

Анализ и идентификация

(Intelligence and Identity, by Mark Rittman and Joel Crisp)

Марк Риттман,

Джозел Крисп

Источник: журнал "Oracle Magazine" #1 2008,

<http://www.oracle.com/technology/oramag/oracle/08-jan/o18identity.html>



Mark Rittman (Марк Риттман) – директор Oracle ACE и сооснователь Rittman Mead Consulting, расположенной в Великобритании компании со статусом Oracle Partner, предоставляющей специализированные решения в области бизнес-анализа и хранилищ данных.

Joel Crisp (Джозел Крисп) – главный инженер Oracle по развитию Oracle Business Intelligence Suite.

Интеграция пакетов Oracle Business Intelligence и Oracle Identity Management

При развертывании пакета Oracle Business Intelligence Enterprise Edition то, как вы справитесь с управлением идентификационными данными (identity management) так же важно, как скорость выполнения запросов и качество данных. Построенное на основе хорошей архитектуры решение по управлению идентификационными данными позволяет легко "подключать" новых пользователей, чтобы они могли быстро получить доступ к приложениям и данным, соответственно их ролям, которые, в принципе, меняются со временем. При этом персональные данные пользователей и привилегии доступа могут легко управляться.

В этой статье рассматривается интеграция пакета Oracle Business Intelligence Enterprise Edition с двумя основными инструментами Oracle для управления идентификационными данными: Oracle Internet Directory и Oracle Application Server Single Sign-On. Мы покажем, как сочетать функции обеспечения безопасности в Oracle Business Intelligence Enterprise Edition и пакете Oracle Identity Management для реализации детализированного, безопасного доступа к данным.

В фокусе – управление идентификационными данными

Управление идентификационными данными пользователей обладает своим жизненным циклом, начиная с приема человека на работу, продолжаясь с его продвижениями по службе, переходами в другие подразделения, изменениями в обязанностях (ролях) и заканчивая увольнением, когда доступ данного человека к приложениям ликвидируется. За время работы служащим, как правило, нужен доступ ко многим системам, и их требования по доступу к данным

меняются в соответствии с изменениями их ролей.

Пакет Oracle Identity Management – это полный набор продуктов, которые обеспечивают управление идентификационными данными на основе стандартов: Oracle Access Manager, Oracle Application Server Single Sign-On, Oracle Enterprise Single Sign-On Suite, Oracle Identity Federation, Oracle Identity Manager, Oracle Internet Directory, Oracle Virtual Directory и Oracle Web Services Manager. Oracle Internet Directory – это директория, соответствующая LDAP v.3 и использующая масштабируемость и высокую готовность СУБД Oracle, чтобы хранить профили отдельных пользователей и их групп (user and group profiles). Oracle Internet Directory широко используется в собственных приложениях и продуктах класса middleware корпорации Oracle для обеспечения единого хранилища идентификационных данных. (Обзор концепций управления идентификационными данными и Oracle Identity Management см. в статье "Access Granted" в номере Oracle Magazine за июль/август 2006 г. - <http://www.oracle.com/technology/oramag/oracle/06-jul/o46identity.html>)

Пакет Oracle Business Intelligence Enterprise Edition обладает своей собственной инфраструктурой обеспечения безопасности для управления данными пользователей и их групп, контроля доступа к источникам данных, и эта инфраструктура может быть интегрирована с многими другими индустриально-стандартными средствами управления идентификационными данными, включая пакет Oracle Identity Management.

В состав пакета Oracle Business Intelligence Enterprise Edition входят продукты Oracle Business Intelligence Server, Oracle Business Intelligence Presentation Services и Oracle Business Intelligence Administration Tool, плюс несколько других серверных и клиентских приложений.

Oracle Business Intelligence Server включает также локальный репозиторий, который содержит информацию об источниках данных (хранилища данных, витрины данных, пакетные приложения и т.д.). Бизнес-пользователям предоставляется доступ к этим источникам через информационные панели - Oracle Business Intelligence Interactive Dashboards.

Oracle Business Intelligence Presentation Services включает свою собственную отдельную инфраструктуру обеспечения безопасности данных о пользователях и их группах, которые хранятся в отдельном репозитории, известном как Web Catalog. Oracle Business Intelligence Interactive Dashboard – это главный пользовательский интерфейс в составе Oracle Business Intelligence Presentation Services.

Когда пользователи подключаются (log in) к своим панелям (dashboards), Oracle Business Intelligence Server аутентифицирует их мандатные данные. Если учетная запись (account) еще не существует в Web Catalog, она создается для пользователя. Если пользователь является членом каких-то групп, у которых уже есть соответствующие записи в Web Catalog, то ему дается доступ на основе членства в группах.

Как будет показано позднее, информация о пользователях и их группах в Oracle Internet Directory может использоваться для облегчения составления сценариев доступа.

Oracle Business Intelligence Server позволяет привилегированным пользователям “олицетворять” (“to impersonate”) других пользователей — эта технология используется в Oracle Business Intelligence Presentation Services для реализации единого подключения (single-sign-on) в различных сценариях, включая тот, который будет продемонстрирован далее в этой статье.

За более подробной информацией обращайтесь к руководствам Oracle Business Intelligence Presentation Services Administration Guide (глава 8) и Oracle Business Intelligence Server Administration Guide (глава 15), доступным на Oracle Technology Network.

Средства управления идентификационными данными – в одной руке

Организации, которые уже развернули пакет Oracle Identity Management, могут легко использовать его для реализации в среде Oracle Business Intelligence Enterprise Edition интегрируемых, масштабируемых решений по управлению идентификационными данными, удовлетворяя все свои потребности в получении отчетов. В данной статье представлено три интеграционных сценария, которые показывают, как можно использовать функциональность обоих этих пакетов.

- **Пример 1:** Использование директории Oracle Internet

Directory для обеспечения безопасности с применением Oracle Business Intelligence Interactive Dashboard Security предоставляет пользователям Oracle Business Intelligence Interactive Dashboard подключение к их информационным панелям (с использованием логинов и паролей Oracle Internet Directory).

- **Пример 2:** Совместное применение Oracle Internet Directory User Identity с Oracle Business Intelligence Server Security Features показывает, как функциональность Oracle Business Intelligence Server может обеспечивать детализированный на уровне строк контроль над данными отчетов для пользователей, аутентифицируемых с Oracle Internet Directory.

- **Пример 3:** Упрощение доступа к Oracle Business Intelligence, благодаря использованию Oracle Single Sign-On и конфигурированию Oracle Business Intelligence Enterprise Edition и с применением механизма Oracle Application Server Single Sign-On как приложения-партнера. В этом случае бизнес-пользователи смогут получать доступ к функциональности Oracle Business Intelligence Server, используя ту же самую учетную запись пользователя, которая применяется и для других приложений, а также смогут получать доступ к своим информационным панелям в Oracle Business Intelligence Server на основе членства в группах.

В данных примерах используются следующие версии:

- Oracle Business Intelligence Enterprise Edition 10.1.3.2, установленный с опцией Advanced Security, которая предоставляет нужные компоненты (Web Bridge servlet, JMX Bean Server и Oracle Business Intelligence Publisher) для развертывания в Oracle Application Server 10.1.3 (а не Oracle Containers for J2EE [OC4J] - по умолчанию). Как правило, для Oracle Business Intelligence Enterprise Edition в производственных средах рекомендуется применять Oracle Application Server.

- Oracle Identity Management и Oracle Application Server Metadata Repository, установленные как часть инфраструктуры развертывания Oracle Application Server 10.1.2. Oracle Identity Management 10.1.4.0.1 включает много расширений и исправленных ошибок и входит в единый дистрибутив, включающий инфраструктуру Oracle Application Server, Oracle Database Server и т.д.

В дополнение к этим продуктам отметим, что:

- Серверы, на которых устанавливаются все эти компоненты, должны обладать полностью квалифицированными доменными именами (fully qualified domain names (FQDNs)), чтобы поддерживать сценарии единого подключения (single-sign-on scenario).

- Если вы используете протокол DHCP (dynamic host configuration protocol, протокол динамической конфигурации хоста) для сетевых адресов на платформе Microsoft Windows, обязательно сконфигурируйте Microsoft Loopback Network Adapter до установки любого

программного компонента. С вопросами обращайтесь к руководствам по установке соответствующих продуктов.

- До внесения изменений в существующие конфигурационные файлы (instanceconfig.xml, например), сделайте копию этого файла, как описано в любом из данных примеров.

- В рассматриваемых примерах предполагается, что экземпляр Oracle Internet Directory установлен и сконфигурирован. Чтобы установить соединение между аутентификацией Oracle Business Intelligence Server и Oracle Internet Directory, учетные записи пользователей должны существовать в Oracle Internet Directory. Чтобы создать учетные записи пользователей:

1. Из Web-браузера перейдите к Oracle Identity Management Provisioning Console:
2. <http://yourservername:7777/oiddas/> Нажмите кнопку Directory для активации страницы заведения пользователя (user setup page). Заведите учетные записи пользователей, если нужно.

Пример 1. Использование Oracle Internet Directory для Oracle Business Intelligence Interactive Dashboard Security

В этом первом примере Oracle Business Intelligence Server присоединяется к Oracle Internet Directory, чтобы позволить пользователям Oracle Business Intelligence Interactive Dashboard аутентифицироваться с использованием их логинов и паролей в Oracle Internet Directory. В работе, когда бизнес-пользователь старается получить доступ к отчету, Oracle Business Intelligence Presentation Services выберут из Oracle Internet Directory информацию о группе, членом которой является этот пользователь.

Этот пример основан на использовании Oracle Internet Directory исключительно для управления пользовательскими идентификационными данными (user IDs) и членством в группах. Можно, однако, также использовать Oracle Security Manager для переноса подробных данных о пользователях и группах прямо в репозиторий Oracle Business Intelligence Server и затем поддерживать актуальность этих данных либо через инструмент Oracle Security Manager LDAP Synchronization, либо через Oracle Directory Integration Platform, предоставляемую с Oracle Internet Directory. (Oracle Directory Integration Platform позволяет создать workflow-процесс, который может добавлять (данные) пользователей в репозиторий Oracle Business Intelligence Server так быстро, как они заведены в Oracle Internet Directory.) За более подробной информации о других возможностях конфигурирования следует обратиться к руководству Oracle Business Intelligence Enterprise Edition Deployment Guide.

Чтобы обеспечить аутентификацию с Oracle Internet Directory, нужно создать “инициализационный блок” (“initialization block”), который подключается, когда пользователь подсоединяется (logs in), выбирая данные из Oracle Internet Directory. Этот “инициализационный блок” выполняется на уровне сессии.

Инструмент Oracle Business Intelligence Administration Tool Variable Manager позволяет определять переменные репозитория и переменные сессии. Мы будем использовать переменные сессии для определения инициализационного блока на уровне сессии.

Чтобы создать “блок инициализации”, используйте Oracle Business Intelligence Server Administration для запуска Variable Manager, следующим образом:

1. Запустите Oracle Business Intelligence Administration Tool.

(Например, нажмите Start -> Programs -> Oracle Business Intelligence -> Administration.)

2. Из меню Manage выберите Variables... для запуска Variable Manager.
3. В левой части панели под Session нажмите Initialization Blocks.
4. В правой части панели Variable Manager нажмите правую кнопку мыши, наведенной на New Initialization Block... (рис.1), чтобы показать редактор Session Variable Initialization Block.
5. Назовите переменную Authenticator.
6. Нажмите Edit Data Source... для создания нового LDAP datasource.
7. Используя LDAP Server dialog box, введите следующие данные соединения:

```
Host name = имя сервера, где находится Oracle Internet
Director
Port = 389
Base DN = dc=, dc=
Bind DN = cn=orcladmin
Bind Password =
LDAP Version = 3
```

8. Нажмите Test Connection, чтобы убедиться, что все работает правильно.

Установив соединение к Oracle Internet Directory, вы должны отобразить внутренние переменные Oracle Business Intelligence Server в переменные к Oracle Internet Directory LDAP следующим образом:

1. Нажмите на кнопку Return в редакторе Session Variable Initialization Block editor.
2. Нажмите Edit Data Target....
3. Используя Session Variable Initialization Block Data Target dialog box, отобразите эти три переменные Oracle Business Intelligence Server в соответствующие переменные Oracle Internet Directory LDAP:

```
USER = uid
GROUP = departmentnumber
PASSWORD = userpassword
```

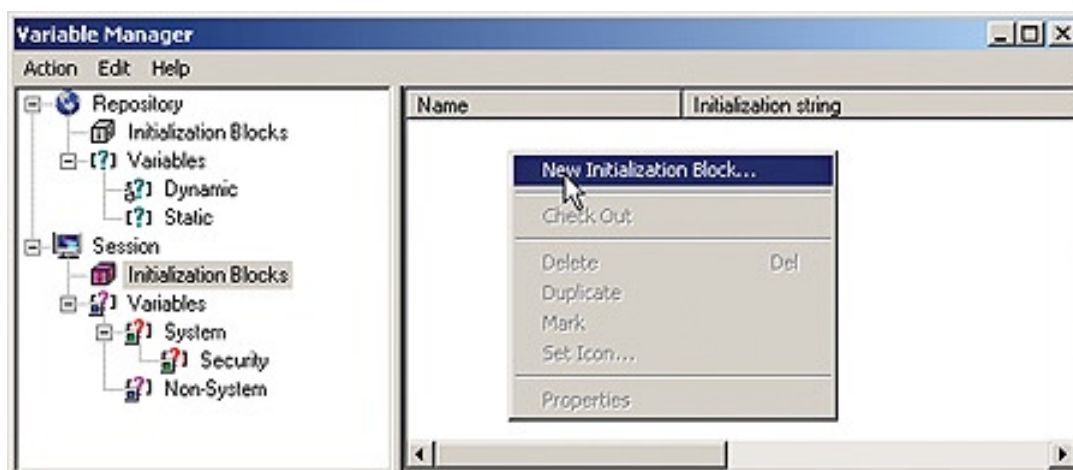


Рис. 1: Создание нового “инициализационного блока” в Oracle Business Intelligence Administration Tool Variable Manager

Можно игнорировать сообщения-предупреждения, которые появятся, если вы используете такие имена переменных, как USER и PASSWORD (password is optional). Эти предупреждения генерируются, так как мы прямо вводим значения для этих внутренних переменных Oracle Business Intelligence Server — что вы никогда не будете делать в производственной среде.

4. Нажмите **ОК**, чтобы сохранить определение целевой переменной (variable target definition).
5. Нажмите **ОК** снова для создания “блока инициализации”.

Отметим, что вместо использования этого атрибута LDAP uid attribute для заведения идентификационных данных пользователя, можно использовать атрибут orclguid, который гарантирует уникальность даже тогда, когда один пользователь удален из Oracle Internet Directory, а другой создан с тем же самым именем. Однако, в данном примере мы используем атрибут the uid attribute, который делает Web Catalog paths немного более читаемым (но за счет риска “столкновения” новых пользователей с удаленными). Можно также создавать дополнительные связи переменных (variable bindings) для адресов электронной почты пользователя или для атрибутов LDAP.

6. Нажмите **ОК**, чтобы перепоказать Server Variable Initialization Block dialog box.
7. Проверьте поле **Required for Authentication**, чтобы потребовать всех пользователей (за исключением пользователя administrator) аутентифицирование через сервер Internet Directory server. (Если вы не проверите это контрольное поле, пользователи в Oracle Internet Directory таки смогут аутентифицироваться, если их данные находятся в репозитории Oracle Business Intelligence Server.)
8. Перестаруйте Oracle Business Intelligence Server.

Проверьте эту установку, предложив одному из пользователей подключиться к Oracle Business Intelligence

Interactive Dashboard, используя его мандатные данные в Oracle Internet Directory. Этому пользователю должен быть дан доступ к Oracle Business Intelligence Interactive Dashboard согласно членству в группе, описанной в Oracle Business Intelligence Presentation Services Web Catalog, и перечисленному в профайле Oracle Internet Directory.

Пример 2: Совместное применение Oracle Internet Directory User Identity с Oracle Business Intelligence Server Security Features

В этом примере создаются группы в Oracle Business Intelligence Server и обеспечивается безопасность при доступе на уровне строки (row-level security) для групп, так что у пользователей будет доступ к данным на основе ролей, независимо от того, как они подсоединяются (через Security Manager или Oracle Internet Directory).

Прежде всего создайте группы в Oracle Business Intelligence Server, используя Oracle Business Intelligence Administration Tool.

1. Из главного меню **Oracle Business Intelligence Administration Tool** выберите **Manage -> Security** для запуска Security Manager.
2. Из левой части панели Security Manager, выберите **Groups**.
3. Добавьте название группы, которое соответствует группе, заведенной в Oracle Internet Directory.
4. Создайте группы, которые соответствуют группам, уже созданным в Oracle Business Intelligence Presentation Services Web Catalog и которые соответствуют названиям групп, использованных в Oracle Internet Directory.
5. Создав эти группы, используйте User Group/Permissions dialog box, чтобы создать и применять один или больше фильтров к таблицам, доступных каждой группе, тем самым ограничивая доступ к ним.

Например, можно создать фильтр, чтобы ограничить доступ членов Восточной группы (Eastern group) таким

образом, что они смогут увидеть данные о клиентах только из Нью-Йорка и Массачусетса (см. рис. 2). Каждый фильтр определяет данные, которые пользователь сможет увидеть. Фильтры кумулятивны, пользователи, принадлежащие как к Восточной, так и к Северной группе, увидят данные о клиентах и из восточных, и из северных штатов.

Однако, пользователи без каких-либо фильтров, применяемых к заданной таблице в репозитории, смогут увидеть все данные в этой таблице.

Когда кто-то из Восточной группы подключается, он увидит данные по этому региону (см. рис. 3); если же он также принадлежит к другой группе, либо подключится пользователь, который принадлежит к другой группе, то

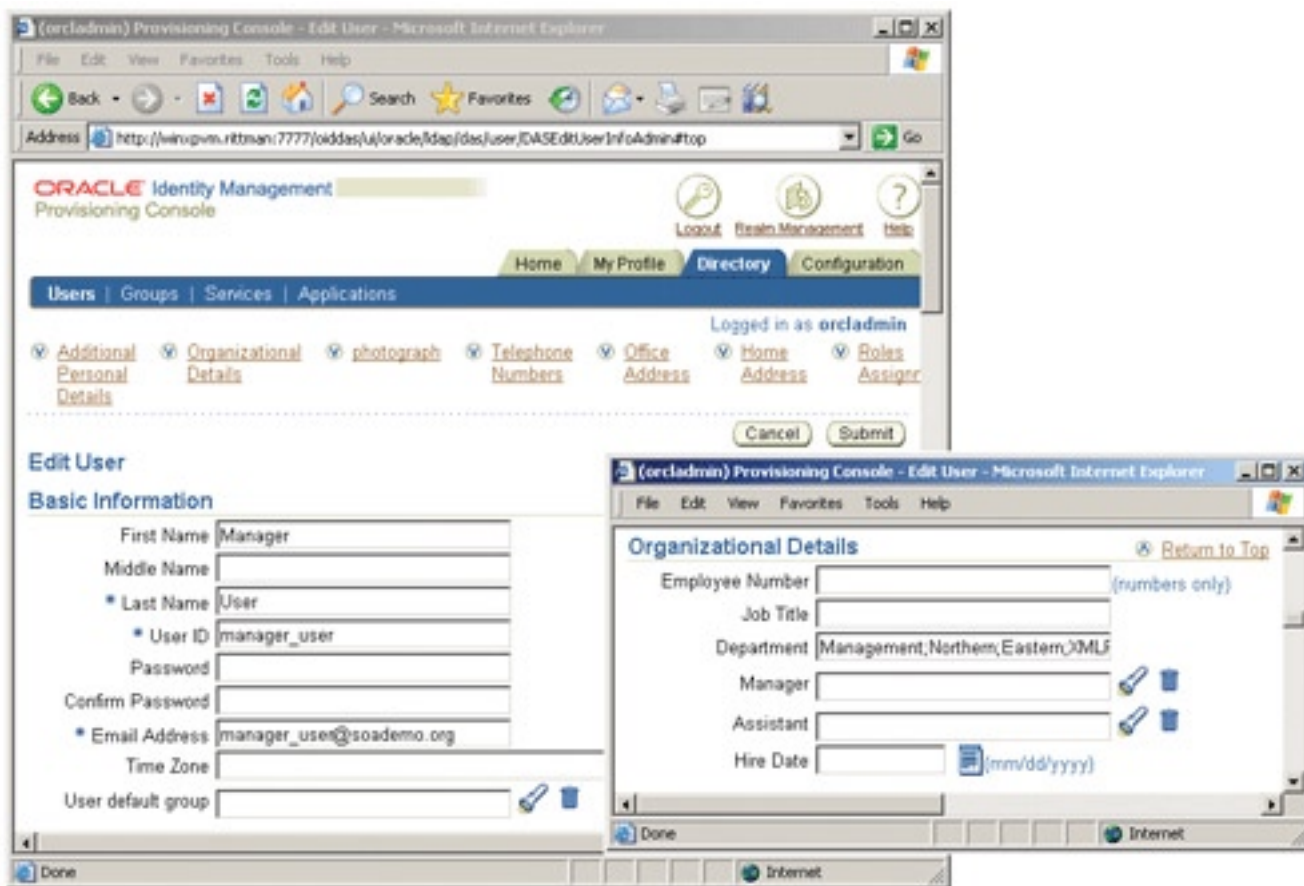


Рис. 2: Фильтрация доступа различных групп через Oracle Internet Directory



Рис. 3: Просмотр данных, доступных только Восточной группе

они увидят данных из соответствующих штатов.

Пример 3: Упрощение доступа Oracle Business Intelligence Enterprise Edition с использованием Oracle Application Server Single Sign-On

Функция единого подключения (SSO) в Oracle Application Server обеспечивает пользователя единым идентификатором (ID) и паролем (password), которые дают ему доступ к приложениям Oracle. Эти приложения могут быть либо полноправными участниками (full participants) в Oracle Application Server Single Sign-On (в котором все управление пользователями и профилями реализуется через Oracle Internet Directory), либо они могут быть партнерами приложениями, которые используют свои собственные пользовательские профили.

В этом примере показано, как конфигурировать Oracle Business Intelligence Enterprise Edition в качестве партнерского приложения в Oracle Application Server Single Sign-On: пользовательские данные для SSO (single-sign-on user IDs)

отображаются в соответствующие данные Oracle Business Intelligence Enterprise Edition, так что пользователи могут получить доступ к своим отчетам и данным.

Конфигурирование Oracle Business Intelligence Enterprise Edition для работы с Oracle Application Server Single Sign-On – это вполне очевидный процесс, если Oracle Business Intelligence Suite установлен с опцией Advanced Security.

Конфигурирование Oracle Business Intelligence Enterprise Edition для использования SSO на платформе Microsoft Windows XP:

1. Откройте подсказку команд Open a command prompt.
2. Установите переменную среды ORACLE_HOME в Oracle home, используемый пакетом Oracle Application Server Identity Management:

```
C:\>set ORACLE_HOME=c:\oracle\OraHome_1
```

3. Используйте утилиту Oracle Internet Directory SSOREG для создания конфигурационного файла, который указывает на ваш Oracle Business Intelligence Presentation Server URL (используя только hostname и номер порта (port number)):

```
C:\> C:\oracle\OraHome_1\ssobin\ssoreg.bat -oracle_home_path c:\oracle\OraHome_1 -config_mod_osso TRUE -site_name <bi host name>:<bi port number> -remote_midtier -config_file c:\oracle\OraHome_1\Apache\Apache\conf\osso\biosso.conf -mod_osso_url http://<bi host name>:<bi port number>
```

4. Копируйте конфигурационный файл, сгенерированный утилитой SSOREG в Oracle Application Server 10.1.3 Oracle home (в который Oracle Business Intelligence Enterprise Edition было установлено). Например,

```
C:\> copy c:\oracle\OraHome_1\Apache\Apache\conf\osso\biosso.conf c:\oracle\OraHome_2\Apache\Apache\conf\osso\
```

5. В текстовом редакторе откройте файл mod_osso.conf в Oracle Application Server 10.1.3 Oracle home (размещенный в директории ORACLE_HOME/Apache/Apache/conf) и добавьте следующую директиву:

```
OssosConfigFile c:/oracle/OraHome_2/Apache/Apache/conf/osso/biosso.conf
```

6. Добавьте следующий XML-фрагмент, чтобы статически защитить Oracle Business Intelligence Presentation Server URL:

```
<IfModule mod_osso.c>
  <Location /analytics>
    OssoIpCheck off
    OssoIdleTimeout off
```

```
Header unset Pragma
OssosSendCacheHeaders off
AuthType Basic
require valid-user
</Location>
</IfModule>
```

7. Сохраните изменения и закройте текстовый редактор. Внутри того же самого Oracle home, перейдите к поддиректории /Apache/Apache/conf:

```
ORACLE_HOME/Apache/Apache/conf
```

8. Используя текстовый редактор, откройте файл httpd.conf и раскомментируйте следующую строчку:

```
include "Oracle_HOME/Apache/Apache/conf/mod_osso.conf"
```

9. Если нужно, модифицируйте название Oracle home, на который есть ссылка в данной строке, так, чтобы она относилась к Oracle home, используемому Oracle Application Server 10.1.3. Когда сервер Apache стартует, он прочитает файл mod_osso.conf, который вы модифицировали.

10. Сохраните изменения и закройте текстовый редактор.

11. Перестаруйте Oracle HTTP Server, используя следующие команды:

```
ORACLE_HOME/opmn/bin/opmnctl
restartproc process-type=HTTP_Server
```

Чтобы установить делегированную аутентификацию, стартуйте Oracle Business Intelligence Administration Tool снова и создайте “олицетворяющего пользователя” (“impersonation user”), которого Oracle Business Intelligence Presentation Server будет использовать для создания соединения к Oracle Business Intelligence Server от имени аутентифицируемого пользователя.

Внутри Oracle Business Intelligence Administration Tool, выберите Manage -> Security и New -> User. Создайте пользователя с именем Impersonator и паролем fakeuser (в производственных средах выбирайте более сильный пароль). Добавьте этого пользователя в группу Administrators и заведите его имя (username) и пароль.

Теперь вы добавляете подробности этого олицетворяющего пользователя в хранилище мандатных данных Oracle Business Intelligence Presentation Server, используя утилиту Presentation Server CRYPTOTOOLS:

1. Откройте подсказку команд.
2. Перейдите к расположению криптографических средств и хранилища мандатных данных Oracle Business Intelligence. Расположение по умолчанию – поддиректория \Or-

acleBI\web\bin subdirectory в инсталляции Oracle Business Intelligence Suite. Например,

```
cd c:\oracle\OracleBI\web\bin
```

3. Введите следующую команду:

```
cryptotools credstore -add -infile
c:\oracle\OracleBIData\web\config\
credentialstore.xml
```

Вам будет предложено ввести алиасы мандатных данных, имя пользователя (username), пароль (password) и другие детали:

4. Введите impersonation для credential alias.
5. Введите Impersonator для username.
6. Введите fakeuser для password.
7. Ответьте yes, когда получите подсказку зашифровать пароль.
8. На подсказке passphrase, введите storepassword и отметьте passphrase.
9. Ответьте no, когда получите подсказку запомнить passphrase в XML-файле.
10. Ответьте yes, когда получите подсказку переписать credential store file.

Затем нужно изменить конфигурационный файл Oracle Business Intelligence Presentation Services - (instanceconfig.xml) файл, размещенный в директории данных инсталляции Oracle Business Intelligence Suite. Например,

```
c:\oracle\OracleBIData\web\config\instanceconfig.xml
```

11. Используя текстовый редактор, откройте файл instanceconfig.xml file.

12. Добавьте информацию о расположении хранилища мандатных данных в секцию ServerInstance этого файла, заменяя расположение для вашего Oracle Business Intelligence Presentation Server и сервера Oracle Application Server Single Sign-On в этом XML-фрагменте:

```
<CredentialStore>
  <CredentialStorage type="file"
    path="c:\oracle\OracleBIData\web\
    config\credentialstore.xml"
    passphrase="storepassword"/>
</CredentialStore>
```

13. Добавьте в секцию ServerInstance следующий XML-фрагмент для авторизации этого файла:

```
<Auth>
<SSO enabled="true">
<ParamList>
  <!--IMPERSONATE param is used to
  get the authenticated user's username
  and is required -->
  <Param name="IMPERSONATE"
    source="serverVariable"
```

```
  nameInSource="REMOTE_USER"/>
</ParamList>
<LogoffUrl> http://pls/orasso/orasso.wvssso_app_admin.
ls_logout?p_done_url=http%3A%2F%2F:%2Fanalytics%2F
</LogoffUrl>
<LogonUrl>
http://pls/orasso/orasso.wvssso_app_admin.ls_login
</LogonUrl>
</SSO>
</Auth>
```

14. Сохраните файл instanceconfig.xml file.

15. Перезапустите Oracle Business Intelligence Presentation Server.

Ваши пользователи теперь могут подключаться к Oracle Business Intelligence Enterprise Edition, используя Oracle Application Server Single Sign-On.

Полная информация о том, как зарегистрировать Oracle Business Intelligence Enterprise Edition в качестве приложения-партнера Oracle Application Server Single Sign-On, содержится в Секции 11 руководства Oracle Business Intelligence Enterprise Edition Deployment Guide.

Заключение

При создании аналитического приложения на базе Oracle Business Intelligence Enterprise Edition то, как решается проблема управления идентификационными данными также важно, как качество данных и производительность отчетов. Пользователи должны иметь один профиль в рамках своей организации, который обеспечивает им доступ к приложениям и отчетам, благодаря простому (в администрировании) процессу, который реализует жизненный цикл управления их идентификационными данными от приема на работу, до продвижений и увольнения.

Oracle Application Server 10g благодаря использованию инструментов Oracle Identity Management —Oracle Internet Directory, Oracle Delegated Administration Services и Oracle Application Server Single Sign-On—предоставляет решение на основе широко используемых стандартов. Продукт Oracle Business Intelligence Enterprise Edition использует эти стандарты и позволяет создавать единое решение по управлению идентификационными данными для приложений по направлениям бизнеса (line-of-business) и получения отчетности.

Прочитайте “Access Granted” (<http://oracle.com/technology/oramag/oracle/06-jul/o46identity.html>)

Oracle documentation (<http://www.oracle.com/documentation/>)
 Oracle Business Intelligence Presentation Services Administration Guide
 Oracle Business Intelligence Server Administration Guide
 Oracle Business Intelligence Enterprise Edition Deployment Guide

Узнайте больше о Oracle Identity Management (http://oracle.com/technology/products/id_mgmt/), Oracle Business Intelligence (<http://oracle.com/technology/products/bi/>)

Изучите Oracle по примерам

Creating a Repository Using the Oracle Business Intelligence Administra-