

# **Oracle, LDAP and Active Directory Integrating the Technologies**

*Debra Addeo, Douglas County  
School District*

*02/13/2008*

# Overview

- The goal is to give a general understanding of these technologies.
- Definition of LDAP
- Explanation of Active Directory
- Authentication and Authorization
- Knowledge of the Oracle package `dbms_ldap`
- Thoughts for further investigation.

# What is LDAP

- LDAP (Lightweight Directory Access Protocol) is an Internet protocol that programs use to look up information from a server.
- LDAP is a protocol like FTP (File Transfer Protocol).
- LDAP does not define how programs work on either the client or server side.
- LDAP defines the "language" used for client programs to talk to servers (and servers to servers, too) and access information in a directory also known as an LDAP directory.
- The client can be any software that can issue the LDAP commands.

# What is LDAP

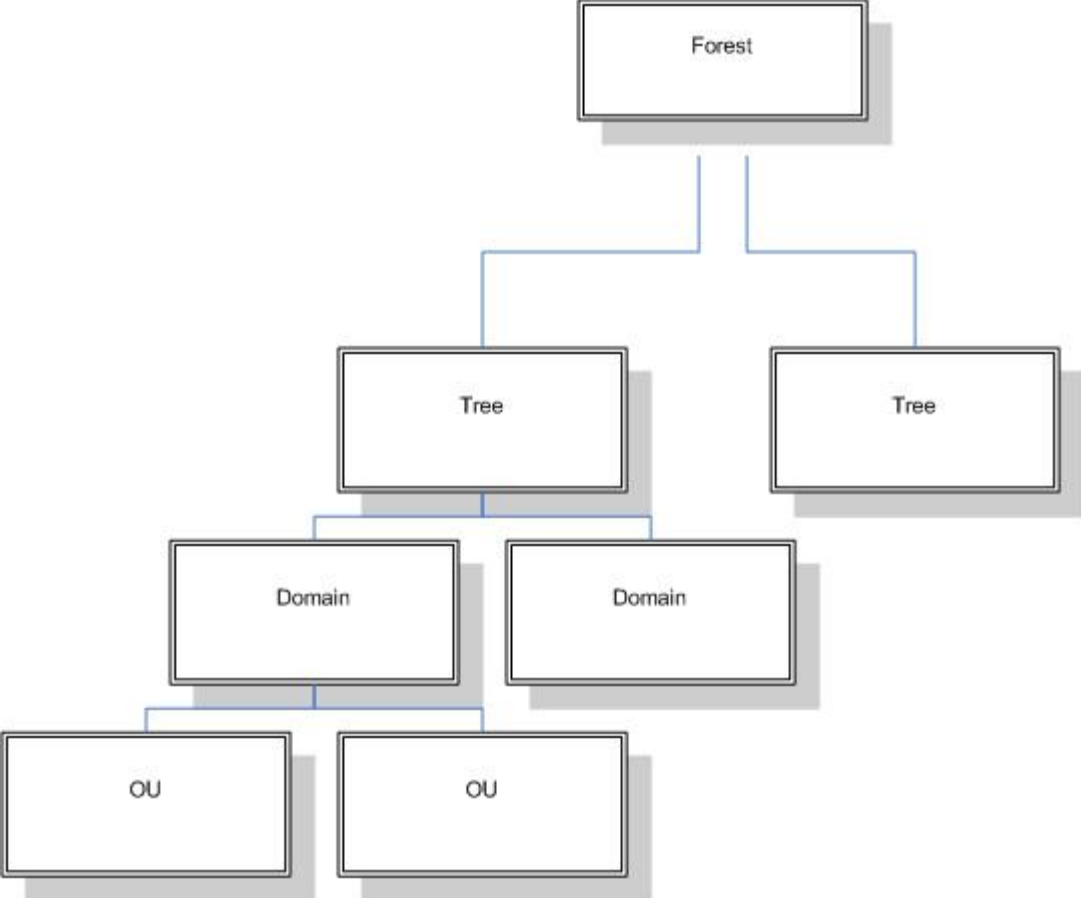
- The LDAP protocol is both cross-platform and standards-based, so applications needn't worry about the type of server hosting the directory.
- LDAP is finding much wider industry acceptance because of its status as an Internet standard.

# What is Active Directory

- An implementation of LDAP directory services by Microsoft for use primarily in Windows environments.
- Provide central authentication and authorization services for Windows based computers.
- Allows administrators to assign policies, deploy software, and apply critical updates to an organization.
- Stores information and settings in a central repository.

# What is Active Directory

- A hierarchical framework of objects. The objects fall into three broad categories: resources (e.g. printers), services (e.g. email) and users (user accounts and groups). AD provides information on the objects, organizes the objects, controls access and sets security.
  - Top Level of the framework structure is the Forest.
  - Next level is a tree which holds one or more Domain and domain trees (Domains are identified by their DNS name structure, the namespace can be called dn)
  - The objects held within a domain can be grouped into containers called Organization Units (OUs).
  - The OU is the common level at which to apply group policies, which are AD objects themselves called Group Policy Objects (GPOs).



# Authentication

- Authentication is the process of verifying who a person is using a username and password.
- Just because someone has the correct username and password it does not mean that they should have full access to your system.

# Authorization

- Authorization is the finding out if the person with the correct username and password are authorized to access the application and the data within the application.
- One can check a group in Active Directory or there could be a simple list in a database table that allows access to the data in the application.
- An example is to verify if someone has administrative privileges.

# Why would I use Active Directory and LDAP?

- Let another application handle part of the work:
  - Username, password policies and procedures.
  - Store what privileges a person has by their position
  - Global privileges for a corporation that get provisioned without writing any additional code

# Coding the Access

- DBMS\_LDAP package can:
  - Issue LDAP commands from the database.
  - Verify a username and password.
  - Search the tree to see what groups the user is currently in.
  - Add, delete or modify a user.
  - Search the tree to extract other information.

# Code for Simple Username and Password Verification

- Connect to the server and get a session
- `my_session := DBMS_LDAP.init(ldap_host,ldap_port);`
- Bind to the server to authenticate the user.
- `retval :=DBMS_LDAP.simple_bind_s(my_session, ldap_user,ldap_passwd);`
- Unbind the Session
- Code completed

# Search for User Attributes

- `retval := DBMS_LDAP.search_s(my_session,  
ldap_base,  
DBMS_LDAP.SCOPE_SUBTREE,  
'(userPrincipalName=||  
in_search_username||@mycompany.com)',  
*,  
0,  
my_message);`

# Look Through The Attributes

- `retval :=  
DBMS_LDAP.count_entries(my_session,  
my_message);`

# Look at the Entries

Loop through each of the entries one by one

while my\_entry IS NOT NULL loop

```
my_dn := DBMS_LDAP.get_dn(my_session, my_entry);
```

```
DBMS_OUTPUT.PUT_LINE ('    entry #' ||  
TO_CHAR(entry_index) || ' entry ptr: '  
||RAWTOHEX(SUBSTR(my_entry,1,8)));
```

End loop;

# Performance

- AD can be indexed just like a database table.
- Performance can be enhanced with a few strategically placed indexes.
- Ask the administrator to index the item that is being searched.
- It can make a large difference in the speed of the above commands.

# Conclusion

- Oracle, Active Directory (or any other LDAP based Directory) and LDAP can be used to handle the authorization and authentication for an application.
- This allows the application builder to handle application specific issues and not worry about the username and password functions that need to be performed by an application.

Questions ?

Thanks for attending