International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 6, No. 1
February 2017

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 6, No. 1, February 2017

Research Paper

SOA BASED CENTRAL IDENTITY AND ACCESS MANAGER

Madhavi Vallabhaneni[1]* and Mohan Arava[2]

*Corresponding Author: Madhavi Vallabhaneni ✉ chandanaditya327@gmail.com

Build a common resource identity and access management solution to grant and revoke access privileges and access rights of all resources using a single web based loosely coupled system (SOA based) to easily integrate with new systems and to provide detailed dashboard of usage of different resources and their compliance adherence.

Keywords: Identity and access management, SSO, SOA based integration, SOA work flows, Centralization of IAM

INTRODUCTION

SOA based central Identity and access Manager provides a secure single view. The portal will allow users to have access to data from Siebel, etc., Oracle applications along with access to product documentations. This document defines the design specification for the Au Financiers IDAM Solution and forms the basis with SOA from which the technology solutions are designed. The document contains description of the features to be implemented as well as requirements for the solution.

Through a state-of-the-art, standards-based solution, Oracle's proposed technology delivers authentication, Web single sign-on, access policy creation and enforcement, user self-registration and self-service, delegated administration, reporting, and auditing. Real-time access to identity information ensures that applications get access to changes in identity information directly from the source, avoiding user confusion and security issues involved in synchronization delays. Required Customizations will be done with SOA .

Existing System

- Everything is manually operated.
- Student admissions and their entries into the institution and into their respective departments are handled by the people in admin section.

[1] M.Tech Student, Department of Computer Science and Engineering, Vishwa Bharathi PG College of Engineering & Management, (Approved by AICTE, New Delhi, Ministry of HRD, Govt. of India), Kuppenakuntla (V), Penuballi (M), R.R. District 501503, India.

[2] Assistant Professor, Department of Computer Science and Engineering, Vishwa Bharathi PG College of Engineering & Management, (Approved by AICTE, New Delhi, Ministry of HRD, Govt. of India), Kuppenakuntla (V), Penuballi (M), R.R. District 501503, India.

- Checking of persons into the examination hall is manually done.
- Staff entrance into the department and their access over any resource is not actually maintained. Even this is with respect to the students and other staff in the college.
- The daily log of students, staff and management is maintained in manual registers which are later entered into the systems by other persons.
- Requires a lot of time-effort.

Proposed System

- Automating every operation by implementing IAM.
- Students or staff once they join into the college will be automatically identified and their access over any resource will be pre-defined.
- So trying for any resource which the person is not authorized will be denied by checking it.
- Security is provided for each and every resource present in the institution.
- Notification regarding any event or information will be directed to the respective persons with reduced time effort compared to existing system.
- Centralised system.

TOOLS, TECHNOLOGY USED AND METHODOLOGY

Identity Management: Broad administrative area that deals with identifying individuis aals in a system (such as an org, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

Identity Management: Is an Lifecycle maintenance of organization

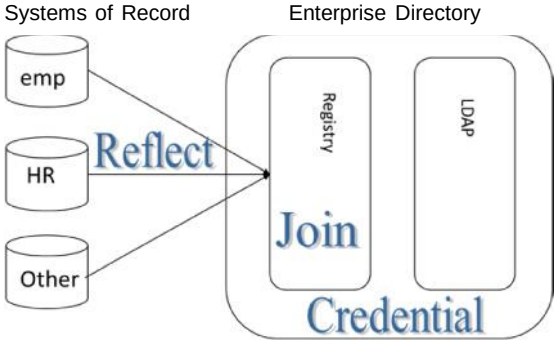
- Provisioning
- Account creation
- Account updates
- Role maintenance
- Account removal
- Authentication & Authorization
- Access Control

Identity and Access Management: IAM technology is used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

Access Management

- Provides a single sign on to web recourses
- Centralized policy based authentication and authorization
- Tracks all users authentication
- Extends access beyond organization boundaries

Figure 1: Systems of Record, Enterprise Directory



Provisioning

- The process of providing users with access to data and technology resources.
- The term typically is used in reference to enterprise-level resource management. Provisioning can be thought of as a combination of the duties of the human resources and IT departments in an organization, where users are given access to data repositories or granted authorization to systems, applications and databases based on a unique user identity, and users are appropriated hardware resources, such as computers, mobile phones and pagers.
- The process of providing customers or clients with accounts, the appropriate access to those accounts, all the rights associated with those accounts, and all of the resources necessary to manage the accounts.

Reconciliation

- Reconciliation is the process by which operations, such as user creation, modification, or deletion, started on the target system are communicated to Oracle Identity Manager.
- The reconciliation process compares the entries in Oracle Identity Manager repository and the target system repository, determines the difference between the two repositories, and applies the latest changes to Oracle Identity Manager repository.
- The reconciliation process involves generation of events to be applied to Oracle Identity Manager. These events reflect atomic changes in the target system, and contain.
- The reconciliation events that are generated consequently because of changes occurring in the target system are managed by using the Event Management section in Oracle Identity System Administration, which addresses these event management needs.

Password Management

- Password manager software is used by individuals to organize and encrypt many personal passwords using a single login. This often involves the use of an encryption key as well. Password managers are also referred to as password wallets.
- Password synchronization software is used by organizations to arrange for different passwords, on different systems, to have the same value when they belong to the same person.
- Self-service password reset software enables users who forgot their password or triggered an intruder lockout to authenticate using another mechanism and resolve their own problem, without calling an IT help desk.

Figure 2: Provisioning and Reconciliation

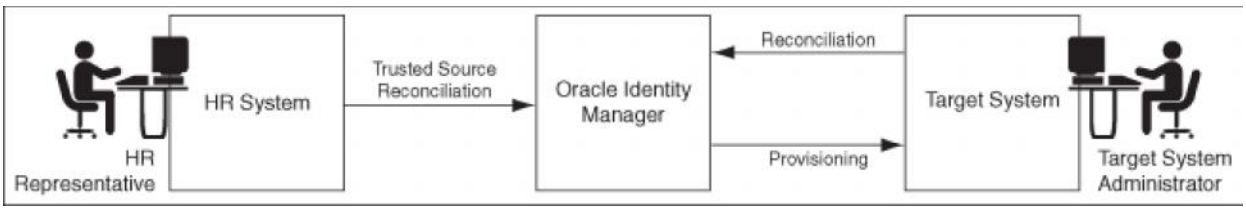
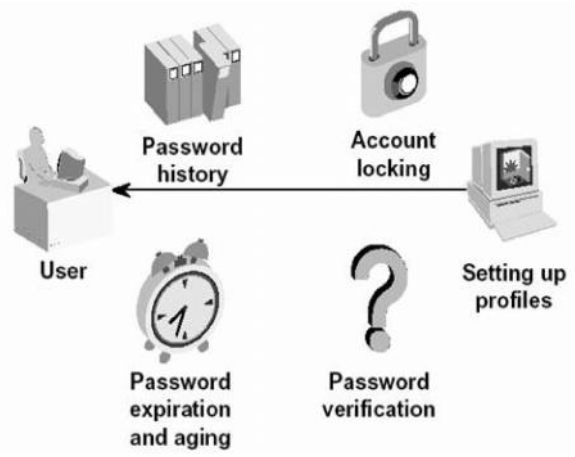


Figure 3: Password Management



SOA (Service Oriented Architecture): Automating the entire system along with its resources, handling many functions and having security for the entire system, all this process makes use of many modules, policies under AM.

Managing entire process with a centralised approach.

Integrating different applications, systems, etc., is done using API's.

The modules that are going to be covered in this Environment are:

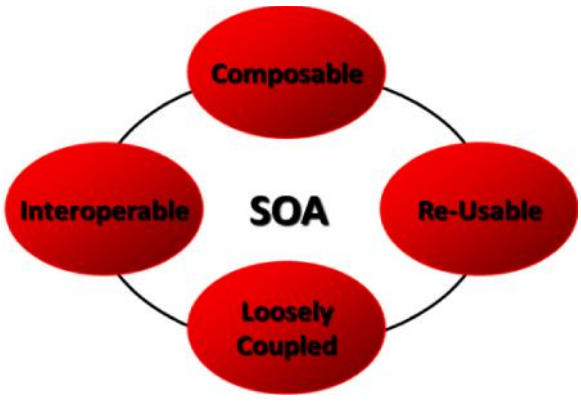
- Integrating all systems and resources available
- User life cycle management
- Auditing.
- Provisioning
- Reconciliation
- Password management

"A service-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed." (http://www.service-architecture.com/web-services/articles/service oriented_architecture_soa_definition.html)

Characteristics of SOA

- Services have platform independent, self describing interfaces (XML)
- Messages are formally defined
- Services can be discovered
- Services have quality of service characteristics defined in policies
- Services can be provided on any platform
- Distributed functionality exposed as shared, reusable services
- Goal is to streamline deployment, reduce duplication of functions, and allow execution of business processes across diverse application platforms in a network
- Tightly-bound to object representation

Figure 4: Characteristics of SOA



Integration of Application

Application Integration is defined as the process of making independently designed application systems work together. Integration is generally

difficult because, in every case, developers must reconcile disparate information architectures involving different data, process and object models. In addition, in most cases, developers must also make the overall solution operate across multiple operating systems, databases and middleware technologies.

OAM INTIGRATION WITH SOA

Oracle Fusion Middleware allows using different types of credential and policy stores in a Web Logic domain. Domains can use stores based on an XML file or on different types of LDAP providers. When a domain uses an LDAP store, all policy and credential data is kept and maintained in a centralized store. However, when using XML policy stores, the changes made on Managed Servers are not propagated to the Administration Server unless they use the same domain home. The Oracle Fusion Middleware SOA Suite EDG topology uses different domain homes for the Administration Server and the Managed Server, thus Oracle requires the use of an LDAP store as policy and credential store for integrity and consistency. By default Oracle WebLogic Server domains use an XML file for the policy store.

Figure 5: Admin Login Page

Figure 6: Identity Self Service Console

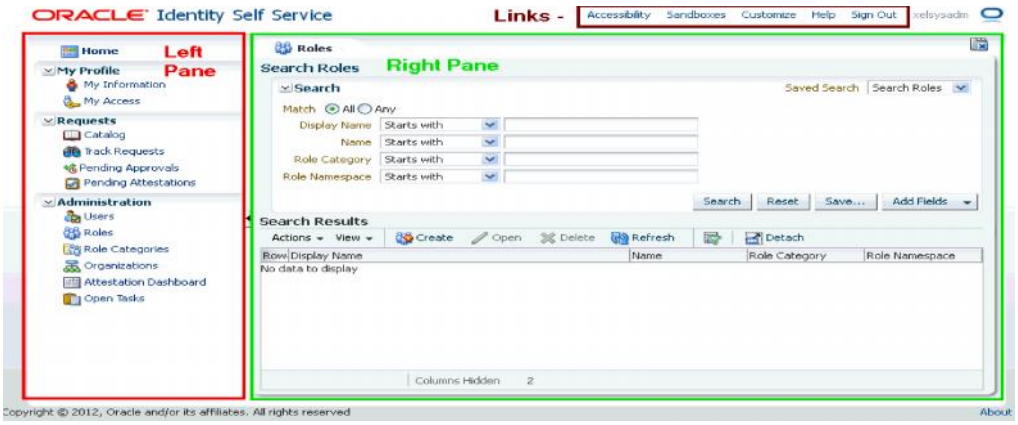


Figure 7: Identity Admin Service Console

Figure 8: Creation User in OIM

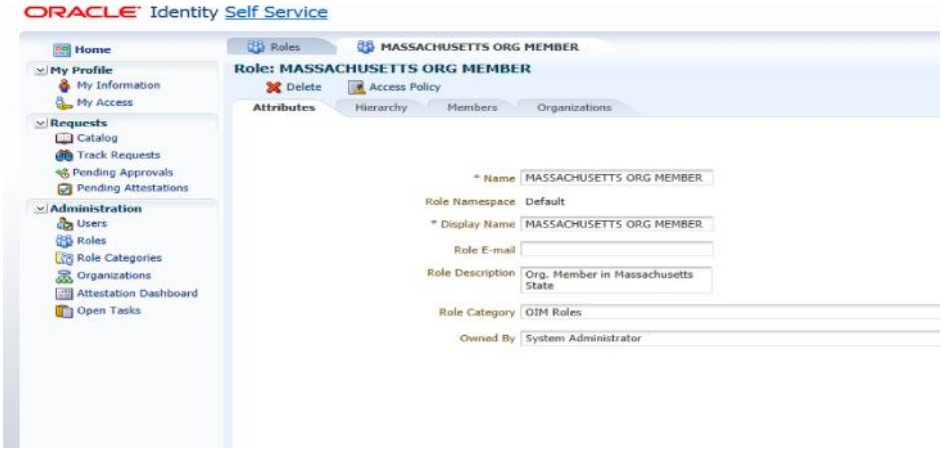


Figure 9: Provisioning

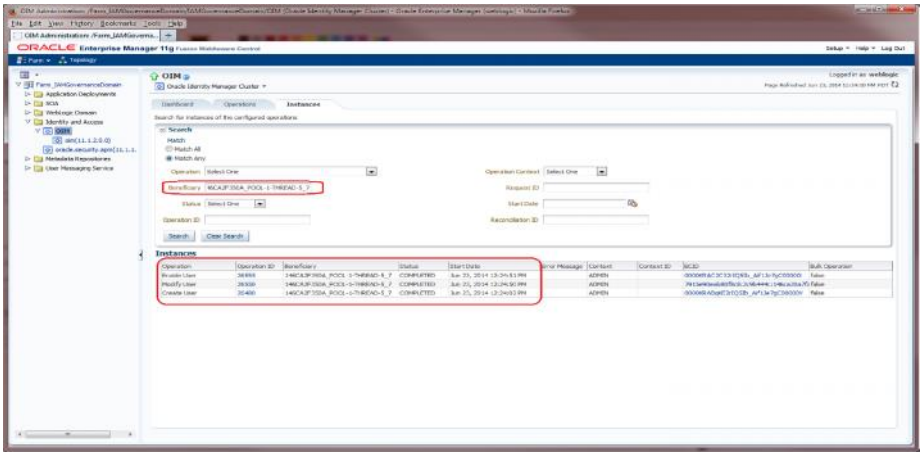
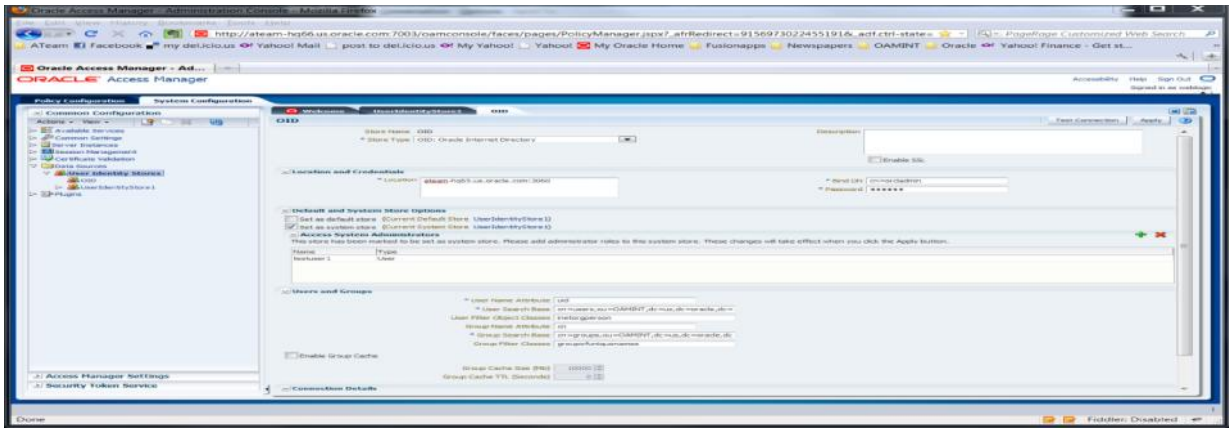


Figure 10: Reconcile the User in OIM

Figure 11: OAM Console



Sample Code for SOA Based Identity Management and Access Management

- Create User
- Lock User
- Unlock User
- Disable User
- Enable User
- Reset Password

```
package oimclient;

import java.util.HashMap;

import java.util.Hashtable;

import javax.security.auth.login.Login Exception;

import oracle.iam.identity.exception.NoSuch UserException;

import oracle.iam.identity.exception.User AlreadyExistsException;

import oracle.iam.identity.exception.User CreateException;

import oracle.iam.identity.exception.User DisableException;

import oracle.iam.identity.exception.User EnableException;
```

```
import oracle.iam.identity.exception.User LockException;
import oracle.iam.identity.exception.User ManagerException;
import oracle.iam.identity.exception.User UnlockException;
import oracle.iam.identity.exception.Validation FailedException;
import oracle.iam.identity.usermgmt.api. UserManager;
import oracle.iam.identity.usermgmt.vo.User;
import oracle.iam.platform.OIMClient;
public class OIM {
    UserManager userManager;
    public OIM() {
        super();
    }
public static void main(String[] arg) {
OIM oim=new OIM();
oim.OIMConnection();
oim.createUser("sachinTen"); //comment if you are calling any other methods below
//oim.lockUser("sachinTen"); //uncomment to lock user
//oim.unLockUser("sachinten"); //uncomment to unlock user
//oim.disableUser("sachinTen"); //uncomment to disabel user
//oim.enableUser("sachinTen"); //uncomment to enable user
//oim.resetPassword("sachinTen"); // uncommnet to reset password
    }
public void OIMConnection(){ //Function to Connection to OIM
Hashtable<Object, Object> env = new Hashtable<Object, Object>();
env.put(OIMClient.JAVA_NAMING_FACTORY_ INITIAL, "weblogic.jndi.WLInitialContextFactory");
env.put(OIMClient.JAVA_NAMING_PROVIDER_ URL, "t3://localhost:14000"); //Update localhost with your OIM machine IP
System.setProperty("java.security.auth.login. config", "D:/Oracle_New/Middleware/Oracle_ IDM1/server/client/oimclient/conf/authwl.conf"); //Update path of authwl.conf file according to your environment
System.setProperty("OIM.AppServerType", "wls");
System.setProperty("APPSERVER_TYPE", "wls");
oracle.iam.platform.OIMClient oimClient = new oracle.iam.platform.OIMClient(env);
try {
oimClient.login("xelsysadm", "Password". toCharArray()); //Update password of Admin with your environment password
System.out.print("Successfully Connected with OIM ");
} catch (LoginException e) {
System.out.print("Login Exception"+ e);
}
userManager = oimClient.getService(User Manager.class);
}
```

```
public void createUser(String userId) { // Function to create User
    HashMap<String, Object> userAttribute ValueMap = new HashMap<String, Object>();
    userAttributeValueMap.put("act_key", new Long(1));
    userAttributeValueMap.put("User Login", userId);
    userAttributeValueMap.put("First Name", "Sachin");
    userAttributeValueMap.put("Last Name", "Ten");
    userAttributeValueMap.put("Email", "Sachin.Ten@abc.com");
    userAttributeValueMap.put("usr_ password", "Password123");
    userAttributeValueMap.put("Role", "OTHER");
    User user = new User("Sachin", userAttributeValueMap);
  try {
    userManager.create(user);
    System.out.println("\nUser got created....");
    } catch (ValidationFailedException e) {
      e.printStackTrace();
    } catch (UserAlreadyExistsException e) {
      e.printStackTrace();
    } catch (UserCreateException e) {
      e.printStackTrace();
    }
  }
  public void disableUser(String userId) { // Function to disable user
    try {
      userManager.disable(userId, true);
      System.out.print("\n Disabled user Successfully");
    } catch (ValidationFailedException e) {
      e.printStackTrace();
    } catch (UserDisableException e) {
      e.printStackTrace();
    } catch (NoSuchUserException e) {
      e.printStackTrace();
    }
  }
  public void enableUser(String userId) { // Function to enable user
    try {
      userManager.enable(userId, true);
      System.out.print("\n Enabled user Successfully");
    } catch (ValidationFailedException e) {
      e.printStackTrace();
    } catch (UserEnableException e) {
      e.printStackTrace();
    } catch (NoSuchUserException e) {
      e.printStackTrace();
    }
  }
  public void resetPassword(String userId) { // Function to reset user password
    try {
      userManager.resetPassword(userId, true,true); //Random Password will be set and
```

```
will be sent to user mail if notifications are enabled
            System.out.println("Reset Password done...");
        } catch (NoSuchUserException e) {
            e.printStackTrace();
        } catch (UserManagerException e) {
            e.printStackTrace();
        }
    }
    public void lockUser(String userId) { //Function to Lock User
        try {
            userManager.lock(userId, true,true);
        } catch (ValidationFailedException e) {
            e.printStackTrace();
        } catch (UserLockException e) {
            e.printStackTrace();
        } catch (NoSuchUserException e) {
            e.printStackTrace();
        }
    }
    public void unLockUser(String userId) { // Function to Unlock user
        try {
            userManager.unlock(userId, true);
        } catch (ValidationFailedException e) {
            e.printStackTrace();
        } catch (UserUnlockException e) {
            e.printStackTrace();
        } catch (NoSuchUserException e) {
            e.printStackTrace();
        }
    }
}
```

Uses

- Organizations have to bring together a well understood set of identity management capabilities in an organized fashion if they are to respond effectively.
- Effective control of identity management services for a SOA will require the use of policies which define the identity-specific requirements of each interaction, such as how a employee of a organization service must be authenticated or their rights to access particular information.
- SOA allows different ways to develop applications by combining services.

SOA is to erase application boundaries and technology differences.

Disadvantages

Increased Overhead: Every time a service interacts with another service, complete validation of every input parameter takes place. This increases the response time and machine load, and thereby reduces the overall performance.

High Investment Cost: Implementation of SOA requires a large upfront investment by means of technology, development, and human resource.

Complex Service Management: The service needs to ensure that messages have been delivered in a timely manner. But as services keep exchanging messages to perform tasks, the number of these messages can go into millions even for a single application. This poses a big

challenge to manage such a huge population of services.

CONCLUSION AND FUTURE ENHANCEMENT

This section provides general information about the evolution of Oracle Identity Management after the 11g R2 release. Such evolution revolves around three main axes: role management, identity as a service, and identity and access management analytics. Future releases of Oracle Identity Management will leverage its service-based architecture to enhance Oracle's overall identity and access management offering.

Oracle Identity Manager is an identity management product that automates user provisioning, identity administration, and password management, integrated in a comprehensive workflow engine.

REFERENCES

1. Cloud Corporation_Response.ppt
2. Documents from Cloud Authentication and Authorization Security.
3. Hassan Qusay (2011), "Demystifying Cloud Computing", *The Journal of Defense Software Engineering (CrossTalk),* January/ February, pp. 16-21, Retrieved 11 December 2014.
4. Fonebell (2015), "Know Why Cloud Computing Technology is the New Revolution".
5. Peter Mell and Timothy Grance (2011), "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Retrieved 24 July.
6. Baburajan and Rajani (2011), "The Rising Cloud Storage Market Opportunity Strengthens Vendors", *InfoTECH*.
7. Oestreich and Ken (2010), "Converged Infrastructure", CTO Forum, Thectoforum.com
8. Oracle identity management.pdf
9. Sample opportunity data.xls

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com