

Identity and Access Management

James Alexander

Computing & Information Services

Oklahoma State University

Tina Meier PMP

Computing & Information Services

Oklahoma State University

Identity and Access Management

Managing identities and authorities is a major component to an information technology infrastructure. Knowing who some is and what authorities they have are vital to the system use and security. Keeping the information in sync within all the systems can be a time consuming and very labor intensive operation. Computing & Information Services at Oklahoma State University developed a universal directory of core identity and access information. The Universal Directory becomes the hub for identity and access updates, which then passes the information to systems managed by CIS. By implementing this infrastructure, CIS will improve the time to provide access system, update the information across all systems simultaneously and reduce the overhead in maintaining identities.

Introduction of the Organization

Oklahoma State University (OSU) consists of approximately 5,000 faculty and staff with 22,000 students. OSU has a main campus located in Stillwater, Oklahoma with four branch campuses throughout the state of Oklahoma. Computing & Information Services (CIS) at OSU is responsible for providing information technology and customer support for OSU, its branches and four other institutions under the OSU/A&M Board of Regents. CIS maintains the userids and passwords for over 168,000 people for the OSU/A&M system.

Problem/Initiative Statement

Managing identities and authorities is a major component to an information technology infrastructure. Each semester, 7,000 students are transitioned into Oklahoma State University along with several hundred faculty and staff. They need access to email, file/print services, course management systems, telephone service, library privileges, and student information system access to start their career at OSU. Knowing who some is and what authorities they have are vital to the system use and security. Several separate system administrators spend hundreds of hours setting up access and there is a time lag between start up and set up. Once the information gets into the system, the data gets out of sync and the individual has to maintain identity information in each system. Keeping the information in sync within all the systems can be a time consuming and very labor-intensive operation. Computing & Information Services (CIS) saw identity management to be a strategic asset to the organization. CIS developed a Universal Directory containing core identity and access information. The Universal Directory becomes the

hub for identity and access updates, which then passes the information to systems managed by CIS. The scope for this initiative is to create an environment for real-time identity management and maintenance for OSU/A&M constituents utilizing the Human Resources System, Student Information System and other sources deemed appropriate for granting access to OSU/A&M information technology. If information changes in one system, this information gets update in all other systems, real-time. This best practice will discuss the design and implementation of the Universal Directory at OSU.

Design & Implementation

The important components of the Universal Directory are data, the business logic, and infrastructure. Data for identity resides in several sources. At OSU, the Human Resources System (HRS) and the Student Information System (SIS) are the two main authoritative sources for data along with a web application to enter exception identity data. Examples of data captured are name, course and major information for students, and department information for employees. The data is pulled in order to make business decisions on what services and permissions to provide. The first attempt at OSU for a central data source was called Personal User Identification System (PUD). CIS has utilized PUD for the past seven years to create a common userid and default password. The issue with PUD is being a batch environment with a 48 to 72 hour time lag from the time information is entered into either system until a userid is created on a system.

With the Universal Directory, data is captured each evening during the same batch-processing window as HRS and SIS. Files are transferred to the Universal Directory

environment and the files are processed. This has the potential to decrease the set up time for each student and employee by 24 to 48 hours.

When PUD was implemented, roles were identified with the assistance of Human Resources and the Registrar's office. These roles provide different access to the university resources, which provides the business logic for programming purposes. The business logic or business rules are captured into Extensible Markup Language (XML) stylesheets to translate the XML data files outlined above. Based on a role or roles, access and permissions are assigned to an individual. If the individual's role changes based on new data from the authoritative systems, then their access changes in the systems. From a security standpoint, this provides for a clean method for exiting students and employees along with the daily up keep of system security.

OSU chose Novell's eDirectory as the core infrastructure due to its low cost and the Novell expertise already in-house. The software was available to OSU through its existing campus contract with Novell. Six servers costing approximately \$30,000 were purchased for the environment. To learn the XML technology, an on-site training course for the core team members. Even with the training, OSU has some complex business logic. CIS contracted with Novell to assist with the development of the stylesheets. This consulting engagement provided OSU with the needed boost to assist developers and to work closely with XML experts. This work relationship has proven to be very beneficial.

The project team spent a majority of their time testing the interfaces in a complete test environment. The test environment mirrored the production environment, so that they could understand what would happen once the interfaces were implemented.

The beauty of the Universal Directory is the ability to add systems in phases. CIS will have several phases to fully implement the entire capabilities of the Universal Directory. The first phase consisted of the Universal Directory and the card management system. This phase has been in production for several months and is working very well. The next phase will consist of the interfaces from the Universal Directory to the current Novell file/print environment, a new on-line White Pages directory, and a LDAP compatible environment for web application authentication. Other systems to be added in the near future are: Lotus Notes user ids, telephone directory, and course management system.

Benefits

The benefits are not only to the CIS staff, but each new student and employee. Productivity lost is being minimized. Students and employees have information resources available to them quicker. Over time, all systems CIS maintains will be covered under Universal Directory. Just a rough estimate of time costs saved in the first two phases is approximately \$40,000 per semester (\$10 per hour, save 8 hours lost productivity for 500 employees per semester). CIS also regains back ¼ System Administrator with the implementation of the file/print interface. These timesavings will continue with the additional of other systems.

Security is another benefit. With the consistent business rules, all roles receive the same permissions and access. Also, permissions are revoked in a consistent manner to insure the safety of the data once an individual leaves the university. System administrators recognize the benefits by not “guessing” what permissions to give and regaining user id maintenance time.

Retrospect

If we did this over again, there would be several things done differently. First of all, the research and training component would have been broken out into a separate project. The team learned the technology, completed training, developed and implemented all in the same project. This led to the perception that nothing was being done, which was far from the case. Another change would be setting up the test environment earlier in the process. This would have facilitated the learning process and accelerated the testing time involved in the project. For future phases, CIS will be looking at a single system instead of several in one project. The team’s focus was spread too thin and it was difficult finishing.

Identity management is a core component of information technology. CIS will continue leveraging the Universal Directory to become efficient at maintaining identities and authorities in the OSU information technology environment. This best practice provides an overview to begin the process of implementing identity management at any institution.