Una Introducción a 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** .

Si trabajas en la industria informática, hasta ahora has oído hablar de buenas oportunidades de LDAP. Te preguntas de qué va toda esa novedad ? Quieres saber un poco más acerca de la tecnología subyacente? Has venido al lugar adecuado. En esta introducción - la primera en una serie de artículos describiendo como diseñar, implementar, e integrar un entorno LDAP en tu empresa - te familiarizarás con los conceptos que hay tras LDAP mientras que se dejan los detalles duros del núcleo del asunto para más tarde. Aquí trataremos los siguientes asuntos;

Para empezar con ello, lo que está ocurriendo con LDAP hoy es novedoso. Una implementación a lo largo de la empresa puede facilitar la obtención de información de tu directorio LDAP a casi cualquier aplicación, ejecutándose en cualquier plataforma de computación . Y en teoría puede ser utilizada para almacenar un amplio rango de datos: dirección de correo electrónico e información de encaminamiento de correo, datos de RRHH, claves publicas de seguridad, listas de contactos, y mucho más. Haciendo un directorio LDAP un punto de enfoque en tu integración de sistemas, estas proveyendo de un almacén de ’única parada’ para cualquier persona que busque información dentro de tu empresa - incluso si la fuente primaria de datos reside en cualquier otro lugar.

Espera, me diras. Ya estás utilizando una base de datos Oracle, Sybase, Informix, o Microsoft SQL para almacenar mucha de esa misma información. ¿ Qué tiene de diferente LDAP? ¿ Qué lo hace mejor? Sigue leyendo.

De cualquier manera, qué es LDAP ?

El Protocolo de Acceso Ligero a Directorio, mejor conocido como LDAP (por sus siglas en inglés), está basado en el estándar X.500, pero significativamente más simple y más realmente adaptado para satisfacer las necesidades del usuario. A diferencia de X.500 LDAP soporta TCP/IP, que es necesario para el acceso a Internet. El núcleo de las especificaciones LDAP está totalmente definido en las RFCs -- una lista completa de las RFCs relacionadas se puede encontrar en la página LDAPman RFC.

Utilizando "LDAP" en una frase
En una conversación de cualquier día, oirás que gente bien intencionada dice cosas como, "¿ Deberíamos almacenarlo en LDAP ?" o "Simplemente obtén los datos de la base de datos LDAP", o "¿ Cómo hacemos para enlazar LDAP con una RDB (Base de Datos Relacional en ingles) ?". Hablando estrictamente, piensa, LDAP no es una base de datos en absoluto, sino un protocolo utilizado para acceder a información almacenada

en un directorio de información (también conocido como un directorio LDAP). Una formulación más precisa se podría parecer a algo como esto: "Utilizando LDAP, los datos serán recuperados (o almacenados en) la localización correcta dentro de nuestro directorio de información." Pero no me encontrarás corrigiendo a nadie en este punto: de otro modo, te harás una idea a lo largo de este punto, y eso es lo que cuenta.

¿ Es un directorio de información LDAP una base de datos ?
Así como un Sistema de Gestión de Base de Datos (DBMS por sus siglas en ingles) como Sybase, Oracle, Informix o Microsoft se utiliza para procesar consultas y actualizaciones a una base de datos relacional, un servidor LDAP es utilizado para procesar consultas y actualizaciones a un directorio de información LDAP. En otras palabras, un directorio de información LDAP es un tipo de base de datos, pero no es una base de datos relacional. Y a diferencia de una base de datos que está diseñada para procesar cientos o miles de cambios por minuto - como los sistemas de Procesamiento de Transacciones En Linea (OLTP por sus siglas en ingles) a menudo utilizados en el e-commerce - los directorios LDAP están fuertemente optimizados para el rendimiento en lectura.

Las ventajas de los directorios LDAP
Ahora que nos hemos "enderezado", ¿ cuales son las ventajas de los directorios LDAP ? La actual popularidad de LDAP es la culminación de un numero de factores. Te daré unas pocas razones básicas, con tal que tengas en mente que es solo una parte de la historia.

Tal vez la mayor ventaja de LDAP es que tu empresa puede accedes al directorio LDAP desde casi cualquier plataforma de computación, desde cualquier del numero creciente de aplicaciones fácilmente disponibles para LDAP. Es también fácil personalizar tus aplicaciones internas de empresa para añadirles soporte LDAP.

El protocolo LDAP es utilizable por distintas plataformas y basado en estándares, de ese modo las aplicaciones no necesitan preocuparse por el tipo de servidor en que se hospeda el directorio. De hecho, LDAP esta encontrando mucha más amplia aceptación a causa de ese estatus como estandard de Internet. Los vendedores están más deseosos de codificar en sus productos integración con LDAP por que no tienen que preocuparse de lo que hay al otro lado. Tu servidor LDAP puede ser cualquiera de un numero de los servidores de directorio LDAP de código abierto o comercial (o incluso un servidor DBMS con una interfaz LDAP), puesto que interactuar con cualquier servidor LDAP verdadero acarrea el mismo protocolo, paquete de conexión cliente y comandos de consulta. Por contraste, los vendedores que intentan integrar directamente con un DBMS habitualmente deben personalizar sus productos para trabajar con cada servidor de base de datos de cada vendedor individualmente.

A diferencia de las bases de datos relacionales, no tienes que pagar por cada conexión de software cliente o por licencia.

La mayoría de los servidores LDAP son simples de instalar, fácilmente mantenibles, y fácilmente optimizables.

Los servidores LDAP pueden replicar tanto algunos de sus datos como todos a través de métodos de envío o recepción, lo que permite enviar datos a oficinas remotas, incrementar tu seguridad y demás. La tecnología de replicación está incorporada y es fácil de configurar. Por contraste, muchos de los vendedores de DBMS cobran un extra por esta característica, y es bastante más difícil de gestionar.

LDAP te permite delegar con seguridad la lectura y modificación basada en autorizaciones según tus necesidades utilizando ACIs (colectivamente, una ACL, o Lista de Control de Acceso por sus siglas en inglés). Por ejemplo, tu grupo de facilidades puede dar acceso a cambiar la localización de los empleados, su cubículo, o número de oficina, pero no se permite que se modifiquen entradas de cualquier otro campo. Las ACIs pueden controlar el acceso dependiendo de quien está solicitando los datos, que datos están siendo solicitados, dónde están los datos almacenados, y otros aspectos del registro que está siendo modificado. Todo esto hecho directamente a través del directorio LDAP, así que no necesitas preocuparte de hacer comprobaciones de seguridad en el nivel de aplicación de usuario.

LDAP es particularmente utilizable para almacenar información que desees leer desde muchas localizaciones, pero que no sea actualizada frecuentemente. Por ejemplo, tu empresa podría almacenar todos los datos siguientes en un directorio LDAP:

- La listín de teléfonos de empleados de la empresa y el esquema organizacional
- Información de contacto de clientes externos

- Información de la infraestructura de servicios, incluyendo mapas NIS, alias de email, y demás
- Información de configuración para paquetes de software distribuidos
- Certificados públicos y claves de seguridad

Cuando deberías utilizar LDAP para almacenar tus datos?

La mayoría de los servidores LDAP están fuertemente optimizados para operaciones de lectura intensivas. A causa de esto, típicamente uno puede ver un orden de magnitud diferente cuando lee datos de un directorio LDAP frente a la obtención de los mismos datos de una base de datos relacional optimizada para OLTP. Sin embargo, a causa de esta optimización a la mayoría de los directorios LDAP no les viene bien el almacenamiento de datos donde los cambios son frecuentes. Por ejemplo, un servidor de directorio LDAP es bueno para almacenar el directorio de teléfonos internos de la empresa, pero ni se te ocurra pensar en utilizarlo como repositorio de base de datos para un sitio de comercio electrónico de alto volumen.

Si las respuestas a cada una de las siguientes preguntas es Sí, entonces, almacenar tus datos en LDAP es una buena idea.

- Te gustaría que tus datos estén disponibles a través de varias plataformas?
- Necesitas acceso a estos datos desde un número de ordenadores o aplicaciones?
- Los registros individuales que estás almacenado cambian unas pocas veces al día o menos, como media?
- Tiene sentido almacenar este tipo de datos en una base de datos plana en lugar de una base de datos relacional? Esto es, puede almacenar todos los datos, para un item dado, efectivamente en un solo registro?

Esta cuestión final a menudo hace que la gente tome una pausa, porque es muy común acceder a un registro llano para obtener datos que son relacionales en su naturaleza. Por ejemplo, un registro para un empleado de una empresa puede incluir el nombre de login del gerente de ese empleado. Es bueno emplear LDAP para almacenar este tipo de información. La prueba del algodón: si puedes imaginarte almacenado todos tus datos en un Rodolex electrónico, entonces puedes almacenar tus datos fácilmente en un directorio LDAP.

La estructura de un árbol de directorio LDAP

Los servidores de directorio LDAP almacenan sus datos jerárquicamente. Si has visto las reresentaciones de árboles DNS descendientes o directorios de ficheros UNIX, una estructura de directorio LDAP te será un terreno familiar. Como con los nombres de host en DNS, un registro Nombre Distinguido (Distinguished Name en ingles, DN en corto) de un directorio LDAP se lee desde su entrada individual, recursivamente a través del árbol, hasta el nivel más alto. Más sobre este punto después.

¿ Porque seccionarlas dentro de una jerarquía ? Hay un número de razones. He aquí algunos escenarios posibles:

- Puedes querer enviar todos tus contactos de clientes con base en US a un servidor LDAP en la oficina de Seattle (que esta dedicada a ventas), mientras que probablemente no necesites enviar allí la información de gestión de los activos de la empresa.
- Puedes querer conceder permisos a un grupo de individuos basado en la estructura del directorio. En el ejemplo listado abajo, el equipo de gestión de activos de la empresa puede necesitar acceso completo a la sección activos-gest, pero no a otras áreas.
- Combinado con replicación, puedes hacer a la medida la expansión de tu estructura de directorio para minimizar la utilización de ancho de banda de tu WAN. Tu oficina en Seattle puede necesitar actualizaciones al minuto de los contactos de ventas en US, pero solo actualizaciones cada hora para la información de ventas Europeas.

Yendo a la raíz del asunto: Tu DN base y tú
El nivel superior de un directorio LDAP es la base, conocido como el "DN base". Un DN base, generalmente, toma una de las tres formas listadas aquí. Asumamos que trabajo en una empresa de comercio electrónico de US llamada FooBar, Inc., la cual está en Internet en foobar.com.

o="FooBar, Inc.", c=US
(DN base en formato X.500)
En este ejemplo, o=FooBar,inc. se refiere a la organización, que en este contexto debería ser tratada como un

sinónimo del nombre de la empresa. c=US indica que el cuartel general de la empresa está en los US. Erase una vez en que éste fue el método de especificar tu DN base. Los tiempos y las modas cambian, sin embargo; estos días, la mayoría de las empresas están (o planean estar) en Internet. Y con la globalización de Internet, utilizar un código de país en el base DN probablemente haga las cosas más confusas al final. Con el tiempo, el formato X.500 ha evoluciado a otros formatos listados más abajo.

o=foobar.com
(DN base derivado de la presencia en Internet de la empresa)
Este formato es bastante sencillo, utilizando el nombre de dominio de la empresa como base. Una vez has pasado la porción o= (la cual viene de organization=), cualquiera en tu empresa debería saber de dónde viene el resto. Este fue, hasta hace poco, probablemente el más común de los formato usados actualmente.

dc=foobar, dc=com
(DN base derivado de los componentes de dominio DNS de la empresa)
Como el formato previo, este utiliza el nombre de dominio DNS como su base. Pero donde el otro formato deja en nombre de dominio intacto (y así legible para las personas), este formato está separado en componentes de dominio: foobar.com deviene dc=foobar, dc=com. En teoría, esto puede ser levemente más versátil, aunque es un poco más duro de recordar para los usuarios finales. A modo de ilustración, consideremos foobar.com. Cuando foobar se fusiona con gizmo.com, simplemente empiezas a pensar en "dc=com" como el DN base. Pon los nuevos registros en tu directorio existente bajo dc=gizmo, dc=com y listo para seguir. (Por supuesto, esta aproximación no ayuda si foobar.com se fusiona con wocket.edu) Este es el formato que recomiendo para cualquier instalación nueva. Oh, si estás planeando utilizar Active Directory, Microsoft ya ha decidido por ti que éste es el formato que necesitas.

Tiempo de ramificar: Cómo oraganizar tus datos en tu árbol de directorio
En un sistema de ficheros UNIX, el nivel más alto es el raíz. Por debajo de la raíz tienes muchos ficheros y directorios. Como mencione anteriormente los directorios LDAP están configurados en gran parte de la misma manera.

Debajo de tu base de directorio, querrás crear contenedores que separen lógicamente tus datos. Por razones históricas (X.500), la mayoría de los directorios configuran estas separaciones lógicas como entradas OU. OU vienen de "Unidades Organizacionales" (Organizational Units, en ingles), que en X.500 eran utilizadas para indicar la organización funcional dentro de la empresa: ventas, finanzas, etcétera. Actualmente las implementaciones de LDAP han mantenido la convención del nombre ou=, pero separa las cosas por categorías amplias como ou=gente (ou=people), ou=grupos (ou=groups), ou=dispositivos (ou=devices), y demás. Los niveles inferiores de OUs son utilizados a veces para separar categorías por debajo más lejos. Por ejemplo, un árbol de directorio LDAP (sin incluir entradas individuales) podría parecerse a esto:

```
dc=foobar, dc=com
    ou=customers
        ou=asia
        ou=europe
        ou=usa
    ou=employees
    ou=rooms
    ou=groups
    ou=assets-mgmt
    ou=nisgroups
    ou=recipes
```

Registros individuales LDAP

¿ Qué hay en un nombre ? El DN de una entrada LDAP
Todas las entradas almacenadas en un directorio LDAP tienen un único "Distinguished Name," o DN. El DN para cada entrada está compuesto de dos partes: el Nombre Relativo Distinguido (RDN por sus siglas en ingles, Relative Distinguished Name) y la localización dentro del directorio LDAP donde el registro reside.

El RDN es la porción de tu DN que no está relacionada con la estructura del árbol de directorio. La mayoría de los items que almacenas en un directorio LDAP tendrá un nombre, y el nombre es almacenado frecuentemente en el atributo `cn` (Common Name). Puesto que casi todo tiene un nombre, la mayoría de los objetos que almacenarás en LDAP utilizarán su valor `cn` como base para su RDN. Si estoy almacenando un registro para mi receta favorita de comida de avena, estaré utilizando **`cn=ComidaDeAvena Deluxe`** como el RDN de mi entrada.

- El DN base de mi directorio es **`dc=foobar,dc=com`**
- Estoy almacenando todos los registros LDAP para mis recetas en **`ou=recipes`**
- El RDN de mi registro LDAP es **`cn=Oatmeal Deluxe`**

Dado todo esto, ¿ cuál es el DN completo del registro LDAP para esta receta de comida de avena ? Recuerda, se lee en órden inverso, hacia atrás - como los nombres de máquina en los DNS.

cn=ComidaDeAvena Deluxe,ou=recipes,dc=foobar,dc=com

Las personas son siempre más problemáticas que los objetos inanimados
Ahora es el momento de abordar el DN de un empleado de una empresa. Para las cuentas de usuario, típicamente verás un DN basado en el `cn` o en el `uid` (ID del usuario). Por ejemplo, el DN del empleado de FooBar, Fran Smith (nombre de login: fsmith) puede parecerse a uno de estos dos formatos:

uid=fsmith,ou=employees,dc=foobar,dc=com
(basado en el login)
LDAP (y X.500) utilizan `uid` para significar "ID del usuario", no se debe confundir con el numero uid de UNIX. La mayoría de las empresas intentar dar a cada uno un nombre de login, así esta aproximación hace que tenga sentido el almacenar información sobre los empleados. No tienes que preocuparte sobre que harás cuando contrates al próximo Fran Smith, y si Fran cambia su nombre (¿se casa? se divorcia? ¿tiene una experiencia religiosa?), no tienes que cambiar el DN de la entrada LDAP.

cn=Fran Smith,ou=employees,dc=foobar,dc=com
(basado en el nombre)
Aquí vemos la entrada Nombre Común (CN por sus siglas en ingles) utilizada. En el caso de un registro LDAP para una persona, piense en el nombre común como sus nombres completos. Uno puede ver fácilmente lo colateral de esta aproximación: si el nombre cambia, el registro LDAP debe "moverse" de un DN a otro. Como se indica anteriormente, debes evitar cambiar en DN de una entrada siempre que sea posible.

Personalizando las clases de objeto de tu directorio

Tu puedes utilizar LDAP para almacenar datos en casi cualquier tipo de objetos, mientras que el objeto pueda ser descrito en términos de varios atributos. Aquí hay algunos ejemplos de información que puedes almacenar:

- Empleados: ¿ Cual es el nombre completo del empleado, nombre de login, contraseña, número de empleado, login de su gerente, servidor de correo ?
- Seguimiento de "activos": ¿ cual es el nombre de la computadora, dirección IP, etiqueta del activo, información de marca y modelo, localización física ?
- Listas de contacto de clientes: ¿ Cual es el nombre de la empresa del cliente? ¿ Primer teléfono de contacto, fax, e información de correo electrónico ?
- Información de la sala de reuniones: ¿ Cual es el nombre de la habitación, localización, capacidad en asientos, número de teléfono ? ¿ Hay acceso para silla de ruedas? ¿ Hay un proyector?
- Información de recetas: Nombre que se le da al plato, la lista de ingredientes, el tipo de cocina, y las instrucciones para prepararlo.

A causa de que tu directorio LDAP puede ser personalizado para almacenar cualquier tipo de texto o dato binario, aquello que almacenes será realmente lo que decidas. Los directorios LDAP utilizan el concepto de clases de objeto para definir qué atributos son permitidos para objetos de un tipo dado. En casi todas las implementaciones LDAP, querrás extender la funcionalidad básica de tu LDAP para adecuarlo a tus necesidades específicas, o creando nuevas clases de objetos o extendiendo las existentes.

Los directorios LDAP almacenan toda la información para unas entradas dadas de registros como una series de pares de atributos, cada una consistente en un tipo de atributo y un valor de atributo. (Esto es completamente diferente a la manera en que los servidores de bases de datos relacionales almacenan datos, en columnas y filas.) Considera esta porción de mi registro de receta, como se almacena en un directorio LDAP:

```
dn: cn=ComidaDeAvena Deluxe, ou=recipes, dc=foobar, dc=com
cn: Comida de avena instantánea Deluxe
recipeCuisine: desayuno
recipeIngredient: 1 paquete de comida de avena instantánea
recipeIngredient: 1 tazón de agua
recipeIngredient: 1 pizca de sal
recipeIngredient: 1 tsp de azúcar marrón
```

```
recipeIngredient: 1/4 de manzana, de cualquier tipo
```

Nótese que en este caso, cada ingrediente es listado como un valor del tipo de atributo `recipeIngredient`. Los directorios están diseñados para almacenar múltiples valores de un tipo único de esta manera, más que almacenando la lista entera en una único campo de la base de datos con algún tipo de delimitador para distinguir los valores individuales.

A causa de que los datos son almacenado de este modo, la forma de la base de datos es completamente fluida - no necesitas recrear una tabla de base de datos (y todos sus índices) para empezar a seguir un nuevo trozo de datos. Aún más importante, los dorectorios LDAP no utilizan memoria o almacenamiento para manejar campos "vacíos" - de hecho, tener campos opcionales no utilizados no te supone ningún coste en absoluto.

Un ejemplio de una entrada individual LDAP

Miremos un ejemplo. Utilizaremos el registro de LDAP de Fran Smith, nuestro amigable empleado de Foobar, Inc. El formato de esta entrada es un LDIF, el formato utilizado cuando exportamos e importamos entradas del directorio LDAP.

```
dn: uid=fsmith, ou=employees, dc=foobar, dc=com
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: foobarPerson
uid: fsmith
givenname: Fran
sn: Smith
cn: Fran Smith
cn: Frances Smith
telephonenumber: 510-555-1234
roomnumber: 122G
o: Foobar, Inc.
mailRoutingAddress: fsmith@foobar.com
mailhost: mail.foobar.com
userpassword: {crypt}3x1231v76T89N
uidnumber: 1234
gidnumber: 1200
homedirectory: /home/fsmith
loginshell: /usr/local/bin/bash
```

Para empezar, los valores de los atributos son almacenados con las mayúsculas intactas, pero las búsquedas contra ellos no distinguen mayúsculas por defecto. Ciertos atributos (como la contraseña) distinguen mayúsculas cuando se buscan.

Separemos esta entrada y observemosla pieza a pieza.

```
dn: uid=fsmith, ou=employees, dc=foobar, dc=com
```

Este es el DN completo de la entrada LDAP de Fran, incluyendo el path completo a la entrada en el árbol del directorio. LDAP (y X.500) utilizan `uid` para representar "ID de Usuario", no debe ser confundido con el número uid de UNIX.

```
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: foobarPerson
```

Uno puede asignar tantas clases de objeto como sean aplicables a cualquier tipo de objeto dado. La clase de objeto `person` requiere que los campos `cn` (nombre común) y `sn` (apellido, por sus iniciales en inglés surname). La clse de objeto `person` también permite otros campos opcionales, incluyendo nombre dado (givenname), número de teléfono (telephonenumber) y otros más. La clase de objeto `organizationalPerson` añade más opciones a los valores de `person` e `inetOrgPerson` añade aún mñas opciones a esta (incluyendo la información de correo electrónico). Finalmente `foobarPerson` es una clase de objeto personalizada de Foobar que añade todos los atributos del cliente que ellos desean conservar en su empresa.

```
uid: fsmith
givenname: Fran
sn: Smith
cn: Fran Smith
cn: Frances Smith
telephonenumber: 510-555-1234
```

```
  roomnumber: 122G
  o: Foobar, Inc.
```

Como se menciono antes, `uid` representa el ID de Usuario. Simplemente trad&uacutecelo en tu cabeza por "login" dondequiera que los veas.

Date cuenta que hay m&uacuteltiples entradas para el CN. Como se mencionó anteriormente, LDAP permite que algunos atributos tengan valores m&uacuteltiples, con el número de valores sean arbitrarias. ¿ Cuando puedes querer esto ? Digamos que estás buscando en el directorio LDAP de la empresa el número de teléfono de Fran. Mientras que *tu* puedes conocerla como Fran (habiendola oido derramar sus tripas sobre las margaritas del almuerzo en más de una ocasión), la gente en RRHH pueden referirse a ella (algo más formalmente) como Frances. A causa de que ámbas versiones de su nombre están almacenadas, las dos búsquedas encontrarán exitosamente el número de teléfono de Fran, su dirección de correo electrónico, el número de su cubículo, y demás.

```
mailRoutingAddress: fsmith@foobar.com
mailhost: mail.foobar.com
```

Como la mayoría de las empresas en Internet, Foobar utiliza Sendmail para la entrega de correo interno y su enrutamiento. Foobar almacena toda la información de enrutamiento de correo de los usuarios en LDAP, el cual es totalmente soportado por las recientes versiones de Sendmail.

```
userpassword: {crypt}3x1231v76T89N
 uidnumber: 1234
 gidnumber: 1200
 gecos: Frances Smith
 homedirectory: /home/fsmith
 loginshell: /usr/local/bin/bash
```

N&oacutetese que los adminitradores de sistema de Foobar almacenan toda la información de contraseñas NIS también en LDAP. En Foobar la clase de objeto `foobarPerson` añade ésta capacidad. Notese que la contraseña del usuario es almacenada en el formato crypt de UNIX. El uid de UNIX es almacenado aquí como `uidnumber`. Tenga en cuenta, que hay una RFC completa acerca de almacenar información NIS en LDAP. Hablaré de integración con NIS en un futuro articulo.

Replicación LDAP

Los servidores LDAP pueden ser configurados para replicar algunos o todos de sus datos, basándose en enviar o recojer la información, utilizando autentificación simple o autetificación basada en certificados.

Por ejemplo, Foobar tiene un servidor LDAP "público" corriendo en el puerto 389 de ldap.foobar.com. Este servidor es utilizado por la característica direccionamieto de correo electrónico pinpont de Communicator de Netscape, el comando "ph" de UNIX, y otras localizaciones dónde el usuario pudiera consultar un número de teléfono de un empleado o el contacto de un cliente. El servidor LDAP maestro de la empresa está ejecutandose en el mismo sistema pero, en cambio, en el puerto 1389.

Podrías no querrer que los empleados necesariamente esten buscando en el directorio para preguntar por el gerente de activos o recibir datos, no sería deseable ver las cuentas de TI (como "root") mostrandose en el directorio de la empresa. Para acomodar esas desagradables realidades, Foobar replica subárboles de directorio seleccionados desde su servidor LDAP maetroa su servidor "público". La replicación excluye los subárboles conteniendo datos que ellos desean ocultar. Para mantener las cosas actualizadas en todo momento, el servidor del directorio master se configura para hacer inmediatamente la sincronización basada en envio. N&oacutetese que esta aproximación está diseñada por conveniencia, no por seguridad: la idea es permitir a potenciales usuarios hacer simples consultas al otro puerto LDAP si desean buscar todos los datos disponibles.

Digamos que Foobar está gestionando si informacion de contacto de clientes via LDAP, sobre una conexión de bajo ancho de banda entre Oakland y Europa. Pueden querer configurar la repliación desde ldap.foobar.com:1389 a munich-ldap.foobar.com:389 como sigue:

```
periodic pull: ou=asia,ou=customers,o=sendmail.com
periodic pull: ou=us,ou=customers,o=sendmail.com
immediate push: ou=europe,ou=customers,o=sendmail.com
```

La conexión de recepción mantendrá las cosas en sincronia cada 15 minutos, lo cual probablemente podría ser

bastante ajustado en este escenario. La conexión de envío garantizará que cualquier cambio hecho a la información del contacto Europeo será enviado a Munich inmediatamente.

Dado este esquema de replicación, ¿ dónde podrían los usuarios conectar para acceder a sus datos ? Los usuarios en Munich simplemente podrían conectar a su servidor local. Si se estuvieran haciendo cambios a los datos, el servidor local LDAP podría referirse para esos cambios al servidor LDAP maestro, el cual podría enviar todos los cambios de nuevo el servidor local para mantenerlo en sincronia. este es uno de los tremendos beneficios para los usuarios locales: todas sus consultas LDAP (la mayoría en lectura) son hechas contra su servidor local, que es sustancialmente más rápido. Cuando es momento de hacer un cambio a su información, los usuarios finales no necesitan preocuparse acerca de la reconfiguración de su software cliente, porque los servidores de directorio LDAP manejan el intercambio de datos por ellos.

Securidad y control de acceos

LDAP provee de una complejo nivel de instancias de control de acceso, o ACIs. A causa de que el acceso puede ser controlado en el lado del servidor, es muchos más seguro que los metodos de seguridad que trabajan haciendo seguro a través del software cliente.

Con LDAP ACIs, puedes hacer cosas como:

- Conceder a los usuarios la capacidad de cambiarse su número de teléfono de casa y su domicilio, mientras que se les restringe el acceso a solo lectura para otro tipo de datos (como título de trabajo o login de gerente).
- Conceder a cualquiera en el grupo "HR-admins" (administradores de RRHH) la capacidad de modificar la información de los usuarios para los siguientes campos: gerente, título de trabajo, número ID del empleado, nombre del departamento, y número del departamento. No habrán permisos de escritura para otros campos.
- Denegar el acceso de lectura a cualquiera que intente consultar al LDAP por la contraseña de un usuario, mientras que se seguirá permitiendo al usuario cambiar su propia contraseña.
- Conceder permisos solo de lectura a los gerentes para los números de teléfono de casa de sus informadores directos, mientras que se deniega este privilegio a cualquier otro.
- Conceder a cualquiera en el grupo "host-admins" crear, borrar, y editar todos los aspectos de información del hosts almacenados en LDAP.
- A través de una página Web, permitir a la gente en "foobar-ventas" selectivamente conceder o denegarse a ellos mismos el acceso de lectura a subsets de la base de datos de contactos de cliente. Esto podría, a su vez, permitir a esos individuos descargar información de contacto de los clientes a sus ordenadores portátiles o a sus PDA. (Esto será más útil si tu herramienta de forzamiento de automatización para ventas es LDAP-izable.)
- A través de una página Web, permitir a cualquier propietario de grupo añadir o eliminar entradas de sus grupos. Por ejemplo, esto podría permitir a los gerentes de ventas conceder o eliminar el acceso a la gente de ventas para modificar las páginas Web. Esto podría permitir a los propietarios de los alias de correo añadir o eliminar usuarios sin contactar con TI. Las listas de distribución designadas como "pública" pueden permitir que los usuarios se añadan o se eliminen ellos mismos (pero solo a ellos mismos) de o a esos alias de correo. Las restricciones pueden basarse también en direcciones IP o nombres de máquina. Por ejemplo, los campos pueden hacerse legibles solo si la dirección IP del usuario empeiza por 192.168.200.*, o si la resolución inversa del nombre de máquina del usuario por DNS se mapea a *.foobar.com.

Esto te dará una idea de lo que es posible utilizando el acceso controlado con directorios LDAP, pero ten presente que una correcta implementación requiere mucha más información de le dada aquí. Explicaremos el control de acceso en más detalles en un futuro articulo.

Esto es todo por ahora. Espero que hayas encontrado este articulo útil Si tiene comentarios o cuestiones, envia un correo electrónico a donnelly@ldapman.org.

28 abril 2000