IDM/Active Directory Roadmap

Presented by
Chuck Phillips, Dilek Inal and Louis Sullo

Business Problem

- Provisioning, authentication, and authorization are not standard across campus. This causes problems such as
  - Lots of work to sync systems
  - System integrity challenges
Brief History of Account Management on Campus

- **IBM Mainframe (1970s)**
  - First system requiring "Management" of accounts via the User Number Clerk

- **Growth of UNIX on campus early 1990s**
  - Network Information Service or NIS (originally called Yellow Pages or YP)
  - Large growth of the number of accounts on large number of machines
  - Need for automated account management and synchronization

- **CCAT "Convenient Computer Access Today" was developed (1992-1993)**
  - Automated management of MVS, CMS, VMS and UNIX accounts.
  - Any user can have UNIX/Email account.

  - Installation of CorporateTime Calendar was the driving force.
  - Simple scripts were put in place to sync LDAP and UNIX accounts.

- **LAMB "LDAP Access Management Bundle" Was Born (2003)**
  - CCAT was demised
  - Real time provisioning of accounts
  - Real time synchronization of passwords between LDAP, Unix, Oracle.

- **PICES Was Spawned (2007)**
  - Provided structured way to provision directories across campus.

- **Enterprise Active Directory adopted (2008)**
  - Campus wide committee re-designed active directory structure and standards.

The Legacy

- The mainframe had an account length Limit of 8 characters for account.
- UNIX NIS (Network Information System) used single DES “Data Encryption Standard” encryption which only allowed 8 character passwords.
- Scripts to manage accounts were based on field length so increase of length was not addressed.
- Oracle passwords only allow _ and #.
Recent Milestones Reached

- Password Length Increased
  - Legacy length of 8 characters removed
  - Legacy limitation of 2 special characters removed
- IT LDAP to Active Directory Synchronization
  - Automatic creation of AD accounts.
  - Synchronization of passwords
  - AD Organizational structure based on department.

2010 Security Modifications

- Anonymous Access to LDAP Disabled
  - Reduces SPAM
  - Reduces attacks
- Failed Authentication Lockouts
  - Common across systems
**Desired Outcomes**

- Separate legal name from the public name in UNM systems
- Standardized rules for identifying people across UNM environments.
- Synchronization of these identities
- Manage the Identity Lifecycle
- Self-service management of identity and passwords

**2011 Goals**

1. Standardize and use ‘Display Name’ for online directory and email lookups. (By June 1)
2. Develop a way to provide users with a ‘Preferred’ email address. (Fall 2011)
3. Remove legacy 8 character limitation on UNM-IT NetID. (Winter 2011)
4. Standardize rules to create user names. (Winter 2011)
5. Implement Federation. (Fall 2011)
6. Directory Reconciliation (Winter 2011?)
Accomplishing the 2011 Goals

The IT Managers chartered the Identity Management Taskforce. This group defined the following aspects of this initiative, separate from the Active Directory project.

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Project Mgt</th>
<th>Team</th>
<th>Decision</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>IT</td>
<td>IT</td>
<td>IT</td>
<td>IT Agents, IT-UNM, IT Mgrs</td>
</tr>
<tr>
<td>Preferred E-mail @UNM</td>
<td>IT</td>
<td>IT, IDM Task Force</td>
<td>IT</td>
<td>&quot;</td>
</tr>
<tr>
<td>Grtr than 8-character NetID</td>
<td>IT</td>
<td>IT, IDM Task Force</td>
<td>IT</td>
<td>&quot;</td>
</tr>
<tr>
<td>NetID Creation Name Standards</td>
<td>HSLIC</td>
<td>IT, HSC, UNMH, UL, CARC, ASM</td>
<td>IT Mgrs</td>
<td>&quot; + KMIT</td>
</tr>
<tr>
<td>Federated ID</td>
<td>IT</td>
<td>IT, Legal</td>
<td>IT</td>
<td>&quot;</td>
</tr>
<tr>
<td>Directory Reconciliation</td>
<td>HSLIC</td>
<td>HSC, UNMH, IT</td>
<td>IT Mgrs</td>
<td>&quot; + KMIT</td>
</tr>
</tbody>
</table>

Preferred Display Name

- Demographic Self Service has been collecting ‘Display Name’ for years. However, it is only used for the online directory.
- Populating email servers with this value will enhance the ability to find users.
Preferred email address

- Users can have a professional email address without changing the way they authenticate.
- Separation of email address from NetID can be used to protect against attacks.
- Allows modifications to email address without changing authentication method.

Why Remove 8 character limitation?

- NetIDs are no longer being reused
- The flexibility of “good” 8 character NetIDs is being strained. i.e. amarti89
- Silos were created across campus because of this limitation.
- Removal of limitation will enable UNM to create standardized NetIDs on campus.
- The non IT scope of this change is unknown.
Account Creation Rules

- Zero day provisioning can be achieved.
- The preferred email and display name projects allow a user to manage their own outward identity separating their NetID from that identity.

Federation Mission

- Joining InCommon Federation
  - The mission of the InCommon Federation is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States....
  - InCommon is intended to enable production-level end-user access to a wide variety of protected resources.