Using Oracle with Microsoft Active Directory

An Oracle Technical White Paper
September 2004

ORACLE

Using Oracle with Microsoft Active Directory

INTRODUCTION

In today's information technology environment, administrators are challenged with managing user access to a wide variety of systems, including email, portals, ERP, CRM, and network operating systems. Users can have a separate id on each system along with a varying access control rights. Directory servers centralize user access and authentication for these systems into one repository. User management becomes simpler and single sign-on easier to implement, providing better productivity for both administrators and end users.

With the near-ubiquity of Windows on the desktop, Microsoft Active Directory is one of the most common directory solutions. Active Directory can be easily integrated with Oracle databases and application servers to provide a unified user management experience.

ACTIVE DIRECTORY INTEGRATION WITH ORACLE DATABASE

Oracle makes Windows single sign-on possible and user management easier by allowing user mappings to be stored in Active Directory. Moreover, Net naming (tnsnames.ora) can be stored in Active Directory for centralized management.

Oracle9*i* Database and Oracle Database 10*g* directly integrate with Active Directory through support of single sign-on and integrated user provisioning. These features facilitate integrated Oracle database and Active Directory user access and administration, while maintaining enterprise-scale security. Because these database features integrate directly with Active Directory, they do not require Oracle Internet Directory.

Native Authentication and Active Directory

The Oracle database provides single sign-on capabilities with Active Directory. In this way, end users and administrators simplify user administration and eliminate redundant security credentials. Single sign-on is used through the Windows Native Authentication (WNA) adapter from Oracle, allowing the operating system to perform user identification for Oracle databases. With native authentication enabled, users can leverage single sign-on and access Oracle simply by logging onto Windows. As an additional benefit for administrators, the native authentication adapter provides database lookup of operating system roles.

To provide the single sign-on capability, Oracle database external users and roles can be assigned to Active Directory users and roles. External user mappings allow an operating system user to access an Oracle database as an Active Directory user.

Role mappings allow sets of privileges to be mapped between database users and directory users. In Windows-only environments, these mappings make user administration easier as only a smaller set of common users and roles need to be maintained.

Authentication can occur using either Kerberos or Secure Sockets Layer (SSL). With Kerberos, a Windows client can authenticate with a database server on a Windows or non-Windows platform using the Microsoft Key Distribution Center. Using the WNA adapter, Kerberos authentication can be used on any Windows 2000 or newer operating system. For older Windows operating systems, NT LAN Manager (NTLM) is the default protocol.

With SSL, a Windows client can authenticate with a database server on a Windows or non-Windows platform. If Oracle SSL is used in conjunction with the Microsoft Certificate Store for X.509 certificates, then the client and server environments must both be on Windows. In either case, IT organizations can choose the security protocol that best fits their need depending on their requirements.

Oracle Net Naming with Active Directory

Traditionally, end-users reference databases with Oracle net service names resolved through the TNSNAMES.ORA configuration file that exist on the client machines. These net service names map to the actual database server connection information. Normally, this file must be administered on each client machine that connects to a database server. With Active Directory, net service names can be stored and resolved using the directory. Centralizing the information in a directory eliminates administrative overhead and relieves users from configuring their individual client machines.

To ease administration, the Windows Explorer and Active Directory Users and Computers tools can connect to Oracle databases and test database connectivity. These tools can host database service names, net service names, and role information. Oracle's own configuration tools have been enhanced to make user management with Active Directory easier. The Oracle Net Manager creates net service names in the directory. The Oracle Net Configuration Assistant performs the setup necessary to use Oracle Net naming with Active Directory. These enhancements further simplify administration.

Oracle Database Components Integrated with Active Directory

Component	Description
Oracle Net Configuration Assistant	Net Configuration Assistant is used to do the initial configuration necessary for Active Directory to be used for Oracle Net directory naming. This includes adding the necessary directory schema objects and initial entries in Active Directory.
Oracle Database Configuration Assistant	Database Configuration Assistant registers a database running in a member server or workstation in Active Directory on a Windows domain from a member server or workstation.
Oracle Net Manager	Oracle Net Manager creates net service names in Active Directory, as well as modifies Oracle Net attributes of the database service entry.

ACTIVE DIRECTORY INTEGRATION WITH ORACLE INTERNET DIRECTORY

Oracle's Directory Integration and Provisioning platform, part of Oracle Application Server, allows Oracle Internet Directory to centralize synchronization and provisioning with other directories, include Active Directory.

Many large organizations are choosing to consolidate their directory services with Oracle Internet Directory, part of the Oracle Application Server, for easier user management and maintenance. OID is used as a central repository for signing on to the Oracle database, application server, collaboration suite, and E-Business Suite, especially in environments with a mix of Windows and non-Windows environments. Sometimes there are departmental Active Directory deployments that must be synchronized with OID. OID allows enterprises to centralize their directory store and leverage their existing directory servers, such as Active Directory.

Oracle Directory and Integration Provisioning

Oracle Directory Integration and Provisioning (DIP) platform, a new feature of Oracle Application Server 10*g*, consists of a set of services and interfaces built into OID. It facilitates the development of synchronization and provisioning solutions between the directory and other repositories. These may include other directories, including Microsoft Active Directory Services, application user repositories, or database tables containing human resources information.

DIP provides a number of services that synchronize with Active Directory, allowing administrators to:

- Provision users and groups
- Provide single-sign on capabilities for these users once they've been authenticated with the directory

- Update user and group privileges
- Update user or group data, such as password updates

This platform includes two services: a provisioning service and a synchronization service. The provisioning service facilitates automatic execution of application-specific user provisioning activities when user or group entries in the directory are updated or deleted. These are executed as PL/SQL procedures that may add, delete or suspend privileges for a user in a connected system. Various Oracle product components use the provisioning engine to automatically create "account footprints" for users managed in the directory.

The synchronization service publishes changes made to data contained in Oracle Internet Directory to connected agents that subscribe to specific sets of directory data. It also reads and applies changes made in connected systems. These together facilitate a "synchronization" of data contained in Oracle Internet Directory and the connected system, such as Microsoft Active Directory Services.

DIP Potential Solutions

There are a number of ways that Oracle DIP can be deployed as part of an enterprise user provisioning solution. For example:

- A user provisioning workflow might be driven from the Windows environment, creating users in the Oracle environment. For instance, an Oracle Portal user might be created when a new user is created in the Windows operating system or Microsoft Exchange.
- A user provisioning workflow might be driven from the Oracle environment, creating users in the Windows environment. For example, creation of an employee entry in Oracle Human Resources might trigger user account creation in Microsoft Windows.
- Finally, third-party provisioning solutions, which are integrated with Oracle Internet Directory, may be leveraged to drive provisioning workflows in both Windows and Oracle environments.

In all three cases, Oracle Internet Directory provides a single point of integration for all user provisioning in the Oracle application environment.

In addition to supporting an integrated user provisioning solution, an Oracle-to-Windows directory connector is useful for ongoing user administration. For instance, a change in user group membership in the Windows environment can result in a corresponding change in group membership (and therefore application privileges) in the Oracle environment.

Oracle Internet Directory Components Integrated with Active Directory

Component	Description
Oracle Internet Directory	The repository in which Oracle components and third-party applications store and access user identities and credentials. It uses the Oracle directory server to authenticate users against the stored credentials. When credentials are stored in a third-party directory and not in Oracle Internet Directory, users can still be authenticated. In this case, Oracle Internet Directory uses an external authentication plug-in that goes to the Active Directory server for authentication.
Oracle Directory Integration and Provisioning Platform	This platform enables: • Synchronization between Oracle Internet Directory and other directories and user repositories • Automatic provisioning services for Oracle components It is installed as part of the Oracle Application Server infrastructure, but you can install it separately. This platform includes connectors for synchronizing between Oracle Internet Directory and other LDAP directories. One of its connectors, the Active Directory connector, is designed for two-way synchronization between Oracle Internet Directory and Microsoft Active Directory. The Active Directory connector enables you to: • Configure either one-way or two-way synchronization • Designate a specific subset of attributes for synchronization. You do this by configuring the appropriate mapping rules, which you can then change at runtime. • Synchronize against multiple Microsoft Active Directory servers. You can synchronize changes both directly against an individual server and from an entire Microsoft Active Directory environment by using the Microsoft Global Catalog.
Directory Integration and Provisioning Assistant	This tool enables you to migrate data between Oracle Internet Directory and Active Directory. More specifically, it enables you to: • Migrate data in either direction

	• Migrate a large set of data by using an LDIF file, or a smaller set of data by using straight LDAP • Migrate all or a subset of attributes within each entry. This tool uses the same set of mapping rules as the Oracle directory integration and provisioning server.
Oracle Application Server Single Sign-On	Oracle Application Server Single Sign-On enables users to access Oracle Web-based components by logging in only once. Oracle components delegate the login function to the OracleAS Single Sign-On server. When a user first logs into an Oracle component, the component redirects the login to the OracleAS Single Sign-On server. The OracleAS Single Sign-On server authenticates the user by verifying the credentials entered by the user against those stored in Oracle Internet Directory. After it has authenticated the user, and throughout the rest of the session, the OracleAS Single Sign-On server grants the user access to all the components the user seeks and is authorized to use. Oracle Application Server Single Sign-On enables native authentication, also called autologin, in a Microsoft Windows environment. Once logged into the Windows desktop, the user automatically has access to Oracle components. OracleAS Single Sign-On automatically logs the user into the Oracle environment using user's Kerberos credentials.
Active Directory External Authentication Plug-in	This plug-in, which is part of the Oracle directory server, enables Microsoft Windows users to log into the Oracle environment by using their Microsoft Windows credentials. When such a user tries to log in, the OracleAS Single Sign-On server tries to verify the credentials the user enters against those stored in Oracle Internet Directory. If the user credentials are not there, then the Oracle directory server invokes the Active Directory external authentication plug-in. This plug-in verifies the user credentials in Microsoft Windows. If the verification is successful, then the Oracle directory server notifies the OracleAS Single Sign-On accordingly. In addition to enabling external authentication against Microsoft Windows, this plug-in also automatically provisions Microsoft Windows users into the Oracle Identity Management system.

Oracle Internet Directory Self-Service Console	Oracle Internet Directory Self-Service Console is a Web-based tool for managing users, groups, and their credentials in Oracle Internet Directory. Built from service units of Oracle Delegated Administration Services, this tool enables users to manage user passwords and password policies.
Oracle Directory Manager	Oracle Directory Manager is a Java-based tool for administering Oracle Internet Directory. It enables directory administrators to manage all directory data including user information and configuration information used by the Oracle directory integration and provisioning server.

Using Oracle with Microsoft Active Directory
September 2004
Author: Alex Keh
Contributing Authors: Toby Close, Santanu Datta, Sudha Iyer, Michael Mesaros

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Oracle Corporation provides the software
that powers the internet.