

# BIEE 11G 培训

## 主题: BIEE Security

编写人: 罗勇  
编码: GJZQ\_BI  
编写日期: 2011-07-02  
版本: 1.0



汉得信息技术有限公司  
HAND Enterprise Solutions Company Ltd.  
[www.hand-china.com](http://www.hand-china.com)





## BIEE - 安全性

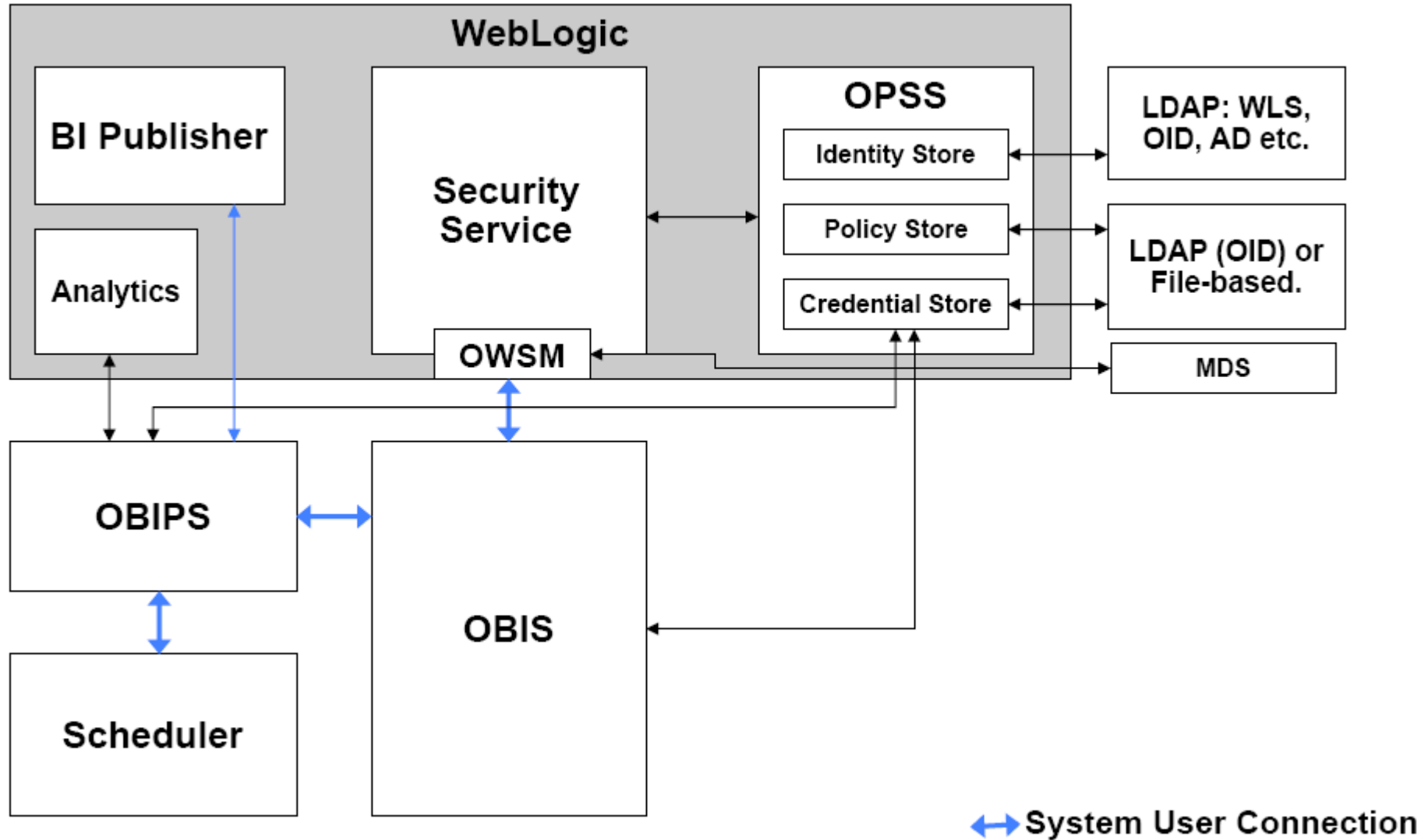
- 安全体系架构
- 支持的安全认证配置
- System Users 与Credential Store( 身份证明)
- 数据安全
- 目录安全



# BIEE - 安全性

- 安全体系架构
- 支持的安全认证配置
- 配置SSO单点登录
- System Users 与Credential Store( 身份证明)
- 数据安全与目录安全

## BIEE - 安全架构





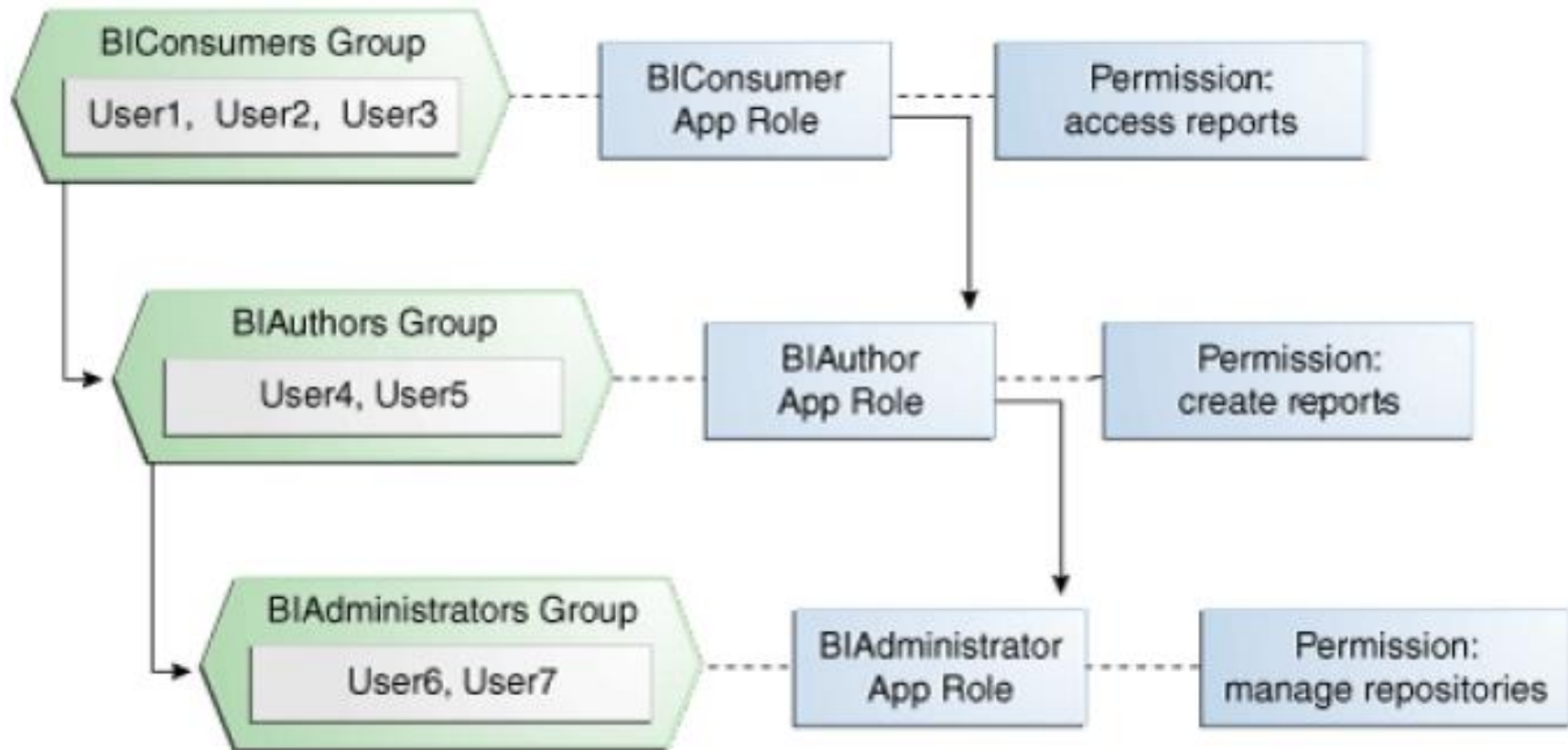
# BIEE - 安全架构

- Identity store 身份存储  
包含定义的用户，组和组的层级关系。
- Policy store 策略存储  
包含应用程序的角色定义，权限授予的角色，和成员（用户，组，和应用程序角色）的角色。
- Credential store 身份证明  
存储与安全相关的凭据，如用户名和密码组合，用于访问外部系统，如数据库或LDAP服务器




# BIEE - 安全基本概念

## ■ 默认的应用程序角色(App role)层次




# BIEE - 安全基本概念

## ■ 默认的应用程序角色(App role)层次

**coreapplication** ⓘ  
 Business Intelligence Instance ▼

### Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These role accessing the application.

 To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).


#### Policy Store Provider





Scope WebLogic Domain  
 Provider XML  
 Location ./system-jazn-data.xml

#### Search

Enter search keyword for role name to query roles defined by this application. Use application stripe to search

Select Application Stripe to Search ☒ obi ▼

Role Name  

 Create...  Create Like...  Edit...  Delete...

Role Name	Members	Description
<a href="#">BISystem</a>	BISystemUser	
<a href="#">BIAdministrator</a>	BIAdministrators	
<a href="#">BIAuthor</a>	BIAuthors, BIAdministrator	
<a href="#">BIConsumer</a>	BIConsumers, Users, rkalavz, BIAuthor, authenti	
<a href="#">newrole</a>	BIConsumers, BIAuthors	
<a href="#">Users</a>	mzanchel	

# BIEE - 安全基本概念

## ■ 默认的应用程序角色策略

Create... Create Like... Edit... Delete...	
Principal	Permission
BIAdministrator	oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.server.permission,resourceName=oracle.bi.server.manageRepositories _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.scheduler.permission,resourceName=oracle.bi.scheduler.manageJobs _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.presentation.catalogmanager.permission,resourceName=oracle.bi.presentation.catalogmanager.manageCatalog _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.publisher.permission,resourceName=oracle.bi.publisher.administerServer _all_) oracle.security.jps.ResourcePermission ( resourceType=epm.calcmgr.permission,resourceName=EPM_Calc_Manager_Administrator _all_) oracle.security.jps.ResourcePermission ( resourceType=epm.fr.permission,resourceName=oracle.epm.financialreporting.administerReporting _all_) oracle.security.jps.ResourcePermission ( resourceType=rtd_ils,resourceName=_all_ open_service:read,open_service:write ) oracle.security.jps.ResourcePermission ( resourceType=rtd_dc_persp,resourceName=_all_dc_perspective ) oracle.security.jps.ResourcePermission ( resourceType=rtd_ils,resourceName=_all_deploy_service ) oracle.security.jps.ResourcePermission ( resourceType=rtd_ils,resourceName=_all_download_service ) oracle.security.jps.ResourcePermission ( resourceType=rtd_batch,resourceName=_all_batch_admin ) oracle.security.jps.ResourcePermission ( resourceType=rtd_ils,resourceName=_all_choice_editor ) oracle.security.jps.ResourcePermission ( resourceType=rtd_ils,resourceName=_all_decision_service:normal,decision_service:stress )
BISystem	oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.scheduler.permission,resourceName=oracle.bi.scheduler.manageJobs _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.server.permission,resourceName=oracle.bi.server.manageRepositories _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.server.permission,resourceName=oracle.bi.server.impersonateUser _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.server.permission,resourceName=oracle.bi.server.queryUserPopulation _all_)
BIConsumer	oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.publisher.permission,resourceName=oracle.bi.publisher.accessExcelReportAnalyzer _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.publisher.permission,resourceName=oracle.bi.publisher.accessOnlineReportAnalyzer _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.publisher.permission,resourceName=oracle.bi.publisher.runReportOnline _all_) oracle.security.jps.ResourcePermission ( resourceType=oracle.bi.publisher.permission,resourceName=oracle.bi.publisher.accessReportOutput _all_)





# BIEE - 安全性

- 安全体系架构
- 支持的安全认证配置
- System Users 与Credential Store( 身份证明)
- 数据安全
- 目录安全



# BIEE - 安全认证

## ■ BIEE 11g 所支持的安全认证

	FMW Security	Init Block
✓	<p>Users and Groups in LDAP</p> <p>Certified/Supported LDAP versions as listed in published matrix:</p> <ul style="list-style-type: none"> <li>•OID (OID Authenticator)</li> <li>•OVD (OVD Authenticator)</li> <li>•AD (AD Authenticator)</li> <li>•OpenLDAP (OpenLDAP Authenticator)</li> <li>•Sun Java System Directory Server version 6.3 (iPlanet Authenticator)</li> <li>•eDirectory 8.8. (NovellAuthenticator)</li> </ul> <p>Native Weblogic LDAP (Default Authenticator)</p>	<p>All 10g authentication mechanisms other than RPD users/groups</p> <ul style="list-style-type: none"> <li>•Users in LDAP, group membership in database</li> <li>•Database Authentication</li> <li>•Custom Authenticators</li> <li>•*multiple AD Domains</li> <li>•EBS authentication</li> <li>•64bit platforms (requires patch 10395783)</li> </ul>
✗	<ul style="list-style-type: none"> <li>• SiteMinder 6 or OAM as an Authenticator</li> <li>• Group membership in a database</li> <li>• Multiple Authenticators*<sup>2</sup></li> <li>• *<sup>3</sup>Any 'Authenticator' other than those used for the list of certified LDAPs listed above plus the Default Authenticator.</li> </ul>	<ul style="list-style-type: none"> <li>• Use of Asserters and Authenticators combined with Init Block Authentication</li> <li>• BI Publisher Limitations</li> <li>• RTD</li> <li>• Delivers Limitations when using EBS authentication</li> <li>• Hyperion CSS integration</li> </ul>

\* - Not re-tested

\*<sup>2</sup> - OBIEE restriction only (BIP and RTD can use multiple authenticators)

\*<sup>3</sup> - Only those Authenticators related to Identity Stores that have an appropriate implementation of the OPSS UserRole API may be used. OBIEE restriction only (BIP and RTD can use multiple authenticators).



# BIEE - 单点登录

## ■ BIEE 11g 所支持的单点登录机制

	FMW Security	Other Authentication Schemas
1	<p>Use of most Asserters delivered in Weblogic* when combined with a supported Authenticator as listed on the previous slide.</p> <p>This includes:</p> <ul style="list-style-type: none"> <li>•OAM Asserter (but not Authenticator)</li> <li>•OSSO Asserter</li> <li>•Default Asserter (for Client Certificate Authentication)</li> <li>•NegotiateIdentityAsserter (for Windows Native Authentication without IIS)</li> </ul>	<ul style="list-style-type: none"> <li>• SSO via http header or cookie – ie. where the SSO product provides the authenticated User via an http header or cookie (requires customization of BI Config)</li> <li>• E-Business Suite ICX Cookie mechanism*<sup>2</sup></li> <li>• Windows Authentication using IIS (uses http header) (requires a patch)</li> <li>• Siteminder 6 via http header</li> <li>• &amp;NQUSER/&amp;NQPASSWORD URL parameters via get or post</li> </ul>
x	<ul style="list-style-type: none"> <li>• Use of Authenticators against SSO products rather than directly to the underlying LDAP Identity Store*<sup>3</sup></li> <li>• BI Office and Client tools and BI session-based web services are not able to use SSO, but will still work using UID/Password</li> </ul>	<ul style="list-style-type: none"> <li>• Use of Asserters and Authenticators combined with Init Block Authentication</li> <li>• SSO via URL parameter other than when using &amp;NQUSER/&amp;NQPASSWORD</li> <li>• Hyperion CSS Token</li> <li>• BI Office and Client tools and BI session-based web services are not able to use SSO, but will still work using UID/Password</li> </ul>

\* - Not all Asserters have been tested against. The SAML Asserters have not been tested or certified and may not work.

\*<sup>2</sup> - Both BI and E-Business Suite must appear to be in the same Internet Domain.

\*<sup>3</sup> - OBIEE restriction only (BIP and RTD can use additional authenticators)



## BIEE - 用户信息

- 用户配置信息，如 显示名称，语言种类，Email地址等可以从如下位置获取：
  - LDAP Attribute
  - Webcat Profile
  - Init Blocks
- GUID 也是用户信息之一



# BIEE - 安全性

- 安全体系架构
- 支持的安全认证配置
- **System Users 与 Credential Store( 身份证明)**
- 数据安全
- 目录安全



# BIEE - System User

## ■ BISystemUser

- 默认为**BISystemUser**，但可以是任何用户，用于组件之间的通信
- 用于为模拟身份证明
- 身份证明凭据用户，存储于**oracle.bi.system - system.user**
- 不需要目录组权限，但需要**Weblogic** 的管理员角色，默认是‘Administrators’ 组成员

## ■ OracleSystemUser

- 由**OWSM**使用
- 默认用户为**OracleSystemUser**，属于**OracleSystem**组成员
- 用户名可以改变，但需要做额外的修改，参考官方文档



# BIEE - Credential Store

- 身份证明存储如下信息
  - BISystemUser 身份凭据
  - Actions/OWSM 身份凭据
  - SSL 凭据及证书
  - RPD凭据
  - Web Services for SOA浏览凭据
  
- 通过EM 管理，文件名为cwallet.sso,存储于domian文件夹下
  - 不要尝试直接文本修改 cwallet.sso,里面存储有版本信息
  - 可以使用 Pyhton Scripts管理证明凭据



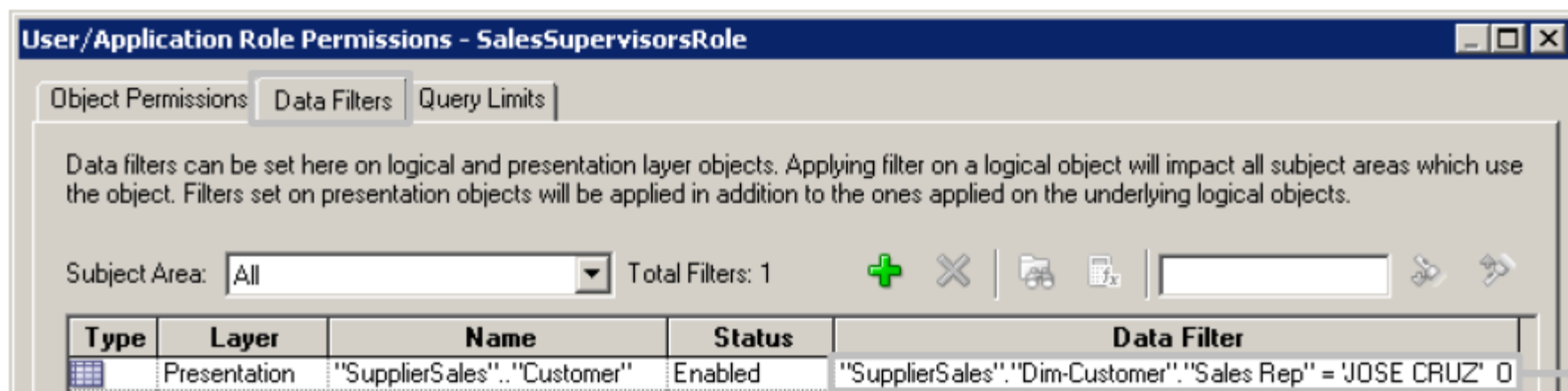
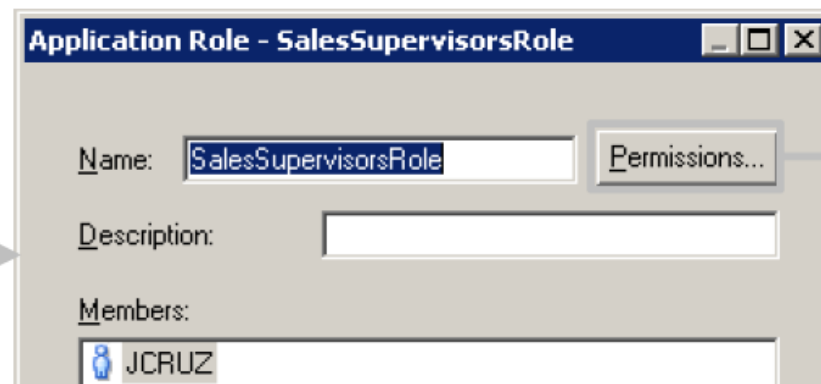
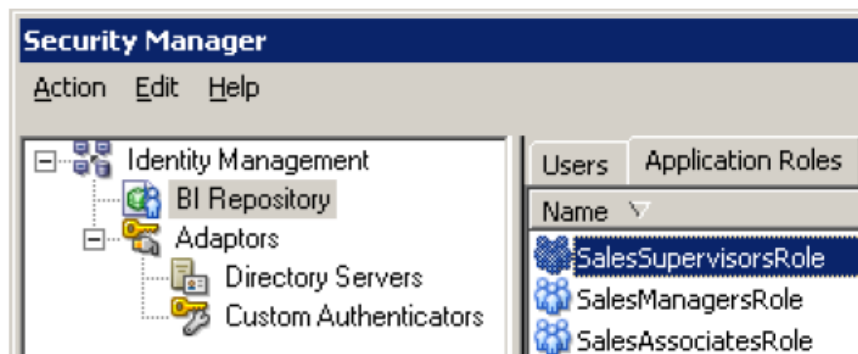
# BIEE - 数据安全

- 安全体系架构
- 支持的安全认证配置
- System Users 与Credential Store( 身份证明)
- 数据安全
- 目录安全



# BIEE - 数据安全

## ■ 设置数据筛选器





# BIEE - 数据安全

- 安全体系架构
- 支持的安全认证配置
- System Users 与Credential Store( 身份证明)
- 数据安全
- 目录安全

# BIEE - 目录安全

## ■ 管理目录安全

**ORACLE Business Intelligence** Search   Administration Help  Catalog Dashboards   Signed In As **you found me!**

**Administration**  
**Manage Privileges**

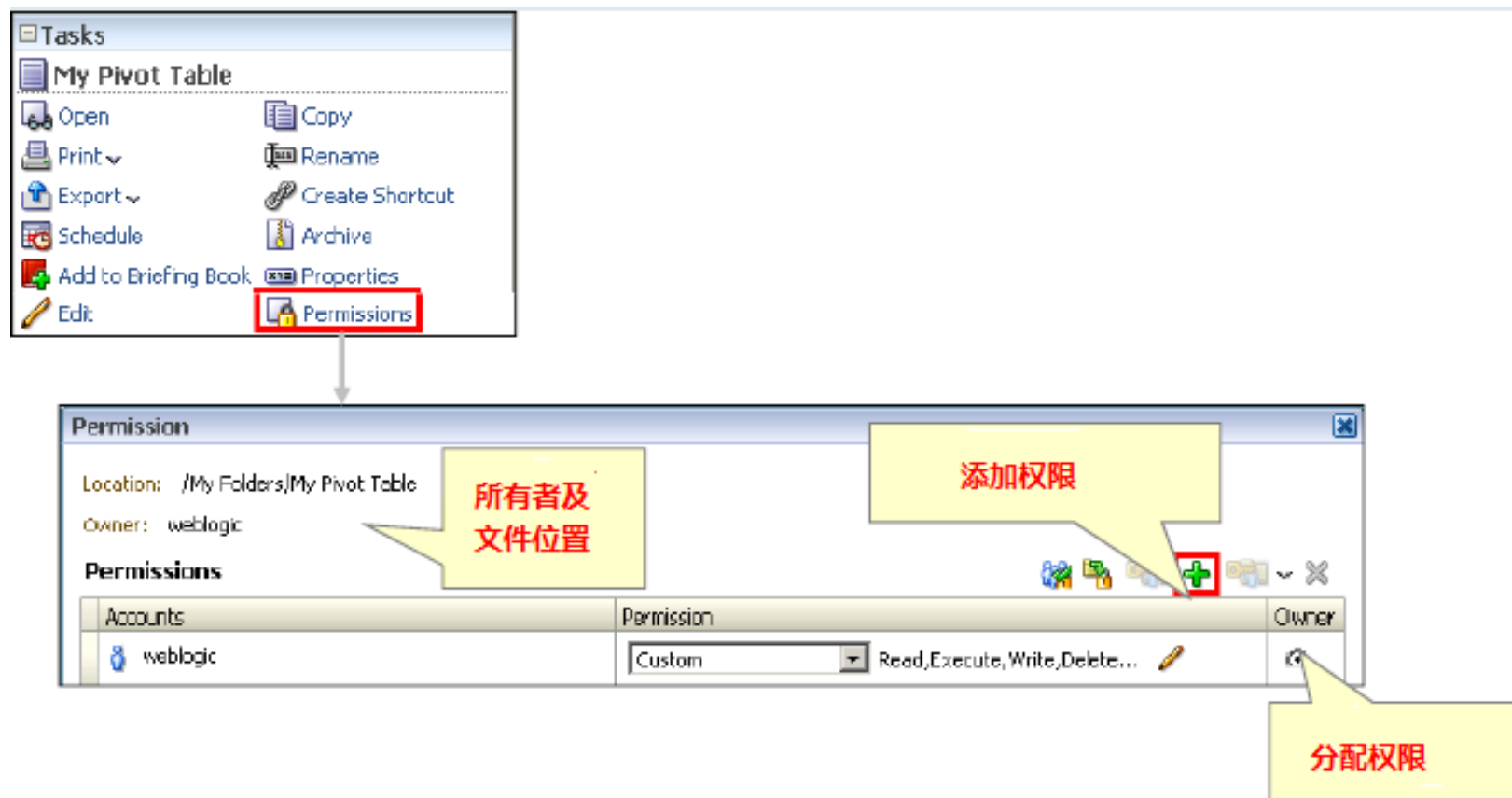
This page allows you to view and administer privileges associated with various components of Oracle Business Intelligence.

<b>Access</b>	Access to Dashboards	<a href="#">BIConsumer</a>
	Access to Answers	<a href="#">BIAuthor</a>
	Access to Delivers	<a href="#">BIAuthor</a>
	Access to Briefing Books	<a href="#">BIConsumer</a>
	Access to Administration	<a href="#">BIAdministrator</a>
	Access to Segments	<a href="#">BIConsumer</a>
	Access to Segment Trees	<a href="#">BIAuthor</a>
	Access to List Formats	<a href="#">BIAuthor</a>
	Access to Metadata Dictionary	<a href="#">BIAuthor</a>
	Access to Oracle BI for Microsoft Office	<a href="#">BIConsumer</a>
	Access to Conditions	<a href="#">BIAuthor</a>
	Access to KPI Builder	<a href="#">BIAuthor</a>
<b>Actions</b>	Access to Scorecard	<a href="#">BIConsumer</a>
	Create Navigate Actions	<a href="#">BIConsumer</a>
	Create Invoke Actions	<a href="#">BIAuthor</a>
<b>Admin: Catalog</b>	Save Actions containing embedded HTML	<a href="#">BIAdministrator</a>
	Change Permissions	<a href="#">BIAuthor</a>
	Toggle Maintenance Mode	<a href="#">BIAdministrator</a>
	Manage Sessions	<a href="#">BIAdministrator</a>
	Manage Dashboards	<a href="#">BIAuthor</a>
	See sessions IDs	<a href="#">BIAdministrator</a>

Local intranet 100%

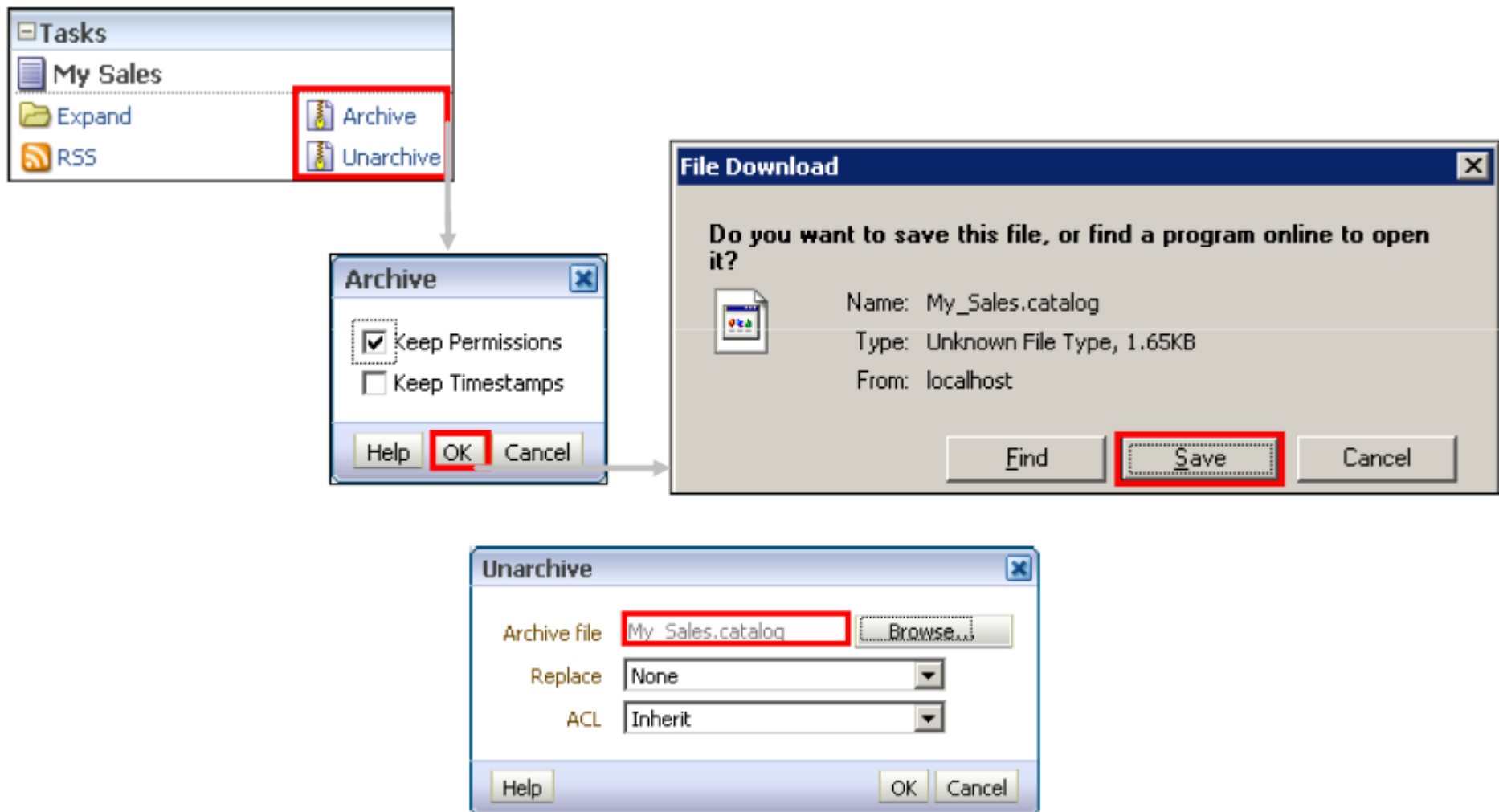
# BIEE - 目录安全

## ■ 管理目录安全



# BIEE - 目录安全

- 归档方式移动目录，并保留权限





# Question Time!

# Q & A

## Questions & Answers

# Thank You !



上海汉得信息技术有限公司  
HAND Enterprise Solutions Company Ltd.  
[www.hand-china.com](http://www.hand-china.com)

