OpenLDAP

Akshay Pushparaj

Introduction to LDAP

What is LDAP?

LDAP or Lightweight Directory Access Protocol is a standards-based protocol for accessing and maintaining distributed directory information services. LDAP has always been considered a standard for user management in organizations of all sizes.

What is directory service?

- Directory is a specialized database specifically designed for searching and browsing, in additional to supporting basic lookup and update functions.
- Directories tend to contain descriptive, attribute-based information and support filtering capabilities.
- Directories generally do not support complicated transaction or roll-back schemes found in database management systems designed for handling high-volume complex updates.
- Directories are generally tuned to give quick response to high-volume lookup or search operations.

What kind of information can be stored in the directory?

LDAP information model is based on entries. An entry is a collection of attributes that has a globally-unique Distinguished Name (DN). The DN is used to refer to the entry unambiguously. Each of the entry's attributes has a type and one or more values.

How is the information arranged?

Directory entries are arranged in a hierarchical tree-like structure.

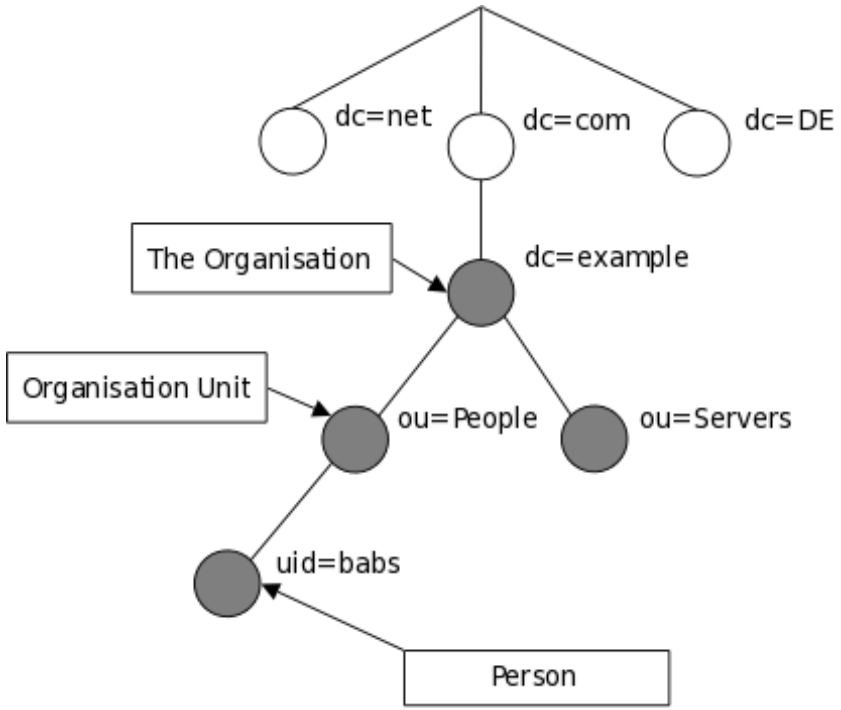

Figure 1: LDAP Tree

Differences between traditional databases

- LDAP is a open standard protocol.
- LDAP is heavily read optimized.
- LDAP is lightweight.

Usecases

Some of the usecases of LDAP are:

- Machine Authentication
- User Authentication
- User/System Groups
- Address book
- Organization Representation
- Asset Tracking
- Telephony Information Store
- User resource management
- E-mail address lookups
- Application Configuration store Machine Authentication
- etc

OpenLDAP

What is OpenLDAP?

- OpenLDAP is an free and open source implementation of LDAP. The project started at University of Michigan, now maintained by the OpenLDAP Foundation.

Features

- Lightweight
- Supports a wide variety of backends or databases.
- Supports components called overlays which can be used to customize backend behaviour without the need to write a custom backend.
- Has support for wide variety of OS and services.
- OpenLDAP is highly flexible. Has code-reliant functionality which doesn't lock users into predetermined workflows; rather, we can manipulate the software to our exact needs.

Cons

- Directory configuration and management are manual.

Alternative LDAP implementation

389 DS and FreeIPA

- Like OpenLDAP, 389 DS or 389 Directory Server is a LDAP implementation by RedHat as part of the community-supported Fedora project.
- 389 DS have a graphical interface that can be used for administration.
- FreeIPA is an identity management system created by RedHat. The aim with FreeIPA is to provide a centrally managed Identity, Policy and Audit(IPA) system.
  - Identity management ensure the right users have appropriate access to resources.
  - Security policies are a set of requirements to maintain a safe and secure computing environment.
  - Audit trail are records of events, procedures or operations being done on the system.
- FreeIPA uses a combination of different software inorder to