How to Herd Cats
Managing IAM Roles and User Access
1. Lots of affiliations
2. Lots of possible systems of record
3. Lots of types of access to grant
Meet the Champion Cat Herders

1. Brett Bieber, Nebraska - faculty and staff
2. Ester Cha, Illinois - affiliate users
3. DePriest Dockins, Michigan - putting it all together with a vended solution
Nebraska’s Journey with Roles

Internal Audit is your friend

Find Key Stakeholders and prepare for battle

Remediating/Implementing (Unleash the data)
Audit Findings

“When any user terminates his or her relationship with the University of Nebraska, his or her ID and password shall be denied further access to computing resources.”

**Finding 1:**
Former employees have access 8-weeks longer than they should.

**Finding 2:**
Access is not being properly managed.
Audit Findings

- Letter of Offer
- HR Entry
- Job Start Date
- (movers)
- Job End Date
- Separation
- +8 Weeks
- Death

Out of Compliance

- Email
- Canvas/Blackboard
- Door Access

Faculty/Staff/Affiliate/Volunteer
Audit Findings

- Email
- Canvas/Blackboard
- Door Access

Faculty/Staff/Affiliate/Volunteer

- Letter of Offer
- HR Entry
- Job Start Date
- (movers)
- Job End Date
- Separation
- +8 Weeks
- Death
Identifying Key Stakeholders

Human Resources
- Director of Employee Relations

Academic Affairs
- Chief of Staff
- Chief Academic Business Officer

Business & Finance
- Security Coordinators
- Director of Business Systems

Information Technology
- Director IdM
- Enterprise Architect
Remediation Plans

Develop Communication Materials

Host Workshops with All Units
   HR representatives and IT representatives

New Tools/Reports
   Employees losing services in the next 65 days
   Temp/hourly workers that haven’t been paid in a while
   Deploy Grouper with helpful Reference Groups

Offboarding Checklist

Develop Onboarding/Offboarding Websites
Grouper: Unleashing the Data

People

Mary
John
Michael
Grouper: Unleashing the Data

Employee/Faculty/Staff/Affiliate

Organizational

People

Mary
John
Michael
Grouper: Unleashing the Data

Cat Herder Department

People
- Mary
- John
- Michael

Employee/Faculty/Staff/Affiliate

Organizational +
Grouper: Unleashing the Data

People
- Mary
- John
- Michael

Position/Job/Role
- Cat Herder
- Cat Analyst
- Cat Developer

Organizational +

Cat Herder Department
Employee/Faculty/Staff/Affiliate
Grouper: Unleashing the Data

People
- Mary
- John
- Michael

Position/Job/Role
- Cat Herder
- Cat Analyst
- Cat Developer

Relational
- Cat Herder Reports
- Cat Herder Team

Organizational + Cat Herder Department
- Employee/Faculty/Staff/Affiliate
Nebraska Grouper Examples

12345678

- ref:hr:employee [faculty|staff|affiliate|...]
- ref:hr:orgs:1000:employee [faculty|staff|affiliate|...]
- ref:hr:position:00001
- ref:hr:supervisor:00001
- ref:hr:team:00001

*Group IDs (GROUP_NAME) does not change.*
Nebraska Grouper Examples

Mary
 Employee  [Faculty|Staff|Affiliate|...]

Cat Herder Department - Employee  [Faculty|Staff|Affiliate|...]

Cat Herder (Position 00001 - Mary*)

Cat Herder’s Reports (Supervisor 00001 - Mary*)

Cat Herder’s Team (Position+Supervisor 00001 - Mary*’s Team)

*Group display name (GROUP_DISPLAY_NAME) reflects current position holder.
## Search results

### Search for:

- [unrelated] Brett Bieber

### Filter for:

- Everything

---

### Results:

<table>
<thead>
<tr>
<th>Folder</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNL : Reference : Human Resources : position</td>
<td>Mgr Identity Access Mgmt Programming (Position 00003276 - Brett Bieber)</td>
</tr>
<tr>
<td>UNL : Reference : Human Resources : position</td>
<td>OneIT (Position 00053804 - Brett Bieber)</td>
</tr>
<tr>
<td>UNL : Reference : Human Resources : team</td>
<td>Mgr Identity Access Mgmt Programming Team (Manager+Supervisor 00003276 - Brett Bieber’s Team)</td>
</tr>
<tr>
<td>UNL : Reference : Human Resources : team</td>
<td>OneIT Team (Manager+Supervisor 00053804 - Brett Bieber’s Team)</td>
</tr>
</tbody>
</table>

---

**Showing 1-5 of 5**  
First | Prev | Next | Last
Next Steps

Continue to replace manually maintained groups with automated entitlements

Develop a Grouper affinity cohort to support distributed IT

Loosen restrictions on viewing reference data

Scale out!
   Bring these tools to all University and State College Campuses
Current State

- Request application roles
- Manual access management
- Minimal record keeping
- Limited awareness of job changes

Future State

- Request business roles
- Automatic access management
- Audit-level records
- Automatic Notification on job changes

Consistent
Efficient
Secure
Phases of Identity and Access Management

Students

Affiliates

Staff

NetID Lifecycle

Creation/provisioning

Credentials and roles

Deprovisioning
If you’re not faculty, staff, or student, who are you?

I’m with an established program
I’m with an allied agency
I’m special!
Affiliates at the University of Illinois today

- **Established Affiliate Programs**
  - Osher Lifelong Learning Institute
  - Intensive English Institute
  - University High School
  - Chicago College of Medicine and Nursing students

- **“Allied” agencies**
  - Foundation
  - Alumni Association
  - AITS
  - Research Park
  - Other “allied” corporations

- **“Special”**
  - Visiting scholars
  - Vendors
  - Special programs
  - Research collaborators
  - Anyone else who doesn’t have a label
The problem(s) with affiliates

Affiliates (non-faculty/staff/students)

- Don’t have a streamlined onboarding process
  - Don’t exist in the University’s ERP
  - Numerous processes and persons involved
  - Onboarding takes several days to a week

- Have an incredibly diverse set of needs
  - Every unit is unique
  - Need access to a limited, but wide range of resources
  - Difficult to determine eligibility
  - Are often not defined in licensing requirements
Problem 1: Provisioning

Obtaining credentials can be a multi-day process - many potential points of delay
Problem 1: Provisioning

Sponsoring departments are responsible for distributing credentials in a “secure” manner.

Departments with savvy IT staff will set up local AD credentials or use other ad hoc processes.

Departments need to know what services to ask for.
Problem 2: Access Management (or lack thereof)

Affiliates are not well defined
- Service owners don't know who's who and whether they're eligible
- Many ad-hoc policies for non-standard groups
- Very little if no documentation on affiliate access

AuthZ is complicated
- Comprehensive understanding of all campus populations is specialized
- Often need nested or chained groups and policies
- AuthZ policies in practice become overgeneralized whitelists or blacklists
Solution part 1: Investigate

Identify the stakeholders
  - Campus units
  - Service owners/administrators
    - Central IT
    - Library
    - Gatekeepers
  - Affiliated programs/departments
  - Support staff

Engage
  - Actively listen
  - Gather requirements
  - Educate
Solution part 2: Redo

Streamline the netID provisioning process

Redefine affiliations and roles

Redesign the infrastructure for storing identity data for non-traditional users

Remove the middle people when distributing credentials
Redefining Affiliates

- AITS
- Alumni Association
- Foundation
- Visiting scholars
- Vendors
- Established Affiliate Programs
- Allied agencies
- Research Park
- Other
Requesting affiliate netIDs (future state)
Solution part 3: Support

Educate and train service owners/administrators

Simplify service provisioning

Provide tools for access management

GROUPER!

Documentation
Why not use social IDs or federate?

Social IDs
- Identity matching can become cumbersome
- Users can potentially have multiple identities that aren't linked
- Need to position the infrastructure first
- Don't have the resources yet to implement

Federation
- Not all affiliates are associated with other institutions
- Setting up federation for a single user is inefficient
- Getting SP admins to join InCommon is like herding cats
**Current State**

- Ad hoc methods for obtaining credentials
- Many players involved in multi-day process
- Passing of credentials from one person to another

**Future State**

- One-stop shop for all affiliates
- Single point of contact for unit & Automation
- Self-service application with elimination of middle man

**Consistent**

**Efficient**

**Secure**
What We Heard: **Key Pain Points & Needs**

*It is not clear: what access is needed to do a job, how to get the access, and what the requirements/dependencies are to get access.*

*It takes too long to get the proper access when starting a job.*

For transfers, employees end up with too much or too little access.

*I need the ability to grant access based on a specified time frame.*

*I need a complete view of a user's access: who has what access, why they have the access, and when they had access.*

*I need to easily audit and reconcile my employees’ access on a regular basis.*

**Ability to grant/revoke access using business roles**

**Streamline access workflows to remove manual steps and trigger notifications**

**Ability to specify date ranges for access**

**Improve auditing and reporting**

**Provide access control management at multiple levels**
Business Roles Are Automatically Assigned

HR Attribute Data

Institutional Role: Ann Arbor Staff
Job Code: 12346
Title: AP Invoice Processing Senior Associate
Dept: Shared Service Center
Business Roles Map to Entitlements

Then automated provisioning into PeopleSoft
Role & Access Management RFP Scope

ITS and Health ITS select an Identity Governance and Administration system that will support Role & Access Management for all U-M campuses, including Ann Arbor, Dearborn, Flint, and Michigan Medicine.

Establish a Role & Access Management Framework based on industry best practices

_The Role & Access Management solution must integrate with existing IAM solutions for both the University of Michigan and Michigan Medicine._
RFP Functional & Technical Evaluation Criteria

**Vendors**
- Deloitte / SailPoint
- Micro Focus
- Simeio / Saviynt

**Supplier Evaluation**
- Role Management
- Workflow
- Access Request Process
- Auditing & Reporting
- Integrations & Connectors

**Technical Standards Evaluation**
- Budget and Financial Evaluation
Role Access Management Deployment Options

Scenario 1

Michigan Medicine IAM

Campus IAM

Single RAM Instance

Scenario 2

Michigan Medicine IAM

Campus IAM

RAM Instance 1

RAM Instance 2

Scenario 3

Michigan Medicine IAM

Campus IAM

RAM Instance 1

RAM Instance 2

Scenario 4

Michigan Medicine IAM

Campus IAM

Single RAM Instance
Scenario #2 (Two Instances On-Premise)

Ideal solution based on current Business and Technical practices:
- Technical landscape across campus are not aligned (e.g. network topology)
- Business processes, operational processes and support models are not aligned (e.g. change management processes, compliance regulations, funding models)
- Single instance requires added resources, funding and campus leadership support

Vendors recommended on-premise solution to address performance and latency issues with a cloud based deployment, given the IAM systems are on-premise.

Per Michigan Medicine, higher confidence in meeting high-availability requirements.
Role and Access Management Pilot Participants

College of Engineering Door Access

PeopleSoft Procurement

UM-Dearborn Active Directory Roles
Roles Pilot Key Deliverables

Establish a governance structure to support new roles management practices

Enable report and analysis capabilities:
  - Identify and address application access risks like orphaned accounts or inappropriate access
  - Analyze the type of users who are accessing applications to identify opportunities automated provisioning, approval-based access, etc.)

Demonstrate the ability to maintain business roles for automating access provisioning/deprovisioning

Validating that our solution will support critical enterprise applications
Current State

- Request application roles
- Manual access management
- Minimal record keeping
- Limited awareness of job changes

Future State

- Request business roles
- Automated access management
- Audit-level records
- Automatic notification on job changes

Consistent
Efficient
Secure
Questions & Thanks
IAM Online Evaluation

https://www.surveymonkey.com/r/Feb2018IAMOnline
Upcoming Webinars

Wednesday, February 21, 2018
The Federation Doctor Will See You Now: Baseline Expectations Health Checks
2 pm ET | 1 pm CT | Noon MT | 11 am PT
https://spaces.internet2.edu/x/sALxBg
Brett Bieber, University of Nebraska-Lincoln
Nick Roy, Internet2

Wednesday, March 7, 2018
InCommon Baseline Expectations: The Business Value Explained --- It’s Not Just About Health Checks
2 pm ET | 1 pm CT | Noon MT | 11 am PT