

# Oracle Identity Manager (OIM) as Enterprise Security Platform - A Real World Implementation Approach for Success



Manvendra Kumar – AST Corporation, IL  
Scott Brinker – College of American Pathologist, IL  
August 17, 2012

# Agenda



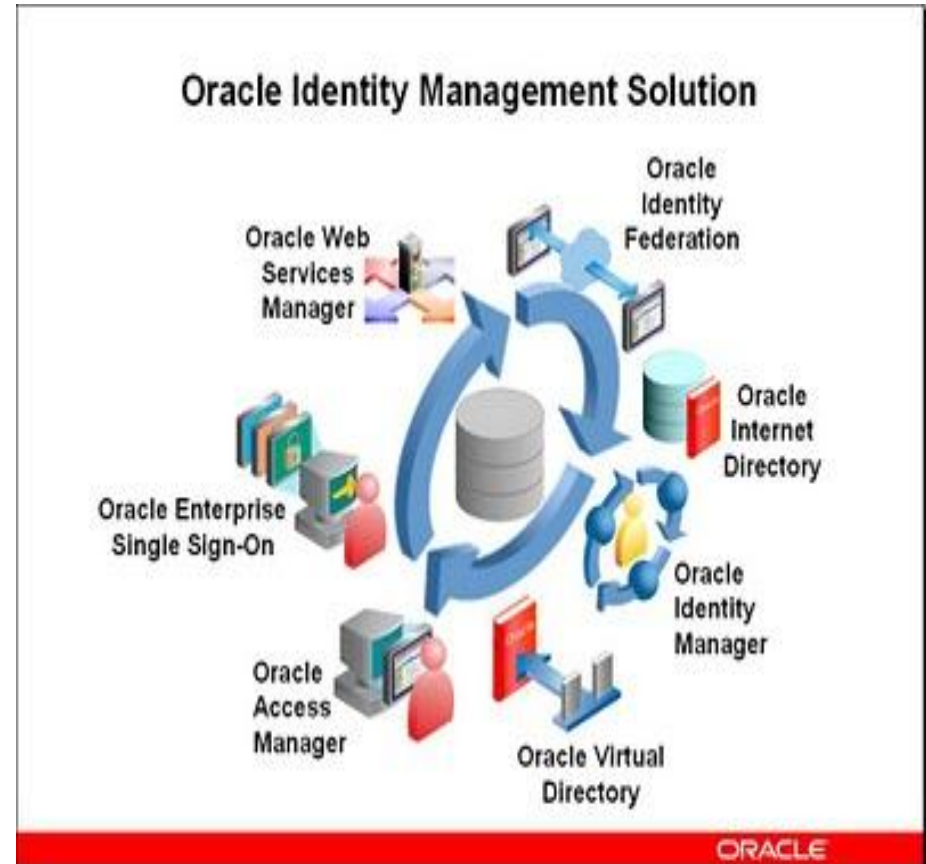
- Oracle Identity Management Components
- Case Study: Oracle Security Product Implementation at College of American Pathologist (CAP)
  - Business Challenges
  - Architecture
  - Implementation Strategy
  - Implementation Challenges
- Recommended Approach for Oracle Security Product Implementation
- Questions

# WHAT IS ENTERPRISE SECURITY?

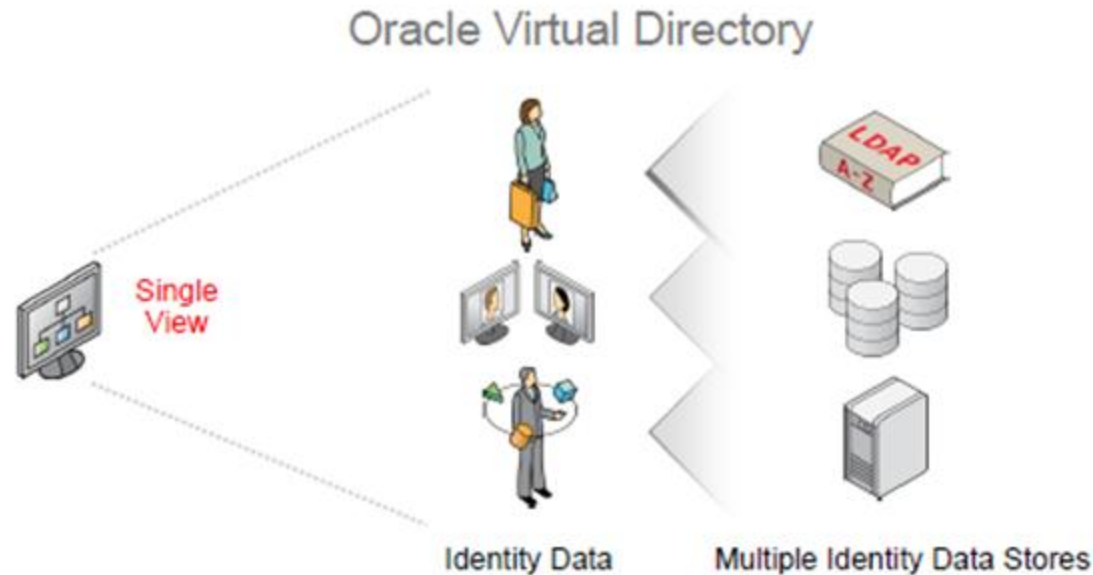
# Oracle Identity Management Components

Enables enterprise to

- Manage data about users, devices and services in a accurate and secure manner
- Configure and manage identity data
- Control access to applications and resources
- Synchronize and combine data from different resources
- Share data across domains



# Directory Services (OID/OVD)

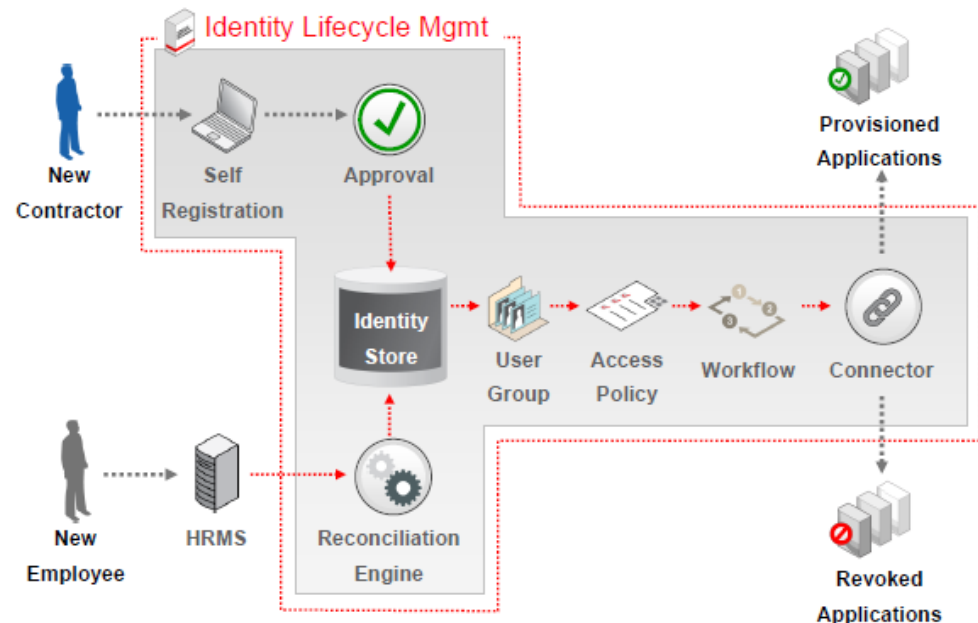


- Oracle Internet Directory (OID) is a specialized database that stores and retrieves collections of identity and security information about objects (can be user, resource, etc.)
- OID is built on Oracle Database and uses LDAP (Lightweight Directory Access Protocol) interface for data retrieval
- Oracle Virtual Directory (OVD) is an LDAP service that provides a single, abstracted view of enterprise directory servers and databases from a variety of vendors
- OVD addresses the challenge of lack of single source for identity data within enterprise

# Oracle Identity Manager (OIM)



- Identity Provisioning
  - Automates the administration of user access privileges across a company's resources—from initial on-boarding to final de-provisioning of an identity
  - Who, What, When & Why
  - Rules & Access Policies
  - Integration framework
- Identity Administration
  - Delegated Administration
  - Self-Registration & Self-Service
  - User & Group Management



# Oracle Access Manager (OAM)



- Replacement for OSSO solution offered by Oracle for EBS Suite
- Provides Single Sign-On (SSO) for Web Applications
- 11g enables Microsoft Internet Explorer users to automatically authenticate to their SSO Web applications using desktop credentials
- Enables application protection using Authentication & Authorization



# Other Oracle Identity Management Components



- OIF
- OES
- OAAM
- OIA etc...



Oracle Identity Manager (OIM): A Real World Implementation  
Approach for Success

# CASE STUDY: ORACLE SECURITY PRODUCT IMPLEMENTATION AT COLLEGE OF AMERICAN PATHOLOGIST (CAP)

# About CAP



- The College of American Pathologists (CAP) is the leading non-profit organization of board-certified pathologists, serving patients, pathologists, and the public
- CAP has about 18,000 members and 600 staff members
- CAP has a total of 4 legacy environments and 5 oracle environments which contains a variety of oracle applications from EBS, OBIEE, Hyperion, WCS, UCM and SOA

# Business Challenges At CAP



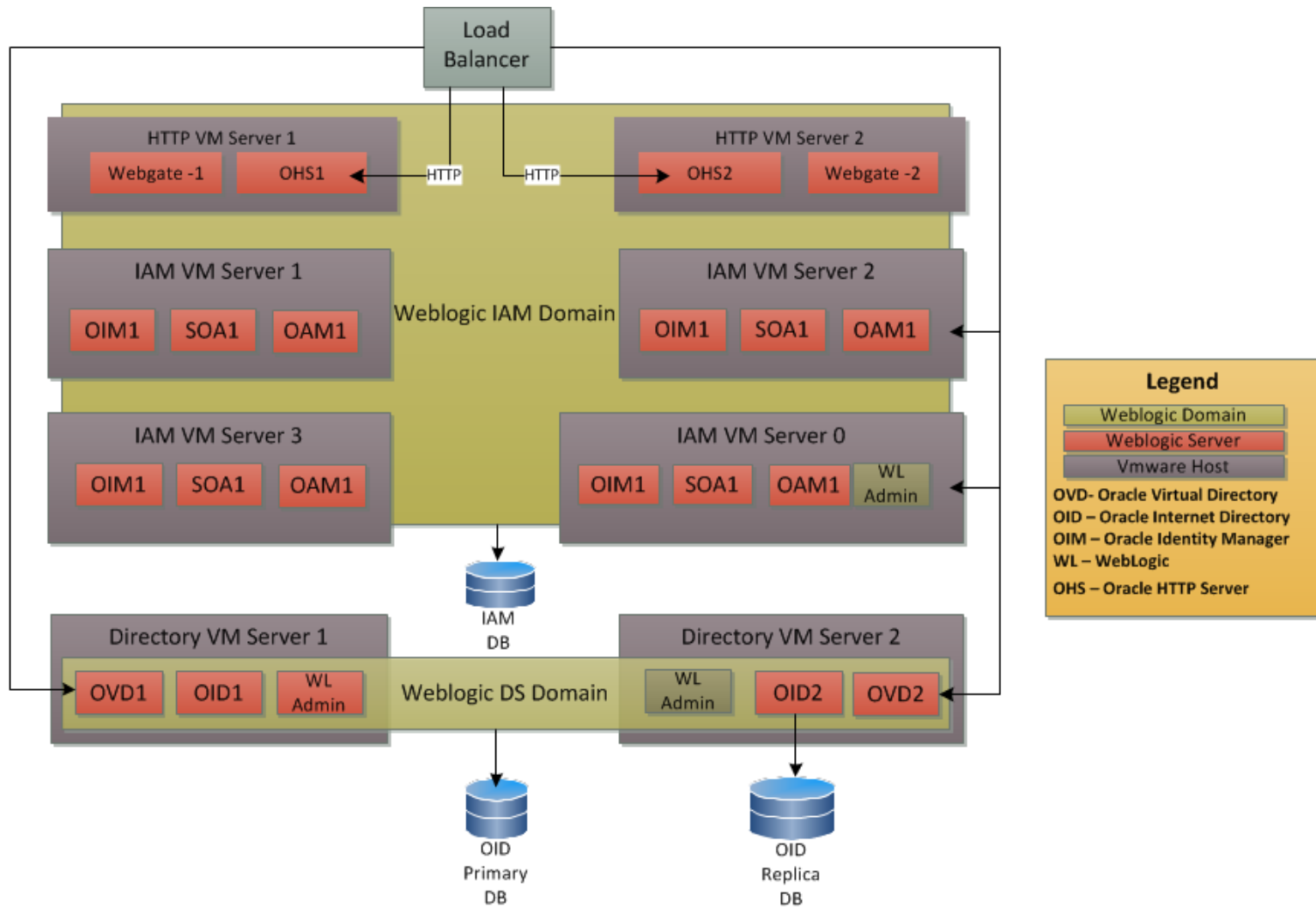
- Multiple Identity Repositories
  - Tactical OID
  - RedHat LDAP
  - Microsoft Active Directory (AD)
  - Application Specific local Identity Stores
- End User having multiple identities across enterprise
- License Management & Limitations
- Supporting different technologies
- Manual User on-boarding, provisioning and de-provisioning process causing
  - Loss of productivity
  - Incomplete and inconsistent access control
- Lack of single source of truth for user identity
  - Ceridian HR System for Staff and Temps
  - Tactical OID & AD for Staff, Consultants, Contractors and Temps
  - RedHat LDAP & TCA for Staff, External Users, Members, Inspectors
- Duplication of Identities across enterprise for users with multiple roles

# Solution Identified to address Business Challenges

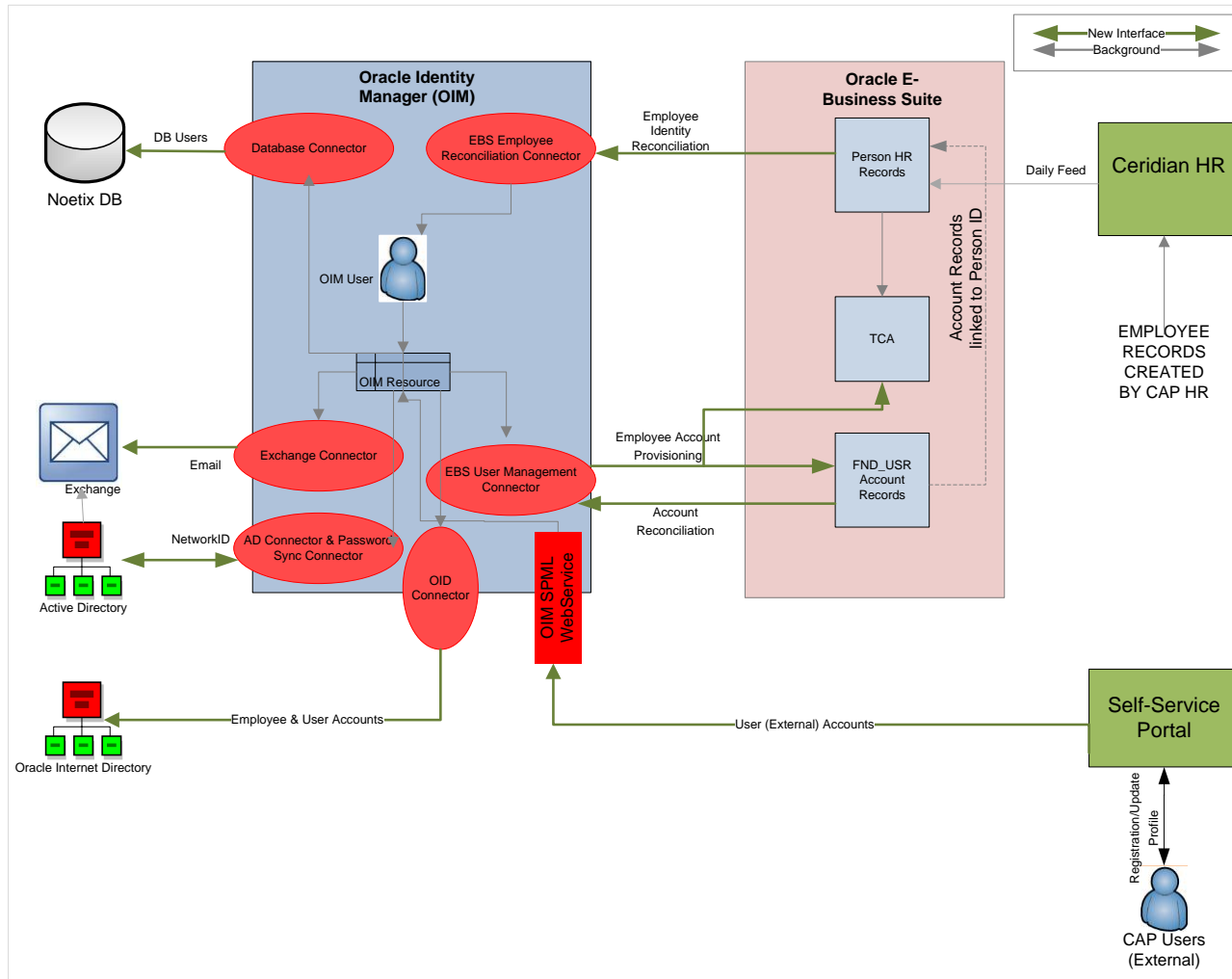


- Consolidation of multiple identity repositories
- Have single identity for every user across enterprise (one set of user id & password across all application)
- Automation around User On-boarding, provisioning and de-provisioning processes
- Enable single sign-on functionality across critical applications

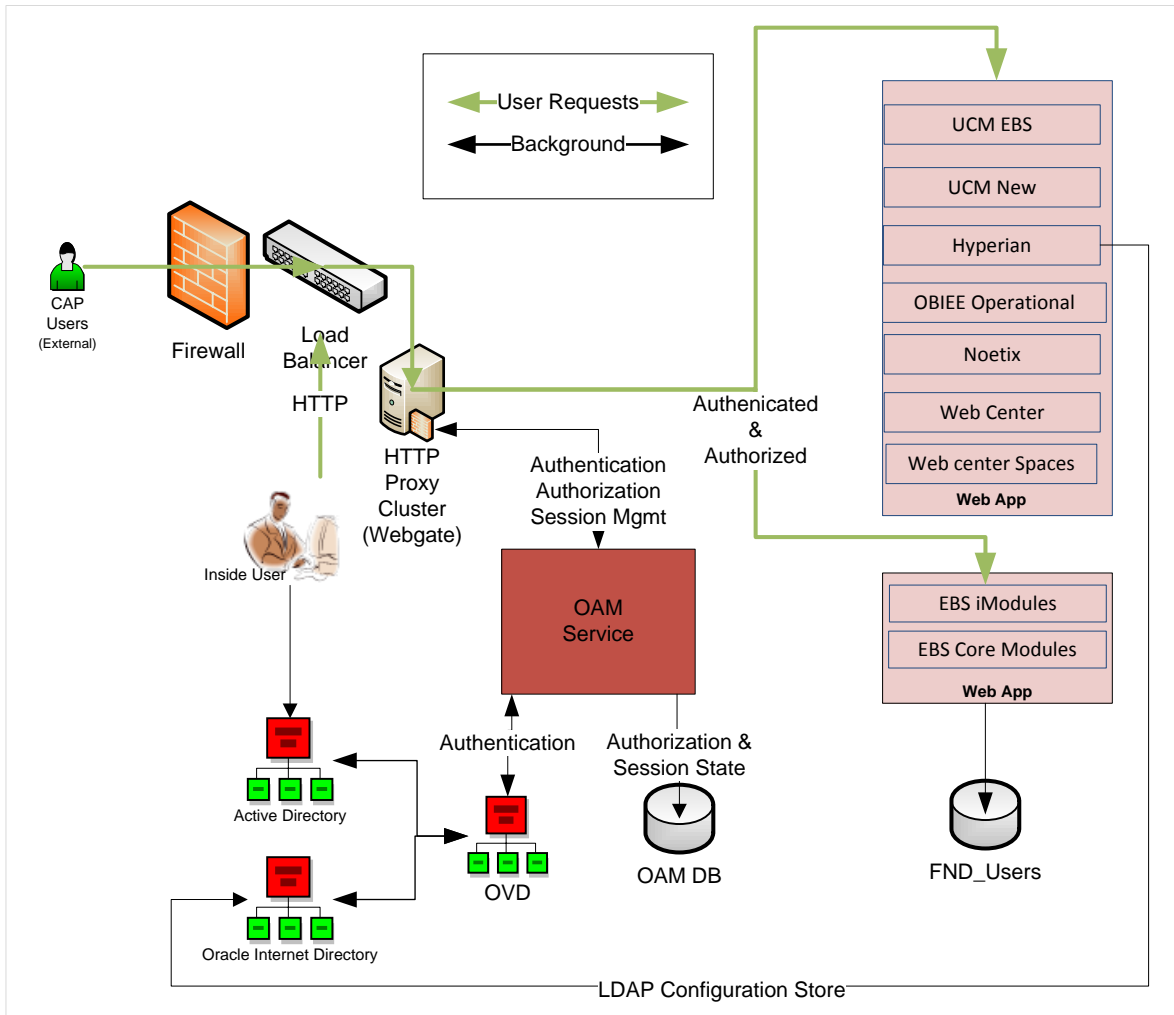
# Physical Architecture



# Logical Architecture: User Provisioning



# Logical Architecture: User Access Management (SSO)



# Implementation Strategy



- Phased Implementation Approach
  - Phase 1 – Planning & Discovery
  - Phase 2 – Implementing Security Infrastructure, User provisioning, Single Sign On and Identity Federation
  - Phase 3 – Role based provisioning & Delegated Administration
- Creating Application Software Version Matrix
- Identifying Applications (Oracle & Non-Oracle) for Security Integration
- Engagement Plan
  - For Oracle Support Escalation Team
  - For Interfacing Application SMEs
  - For Interfacing Application Test Resources
- Detailed Test Plan
- Communication Plan for different group of users



# Application Software Version Matrix



CAP Application Software Version Matrix												
Application Details							Oracle IDM Component					
#	Application	Version	Application Servers	Vendor	SSO	Provisioning	OAM	OIF	OIM	OID,OVD	OES	Others (Connector)
1	Ceredian - SelfService			Ceredian	Not Required	Not Required		X				Require a non-network ID to access.
2	Ceredian - Time & Attendance			Ceredian	Not Required	Not Required		X				Require a non-network ID to access.
3	ECM-UCM (EBS)		Weblogic 10.3	Oracle	Required	Required	X		X			Oracle Internet Directory
4	ECM-UCM (New Portal)	11.1.1.3	Weblogic 10.3	Oracle	Required	Required	X		X	X	X	Oracle Internet Directory
5	ECM-IPM	11.1.1.3	Weblogic 10.3	Oracle	Required	Required	X		X	X		Oracle Internet Directory + Custom
6	ECM-ODC	11.1.1.3	NA	Oracle	Not Required	Not Required	X		X	X		Not Required
7	ECM-10g (Spaces)	10.x	Weblogic 10.3	Oracle	Required	Required	X		X	X		Oracle Internet Directory + Custom
8	WebCenter Portal/Spaces	11.1.1.2.0	Weblogic 10.3	Oracle	Required	Required	X		X	X		Oracle Internet Directory + Custom
9	OBIEE Operational	11.1.1.3	Weblogic 10.3	Oracle	Required	Required	X		X	X		Oracle Internet Directory + Custom
10	OBIEE Data Warehouse (future)	11.1.1.3	Weblogic 10.3	Oracle	Required	Required	X		X	X		TBD
11	Noetix/Answers		Weblogic 10.3	Noetix	Required	Required			X	X		Oracle e-Business User Management + Database Application Tables
12	Hyperion	11.1.2.1	Weblogic 10.3	Oracle	Not Required	Required	X		X	X		Oracle Internet Directory + Custom
13	TCA	12.1.3	OiAS	Oracle	Not Required	Required						Oracle e-Business User Management + Database Application Tables

# Implementation Challenges



- Technical Challenge
  - Timely response and patch delivery from Oracle for issues like
    - LDAP SYNC do not work as stated
    - Trusted Source Reconciliation connector fails when user id is blank
    - OIM SPML Web Service operations not supported
    - Undesired error logs during execution of configuration and install scripts
    - Event Handler limitations for Trusted Source Reconciliation
  - Multiple integration paths
    - Connectors
    - Adaptors
    - SPML Services
    - Custom Web Services for Legacy application
  - Keep Staging Environments up to date with all patches
  - Not all Oracle Applications (to be integrated) configured the same way
  - Identifying source of truth for provisioning

# Implementation Challenges (cont.)



- Requirement Challenges
  - Identifying all potential interfacing applications (oracle and non-oracle)
  - Identifying target applications for automated provisioning
  - Identifying applications as a valid candidate for Single Sign-On
  
- Engagement Challenges
  - Identifying technical SMEs for every identified application
  - Identifying Testing resources for every identified application
  - Ensuring SMEs and Testing resources availability for the project
  - Follow-up with SMEs and Testing resources

# Recommendations



- Oracle Security Solution is for Enterprise and not a point solution (Ensure Value Proposition)
- Phased Approach for Oracle Identity Management Implementation can avoid failure and cost overrun
- Selecting correct Software Version can avoid compatibility issues (11.1.1.5 & 11.1.1.6 are certified versions available for use)
- Having a good escalation path to address Oracle Support issues can help in keeping the project on schedule
- Having an engagement strategy plan can help in addressing unknowns during early phase of implementation cycle
- Defining Testing Scope can avoid duplicate testing effort as well as ensure completeness
- Utilizing ticketing system for application integration, if available

# Questions & Answers



# Contact Information



## Presenter's Name:

Manvendra Kumar  
[mkumar@astcorporation.com](mailto:mkumar@astcorporation.com)  
[www.astcorporation.com](http://www.astcorporation.com)

Scott Brinker  
[sbrinke@cap.org](mailto:sbrinke@cap.org)  
[www.cap.org](http://www.cap.org)