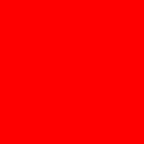




# ORACLE®

## **iDay – Identity Management Web Access Management / Web SSO: from zero to hero**

**Kenneth Heung, Senior Architect,  
APAC Channel Enablement, Oracle Fusion Middleware**



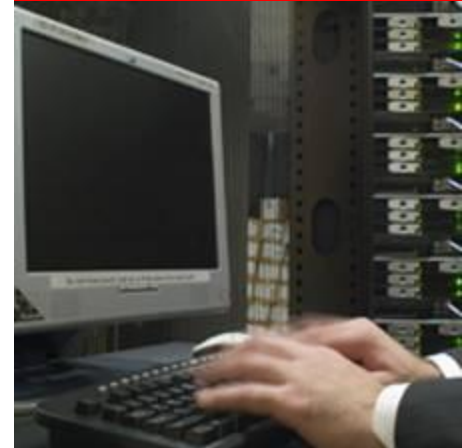
This presentation is for informational and enablement purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle.

# Web Access Management – from **zero** to hero

- Objectives
  - Quick introduction to Web Access Management and Web Single Sign-On; Oracle Access Manager (features & functions, technical architecture)
  - Typical SSO integration to applications
  - Oracle Access Manager 11g - highlights and positioning
  - Introduction to “Federation” – extending SSO to partners (concepts, not deep dive), Oracle Identity Federation & Fedlet

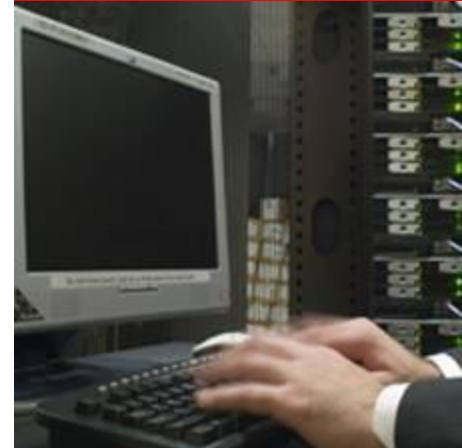
# Agenda

- Web Access Management – A quick introduction
- Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details
- Web SSO with OAM 11g – typical integration scenario example(s)
- Highlights in OAM 11g
- Extending Web SSO from enterprise environment to cross security domain – Identity Federation
- Demonstrations

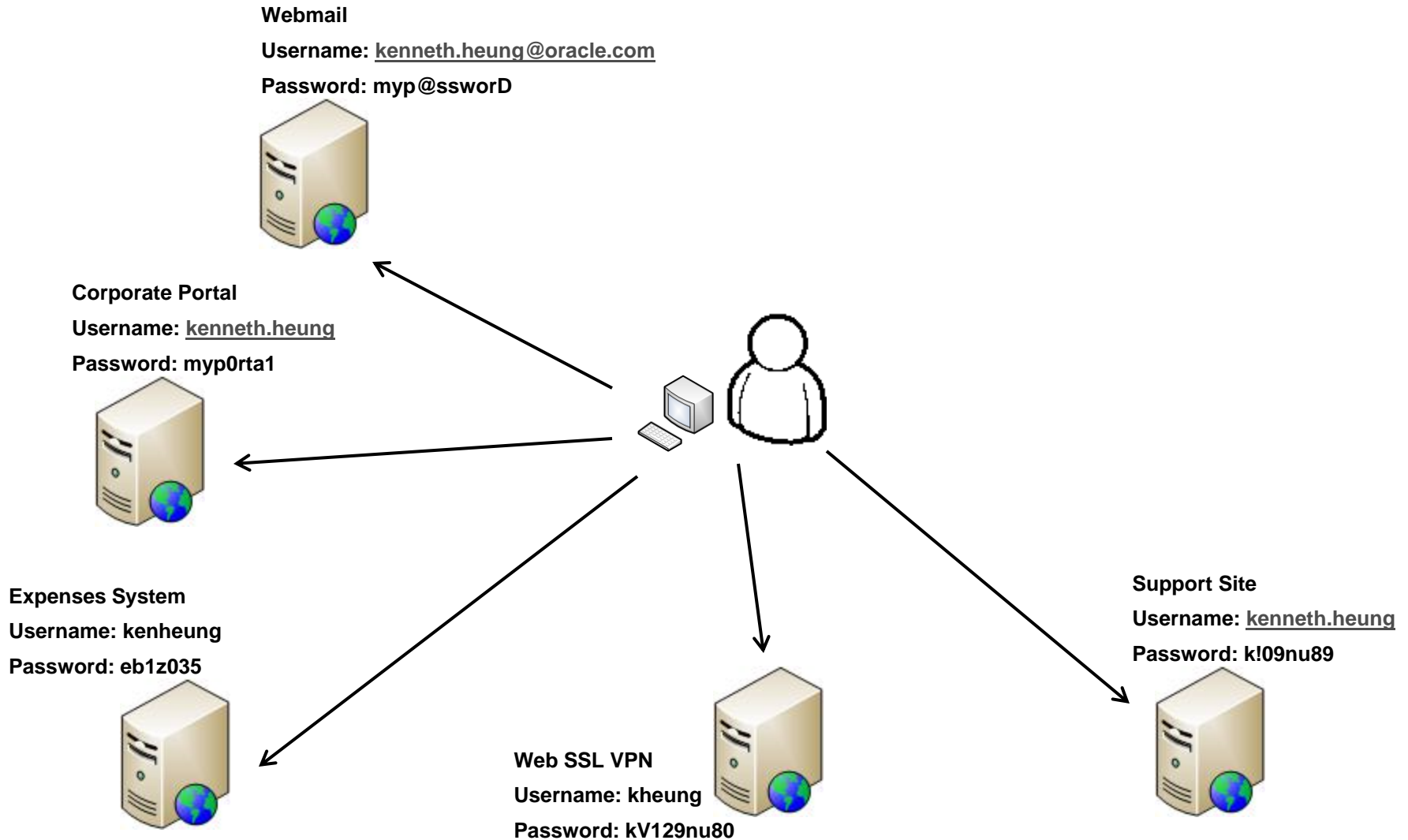


# Agenda

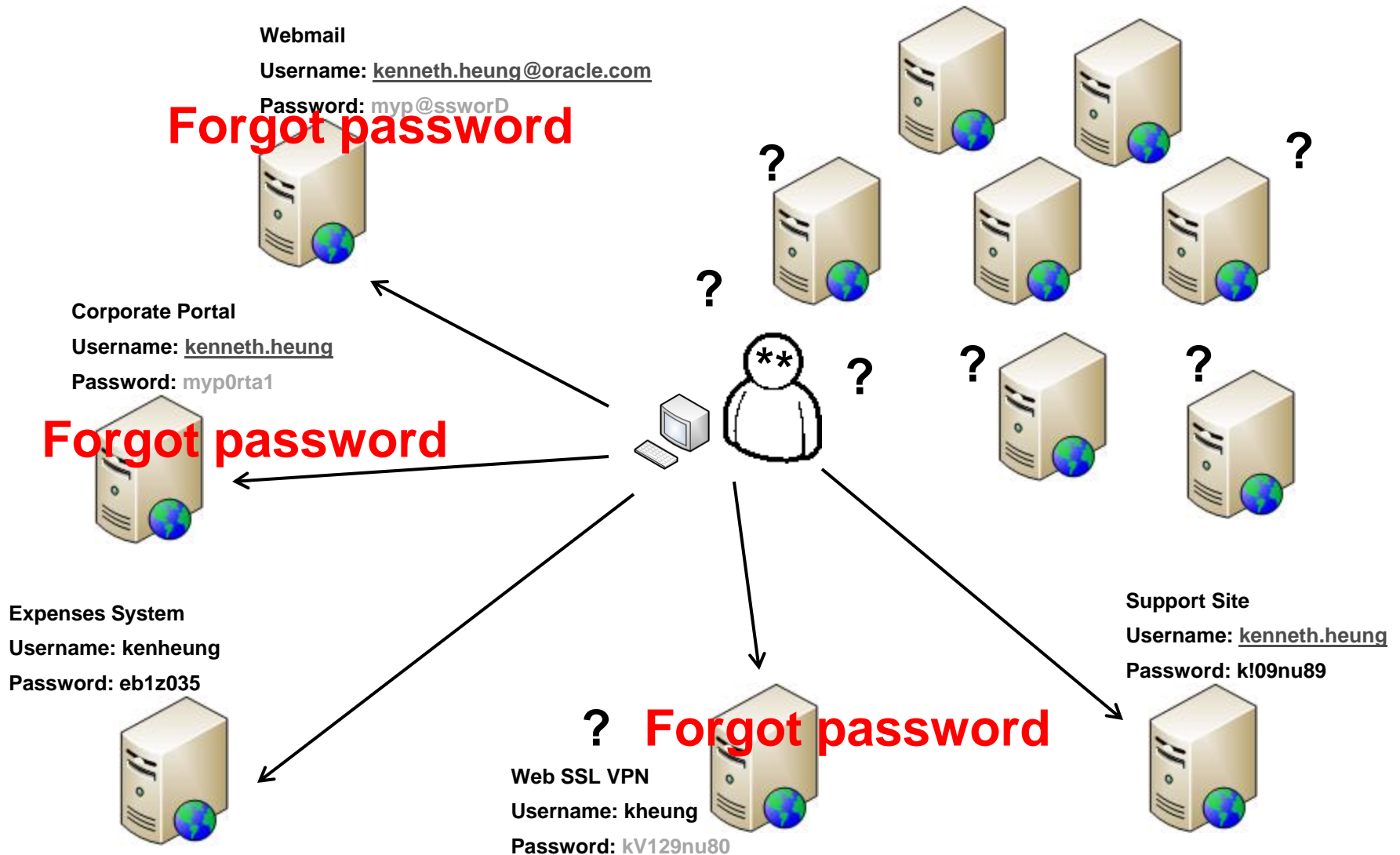
- **Web Access Management – A quick introduction**
- Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details
- Web SSO with OAM 11g – typical integration scenario example(s)
- Highlights in OAM 11g
- Extending Web SSO from enterprise environment to cross security domain – Identity Federation
- Demonstrations



# Web-based Single Sign-On (WSSO)



# Web-based Single Sign-On (WSSO)



# Web-based Single Sign-On (WSSO)

- For a large enterprise, as the number of passwords each user is required to maintain increases, so do the support calls. With each of these calls having an associated operational cost and the increasing number of applications in use, businesses cannot afford the productivity lost through continuous password resets.
- Single sign-on has evolved as a cost savings solution to minimize support calls, and at the same time simplify the administrative process of authentication and authorization.
- **User Experience + Cost Saving (support) + Increase Productivity**



# Web-based Single Sign-On (WSSO)

- Web SSO concept is simple – login once, access to different applications (web)

# Web-based Single Sign-On (WSSO)

- Web SSO concept is simple – login once, access to different applications (web)
- Single username/password

## Web Access Management (WAM)

- **Centralized** Access Management for Web Applications to provide **Authentication, Authorization, Audit.**

# Web-based Single Sign-On (WSSO)

- Web SSO concept is simple – login once, access to different applications (web)
- Single username/password

## Web Access Management (WAM)

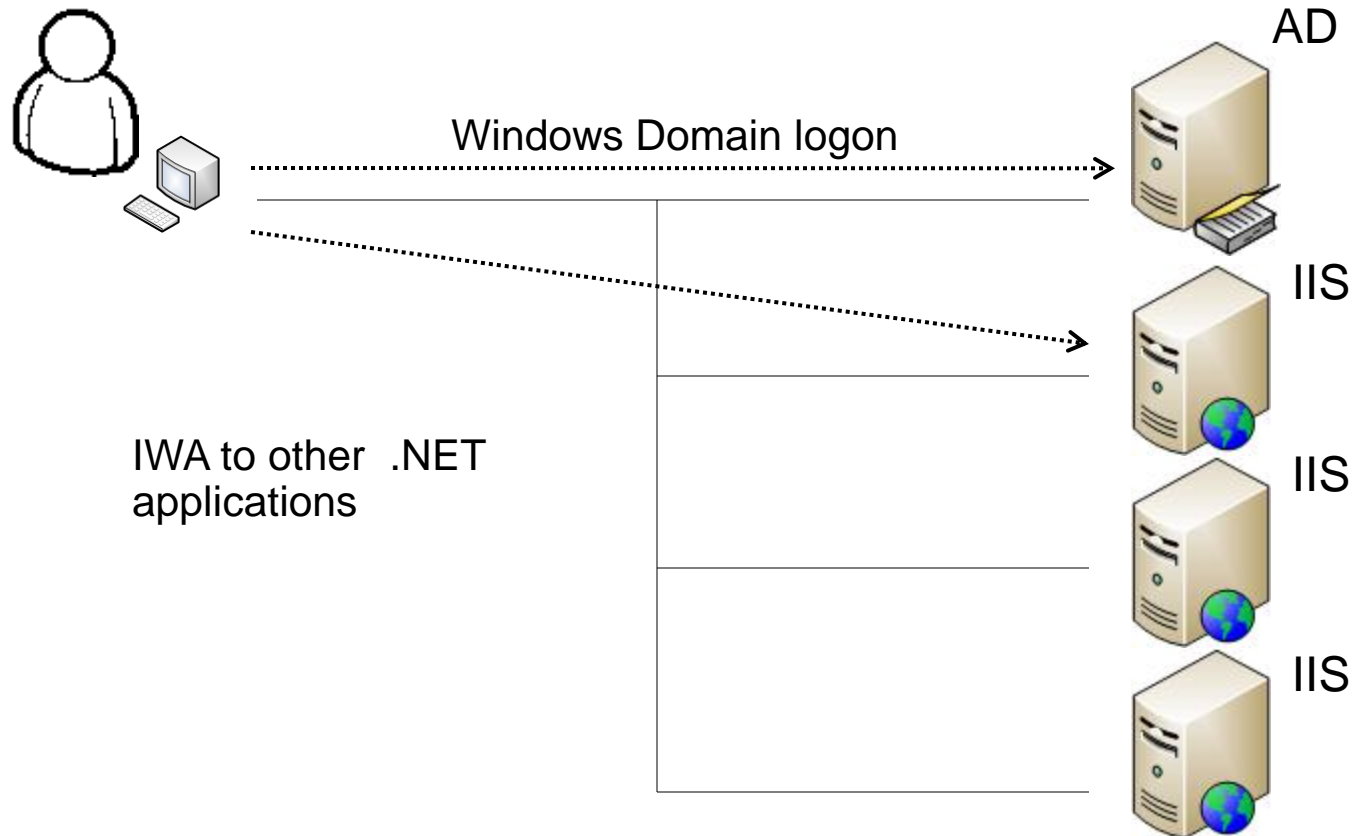
- **Centralized** Access Management for Web Applications to provide **Authentication (SSO)**, **Authorization**, **Audit**.

# Web Access Management - benefits

- **Centralized** Access Management for Web Applications to provide **Authentication (SSO), Authorization, Audit.**
  - Centralized management – improve security
  - Standardize AAA
    - improve security
    - easier to maintain
    - reduce audit & compliance cost
  - Decouple & Externalize AAA
    - application developers focus on business requirements & functionality
    - shorten development time, shorten time-to-market
    - easier to integrate with MFA
  - SSO – *improve user experience*
  - SSO – *reduce cost (helpdesk/support), increase productivity*

# Web SSO Approach - example

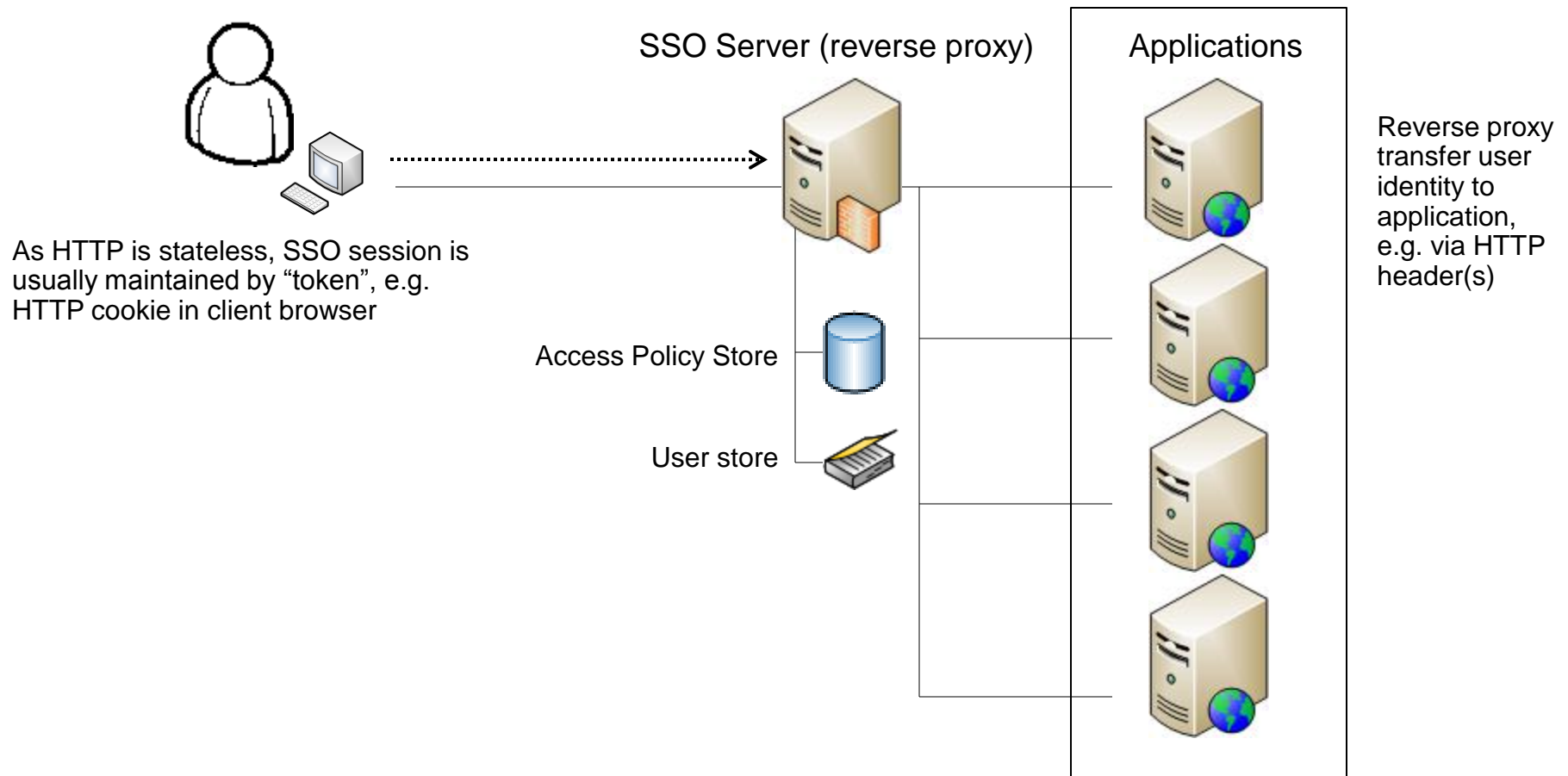
- Integrated Windows Authentication (IWA) – pure IIS environment



*\* This is not a WAM example, e.g. no centralized authorization*

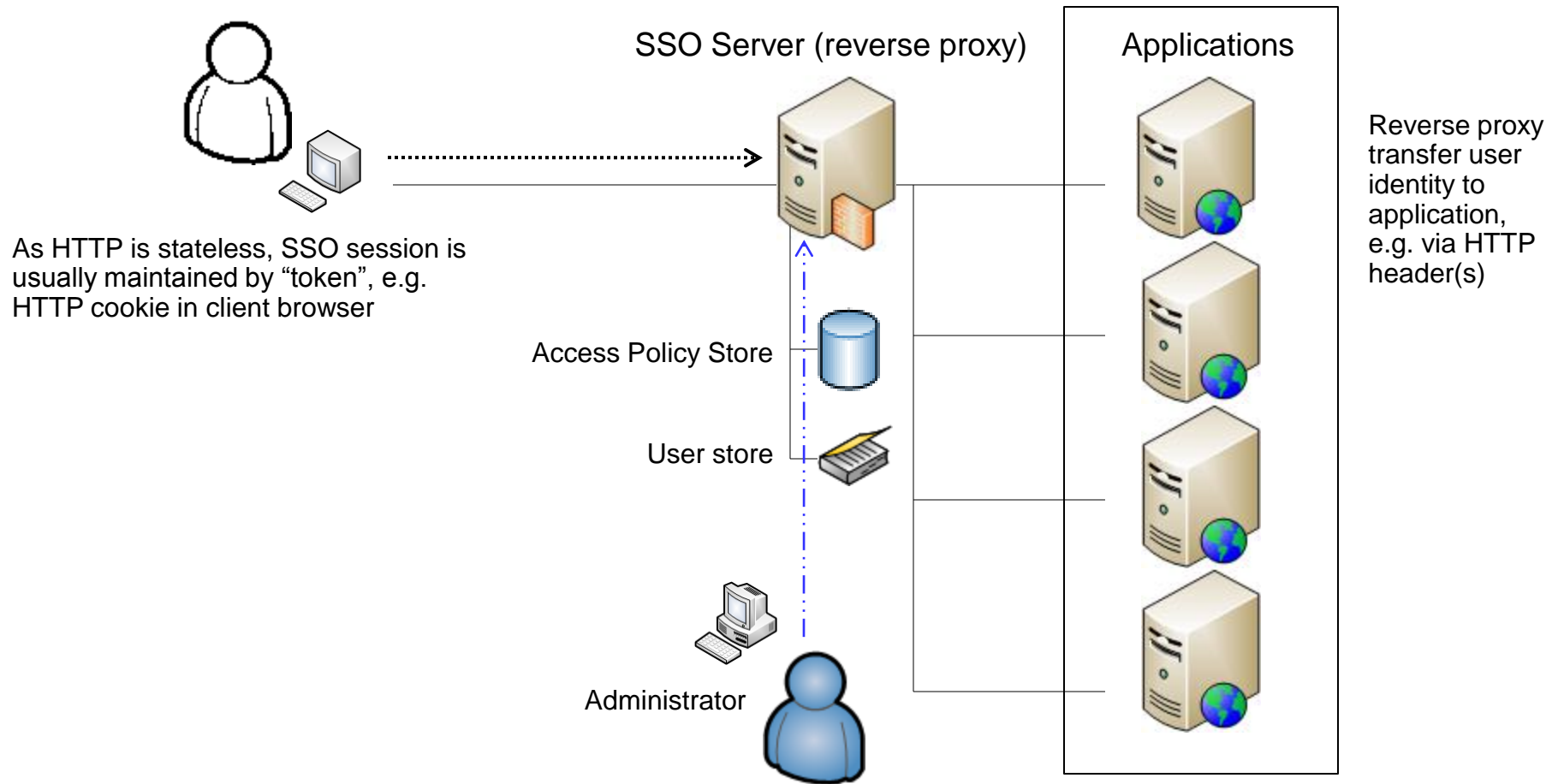
# Web SSO / WAM Architecture 1/2

- Reverse proxy based (agent-less)



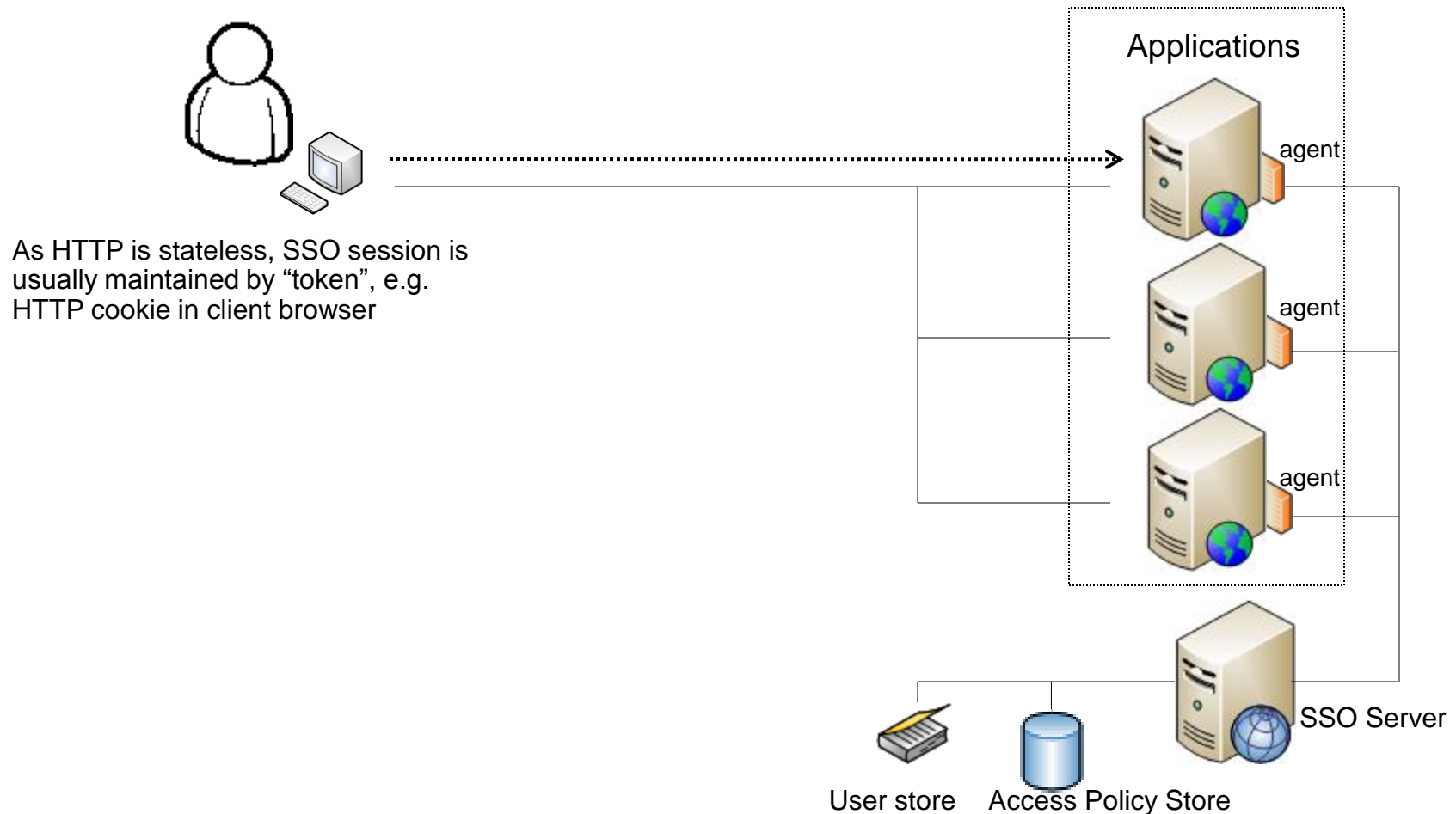
# Web SSO / WAM Architecture 1/2

- Reverse proxy based (agent-less)



# Web SSO / WAM Architecture 2/2

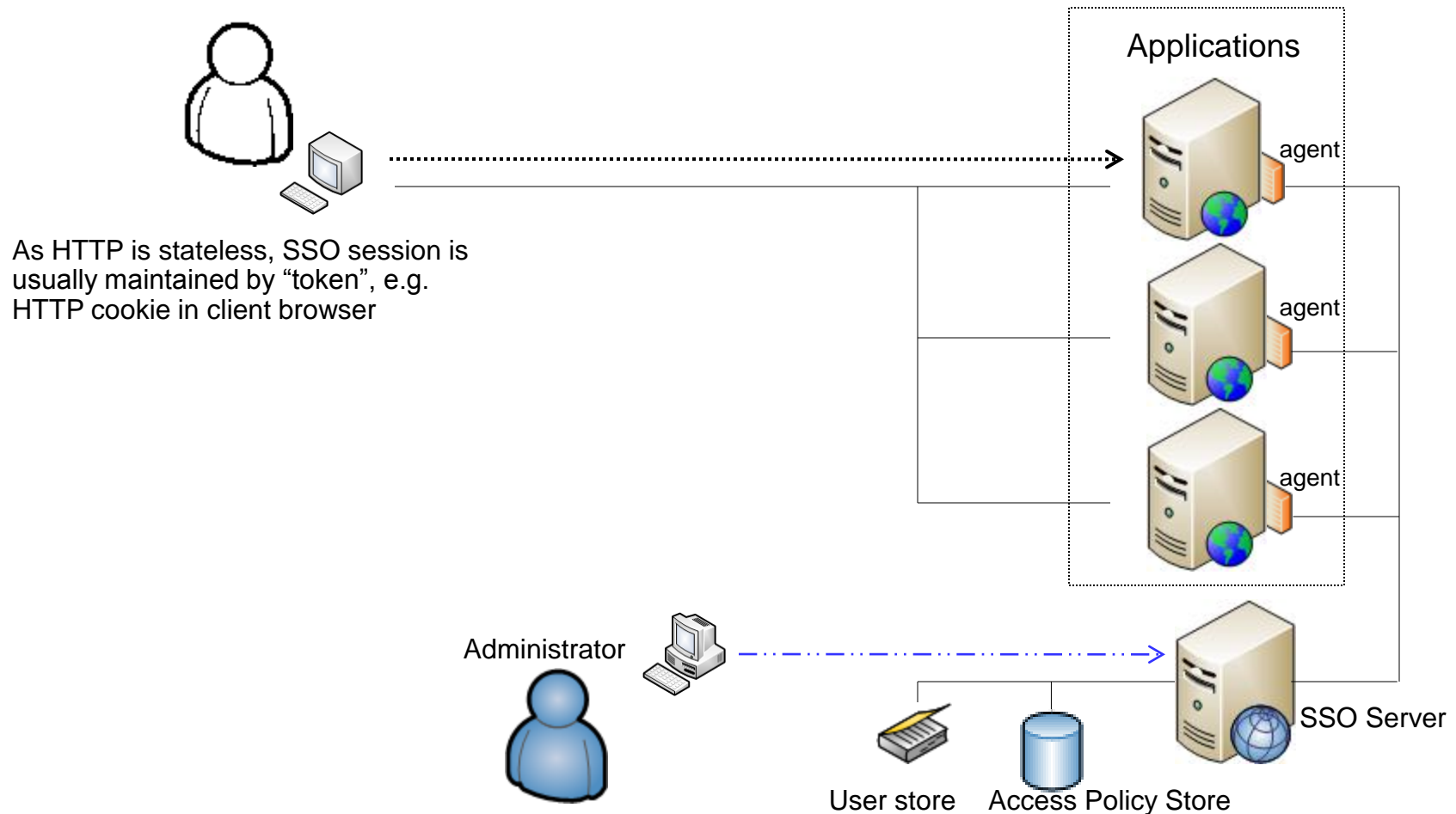
- Agent-based





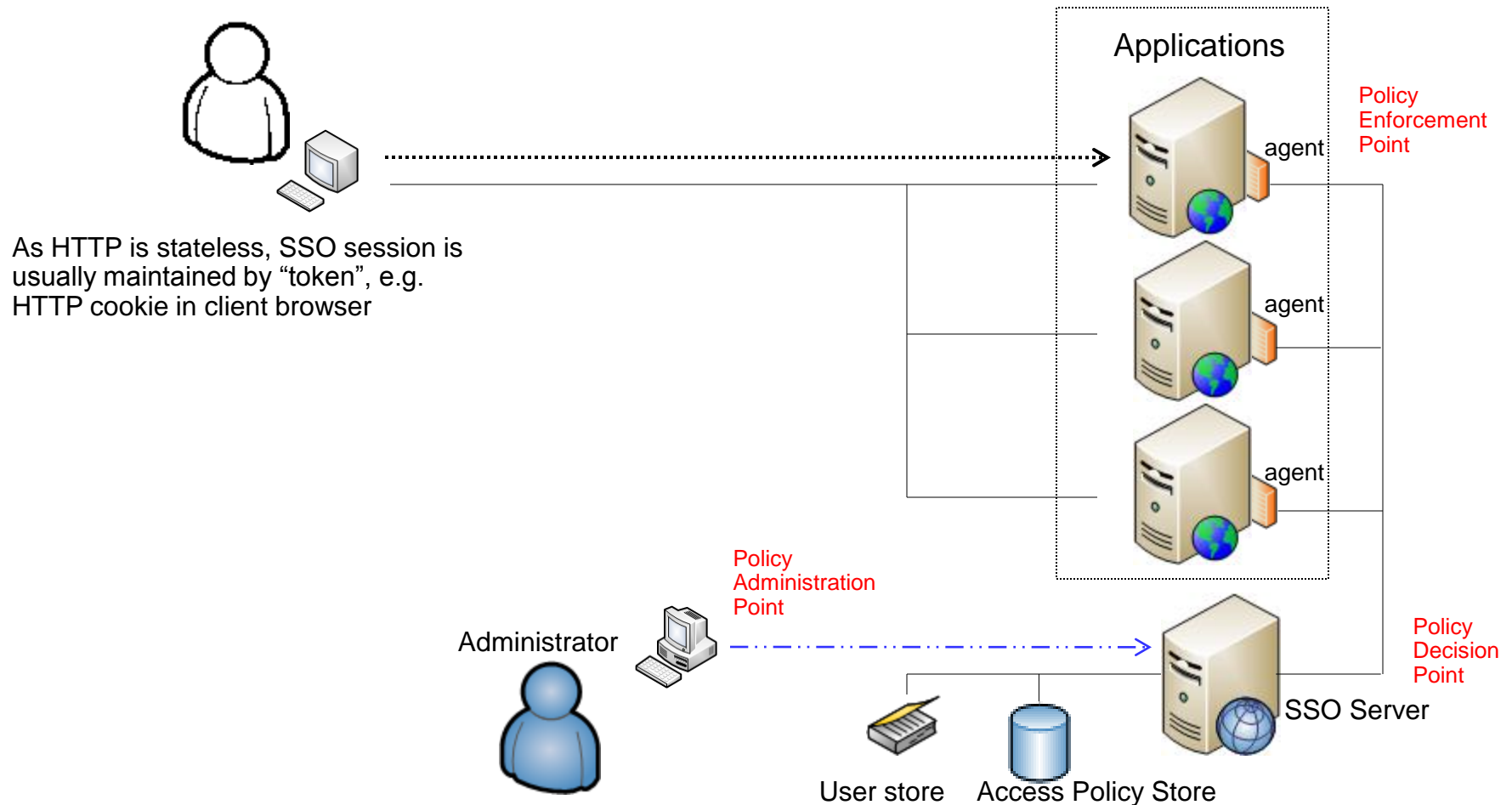
# Web SSO / WAM Architecture 2/2

- Agent-based



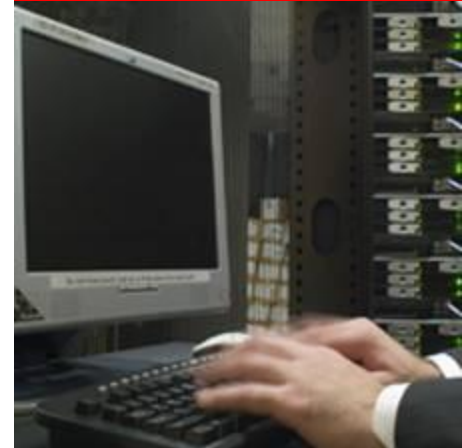
# Web SSO / WAM Architecture 2/2

- Agent-based



# Agenda

- Web Access Management – A quick introduction
- **Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details**
- Web SSO with OAM 11g – typical integration scenario example(s)
- Highlights in OAM 11g
- Extending Web SSO from enterprise environment to cross security domain – Identity Federation
- Demonstrations



# Oracle's Identity Management Suite

## Information Rights Management (IRM)

### Identity Admin.

**Identity Manager**

### Access Management

#### Access Manager

**Adaptive Access Manager**

**Enterprise Single Sign-On**

**Identity Federation + Fedlet**

**Entitlements Server**

**Web Services Manager**

**OpenSSO STS**

### Directory Services

**Internet Directory**

**Virtual Directory**

**Directory Server EE**

### Identity & Access Governance

**Identity Analytics**

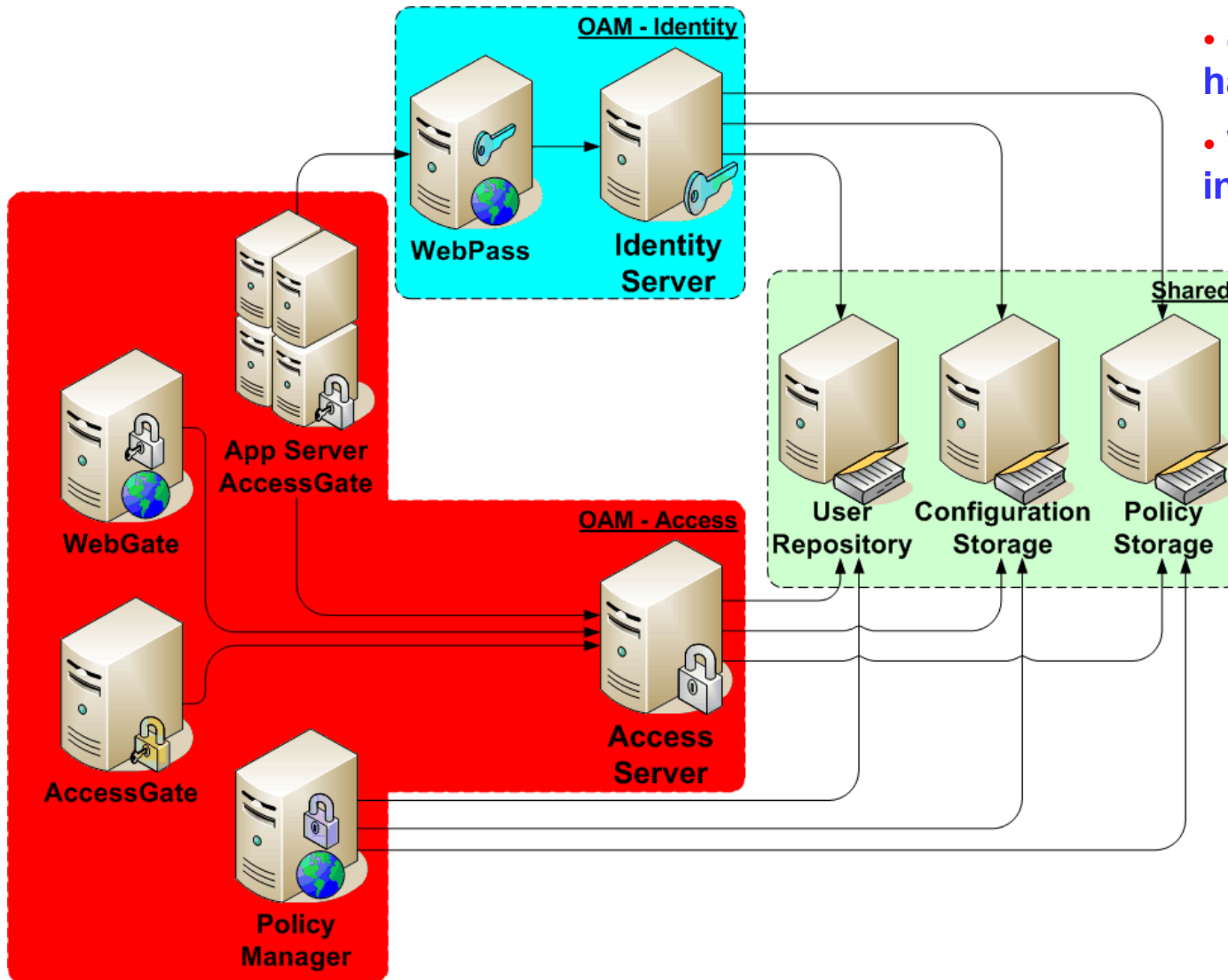
### Manageability

**Enterprise Manager IdM Pack**

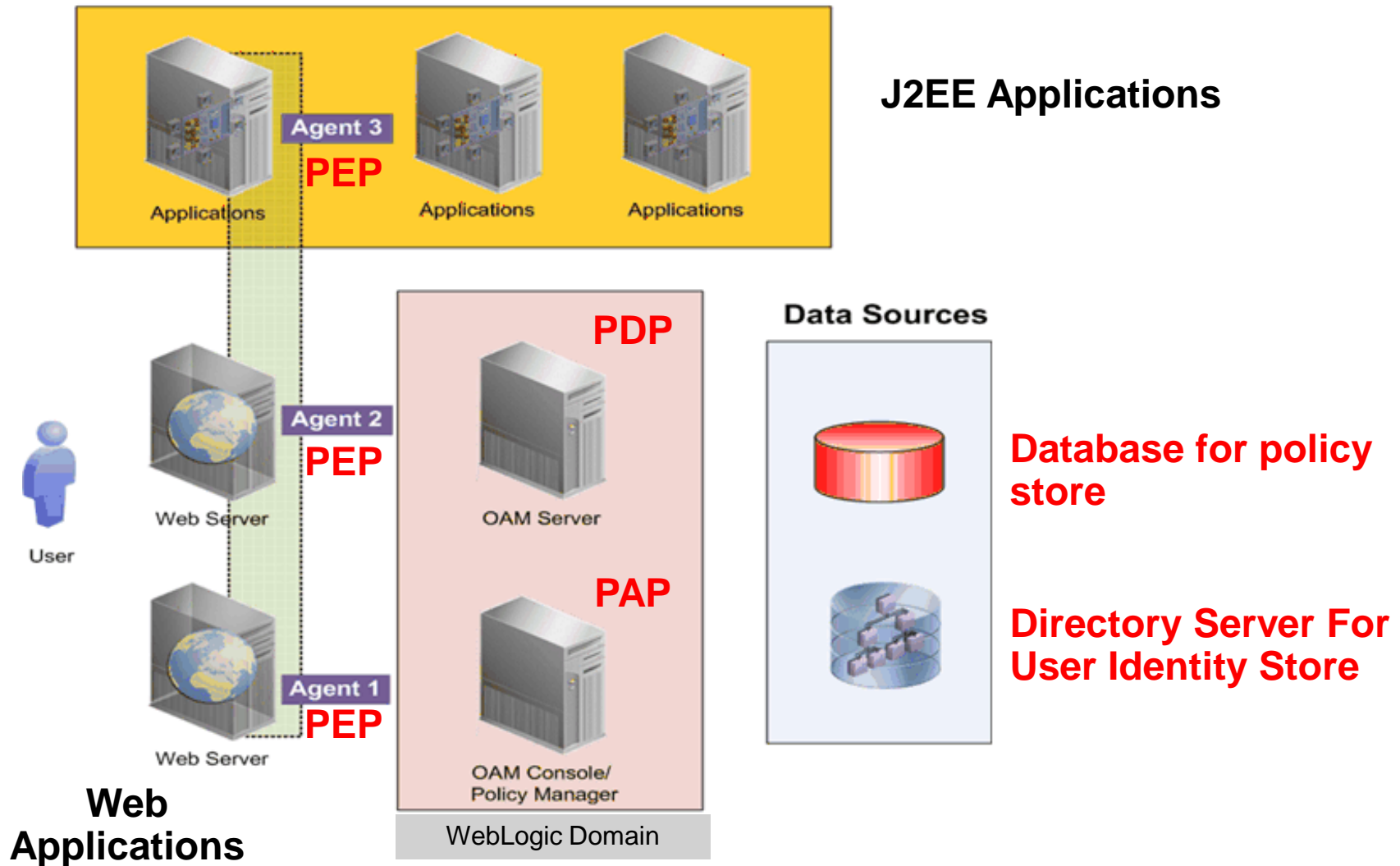
ORACLE

# OAM 10g: Architecture Overview

- Recap for those familiar with 10gR3
- don't worry if you haven't tried 10gR3
- We will focus on 11g in the next slide

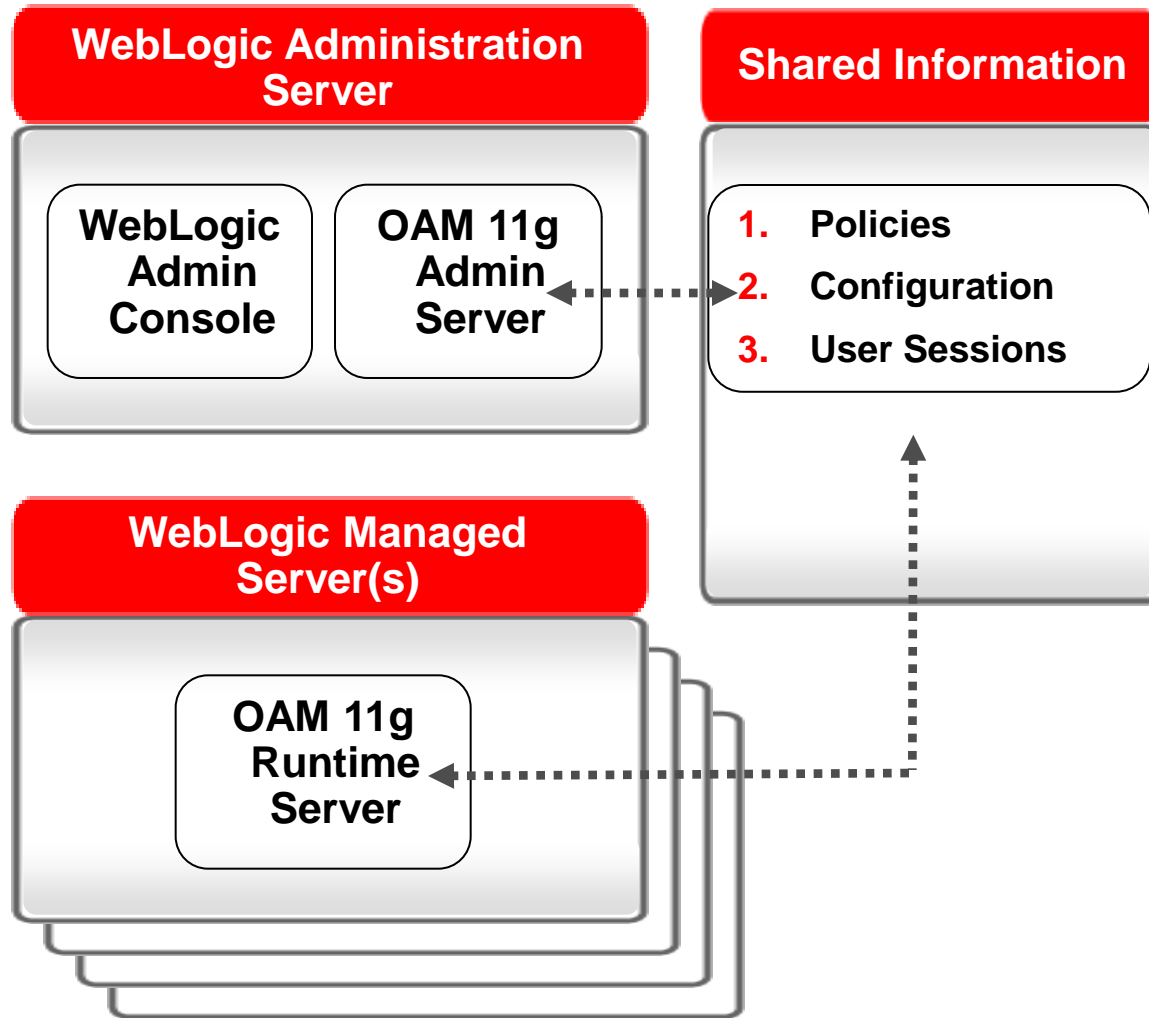


# OAM 11g Overview



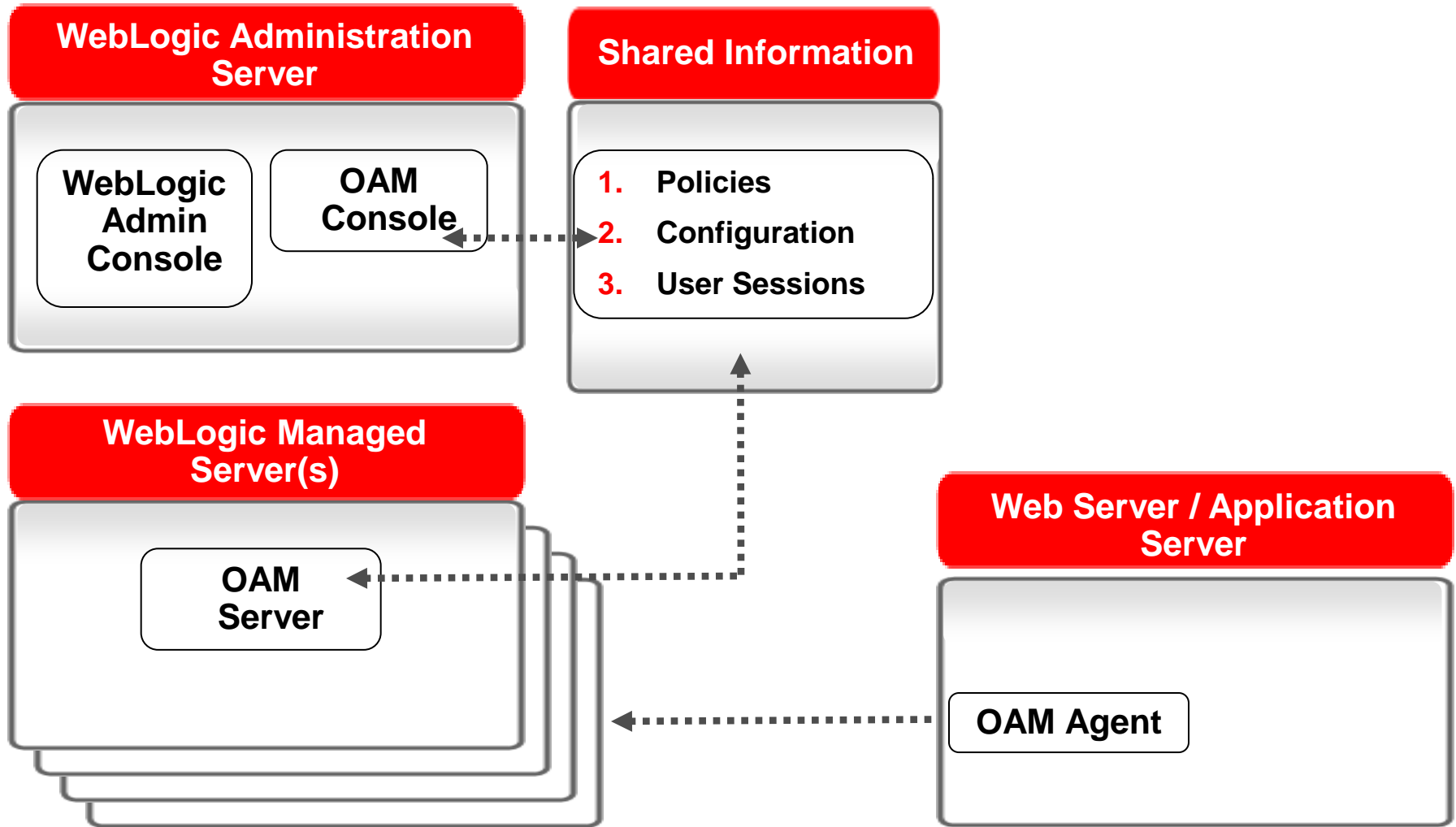
# Oracle Access Manager 11g

## Deployment Architecture



- Deploy in J2EE container – WebLogic Managed Server
- Isolated runtime and admin server
- Configuration and policy propagation
- User sessions shared across all runtime servers

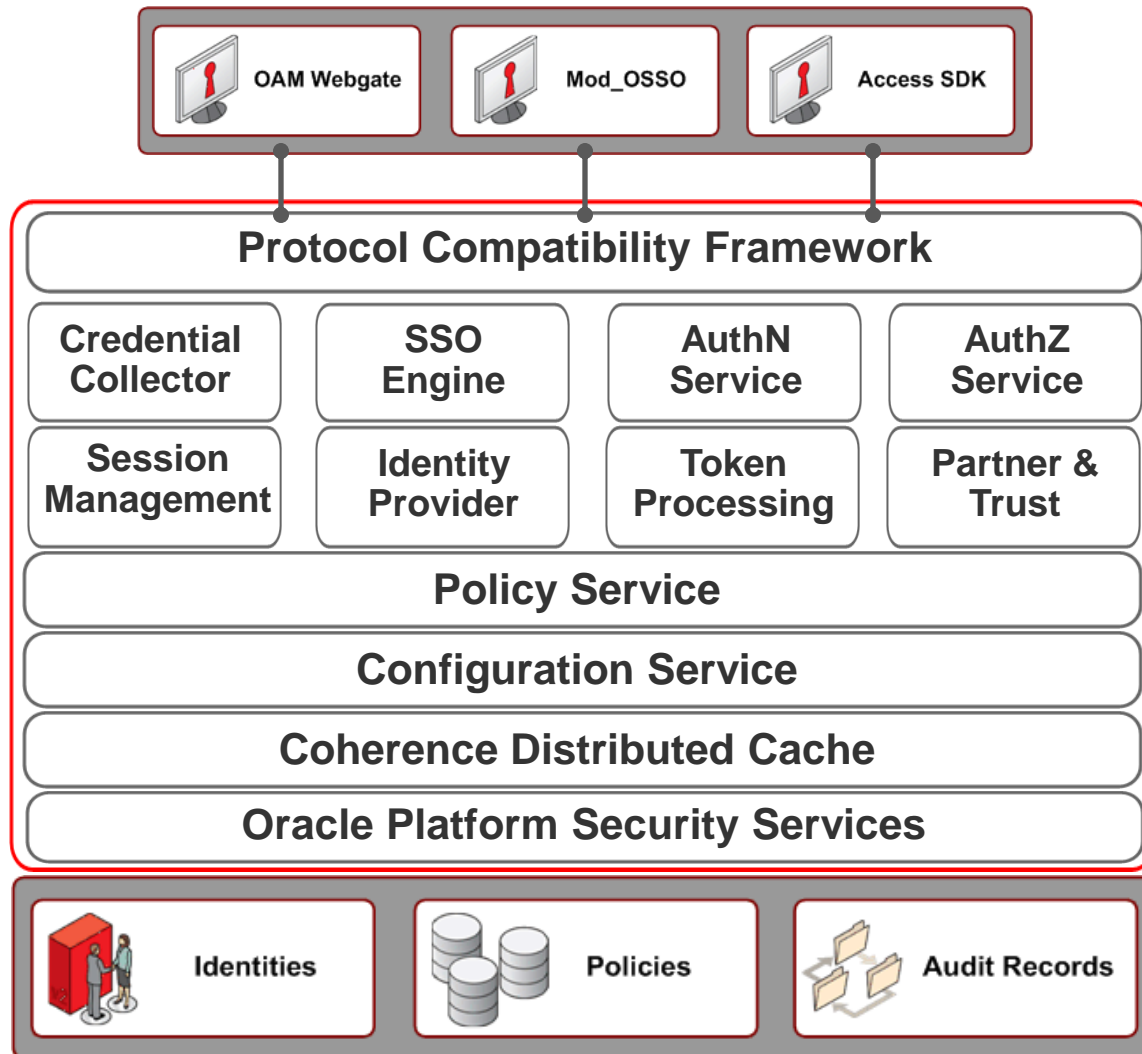
# Oracle Access Manager 11g





# Oracle Access Manager 11g

## Architecture – Runtime Server



# OAM11g Drilldown View

## OAM 11g Runtime Server (PDP)

- Access Control
  - Authentication (BASIC, FORM, WNA...)
  - Authorization (User/Group, IP/Time Constraints)
- Token Processing
- SSO & SLO
- Protocol Compatibility Layer(OSSO, OAM)
- Credential Collector
- NAP Endpoint
- Session Management
- Identity Provider

## Agents (PEP)

- OAM 10g, 11g, WLS Agents
- OSSO Agents
- ASDK

# OAM11g Drilldown View

OAM Console / Administration Console (PAP)

## Data Repositories

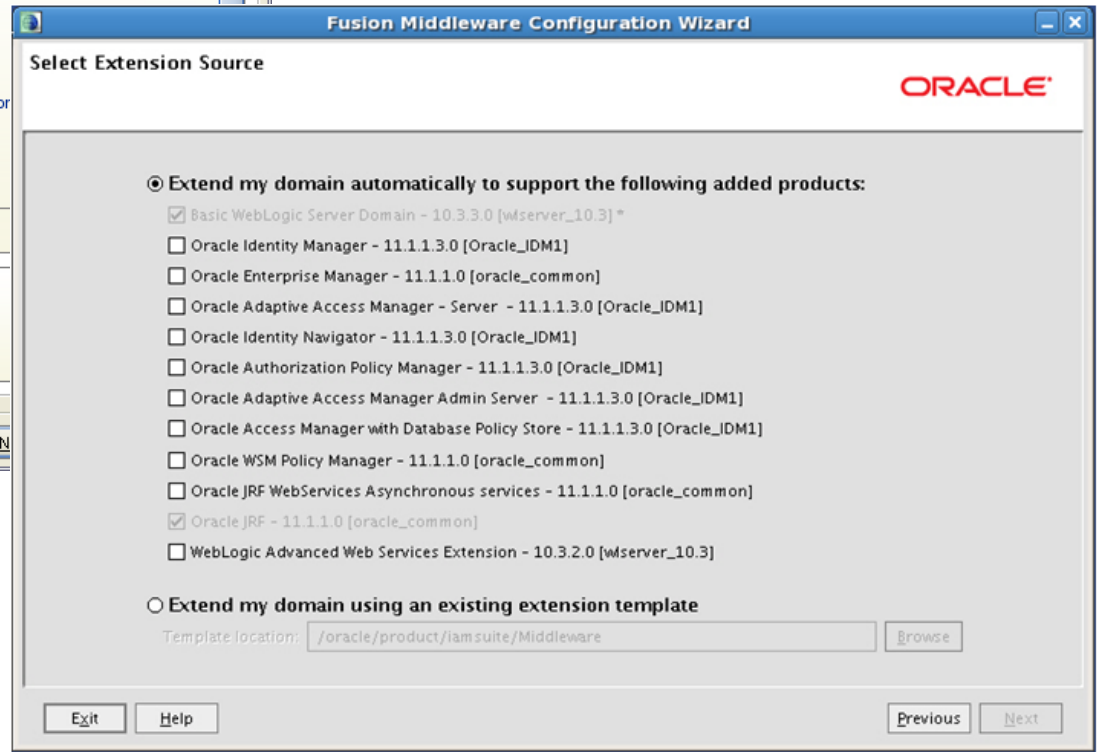
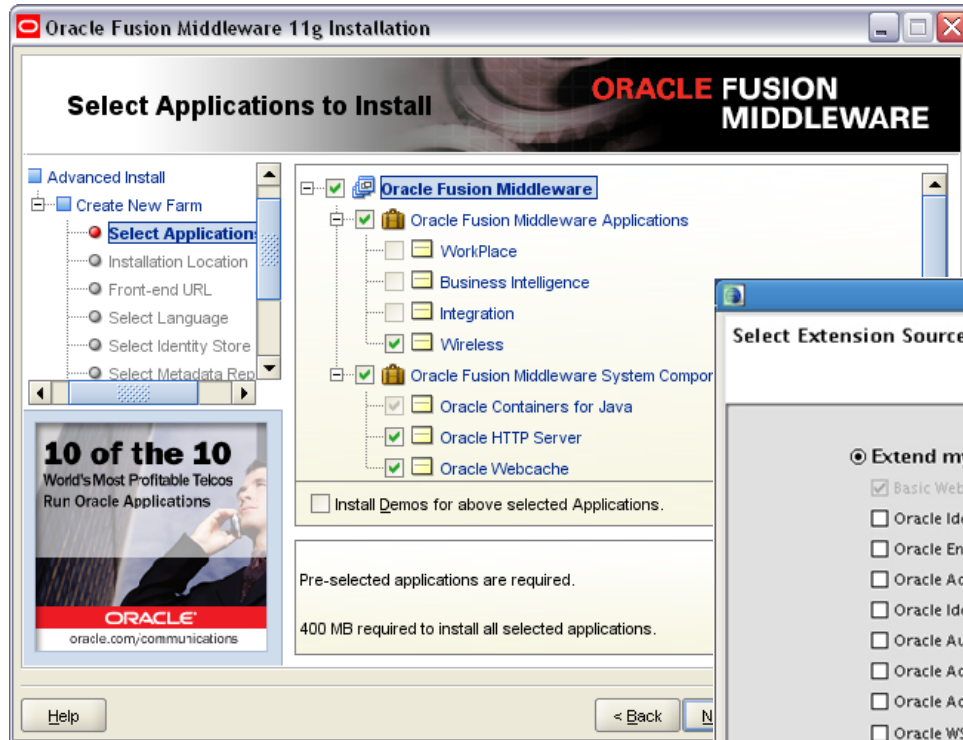
- Identity Store - OID, OVD, AD, DSEE ...
- Policy Store - Oracle DB
- Session Store - Coherence In-Memory, Oracle DB
- Config Store - File
- Key Store – CSF(Credential Store Framework), JKS (Java Key Store)
- Audit Store - File, Oracle DB

# Oracle Access Manager 11g

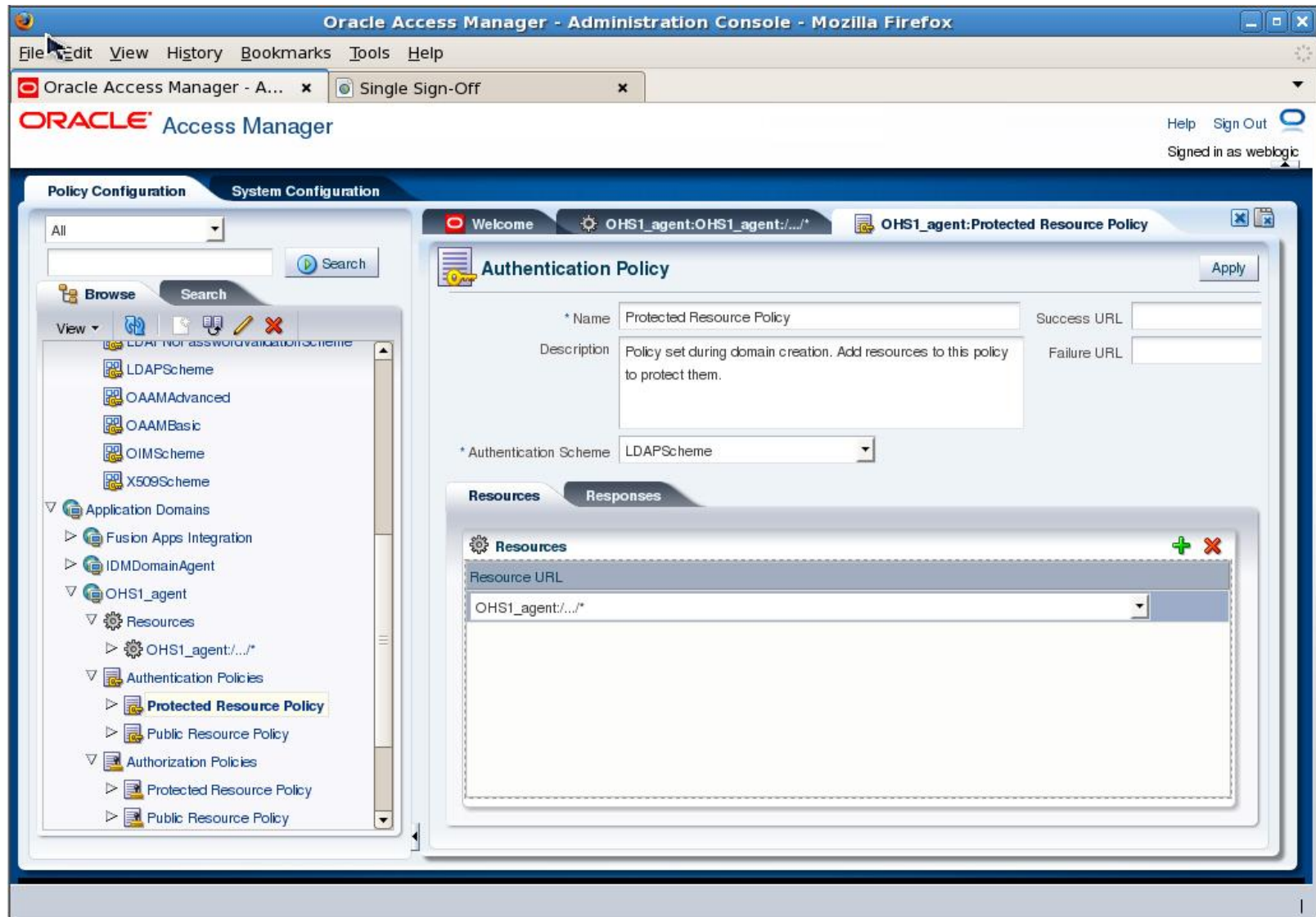
Key Features	Benefits
Modular Architecture	Separated admin and runtime server to enable independent operations
Secure Policy Model	Access is denied by default until policies are created to allow access
Simplified Install & Config	One package to install and one series of steps to configure a simple working environment
Session Management	Allows admin tracking and termination of user sessions
Diagnostics & Monitoring	Allows administrators to monitor key operational metrics in real-time
Central Agent Management	Administration console provides a holistic view of all agents and shows the server they are connected to
Backwards Compatibility	Compatible with 10g webgates and 10g mod_osso
Windows Native AuthN	Enables Windows desktop to web single sign-on
Improved Utilities	Remote registration utility, remote access tester, and WLST cmds for policy operations
Auditing and Logging	Allows administrative action auditing

# Installation & Configuration

Simplified and standardize OUI installation / WLS configuration



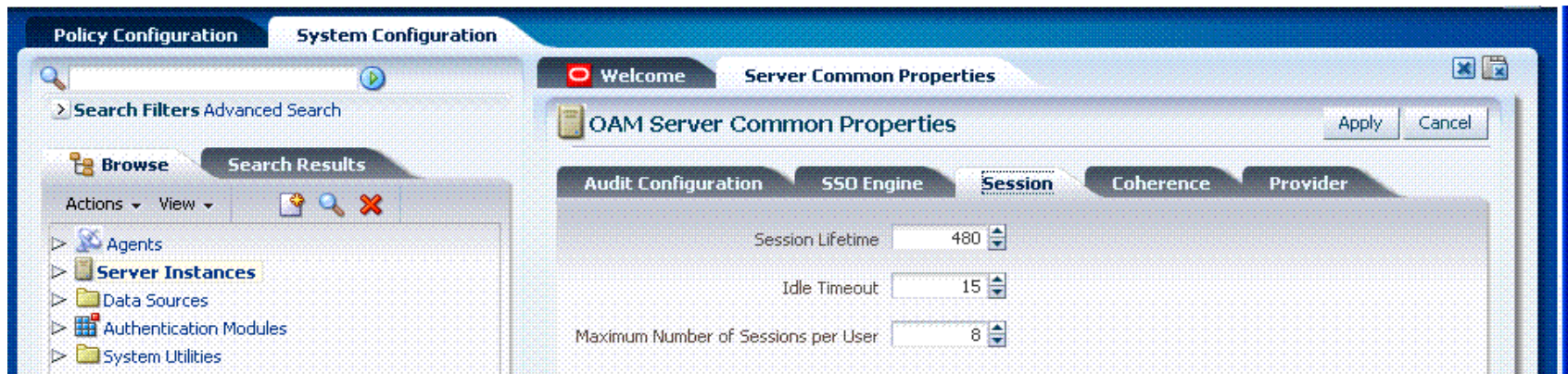
# Rich ADF-based UI



# Session Management

## Common Settings

- Global session lifetime across all protected applications
- Global idle timeout across all protected applications
- Maximum concurrent sessions per user



# Session Management

- Centralized, server side, stateful session management
  - Tracks session with a distributed cache system
  - Provides detailed security context information that can be further propagated
  - Can be done with or without persistent storage
  - Provides automatic session failover
- Advanced session management features
  - Policy-based limits to the number of concurrent sessions per user
  - Out-of-band session termination by administrators



# Operational Metrics Monitoring

The screenshot displays the Oracle Access Manager Administration Console in a Mozilla Firefox browser. The interface includes a top navigation bar with 'Policy Configuration' and 'System Configuration' tabs. The main content area is titled 'Monitor: oam\_server1' and shows server details: Name 'oam\_server1', Host 'lamlinux.oracle.vm', and Port '19001'. Below this, the 'Server Metrics' section is active, showing a 'Server Processes Overview' table. The table has columns for 'Authz Process', 'Authz Requests', 'Authn Process Failure', 'Authn Process Success', 'Pre Authn Process Failure', and 'Pre Authn Process Success'. The 'Max Active Threads' row shows values of 1, 4, 0, 9, 0, and 22 respectively. Other metrics include 'Active threads 0', 'Avg (msecs) 15.0', 'Completed (ops) 4', 'Max Time (msecs) 43', 'Min Time (msecs) 3', and 'Time (msecs) 60'. A 'Columns Hidden' button is at the bottom of the table.

Oracle Access Manager - Administration Console - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Oracle Access Manager - A... x Single Sign-Off x

ORACLE Access Manager

Help Sign Out Signed in as weblogic

Policy Configuration System Configuration

Welcome Monitor: oam\_server1

Monitor: oam\_server1 Refresh

Name oam\_server1 Port 19001

Host lamlinux.oracle.vm

Server Metrics

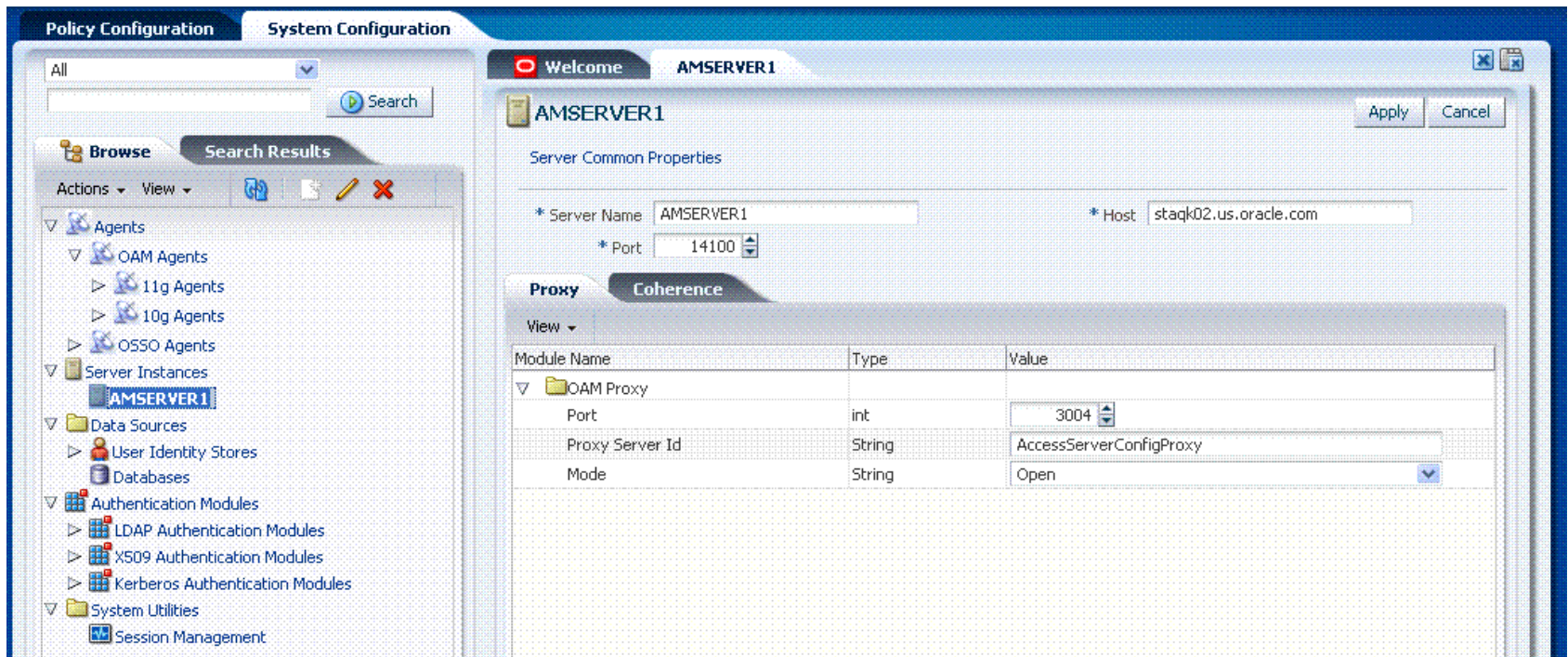
Server Processes Overview Session Operations Server Operations OAM Agents

View ▾ Detach

Authz Process	Authz Requests	Authn Process Failure	Authn Process Success	Pre Authn Process Failure	Pre Authn Process Success
Active threads 0					
Avg (msecs) 15.0					
Completed (ops) 4					
Max Active Threads 1	4	0	9	0	22
Max Time (msecs) 43					
Min Time (msecs) 3					
Time (msecs) 60					

Columns Hidden

# Centralized Agents Management: OSSO Agents, OAM 11g & 10g Agents



# Coexistence & Backwards Compatibility

- Server coexistence with Oracle SSO 10g and OAM 10g servers to ease migration
- Backwards compatible with Oracle SSO agents (mod\_osso)
- Backwards compatible with OAM 10g WebGates and Access SDK
- Provides single sign-on experience across both Oracle SSO and OAM agents.

# OOTB Supported Authentication Mechanisms

- Form based authentication
- Basic authentication
- X.509 authentication (Client SSL Cert with OOTB validation, e.g. OCSP)
- OAAM virtual pad based authentication
- Kerberos based authentication (windows native authentication – SSO with Domain Logon without IIS)
- Anonymous authentication

# Utilities

## Remote Registration Tool

- Remote registration is aimed at helping application administrators
- Application administrators can register agents without the help of the Security team
- Policy objects can be automatically created to protect resources of a given application at registration time
- Registration process can be further secured as a 2 step process requiring the Security team's review

# Utilities

## Access Tester

**Oracle Access Manager Connection Simulator**

File Help

**Connection**

\*Server IP: dadvmh0172 \*Server Port: 3004 Mode: OPEN Is Connected

\*Client ID: agent1 \*Client Password: ..... Configure ...

**URI**

Scheme: HTTP:// \*Host: dadvmh0172 Port: 6666 Is Protected

Resource: /index.htm Operation: GET

**Identity**

IP Address: \*Username: weblogic Password: ..... Is Authenticated

Certificate File: Browse... Is Authorized

**Status**

1. Connected : Yes

2. Is Protected : Yes  
Authentication scheme : LDAPScheme, level : 2  
Redirect URL : http://dadvmh0172.us.oracle.com:7499/ngam/server/  
Credentials expected: 0x2 (x509 cert)

3. Is Authenticated : Yes  
User DN : cn=weblogic,dc=us,dc=oracle,dc=com  
Session ID : 2

4. Is Authorized : Yes

Elapsed: 76 ms

# Audit & Logging

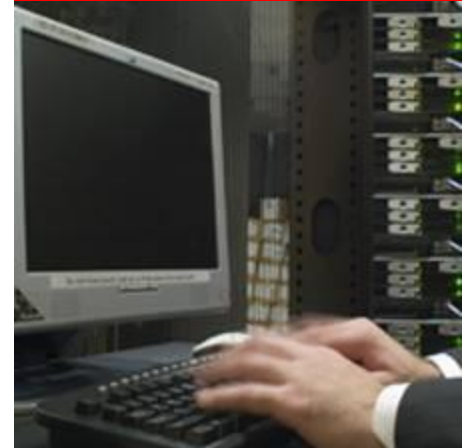
## Features

- Logging
  - Centralized log management
  - Graphical tools for configuring and viewing logs
  - Multiple logging levels
- Auditing
  - Standardized auditing across FMW components
  - Reports generated via Oracle BI Publisher
- Unified logging across products
  - Accessed via EM or OS
  - Standardized log levels
  - ECID – provides an identifier that can be used to track requests across FMW products (e.g. WLS to OID to DB)



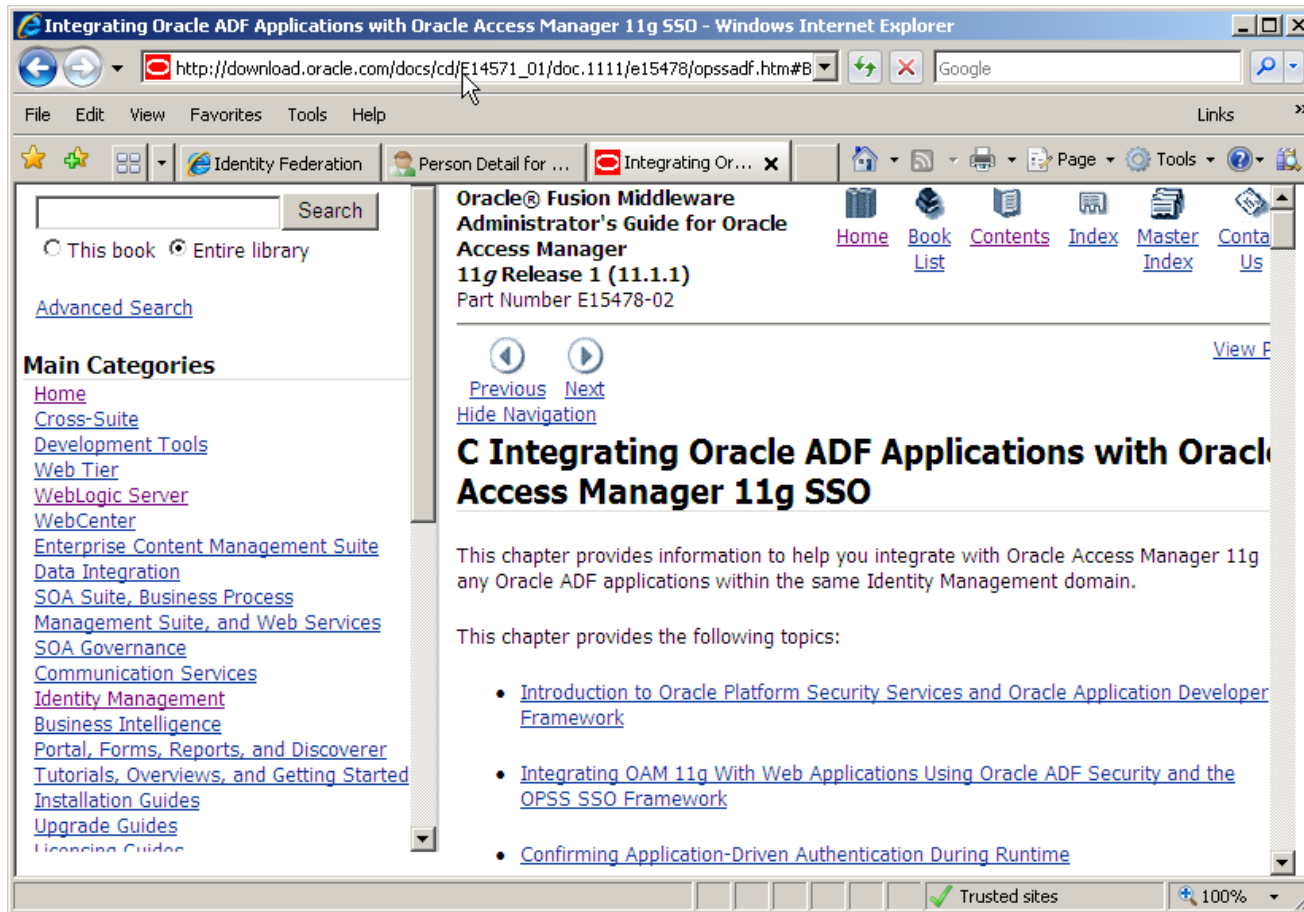
# Agenda

- Web Access Management – A quick introduction
- Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details
- **Web SSO with OAM 11g – typical integration scenario example(s)**
- Highlights in OAM 11g
- Extending Web SSO from enterprise environment to cross security domain – Identity Federation
- Demonstrations



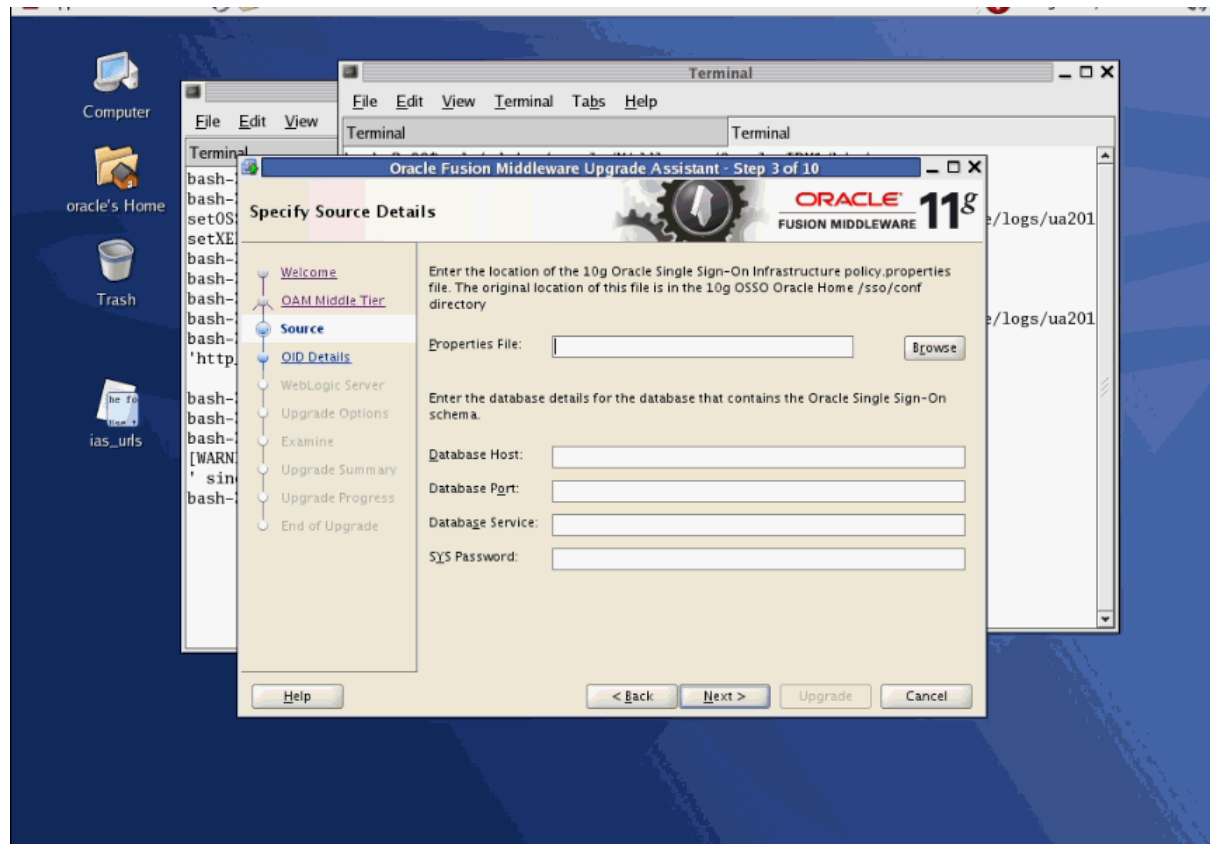


# SSO with OAM – Oracle Fusion Middleware - ADF Applications



# SSO with OAM – OSSO – Upgrade Assistant

- Oracle E-Business Suite
- Oracle Portal
- Oracle Application Server (iAS)
- Oracle Forms



# SSO with OAM – compatible with OAM 10g WebGates

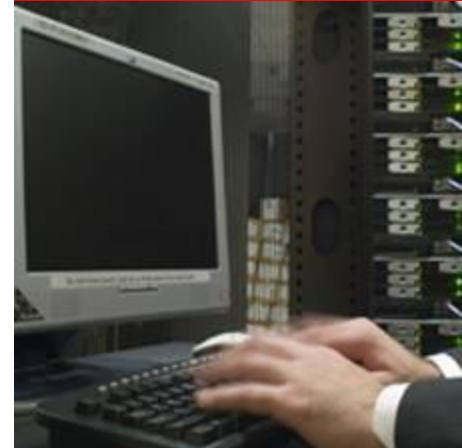
- Oracle HTTP Server, Apache HTTP Server, Microsoft IIS, IBM HTTP Server, Lotus Domino, Sun Java Web Server, Oracle WebLogic, IBM WebSphere and more.....
- OOTB support for some COTS applications, e.g. Outlook Web Access, SharePoint Server / SharePoint Services, Lotus Notes Web Access, etc
- ASDK for custom integration

# SSO with OAM – integration approaches

- Install Agent (WebGate) in the front-end web proxy, pass credential as HTTP headers (if applicable)
- Install Agent (e.g. WebLogic SSPI, WebSphere Connector) in Application Server
- Install Agent in the Web Server hosting the application, modify the application
  - e.g. remove original authentication / authorization code
  - e.g. typical JSP, PHP, etc application use include file to check session variable & redirect user to login page if login session is not exists
- *Might requires modification of existing application*

# Agenda

- Web Access Management – A quick introduction
- Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details
- Web SSO with OAM 11g – typical integration scenario example(s)
- **Highlights in OAM 11g**
- Extending Web SSO from enterprise environment to cross security domain – Identity Federation
- Demonstrations

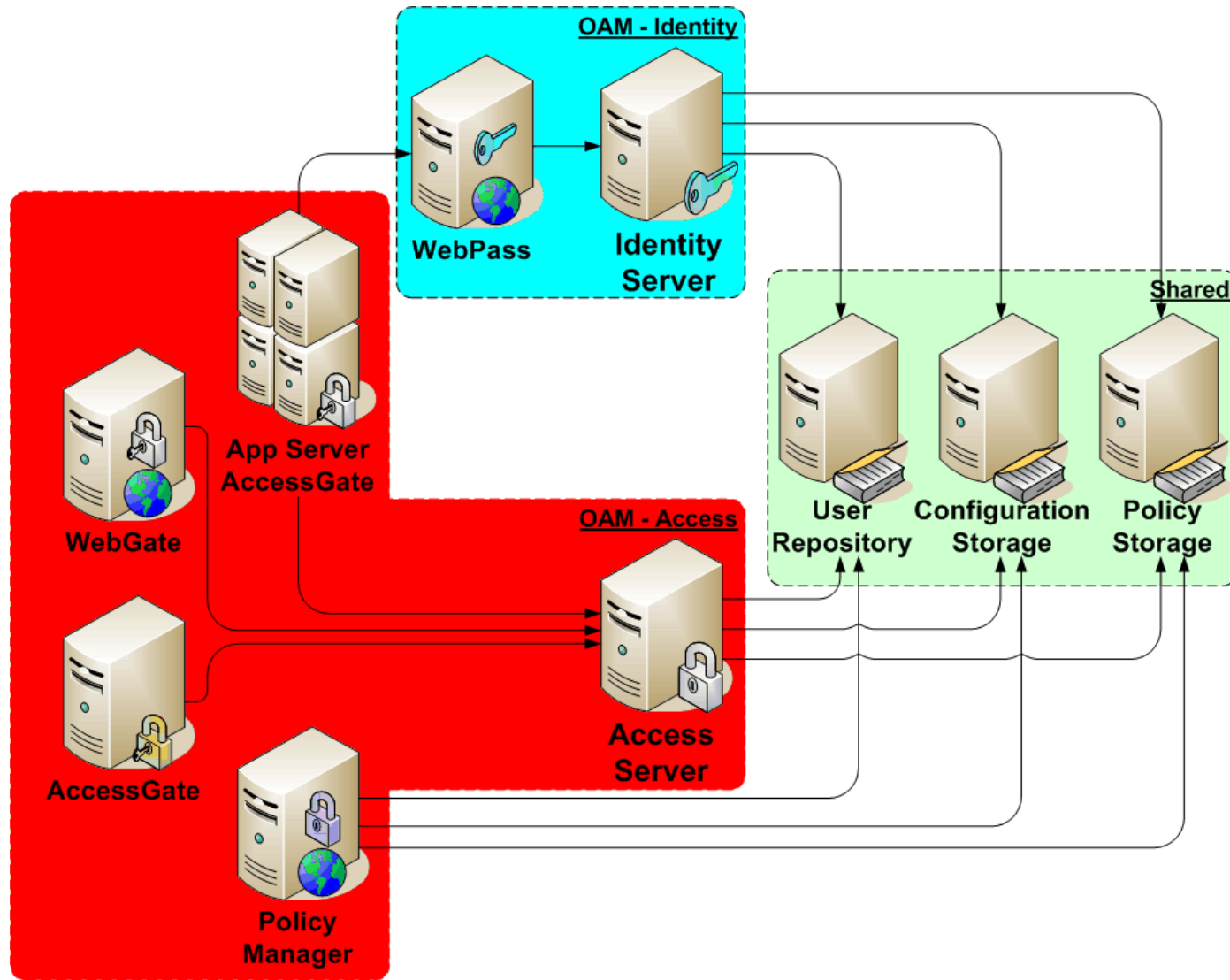


# Oracle Access Manager 11g

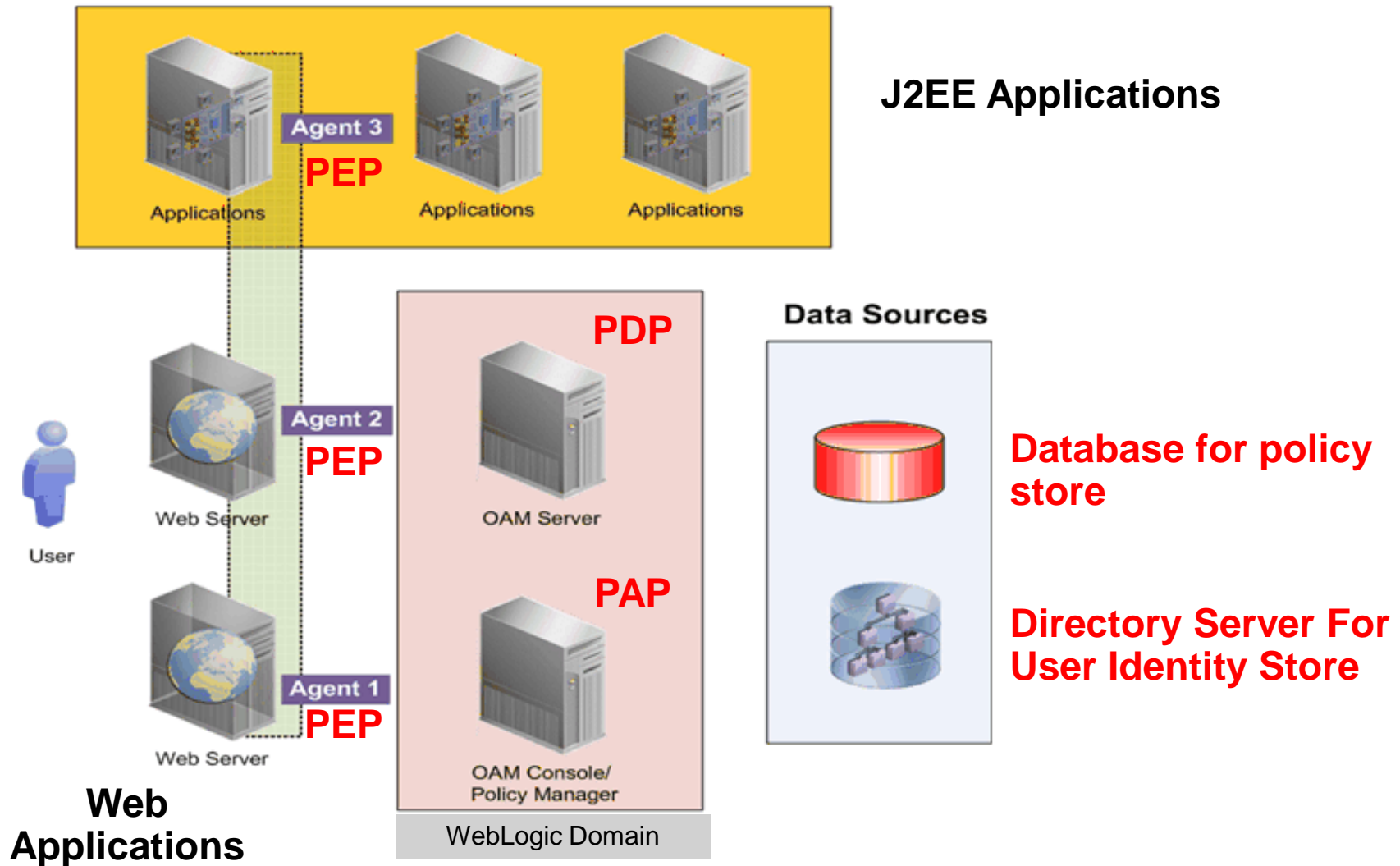
## Key Comparison with OAM 10g

Feature	OAM 10g	OAM 11g
Deployment	Stand alone server	Deployed in container
Authentication to LDAP	LDAP defined system-wide	LDAP defined in authentication scheme
Available agents	WebGates, AccessGate	mod_osso and WebGates
Session management	Stateless sessions in a cookie	Stateful sessions at a centralized server
Application integration	OAM configuration tool	UI or command line remote registration tool
Identity administration	OAM Identity Server	Identity agnostic (OIM 11g by default)
Policy model	Open (default allow)	Closed (default deny)
Policy store	LDAP	RDBMS
Configuration store	LDAP	File based

# OAM 10g: Architecture Overview



# OAM 11g Overview



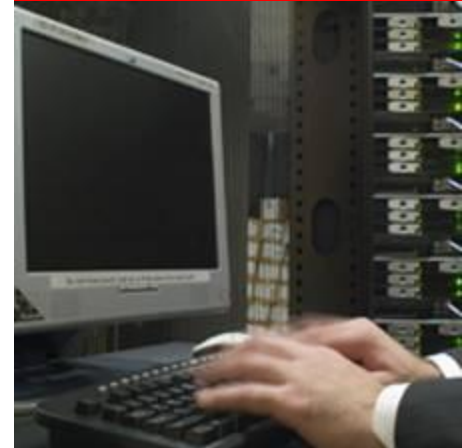


# Oracle Access Manager 11g

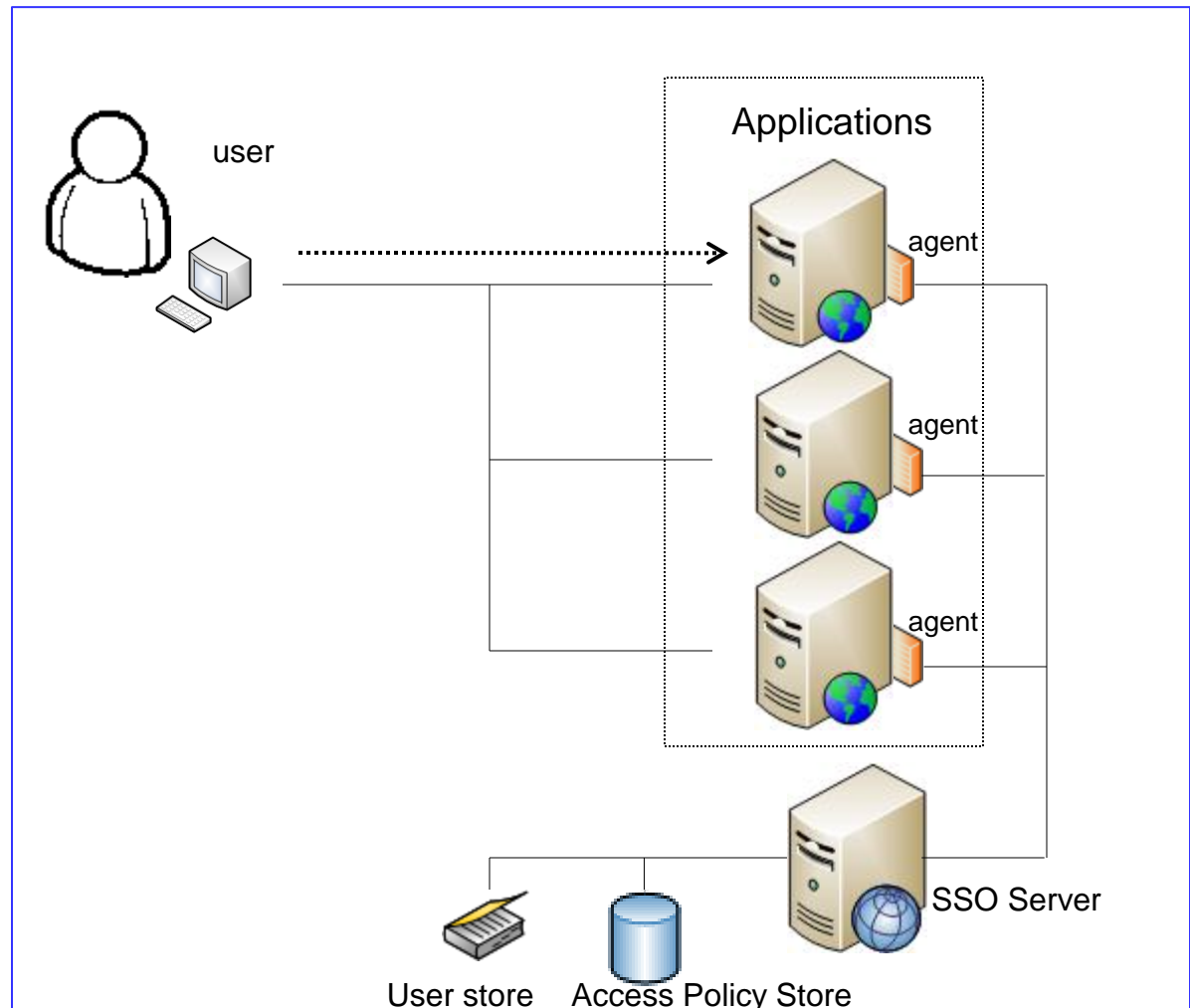
- Objective
  - Replace OSSO and converge OAM and OSSO
  - Provide foundation for Access Management Suite
  - Provide foundation for OpenSSO convergence
  - Manage all agents and policies centrally
  - Provide new and advanced functionality to customers
- 11gR1 Primary Audience
  - Existing OSSO 10.1.4.3.0 customers
  - Brand new OFM or IDM customers
- 11gR1 Secondary Audience
  - Existing OAM 10.1.4.3.0 customers
  - Existing OpenSSO customers

# Agenda

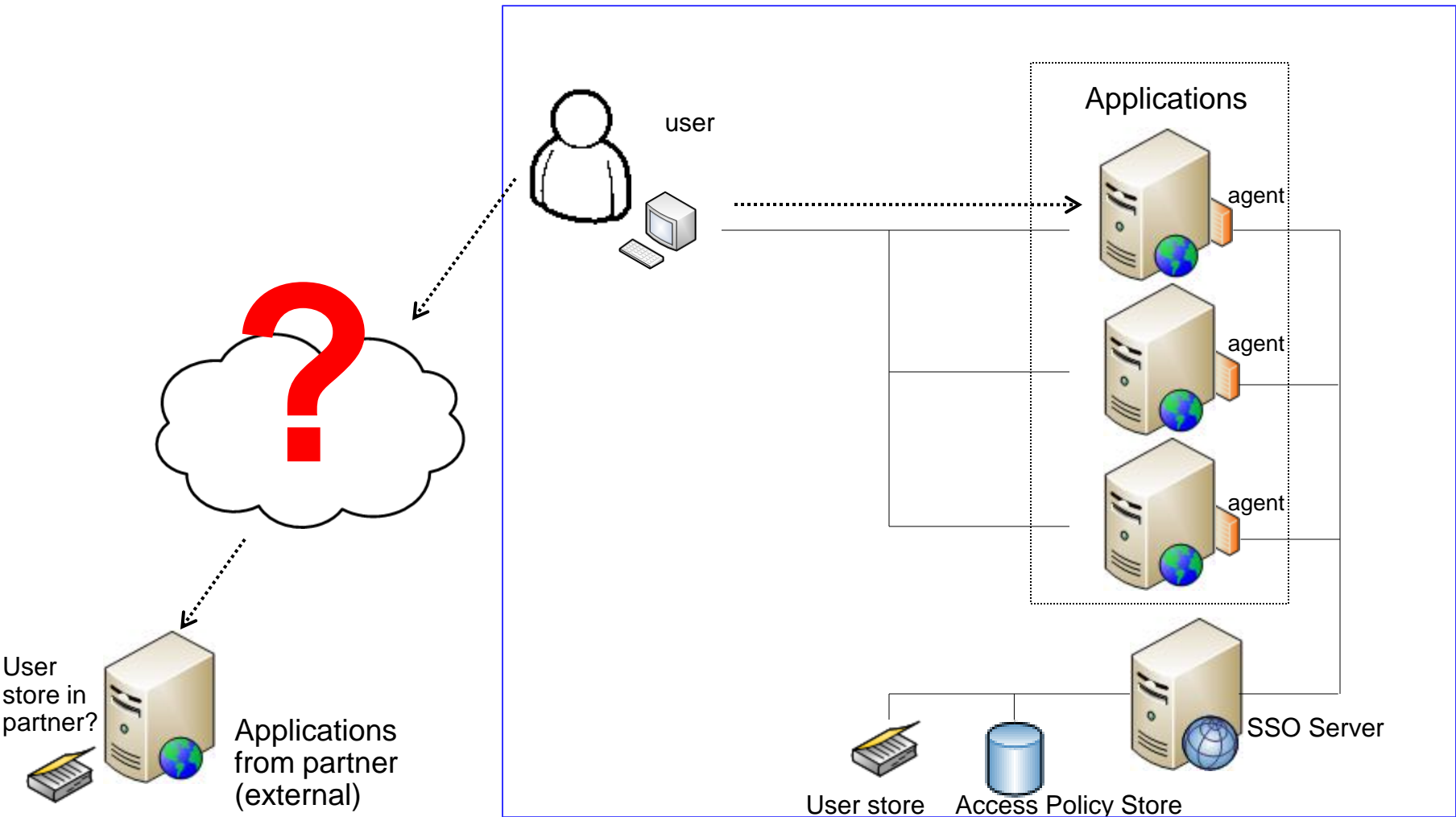
- Web Access Management – A quick introduction
- Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details
- Web SSO with OAM 11g – typical integration scenario example(s)
- Highlights in OAM 11g
- **Extending Web SSO from enterprise environment to cross security domain – Identity Federation**
- Demonstrations



# What if application is NOT in the same security domain



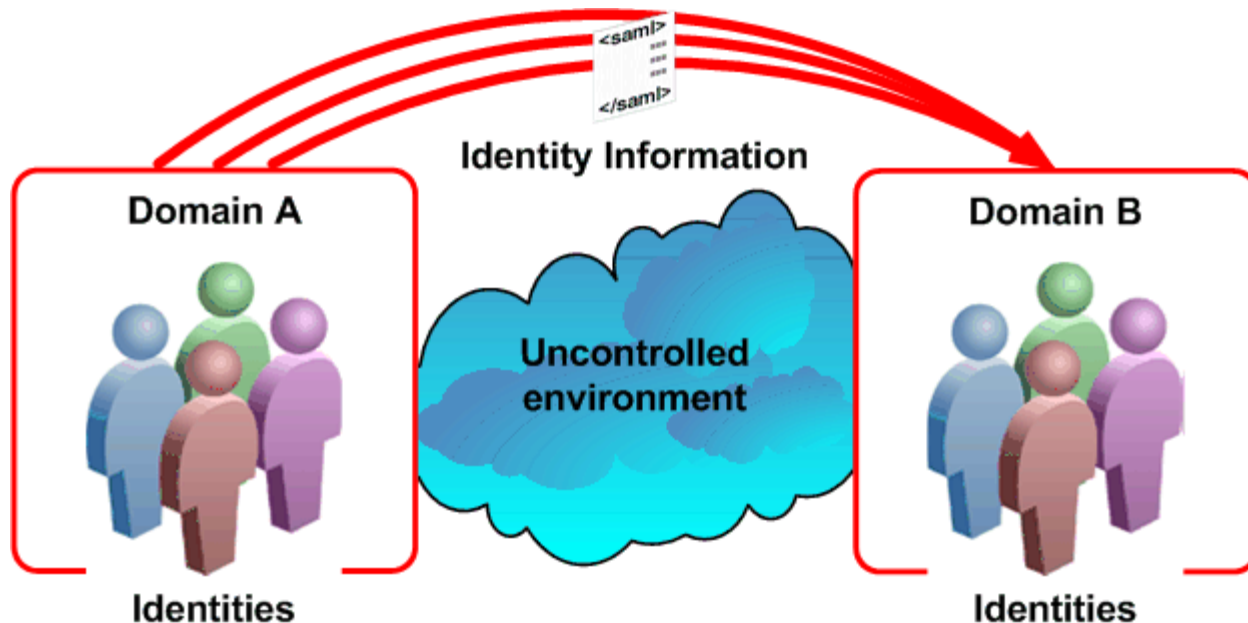
# What if application is NOT in the same security domain



# Identity Federation

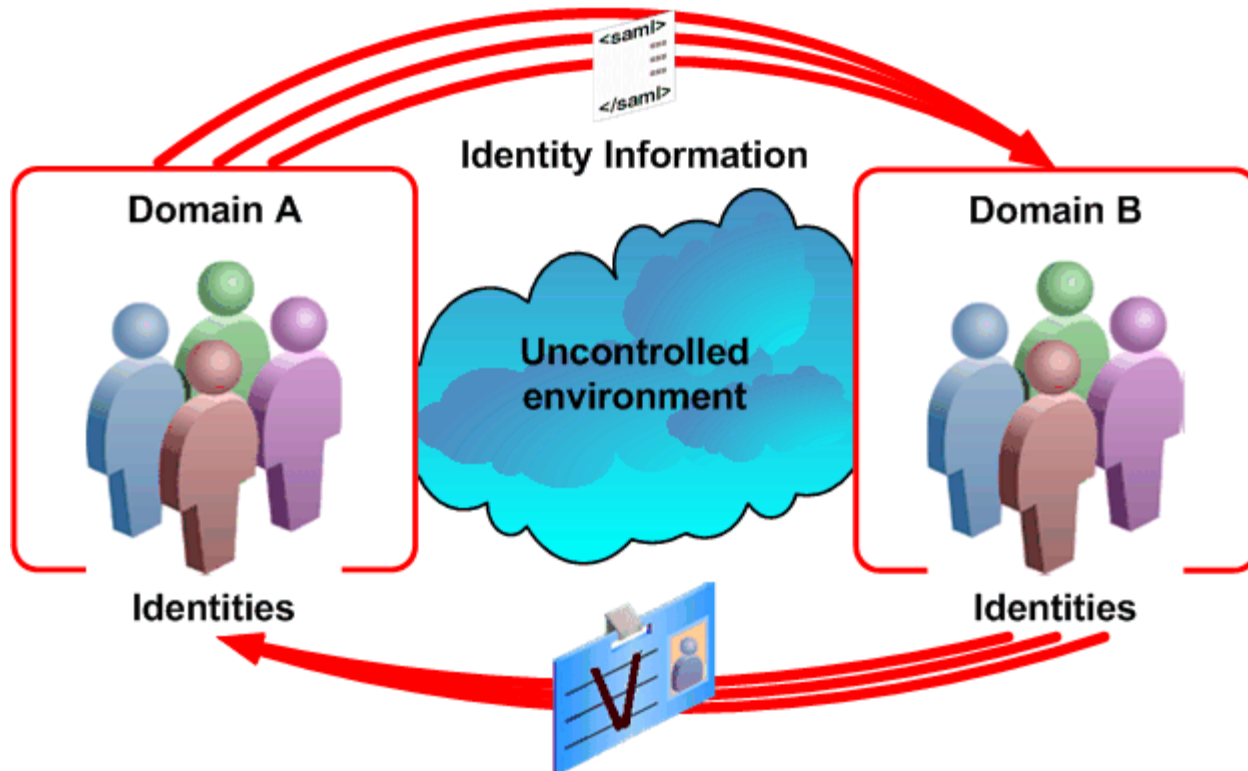
**Identity Federation** is an act of exchange of identity information between two separate entities (domains).

**Identity Domain** is a self-contained system that manages a repository of identity information about its users.



# Direction of Trust

In identity federation **trust** always has a direction.  
The receiving domain needs to **trust** identity information coming from the sending domain.



# Identity Providers and Service Providers



- Domain B trusts Domain A
- Domain A acts in an Identity Provider role
- Domain B acts in a Service Provider role

# What is OIF?

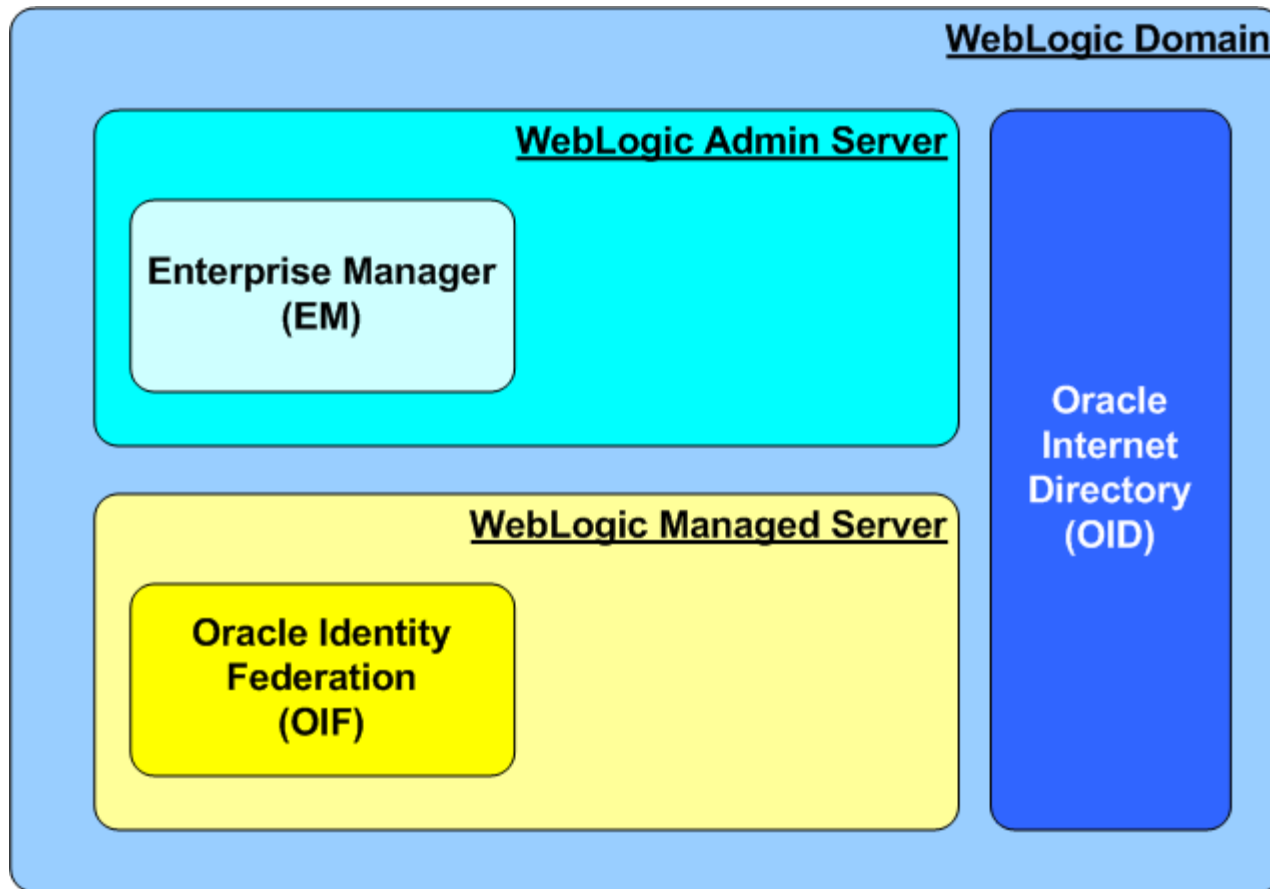
- Oracle Identity Federation is a federation solution with a scalable, standards-based, proven interoperable architecture. Federation and federated identities allow businesses to benefit from trust relationships with their partners.
- With Oracle Identity Federation, business process integration becomes cheaper, simpler, and more secure while increasing compliance with privacy and security regulations.
- Oracle Identity Federation provides the infrastructure that enables identities and their relevant entitlements to be propagated across security domains. This applies to domains existing within an organization as well as between organizations.



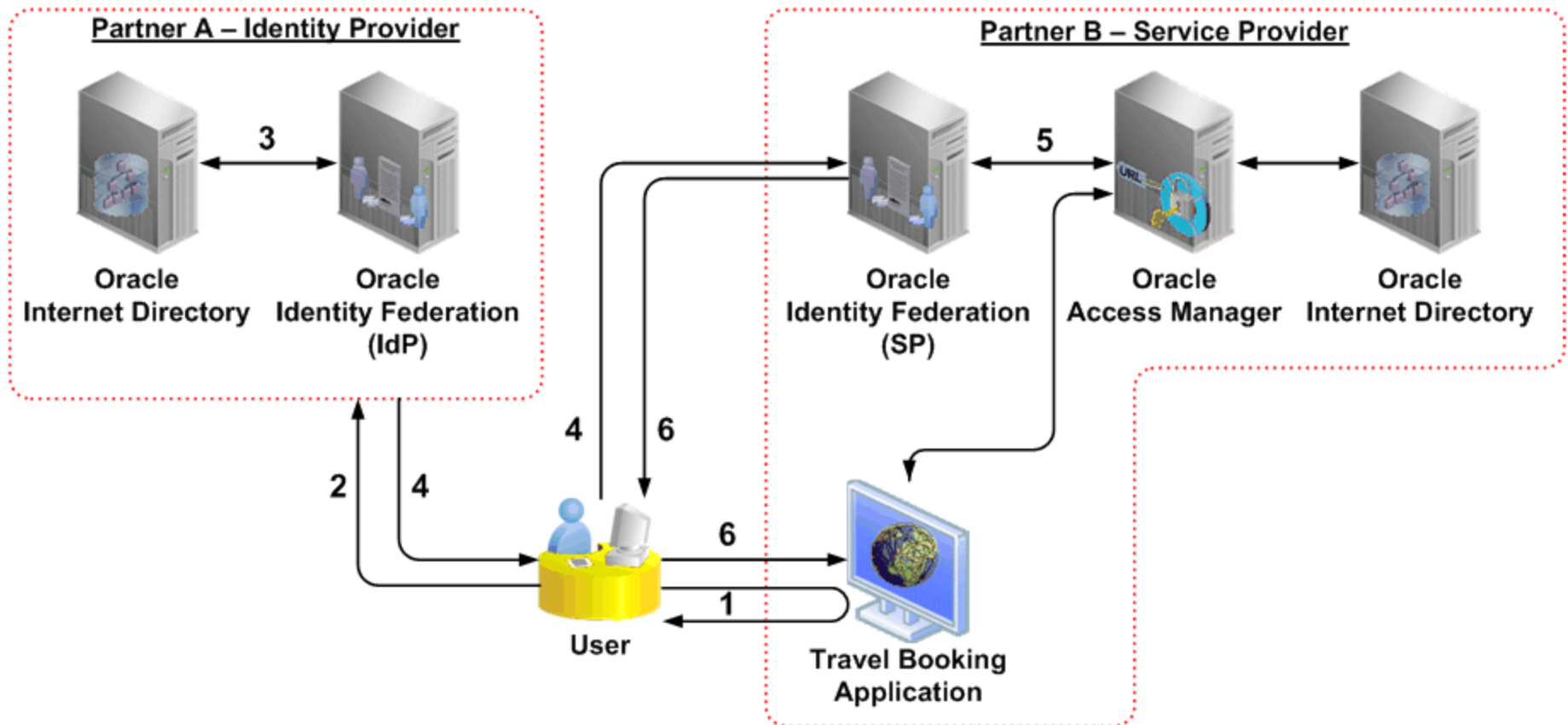
# OIF Top Features

- Oracle Universal Federation Framework (OUFF)
  - OOTB and custom authentication modules
  - OOTB and custom SP integrations
  - Multiple federation protocols in a single stack
  - Flexible data store options
- Oracle Federation Services Manager
  - Unified UI Management Interface
  - WLST Management Interface
- Oracle WLS platform integration
  - Best of Breed Application Server Platform
  - J2EE application
- Oracle Fusion Middleware
  - Enterprise Manager
  - Logging
  - Auditing

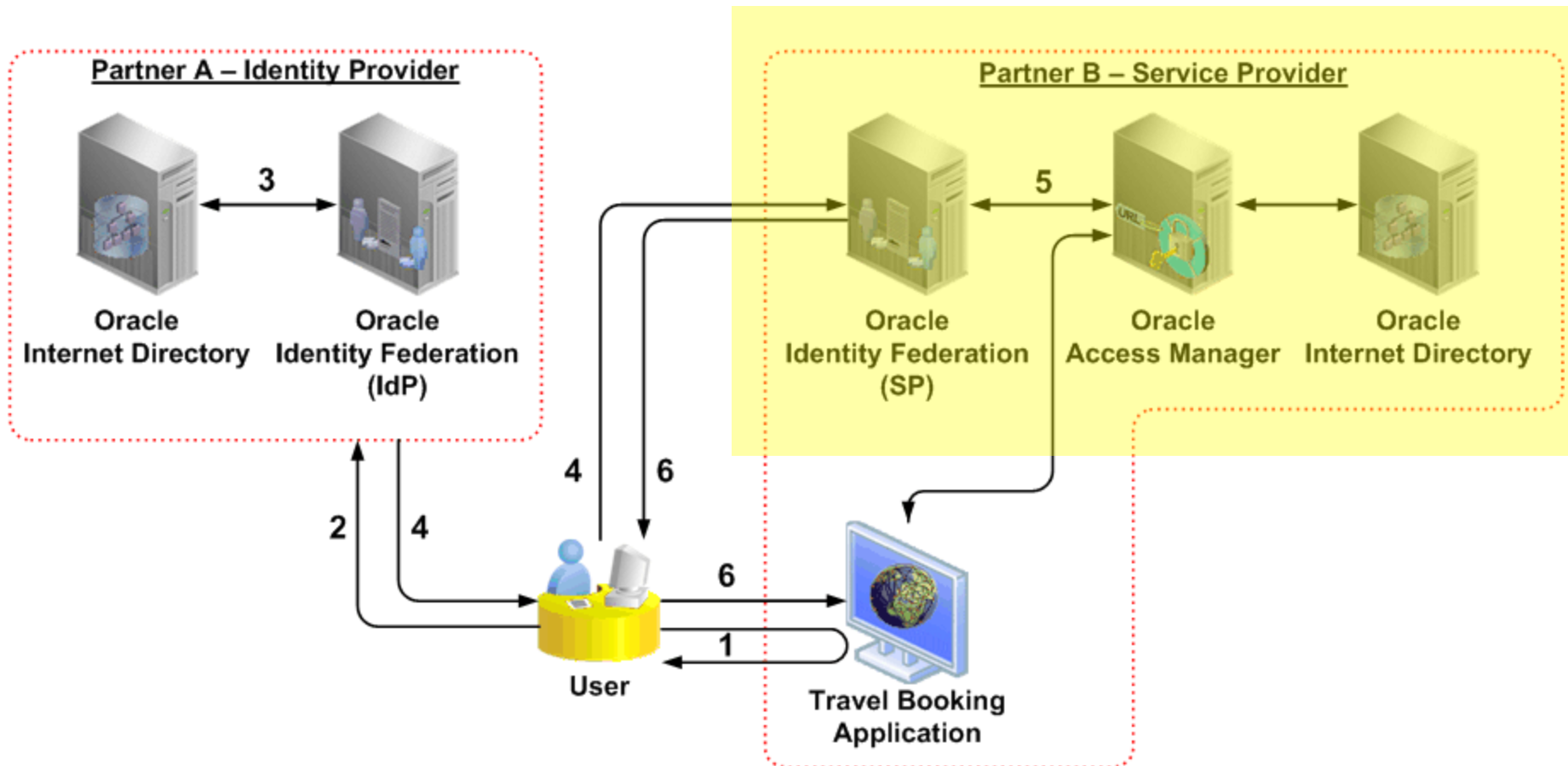
# OIF High-level architecture



# How OIF works - example

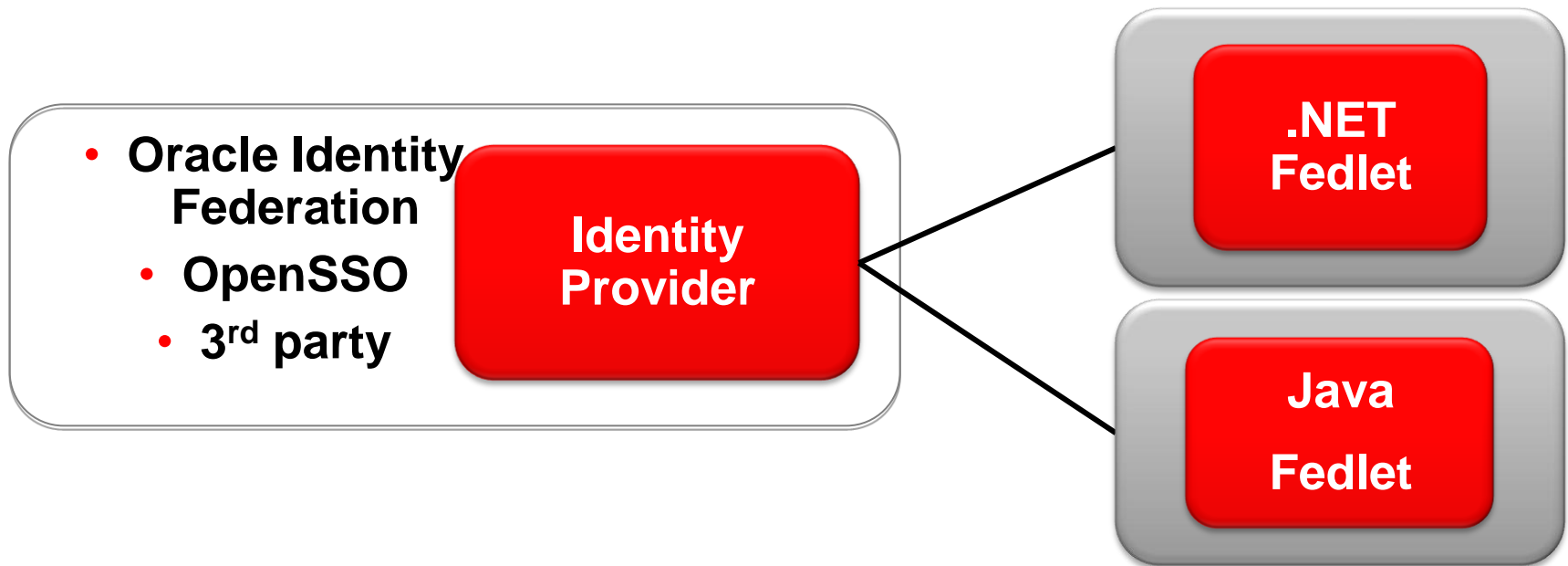


# How about the SP? Any simple integration approach?



# What is Oracle OpenSSO Fedlet?

- Oracle OpenSSO Fedlet is a lightweight SP-only implementation of SAML 2.0 SSO protocols
- Can be used to SSO enable:
  - Internal apps
  - Partner apps



# Benefits of OpenSSO Fedlet

- Ease of deployment
  - Embeddable into any Java or .NET application
  - Multiple integration options
  - Deploys with your application – no additional effort
- Reduced training time
  - Intuitive, developer-friendly
  - Easy to understand, no new skills required
- Earth-friendliness
  - Extremely small footprint
  - Uses your existing infrastructure
  - No new hardware or software requirements
- Reusability and consistency
  - Used the most widely adopted industry standard (SAMLv2)
  - Unified SSO approach across internal and external apps



# Oracle's Identity Management Suite

## Information Rights Management (IRM)

### Identity Admin.

Identity Manager

### Access Management

Access Manager

Adaptive Access Manager

Enterprise Single Sign-On

Identity Federation + Fedlet

Entitlements Server

Web Services Manager

OpenSSO STS

### Directory Services

Internet Directory

Virtual Directory

Directory Server EE

### Identity & Access Governance

Identity Analytics

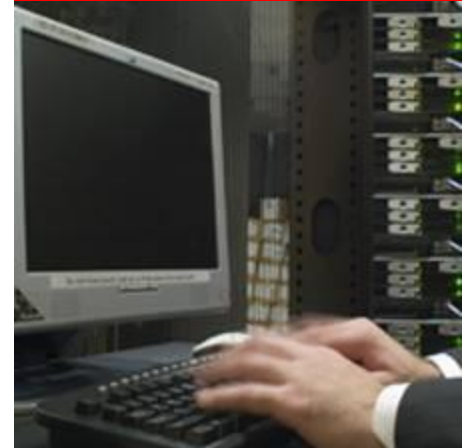
### Manageability

Enterprise Manager IdM Pack

ORACLE

# Agenda

- Web Access Management – A quick introduction
- Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details
- Web SSO with OAM 11g – typical integration scenario example(s)
- Highlights in OAM 11g
- Extending Web SSO from enterprise environment to cross security domain – Identity Federation
- **Demonstrations**



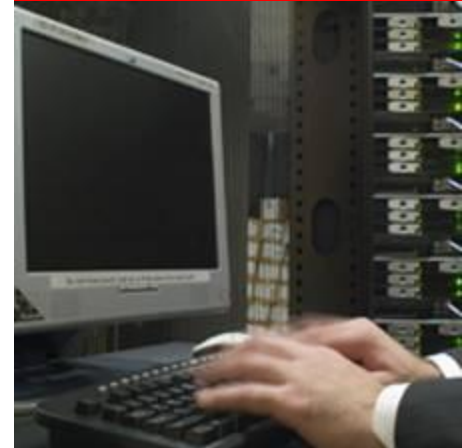


# What's Next?

- Get Trained - contact your local PDM, local presales and/or sales team
  - ACE (APAC Channel Enable Team)
  - PTS
  - Oracle University
- e.g. OAM 11g Hands-on Training: 3-5 days
  - Upcoming training & tentative schedules
    - this week: India
    - Mid Feb ~ late Feb: Australia
    - Late Feb ~ early March: ASEAN – Singapore, Thailand

# Agenda

- Web Access Management – A quick introduction
- Oracle Access Manager 11g (the Web Access Management solution from Oracle): Technical Details
- Web SSO with OAM 11g – typical integration scenario example(s)
- Highlights in OAM 11g
- Extending Web SSO from enterprise environment to cross security domain – Identity Federation
- **Demonstrations (OAM – recorded viewlet – Cert AuthN)**



# Questions..

