Oracle Business Intelligence Enterprise Edition (OBIEE)

Security Examined

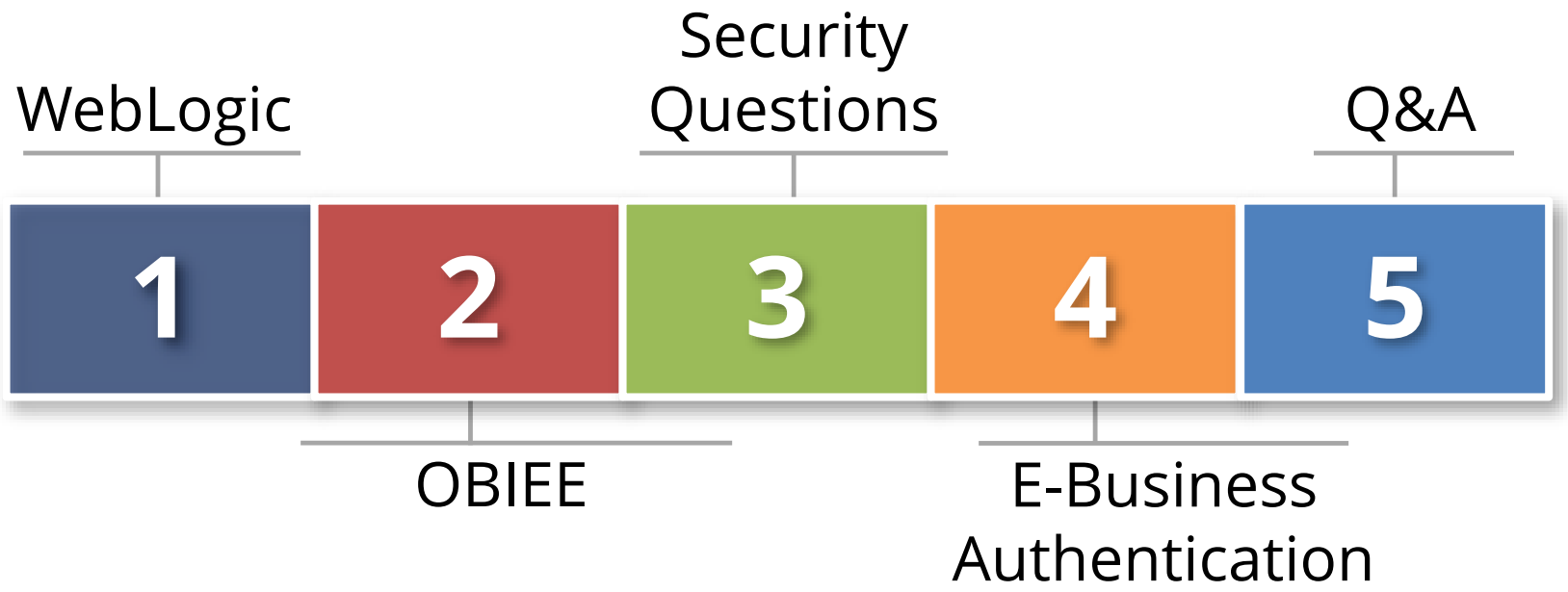
March 19, 2014

Mike Miller
Chief Security Officer
Integrigy Corporation

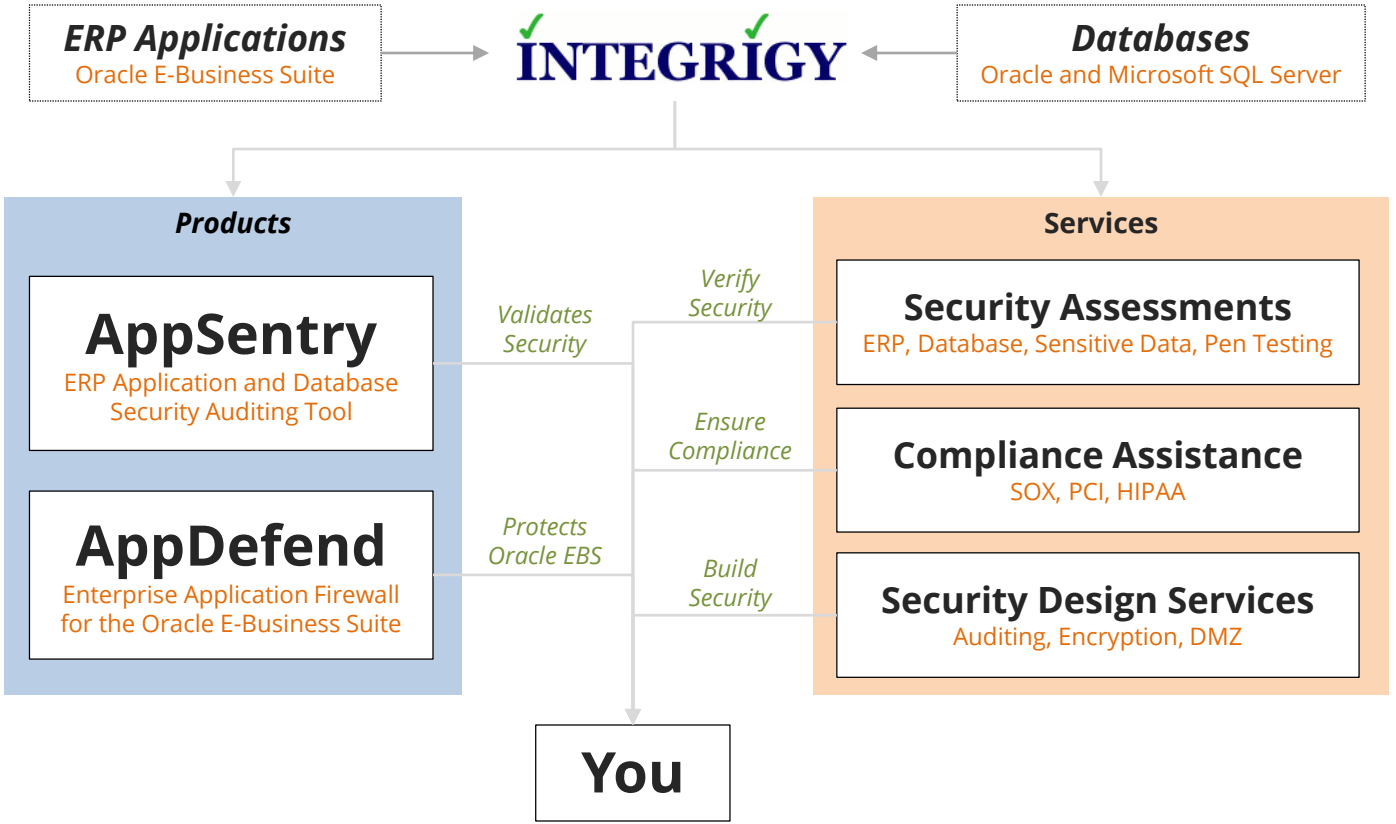
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

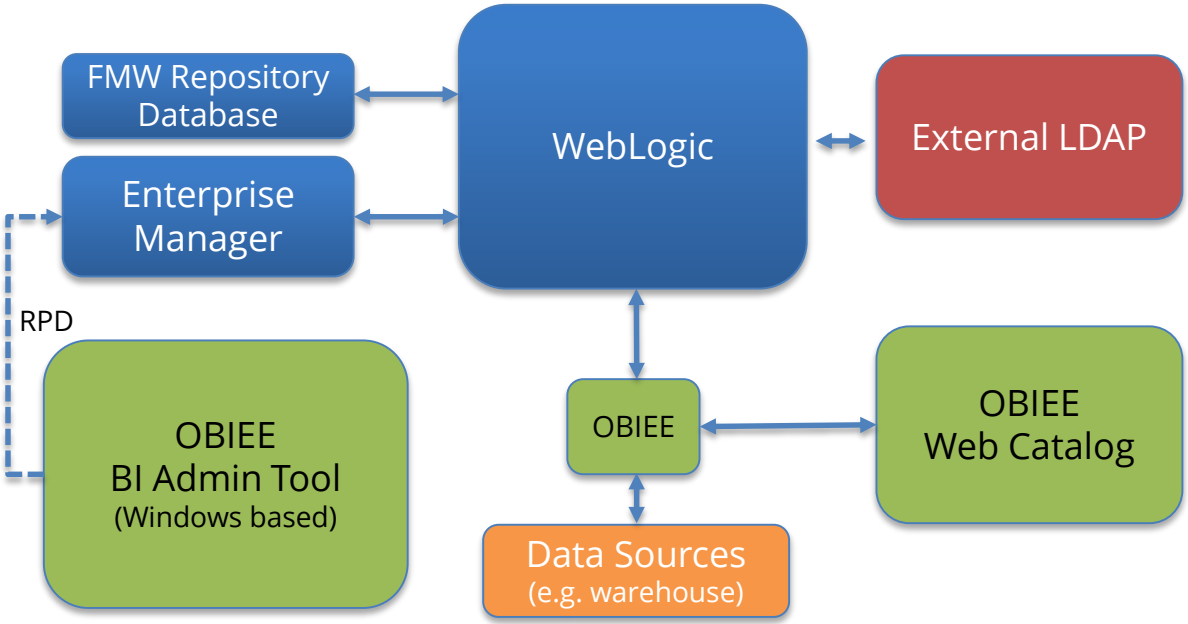
Agenda


WebLogic
Security Questions
Q&A
1
2
3
4
5
OBIEE
E-Business Authentication

About Integrigy

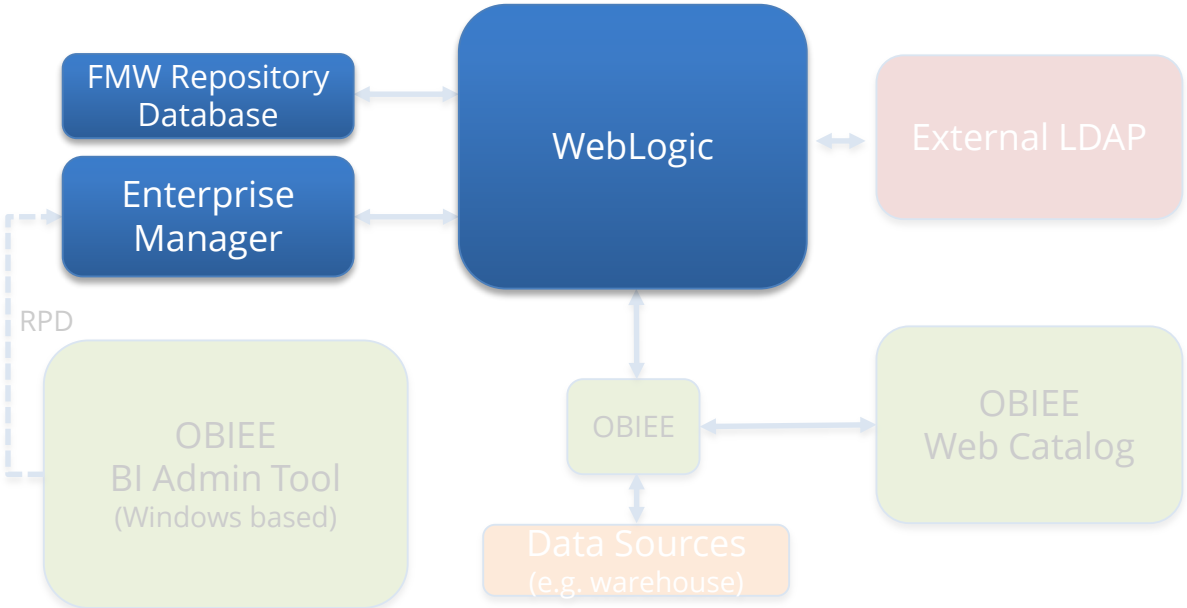


OBIEE Security Examined



Size of box proportionate to component's impact on security

Agenda


FMW Repository Database
Enterprise Manager
WebLogic
External LDAP
RPD
OBIEE
BI Admin Tool
(Windows based)
OBIEE
OBIEE
Web Catalog
Data Sources
(e.g. warehouse)

WebLogic Security

- **OBIEE runs inside of WebLogic**
  - Authentication
  - Key authorization steps
  - Java and Web services

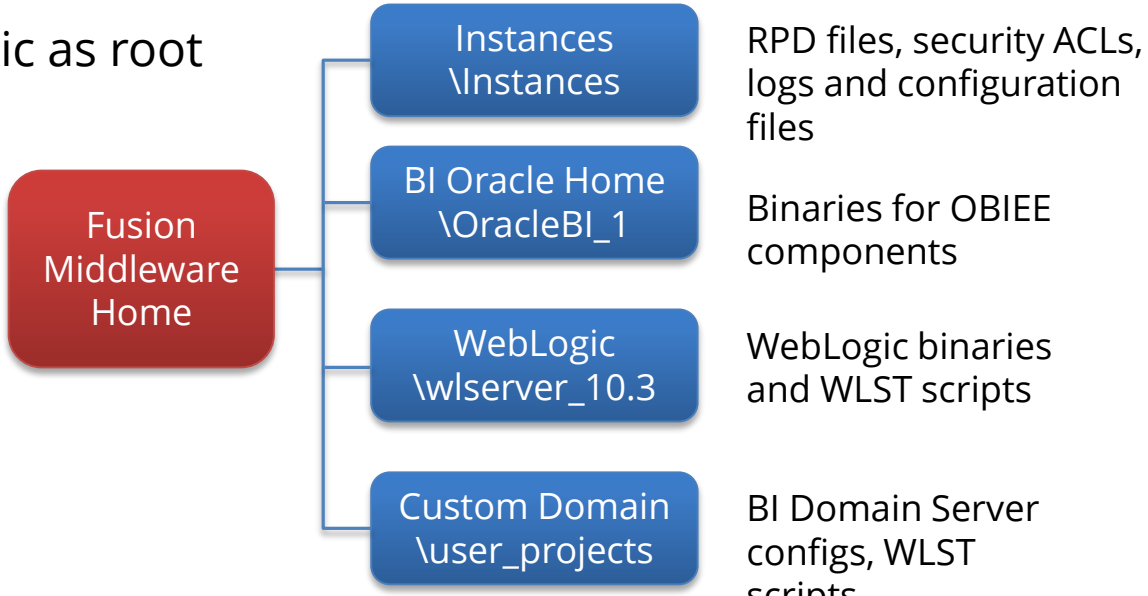
- **Secure WebLogic to Secure OBIEE**

Keep Current with WebLogic Patches

- **10.3.5**
  - Released May 2011
  - Grace period ended August 2013
- **10.3.6**
  - February 2012
  - Grace period ends December 2021
  - Terminal patch set for 11g

WebLogic File system

- Protect the file system
- Do not run WebLogic as root



Public Facing?

- Web Application Firewall
- WebLogic 10.3.6
- Java 1.6 vs. 1.7
- WebLogic Configurations
  - Robots.txt
  - Powered By
  - Services exposed

Metadata Repository

- **Metadata repository database required for each Fusion Middleware product**
  - Oracle is recommended but not required
  - ‘Repository Creation Utility’ used to create
- **OBIEE metadata schemas**
  - BIPLATFORM
  - MDS
- **Security of metadata repository database is critical**
  - All standard security best practices apply
  - Do not manually edit or allow access

Security Realms

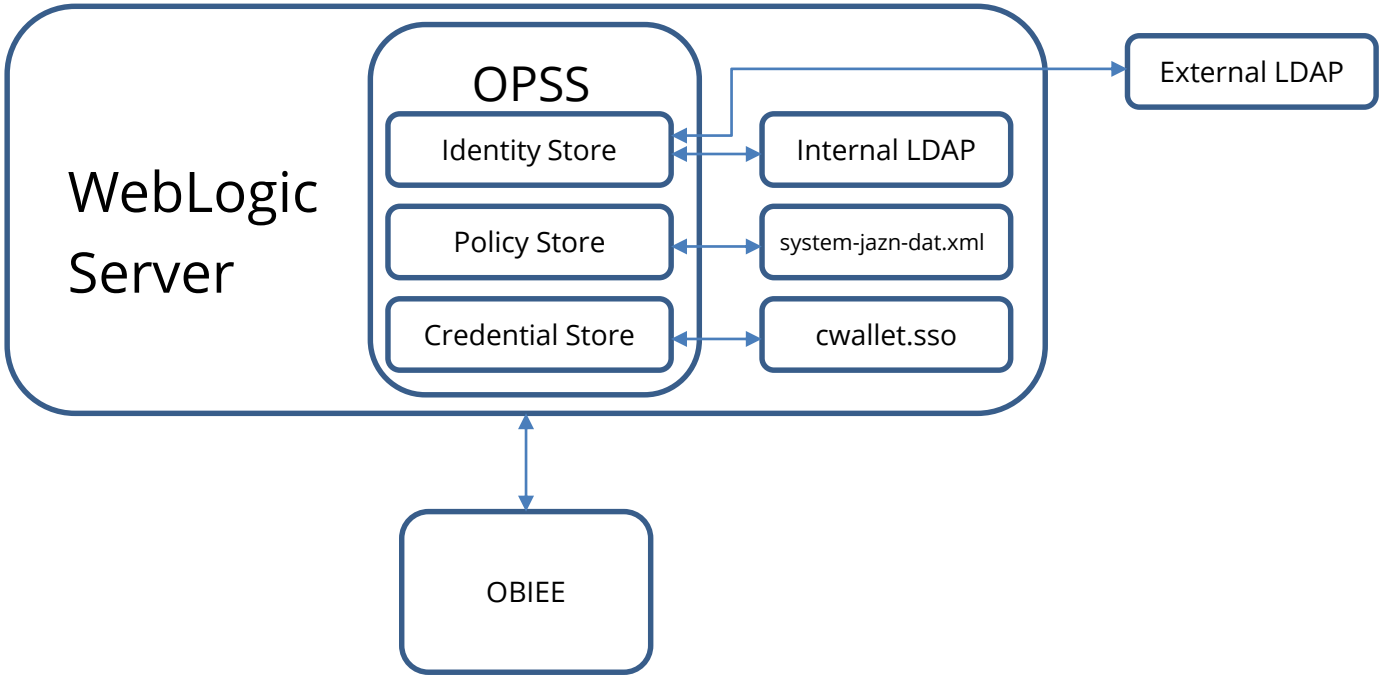
- **OBIEE 11g uses WebLogic for centralized common services**
  - Common security model included
  - Significant change from OBIEE 10g

- **WebLogic common security defined through security realms. Realms define:**
  - Users
  - Groups
  - Security roles and policies

- **Key decision**
  - Use default security realm or custom for OBIEE

Oracle Platform Security Services (OPSS)

Transcends ALL Fusion Middleware Products



WebLogic Scripting Tools (WLST)*

- Command line scripting tool to manage WebLogic
  - Jython based
- On and offline modes
    - Both are powerful
- Access remotely or console
- WebLogic Security Framework used to enforce same rules as user interface

- Connect using administration port
- Use appropriate WebLogic accounts for WLST scripting
- Do not hardcode credentials
- Do not expose encrypted attributes
  - E.g. listCred()

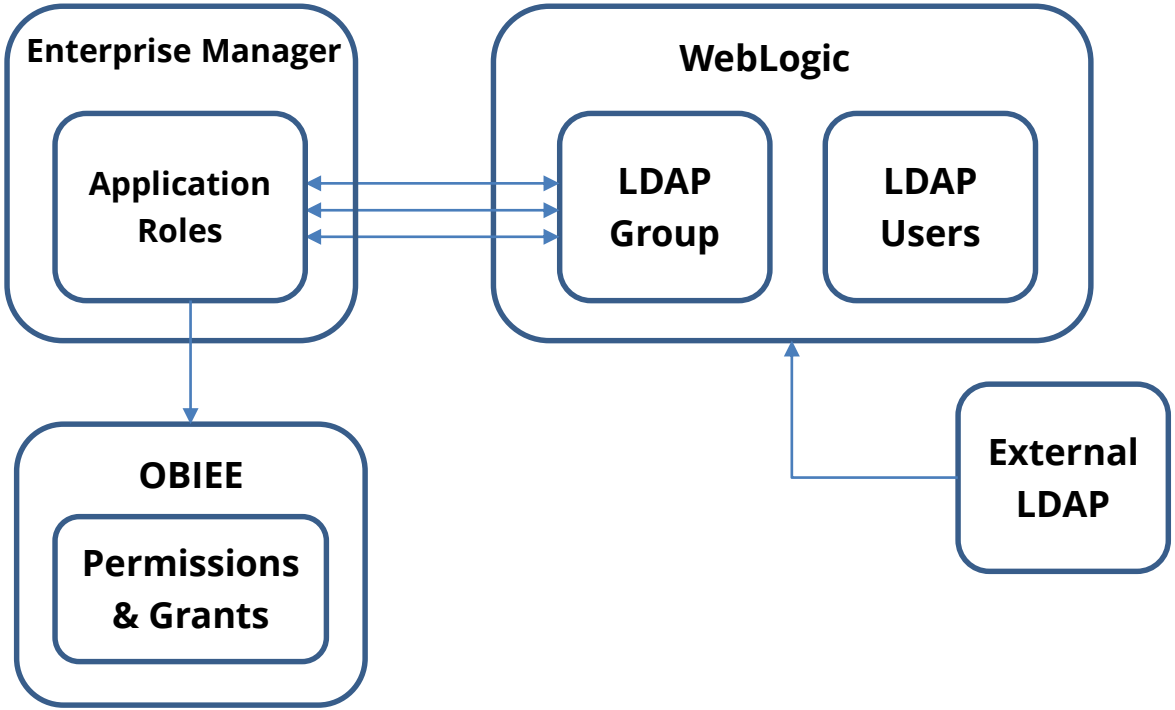
* DBAs use SQL, WebLogic Admins use WLST

WebLogic Auditing

- Prebuilt compliance reporting features
- Flexible and extensive
  - Specific criteria
  - Severity levels
- Authentication history/failures
- Authorization history

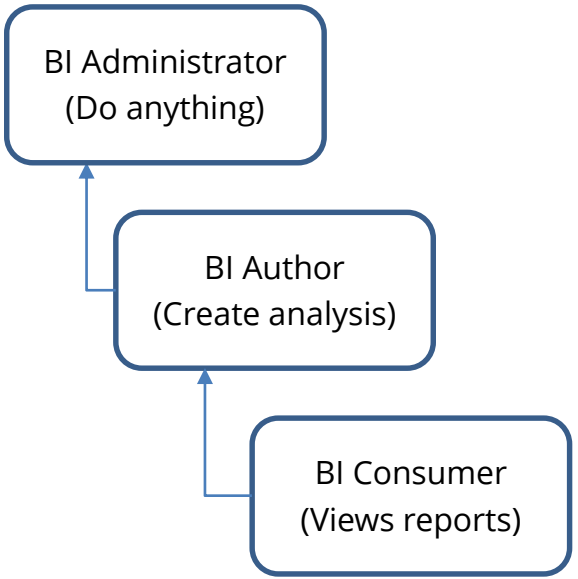
- Common audit record format
- Write audit data to:
  - Database
  - File
- Use audit data in
  - BI Publisher
  - Splunk, ArcSight etc....

Applications Roles

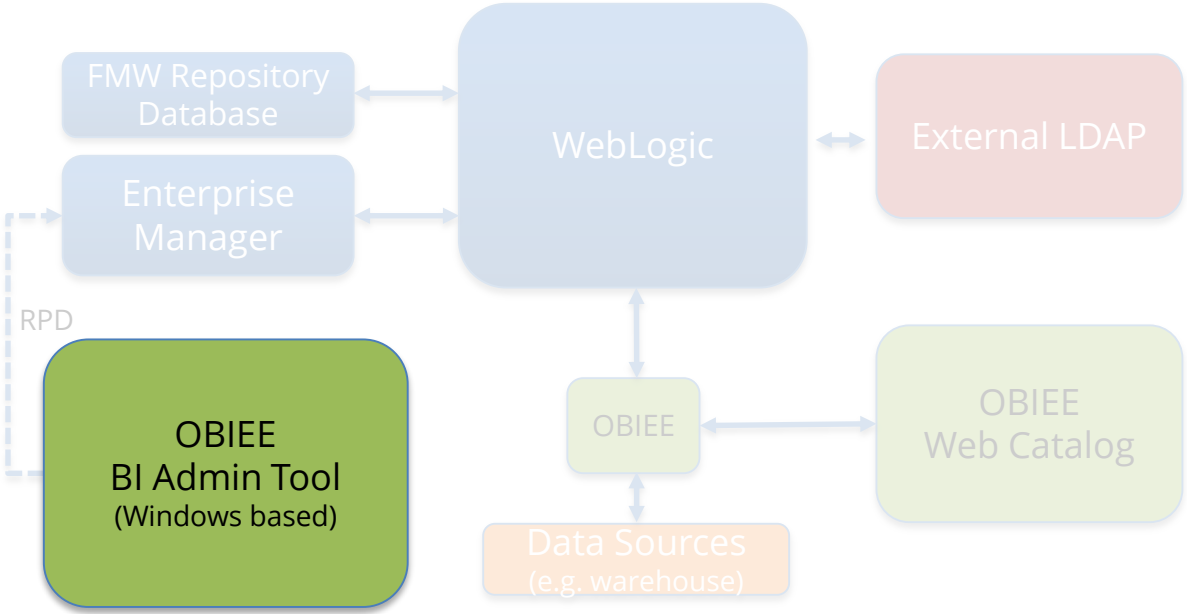


Application Roles

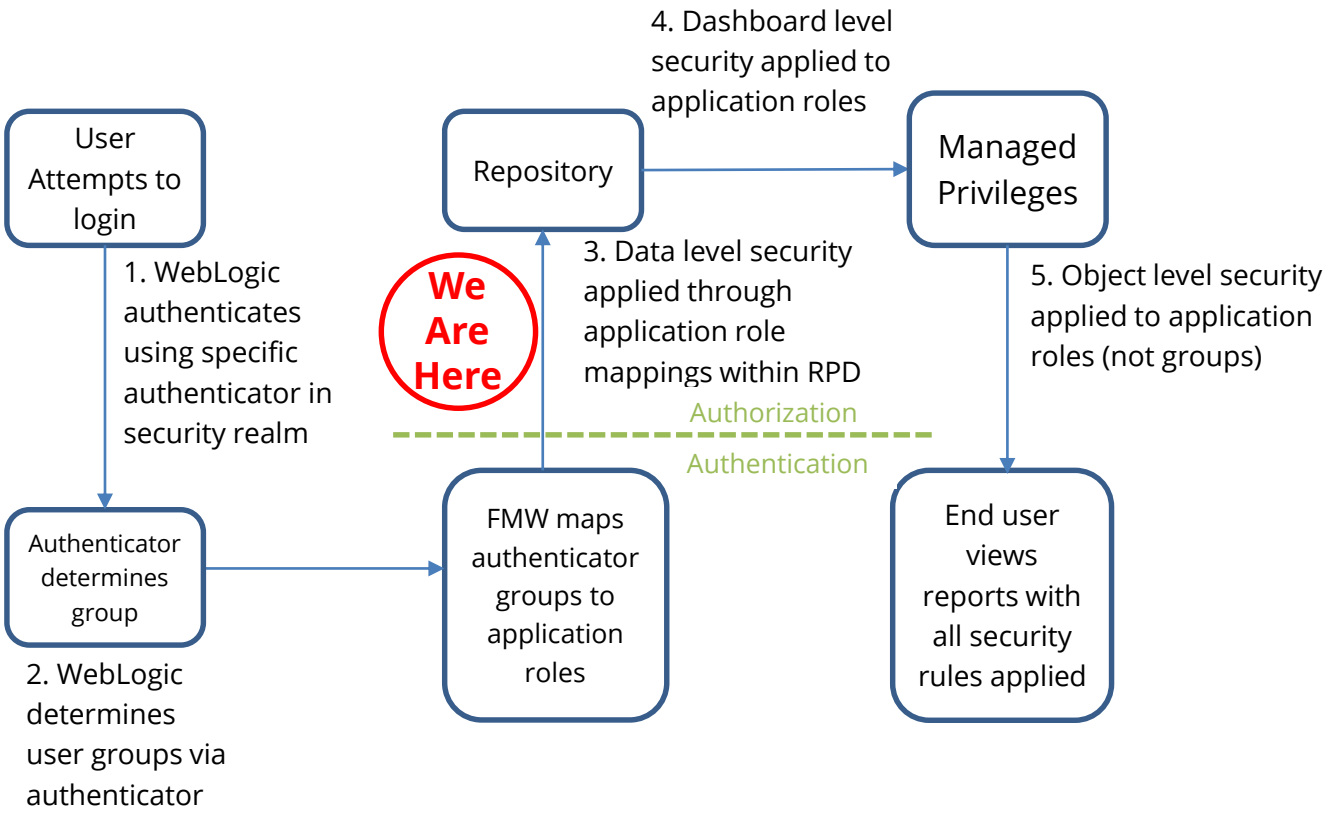
- **Transcend ALL Fusion Products**
- **Defined in Enterprise Manager**
- **Map to LDAP groups**
  - External or internal
- **Key Decision:**
  - Use default or custom



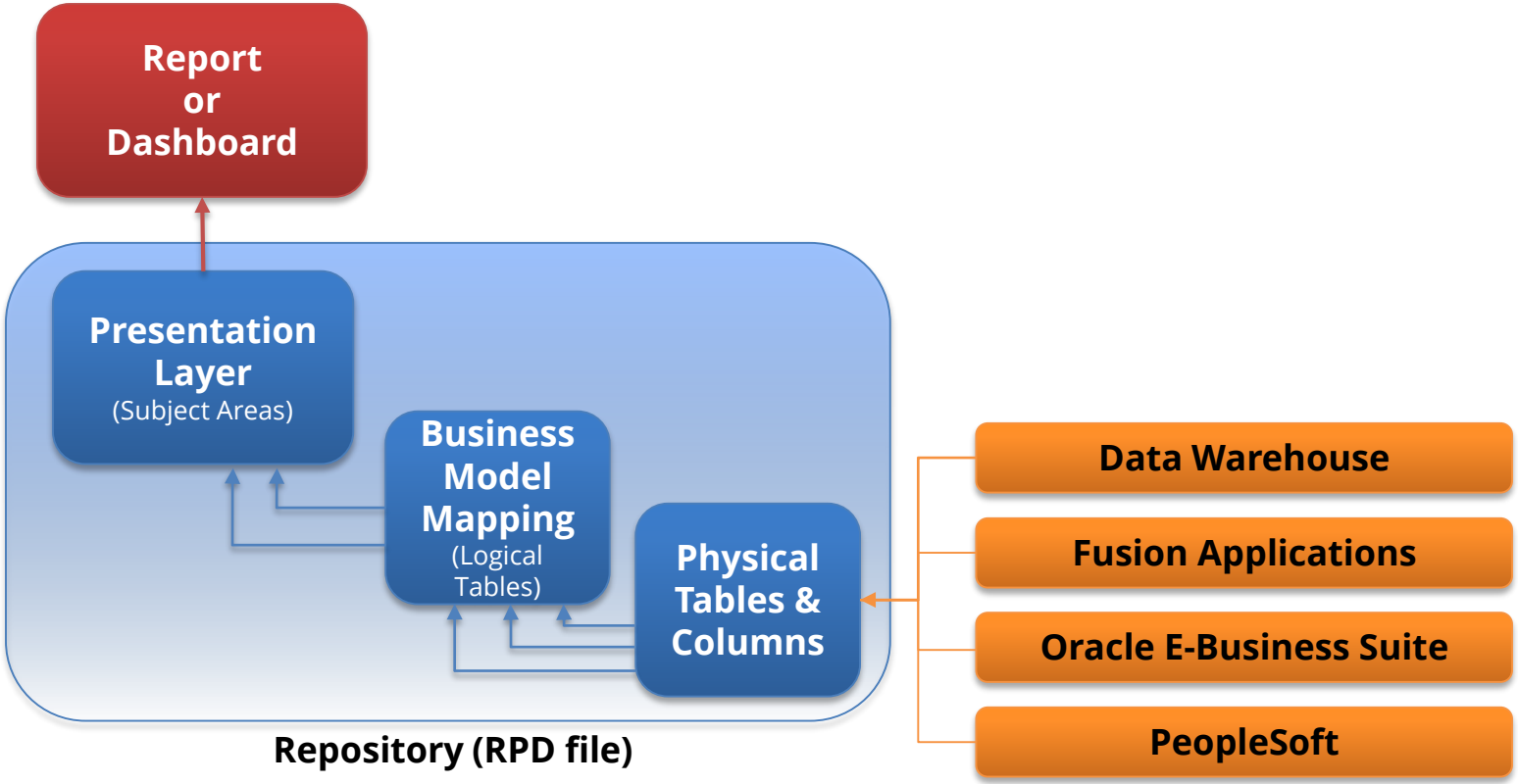
Agenda


FMW Repository Database
Enterprise Manager
WebLogic
External LDAP
RPD
OBIEE BI Admin Tool (Windows based)
OBIEE
OBIEE Web Catalog
Data Sources (e.g. warehouse)

Where Are We?

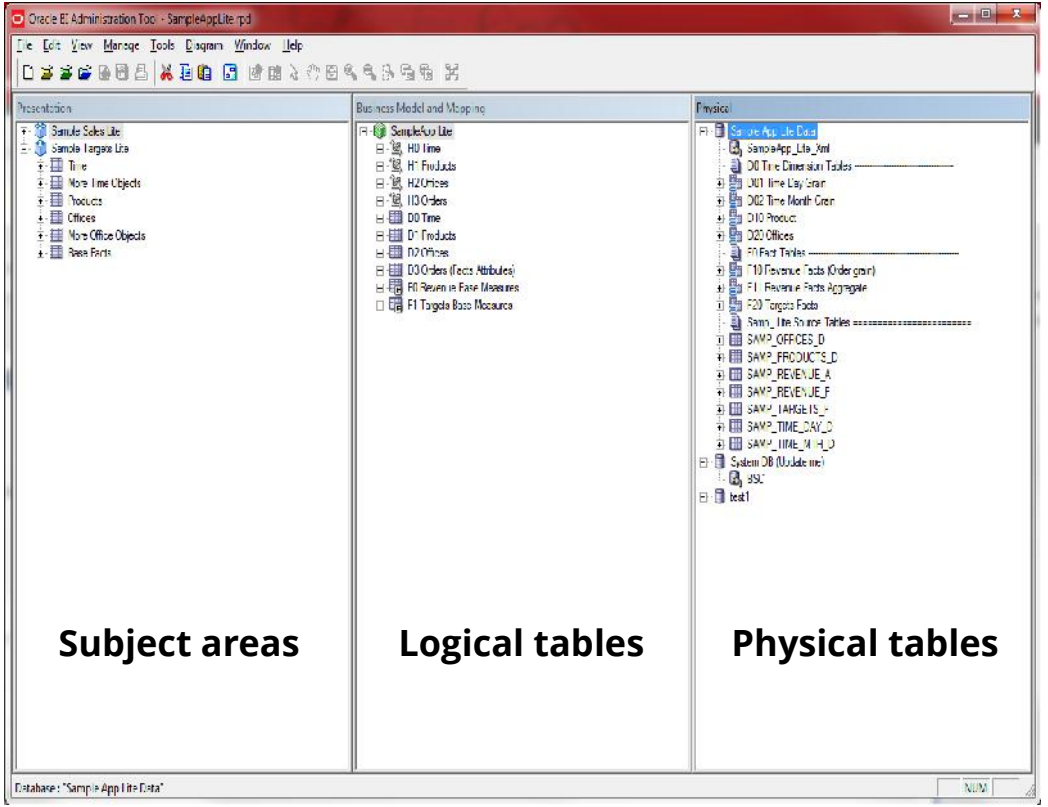

User Attempts to login
1. WebLogic authenticates using specific authenticator in security realm
Authenticator determines group
2. WebLogic determines user groups via authenticator
FMW maps authenticator groups to application roles
We Are Here
Repository
3. Data level security applied through application role mappings within RPD
4. Dashboard level security applied to application roles
Managed Privileges
5. Object level security applied to application roles (not groups)
End user views reports with all security rules applied
Authorization
Authentication

Oracle Business Intelligence Enterprise Edition



OBIEE Repositories

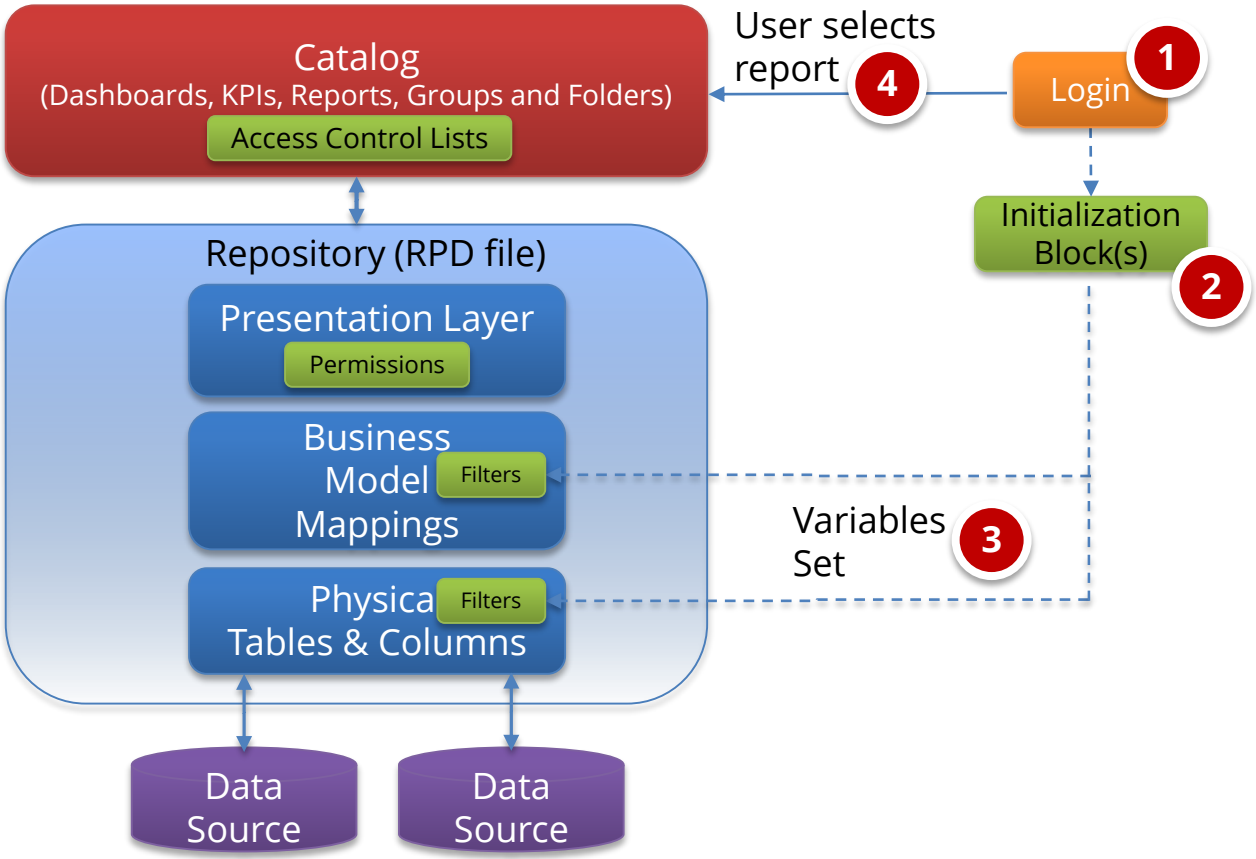
- **OBIEE Solutions are built using Repositories**
  - Single file (“RPD”) defines EVERTHING
  - Security included
- **BI Admin Tool used to create and maintain RPD files**
  - Windows based



RPD Security

- **Need to Secure RPD files**
  - Data source connection passwords
  - Security rules and filters
- **Password to open**
  - Production vs Non-production
  - Password needed to deploy within Enterprise Manager
- **Encrypted**
  - Password used to encrypt
  - Can export and save as XML files

OBIEE Security



Three Levels of OBIEE Security (Authorization)

Data-level security	▪ Data filters to eliminate rows from result sets ▪ Set in RPD file
Object-level security	▪ Permissions on specific objects such as subject areas, presentation or physical tables and columns ▪ Set in RPD file
Presentation Catalog security	▪ What reports and dashboards are available to specific users, application roles and LDAP groups ▪ Set in catalog

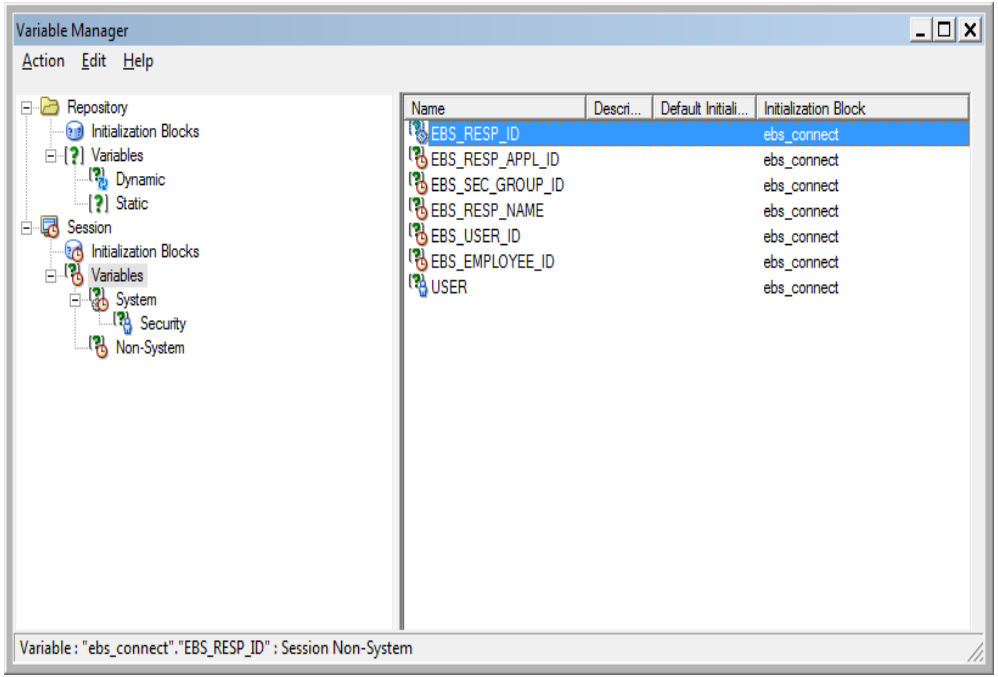
Data Level Security

- **Deny or allow access to physical or logical table, row or column**
  - Apply to users or roles
  - Use filters restrict
  - Use variables to define filters

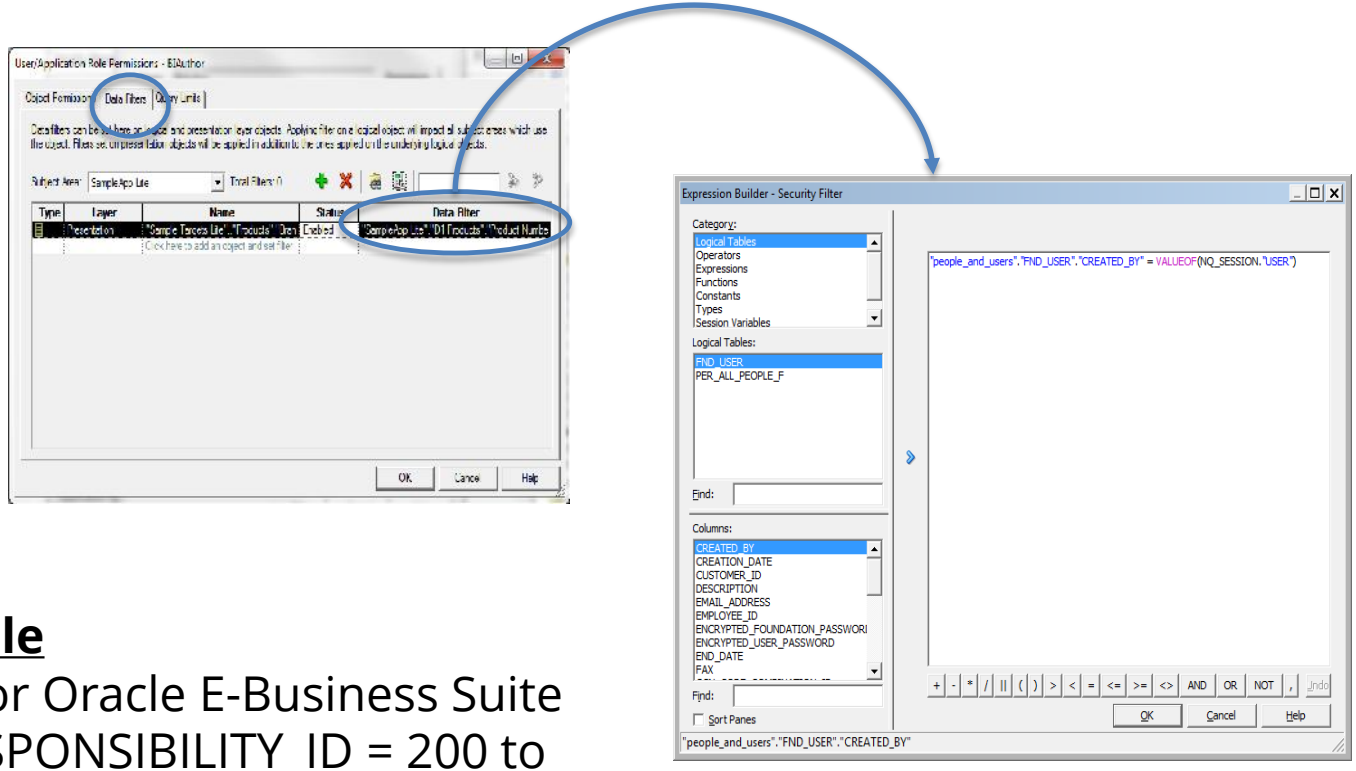
- **Two types of variables**
  - Repository **–** Static or dynamic, same for all users
  - Session **–** initialized when user logs in

Data Level Security

- **Initialization block**
  - Set variables (repository & session) when a user connects
- **Two types of session variables**
  - System: reserved names e.g. USER
  - Non-system: defined by author of RPD e.g. EBS_RESP_ID



Data Level Security



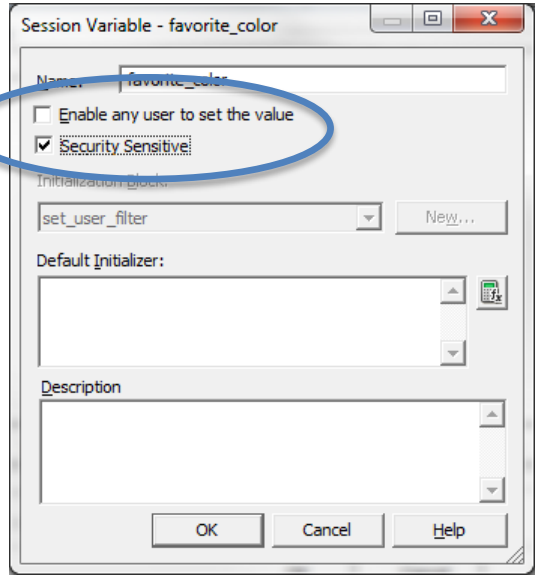
Example

Filter for Oracle E-Business Suite
Set RESPONSIBILITY_ID = 200 to see only hourly employees

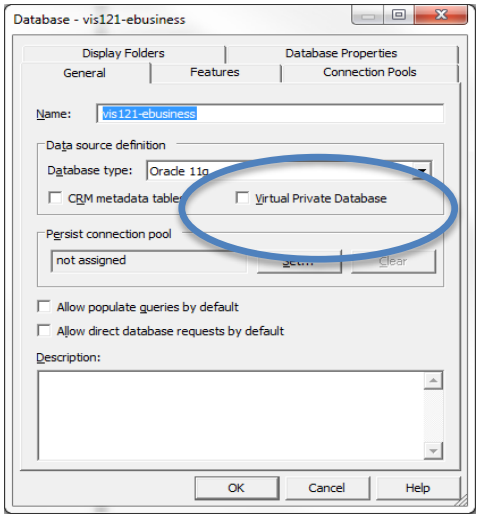
Data Level Security

- **Be careful of caching with session variables and VPD**
  - DBMS_SESSION.SET_IDENTIFIER

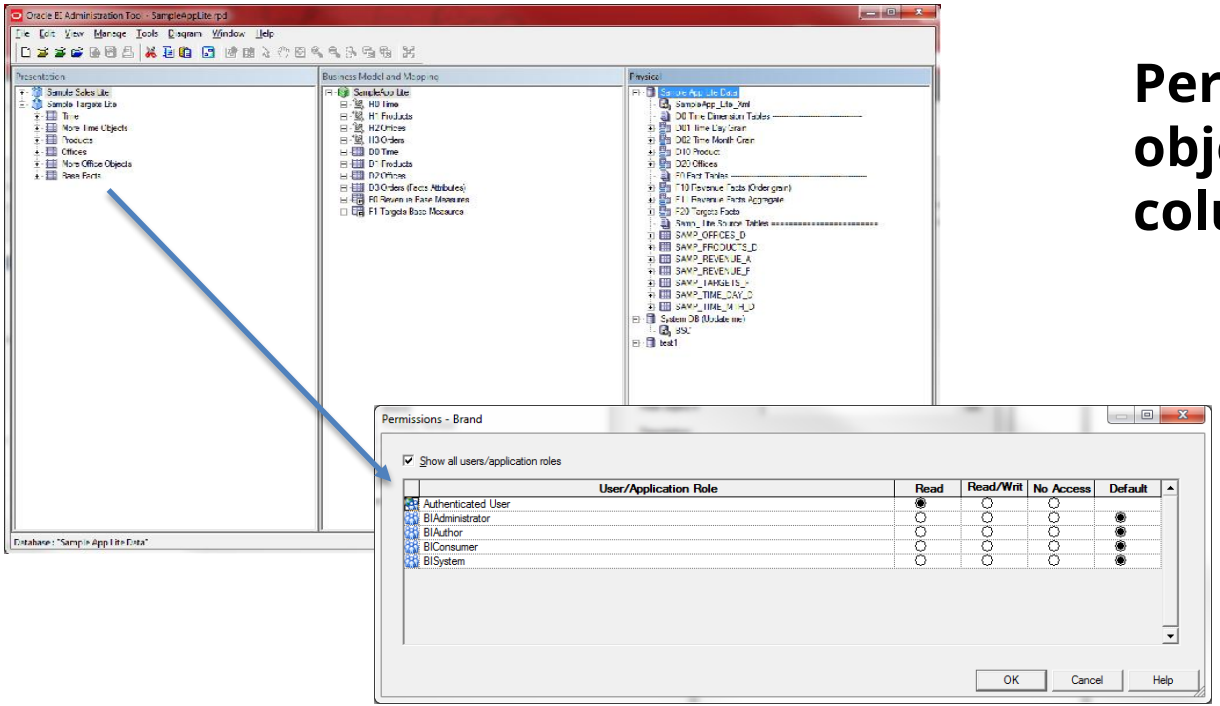
Session Variable



Connection

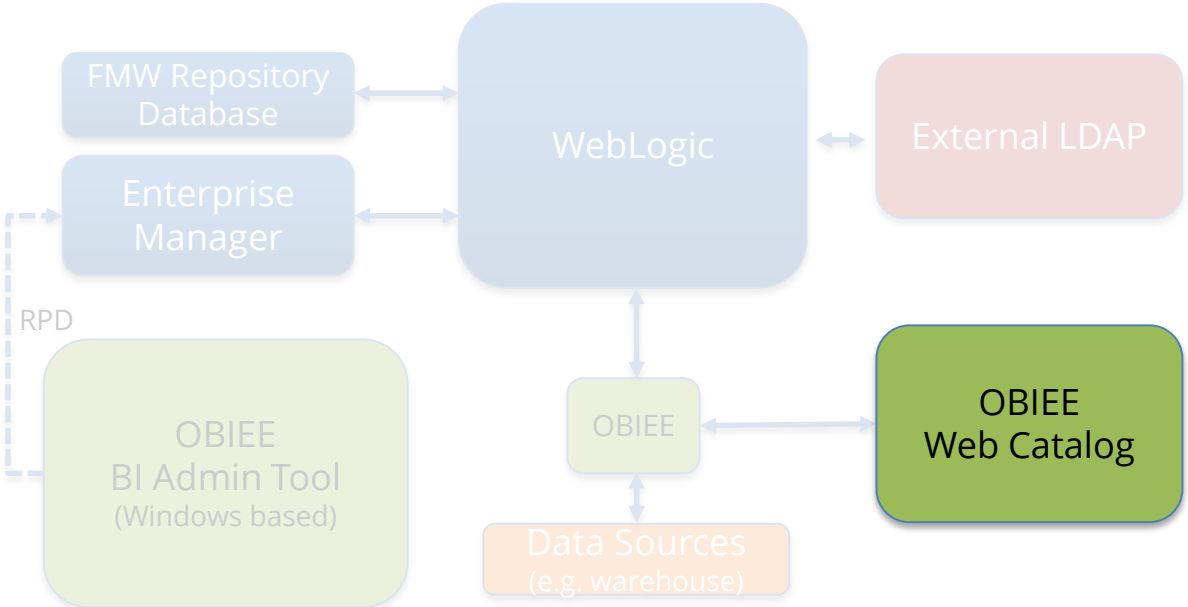


Object Level Security



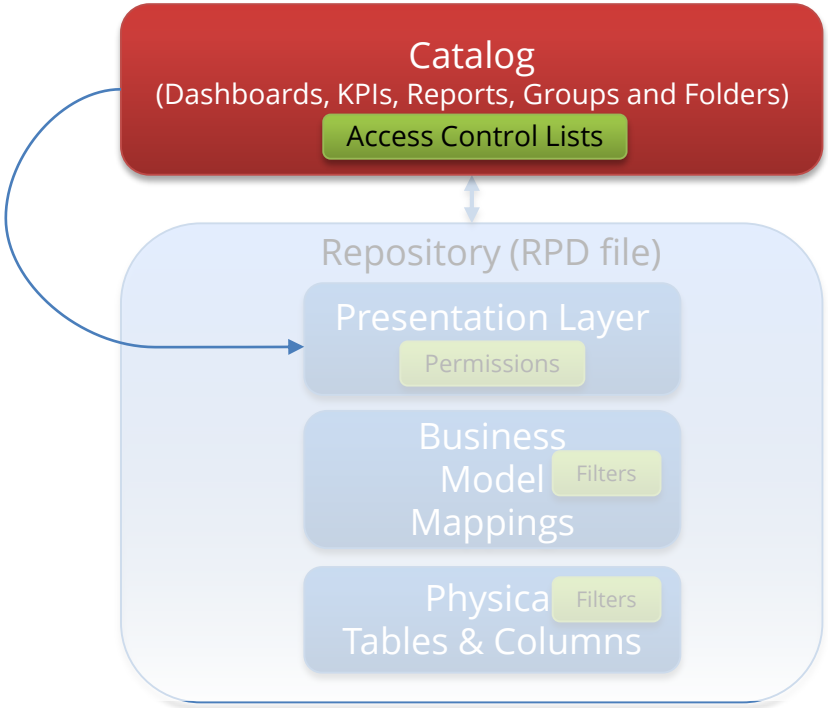
Permissions for object, row and column security

Agenda


FMW Repository Database
Enterprise Manager
WebLogic
External LDAP
RPD
OBIEE BI Admin Tool (Windows based)
OBIEE
OBIEE Web Catalog
Data Sources (e.g. warehouse)

OBIEE Web Catalog

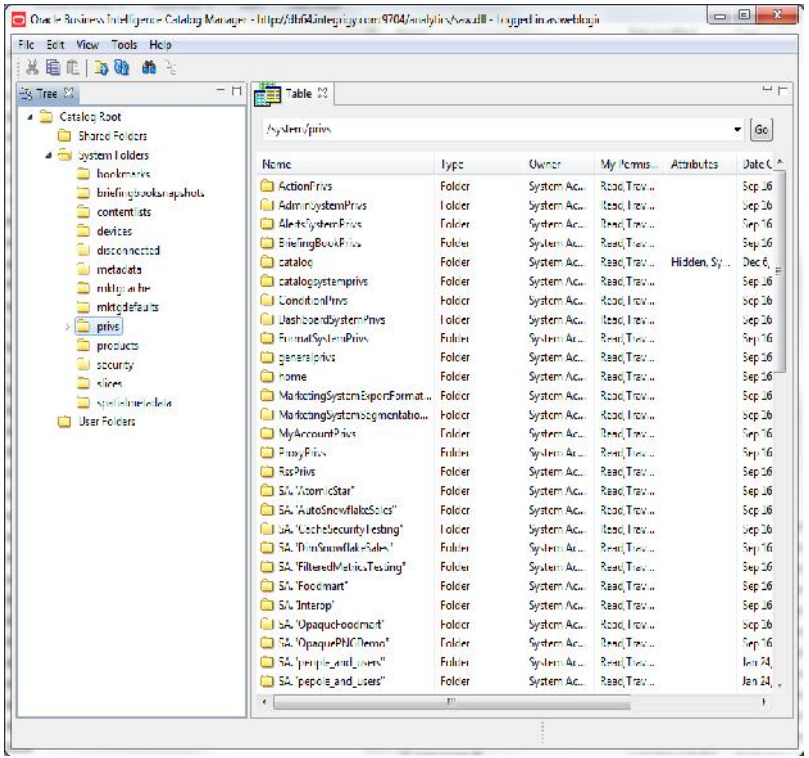
Catalog only sees Subject Areas within Presentation Layer



Presentation Catalog Security

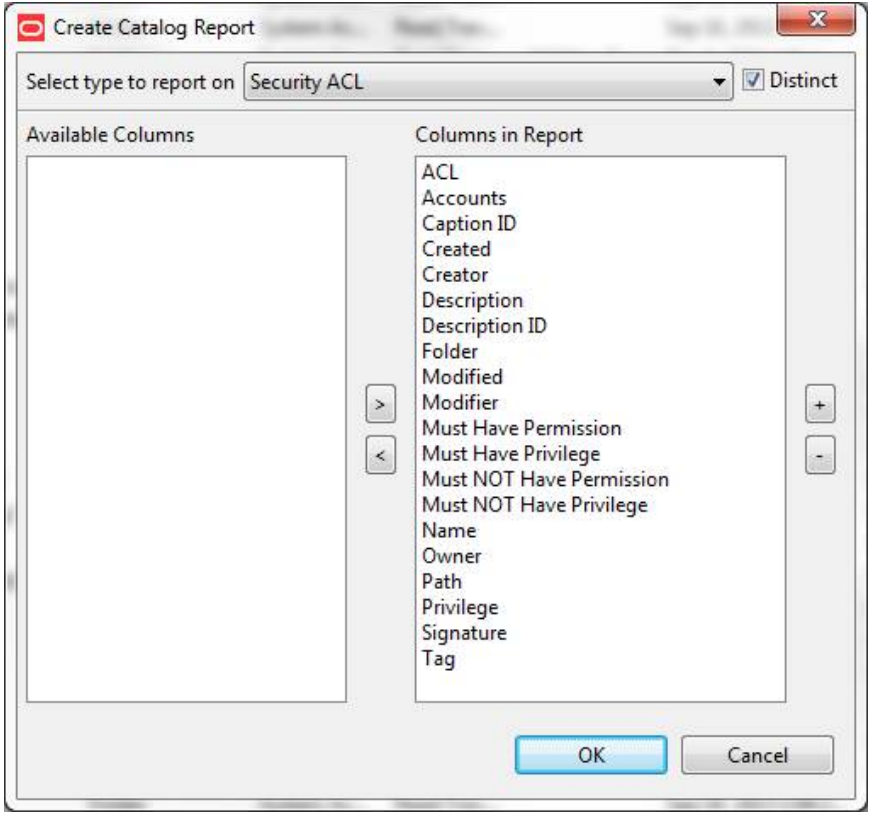
- **Access Control List (ACL) defined for each object**
  - Stored in *.ATR files
- **Works only at the subject area level of RPD**
- **BI Publisher is a separate catalog**
- **Catalog of permissions:**
  - Dashboards
  - Reports
  - KPIs
  - Groups of
  - Folders
  - Permissions

Windows Catalog Client



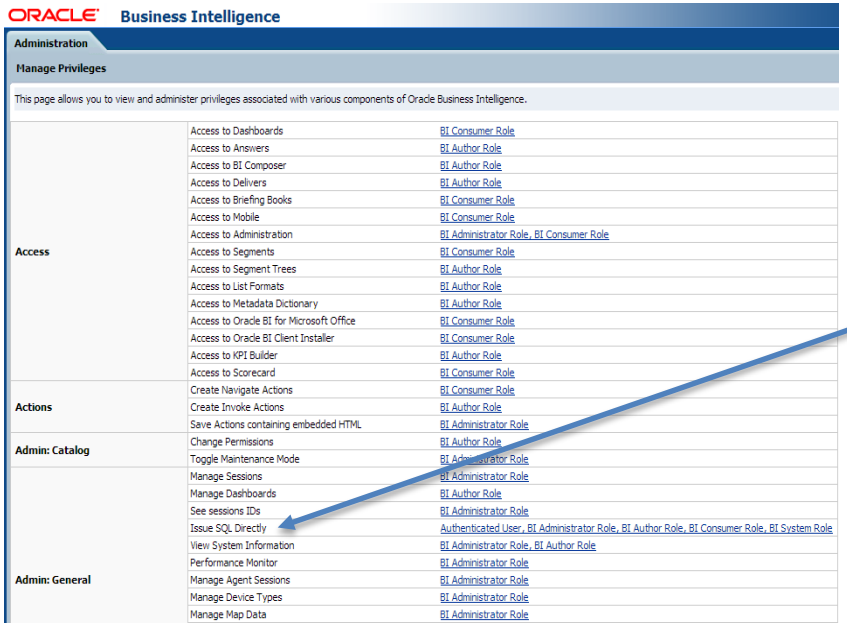
Presentation Catalog Reports

- **Catalog reports are critical feature**
- **Export to Excel for analysis and reporting**



Presentation Catalog Security

- Administration Rights also set with ACLs
  - **Security ACL** is very important



ORACLE Business Intelligence

Administration

Manage Privileges

This page allows you to view and administer privileges associated with various components of Oracle Business Intelligence.

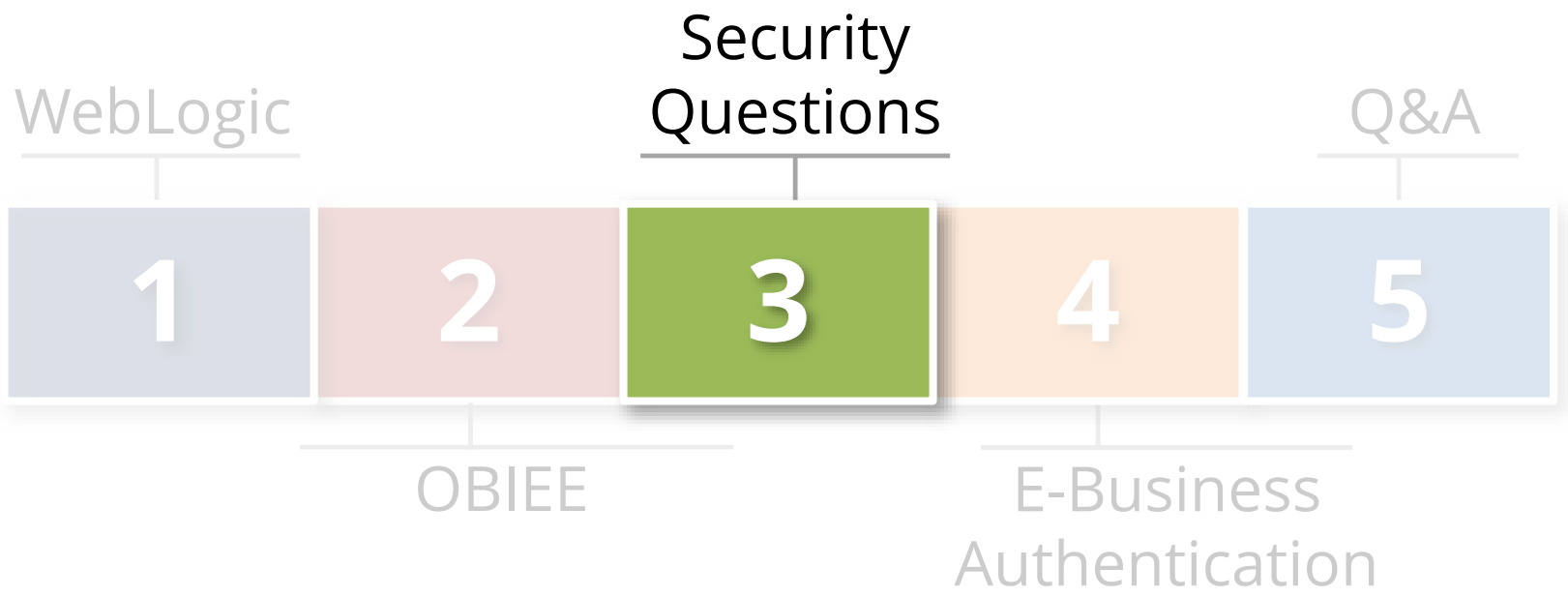
Access	Access to Dashboards	BI Consumer Role
	Access to Answers	BI Author Role
	Access to BI Composer	BI Author Role
	Access to Delivers	BI Author Role
	Access to Briefing Books	BI Consumer Role
	Access to Mobile	BI Consumer Role
	Access to Administration	BI Administrator Role, BI Consumer Role
	Access to Segments	BI Consumer Role
	Access to Segment Trees	BI Author Role
	Access to List Formats	BI Author Role
	Access to Metadata Dictionary	BI Author Role
	Access to Oracle BI for Microsoft Office	BI Consumer Role
	Access to Oracle BI Client Installer	BI Consumer Role
	Access to KPI Builder	BI Author Role
	Access to Scorecard	BI Consumer Role
Actions	Create Navigate Actions	BI Consumer Role
	Create Invoke Actions	BI Author Role
	Save Actions containing embedded HTML	BI Administrator Role
Admin: Catalog	Change Permissions	BI Author Role
	Toggle Maintenance Mode	BI Administrator Role
Admin: General	Manage Sessions	BI Administrator Role
	Manage Dashboards	BI Author Role
	See sessions IDs	BI Administrator Role
	Issue SQL Directly	Authenticated User, BI Administrator Role, BI Author Role, BI Consumer Role, BI System Role
	View System Information	BI Administrator Role, BI Author Role
	Performance Monitor	BI Administrator Role
	Manage Agent Sessions	BI Administrator Role
	Manage Device Types	BI Administrator Role
	Manage Map Data	BI Administrator Role

For example: Who can Issue SQL direct

OBIBEE Security Changes with 11g

- **Users and groups no longer defined in RPD**
  - Defined now in WebLogic & OEM
- **Security policies mapped to Application Roles not groups**
  - Roles transcend ALL Fusion Applications
- **No more Administration user**
  - Any number of users have Admin privileges

Agenda


WebLogic
Security Questions
Q&A
1
2
3
4
5
OBIEE
E-Business Authentication

OBIEE Security and Discussion Questions

- Permission reports
- Usage Tracking
- Key Accounts
- Act As/Impersonation
- Direct SQL Access
- GO URL
- Configuration migrations
- Writeback
- Time limits
- VPD support
- Source code control
- Logging and log levels

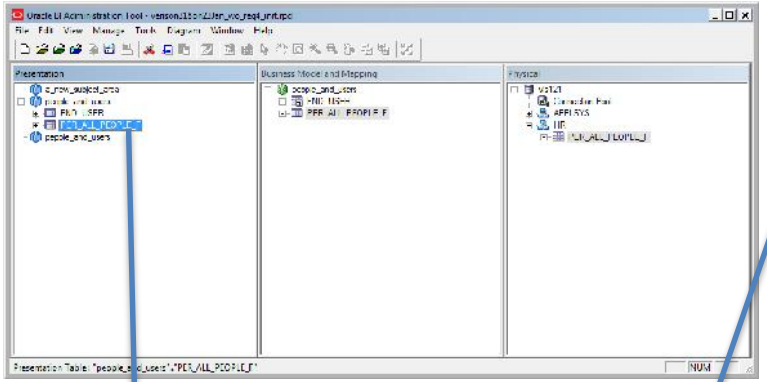
Key Accounts

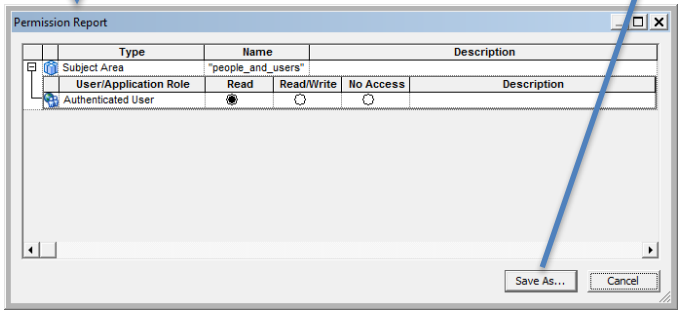
Account	Security Issue
OS owner of WebLogic	Try not use to ‘weblogic’ or to use welcome1 for a password
OS user that runs WebLogic	Do not use root or a privileged user. Do not hardcode this user’s credentials in startup/shutdown scripts.
WebLogic administration user(s)	End-user(s) with full Administration rights to WebLogic
BI Admin User	Seeded end-user with full Administration rights to OBIEE
BI System User	Seeded account used for service-to-service authentication. Not intended to be used by users. Do not change password without following the specific Oracle support instructions.
OracleSystemUser	Seeded account created during installation. User name can be change later but need to follow instructions.

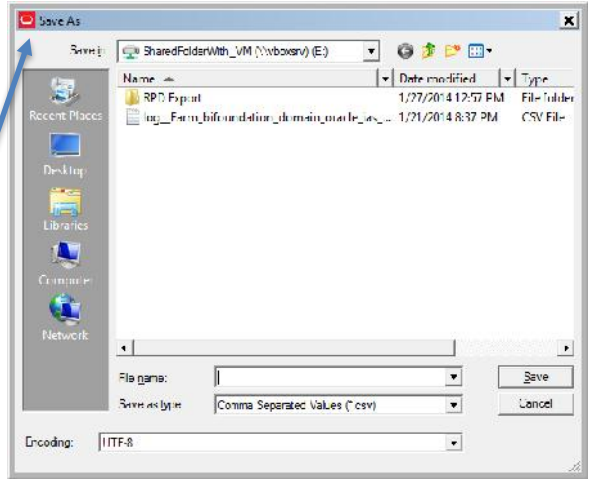
Ask Questions About …

Write-backs	▪ Connection pools can be flagged to allow users to update the database ▪ Who can and to what? ▪ Can they also issue Direct SQL?
Security configurations & migrations	▪ How are OPSS (policies and credentials) migrated from non-production to production? ▪ GUI or WLST?
Source code control	▪ Are RPD files under source code control? ▪ Are XML exports being used?

Ask For RPD Permission Reports







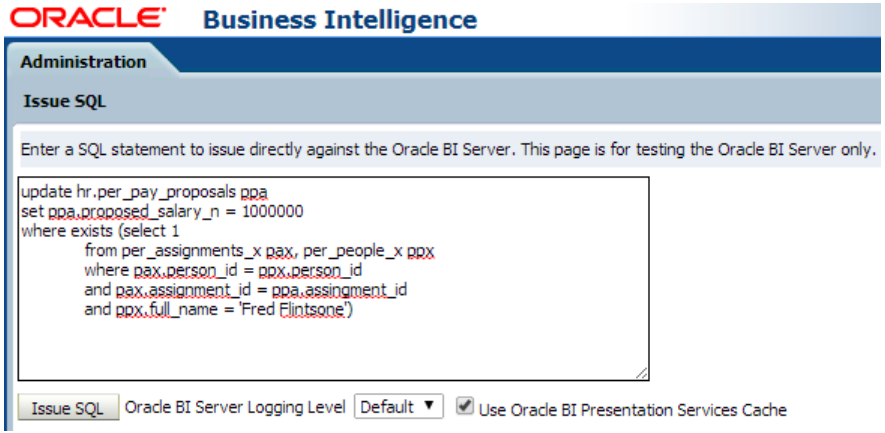
Note: Permission reports do NOT include BMM or Physical filters and limits

Use OBIEE Usage Tracking

- **Oracle provides sample RPD**
  - Manually copy components into your RPD
- **Reports on changes to**
  - Enterprise manager configuration changes
  - RPD changes
  - Who ran what report when
- **Recommend redirect to log files**
  - Set STORAGE_DIRECTORY in NQSConfig.ini
  - Pass to centralized logging (e.g. Spunk, ArcSight, etc…)
  - Part of holistic log and audit solution

Direct SQL Access/Go URL SQL Access

Direct SQL:



- **Only objects in RPD can be queried**
- **Have PUBLIC user? How is it locked down?**

GO URL

http://testobiee:9704/analytics/saw.dll?Go&SQL=**select+person,salary+from+hr_salary_info**

FROM clause is the name of the Subject Area to query

Act-As and Impersonation

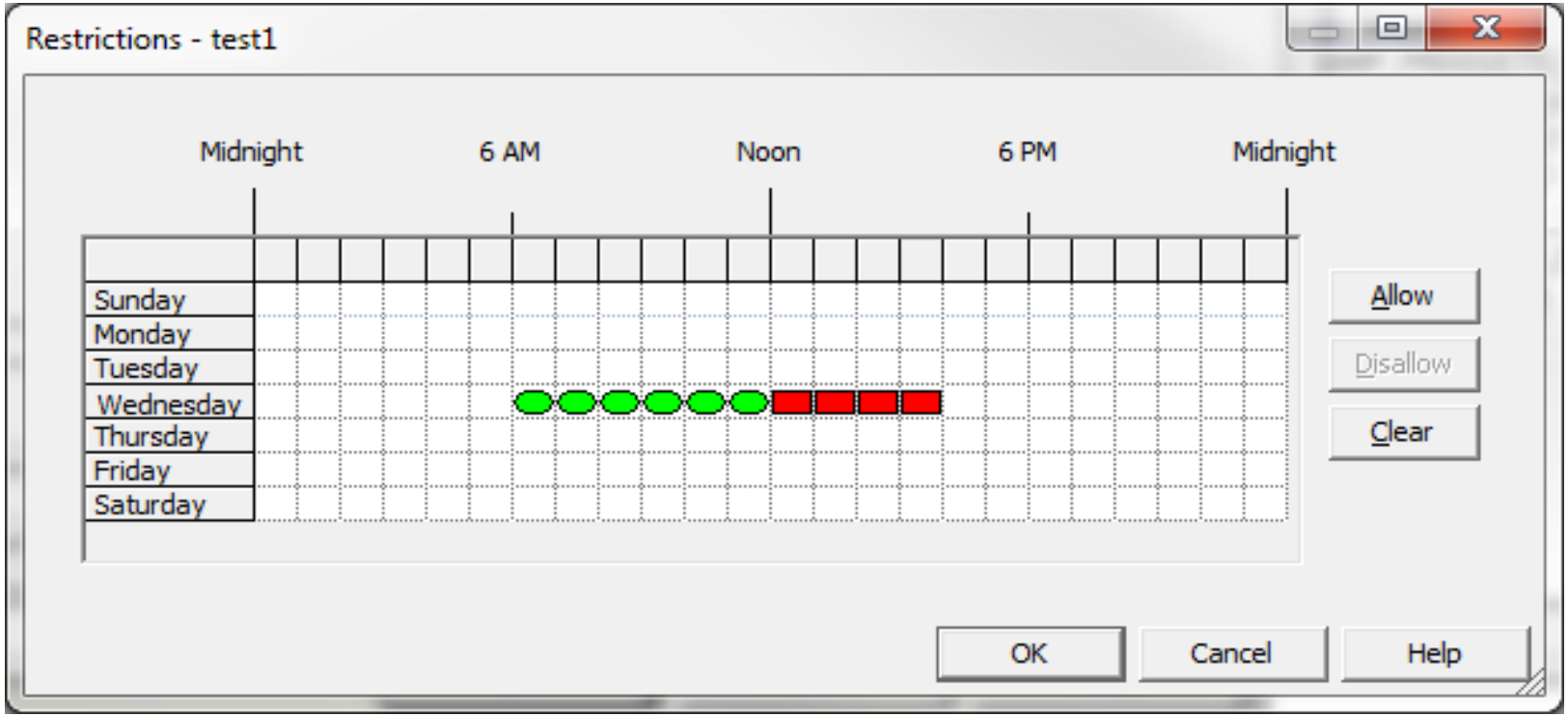
	Act-As	Impersonate
Level of access	Full or read-only access, on a single user	Full access
Users whose identity can be assumed by the proxy user	Defined list of users	Any and all users, anytime
Access method	Standard functionality of UI	Construct URL manually
How to know if being used	Both proxy and Target are shown in the UI	No indication given
Security risk	Little to none	Credentials exposed in plain text when URL submitted

Log Levels and Logs

BI Component	Log File
OPMN	debug.log
OPMN	opmn.log
BI Server	nqserver.log
BI Server Query	nquery<n>.log <n>=data and timestamp for example nqquery-20140109-2135.log
BI Cluster Controller	nqcluster.log
Oracle BI Scheduler	nqscheduler.log
Useage Tracking	NQAcct.yyymmdd.hhmmss.log
Presentation Services	sawlog*.log (for example, sawlog0.log)
BI JavaHost	jh.log

- Should be part of holistic logging solution
  - WebLogic
  - OBIEE
  - Data sources
- OBIEE Logging Level
  - Set in BI Admin Tool
    - Users only, not possible for roles
  - Log Levels 0 to 7

Time Restrictions for Roles and Users

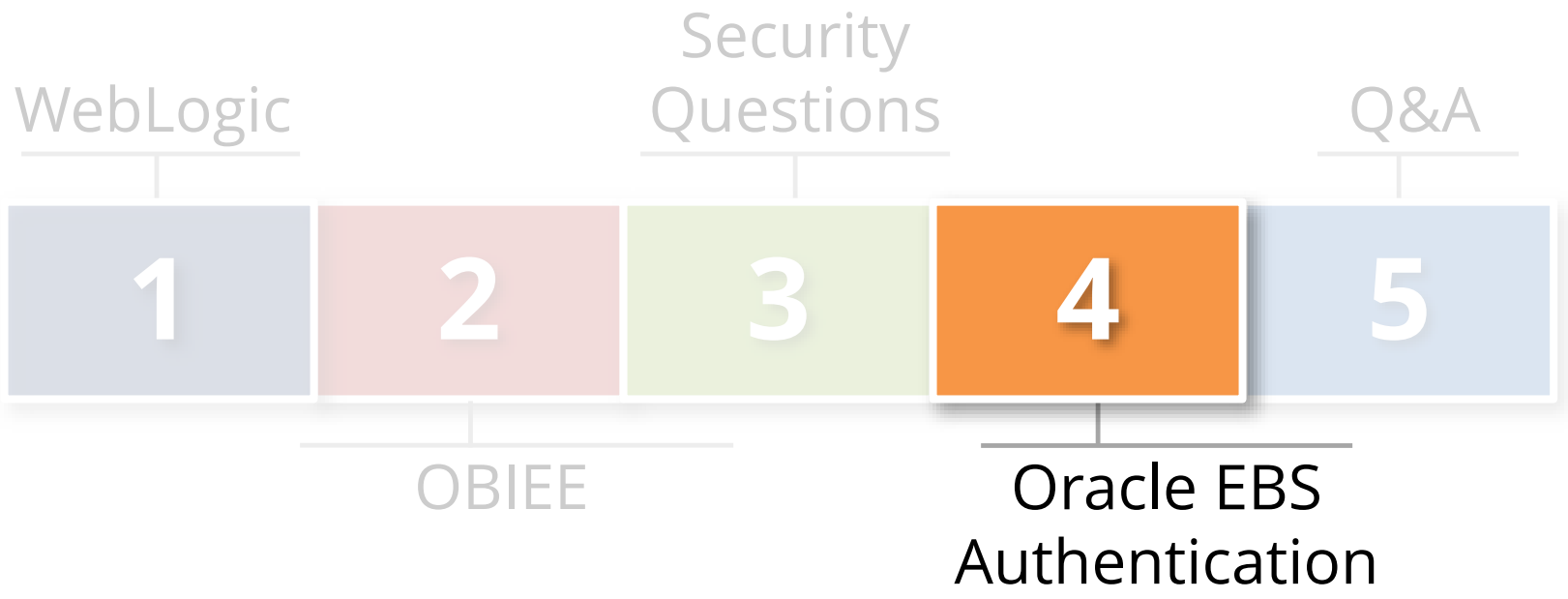


VPD, Data Vault and Row Level Security

- **Is a connection with VPD or Data Vault being used?**
  - What are the rules?

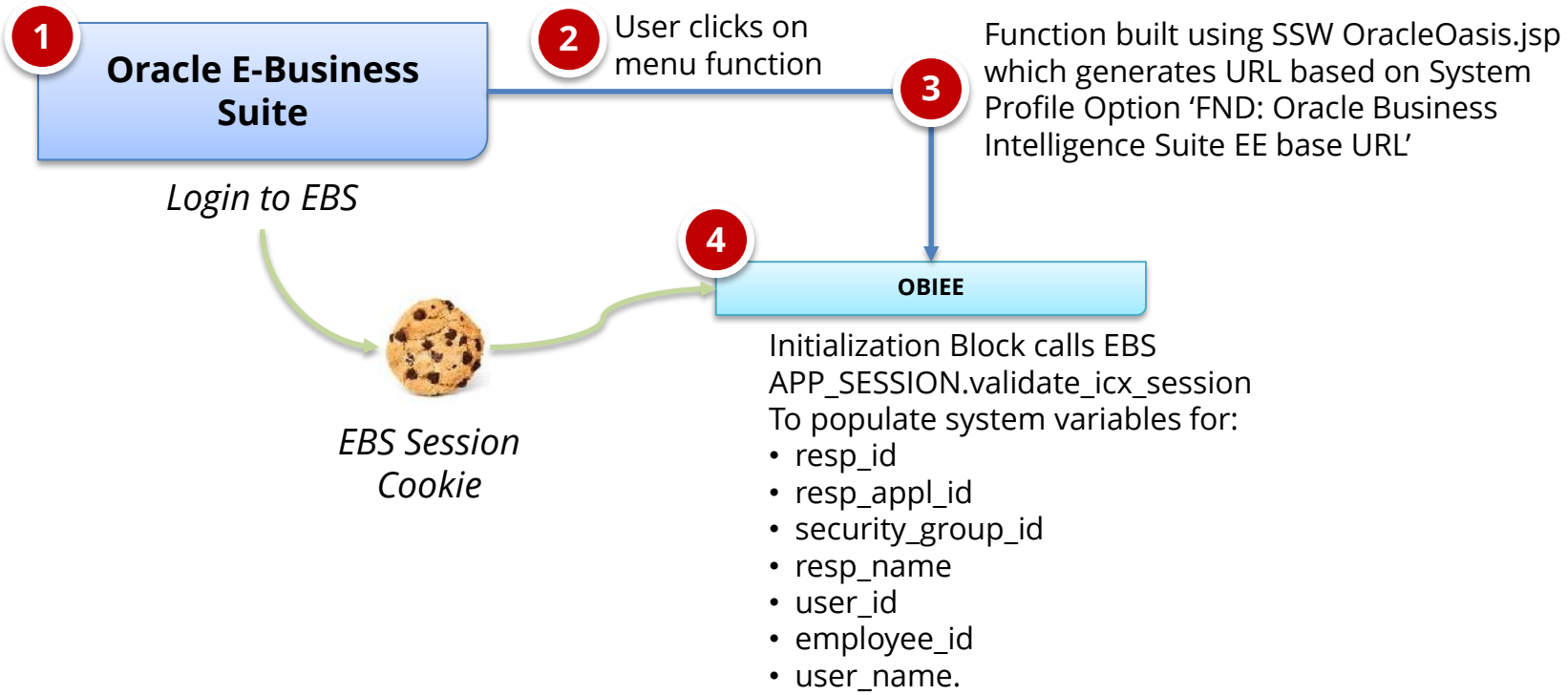
- **Which is better VPD, Data Vault or OBIEE row level security?**
  - VPD and Data Vault protect data at the data source
    - Is OBIEE the only consumer or user?

Agenda

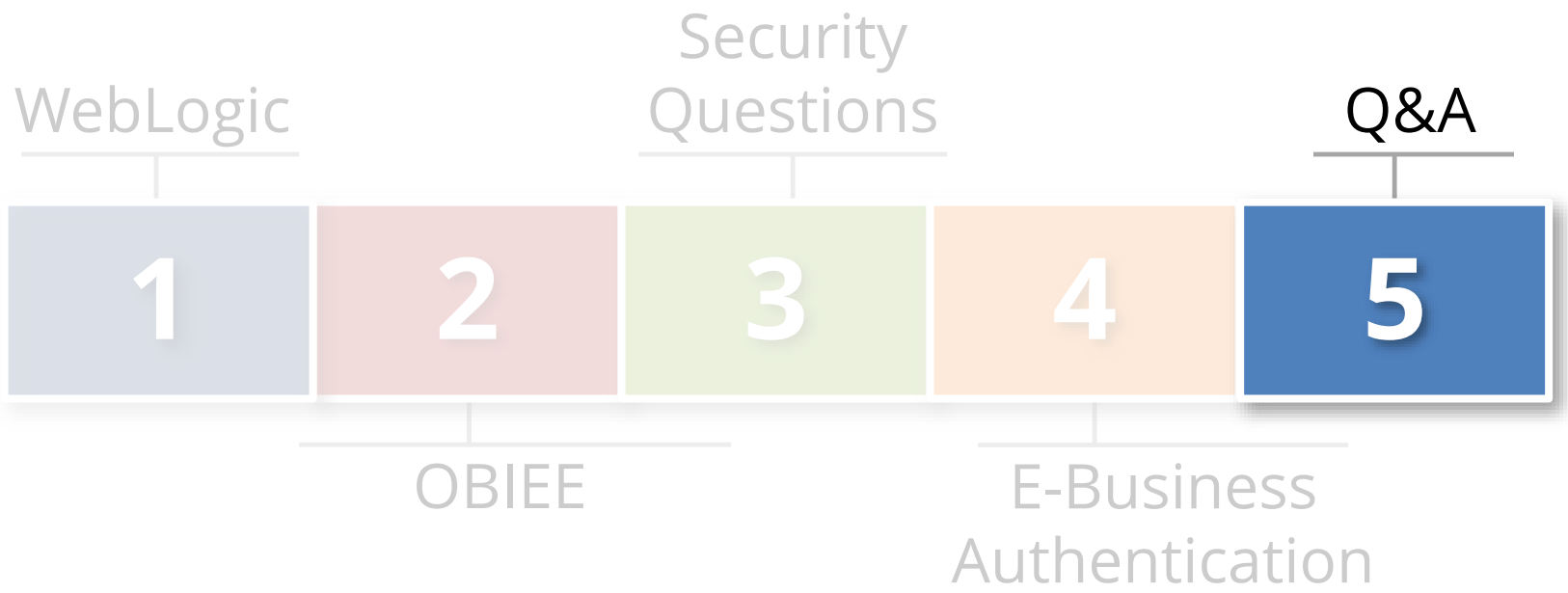

WebLogic
Security Questions
Q&A
1
2
3
4
5
OBIEE
Oracle EBS Authentication

Oracle E-Business Suite Authentication

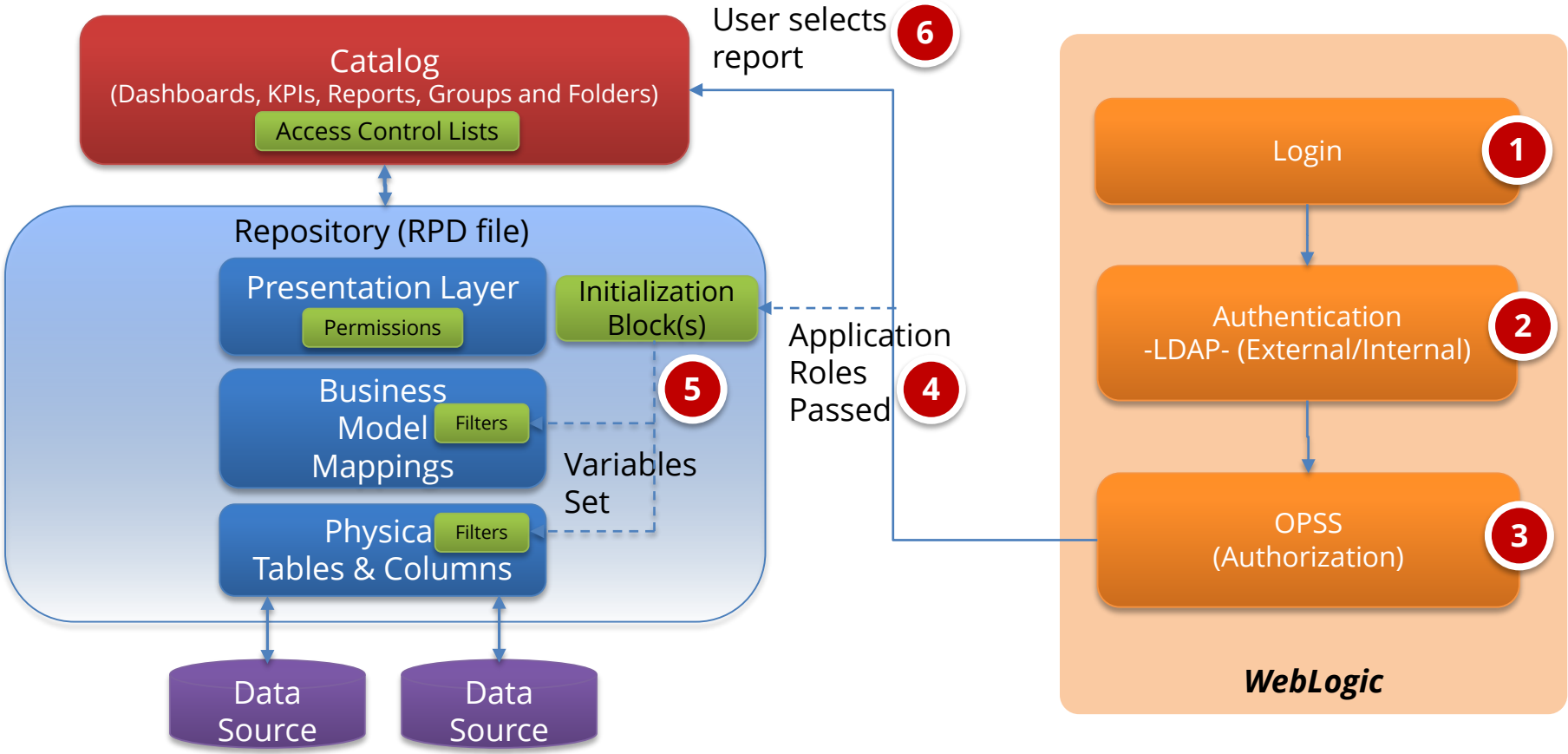
Access through E-Business not SSO



Agenda


WebLogic
Security Questions
Q&A
1
2
3
4
5
OBIEE
E-Business Authentication

OBIEE Security



Come See Us At Collaborate 2014

- **Oracle Security Vulnerabilities Dissected**
  - #526 Wednesday, April 9, 11:00am
- **New Security Features in Oracle E-Business Suite 12.2**
  - #14365 Friday April 11, 9:45am
- **OBIEE Security Examined**
  - #14366 Friday, April 11, 12:15pm

Contact Information

Mike Miller

Chief Security Officer

Integrigy Corporation

web: www.integrigy.com

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**