Contenido

Introdución ao LDAP

Introdución

LDAP (*Lightweight Directory Access Protocol*, Protocolo Lixeiro de Acceso a Directorio) é un protocolo do nivel de aplicación que permite o acceso a un servizo de directorio para buscar diversa información, xa sexan usuarios, grupos, equipos, etc. O directorio é un conxunto de obxectos organizados de forma xerárquica, de forma que o servidor LDAP pode verse como unha base de datos en forma de árbore, que está optimizada para realizar consultas e buscas. O servizo LDAP é moi utilizado para a autenticación de usuarios.

Estrutura do LDAP

A estrutura dun directorio baséase nos seguintes elementos:

- Un **directorio** é unha árbore de **entradas de directorio**.
- Unha entrada (equivalería a un obxecto) ten un conxunto de **atributos** (non teñen ningunha orde específica). Entre os atributos dunha entrada están os **objectClass**, que indican a que clases pertence a entrada e polo tanto os atributos que pode ter.
- Un atributo ten un nome e un ou máis valores. Os atributos son definidos nun **esquema**.
- Cada entrada ten un identificador único, o seu **Nome Distinguido** (*Distinguished Name*, DN). Este consta do seu Nome Distinguido Relativo (*Relative Distinguished Name*, RDN) formato por algún ou algúns atributos da entrada, seguidos do DN da entrada pai.

Un servidor LDAP almacena unha subárbore que comeza por unha entrada específica, por exemplo *dc=omeucentro,dc=local* (onde **dc** indica *domain component* ou compoñente de dominio) e os seus fillos.

O formato LDIF

O formato LDIF (*LDAP Data Interchange Format*) permítenos introducir e extraer as entradas do servidor LDAP mediante arquivos de texto (hai que ter en conta que LDAP por si mesmo é un protocolo binario). Aquí pódese ver un exemplo dun ficheiro LDIF coa información dun usuario:

```
dn: cn=carlos,dc=iescalquera,dc=local
cn: carlos
givenName: Carlos
sn: Insua
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: carlos@edu.xunta.es
manager: cn=barbara,dc=iescalquera,dc=local
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Onde:

- **dn** é o nome da entrada, e non é un atributo ni tampouco parte da entrada.
- **cn=carlos** é o nome distinguido relativo
- **dc=iescalquera,dc=local** é o nome distinguido da entrada do pai, onde *dc* indica compoñente de dominio(*domain component*).
- As outras liñas conteñen os atributos da entrada. Os nomes de atributos son xeralmente cadeas mnemotécnicas, como "cn" para nome común(*common name*), "mail" para dirección de e-mail, "sn" para apelido(*surname*), etc.

Características técnicas do servizo LDAP

- A última versión do protocolo LDAP é a versión 3 (LDAPv3), que ofrece como principais vantaxes con respecto á versión anterior (LDAPv2) o uso de conexións seguras con TLS/SSL e autenticación con SASL, uso do xogo de caracteres Unicode, e unha maior estensibilidade, polo que se recomenda utilizar sempre esta última versión.
- O protocolo LDAP utiliza o porto TCP 389, e o protocolo LDAPS (versión segura do protocolo que cifra os datos transmitidos) usa o porto 636.

Características de OpenLDAP

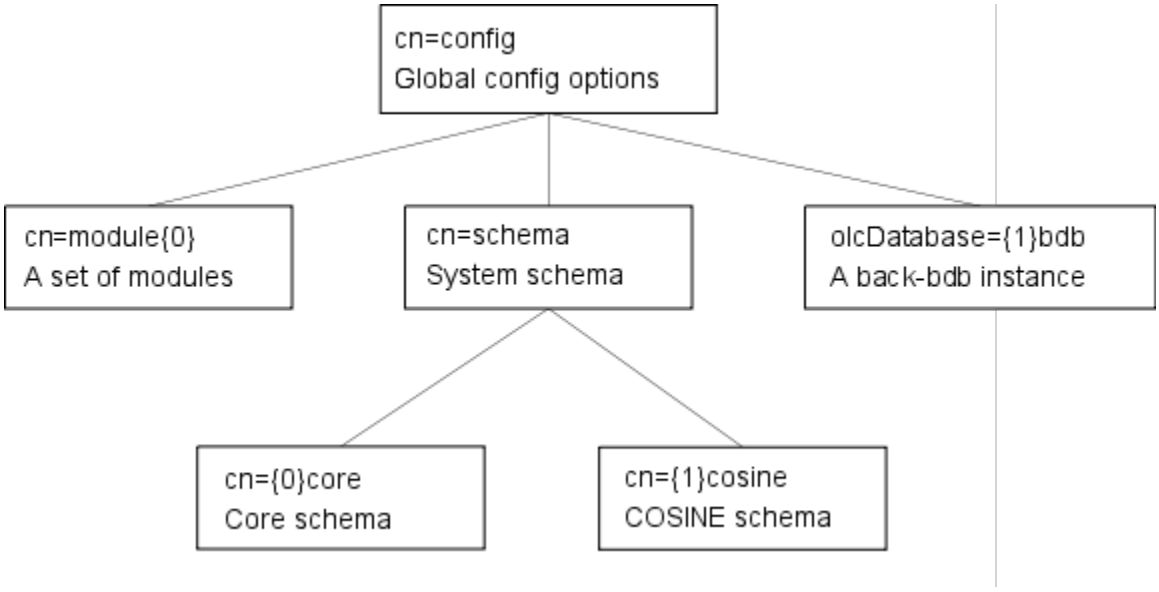
OpenLDAP (http://www.openldap.org) é unha implementación libre do protocolo que soporta múltiples esquemas, polo que pode ser usada para conectarse a calquera outro LDAP. OpenLDAP ten tres compoñentes principais:

- slapd : demonio de servidor LDAP autónomo.
- Librerías que implementan o protocolo LDAP.
- Utilidades, ferramentas e clientes, como *ldapsearch*, *ldapadd*, *ldapdelete*, etc..

Configuración básica de OpenLDAP

Ata a versión 2.3 de OpenLDAP, a configuración básica do servidor era almacenada no ficheiro de configuración *slapd.conf*. En cambio, nas versións actuais a información de configuración do servidor tamén se xestiona co formato LDAP e pode ser modificada usando ficheiros LDIF. Esta información de configuración é almacenada no directorio *slapd.d*, que no caso se Ubuntu Server se atopa dentro de */etc/ldap*.

Desta forma, teremos un directorio ou unha *rama* (se vemos a información almacenada como unha árbore) especial no LDAP con un esquema predefinido para almacenar toda a información de configuración, que inclúe opcións globais de configuración do servidor, módulos dinámicos que se queren cargar, esquemas e configuración dos distintos *backends* (esquemas de almacenamento) e bases de datos do LDAP. Este directorio especial comeza na entrada **cn=config**, e segue a estrutura que se mostra a continuación:



Na páxina do OpenLDAP pódese atopar información detallada sobre as distintas directivas que aquí se poden introducir: http://www.openldap.org/doc/admin24/slapdconf2.html#Configuration%20Directives