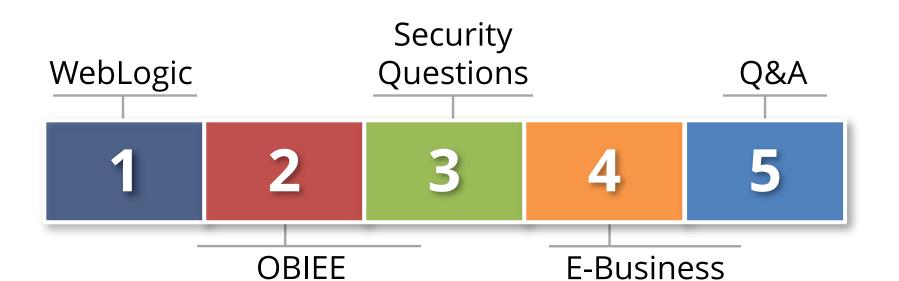


## Oracle Business Intelligence Enterprise Edition (OBIEE) Security Examined

March 19, 2014

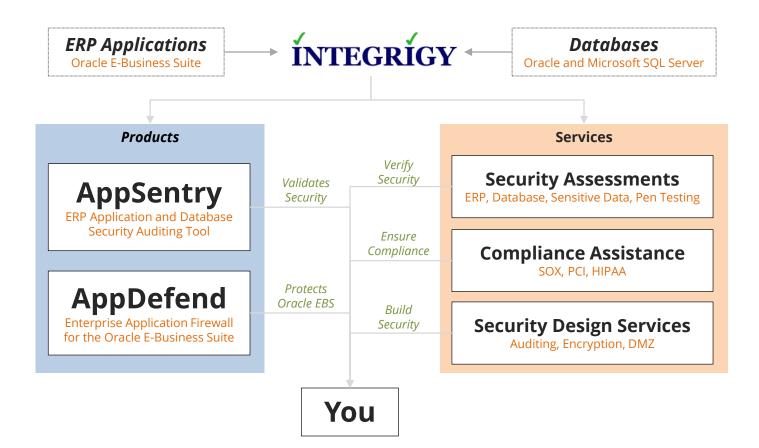
Mike Miller Chief Security Officer Integrigy Corporation Stephen Kost Chief Technology Officer Integrigy Corporation Phil Reimann Director of Business Development Integrigy Corporation



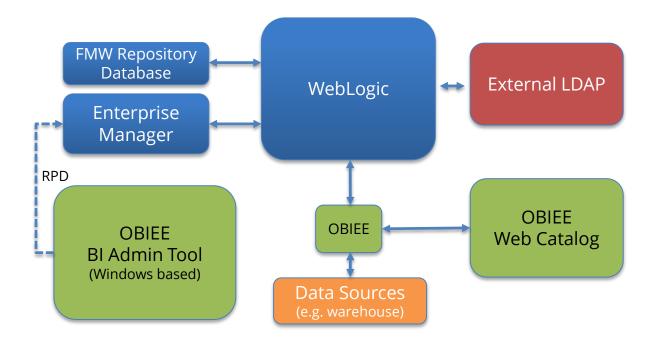


Authentication

## About Integrigy

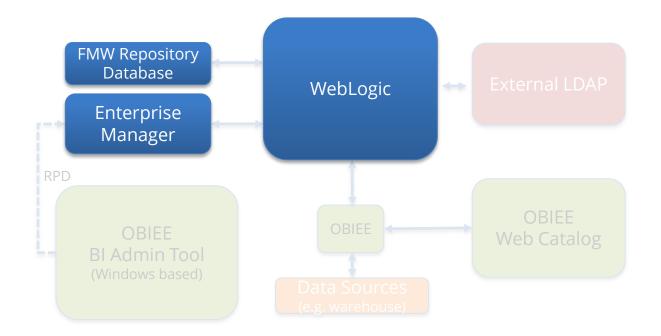


## **OBIEE** Security Examined



Size of box proportionate to component's impact on security

## Agenda



## 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

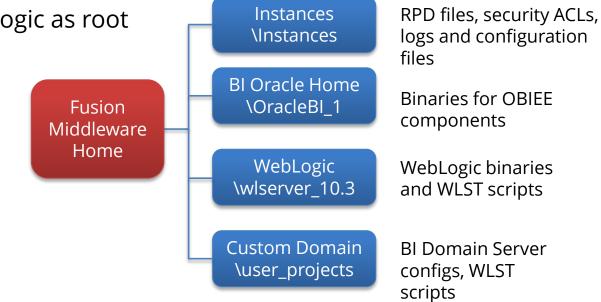
- Released May 2011
- Grace period ended August 2013

# • 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

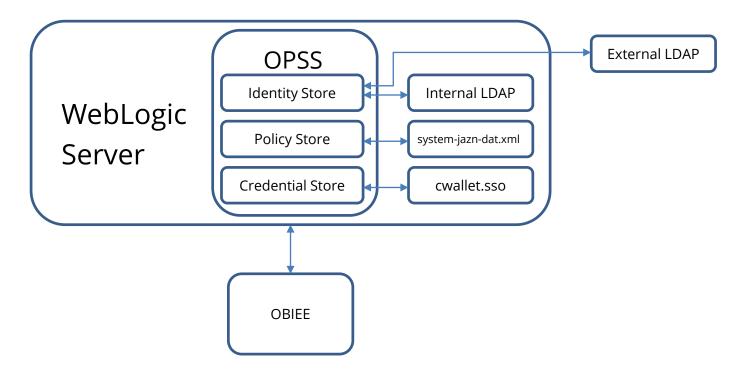
- Common security model included
- Significant change from OBIEE 10g
- WebLogic common security defined through security realms. Realms define:
  - Users
  - Groups
  - Security roles and policies

#### 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

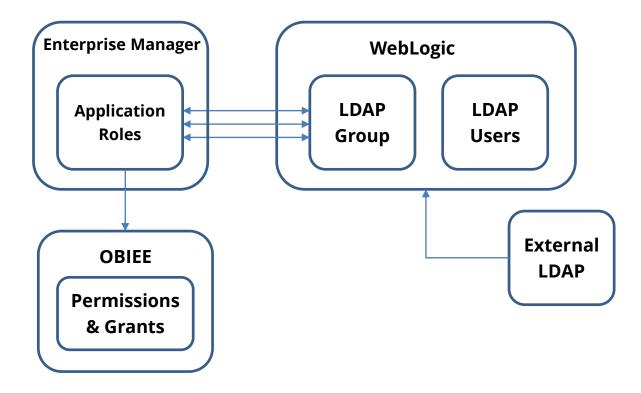
- Connect using administration port
- Use appropriate WebLogic accounts for WLST scripting
- Do not hardcode credentials
- Do not expose encrypted attributes
  - E.g. listCred()

## WebLogic Auditing

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

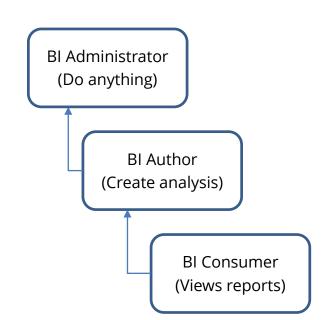
- Common audit record format
- Write audit data to:
  - Database
  - File
- Use audit data in
  - BI Publisher
  - Splunk, ArcSight etc....

## Applications Roles

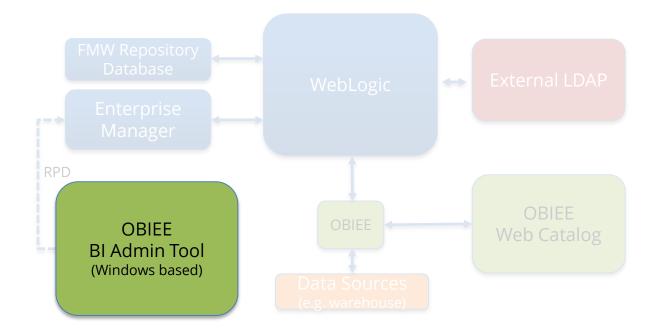


## **Application Roles**

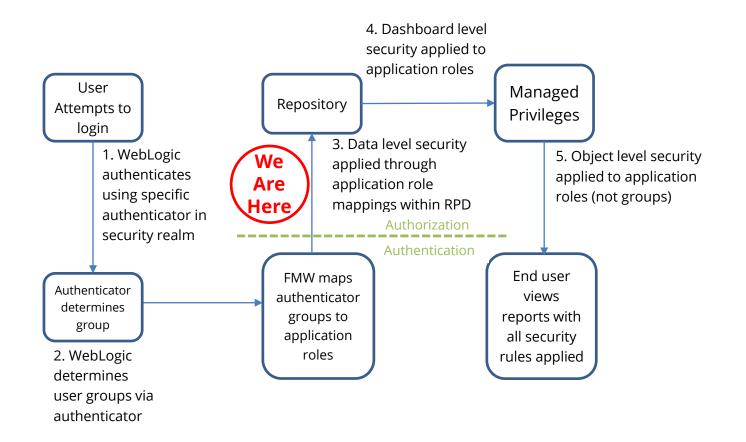
- Transcend <u>ALL</u> Fusion Products
- Defined in Enterprise Manager
- Map to LDAP groups
  - External or internal
- Key Decision:
  - Use default or custom



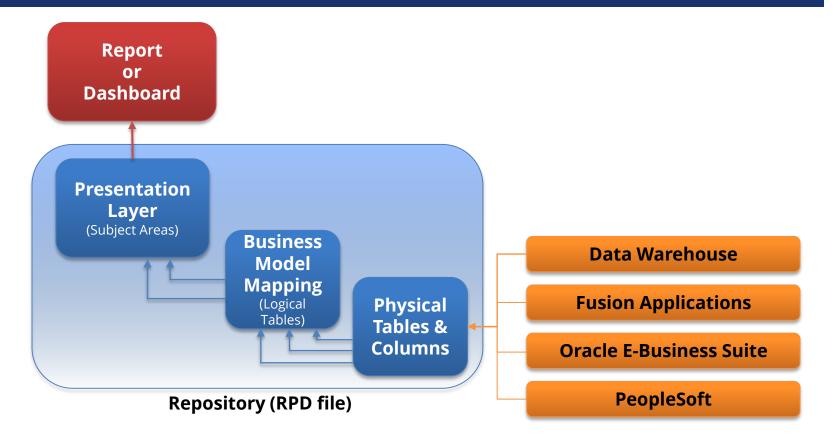
## Agenda



## Where Are We?



## **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

| Presentation   | Business Model and Meaping  | Physical   |
|--|---|--|
| Image: Samuela Sages Lis       Image: Samuela Samuela Sages Lis       Image: Samuela Samuela Sages Lis       Image: Samuela S | R= 100     File       B= 100     H2 (Inne       B= 100     H2 (Inne)       B= 1 | Product State       Same Ang. Unit Data         Call Same Ang. Unit Data       Total State         Difference       Difference         Difference       Difference |
| Subject areas  | Logical tables  | Physical tables  |

## **RPD** Security

#### Need to Secure RPD files

- Data source connection passwords
- Security rules and filters

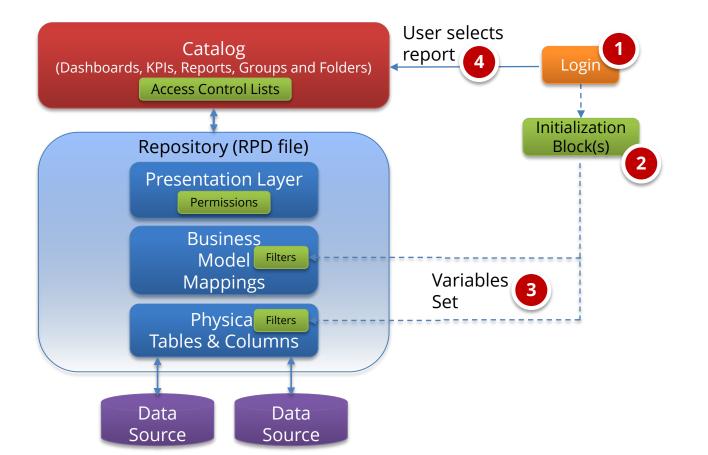
#### Password to open

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

- 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

## Initialization block

 Set variables (repository & session) when a user connects

# Two types of session variables

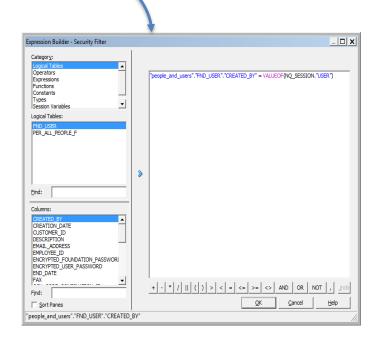
- System: reserved names e.g. USER
- Non-system: defined by author of RPD e.g. EBS\_RESP\_ID

| ~ -   |   | 1      | 1                | 1   |  |
|---|---|--------|------------------|---|--|
| Pepository         Initialization Blocks         Image: Peroperturbation Block | Name<br>EBS_RESP_ID<br>EBS_RESP_APPL_ID<br>EBS_SEC_GROUP_ID<br>EBS_RESP_NAME<br>EBS_USER_ID<br>EBS_LUSER_ID<br>USER | Descri | Default Initiali | Initialization Block<br>ebs_connect<br>ebs_connect<br>ebs_connect<br>ebs_connect<br>ebs_connect<br>ebs_connect<br>ebs_connect |  |

| ect Arear       | Sample.App Life | Total Files: 0   | 🔶 🗶 🕴  | à 🗓 🗖                   | \$ 3                |
|-----------------|-----------------|--|--------|-------------------------|---------------------|
| ne              | layer           | Name   | Status | Data F                  |                     |
| <sup>n</sup> ca |                 | Tarcets Life" Frocuds " Dran<br>e to add an opect and set filler |        | ampiertap Lte", "D1 Fra | ducts"."Product Nur |
| 1               | Uccre           | e to apo an colect and set tille.                                | 1      |                         |                     |
|                 |                 |  |        |                         |                     |
|                 |                 |  |        |                         |                     |
|                 |                 |  |        |                         |                     |
|                 |                 |  |        |                         |                     |
|                 |                 |  |        |                         |                     |

#### **Example**

Filter for Oracle E-Business Suite Set RESPONSIBILITY\_ID = 200 to see only hourly employees



# Be careful of caching with session variables and VPD DBMS\_SESSION.SET\_IDENTIFIER

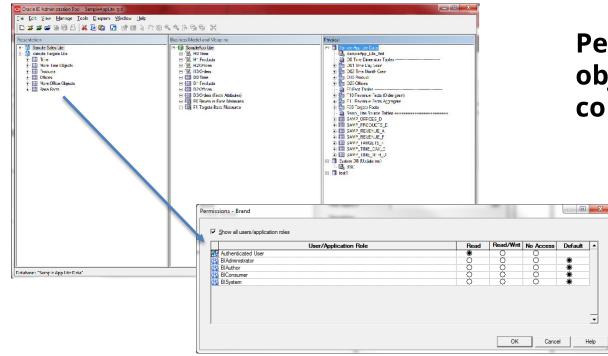
| Session Variable - favorite_color |          |
|-----------------------------------|----------|
| Name. Favorite_color              |          |
| Enable any user to set the value  |          |
| Initialization glocis             | ▼ New    |
| ,<br>Default <u>I</u> nitializer: |          |
|                                   |          |
| Description                       |          |
|                                   | <u>^</u> |
| OK Cance                          |          |
|                                   |          |

#### Session Variable

#### Connection

| Display Folders Database Properties<br>General Features Connection Poor<br>me: Vis121 ebusiness<br>Database type: Oracle 110<br>CBM metadata table<br>Persist connection pool<br>not assigned <u>Jecure</u> Clear<br>Allow populate gueries by default<br>Allow direct database requests by default<br>scription: |    |
|---|----|
| me: Vis121 ebusiness<br>Data source definition<br>Database type: Orade 110<br>CgM metadata table Virtual Private Database<br>Persist connection pool<br>not assigned <u>Qecure</u> Clear<br>Allow populate gueries by default<br>Allow direct database requests by default  |    |
| Data source definition Database type: Oracle 110 CBM metadata table Persist connection pool not assigned Allow populate gueries by default Allow direct database requests by default  | 15 |
| Data source definition Database type: Oracle 110 CBM metadata table Persist connection pool not assigned Allow populate gueries by default Allow direct database requests by default  |    |
| Database type: Oracle 110<br>CQM metadata table Virtual Private Database<br>Persist connection pool<br>not assigned <u>2ccm</u> Clear<br>Allow populate gueries by default<br>Allow direct database requests by default   |    |
| CBM metadata table Virtual Private Database<br>Persist connection pool<br>not assigned <u>2cccc</u> Clear<br>Allow populate gueries by default<br>Allow direct database requests by default   |    |
| Persist connection pool<br>not assignedClear<br>Allow populate gueries by default<br>Allow direct database requests by default  | -  |
| not assignedClear<br>Allow populate gueries by default<br>Allow direct database requests by default   |    |
| not assignedClear<br>Allow populate gueries by default<br>Allow direct database requests by default   |    |
| Allow populate gueries by default<br>Allow direct database requests by default  |    |
| Allow direct database requests by default   |    |
| Allow direct database requests by default   |    |
|   |    |
| scription:  |    |
|   |    |
|   | _  |
|   | -  |
|   |    |
|   |    |
| OK Cancel   | -  |

## **Object Level Security**

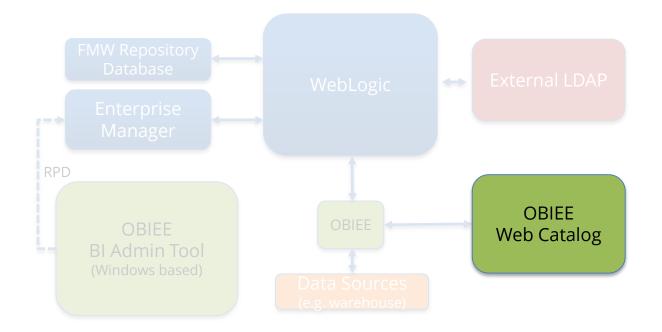


**Permissions for** object, row and column security

-

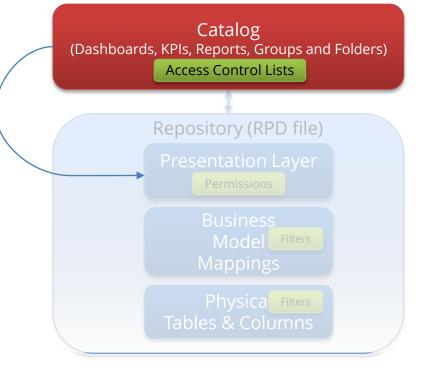
Help

## Agenda



## **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**

| c Edit View Tools Help  |                               |        |                 |               |   |        |
|---|-------------------------------|--------|-----------------|---------------|---|--------|
| K 眭 作   3 00 的 h  |                               |        |                 |               |   |        |
| Tree 🛛 👘 👘  | Table 🛛                       |        |                 |               |   | 5      |
| <ul> <li>Catalog Root</li> <li>Shared Folders</li> </ul>  | /system/privs                 |        |                 |               |   | • [Go  |
| a System Lolders<br>bookmarks   | Name                          | lype   | Owner           | My I'cmis     | Attributes  | Date   |
| bookmaps  | C ActionPrivs                 | Folder | System Ac.      | Read, Troy    |   | Sep D  |
| content ists  | Admin SystemPrivs             | lolder | System Ac.      | tead I rev    | Attributes         J           ov         S           ov         S           ac         S           ac | Sep D  |
| devices   | C AletsSystemPrivs            | Folder | System Ac.      | Read Traves   |   | Sep 10 |
| and the second se | BriefingBookPrivs             | Folder | System Ac.      | Read Traville |   | Sep 10 |
| disconnected  | Catalog                       | Folder | System Ac.      | Read Trav     | Hidden, Sy  | Dec 6  |
| intracats   | atalogsystemprivs             | Folder | System Ac.      | Read Trav     |   | Sep 10 |
| mktodefaults  | ConditionPrivs                | Folder | System Ac.      | Read, Frey    |   | Sep 1  |
|   | DashboardSystemPrivs          | lolder | System Ac.      | Read, Litery  |   | Sep D  |
|   | EnmalSystemPrivs              | Folder | System Ar       | Read Travia   |   | Sep 16 |
| products<br>security  | 📋 generalprivs                | Folder | System Ac.      | Read Trav     |   | Sep 10 |
| securey   | 🗀 home                        | Folder | System Ac.      | Read Trav     |   | Sep 1  |
| <ul> <li>spatialmetadata</li> </ul>   | 📋 MarketingSystemExportFormat | Folder | System Ac       | Read Trav     |   | Sep 1  |
| User Folders  | MarketingSystem segmentatio   | Folder | System Ac.      | Read, Fray    |   | Sep 10 |
| Diser Policers  | MyAccountPrive                | Folder | System Ac.      | Read Trav     |   | Sep 10 |
|   | DrawyPrice 1                  | Folder | System Ar.      | Read Trev.    |   | Sep 16 |
|   | C Rss Privs                   | Folder | System Ac.      | Read Trav     |   | Sep 10 |
|   | 🗀 SA. 'AtomicStar'            | Folder | System Ac.      | Read, Trav    |   | Sep 1  |
|   | SA 'AutoSnowflakeSoles'       | Folder | System Ac.      | Read, Trav    |   | Sep 10 |
|   | 🔒 SA. 'CecheSecurity Lesting' | lolder | System Ac       | Itead, I revi |   | Sep 10 |
|   | 🛄 SA. 'DimSnowflak +Sales '   | Folder | System Ar       | Read Traves   |   | Sep 10 |
|   | SA. 'FilteredMetricsTesting'  | Folder | System Ac       | Read, Travill |   | Sep 10 |
|   | SA 'Foodmart'                 | Folder | System Ac       | Read, Trav    |   | Sep 10 |
|   | 🗀 S/L 'Interop'               | Folder | System Ac       | Read, Trav    |   | Sep 10 |
|   | 📋 SA. 'OpaqueFoodmart'        | Folder | System Ac.      | Read, Frew    |   | Sep 10 |
|   | SA. 'OpaquePNGDemo'           | Folder | System Ac.      | Read Travia   |   | Sep 10 |
|   | 54. 'people_and_uses"         | Folder | System Ar       | Read, Travia  |   | len 24 |
|   | 🛄 SA. "pepole_and_users"      | Folder | System Ac       | Read, Trav    |   | Jan 24 |
|   |                               | 10     | 2.2.2. CONSIGCO | -             |   | F      |

## **Presentation Catalog Reports**

 Catalog reports are critical feature

 Export to Excel for analysis and reporting

| Select type to report on Security | ACL |   | • D | istinct |
|-----------------------------------|-----|---|-----|---------|
| Available Columns                 | ×   | Columns in Report<br>ACL<br>Accounts<br>Caption ID<br>Created<br>Creator<br>Description ID<br>Folder<br>Modified<br>Modifier<br>Must Have Permission<br>Must Have Permission<br>Must NOT Have Permission<br>Must NOT Have Permission<br>Must NOT Have Privilege<br>Name<br>Owner<br>Path<br>Privilege<br>Signature<br>Tag |     | •       |

## Presentation Catalog Security

Administration Rights also set with ACLs
 Security ACL is very important

| Administration                 |  |   |  |
|--------------------------------|--|---|--|
| Manage Privileges              |  |   |  |
| This page allows you to view a | and administer privileges associated with various components o | of Oracle Business Intelligence.  |  |
|                                | 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                         | 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  |  |
|                                | Create Navigate Actions  | BI Consumer Role  |  |
| Actions                        | Create Invoke Actions  | BI Author Role  |  |
|                                | Save Actions containing embedded HTML                          | BI Administrator Role   |  |
| Admin: Catalog                 | Change Permissions   | BI Author Role  |  |
| numini: Catalog                | Toggle Maintenance Mode  | BI Advisionator Role  |  |
|                                | 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   |  |
| Admin: General                 | Manage Agent Sessions  | BI Administrator Role   |  |
|                                | Manage Device Types  | 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





## 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



| 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<br>administration user(s) | End-user(s) with full Administration rights to WebLogic   |
| BI Admin User                      | Seeded end-user with full Administration rights to OBIEE  |
| Bl 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                          | <ul> <li>Connection pools can be flagged to allow users to update the database</li> <li>Who can and to what?</li> <li>Can they also issue Direct SQL?</li> </ul> |
|--------------------------------------|--|
| Security configurations & migrations | <ul> <li>How are OPSS (policies and credentials)<br/>migrated from non-production to<br/>production?</li> <li>GUI or WLST?</li> </ul>                            |
| Source code control                  | <ul><li>Are RPD files under source code control?</li><li>Are XML exports being used?</li></ul>   |

## Ask For RPD Permission Reports

| Ovacle Li Administration ( look - versonul bon/20en_voureq4_unfund | _1                    |   |
|--|-----------------------|---|
| File Edit View Manage Tools Diagram Window Help                    | i l                   |   |
|  | 8                     |   |
| Presentation Business Model and Mepping                            | F T/SICB              |   |
| Presentation Table "people" of Users", MET VIT SCOPELT.            |                       | Same As     Image: Same decider/Why_VM (Wybowsho) (E)     Image: Same decider/Whyb_VM (Wybowsho) (E)     Image: Same decider/Whyb_VM (Wybowsho) (E)     Image: Same decider/Whybowsho) (E)     Image: Same decid |
|  |                       |   |
| Permission Report  |                       | TX Flangame: V Save   |
| Type Name  | Description           | Save as lyter Comma Separated Values ("csv) ▼ Concel  |
| Subject Area "people_and_users"                                    |                       |   |
| User/Application Role Read Read/Write                              | No Access Description | Grooding: IITF-8  |
|  | Save As               | Note: Permission repo<br>NOT include BMM or l   |

orts do hysical 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:**

| ORACLE Business Intelligence   |
|--|
| Administration   |
| Issue SQL  |
| Enter a SQL statement to issue directly against the Oracle BI Server. This page is for testing the Oracle BI Server on   |
| update hr.per_pay_proposals ppg<br>set ppa.proposed_salary_n = 1000000<br>where exists (select 1<br>from per_assignment_x pax, per_people_x ppx<br>where pax.person_id = ppx.person_id<br>and pax.assignment_id = ppa.assingment_id<br>and ppx.full_name = 'Fred Elintsone') |
| Issue SQL Oracle BI Server Logging Level Default 🔻 🗹 Use Oracle BI Presentation Services Cache   |

- 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

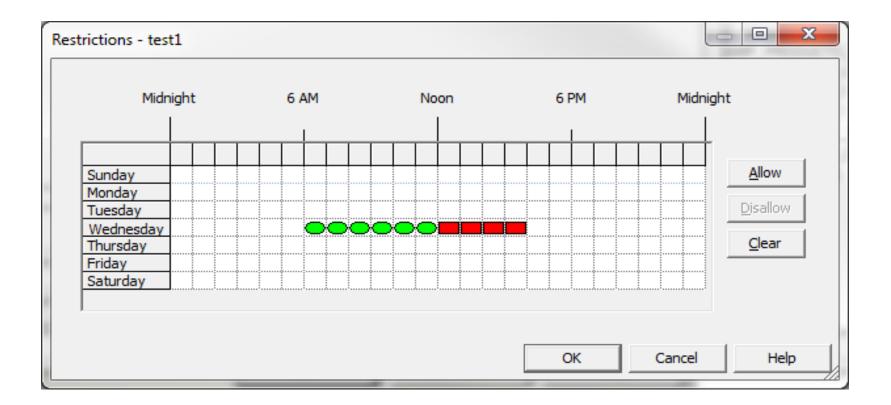
|   | Act-As                                     | Impersonate   |
|---|--|---|
| Level of access   | Full or read-only access, on a single user | Full access   |
| Users whose identity can<br>be assumed by the proxy<br>user | Defined list of users                      | Any and all users, anytime                              |
| 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<br>text when URL submitted |

# Log Levels and Logs

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

- Should be part of holistic logging solution
  - WebLogic
  - OBIEE
  - Data sources
- OBIEE Logging Level
  - Set in Bl 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?

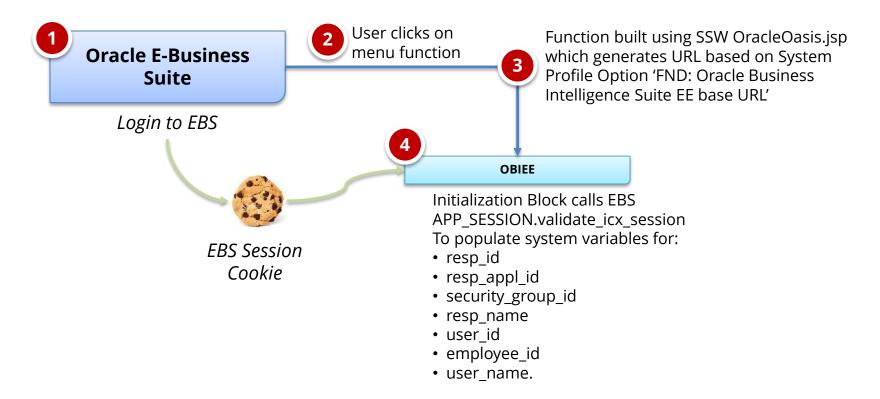




# Authentication

#### **Oracle E-Business Suite Authentication**

#### Access through E-Business not SSO



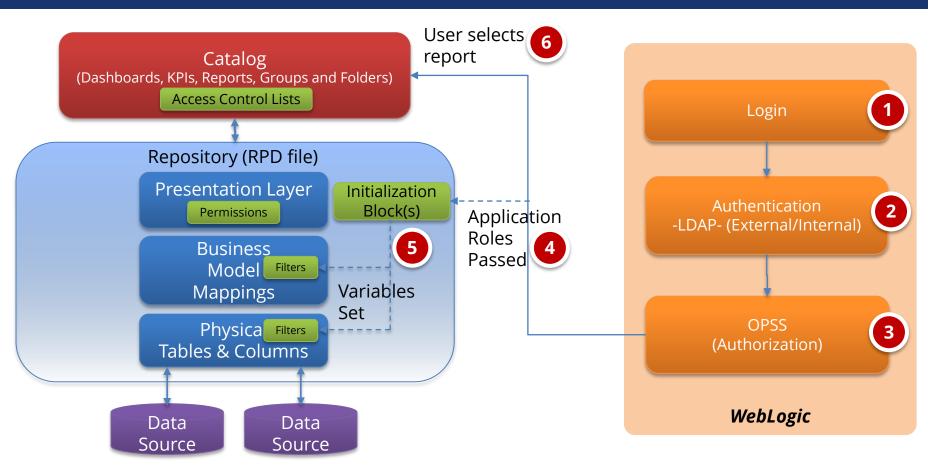






E-Business Authentication

## **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