Oracle Identity Management: Integration with Windows

An Oracle White Paper
December. 2004

ORACLE

Oracle Identity Management: Integration with Windows

Oracle Identity Management: Integration with Windows

INTRODUCTION

Oracle Identity Management is an integrated, scalable and robust identity management infrastructure. Oracle Identity Management includes an LDAP directory service, directory integration and provisioning services, a delegated administration service application, authentication and authorization services, and an X.509 V3 certificate authority. Key benefits of Oracle Identity Management are its robustness and scalability, out-of-the-box deployment support for Oracle products, utility as a single point of integration for other enterprise identity management option solutions, and open, standards-based implementation.

Oracle Internet Directory is an LDAP V3-complient directory service implemented on the Oracle Database. As an enterprise directory service, Oracle Internet Directory provides exceptional levels of availability, scalability and reliability. Oracle Internet Directory is a central component of Oracle Identity Management, which provides security services, user and name service management for multiple components in the Oracle Database, Oracle Application Server and Oracle E-Business Suite.

Administrators in enterprise environments are challenged with providing and managing user access to a wide variety of systems, including e-mail systems, portals, ERP and CRM applications, and network operating systems. Integration of the disparate enterprise directories therefore plays a central role in the deployment of comprehensive user provisioning and administration solutions. In particular, Windows near-ubiquity on the desktop means that many Oracle administrators are looking for ways to integrate Microsoft Active Directory Services and Oracle Identity Management.

This paper describes the mechanisms available for integrating Oracle user management with other enterprise services, especially Microsoft Windows. We describe motivations for Windows integration (user provisioning, privilege management, single sign-on), major integration points between the Oracle and Windows environments, and integration strategies. It is our expectation that this information will be particularly useful to Oracle customers and partners who are planning Windows deployments, or are managing systems in environments where Windows deployments are planned.

GOALS FOR WINDOWS INTEGRATION

In our experience, Windows integration can mean different things to different people. This is particularly true with respect to user security interoperability, where a Windows integration requirement can mean any combination of:

- A single tool for user self-administration of basic application user information such as user names, passwords and user preferences.
- The ability to have role-based administration of groups of applications users in one environment to be reflected in the other.
- Automatic provisioning of new users entered in one application environment into the other.
- Ability for an administrator to suspend or delete user accounts centrally.
- "Single sign-on" from the Windows environment into the Oracle application, portal, and/or database environment.

From a directory and security integration perspective, these requirements can be distilled into three major benefits:

- *Unified user provisioning* - User provisioning refers to the process by which new users are added and deleted from the various enterprise systems. New user provisioning can potentially be driven from a number of different sources, for example HR systems, CRM systems, network administration environments, etc. When a new user is created in one system, automated user provisioning creates the required user account "footprints" in other enterprise applications.
- *Centralized user administration* - Once a user account is created, it needs to be maintained and administered. Centralized user administration ensures that all of the application-related information associated with a user, such as passwords, roles and application preferences, are administered in one place.
- *Runtime security service integration* - Finally, customers want to be able to provide their users with a transparent runtime experience. This means that the various applications in the enterprise environment must be capable of leveraging a common set of security services for purposes of authentication and data privacy.

Delivering these benefits requires tools and solutions for integrating the Oracle and Windows directory environments. In the following section we describe capabilities implemented with Oracle Identity Management that facilitate development of directory integration solutions.

DIRECTORY INTEGRATION TOOLS

Oracle Identity Management provides useful tools for integrating with the Windows administration environment. Two of these, the Directory Integration

Platform and the Oracle Internet Directory Plug-In Architecture, are described below.

Directory Integration Platform

Oracle Identity Management's Directory Integration Platform consists of a set of services and interfaces built into Oracle Internet Directory. These facilitate the development of synchronization and provisioning solutions between the directory and other repositories. These may include directories (such as Sun/iPlanet Directory and Microsoft Active Directory Services), application user repositories (as might be stored in a flat file, for example), or database tables containing human resources information.

The Directory Integration Platform includes two services: a provisioning service and a synchronization service (Figure 1). 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, for example Microsoft Active Directory Services or Sun/iPlanet Directory Server.

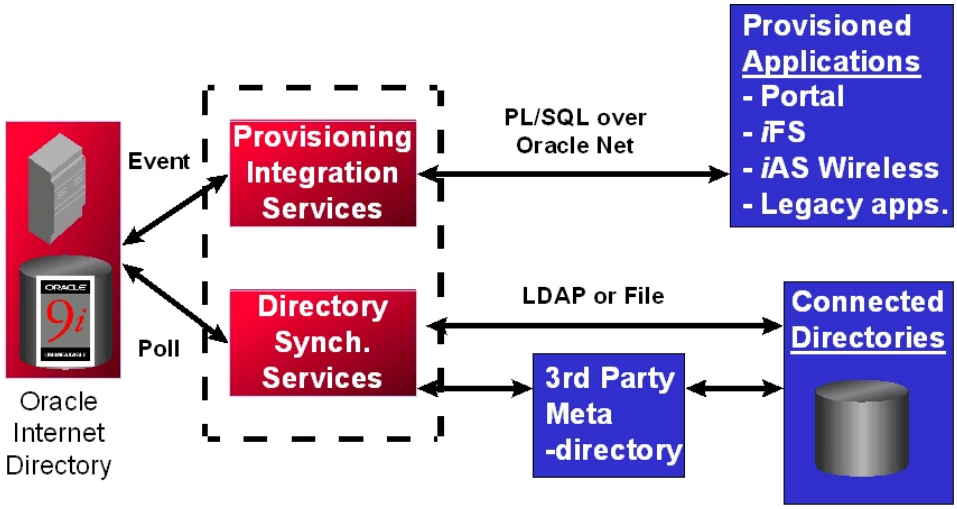

Figure 1: Oracle Directory Integration Platform.

The Oracle Directory Integration Platform includes a documented application-programming interface and incorporates available industry standards where they exist. This makes it possible for Oracle, customers and third-parties to develop and deploy customized synchronization and provisioning solutions. It also facilitates

interoperability between Oracle Internet Directory and third-party metadirectory (shown) and provisioning solutions.

Oracle Internet Directory Plug-In Architecture

Oracle Internet Directory starting with Oracle9*i*AS R2 supports a PL/SQL-based plug-in framework. This framework allows the inclusion of custom routines (Oracle, customer-written or third-party) which may execute before, during or after a directory operation. For example, this framework may be used to:

- Validate data before the directory server performs an operation on it.
- Perform specified actions after the server performs an operation.
- Define custom password policies.
- Authenticate users through external credential stores such as NOS directories.

Oracle Internet Directory plug-ins run as PL/SQL routines, and are executed in the protected memory space of the Oracle Database. By executing in a separate memory space from the server, this architecture ensures that plug-ins do not potentially have access to server memory space, thus closing a frequent security concern with plug-ins.

A diagram illustrating the Oracle Internet Directory plug-in architecture is shown below (Figure 2).

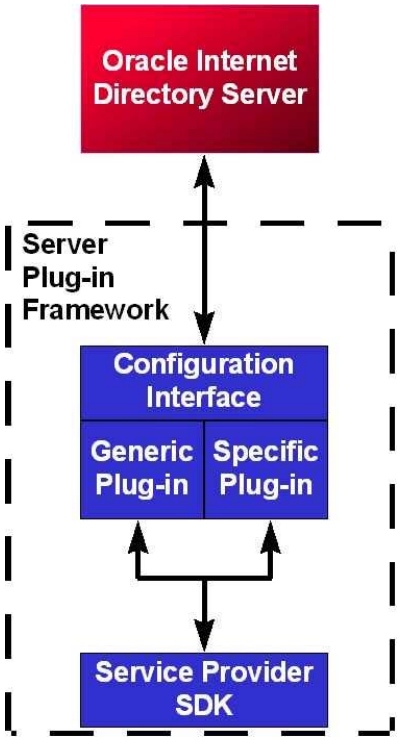

Figure 2: Oracle Internet Directory Server Plug-in Framework.

CLIENT/SERVER INTEGRATION WITH WINDOWS SECURITY SERVICES

In the client/server environment, there are three options for sites wishing to leverage Windows credentials or authentication services for signing on to the Oracle Database.

- On the Windows platform, the Oracle Database includes the Windows Native Authentication Adapter, which installs automatically with Oracle Net Server and Client. This feature allows Oracle Database users to authenticate to the database using their Windows user credentials. To use this feature, Windows users must be defined as database external users. These users can have external roles assigned to them in Microsoft Active Directory Services which will be respected by the database.
- Oracle Advanced Security, a database option, supports database authentication using Kerberos tickets issued by the Microsoft Key Distribution Center (MSKDC). This capability allows users who have been issued a valid Kerberos ticket in the Windows environment to sign-on to their database accounts without having to provide a username/password.
- Finally, the Oracle Advanced Security option also supports database authentication over SSL using an X509v3 certificate. The Microsoft Certificate Store (MCS) may issue this certificate. To use this feature, the certificate must be contained in an Oracle Wallet configured on the client.

The Oracle Wallet may be stored either in the User Profile area of the Windows Registry or in an arbitrary file location on the client.

WEB-BASED INTEGRATION WITH WINDOWS SECURITY SERVICES

Directory Connectors

To provide interoperability between the Oracle and Windows directory environments, Oracle's strategy aims to address the interoperability of its technology stack as a whole instead of on an individual component-by-component basis. This is accomplished by making Oracle Identity Management the common point of integration between all Oracle products and components and third-party directories. Leveraging existing third-party directories involves deployment of a directory integration component, called a connector, based on Oracle Internet Directory and the Directory Integration Platform. This approach to platform integration simplifies the certification, support and maintenance of such configurations for customers and for Oracle.

The Oracle-to-Windows directory connector can be deployed as part of an enterprise user provisioning solution. This could be used to support different provisioning models, for example:

- A user provisioning workflow might be driven from the Windows environment, creating users in the Oracle environment. For example, 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 that are integrated with Oracle Identity Management may be leveraged to drive provisioning workflows in both Windows and Oracle environments.

In all three cases, Oracle Identity Management 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 example, 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.

Windows Authentication and Password Modifier Plug-In

As was described above, Oracle Internet Directory includes a plug-in architecture which permits integration of Oracle Internet Directory with external authentication mechanisms, such those used by Windows. Oracle Identity Management includes a

Windows authentication plug-in as a prepackaged capability. This allows Oracle's directory-enabled security components to manage user information in Oracle Internet Directory while leveraging the credentials stored in Windows as the authentication source of truth. This solution provides users and administrators with the benefits of a single point of password management, while eliminating a need to synchronize passwords or password descriptors between the two environments.

Even if passwords are stored in Windows, it may be desirable to allow users to manage them in the Oracle application environment. A Windows password modifier plug-in facilitates this by triggering a change in the Windows password when the Oracle Internet Directory password is modified through the LDAP interface. This allows centralized password management for both Windows and Oracle environments from Oracle self-service tools.

Single Sign-On Integration with Windows Security

As was mentioned above, Oracle today provides runtime integration with the Windows security services. For example, through Oracle Advanced Security, Microsoft Kerberos credentials can be used to authenticate Oracle Database users. Some customers, however, are looking to provide their users with an enterprise-wide single sign-on experience. For example, a user signed on to the Windows operating system might be automatically authenticated to an Oracle-based portal and application environment. While the directory integration described above has its own benefits, it is also a necessary step in providing this kind of enterprise single sign-on functionality. Another necessary step is for the security services in the Oracle environment need to respect credentials issued in the Windows environment.

For web-based applications, OracleAS Single Sign-On provides the authentication services for Oracle and partner applications. OracleAS Single Sign-On allows users already authenticated to a Windows environment to be automatically signed-on to OracleAS partner applications.

Integration with MCS is also possible through Oracle Single Sign-On. In addition to supporting password-based authentication mechanisms, the OracleAS Single Sign-on Server supports certificate-based authentication. This certificate can be generated by MCS. To use certificate-based authentication, a user certificate must be populated into the browser wallet and into the corresponding user entry in Oracle Internet Directory.

CONCLUSION

Through integration with the Oracle Identity Management, Oracle has integrated user security services and administration for the Oracle environment. Through the integration tools presented in this paper, Oracle can provide the same degree of integration with other enterprise systems, such as the Window security environment. This can provide administrators with transparent user provisioning

across the two environments, and end users with a single point of password administration, and ultimately, single sign-on across the two environments.

Oracle Identity Management: Integration with Windows
December, 2004
Author: Michael P. 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