Oracle Advanced Security: Security and Directory Integration

Features Overview

November 1999

PRODUCT SUMMARY

With the continued growth of distributed systems, the problem of user authentication and user management has become acute. Users have too many passwords; consequently, they write them down, or choose the same password for all accounts. Organizations must manage multiple accounts for each user; as a result, they devote significant resources to user administration, or invest in network authentication services, many of which promise single sign-on and centralized authorization management. Common information used by multiple applications — such as username, user's office location and phone number — is often fragmented across the enterprise, leading to data that is redundant, inconsistent, and expensive to manage. The lack of centralization is a security risk, because old or unused accounts and privileges can be misused.

Oracle Advanced Security addresses the above needs for strong security, single sign-on and centralized user management by offering integrated security and directory services; specifically, by storing and managing user information in a directory which supports the Lightweight Directory Access Protocol (LDAP). Multiple Oracle applications can rely on a common, centralized definition of a user to determine which applications, services, and data servers a user may access, and with what privileges. The benefits of integrated security and directory services include:

- Single sign-on to multiple Oracle8*i* databases throughout the enterprise.
- Single enterprise user account, instead of multiple accounts per user.
- Reduced total cost of ownership through single station administration (SSA).
- Well-integrated, standards-based public key infrastructure (PKI).
- Better security through centralized authorization management and strong authentication.

Oracle Advanced Security's integrated security and directory services incorporates multiple Oracle components, including:

- *Oracle Wallet Manager* — A tool which is used to protect and manage user certificates, keys, and trustpoints.
- *Oracle Enterprise Login Assistant* — An easy-to-use tool which enables single sign-on for users.
- *Oracle Internet Directory* — An LDAPv3-compliant directory service, built on the Oracle8*i* database, which stores information about enterprise users and enterprise roles.
- *Oracle Enterprise Security Manager* — An administration tool available through Oracle Enterprise Manager, which allows administrators to manage enterprise users and enterprise roles in Oracle Internet Directory, and across multiple Oracle8*i* databases, from a single console.

- *Oracle8i* — A data server which retrieves users' enterprise roles from Oracle Internet Directory and authenticates users over SSL.

Oracle Advanced Security's integrated security and directory services also requires the following non-Oracle component:

- *Certificate Authority* (CA)— An X.509-compliant certificate authority which creates digital certificates.

Oracle Wallet Manager

An advantage of X.509 certificates is that they may be used to uniquely identify an individual within an organization, and thus enable strong authentication. Oracle Wallet Manager provides secure management of PKI (public key infrastructure)-based user credentials. Oracle Wallet Manager creates a private and public key pair for a user, and issues a Public Key Certificate Standard (PKCS) #10 certificate signing request which can be fulfilled by any X.509 v3-compliant CA. After the CA issues an X.509 certificate, the user can load the certificate into his wallet. Oracle Wallet Manager stores and manages PKI credentials for servers, such as Oracle Internet Directory and Oracle8*i*, as well as users.

Oracle Wallet Manager also manages user trustpoints, the list of root certificates that the user trusts, and is pre-configured with root certificates from PKI vendors such as VeriSign and GTE. Wallets are protected using password-based, strong encryption, and are stored on the client.

PKI-based Single Sign-On

Oracle Advanced Security (formerly Advanced Networking Option) supports multiple single sign-on mechanisms, including Kerboros and DCE. Release 8.1.6 of Oracle Advanced Security enhances the single sign-on options available to customers by providing PKI-based single sign-on.

In most cases, a user need never access a wallet once it has been configured, but can easily access his wallet using Oracle Enterprise Login Assistant, a very simple, easy-to-use login tool that hides the complexity of a private key and certificate from users. Users provide a password to Oracle Enterprise Login Assistant, which then opens the user's encrypted wallet. The certificate and private key contained in an Oracle wallet are used to authenticate the user to multiple databases, which need no longer store and manage local passwords for users. Furthermore, authentication is transparent to the user, who need not provide any additional passwords once his wallet has been opened.

Oracle Advanced Security offers enhanced PKI-based single sign-on through use of interoperable X.509 (version 3) certificates for authentication over Secure Sockets Layer (SSL), the standard for Internet authentication. In addition to strong user authentication, SSL also provides network data confidentiality (through encryption) and data integrity for multiple types of connections: LDAP, IIOP (Internet Intra-ORB Protocol), and Net8™.

PKI-based single sign-on over SSL can be used alone, or in conjunction with enterprise user management, described below.

Enterprise User Management

Enterprises today face tremendous challenges in managing information about users, keeping user information current, and securing access to all the information in an enterprise. Each user may have multiple accounts on different databases, requiring her to remember passwords for each of these accounts. Users not only have too many passwords, but there are too many accounts for administrators

to manage. Furthermore, the lack of centralization is a security risk, because old or unused accounts and privileges can be misused.

To address these challenges, Release 8.1.6 introduces enterprise user management. *Enterprise users* and their authorizations are managed in Oracle Internet Directory, an LDAP-based directory service, using Oracle Enterprise Security Manager, a tool accessible through Oracle Enterprise Manager.

Enterprise users can be assigned *enterprise roles* (which are containers of database-specific *global roles*), that determine their access privileges in specific databases. For example, the enterprise role CLERK could contain the global role HRCLERK on the Human Resources database, and the global role ANALYST on the Payroll database. An enterprise role can be granted or revoked to one or more enterprise users. For example, an administrator could grant the enterprise role CLERK to a number of enterprise users who hold the same job. This information about users and roles is protected in the directory through Access Control Lists, ensuring that only a privileged administrator can manage users, and grant and revoke roles.

Oracle's LDAP version 3-compliant directory server, Oracle Internet Directory, is fully integrated with Oracle8*i* and supports "off-the-shelf" enterprise user management. Other LDAP directories, including Novell Directory Service (NDS) and Microsoft's Active Directory for Windows 2000 will be certified to operate with Release 8.1.6.

User/Schema Separation

Single sign-on solutions address the "too many passwords" problem and generally result in both stronger authentication and an improved user experience. However, users all too often still need to have multiple accounts: one for each application, database, or network service which they access, and organizations must still expend large amounts of time and money creating, administering, and deleting these user accounts. Therefore, deploying a directory service for enterprise user management is only beneficial if you can actually *reduce* the number of user accounts; otherwise, the directory service is just another place to create user accounts!

In general, users really do not need their own accounts – or their own schemas – in a database, they merely need to access an application schema. For example, suppose users John, Firuzeh and Jane are all users of the Payroll application, and they need access to the Payroll schema on the Finance database. None of them needs to create his or her own objects in the database; in fact, they need only access objects associated with the Payroll schema, such as the Employees table, the Salary table, and so forth.

Release 8.1.6 allows you to separate users from schemas, so that many enterprise users can access a single, *shared application schema.* Instead of creating a user account (that is, a user schema) in each database a user needs to access, you need only create an *enterprise user* in the directory, and "point" or "map" the user to a shared schema that many other enterprise users can also access. For example, if John, Firuzeh and Jane all access the Sales database, you need only create a single schema in the database, e.g. 'sales_application' which all three enterprise users can access, instead of creating an account for each user on the Sales database. Enterprise users may also share schemas on multiple databases. For example, Firuzeh and Jane may also access the shared schema 'financials' on the General Ledger database.

Organizations deploying Internet applications reap the greatest benefit of user/schema separation. These organizations want to have identified users, but cannot afford the management or storage

overhead of creating potentially hundreds of thousands of users, certainly not in the applications and databases behind their Internet front-end. However, directories excel at management, search, and retrieval of hundreds of thousand of user records. Creating "Internet application users"—that is, enterprise users — as directory entries gives organizations the benefit of keeping track of their users (and their users' preferences), with high security and low overhead.

The separation of users from schemas is truly the payoff for deploying a directory service. Thousands of users can connect to a database, be known to the database (and audited in the database), with specific privileges in the database, without being created in the database. Now, you can truly create an enterprise user once, in the directory — a single enterprise user account — who nonetheless can access multiple databases, using only the privileges she needs to perform her job.

Enterprise user management thus offers the following benefits:

- *Fewer User Accounts* — Enterprise users no longer need to be database users nor have identified schemas.
- *Internet Scalability* — You can support hundreds of thousands of users, who are known to multiple databases, accountable (and audited in) multiple databases, without creating thousands of database user accounts.
- *Easily-Enforced Security* — If a user changes jobs or leaves, his privileges can be altered or removed, everywhere, merely by changing his user entry in Oracle Internet Directory. Organizations no longer need to worry about "orphan" accounts or out-of-date privileges, which consume valuable system resources and are targets for hackers.
- *Reduced Cost of Ownership* — Organizations save significant resources by managing a single enterprise user account and assigning enterprise roles once, instead of creating multiple user accounts with multiple passwords, each having multiple authorizations.

Single Station Administration (SSA)

Managing thousands of user accounts is one of the largest administration challenges facing large organizations. Creating user accounts and assigning privileges is often a multi-step process, requiring multiple tools.

Significant new functionality has been added in Release 8.1.6 to address this need. Oracle Enterprise Security Manager (an extension to Oracle Enterprise Manager) provides single station administration. From a single console, an administrator can perform the following:

- Create enterprise users in Oracle Internet Directory.
- Create shared schemas in databases
- Map enterprise users to shared schemas
- Create enterprise roles that span multiple databases.
- Assign one or more enterprise roles to a user.
- Configure Access Control Lists on directory objects

Oracle Enterprise Security Manager provides one tool for enterprise user management, resulting in a lower cost of user administration throughout the enterprise. Another benefit of single station administration is that if security is easy to administer, organizations are more likely to implement strong security throughout the enterprise.

Robust Directory Services

Oracle Internet Directory is a native LDAP version 3 implementation that combines the mission-critical strength of Oracle's database technology with the flexibility of the Internet standard. Oracle Internet Directory is the default data repository for accessing Oracle8*i* enterprise user information, including enterprise roles and shared schema information.

Oracle Internet Directory offers flexible, highly-granular access control mechanisms which protect the sensitivity of common application information as well as Oracle's enterprise user information. Oracle Internet Directory's Access Control Lists (ACLs) can be used to specify, at the attribute level, the users entitled to access and the type of access permitted. For example, a user's manager may have read and write access to a user's salary attribute, the user can read his own salary, but no other user has access to it. Oracle Internet Directory also offers configurable default, guest, and super-user permissions, to enable users to have "least privilege"— just the privileges they need to perform their jobs, and no more. Oracle Internet Directory can be automatically configured with the schema and required Access Control Lists (ACLs) the Oracle8*i* database needs for enterprise user management,

Oracle Internet Directory exploits the built-in availability and performance of the underlying Oracle8*i* data server, as well as offering bulk loading, deletion, and updates of directory entries, high-speed backup and recovery tools, the ability to add or delete directory nodes without service disruption, and other high availability features.

Availability

Integrated security and directory services are available with Release 8.1.6 of Oracle Advanced Security, including Oracle Wallet Manager, Oracle Enterprise Login Assistant, Oracle Enterprise Security Manager, use of SSL for encryption, authentication and single sign-on, user/schema separation and the use of Oracle Internet Directory for enterprise user management.

Oracle Internet Directory may also be purchased separately.

Summary

Oracle Advanced Security's integration of security and directory services offers strong user authentication through standards-based single sign-on, and reduces users' frustration with too many passwords. Administrators spend less time managing user accounts, because they are able to centrally administer users across multiple databases. The Single Enterprise User offers even greater benefits for organizations that need only create one account per user for the entire organization. Oracle environments may store their entire definition of a user, and the user's roles and privileges, within a directory service. The Single Enterprise User enables organizations deploying Internet applications to support thousands of users securely, with reduced cost of ownership, and scale to tens of thousands, hundreds of thousands, or even millions of users over a distributed enterprise.

Key Security and Directory Features

Authentication

- SSL offers strong, standards-based authentication and single sign-on to Oracle
- Mutual authentication of databases over SSL
- SSL authentication of Oracle8*i* to Oracle Internet Directory

Management/Ease of Use

- Single Station Administration of users across multiple Oracle8*i* databases using Oracle Enterprise Security Manager
- Oracle Enterprise Login Assistant for easy-to-use single sign-on
- Single Enterprise User defined and managed in a directory
- Easy installation of certificates and certificate trustpoints using Oracle Wallet Manager
- Bundled, well-integrated LDAP v3-compliant directory service
- Default Access Control Lists

Application Integration

- Support for NDS and Active Directory
- Support for multiple standards, including LDAP (version 3), X.509(version 3), and SSL

Performance

- Oracle Internet Directory leverages high availability and scalability of the underlying Oracle8*i* data server

Encryption

- SSL encryption of IIOP, LDAP, and Net8 connections

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

Worldwide Inquiries:
+1.650.506.7000
Fax +1.650.506.7200
http://www.oracle.com/