Deploying Commercial Identity Systems in Higher Ed

Dominic Sanchez

THE UNIVERSITY OF CHICAGO

Andy Morgan & Jason Peak

Oregon State University

Background

University of Chicago

- 29,000 students
- 23,000 employees
- 238,000 accounts
- 270,000 active identities
- 7 IAM staff

Oregon State University

- 35,000 students
- 8,700 employees
- 100,000 accounts
- 500,000 identities
- 3 IAM staff

Similar Projects

University of Chicago

- Cirrus Bridge and Okta first, new identity system later
- Retire ODSEE LDAP

Oregon State University

- New identity system first, Cirrus Bridge and Azure SSO later
- Retire ODSEE LDAP

UChicago Commercial Identity Software

- Okta as IDP
- Cirrus Bridge as proxy IDP for apps not migrated to Okta and for federated apps (InCommon + eduGAIN)

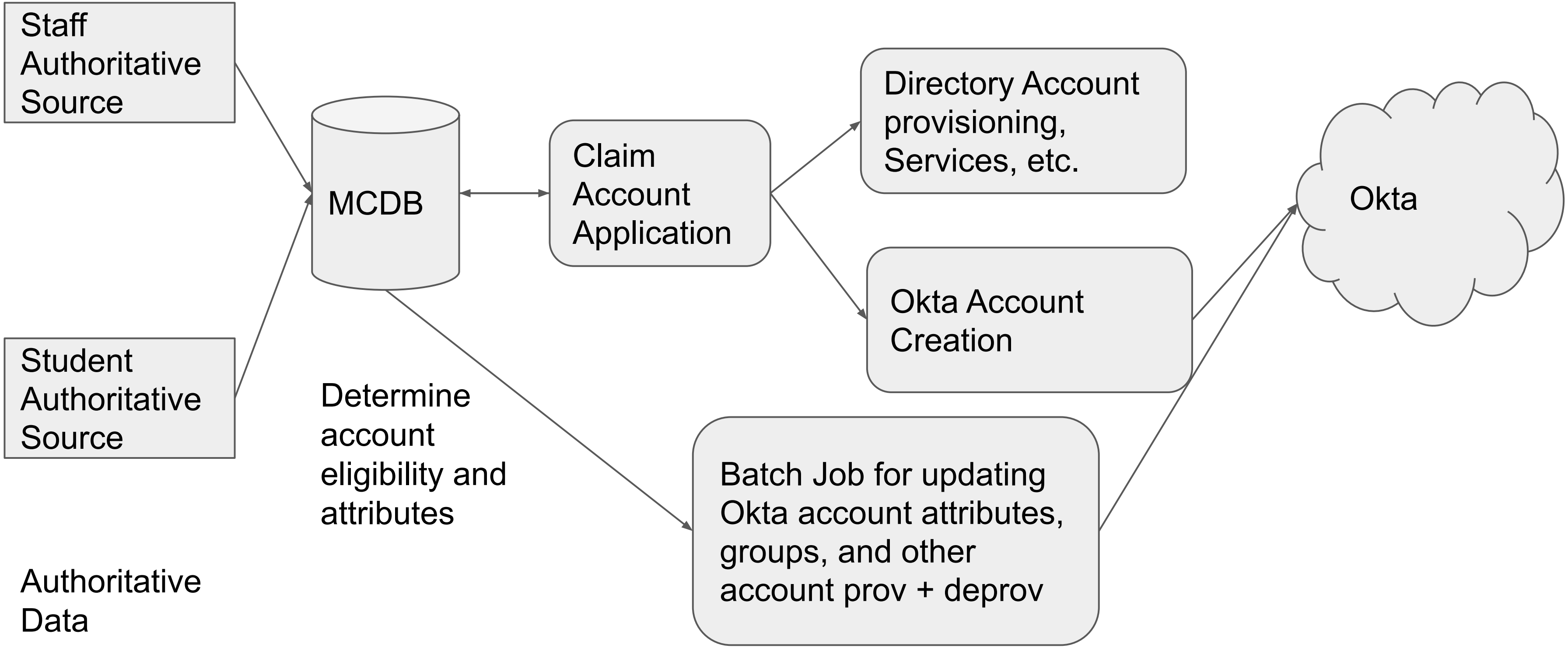
Why Deploy Okta + Cirrus Bridge in Higher Education

- Less overhead/maintenance for IDP as we use Okta as a cloud service
- Increased operational efficiency from an app integration standpoint
- Allow us to still use federated services with the Cirrus Bridge and more time for other services to migrate to our Okta instance as a proxy layer
- Service provisioning/deprovisioning possibilities within Okta for future work
- Easier logging/auditing

Commercial software is not perfect - Lessons learned

- UChicago’s attribute/profile requirements did not fit or work in Okta’s standard practices
- Some SPs could not work w/Okta being a proxy IDP or the Cirrus Bridge
- Setting up the Cirrus Bridge on the Okta side takes some effort, YMMV

UChicago Account + Claim Backend Implementation w/Okta



Staff Authoritative Source

Student Authoritative Source

Authoritative Data

MCDB

Determine account eligibility and attributes

Claim Account Application

Directory Account provisioning, Services, etc.

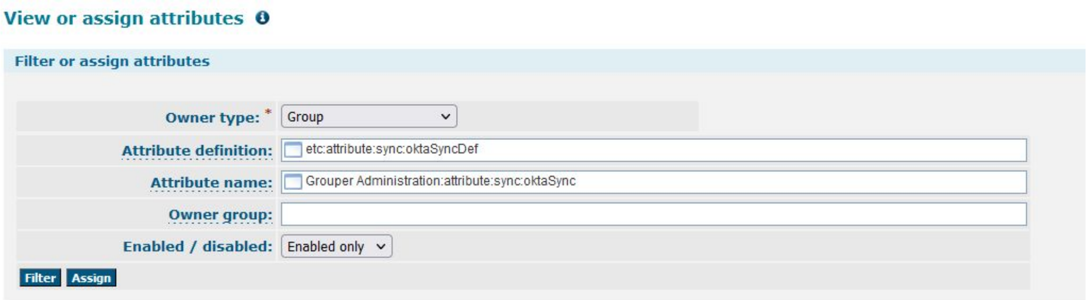
Okta Account Creation

Batch Job for updating Okta account attributes, groups, and other account prov + deprov

Okta

How does this software fit with InCommon TAP components?

- Grouper groups are utilized for Okta application access with custom attribute



View or assign attributes

Filter or assign attributes

Owner type: * Group

Attribute definition: etc:attribute:sync:oktaSyncDef

Attribute name: Grouper Administration:attribute:sync:oktaSync

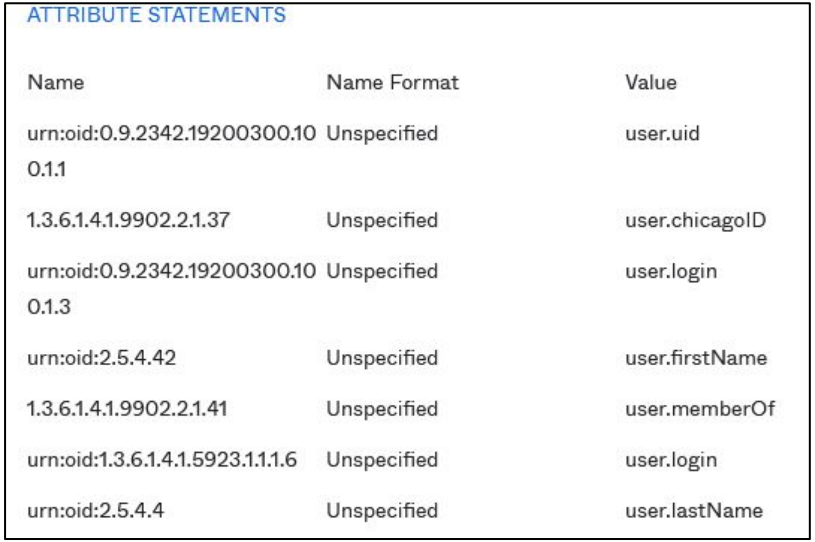
Owner group:

Enabled / disabled: Enabled only

- Shibboleth is used for apps that are not migrated to Okta via IDP SAML proxy

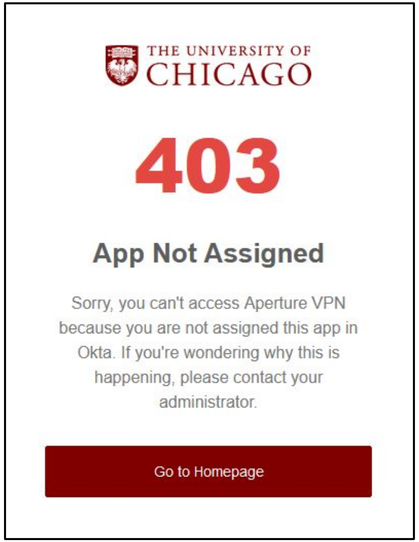
Native Okta SAML App Implementation Example

- Like a Shibboleth integration, except with more copy + paste
- Almost mandatory group assignment



ATTRIBUTE STATEMENTS

Name	Name Format	Value
urn:oid:0.9.2342.19200300.100.1.1	Unspecified	user.uid
1.3.6.1.4.1.9902.2.1.37	Unspecified	user.chicagoID
urn:oid:0.9.2342.19200300.100.1.3	Unspecified	user.login
urn:oid:2.5.4.42	Unspecified	user.firstName
1.3.6.1.4.1.9902.2.1.41	Unspecified	user.memberOf
urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Unspecified	user.login
urn:oid:2.5.4.4	Unspecified	user.lastName



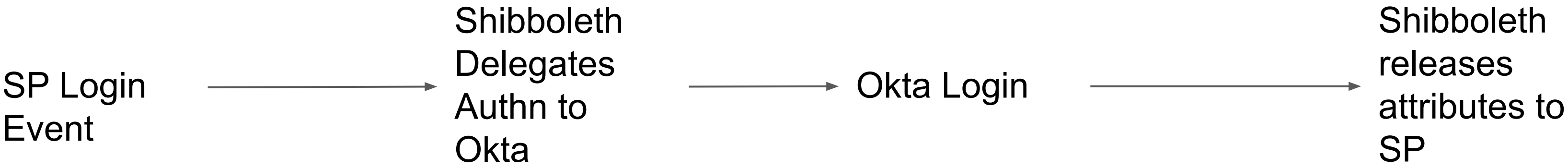
THE UNIVERSITY OF CHICAGO

403

App Not Assigned

Sorry, you can't access Aperture VPN because you are not assigned this app in Okta. If you're wondering why this is happening, please contact your administrator.

Okta Implementation Phase 1 - SAML Proxy (Current)

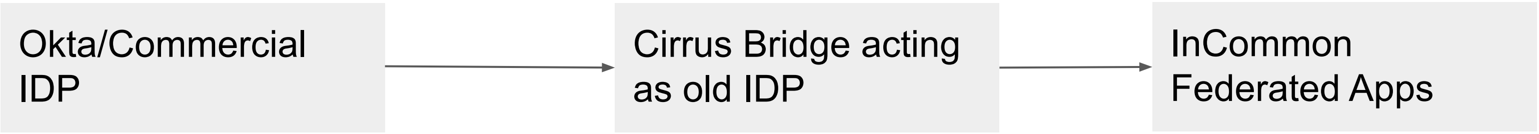


SP Login Event → Shibboleth Delegates Authn to Okta → Okta Login → Shibboleth releases attributes to SP

Legacy Shibboleth

What is the Cirrus Bridge?

- Essentially another SAML proxy for InCommon/eduGAIN (and more) but for commercial/enterprise IDPs
- AWS hosted



Okta/Commercial IDP

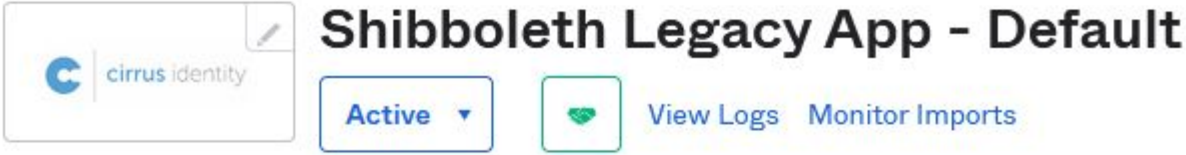
Cirrus Bridge acting as old IDP

InCommon Federated Apps

Attribute/NameID/Assertion configuration

Cirrus Identity Bridge Setup Part 1 (For Federation)

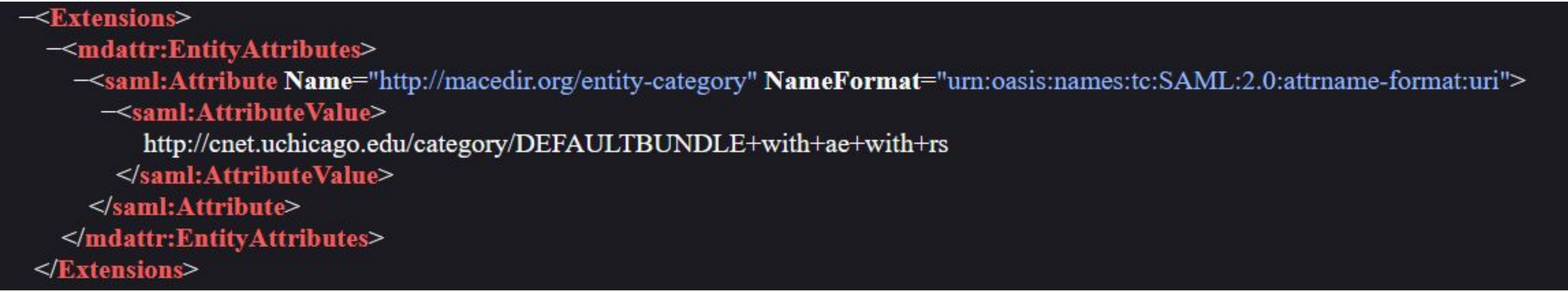
1. Provide Cirrus our IDP metadata
2. Create group in Okta for bridge use and give Cirrus the ID
3. Create Okta service account for bridge use
4. Create an application for InCommon Federated Applications



Shibboleth Legacy App - Default

Cirrus Identity Bridge Setup (Shibboleth Retirement) Part 1

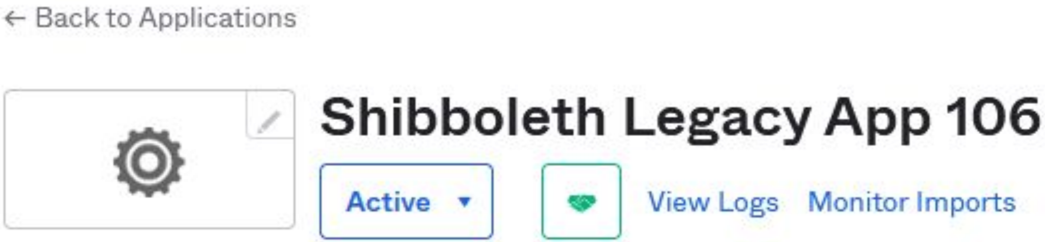
- Provide entity category tagged metadata aggregate to Cirrus
- Had to build a program to tag these according to an arbitrary pattern



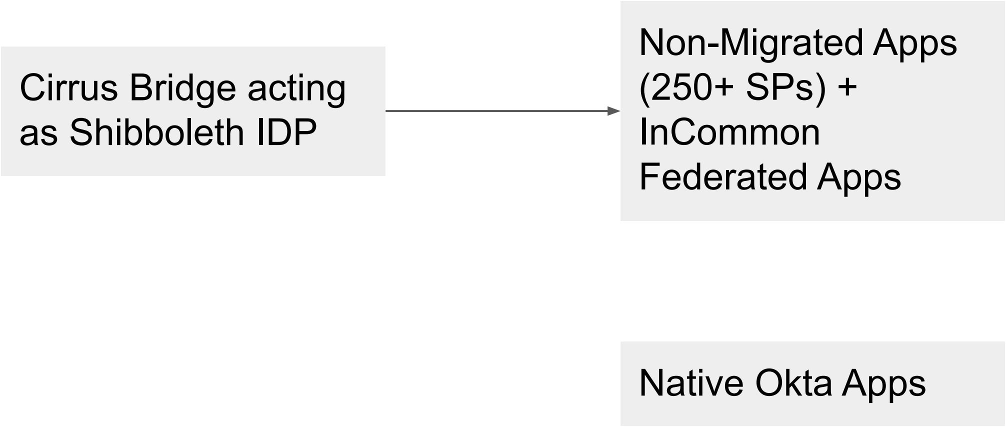
```
-<Extensions>
  -<mdattr:EntityAttributes>
    -<saml:Attribute Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      -<saml:AttributeValue>
          http://cnet.uchicago.edu/category/DEFAULTBUNDLE+with+ae+with+rs
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
```

Cirrus Identity Bridge Setup (Shibboleth Retirement) Part 2

1. Create Okta service account for Okta Application Management
2. Create Okta apps programmatically with service account and assign to users



Okta Implementation Phase 2 - Cirrus Identity Bridge



Cirrus Bridge acting as Shibboleth IDP

Non-Migrated Apps (250+ SPs) + InCommon Federated Apps

Native Okta Apps

Where are we with Okta and Cirrus Bridge?

- Okta deployment is complete/live and is working well
- Cirrus Bridge staged
- We need to migrate some problematic SPs and update one application

Oregon State University

Building a new identity system

Why Change?

- Improve security
- Expand IAM capabilities

Zero-Trust at OSU

Access decisions based on:

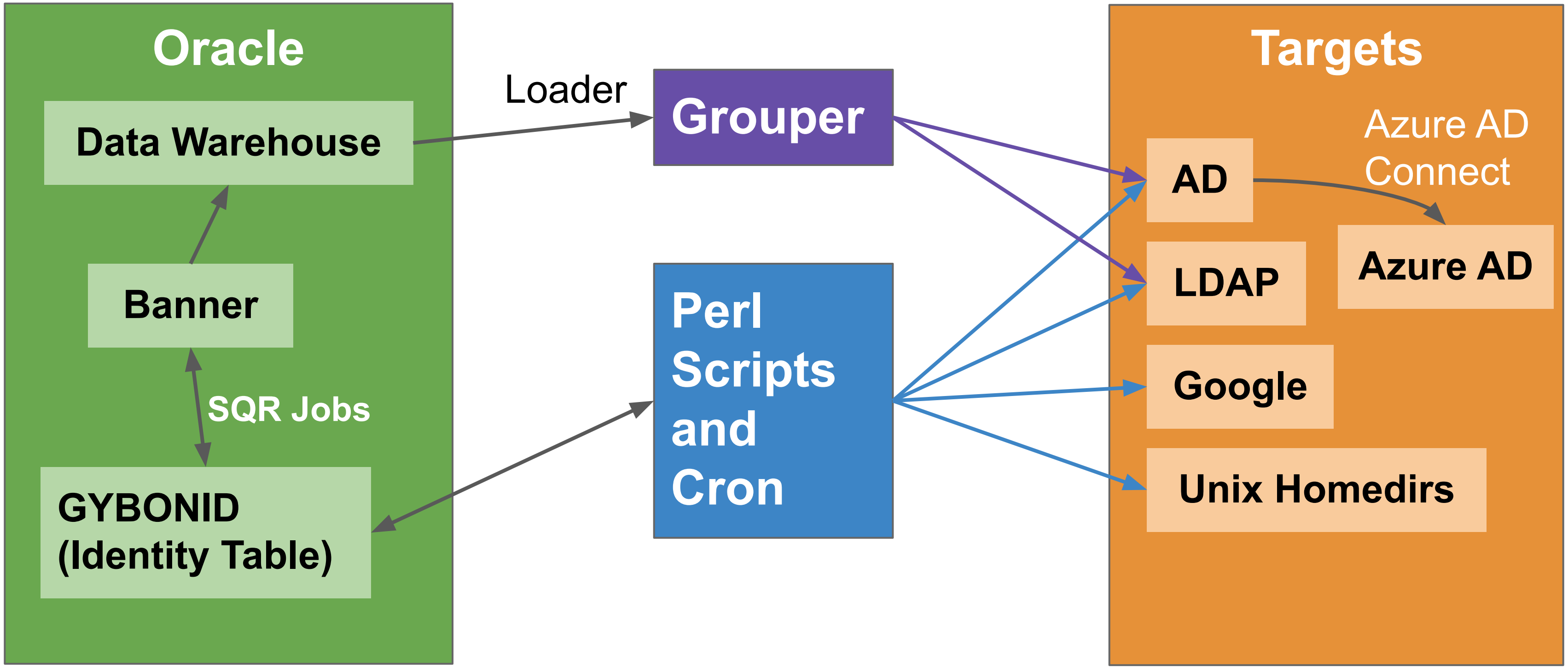
- who (identity)
- what (device)
- where (location)
- data (application)

Begins with Identity!

OSU’s Current Identity System

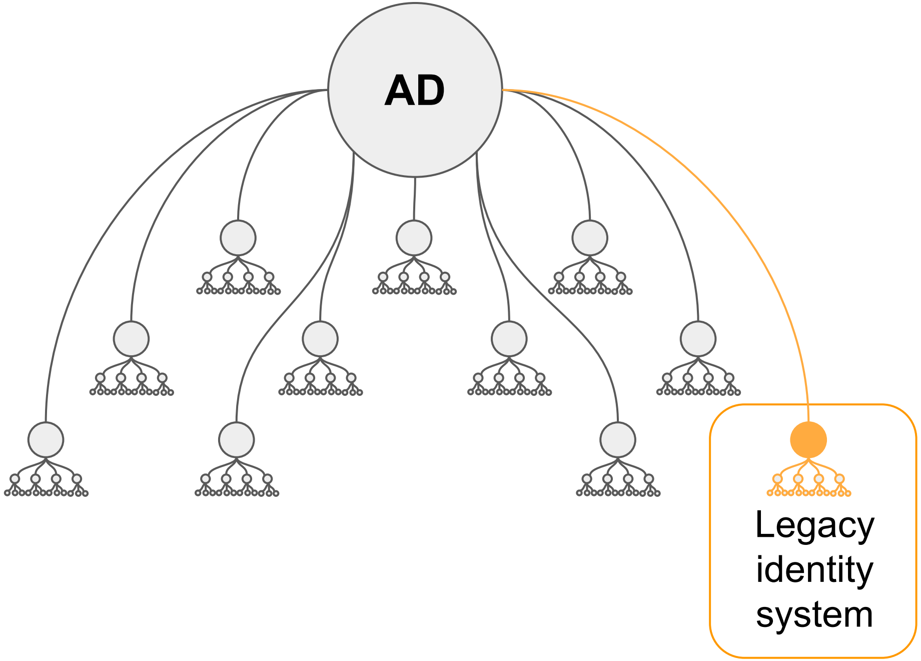
- Home-grown
- No separation between identities and accounts
- Batch updates every 2 hours
- Hard to customize

Current Environment



Unmanaged AD Accounts

- 11 domains
- One managed domain
- Thousands of manually-created accounts



Moving Forward (Maturing IAM at OSU)

- Read multiple Systems of Record
- Achieve real-time processing
- Manage all of AD
- Improve Access Control
- Governance

We need better tools!

Hello, IGA.

What’s an IGA?

Identity Governance and Administration

- Collects data about people from Authoritative Data Sources
- Manages identities for people (and things)
- Provisions accounts (AD, AAD, applications with user stores)
- Manages access (group memberships or directly in applications)
- Automatically provisions access based on roles and attributes
- Provides visibility - who has access to what

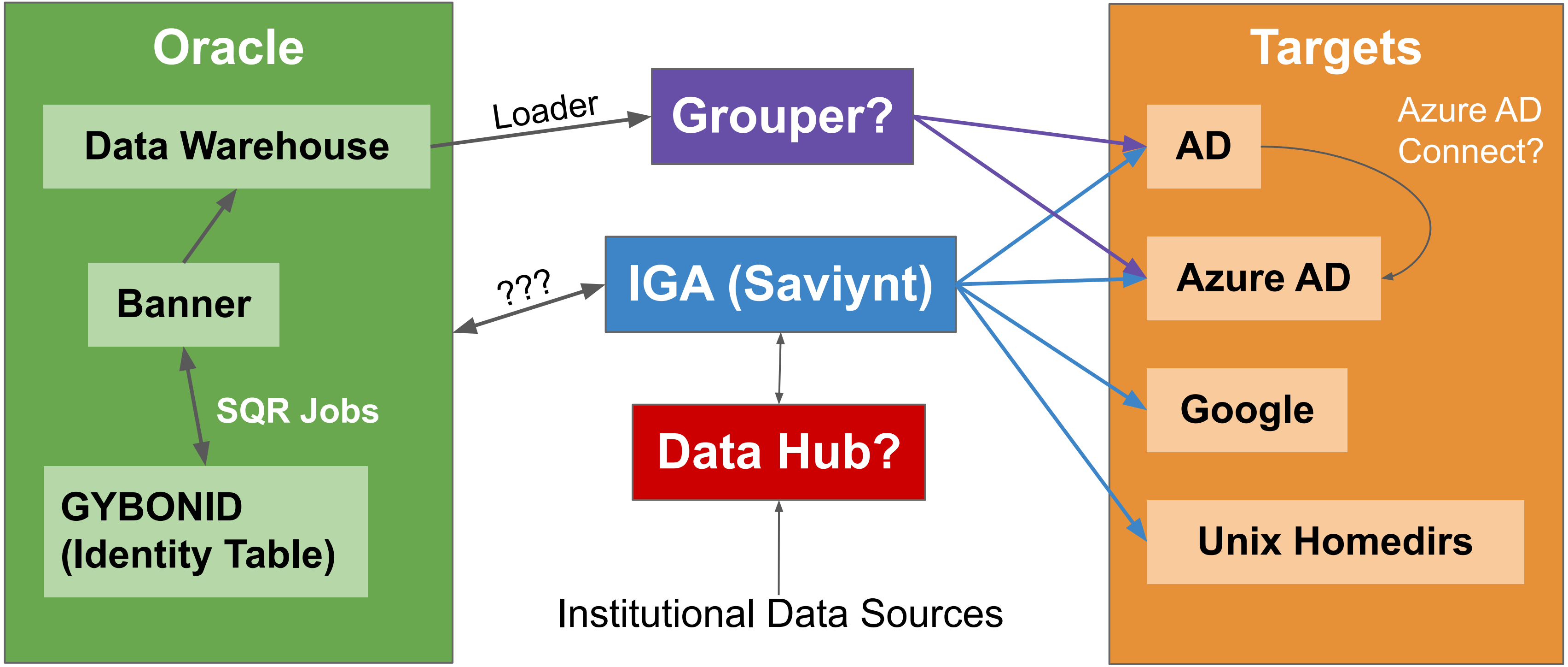
RFP Result

Saviynt

+

Grant Thornton

Future Environment?



Implementation Plan

Phase 1

- Replace legacy identity system with Saviynt by 30 June 2023

Phase 2

- Integrate additional core applications by November 2023

Phase 3

- Develop enterprise roles and access request workflows by December 2023

Where Are We Now?

Not as far as we'd like, but…

- Kickoff week - Done!
- Requirements gathering
- IGA training underway

Lessons Learned So Far

- Understand your current environment
- Determine the capabilities you need
- Use a phased approach - don’t try to implement everything at once
- Contracts and licensing are time-consuming and annoying (obviously)

Why Not Deploy an Open-Source Solution? (1)

- Have limited personnel
- SaaS / cloud / hosted solutions:
  - Very little infrastructure to manage
  - Application upgrades and security patching
- More separate applications/tools needed for open-source
- Can be faster to buy software than develop software
- Paid support contract with SLA
- More advanced skills may be needed for open-source

Why Not Deploy an Open-Source Solution? (2)

- Need Zero-Trust capabilities:
  - Evaluate device status (patch level, screen lock, biometrics, etc.)
  - Check location (impossible travel, unfamiliar location, etc.)
- Have Microsoft already…
  - Use Microsoft Azure Conditional Access
  - Microsoft “machine” to detect anomalies

Why Not Deploy an Open-Source Solution? (3)

Prevailing winds

- C-suite preference for software with an SLA
- “Clicks not code”, “low-code”, or “no-code”
- Open-source solutions underrepresented in RFP process

Acknowledgements

- Cirrus Identity Team
  - Mark Rank
- UChicago IAM Team
  - Dave Langenberg (Manager)
  - Blair Christensen (Lead)
- OSU IAM Team
  - Chris Evans
  - Michelle Lewis (Manager)
  - Erica Lomax (former Director)

THE UNIVERSITY OF CHICAGO

Oregon State University

QUESTIONS