Oracle Business Intelligence Enterprise Edition LDAP-Security Administration

White Paper by Shivaji Sekaramantri
November 2008

OBIEE LDAP-Security Administration
Introduction and On-line Documentation

BEFORE YOU START

This white paper assumes a working knowledge of the major components of Oracle Business Intelligence Enterprise Edition (Repository, Answers, and Dashboard) and knowledge of the basic Oracle Business Intelligence Enterprise Edition (OBIEE) security concepts. The following resources are available to prepare you to configure OBIEE and Single Sign-On (SSO).

- OBIEE On-line Documentation
  http://www.oracle.com/technology/documentation/bi_ee.html
- Oracle® Business Intelligence Enterprise Edition Deployment Guide - Chapters 8, 10, and 11
- Oracle® Business Intelligence Server Administration Guide - Chapter 15

EXECUTIVE OVERVIEW

This document discusses the issues and resolutions for Lightweight Directory Access Protocol (LDAP) Server Authentication.

After a successful integration of OBIEE with a LDAP server using a SSO process, User authentication is transferred to the LDAP server. The entire User authentication process is then performed against the LDAP Server.

This process introduces a new problem. The problem is it deactivates all OBIEE local User access, which means that the dashboards and reports they developed are no longer accessible to anyone. In addition, the OBIEE Administrator User cannot setup a Security Model for the LDAP Users.

This poses a major data security setup issue across organizations related to access privileges of the OBIEE Presentation services content.

OVERVIEW OF OBIEE SECURITY FEATURES

Security is an important aspect of every BI deployment. It controls the authorization mechanisms of the enterprise. To protect against unauthorized access, the current release of OBIEE supports features such as distributed security, single sign-on, resource access and security, including access rights to granular objects.

Overall, OBIEE Security can be divided into two parts - Authentication and Authorization.

Authentication

Authentication is the process used to verify the identity of a User who tries to access the system. This is implemented by the BI Server using either the Internal Authentication or External Authentication methods.

As a default mechanism, the Internal Authentication checks incoming User credentials against a stored list of Usernames and passwords.

External Authentication integrates external identity management tools such as Oracle Internet Directory (OID) or other third party LDAP servers (e.g., Microsoft AD or Sun LDAP Servers).

Authorization

Authorization is the process used to verify that a User has been granted sufficient privileges to perform the requested action on the specified object. In OBIEE, the Authorization process is carried out in OBIEE-Rpd file and in the Presentation Layer.

OBIEE AND LDAP SECURITY INTEGRATION ISSUES

This section describes the technical issues pertinent to security integration

- *In External Authentication process,* OID Groups and OID Users can not be brought into the OBIEE-Rpd file using a LDAP Server setup process due to technical complexities. It is possible to bring either the OID Groups or the Users but not both. Assigning LDAP Groups to LDAP Users in OBIEE-Rpd file is challenging.
- *Once the SSO enabled* for OBIEE, all OBIEE local accounts such as Administrator and other local OBIEE Users are disabled and all LDAP Users' accounts are activated.
- *All Dashboards/reports are developed in OBIEE* with local OBIEE Administrator or Local Users are disabled and are inaccessible to the

LDAP Users. In other words, the Administrator cannot setup the Security Model.

OBIEE SECURITY INFRASTRUCTURE

Before we resolve the security integration issues, we must discuss the constructs of the OBIEE Security infrastructure as shown in following picture. OBIEE has its own security infrastructure for Group/User management and the control of access to various data sources. It can also be integrated with other third party identity management tools or different LDAP servers.

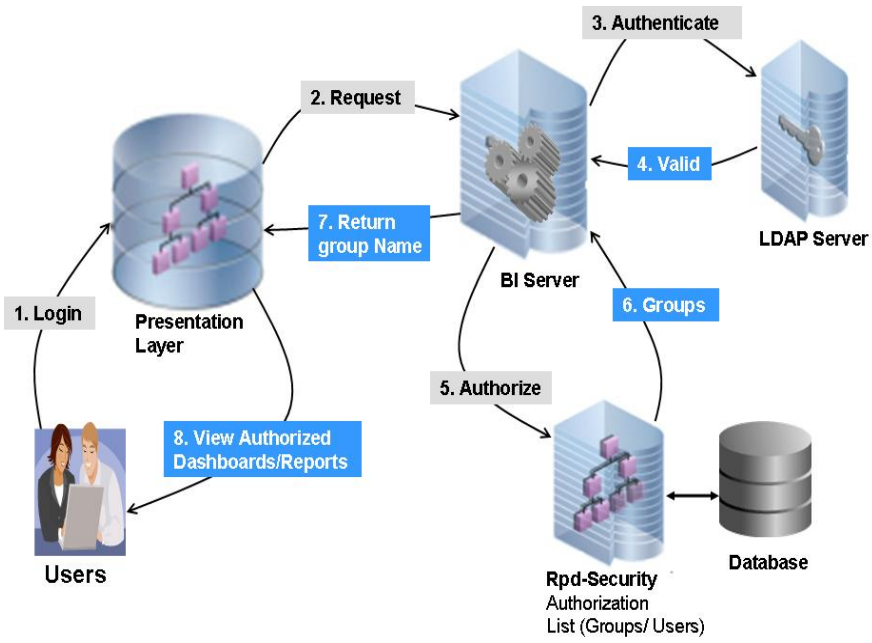


Figure 1 - Basic OBIEE-Login

OBIEE SECURITY REPOSITORIES

OBIEE has two distinct file-based repositories.

- *Oracle BI Server repository*
- *Oracle BI Presentation Services Repository, also known as the Web Catalog*

Oracle BI Server Repository: Oracle BI server has a local repository that contains information about all Groups/Users and all data sources (for example Multidimensional Models, Data Warehouses/Data marts, various databases, XML and etc.)

Web Catalog: Oracle BI Presentation Services has a separate security infrastructure for Groups and Users. It is stored in a repository, known as the Web Catalog.

Oracle Internet Directory & Oracle Single Sign-On

This paper focuses on integrating OBIEE repositories with other Oracle middleware products like OID and Oracle SSO and thus integrating with an enterprise wide Single Sign-On.

Single Sign-On (SSO): is a method of access control that enables a User to log in just once to gain access to the resources of multiple software systems.

Oracle BI provides an open interface that enables web integration with SSO products. Any SSO product that complies with industry standard techniques for passing authentication credentials can achieve SSO integration with Oracle BI.

Implementing SSO has following benefits for any organizations.

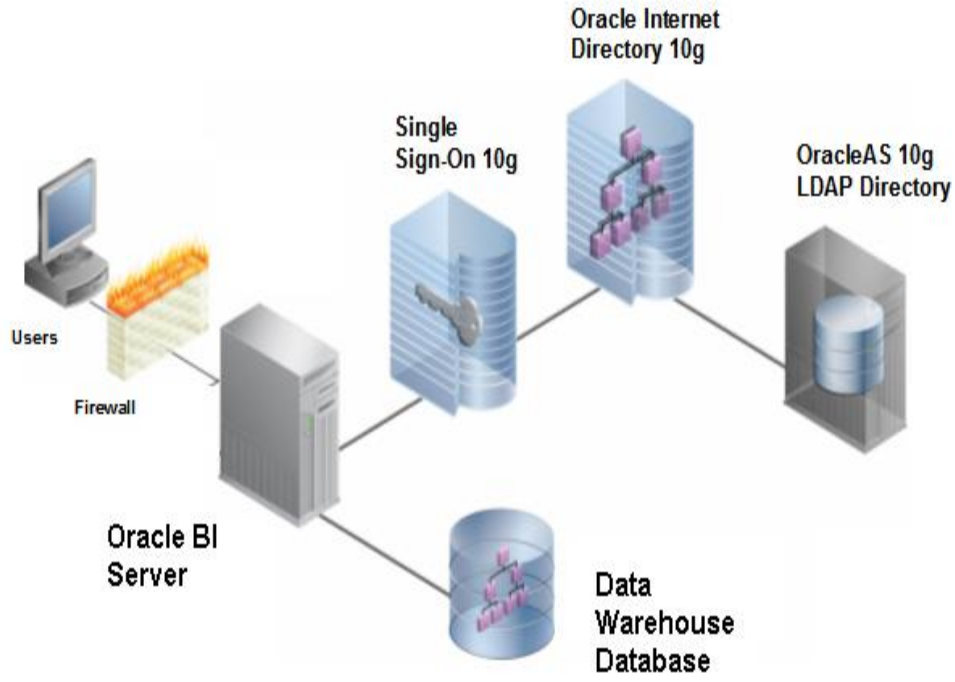
RESOLVING THE SECURITY INTEGRATION ISSUES

To resolve the security Integration issues, create a User who is administrator in the OID-OBIEE Administrator Group, the OBIEE –RPD and in the OBIEE – Presentation Services. The rest of the configuration steps are outlined in subsequent sections below.

The configuration described in this section requires the following list of Oracle Products.

List of Oracle Software needed for Integration.

1. Oracle Internet Directory or Third Party LDAP servers
2. Oracle Application Server (OAS) 10.1.3 or any other Application Server
3. Oracle Business Intelligence Enterprise Edition (OBIEE) 10.1.3.x deployed in advanced mode in the Application Server.



The above components require a pre-configuration setup, which is described in the following section.

SSO PRE-CONFIGURATION SETUP

Following steps must be completed before we start the SSO integration process.

1. Database setup

Create a small function in database to dynamically link User to a Group in OID and used in OBIEE-Rpd file to access User /Group relationship.
This function is used in OBIEE Session variables and is called when User logins into the system, the User ID is passed to the function and function returns the OID Group Names associated with that User.

This resolves the User to Group assignment problem in the OBIEE-rpd file.

2. Configuration Table

To resolve the second and third problems in the problem statement please follow individual sections defined in the table below. The following table describes the individual steps required in the Oracle Internet directory (OID), OBIEE – Administration, and OBIEE Presentation Server/Web Catalog level. (Each column address that component.)

OID Groups/Users	OBIEE – Rpd file	OBIEE – Presentation Layer or Web Catalog	SSO Configuration
Groups	Configure Rpd file to use the LDAP Server	Create same OID Groups in Presentation layer	Setup Oracle Single Sign-On
Users	Create OID Groups		
Assignment Users to Groups	Create special Impersonator User		
	Create Session Variables		

The following sections cover each of the configuration settings in detail.

2.1.1 OID Groups/Users -Configuration

OID is the place where the centralized security defined for all enterprise wide applications. In OID, all the Groups and Users are created and the assignment of Users to Groups is maintained. These Users are setup to access Portal, OBIEE and other Oracle applications.

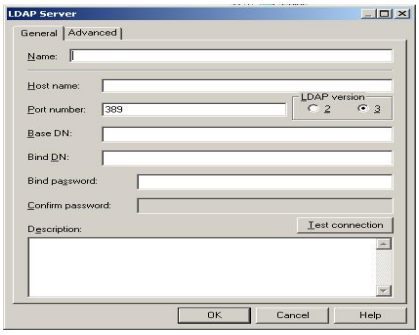
The Groups/Users are not created in any particular application and all applications will need to access Users defined in OID when Oracle SSO is enabled.

2.1.2 OBIEE- RPD file Setup

This is where the LDAP Server configuration, Groups, and Session Variables are defined to configure the OBIEE-RPD file for using SSO.

2.1.2.1 Configure Rpd file to use the LDAP Server

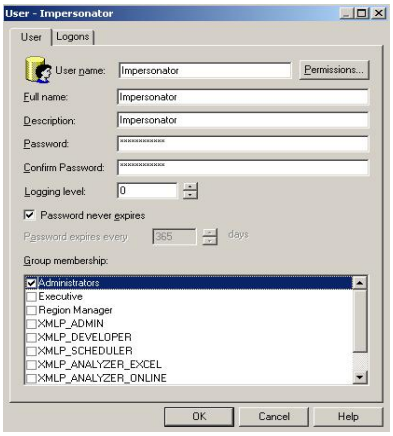
First step is to configure the LDAP Server information by defining its Name, Port #, Base/ Bind DNs and Passwords and ping the LDAP Server to test for a successful setup.



2.1.2.2 Create OID Groups/Users

Create all OID Groups in the OBIEE –RPD file. First, create a special User called Impersonator within the Oracle BI Administration Tool. Oracle BI Presentation Services uses the Oracle BI Impersonation feature to establish a connection to the Oracle BI Server on behalf of the authenticated end User. For this purpose, a special User that Oracle BI Presentation Services will utilize for impersonating the authenticated end User must be created. This section of the document refers to this special User as the impersonator User.

Make sure to follow the length of the password defined in NQSConfig.ini XML file and also in production situations, choose a different password



Note: There is no need to create any other Users since all Users will be passed from OID (LDAP) Server.

2.1.2.3 Initialization Blocks and Session Variables in RPD

Initialization blocks are used to initialize session variables. An Initialization block contains the SQL that will be executed to initialize or refresh the variables associated with that block.

The Session Variables run at beginning of every User session. Session Variables obtain their values from Initialization blocks. The Authentication against external sources like OID is done through Session Variables.

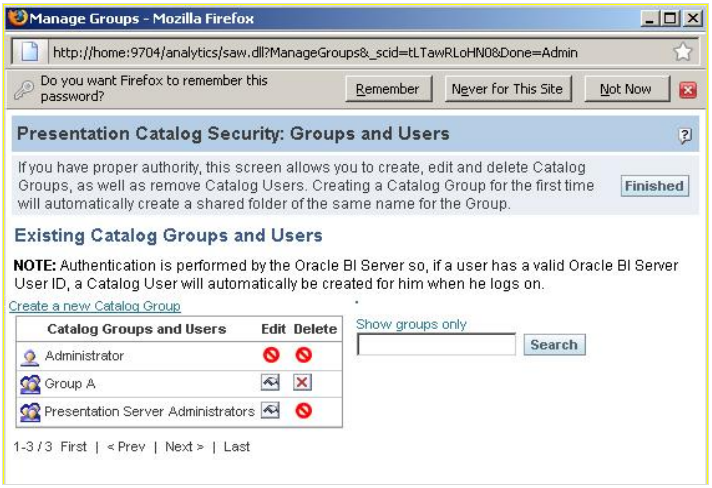
Create following two session variable Initialization blocks for OID (or LDAP) authentication.

1. One Session variable Initialization block for pinging LDAP Server.

2. The second Session variable Initialization block executes a database function when the User logs in and returns the User's associated Group Names. In other words the function call will dynamically assign the User to the Group Names. This resolves the first issue defined in the problem statement.

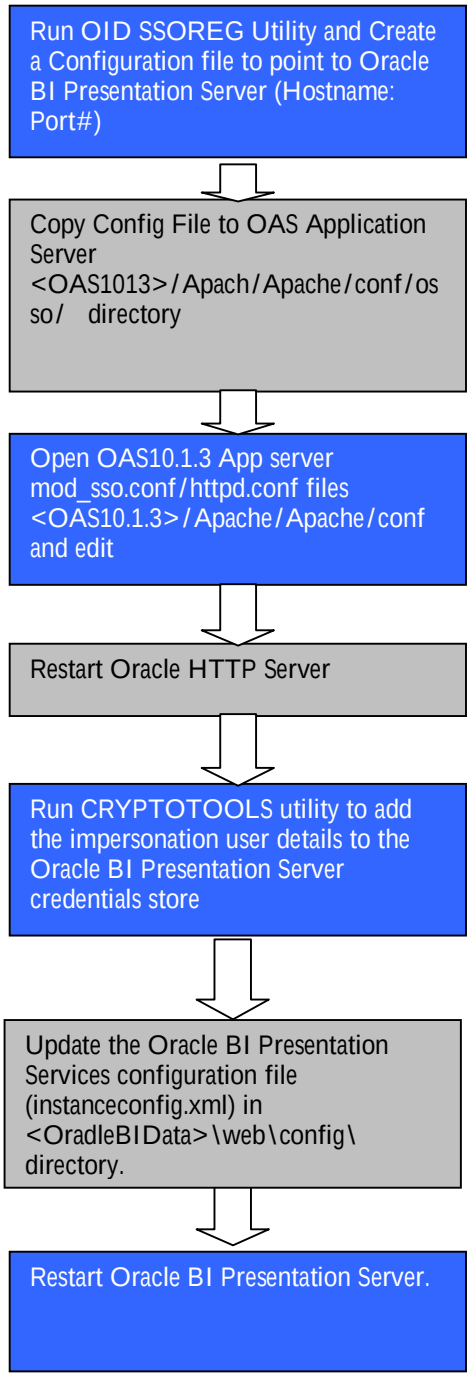
2.1.3 Create Groups in OBIEE- Presentation Layer

Define the same Groups that are in OID in Presentation Server Groups and the Presentation Server layer.



2.1.4 OBIEE -SSO Configuration Settings

The following high level integration steps describe how to configure OBIEE as an OAS Single Sign-On application. Detail steps are thoroughly documented in Chapter 11 in Oracle Business Intelligence Enterprise Edition Deployment Guide for real-time implementation.



Note: Make backup copies of all files before modifying them.

CONCLUSION

In the final analysis, the Security Model setup is simply assigning Groups/Users to Presentation Layer Content (i.e., Dashboards and Reports).

After completing the above steps, the Administrator Group User can safely complete the setup of the OBIEE Security Model for the organization.

ABOUT SW EXCELLENCE

SW Excellence Inc. is an Information Technology services firm providing enterprise-consulting services located in Northern VA. Our goal is to provide top-quality consulting services in the area of Data warehousing and Business Intelligence space. We are a focused, committed team of technical consultants who are driven by the desire to see our clients succeed.

SW Excellence Inc. also focuses on providing high end enterprise pre-built Products and custom Product development to meet challenges facing our clients in Business Intelligence. Please visit us at http://www.swexcellence.com/product.htm

We offer the following end-to-end Oracle BI & DW solutions for your organization. For more information visit http://www.swexcellence.com

INSTALLATIONS OF ORACLE PRODUCTS (UNIX / LINUX/WINDOWS PLATFORMS)

- Oracle 10G Database and upgraded database.
- Oracle App server 10.1.2 Infrastructure (OID,SSO,Oracle Portals)
- Oracle App Server 10.1.3
- Installation and deployment of OBIEE 10.1.3.x on OAS 10.1.3 App server

DEVELOPMENT

- Development of Data warehouse schemas
- ETL strategy to populate Database
- Create Rpd files using OBIEE administration
- Create powerful dashboards using Dashboards/Answers
- Create iBots to deliver reports via Email or cell Phone

CONFIGURATION

- Deployment of OBIEE on any Application Servers
- Configure Oracle Single sign-On for OBIEE.
- Configure Multiple Presentations servers on UNIX.
- Configure Scheduler on Unix/Windows.
- Configure BI Publisher on Unix/Linux/Windows.
- Integrated OBIEE with Oracle Portals.

MIGRATIONS

- Migrations from One OBIEE Environment to Other

SW Excellence Inc.

Intelligence Behind Business

OBIEE LDAP-Security Administration
White Paper
September 2008
Author: Shivaji Sekaramantri

SW Excellence Inc.
Suite #131
400 Rusurt Drive SE
Leesburg, VA 20175
U.S.A.

Inquiries:
Phone: +1.571.344.3479
Fax: +1.703.953.2255
http://www.swexcellence.com