General Precautions on the LDAP Directory

ENT Installer

This document aims to record feedback from experience on the organisation of the LDAP directory and its consequences on the ENT Installer configuration.

LDAP directory: definition reminder

An **LDAP directory** is a set of data organised in a hierarchical form containing mainly descriptions of business objects related to the architecture of the information system. It is originally a technical service intended to catalogue IT resources and its users. By extension of the model, more and more business definitions are now included in it, provided they respect the basic principles of directory organisation:

Object class

A directory can store definitions/descriptions (attribute sets) relating to elements of different natures. Object classes make it possible to fill in and label these different types of records. Object classes can be standard ones generic to LDAP, provided by standard directory models, or fully customisable.

Typical examples:

- (objectClass=user)
- (objectClass=posixAccount)
- (objectClass=organisationalPerson)

User

Users record people who will have a certain number of rights in certain applications.

Machine

An LDAP directory can list machines, computer workstations, servers and other elements of the IT estate in which users may have accounts, access and rights.

Application

An LDAP directory can describe applications or programs in which users may have accounts, access and rights.

Groups

A directory can define groups containing members that can be any other LDAP description (including other groups)

Context

An LDAP directory is organised hierarchically in a tree of nodes (directories) in which entries or sub-nodes are found. Each entry has a unique “perfectly identified” identity **(DN)** composed of the full path of the entry's placement up to the root.

Precautions in structuring

Directory structuring errors can lead to poor directory exploration performance, which can cause temporary overloads of the directory for other services, or abnormally long synchronisation times.

Preferably, models that will be favoured are those that:

- Provide separate contexts where the synchronisable business entities are well isolated from other definitions
- Isolate the hierarchies storing people from those storing groups and from those storing other types of entities.
- Provide a hierarchy of reduced depth
- Do not overuse references in attribute values, or provide an alternative means of finding the final values quickly.

Precaution in querying

Query filters can in no case use a partial search on DNs (distinguishedName). The DN is not an attribute of an LDAP entity, even if its value can be retrieved in a query result.

Back to the component index - Back to the technical guide - Back to the plugin index - Back to the catalog

From:
https://docsen.activeprolearn.com/ - **Documentation Moodle ActiveProLearn**

Permanent link:
https://docsen.activeprolearn.com/doku.php?id=local:entinstaller:entity:ldap

Last update: **2026/11/13 21:59**