TEMA 3 – Servicios de nombres

Servicios de nombres

Proporcionar una aproximación de la importancia de los nombres y el papel de:

- Servicios de nombres y de directorios
- Servicios de descubrimiento de recursos

Entender los aspectos más importantes en el diseño e implementación de un servicio de nombres:

- El espacio de nombres
- El mecanismo de resolución
- La división y replicación de datos de nombrado entre servidores y caché atributos

Comprender las características clave de:

- Servicios de nombres
  - DNS, LDAP "Servicio de directorios" (OpenLDPA, ActivieDirectory)
- Servicios de descubrimiento
  - JINI, UPnP y WS

Servicio de nombres

Nombrado

- Nombres
  - Identificador
  - Legible para el ser humano
- Referenciar recursos y usuarios
  - Objetos, archivos, computadores…
  - E-mail
  - Extensiones de archivos
- Comunicar y compartir recursos
  - Legible por los diferentes sistemas
- Atributo -> Valor de una propiedad del objeto (dirección)

Definiciones generales

- Enlace o Unión (Nombre lógico::Atributo)
  - Archivos (sistema archivos)
  - Objetos remotos (jndi, rmiregistry)
  - Computadoras (dns)
  - Servicios (url)
  - Usuarios (servicios de directorios)

- Convención de nombrado: Sintaxis de los nombres
  - Archivos -> /home/prueba.txt
  - DNS -> dtic.ua.ues
  - Ldap -> cn=Virgilio Gilart, o=ua, c=es

- Referencias y direcciones: No el propio objeto
    - Objeto::Impresora
        - Estado de la cola de impresión
        - Papel
        - Cartucho de tinta
    - Referencia::Impresora
        - Localización
        - Protocolo
- Contexto -> conjunto de unciones nombre::objeto
    - Convención de nombrado
    - Proporciona operaciones (API JNDI)
        - Operaciones
            - Resolución
            - Crear, eliminar, listar enlaces
            - Añadir y eliminar contextos
        - Sistema de archivos
            - /usr -> Contexto
            - /usr/bin -> Subcontexto
- Espacio de nombres -> Conjunto de nombres válidos en un sistema de nombrado (los que se pueden buscar)

Definición

Servicio de nombrado -> Devuelve un atributo a partir de un nombre conocido

- Base de datos con información que facilita la referencia de recursos
    - Resolución de un nombre
    - Localización de un recurso
- Independencia de su ubicación
- Paradigma C/S
- Servicio independiente -> Escalabe
- La información se almacena jerárquicamente
    - La jerarquía y estructura se definen en función de las necesidades de la organización
- Servicios:
    - Nombres (DNS, NIS)
    - Directorio (x.500, LDAP, Active Directory)

Características

- BD Optimizada
    - Orientada a la lectura de la información
    - Datos de una entrada en un único registro
    - No son necesarias transacciones ni bloqueos
- Modelo distribuido de almacenamiento de información -> Flexibilidad
- Débil consistencia de replicación entre servidores de directorios (p.ej: servidores secundarios)
- Escalabilidad
- Alta disponibilidad

DNS (Domain Name System)

Comenzó denominándose Raíz administrada por el Internet Network Information Center, es decir, la interNIC y evolucionó en el Sistema de nombres de domino (DNS). DNS establece una jerarquía de nombres para nodos en redes TCP/IP. Asocia cada nombre con una dirección IP. Es todo un sistema de Base de Datos distribuida que permite resolver, directa o inversamente, nombres DNS a dirección IP y viceversa.

Elementos

- Espacio de nombres: Jerarquía estructurada de dominios para organizar los nombres
- Registros de recursos: Asignan nombres a un tipo específico de información de recurso (utilizada para resolver el nombre en el espacio de nombres) (p. ej: [nombre] [TTL] [clase] Tipo_de_Registro Valor_del_Dato)
- Los servidores DNS: Almacenan y responden a las consultas de nombres
- Los clientes DNS (o solucionadores): Consultan a los servidores para buscar y resolver nombres de un tipo de registro de recurso.

Funcionamiento básico DNS

1. Petición de un cliente
2. Comprueba cache del cliente si está se resuelve si no pasamos al siguiente paso
3. El cliente DNS solicita la resolución de un nombre
4. El servidor DNS devuelve la IP asociada al nombre
5. El cliente puede realizar su petición

Espacio de nombres

- Dominio: Agrupación lógica del espacio de nombres. Un subárbol del espacio de nombres de dominio.
- Subdominio: Otros dominios dentro de un dominio.
- Zona: Unidad más pequeña y manejable, creada por delegación. Relacionada con la gestión y resolución de recursos. Normalmente es un archivo físico que gestiona un conjunto de recursos, puede que varios dominios.

Registros

Tipo de registro	Significado	Contenidos principales
A	Una dirección de computador	Número IP
NS	Un servidor de nombres autorizado	Nombre de domino para un servidor
CNAME	El nombre canónico de un alias	Nombre de dominio para un alias
SOA	Marca el comienzo de datos en una zona	Parámetros que gobiernan en una zona
WKS	Una descripción de servicio bien conocido	Lista de nombres de servicio y protocolo
PTR	Puntero de nombres de dominio (búsqedas inversas)	Nombre de dominio
HINFO	Información de host	Arquitectura de la máquina y del sistema operativo
MX	Intercambio de correo	Lista de pares <preferencia, host>
TXT	Cadena de texto	Texto arbitrario

- Resolución directa: Dado un DNS, localizar su dirección IP asociado.
- Resolución inversa: Dada una dirección IP, localizar el nombre DNS asociado.
- Resolución iterativa gestionada por el propio cliente
    - Es el cliente el encargado de ir consultado los servidores DNS desde el local, primario, secundario, etc. Hasta que uno le responda a su solicitud.
- Resolución iterativa gestionada por el servidor
    - El cliente solicita la traducción de un nombre a su servidor DNS y este es el encargado de que si no tiene la solución preguntar recursivamente desde los servidores raíz hasta encontrar un servidor que resuelva la petición del cliente y una vez obtenida devolvérsela a este.
- Resolución recursiva gestionada por el servidor
    1. El cliente busca en la caché de resolución DNS
    2. Pregunta a su servidor DNS
    3. El servidor DNS comprueba si gestiona la zona que solicita el cliente
    4. El servidor DNS comprueba su cache DNS
    5. Realiza una consulta C/S a los servidores raíz

Caché DNS

- Permite agilizar el proceso de consultas
- Almacena resoluciones realizadas
- Alta disponibilidad
- Consistencia de datos
- Caché en el resolver
    - 24 horas -> Problema si la IP cambia
    - Respuesta negativa
- Caché en el servidor
- O devuelve la respuesta o el más cercano al dominio

LDAP

Contiene información almacenada acerca de objetos relacionados como:

- Recursos de red (servidores, impresoras…)
- Personas
- Departamentos

Además, posee un servicio de nombres (pág. Blancas) y otro de directorios (Pág. Amarillas). 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.

Definición

- Servicio directorio (RFC 2251-2256; 2829 (autenticación); 2830 (seguridad); 3377 (especiaciones técnicas).
- Alternativa ligera a X.500
    - Sobre TCP/IP
    - Conjunto de operaciones reducidas

- Protocolo de acceso diferente a servidor y árbol LDAP
    - Protocolo C/S basado en mensajes
    - Comunicación asíncrona

Funcionamiento

1. Petición de búsqueda de un cliente
2. El servidor devuelve el mensaje de respuesta

Modelos LDAP

Representa los servicios que proporciona un Servidor LDAP vistos por el cliente. Se pueden distinguir cuatro modelos:

- Modelo de información: Estructura y tipos de datos (esquemas, entradas, atributos). Utiliza ficheros ASCII para entradas LDAP: formato LDIF
- Modelo de asignación de nombres: Define cómo referenciar de forma única las entradas y los datos en el árbol de directorios -> RDN y DN
- Modelo funcional: El protocolo LDAP operaciones para acceder al árbol de directorio: autenticación, solicitudes y actualizaciones
- Modelo de seguridad: Para el cliente, cómo probar su identidad (autenticación) y para el servidor, cómo controlar el acceso (autorización)

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

JNDI

JNDI similar JDBC

- Unifica el acceso a S.N. y S.D.
- API de acceso a
    - Servicio de nombres
    - Servicios de directorio
- SPI: Interfaz de Proveedor de Servicios
- Arquitectura de plug-in: Conexión dinámica de diferentes implementaciones
- Federación: Comunicación entre proveedores de servicios (LDAP -> DNS)

Estructura

Interfaz Context (javax.naming)

- Inicializar el contexto
- Buscar (lookup)
- Unir y Desunir (bin y unbind)
- Renombrar objetos (rename)
- Crear y eliminar subcontextos (createSubcongtext y destroySubcontext)
- Enumerar enlaces (listBindings)

Interfaz DirContext (javax.naming.directory)

- Extiende javax.naming
- Acceso a directorios además de nombres
- Trabaja con atributos
- Obtener atributos (getAttributes)
- Modificar atributos (modifyAttributes)
- Búsqueda por filtros (search)

JNDI -> rmiregistry

Servicios de descubrimiento

Objetivos

- Mecanismo que facilite la interoperatividad y la coordinación de dispositivos y servicios
- Sin intervención del usuario
- Sin administración
- Propuestas:
    - JINI
    - UPnP
    - Servicios Web (WS)
    - JXTA

Funcionamiento

1. Broadcasting para localizar servidores lookup
2. Respuesta (proxy del servidor lookup)
3. Registro del servicio (proxy y atributos)
4. Permiso (temporales)
5. Broadcasting para localizar servidores lookup
6. Respuesta (proxy del servidor lookup)
7. Busca servicios (de impresión)
8. Proporciona información del servicio (proxy)
9. Usa el servicio a partir del proxy de objeto (tomado del Servidor HTTP)

UPNP (Universal Plug and Play)

UPnP	JINI
Definido en el núcleo del SO	Actúa por encima (a modo de middleware)
Trabajo con Puntos de Control o sin ellos	Trabaja con Servidores Lookup
Está basado en TCP/IP, HTTPx y XML	Está basado en proxys de objetos
No describe modo de acceso a métodos	Utiliza JavaRMI
Ambos permiten proporcionar información de registro desde servidores externos Web	
Ambos trabajan y soportan eventos para actualización dinámica	
Ambos cubren el mismo tipo de problemas, pero con enfoques estructurales muy diferentes	

UPnP está definido en el núcle del SO -> JINI actúa por encima (a modo de middleware)

UPnP

Funcionamiento

0. Se conecta impresora de red (con UPnP habilitado)
1. Direccionamiento
2. Descubrimiento – (anuncio, búsqueda)
3. Descripción
4. Control
5. Presentación
6. Evento – (subscripción)