ORACLE

FUSION MIDDLEWARE
IDENTITY AND ACCESS
MANAGEMENT SUITE

Oracle Directory Services Integration with Database Enterprise User Security

ORACLE WHITE PAPER | FEBRUARY 2015

ORACLE

Disclaimer

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.

Table of Contents

Introduction

IT departments are under consistent pressure to reduce cost, enhance security, and improve compliance to support ever-competitive business. Databases are critical components of enterprise IT infrastructure, so it is key to centralize and integrate database users and privileges into an enterprise identity management framework.

However, many enterprises today still manage users and privileges on an individual database basis. From an end-user perspective, this means that each user must remember multiple passwords. From an administration perspective, redundant user management is costly; managing user authorizations in multiple databases is error-prone. From an auditing and compliance perspective, on-time provisioning and de-provisioning 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. EUS reduces administration costs and increases security. EUS also improves compliance by centralizing database user account management, provisioning and de-provisioning of database users, password management and self-service password reset, and management of authorizations using global database roles. Furthermore, password policies (including account lockout and password expiration settings) defined in the LDAP-compliant directory and stored in user entries can be used by EUS.

This paper presents the EUS deployment options available with Oracle Unified Directory (OUD) and Oracle Internet Directory (OID). Both use cases will be covered in this document.   The two directories can be used as the central directory repository for database users and privileges as well as be used as a EUS directory virtualization service to leverage existing directory infrastructures based on Microsoft Active Directory (AD), Novell eDirectory, or Oracle Directory Server Enterprise Edition (ODSEE) or even OUD.

Centralizing DB Accounts with OUD

➔ DB Accounts Stored in OUD

OUD works seamlessly with EUS. Database user information, passwords and privileges information for a database or for a database domain can be stored in OUD.

EUS can leverage existing user and group information stored in OUD to provide single password authentication and consistent password policy across enterprise applications. User data, database metadata, such as DB registration information, user/role Mappings, and other EUS specific metadata are stored in OUD using a specific, supported, ready-to-use LDAP schema. These metadata are stored in a separate OUD suffix, called Oracle Context, making a clean logical separation between EUS data and user information that can be shared across applications.

In addition to providing centralized database user management, Enterprise EUS provides three different methods of user authentication:

1. X.509 certificate authentication (introduced in DB 8i)
2. Password-based authentication (since DB 9i)
3. Authentication via Kerberos (since DB 10g).

OUD support for Password-based authentication for EUS was introduced in OUD 11gR2 (11.1.2.0.0). The other authentication methods were introduced in OUD 11gR2PS1 (11.1.2.1).

In the password authentication scenario, the database does not perform user authentication via LDAP bind to OUD. Instead the database performs the authentication via reading user credentials, hashing the password, and comparing the password hash value retrieved from OUD. More detailed information about EUS can be found in the Enterprise User Administrator's Guide in the Database documentation section on Oracle technology Network.

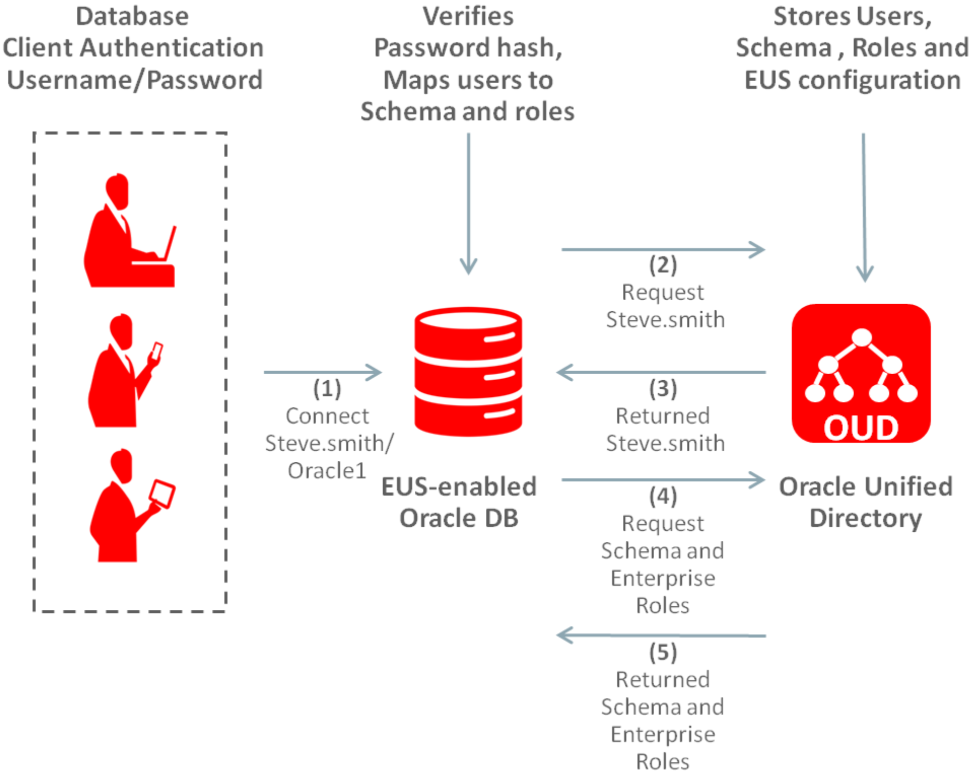

Figure 1: EUS Account management with OUD

➔ DB Accounts Proxy-ed by OUD into existing Directories

As most enterprises already have existing corporate directories in place, via EUS customers do have choice to also leverage the existing directory infrastructure and user information base without putting in place synchronization between directories. In this way, OUD acts as a real-time interpreter for Oracle database information requests to user data.

Using OUD enables the database to interact with third-party directories. OUD leverages existing user and group information in the existing third-party directory infrastructure by forwarding LDAP requests and responses back and forth to the third-party directory holding user data. Database metadata such as DB registration information, user/role Mappings, and other EUS specific metadata are stored locally in OUD, without requiring any schema changes to store EUS configuration in the existing third-party directory.

As of release 11gR2PS1, OUD is certified with EUS to support Active Directory, Oracle Directory Server Enterprise Edition, and Novell eDirectory. Working with these products, OUD eliminates user data duplication and synchronization and consequently lowers total cost of ownership (TCO).

Accounts in Microsoft Active Directory

You can integrate Active Directory for password-based authentication or integrate Active Directory with Kerberos authentication.

Active Directory Integration for Password-based authentication

Such a scenario requires deployment of an additional component: the OUD Password Change Notification plug-in (`oidpwdcn.dll`). Microsoft uses a proprietary implementation to hash passwords in Active Directory that is incompatible with the Oracle DB requirements. The OUD Password Change Notification plug-in is notified when a password change occurs, and stores hashes in Active Directory. The `oidpwdcn` dll must be installed on every Active Directory domain controller.

Active Directory Schema extension is required to store the hashed passwords.

The database establishes a connection to OUD. OUD retrieves user data (users and groups) from Active Directory. User passwords are retrieved from the hashed password stored by the OUD Password Change Notification plug-in. EUS metadata are stored and retrieved from OUD.

The database version must be 10.1 or later as earlier versions use a different and incompatible password format.

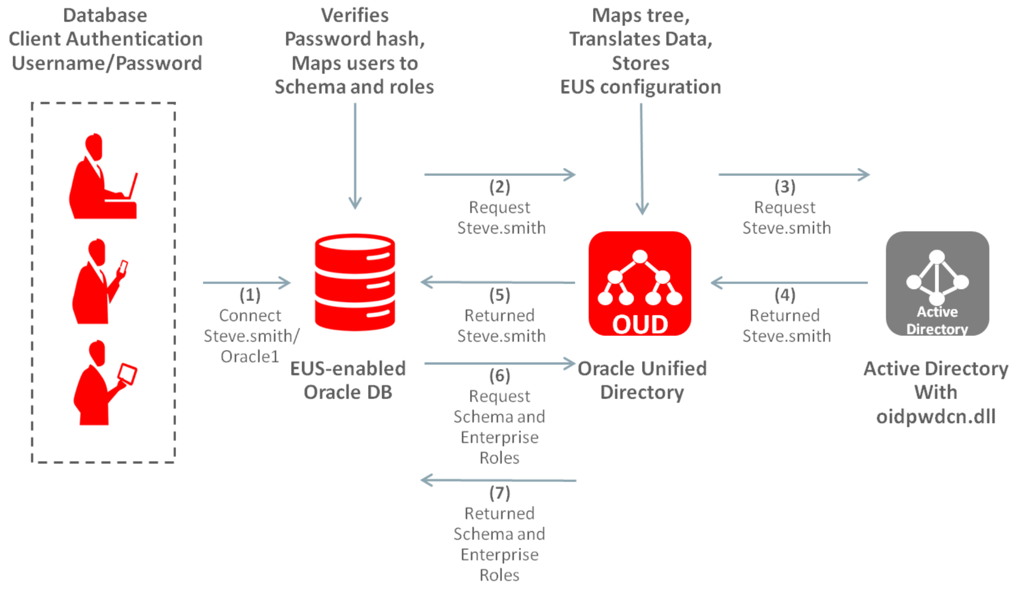

Figure 2: EUS Account management with Active Directory

Active Directory Integration with Kerberos Authentication

In this scenario, Kerberos is used for DB authentication. EUS with DB Kerberos authentication does not require any changes to the database beyond standard EUS configuration. The database establishes a connection to OUD. OUD looks up the requested DB information in Active Directory. All database clients must be Kerberos-enabled to use this option. This capability is only supported with DB version 10.1 or higher.

The database establishes a connection to OUD. OUD retrieves user data (users and groups) from Active Directory. EUS metadata are stored and retrieved from OUD. Access to the hashed user password is not required, so no schema extensions and no Password Change Notification dll have to be deployed on Active Directory.

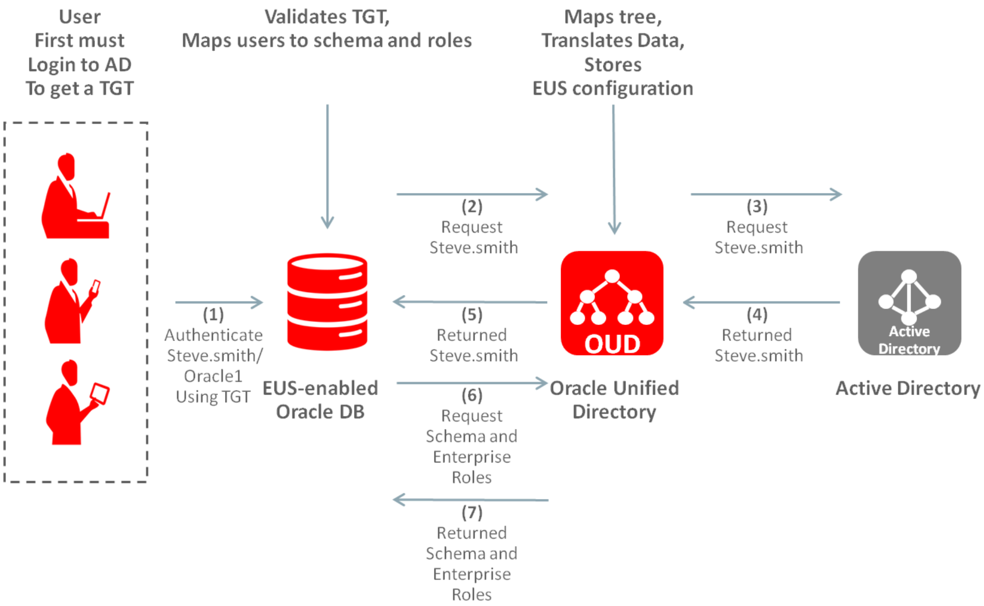

Figure 3: EUS Account management with Kerberos and Active Directory

Accounts in ODSEE

The database establishes a connection to OUD. OUD retrieves user data (users and groups) from Oracle Directory Server Enterprise Edition (ODSEE). EUS metadata are stored and retrieved from OUD.

This integration does not require any changes in the database nor for database clients that use password authentication.

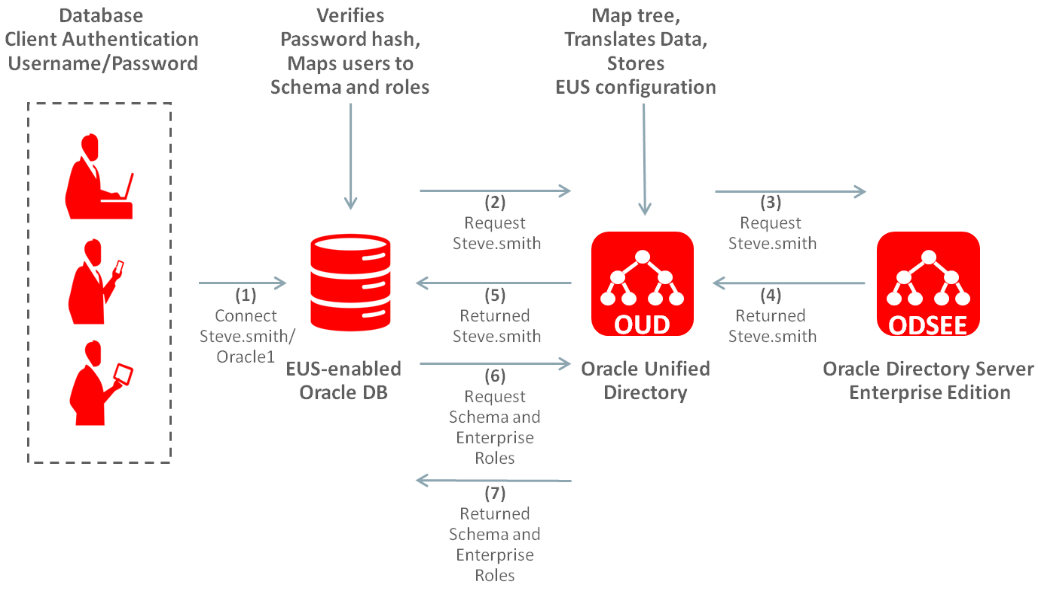

Figure 4: EUS Account management with ODSEE

Accounts in Novell eDirectory

The database establishes a connection to OUD. OUD retrieves user data (users and groups) from Novell eDirectory. EUS metadata are retrieved from OUD.

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.

Using Novell eDirectory doesn't require an Oracle password filter. You have to enable Universal Password in eDirectory, and allow the administrator to retrieve the user password. Refer to Novell's eDirectory documentation on Password Management for more information.

This configuration can only be used with DB versions 10.1 or higher due to incompatible password formats in earlier DB versions.

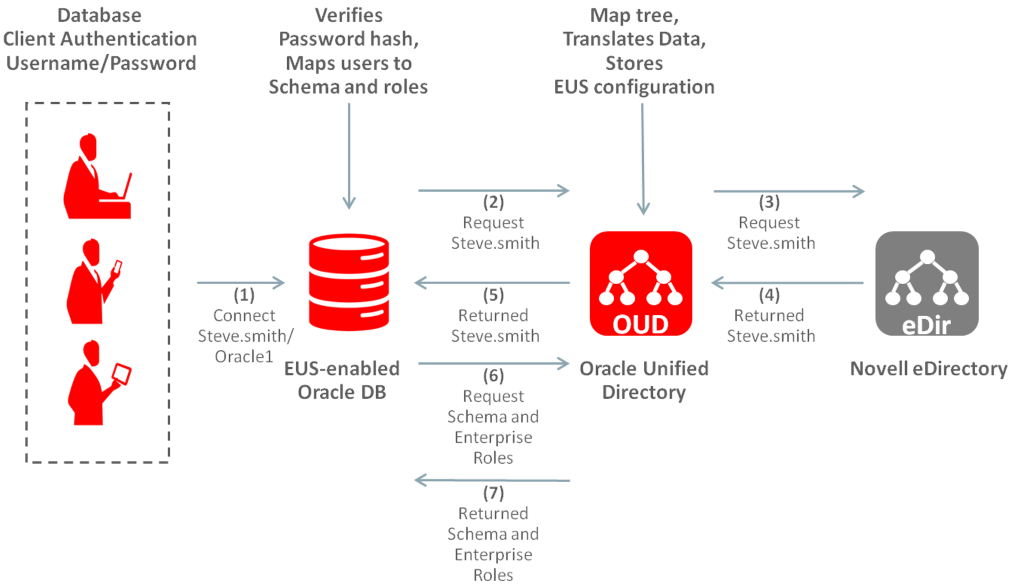

Figure 5: EUS Account management with eDirectory

Centralizing DB Accounts with OID

➔ DB Accounts Stored in OID

EUS deployment can use OID with the database instances registered in OID together with the user authentication and authorization information.

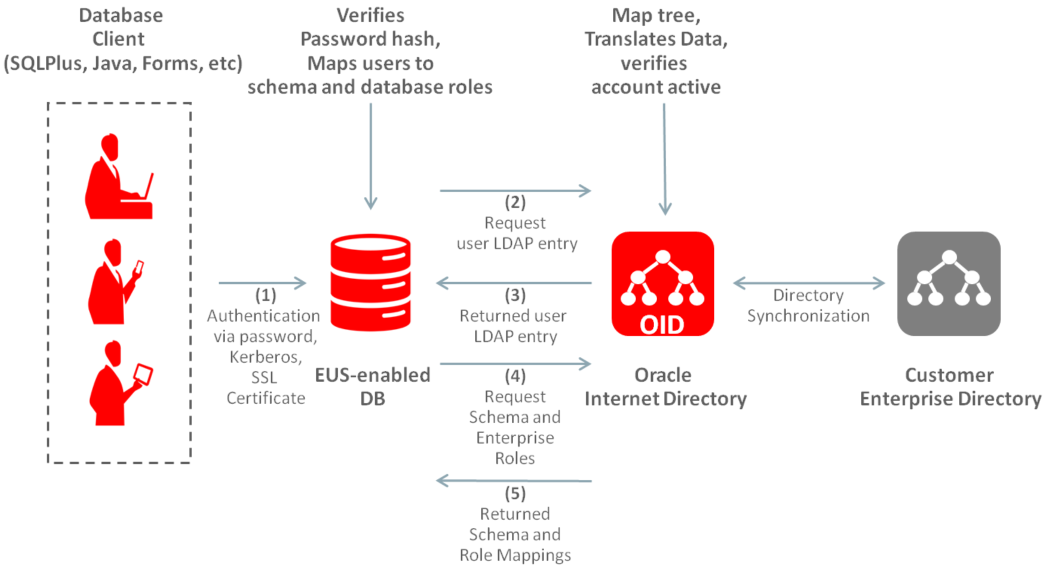

Figure 6: EUS Account management with OID

The communication between the databases can be secured via SSL (which requires the Database Advanced Security Option). The SSL connection is used for OID/Database mutual authentication, not for user authentication. The database uses multiple LDAP search operations to lookup user and password information. OID is actually NOT doing the user authentication through LDAP bind operation, but is only used as data storage for the database, while the database is still authenticating the user.

User information typically will be stored in the default OID user Directory Information Tree (DIT). Database metadata like DB registration information, user/role mappings etc is stored in the OracleContext, a separate container within OID.

EUS supports different methods of authentication:

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

It’s important to distinguish them from the authentication mechanism provided by the Oracle Database (without EUS) and the Advanced Security Option.

The implementation of EUS requires a user footprint in OID including the user password. Besides storing the OracleContext OID is used to enforce access control to protect EUS related data.

More detailed information about EUS can be found in the Enterprise User Administrator's Guide in the Database documentation section on Oracle technology Network.

➔ DB Accounts in existing directories referred to via OID

Often, EUS will be deployed in customer environment where third-party directories are in use, and OID integration with other directories is required to ensure consistent user information. The following use cases describe the integration with Active Directory and ODSEE.

Active Directory Integration for Password Authentication

In this case of using password authentication, database user accounts, including passwords and enterprise roles MUST be stored in OID.

AD as the source for password change, integration using DIP and AD Password Filter

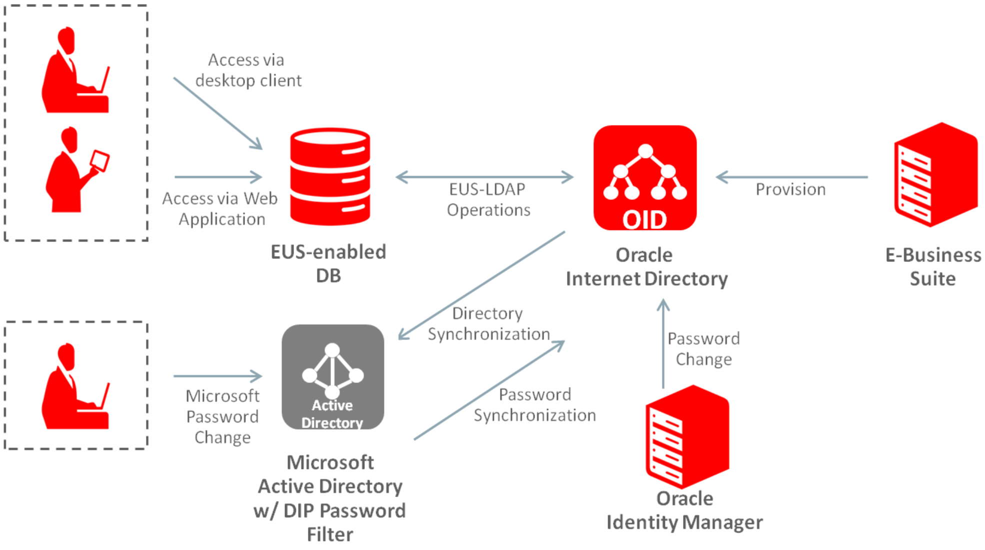
Access via desktop client
Access via Web Application
EUS-enabled DB
EUS-LDAP Operations
OID
Oracle Internet Directory
Provision
E-Business Suite
Directory Synchronization
Password Change
Microsoft Password Change
Active Directory
Microsoft Active Directory w/ DIP Password Filter
Password Synchronization
Oracle Identity Manager

Figure 7: EUS Account management with OID and AD, AD being the source for password change

Synchronization of Active Directory users and groups to OID is handled using the Directory Integration Platform (DIP). This could be done via one time bootstrap using the Directory Integration Platform (e.g. dipassistant). In case the user population doesn't change in Active Directory the DIP server doesn't need to be up and running all the time.

Active Directory Password Filter is used and needs to be installed on each Domain Controller. The filter hooks into the Active Directory LSA to capture password changes via a publish Microsoft API and send them via SSL to OID. In case the password change cannot be pushed into OID (e.g. no connection to OID) the password will be stored encrypted in Active Directory until the connection to OID can be established.

However, the filter has to be stored on all domain controllers. The global catalog server cannot be used together with the password filter, since the passwords are encrypted using a proprietary Microsoft schema.

OID as the source for password change, integration using DIP

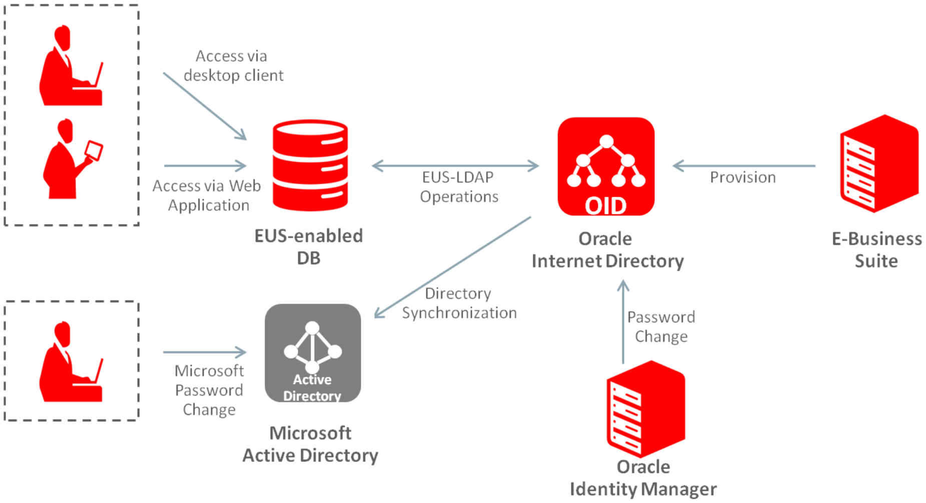

Figure 8: EUS Account management with OID and AD, OID being the source for password change

Enables password based authentication using the Active Directory username by synchronizing the Active Directory user footprint (consisting of Active Directory attributes like samAccountName, krbUserPrincaplName and others) to OID as well as AD group information. Password changes can be synched from OID via SSL to Active Directory, i.e. password will be stored twice. This model assumes OID to be the central source in the deployment.

Initial user passwords have to be generated in OID and the user has to change his password in OID.

Active Directory Integration for Kerberos Authentication

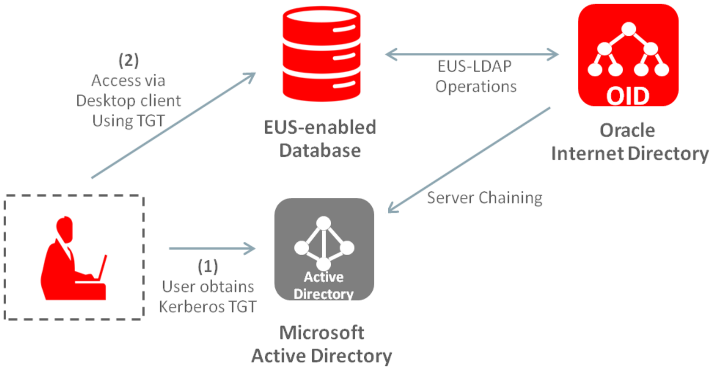

Figure 9: EUS Account management with OID chaining to AD

The usage of Kerberos and OID server chaining eliminates the need to use either DIP synchronization to create the user footprint in OID or install the Active Directory Password Filter to capture password changes in Active Directory. Important to notice, OID is not Kerberos enabled. OID server chaining is used to lookup user and group information in Active Directory on behalf of the DB.

Please note: Kerberos is difficult to install and configure. OID server chaining might expose a performance impact. Only DB versions 10.1+ are supported with EUS Kerberos. OID server chaining can only be used with one Active Directory servers.

DSEE Integration

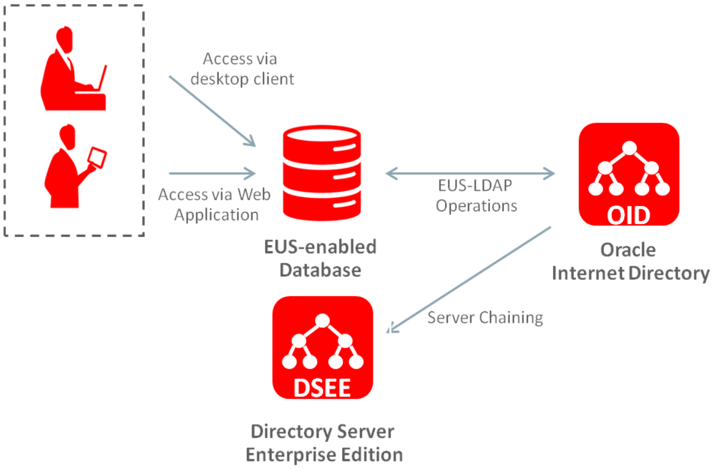

Figure 10 EUS Account management with OID chaining to DSEE

The usage of OID server chaining eliminates the need to install DIP to create the user footprint in OID. Passwords will only be managed in DSEE. OID server chaining is used to lookup password, user and group information in DSEE/OUD. The password is stored in DSEE only.

Please note that server chaining might expose a performance impact. Only DB versions 10.1+ can be used since DB 9i versions expect the DB password to be stored in the user '`orclpassword`' attribute using an Oracle specific password verifier. This password verifier is not available in DSEE directory, hence DB version 9i are not supported in this scenario. User and group changes in DSEE are not propagated back to OID. These kinds of mapping are stored in OID and are not updated.

Conclusion

Centralized management of database user accounts and role memberships using Oracle Database Enterprise User Security (EUS) ensures strong security, reduces administration costs, and improves compliance. OUD provides options for customers to support EUS natively, or to leverage their existing ODSEE, Active Directory, or Novell eDirectory to lower total cost of ownership (TCO).

Appendix A: Supported Deployments with minimum version numbers

Authentication Type	3^{rd} Party Directory	DB	OID	OUD
Certificate		8i+	8i+	
Certificate		10g,11g+		11.1.2.1
Certificate		11g+		11.1.2.2+
Password		9i+	9i+	
Password		10g, 11g		11.1.2.0, 11.1.2.1
Password		11g+		11.1.2.2+
Kerberos		10g, 11g	10g+	11.1.2.1
Kerberos		11g+	10g+	11.1.2.2+
Password	AD + DIP + OIM	9.2.0.3+	10g+	
Password	AD + DIP + Password Filter	10.1+	10.1.4	
Password	ODSEE	10.1+	10.1.4	
Password	ODSEE + OID Server Chaining	10.1+	*10.1.4*	
Kerberos	AD + OID Server Chaining	10.1+	*10.1.4*	
Kerberos	AD + OUD	10.1+		11.1.2.1+
Password	AD + OUD	10.1+		11.1.2.1+
Password	DSEE + OUD	10.1+		11.1.2.1+
Password	eDir + OUD	10.1+		11.1.2.1+

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Hardware and Software, Engineered to Work Together

Oracle is committed to developing practices and products that help protect the environment