

An Oracle White Paper
July 2014

Private Cloud Planning Guide Oracle Public Sector Revenue Management

Introduction	2
Architecture	2
Virtualization	4
Security	6
Management	8
Integration	9
High Availability	10
Backup and Recovery	10
Resources	10
Whitepapers	10
Minimal Reference Architecture	12

Introduction

The Oracle Public Sector Revenue Management (PSRM) application can be deployed on cloud infrastructure and hosting services to provide a Private Cloud, Software As A Service (SaaS) and hosted solutions for tax and revenue authorities. This document outlines the required architecture to implement Oracle Public Sector Revenue Management (PSRM) on such services.

This document applies to Oracle PSRM V2.4.0.0.0 and above.

Architecture

Oracle Public Sector Revenue Management (PSRM) can be implemented in a private cloud, public cloud or a hosted option as a complete solution with a number of key Oracle technologies¹. To implement a complete solution, the cloud implementation of the products must include additional technologies for security, management and integration.

For an Oracle PSRM cloud offering the following architecture is recommended:

¹ Non-Oracle alternatives may be used but the integration and testing of these alternatives are the responsibility of the hosted solution vendor.

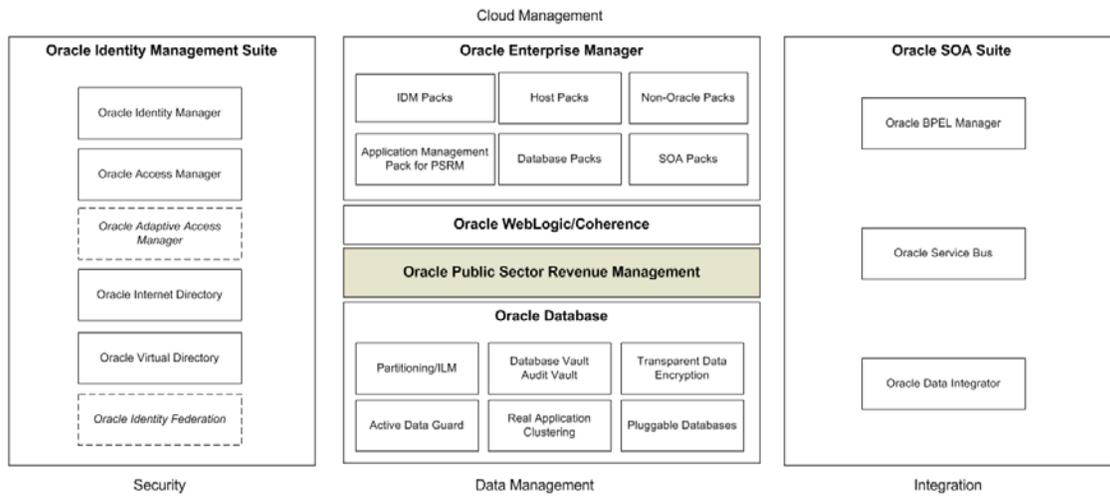


Figure 1 – Oracle PSRM Cloud Architecture

The components for this architecture are as follows:

TABLE 1 – COMPONENTS USED IN ORACLE PSRM CLOUD

COMPONENT	USE
Active Data Guard	High availability data replication
Application Management Pack for PSRM	Software Lifecycle Management Pack for Oracle PSRM
Audit Vault	(Optional) Centralized Auditing
Database Vault	Data protection from database privileged users
Information Lifecycle Management	Managing key tables using partitioning and management rules
Oracle Access Manager	Access Control and Single Sign On and Password Management
Oracle Adaptive Access Manager	(Optional) Fraud Detection
Oracle BPEL Process Manager	SOA based Orchestration
Oracle Coherence ²	Cluster used for Batch Architecture (<i>bundled with Oracle PSRM</i>)
Oracle Data Integrator	SOA based data integration for data loading and/or conversion
Oracle Database	Data Management and Storage
Oracle Enterprise Manager	Enterprise wide system management
Oracle Identity Analytics	(Optional) Analytics for all Identity Management Suite components
Oracle Identity Federation	(Optional) Allow external security stores to be included in architecture

² The bundled version of Oracle Coherence within Oracle PSRM is subject to a Restricted Use License. Refer to the Installation documentation for details.

COMPONENT	USE
Oracle Identity Manager	User Provisioning and Password Rules
Oracle Internet Directory	Default Security Store
Oracle Service Bus	SOA based Service Bus
Oracle Traffic Director	Software based connection routing for the cloud
Oracle Virtual Assembly Builder	Cloud Assembly Building
Oracle Virtual Directory	Virtualized Security (can also be used for including non-LDAP security sources into Cloud)
Oracle Virtual Machines	Core technology for deploying the components
Oracle WebLogic	J2EE Container for online and Web Services (also used by other components)
Other OEM Packs	Set of Packs to augment Oracle Enterprise Manager (OEM) with advanced functionality for all components
Partitioning	Data Partitioning for availability and data management
Pluggable Databases	Multi-tenant databases
Real Application Clustering	High availability database architecture
Transparent Data Encryption	Data file level encryption to protect backups

Virtualization

One of the basic building blocks of a cloud offering is the implementation of virtualization. This separates the architecture into manageable components and also offers customers flexibility in which parts of the solution are applicable to their preferred solution.

When implementing virtualization for the solution the following guidelines should be taken into account:

- Each component of the solution can exist on individual virtualized machines or combined to offer a reduced cost solution. The ability for individual components to live on the same virtualization should be checked prior to implementation by consulting the individual component installation documentation. For example, certain components must live on their own virtualizations and cannot share resources for architectural reasons. [Oracle Enterprise Manager](#) is an example of this.
- A simple virtualized deployment would be as follows:
 - Oracle PSRM separated into its own virtual machine with online and batch separated for scalability of individual components.
 - [Oracle Identity Management Suite](#) and [Oracle SOA Suite](#) in their own composite virtual machines. Individual components of the suite can be separated into their own virtual machines if the requirements deem it necessary. For example, if the security functions of the customer are separated then it may be necessary to split the components into individual machines for management points of view.

- Database components of all the technologies should be implemented on individual virtual machines with the necessary [Real Application Clusters](#) per product being implemented for high availability.
- Typically [Audit Vault](#) is used by specialists within the customer base or external auditors. If this is the case and [Audit Vault](#) is to be used it is recommended to separate this as its own virtual machine.
- [Oracle Enterprise Manager](#) and [Oracle Traffic Director](#) are typically not included in virtual machines but may be considered for virtual machines if necessary.

The example of this simple architecture is as shown:

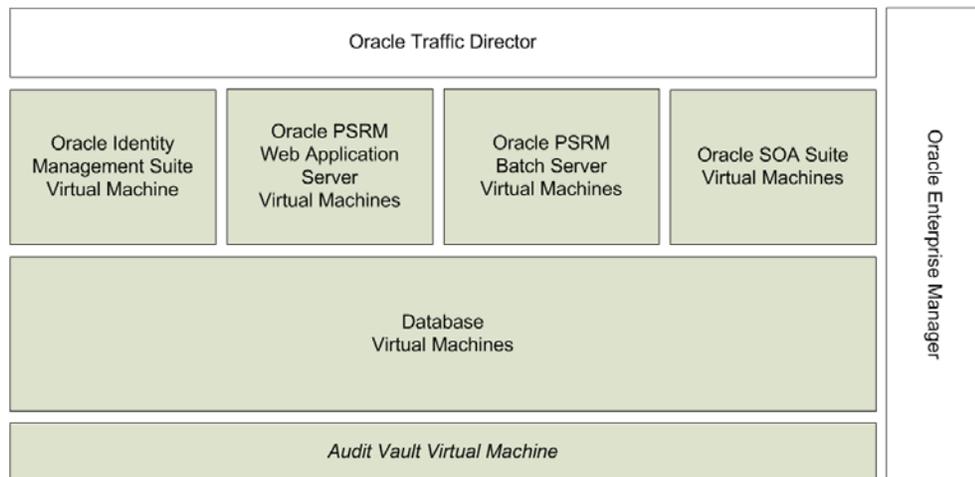


Figure 2 – Example Virtual Machine Architecture

- If complex combinations components are required, it is highly recommended that Cloud implementation consider using [Oracle Virtual Assembly Builder](#) to build necessary assemblies.
- The database components of each of the technologies can be on its own virtual machines or be implemented as a Pluggable Database within a common instance of Oracle 12c. At a minimum the database installation should be separated from the software.
- Oracle PSRM should be installed with the Web Application Server and Business Application Server co-existing on the same virtualized machine (known as a local installation). It is not recommended to separate the tiers on different virtualizations to reduce costs.
- To implement virtualization it may be necessary to manually install and configure the production settings for products on virtualized hardware and deploy from that source. If using [Oracle Virtual Assembly Builder](#) it is recommended to build assemblies from these prebuilt virtual installations.

Security

One of the major tenets of a cloud solution for Oracle PSRM is to ensure that the product is installed in a secure fashion and provides a security framework to allow customers to manage their environment (directly or indirectly). Oracle offers a wide range of technology that can be used to provide a secure environment for a cloud solution. The following diagram illustrates the preferred Oracle solution based security architecture for a cloud based solution:

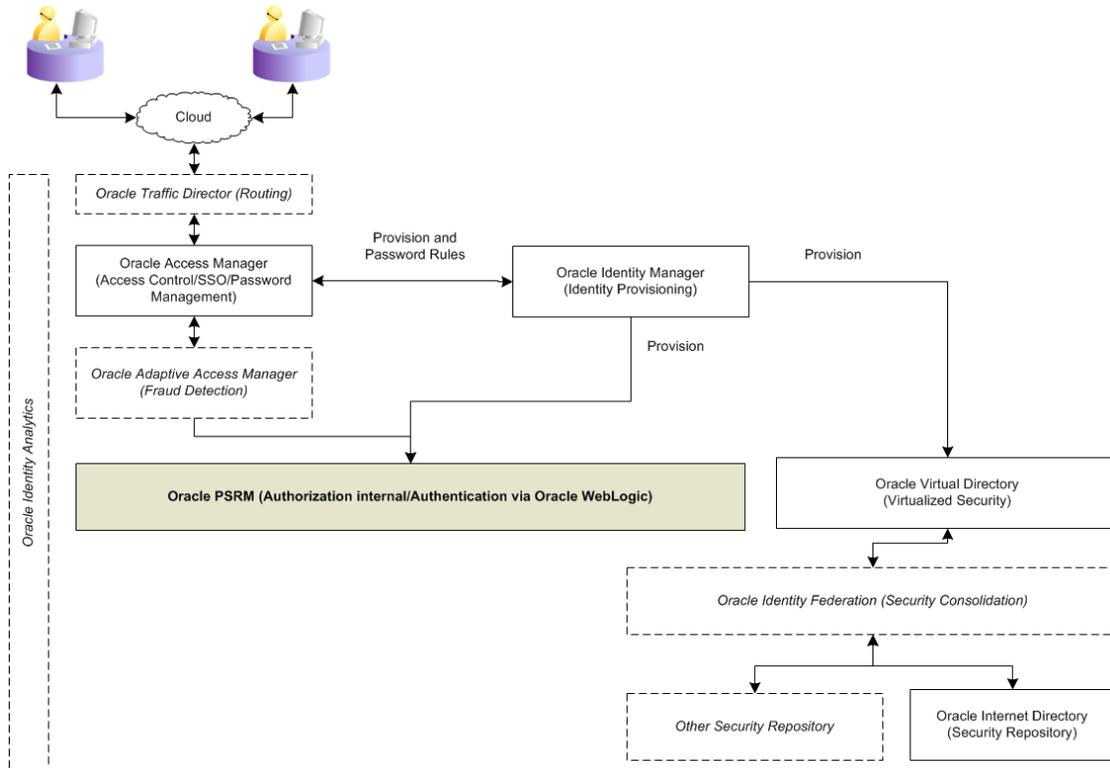


Figure 3 – Oracle PSRM Cloud Security Architecture

The following considerations should be implemented using this solution:

- All network access should use secure protocols such as https and t3s with the appropriate level of encryption and relevant certificates.
- All passwords used for administration should be protected in keystores using JCEKS based approaches and/or [Oracle Wallet](#). Passwords for administration should be protected using Credential Management within [Oracle Enterprise Manager](#).
- A security repository should be created for the customer within [Oracle Internet Directory](#) (or similar). This will act as the overall security repository for all components in the architecture. All the other components need to be configured to use this repository.
- If the customer prefers to use their own internal security repository it is recommended to implement [Oracle Identity Federation](#) to combine or replace security repositories.

- To combine repositories or provide a common LDAP interface it is recommended that [Oracle Virtual Directory](#) be used. Even if the customer uses [Oracle Internet Directory](#) only, it is recommended to implement [Oracle Virtual Directory](#) to provide a common interface and also allow expansion for the future. [Oracle Virtual Directory](#) can also be used to incorporate a non-LDAP based security repository as an LDAP source.
- To manage the user provisioning it is recommended to implement [Oracle Identity Manager](#). Oracle PSRM implements a [Service Provisioning Markup Language](#) (SPML) based interface to manage user identities from Oracle Identity Manager to the Oracle PSRM. The basic implementation steps are as follows:
 - The Oracle PSRM SPML based interface is loaded into [Oracle Identity Manager](#) using the Generic Technology Connector (GTC) interface within [Oracle Identity Manager](#). This provides full access to the user object within Oracle PSRM.
 - The customer/partner configures the mapping and business rules dictating the users profile, group access, data access rules, portal definitions, To Do roles, favorites and any other attributes for their site. It is recommended to use template users to greatly reduce the amount of configuration for this mapping and setting of rules.
- Password rules for the customer should be configured in [Oracle Identity Manager](#).
- It is strongly recommended to implement [Oracle Access Manager](#) for Access Control, Single Sign On and Password Management. This will allow the customer to finitely control access to their instances and also enforce password rules contained in [Oracle Identity Manager](#). [Oracle Access Manager](#) also offers comprehensive access auditing and logging facilities.
- If the customer requires fraud protection within their implementation it is recommended that [Oracle Adaptive Access Manager](#) be considered. This would require [Oracle Access Manager](#) to be configured to pass through [Oracle Adaptive Access Manager](#). The customer would then configure [Oracle Adaptive Access Manager](#) to recognize suspicious activities according to their company policies.
- For network routing in the cloud, Oracle recommends [Oracle Traffic Director](#).
- Optionally, if the customer wants a comprehensive solution for analyzing and collecting security metrics then [Oracle Identity Analytics](#) can be included in the solution.
- At the Database additional security should be considered:
 - [Transparent Data Encryption](#) should be enabled to protect backups from theft.
 - [Database Vault](#) should be installed and enabled to protect data from privileged database users.
- If the customer wishes to implement common auditing in the cloud then consider [Oracle Audit Vault](#).

Refer to the [References](#) section for documentation on how to implement these technologies with Oracle PSRM.

Management

An important aspect of Oracle PSRM on the cloud or hosted solution is to manage the technology with minimal effort to reduce costs and increase viability of a hosted/cloud solution. Oracle offers the [Oracle Enterprise Manager](#) set of products to manage, automate and monitor the technology across the various products from a common console.

[Oracle Enterprise Manager](#) provides a centralized console which house the configuration repository and provides the IT Operations with a set of comprehensive tools to manage their environment. This includes the following features:

- A security framework which allows individual administrators' access to operations credentials and operations functions.
- A job scheduling framework to execute processes outside of working hours to minimize outages.
- An incident management framework which automatically creates incidents from detected issues (with configurable tolerances). The incident can be assigned and tracked within the console for individual operators and can even be converted into a Service Request for referral to Oracle Support with relevant support data attached.
- An alerting framework to complement the incident management system to email, sms etc operators when specific tolerances have been reached.

The Oracle Enterprise Management console provides this framework and provides basic functionality for managing individual components but individual Enterprise Management packs provide advanced functionality and deep integration with their associated technology. The packs are divided into groups:

- [Cloud Management](#) – Managing aspects of the cloud from Enterprise Manager.
- [Application Management](#) – Managing Oracle's vertical and packaged applications. A pack is available for Oracle PSRM in this category.
- [Middleware Management](#) – Managing Oracle's WebLogic, SOA and Identity Management middleware products.
- [Database Management](#) – A comprehensive set of packs to manage all aspects of the database.
- [Hardware and Virtualization Management](#) – Managing the hardware and virtualizations.
- [Application Performance Management](#) – A set of packs that are focused on managing performance across the architecture.
- [Application Quality Management](#) – A set of packs used to minimize and reuse application quality assets across the architecture.
- [Lifecycle Management](#) – A set of packs to reduce deployment and provisioning time.
- [Heterogeneous Management](#) – A set of packs to manage non-Oracle technology and integrate Oracle Enterprise Manager with other consoles and help desk tools.

The recommended architecture of the management aspects is as follows: !

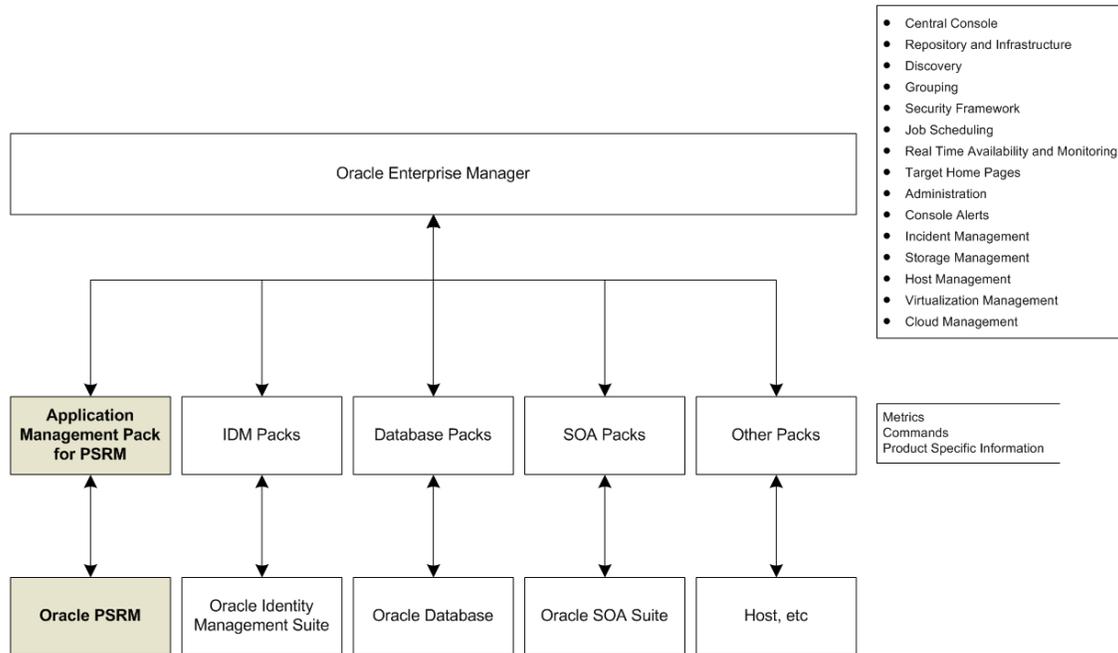


Figure 4 – Oracle PSRM Cloud Management Architecture

It is recommended to implement the following using [Oracle Enterprise Manager](#) for solutions using Oracle PSRM:

- Create a centralized console for the architecture using [Oracle Enterprise Manager](#) (OMS).
- Decide the packs to include in your solution to minimize your manual efforts and maximize effectiveness. The packs all automate and allow extension to cross automate across technologies with minimal intervention.
- Include the Application Management Pack for PSRM in your architecture.
- Install the agents on all the hosts you want to manage and discover the targets to manage in that architecture
- Define alerts, metrics and incident detection rules for your solution.

Integration

One of the basic facilities that is needed in any hosted/cloud solution is to integrate to other systems for transfer of data. Oracle offers the Oracle SOA Suite for integration. The components of this architecture are:

- [Oracle BPEL Process Manager](#) – An orchestration SOA based integration engine ideal for complex cross application integration.

- [Oracle Service Bus](#) – A high volume SOA based enterprise service bus.
- [Oracle Data Integrator](#) – A high volume data integration tool that is useful for bulk data integration and transformation.

Oracle PSRM has integrations to these SOA Suite components for inbound and outbound integrations.

High Availability

Any implementation of Oracle PSRM on a hosted/cloud implementation must be configured for high availability. It is recommended that the recommendations outlined in Oracle's [Maximum Availability Architecture](#) be implemented for the solution with the following additions:

- The Web Application and Business Application components of Oracle PSRM should be deployed to an [Oracle WebLogic](#) cluster. It should be noted that Oracle PSRM is stateless so any stateful configurations in the [Maximum Availability Architecture](#) are not applicable.
- The Batch Application Server should be deployed using an Oracle Coherence Cluster.
- It is recommended to use GridLink based data sources for the online system.
- Any JMS resources implemented on Oracle PSRM should be configured for high availability using the [Oracle Fusion Middleware High Availability Guide](#).
- It is recommended to implement [Real Application Clusters](#) on the Database server. Additionally [Active Data Guard](#) (or [Data Guard](#)) can be used for Business Continuity Planning purposes.

Backup and Recovery

Once the product is installed on the hardware it needs to be backed up as part of normal operations. Oracle PSRM is flexible in terms of implementing a backup strategy in the following aspects:

- Operating system backups are the minimal requirement for the software for the product. Other backup strategies that involve copying files or synching files at the operating system level are appropriate for Oracle PSRM software.
- [Database backup strategies](#) supported by the Oracle database are supported for the product.

Resources

Whitepapers

The Oracle PSRM set of products has a number of whitepapers that can be used to give details of integrations and configurations for hosted/cloud implementations. The following whitepapers, available from My Oracle Support, apply to this subject:

Security

- Oracle Utilities Application Framework Security Overview (Doc Id: 773473.1)
- LDAP Integration for Oracle Utilities Application Framework based product (Doc Id: 774783.1)
- Database Vault Integration (Doc Id: 1290700.1)
- Oracle Utilities Application Framework Advanced Security (Doc Id: 1375615.1)
- Oracle Identity Management Suite Integration with Oracle Utilities Application Framework based products (Doc Id: 1375600.1)

Best Practices

- Technical Best Practices for Oracle Utilities Application Framework Based Products (Doc Id: 560367.1)
- XAI Best Practices (Doc Id: 942074.1)
- Batch Best Practices for Oracle Utilities Application Framework based products (Doc Id: 836362.1)

Integration

- Oracle Utilities Application Framework Integration Overview (Doc Id: 789060.1)
- BI Publisher Integration Guidelines (Doc Id: 1299732.1)
- Oracle SOA Suite Integration with Oracle Utilities Application Framework based products (Doc Id: 1308161.1)
- Oracle WebLogic JMS Integration and Oracle Utilities Application Framework (Doc Id: 1308181.1)
- Integration Reference Solutions Oracle Utilities Application Framework (Doc Id: 1506855.1)
- Oracle Service Bus Integration Oracle Utilities Application Framework (Doc Id: 1558279.1)
- Audit Vault Integration (Doc Id: 1606764.1)

Other

- Performance Troubleshooting Guideline Series (Doc Id: 560382.1)
- Software Configuration Management Series (Doc Id: 560401.1)
- Oracle Utilities Application Framework Architecture Guidelines (Doc Id: 807068.1)
- Production Environment Configuration Guidelines (Doc Id: 1068958.1)

- What's New In Oracle Utilities Application Framework V4 (Doc Id: 1177265.1)
- Implementing Oracle ExaLogic and/or Oracle WebLogic Clustering (Doc Id: 1334558.1)
- IBM WebSphere Clustering for Oracle Utilities Application Framework (Doc Id: 1359369.1)
- Implementing Oracle Exadata with Oracle Utilities Customer Care and Billing (Doc Id: 1486886.1)
- Certification Matrix for Oracle Utilities Products (Doc Id: 1454143.1)
- Oracle Application Management Pack for Oracle Utilities Overview (Doc Id: 1474435.1)
- Native Installation Oracle Utilities Application Framework (Doc Id: 1544969.1)

Minimal Reference Architecture

When implementing Oracle PSRM on a cloud there are a number of architectures that can be used to implement specific use cases.

For customers who want a minimal solution the following architecture is recommended:

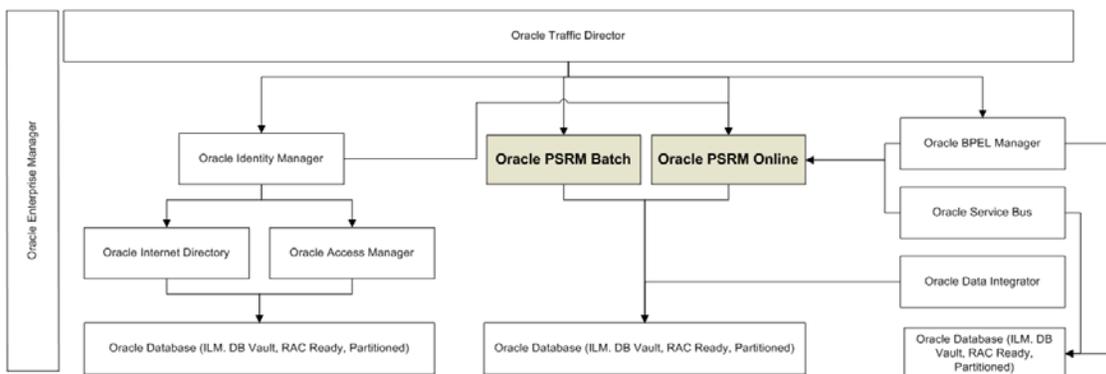


Figure 5 – Minimal Oracle PSRM Cloud Management Architecture

The following components constitute this architecture:

- [Oracle Traffic Director](#) will provide the routing rules and load balancing for all the components in the solution.
- [Oracle Identity Manager](#) will provide the user provisioning for all the components of the solution as well as centrally storing password formatting rules. It is recommended to start with a simple set of configuration rules for Oracle Identity Manager and build the rules for the individual customers. Refer to *Oracle Identity Management Suite Integration with Oracle Utilities Application Framework based products (Doc Id: 1375600.1)* whitepaper for more details.
- [Oracle Access Manager](#) will provide the single sign on interface, password management (via an interface to [Oracle Identity Manager](#)) and session tracking capabilities (via WebGate) for all the components of the solution. The customer will see the [Oracle Access Manager](#) logon screen at the start of their sessions which will logon across systems. The [Oracle Access](#)

[Manager Security Provider](#) adapter for Oracle WebLogic is used to connect the components to [Oracle Access Manager](#). Refer to *Oracle Identity Management Suite Integration with Oracle Utilities Application Framework based products (Doc Id: 1375600.1)* whitepaper for more details.

- [Oracle Internet Directory](#) will act as the centralized security store using the LDAP protocol for integration to other components in the solution. Depending on the security requirements of the customer [Oracle Virtual Directory](#) may also be required. Refer to *Oracle Identity Management Suite Integration with Oracle Utilities Application Framework based products (Doc Id: 1375600.1)* whitepaper for more details.
- [Oracle SOA Suite](#) components such as [Oracle BPEL Process Manager](#), [Oracle Service Bus](#) and [Oracle Data Integrator](#) should be used for interfacing to other cloud offerings or on premise applications. Refer to *Oracle SOA Suite Integration with Oracle Utilities Application Framework based products (Doc Id: 1308161.1)* and *Oracle Service Bus Integration Oracle Utilities Application Framework (Doc Id: 1558279.1)* whitepapers for more details of the integration.
- Oracle PSRM should be housed on cloud infrastructure and ideally online and batch should be separated for sizing and optimization purposes. At a minimum clustering should be used for high availability with [Oracle WebLogic](#) clustering used for online clustering and [Oracle Coherence](#) clustering used for batch clustering. Refer to *Implementing Oracle ExaLogic and/or Oracle WebLogic Clustering (Doc Id: 1334558.1)*, *Batch Best Practices for Oracle Utilities Application Framework based products (Doc Id: 836362.1)* and *Oracle Utilities Application Framework Architecture Guidelines (Doc Id: 807068.1)* whitepapers for more information.
- [Oracle Database](#) should be used to house all the data from each component. Where possible each product groups information should be stored in a separate database (or pluggable database) according to the guidelines for each of the products. At a minimum the database should be setup as [Real Application Cluster](#) ready, [Database Vault](#) installed and [ILM/Partitioning](#) installed for data lifecycle management.
- [Oracle Enterprise Manager](#) should be installed with relevant packs to manage the components that have been installed in the architecture.

The High availability dimension to the architecture should conform to Oracle's [Maximum Availability Architecture](#).



Private Cloud Planning Guide
July 2014
Author: Anthony Shorten, Principal Product
Manager

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 1010

Hardware and Software, Engineered to Work Together