Manage Oracle Database Users and Roles Centrally in Active Directory or Sun Directory

Overview
August 2008
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Centralizing DataBase Account Management using Existing Directories with OVD</td>
<td>4</td>
</tr>
<tr>
<td>Centralizing Database Account Management using Active Directory</td>
<td>6</td>
</tr>
<tr>
<td>Active Directory Integration for Password Authentication</td>
<td>6</td>
</tr>
<tr>
<td>Active Directory Integration for Password Authentication with OID as meta-data store</td>
<td>7</td>
</tr>
<tr>
<td>Active Directory Integration with Kerberos Authentication</td>
<td>8</td>
</tr>
<tr>
<td>Centralizing database account management using Sun Java System Directory Server</td>
<td>9</td>
</tr>
<tr>
<td>Sun JSDS Integration for Password Authentication</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>10</td>
</tr>
<tr>
<td>Appendix A: Supported Deployments</td>
<td>11</td>
</tr>
</tbody>
</table>
INTRODUCTION

IT departments are under consistent pressure to reduce cost, enhance security, and improve compliance to support ever-competitive business. Centralized management of user accounts and access rights is a key part of enterprise identity management initiative that delivers on the promises. Since databases are critical components of enterprise IT infrastructure that house sensitive corporate data, database user accounts and privileges should be centralized and integrated into enterprise identity management framework.

However, many enterprises today are still managing database users and privileges in individual databases. From end user perspective, managing passwords in multiple databases is confusing and results in poor user experience. From administration perspective, redundant user management is costly, and managing user authorizations in multiple databases is error prone. From auditing and compliance perspective, on time provision and de-provision of user access and privileges across databases is challenging.

Enterprise User Security (EUS), an Oracle Database Enterprise Edition feature, leverages the Oracle Directory Services and gives you the ability to centrally manage database users and role memberships in an LDAP directory. Enterprise User Security reduces administration cost, increases security, and improves compliance through centralized database user account management, centralized provisioning and de-provisioning of database users, centralized password management and self-service password reset, and centralized management of authorizations using global database roles.

Most enterprises, if not all, already have an existing enterprise directory, such as Microsoft Active Directory or Sun Java System Directory Server, and would like to leverage the existing infrastructure to centralize Oracle database users and roles. Oracle Virtual Directory (OVD), a directory virtualization service (not a repository), enables enterprises to implement EUS leveraging their existing directory infrastructure, so as to lower total cost of ownership (TCO).

This paper presents the EUS deployment options available using OVD with Active Directory and Sun Java System Directory Server, and the use cases will help determine when one is more appropriate than the other based on customer environment.
CENTRALIZING DATABASE ACCOUNT MANAGEMENT USING EXISTING DIRECTORIES WITH OVD

Oracle Database Enterprise User Security was developed to use Oracle Internet Directory (OID) as the default meta-data and identity store for an Oracle database. So the database interaction is specifically tailored to work seamlessly with OID, e.g. where to find user information, passwords, or user privilege information for a particular database.

Most enterprises, if not all, already have deployed enterprise directories, and prefer EUS implementation to leverage their existing directory infrastructure. To realize this requirement without using OID, Oracle Virtual Directory acts like an interpreter for Oracle database information requests.

OVD provides a real-time, virtual view of identity data from any data-store including directories, databases and Web Services without data persistence and synchronization. The database will communicate with OVD in the same way it does with OID without knowing the information it receives is actually stored in a third party directory. Using OVD enables the database to interact with third party directories without losing database functionality or changing the database code.

Oracle Virtual Directory will leverage existing user and group information in the existing third party directory infrastructure. Besides user data, database meta-data like DB registration information, user/role mappings and other EUS specific meta-data have to be stored in the third party directory. To manage this data, it is required to enhance the existing third party directory schema. In some Active Directory deployments this might be prohibited by corporate policy. To meet this policy and prevent required schema changes in Active Directory for EUS specific metadata, Oracle Internet Directory could be deployed (or leveraged if already being used) to manage the meta-data, together with OVD that will provide access to AD user and group information.

Oracle Virtual Directory is certified with EUS to support Active Directory and Sun Java System Directory (JSDS) for deployments. Deploying EUS using OVD with existing AD or Sun directories eliminates user data duplication and synchronization and lowers total cost of ownership (TCO).

Another aspect of Enterprise User Security, besides centralizing database user management, are the different methods of user authentication EUS provides:

1. Certificate (X.509) introduced in DB 8i
2. Password introduced in DB 9i
3. Kerberos introduced in DB 10g

OVD cannot be used together with certificate based authentication and requires a DB 10.1+ version.

The database is doing user authentication, not through LDAP bind to OVD or the third party directory behind OVD. For example, in the password authentication
scenario, the database collects user credentials, hashes the password, and compares the password hash value retrieved from AD or Sun Directory through OVD.

More detailed information about EUS can be found in the Enterprise User Administrator's Guide in the Database documentation section on OTN.
CENTRALIZING DATABASE ACCOUNT MANAGEMENT USING ACTIVE DIRECTORY

Active Directory Integration for Password Authentication

Figure 1

This is the default deployment for EUS with OVD. The database is establishing a connection to OVD which will lookup the requested DB information in Active Directory. This integration does not require any changes in the database (beyond what is usually required for EUS) nor for database clients that use username/password authentication. All of the EUS meta-data, as well as user/group information including passwords are stored in Active Directory.

Another required deployment component is the Oracle password filter ("oidpwdcn"). Microsoft uses a proprietary way to hash password in Active Directory that is incompatible with the Oracle DB requirements. The filter will be notified when a password change occurs, hashes the password in a DB compatible format, and stores the hash in AD. The password filter uses published Microsoft APIs to capture password change notification. The oidpwdcn DLL must be installed on the domain controller to capture password changes in order to hash and store them in a format requested by the database.

The database must be 10.1 or later because earlier versions use a different and incompatible password format. The Oracle password filter cannot be installed on the Global Catalog Server.
The difference for this deployment scenario compared to the default OVD and Active Directory use case is the introduction of Oracle Internet Directory to store EUS meta-data information. As outlined above this will meet corporate guidelines when schema changes in AD is not possible.

The database establishes a connection to OVD that will lookup user and group information in AD and all other requested data from OID. This integration does not require any changes in the database (beyond what is usually required for EUS) nor for database clients that use username/password authentication. The Oracle password filter ("oidpwdcn") must be installed on the domain controller to capture password changes in order to hash and store them in a format requested by the database.

The database must be 10.1 or later because earlier versions use a different and incompatible password format. The Oracle password filter cannot be installed on the Global Catalog Server.
Active Directory Integration with Kerberos Authentication

This scenario introduces Kerberos for DB authentication. It doesn’t require OVD to be Kerberos enabled. EUS with DB Kerberos authentication does not require any changes to the database beyond standard EUS configuration. The database is establishing a connection to OVD that will lookup the requested DB information in Active Directory.

All of the EUS meta-data, as well as user/group information including passwords are stored in Active Directory. No password filter needs to be deployed on the AD domain. All database clients must be Kerberos enabled to use this option. Only 10.1 or later databases are supported. The Database supports Kerberos natively when advanced DB security is used (and licensed). A Kerberos enabled DB is a prerequisite to use Kerberos for user authentication with EUS.
CENTRALIZING DATABASE ACCOUNT MANAGEMENT USING SUN JAVA SYSTEM DIRECTORY SERVER

Sun JSDS Integration for Password Authentication

This is the default deployment for EUS with OVD and SUN directory. The database is establishing a connection to OVD which will lookup the requested DB information in SUN JSDS. This integration does not require any changes in the database (beyond what is usually required for EUS) nor for database clients that use username/password authentication. All of the EUS meta-data, as well as user/group information including passwords are stored in JSDS.

Using SUN JSDS doesn’t require an Oracle password filter since the password hashing schemes used by SUN are compatible to the DB. Only works with database versions 10.1 or later due to incompatible password formats in earlier DB versions.
CONCLUSION

Centralized management of database user accounts and role memberships using Oracle Database Enterprise User Security (EUS) ensures strong security, reduces cost, and improves compliance. Oracle Virtual Directory provide options for customers to leverage their existing Active Directory or Sun Java System Directory Server to lower total cost of ownership (TCO).
## APPENDIX A: SUPPORTED DEPLOYMENTS

### Summary of OVD and EUS Integration Options

<table>
<thead>
<tr>
<th>Authentication</th>
<th>3rd Party Directory</th>
<th>DB</th>
<th>OID meta-data store</th>
<th>OVD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos</td>
<td>AD + OVD</td>
<td>10.1+</td>
<td></td>
<td>10.1.4.2</td>
</tr>
<tr>
<td>Password</td>
<td>AD + OVD</td>
<td>10.1+</td>
<td></td>
<td>10.1.4.2</td>
</tr>
<tr>
<td>Password</td>
<td>AD + OVD</td>
<td>10.1+</td>
<td>10.1.4.2</td>
<td>10.1.4.2</td>
</tr>
<tr>
<td>Password</td>
<td>SUN + OVD</td>
<td>10.1+</td>
<td></td>
<td>10.1.4.2</td>
</tr>
</tbody>
</table>