por el servidor en respuesta a una petición de protocolo de servicio

Las características principales de los servicios de nombre son:

- Utilizan el paradigma cliente/servidor.
- Es un servicio independiente fácilmente escalable.
- Independencia de su ubicación.
- Alta disponibilidad.
- La información se almacena jerárquicamente.
- Débil consistencia de replicación.
- Flexibilidad.
- BD optimizada: orientada a la lectura de información, datos de una entrada en un único registro, no necesita transacciones y tampoco bloqueos.

SERVICIO DE DIRECTORIO

Un servicio de directorio almacena información y la organiza de forma jerárquica sobre una red de ordenadores, usuarios y servicios.

Un directorio es al fin al cabo una base de datos que almacena y organiza información sobre una red informática. Comprendiendo como red informática sus recursos (pcs, impresoras, carpetas compartidas, etc) sus usuarios (entendiendo como tales las cuentas de usuarios y las de grupos) y sus servicios (correo electrónico, servidores web, ftp, etc)

Además de las características de los servicios de nombre, los servicios de directorio también poseen las siguientes:

• Información acerca de objetos relacionados (recursos de red, personas..).

• Refuerza la seguridad para proteger a los objetos de intrusos.

- Servicios de nombres (páginas blancas): DNS (específico)

LDAP

LDAP viene a significar protocolo ligero de acceso a directorios. LDAP es, por lo tanto, un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio.

LDAP utiliza el protocolo TCP/IP debido a que requiere menos recursos.

Además, posee un servicio de nombres y otro de directorios. Es de ámbito más general y también replicado. Refuerza la seguridad para proteger los objetos de intrusos y aumenta las capacidades de búsqueda por cualquiera de los atributos. Es una herramienta administrativa y de usuarios final.

Modelos de LDAP.

Además de definir el protocolo de acceso al directorio, el estándar LDAP define cuatro modelos que permiten entender mejor el servicio de directorio.

- **Modelo de información**, describe la estructura de la información almacenada en el directorio LDAP.
- **Modelo de nombrado**, describe cómo se organiza e identifica la información en el directorio LDAP.
- **Modelo funcional**, describe que operaciones pueden ser realizadas sobre la información almacenada en el directorio LDAP.
- **Modelo de seguridad,** describe cómo puede protegerse la información contenida en el directorio LDAP frente a accesos no autorizados.

Características distributidas

- Puede utilizar BDs como back-storage
- Puede dividir el árbol de directorios en subárboles gestionados por diferentes servidores LDAP. Motivos:
    - Rendimiento
    - Localización Geográfica
    - Cuestiones Administrativas
- Cada subárbol o rama será referenciada desde el árbol padre (objectClass::referral)
- Modos de funcionamiento:
    - El servidor LDAP resuelve la solicitud
    - El cliente resuelve

Escenarios LDAP

- Usos empresariales
- Directorios de información
- sistemas de Autenticación/Autorización
- Sistemas de correo electrónico
- Grandes sistemas de autenticación basados en RADIUS (Remote Access Dial-In User Server – con control de consumo)
- Servidores de certificados públicos y llaves de seguridad
- Perfiles de usuarios centralizados

ESQUEMA DE INTERACCION ENTRE CLIENTE Y LDAP

El esquema de interacción entre el cliente y el servidor LDAP sigue el siguiente esquema:

1. El cliente establece una sesión con el servidor LDAP. El cliente indica el servidor y el puerto en el que el servidor LDAP está escuchando. El cliente puede proporcionar información de autenticación o establecer una sesión anónima con los accesos por defecto.

2. El cliente efectúa las operaciones sobre los datos. LDAP proporciona capacidades de búsqueda, lectura y actualización.

3. Una vez finalizadas las operaciones, el cliente cierra la sesión.

DNS

El DNS (Domain Name System) es un servicio de traducción de nombres a direcciones IP.

El esquema de resolución de nombres DNS se realiza empleando el paradigma cliente-servidor

Un servidor dispone de una base de datos con información sobre nombres de recursos y sus correspondientes direcciones ip.

Elementos que los componen:

Espacio de nombres

- Agrupación lógica de dispositivos u objetos definidos por un conjunto de reglas
- Los nombres de los objetos han de ser únicos.

Dominio

- Agrupación lógica de dispositivos u objetos definidos por un conjunto de reglas.
- Cada dominio puede tener un padre y diversos hijos.
- El nombre completo del dominio se obtiene concatenando a su nombre los de sus superiores.

ZONA y SERVIDORES

Una zona es un subconjunto del esquema de nombres jerárquicos DNS. Las zonas son responsabilidad de un servidor DNS. Un servidor DNS tiene la autoridad sobra una o más zonas, cada zona tiene que ser atendida por un servidor principal.

También puede haber servidores secundarios, que tienen una copia del servidor principal.

Por ultimo un servidor puede estar en más de una zona, ya sea principal o secundario.

JERARQUIA DE NOMBRES:

Los nombres DNS están jerarquizados en niveles, los cuales se pueden distinguir los siguientes:

- Dominios raíz (origen de un espacio de nombre)
- Dominios de primer nivel
- Dominios de segundo nivel
- Subdominios (diversos niveles)
- Nombres de objetos (servicios o hosts)

En un servicio DNS se pueden distinguir 2 tipos de consulta;

Consulta Iterativa: Consultas consecutivas realizadas por un cliente DNS que tiene definidos más de un Servidor DNS. Se configura únicamente desde el cliente DNS

Consulta Recursiva: las consultas que arriban al servidor, si este no es capaz de resolverla con la información de su base de datos, las envía a otro servidor.

El servidor puede relanzar la consulta a un servidor especifico, un servidor raíz y cuando obtenga una respuesta, la proporciona al cliente.

SERVIDOR CACHE: no tienen ninguna información de zona. Solo reenvían consultas y mantienen una cache con las resoluciones realizadas.