Diseñando un árbol de Directorio LDAP

Michael Donnelly

N.del T. : El presente articulo de **Michael Donnelly** en **http://www.ldapman.org** es traducido al castellano con el ánimo de ayudar a los que quieren aprender acerca de LDAP. La traducción no está sujeta a garantía de ningún tipo y el original pertenece a **Michael Donnelly**. El traductor **Pere Benavent** pone la traducción bajo licencia **GFDL GNU Free Documentation License** .

En un primer vistazo, el diseño de la topología de directorio de un servidor LDAP puede parecer una tarea intimidatoria. Con un poco de prudencia, pensemos, el proceso puede ser relativamente directo. En este artículo, pasaremos por cada uno de los tópicos que necesitarás considerar:

Este es el segundo de una serie de articulos para sendmail.net sobre el asunto LDAP. Las series como un todo te llevarán desde el "simplemente échale un vistazo dentro" hasta el proceso completo de desplegar un conjunto de aplicaciones y servicios habilitados para trabajar con directorios basados en LDAP. Un archivo de otros árticulos en esta serie pueden encontrarse en http://www.ldapman.org/articles/. También puedes querer echar un vistazo a las partes uno y dos de "Una Introducción a LDAP", que tambien se puede encontrar en ldapman.org.

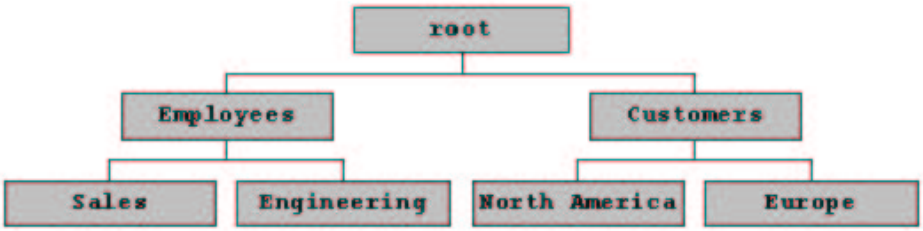
Qué es un Árbol de Directorio?

Simplemente recuerda, un árbol de directorio no es nada más que una manera organizada de proveer contenedores para almacenar diferentes tipos de información. Piénsa en ello como un sistema para que tus datos lo llenen.

Los servidores de directorio LDAP almacenan su información jerárquicamente, no distinto a un sistema de ficheros UNIX. La jeraquía proveé de un método para agrupamiento (y subagrupamiento) lógico de ciertos items juntos. Estos agrupamientos puedne ser útiles en un número de situaciones:

- Delegación de "autoridad" para uno o más grupos de datos a otro servidor o a otro sitio (site)
- Replicación de datos
- Seguridad y control de acceso
- Escalabilidad

Considera este ejemplo de un árbol de directorio muy simple. Dejaré fuera todos los LDAPismos por ahora, así podremos centrarnos en árbol en sí mismo.



Arriba tenemos la raiz, el punto de inicio para todos el árbol de directorio. Bajo la raiz hay dos categorias, cada una con dos subcategorias. Notese que en el caso de `Empleados (Employees)` estamos agrupando por departamento, mientras que para `Clientes (Customers)` estamos agrupando geográficamente. No hay restricciones de como un grupo dado es subagrupado. Piensa que he mostrado solo dos grupos por nivel aquí, tu directorio puede tener tantos grupos de datos como tu necesites, en cualquier nivel del directorio.

Escojiendo tu DN Base de Directorio

Déjame comenzar diciendo que no hay una manera correcta de configurar una estructura de directorio. El diseño que escojas puede parecer similar a otros que veas, y otra vez después puede no parecerlo. ¿ Querrás medir el diseño de tu árbol de directorio por uno de los criterios principales: Satisface tus actuales y proyectadas necesidades, eficientemente ? Si lo hace, estás haciendo las cosas correctamente.

La parte más alta del directorio, referida anteriormente como *raiz* del árbol del directorio, también es conocida como la *base*. El *nombre* de esa base es el *Nombre Distinguido de la Base*, o base DN. En principio, es decisión tuya elegir el formato de tu DN base; voy a recomendarte un DN base que sigue el que es formato más popular actualmente. (Puedes querer aprovechar esta oportunidad para refrescar tu memoría acerca de formatos DN base alternativos.)

Antes en 1988, la RFC 2247 cubría la fundación para codificar los nombres de dominio DNS en nombres distinguidos LDAP (y X.500). Desde entonces, más y más instalaciones han hecho de este formato su elección. Si estás planeando integrar con el Directorio Activo de Microsoft, este es el *único* formato que *puedes* utilizar, así que no te preocupes eligiendo - Redmon hizo la elección por ti.

El formato es muy simple. Digamos que la presencia de tu empresa en Internet es (o será) foobar.com. La RFC 2247 traduce este dominio DNS en el siguiente DN:

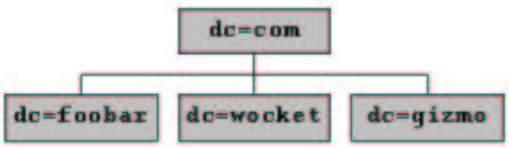
```
dc=foobar, dc=com
```

El "dc" representa "Componente de Dominio" (en ingles, "Domain Component."). Nota que cada porción del nombre DNS está representado en orden.

Así que, cual debería ser tu DN base? Asumiendo que la presencia de tu empresa en Internet acaba en .com, tu mejor opción es `dc=com`. Si tu presencia en Internet acaba en .net utiliza un DN base de dc=net. ¿ Captas la idea ? Si tu empresa no está ahora y nunca jamás estará en Internet, puedes utilizar dc=local en su lugar.

Bajo el DN base, tendrás solo una entrada sola que corresponde al resto de tu nombre de dominio DNS. Por ejemplo, los niveles más altos de foobar.COM podrían parecerse a esto:

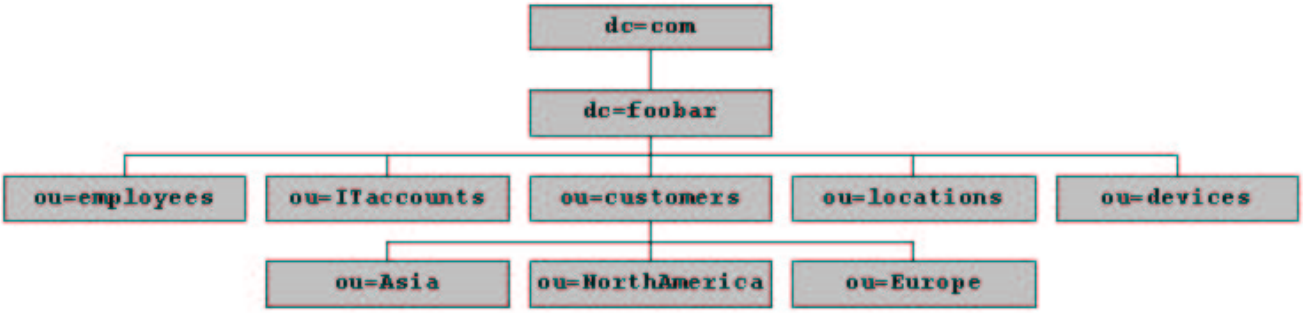
Digamos que foobar.com está destinado a fusionarse con wocket.com y gizmo.com. No hay problema! Gracias a tu pre ciencia, tu estructura de directorio está lista para acomodar este cambio atontante a favor de tu empresa. Simplemente añade las entradas `dc=wocket` y `dc=gizmo` bajo `dc=com`. Los niveles más altos de tu árbol de directorio ahora aprarecerán como esto:



Un Ejemplo de un Árbol de Directorio

La mejor estructura inicial de directorio, es la que menos se necesite mejorar después. En general, querrás diseñar tu directorio de modo que las entradas individuales no deban ser movidas de un árbol a otro. Probablemente encontrarás que un estructura bastante poco profunda funciona mejor, una donde cada rama del árbol contiene objetos que es improbable que se muevan mucho, si lo son en absoluto. Considera lo siguiente, un árbol de directorio para la ficticia foobar.com.

Han empleado alrededor de un año desenrrollando su directorio LDAP en fases, basando gradualmente más y más servicios en LDAP a lo largo del despliegue.



Nótese que cada rama es de la forma `ou=<name>` . OU representa Unidad Organizacional (por sus siglas en ingles Organizational Unit). Antes, en los días del X.500, los OU's fueron utilizados para representar organizaciones internas de tu empresa. Mientras que aún puedes hacer esto hoy en día, deberas reorganizar tu árbol de directorio cada vez que la estructura departamental cambie, y porqué darte a ti mismo un trabajo extra? En lugar de ello, foobar tomó el acercamiento fácil: ellos almacenan quien trabaja para quien, la información departamental y datos similares en la entrada de cada empleado. Siguen almacenando aún los mismos datos, pero con mucho menos trabajo.

ou=employees

Todos los empleados de foobar.com se listan aquí. Foobar ha desestimado la intención de separar este en subgrupos de ningún tipo, porque los esquemas de subagrupamiento invitablemente podrían cambiar a lo largo del tiempo: gente cambiando de posición, departamento, e incluso desplazandose de continente a continente. En lugar de eso, la localización, departamento, e información de la división de la compañía para cada empleado se almacena en la entrada LDAP del empleado, junto con el email, la información pública de RRHH y la información NIS.

ou=ITaccounts

Cuando foobar.com consolidó su información de contraseñas NIS y correo en un LDAP, hubo un poco de incertidumbre. ¿ Qué hacer con cuentas como "root", "nobody", "www" y demás ? Las cuentas TI como esas comparten los mismos atributos que las cuentas de empleado (contraseña, uid e información gid, dirección de correo electrónico y demás) pero son funcionalmente distintas de people. (Cuando fue la última vez que quisiste mirar el número de teléfono de "root"?) Para mantener estos datos distintos de la información de empleado, ellos crearon una OU de proposito especial solo para agrupar cuentas de este tipo. Los controles de acceso LDAP fueron añadidos entonces para impedir al personal no TI la lectura de los datos en esta localización.

ou=customers

Foobar.com ha elegido poner la información de contacto de sus clientes dentro del direcotorio LDAP. Esto permite a cualquier empleado consultar el directorio para encontrar la inforación de ventas del cliente, direcciones, información de contacto para soporte, y demás. En este caso, es improbable que un cliente se desplazara de un continente a otro.

Como la empresa crece, puede querer configurar replicación de esta información entre servidores regionales localizados. Ellos son capaces de ajustar a las necesidades de la gente de ventas de cada delegación porque han separado la información de contacto de cliente en subgrupos.

ou=locations

¿ Te has preguntado alguna vez la dirección de tu oficina en Nueva York ? O el número de teléfono en la "Sala de Conferencias Cafe Stain"? Alguna vez te han hablado de una reunión a las 10 am en la sala de reuniones "Scenic View", una sala de reuniones de la que no tienes ni idea de cómo encontrarla?

Bien, eso no les pasará a los amigos de foobar.com. Ellos almacenan la información de todas sus oficinas, salas de conferencias, y cosas similares en su directorio LDAP. El listin de teléfono de la empresa basado en LDAP puede mostrar toda esta información rápida y facilmente.

ou=devices

Foobar ha decidido también almacenar información acerca de sus ordenadores, impresorar, y otros dispositivos informáticos en LDAP. Esto permite a sus administadores de sistema almacenar nombre de host, dirección IP, dirección MAC, usuario primario o grupo, etiquetas de propiedad, número de serie, marca y modelo, nombre y versión de SO, localización, e información descriptiva para cada dispositivo en su red en un solo lugar.

Una GUI (Interfaz Gráfica Uversal, por sus siglas en ingles) Web permite a los administradores de sistema y a los gerentes de componentes de la empresa añadir, modificar, y consultar esta información. Un conjunto de scripts personalizados se utiliza para generar maquinas DNS y NIS mapeadas directamente desde LDAP. Las herramientas de gestión de componentes son utilizadas para actualizar automáticamente la información hardware en periodos regulares de tiempo, asú se mantiene la información al día con un mínimo esfuerzo.

Pero porque amontonar todos los routers, switches, impresoras, Pcs, Macs y sistemas UNIX en una OU? Porque todos ellos comparten los mismos tipos de información. Un servidor UNIX es muy diferente a una impresora, pero el tipo de información almacenada para cada uno es esencialmente la misma. Para facilitar una consulta como "Dáme una lista de todos los PCs Windows", simplemente consulta por Nombre de SO.

Bien, pero como se hace para "Dáme una lista de todos los portátiles"? Foobar.com ha implementado un número de atributos LDAP personalizados para proveer el grado de granularidad que ellos requieren, que les permititen rastrear un atributo "Clase de Máquina" y "SubClase de Máquina" para cada dispositivo. Los valores de "Clase de Máquina" incluyen Netgear, Impresora, Windows, Mac, UNIX. Los valores de "SubClase de Máquina" incluyen router, switch, impresosa de tinta, láser, portátil, estación de trabajo, servidor. La combinación de información clase y subclase provee la flexibilidad y la precisión para rastrear cualquier dispositivo de red de maneras distintas.

Planeando tu Topología de Directorio

Ahora lo que hemos visto en el ejemplo, probablemente te estes preguntando como diseñar tu propio directorio. En el ejemplo listado arriba, foobar.com está utilizando cinco categorias extensas, con `ou=customers` separado en subgrupos. (Recuerda que esto es solo un ejemplo; no es, ciertamente, el mejor diseño para todas las empresas.) En la práctica, probablemente querrás también categorias adicionales para manejar informacion de grupos NIS, información de listas de correo, y demás.

Así que, qué OUs son las correctas para ti ? Te dejo el proceso de diseño a ti. Después de todo, estas construyendo tu servidor LDAP para hacer frente a las necesidades específicas de tu propia situación. El ejemplo anterior debería ayudarte a tomar el pulso de como quieres organizar tus datos. He aquí una amplia lista de lineas generales para ayudarte en el proceso:

- Si esposible, del todo, evita que un diseño de arbol de directorio tenga que cambiar. Procura mantenerte alejado de arboles de directorios basados en diagramas de organización de la empresa, un modelo de negocio actual, y los similares.
- Querrás evitar mover registros LDAP desde un OU a otros. Si prevees que esto sucederá amenudo con tu actual diseño, intenta rediseñarlo. ¿ Puedes consolidar dos o mas ramas en una localización ? ¿ Puedes utilizar un atributo - localización. departamento - para conseguir el mismo fin ?
- ¿ Tienes tipos de datos que son similares en algunos aspectos, pero que difieren ampliamente en como se utilizan ? ¿ Puedes crear un OU separado para cada tipo de entrada ? Si las entradas no necesitan moverse de un OU a otro por cualquier razón, manten los grupos separados. (Considera el ejemplo anterior, con `ou=Employees` y `ou=ITaccounts`).
- Si estarás replicando datos en algún punto, considera si puedes separar un OU en sub-OUs basados en las necesidades de tus usuario. Piensalo dos veces, si lo haces de ese modo se originará un objeto moviendose de un OU a otro. (En el ejemplo anterior, la OU para clientes fue una candidata natural para sub-agruparse; la OU no lo fue)
- Si necesitas ocultar una porción de los datos de tu directorio, tanto por razones de seguridad o simplemente para evitar cinfusión, puedes querer utilizar una OU para esa tarea. Si esto significa violación de alguna de las lineas generales anteriores, tendrás que juzgar por ti mismo qué hacer - la seguridad es un asunto engañoso, las personas razonables pueden y lo hacen diferir.

Aquí hay algunas categorias amplias de objetos de datos que puedes considerar almacenar en un directorio LDAP, Dependiendo de tus necesidades, cada una puede autorizar una OU separada.

- Información de Empleado
- Información del Cliente, tanto para nuevos por primera vez como para clientes establecidos
- Números de teléfono y descripciones de restaurantes locales, servicios de taxi y demás
- Salas de Conferencia, información de localización de oficinas y demás
- Projectores LCD, flip charts, y otras utillerías portátiles para "salas de reuniones"

- Ordenadores: sobremesa, portátiles, servidores, impresoras, herramientas en red
- Listas de Correo
- Mapa de grupos NIS
- Mapa de grupos de red NIS

Parece fácil, verdad ? Pero no te dejes cautivar por items como estos:

- mapa de contraseñas NIS. Este mapa almacena informacion que aplica a empleados individuales. Puedes analizar este fichero y almacenar el login, contraseña y números uid y gid, el usuario de shell, y directorios home de cada usuario como atributos específicos por usuario de entradas LDAP individuales en `ou=employees` y `ou=ITaccounts` .
- Diagramas organizacionales. Los diagramas organizacionales reflejan esencialmente el título de la tarea de cada empleado, su director, departamento, y/o unidad de negocio. Simplemente analiza a traves de tu diagrama organizacional y asigna la información pertinente a cada registro individual de empleado. Siempre puedes derivar el diagrama organizacional de la empresa de la cadena de directores almacenada en el directorio.
- mapa de aliases NIS. Los mapas de alias contienen muchos tipos diferentes de infomación. Información de enrutamiento de correo y direcciones de correo alternativas para individuales deberían ser almacenadas como parte de la entrada LDAP de cada empleado. La información de listas de distribución podría ser almacenada en su propio OU, etc. Tendré un articulo entero dedicado a almacenamiento de información de correo en LDAP, así que se paciente.

Esto es lo que hay por ahora. Espero que hayas encontrado útil este articulo. Si tienes algún comentario o pregunta, enviame un correo electrónico a
donnelly@ldapman.org.

michael donnelly
9 may 2000