Use Cases for Evaluating IAM Solutions

Access Management

UC Berkeley - Enterprise Data Warehouse Access Request

The campus has a need to provide individual users (employees, student workers, and consultants) with temporary and limited access to the Enterprise Data Warehouse (EDW). The users make a request specifying the type of information (department) and their expected use (role). Before the request is forwarded, a webservice call verifies whether or not the requestor has completed FERPA (Family Educational Rights and Privacy Act).

Once forwarded, the request requires two levels of approval. First a manager confirms or rejects the request (for each role/department assignment). Then an administrator provides final approval or disapproval of each role assignment. Notifications are provided to appropriate parties throughout the process, and the reasons for all rejects are included in the notifications as well as stored for later review. Role and department assignments are provisioned to Oracle 11g security tables used to authorize access to the Data Warehouse. An audit log is maintained of all the activities for audit and analytics.

Describe how the IAM system will facilitate creation and management of the workflow, needed to support a request and approval process, for accessing the Student Enterprise Data Warehouse. Describe the work, configuration and customization, needed for each of the following product areas of your IAM:

- Workflow/UI
- Provisioning for all roles
- Role management
- Authentication (including Federation model)
- Registries
- Reporting and Analytics

Describe the out-of-the-box and customizations necessary to implement such an access request process in the Oracle IAM suite. Give an estimate of any programming/integration effort for someone thoroughly familiar with the IAM and the development environment.

UCSF - Mainframe Apps Access Management

Employees who need access to these systems notify their departmental Access Administrators, who then submit an authorization request via a web form. Each business application has a handful of roles which can be assigned to a given user. The request is approved by a manager and then the role assignment is provisioned either to DB2 security tables or to LDAP groups. All transactions related to access requests and approvals must be auditable for reporting.

Describe how the Oracle IAM solution would be used to implement the delegated administration for Access Administrators, the access request and approval workflow, and the provisioning and storage of authorization data for users (by role assignment or group membership), and the audit and reporting functionality.

Provisioning and Group Management for Federated Collaboration

UC Berkeley - Sakai Open Academic Environment (OAE)

Overview of Sakai OAE
Permeable
Our students, teachers and researchers inhabit an academic world that extends beyond the institution. Our institutional platforms complement this fuller experience; they should not try to dominate it.

Social
Social networks were fundamental to academic success long before there was an internet.Sakai provides a social networking rooted in academic societies: a scholarly networking for learners and researchers alike.

Personal
Individuals need to be free to organize and make sense of their experience, even where it extends (as it often does) beyond the institutional boundary. Sakai aims to support these preferences of personal control.

Remixable
Sakai achieves a balance of scaffolded freedom through storing structures of content, spaces and activities as templates and then allowing these templates to be widely shared, reviewed and revised. The innovators are put back in the driver's seat.

Challenges
The Sakai OAE group is creating a federated collaboration environment for all the UC schools. User account and group information needs to be provisioned in Sakai OAE from systems of record. Since Sakai OAE is a remixable system, group information created within Sakai OAE that will be useful for other applications needs to move out of Sakai OAE as well. Users of the Sakai OAE may have multiple roles within the system, ex: student, lecturer, researcher, admin, and need appropriate access for those roles in different parts of Sakai OAE.

Key Questions
Describe how the IAM system will integrate with systems of record for group data to provision authorization data to applications. Describe whether the group data will be:

(1) stored as part of the IAM system and exposed via APIs and how so exposed, or

(2) how it would integrate with a specialized system for managing groups, specifically Grouper <http://www.internet2.edu/grouper/>, to provision the same authZ data to applications while linking such authZ data to internal IAM accounts.

In either case describe how group data information is available for internal IAM processes and which ones as well as exposed via APIs and how so exposed.

Much of this implies customization of the IAM system for integration and business functions: describe the development environment required and the estimated effort in terms of programming time for someone thoroughly familiar with that environment.

Provisioning

UC Berkeley, MIT and AD Kerberos provisioning

Creation and updating of new records requires provisioning to both MIT Kerberos and Active Directory. The IAM adapter must support provisioning and deprovisioning of Kerberos principals as well as administrative functions such as resetting and changing passwords. Leveraging an existing Java API such as documented at the Stanford kadmin-remctl site would be the preferred integration method.
Please describe out-of-the-box and/or customization functionality of the Oracle IAM related to the provisioning and deprovisioning of Kerberos credentials and password administration.

Creating Digital Identities - Identity Match

UC Berkeley ID Match

One important part of a campus IAM system is identifying an individual user's data within several disparate authoritative data sources through the use of a partial SSN (last five digits), birth date, and last name. Describe how this would be achieved with the Oracle IAM suite. Below is more detail to describe the current approach at UCB.
Here is an example of the logic followed when a brand new employee affiliation is added to the CalNet Directory.

1. Load the employee data for the user from HRMS (the authoritative source for employee data). After the employee data has been loaded into memory, search the LDAP directory to see if an entry already exists for the employee.
2. If no related LDAP entry is found, search all other authoritative data sources for related identity data. To accomplish this, first check whether or not a student id was provided in the employee data. If a student ID was provided, check LDAP again to see if an existing entry matching the student ID exists.
3. If still no LDAP entry has been found, use the last five digits of the user's SSN, the birth date, and last name from the employee data and search SIS's (student) data for a student ID. If a record is found, use the student ID to look for an existing LDAP entry yet again.
4. If still no LDAP entry has been found, use the last five digits of the user's SSN, the birth date, and last name from the employee data and search HRMS data for a related affiliate ID (affiliate affiliation). If a record is found, use the affiliate ID to look for an existing LDAP entry.
5. If still no LDAP entry has been found, use the last five digits of the user's SSN, the birth date, and last name from the employee data and search UREL data (another authoritative source of affiliates) for a related affiliate ID. If a record is found, use the affiliate ID to look for an existing LDAP entry.

The process described above is one example of the identity matching logic used by our current CalNet sync code.