An Oracle White Paper
August 2010

Setting Up Security for an Integration Project—What to Consider:

An Oracle Data Integrator Technical Brief

Setting Up Security for an Integration Project—What to Consider: An Oracle Data Integrator Technical Brief

INTRODUCTION

The first steps in securing an integration project are setting up access to Oracle Data Integrator objects and defining user profiles and access privileges for those users.

As you plan the security for an integration project, you need to consider two distinct types of data:

- Development data—Controlling access to development objects
- Production data—Controlling access in the operational source and the target systems

Oracle Data Integrator can provide the security your integration project requires, even in the most highly sensitive environments. This technical brief describes the security considerations for development data and production data, and how Oracle Data Integrator can address security needs for both types of data.

SECURING DEVELOPMENT DATA

Setting Up Access to Oracle Data Integrator Objects

Before developers and other team members can create or modify Oracle Data Integrator development objects, you must do three things:

- **Install Oracle Data Integrator.**
- **Set up login and password information for the database on which the Oracle Data Integrator repository is located.** Follow the database's requirements for this information (for example, minimum password length, password complexity, and password expiration schedule).
- **Set up login and password information for Oracle Data Integrator.** This information can be the same as for the database. It can be provided to developers in encrypted format, so that it can be used only from within the Oracle Data Integrator environment.

Defining Users, Profiles, and Privileges

To determine who can perform operations on Oracle Data Integrator development objects and which operations users can perform, define user profiles and access privileges. User profiles and access privileges are defined using Oracle Data Integrator Security Manager.

Access privileges can be assigned as Generic or Nongeneric.

- **Generic** privileges apply to all objects of a particular class. For example, a user might be given access to all datastores or all packages.
- **Nongeneric** privileges control access based on specific instances of objects. For example, a user might be allowed to edit the Daily Load project, to view (but not edit) the Monthly Summaries project, and to neither view nor edit the Financial Data project.

External authentication of users

ODI user passwords can be stored in external identity stores as well. When used with middleware components like Oracle Enterprise Manager, this allows single sign on. The identity store location is configured as JPS standard. After setting up the external identity store, ODI repository has to be switched to authenticate externally. This way all ODI users will be mapped to users in external identity store and authentication requests will be passed to external authentication server.

For more information please refer to ODI 11g security documentation.

SECURING PRODUCTION DATA

Planning the security for an integration project involves two distinct areas of a project: development data and production data.

Storing Centralized Login Information

The login and password information needed to access development, test, and production data is stored in the Oracle Data Integrator repository and accessed from Oracle Data Integrator Topology Manager. Because the repository centralizes this information for all data servers, the topology administrator (who might also be the database administrator) sets up login and password information only once.

Passwords are stored in encrypted format; they are never stored as plain text. Other developers can access data by using the login and password information, but they cannot actually see the password. Passwords are never revealed, including through the Oracle Data Integrator application windows and logs.

Centralizing login information ensures that developers work with only the databases they are authorized to access. And they can access all appropriate systems without having to remember their login information or expose that information in an unsafe or insecure way.

Developing Securely with Contexts

Certain data servers can be protected with passwords, based on Contexts. Contexts provide the abstraction to allow developers to work in a logical environment and then execute their work in the physical environments to which they have access privileges. This capability allows, for example, a developer to have access to development data but not to the test or production environment.

Password Storage in credential store

Alternatively the password information for data servers and contexts can be stored in external storage in middle tier credential store so that developers don't have access to it at all. ODI master repository has to be setup as using external storage for password and MBean server information has to be supplied. MBean server is used to connect to external credential store.

For more information please refer to ODI 11g security documentation.

Retrieving Login Information from a Directory

For organizations that store login information in a directory such as a Lightweight Directory Access Protocol (LDAP) server, Oracle Data Integrator can retrieve connection information from that server. In this case, the repository does not store the database's login information (including login information in encrypted format).

Establishing Secure Data Transmission

When data is being transferred between source and target systems, security for the data is provided by the communication method, not by Oracle Data Integrator. However, Oracle Data Integrator products fully support secure communication methods. (For example, data can be accessed using Secure Sockets Layer [SSL], Secure Shell [SSH], or Secure-FTP.) Oracle Data Integrator takes advantage of any security features in the available Java Database Connectivity (JDBC) drivers that are used.

At many sites, the entire system—from source to target—is behind the corporate firewall, making security of the connection less important. At other sites, the data might move between global locations across an internet connection, making it more important to use a secure communication method.

Data that is moved across the internet requires a more secure communication method than data that is moved behind the corporate firewall.

Security Benefits of ELT Architecture

Finally, Oracle Data Integrator's extract, load, and transform (ELT) architecture provides several security benefits within an Oracle Data Integrator production environment. In the ELT architecture, data moves only from source to target without involving any intermediate server, as in traditional extract, transform, and load (ETL) architectures. Thus, the

ELT architecture limits the number of potential points where security breaches may occur.

In addition, because the ELT architecture enables the target database engine to perform the data transformations, data does not have to be moved from the target to handle future transformations. This not only frees up bandwidth and increases performance, but also allows the data to remain in its secure target environment. New data can be added to the target server quickly, easily, and securely.

CONCLUSION

Oracle Data Integrator can be used to securely extract and transform data even in highly sensitive environments. It has been used successfully with banking, insurance, and healthcare customers, and with other customers who require tight security. Because Oracle recognizes the importance of providing security in the development environment and for operational data, Oracle software provides technical features to fully address the needs of both areas.

White Paper Title
August 2010
Author: ODI Product Management
Contributing Authors: ODI Product Management

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
oracle.com

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

SOFTWARE. HARDWARE. COMPLETE.