MarketSphere®

ORACLE Platinum Partner

- **A Deep Dive into OBIEE 11g Security**
  Rittman Mead BI Forum, Atlanta 2012

ORACLE Platinum Partner
Specialized
Oracle Essbase

ORACLE Platinum Partner
Specialized
Oracle Business Intelligence Foundation

ORACLE Platinum Partner
Specialized
Oracle Business Intelligence Applications

ORACLE Platinum Partner
Specialized
Oracle Hyperion Financial Management

ORACLE Platinum Partner
Specialized
Oracle Hyperion Planning

ORACLE Platinum Partner
Specialized
PeopleSoft General Ledger

ORACLE Platinum Partner
Specialized
JD Edwards EnterpriseOne Financial Management

ORACLE Platinum Partner
Specialized
Oracle E-Business Suite Financial Management

About the Speaker

Ramke Ramakrishnan

Practice Director - Business Intelligence & EPM

MarketSphere Consulting

ramke.ramakrishnan@marketsphere.com

www.marketsphere.com

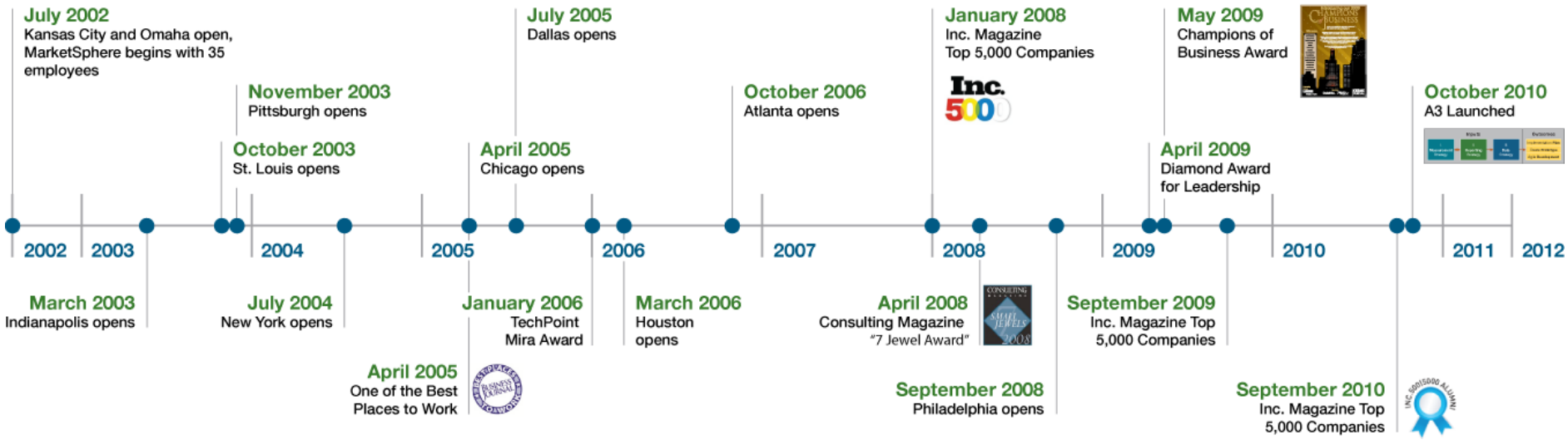
- Performing lead architect and technical leadership roles for over 15 years on Business Intelligence by effectively managing the project team and the business customer expectations.
- Continuously demonstrated hands-on capabilities in the configuration of robust Oracle database and BI architectures, Oracle's Essbase infrastructure and large scale Business Intelligence Reporting, OBI Applications and EPM implementations.
- Key contributor for Business Analytics and Enterprise Reporting by integrating various applications systems into analytics to empower business customers, executives and end-users.
- Oracle Certified in DBA, Essbase, BI Foundation Suite and OBI Applications;
- Active member and designated Deputy CTO (DCTO) on Oracle Business Intelligence Investment Partner Community (IPC)

About MarketSphere

Business Overview

Strategic advisory and technology experts to help you deliver integrated ERP, BI and EPM solutions to optimize business performance.

- Our focus is on solving complex business challenges and strategic opportunities for Fortune 500 and emerging, high-growth companies
- Services delivered out of eleven formal market locations throughout the United States
- In 2011, engaged by more than 260 clients on over 400 projects



About MarketSphere

Creating Business Harmony

MARKETSPHERE BEST PRACTICES

Finance Advisory | Human Capital Advisory | Supply Chain Advisory | Marketing Advisory | Change Assurance

BUSINESS INSIGHT

Interactive Dashboards  | Publishing & Reporting  | Ad-hoc Analysis  | Mobile & Disconnected  | Office Integration  | Search 

Analytic Assessment Approach™ (A3)

ENTERPRISE PERFORMANCE MANAGEMENT (EPM)

Planning & Forecasting	• Hyperion Planning • Workforce Planning • Capital Asset Planning • Exalytics	**Consolidations & Reporting**	• HFM • Disclosure Management • FDQM	**Profitability Analysis**	Hyperion Profitability & Cost Management

BUSINESS INTELLIGENCE (BI)

Reporting & Analytics Strategy	**Data Governance**	Oracle Data Relationship Management	**Configurable Analytics**	• Foundation Analytics by ERP • Exalytics	**Packaged Analytics**	• ERP Analytics • CRM Analytics • Exalytics

Essbase, OBIEE 11g, Scorecards

Oracle Fusion

ENTERPRISE RESOURCE PLANNING (ERP)

ORACLE E-BUSINESS SUITE | ORACLE PEOPLESOFT ENTERPRISE | ORACLE JD EDWARDS | ORACLE FUSION APPLICATIONS

A Deep Dive into OBIEE 11g Security

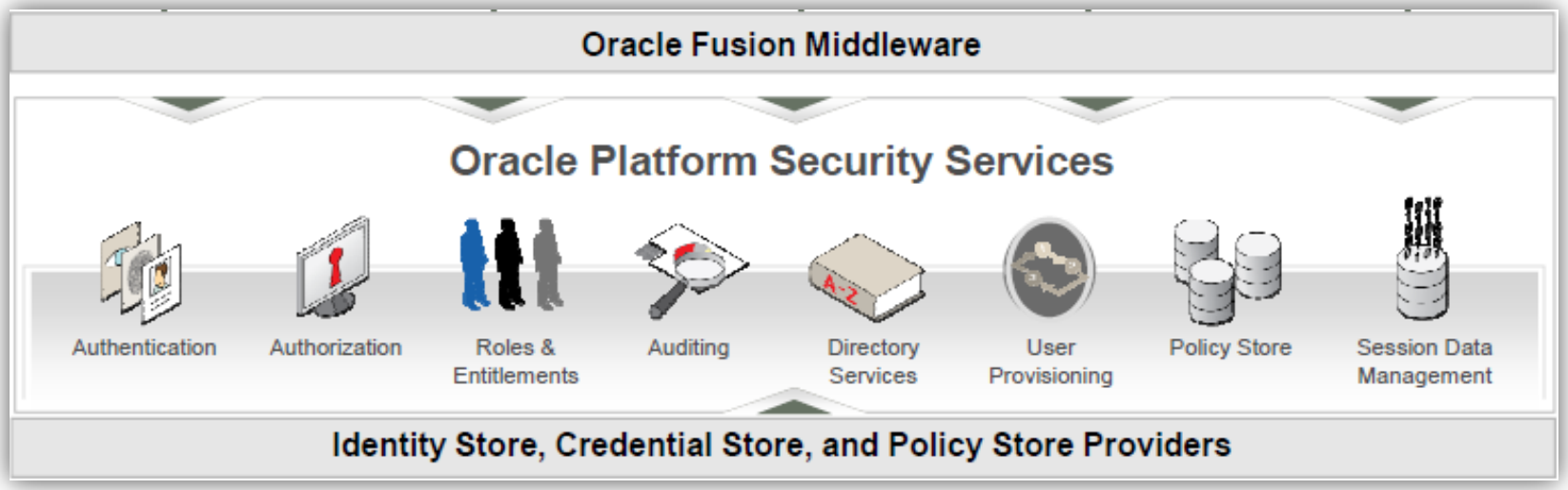
Agenda

1. Introduction
2. OBIEE 11g Security Controls
3. Authentication
4. Authorization
5. Content Security
6. User GUIDs
7. Multiple Authentication Providers
8. Row Level Security
9. Security Store Migration
10. Single Sign-On (SSO)

Introduction

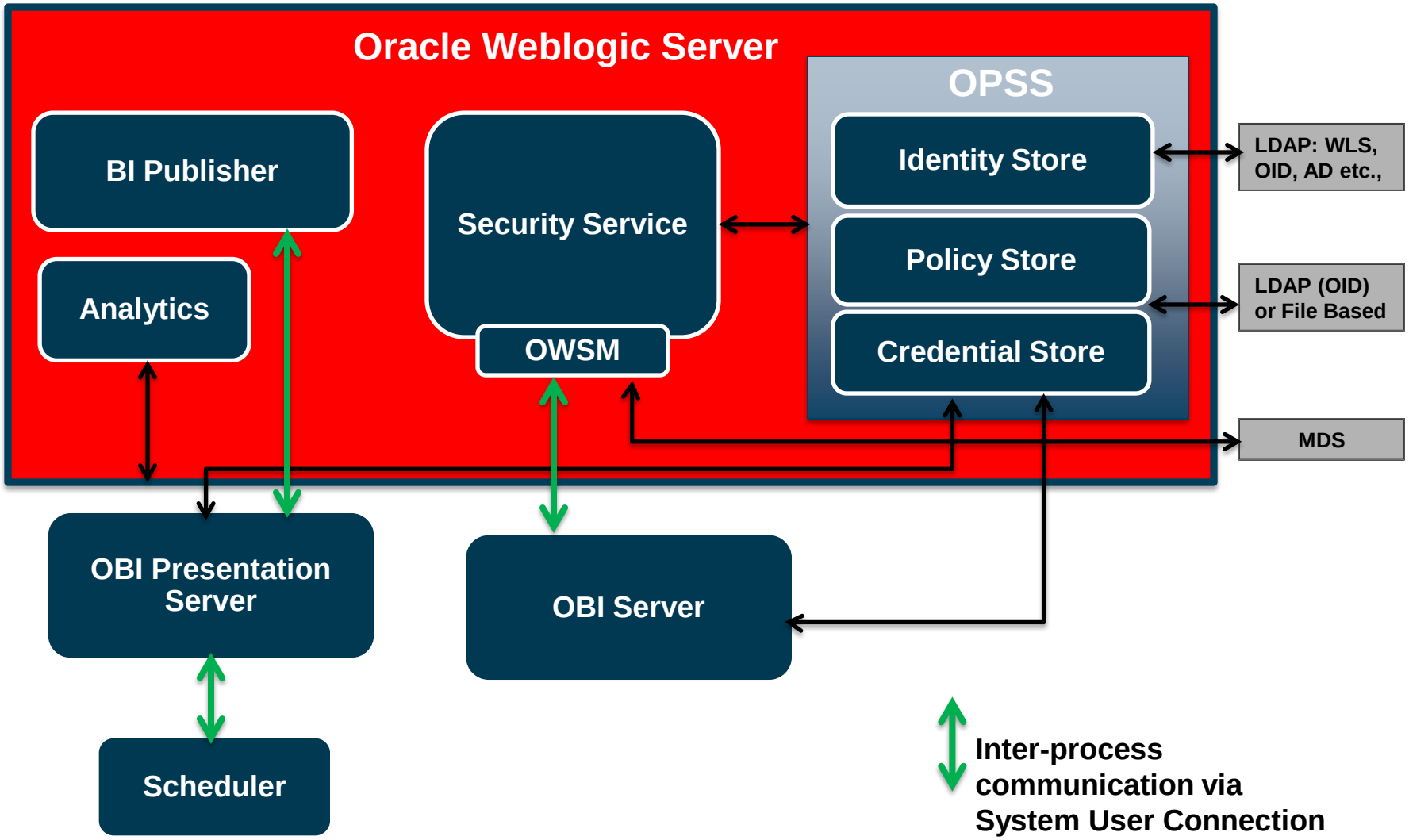
OBIEE Security Overview

- OBIEE 11g provides a scalable default security mechanism to manage users and groups, permission grants and credentials through native and external authentication providers.
- OBIEE 11g implements Fusion Middleware stack leveraging common security architecture. Also introduces a significant change in both the approach and architecture of OBIEE for authentication , provisioning and authorization of users
- OBIEE 11g uses the architectural components of Oracle Fusion Middleware (FMW) called Oracle Platform Security Services (OPSS), the underlying security platform that provides security. The OPSS components listed provides a common security framework across many Oracle applications that runs on FMW including OBIEE 11g and Fusion Applications
- OBIEE 11g delegates security to OPSS which uses features such as Credential Store Framework, Policy Store and identify store through WLS authenticators to provide security to the Oracle BI system.



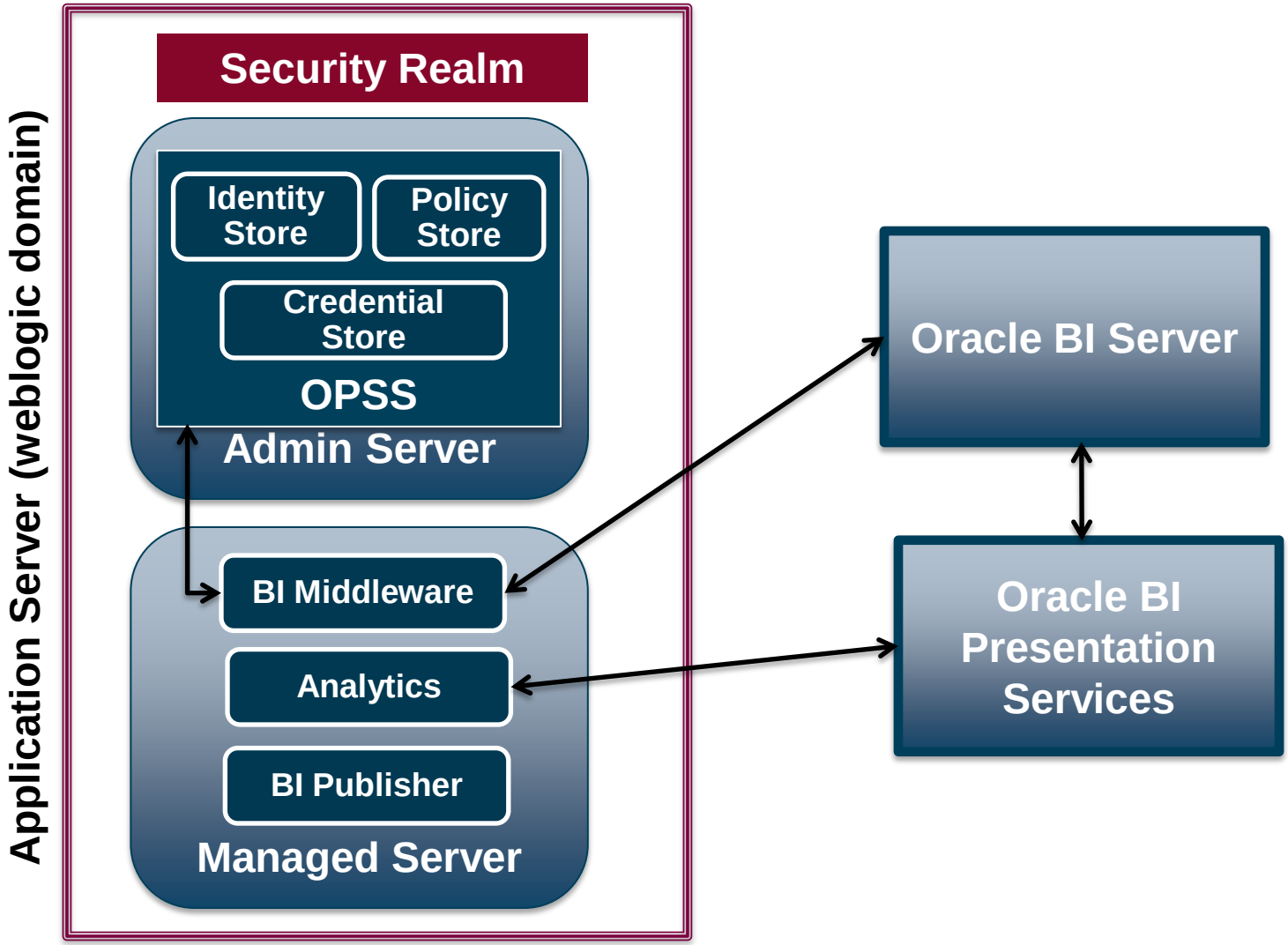
OBIEE Security Architecture

Application Server - Core Components



OBIEE Security Architecture

Fusion Middleware Model

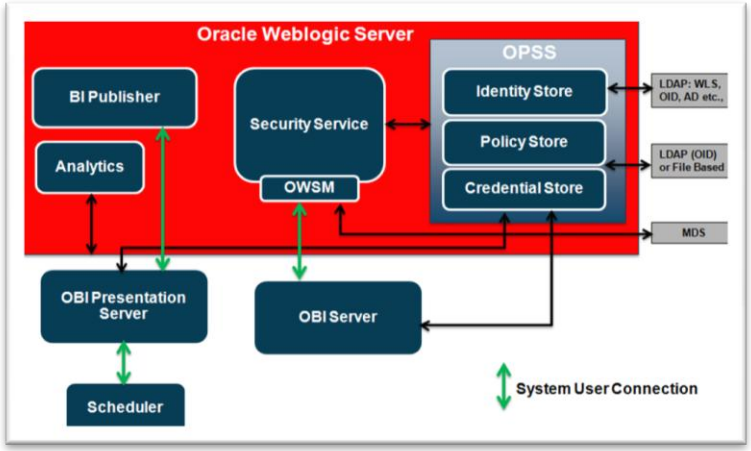


OBIEE Security Controls

OPSS and OWSM components

- OBIEE 11g security is more aligned with the Oracle middleware and fusion applications architecture that includes components of OPSS, OWSM services as part of the security controls.

- **Oracle Platform Security Services (OPSS)** consists of
  - An embedded LDAP **"Identity Store"** to store users and groups which can also be configured to use external stores and/or providers such as MSAD and other authenticators
  - A "**Policy Store**" container that consists of application roles, application policies and the permissions, grants information. By default, it is stored in a file called system-jazn-data.xml but can be redirected to an LDAP or file-based policy store. Oracle Fusion Middleware (FMW) concept of Application roles and policies is utilized for assignment of permissions and privileges



  - A "**Credential Store**" file system container that stores user and system credentials for inter process communication which can be also be configured to use external providers. The credential store holds BISystemUser, OracleSystemUser credentials, RPD, SSL, Web Services credentials and certificates in cwallet.sso file at the weblogic domain level

- **Oracle Web Services Manager (OWSM)** integrated with WLS EM Console provides the management and securing of web services through administration of policies

- Some of the basic concepts of presentation object-level and data-level security remain the same in 11g

System Users

Inter BI Component communication

- The key user accounts that is added to the Credential Store by default as part of the OBIEE 11g installation are **BISystemUser** and **OracleSystemUser**

BISystemUser

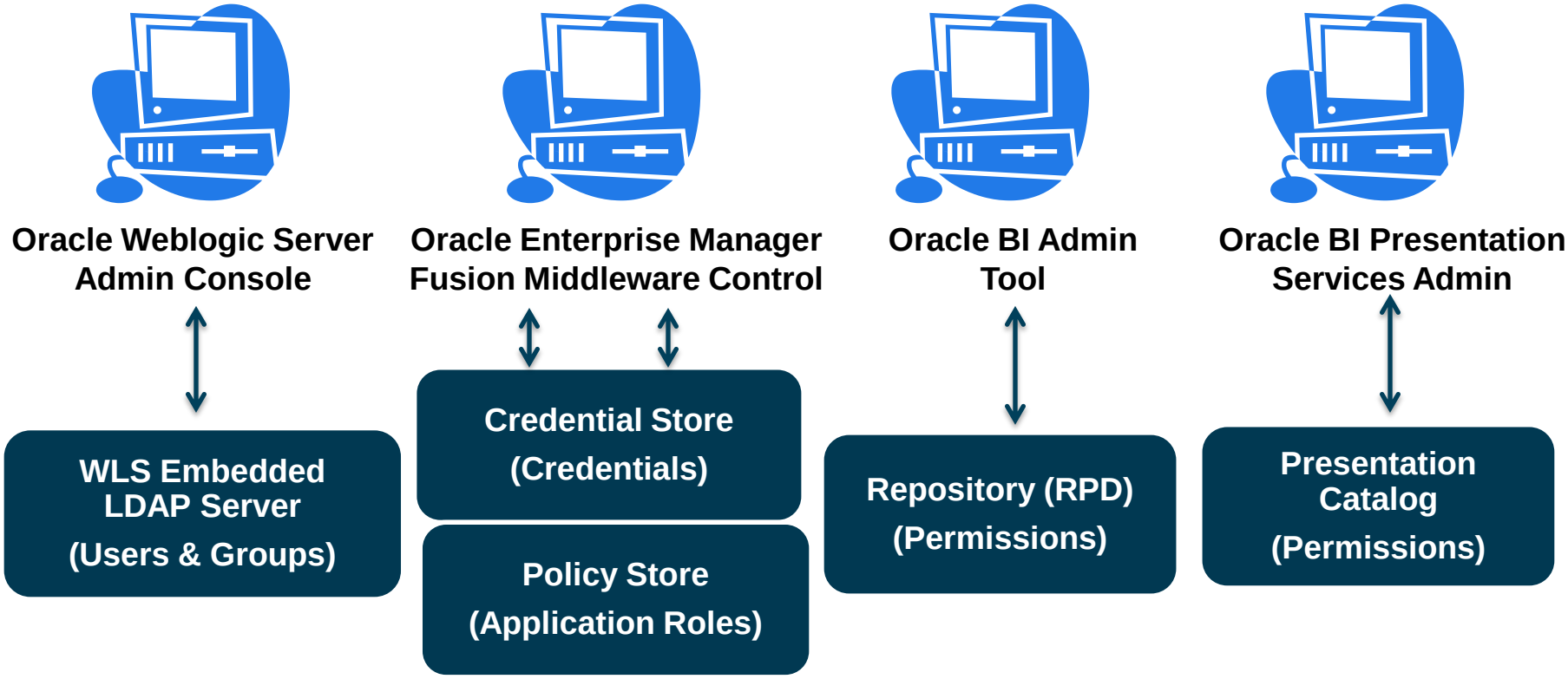
- primarily used for inter-bi-component communication by default referenced via WLS Default Authenticator or through external authenticator
- acts as user for Impersonation
- credentials is stored in the Credential Store under oracle.bi.system – system.user
- by default BISystemUser is a member of an LDAP Group called ‘Administrators’ which is assigned to the Weblogic Global Admin Role. BISystemUser is also automatically assigned to BISystem application role

OracleSystemUser

- Utilized by OWSM
- by default called OracleSystemUser and a member of the OracleSystemGroup. The User name can be changed, but need to follow FMW documentation for detailed steps. Also, by default it is created and referenced via the Default Authenticator and can be changed to external authenticator

OBIEE 11g Security Components

Security Administration

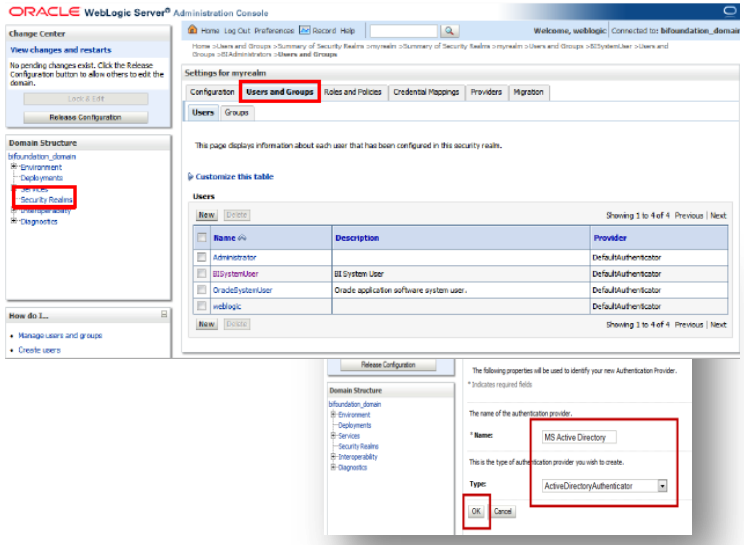


- WebLogic Server Admin Server (LDAP Server, Security Providers)
- Fusion Middleware Control (Application Roles)
- BI Administration tool (subject-area, and row-level security)
- Catalog Manager and Presentation Services Catalog View (object permissions)
- Présentation Services Administration Page (Permissions to End-User Présentation)

Authentication

OBIEE Identify Management

- WebLogic provides the default authentication provider for OBIEE 11g. The default authentication provider accesses user and group information stored in the LDAP server embedded in the Oracle Business Intelligence's Oracle WebLogic Server domain.
- Users are authenticated by the WebLogic server based on the credentials defined in the embedded WebLogic LDAP server.
- WebLogic also supports integration with other identity management products and/or alternate directory (also known as Authentication providers)
- Users, Groups and related attributes can be managed and administered in WebLogic LDAP server or other external authentication providers and retrieved during the authentication process

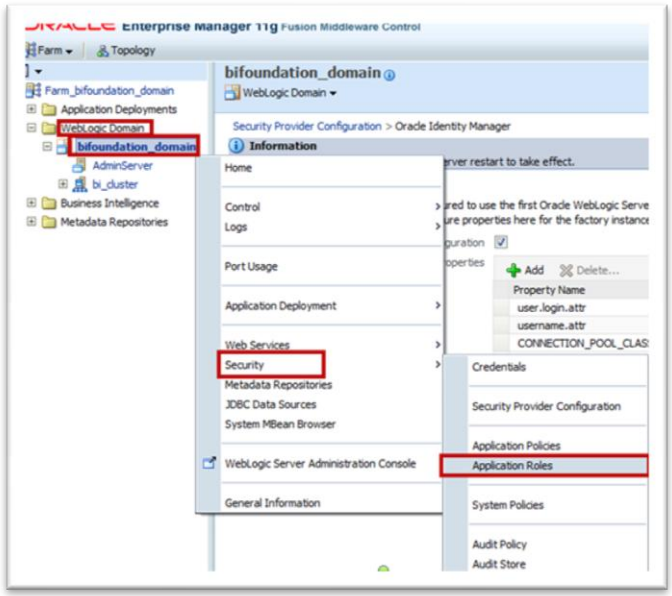


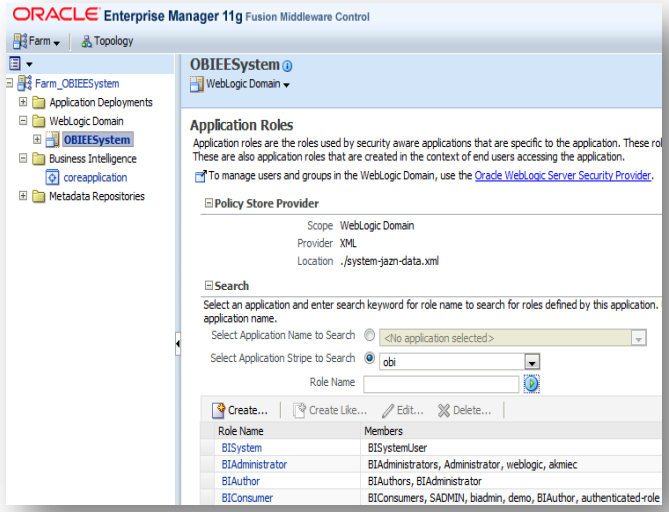
- With direct integration of OPSS to security stores and authentication providers, the details of users and their application roles will automatically inherited and shown in the Identity Manager within the OBIEE Administration tool though not editable. Hence, BI server does not require the use of initialization block in the repository for authentication (not recommended for 11g) as it is now embedded in the WebLogic Server.
- Unlike 10g, the entire RPD is encrypted in 11g and will require repository password to access RPD through the OBIEE Administration Client tool.

Authorization

Privileges and Permissions Management

- Application Roles and Policies are the key components for defining authorization for OBIEE 11g and it comes with pre-defined set of groups, application roles and application policies.
- WLS provides a default policy store provider, which is accessed through Fusion Middleware Control allows to create and maintain application roles, assign policies to the roles and then map external LDAP authenticator groups to these roles
- Application roles allows the artifacts of a business intelligence system to be easily moved between environments as no change to the security policy is needed and all that is required is to assign the Application roles to the users and groups available in the target environment
- An application role typically specific to a given application can be mapped to other application roles defined in the same application scope as well as to the enterprise users or groups, and they are used in authorization decisions.

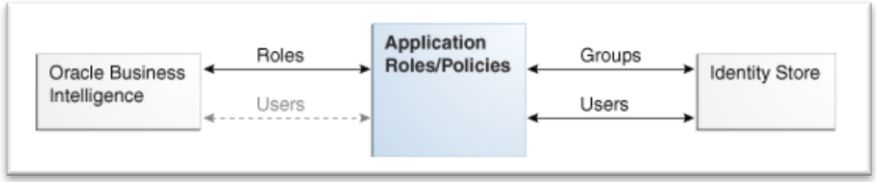


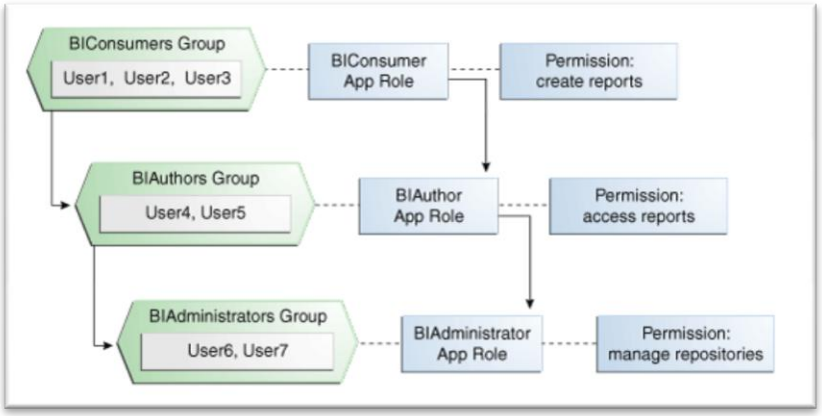


Authorization

Privileges and Permissions Management

- Within the context of OBIEE, the “Application roles” replaces “Groups” in OBIEE10g. In OBIEE 10g, any changes to corporate LDAP groups require a corresponding change to Groups and their permission assignment. In OBIEE 11g, Application roles provide a logical mapping between permission definitions and corporate LDAP Groups. Permissions are defined at Application Role level and changes to LDAP groups just require a reassignment of the Group to the Application Roles. The same applies for web catalog objects as well.
- The default Application Roles available as default are BIAdministrator, BISystem, BIConsumer and BIAuthor.
- WLS admin user (usually weblogic) specified during installation assigned to a group called “BIAdministrators” which has the BIAdministrator application role granted to it. There are also groups called BIAuthors and BIConsumers which have the BIAuthor and BIConsumer application roles granted, and provides the ability to add new users, groups and application roles



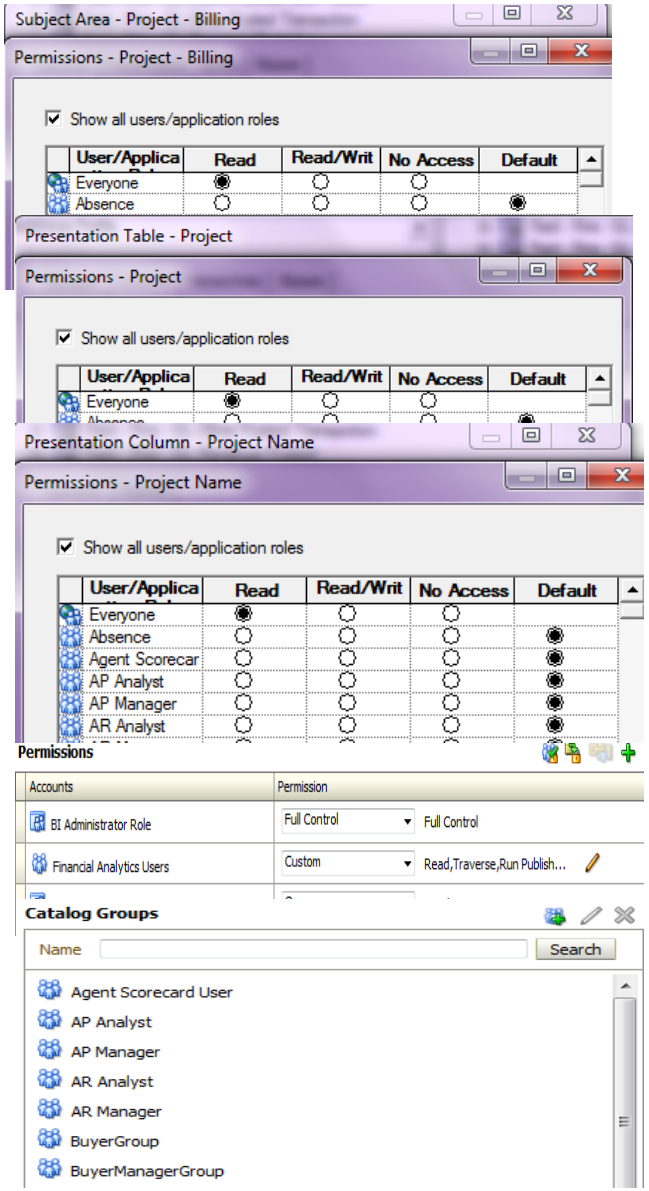


- Application policies are the authorization policies that an application relies for controlling access to its resources. An Application Role is defined and governed by the Application Policy

Content Security

Administering Object Level Permissions

- Restriction of the content and presentation is typically managed within the combination of RPD, Presentation Administration interface and catalog manager
- To restrict to have access to certain presentation catalog objects such as subject area, presentation folders and columns in the repository, you modify the permissions to the application roles assigned to the user at the OBIEE repository
- In case of situations where you want to override the permission only at the creation of the analysis/report i.e., you want to restrict the users to use specific presentation objects in their own analysis but can view the data from a shared analysis/report, you have to administer the privileges at the catalog and/or presentation services. Access to certain features and functions of the OBIEE presentation is also managed and administered at the presentation services level
- Permissions to the catalog objects such as dashboards and other presentation objects and folder permissions are managed via the catalog manager to individual users, application roles as well as catalog groups (to support backward compatibility for 10g)



User GUIDs

Synchronization and Refresh

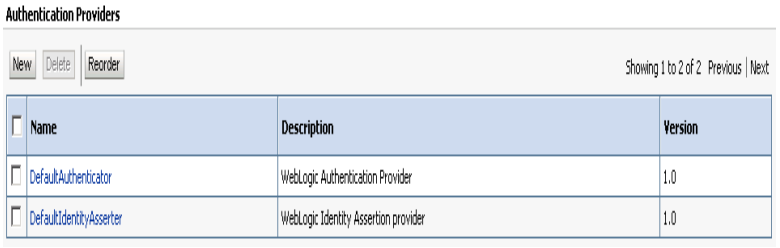
- In OBIEE 11g, Users are uniquely identified by Global Unique Identifiers (GUIDs), an identifier that is completely unique to a given user
- GUIDs provides greater level of security to ensure that both the metadata and data is securely provisioned for a specific user that is added to the BI System
- GUIDs are likely to change and goes “out of sync” and prohibits login to the Presentation as the user gets added and/or removed or during migration between environments or migration of security store from weblogic LDAP to external authenticators
- The synchronization of GUIDs can be fixed using “Refresh / Regenerating GUIDs” and the key steps includes:
  - Change the parameter FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = YES in the NQSConfig.INI
  - Add the below tag to the Catalog section in the instance config.xml

    <ps:Catalog xmlns:ps="oracle.bi.presentation.services/config/v1.1">
    <ps:UpgradeAndExit>false</ps:UpgradeAndExit>
    <ps:UpdateAccountGUIDs>UpdateAndExit</ps:UpdateAccountGUIDs>
    </ps:Catalog>
  - Restart the BI System components using opmnctl with stopall and startall parameters
  - Reset the parameter FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = NO in the NQSConfig.INI
  - Delete or Comment out the entry **<ps:UpdateAccountGUIDs>UpdateAndExit</ps:UpdateAccountGUIDs>** in the instance config.xml
  - Restart the BI System as above

Multiple Authentication Providers

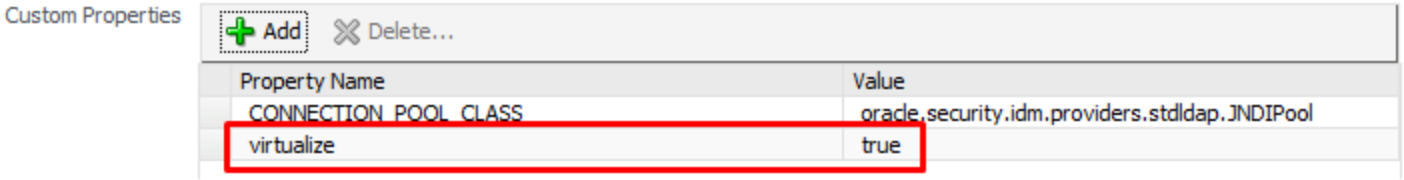
Virtualize Identity

- OBIEE supports adding multiple identify providers for authentication within the Weblogic Admin Console
- The default embedded weblogic providers are “DefaultAuthenticator” and “DefaultIdentifyAsserter”



- Providers support for
  - Users and Groups in LDAP
  - Users and Groups in Database
  - **Users in LDAP and Groups in Database using new provider “BISQLGroupProvider”**

- When multiple Identity Providers are used, set the “virtualize = true” custom property within FMW Control

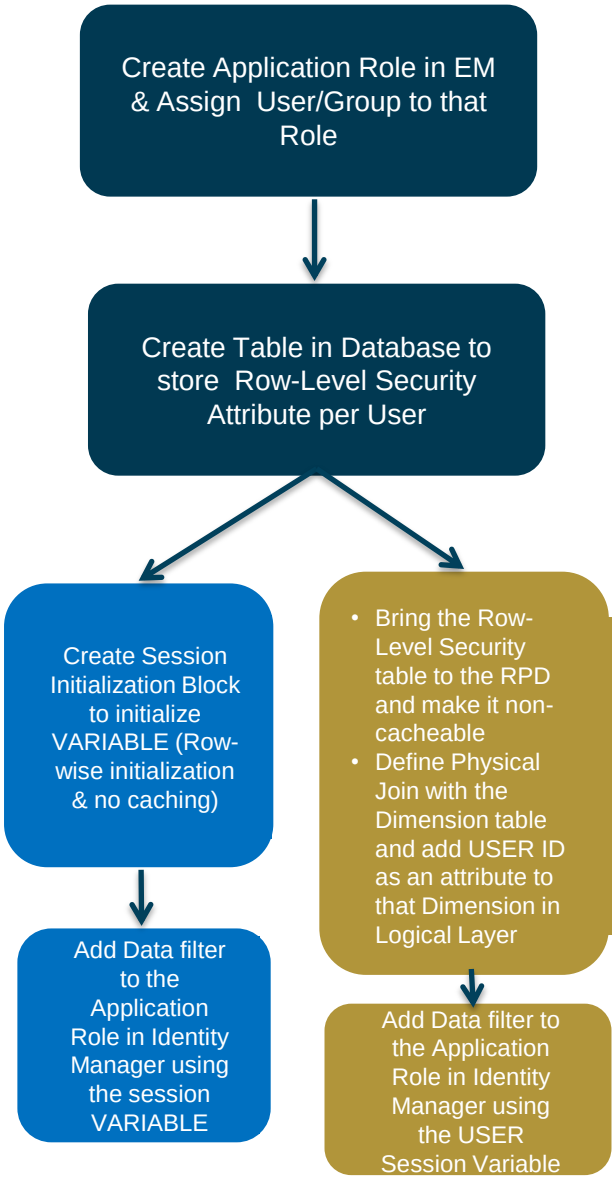


- Always keep the “BISystemUser” in the local weblogic LDAP store and not to the external LDAP provider as suggested in the documentation. Having the BISystemUser locally will help us to manage and adminster the Oracle BI even when the external LDAP is unavailable

Row-Level Security

Securing Data Access

- Row-Level security in OBIEE provides the ability to restrict and/or filter data so that different sets of data is presented to the end users for the same set of dashboards and reports
- The context of Row-Level security typically applied automatically at the BI Server and/or at the database level based on the user credentials and not in the Analysis/Report by itself
- Restriction of data at the database level based on the users are typically handled by leveraging the database features. In case of Oracle, Virtual Private Database can be used and for Essbase, security filter can be applied in EAS and provisioning in shared services. For other databases, native security features can be leveraged.
- For row-level security, the security filter is defined at the application role in the Admin client Identity Manager
- In case of multiple values to be used in the filter, the row-wise initialization variable can be used to store multiple values
- Except for the 11g terminology and mapping of application roles, the row-level security is similar to how it works in 10g

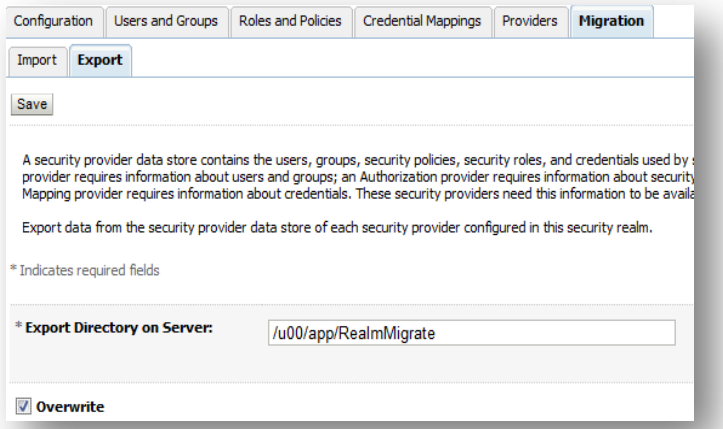


Security Migration

Identify Store Migration

- With the revamped security architecture , the security migration in OBIEE 11g will require lot more attention and considerations
- For scope of security migration include the migration of Identify Store, Policy Store, Credential Store even though not all of them will require migration and may remain static/constant values across the environments
- Migration of OBIEE security store supports both full and incremental migration. However, some of the security store such as policy store may not support a complete export/full migration
- Identity Store can be migrated from the WLS admin console through the export/import interface in Security Realm . After the export the following files are created for migration.

  DefaultAuthenticator.dat
  DefaultCredentialMapper.dat
  exportIndex.dat
  XACMLAuthorizer.dat
  XACMLRoleMapper.dat

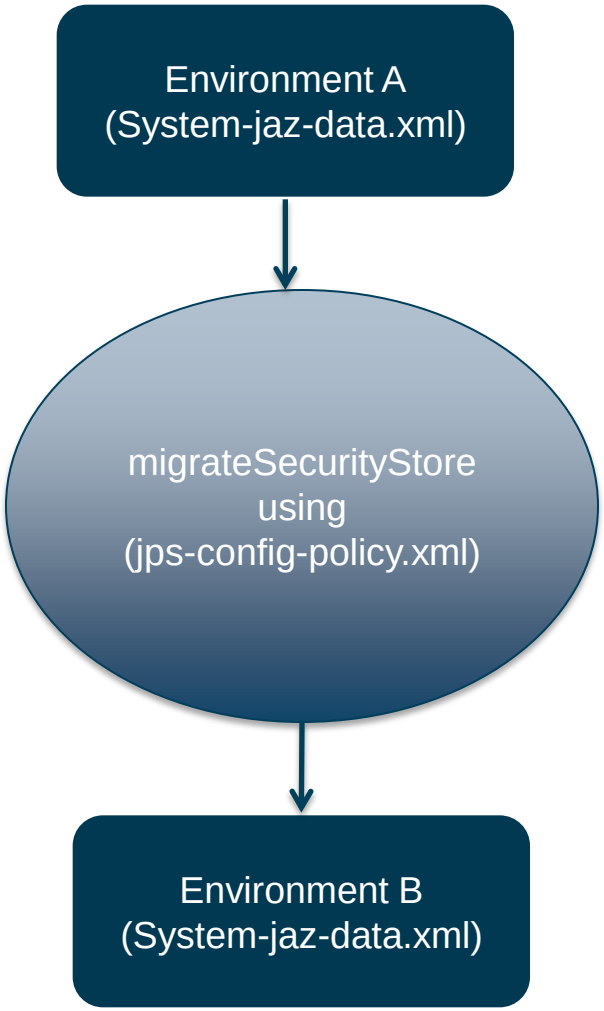


Note: The roles migrated through this process are the policies specific to the Admin Server and not the application roles and policies

Security Migration

Policy Store Migration

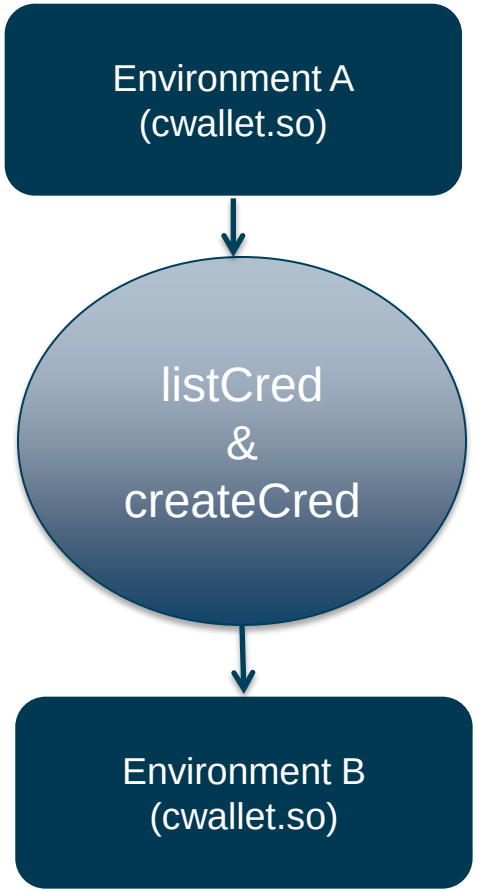
- Migrating Policy Stores/Application Roles will require WLST
  - Policy Store is nothing but a physical file that contains the Application Role, Applications Policies and their corresponding mapping to the authenticatorUsers and Groups.
  - It's stored in system-jazn-data.xml under <OBIEEHOME>/middleware/user_projects/domains/bifoundation_domain/config/fmwconfig
  - During migration, you copy the file to a temporary location in the target environment and run the MigrateSecurityStore WLST scripting method.
  - For incremental migration, createAppRole, grantAppRole commands can be applied to propagate the incremental changes from one environment to the other



Security Migration

Credential Store Migration

- Migrating Credential Store can also be accomplished using WLST
  - Credential Store contains system credentials in an encrypted format inside a security file called cwallet.so
  - Prior to migration, we need to extract the full system credentials from the Credential Store using listCred method and recreate using createCred method.
  - Alternatively, we can do a full migration of the credential store using MigrateSecurityStore, it is generally not recommended unless you want to retain the same credentials for the oracle.bi.enterprise and oracle.bi.system entries

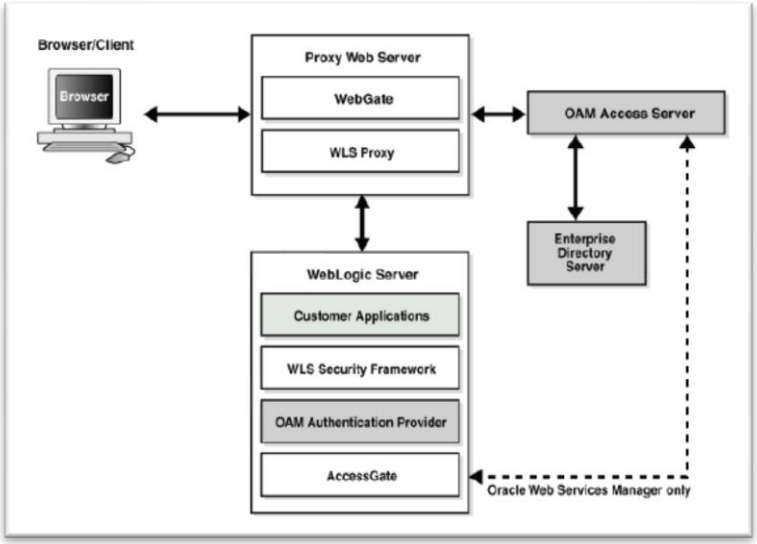


- In addition to the manual approach of export/import of the security store content, weblogic also provides Weblogic Scripting Tool (WLST) interface for invoking through command line and automation. As an alternate, Java API interface using JMX bean scripting can also be utilized

Single Sign-On (SSO)

Overview

- Integrating a single sign-on (SSO) solution enables a user to log on (sign-on) and authenticated once and have seem less access to across all application including OBIEE.



SSO Configuration for OBIEE include the following:

- Configure Oracle Access Manager or Custom Solution (SiteMinder or Native Windows) as the SSO authentication provider
- Configure the Web proxy to forward requests from the Oracle BI Presentation Server to the SSO provider
- Configure a new authenticator for Oracle WebLogic Server
- The Oracle WebLogic Server domain in which Oracle Business Intelligence is installed must be configured to use an Oracle Access Manager asserter (OAMIdentityAsserter). This feature uses the Oracle Access Manager authentication services and validates already-authenticated Oracle Access Manager users through a suitable token and creates a WebLogic-authenticated session. It also provides single sign-on between WebGate and portals. WebGate is a plug-in that intercepts Web resource (HTTP) requests and forwards them to the Access Server for authentication and authorization

Single Sign-On (SSO)

SSO Methods

Enable Oracle Business Intelligence to accept SSO authentication from the security page in Enterprise Manager. The appropriate form of SSO is determined by the configuration settings made for the chosen SSO provider. If required, enter logon and logoff URLs for the configured SSO provider. The logoff URL (specified by the SSO provider) must be outside the domain

Supported SSO Mechanisms

FMW Security:

- Oracle Access Manager (OAM) Asserter
- Oracle Single Sign On (OSSO) Asserter
- Weblogic Default Asserter (for Client Certificate Authentication)
- Negotiate Identity Asserter (Kerberos - Windows Native Authentication without IIS)

Other Authentication Methods:

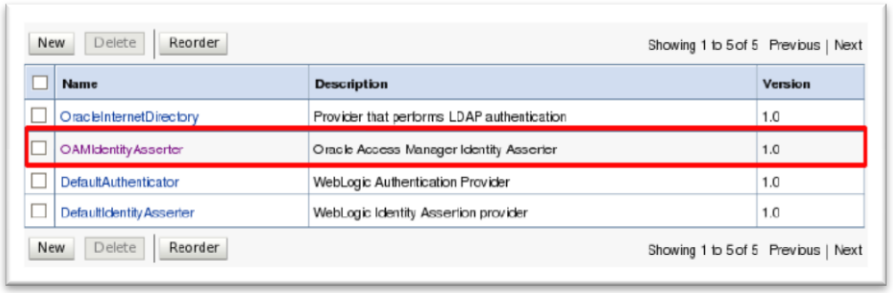
- SSO via http header or cookie
- E-Business Suite ICX Cookie mechanism
- Windows Authentication using IIS (uses http header)
- Siteminder 6 via http header
- Go URL parameters via get or post (using &NQUSER/&NQPASSWORD)

Single Sign-On (SSO)

Identify Providers and FMW Setup

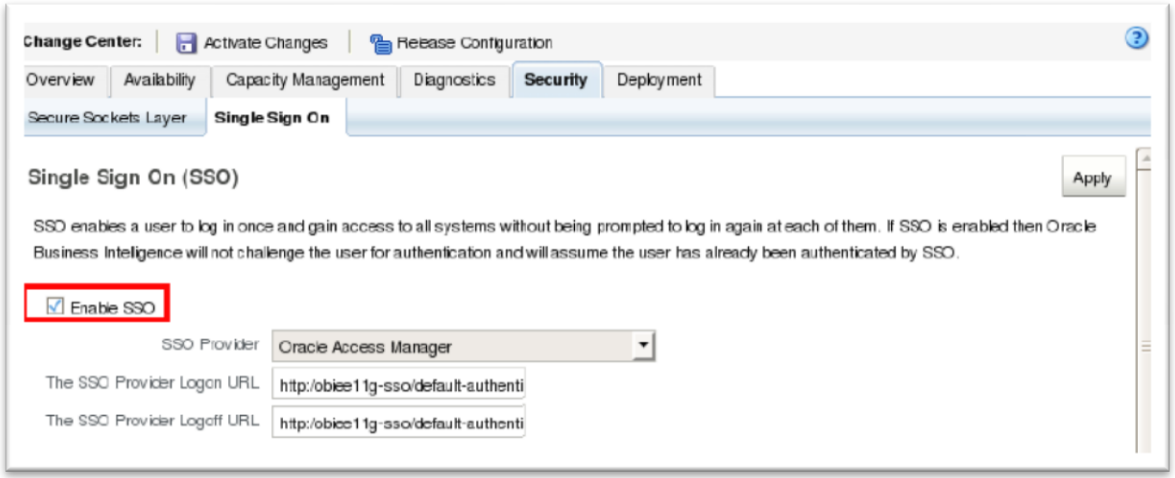
For SSO enablement, the order of authenticators has to be defined as follows:

- LDAP Authenticator (sufficient)
- SSO Asserter (required)
- Embedded Weblogic LDAP (sufficient)



LDAP authenticator is required for obtaining groups for users as well as for authentication for non-SSO access such as BI Office

Enable the SSO through the FMW Control.



Single Sign-On (SSO)

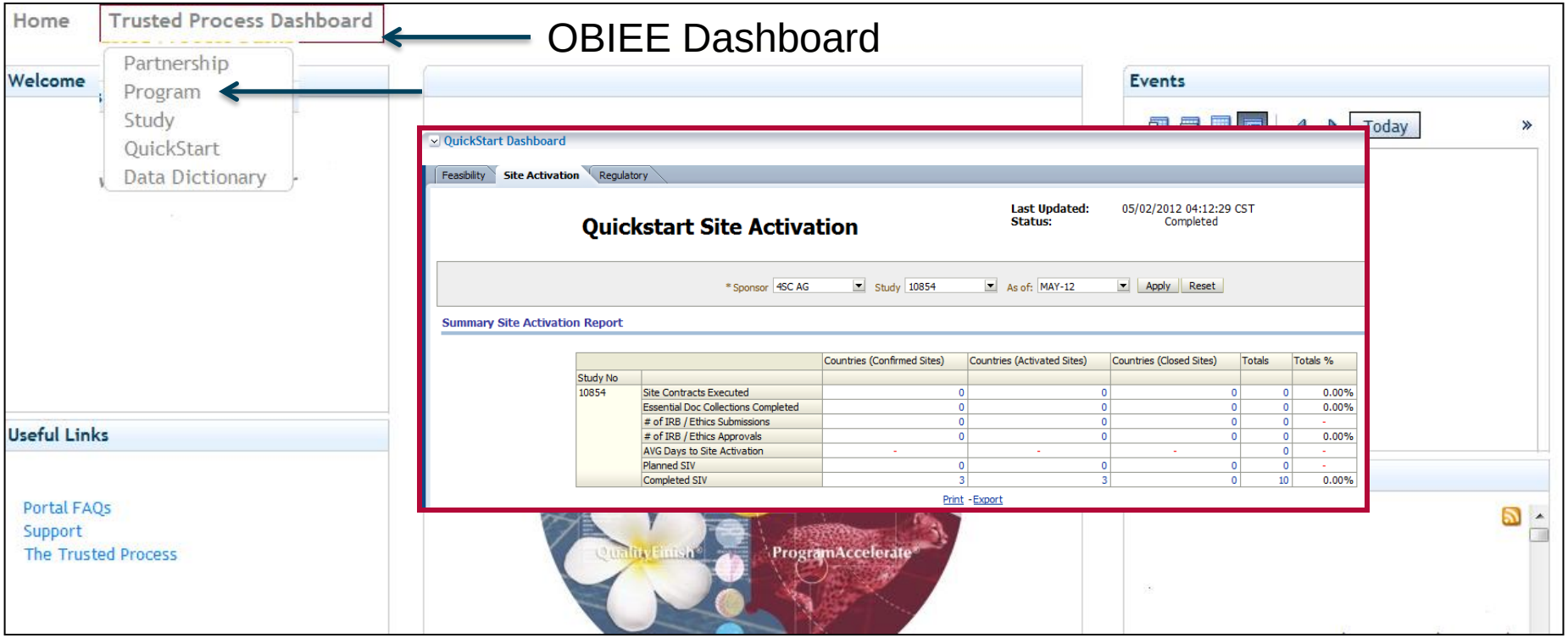
OBIEE and WebCenter Integration

- The integration uses the impersonate abilities of OBIEE to ensure reports and data are secured correctly.
- The integration requires the same user name population across the Web Center and OBIEE for the integration to work. This can be achieved by sharing the same LDAP Authentication provider.
- Create BIImpersonatorUser user & assign Impersonate policy to the user in OBIEE
- Create SOAP connection in Web Center through Mbean browser to connect to OBIEE

Single Sign-On (SSO)

OBIEE and WebCenter Integration

- The integration uses the impersonate abilities of OBIEE to ensure reports and data are secured correctly.
- The integration requires the same user name population across the Web Center and OBIEE for the integration to work. This can be achieved by sharing the same LDAP Authentication provider.
- Create BIImpersonatorUser user & assign Impersonate policy to the user in OBIEE
- Create SOAP connection in Web Center through Mbean browser to connect to OBIEE



- Questions?

MarketSphere®

- Ramke Ramakrishnan
  Practice Director, Oracle Business Intelligence
  ramke.ramakrishnan@marketsphere.com