OID, LDAP, PL/SQL and Beyond

Peter Koletzke
Technical Director & Principal Instructor
ORACLE ACE Director

quovera

utoug utah oracle users group

Best Use of a Directory

I'd rather entrust the government of the United States to the first 400 people listed in the Boston telephone directory than to the faculty of Harvard University.

— *William F. Buckley, Jr.* (1925–2008), editor, author, loyal Yale graduate

Survey

- Job responsibilities?
  - DBA
  - Developer
  - Sys admin
- Languages?
  - PL/SQL
  - Java
  - Other

Agenda

- LDAP Basics
- Intro to OID
- The PL/SQL API
- Beyond: Additional Techniques

Slides will be available on the UTOUG and Quovera websites.

What is LDAP?

- Lightweight Directory Access Protocol
- Protocol = standard format for communication
  - "Agnostic" sender and receiver
  - Specified by IETF (Internet Engineering Task Force)
- It's an application layer Internet Protocol (I.P.)
  - Like HTML, FTP, POP, SMTP, Telnet, DNS, MIME, URI (URL) **A URL is a URI**
- Used to access "directory services"
  - Most often for user account information
    - Name, password, profile, user groups

Directory Services

- A directory maps the name of a resource to a network address
  - Like a phone directory maps a name to a phone number
  - A **resource entry** is identified by a *uniform resource identifier* (URI)
    - Example resource: user account information
- Directories are arranged in hierarchies
  - Stated in reverse like fully-qualified domain names
    - Example domain:

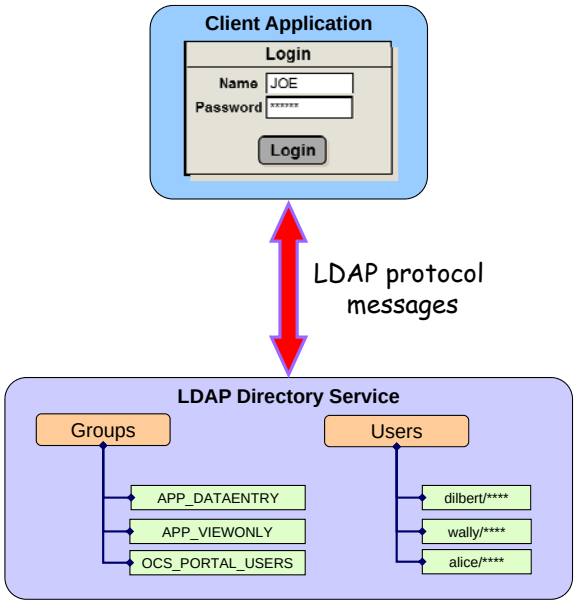
app.tuhra.com

Department or Subcategory (Applications)

Company or parent entity (The Ultimate Human Resources Association)

Top-level domain (Commercial entity)

The Path



Uses for a Directory Service

- Any information that contains "attributes" (name-values)
- Not for transactional data
- Email address lookups
- Address book
- Organization representation (org chart)
- Authentication
  - User account and user group information
    - Password, user profile (name, address, etc.)
  - Each **entry** represents a group or a user

Identifying an Entry with LDAP

`ldap://host:port/DN?attributes?scope?filter?extensions`

- **host:port** – IP address or host name of directory server
  - Default port is 389, for secure LDAP (LDAPS): 636
- **DN** – *distinguished name*: a specially formatted name unique within a node
- **attributes** – details of the resource
  - For example, lastName for a user account
- **scope** – where in the hierarchy the server should start the search for the entry; default is "base"
- **filter** – reduces the types of results returned. Default is "objectClass=*"
- **extensions** – specifies how search should be processed (optional)

The Distinguished Name

- The DN
- Constructed hierarchically in reverse order
  - Hierarchy is setup during LDAP installation
  - A string of names in the hierarchy
- CN: common name
  - A single (simple) name
  - May not be unique between nodes
- DN must be unique between nodes

Sample DN

cn=dilbert,cn=cust,cn=Users,dc=app,dc=tuhra,dc=com

Node identifier

Name

- Internet Engineering Task Force maintains the standards
  - Changes made through the Request for Change (RFC) process

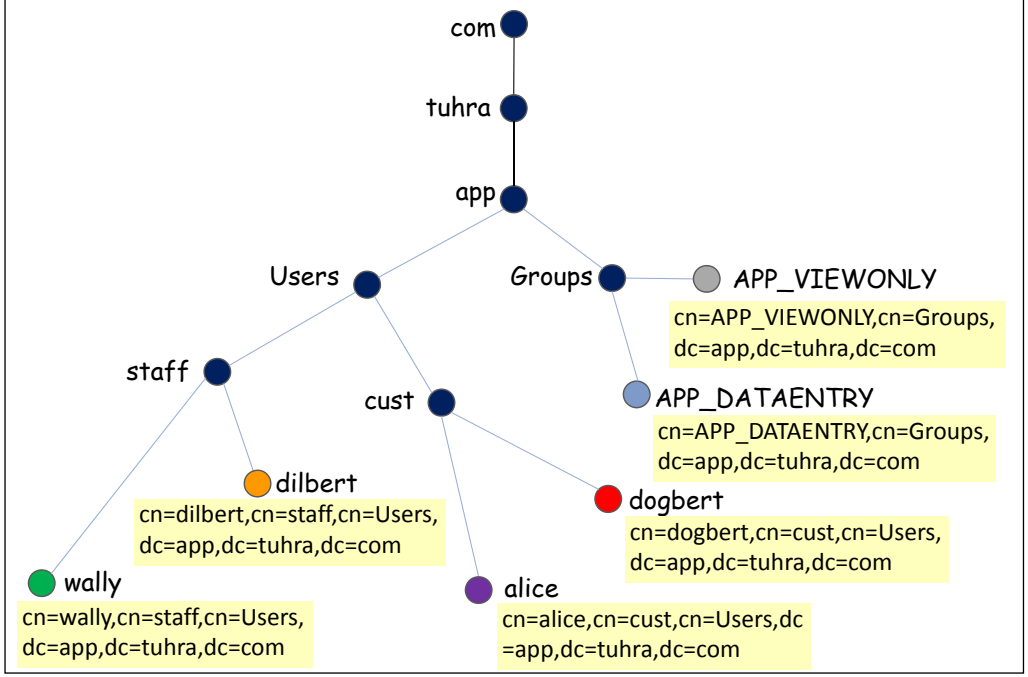
From The IETF RFC 2253

"UTF-8 String Representation of Distinguished Names"

String	X.500 AttributeType
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

https://www.ietf.org/rfc/rfc2253.txt

Sample Directory Hierarchy



A DN Identifies an Instance of one or more LDAP Classes

- A class consists of a set of attributes
- For example, a user account is a set of classes with attributes like:
  - First name
  - Last name
  - Middle initial
  - Email
  - Phone
  - Password
  - Enabled

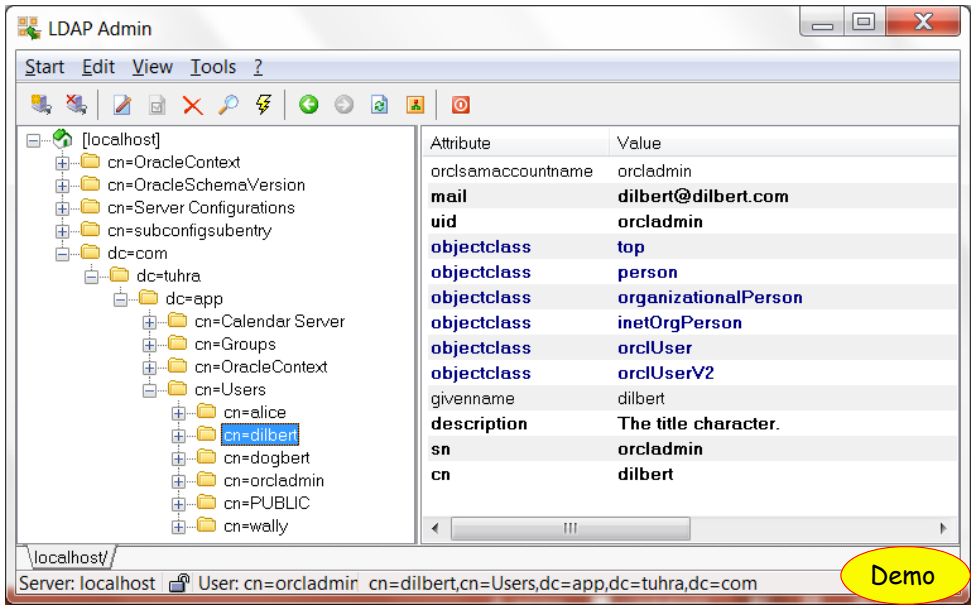
Popular LDAP Directory Services

- OpenLDAP
  - http://www.openldap.org/
- Microsoft Active Directory (A.D.)
  - Used for Outlook, SharePoint, Exchange
- Oracle Internet Directory (O.I.D.)
  - Part of Oracle Identity Management Suite
  - Integrated with WebLogic Server and all other Oracle products

Some LDAP Clients

- LDAP Admin – Windows tool
  - www.ldapadmin.org
- Oracle Directory Manager (10*g*)
  - Installed with Oracle Client
- Oracle Directory Services Manager (ODMS) (11*g*+)
- MS Active Directory Explorer (AD Explorer)
  - https://technet.microsoft.com/en-us/sysinternals/adexplorer.aspx
  - Like Windows Explorer except for LDAP
- **Important**: Stick with the tool designed for the specific directory
  - AD = AD Explorer
  - OID = ODM or ODMS

LDAP Admin



Agenda

- LDAP Basics
- Intro to OID
- The PL/SQL API
- Beyond: Additional Techniques

Fact-OIDs

- Oracle Internet Directory
  - Part of Oracle Identity Management Suite
  - An LDAP directory service
    - Specifically for secure storage and retrieval of names and values
- A directory service taps into a database
  - OID is implemented in an Oracle database–ODS schema
  - Accessed with commands not SQL

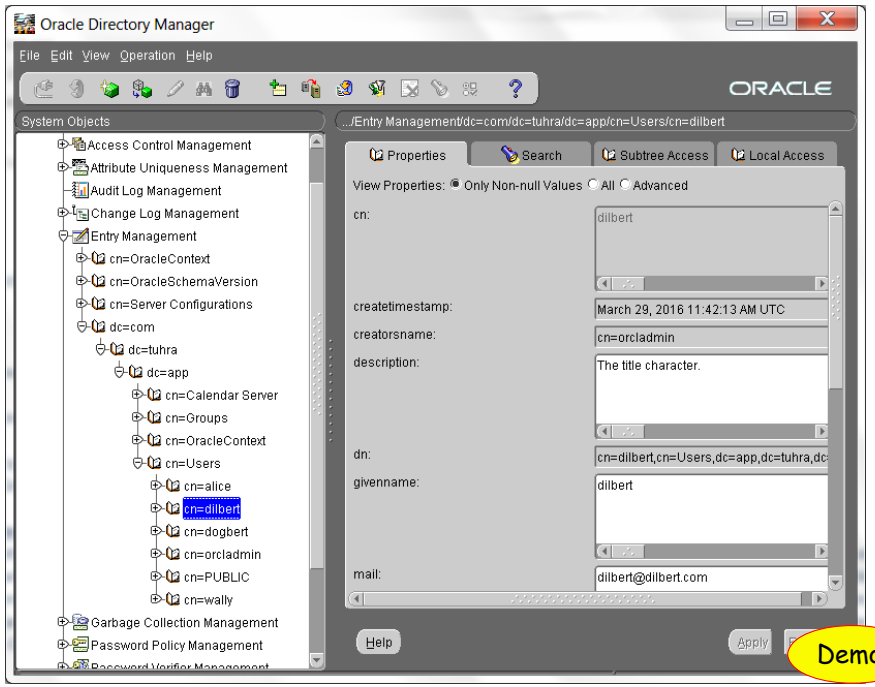
Accessing OID

- An LDAP client (mentioned before)
- Command line, for example:
  - ldapadd
  - ldapbind
  - ldapdelete
  - ldapmodify
  - ldapsearch
  - http://docs.oracle.com/cd/E36909_01/core.1111/e10105/cmdline.htm (11g)
- APIs (more later)

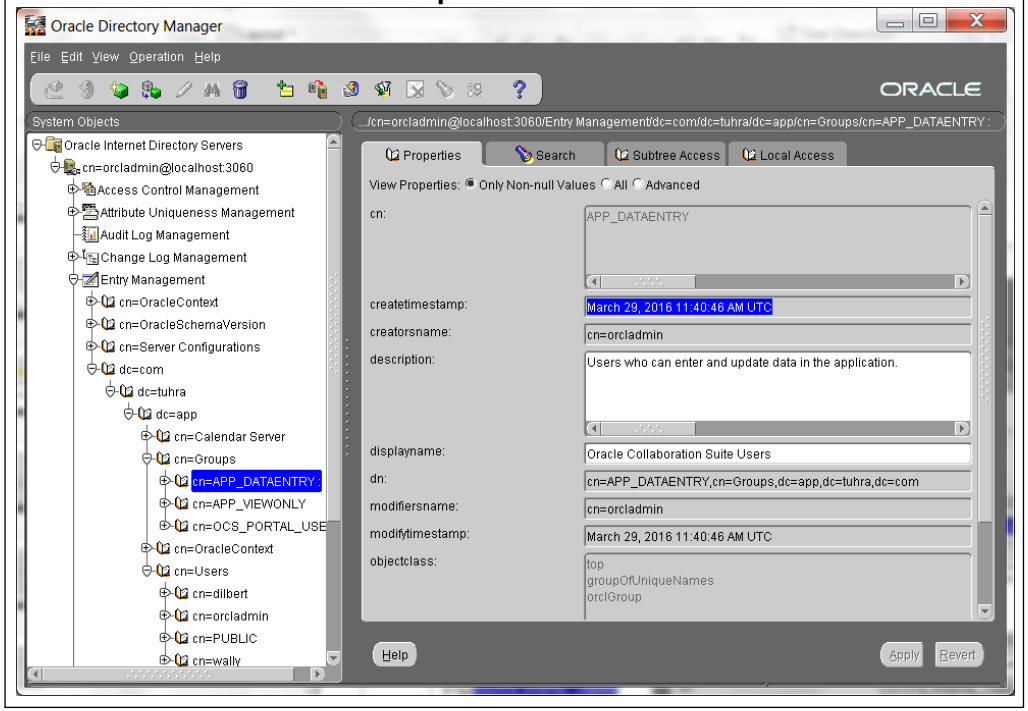
More Fact-OIDs

- Users are “members” of groups
- This membership is stored as an attribute of the group object
- Best demonstrated using a client
- For example, Oracle Directory Manager
  - Very powerful tool
  - Used for OID setup and maintenance as well as browsing
  - Part of Oracle Client 10*g*
    - For 11*g*+, use Oracle Directory Services Manager

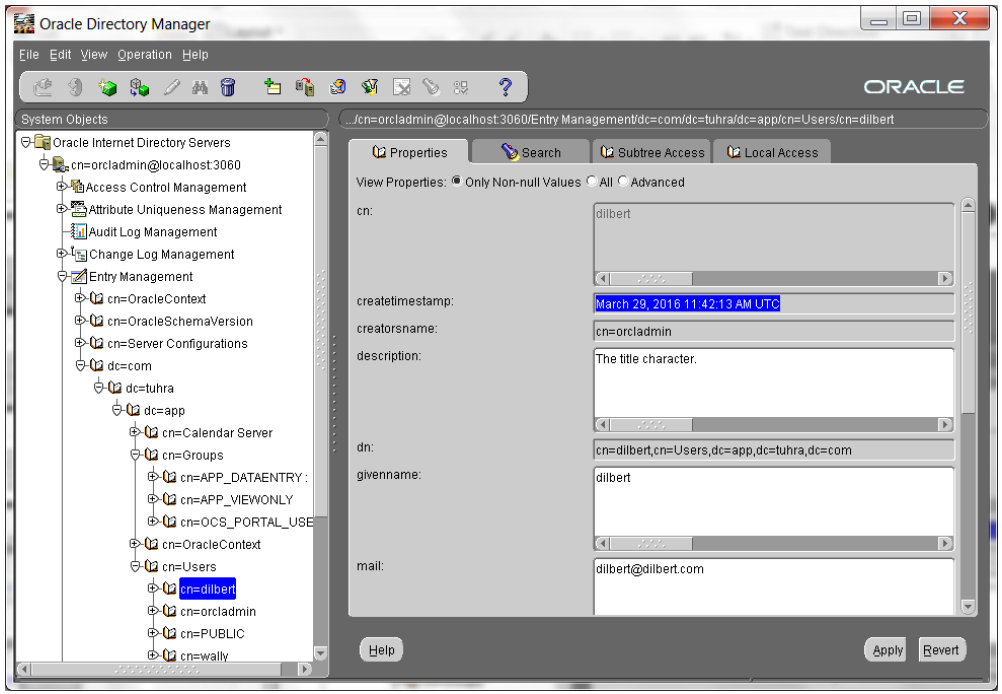
Oracle Directory Manager



Group Definition

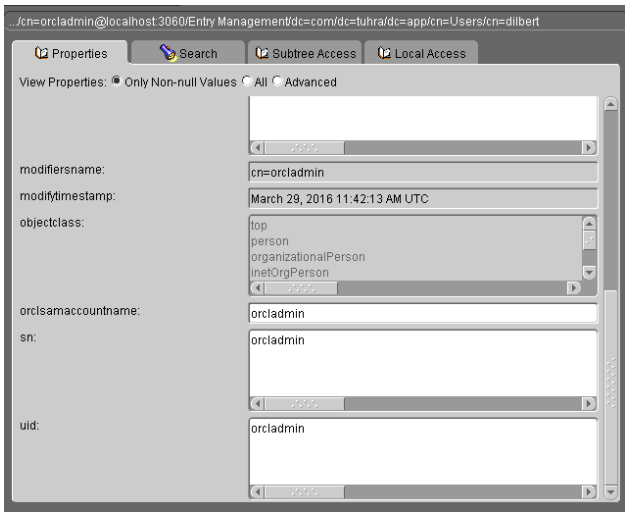


User Account Definition



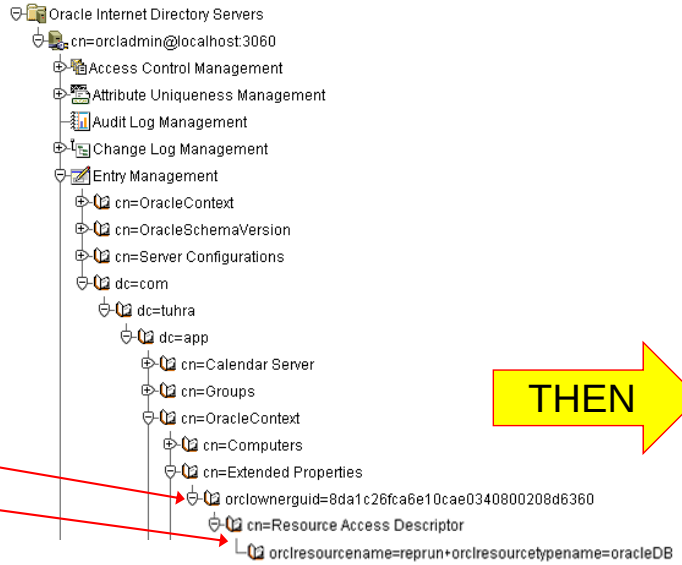
User Definition (continued)

- Lots of attributes
- But none for a *Resource Access Descriptor* (RAD)
  - Provides Single Sign-on (SSO) connection ifor Oracle Forms or Reports
  - AUTHID parameter in Reports



Where Are the RADs?

- Extended Properties node



THEN

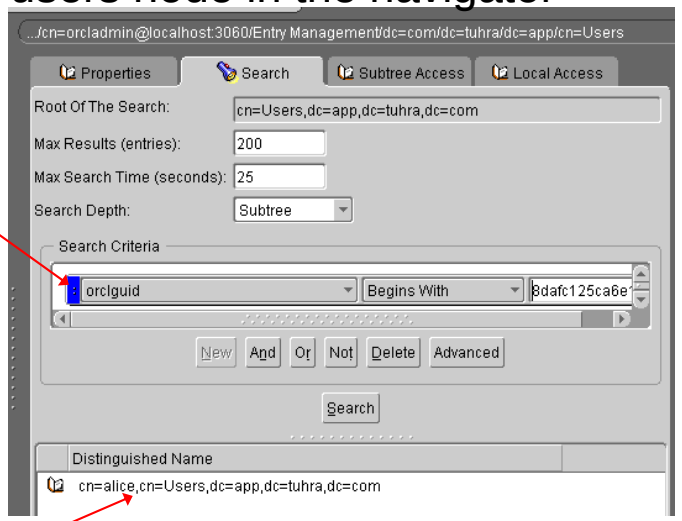
RAD owner's global unique identifier (GUID)

RAD definition (user/pwd/database)

Search For a User By a GUID

- Start from users node in the navigator

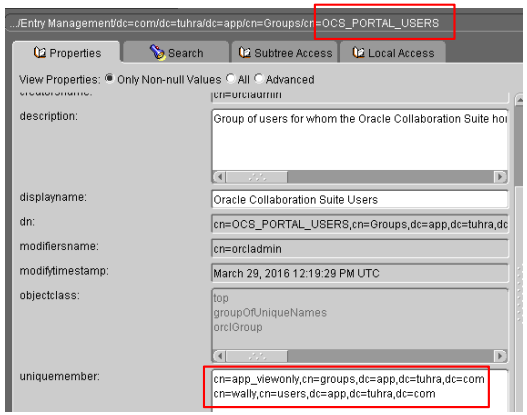
Enter the GUID as orclGuid and Search



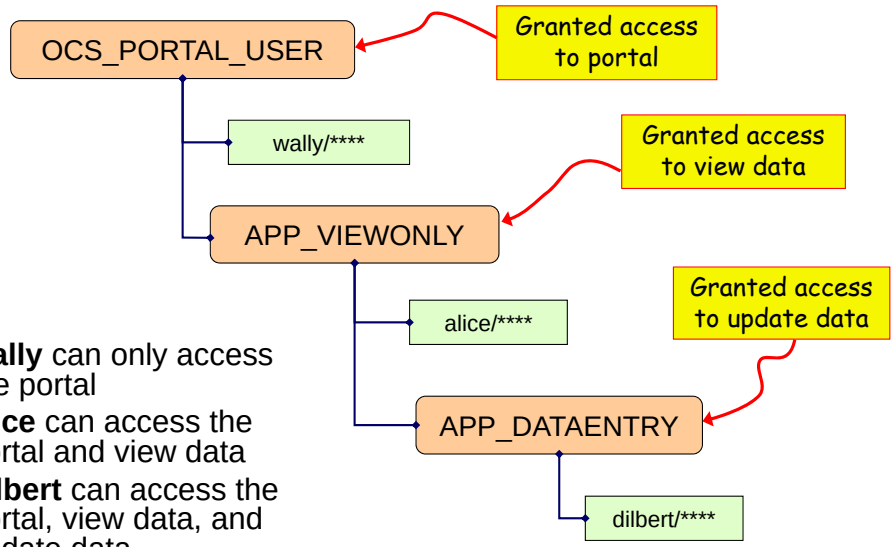
User's DN for that GUID (the user who owns that RAD)

Group Hierarchy

- Groups can be members of groups
  - Just as Oracle database roles can be granted another role
- Application authorization can navigate the hierarchy
  - Privileges assigned to the group
  - Users enrolled in the bottom-level group will have authorization to top-level group privs



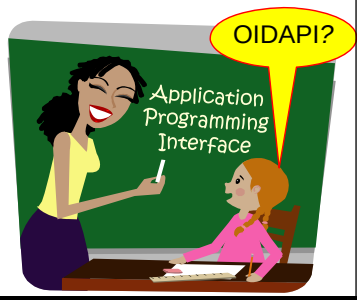
Group Hierarchy Example



- **wally** can only access the portal
- **alice** can access the portal and view data
- **dilbert** can access the portal, view data, and update data

OID APIs

- Java
  - oracle.idm and oracle.ldap class packages
  - http://docs.oracle.com/cd/B28196_01/idmanage.1014/b15992/toc.htm (10*g*)
- PL/SQL
  - DBMS_LDAP package
  - ./rdbms/admin/catldap.sql
  - https://docs.oracle.com/cd/E28280_01/dev.1111/e10186/dbmsldap_ref.htm#OIMAD009 (11g)



More From Bill

Liberals claim to want to give a hearing to other views, but then are shocked and offended to discover that there are other views.

—*William F. Buckley, Jr.* (1925–2008), "Father of Modern Political Conservatism"

Agenda

- LDAP Basics
- Intro to OID
- The PL/SQL API
- Beyond: Additional Techniques

DBMS_LDAP PL/SQL Package

- As the name implies:
  - Functions and procedures used to access LDAP systems
  - Declared datatypes specific to LDAP
  - The PL/SQL API for LDAP
- Transactions work similarly to any programmatic data access
  - Like DBMS_SQL, C/C++, JDBC
  - Open, connect, issue the statement, close, disconnect

Sample Steps (Find a DN)

- Declare variables: using DBMS_LDAP types
- Open connection: **`init()`**
- Bind (login): **`simple_bind_s()`**
- Search: **`search_s()`**
- Clear messages: (**`ber_free, msgfree`**)
- Unbind (close): **`unbind_s()`**

Find a DN Code Snippet (1)

```
-- Package spec or package body variables
tuhra_mem_session     DBMS_LDAP.session;
tuhra_mem_dn          VARCHAR2(256);
tuhra_mem_rdn         VARCHAR2(256);
tuhra_mem_array       DBMS_LDAP.mod_array;
tuhra_mem_vals        DBMS_LDAP.string_collection;
tuhra_mem_attrs       DBMS_LDAP.string_collection;
tuhra_mem_message     DBMS_LDAP.message;
tuhra_mem_entry       DBMS_LDAP.message;
tuhra_mem_ber_elmt    DBMS_LDAP.ber_element;
-- Package procedure
DECLARE
   v_ldap_session DBMS_LDAP.session;
   v_ldap_status PLS_INTEGER;
   v_return PLS_INTEGER;
```

Find a DN (2)

Exception handling removed

```
BEGIN
   v_ldap_session := DBMS_LDAP.INIT(
         p_ldap_host, p_ldap_port);
   v_ldap_status := DBMS_LDAP.SIMPLE_BIND_S(
         v_ldap_session, p_bind_user, p_bind_passwd);
   tuhra_mem_attrs(1) := 'cn';
   v_return := DBMS_LDAP.SEARCH_S(
      ld     => tuhra_mem_session,
      base   => 'cn=Users,dc=app,dc=tuhra,dc=com',
      scope  => DBMS_LDAP.SCOPE_SUBTREE,
      filter => 'cn=' || p_username,
      attrs  => tuhra_mem_attrs,
      attronly=> 0,
      res    => tuhra_mem_message);
   tuhra_mem_entry := DBMS_LDAP.FIRST_ENTRY(
      ld     => tuhra_mem_session,
      msg    => tuhra_mem_message);
```

Find a DN (3)

```
   -- Loop here if you expect more than one entry
   v_dn := DBMS_LDAP.GET_DN(
         tuhra_mem_session, tuhra_mem_entry);
   tuhra_mem_attr_name :=
         DBMS_LDAP.FIRST_ATTRIBUTE(
             tuhra_mem_session, tuhra_mem_entry,
             tuhra_mem_ber_elmt);
   -- message cleanup
   DBMS_LDAP.BER_FREE(tuhra_mem_ber_elmt, 0);
   -- DBMS_LDAP.NEXT_ENTRY() if more than 1 result
   -- end of loop (if any)
   -- Clear message collection
   v_return := DBMS_LDAP.MSGFREE(tuhra_mem_message);
   v_return := DBMS_LDAP.UNBIND_S(temp_session_id);
END;
```

Enrolling a User in a Group

- **`init()`** and **`simple_bind_s()`**
- Create modification array: **`create_mod_array()`**
  - Include user DN to add
- Populate the array with an operation:

```
DBMS_LDAP.POPULATE_MOD_ARRAY(
   tuhra_mem_array,
   DBMS_LDAP.MOD_ADD,
   'uniquemember',
   tuhra_mem_vals);
```

use **`MOD_DELETE()`** to remove user from group

- Modify the group

```
v_return := DBMS_LDAP.MODIFY_S(
   tuhra_mem_session, v_group_dn,
   tuhra_mem_array);
```

- **`unbind_s()`**

Other Common Tasks

- Create a user account or group
  - Assign attribute values into a record variable
  - **`add_s()`**
- Enroll a group in a group
  - Add member group's DN to the parent group's uniquemember attribute
  - Same as user in a group: **`modify_s()`**
- Disable a user account
  - Set the *orclisenabled* property
- Rely on samples:
  - https://docs.oracle.com/cd/B10464_05/manage.904/b10461/smplcode.htm (10*g*)
  - 11*g* docs show a broken link for samples

Agenda

- LDAP Basics
- Intro to OID
- The PL/SQL API
- Beyond: Additional Techniques

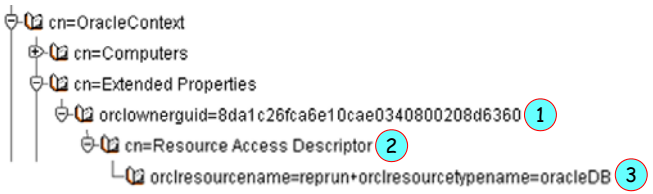
Creating RADs Programmatically

- init()
- simple_bind_s()
- Get orclguid attribute for user
  - similar to get DN example earlier but
  - `tuhra_mem_attrs(1) := 'orclguid';`
- Set the top node dn
  - `v_entry_dn := 'orclownerguid=' || v_guid || ',cn=Extended Properties,cn=OracleContext,'||ldap_admin.ldap_base;`

Creating RADs (continued)

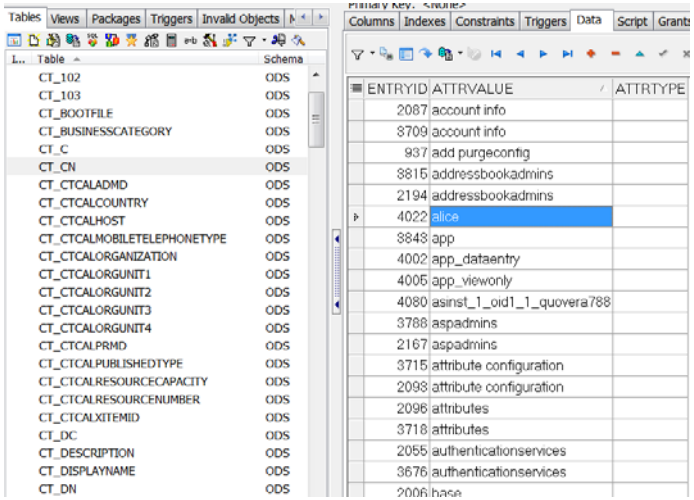
- Create extended properties container for top level DN: **`DBMS_LDAP.ADD_S()`** 1
- Create RAD name under container: **`DBMS_LDAP.ADD_S()`**again 2
- Add resource container for user: **`DBMS_LDAP.ADD_S()`**again 3

Sample code (for Forms RADs)
http://www.oracle.com/technetwork/developer-tools/forms/howtoplsqlrad-101335.html



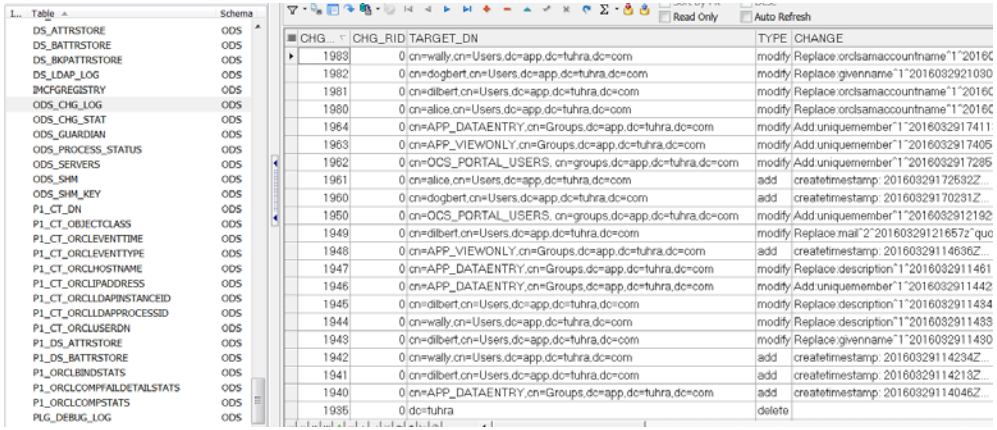
ODS Schema Tables

- CT_* tables hold attribute values



ODS Schema Tables

- Change log table: ODS_CHG_LOG



- Tip: Don't change these tables using SQL.

Gotchas

- Phantom memberships
  - If you delete the user account, the membership persists
  - Fix: delete the membership first or disable the account (enabled property)
- Enrolling a user in a child and parent group can throw an error
  - Fix: enroll in the bottom-level group
- Be sure to close the connection
  - Number of concurrent connections is limited

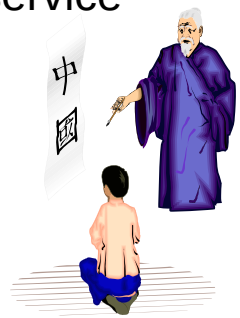
Director-y Strategy

Be extremely subtle,
even to the point of formlessness.
Be extremely mysterious,
even to the point of soundlessness.
Thereby you can be the director
of the opponent's fate.

—*Sun-tzu 孙子 (c. 4th century BCE)*
The Art of War

Summary

- LDAP is a protocol used to access directory services
- "LDAP" is a generic term referring to an *LDAP-accessible directory*
- OID is Oracle's LDAP directory service
- You can access OID programmatically using PL/SQL
  - DBMS_LDAP package
  - Rely on samples
    - Especially when creating RADs



Books co-authored with Dr. Paul Dorsey, Avrom Roy-Faderman, & Duncan Mills

quovera

http://www.quovera.com

- **Founded in 1995 as Millennia Vision Corp.**
- **More technical white papers and presentations on the web site**