PROPUESTA PARA LA RE-ESTRUCTURACIÓN Y MIGRACIÓN DEL LDAP DE LA OPSU

CARACAS, FEBRERO 2010

Corcaribe Tecnología C.A. - C.C. El Refugio Piso 2, Oficinas CL-40, CL-46, Guatire, Miranda 1221
Teléfonos: (212) 339-8939, 613-8680, Fax: (212) 381-0208

Introducción

El presente documento tiene como finalidad describir la estructura propuesta para el LDAP de la Opsu, aprovechando la migración a OpenLDAP y la nueva visión de integración del LDAP con el resto de los procesos y aplicaciones de la Opsu.

Marco Referencial

Para la elaboración de este documento se investigaron diversas fuentes de información, sobre todo, los RFC que definen a LDAP v2 y LDAP v3, así como fuentes originales de X.500. Adicionalmente, se consultaron listas de correo, foros y otras fuentes de información en las cuales se buscaba obtener la experiencia de otros usuarios y organizaciones en la implementación de esta tecnología. Las referencias son citadas directamente en el texto donde sea preciso.

Estructura del Arbol LDAP

Durante la elaboración de la siguiente propuesta se investigó a fondo el tema de las estructuras y las clases de Objetos de que las definen. Se estudiaron los esquemas base (schema) y los comúnmente utilizados para la administración de dominios Samba, Windows y cuentas Posix, así como los usados para sistema de correo entre otros.

Lo importante a comprender es que tanto la forma tradicional X.500 (c,st,o,ou,cn) así como la más moderna de LDAP (basada en dominios dc,cn/uid) no son definiciones estrictas y sirven solo como marco referencial y como ejemplo para los diferentes usos que se le pueden dar a un directorio. De hecho, es importante refrescar algunos conceptos fundamentales sobre DAP (X.500) y LDAP (IETF) en general:

La Entrada (Entry) y el Árbol (DIT)

El elemento atómico más importante del directorio es la **entrada** (“**entry**” en inglés). Un directorio LDAP no es más que un conjunto de entradas organizadas de una forma jerárquica también conocida como **DIT** o árbol de información del directorio (“Directory Information Tree” en inglés). Cada entrada está identificada por un nombre distinguido (único) en el árbol conocido como **DN** (“Distigushed Name” en inglés). Como se ha mencionado, el DN de cada entrada es único aunque el mismo puede cambiar durante la vida de la entrada en el DIT (se explica más adelante).

Distinguished Name (DN) y Relative Distinguished Name (RDN)

El nombre distinguido o “DN” es único para cada entrada del árbol en un momento dado, es decir, no pueden existir dos entradas con el mismo DN al mismo tiempo[1]. El DN es la suma de un nombre

1 RFC4512 (http://www.ietf.org/rfc/rfc4512.txt), sección 2.3.2

distinguido relativo RDN ("Relative Distinguished Name")[2] más un sufijo que ubica la entrada en el árbol (el sufijo no es más que el DN del nodo padre[3]). El RDN es único para cada nodo hermano ("sibling" en inglés), ya que los nodos hermanos tienen el mismo sufijo. "Se puede pensar en el RDN como el nombre de un archivo, y en el DN como el nombre completo"[4] (la ruta + el nombre del archivo).

El DN de una entrada puede cambiar en el tiempo, por lo cual algunos servidores LDAP ofrecen un atributo especial denominado **entryUUID**[5], el cual nunca cambia durante la vida de la entrada, incluso si cambia el RDN y/o el DN. Este *atributo operacional* es fundamental, por ejemplo, para relacionar/integrar las entradas de LDAP con aplicaciones que usen bases de datos relacionales, y se puede pensar en el entryUUID como una clave única de todo el DIT. No todos los servidores LDAP soportan este atributo operacional, sin embargo la mayoría si lo hacen.

El DN está conformado por un conjunto de atributos que identifican a la entrada. Los atributos que pueden formar parte del DN están especificados en la clase estructural de la entrada. Cada entrada tiene asociada obligatoriamente una clase estructural ("Structural Object Class") que define el *tipo* de entrada. La clase estructural es muy importante ya que define los *atributos obligatorios y opcionales* que debe poseer la entrada, especialmente aquellos atributos que se usan en la identificación de la misma[6], de hecho, lo más común es que las clases estructurales definen un solo atributo obligatorio, y este atributo es el atributo que por si solo es el RDN (no siempre es el caso, ya que el RDN puede estar conformado por más de un atributo, pero en la mayoría de las clases más comunes suele ser así).

Object Classes

Cada entrada en el directorio puede ser de diferente *tipo* o clase estructural, y puede tener asociada una o más clases auxiliares. El tipo de entrada se establece en función de las "clases de objeto" ("object classes" en inglés) que estén asociadas a la misma. Las clases de objeto están divididas en tres tipos:

- Abstractas: definen características base para ser heredada por otras clases (no por entradas). Todas las clases derivan de la superclase abstracta denominadfa "top".
- Estructurales: definen las características de las entradas del DIT. Es decir, que representan objetos del mundo real.
- Auxiliares: definen características adicionales (atributos adicionales) que se pueden incluir a las entradas del DIT.

Cada entrada debe derivar de al menos una o mas clases estructurales y cero o más clases auxiliares. Las clases estructurales definen atributos obligatorios *que generalmente* (aunque no siempre) se usan en el RDN de la entrada. Lo más común es que la clase estructural define un solo atributo obligatorio ("MUST" en el esquema) que en sí, es el RDN de la entrada, y el resto de atributos es opcional

2 RFC4512 (http://www.ietf.org/rfc/rfc4512.txt), sección 2.3.1
3 RFC4512 (http://www.ietf.org/rfc/rfc4512.txt), sección 2.3.2
4 Wikipedia (http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#Directory_structure)
5 RFC4530 (http://www.ietf.org/rfc/rfc4530.txt)
6 RFC4512 (http://www.ietf.org/rfc/rfc4512.txt), sección 2

("MAY" en el esquema).

Ejemplo

Si una entrada deriva de la clase estructural "organization", ésta define como obligatorio el atributo "o", por lo tanto el RDN de la entrada será algo como "o=Sistemas". El sufijo sería el DN del nodo padre, por ejemlo: "dc=empresa,dc=com", por lo tanto el DN de la entrada sería:

o=Sistemas,dc=empresa,dc=com

Nota Importante

Gran parte de la confusión que existe alrededor de LDAP, viene dada por el "atributo identificador" ya que muchas veces se piensa que con este atributo se puede inferir directamente la clase estructural a la que pertenece la entrada. Aunque muchas veces sea así, por ejemplo si el RDN es "o=", se tiende a asumir que la clase es "oraganization", sin embargo hay atributos identificadores tales como el "cn=" que pudiesen derivar de varias clases estructurales. De hecho, "cn" ("common name" en inglés) suele estar presente como atributo en varias clases estructurales y puede usarse indistintamente en el DN, tanto es así que una misma entra puede tener más de un DN ("Alias Names"[7]).

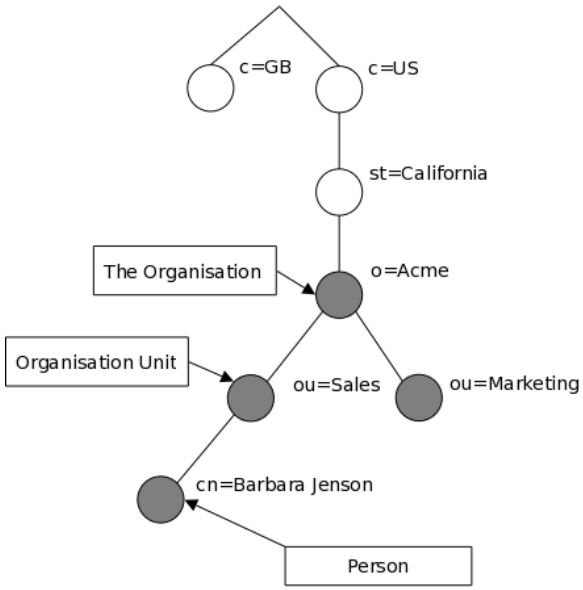
7 RFC4512 (http://www.ietf.org/rfc4512.txt) sección 2.6

Estructura Jerárquica del DIT

Hoy en día se han establecido dos “modelos” principales de estructuras jerárquicas del DIT: la tradicional X.500 y la más nueva basada en el modelo del DNS. Sin embargo, ambas representan solo los lineamientos generales, y no son modelos estrictos en el uso de LDAP. De hecho, una de las fortalezas de X.500 y LDAP es precisamente que el modelo es flexible y adaptable en el tiempo a las necesidades particulares de cada organización.

Forma X.500

El modelo X.500 se basa fundamentalmente en divisiones geográficas y organizacionales[8]:

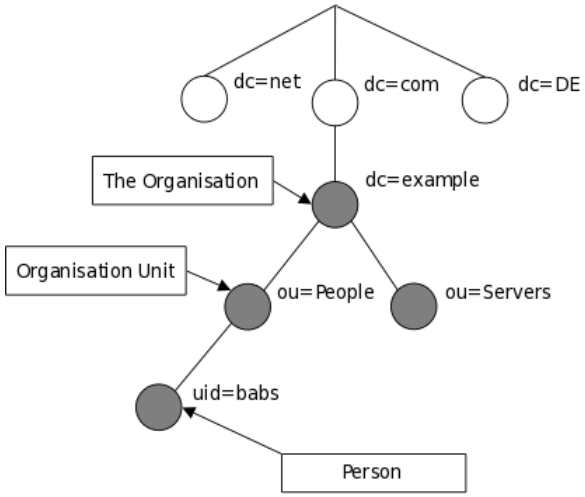


El nodo raíz suele ser el país, y luego la estructura se subdivide geográficamente y luego organizacionalmente en organizaciones y unidades organizacionales.

8 Imágen tomada de: http://www.openldap.org/doc/admin24/intro.html sección 1.2

Forma DNS

En la medida en que la Internet se ha hecho más popular, se viene usando otra forma de jerarquización basada en DNS:



En este modelo, las entradas están organizadas en función de los dominios y sub-dominios de la organización, para luego llegar a las unidades organizacionales y a las personas.

Modelo Propuesto

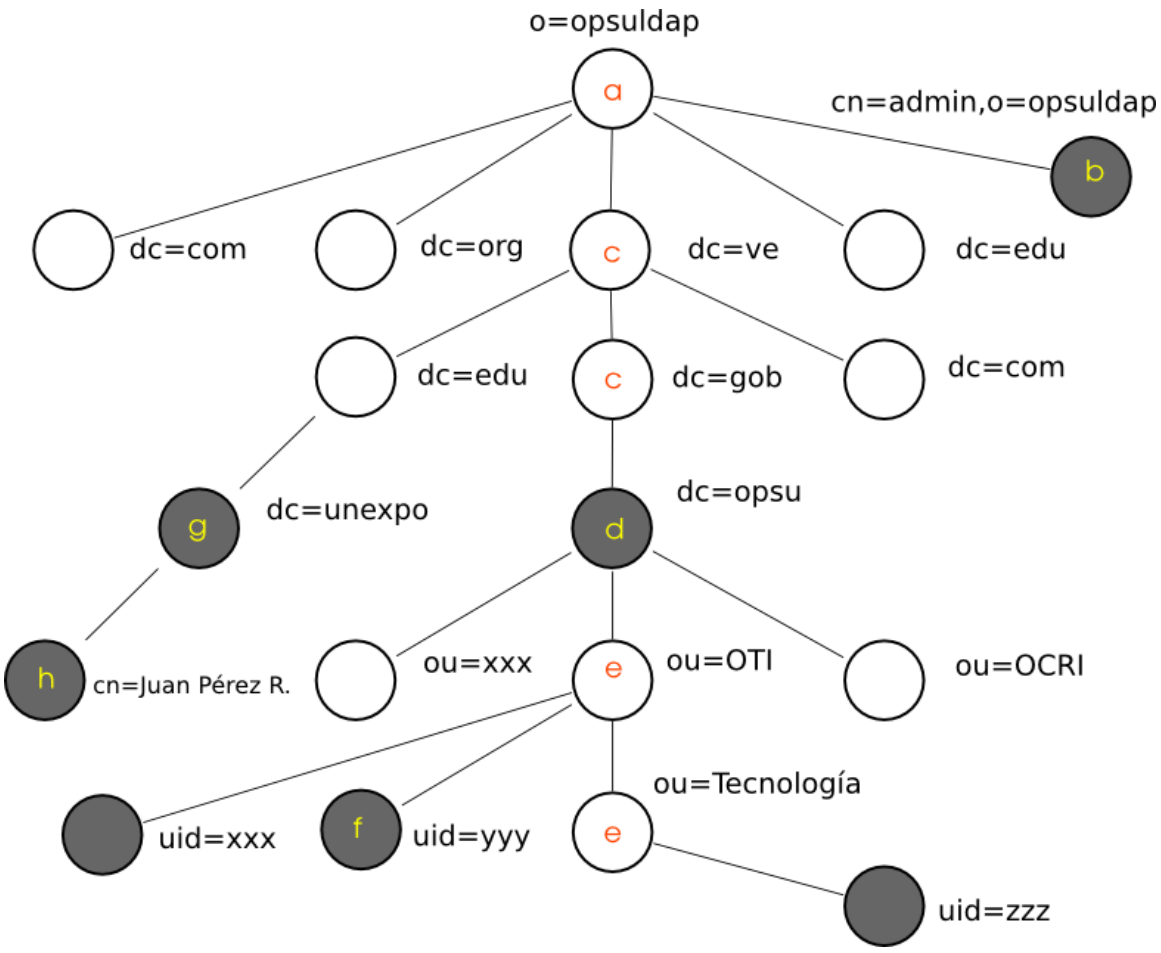
Cada organización debe adaptar estos modelos “base” a sus necesidades particulares ya que la información del directorio puede servir para mucho más que tan solo cuentas de usuario y servidores. Por ende, sugerimos que la Opsu adopte un modelo mixtos que sirva tanto para las necesidades de Infraestructura (cuentas de dominio, correo, etc.) como de Aplicaciones, particularmente el SCD, sistema que depende en gran medida en la información del LDAP.

El modelo que se propone es una combinación entre el modelo X.500 y el modelo DNS, acomodando las necesidades completas de la Opsu. Los niveles son muy sencillos, comenzando por el nodo raíz **opsuldap**, como organización principal y luego los TLD de DNS, seguidos de los docminios y luego unidades organizacionales, y finalmente contactos o elementos reales.

La estructura propuesta no define niveles nuevos fuera de X.500 y DNS, de esta forma el DIT es conforme a los estándares conocidos. Lo que sí se ha hecho es combinar ambos modelos para que el DIT sea muy flexible y moldeable/extensible en el tiempo.

Hay niveles donde se use el mismo atributo RDN, por ejemplo en el caso de las “Unidades” y “Sub-Unidades” de la Opsu, en las cuales se usa el atributo *ou* como atributo RDN. El nivel como tal viene definido por las clases de las cuales derive una entrada (más detalle en). Esta propuesta permite tener un árbol muy flexible y que puede evolucionar en el tiempo y adaptarse fácilmente a los cambios:

Ejemplo del Modelo Propuesto



Clases Usadas en el Modelo Propuesto

Como se menciona arriba, solo se usan los atributos de RDN más comunes tales como: *o*, *dc*, *ou*, *cn* y *uid* principalmente. El nivel viene dado tanto por la clases principales de las entradas, así cómo de algunos atributos importante, por ejemplo, tanto “Unidades”, como “Sub-unidades” usan el atributo *ou* como RDN, y se diferencian por el atributo *tipoOU*, que es un atributo local definido en la clase *opsuObject* el cual puede tener los valores “

(a) top, organization

Atributo RDN: o

(b) organizationalRole

Atributo RDN: cn

(c) domain, dcObject

Atributo RDN: dc

(d) dcObject, organization, opsuObject

Atributo RDN: dc

Atributos Importantes:

- businessCategory: [interna|externa]
- codigoDistribucion: Ejemplo: FOR-4200-001
- codigoRuta: Ejemplo: FOR-4100-016
- o: igual al dc

(e) organizationalUnit, opsuObject

Atributo RDN: ou

Atributos Importantes:

- businessCategory: [interna|externa]
- codigoUnidad: Ejemplo: 3700
- siglas: Ejemplo: UAFS
- tipoOU: [unidad|subunidad]

(f) person, organizationalPerson, inetOrgPerson, posixAccount, opsuObject

Atributo RDN: uid

Atributos Importantes:

- cedula
- cn: Ejemplo: Nombre I. Apellido S.
- employeeType: Ejemplo: Jefe de Departamento
- gidnumber: según cuenta posix
- givenName: primer nombre
- sn: apellido

- title: Ejemplos: Ing., Lic., etc.
- uid: según cuenta posix
- uidnumber: según cuenta posix
- mail
- otros: todos aquellos existentes (shell, home, etc.)

(g) dcObject, organization

Atributo RDN: dc

Atributos Importantes:

- businessCategory: externa
- o: igual al dc

(h) person, organizationalPerson, inetOrgPerson, opsuObject

Atributo RDN: cn

Atributos Importantes:

- businessCategory: externa
- cedula
- cn
- employeeType: Cargo
- givenName
- sn
- mail
- title: Ejemplos: Ing., Lic., etc.