OpenLDAP™

http://www.OpenLDAP.org

community developed LDAP software

- The Project
  - **Conferences**
  - *Other Publications*
- The Foundation
  - Sponsors
- **Development**
  - *Contributing*
  - Browse Sources
  - Repository Access

- **Software**
  - ***Download!***
  - OpenLDAP Admin Guide
    - ***Quick Start Guide***
  - Manual Pages
  - *Roadmap*

- **Support**
  - *Faq-O-Matic*
  - **Issue Tracking**
  - Mailing Lists
- ***Search!***

Linux Network Services:

Directory Services: LDAP

This material is based on work supported by the
National Science Foundation under Grant No. 0802551

National Science Foundation
WHERE DISCOVERIES BEGIN

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author (s) and do not necessarily reflect the views of the National Science Foundation

C4L4S1

Lesson Overview

If you manage a large corporate network that has several hundred or thousands of machines, you will quickly realize how much duplication of effort is involved with normal administrative tasks.

Routine operations like changing passwords, canceling accounts, and modifying groups become time-consuming if repeated on individual machines. Centralizing user and authentication information can solve these issues.

Lightweight Directory Access Protocol (LDAP) is a set of protocols that has become the Internet standard for accessing information directories. LDAP and Active Directory allow administrators the capability to decentralize information in a secure and reliable manner.

This lesson will introduce the student to the terminology and basic skill sets required to administer both Active Directory and LDAP components.

Active Directory Lightweight Directory Services (A
Windows7

Brief Description

Active Directory Lightweight Directory Services (AD LDS) provides directory services for directory-enabled application. This download pertains to AD LDS for Windows® 7 operating system.

Files in this Download

The links in this section correspond to separate files available in this download. Download th

File Name:	Size:
Windows6.1-KB975541-x64.msu	15.4 MB
Windows6.1-KB975541-x86.msu	14.5 MB

Quick Details

Version: 6.1.7600.16494
Date Published: 2/16/2010
Change Language: English

Microsoft Active Directory

Objective

You should know what will be expected of you when you complete this lesson. These expectations are presented as objectives. Objectives are short statements of expectations that tell you what you must be able to do, perform, learn, or adjust after reviewing the lesson.

Lesson Objective:

Given a need for system interoperability, the student will analyze two directory services (LDAP and Active Directory) and connect both to Linux as per industry standards.

Lesson Outline

In this lesson, you will explore:

- **Overview of LDAP**
  - Directories and databases
  - Benefits & use of LDAP
- **Directory Management**
  - LDAP terminology
  - Namespace
  - Client LDAP operations
  - Access control lists
  - Slapd.conf file
- **Active Directory**

Resources and Notes

You will find the information contained in the following links to be quite helpful. Please select each link and review its contents:

- What is LDAP?
- Introduction to OpenLDP services
- LDAP quick-start guide
- Introduction to LDAP
- Microsoft Directory Services Guide
- Understanding LDAP (Word.doc)

TechNet Library

- Books, Magazines, and Columns
- Customer Relationship Management
- Deployment
- Exchange Server
- Forefront
- Infrastructure Optimization
- Internet Explorer
- Interoperability and Migration
- Networking and Messaging
- Office
- Online Services
- Scripting
- Security and Updates
- Products and Technologies
- SharePoint Products
- Solution Accelerators
- SQL Server

TechNet ▸ TechNet Library ▸ Windows Serv

Active Directory

Chapter 11 from *Introducing Windows 2000 Ser*

On This Page

Overview
Active Directory Components
Managing Active Directory
Security
Use of DNS (Domain Name System)
Global Catalog
Replication
Partitioning
Schema: Attributes and Object Classes
Objects
Standard Object Classes
Lightweight Directory Access Protocol (LDAP)
ADSI (Active Directory Service Interface)
Planning Your Network for Active Directory
Summary

What is LDAP?

Directories help people find their way by showing or pointing to the location of relevant items . When you enter a hospital or large facility, one of the first things we look for is a directory to show us where the emergency room or the X-ray lab may be located. Computer directories serve the same purpose. They point users to the desired information in a quick and efficient manner.

LDAP is a protocol or set of specifications that define how data is stored and retrieved in an information directory. LDAP allows users to centralize data management which results in increased efficiency and decreased support costs. LDAP allows one or two administrators to remotely manage directory information all over the world using an LDAP server. By decreasing the number of people managing data, efficiency and data integrity are improved at minimal cost.

LDAP was pioneered at the University of Michigan, and a free implementation of LDAP is available from their web site along with documentation, source code, and other resources.

Select **PLAY** below for a video introducing CUPs.

View Video
VideoLesson4LDAPIntro(C4L4S6).mp4

Data Storage in Directories

A directory is composed of entries. The *entry* is the basic unit of the directory. An entry may contain information such as a name, address, email contact, fax, and phone number. Entries in the directory have the same type of data but individual data sets are different. For example, the *name* data would all be listed as *names* but the data itself would be different (John Doe and Mary Smith are both names).

The information associated with an entry is called the *attributes* of the entry. An entry is essentially a collection of attributes. In our earlier example, the person's name and phone number are attributes of that person's entry in the directory. Depending on how the directory is set up and initiated, entries can have a set of mandatory attributes as well as a set of optional attributes.

Think of a directory as a repository that stores objects. The directory serves the purpose of arranging the objects and their extended details (attributes). A directory usually describes an object such as a person, a printer, a server or some other resource. Each entry has a name called a **distinguished name** (DN) that UNIQUELY identifies it (also called a key). The DN consists of a sequence of parts called *relative distinguished names* (RDN's), much like Windows and Unix files contain path names to identify the complete file.

Required Reading

- Introduction to LDAP
- LDAP DN
- Distinguished Name

Data Storage in Directories (Contd)

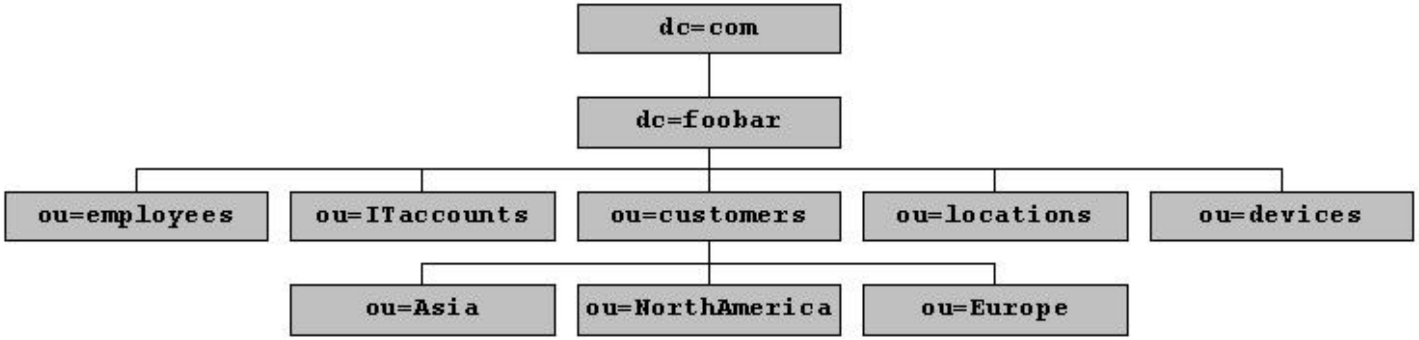


Image from ldapman.org

*Select **PLAY** below for videos on directory services.*

View Video
VideoLesson4TreeDirectory(C4L4S8).mp4

Tree directory video

View Video
VideoLesson4DirectoryServices(C4L4S8).mp4

Directory services

Recommended Reading

- Directory tree design

Object Classes

There is a special attribute that is mandatory for all entries, called the **objectclass** attribute. This attribute determines what rules the entry follows. These rules establish the content of the entry by specifying the set of attributes that are considered mandatory and another set that is considered optional.

At the most basic level, the object class defines what attributes can be used in the entry. The schema of the directory determines which object classes are available in the directory.

The schema essentially defines the set of rules the directory data must follow. Several default schemas are included with most LDAP installations.

Note: Schemas are not selected by the installation default configuration though.

Required Reading

- ObjectClass Attributes

Directories & Databases

A directory is a specialized database, but in reality, it is much more complex. The basic functionality of an LDAP server is similar to a database but optimized for fast reading of static information (information that does not change frequently). Passwords and groups are good examples of relatively static information that needs to be read quickly.

Directories are normally used to search, view, or compare information (read processes) while databases are used to write, store, and read information. As such, both are designed at the programming level to be optimal for their required tasks. Directories read information in an efficient manner, while databases write and store information in an efficient manner.

Directories are suited for several commonly required purposes such as specialized data storage systems and for objects that need a hierarchy. Directories can be replicated across servers to allow access from multiple locations. Text-based information is particularly well suited for a directory because text can be easily searched. However, any type of data can be stored in a directory.

A directory may consist of personal information and tags that link to an image of someone associated with the data. You should not think of a directory as just a repository for text data. Text may be linked to various kinds of data objects depending on the directory design and structure.

Benefits & Uses of a Directory

- **Make network administration easier**
  - Central management of people information
  - Central management of computer and machine configuration
  - Central management of user accounts
  - Reduced support costs from centralized management
- **Unify access to network resources**
  - Uniform naming convention
  - Potential for single login to network resources
- **Provide single destination for users to search for information**
  - Contact information
  - Central location of network resources
  - Potential as a catalog for any kind of data (e.g. product documentation)
- **Improve data management**
  - Improve the consistency of data that is widely used
  - Provide centrally managed security for business-critical data
  - Organize data in a logical structure
- **Help streamline business processes**
- **Provide repository and lookup for application and service data**

This information is from pearsonhighered.com (pg 17)

Required Reading

- LDAP Vs Database
- Directories compared
- Differences
- LDAP Overview

Users of LDAP & Directory Services

“Often people that use LDAP are not even aware they are using it. It is the protocol used to access your corporate e-mail directory. LDAP may be consulted every time you access a private web page, and it often stores configuration for the services you access. In these applications and others, LDAP provides the behind-the-scenes support needed to control access to resources and look up information. LDAP has also been used for applications ranging from storing and retrieving images to calculating chess moves.”

The answer to who uses LDAP? Everyone does and has!

When to use LDAP?

- ❖ Would you like your data to be available cross-platform?
- ❖ Do you need to access this data from a number of computers or applications?
- ❖ Do the individual records you're storing change a few times a day or less, on average?
- ❖ Does it make sense to store this type of data in a flat database instead of a relational database? That is, could you effectively store all the data for a given item in a single record?
- ❖ Matches unreferenced content word-for-word

Source: LDAP Directories Explained (Pg 10)

Recommended Reading

- Intro to LDAP
- LDAP URLs

For Review

- LDAP from Microsoft

Additional Directory Management

There are many management tasks associated with a directory. Some of these include:

- **Certificate authority management**— Management of certificates, revocation lists, and the certificates used to establish trust between certificate authorities is a critical function.
- **User account management**— People have to log in, and LDAP directories often store the organization's user accounts. Providing account management is a common task.
- **Directory server storage management**— The directory must have space to grow.
- **DNS records**— The records that provide access to the directory are a critical dependency. There is no maintenance needed; but should the records break, you will want to know how to fix them quickly.
- **Performance monitoring**— Perception is everything. Performance monitoring will help you provide a reliable directory that does not seem slow to users. It will help you gauge when to upgrade or add additional servers, and maybe help detect a problem before users do.
- **Backups**— Loss of data is still far too common an occurrence. Have a backup system in place before bringing up a directory.

Source: LDAP Directories Explained – Brian Arkills (pg 163)

LDAP Terminology

Aliases
An alias provides a means to refer to a single entry – (Aliases allow an entry to be in two places at once). An alias provides a useful means of placing an entry in two or more locations in the directory. The LDAP namespace prohibits a Web-like structure; but by using an alias, you can circumvent this restriction for a single entry. This functionality can help to eliminate problems that a structure introduces.

For example Bob Jones's person entry might belong in both the Engineering and Marketing OUs because he fills two functional roles. But these functional roles are not under the same branch in the directory, so two entries are needed. The alias solves this problem. An alias could be placed in one of the OUs and the real entry placed in the other OU.

Namespace
To find information in a directory, a common set of naming rules is needed. These rules are called a *namespace*. Every directory needs a namespace. A namespace refers primarily to how entries are named. However, it can also imply other characteristics such as an organizational structure for the entries. Incidentally, the term "namespace" can also be used in a general sense to refer to all the objects in a specific container.

Recommended Reading
- Aliases
- LDAP Aliases

LDAP Terminology (Contd)

Protocol
LDAP is primarily a set of server operations based on the TCP/IP protocol (required for LDAP-port 389)

Schema
The schema defines the rules. A game without rules is chaotic and subject to the players' whims. The set of rules that defines what types of entries can be in the directory is known as the schema. If a particular object class is not in the schema, you cannot create an entry with that object class. You extend the schema to include a new object class or to allow new optional attributes on an existing object class.

The schema further defines pertinent rules like what type of value can be placed in an attribute, and what operators are valid for those attributes. The operators are what the directory uses to compare one attribute's data value to another value. Greater than, less than, and equality are examples of common data operators.

*Select **PLAY** for a video on schema.*

View Video
VideoLesson4Schema(C4L4S15).mp4

Recommended Reading
- LDAP Schemas
- Schema Specs
- Schema Design

LDAP Terminology (Contd)

Management
Information that is centrally organized in an LDAP directory lends itself to management. In fact, an LDAP directory can become the hub of IT management and can lead to more efficient data management.

The support for LDAP directory management functionality is therefore very important. Management functionality that is easy to use or provides ways to simplify integration is highly desirable. Products are sure to evolve over the next few years to allow for data management in an LDAP environment.

Currently, most data is managed through the CLI using files consisting of data formatted in the LDIF format. This data is then imported into the LDAP directory via the command line.

Source: LDAP Directories Explained – Brian Arkills (pg 38)

*Select **PLAY** for a video on LDIF structure.*

View Video VideoLesson4LDIEStructure(C4L4S16).mp4

Recommended Reading

- LDAP Account Mgr

LDAP Terminology (Contd)

Security
Authentication, authorization, and encryption are needed to secure information. The term security is used in a broad sense in the computer industry. In fact, if you asked one hundred people to define computer security you might get 100 different definitions depending on their experience in the field.

In discussions of computer security, typically two areas are of concern: authentication and authorization. Authentication is the means of proving we are who we say we are. *Authorization* is the means of designating access permissions to users. Privacy is our third area of concerns in networking.

Privacy is the means of ensuring that data is kept safe so that it is available only to those for whom it is intended. Some form of encryption is usually used to keep data private.

Note: LDAP supports cleartext, Kerberos, and SASL for authentication.

Source: LDAP Directories Explained – Brian Arkills (pg 39)

*Select **PLAY** for a video on LDIF structure.*

View Video VideoLesson4LDIFAuthentication(C4L4S17).mp4

Recommended Reading

- Security with LDAP
- Security Issues
- LDAP for Security

LDAP Terminology (Contd)

Replication
Your organization’s decision to implement an LDAP directory may be initially complicated. You will centralize critical information into a single repository and integrate key business processes with this directory. As you and your company plan the process of moving important data to a centralized location, there will be fears of data loss and possibly loss of business. Changes in data structure and implementation of LDAP should be thought out in detail including contingency plans should something go wrong.

Replication is the simplest solution. With replication, you deploy more than a single directory server. The information in the directory is then replicated between multiple directory servers, and the replicated information can be accessed from several points of distribution.

Replicas
A replica is a replicated copy of directory information. The term "replica" refers to the subservient copies of the master partition. The difference between a partition and a replica is subtle. A replica is the replicated unit of the directory.

Source: LDAP Directories Explained – Brian Arkills (pg 124)

Recommended Reading

- Enabling Replication
- LDAP Howto

Various LDAP Servers

Vendor	LDAP Server
Computer Associates	eTrust Directory
Critical Path	CP Directory Server
IBM	SecureWay
Sun AND Netscape	Directory Server (used to be iPlanet and Netscape Directory Server)
Microsoft	Exchange 5.5 AND Active Directory
Netscape	Directory Server (no longer offered)
Novell	eDirectory (formerly NDS)
OpenLDAP	OpenLDAP
Oracle	Internet Directory
Syntegra	Global Directory AND Aphelion Directory
University of Michigan	Slapd (most common)

Namespace

"Namespace" implies that a name is not simply a name, but holds meaning in terms of structure as well. The term takes two different aspects of the directory and seeks to tie them together: how to name things and how they can be organized.

The definition of a service's namespace is critical and should be carefully planned. Namespace allows us to find items in the directory. Without a namespace that we agree on, you and I might be referring to the same thing, but using different languages.

Example… In the postal namespace, a letter is addressed to someone may be as follows:

Person's name
Street number Street
City, State/Province/Region Zip code
Country

This address tells us many things by the way it is constructed and the value of each component, while also uniquely designating the recipient. We know that the person lives in this country, in this state, in this city, etc. Note: Namespace is white space sensitive, so be careful when cutting and pasting data.

Source: LDAP Directories Explained – Brian Arkills (pg 45)

Required Reading

Namespace:

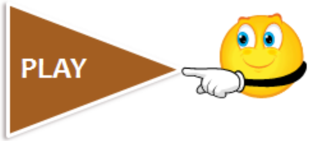
- Namespace (IBM)
- Configuration
- Namespace Structure
- Active Directory

Client LDAP Operations

The LDAP client is what a user sees when accessing a directory. The end user must have an easy way to access and read the information that is contained within the directory.

Easy to use graphical user interfaces such as **phpldapadmin** are available, but are often tricky to configure. Once installed, they simplify the data management process for non-technical type administrators and data entry clerks.

*Select **PLAY** for a Youtube video on phpldapadmin.*



Note: The speaker in the video uses a previous version of Ubuntu that may be different from yours. Your lab work has a few videos defining what you will need to do.

Required Reading

- PHP LDAP Admin

ACLs & Slapd.Conf

Access Control Lists (ACLs)
The Directory ACLs provided by OpenLDAP are simple in their syntax, yet very flexible and powerful in their implementation. The basic idea is to define the users who has access to various resources or privileges. The most frequent privileges include:

- ❖ Read access
- ❖ Write access
- ❖ Modify access

Slapd.conf
Recently, the LDAP standard has changed and does not require a slapd.conf file for the slap daemon to run. Users should research their particular flavor of Linux to see which version of the slap.d daemon that is initiated. As an example, Ubuntu 10.4 and greater has dropped the need for a slapd.conf file but users are finding it difficult to implement. Students are cautioned when installing and configuring the new daemon to use the most recent updated instructions. Many existing websites have improper instructions that can lead to major headaches later.

Required Reading
- Access Control Examples

Active Directory

Active Directory is Microsoft’s proprietary equivalent to LDAP. Like LDAP, Active Directory can be used as:

- Central location for network administration and security
- Information security and single sign-on for user access to networked resource
- The ability to scale up or down easily
- Standardizing access to application data
- Synchronization of directory updates across servers

*Select **PLAY** for two helpful videos.*

PLAY *Overview of Active Directory*

PLAY *Installing Active Directory*

Lesson Summary

Distribution and integration of LDAP directories rely on several critical functionalities. Distributing LDAP directories across multiple servers increases reliability and makes maintenance more manageable.

Centralized data management can lead to more accurate information and more efficient use of remote network services. This functionality also reduces TCO (Total Cost Ownership) and contributes to a company's bottom line profits.

In this lesson, students were introduced to the basic terminology of the LDAP directory service. Students reviewed ACL's, LDAP structure, LDIF's, the slapd daemon, LDAP management, objectclasses and more.

The assignment will introduce students to installing LDAP and adding, listing and displaying information contained in an LDAP server from the client tool phpldapadmin.

LDAP Manual

❖ LDAP Directories