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

E TRANS_ENTERPRISE PORTAL SECURITY MANAGEMENT

Sravanthi Kokkula[1]* and Mohan Arava[2]

*Corresponding Author: Sravanthi Kokkula ✉ sravi1205@gmail.com

Identity and Access Management in Cloud Computing is focused on the implementation challenges of Identity and Access Control Architectures as they relate to cloud computing. Identities for cloud computing can be broken down into the following categories: Enterprise - Enterprise Users, and applications that will access cloud applications. Internet - Customers, Partners, and Unanticipated Users that will access cloud applications. Cloud - Cloud applications that will access cloud, enterprise, and partner applications. Whether we are talking about cloud usage, or cloud administration, identities can be binned into one of these three categories. The following paragraphs focus on the options and challenges in implementing an identity and access control architecture for cloud computing.

Keywords: Identity, Access management, Cloud computing, SOA work flows

INTRODUCTION

Identity and Access Management in Cloud Computing is focused on the implementation challenges of Identity and Access Control Architectures as they relate to cloud computing. Identities for cloud computing can be broken down into the following categories:

Identity Management

Broad administrative area that deals with identifying individuisals 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.

Oracle Access Manager will provide for coarse-grain Access control for http resource.

- Workflow complexity level will be Simple, Medium, Complex.
- Workflow with One step approval will be considered as Simple.

[1] 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.

- Workflow with 2 or 3 step approval will be considered as Medium.

Content Management

All the documents and folders will be managed through the Oracle Cloud application.

SOA and Process Management

- Web Services management through the SOA and Process Management.
- BPEL will be used for Workflows design.

Cloud

- Many of the same issues encountered in moving identity management to the cloud are encountered with this approach.
- Possible breach and release of identities to the internet.
- Administrative burden in managing two systems.
- Siebel provides out of box portlet services and is directly integrate with portal. All the Siebel application URLs will be provided as links with in the portal page and once the user clicks these links Siebel application will be opened in another browser.
- The single sign on feature provided by Oracle portal as out of box is only considered for integration with portal as security. There is no addition security related features considered for this scope of work.
- Folder level policies will be configured by Identity Management Team.
- URL resource protection policies will be configured by Identity Management Team.

Here Our procedure consist of

1. Provisioning
2. Reconciliation
3. User Life Cycle Management
4. Web Single Sign On (SSO)
5. Password Management

Oracle Identity Manager is the identity administration and user provisioning solution, provides operational and business efficiency through centralized administration and complete automation of identity and user provisioning events across the enterprise, as well as extranet applications. It is used to administer the entire user lifecycle through a common platform and along with its powerful audit and compliance module along with reporting ensures that all the security norms are adhered to in an organization.

The Proposed Oracle Identity Management system will provide complete user life cycle management includes user provisioning, de-provisioning.

User Provisioning

The proposed solution will provide a centralized point of entry for user access provisioning to the various applications in the scope. User provisioning will be configured by extending the OOTB connector functionality.

De-Provisioning

On termination of users, HRMS will send feed file for the users marked as 'Disabled'. IDAM will reconcile the feed file and disable the users. Subsequently the users will be disabled in all the connected target systems. The disablement of the user will happen automatically and real-time basis.

Reconciliation

At Day 1, Initial user load will be done through the full reconciliation of enterprise user base. HRMS will provide the flat file consisting all user records. IDAM will run the GTC for the reconciliation.

GTC (Generic Technology Connector)
Solution: GTC is the one of the OIM feature helps users to load to OIM User repository.

HRMS_Feed_1.csv file should be consists of all the internal User Profiles information, OIM Admin defined scheduler will run and start creating the users as reconciliation process.

Note: HR Team should upload the CSV file to/ Stage location and IDM team will manage the same file in/Stage/Archive location for Audit log.

Brith Right Role Management

Once the user created in OIM automatically user will be provisioned to AD target system. If user want to get any application access he/she has to submit the Application request. Based on one level department_approver approval done user will be Provisioned to respective target systems. As part of the BirthRightAccess user request for Role in OIM will trigger the updated provisioning and respective application roles/access will be provisioned in the target system.

User Life Cycle Process – Joiner/Mover/ Leaver

Joiner operation will be initiated in HRMS when new employee/user joins target system. HRMS feed file will be reconciled in IDAM for user creation and default password generated. First time password will be shared to Manager. Birth right application access will be provided to the created users.

All external users should be having De-Provisioning date. Based on de-provisioning date access will be terminated from the applications. IT Admin should be having emergency access on External Users cycle management. User separation can be updated from Status attribute also. Once user status updated to "Disabled" automatically user access will be terminated from all the applications. There is no enable feature if user is disabled.

HRMS Initiated: User modification feed file will be reconciled to IDAM. Respective modification will be done based on attribute change. All the modifications will be propagated to all the target applications by OIM.

Self Service Initiated: Moving from one role to another. User have to request for the new access/ role, assignment will be granted upon approval (one level approval). In OIM user will initiate the Role request from OIM self service console.

IDAM Password Policy

IDAM will maintain below password policy. This policy is the default and enabled in OIM as main password policy and maintained same in all the target applications. Applications will disable its native password management functionality.

OIM Provides Default OOTB Password Policy Configurations

Web Single Sign On (SSO)

Single Sign-On (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.

This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on servers. A simple version of single sign-on can be achieved using cookies but only if the sites are on the same domain.

Conversely, single sign-off is the property whereby a single action of signing out terminates access to multiple software systems.

As different applications and resources support different authentication mechanisms,

Table 1

Parameter	Value
Password Length	8 – 16 character long
Alphanumeric Characters Allowed	A-Z, a-z, 0-9
Special Characters Allowed	For example: @#$%^&*()_+|~-=\`{}[]:";'<>/, and other such characters
Password History	Last 5 passwords not allowed
Password Expiry	90 days
Password Lock	Lock after 3 unsuccessful attempts
Password Lock Duration	30 mins
Random Generated Password	8 char long with combination of alphanumeric and special characters
Password Communication	Email to user and Manager. If manager is not available, <AUF> to advise. First time password will be generated RANDOMLY as per policy
Password Synch	Password will be pushed from IDAM to target applications not vice versa. Reverse synch with AD <AUF> to advise
Secret Q & A	Set of 3 questions which are available out of box from IDAM
Min password age	1 day
Password Complexity	Contain at least three of the four following character classes:
	§ Lower case characters
	§ Upper case characters
	§ Numbers
	§ "Special" characters or Punctuation (For example: @#$%^&*()_+|~-=\`{}[]:";'<>/, and other such characters)

single sign-on must internally translate and store credentials for the different mechanisms, from the credential used for initial authentication.

- Passport is not the only Web SSO protocol that had vulnerabilities, flaws in others protocols were identified by [Ptzmann03, Groß03]. Although Web SSO is conceptually similar to Single Sign-On (SSO) protocols like Kerberos, they must operate within limitations of commercial browsers.
- Web SSO systems are proxy-based true SSO systems [Pashalidis03]. Web SSO protocols are also called browser-based or *zero-footprint*protocols since they operate within the constraints of web browsers.
- Furthermore, messages exchanged in browser-based protocols must be encapsulated in Hypertext Transfer Protocol (HTTP) supported by all commercial browsers since users should not be expected to install software to support a new protocol. Moreover, browser cookies are tied to a single domain so cannot be used for the Multi-Domain SSO (MDSSO).
- MDSSO refers to the case where SSO occurs between security domains operated by disparate organizations. For example, in the web-based MDSSO, Alice uses her browser to book her flight at airlineinc.com and is transparently logged in at hotelinc.com to reserve her room. A trust relationship must exist between the two domains to support this federated authentication since the domains may have different security polices. This paper does not cover the trust establishment problem. It also does not focus on the federation of attribute and authorization data. It deals with federated authentication of users in the web-based MDSSO case.
- Security analysis of web-based MDSSO protocols demands unconventional requirements and models, and to date only one protocol has been proved cryptographically secure [Groß05]. In the paper, we focus on the three-party authentication protocols for Web SSO since these protocols have been analyzed by [Groß03, Groß05].

- The three parties include a service provider(SP), identity provider(IP), and user agent(UA). The UA is the web browser operated by the user, the IP authenticates the UA, and the SP is the web application.

METHODOLOGY AND USED TOOLS

Portal Management

Design a Cloud layout which is used as a common interface to log into cloud and access different applications.

Based on the User type and role portlets should be given access with the integration of identity management for single sign on access.

Integration of Cloudl with site caching service provided by EMC for search capabilities on the Portal.

Portal provides access to Siebel application links with the help of single sign on from IDM for all the registered users at Cloud Platform.

Cloud is the single point of access for different web services through SOA and BPEL Process.

Cloudl provides access to BI Reports used by the internal eTrans Corporation users and external users based on their role

Identity and access management integration with Cloud will provide single sign on access to application like Siebel CRM, RMA , BI Reports for the Internal and external users of eTrans Corporation.

Cloud admin provides features like publishing and editing the content to portal.

Integration of Enterprise Google Search with Cloud.

Identity Management

Setup Application/Web server

Setup Oracle Access Manager components (WebPass, WebGate, Identity Server, Access Server, Policy Manager, Oracle Internet Directory).

Setup policy domains to protect web (http(s)) resources in a given period of in a given period of configure password Policy for Users in Identity Server.

Enforce password history = 8. Maximum password age = 90 days. Minimum password age = 1 days. Minimum password length = 7 characters, Password must meet complexity requirements = Yes. Account lockout duration = 90 minutes. Account lockout threshold = 3 invalid logon attempts. Reset account lockout counter after = 90 minutes.

- Authentication and authorization for Oracle Portal
- Setup WebGate for Oracle Portal server
- Customization of User Self registration screen to accommodate Business type & user roles.
- Create one step Approval process for Delegated admin.
- Create an Email Notification for Approver.
- Provision External user to Oracle internet directory after approval process.
- If rejected by the approver, send a notification to the user citing reasons for denial.
- Send Email Notification to helpdesk team for manual user creation in Siebel/Oracle/Other (DW) system.
- Workflow should handle the helpdesk feedback and notify the user that he has been provisioned.
- After authentication, External/Internal User should be able to modify his profile detail like address, Phone number.

- This link or URL would be exposed through Portal once the user is authenticated.
- AD team will delete/disable users from Active Directory.
- Periodically, Oracle internet directory should be synchronised with user status in real-time.
- Admin user (from Sales Admin group) should be allowed to disable/delete External user.
- For this, a user(s) would be identified and added to this admin group for administering the account.
- User should be allowed to reset their password from eTrans Corporation Enterprise Portal
- User will be authenticated based on personalized security questions.
- Once User is identified, he/She should be allowed to change password.
- Changed password should be synchronised with AD immediately.
- Auditing User Access to database.
- End User should be allowed to change user profile after Authenticating to the System
- End user should be allowed to modify his relevant attributes like Address detail, Contact Number, etc.
- Logout URL should be provided to the portal team so that they can embed the same in portal.
- The logout URL removes session cookies and redirects users to a logout page.

Cloud Authentication in Identity Management

Users should be authenticated, when he/she tries to access any HTTP resource.

- All - external, internal and anonymous users should be able to access Home page.
- All User should be able to see Login screen of Oracle Access Manager in Portal.
- Any Business user - External or Internal (only RSM), has to provide user name and password on the login screen for authentication.
- User should be validated/authenticated against Oracle Internet Directory (OID).
- Once user is authenticated, he/she should be allowed to access the resources/applications based on user role.
- If user authentication fails, he/she should be informed appropriately and should be challenged with Login screen.
- Anonymous User, when tries to access any protected HTTP resource should be challenged for User credentials.
- Form based single factor authentication scheme would be used for user authentication.
- Internal users would be the employees (including RSM) of ETrans Corporation Corporation.
- Customers, Suppliers, Distributors, Sales reps and Enterprise customer constitutes External users.

So we can assume that

- HTTP URLs for various applications are identified and same are protected using policy domains in OAM Policy Manager.
- External user data would be migrated/uploaded into OID and authentication of external user happens against OID.

Internal user data for AD would be migrated/ uploaded into OID and authentication of Internal user will be done using OID.

CONCLUSION

Whether we are talking about cloud usage, or cloud administration, identities can be binned into one of these three categories. The following paragraphs focus on the options and challenges in implementing an identity and access control architecture for cloud computing.

REFERENCES

1. Baburajan and Rajani (2011), "Baburajan, Rajani, "The Rising Cloud Storage Market Opportunity Strengthens Vendors," *Infotech*.
2. Fonebell (2015), "Know Why Cloud Computing Technology is the New Revolution".
3. Hassan, Qusay (2011). "Demystifying Cloud Computing" (PDF). *The Journal of Defense Software Engineering* (CrossTalk).
4. Mell P (2011), "The NIST Definition of Cloud Computing" (PDF). National Institute of Standards and Technology.
5. Oestreich Ken (2010), "Converged Infrastructure". *CTO Forum*.
6. What is Cloud Computing (2013), *Amazon Web Services*.

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