Oracle Identity and Access Management
AGENDA

- Overview
- Features
- Components
- Customizations
- APIs
- Oracle Identity Manager Connectors
- High Availability Concepts
- High Availability Architecture
Identity & Access manager is a framework of business processes that facilitates the management of electronic or digital identities.

What is your Identity?
OVERVIEW

Identity & Access manager is a framework of business processes that facilitates the management of electronic or digital identities.

What is your Identity on all these applications?
Identity Self Service allows users to access the Unauthenticated Self Service Console by clicking the Forgot User Login?, Forgot Password?, New User Registration, or Track My Information links.

What if you register only once?
IDAM provides an authentication process that allows a user to access multiple applications with one set of login credentials.

What if you Sign in only once?
IDAM incorporates three major concepts: identification, authentication and authorization.

Use of IDAM in Organizations?

- Few Administrators
- Lack of Audit Staff
- Too many privileged accounts

Thousand of systems
10 thousands of apps
100 thousands of users
Millions of Entitlements
FEATURES

- No Need to Change Existing Infrastructure
- Simplified Self Service
  - Self registration, password management & request tracking.
- Eliminates Ghost Accounts/Access or Privileges
  - Account effective dates.
- Comprehensive User Administration
  - User, role and organization management.
- Reduces IT Operational Costs and Administration Overhead
- Centralize Audit Trails of Security Events
- Automatic Policy Enforcement Across Systems
COMPONENTS

List of basic components required to deploy an IDAM solution. All of these components are deployed on WebLogic server.

- Oracle Access Manager (OAM)
- Oracle Identity Manager (OIM)
- Oracle Adaptive Access Manager (OAAM)
- Oracle Identity Federation (OIF)
- Oracle Unified Directory (OUD)
- Business Intelligence Publisher (BIP)
- Service Oriented Architecture (SOA)
- Oracle HTTP Server (OHS)
COMPONENTS- Oracle Access Manager

Oracle Access Manager’s Access System provides centralized authentication, authorization, and auditing to enable single sign-on and secure access across enterprise resources such as web and J2EE resources (JSP, Servlets, EJBs, etc.) and legacy systems.

- Single Sign On
- Session management, session expiration and timeout
- Password policies, password expiration
- Custom authentication plugins
COMPONENTS- Oracle Identity Manager

Oracle Identity Management enables organizations to effectively manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall and into the cloud.

- User management
- Role management
- Organization management
- Provisioning & Reconciliation
- Connectors
- LDAP sync
- Track requests
- Pending approvals
- Password policies
COMPONENTS- Oracle Adaptive Access Manager

Oracle Adaptive Access Manager is an innovative, comprehensive feature set to help organizations prevent fraud and misuse. It provides standard authentication mechanisms, innovative risk-based challenge methods.

- Real time risk analysis
- Security questions & answers
- One Time Password (OTP)
- Device fingerprinting
- Virtual authentication devices
- Search & compare transactions
- Policy management

Authentication is valid but is this really John Smith? Is anything suspicious about John’s access request? Can John answer a challenge if the risk is high?
COMPONENTS - Oracle Identity Federation

Oracle Identity Federation enables business partners to achieve integration in the identity management realm, by providing a mechanism for companies to share identity information across their respective security domains.

- **Transient Federation**
  - Session based federation
  - May or may not have account with IDP/SP.

- **Mapped Federation**
  - One to one linking of user account on IDP/SP.
  - User account on IDP/SP with common attributes.

- **Linked Federation**
  - No common attributes.
  - Account linking based on UID, Employee code etc.

- **Role Based Federation**
  - Based on Role of Identity manager/developer.
COMPONENTS- Oracle Unified Directory

Oracle Unified Directory is a comprehensive next generation directory service. It is designed to address large deployments and to provide high performance, and is highly extensive. Oracle Unified Directory is easy to deploy, manage, and monitor.

- Data replication
- High availability
- Indexing
- Access control
- Virtualization
- Directory service schema
- Schema mapping
COMPONENTS - BI Publisher

Oracle BI Publisher is the reporting solution to author, manage, and deliver all your reports and documents easier and faster than traditional reporting tools.

- Create any kind of report with any kind of data
- Generate report in any kind of format (excel, pdf, csv etc.)
- View at any kind of platform
- Link & filter with any kind of data
- Reports creation with no coding/scripting
COMPONENTS- SOA

Oracle SOA Suite enables services to be created, managed, and orchestrated into SOA composite applications.

- Messaging
- Service discovery
- Orchestration
- Web services management & security
- Business rules
- Events framework
- Business activity monitoring
COMPONENTS- Oracle HTTP Server

Oracle HTTP Server is deployed at top of IDAM components to accept and manage user requests based on internal configuration.

- HTTP listener
- Load balancing
- URL rewriting
- Proxy server capabilities
- mod_wl_ohs plugin
Customization

This section describes utilities used to customize various components and features of Oracle Identity Manager.

- **Event handlers**
  - **Types:** Preprocess, post process, validation, finalization
- **Schedulers**
- **Plugins**
- **UI customization using ADF**
- **Custom workflows**
- **OIM, OAM & OAAM APIs**
- **Notification service**
- **Reports & audit**
APIs

Oracle provides a network-aware, Java-based application programming interface (API) that exposes Services. These APIs can be used for building clients for Oracle Identity Manager and for integrating third-party products with the Oracle Identity Manager platform.

- OIM API
- OAM API
- OAAM API
**OIMClient Library** is the entry point for accessing the APIs available in Oracle Identity Manager. It is used to make initial connection with Oracle Identity Manager to perform different tasks.

- UserManager API
- RequestService API
- RoleManager API
- OrganizationManager API
- SchedulerService API
- NotificationService API
APIs- Oracle Access Manager

The oracle.security.am.asdk & com.oblix.access package provides the Oracle Access Manager 10g & 11g version of the Application Programming Interface (API).

- **Oracle Access Manager Access SDK Java API**
  - Provides authentication and authorization API for compatibility with the OAM 10g and 11g.

- **Oracle Access Manager Extensibility Java API**
  - Provides a set of authentication plugin interfaces and SDK tooling for customers to build customized authentication plugins, and to plug the customized authentication plugins into the system.

- **Oracle Security Token Service Java API**
  - Allows developers to write classes that allow OSTS to issue and validate custom tokens.
APIs- Oracle Adaptive Access Manager

OAAM native integration involves customizing the client application to include OAAM API calls at various stages of the login process.

- **Native Integration**
  - SOAP service wrapper API for Java or .NET applications
  - In-Proc API for Java applications only

- **Non Native Integration**
  - **VCryptCommon** contains the common APIs.
  - **VCryptTracker** contains the APIs for fingerprinting and collecting authentication and transaction logs.
  - **VCryptAuth** contains the APIs for accessing the Authenticator and KBA modules.
  - **VCryptRulesEngine** contains the APIs for running the rules.
  - **VCryptCC** contains the APIs for invoking customer-care-related requests.
Oracle Identity Manager Connectors

Identity Connectors are used to integrate Oracle Identity Manager with external, identity-aware applications.

- **Provisioning**
  - You can use Oracle Identity Manager to create, maintain, and delete users on target systems. In this configuration, Oracle Identity Manager acts as the front-end entry point for managing user data on the target systems.

- **Reconciliation**
  - Oracle Identity Manager periodically poll target systems data for maintaining an up-to-date profile of all accounts that exist on those systems.
High Availability Concepts

High-availability clusters (also known as HA clusters or fail-over clusters) are groups of computers that support server applications that can be reliably utilized with a minimum amount of down-time.

- Protection from downtime
- Saves you from lost revenue
- Simplify maintenance
- Maximum flexibility
- Improve agility

*Let's have a look at IDAM high availability architecture on next slide...*
IDAM High Availability Architecture
Thank You