MIDPOINT
AN ENTITY REGISTRY & PROVISIONING ENGINE

ERICA LOMAX
ANDY MORGAN

University Information and Technology

Oregon State University
What is midPoint?

Open Source Identity Management system

Built by Evolveum
Oregon State University

31,000 students

130 central IT FTE, 150 distributed IT FTE
OSU IAM

3 technical staff, 1 manager

80,000 active identities
Current IAM “System”

More than 15 years old!
Fine for employees and students
No longer meets campus needs
Pre-midPoint account environment

- Oracle
  - Banner
    - APPWORX JOBS
  - GYBONID (Identity Table)
  - ODS

Perl Scripts and CRON

Targets
- AD
- LDAP
- Google
- Unix Homedirs
- Legacy Cyrus Mailbox
Entity Registry as part of CSP?

Let’s Do It!

https://www.flickr.com/photos/bryndavies/3879077675/ CC by NC ND 2.0
CSP Project Goals

Implement midPoint registry
Replace account management scripts
Complete by Fall term 2018
Long term vision

- Oracle
  - Banner
  - ODS

- Ethos
- Grouper
- midPoint

- Targets
  - AD
  - LDAP
  - Google
  - Box
  - Office 365

Future Systems of Record
When man plans, God laughs
Staffing or lack thereof
timeline

CSP Kickoff Nov 2017
Built first midPoint dev Nov 2017
Midpoint training Feb 2018

Crisis timeline – 15 weeks to fall term, 18 weeks to TechEx
All the scope we left behind

Username generation
Legacy email creation
Home directory creation
Username changes
Attribute synchronization
Improved data integration with Banner
Revised CSP Project Goals

Implement midPoint registry
Replace AD, LDAP, and Google account
create and delete steps
Complete by Fall term 2018
Our revised goal environment

- Oracle
  - Banner
  - GYBONID (Identity Table)
  - ODS

- midPoint

- Perl Scripts and CRON

- Targets
  - AD
  - LDAP
  - Google
  - Unix Homedirs
  - Legacy Cyrus Mailbox
Terminology

User – an identity stored in midPoint
Resource – a connected system
Account – resource object
midPoint infrastructure

Terraform and Ansible

CentOS7 VMs

1 midPoint VM and 1 MariaDB VM

midPoint Spring-boot WAR
Isn’t CSP about containerization?

Campus plan - Architecture for containers in AWS

Challenges connecting to on-prem resources

TIER container wasn’t ready
Migrating to midPoint

You have existing accounts
midPoint has no users
Don't delete my accounts!!!
Migrating to midPoint

Start midPoint as read-only
Create Users
Add each target/downstream resource
Keep midPoint in sync with account management processes
Before Going Live

Run midPoint in read-only mode for a while until you are comfortable
Go Live!

Take a deep breath

Update your resource configs to enable C/U/D

Set Projection Policy to "relative"

STOP! Watch the logs to see what midPoint tries to do

Grant write to your midPoint service accounts
Are we in production?

NO
Outstanding Issues

Simple dev/test environment

Roles attempting to apply new account settings to existing accounts
Strict LDAP standards

Structural vs Auxiliary ObjectClass

Active Directory’s adherence to LDAP standards is lacking
Bugs!

AD dirsync token size (fixed for v3.9, which is not released)

Google connector broken in v3.8, not yet fixed
More Bugs!

LDAP INTEGER syntax

Listing accounts on a resource page fetches all accounts, fails on large numbers
Support

New to Internet2 and higher ed

Complexity!

Lacks a robust open source community
Support model?

Vendor models – Evolveum, Unicon

What does the community expect for support?

ACAMP session to discuss
References

OSU configs
https://github.com/OSU-IAM/midpoint-config

Ansible playbook
https://github.com/OSU-IAM/ansible-midpoint

midPoint home
https://evolveum.com/midpoint/about-midpoint/
<table>
<thead>
<tr>
<th>Name</th>
<th>Given name</th>
<th>Family name</th>
<th>Full name</th>
<th>Email</th>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>10235524039</td>
<td>John</td>
<td>Smith</td>
<td>John Smith</td>
<td><a href="mailto:john.smith@email.com">john.smith@email.com</a></td>
<td>3</td>
</tr>
<tr>
<td>10235528427</td>
<td>Emily</td>
<td>Johnson</td>
<td>Emily Johnson</td>
<td><a href="mailto:emily.johnson@email.com">emily.johnson@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235526850</td>
<td>Tony</td>
<td>Williams</td>
<td>Tony Williams</td>
<td><a href="mailto:tony.williams@email.com">tony.williams@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235526999</td>
<td>George</td>
<td>Davis</td>
<td>George Davis</td>
<td><a href="mailto:george.davis@email.com">george.davis@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235526723</td>
<td>Jane</td>
<td>Brown</td>
<td>Jane Brown</td>
<td><a href="mailto:jane.brown@email.com">jane.brown@email.com</a></td>
<td>3</td>
</tr>
<tr>
<td>10235530176</td>
<td>Sarah</td>
<td>White</td>
<td>Sarah White</td>
<td><a href="mailto:sarah.white@email.com">sarah.white@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235530259</td>
<td>Tom</td>
<td>Stewart</td>
<td>Tom Stewart</td>
<td><a href="mailto:tom.stewart@email.com">tom.stewart@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235530648</td>
<td>Paul</td>
<td>Smith</td>
<td>Paul Smith</td>
<td><a href="mailto:paul.smith@email.com">paul.smith@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235530661</td>
<td>Mary</td>
<td>Johnson</td>
<td>Mary Johnson</td>
<td><a href="mailto:mary.johnson@email.com">mary.johnson@email.com</a></td>
<td>3</td>
</tr>
<tr>
<td>10235531422</td>
<td>David</td>
<td>Brown</td>
<td>David Brown</td>
<td><a href="mailto:david.brown@email.com">david.brown@email.com</a></td>
<td>3</td>
</tr>
<tr>
<td>10235531846</td>
<td>Alex</td>
<td>Williams</td>
<td>Alex Williams</td>
<td><a href="mailto:alex.williams@email.com">alex.williams@email.com</a></td>
<td>3</td>
</tr>
<tr>
<td>10235531752</td>
<td>Lisa</td>
<td>Smith</td>
<td>Lisa Smith</td>
<td><a href="mailto:lisa.smith@email.com">lisa.smith@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235532227</td>
<td>Robin</td>
<td>Johnson</td>
<td>Robin Johnson</td>
<td><a href="mailto:robin.johnson@email.com">robin.johnson@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235532016</td>
<td>James</td>
<td>Smith</td>
<td>James Smith</td>
<td><a href="mailto:james.smith@email.com">james.smith@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235532107</td>
<td>Emily</td>
<td>Davis</td>
<td>Emily Davis</td>
<td><a href="mailto:emily.davis@email.com">emily.davis@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235532453</td>
<td>Lisa</td>
<td>White</td>
<td>Lisa White</td>
<td><a href="mailto:lisa.white@email.com">lisa.white@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235533923</td>
<td>Sarah</td>
<td>Johnson</td>
<td>Sarah Johnson</td>
<td><a href="mailto:sarah.johnson@email.com">sarah.johnson@email.com</a></td>
<td>3</td>
</tr>
<tr>
<td>10235534039</td>
<td>Mary</td>
<td>Smith</td>
<td>Mary Smith</td>
<td><a href="mailto:mary.smith@email.com">mary.smith@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10235534406</td>
<td>Emily</td>
<td>Davis</td>
<td>Emily Davis</td>
<td><a href="mailto:emily.davis@email.com">emily.davis@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>1023553581</td>
<td>Lisa</td>
<td>White</td>
<td>Lisa White</td>
<td><a href="mailto:lisa.white@email.com">lisa.white@email.com</a></td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>Connector type</td>
<td>Version</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AD</td>
<td>com.evolveum.polygon.connector.idap.ad.AdlDapConnector</td>
<td>1.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYBONID</td>
<td>org.identityconnectors.datatable.DatabaseTableConnector</td>
<td>1.4.2.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ONID LDAP</td>
<td>com.evolveum.polygon.connector.idap.IdapConnector</td>
<td>1.6-string1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Display name</td>
<td>Identifier</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approver</td>
<td></td>
<td></td>
<td>Role authorizing users to make approval decisions on work items.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base ONID</td>
<td></td>
<td></td>
<td>Assigns the LDAP and AD ressources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delegator</td>
<td></td>
<td></td>
<td>Role authorizing users to delegate their own privileges to any other user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End user</td>
<td></td>
<td></td>
<td>Role authorizing end users to log in, change their passwords and review assigned accounts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td></td>
<td></td>
<td>Creates an account in the Google resource and assigns appropriate Google attributes in LDAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IAM Service API</td>
<td></td>
<td></td>
<td>Allows service access to midPoint API</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewer</td>
<td></td>
<td></td>
<td>Role authorizing users to make decisions on certification cases.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Superuser</td>
<td></td>
<td></td>
<td>Role that gives user full authorization in MidPoint.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unix</td>
<td></td>
<td></td>
<td>Assigns Posix attributes in LDAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Category</td>
<td>Object reference</td>
<td>Execution</td>
<td>Executing at</td>
<td>Progress</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>Cleanup</td>
<td>System</td>
<td></td>
<td>Rannable</td>
<td>0</td>
<td>212291</td>
</tr>
<tr>
<td>LiveSync AD</td>
<td>Live synchronizatio n</td>
<td>AD</td>
<td>Rannable</td>
<td>69793</td>
<td></td>
</tr>
<tr>
<td>LiveSync GYBONID</td>
<td>Live synchronizatio n</td>
<td>GYBONID</td>
<td>Rannable</td>
<td>65659</td>
<td></td>
</tr>
<tr>
<td>LiveSync LDAP</td>
<td>Live synchronizatio n</td>
<td>ONID LDAP</td>
<td>Rannable</td>
<td>325003</td>
<td></td>
</tr>
<tr>
<td>Reconcile AD</td>
<td>Reconciliation</td>
<td>AD</td>
<td>Rannable</td>
<td>84205</td>
<td></td>
</tr>
<tr>
<td>Reconcile GYBONID</td>
<td>Reconciliation</td>
<td>GYBONID</td>
<td>Running</td>
<td>DefaultNode</td>
<td>78664</td>
</tr>
<tr>
<td>Reconcile LDAP</td>
<td>Reconciliation</td>
<td>ONID LDAP</td>
<td>Rannable</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Trigger Scanner</td>
<td>System</td>
<td></td>
<td>Rannable</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Validity Scanner</td>
<td>System</td>
<td></td>
<td>Rannable</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>