Installing and Configuring Oracle Analytics Server with Oracle Enterprise Manager Cloud Control

A guide for using OAS with Enterprise Manager 13.4 and 13.5
PURPOSE STATEMENT

This document provides an overview of the installation and configuration of Oracle Analytics Server, version 5.5.0 or above, for use with both Enterprise Manager 13.4 and release 13.5. It is intended solely to help you assess the business benefits of upgrading to Enterprise Manager 13.5 and to plan your I.T. projects.

DISCLAIMER

This document in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

DISCLAIMERS FOR PRE-RELEASE, PRE-GA PRODUCTS

The revenue recognition disclaimer on this page is required for any white paper that addresses future functionality or for products that are not yet generally available (GA). If you are unsure whether your statement of direction needs the disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.

The testing disclaimer in the copyright section on the last page (highlighted in yellow) is provided by the FCC for hardware products. It must appear in the copyright section for all pre-release, pre-GA hardware products. Be sure to remove the yellow highlighting before publishing. When the product becomes GA, update your collateral by removing the disclaimer from the copyright section. If your product is already GA or if you are writing about a software product, delete the disclaimer from the copyright section.

Important: If your product is not GA, then you cannot include any regulatory compliance information in the statement of direction. Regulatory compliance information may be included for GA products only if you have completed all required safety and emissions testing, and you have received the certificates issued by the testing organization.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview of Base Install and Configuration of OAS</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>Overview of post install of OAS</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>Overview of OAS Security Configurations</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>Overview of Enterprise Manager Security</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>4.1 EM Repository based authentication.</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>4.2 LDAP-based authentication</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>Flow chart for all Procedures</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>Overview of Upgrading from Enterprise manager 13.4</td>
<td>20</td>
</tr>
<tr>
<td>7</td>
<td>Complete steps to install and configure OAS</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>7.1 Install JDK: JDK8 : U251 Or Newer</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>7.2 Confirm Correct Installation</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>7.2.1 First Oracle product being installed on this system</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>7.2.2 Step 1 – Welcome; Step 2 – Auto Updates</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>7.2.3 Step 3 – Installation Location</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>7.2.4 Step 4 – Installation Type</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>7.2.5 Step 5 – Prerequisite Checks; Step 6 – Installation Summary</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>7.2.6 Step 7 – Installation Progress; Step 8 – Installation Complete</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>7.3 Install required Fusion Middleware one-off</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>7.4 Install OAS</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>7.4.1 Step 1 – Welcome ; Step 2 Auto Updates</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>7.4.2 Step 3 – Choose Oracle Home</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>7.4.3 Step 4 – Pre-requisite Checks</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>7.4.4 Step 5 – Installation Summary</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>7.4.5 Step 6 – Installation Progress</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>7.4.6 Step 7 – Installation Complete</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>7.5 Install latest OAS Bundle Path (OAS 5.5.0-201216 BP – 32294034)</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>7.6 Configure OAS</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>7.6.1 Step 1 - Welcome Screen</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>7.6.2 Step 2 - Configuration</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>7.6.3 Step 3 - Prerequisite Checks</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>7.6.4 Step 4 - Define Domain</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>7.6.5 Step 5 - Database Details</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>7.6.6 Step 6 - Port Management</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>7.6.7 Step 7 - Initial Application</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>7.6.8 Step 8 - Summary</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>7.6.9 Step 9 - Configuration Progress</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>7.6.10 Step 10 - Configuration Complete</td>
<td>36</td>
</tr>
<tr>
<td>8</td>
<td>OAS Security Configuration</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>8.1 Oracle Analytics Publisher Authentication and Report Execution Flow</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>8.1.1 OAS Authentication</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>8.1.2 OAS User Interface Privileges</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>8.1.3 OAS Server Catalog Access</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>8.1.4 OAS Report Execution</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>8.1.5 OAS Login Processing</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>8.1.6 OAS Privilege Assignment</td>
<td>41</td>
</tr>
<tr>
<td>9</td>
<td>OAS For Enterprise Manager Repository-based Security</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>9.1 Create required DBMS roles and grant to required EM administrators.</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>9.2 Configure OAS for ‘Database Security Model’</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>9.3 Screenshots for Oracle Database Security Model</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>9.3.1 Step 1 - Login to OAS as the weblogic user</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>9.3.2 Step 2 - Click on ‘Administration’ link</td>
<td>43</td>
</tr>
</tbody>
</table>
Chapter 10. OAS For Enterprise Manager LDAP Configuration 49

10.1 OAS Security Model Configuration
10.1.1 Step 1 - Login to OAS as the 'weblogic' user
10.1.2 Step 2 - Click on 'Administration' link
10.1.3 Step 3 - Choose 'Security Configuration' (under 'Security Center')
10.1.4 Step 4 - Fill in required entries for the 'Local Superuser':
10.1.5 Step 5 - Confirm correct configuration of 'Fusion Middleware Security Model'

10.2 WebLogic Security Configuration
10.2.1 Step 1 - Login to WebLogic console
10.2.2 Step 2 - Click on Security Realms
10.2.3 Step 3 - Click on myrealm and then the Providers tab
10.2.4 Step 4 - Comparison of WebLogic Security between EM and OAS
10.2.5 Step 5 - WebLogic Security Configuration for OAS
10.2.6 Step 6 - WebLogic Configuration for EM with OID (without SSO)
10.2.7 Step 7 - Overall goal of configuring OAS identically to EM

Chapter 11. Procedure for Configuring WebLogic for LDAP 59

11.1 Step 1 – Prepare to edit the runtime configuration of the OAS WebLogic Domain
11.2 Step 2 - Configure WebLogic Providers
11.3 Step 3 - Re-order the providers
11.4 Step 4 – Confirm correct ordering of providers
11.5 Step 5 – Change the OID Provider to SUFFICIENT
11.6 Step 6 – Configure OID Provider for OAS WebLogic Domain
11.6.1 1st Section of OID Provider Specific Configuration Parameters
11.6.2 2nd Section of OID Provider Specific Configuration Parameters
11.6.3 3rd Section of OID Provider Specific Configuration Parameters
11.7 Step 7 – Change the DefaultAuthenticator from REQUIRED to SUFFICIENT
11.8 Step 8 – Save and Activate the changes
11.9 Step 9 – Restart the OAS WebLogic Domain’s Managed Servers
11.10 Step 10 - Configuration of Java Platform Services (JPS)
11.10.1 Part 1 - Configure Java Platform Services
11.10.2 Part 2 - Configuring Oracle Virtual Directory (OVD)
11.10.3 Part 3 - Mapping of OBI-stripe Roles to LDAP Users and/or LDAP Groups
11.11 Step 11 - Granting OAS Fusion Middleware Application roles to EM LDAP Users
11.11.1 Part 1 - Login to Fusion Middleware Control and Navigate to Application Roles
11.11.2 Part 2 - Select the ‘obi’ Application Stripe
11.11.3 Part 3 - Select the Role, for example ‘BIServiceAdministrator’
11.11.4 Part 4 - Press Edit
11.11.5 Part 5 - Add the required Principals
11.11.6 Part 6 - Press OK
11.11.7 Part 7 - Push any changes to OBI stripe

Chapter 12. OAS Optional Configuration of SSO on top of LDAP 73

12.1 Installation of OHS
12.1.1 Step 1 - OHS Installation - Welcome
### Chapter 12. Creating OHS Using wlst.sh

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1.2</td>
<td>Step 2 - OHS Installation – Auto Updates</td>
</tr>
<tr>
<td>12.1.3</td>
<td>Step 3 - OHS Installation – Choose Middleware Home</td>
</tr>
<tr>
<td>12.1.4</td>
<td>Step 4 - OHS Installation – Installation Type</td>
</tr>
<tr>
<td>12.1.5</td>
<td>Step 5 - OHS Installation - Choose JAVA HOME location</td>
</tr>
<tr>
<td>12.1.6</td>
<td>Step 6 - OHS Installation – Prerequisite Checks</td>
</tr>
<tr>
<td>12.1.7</td>
<td>Step 7 - OHS Installation – Installation Summary</td>
</tr>
<tr>
<td>12.1.8</td>
<td>Step 8 - OHS Installation – Installation Progress</td>
</tr>
<tr>
<td>12.2</td>
<td>Extending OAS WebLogic domain with collocated OHS using the config.sh script</td>
</tr>
<tr>
<td>12.3</td>
<td>OHS Configuration</td>
</tr>
<tr>
<td>12.3.1</td>
<td>Step 1 - OHS Configuration – Update an existing WebLogic Domain</td>
</tr>
<tr>
<td>12.3.2</td>
<td>Step 2 - OHS Configuration – Choose Oracle HTTP Server (Collocated [OHS])</td>
</tr>
<tr>
<td>12.3.3</td>
<td>Step 3 - OHS Configuration - High Availability Options</td>
</tr>
<tr>
<td>12.3.4</td>
<td>Step 4 - OHS Configuration – Database Configuration Type</td>
</tr>
<tr>
<td>12.3.5</td>
<td>Step 5- OHS Configuration – Component Datasources</td>
</tr>
<tr>
<td>12.3.6</td>
<td>Step 6 - OHS Configuration – JDBC Test</td>
</tr>
<tr>
<td>12.3.7</td>
<td>Step 7 - OHS Configuration – Advanced Configuration</td>
</tr>
<tr>
<td>12.3.8</td>
<td>Step 8 OHS Configuration – System Components</td>
</tr>
<tr>
<td>12.3.9</td>
<td>Step 9 - OHS Configuration – OHS Server</td>
</tr>
<tr>
<td>12.3.10</td>
<td>Step 10 - OHS Configuration – Machines</td>
</tr>
<tr>
<td>12.3.11</td>
<td>Step 11 - OHS Configuration – Assign System Components</td>
</tr>
<tr>
<td>12.3.12</td>
<td>Step 12 - OHS Configuration – Configuration Summary</td>
</tr>
<tr>
<td>12.3.13</td>
<td>Step 13 - OHS Configuration – Configuration Progress</td>
</tr>
<tr>
<td>12.3.14</td>
<td>Step 14 - OHS Configuration – End of Configuration</td>
</tr>
</tbody>
</table>

### Chapter 13. OAS for Configuration of Oracle Access Manager SSO

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1.1</td>
<td>Step 1 - Login to WebLogic Console</td>
</tr>
<tr>
<td>13.1.2</td>
<td>Step 2 - Click on Security Realms and myrealm</td>
</tr>
<tr>
<td>13.1.3</td>
<td>Step 3 - Click on the Providers tab</td>
</tr>
<tr>
<td>13.1.4</td>
<td>Step 4 - Prepare to make the required edits</td>
</tr>
<tr>
<td>13.1.5</td>
<td>Step 5 - Create the new OAM Identity Asserter</td>
</tr>
<tr>
<td>13.1.6</td>
<td>Step 6 - Configure the BIP_OAM_Provider Provider to match Enterprise Manager</td>
</tr>
<tr>
<td>13.1.7</td>
<td>Step 7 - Configuration of Oracle Webgate, running on top of OHS.</td>
</tr>
<tr>
<td>13.1.8</td>
<td>Step 8 - OAS Required Steps</td>
</tr>
</tbody>
</table>

### Chapter 14. Configuration of required OAS Datasource(s)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Step 1 - For the first EM system (and optionally any additional EM systems)</td>
</tr>
<tr>
<td>14.2</td>
<td>Step 2 OAS Datasource Configuration Steps</td>
</tr>
</tbody>
</table>

5 WHITE PAPER | Installing and Configuring Oracle Analytics Server with Oracle Enterprise Manager Cloud Control | A guide for using OAS with Enterprise Manager 13.4 and 13.5 | Version 1.02
Copyright © 2021, Oracle and/or its affiliates | Confidential – Public
Part 5 - Fill in the required details 105
Part 6 - Test the connection and ensure the results of a successful connection: 105
Part 7 Granting Required Roles to OAS Datasource 106

Chapter 15. Installation of Oracle Provided Out of Box Reports 108

15.1 Per-requisite Step to support Enterprise Manager Provided Out of Box Reports 108
15.1.1 Standalone OAS 5.5.0 support for EM Provided Reports: Database Security Model 109
15.2 OAS 5.5.0 support for EM Provided Reports: Fusion Middleware Security Model 110
15.2.1 Step 1 - Create EMBIP* Roles as OBI-Stripe Roles 110
15.2.2 Step 2- Create Mapping of BI Service Administrator to EMBIPAdministrator 112
15.2.3 Step 3 - Repeat so below screenshots are shown 115
15.3 Uploading Enterprise Manager Provided Out of Box Reports 116
15.3.1 Framework Reports 116
15.3.2 Plugin Reports 116
15.3.3 Common File name for all Oracle Provided Out of Box Reports 116
15.3.4 Preparing the Enterprise Manager 13.5 Out of Box Reports for uploading to OAS 117
15.4 Uploading Oracle Provided Out-of-box Reports to standalone OAS 118
15.4.1 Platform reports 118
15.4.2 Repeat the above procedure for each EM plugin 119
15.5 Steps to complete after uploading the Enterprise Manager Provided Reports 120
15.5.1 OAS Catalog Object Types 120
15.5.2 Resolving Permissions issues against one or more OAS Catalog Object(s) 121

Chapter 16. Upgrading from EM 13.4 to EM 13.5 124

16.1 Migrating BIP Schedules from EM 13.4 124
16.2 Arguments for OAS Scheduler Migration Script 125
16.2.1 Example execution of OAS Scheduler Migration Script using example values 126
16.3 Migrating any customized BIP reports to the standalone OAS. 127
16.3.1 Example Use Case 127
16.4 Outline of steps to download the report from EM 13.4: 127
16.4.1 Step 1 – EM 13.4 – Login to BIP 128
16.4.2 Step 2 – From the BIP home screen, click on the link for ‘Catalog Folders’ 128
16.4.3 Step 3 – If needed, expand the ‘Shared Folders’ node in the catalog tree. 129
16.4.4 Step 4 - Click on the MyReports’ Folder. 129
16.4.5 Step 5 - Click on Download. 130
16.4.6 Step 6 – You may be asked what to do with the file named MyReports.xdrz 131
16.4.7 Step 7 - Confirm that the file was downloaded correctly. 131
16.5 EM 13.5 – Upload Report Folder to OAS 132
16.5.1 Step 1 - Login to the OAS system on the standalone OAS host as the user 'jerry'. 132
16.5.2 Step 2 - From the OAS home screen, click on the link for ‘Catalog Folders’. 133
16.5.3 Step 3 - If needed, expand the ‘Shared Folders’ node in the catalog tree. 133
16.5.4 Step 4 - Click on Upload. 134
16.5.5 Step 5 - Click the button ‘Choose File’ in the Upload popup window. 134
16.5.6 Step 6 - Choose the file named ‘MyReports.xdrz’ from the operating system dialog. 135
16.5.7 Step 7 – Proceed with the upload 135
16.5.8 Step 8 – Monitor the status of the upload 135
16.5.9 Step 9 – Confirm the correct layout of the OAS Catalog Folders. 136
16.5.10 Step 10 – Confirm that the report executes as expected. 136

Chapter 17. Updating the EM 13.5 WebLogic Domain target 137

17.1 Login to Enterprise Manager 13.5 and Navigate to GCDomain 137
17.2 Refresh WebLogic Domain and Delete Stale Targets 137
17.3 Stale embedded BIP* targets are removed 138
TABLES

Table 1. Overview of Guide 13
Table 2. Mapping of Enterprise Manager Security Configurations to OAS Configuration 16
Table 3. Required OAS Installer 21
Table 4. Key to directories used in examples 21
Table 5. OAS Security Configuration Steps 37
Table 6. OAS Privileges 38
Table 7. OAS Catalog Permissions 39
Table 8. Ensure correct Catalog Permissions for OAS Shared Folder 123
Table 9. Arguments for OAS Scheduler Migration Script 125
Preface

» For Enterprise Manager 13.5, BI Publisher is no longer installed nor configured alongside Enterprise Manager.
» Additionally, BI Publisher cannot be utilized in the same WebLogic domain as that is used for Enterprise manager.
» This handbook is meant to be utilized as a supplement to, and not a replacement for, the existing Fusion Middleware Documentation Book Sets specific to Oracle Analytics Server and Oracle Analytics Publisher.

BEFORE BEGINNING THE PROCEDURES DOCUMENTED IN THIS HANDBOOK, DOWNLOAD ANY CUSTOMIZED BIP REPORTS FROM THE EMBEDDED BIP IN EM 13.4, USING THE BIP USER INTERFACE.

Background
1. BI Publisher is part of the on-premises product formerly known as Business Intelligence Enterprise Edition (BIEE).
2. BIEE has been re-branded Oracle Analytics Server (OAS).
3. BI Publisher has likewise been re-branded as Oracle Analytics Publisher.
4. OAS, to a certain extent, is an on-premises version of Oracle Analytics Cloud (OAC).

Design
For those customers who want to continue to use BI Publisher capabilities with Enterprise Manager, the licensing and support model included with Enterprise Manager 13.5 will continue to support this for Oracle Analytics Publisher.

However, installation and configuration of BI Publisher (BIP), now rebranded as Oracle Analytics Publisher (OAS), will be the responsibility of the customer.

Requirements
This is guide provides details on OAS installation and configuration.

Additionally, Enterprise Manager will continue to supply and support a set of feature-rich Oracle provided Out of Box reports designed and tested with Oracle Analytics Publisher.

Multiple copies of each set of these Out of Box Reports are also available, for support against multiple Enterprise Manager installations (when LDAP security store is utilized).

This guide is not meant to replace or otherwise supersede the large set of documentation books that are currently developed and available via the Oracle Help Center.

Where appropriate, screenshots and other pointers are being provided to help navigate these procedures.

References to specific documentation books in the OAS product library will be referenced for further details.

Enhancements
New for Enterprise Manager 13.5, for certain configurations of Enterprise Manager, a single installation of OAS can be utilized to run reports against multiple, distinct, Enterprise Manager installations, utilizing a common LDAP configuration.

Note, a single Enterprise Manager installation can be composed of multiple hosts, running in supported High Availability and/or Disaster Recovery scenarios.
Upgrading to Enterprise Manager 13.5

Prior to utilizing the steps in this work-book, download any customized BIP reports from the embedded BIP in EM 13.4, using the BIP user interface.

Best practices

» follow the detailed steps in this workbook before upgrading to EM 13.5.
» Utilize this workbook to install and configure a standalone OAS installation on a separate, dedicated, system.
» Integrate the standalone OAS security configuration, as detailed, against one or more existing Enterprise Manager installation(s).
» Utilize the existing Enterprise Manager 13.4 environment to transfer any customized reports from the EM 13.4 integrated BIP to your desktop.
» Utilize the standalone OAS User Interface to upload these same customized reports from your desktop to the standalone OAS.
» After the upgrade to Enterprise Manager 13.5 is complete, the updated set of Oracle Provided Out of Box reports can be found in the Oracle Home for EM 13.5.
» Utilize the standalone OAS User Interface to upload this new set of Oracle Provided Out-of-Box reports to OAS.
» Post upgrade of Enterprise Manager 13.5 migrate the BIP report schedules, from the embedded BIP, to the standalone OAS.

Customer Impact

Enterprise Manager supports a rich set of architectural and security options, as does BI Publisher and Oracle Analytics Publisher.

In past releases of Enterprise Manager, prior to Enterprise Manager 13.5, all these Enterprise Manager options had been enhanced to incorporate BIP, in parallel, with the OMS.

Some examples include:

» Enterprise Manager login using repository-based authentication (default configuration).
  » Repository-based authentication is also utilized alongside Oracle RDBMS Enterprise User Security (EUS).
» Enterprise Manager login using LDAP, based upon WebLogic Security Providers.
» Enterprise Manager Single Sign On.
» EM High Availability and Disaster Recovery.
» EM runtime tools (start, stop, status, etc.…)
» Deployment and management of Oracle Provided BIP Reports.
» The capability to patch EM with updated BIP reports.
» Target Level permissions (VPD) for BIP Report Execution.

All this automation has been removed in Enterprise Manager 13.5.

The purpose of this document is to ease this transition from the integrated BIP to a standalone OAS installation.
Recommendation for the version of OAS to utilize

» This guide has been written by the Enterprise Manager Development organizations and has been extensively tested utilizing Oracle Analytics Server (OAS) 5.5.0.

» Newer versions of OAS may become available now, or in the future, and there is a strong likelihood that this guide should work against these newer versions as well.

» However, for important internal development efforts, and especially for production deployments, it is recommended that OAS 5.5.0 be utilized as a starting point.

» Once the standalone OAS 5.5.0 has been configured and is fully functional when used with Enterprise Manager 13.4 or 13.5, upgrades to versions of OAS beyond 5.5.0 can be planned out using standard internal deployment methodologies.

Cross References to Relevant Oracle Documents

OAS supports all the same architectural and security options as was provided via the embedded BI Publisher.

The approach utilized by the standalone OAS product is via a rich, and complex, set of documentation books.

Beyond OAS, numerous other Oracle technologies and products are referenced and outlined within these pages.

The complete list of referenced documents is shown in the bibliography, located here:

» Chapter 18 - References
Organization of this Guide
This guide is organized as follows:

<table>
<thead>
<tr>
<th>STEP</th>
<th>DESCRIPTION</th>
<th>CROSS-REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Basic installation and configuration of Oracle Analytics Server.</td>
<td>Chapter 7 and Chapter 2</td>
</tr>
<tr>
<td>2</td>
<td>Security configurations</td>
<td>Chapters: 8, 9, 10, 11, 12, 13</td>
</tr>
<tr>
<td>A</td>
<td>Oracle Analytics Server</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>B</td>
<td>Enterprise Manager RDBMS Repository.</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>C</td>
<td>Fusion Middleware and Specific WebLogic Security Configurations.</td>
<td>Chapter 10 and 11</td>
</tr>
<tr>
<td>i</td>
<td>Optional configuration of Oracle HTTP Server (OHS)</td>
<td>Chapter 12</td>
</tr>
<tr>
<td>ii</td>
<td>Optional configuration of Oracle Access Manager (OAM) Single Sign On.</td>
<td>Chapter 13</td>
</tr>
<tr>
<td>3</td>
<td>Configuration of required Oracle Analytics Server Datasource(s).</td>
<td>Chapter 14</td>
</tr>
<tr>
<td>4</td>
<td>Installation of Oracle provided Out of Box Reports to the standalone OAS.</td>
<td>Chapter 15</td>
</tr>
<tr>
<td>5</td>
<td>Upgrading from Enterprise Manager 13.4 to Enterprise Manager 13.5.</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>A</td>
<td>Migrating schedules from the Enterprise Manager 13.4 embedded BIP.</td>
<td>Section 16.1</td>
</tr>
<tr>
<td>B</td>
<td>Migrating any customized BIP reports from the embedded BIP to the standalone OAS.</td>
<td>Section 16.3</td>
</tr>
<tr>
<td>8</td>
<td>Updating the Enterprise Manager 13.5 WebLogic Domain target.</td>
<td>Chapter 17</td>
</tr>
</tbody>
</table>

There is also a flow chart of the above items:
» Chapter 5 - Flow chart for all Procedures
CHAPTER 1. OVERVIEW OF BASE INSTALL AND CONFIGURATION OF OAS

There are four steps to get OAS installed and preliminarily configured.

All the binaries for the below items can be downloaded utilizing the standard Oracle eDelivery website.

1. Install Required JDK: JDK8: u251 or newer.
2. Install Fusion Middleware Control Infrastructure (do not configure).
3. Application of Fusion Middleware one-off patch.
4. Installation and configuration of OAS 5.5.0, and associated OAS Database Schema objects.

---

1 (Java Platform, Standard Edition - Release 8, 2020) JDK8
2 (Oracle® Fusion Middleware, 2020) Fusion Middleware
3 (OAS – Oracle WebLogic Server 12.2.1.4 Patch 30657796, n.d.) 30657796
4 (Configuring Oracle Analytics Server, 2021) OAS Configuration
CHAPTER 2. OVERVIEW OF POST INSTALL OF OAS

The steps in this document were specifically developed and tested against both Enterprise Manager 13.4 and Enterprise Manager 13.5.

Below is an outline of the steps needed to be followed the successful base install and configuration of OAS.

It is important to follow these detailed steps against Enterprise Manager 13.4, prior to upgrading to Enterprise Manager 13.5.

1. Configure the appropriate OAS security model and required roles.\(^5\)
2. Configure the OAS Datasource(s), for use with the Enterprise Manager repository database(s).\(^6\)
3. Configure the EM repository database such that EM administrators have access to EM data, when logged into the standalone OAS.

After the Enterprise Manager 13.5 upgrade

1. Install and utilize the Oracle provided out-of-the-box Reports.
2. Upload any customized reports from the prior release of EM.
3. Migrate the BIP Report Schedules from the embedded BIP in Enterprise Manager 13.4 to the standalone OAS.\(^7\)

---

\(^6\) (OAS - Set Up Data Sources, 2021) Data Sources
\(^7\) (Migrating Scheduler Jobs and Job History, 2021) Migrating Scheduler Jobs
CHAPTER 3. OVERVIEW OF OAS SECURITY CONFIGURATIONS

Enterprise Manager is generally configured with one of the security configurations shown below. The standalone OAS can then be configured to match, or map, to this same security configuration.

<table>
<thead>
<tr>
<th>ENTERPRISE MANAGER SECURITY CONFIGURATION</th>
<th>CORRESPONDING OAS SECURITY MODEL</th>
<th>NUMBER OF EM INSTALLS PER OAS INSTALL</th>
<th>UNDERLYING SECURITY STORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Repository-based security:</td>
<td>Database Security Model</td>
<td>One</td>
<td>• Enterprise Manager repository database system. (RDBMS):</td>
</tr>
<tr>
<td>• Default, out-of-box EM security configuration.</td>
<td></td>
<td></td>
<td>• All users and roles defined in the RDBMS.</td>
</tr>
<tr>
<td>• LDAP, with or without SSO:</td>
<td>Fusion Middleware</td>
<td>One or more</td>
<td>• LDAP server (i.e., OID or AD):</td>
</tr>
<tr>
<td>• Configured utilizing standard commands.</td>
<td></td>
<td></td>
<td>• All users and groups defined in the LDAP server.</td>
</tr>
</tbody>
</table>

Table 2. Mapping of Enterprise Manager Security Configurations to OAS Configuration

The following chapter provided an overview of the two Enterprise Manager Security Configurations from the table above.

---

CHAPTER 4. OVERVIEW OF ENTERPRISE MANAGER SECURITY

4.1 EM Repository based authentication.

Requirements:
» OAS ‘Database Security Model’
» Fallback ‘Superuser’
» Create required DBMS roles.
» Grant/Revoke these roles to appropriate Enterprise Manager administrator(s).
  » Note: Out of box, EM administrators have a corresponding DBMS user.
» Create the JDBC Datasource EMREPOS for use with Enterprise Manager.

4.2 LDAP-based authentication

Requirements:
» OAS ‘Fusion Middleware Security Model’
» corresponding Fusion Middleware Configuration,
» Configuration steps are required, utilizing the Fusion Middleware Control that is bundled with OAS
» Additional manual steps involving editing of specific Fusion Middleware configuration files.
» If EM is also utilizing SSO, OAS is to be likewise configured:
  • Manual configuration of additional Fusion Middleware configuration files.
  • Installation of Oracle HTTP Server (OHS) into the same domain as OAS.
  • Configuration of OHS Webgate in the OAS domain by editing additional Fusion Middleware configuration files.
  • Additional configuration of OAS.
» Configure the JDBC Datasource(s) EMREPOS [, EMREPOS2 [, EMREPOS3 ...]] for use with Enterprise Manager.
CHAPTER 5. FLOW CHART FOR ALL PROCEDURES

Figure 1. Flow Chart – Overview of installation and configuration steps

Standalone OAS Install and configuration (For use with Enterprise Manager)

Chapter 7 - Complete steps to install and configure OAS
7.1 - Install JDK: JDK8 : U251 Or Newer
7.2 - Install Fusion Middleware Infrastructure
7.3 - Install required Fusion Middleware one-off
7.4 - Install OAS
7.5 - Install latest OAS Bundle Path (OAS 5.5.0-201216 BP – 32294034)
7.6 - Configure OAS

Chapter 9
OAS For Enterprise Manager Repository-based

Chapter 9, Sections:
9.1 Create required DBMS roles and grant to required EM
9.2 Configure OAS for ‘Database Security Model’
9.3 Screenshots for Oracle Database Security Model

Chapter 10
OAS For Enterprise Manager LDAP Configuration

Chapter 10, Sections:
10.1 OAS Security Model Configuration
10.2 WebLogic Security Configuration

Chapter 11:
Procedure for Configuring WebLogic for LDAP

Chapter 12
OAS Optional Configuration of SSO on top of LDAP

Chapter 13

Is EM Utilizing OAM Single Sign on?

No

Yes
Figure 2. Flow Chart – Final steps - Continued from prior page

**Chapter 9, Sections:**

9.1 Create required DBMS roles and grant to required EM
9.2 Configure OAS for ‘Database Security Model’

**Chapter 12**

OAS Optional Configuration of SSO on top of LDAP

**Chapter 13**

OAS for Configuration of Oracle Access Manager SSO

**Chapter 14**

Configuration of required OAS Datasource(s)

Chapter 15

Installation of Oracle Provided Out of Box Reports

Chapter 16

Upgrading from EM 13.4 to EM 13.5

Chapter 17

Updating the EM 13.5 WebLogic Domain target
There are several distinct requirements to successfully upgrade from a prior release of EM, with the embedded BI Publisher, to the standalone OAS.

It is crucial that planning for the upgrade to EM 13.5 begin well prior to the upgrade.

The most important considerations are:

» Ensuring any customized BIP reports are available in the standalone OAS.

» Ensuring any prior BIP report schedules are migrated to the standalone OAS.

Complete details and examples are shown in “section Chapter 16 - Upgrading from EM 13.4 to EM 13.5”
CHAPTER 7. COMPLETE STEPS TO INSTALL AND CONFIGURE OAS

The following section details the standard installation and configuration of Oracle Analytics Server (OAS) 5.5.0.

The below 6 steps are detailed in section 7.1 through 7.6.

1. Installation of a supported Java Development Kit (JDK) [JDK8 : u251 or newer].
2. Installation of Fusion Middleware Infrastructure
3. Application of required one-off patch to Fusion Middleware.
4. Installation of the OAS binaries into the existing WebLogic Middleware Home.
5. Applying latest OAS 5.5.0 Bundle Patch using OPatch.
6. Configuration of OAS into the WebLogic Domain, along with the required Database schema objects.

The required installers for the first 5 steps can be downloaded from OTN or eDelivery, as appropriate.

<table>
<thead>
<tr>
<th>STEP</th>
<th>FILENAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>jdk-8u251-linux-x64.tar.gz</td>
<td>Required JDK for OAS</td>
</tr>
<tr>
<td>2</td>
<td>fmw_12.2.1.4.0_infrastructure.jar</td>
<td>Required FMW for OAS</td>
</tr>
<tr>
<td>3</td>
<td>p30657796_generic.zip</td>
<td>Required FMW one off for OAS</td>
</tr>
<tr>
<td>4</td>
<td>Oracle_Analytics_Server_5.5.0.jar</td>
<td>OAS Installer</td>
</tr>
<tr>
<td>5</td>
<td>p32294034_55000_Linux-x86-64.zip</td>
<td>Latest OAS Bundle Patch as of February 2021: OAS 5.5.0-201216 BP - 32294034</td>
</tr>
</tbody>
</table>

Table 3. Required OAS Installer

Throughout the rest of this document, example directories are color coded, as below:

<table>
<thead>
<tr>
<th>NOTATION</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>stagedir/OASMW</td>
<td>The ORACLE_HOME and MW_HOME for OAS</td>
</tr>
<tr>
<td>stagedir/java/jdk1.8.0_251</td>
<td>The JAVA_HOME</td>
</tr>
<tr>
<td>stagedir/30657796</td>
<td>Required FMW one off for OAS</td>
</tr>
<tr>
<td>stagedir/32294034</td>
<td>Latest OAS Bundle Patch as of February 2021: • OAS 5.5.0-201216 BP - 32294034</td>
</tr>
<tr>
<td>zipdir</td>
<td>Location of all Shiphomes and ZIP files</td>
</tr>
</tbody>
</table>

Table 4. Key to directories used in examples

---

(OAS: Quick Reference For In-Place Upgrade From Oracle Business Intelligence Enterprise 12c To OAS On Linux (Doc ID 2645014.1), 2020) 13
(Java Platform, Standard Edition - Release 8, 2020) 14
(Oracle® Fusion Middleware, 2020) 15
(OAS – Oracle WebLogic Server 12.2.1.4 Patch 30657796, n.d.) 16
(OAS - Installing the Oracle Analytics Server Software, n.d.) 17
(Required and Recommended Patches and Patch Sets For Oracle Business Intelligence 12c and Oracle Analytics Server (Doc ID 2070465.1), n.d.) 18

18 © 2021, Oracle and/or its affiliates | Confidential – Public
7.1 Install JDK: JDK8 : U251 Or Newer

Choose the location for the JAVA HOME, and untar the distribution jdk-8u251-linux-x64.tar.gz

```bash
# Create JAVA_HOME staging area
$ mkdir -p stagedir/java
$ cd stagedir/java
$ pwd
stagedir/java

# Set required environment
$ JAVA_HOME=stagedir/java/jdk1.8.0_251 ; export JAVA_HOME
$ echo $JAVA_HOME
stagedir/java/jdk1.8.0_251

# Install Java bits
$ tar xzf zipfile/jdk-8u251-linux-x64.tar.gz
$ ls jdk1.8.0_251
bin  include  lib  man
....
$ cd $HOME
```

7.1.1 Confirm Correct Installation

```bash
$ PATH=$JAVA_HOME/bin:$PATH; export PATH
$ which java
stagedir/java/jdk1.8.0_251/bin/java
$ java -version
java version "1.8.0_251"
Java(TM) SE Runtime Environment (build 1.8.0_251-b08)
Java HotSpot(TM) 64-Bit Server VM (build 25.251-b08, mixed mode)
```
7.2 Install Fusion Middleware Infrastructure

**NOTE:** FMW is always a software-only install.

```
$ MW_HOME=stagedir/OASMW ; export MW_HOME
$ mkdir -p $MW_HOME
$ cd $MW_HOME
$ java -jar zipsdir/fmw_12.1.4.0_infrastructure.jar
```

7.2.1 First Oracle product being installed on this system

A preliminary screen is presented for the first Oracle Product Installed on a System:

1. Enter the directory location for Oracle Inventory files.
2. Enter the operating system group for Oracle Inventory files.

7.2.2 Step 1 – Welcome; Step 2 – Auto Updates

7.2.3 Step 3 – Installation Location

For the **Oracle Home**, choose the MW_HOME location from above (i.e., `<stagedir>/OASMW`)

7.2.4 Step 4 – Installation Type

Choose ‘Fusion Middleware Infrastructure’
7.2.5 Step 5 – Prerequisite Checks; Step 6 – Installation Summary

7.2.6 Step 7 – Installation Progress; Step 8 – Installation Complete

**NOTE:** OAS comes with its own configuration tools, do not run $MW_HOME/oracle_common/common/bin/config.sh
7.3 Install required Fusion Middleware one-off

```bash
$ PATH=$MW_HOME/OPatch:$PATH
$ cd stagedir
$ export ORACLE_HOME=$MW_HOME
$ cp -rp zipsdir/30657796 .
$ cd 30657796
$ opatch apply
```
7.4 Install OAS

```
$ cd $MW_HOME
$ java -jar zipsdir/Oracle_Analytics_Server_5.5.0.jar
```

7.4.1 Step 1 – Welcome ; Step 2 Auto Updates

7.4.2 Step 3 – Choose Oracle Home

Enter the same value here as was chosen for Fusion Middleware (‘section 7.2.3 - Step 3 – Installation Location’)

7.4.3 Step 4 – Pre-requisite Checks
7.4.4 Step 5 – Installation Summary

Installation Summary

- Welcome
- Auto Updates
- Installation Location
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

- Install oa_platform
- Installation Location
  - Oracle Home Location: <stagedir>/OASMN
  - Log File Location: <stagedir>/OASMN/

- Disk Space
  - Required: 7385 MB
  - Available: 231763 MB

7.4.5 Step 6 – Installation Progress

Installation Progress

Welcome
- Auto Updates
- Installation Location
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

- 100%
- Prepare
- Copy
- Generating Libraries
- Performing String Substitutions
- Linking
- Setup
- Saving the Inventory
- Post Install Outputs

7.4.6 Step 7 – Installation Complete

Installation Complete

Welcome
- Auto Updates
- Installation Location
- Prerequisite Checks
- Installation Summary
- Installation Progress
- Installation Complete

- Install oa_platform
- Installation Location
  - Oracle Home Location: <stagedir>/OASMN
  - Log File Location: <stagedir>/OASMN/
7.5 Install latest OAS Bundle Path (OAS 5.5.0-201216 BP – 32294034)
Install using standard OPatch procedures:

```
$ cd stagedir
$ unzip p32294034_55000_Linux-x86-64.zip
$ export ORACLE_HOME=$MW_HOME
$ cd 32294034
$ $MW_HOME/OPatch/opatch apply
```

7.6 Configure OAS
For full details, see (Configuring Oracle Analytics Server, 2021) reference

```
$ cd $MW_HOME/bi/bin
$ ./config.sh
```

» Ensure to use the default domain name (bi).
» Make sure no other Fusion Middleware products are running on the same physical host.
  » If you absolutely must run two or more FMW products on the same host, the following requirements must be met.
    o All WebLogic domain(s) must be in 'production mode'.
    o Ensure that that all 'defaultCoherenceClusters', within each WebLogic cluster, in each and every domain, use 'unicast addressing'.
    o Also ensure that each defaultCoherenceClusters has a unique listen port.
  » The symptoms of this failure are that one or more managed servers, in one or more domains, will fail to start.
  » The reasons for these restrictions are:
    o licensing requirements of the Coherence Clustering technology, which is utilized by the WebLogic Cluster technology.
    o TCP/IP Port Requirements.
  » It is extremely difficult to triage and debug this failure condition.
» By convention, the schema prefix for the OAS required database schema shall be ‘oas’.

---

*Because of these complexities, it is highly recommended that a host be dedicated for OAS.*
OAS Configuration Screenshots

7.6.1 Step 1 - Welcome Screen

Figure 3. Step 1 of 10: Start OAS Configuration

7.6.2 Step 2 - Configuration

Figure 4. Step 2 of 10: Only configure Oracle Analytics Publisher

NOTE: It is extremely important to only select “Oracle Analytics Publisher”
7.6.3  Step 3 - Prerequisite Checks

Figure 5.  Step 3 of 10: Prerequisite Checks

» Make sure that all Prerequisite checks pass.
7.6.4 Step 4 - Define Domain

» For this example, the MW_HOME for OAS is chosen as:
  » /u01/oracle/OAS

» And the domain is chosen as:
  » /u01/oracle/OAS/user_projects/domains/bi

![Step 4 of 10: Define Domain](image)
7.6.5  Step 5 - Database Details

» The best practice is to choose the schema prefix:

  » oas

» The OAS schema can be installed either on a dedicated Oracle RDBMS or co-located on the same database utilized for the Enterprise Manager Repository.

» An Example of a dedicated OAS DBMS connect descriptor:
  ○ oasrepos.example.com:1521:orcl

7.6.6  Step 6 - Port Management

» The default ranges from 9500 to 9999 should be adequate.
7.6.7  Step 7 - Initial Application

It is critical that the radio button for “Clean Slate (no predefined application)” is chosen.

Figure 9.  Step 7 of 10: Initial Application
7.6.8  Step 8 - Summary

» As soon as the 'Configure' button is pressed, the configuration process begins.
» It can take some time for this to complete, and the real-time status can be monitored in the windows below.

7.6.9  Step 9 - Configuration Progress

Figure 10.  Step 8 of 10: Summary

Figure 11.  Step 9 of 10: Configuration Progress
7.6.10 Step 10 - Configuration Complete

» When the configuration is complete, details of the environment are presented below.

» Please take note of these, as they are required in order to utilize OAS.

Figure 12. Step 10 of 10: Configuration Complete
CHAPTER 8. OAS SECURITY CONFIGURATION

This chapter provides an overview of the remaining configuration steps, which are somewhat complex.

BEFORE BEGINNING THE PROCEDURES DOCUMENTED IN THIS HANDBOOK, DOWNLOAD ANY CUSTOMIZED BIP REPORTS FROM THE EMBEDDED BIP IN EM 13.4, USING THE BIP USER INTERFACE.

There are two distinct OAS security models that are fully documented below.

Each of these two OAS security models map directly to a corresponding Enterprise Manager Security Configuration.

- A single installation of OAS can only support one of the two security models below at any given time.

<table>
<thead>
<tr>
<th>EM SECURITY CONFIGURATION</th>
<th>OAS SECURITY MODEL AND ADDITIONAL REQUIRED STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enterprise Manager Repository-based security</td>
<td>OAS Database Security Model</td>
</tr>
<tr>
<td>• Out of box configuration</td>
<td>Additional steps:</td>
</tr>
<tr>
<td></td>
<td>2. On EM Repository DBMS, perform DBMS role assignments.</td>
</tr>
<tr>
<td>2. LDAP</td>
<td>OAS Fusion Middleware Security Model</td>
</tr>
<tr>
<td>a. Without Single Sign On (SSO)</td>
<td>Additional steps:</td>
</tr>
<tr>
<td>b. With Single Sign On (SSO)</td>
<td>1. Ensure OAS is configured for Fusion Middleware Security Model.</td>
</tr>
<tr>
<td></td>
<td>2. On OAS WebLogic Domain:</td>
</tr>
<tr>
<td></td>
<td>a. WebLogic Authentication Provider configuration.</td>
</tr>
<tr>
<td></td>
<td>b. Fusion Middleware Control Application Role assignments.</td>
</tr>
<tr>
<td></td>
<td>c. Edits to Java Platform Services (JPS) configuration file.</td>
</tr>
<tr>
<td></td>
<td>3. Further configuration steps for SSO on OAS WebLogic Domain:</td>
</tr>
<tr>
<td></td>
<td>a. Additional WebLogic Authentication provider configuration.</td>
</tr>
<tr>
<td></td>
<td>b. Installation of Oracle HTTP Server (OHS).</td>
</tr>
<tr>
<td></td>
<td>c. Configuration of OHS with Oracle Webgate.</td>
</tr>
<tr>
<td></td>
<td>d. Oracle Access Manager (OAM) configuration.</td>
</tr>
<tr>
<td></td>
<td>e. Ensure OAS is a partner OAM application.</td>
</tr>
<tr>
<td></td>
<td>f. Edits to OHS Configuration files.</td>
</tr>
</tbody>
</table>

Table 5. OAS Security Configuration Steps

In order to change the OAS Security Model, access to the OAS Administration link, and the subsequent Administration screens, as shown in ‘Figure 17 - Administration Screens and Security Center. Needed for Security Configuration’, it is necessary to login to OAS as a user with the required permissions to access these pages.

When OAS is initially installed, the OAS Fusion Middleware security model is configured by default.

In this configuration, the weblogic user will always be available, with the password that was chosen during OAS configuration. See ‘section 7.6.4 - Step 4 - Define Domain’.

Additionally, the weblogic user will by default have the required permissions to access the Administration screens.

If mistakes are made, and login to OAS using standard procedures is unavailable, or no user has the required permissions to access to the Administration link (and subsequent Administration screens), then there is no way to resolve issues using the OAS user interface and manual edits to XML configuration files would be required.

Given this, it is strongly recommended to enable the internal Superuser during these initial configuration steps.

This special Superuser does not rely on any underlying OAS security model, but instead utilizes the simpler file-based security model that is built-in to OAS.

For simplicity and proper management of OAS, ensure that the username chosen for this internal OAS Super User does not overlap with a real Enterprise Manager (or LDAP) user.

For example, do not use the name sysman.
8.1 Oracle Analytics Publisher Authentication and Report Execution Flow

There are four main interactions that all Enterprise Manager Administrators will utilize when Oracle Analytics Publisher is accessed.

1. Oracle Analytics Server Authentication
2. Oracle Analytics Server User Interface Capabilities.
3. Oracle Analytics Server Catalog Access.

8.1.1 OAS Authentication

As specified above, for Enterprise Manager 13.5, two main mechanisms for user authentication are provided:

1. Enterprise Manager Repository-based Security
2. LDAP, with or without SSO, based upon Fusion Middleware Security Providers.

8.1.2 OAS User Interface Privileges

OAS supports three hierarchical levels of User Interface Privileges. As the levels below are followed, they are additive.

All capabilities from level 1 are available in level 2, and all capabilities from level 1 and level 2 are available in level 3, and all capabilities from levels 1, 2, and 3, are available in level 4.

<table>
<thead>
<tr>
<th>#</th>
<th>DESCRIPTION</th>
<th>DBMS ROLE</th>
<th>LDAP ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>View and execute OAS Reports.</td>
<td>MGMT_USER</td>
<td>BI Consumer</td>
</tr>
<tr>
<td>2</td>
<td>Schedule OAS Reports</td>
<td>XMLP_SCHEDULER</td>
<td>BI Consumer: Includes</td>
</tr>
<tr>
<td>3</td>
<td>Author OAS Reports (and manipulate catalog objects, see next table).</td>
<td>XMLP_DEVELOPER</td>
<td>BI Author</td>
</tr>
<tr>
<td>4</td>
<td>Administer OAS</td>
<td>XMLP_ADMIN</td>
<td>BI Administrator</td>
</tr>
</tbody>
</table>

○ Manage and maintain the OAS Security Model.
○ Manage and maintain the OAS Data Source Configuration (i.e., EMREPOS, EMREPOS2, etc.)
○ Manage and maintain the OAS Scheduler.
○ General OAS System Administration.

Table 6. OAS Privileges
8.1.3 OAS Server Catalog Access

The same Role Names specified above are also utilized to provide varying levels of access to each OAS Catalog Object (reports, Datamodels, folders).

Typically, these Role Names are applied in a similar hierarchical manner as User Interface Level Access.

This works out as below:

<table>
<thead>
<tr>
<th>#</th>
<th>DESCRIPTION</th>
<th>DBMS ROLE</th>
<th>LDAP ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EM REPOSITORY BASED</td>
<td>LDAP, WITH OR WITHOUT SSO</td>
</tr>
</tbody>
</table>
| 1 | • View Reports, and corresponding Datamodels.  
   • Expand Folder Nodes.  
   • Execute Reports (not applicable to Datamodels). | MGMT_USER | BI Consumer |
| 2 | • Schedule OAS Reports. | XMLP_SCHEDULER | BI Consumer  
   *(there is no separate FMW Scheduler Role by default)* |
| 3 | • Edit, Cut/Copy/Paste/Delete OAS Catalog Objects (i.e. Reports, Datamodels, and folders). | XMLP_DEVELOPER | BI Author |
| 4 | • Full Capabilities on all Catalog Objects | XMLP_ADMIN | BI Administrator |

Table 7. OAS Catalog Permissions

8.1.4 OAS Report Execution

Once an Enterprise Manager Administrator is logged into OAS, and has access to an OAS Report, the report itself can be executed (or scheduled).

When an OAS Report Executes, the execution model from Enterprise Manager 13.4 is maintained.

That is, for a given user logged into OAS, OAS Reports will only have target-level access to those Enterprise Manager Targets that that EM Administrator normally would have access to.

In this way, EM Data can be viewed inside of OAS with the same visibility as when utilizing the Enterprise Manager Console directly.

The following two sections provide a flow chart of the two main components of OAS Report Execution.

1. OAS Login Flow – Valid or invalid credentials provided.
2. OAS privilege assignment – If a user is valid, associate roles.
8.1.5 OAS Login Processing

Figure 13. OAS Login flow
8.1.6 OAS Privilege Assignment

Figure 14. OAS Privilege Assignment flow

OAS Privilege Assignment

From OAS Login Flow

Username

OAS Security Model

DBMS

FMW

Fusion Middleware

EM Repository DBMS

WebLogic LDAP Authenticator

OPSS Policy Store

1 or more from:
- MGMT_USER
- XMLP_DEVELOPER
- XMLP_SCHEDULER
- XMLP_ADMIN

1 or more from:
- BI Consumer
- BI Author
- BI Administrator

OAS UI

- Administration Links?
- Create/Edit Report Objects?
- Schedule Reports?
- Catalog Access (per report object)
CHAPTER 9. OAS FOR ENTERPRISE MANAGER REPOSITORY-BASED SECURITY

From this point forward, the required steps are complex, and somewhat error prone.

This chapter details configuration of the standalone OAS against an Enterprise Manager Installation using the default security configuration of ‘Repository based Authentication’.

For this configuration of EM, the OAS ‘Database Security Model’ is utilized.

» Before proceeding with the steps documented in this chapter, make certain that the steps in ‘7.5 - Install latest OAS Bundle Path (OAS 5.5.0-201216 BP – 32294034)’ have been followed.

» If for some reason you were to proceed with the steps in this chapter prior to applying the above bundle patch, login to OAS would be restricted to the SuperUser account.

9.1 Create required DBMS roles and grant to required EM administrators.

Create the required roles, and minimal role grants, on the Enterprise Manager repository database:

```
$ sqlplus sys/******** as sysdba
sql> REM Create base roles
sql> create role XMLP_ADMIN;
sql> create role XMLP_DEVELOPER;
sql> create role XMLP_SCHEDULER;
sql>
sql> REM Create Role Hierarchy
sql> grant XMLP_DEVELOPER to XMLP_ADMIN;
sql> grant XMLP_SCHEDULER to XMLP_ADMIN;
sql> grant MGMT_USER to XMLP_ADMIN;
sql> grant XMLP_SCHEDULER to XMLP_DEVELOPER;
sql> grant MGMT_USER to XMLP_DEVELOPER;
sql>
sql> REM Sysman gets super admin
sql> grant XMLP_ADMIN to sysman;
sql> exit;
```

When additional Enterprise Manager users need OAS permissions beyond basic report viewing, one or more of the above roles will need to be granted to them. For example:

```
$ sqlplus sys/******** as sysdba
sql> REM Grant any required roles to individual EM Administrators
sql> grant XMLP_DEVELOPER to USER1;
sql> grant XMLP_SCHEDULER to USER2;
sql> exit;
```

These roles form the basis of the termination in the flow chart from section 8.1.6 - OAS Privilege Assignment:

```
1 or more from:
- MGMT_USER
- XMLP_DEVELOPER
- XMLP_SCHEDULER
- XMLP_ADMIN
```

9.2 Configure OAS for ‘Database Security Model’

The complete set of steps are outlined below, followed by example screenshots:

- Login to OAS as the **weblogic** user.
- Click on the **Administration** link in the top right-hand section of the user interface.
- Change the security model to **Oracle Database**.

9.3 Screenshots for Oracle Database Security Model

9.3.1 Step 1 - Login to OAS as the weblogic user

![Login to OAS as the weblogic user](image1.png)

**Figure 15. Login to OAS as the weblogic user**

9.3.2 Step 2 - Click on ‘Administration’ link

Towards the top right-hand section of the OAS user interface, above the **Open** link, and to the left of the **Help** link, click on the **Administration** link.

![Click on the Administration link](image2.png)

**Figure 16. Click on the Administration link**
9.3.3 Step 3 - Security Configuration (located under Security Center)

After the **Administration** link is pressed, the **Administration** screen below should be shown.

- Underneath the Security Center label, choose Security Configuration.

![Administration Screens and Security Center](image)

**Figure 17.** Administration Screens and Security Center. Needed for Security Configuration
9.3.4 Step 4 - Enable the local Superuser

» OAS supports a special account that can access the OAS Administration screens irrespective of the security model chosen.

» This special account is not designed to be utilized for running or scheduling reports, but only to administer OAS.

Proceed with these steps to enable this special account:

» Click the check-box next to Enable Local Superuser.

» Enter a username and password, for example:

  » User: SuperUser
  » Password: ●●●●●●

Figure 18. Enable local Superuser
9.3.5 Step 5 - Change the Security Model to Oracle Database
As this is an error prone manual operation, detailed instructions and examples follow.

» The items **marked in blue** below need to be determined based on the specific Enterprise Manager repository database that OAS is to be utilized with.

» The items **marked in green** will be different than shown in the examples below.

9.3.6 Step 6 - Determining the proper value for the Connection String
Please note that Oracle SIDs have been deprecated since Oracle DBMS 12c.

» For Oracle DBMS 18c and newer, SIDs do not work well at all, given the new container database (CDB) and pluggable database (PDB) architecture.

» Please ignore the example options presented in the connect string fields inside of OAS.

For the examples below:

<table>
<thead>
<tr>
<th>orcl.example.com – The Container Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdborcl.example.com – A Pluggable Database inside of the above Container Database</td>
</tr>
</tbody>
</table>

With the required SERVICE_NAME, the mechanism that JDBC utilizes to differentiate between the deprecated ORACLE_SID and the SERVICE_NAME is a bit confusing.

To utilize SIDs one used to specify the below notation. Notice that the last element is prefixed with a ‘:’.

```plaintext
jdbc:oracle:thin:@emepos.example.com:1521:orcl
```

Since SIDs are longer supported, the full notation is just a bit different.

Notice the final colon ‘:’ is replaced with a forward slash ‘/’:

```plaintext
jdbc:oracle:thin:@//emrepos.example.com:1521/orcl.example.com
```

The ‘//’ is optional, so this also works:

```plaintext
jdbc:oracle:thin:@emrepos.example.com:1521/orcl.example.com - Container Database
jdbc:oracle:thin:@emrepos.example.com:1521/pdborcl.example.com - Pluggable Database
```

9.3.7 Step 7 - Determining the Administrator Username
The Administrator password to use is straightforward, it is simply the **sysman** password.

9.3.8 Step 8 - Example values

<table>
<thead>
<tr>
<th>Security Model: Oracle Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection String: jdbc:oracle:thin:@//emrepos.example.com:1521/orcl.example.com</td>
</tr>
<tr>
<td>Or</td>
</tr>
<tr>
<td>Connection String: jdbc:oracle:thin:@//emrepos.example.com:1521/pdborcl.example.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administrator Username: sysman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Password: ●●●●●●</td>
</tr>
</tbody>
</table>

| Database Driver Class: oracle.jdbc.driver.OracleDriver |
9.3.9  Step 9 - Confirming values using example above
To test out the above settings, before applying them in OAS, a small Java program is included to perform this test easily, without starting and stopping OAS.

Please see the small program, and instructions in ‘Appendix I Validating JDBC Connect String’.

9.3.10  Step 10 - Setting the OAS Security Model to “Oracle Database”
Scroll down to the Authorization section and fill in the appropriate fields.

- Make sure that ‘Use LDAP’ is not checked.
- Make sure that the Security Model is set to Oracle Database
- Fill in the appropriate connect descriptor for the Enterprise Manager Repository DBMS.
- Ensure to provide the sysman credentials.

![Figure 19. Configure OAS for Oracle Database Security Model](image)

NOTE: The database connection string and credentials are for the EM Repository database, and not for the OAS database.
9.3.11  Step 11 - Hit apply

![Apply Security Model Changes](image)

9.3.12  Step 12 - Shutdown OAS

Use the instructions and screenshots from ‘Appendix A - Shutting down OAS using the WebLogic console’ to shutdown OAS.

9.3.13  Step 13 - Startup OAS

Use the instructions and screenshots from ‘Appendix B - Starting OAS using the WebLogic Console’ to start OAS.
CHAPTER 10. OAS FOR ENTERPRISE MANAGER LDAP CONFIGURATION

Whether Enterprise Manager is configured with LDAP alone, or LDAP along with Single Sign-on, the steps in this chapter are a required step.

For this configuration of EM, the default OAS 'Fusion Middleware Security Model' is utilized.

There are several required steps for this configuration:

1. Configure OAS using a straightforward procedure.
2. Configure WebLogic for LDAP.
3. Configure the OAS WebLogic Domain for LDAP.
5. Grant OAS Fusion Middleware Application roles to EM LDAP Users and/or LDAP Groups utilizing Fusion Middleware Control.

If SSO is required, on top of LDAP, there are several more steps.

1. Install Oracle HTTP Server (OHS).
2. Extend the OAS WebLogic Domain with the collocated OHS using the `config.sh` script.
3. Configure OHS for OAS using Fusion Middleware Control.
4. Configure Oracle Webgate, running on top of OHS.
5. Configure and add the OAM Identity Asserter to the list of WebLogic Security Providers.
6. Reorder the WebLogic Authentication Providers.
7. Perform the OAS Required Steps.
8. Edit `ServerName` directive in `httpd.conf`.

Regardless of whether SSO is configured, additional steps are required to map EM Users and/or LDAP groups (if appropriate) to Fusion Middleware Application Stripe Roles.

The specific UI access and catalog permissions are shown in section 8.1.2 - OAS User Interface Privileges, and section 8.1.3 - OAS Server Catalog Access.
10.1 OAS Security Model Configuration

Due to possible user errors locking out access to OAS, a fallback 'Super User' is highly recommended.

Screenshots for OAS Security Configuration

10.1.1 Step 1 - Login to OAS as the ‘weblogic’ user

» Or if needed, and configured, the local SuperUser.

Figure 21. Login to OAS as the weblogic user (or local superuser)

10.1.2 Step 2 - Click on ‘Administration’ link

Towards the top right-hand section of the OAS user interface, above the Open link, and to the left of the Help link, click on the Administration link.

Figure 22. Click on the Administration link
10.1.3 Step 3 - Choose ‘Security Configuration’ (under ‘Security Center’)

![Image of Oracle Analytics Server interface]

Figure 23. Choose Security Configuration underneath security Center

10.1.4 Step 4 - Fill in required entries for the ‘Local Superuser’:

- Click the check-box next to ‘Enable Local Superuser’.
  - Enter a username and password, for example:
    - User: SuperUser
    - Password: ●●●●●●

![Image of Oracle Analytics Server interface showing local superuser configuration]

Figure 24. Enable local Superuser
10.1.5 Step 5- Confirm correct configuration of ‘Fusion Middleware Security Model’

» Make sure that **Use LDAP** is **not** checked.

» Make sure that the Security Model is set to **Oracle Fusion Middleware**.

» Make that **Fusion Apps Security** is **not** checked.

Figure 25. Ensure that **Oracle Fusion Middleware** Security Model is configured correctly.
10.2 WebLogic Security Configuration

The overall goal of these sections is to configure the OAS WebLogic domain’s Security Configuration in such a way that it is functionally identical to Enterprise Manager’s WebLogic domain Security Configuration.

**config.xml**

Inspection of specific details of the WebLogic domain(s) can be found in the `config.xml` file, for the respective WebLogic domains (i.e., the Enterprise Manager WebLogic Domain and/or the standalone OAS WebLogic Domain).

Under no circumstances should the `config.xml` file be directly edited or manipulated directly.

Ensure that all inspection of the `config.xml` is done in **read-only** mode (i.e., using the command-line tools [more, less, view, vi -r]).

Editing the `config.xml`, even if backups are made beforehand, can result in corruption of the WebLogic domain.

**Approved Fusion Middleware Tools**

Throughout the rest of these sections, all examples will utilize the below WebLogic tools.

» WebLogic Console
» Fusion Middleware Control
» WLST Scripting tool.

The screenshots will consistently display the OAS WebLogic console on the left-hand side of the screenshot, and the EM WebLogic console is on the right-hand side of the screenshot.

The easiest approach for implementing the screenshots on the following pages is to bring up the WebLogic console for the EM domain side-by-side with the OAS WebLogic domain.

» Due to certain limitations in the WebLogic console’s user interface, it is necessary to utilize two separate browser sessions.

One approach is to use a specific browser for each of the WebLogic consoles (i.e., Chrome for EM, and Firefox for OAS).

**Preliminary Steps**

For each WebLogic console, it is necessary to get to the Authentication Providers screen.

To navigate to the Authentication Providers screen, on both WebLogic consoles, follow the four steps below (screen shots are on the next page).

1. Login to the WebLogic console as the weblogic user
2. On the left-hand side of the browser window, underneath the Domain Structure, click on the link for Security Realms.
   
   » The list of security realms is shown. There should just be one realm, named myrealm.
3. Click on myrealm.
   
   » The settings for myrealm are shown.
4. Click on the tab for Providers.

Remember, these four steps must be performed for each WebLogic console.

The OAS console should be on the left-hand side of your desktop, and EM on the right-hand side.

If the above four steps are performed correctly, then you will see screens similar to what is shown in either Figure 29 - Comparison of WebLogic Security Configurations – Oracle Internet Directory, or in Figure 30 - Comparison of WebLogic Security Configurations – Microsoft Active Directory.
10.2.1  Step 1 - Login to WebLogic console
-  http://oas.example.com:9500/console

![Step 1: Logic to WebLogic Consoles](image)

10.2.2  Step 2 - Click on Security Realms

![Step 2: Click on Security Realms for each WebLogic console](image)

10.2.3  Step 3 - Click on myrealm and then the Providers tab

![Step 3: Click on myrealm and then the Providers tab in each WebLogic console](image)
10.2.4 Step 4 - Comparison of WebLogic Security between EM and OAS

In the screenshots below, the default WebLogic Security Configuration for OAS is shown on the left. The WebLogic Security Configuration for an Enterprise Manager that is configured to utilize Oracle Internet Directory (OID), and Microsoft Active Directory, respectively, as the LDAP store, is shown on the right.

Please note that these Enterprise Manager Screenshots are from sites with either OID or AD, but without SSO.

The following two screenshots provide some more details of the two separate domains.
10.2.5 Step 5 - WebLogic Security Configuration for OAS

In the end, the overall goal is to configure the OAS WebLogic domain to process authentication requests in a similar manner as EM.

For more details on the WebLogic Authentication Architecture, please refer to 'Appendix J - WebLogic Authentication Providers'.
10.2.7 Step 7 - Overall goal of configuring OAS identically to EM

To repeat, the overall goal is to configure the OAS WebLogic Domain similarly to EM.

When we begin this procedure, this is the comparison between the two WebLogic domains (using OID, without SSO).

---

### Figure 33.  Comparison of OAS WebLogic Domain to EM WebLogic domain at beginning of procedures

At the end of the series of steps on the following pages, the results will look like the below screen shot (without SSO).

### Figure 34.  Comparison of OAS WebLogic Domain to EM WebLogic Domain after successful completion of procedures

---

*Note: We are not modifying or changing anything in the EM WebLogic Domain, but simply using it to assist in the configuration of the OAS WebLogic Domain.*
CHAPTER 11. PROCEDURE FOR CONFIGURING WEBLOGIC FOR LDAP

Returning to the earlier discussion, the easiest approach to achieving parity between the OAS WebLogic Domain, and EM’s WebLogic Domain, is to use a specific browser for each of the WebLogic consoles (i.e. Chrome for EM, and Firefox for OAS).

Bring up the WebLogic console for the EM domain side-by-side with the OAS WebLogic domain.

The screenshots in the remainder of this section assume that the OAS WebLogic console is on the left-hand side of the desktop, and the EM WebLogic console is on the right-hand side.

For each WebLogic console, it is necessary to get to the Authentication Providers.

To navigate to this screen, on both WebLogic consoles, follow these four steps:

1. Login to the WebLogic console as the weblogic user
2. On the left-hand side of the browser window, underneath the Domain Structure, click on the link for Security Realms.

   » The list of security realms is shown. There should just be one realm, named myrealm.
3. Click on myrealm.

   » The settings for myrealm are shown.
4. Click on the tab for Providers.

Screenshots for each of these steps are shown in Sections 10.2.1, 10.2.2, 10.2.3, and Error! Reference source not found..

» Remember, these four steps must be performed for each WebLogic console.

» Repeating, the OAS console will be on the left-hand side of your desktop, and EM on the right-hand side.
If these four steps are performed correctly, then you will see WebLogic console similar to what is shown in (Figure 33 - Comparison of OAS WebLogic Domain to EM WebLogic domain at beginning of procedures).

11.1 Step 1 – Prepare to edit the runtime configuration of the OAS WebLogic Domain

To perform editing operations on a Production WebLogic Domain (the default) it is necessary, while logged into the WebLogic console as the weblogic user, to click on Lock & Edit.
11.2 Step 2 - Configure WebLogic Provides

Add a new WebLogic Authentication Provider for either Oracle Internet Directory (OID) or for Microsoft Active Directory.

Make sure that you have navigated correctly to the Settings for myrealm and Make sure that the first tab Authentication is in focus.

**Steps:**

1. Click on the New button.
2. In the text box for the Name: field, choose a name as appropriate:
   - BIP_OID_Provider or BIP_AD_Provider
3. In the drop-down for the Type: field, scroll down, and choose as appropriate:
   - OracleInternetDirectoryAuthenticator
   Or:
   - ActiveDirectoryAuthenticator

Click on the OK button.

---

**Oracle Internet Directory**

![Oracle Internet Directory](image)

**Microsoft Active Directory**

![Microsoft Active Directory](image)

**Figure 36. Add the BIP_OID_Provider or BIP_AD_Provider to OAS WebLogic Domain**
11.3 Step 3 - Re-order the providers

If Single Sign-on (SSO), with Oracle Access Manager (OAM), it is necessary to re-order the providers such that the OAM Identity Asserter is first, followed by either the Oracle Internet Directory (OID) Authenticator, or the Microsoft Active Directory Authenticator (AD).

The screen shot below demonstrates re-ordering the providers such that the BIP_OID_Provider is moved up.

![Reorder OAS WebLogic Authentication Providers](image)

**Figure 37.** Reorder OAS WebLogic Authentication Providers to match EM WebLogic Domain Provider’s order.

11.4 Step 4 – Confirm correct ordering of providers

![Correct order of WebLogic Authentication Providers](image)

**Figure 38.** Correct order of WebLogic Authentication Providers – Oracle Access Manager (SSO) with OID
11.5 Step 5 – Change the OID Provider to SUFFICIENT

By default, both the BIP_OID_Provider and the BIP_AD_Provider are configured as \textbf{OPTIONAL}, due to WebLogic defaults.

It is necessary to change the appropriate provider, either OID or AD, to \textbf{SUFFICIENT}.

Change the Control Flag: drop-down from \textbf{OPTIONAL} to \textbf{SUFFICIENT}

» This needs to ensure the OAS WebLogic Domain is like the EM WebLogic Domain.

Figure 39. \textbf{Change BIP_OID_Provider from OPTIONAL to SUFFICIENT}
11.6 Step 6 – Configure OID Provider for OAS WebLogic Domain

The next step is to configure the OID Provider for OAS WebLogic Domain to match EM’s WebLogic Domain.

The following sub-sections detail the required configuration requirements that are specific to the BIP_OID_Provider.

» Each WebLogic Authenticator supports provider-specific configuration parameters.

The overall goal is to configure the BIP_OID_Provider’s **Provider Specific** configuration parameters to match the EM_OID_Provider’s **Provider Specific** configuration parameters.

The configuration settings for the **Oracle Internet Directory** provider specific parameters are quite complex.

*Due to the large size of the configuration parameters screen, three screenshots are shown for the single configuration screen*

The procedure will be to copy entries from the right side of your desktop (with the EM WebLogic Domain) to the left side of your desktop (with the OAS WebLogic Domain).

![Configuration Screenshot]

**Figure 40.** Configure BIP_OID_Provider’s **Provider Specific** parameters to match EM_OID_Provider’s **Provider Specific** parameters.
11.6.1 1st Section of OID Provider Specific Configuration Parameters

1) Provide the Hostname of the common LDAP server to be shared between EM and OAS.
2) Provide the same port for OAS as EM is using.
3) Provide same principal for OAS as EM is using.
4) Provide same credential for OAS as EM is using.
5) Copy/Paste the following items from EM to OAS:
   a. User Base DN
   b. All Users Filter
   c. Users from Name Filter
6) Ensure to select Use Retrieved Username as Principal

![Image](image1.png)
Figure 41. First Section of BIP_OID_Provider changes

![Image](image2.png)
Figure 42. Ensure that Use Retrieved User Name as Principal is checked
11.6.2 2nd Section of OID Provider Specific Configuration Parameters

1) Copy/Paste the following items from EM to OAS:
   a. Group Base DN
   b. All Groups Filter
   c. Group from Name Filter

2) Copy/Paste Static Group DNs from Member DN... from EM to OAS.
### 3\textsuperscript{rd} Section of OID Provider Specific Configuration Parameters

1. Copy/Paste Results time limit from EM to OAS.
2. Make sure radio buttons are not selected.

---

#### Figure 44: Third Section of BIP_OID_Provider changes
11.7 Step 7 – Change the DefaultAuthenticator from REQUIRED to SUFFICIENT

The DefaultAuthenticator must be changes from REQUIRED to SUFFICIENT, otherwise logins will fail.

Be sure to save the changes.

![Image of DefaultAuthenticator setting](image)

Figure 45. Change DefaultAuthenticator from REQUIRED to SUFFICIENT

11.8 Step 8 – Save and Activate the changes

11.9 Step 9 - Restart the OAS WebLogic Domain’s Managed Servers

To restart the OAS WebLogic Domain, the following Managed Servers need to be stopped and then started. The easiest approach is to bounce the whole stack:

- Bring Down OAS and Admin Server – See ‘Appendix A’
- Bring Down Node Manager – See ‘Appendix C’
- Start Node Manager – See ‘Appendix D’
- Start Admin Server – See ‘Appendix F’
11.10 Step 10 - Configuration of Java Platform Services (JPS)

To fully utilize an LDAP Server, such as Oracle Internet Directory (OID) or Microsoft Active Directory (AD), it is necessary to configure the Oracle Virtual Directory (OVD) subsystem.

3. Configure the Java Platform Services (JPS) to utilize Oracle Internet Directory (OID) for Fusion Middleware role mapping.
4. Configure OVD to support the ‘BlindTrustManager’.

11.10.1 Part 1 - Configure Java Platform Services

The file **jps-config.xml** needs to be edited as below:

```bash
$ cd $MW_HOME
$ cd user_projects/domains/bi/config/fmwconfig
$ cp jps-config.xml jps-config.xml.ORIG
$ vi jps-config.xml
$ diff -b jps-config.xml jps-config.xml.ORIG
84d83
< <property name="virtualize" value="true"/>
```

After the edits, the file **jps-config.xml** should look something like this:

<table>
<thead>
<tr>
<th>Line#</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>&lt;serviceInstance name=&quot;idstore.ldap&quot; provider=&quot;idstore.ldap.provider&quot;&gt;</td>
</tr>
<tr>
<td>81</td>
<td>&lt;description&gt;LDAP Identity Store Service Instance&lt;/description&gt;</td>
</tr>
<tr>
<td>82</td>
<td>&lt;property name=&quot;idstore.config.provider&quot; value=&quot;......&quot;</td>
</tr>
<tr>
<td>83</td>
<td>&lt;property name=&quot;CONNECTION_POOL_CLASS&quot; value=&quot;......&quot;</td>
</tr>
<tr>
<td>84</td>
<td>&lt;property name=&quot;virtualize&quot; value=&quot;true&quot;/&gt;</td>
</tr>
<tr>
<td>85</td>
<td>&lt;/serviceInstance&gt;</td>
</tr>
</tbody>
</table>

11.10.2 Part 2 - Configuring Oracle Virtual Directory (OVD)

The file **provider.os_xml** needs to be edited as below:

```bash
$ cd $MW_HOME/user_projects/domains/bi/config/fmwconfig/ovd/default/
$ cp provider.os_xml provider.os_xml.ORIG
$ diff -b provider.os_xml provider.os_xml.ORIG
58c58
< <property name="enabled" value="true"/>
---
> <property name="enabled" value="false"/>
```

After the edits, the file should look something like this:

<table>
<thead>
<tr>
<th>Line#</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>&lt;provider name=&quot;BlindTrustManager&quot;&gt;</td>
</tr>
<tr>
<td>56</td>
<td>&lt;configClass&gt;oracle.ods.virtualization.config.BlindTrustManagerProviderConfig&lt;/configClass&gt;</td>
</tr>
<tr>
<td>57</td>
<td>&lt;properties&gt;</td>
</tr>
<tr>
<td>58</td>
<td>&lt;property name=&quot;enabled&quot; value=&quot;true&quot;/&gt;</td>
</tr>
<tr>
<td>59</td>
<td>&lt;/properties&gt;</td>
</tr>
<tr>
<td>60</td>
<td>&lt;/provider&gt;</td>
</tr>
</tbody>
</table>

11.10.3 Part 3 - Mapping of OBI-stripe Roles to LDAP Users and/or LDAP Groups

Once the above edits are made, it is then possible to utilize Fusion Middleware Control to map these roles to LDAP users and/or LDAP groups.

As additional LDAP Based Enterprise Manager users need OAS permissions, one or more of the above roles will need to be granted to them.

The next sections contain example screenshots for utilizing Fusion Middleware Control to perform this mapping.
11.11 Step 11 - Granting OAS Fusion Middleware Application roles to EM LDAP Users

The following sections details the steps for granting OAS Fusion Middleware Application roles to EM LDAP Users, and/or LDAP Groups, utilizing Fusion Middleware Control.

The three roles below are created as part of the initial OAS Configuration.

The specifics role names and mapping form the basis of the termination in the flow chart from section 8.1.6 - OAS Privilege Assignment:

```
1 or more from:
- BI Consumer
- BI Author
- BI Administrator
```

These roles are managed by the Oracle Platform Services (OPSS) as part of the ‘obi-stripe’.

The ‘obi-stripe’ is created as part of OAS configuration, and populated with these three roles, in a hierarchical manner.

<table>
<thead>
<tr>
<th>OBI-Stripe Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI Consumer</td>
<td>Can login to OAS and view reports</td>
</tr>
<tr>
<td><strong>BI Consumer</strong></td>
<td>Can also schedule OAS reports</td>
</tr>
<tr>
<td>BI Author</td>
<td>Can manipulate the OAS catalog (cut/copy/paste/delete)</td>
</tr>
<tr>
<td></td>
<td>Can also edit OAS reports</td>
</tr>
<tr>
<td>BI Administrator</td>
<td>Full access to OAS, including access to the special <strong>Administration</strong> screens.</td>
</tr>
</tbody>
</table>
11.11.1 Part 1 - Login to Fusion Middleware Control and Navigate to Application Roles

11.11.2 Part 2 - Select the ‘obi’ Application Stripe
### 11.11.3 Part 3 - Select the Role, for example ‘BIServiceAdministrator’

![Oracle Enterprise Manager](image)

**Application Roles**

Application roles are the roles used by security-aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the app context ends users accessing the application.

**Policy Store Provider**

**Search**

Select an application scope and enter a search keyword for the role name to search for roles defined by this application.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIServiceAdministrator</td>
<td>This role contains privileges required to administer the sample application.</td>
</tr>
<tr>
<td>DVContentAuthor</td>
<td>Users with this role can create most types of content.</td>
</tr>
<tr>
<td>BIConsumer</td>
<td>Users granted this role can consume content but are restricted in what they can create.</td>
</tr>
<tr>
<td>BIDashletAuthor</td>
<td>Users with this role can author data loads.</td>
</tr>
<tr>
<td>BICoreAuthor</td>
<td>Users with this role can author data models.</td>
</tr>
<tr>
<td>DVConsumer</td>
<td>Users with this role can consume content but are restricted in what they can create.</td>
</tr>
<tr>
<td>DVDataModelAuthor</td>
<td>Users with this role can author data models.</td>
</tr>
</tbody>
</table>

### 11.11.4 Part 4 - Press Edit

![Oracle Enterprise Manager](image)

**Application Roles**

Application roles are the roles used by security-aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the app context ends users accessing the application.

**Policy Store Provider**

**Search**

Select an application scope and enter a search keyword for the role name to search for roles defined by this application.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIServiceAdministrator</td>
<td>This role contains privileges required to administer the sample application.</td>
</tr>
<tr>
<td>DVContentAuthor</td>
<td>Users with this role can create most types of content.</td>
</tr>
<tr>
<td>BIConsumer</td>
<td>Users granted this role can consume content but are restricted in what they can create.</td>
</tr>
<tr>
<td>BIDashletAuthor</td>
<td>Users with this role can author data loads.</td>
</tr>
<tr>
<td>BICoreAuthor</td>
<td>Users with this role can author data models.</td>
</tr>
<tr>
<td>DVConsumer</td>
<td>Users with this role can consume content but are restricted in what they can create.</td>
</tr>
<tr>
<td>DVDataModelAuthor</td>
<td>Users with this role can author data models.</td>
</tr>
</tbody>
</table>

**Membership for BICore**

<table>
<thead>
<tr>
<th>Principal</th>
<th>Display Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BICoreConsumer</td>
<td>DV Consumer</td>
<td>Application Role</td>
<td>Users with this role can create most types of content.</td>
</tr>
<tr>
<td>DVConsumer</td>
<td>DV Consumer</td>
<td>Application Role</td>
<td>Users granted this role can consume content but are restricted in what they can create.</td>
</tr>
</tbody>
</table>
11.11.5  Part 5 - Add the required Principals
In the search field for Add Principal choose User, enter the username, and press the search arrow

11.11.6  Part 6 - Press OK

11.11.7  Part 7 - Push any changes to OBI stripe
It can sometimes be necessary to bounce OAS for the changes to the OBI-stripe to propagate.

11.11.7.1  Shutdown OAS
Use the instructions and screenshots from ‘Appendix A - Shutting down OAS using the WebLogic console’ to shutdown OAS.

11.11.7.2  Startup OAS
Use the instructions and screenshots from ‘Appendix B - Starting OAS using the WebLogic Console’ to start OAS.
CHAPTER 12. OAS OPTIONAL CONFIGURATION OF SSO ON TOP OF LDAP

If Single Sign On is required to allow for a single login to both Enterprise Manager, Oracle Analytics Server, and any other possible applications, several additional steps need to be performed on top of the OAS configuration for LDAP.

For these examples, Oracle Access Manager (OAM) will be configured on top of Oracle Internet Directory (OID). Other single sign on solutions is likely possible but will not be documented in this workbook.

Consult the Fusion Middleware Documentation Set [Here](#) for further details.

The additional steps required for OAM on top of OID, for OAS, are summarized below, with direct cross references to the relevant sections.

1. Installation of Oracle HTTP Server (OHS) – Section 12.1.
2. Extending OAS WebLogic Domain with collocated OHS using the config.sh script.
3. Integrating OHS into WebLogic Domain using wlst.sh – Section 12.4.
4. Configuration of OHS for OAS using Fusion Middleware Control – Section 0.
5. Test access to OAS using the OHS port – Section [Error! Reference source not found.](#).
7. Configuration of Oracle Webgate, running on top of OHS.
8. OAS Required Steps – Section 13.1.8.
12.1 Installation of OHS

A pre-requisite for OAM is a properly configured WebLogic domain, with a co-located OHS installation inside of the same domain.

The following set of screenshots details the installation of OHS.

These steps are somewhat error prone, so a backup of the OAS WebLogic domain should be taken prior to these steps.

See the Fusion Middleware documentation set here for details on this procedure.

» Launch the OHS installation UI for the appropriate Operating System Platform

```
$ ./fmw_12.2.1.4.0_ohs_linux64.bin
Preparing to launch the Oracle Universal Installer from /tmp/OraInstall2020-09-30_11-22-53AM
Launcher log file is /tmp/OraInstall...log.
Checking if CPU speed is above ... Passed
Checking monitor: must be configured to ... Passed
Checking swap space: must be greater than ... Passed
Checking if this platform requires a 64-bit JVM. Actual 64 ... Passed
Checking temp space: must be greater than ... Passed
```

12.1.1 Step 1 - OHS Installation - Welcome

```
Welcome to Oracle Fusion Middleware 12c (12.2.1.4.0) Oracle HTTP Server installer.
Use this installer to create a new Oracle Home or extend an existing Oracle home with the Oracle
Fusion Middleware Web Tier software, including Oracle HTTP Server.
For more information, see Install, Patch, and Upgrade in the Oracle Fusion Middleware
documentation library.

Context-sensitive online help is available from the Help button.
```

12.1.2 Step 2 - OHS Installation – Auto Updates

» You can skip or apply as needed.
12.1.3 Step 3 - OHS Installation – Choose Middleware Home

» Either browse or type path

Either browse or type the full path of the MW_HOME
12.1.4  Step 4 - OHS Installation – Installation Type

» Make sure to select Collocated HTTP Server

12.1.5  Step 5 - OHS Installation - Choose JAVA HOME location

» Provide same JDK as used throughout WebLogic configuration
12.1.6 Step 6 - OHS Installation – Prerequisite Checks

» Confirm no pre-requisite failures

12.1.7 Step 7 - OHS Installation – Installation Summary

» Review results of pre-requisite tests.
12.1.8 Step 8 - OHS Installation – Installation Progress

Follow ongoing status until complete.

12.2 Extending OAS WebLogic domain with collocated OHS using the config.sh script

Launch the WebLogic Configuration Wizard:

```
cd $MW_HOME/oracle_common/common/bin
./config.sh
```
12.3 OHS Configuration

12.3.1 Step 1 - OHS Configuration – Update an existing WebLogic Domain

» Very Important – Update and existing domain

12.3.2 Step 2 - OHS Configuration – Choose Oracle HTTP Server (Collocated [OHS])

» Important – Choose template for Oracle HTTP Server (Collocated [ohs])
12.3.3  Step 3 - OHS Configuration - High Availability Options

» Review entries, do not change

12.3.4  Step 4 - OHS Configuration – Database Configuration Type

» Select Get RCU Configuration.

» Confirm successful connection.

12.3.5  Step 5 - OHS Configuration – Component Datasources

» Review entries – Do not change
12.3.6 Step 6 - OHS Configuration – JDBC Test

» Confirm all successful connections

12.3.7 Step 7 - OHS Configuration – Advanced Configuration

» Only check the box for System Components
12.3.8  Step 8 OHS Configuration  – System Components

12.3.8.1  Part 1 Choose Add

12.3.8.2  Part 2 - Change Name as appropriate – for example, ohs1
12.3.9 Step 9 - OHS Configuration – OHS Server

1) System Component – will be name provided in prior step, i.e., ohs1
2) Admin Host – VERY IMPORTANT: Leave the default value of ‘localhost’ [Mos Note Doc ID 2606314.1]
3) Admin Port – Leave at 7779. No checking for port conflicts are done.
4) Listen Address – Depending on network topology, either leave the field blank (listen on all network interfaces) or provide the local hostname (listen only on physical network connection associated with this hostname).
5) Listen Port – Default of 7777 is good. This is the port of the primary server that OHS is configured with.
6) SSL Listen Port – Default of 4443 is fine. This is the port of the primary SSL virtual server.
7) Server Name – Ensure this is exactly as shown:
   a. http or https (depending on security topology).
   b. Local hostname
   c. :7777 – Must match port from step 5 (http) or step 6 (https) above.

12.3.10 Step 10 - OHS Configuration – Machines

» Confirm Machine Name and Node Manager Listen Address – do not change values
12.3.11 Step 11 - OHS Configuration – Assign System Components

1. Select/highlight the ohs1 component.
2. Select/highlight the Machine
3. Press the right arrow
4. Confirm the tree diagram as below:

Confirm the tree diagram as below:
12.3.12 Step 12 - OHS Configuration – Configuration Summary

» Review

12.3.13 Step 13 - OHS Configuration – Configuration Progress

» Follow progress
12.3.14 Step 14 - OHS Configuration – End of Configuration

» Pay special attention to the instructions at the bottom of the screen.

**Confirmation Screen**

**Special Notice Regarding OHS System Component**

After successful domain creation, you must run the WLST command ohs_updateInstances() to complete all the required steps. Please refer to OHS product documentation for more details.
12.4 Integrating OHS into WebLogic Domain using wlst.sh.

Prior to managing OHS as part of the collocated WebLogic Domain in which OAS is configured, it is required to completely reset WebLogic:

» Bring Down OAS and Admin Server – See 'Appendix A'
» Bring Down Node Manager – See 'Appendix C'
» Start Node Manager – See 'Appendix D'
» Start Admin Server – See 'Appendix F'

12.4.1 Part 1 - Invoke WebLogic Scripting Tool (WLST)

```
$ $MW_HOME/oracle_common/common/bin/wlst.sh
Initializing Web...
Welcome to W...
Type help() f...
```

12.4.2 Part 2 - Connect to Admin Server

```
wls:/offline> connect()
Please enter your username :weblogic
weblogic
Please enter your password :
Please enter your server URL [t3://localhost:7001] :t3://localhost:9500
t3://localhost:9500
Connecting to t3://localhost:9500 with user id weblogic ...
Successfully connected to Admin Server "AdminServer" that belongs to domain "bi".
Warning: An insecure ...
To ensure...
```

12.4.3 Part 3 - Run special command

```
wls:/bi/serverConfig/> ohs_updateInstances()
Location changed to edit custom tree. This is a writable tree with No root.
For more help...
Starting an edit session ...
Started edit session, be sure to save and activate your changes once you are done.
Saving all your changes ...
Saved all your changes successfully.
Activating all your changes, this may take a while ...
The edit lock associated with this edit session is released once the activation is completed.
Activation completed
OHS instances have been updated successfully.
```
12.4.4 Part 4 - Confirm Correct Operations Performed

```
Part 4 - Confirm Correct Operations Performed

wls:/bi/serverConfig/> editCustom()
Location changed to edit custom tree. This is a writable tree with No root.
For more help, use help('editCustom')
wls:/bi/editCustom/> ls()
drw-   EMDomain
drw-   JMImplementation
drw-   oracle.as.jmx
drw-   oracle.as.management.mbeans.register
drw-   oracle.as.ohs
drw-   oracle.as.util
drw-   oracle.bi.admin
drw-   oracle.ohs
wls:/bi/editCustom/> cd('oracle.ohs')
wls:/bi/editCustom/oracle.ohs> ls()
drw-   oracle.ohs:OHSInstance-ohs1,name=127.0.0.1-7779,type=OHSInstance.PortConfig
drw-   oracle.ohs:OHSInstance-ohs1,name=4443,type=OHSInstance.PortConfig
drw-   oracle.ohs:OHSInstance-ohs1,name=7777,type=OHSInstance.PortConfig
drw-   oracle.ohs:OHSInstance-ohs1,name=Audit,type=OHSInstance.AuditConfig
drw-   oracle.ohs:OHSInstance-ohs1,name=VHost---4443,type=OHSInstance.VHostConfig
drw-   oracle.ohs:OHSInstance-ohs1,name=VHost-127.0.0.1-7779-localhost,type=OHSInstance.VHostConfig
drw-   oracle.ohs:OHSInstance-ohs1,name=VHost-<base>,type=OHSInstance.VHostConfig
drw-   oracle.ohs:type=Component.KeyStoreConfig,name=KeyStore,OHSInstance-ohs1,component=OHS
drw-   oracle.ohs:type=OHSInstance, name=ohs1
```

```
drw-   oracle.ohs:type=OHSInstance.WMProp,OHSInstance-ohs1,component=OHS
```

```
drw-   oracle.ohs:type=OHSSystemComponent,name=OHSInstanceManager
```

```
wls:/bi/editCustom/oracle.ohs> exit()
```
12.5 Configuration of OHS for OAS using Fusion Middleware Control.
Prior to managing OHS as part of the collocated WebLogic Domain in which OAS is configured, it is required to completely reset WebLogic:

» Confirm that OAS is still down, from steps in prior section.
» Bring Down Admin Server.
» Bring Down Node Manager – See ‘Appendix C’
» Start Node Manager – See ‘Appendix D’
» Start Admin Server – See ‘Appendix F’

12.5.1 Step 1 - Fusion Middleware Configuration – Login to Fusion Middleware Control

» [Image: http://oas.example.com:9500/em]

12.5.2 Step 2 - Fusion Middleware Configuration – Administer OHS Instances

[Image: WebLogic Domain ➔ Administration ➔ OHS Instances]
12.5.3  Step 3 - Fusion Middleware Configuration – Click on ohs1

12.5.4  Step 4 - Fusion Middleware Configuration – mod_wl_ohs Configuration
12.5.5 Step 5 - Fusion Middleware Configuration – lock and edit

12.5.6 Step 6 - Fusion Middleware Configuration – Search for cluster
12.5.7  Step 7 - Fusion Middleware Configuration – Choose bi_cluster

![Select WebLogic Cluster](image1)

12.5.8  Step 8 - Fusion Middleware Configuration – Populate Locations

![Add OAS Location](image2)
12.5.9  Step 9 - Fusion Middleware Configuration – Apply and Activate Changes

1. Start OAS – See ‘Appendix B’
2. Make sure OHS is running – See ‘Appendix H’.
3. Login to OAS, using the default OHS Port of 7777:  
   [http://oas.example.com:7777/xmlpserver](http://oas.example.com:7777/xmlpserver)
CHAPTER 13. OAS FOR CONFIGURATION OF ORACLE ACCESS MANAGER SSO

Like earlier steps, the overall goal is to configure the OAS WebLogic domain to closely match one (or possibly more) Enterprise Manager WebLogic Domains.

The right side shows an EM site fully configured with both OID and SSO (OAM).

Here is a side-by-side comparison of the current configuration of OAS and Enterprise Manager.

The end goal is shown below

The following sections detail the required steps to achieve this final goal.
13.1.1 Step 1 - Login to WebLogic Console
• http://oam.example.com:9500/console

13.1.2 Step 2 - Click on Security Realms and myrealm

13.1.3 Step 3 - Click on the Providers tab
13.1.4 Step 4 - Prepare to make the required edits

13.1.5 Step 5 - Create the new OAM Identity Asserter

Steps:

1. Click on the New button.
2. In the text box for the Name: field, choose a name as appropriate:
   - BIP_OAM_IDAsserter
3. In the drop-down for the Type: field, scroll down, and choose the type:
   - OAMIdentityAsserter
4. Click on the OK button.
13.1.6 Step 6 - Configure the BIP_OAM_Provider Provider to match Enterprise Manager

13.1.6.1 Part 1 Configure the common configuration

Set the Control Flag to **REQUIRED** and ensure that OAM_REMOTE_USER is on the right side (**Chosen:**)

![Image of BIP_OAM_Provider Provider configuration](image)

13.1.6.2 Part 2 - Configure the provider specific configuration to match Enterprise Manager’s.

» The only relevant item that needs to be configured is the **Primary Access Server**.

» You must scroll to the very bottom of the screen to see this.

![Image of BIP_OAM_Provider Provider specific configuration](image)
13.1.6.3  Part 3 - Reorder the providers as below:

Reorder Authentication Providers

You can reorder your Authentication Providers using

Select authenticator(s) in the list and use arrows to move.

Authentication Providers:

Available:

- BIP_OAM_IDAsetter
- BIP_OID_Provider
- Trust Service Identity Asserter
- DefaultAuthenticator
- DefaultIdentityAsserter

OK Cancel

13.1.6.4  Part 4 - Save and activate the changes

WebLogic Server Administration Console 12c

Change Center

View changes and restarts

Pending changes exist. They must be activated to take effect.

Activates Changes

Domain Structure
13.1.7 Step 7 - Configuration of Oracle Webgate, running on top of OHS.

Oracle Analytics Server (OAS) is built on top of Fusion Middleware 12.2.1.4.

Fusion Middleware 12.2.1.4 includes all the required components needed to integrate an existing WebLogic domain, built on top of Oracle HTTP Server (OHS), using the provided Oracle Webgate (Webgate).

The following is an outline of the required steps:

1. Deploy Webgate to Collocated OHS
2. Edit httpd.conf to include Webgate.
3. Copy required artifacts to OHS (EM Internal Steps, not part of finished document).
4. Troubleshooting Webgate.

For specific details on the required configuration, please consult the following Oracle documentation:

- Oracle® Analytics
- Enterprise Deployment Guide for Oracle Analytics Server

The above document describes how to install and configure Oracle Analytics Server components in an enterprise deployment.
13.1.8 Step 8 - OAS Required Steps

13.1.8.1 Part 1 - OAS Required Steps – wlst.sh

$ $MW_HOME/oracle_common/common/bin/wlst.sh

Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

wls:/offline> readDomain('....../user_projects/domains/bi')

wls:/offline/bi>enableBISingleSignOn('....../user_projects/domains/bi','http://oamserver.example.com:14100/oamsso/logout.html')

wls:/offline/bi>updateDomain()

wls:/offline/bi>closeDomain()

wls:/offline>exit()

Exiting WebLogic Scripting Tool.

13.1.8.2 Part 2 - OAS Required Steps – User Interface

13.1.8.2.1 Login to OAS as the WebLogic user and Click on ‘Administration’ link

13.1.8.2.2 Underneath ‘Security Center’ choose ‘Security Configuration’
13.1.8.3  Part 3 - Configure OAS to utilize Oracle Access Manager

» Click on the Use Single Sign-on check box.

» Change the Single Sign-On Type to Oracle Access Manager

» Input the correct value for the Single Sign-Off URL, for example:


**Note:**
- Local superuser can log in to the system independent from the selected security model. Ensure you have enabled the local superuser to be able to log in.
- Guest Access is not allowed by default.
- Authentication options include either Single Sign-on or LDAP for your authentication method. If you do not select this option, authentication is taken care of by the security model you selected on Authorization section.
- To enable Single Sign-On, first set up B Publisher as a partner application on the SSO Server. Enter the value for the single sign-off URL and other required information provided by the SSO Server below.

![Configuration Screen](attachment:image.png)
13.1.8.4 Part 4 - Edit or confirm the correct entry for the ServerName directive in httpd.conf

An example of the correct entry is shown below:

```bash
$ cd $MW_HOME/user_projects/domains/bi/config/fmwconfig/components/OHS/ohs1
$ diff httpd.conf httpd.conf.ORIG
203,205c203
<  #ServerName http://localhost:7777
<  # Added for OAS+OHS+OAM
<  ServerName http://oas.example.com:7777
---
> ServerName http://oas.example.com:7777
1136,1137d1133
<
< include  "webgate.conf"
```

13.1.8.5 Part 5 - Bounce the stack

1. Bring Down OAS See ‘Appendix A’.
2. Bring down OHS – See ‘Appendix H’.
3. Bring Down the Admin Server – See ‘Appendix E’
4. Bring Down Node Manager – See ‘Appendix C’
5. Start Node Manager – See ‘Appendix D’.
7. Start OAS – see ‘Appendix B’
CHAPTER 14. CONFIGURATION OF REQUIRED OAS Datasource(s)

After successfully configuring OAS for the desired Security Infrastructure, the Oracle Provided Reports, and any customized reports can be uploaded to OAS.

Before the Oracle provided Out of Box reports can be utilized, as well as any customized reports, it is necessary to configure one or more OAS Datasources.  

Each of these configured Datasources are mapped one-to-one for each set of the Oracle provided Out of Box Reports.

14.1 Step 1 - For the first EM system (and optionally any additional EM systems)

The following command sets the password for the MGMT_VIEW user to the specified value. This is required so that the OAS Datasource (i.e., EMREPOS) can be properly configured.

```
emctl config oms -change_view_user_pwd -sysman_pwd ****** -user_pwd ******
emctl stop oms -all
emctl start oms
```

14.2 Step 2 - OAS Datasource Configuration Steps

Use the following screenshots as an example of configuring an OAS Datasource.

14.2.1 Part 1 - Login to OAS as the ‘weblogic’ user

![Login as the weblogic user (or sysman)](image)

Figure 46. Login as the weblogic user (or sysman)

14.2.2 Part 2 - Click on the Administration Link

![Click on the Administration link](image)

Figure 47. Click on the Administration link

---

20 (OAS - Set Up Data Sources, 2021) Data Sources
14.2.3 Part 3 - Choose JDBC Connection under Data Sources

14.2.4 Part 4 - Choose Add Datasource
14.2.5 Part 5 - Fill in the required details

Name: EMREPOS
Driver Type: Oracle 12c
Database Class: oracle.jdbc.OracleDriver
Connection String: jdbc:oracle:thin:@//emrepos1.example.com:1521/orcl.example.com
Use System User: Do Not Check
    Username: MGMT_VIEW
    Password: ********

Pre Process Function: sysman.gc$bip.bip_set_em_user_context(:xdo_user_name)
Post Process Function: Leave Blank
Client Certificate: Leave Blank
Use Proxy Authentication: Leave Blank

14.2.6 Part 6 - Test the connection and ensure the results of a successful connection:

**Warning**: The password entered here for the "mgmt_view" user needs to match that which is configured for the EM repository being connected to (in the above example "emreposdb.example.com")

This is accomplished with the command:
emctl config cms -change_view_user_pwd
14.2.7 Part 7 Granting Required Roles to OAS Datasource

14.2.7.1 Grant required Roles to the OAS Datasource – Database Security Model

When using OAS against a single EM installation, using the ‘Database Security Model’, the default DBMS role granted to all Enterprise Manager Administrators is:

- MGMT_USER

In general, it is not appropriate to select the ‘Allow Guest Access’ unless a specific use case has been identified to support the guest account.

14.2.7.2 Select the MGMT_USER role

![Select MGMT_USER role](image1)

14.2.7.3 Move the MGMT_USER role over to the right-hand side

![Move MGMT_USER role](image2)

14.2.7.4 And finally hit ‘Apply’

![Apply configuration](image3)
14.2.7.5  Grant Required Roles to OAS Datasource – Fusion Middleware Security Model

When using OAS against one or more EM installations, using the ‘Fusion Middleware Security Model’, using LDAP (with or without SSO), the minimum role required for an EM administrator to utilize OAS is ‘BIConsumer’.

It is easiest to just move all the available roles from the left side to the right side, and press **Apply** in the top right of the screen.
CHAPTER 15. INSTALLATION OF ORACLE PROVIDED OUT OF BOX REPORTS

Enterprise Manager 13.5 bundles a full set of the Oracle Provided out-of-box reports. This set of out-of-box reports is being delivered consistent with earlier releases of Enterprise Manager.

As in prior releases of Enterprise Manager, a set of out-of-box reports is being delivered as part of the base platform, as well as for each plug-in.

15.1 Per-requisite Step to support Enterprise Manager Provided Out of Box Reports

The Oracle Provided Out-of-Box reports utilize the Fusion Middleware Security roles from the embedded BIP that was part of prior releases of Enterprise Manager.

When utilizing the Database Security Model with OAS [section Chapter 9 - OAS For Enterprise Manager Repository-based Security], the EMBIP* can easily be created as DBMS roles.

The steps to overlay the roles from the embedded BIP onto the default WebLogic Roles, that are installed along with OAS, when utilizing the Fusion Middleware Security Model [section - Chapter 10 - OAS For Enterprise Manager LDAP Configuration]
The above structure is achieved by utilizing either sqlplus, or Fusion Middleware Control, such that the OAS Role hierarchy is:

<table>
<thead>
<tr>
<th>Fusion Middleware Security Model</th>
<th>Database Security Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMBIPADMINISTRATOR</td>
<td>EMBIPADMINISTRATOR</td>
</tr>
<tr>
<td>BI Administrator</td>
<td>XMLP_ADMIN</td>
</tr>
<tr>
<td>BI Content Author</td>
<td>EMBIPAUTHOR</td>
</tr>
<tr>
<td>BI Consumer</td>
<td>XMLP_DEVELOPER</td>
</tr>
<tr>
<td></td>
<td>MGMT_USER</td>
</tr>
<tr>
<td></td>
<td>EMBIPVIEWER</td>
</tr>
</tbody>
</table>

Figure 48. Mapping of EMBIP* Roles to base OAS Roles

15.1.1 Standalone OAS 5.5.0 support for EM Provided Reports: Database Security Model

Create the required roles, and minimal role grants, on the Enterprise Manager repository database:

```
$ sqlplus sys/***** as sysdba
sql> REM Create base EMBIP roles
sql> create role EMBIPADMINISTRATOR;
sql> create role EMBIPAUTHOR;
sql> create role EMBIPSCHEDULER;
sql> create role EMBIPVIEWER;
sql>
sql> REM Create Role Mapping
sql> grant XMLP_ADMIN to EMBIPADMINISTRATOR;
sql> grant XMLP_DEVELOPER to EMBIPAUTHOR;
sql> grant XMLP_SCHEDULER to EMBIPSCHEDULER;
sql> grant MGMT_USER to EMBIPVIEWER;
sql> exit;
```
15.2  OAS 5.5.0 support for EM Provided Reports: Fusion Middleware Security Model

The steps to achieve the desired mapping when utilizing the Fusion Middleware Security Model is implemented using Fusion Middleware Control.

15.2.1  Step 1 - Create EMBIP* Roles as OBI-Stripe Roles

15.2.1.1  Part 1 - Login to Fusion Middleware Control

15.2.1.2  Part 2 - Create EMBIPADMINISTRATOR Role
15.2.1.3 Part 3 - Create EMBIPAdministrator and all EMBIP* Roles

» Create EMBIPADMINISTRATOR Role

![Role creation screenshot]

- Change name and description and press OK

15.2.1.4 Part 4 - Repeat Above steps for:
- EMBIPAUTHOR
- EMBIPSCHEDULER
- EMBIPVIEWER
15.2.2 Step 2- Create Mapping of BI Service Administrator to EMBIPAdministrator

To achieve the mapping shown in Figure 48 - Mapping of EMBIP* Roles to base OAS Roles, the following steps are required:

» Edit BI Service Administrator

![Application Roles](image)

» Search for EMBIPAdministrator

![Add Principal](image)
» Add EMBIPADMINISTRATOR

- Press OK
» Finished Result for EMBIPADMINISTRATOR

![Image of finished result for EMBIPADMINISTRATOR]

**Application Roles**

Application roles are the roles used by security-aware applications that are specific to the application. These roles define the tasks that end users accessing the application can perform.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Display Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIServiceAdministrator</td>
<td>BI Service Administrator</td>
<td>This role confers privileges to the application.</td>
</tr>
<tr>
<td>DVContentAuthor</td>
<td>DV Content Author</td>
<td>Users with this role can create and edit content.</td>
</tr>
<tr>
<td>BIConsumer</td>
<td>BI Consumer</td>
<td>Users who need to access BI content.</td>
</tr>
<tr>
<td>BIRequestAuthor</td>
<td>BI Request Author</td>
<td>Users who can submit requests for BI data.</td>
</tr>
<tr>
<td>BIDeveloper</td>
<td>BI Developer</td>
<td>Users who develop BI applications.</td>
</tr>
<tr>
<td>EMBIPAUTHOR</td>
<td>EMBIPAUTHOR</td>
<td>This role is for EMBIPAUTHOR users.</td>
</tr>
<tr>
<td>EMBIPADMINISTRATOR</td>
<td>EMBIPADMINISTRATOR</td>
<td>This role confers privileges to the application.</td>
</tr>
<tr>
<td>EMBIPVIEWER</td>
<td>EMBIPVIEWER</td>
<td>Users with this role can view BI content.</td>
</tr>
<tr>
<td>EMBIPSCHEDULER</td>
<td>EMBIPSCHEDULER</td>
<td>This role is for EMBIPSCHEDULER users.</td>
</tr>
</tbody>
</table>

**Membership for BIServiceAdministrator**

<table>
<thead>
<tr>
<th>Principal</th>
<th>Display Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>weblogic</td>
<td>weblogic</td>
<td>User</td>
<td>This user is the creator of the application.</td>
</tr>
<tr>
<td>EMBIPADMINISTRATOR</td>
<td>EMBIPADMINISTRATOR</td>
<td>Application Role</td>
<td>This role confers privileges to the application.</td>
</tr>
</tbody>
</table>
15.2.3 Step 3 - Repeat so below screenshots are shown

**EMBIPAUTHOR**

![Application Roles](image1)

**EMBIPVIEWER**

![Application Roles](image2)
15.3 Uploading Enterprise Manager Provided Out of Box Reports

15.3.1 Framework Reports
The Enterprise Manager Provided Reports for the base framework will be in the MW_HOME in which EM 13.5 is installed.

```
$ ls -sh "$MW_HOME/sysman/jlib/Enterprise Manager Cloud Control.xdrz"
2.5M ./sysman/jlib/Enterprise Manager Cloud Control.xdrz
```

15.3.2 Plugin Reports
Each EM plugin that is bundled with EM Provided Out of Box Reports, whether installed during the initial install/upgrade of EM 13.5, or subsequently installed via self-update or other mechanism, will follow this pattern:

```
$ ls -sh "$MW_HOME/plugins/oracle.sysman.*.plugin_13.5*/metadata/bipublisherreport/emreports/*.xdrz
216K ./plugins/oracle.sysman.xa.oms.plugin_13.5.1.0.0/metadata/bipublisherreport/emreports/Enterprise Manager Cloud Control.xdrz
```

15.3.3 Common File name for all Oracle Provided Out of Box Reports
Each set of these out-of-box reports has the name below, which facilitates straightforward upgrades to the standalone OAS installation:

```
Enterprise Manager Cloud Control.xdrz
```
15.3.4 Preparing the Enterprise Manager 13.5 Out of Box Reports for uploading to OAS

In preparation for uploading the EM provided reports, copy all instances of files named \texttt{Enterprise Manager Cloud Control.xdrz}, from the EM 13.5 \texttt{MW_HOME}, to your local desktop (i.e., using putty, scp, etc...)

Once all XDRZ files are copied to your local desktop, one may see the following structure:

```
├── [ 7.2M] plugins
│   ├── [221k] oracle.sysman.cfw.oms.plugin_13.5.1.0.0
│   │   ├── [220k] metadata
│   │   │   ├── [220k] bipublisherreport
│   │   │   │   └── [220k] \texttt{Enterprise Manager Cloud Control.xdrz}
│   │   ├── [1.5M] oracle.sysman.db.oms.plugin_13.5.1.0.0
│   │   │   ├── [1.5M] metadata
│   │   │   │   ├── [1.5M] bipublisherreport
│   │   │   │   │   └── [1.5M] emreports
│   │   │   │   │   └── [1.5M] \texttt{Enterprise Manager Cloud Control.xdrz}
│   │   ├── [3.3M] oracle.sysman.emas.oms.plugin_13.5.1.0.0
│   │   │   ├── [3.3M] metadata
│   │   │   │   ├── [3.3M] bipublisherreport
│   │   │   │   │   └── [3.3M] emreports
│   │   │   │   │   └── [3.3M] \texttt{Enterprise Manager Cloud Control.xdrz}
│   │   ├── [464k] oracle.sysman.emct.oms.plugin_13.5.1.0.0
│   │   ├── [464k] metadata
│   │   │   ├── [464k] bipublisherreport
│   │   │   │   └── [464k] emreports
│   │   │   │   └── [464k] \texttt{Enterprise Manager Cloud Control.xdrz}
│   │   ├── [146k] oracle.sysman.emfa.oms.plugin_13.5.1.0.0
│   │   │   ├── [146k] metadata
│   │   │   │   ├── [146k] bipublisherreport
│   │   │   │   │   └── [146k] emreports
│   │   │   │   │   └── [146k] \texttt{Enterprise Manager Cloud Control.xdrz}
│   │   ├── [1.5M] oracle.sysman.xa.oms.plugin_13.5.1.0.0
│   │   ├── [1.5M] metadata
│   │   │   ├── [1.5M] bipublisherreport
│   │   │   │   └── [1.5M] emreports
│   │   │   │   └── [1.5M] \texttt{Enterprise Manager Cloud Control.xdrz}
│   ├── [2.6M] sysman
│   │   ├── [2.6M] jlib
│   │   │   └── [2.6M] \texttt{Enterprise Manager Cloud Control.xdrz}
```

Figure 49. Example layout of Enterprise Manager 13.5 Provided Out-of-Box Reports

Once the example layout above is created on your local desktop system, these set(s) can then be directly uploaded to the new OAS installation using the standard OAS upload process.

Any subsequent updates or patching of Enterprise Manager out-of-box reports would be done using the standard OAS user interface, against one or more reports.

The following screenshots demonstrate some examples of uploading these out-of-box reports.
15.4 Uploading Oracle Provided Out-of-box Reports to standalone OAS

15.4.1 Platform reports

1. Login to the standalone OAS as a user with OAS privileges (i.e. ‘weblogic’, ‘sysman’, etc).
2. Navigate to the catalog.
3. Navigate to the ‘Shared Folders’ folder.
4. Select ‘Upload’.
5. Using the browser’s dialog, choose the file associated with the platform reports.
6. Ensure to select the ‘overwrite’ checkbox.

![Image showing the upload process]

Uploading status is shown, and in about 1 minute, Upload Completed is shown.
15.4.2  Repeat the above procedure for each EM plugin
See “Figure 49 - Example layout of Enterprise Manager 13.5 Provided Out-of-Box Reports”

15.4.2.1  Completed View of Standalone OAS Catalog

15.4.2.2  Run the EM Sample Report:
15.5  Steps to complete after uploading the Enterprise Manager Provided Reports

In certain circumstances, the OAS catalog's root folder, which is displayed in the user interface via the Shared Folders icon, does not have the correct permissions.

The symptom of this would be for OAS users without the Super Admin privilege (either BIAdministrator, EMBIPADMINISTRATOR, or XMLP_ADMIN, depending on the security model) will be unable to see the reports that were just uploaded.

There can be circumstances that arise from time to time when the same behavior can be exhibited for customized reports that are either developed directly in OAS, or uploaded to OAS, show this same behavior.

In order to repair or set appropriate permissions for an OAS Catalog Object, note the four types of Catalog Objects that are available.

15.5.1  OAS Catalog Object Types

Every OAS catalog Object has an associated set of permissions, which are derived from the set of available roles. Note that the roles are stored as appropriate, depending on the OAS Security Model.

Review 'Figure 48- Mapping of EMBIP* Roles to base OAS Roles' for review.

<table>
<thead>
<tr>
<th>Object</th>
<th>Comment</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Root of My Folders tree.</td>
<td><img src="image" alt="Folders Screenshot" /></td>
</tr>
<tr>
<td></td>
<td>A subfolder of Shared Folders.</td>
<td></td>
</tr>
<tr>
<td>Datamodel</td>
<td>SQL Queries against EM repository data.</td>
<td><img src="image" alt="Datamodel Screenshot" /></td>
</tr>
<tr>
<td>Report</td>
<td>Layout and properties for viewing report content.</td>
<td><img src="image" alt="Report Screenshot" /></td>
</tr>
<tr>
<td>Subtemplate</td>
<td>Can be included by Report's (i.e., for headers/footers).</td>
<td><img src="image" alt="Subtemplate Screenshot" /></td>
</tr>
</tbody>
</table>
15.5.2 Resolving Permissions issues against one or more OAS Catalog Object(s)

As a user with OAS super admin privileges (i.e., sysman, weblogic, etc...), navigate to the OAS Catalog Object that needs to have its catalog permissions set or reset.

For this example, The Shared Folders OAS Catalog Object is demonstrated:

<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select Shared Folders</td>
</tr>
<tr>
<td>2.</td>
<td>Do not highlight any other items.</td>
</tr>
<tr>
<td>3.</td>
<td>Press Permissions link.</td>
</tr>
<tr>
<td>4.</td>
<td>An empty list.</td>
</tr>
<tr>
<td>5.</td>
<td>Press the + sign.</td>
</tr>
<tr>
<td>6.</td>
<td>Enter EMBIP in Name.</td>
</tr>
<tr>
<td>7.</td>
<td>Press Search button.</td>
</tr>
<tr>
<td>Step</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
</tr>
<tr>
<td>8.</td>
<td>List shown.</td>
</tr>
<tr>
<td>9.</td>
<td>Press <strong>Move All</strong></td>
</tr>
<tr>
<td>10.</td>
<td>Fill to match the screen shot.</td>
</tr>
<tr>
<td>11.</td>
<td>If this checkbox is selected, the catalog operation can take significantly more time.</td>
</tr>
<tr>
<td>12.</td>
<td>Only select this checkbox if it is required.</td>
</tr>
</tbody>
</table>
Table 8. Ensure correct Catalog Permissions for OAS Shared Folder
CHAPTER 16. UPGRADING FROM EM 13.4 TO EM 13.5

There are two main steps in upgrading from EM 13.4 and transitioning to the standalone OAS:

1. Migrating the BIP schedules, from the embedded BIP in EM 13.4, to the schedules in the standalone OAS.
2. Migrating any customized reports from the embedded BIP in EM 13.4, to the standalone OAS.

16.1 Migrating BIP Schedules from EM 13.4

After all steps in this handbook are completed, and the standalone Oracle Analytics Server environment is fully functional, the scheduler jobs and the job history data can be migrated from the embedded BIP in EM 13.4.

The standalone OAS provides a script to perform this migration.

Many of the required arguments to the script can be gleaned from the flow during the initial standalone OAS configuration, from section “7.6.5 - Step 5 - Database Details”, and from the section “14.2.5- Part 5 - Fill in the required details”, which are repeated below:

Name: EMREPOS
Driver Type: Oracle 12c
Database Class: oracle.jdbc.OracleDriver
Connection String: jdbc:oracle:thin:@//emrepos1.example.com:1521/orcl.example.com
Use System User: Do Not Check
Username: MGMT_VIEW
Password: ●●●●●●●●
Pre Process Function: sysman.gc$bip.bip_set_em_user_context(:xdo_user_name)
Post Process Function: Leave Blank
Client Certificate: Leave Blank
Use Proxy Authentication: Leave Blank
16.2 Arguments for OAS Scheduler Migration Script

<table>
<thead>
<tr>
<th>Context</th>
<th>Argument Value (color coded)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL*plus invocation</td>
<td>SYS</td>
<td>The sysdba username usually “sys”</td>
</tr>
<tr>
<td>SQL*plus invocation</td>
<td>******</td>
<td>SYSDBA Password</td>
</tr>
<tr>
<td>SQL*plus invocation</td>
<td>@oasrepos.example.com:1521/orcl</td>
<td>The connect descriptor would be the value of the “Simple connect string” in the screenshot above, reformatted for use with SQL*plus.</td>
</tr>
<tr>
<td>SQL Script Execution</td>
<td>sysman_biplatform</td>
<td>EM 13.4 Embedded BIP Schema Username.</td>
</tr>
<tr>
<td>SQL Script Execution</td>
<td>******</td>
<td>The “sysman” User's password.</td>
</tr>
<tr>
<td>SQL Script Execution</td>
<td>emrepos1.example.com:1521/orcl.example.com</td>
<td>This value would the same as entered in highlighted value from “14.2.5- Part 5 - Fill in the required details”:</td>
</tr>
<tr>
<td>SQL Script Execution</td>
<td>oas_biplatform</td>
<td>The actual username will be the prefixed with the value from the “Schema prefix” field in the screenshot:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Schema_prefix&quot; + &quot;_&quot; + &quot;BIPLATFORM&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In this case, the complete username is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OAS_BIPLATFORM</td>
</tr>
</tbody>
</table>

Table 9. Arguments for OAS Scheduler Migration Script
16.2.1  Example execution of OAS Scheduler Migration Script using example values

16.2.1.1  Change to the directory appropriate for your platform:

```bash
cd /u01/oracle/OAS/bi/modules/oracle.bi.publisher/upgradeutil
```

16.2.1.2  Using the table above as an example, and the color coding in the table, execute the script as follows:

```bash
$ sqlplus /y/*****@oasrepos.example.com:1521/orcl as sysdba
```

16.2.1.3  Run the `bip_12c_schedulerMigration.sql` script

Pass in the command-line parameters, using the color coding from the table.

```
sql> @bip_12c_schedulerMigration.sql  sysman_biplatform  *****  oasrepos.example.com:1521/orcl.example.com  oas_biplatform
old 1: & &1 new 1: sysman_biplatform
old 2: & &2 new 2: 
old 3: '&&3' new 3: emrepos1.example.com:1521/orcl.example.com
old 4: '&&4' new 4: oas_biplatform
12C_BIPLATFORM_SCHEMA_NAME Database link created.
9979 rows created.
9769 rows created.
9739 rows created.
4159 rows created.
6 rows created.
6 rows created.
6 rows created.
Commit complete.
Database link dropped.
SQL> exit;
```

$
16.3 Migrating any customized BIP reports to the standalone OAS.

In addition to support for the Oracle provided out of box reports, customized reports developed in EM 13.4, on BIP 12.2.1.3, can be migrated to OAS 5.5.0.

The standard process for this, using BIP or OAS, is to download the report from the prior release, and upload the report to the current release.

Make sure to download these customized reports from EM 13.4 prior to the upgrade to EM 13.5.

Since BIP reports are composed of 2, and sometimes 3, separate objects, all these need to be downloaded/uploaded.

Additionally, the paths for these objects needs to be maintained.

It is often easiest to download/upload whole catalog folders as opposed to individual objects.

The steps documented in this chapter assume that the download steps are executed against the embedded BIP included with Enterprise Manager 13.4, and that the upload steps are executed against the standalone OAS.

16.3.1 Example Use Case

For this example, a customized report named Targets has been developed.

» This report uses the BIP interactive report editor and viewer.
» The data model and the report are in the BIP shared folder named MyReports.
» Inside of this shared folder are two subfolders: Datamodels and Reports.
» Inside of these two subfolders are the report Datamodel and report, respectively.

For this example, the EM administrator that developed the report is named ‘jerry’.

16.4 Outline of steps to download the report from EM 13.4:

1. Login to the embedded BIP from Enterprise Manager 13.4
2. Navigate to the BIP catalog.
3. Expand the ‘Shared Folders’
4. Click on your customized report folder.
5. Click on Download from the tasks pane.
6. Use the operating system dialog, if required, to save the folder as a xdrz file.
7. Confirm that the file was downloaded correctly.
16.4.1 Step 1 – EM 13.4 – Login to BIP
Login to the BIP system on the EM 13.4 host as the user ‘jerry’.

16.4.2 Step 2 – From the BIP home screen, click on the link for ‘Catalog Folders’
Underneath the Browse/Manage… heading, chose the Catalog Folders link.
16.4.3 Step 3 – If needed, expand the ‘Shared Folders’ node in the catalog tree.
Make sure that you are logged in as the correct user (jerry in this example).
Navigate the OAS catalog tree such that the MyReports node is expanded with two sub-folders.

16.4.4 Step 4 - Click on the MyReports' Folder.
After the node is clicked on the left-hand tree, the right-hand side of the browser will show the contents of that folder. In this case, there are two sub-folders.
16.4.5 Step 5 - Click on Download.
The Download link is in the bottom-left-hand side of the browser window, in the ‘Tasks’ pane.
All catalog related activities can be accessed in the Tasks pane.
When you click on the Download link, an operating system, or browser, dialog may come up asking where to save the downloaded file.
16.4.6  Step 6 – You may be asked what to do with the file named MyReports.xdrz

» Choose to save this on your local disk.

16.4.7  Step 7 - Confirm that the file was downloaded correctly.

$ unzip -l MyReports.xdrz
Archive: MyReports.xdrz

<table>
<thead>
<tr>
<th>Name</th>
<th>Length</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>~metadata.meta</td>
<td>456</td>
<td>06-29-2020</td>
<td>21:17</td>
</tr>
<tr>
<td>Reports/</td>
<td>0</td>
<td>06-29-2020</td>
<td>21:17</td>
</tr>
<tr>
<td>~metadata.meta</td>
<td>420</td>
<td>06-29-2020</td>
<td>21:17</td>
</tr>
<tr>
<td>Reports/Targets.xdoz</td>
<td>2459</td>
<td>06-29-2020</td>
<td>21:17</td>
</tr>
<tr>
<td>Datamodels/</td>
<td>0</td>
<td>06-29-2020</td>
<td>21:17</td>
</tr>
<tr>
<td>~metadata.meta</td>
<td>423</td>
<td>06-29-2020</td>
<td>21:17</td>
</tr>
<tr>
<td>Datamodels/Targets.xdmz</td>
<td>1453</td>
<td>06-29-2020</td>
<td>21:17</td>
</tr>
</tbody>
</table>

5211 7 files
16.5  EM 13.5 – Upload Report Folder to OAS

Outline of steps to upload the BIP report folder to the standalone OAS:

Assumption: The standalone OAS has been configured using the detailed steps from this guide.

1. Login to OAS.
2. Click on Catalog Folders.
3. Expand Shared Folders.
4. Choose the Upload link from the Tasks pane.
5. Press the Choose File button.
6. Choose the file previously downloaded, for example, MyReports.xdrz
7. Optionally choose the Overwrite checkbox.
8. Click the Upload button.
9. Confirm the OAS catalog is displayed as expected.
10. Run the report.

16.5.1  Step 1 - Login to the OAS system on the standalone OAS host as the user ‘jerry’. 
16.5.2 Step 2 - From the OAS home screen, click on the link for ‘Catalog Folders’.
Underneath the **Browse/Manage...** heading, click on the **Catalog Folders** link.

![Catalog Folders Screenshot](image1)

16.5.3 Step 3 - If needed, expand the ‘Shared Folders’ node in the catalog tree.
It may be necessary to expand the **Shared Folders** node to see the equivalent screen shot below.

![Shared Folders Screenshot](image2)
16.5.4 Step 4 - Click on Upload.
The Upload link is in the bottom-left-hand side of the browser window, in the Tasks pane.

» NOTE: This step is symmetrical to the Download steps we performed on BIP earlier.

16.5.5 Step 5 - Click the button 'Choose File' in the Upload popup window.
16.5.6 Step 6 - Choose the file named ‘MyReports.xdrz’ from the operating system dialog.

16.5.7 Step 7 – Proceed with the upload
» If desired, choose the Overwrite existing file checkbox.
» Press the Upload button.

16.5.8 Step 8 – Monitor the status of the upload
» Initially the message Uploading is show.
» Once the upload is completed, the message Upload Completed is briefly displayed.
16.5.9 Step 9 – Confirm the correct layout of the OAS Catalog Folders.

» It might be necessary to expand and collapse the Shared Folders node in the tree, as shown below:

![OAS Catalog after successful upload.](image)

16.5.10 Step 10 - Confirm that the report executes as expected.

» If the report fails to execute with the message Error with Data XML, then the Datamodel may need to be edited to change the Datasource name.

» For example, in EM 13.4 all reports used the Datasource named EMREPOS.

» For EM 13.5, when utilizing LDAP for OAS and EM, multiple EM systems can be reported against, using Datasource named 'EMREPOS1, EMREPOS2 ...'

» In this case, change the Datasource name, in the Datamodel, as appropriate.

» For example, from EMREPOS to EMREPOS1.
CHAPTER 17. UPDATING THE EM 13.5 WEBLOGIC DOMAIN TARGET

After the upgrade to Enterprise Manager 13.5 is completed, the embedded BIP related WebLogic artifacts will still be shown as monitored targets.

Since these targets no longer exist, they are stale, and it is necessary to refresh the WebLogic domain.

17.1 Login to Enterprise Manager 13.5 and Navigate to GCDomain

17.2 Refresh WebLogic Domain and Delete Stale Targets
17.3 Stale embedded BIP* targets are removed
17.4 Delete any remaining stale BIP targets

1. All Targets
2. Search for `bip`
3. For each target:
   a. Right Click on targets
   b. Choose Target Setup
      i. Choose remove Target...
      ii. Confirm Deletion
      iii. Receive Confirmation
Appendix A. Shutting down OAS using the WebLogic console

The WebLogic Administration Server named ‘AdminServer’ should be left running.

1. Login to WebLogic console

2. In the left hand ‘Domain Structure’ choose Servers
3. The summary of servers is displayed

![Summary of Servers](image)

4. Click the checkbox next to **bi_server1** and choose **Shutdown**->**Force Shutdown Now**

![Summary of Servers](image)
Appendix B. Starting OAS using the WebLogic Console

If necessary, navigate back to the WebLogic control panel for Servers, click on the “Control” tab, check the box for **bi_server1**, and choose **Start**.
Appendix C. Stopping Node Manager

% bash
$ $JAVA_HOME/bin/jps | grep NodeManager
nnnn NodeManager
$ kill nnnn
$ $JAVA_HOME/bin/jps | grep NodeManager
$ exit
%

Appendix D. Starting WebLogic Node Manager

% bash
$ cd $MW_HOME
$ nohup $MW_HOME/user_projects/domains/bi/bin/startNodeManager.sh >node.out 2>&1 < /dev/null &
$ exit
%

Appendix E. Stopping WebLogic Admin Server

» Note, it is required to enter the ‘weblogic’ password, shown with the dots below, in cleartext.

» The last argument shown below with the ellipses has to be the actual fully qualified path name to the WebLogic domain.

% bash
$ $MW_HOME/oracle_common/common/bin/wlst.sh
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands
wls:/offline>
nmConnect('weblogic','●●●●●●','oas.example.com',9506,'bi','.../user_projects/domains/bi')
Connecting to Node Manager ...
<Nov 23, 2020 8:00:06 AM PST> <Info> <Security> ...
<Nov 23, 2020 8:00:06 AM PST> <Info> <Security> ...
<Nov 23, 2020 8:00:06 AM PST> <Info> <Security> ...
Successfully Connected to Node Manager.
wls:/nm/bi> nmServerStatus('AdminServer')
RUNNING
wls:/nm/bi> nmKill('AdminServer')
Killing server AdminServer ...
Successfully killed server AdminServer ...
wls:/nm/bi> nmServerStatus('AdminServer')
SHUTDOWN

wls:/nm/bi> nmDisconnect()
Successfully disconnected from Node Manager.
wls:/offline> exit()
Exiting WebLogic Scripting Tool.
$ exit
Appendix F. Starting WebLogic Admin Server

To access either Fusion MiddleWare Control, or the WebLogic Administration Console, the Administration Server needs to be running.

To cleanly support running all WebLogic servers under the control of the WebLogic Node Manager, the below approach is recommended.

Note, it is required to enter the ‘weblogic’ password, shown with the dots below, in cleartext.

The last argument shown below with the ellipses has to be the actual fully qualified path name to the WebLogic domain.

For OAS, this will be under the $MW_HOME.

```bash
% bash
$ $MW_HOME/oracle_common/common/bin/wlst.sh
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands
wls:/offline>
nmConnect('weblogic','●●●●●●','oas.example.com',9506,'bi','...../user_projects/domains/bi')
Connecting to Node Manager ...
Nov 23, 2020 8:00:06 AM PST <Info> <Security> ...
Nov 23, 2020 8:00:06 AM PST <Info> <Security> ...
Nov 23, 2020 8:00:06 AM PST <Info> <Security> ...
Successfully Connected to Node Manager.
wls:/nm/bi> nmServerStatus('AdminServer')
SHUTDOWN
wls:/nm/bi> nmStart('AdminServer')
Starting server AdminServer ...
Successfully started server AdminServer ...
wls:/nm/bi> nmServerStatus('AdminServer')
RUNNING
wls:/nm/bi> nmDisconnect()
Successfully disconnected from Node Manager.
wls:/offline> exit()
Exiting WebLogic Scripting Tool.
$ exit
%```
Appendix G. Recovering from a failed installation/configuration of OAS

The steps below can be utilized to recover from a failed installation/configuration of OAS:

A. Stop any running WebLogic Processes:
   1. Utilize ‘Appendix A - Shutting down OAS using the WebLogic console’.
   2. If appropriate, Utilize ‘Appendix H- Stopping and starting OHS using Fusion Middleware Control’.
   4. Utilize ‘Appendix C - Stopping Node Manager’ to stop the WebLogic Node Manager.

B. Clean up all related OAS artifacts from both DBMS and WebLogic:
   1. Run the RCU utility from the OAS $MW_HOME.
      
      $MW_HOME/oracle_common/bin/rcu
   
   2. On the first pages of the RCU utility, choose to drop a schema.
      Ensure to specify the correct schema prefix (i.e. OAS).
   3. Delete the OAS schema using RCU.
   4. Delete the Domain for OAS in the $MW_HOME for OAS:
      
      rm -rf $MW_HOME/user_projects/domains/bi
   
   5. It is not necessary, nor desirable, to delete the OAS $MW_HOME.

C. Proceed with ‘section 7.6 - Configure OAS’
Appendix H. Stopping and starting OHS using Fusion Middleware Control

» Login to Fusion Middleware Control
  » http://oas.example.com:9500/em

WebLogic Domain
→ Administration
→ OHS Instances

Starting OHS:
Appendix I. Validating JDBC Connect String

Java Program to Validate Database Details

```
import java.util.Properties;
import java.sql.SQLException;
import java.sql.Connection;
import java.sql.DriverManager;
public class SimpleJDBCTester {
    static String U = "user";
    static String P = "password";
    static String G = "v$session.program"; // For SQL Tracking
    static String J = "jdbc:oracle:thin:@"; // JDBC Thin Prefix

    static void usage(String pg) {
        System.out.printf("Usage: %s <conndesc> <username> [pwd]\n", pg);
        System.exit(1);
    }

    public static void main(String[] args) {
        try {
            Class.forName("oracle.jdbc.driver.OracleDriver");
        } catch (ClassNotFoundException ce) {
            System.err.println("OJDBC Jar Not Found: " + ce); System.exit(1);
        }

        if (args.length != 2 && args.length != 3) usage("SimpleJDBCTester");
        String pw = null; String cd = args[0]; String un = args[1].toUpperCase();
        if (!cd.startsWith(J)) {
            System.err.printf("Connect Descriptor must start with '%s'\n", J);
        } else {
            if (args.length == 3) pw = args[2];
            else pw = System.console().readPassword("Password: ");
            ct(cd, un, pw);
        }
    }

    static void ct(String cd, String un, String pw) {
        Connection conn = null; Properties prop = new Properties();
        try {
            if (un.equals("SYS")) un += " AS SYSDBA";
            System.out.print("Connecting to DBMS ... ");
            prop.put(U, un); prop.put(P, pw); prop.put(G, "JDBCTester");
            conn = DriverManager.getConnection(cd, prop);
            if (conn != null)
                System.out.println("Username/Password/ConnectDescriptor valid.");
            else System.out.println("Unknown Error!");
        } catch (SQLException se) {
            System.err.println("Error!\nUnable to connect: " + se);
        }
        finally {
            if (conn != null) {
                try { conn.close(); }
                catch (Exception e) {
                    System.err.println("Error Closing Connection: " + e);
                }
            }
        }
    }
}
```

Figure 50. Java Program to Validate Database Details
Instructions for Using Java Program to Validate Database Details

```bash
#BASH/SH
JAVA_HOME=$MW_HOME/oracle_common/jdk
CP="$MW_HOME/oracle_common/modules/oracle.jdbc/ojdbc8.jar:.
export JAVA_HOME CP

#CSH/TCSH:
setenv JAVA_HOME $MW_HOME/oracle_common/jdk/
setenv CP "$MW_HOME/oracle_common/modules/oracle.jdbc/ojdbc8.jar:.

#Compile code:
$JAVA_HOME/bin/javac SimpleJDBCTester.java

#Run code:
$JAVA_HOME/bin/java -cp "$CP" SimpleJDBCTester ...

#Positive Example:
$JAVA_HOME/bin/java -cp "$CP" SimpleJDBCTester "jdbc:oracle:thin:@/emrepos.example.com:1521/orcl.example.com" sysman
Password: ******
Connecting to DBMS ... Username/Password/ConnectDescriptor valid.

#Negative Examples:
#Bad Classpath:
$JAVA_HOME/bin/java SimpleJDBCTester "jdbc:oracle:thin:@emrepos.example.com:1521/orcl.example.com" sysman
OJDBC Jar Not Found: java.lang.ClassNotFoundException: oracle.jdbc.driver.OracleDriver

#Invalid Username/Password:
$JAVA_HOME/bin/java -cp "$CP" SimpleJDBCTester "jdbc:oracle:thin:@emrepos.example.com:1521/orcl.example.com" sysman
Password: ******
Connecting to DBMS ... Error!
Unable to connect: java.sql.SQLException: ORA-01017: invalid username/password; logon denied

#Incorrect Service name:
$JAVA_HOME/bin/java -cp "$CP" SimpleJDBCTester "jdbc:oracle:thin:@emrepos.example.com:1521/badsid.bad.com" sysman
Password: ******
Connecting to DBMS ... Error!
Unable to connect: java.sql.SQLException: Listener refused the connection with the following error: ORA-12505, TNS:Listener does not currently know of SID given in connect descriptor

#Bad Connect Descriptor:
$JAVA_HOME/bin/java -cp "$CP" SimpleJDBCTester "BADjdbc:oracle:thin:@emrepos.example.com:1521/orcl.example.com" sysman
Connect Descriptor must start with 'jdbc:oracle:thin:'

#Bad Listener Port:
$JAVA_HOME/bin/java -cp "$CP" SimpleJDBCTester "jdbc:oracle:thin:@emrepos.example.com:9999/orcl.example.com" sysman
Password: ******
Connecting to DBMS ... Error!
Unable to connect: java.sql.SQLException: IO Error: The Network Adapter could not establish the connection
```

Figure 51. Instructions for Using Java Program to Validate DBMS Connection Details
Appendix J. WebLogic Authentication Providers

To understand what the configuration goals are, it is important to provide some background.

WebLogic supports two distinct types of providers:

8. Identity Asserters – Only requires that the given username is valid.

Not shown in the above screen shot is a critical flag associated with each item in the list:

» REQUIRED
  » If the test fails, all the remaining providers are still consulted, but an overall result of FALSE is returned.
  » If the test succeeds, the overall result is temporarily set to TRUE, and the rest of the providers are consulted.

» REQUISITE
  » If the test succeeds, the overall result is temporarily set to TRUE, and the rest of the providers are consulted.
  » If the test fails, all the remaining providers are skipped, and FALSE is returned.

» SUFFICIENT
  » If the test succeeds, the rest of the providers can be skipped, and an overall result of TRUE is returned.
  » Otherwise, processing continues with the next provider in the list (if any).

» OPTIONAL
  » If the test succeeds, the overall result is temporarily set to TRUE.
  » If the test fails, the overall result is temporarily set to FALSE.

These flags, in conjunction with the order of the providers, determines whether a given username/password (for Authenticators) or a given username (for Identity Asserters), is valid.

Furthermore, consider that when a username/password, or just username, is being processed by WebLogic, the list of providers is consulted in order.

If the overall result of the chain of providers is TRUE, then the validation succeeds and an overall result of TRUE is returned, otherwise, an overall result of FALSE is returned.

(Google Search, n.d.)
CHAPTER 18. REFERENCES


OAS: Quick Reference For In-Place Upgrade From Oracle Business Intelligence Enterprise 12c To OAS On Linux (Doc ID 2645014.1). (2020, March). Retrieved from https://support.oracle.com/epmos/faces/DocContentDisplay?id=2645014.1


Installing and Configuring Oracle Analytics Server with Oracle Enterprise Manager Cloud Control

April 2021

Author: Abramson, Jerry (Oracle), Bhargava, Shefali (Oracle)
Contributing Authors: Ponnappa, Dechamma (Oracle)