Centralized Oracle Database Authentication and Authorization in a Directory

Paul Sullivan
Paul.J.Sullivan@oracle.com
Principal Security Consultant

Kevin Moulton
Kevin.moulton@oracle.com
Senior Manager, Security Consulting
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Agenda

• Problem Definition
• Enterprise Directory Overview and benefits
• Enterprise Directory Deployment Architectures
• Enterprise Directory Technical Deep Dive
• Demo
The Problem

Each Database is an island. Users are managed separately in each database.
The Problem

- Problem Definition
- EUS Overview and benefits
- EUS Deployment Architectures
- EUS Technical Deep Dive
- Demo
The Cost

User Productivity
- multiple database login names and passwords to remember
- No self-service capability for password reset

Database Administrator time
- DBAs manage the same user many times

Audit & Compliance
- Each database must be examined individually to find out who has which privileges

Security
- Hard to ensure user access to all databases is removed
- Ensuring passwords meet complexity/change requirements is difficult
The Answer

Centralized User Management

• Define users in one place
• Assign a user’s privileges in one place
• Delegate database user management to the help desk
• Control user’s passwords through a common identity store such as your corporate Directory
Database Users are managed in each database. A user has multiple database login names/passwords to remember.
Centralized Database Users

Each person has one username/password for ALL databases. Directory identities are *mapped* to database schemas. Directory groups are *mapped* to database roles.
The Business Benefit

**Decrease Time Spent Managing Users**
Devote more time to value-added activities

**Improve Your End-User’s Experience**
Give your user’s a single username/password, standardized access request procedures

**Reduce the Cost of Compliance**
Delete/disable user access in ALL databases with a single click
Managing Enterprise Authentication
User Authentication Stores

- Active Directory
- Oracle Internet Directory
- Oracle Directory Server Enterprise Edition (Sun)
- Oracle Virtual Directory
- LDAP V3 Compliant Directory
- Kerberos (ASO)
- Radius (ASO)
- X.509 (ASO)
Managing Enterprise User Privileges
Enterprise User Security

- Database Roles
- System Privileges
- Object Privileges

Global Role → Enterprise Role → LDAP Group
Enterprise User Security
Centralized Directory Architectural Options

There are Five ways to integrate your Oracle Databases with your corporate Directory

1. Synchronization
2. Virtualization
3. Chaining
4. Split-Configuration
5. Kerberos (may be used standalone or combined with any of the above options)

Each method has its advantages, each has its disadvantages
Centralized Directory Identity Architecture
Option 1: Synchronization

**Pros**
- Works with 9i databases as well as current versions
- No schema changes made to Active Directory
- No additional data added to Active Directory

**Cons**
- Must synchronize data between Active Directory and Internet Directory (including passwords). Must maintain that synchronization.
- Requires AD agent (oidpwdcn.dll) on all domain controllers to capture passwords.
Centralized Directory Identity Architecture
Option 2: Virtualization

**Pros**
- No need to maintain a separate directory server
- All data maintained in one place

**Cons**
- Will not work with Oracle 9i
- Significant schema changes to Active Directory for metadata
- Need AD Password agent (oidpwdcn.dll)
- DBAs seldom have update privileges in Active Directory
Centralized Directory Identity Architecture
Option 3: Chaining / Leverage External Directory

**Pros**
- No additional data in AD
- Minimal schema changes to AD (one attribute: `orclcommonattribute`)
- DBAs maintain metadata, AD admins maintain users
- Roles may be maintained in AD or OID

**Cons**
- Will not work with 9i DBs
- Must maintain another directory server
- Limited to a single Active Directory domain
Centralized Directory Identity Architecture

Option 4: Split-Configuration

**Pros**
- No additional data added to AD
- Minimal schema changes to AD (one attribute: `orclcommonattribute`)
- DBAs maintain metadata, AD admins maintain users
- Supports multiple AD domains

**Cons**
- Will not work with 9i DBs
- Must maintain another directory server
- Need AD agent (oidpwdcn.dll)
Centralized Directory Identity Architecture

Kerberos Authenticated Database Users

Enterprise and/or local Users are authenticated by Kerberos tickets issued by MS Domain Controllers instead of passwords.

- Pros
  - Single Sign-On with Windows desktop
  - No password synchronization requirements

- Cons
  - May not work with all clients
  - Requires additional client configuration (sqlnet.ora)
Centralized Directory Logical Architecture
Base Case – User Authentication
Declare Users in Database
Enterprise User

EUS Global User Creation SQL (1=1 dedicated schema)

CREATE USER username IDENTIFIED GLOBALLY AS ‘<DN of directory user entry>’;

- When you connect to database you use your Active Directory Credentials to login
- Eliminates management of passwords for users
- All privileges and capabilities are still managed in database.
Connect With Userid and Password
Authentication only

Connect:
username@database_service_name

Enter password:
Declare Enterprise Global Users in Database
Multiple users are mapped to a shared DB schema

EUS Global User Creation SQL (N=1 shared schema)
CREATE USER username IDENTIFIED GLOBALLY;

- When you connect to a database you use your Active Directory credentials to login but you are connected to a global user account. Multiple users will be mapped to this same account.
- Eliminates management of passwords for users
- All privileges and capabilities are mapped to groups in the directory
Connect to Enterprise User Security Authentication and Authorization

Connect: 
username@database_service_name
Enter password:

1. Connect
2. AuthN dn=
3. AuthZ dn=; (role)
4. User, Role and Privilege Info

Oracle DB
Oracle OID
Current Database Environments without Enterprise User Security

DBA’s must perform these tasks on every database:
- Set password policies
- Create users and passwords
- Reset passwords
- Manage roles and privileges
- Assign roles and privileges to users
## Impact of using Enterprise User Security and Shared Schemas

<table>
<thead>
<tr>
<th>DBA Work Item</th>
<th>Current</th>
<th>EUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Changes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 Databases x 200 Users x 4 (quarterly)</td>
<td>160,000</td>
<td>0</td>
</tr>
<tr>
<td><strong>Create New Users</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 Databases x 20 (10% yearly turnover)</td>
<td>4,000</td>
<td>0</td>
</tr>
<tr>
<td><strong>Delete Old Users</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 Databases x 20 (10% yearly turnover)</td>
<td>4,000</td>
<td>0</td>
</tr>
<tr>
<td><strong>Assign Privileges</strong></td>
<td></td>
<td><strong>800</strong></td>
</tr>
<tr>
<td>200 Databases x 20 (10% yearly turnover)</td>
<td>4,000</td>
<td></td>
</tr>
<tr>
<td>**** Total ****</td>
<td></td>
<td>172,000</td>
</tr>
</tbody>
</table>

** Each user was in 5 databases
Enterprise User Security
Assignment of Oracle DB Roles by Directory Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Active Directory Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefit</td>
<td>oracleDemo.com/Users</td>
</tr>
<tr>
<td>Denver</td>
<td>oracleDemo.com/Users</td>
</tr>
<tr>
<td>Domain Users</td>
<td>oracleDemo.com/Users</td>
</tr>
<tr>
<td>Employee</td>
<td>oracleDemo.com/Users</td>
</tr>
<tr>
<td>Employees</td>
<td>oracleDemo.com/Users</td>
</tr>
<tr>
<td>HR Admin Users</td>
<td>oracleDemo.com/Users</td>
</tr>
</tbody>
</table>

![Image of Active Directory properties window showing membership of different groups]
Enterprise User Security

Assignment of Oracle DB Roles by Directory Groups

SQL> select * from DBA_ROLE_PRIVS where GRANTEE='DBA_CONNECT_ROLE';

<table>
<thead>
<tr>
<th>GRANTEE</th>
<th>GRANTED_ROLE</th>
<th>ADV</th>
<th>DEF</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBA_CONNECT_ROLE</td>
<td>CONNECT</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

SQL>
Enterprise User Security

Assignment of Oracle DB Roles by Directory Groups

---

**AD**

**EUS**

**Oracle DB**

**Oracle Global Roles**

Global roles are special roles that can be granted to enterprise roles. Global roles can't

<table>
<thead>
<tr>
<th>Name</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBA_CONNECT_ROLE</td>
<td>orcl</td>
</tr>
</tbody>
</table>

**Grantees**

Upon database login, grantees will receive all privileges contained in the included global

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn=hr_admin_dba_connect, cn=users, dc=oracleDemo, dc=com</td>
<td>GROUP</td>
</tr>
</tbody>
</table>

```
SQL> select * from DBA_ROLE_PRIVS where GRANTEE='DBA_CONNECT_ROLE';

GRANTEE                      GRANTED_ROLE
------------------------------------------------
HR_admin_dba_connect          NO YES

SQL>
```
Enterprise User Security - Demo Architecture
Oracle DB, Oracle Virtual Directory and Active Directory

- AD used for authentication and group information
- AD used for metadata - Global Users and Roles
- EUS used to map database users and roles to user and groups in AD.
Enterprise User Security Demo

- Existing DB Users not affected
- Flag bad userids/passwords using Active Directory
- Log into DB based on AD credentials and groups
  - Show user is mapped to a global user in Oracle
  - Show roles assigned to user in Oracle
  - Show audit log to verify external authentication in Oracle
- Walk through EUS administrative screens
- Create new EUS enterprise role and map to an AD Group
Informational Resources

There are a number of resources that are available to gain a better understanding of Oracle's Enterprise User Security. I've included references to them below:

• Oracle Database Enterprise User Security – A practical example:

• Directory Services Integration with Database Enterprise User Security:

• How to set up Enterprise User Security with Oracle Virtual Directory and Oracle Directory Server Enterprise Edition:

• Oracle’s Documentation: Enterprise User Security Administration:
  http://docs.oracle.com/cd/E11882_01/network.112/e10744.pdf

• Oracle Documentation: Database: