

Introduction to LDAP: “The New Black”

With Two-Factor Authentication by Entrust

WPLUG Tutorial / Presentation

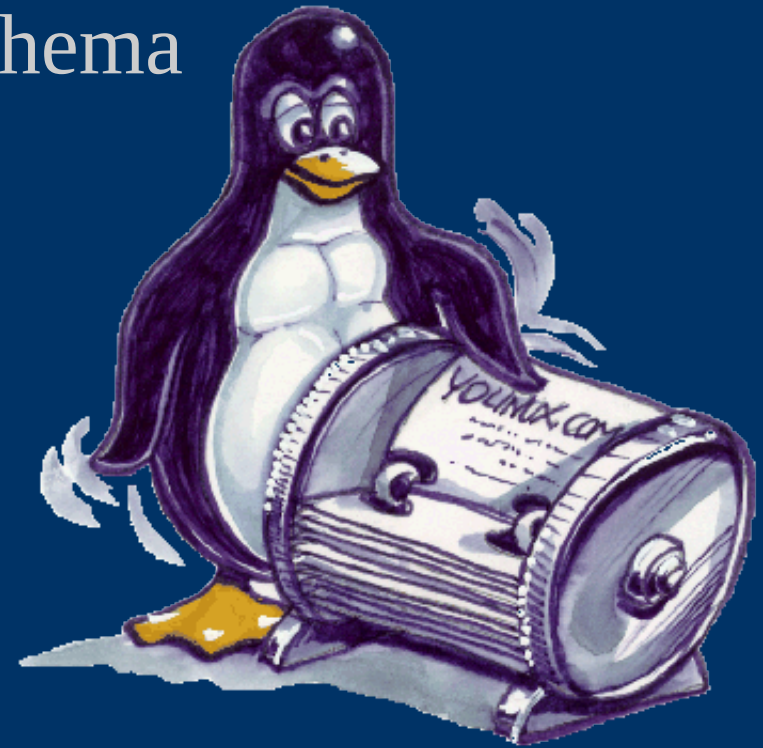
03/2008

Brian A. Seklecki <lavalamp@spiritual-machines.org>



What is LDAP?

- LDAP = Lightweight Directory Access Protocol
- RFC2251, etc..
- What is a directory?
- A database with a quantified schema



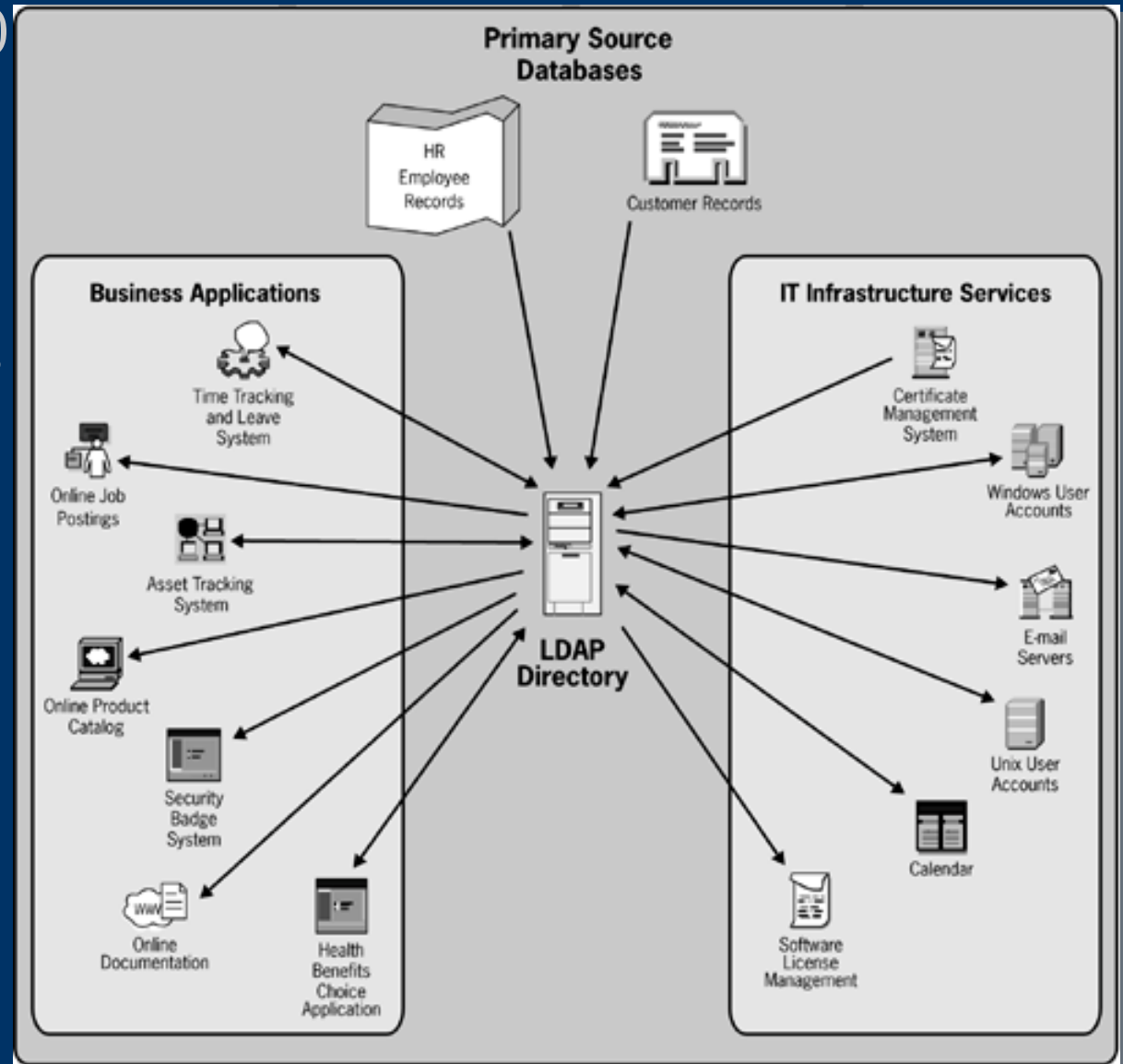
*All the runway models in
London are doing it...*

Don't you want to do runways?



What can the directory store?

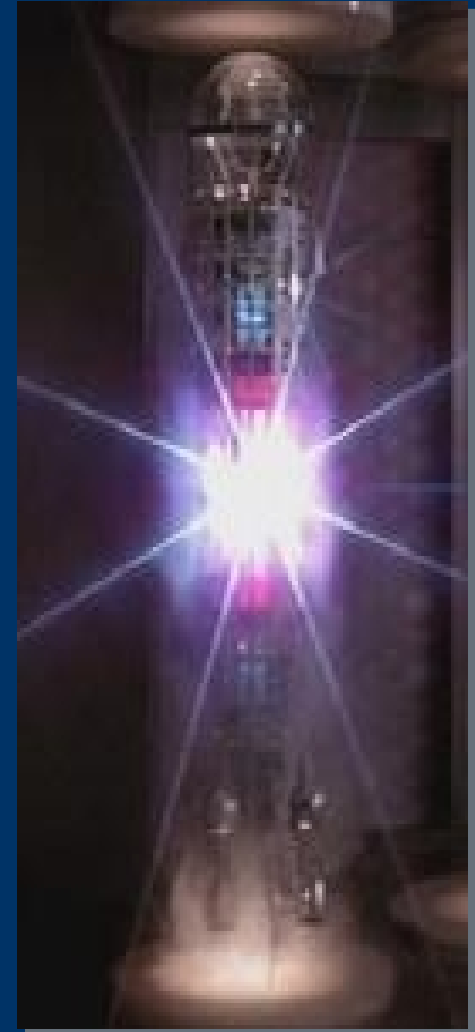
- Identity information
(Employees, Users, Clients)
- Application / System
Groups / Role Membership
- Systems / Servers / Devices
- Departmental / Organization
- Facilities
- Telephony / GIS



What does all of that mean?

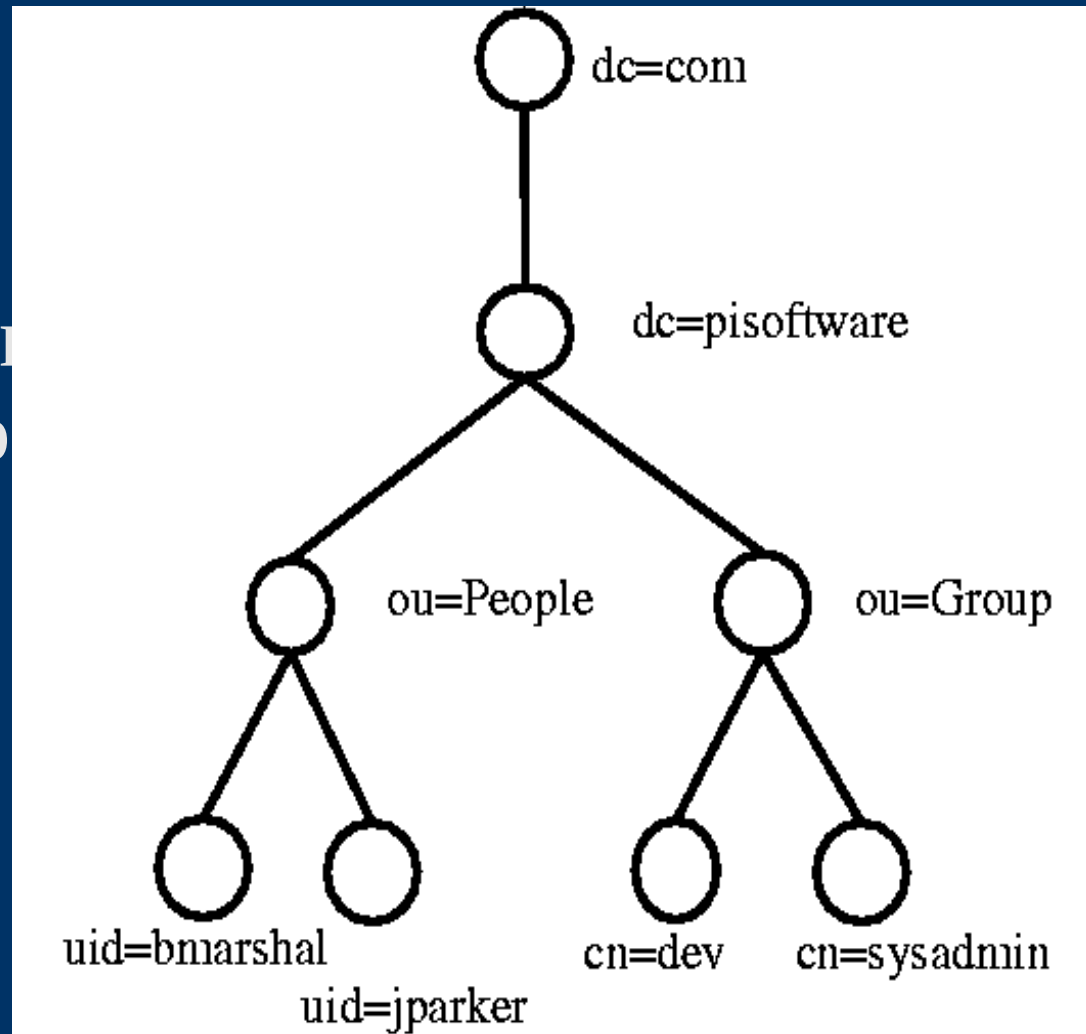
What problems can it solve?

- Centralized identity storage
- Application-neutral format
- Widely supported
- Easily integrates
- Think: Active Directory



The LDAP Directory Layout

- Data is stored in a hierarchy
- Facilities to let you model your LDAP tree after the departmental or geographical structure of your organization
- More details later



LDAP By Itself = Useless

- POSIX Systems for Centralized User Management: NSS + PAM
 - Databases and Applications for Role Population
 - E-Mail Systems for simplified database
 - MUA Address Book population
 - RADIUS (VPN/Wireless/802.1x)
 - VOIP/SIP/H.232 Directories
 - Integrate/Align with PKI (RFC2559)
-
-

When to Use LDAP ?

- When you have more than one user
- And you have at least two systems
- Any heterogeneous environment



When to quit drinking?





OpenLDAP

- Development status: Mature
 - Organizational Model: Dictatorial / Totalitarian
 - Dual-head release engineering cycle
 - Highly portable
 - Modular: Servers, Client, Libraries, Dev
 - Legacy support for Krb/SASL
 - Uses BDB Backend
 - Strong man pages
 - FAQ-o-Matic / vim-style web site
 - License: Custom BSD-Style
 - Responsible Security Posture
-
-

OpenLDAP Pose



Prove it!

- Fedora
- `$ sudo yum install openldap-{client,server,devel}`
- `$ sudo vim /etc/openldap/slapd.conf && sudo \`
`mkdir /var/db/openldap-data`
- `$ sudo chkconfig --level 345 ldap on && sudo \`
`service ldap restart`

More about the Daemon

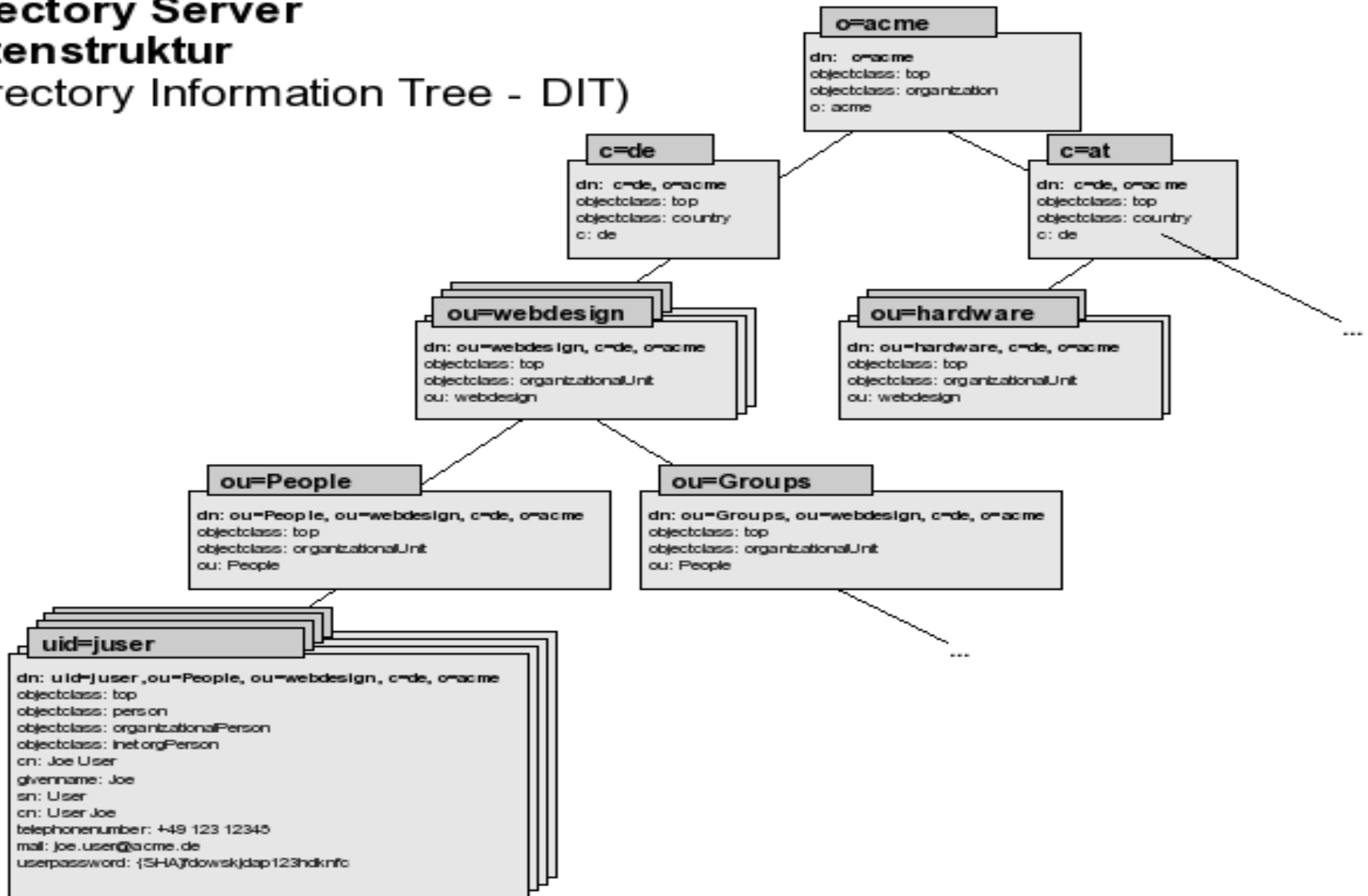
- slapd(8) daemon - TCP listener (SSL/TLS)
 - Two implied nodes: The root, the admin
 - Rest of data is stored in a BDB backend
 - Listens on TCP sockets
-
-

The LDAP Tree (Important Concepts)

- Each node on the tree is accessible by a X.500 name
 - The prefix is defined by the root in the config:
 - - e.g., dc=wplug, dc=org
 - Dc = Domain Control
 - O = Organization
 - Ou = Organizational Unit
 - ex.: “dn: ou=People, dc=wplug,dc=org”
 - A “DN” (Distinguished Name) is any point on the LDAP tree referenced by its unique X.500 Path
 - Syntax in examples, documents is ambiguous
-
-

LDAP Tree Reference Slide

Directory Server Datenstruktur (Directory Information Tree - DIT)



More about DNs

- A DN object is a collection of Attribute + Value pairs
- The valid Attributes in a DN are defined/constrained by the Special Attribute +Value found in each DN known as the objectClass
- Some Attributes can be multi-row arrays
- Some Attributes are required/compelled by the objectClass per the Schema
-



OpenLDAP Interaction / Bindings

- Perl
- PHP
- C
- CLI
- Python



LDAP CLI Utilities

- slapd.conf(5), slapd.access(5), slapacl(8), slapadd(8), slapauth(8), slapcat(8), slapdn(8), slapindex(8), slappasswd(8), slapttest(8), slurpd(8), slapcat(8), ldapadd(1), ldapdelete(1), ldapmodrdn(1), ldapsearch(1)
-
- LDAP Bind Syntax Overview
- Search syntax is LISP-like



Initial Population using slapadd(1)

- \$ slapadd
-
- Common command syntax notes
-
- Example LDIF
-
- Last that you'll see of LDIF



Install PHPLDAPAdmin

- Screen-shot
- Localhost

The screenshot shows the PHPLDAPAdmin web interface in Mozilla browser. The browser title is "phpLDAPadmin - CVS - Mozilla". The address bar shows "http://raider/phpldapadmin/". The interface is divided into two main sections: a left sidebar and a right main content area.

Left Sidebar:

- Sun ONE (schema | search | refresh | create | info | import)
- dc=example, dc=com (4)
 - ou=Company Servers
 - ou=Groups (5)
 - cn=Accounting Managers
 - cn=Directory Administrators
 - cn=HR Managers
 - cn=PD Managers
 - cn=QA Managers
 - ★ Create New
 - ou=People (150)
 - uid=abarnes (selected)
 - uid=abergin
 - uid=achassin
 - uid=ahall
 - uid=ahel
 - uid=ahunter
 - uid=ajensen
 - uid=aknutson
 - uid=alangdon
 - uid=alutz
 - uid=ashelton
 - uid=awalker
 - uid=awhite

Right Main Content Area:

Fax alias
+1 408 555 4661
(add value)

givenName
Anne-Louise
(add value)

I
Santa Clara
(add value)

mail
abarnes@example.com
(add value)

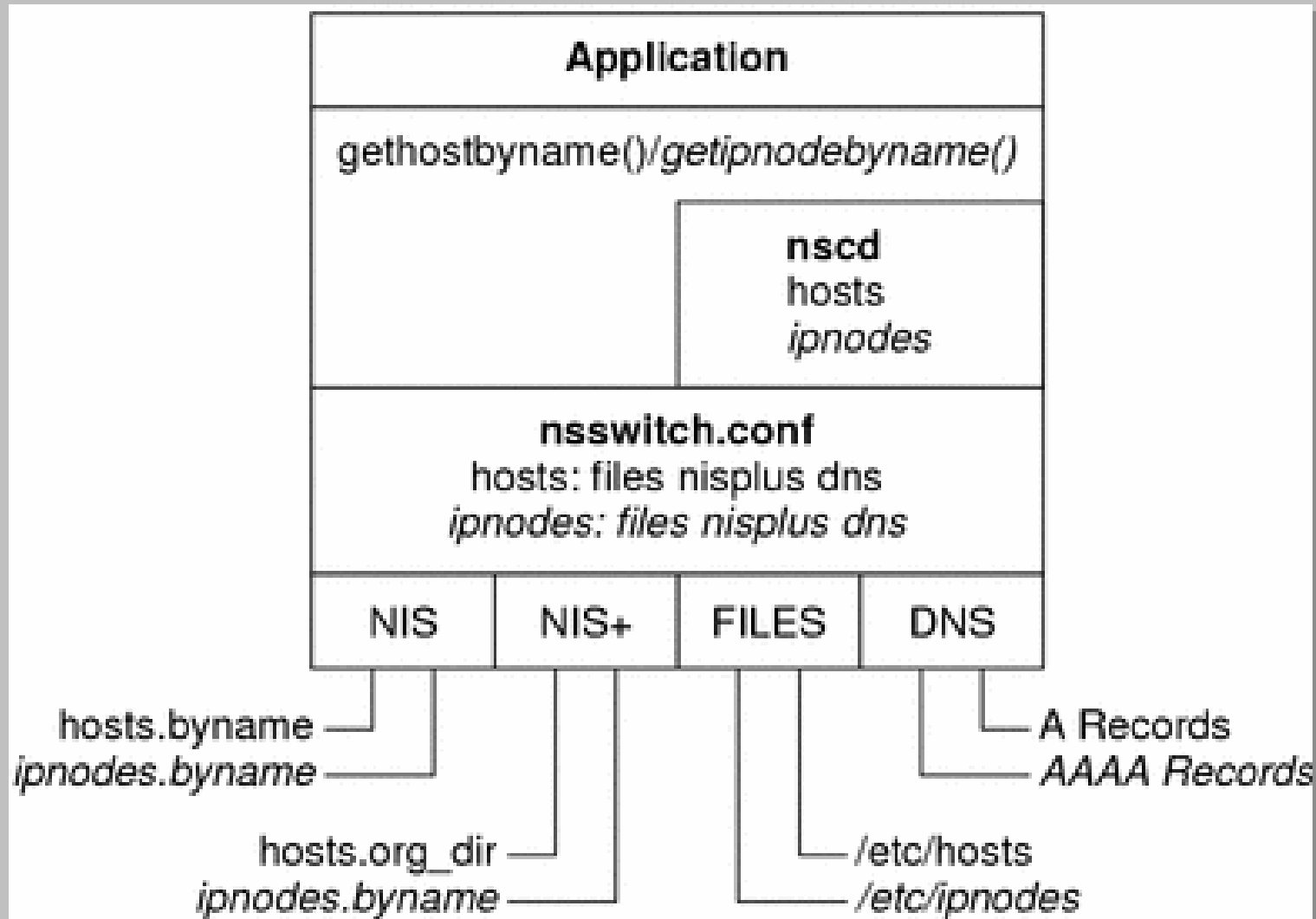
objectClass
top
person
organizationalPerson
inetOrgPerson

ou
Payroll
People
(add value)

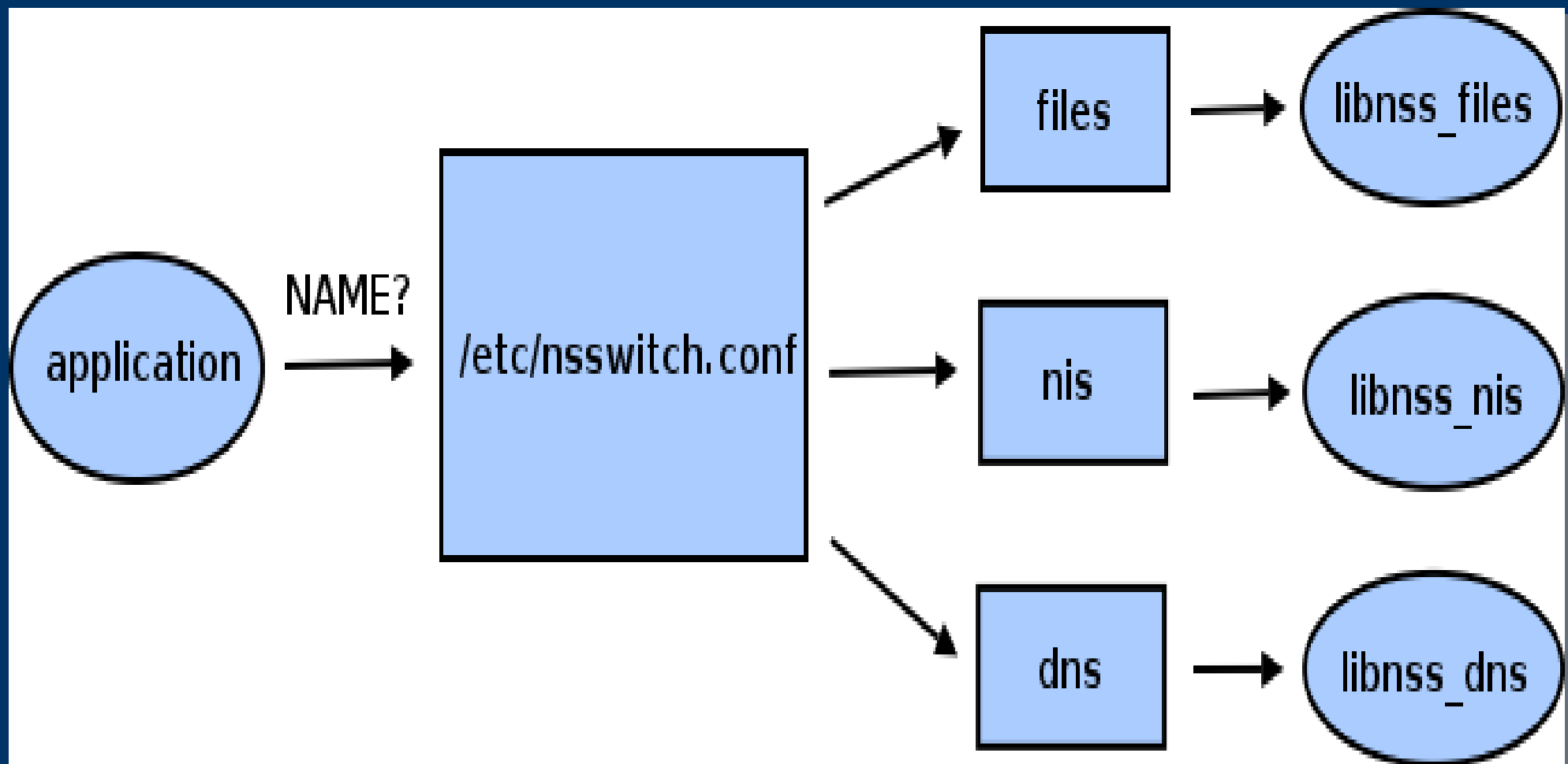
roomNumber
2290

The browser status bar at the bottom shows the URL: "http://raider/phpldapadmin/edit.php?server_id...dn=uid=abarnes, ou=People, dc=example, dc=com".

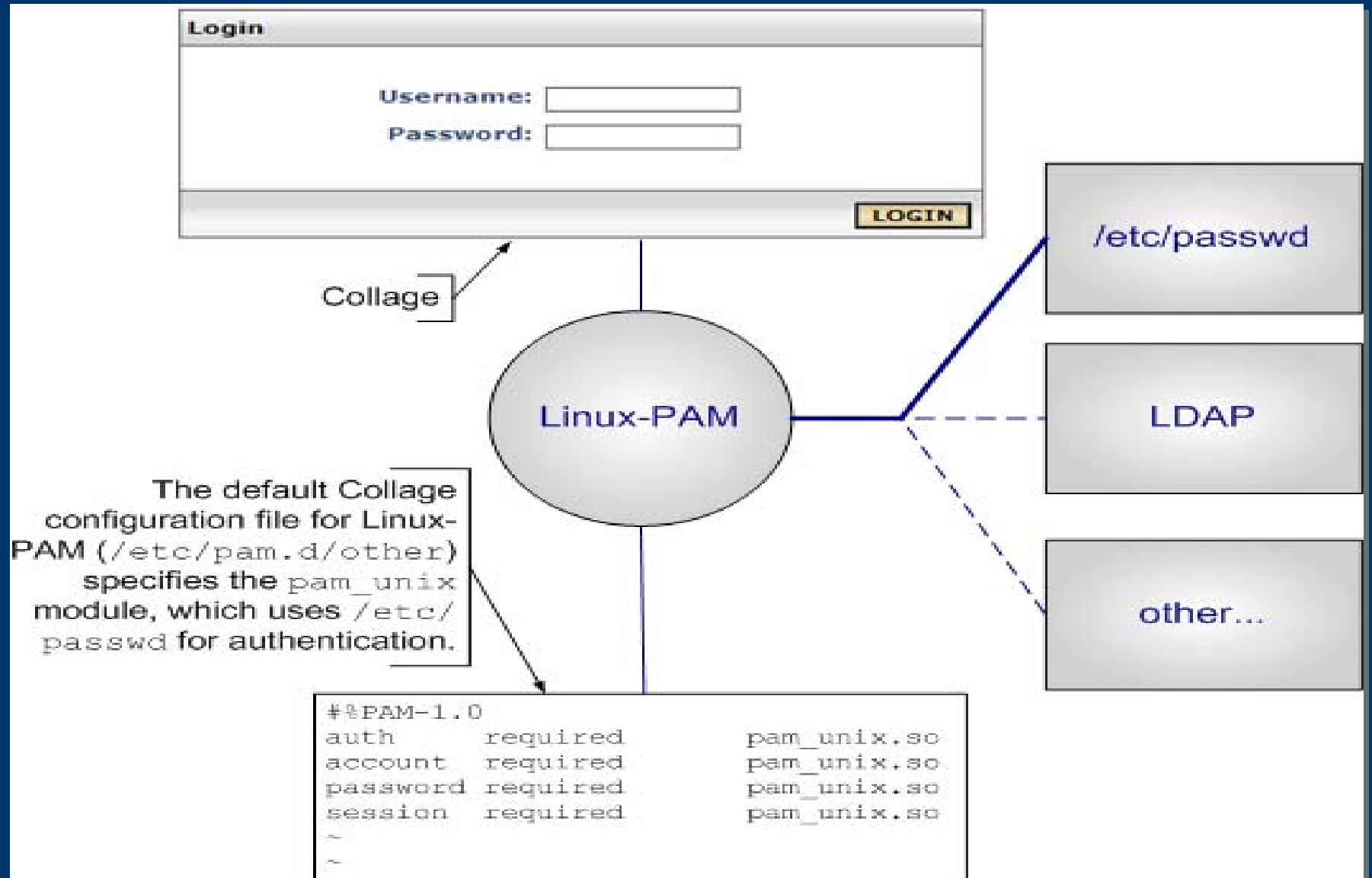
NSS + PAM – libC calls



NSS/PAM API



PAM_LDAP

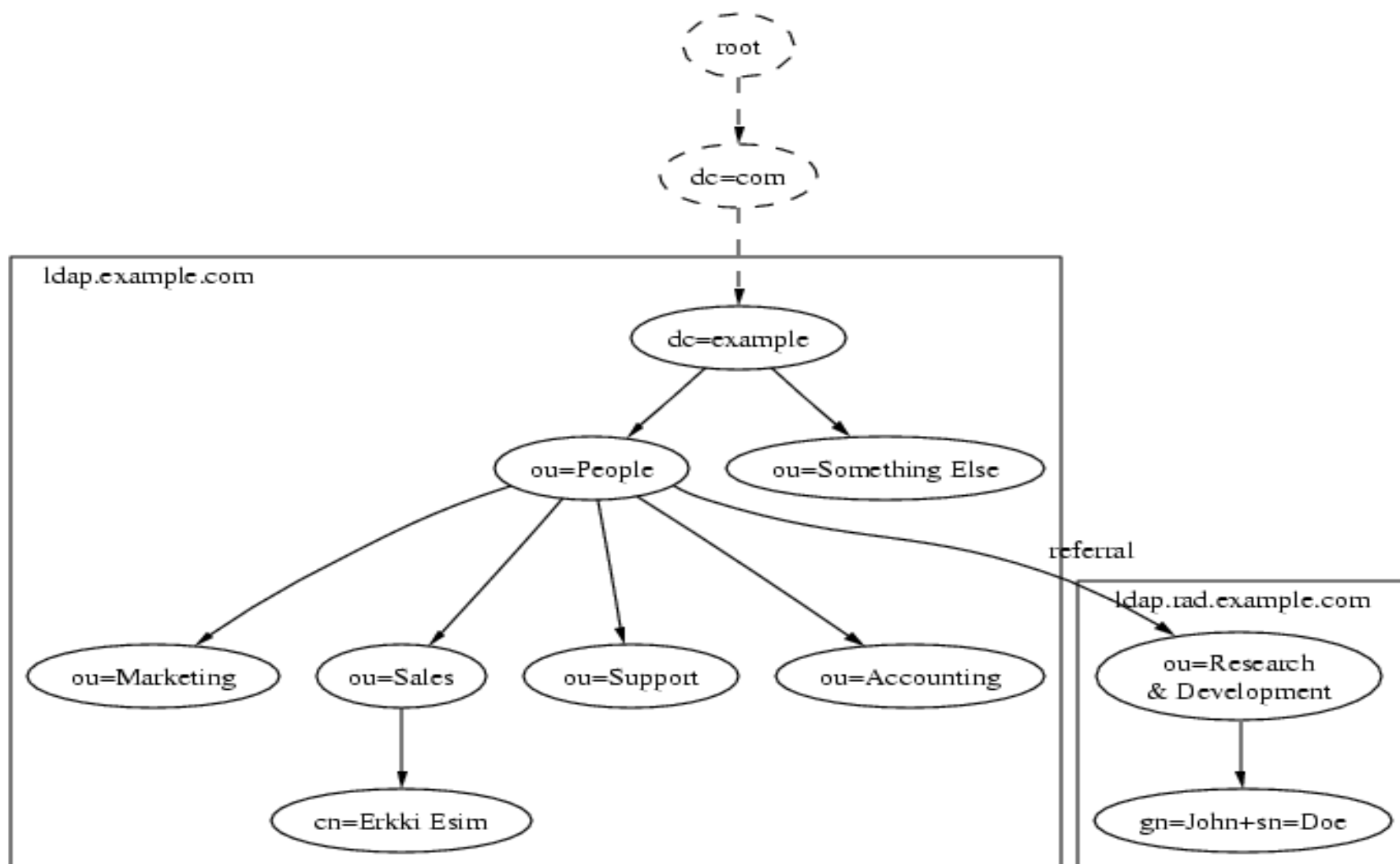


How Groups and Attributes are Used

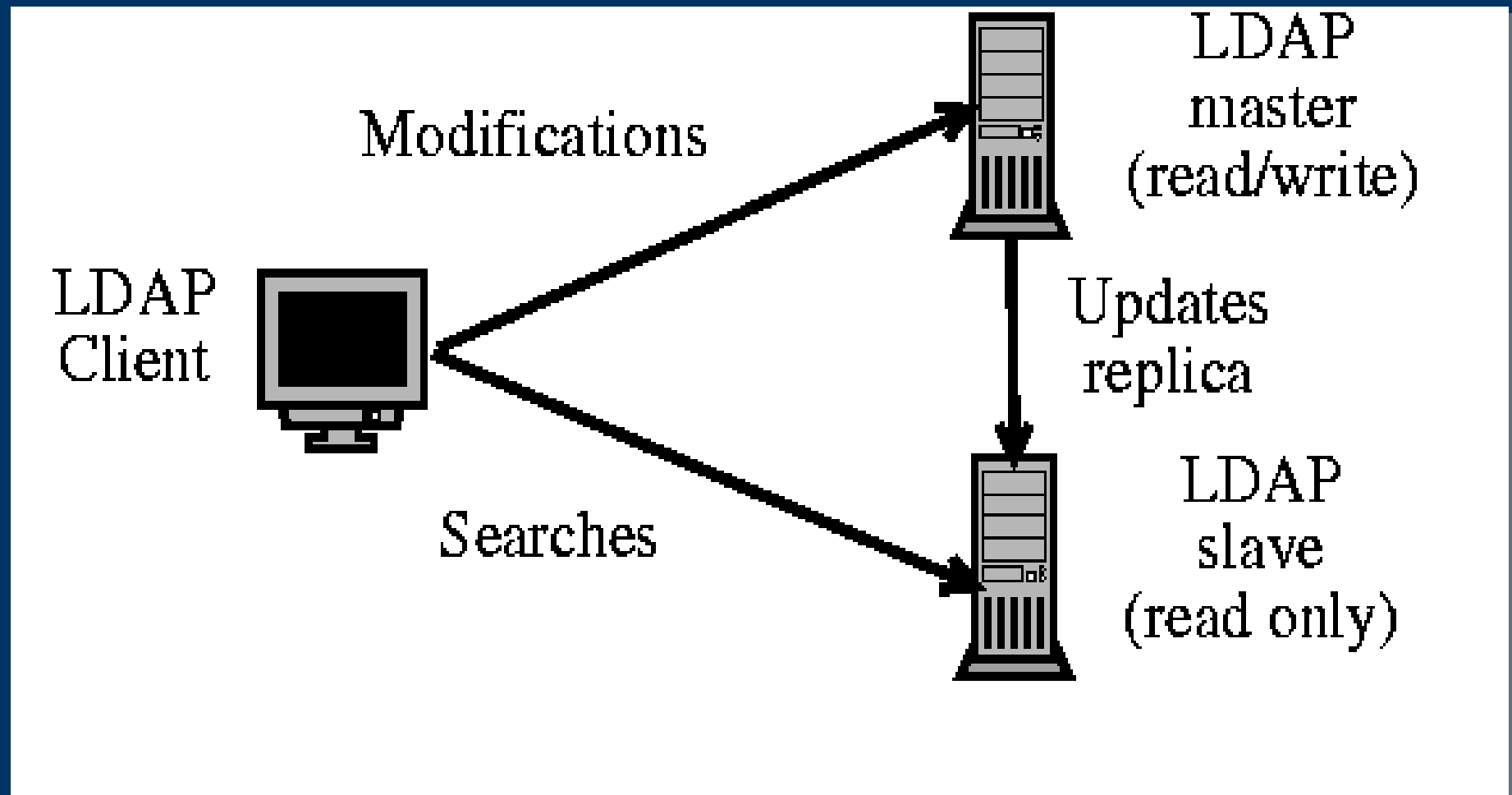
- PAM/NSS
- Apache
- LDAPAuthentication
- Mediawiki
- FreeRADIUS
- Entrust



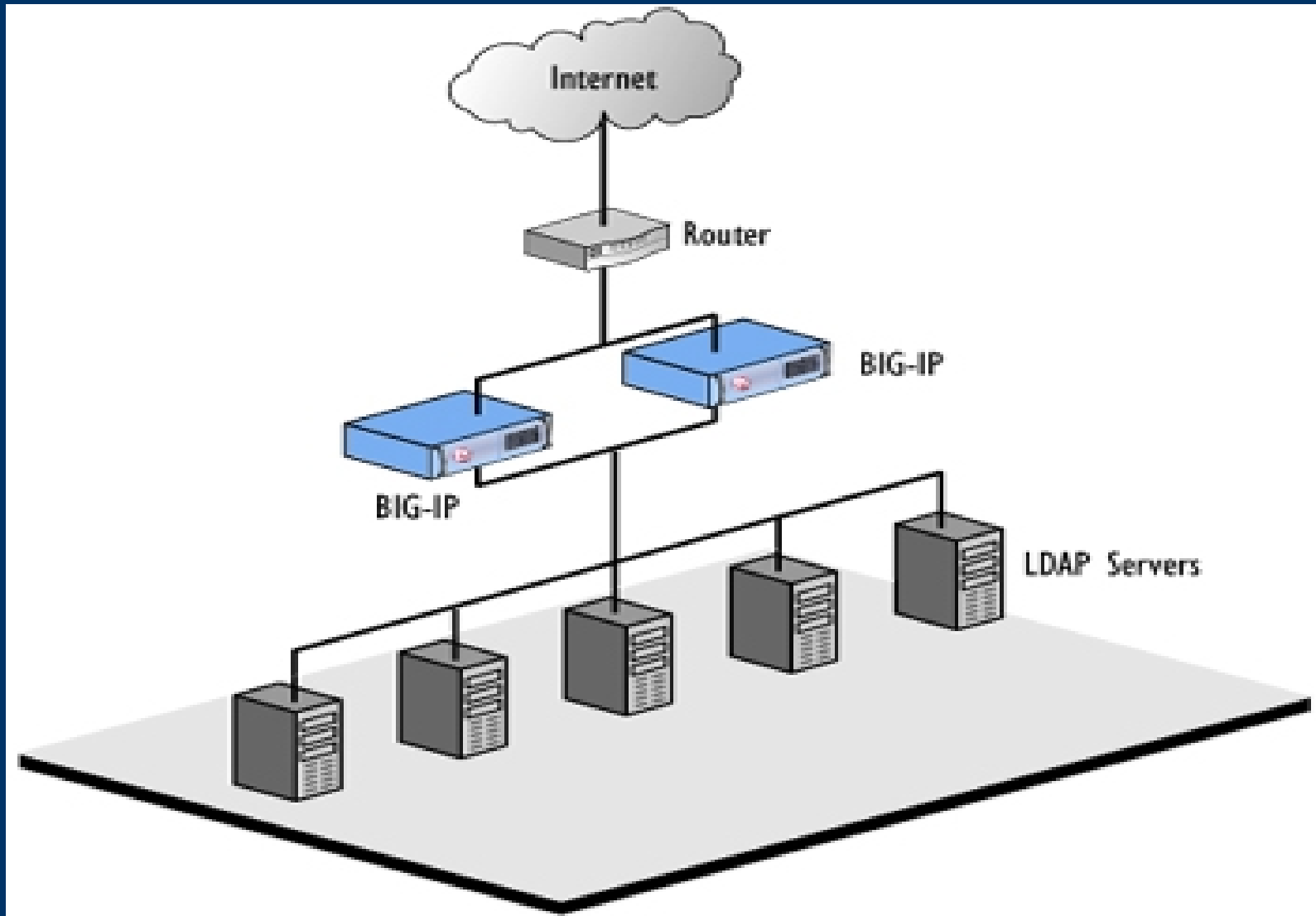
Other: Referrals



Replication



HA with Referrals and Replication



Other: Add a schema

- slapd.conf(5)
 - Add RADIUS



Where do we go from here?

- Lurk the mailing lists
- Install it yourself
- Intermission
- Pizza



Introducing Entrust IdentityGuard

- Two Factor Authentication
- Identity Management
- Linux/POSIX Platform
- Tomcat/Jakarta Platform
- RADIUS (PAM, Dot1x)
- SOAP-XML



Types of Authentication

- Tokens
- Grids
- OTP Lists
- Out-of-Band
- Knowledge-Tokens
- Machine Authentication



Machine Auth
Authorized set
of workstations



Grid Auth
Grid location
challenge and
response



Out-of-Band
One-time-
passcode to
mobile device
or phone



Knowledge Auth
Challenge / response
questions

Number	Passcode
0001	ASUDST22
0002	7SGRKYFZ
0003	HSDJ97DC
0004	GHG1SR4E

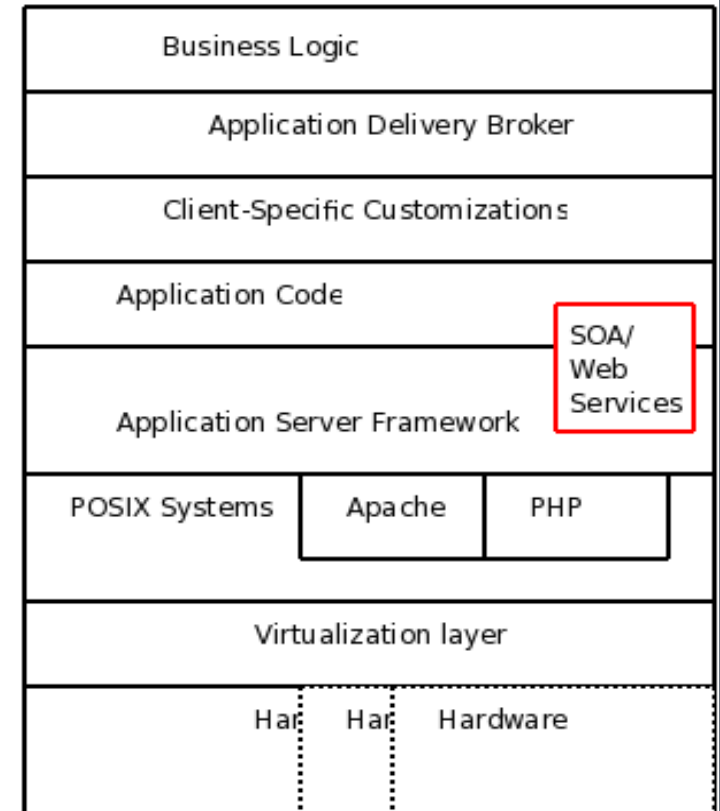
Scratch Pad Auth
One-time
password list



Token
Time-synchronous
hardware device

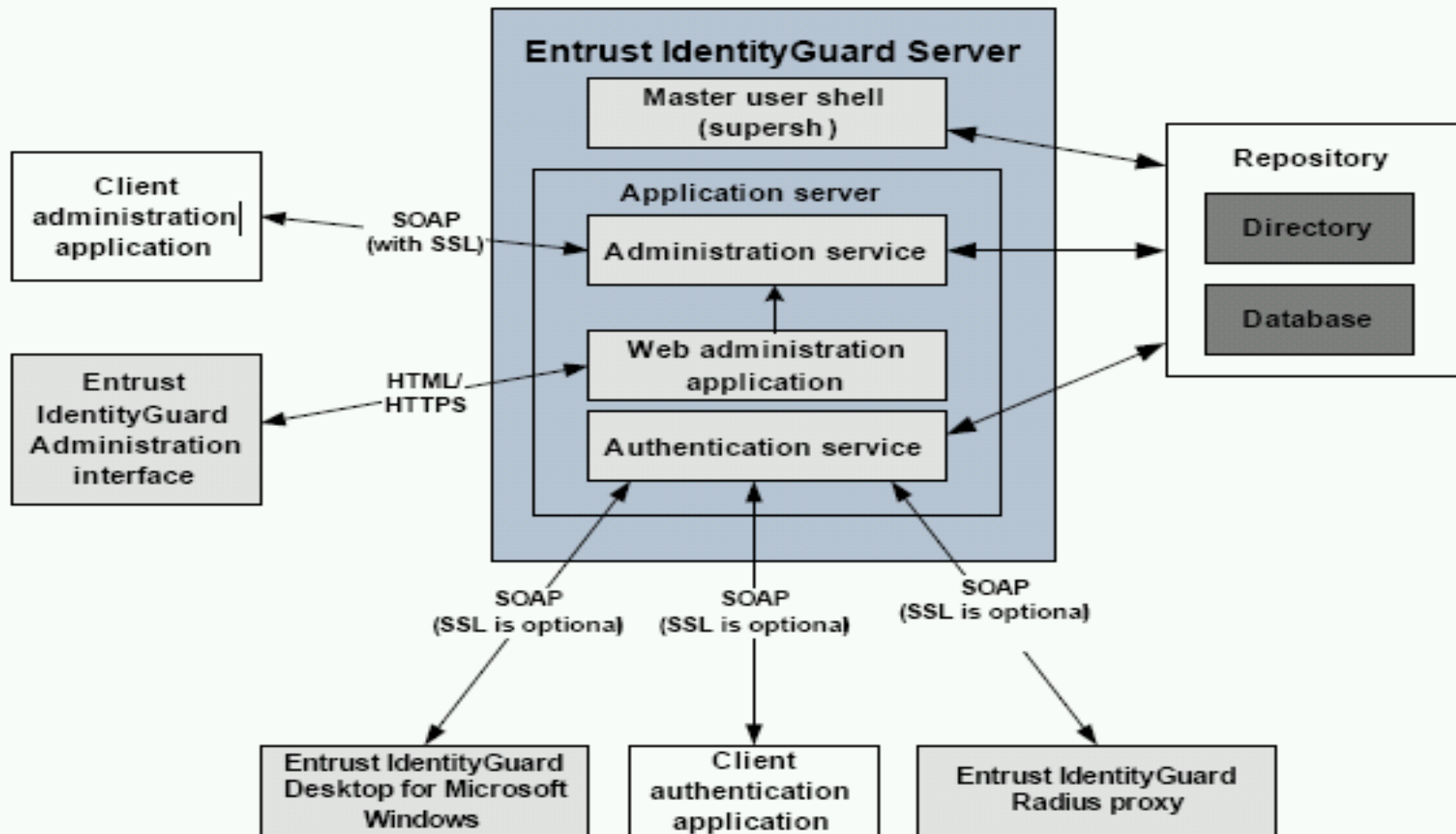
Application Framework Model

PHP+PostgreSQL Application Server Framework/Toolkit
Sub System Layers
02/2008
Brian A. Seklecki <bseklecki@collaborativefusion.com>



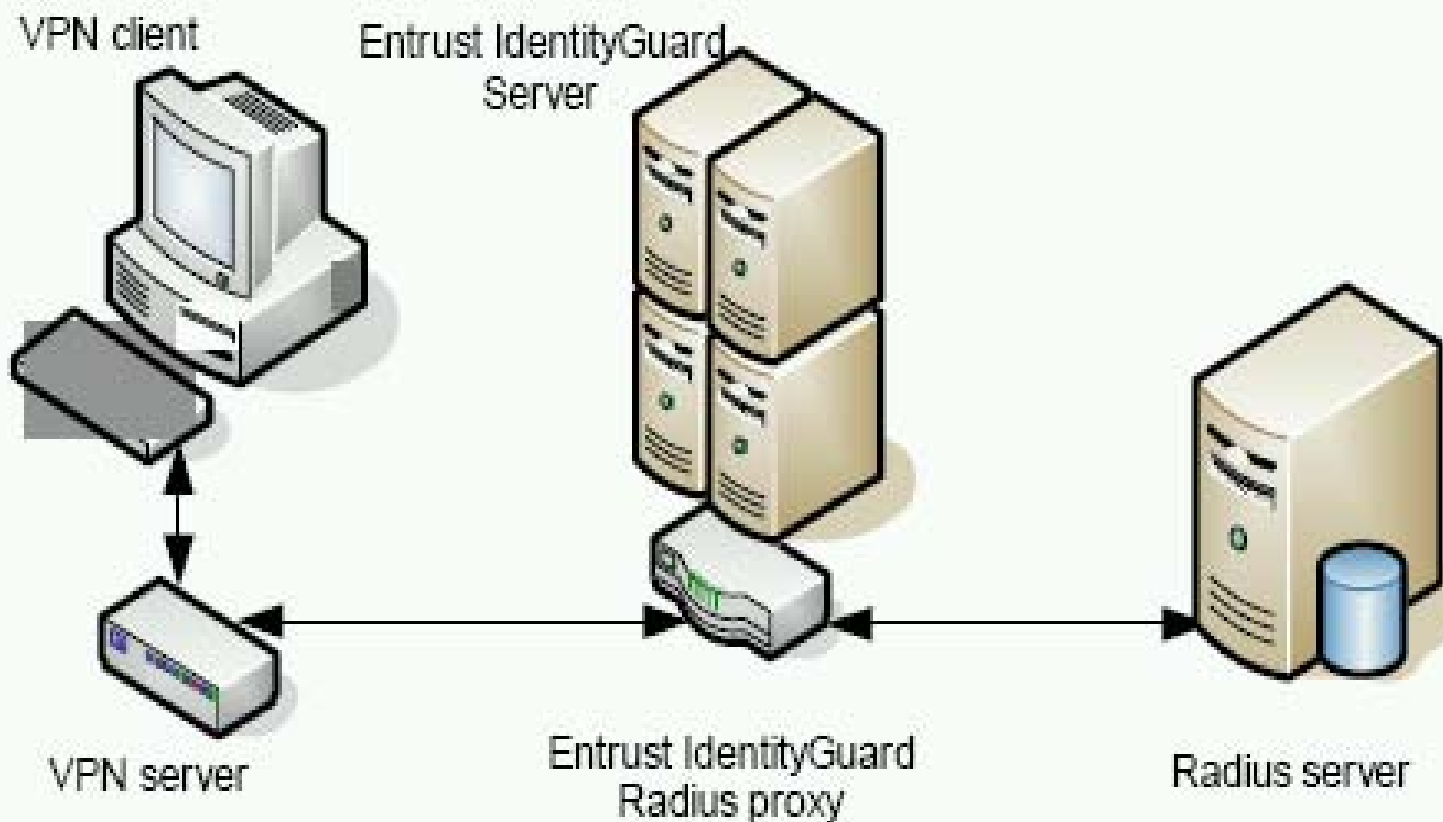
Logical Component Overview

Figure 1: Entrust IdentityGuard components



RADIUS Proxy

Figure 2: Radius proxy integrated with a VPN and Radius server.



JSP Web Interface

- Localhost Presentation

