Oracle8*i*™ Release 8.1.6 New Security Features Summary

Features Overview
November 1999

INTRODUCTION

Oracle8*i* Release 8.1.6 is the first maintenance release of the Oracle8*i* database, including many bug fixes, performance improvements, and feature enhancements. However, this release also includes several critical security new features that are noteworthy. The enhancements and new features in release 8.1.6 can be categorized as:

- Oracle8*i* Improvements
- Oracle Advanced Security Improvements

ORACLE8*i* IMPROVEMENTS

The main focus of Release 8.1.6 is to maintain stability and improve on quality, performance, and installation/configuration and management of the Oracle8*i* database server. Oracle has also added specific enhancements to improve the security and user management capabilities of the Oracle8*i* server.

STORED DATA ENCRYPTION

The growth of electronic commerce has resulted in an increase in the storage of highly sensitive information, such as credit card numbers, in the database. Countries with strict national privacy laws are often required to prevent national identity numbers from being viewed, even by DBAs or other "trusted" users. Companies with trade secrets, such as industrial formulas, may wish to

zealously guard these valuable assets. Applications for which users are not database users may wish to store “application user” passwords, or session cookies, in encrypted form in the database.

Most issues of data security can be handled by Oracle8*i*’s authentication and access control mechanisms, ensuring that only properly identified and authorized users can access data. Data in the database, however, cannot normally be secured against the database administrator's access, since a DBA has all privileges.

For applications with special requirements to secure sensitive data from view, even from DBAs, Oracle8*i* release 8.1.6 provides a PL/SQL package to encrypt (and decrypt) data, including string inputs and raw inputs, using the industry-standard Data Encryption Standard (DES), in exportable keylengths.

The ability to natively encrypt data in the server enables applications to guard their especially sensitive data. Furthermore, developers need no long “roll their own” encryption using algorithms they craft themselves, or download from the Internet.

VIRTUAL PRIVATE DATABASE ENHANCEMENTS

Oracle8*i* introduced the Virtual Private Database, which provides server-enforced, fine-grained access control. Because the Virtual Private Database provides server-enforced security, it cannot be bypassed by users accessing data directly, or using another application. The application context feature can be used to improve the performance of Virtual Private Database by functioning as a secure data cache. Application context has been enhanced in Release 8.1.6 so that additional attributes, including external name, proxy user and userid, protocol, port number, and full DN (distinguished name) from an X.509 certificate, are now accessible and can be used to limit access to data. For example, you could use the OU (Organizational Unit) component of a DN to limit users to viewing their own organization’s records only.

ORACLE ADVANCED SECURITY IMPROVEMENTS

Oracle Advanced Security has improved configuration and management tools to simplify security management. Oracle Advanced Security also provides new forms of network encryption, to ensure the security of all protocols accessing the Oracle8*i* database, and enhanced single sign-on.

NETWORK SECURITY ENHANCEMENTS

Release 8.1.6 enhances Oracle's support for the SSL (Secure Sockets Layer) standard. SSL encryption for Internet Intra-ORB Protocol (IIOP) communications is now available, enabling secure Enterprise Java Beans (EJBs). Also, a Java version of the Oracle Advanced Security encryption libraries is now available to secure thin JDBC connections. The Java implementation of Oracle Advanced Security provides DES encryption, with anonymous Diffie-Hellman key exchange, in 100% Java.

Oracle Advanced Security thus secures *all* protocols into the Oracle8*i* database, whether IIOP, thick or thin JDBC, or Net8.

Oracle Advanced Security has also completed the operational testing phase of FIPS-140 level 2 (Federal Information Processing Standard) certification, a United States government standard that relates to the security of cryptographic products. Completion of the FIPS-140 certification, which is expected in Q4 1999, is required by many organizations, among them the United States government and many financial institutions.

SINGLE SIGN-ON

Oracle Advanced Security already supports many forms of single sign-on for database users, among them Kerberos, SESAME, and DCE. Release 8.1.6 adds support for SSL-based single sign-on.

PKI Credential Management

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 PKCS#10 certificate signing request which can be fulfilled by a Certificate Authority (CA). After the CA issues an X.509 certificate, the user can load the certificate into his wallet. 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 Cybertrust. Wallets are protected using password-based, strong encryption.

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-to-use login tool that hides the complexity of a private key and certificate from users. Once users have securely opened their wallets, they can then connect to multiple databases over SSL, without providing additional passwords. This provides the benefit of strong authentication as well as single sign-on.

SSL for single sign-on 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 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.

USER/SCHEMA SEPARATION

In general, users do not need their own accounts – or their own schemas – in a database, they merely need to access an *application* schema. For example, 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 Payroll objects.

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" the user at 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, e.g. 'sales_application' which all three users can access, instead of creating an account for each user on the Sales database.

Now, you can truly create an enterprise user once, in the directory, who nonetheless can access multiple databases using only the privileges she needs to perform her job, thus lowering the cost of managing users in an enterprise. Another benefit of schema-independent users is that you can manage many more users than could otherwise be done with users tied to individual database accounts. Schema-independent users thus enables scalability of user management for the Internet.

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 enterprise user management.

ENTRUST INTEGRATION

Entrust Technologies, Inc. is a market-leading provider of Public Key Infrastructure (PKI) solutions, through their Entrust/PKI software. Entrust/PKI includes many products, such as Entrust Profile, which secures users' PKI credentials, and Entrust Authority, Entrust's certificate authority product.

Oracle is making specific product modifications to Oracle Advanced Security to enable customers of both Oracle and Entrust to incorporate Entrust-based single sign-on into their Oracle applications. By integrating with Entrust/PKI, Oracle enhances its ability to provide X.509-based single sign-on to large customers who require the extensive key management, certificate revocation, and other features which Entrust provides.

Oracle will implement support for Entrust/PKI in Oracle Advanced Security release 8.1.6, enabling customers to use Entrust Profile, Entrust's "wallet" mechanism, for storage of certificate and private keys, and for secure credential management. Instead of accessing user credentials (private key and certificate) from an Oracle wallet, Oracle Advanced Security accesses a user's Entrust Profile for authentication and single sign-on.

Entrust integration will require both release 8.1.6 of Oracle Advanced Security and Entrust Authority 5. Production use of this feature will be available shortly after general availability of Oracle Advanced Security release 8.1.6.

RELEASE 8.1.6 NEW FEATURES

ORACLE8*i* IMPROVEMENTS

- Encrypt/decrypt package in PL/SQL
- New application context primitives for access control

ORACLE ADVANCED SECURITY IMPROVEMENTS

Network Security

- Single sign-on over SSL
- SSL for IIOP
- 100% Java encryption for “thin” JDBC
- FIPS-140 level 2 certification (in-process)

User Management

- Enterprise user management
- Schema-independent users
- Oracle Enterprise Security Manager

Single Sign-On

- Single sign-on over SSL
- Oracle Enterprise Login Assistant
- Oracle Wallet Manager for credential management
- Entrust/PKI integration

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/