INTERNET2

2022 TECHNOLOGY exchange

Wolverine vs. Grouper

PRESENTERS:
Liam Hoekenga, Sr. Application Developer, University of Michigan
Gail Lift, Lead Application Developer, University of Michigan
Bruce Timberlake, Sr. Systems Administrator, University of Michigan

INTERNET2

Table of Contents

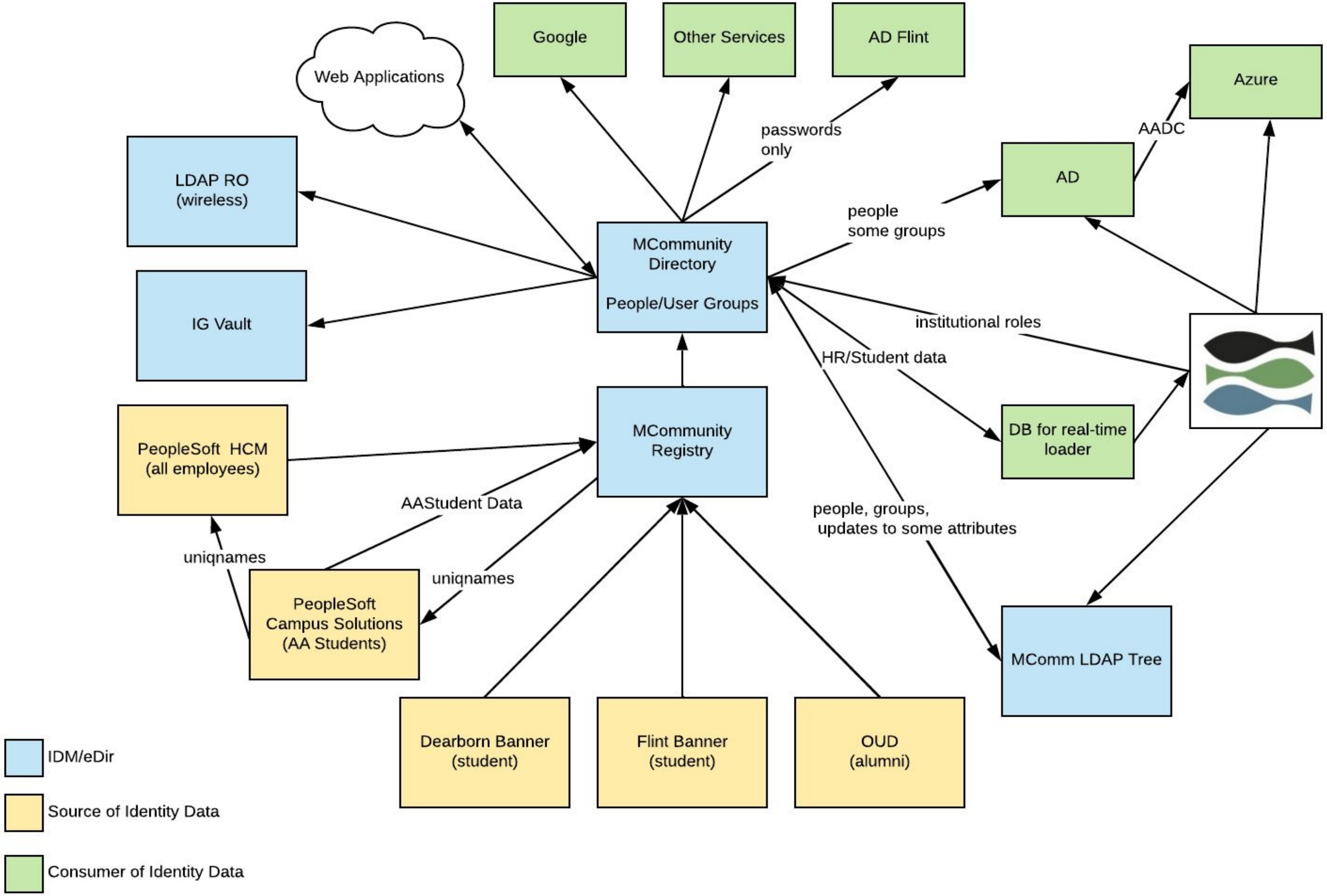
- Michigan Environment Background
- New Provisioning Framework
- ABAC
- Future collaboration topics
- Q&A

University of Michigan IT Environment Background

U-M Environment Background

- 19 colleges, 9 professional schools
- 3 regional campuses (Ann Arbor, Flint, Dearborn)
- Michigan Medicine (medical schools, hospital)
- Peoplesoft, Banner, Blackbaud

- MCommunity (NetIQ eDirectory/Identity Manager + in-house J2EE web apps)
  - 1.4 million identities, 650k active "people" (including alumni)
  - Aggregator of Peoplesoft/Banner/alumni source data
  - Subject source for Grouper



Web Applications

Google

Other Services

AD Flint

Azure

LDAP RO
(wireless)

IG Vault

MCommunity
Directory

People/User Groups

passwords
only

AD

AADC

people
some groups

institutional roles

HR/Student data

DB for real-time
loader

PeopleSoft HCM
(all employees)

MCommunity
Registry

AAStudent Data

uniqnames

uniqnames

PeopleSoft
Campus Solutions
(AA Students)

people, groups,
updates to some attributes

MComm LDAP Tree

Dearborn Banner
(student)

Flint Banner
(student)

OUD
(alumni)

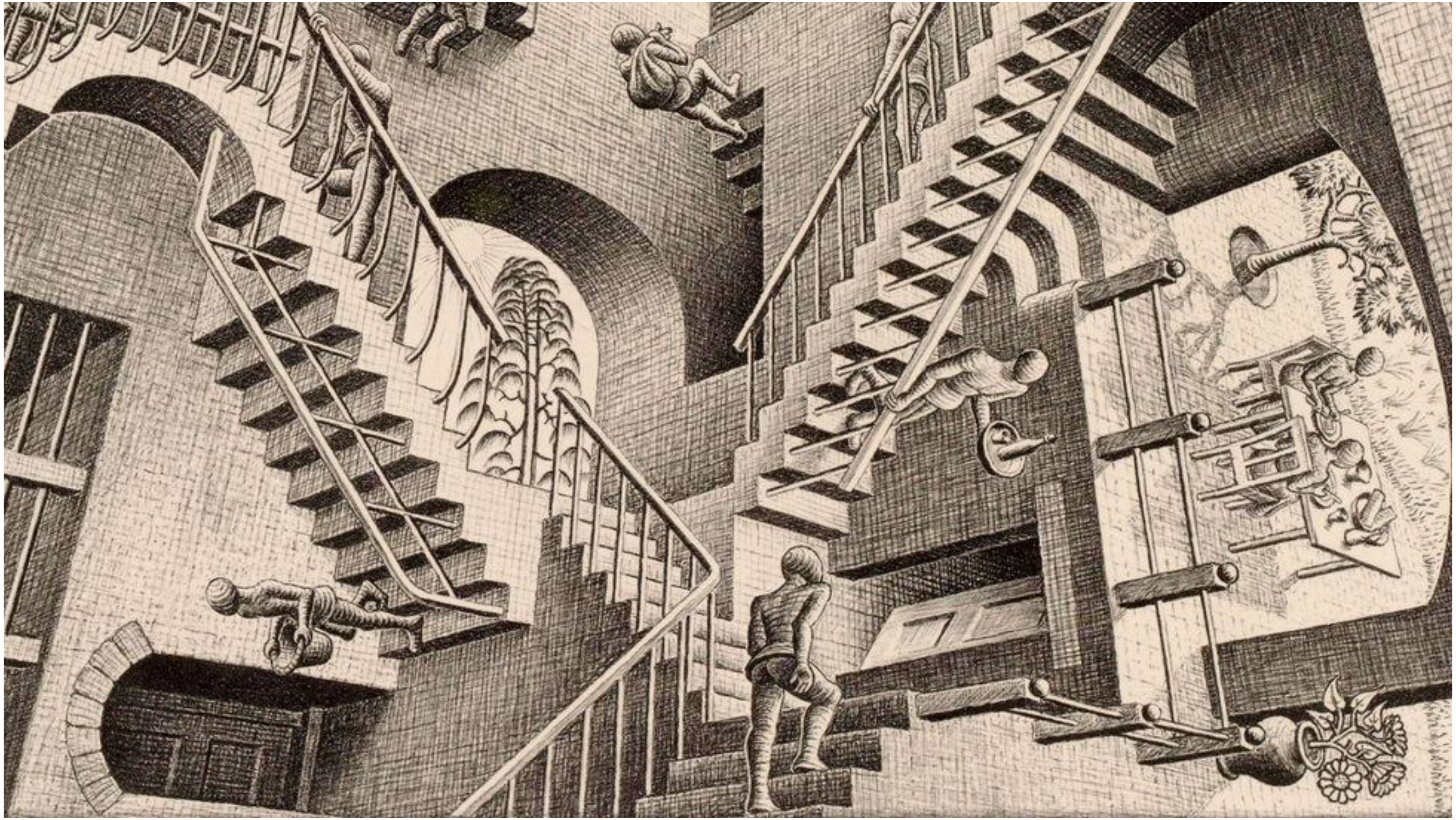
🟦 IDM/eDir

🟨 Source of Identity Data

🟩 Consumer of Identity Data

U-M Environment Background

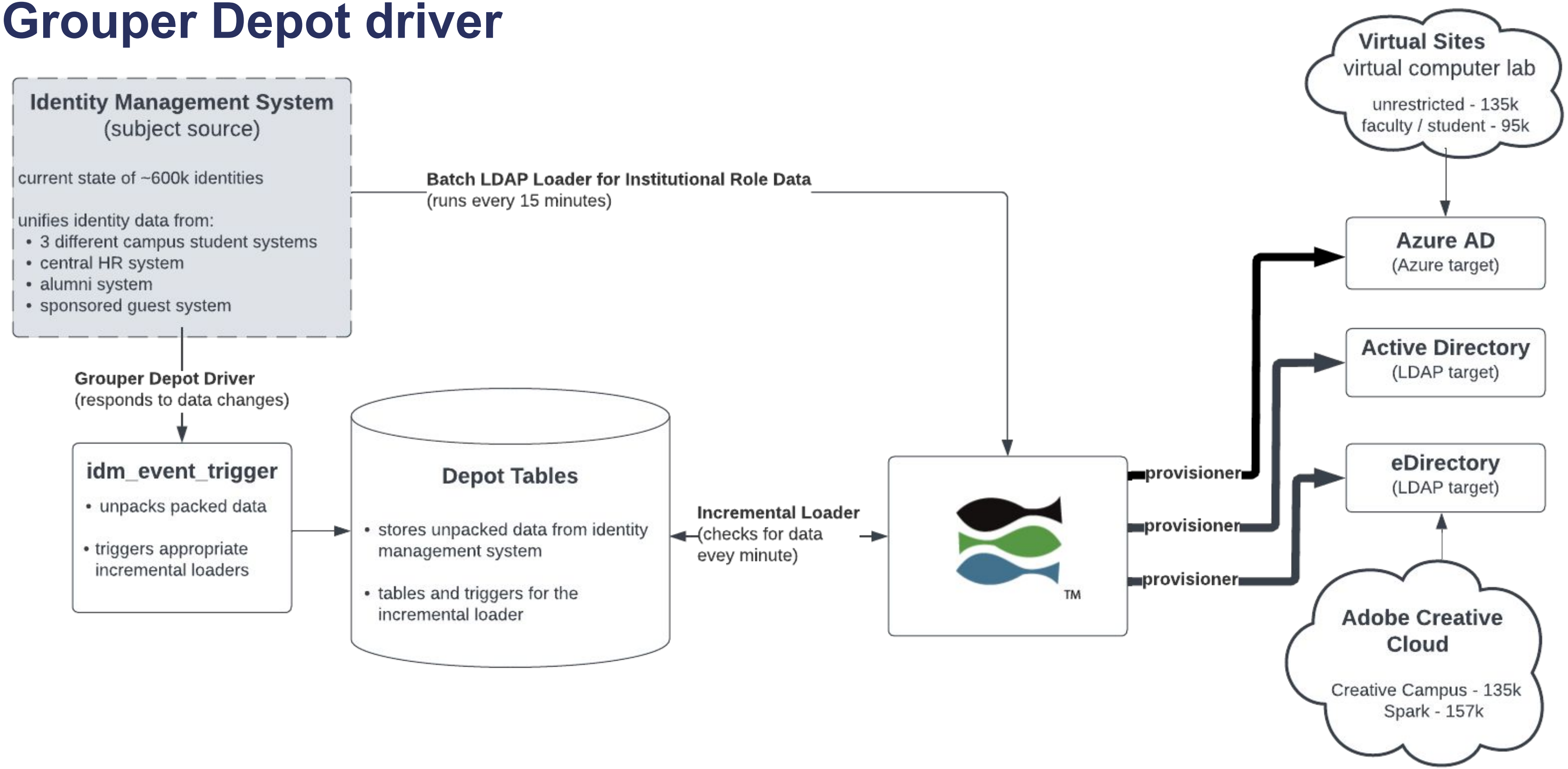
- Starting in the late 1990s, home-built "white pages" application allowed anyone to make groups
- Originally intended for mail groups, morphed to business use for access control
- Now we have
  - 97,000+ "all purpose" groups in MCommunity
  - 57,000+ groups in Active Directory
  - growing number synced to Azure from AD and from Grouper
  - various groups synced to cloud services (Google, Dropbox, Slack)



Provisioning Challenges

- Existing group solutions have been in place for decades
- Decentralized IT
- Grouper is not in charge of everything
  - Needs to co-exist with AD and MCommunity groups that are created/managed in different ways

Grouper Depot driver



Identity Management System
(subject source)

current state of ~600k identities

unifies identity data from:
- 3 different campus student systems
- central HR system
- alumni system
- sponsored guest system

Batch LDAP Loader for Institutional Role Data
(runs every 15 minutes)

Grouper Depot Driver
(responds to data changes)

idm_event_trigger
- unpacks packed data
- triggers appropriate incremental loaders

Depot Tables
- stores unpacked data from identity management system
- tables and triggers for the incremental loader

Incremental Loader
(checks for data evey minute)

Virtual Sites
virtual computer lab
unrestricted - 135k
faculty / student - 95k

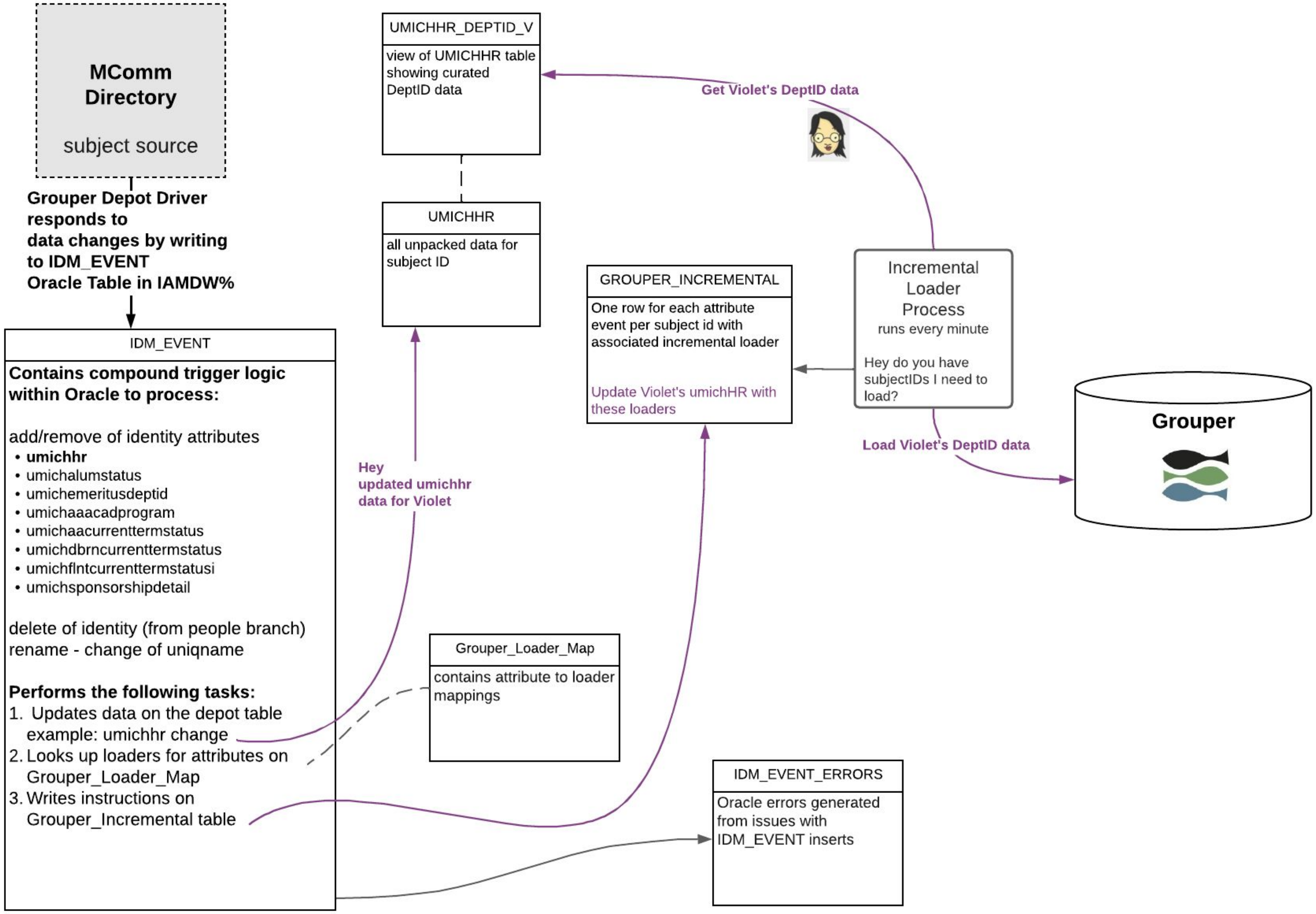
Azure AD
(Azure target)

Active Directory
(LDAP target)

eDirectory
(LDAP target)

Adobe Creative Cloud
Creative Campus - 135k
Spark - 157k

Getting HR details to Grouper: Grouper Depot driver



MComm Directory

subject source

Grouper Depot Driver responds to data changes by writing to IDM_EVENT Oracle Table in IAMDW%

IDM_EVENT

Contains compound trigger logic within Oracle to process:

add/remove of identity attributes

- **umichhr**
- umichalumstatus
- umichemeritusdeptid
- umichaaacadprogram
- umichaacurrenttermstatus
- umichdbrncurrenttermstatus
- umichflntcurrenttermstatusi
- umichsponsorshipdetail

delete of identity (from people branch)
rename - change of uniqname

Performs the following tasks:

1. Updates data on the depot table example: umichhr change
2. Looks up loaders for attributes on Grouper_Loader_Map
3. Writes instructions on Grouper_Incremental table

UMICHHR_DEPTID_V

view of UMICHHR table showing curated DeptID data

UMICHHR

all unpacked data for subject ID

Hey updated umichhr data for Violet

Grouper_Loader_Map

contains attribute to loader mappings

GROUPER_INCREMENTAL

One row for each attribute event per subject id with associated incremental loader

Update Violet's umichHR with these loaders

Incremental Loader Process

runs every minute

Hey do you have subjectIDs I need to load?

Get Violet's DeptID data

Load Violet's DeptID data

Grouper

IDM_EVENT_ERRORS

Oracle errors generated from issues with IDM_EVENT inserts

New Provisioning Framework

INTERNET2

2022

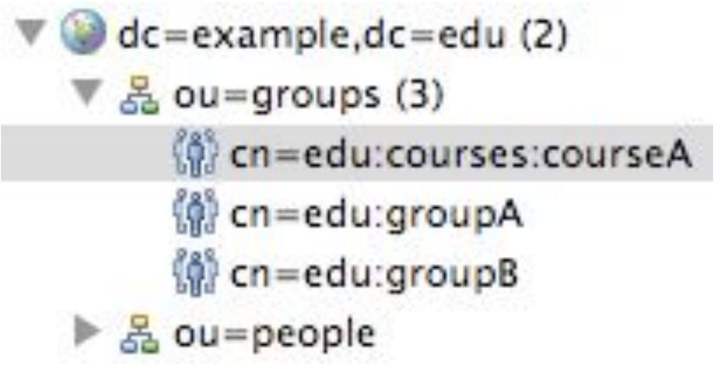
TECHNOLOGY

exchange

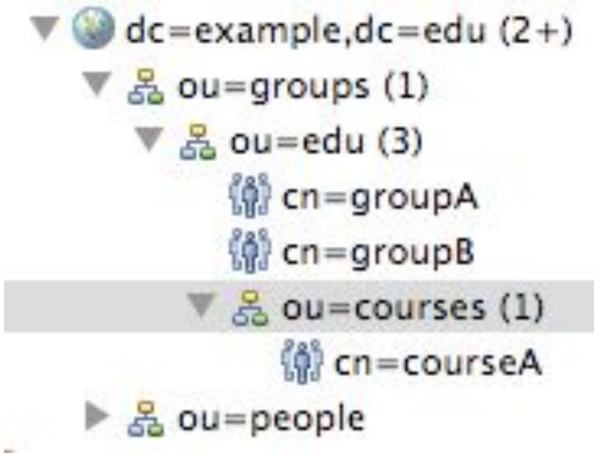
Provisioning

- "Start with"
- Provisioners have consistent features and configuration
- Provisioners re-use external systems
- New provisioners can be easily implemented in Java

Provisioning: Flat vs Bushy



```
▼ dc=example,dc=edu (2)
  ▼ ou=groups (3)
      cn=edu:courses:courseA
      cn=edu:groupA
      cn=edu:groupB
  ▶ ou=people
```



```
▼ dc=example,dc=edu (2+)
  ▼ ou=groups (1)
    ▼ ou=edu (3)
        cn=groupA
        cn=groupB
      ▼ ou=courses (1)
          cn=courseA
  ▶ ou=people
```

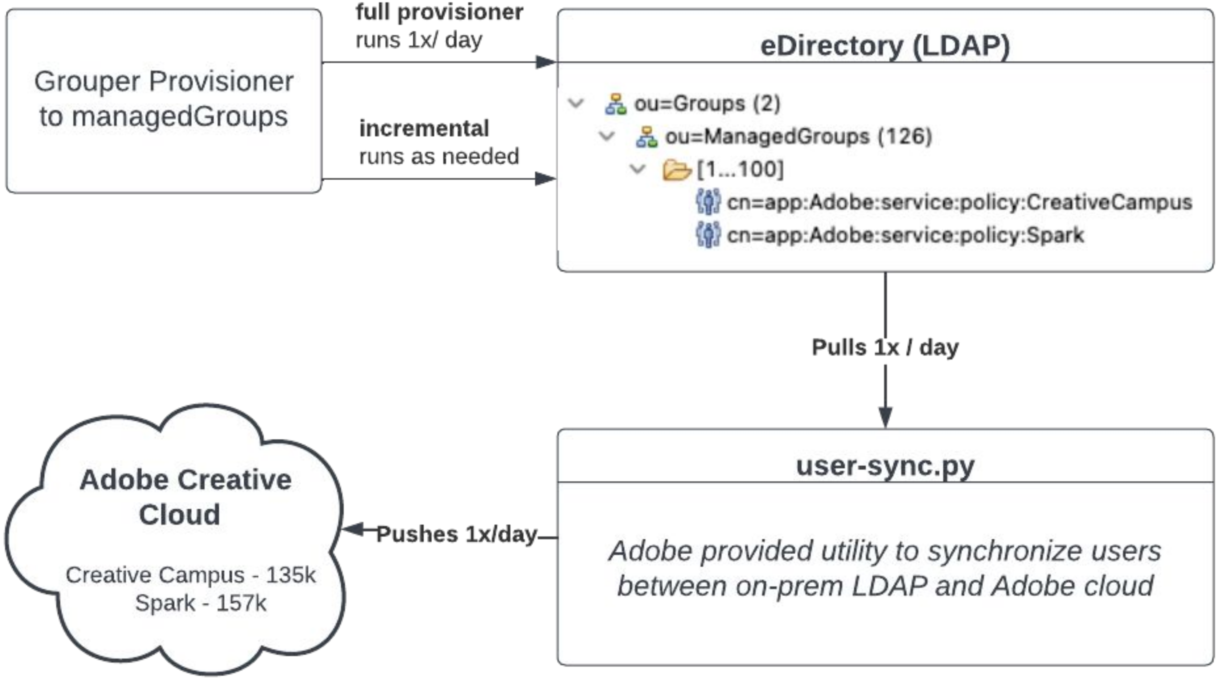
Flat provisioning

Embeds grouper hierarchy in the cn

```
cn=app:Adobe:service:policy:Spark,ou=ManagedGroups,
    ou=Groups,dc=umich,dc=edu
```

- connection to Grouper group easy to see
- less likely to hit dn length limit
- more likely to hit cn length limit
- less likely to confuse someone searching for a cn in `ou=Groups`
- if using GDG recommended hierarchy, may want to prevent `cn=org:blah:org:blahblah...`

Flat naming: Adobe use case



Grouper Provisioner to managedGroups

full provisioner runs 1x/ day

incremental runs as needed

eDirectory (LDAP)

- ou=Groups (2)
  - ou=ManagedGroups (126)
    - [1...100]
      - cn=app:Adobe:service:policy:CreativeCampus
      - cn=app:Adobe:service:policy:Spark

Pulls 1x / day

user-sync.py

Adobe provided utility to synchronize users between on-prem LDAP and Adobe cloud

Pushes 1x/day

Adobe Creative Cloud

Creative Campus - 135k
Spark - 157k

Bushy LDAP provisioning

Matches Grouper hierarchy

```
cn=Flint_AD_Student,ou=policy,ou=service,ou=ActiveDirectory,
    ou=app,OU=Grouper,DC=umflint,DC=edu
```

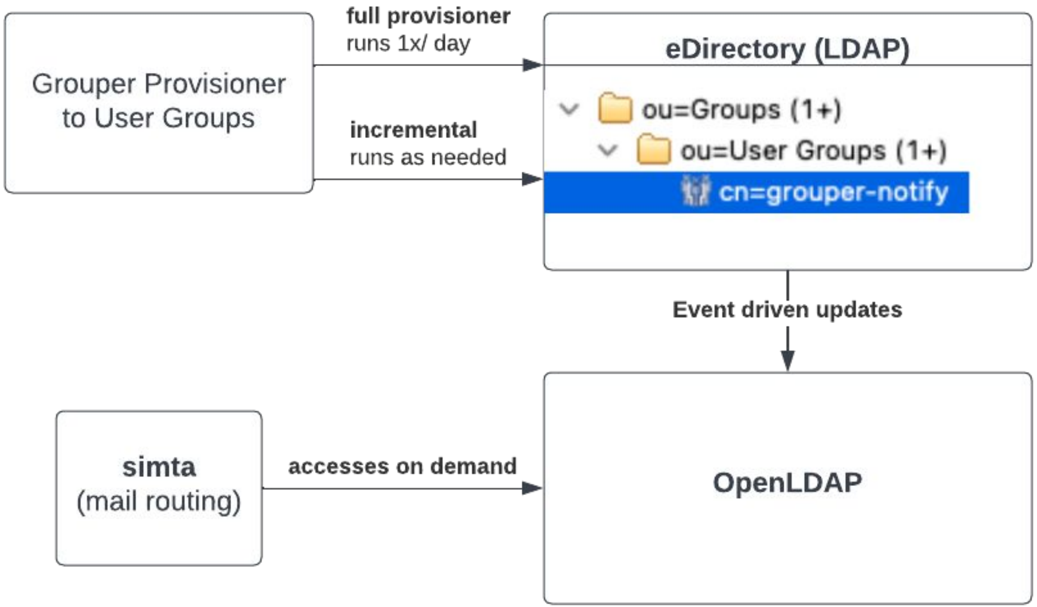
- keeps the cn short -- avoids 60 or 64 character limit
- easy for IT pros to understand
- can automatically omit top of Grouper hierarchy
- searching for a cn in `ou=Groups` might return unexpected results
- deep hierarchies might hit a dn length limit -- typically 255 characters

Specified name (DN override)

```
cn=OVPR All Staff,ou=User Groups,
    ou=Groups,dc=umich,dc=edu
```

- easy to make a readable name
- can map to existing group -- avoid having to change references to name or SID/gid
- easy to avoid dn or cn length limits
- person (or GSH template?) needs to set the name
- need to prevent overwriting existing groups in the LDAP target

DN override use case: AD & MCommunity



Grouper Provisioner to User Groups

full provisioner
runs 1x/ day

incremental
runs as needed

eDirectory (LDAP)

ou=Groups (1+)

ou=User Groups (1+)

cn=grouper-notify

Event driven updates

OpenLDAP

simta
(mail routing)

accesses on demand

Provisioning

- As framework features have grown, the number of config options have also grown. Don't get overwhelmed though!
  - UI improvements have been added to show/hide sections (for example)
  - Developers have provided 1-on-1 help to migrate configurations
  - As usage increases, community knowledge and documentation/ examples will improve too
- able to adjust multithreading
- able to control whether provisioner inspects the entire target (we do not want to inspect Azure device groups)

Attribute-Based Access Control (ABAC)

Current Reference groups

We have this HR information for each appointment:

- department with hierarchy
- faculty/regular staff/temp staff
- jobcode and jobfamily (job classification)
- active / on leave / retired
- primary / secondary job
- supervisor

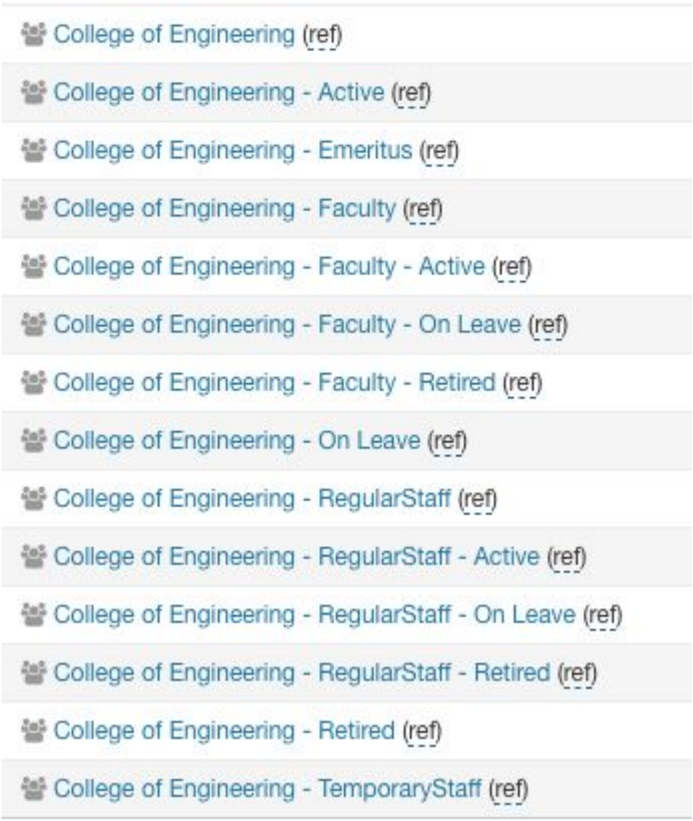
As stored in our IAM system (LDAP):

```
{jobCategory=Faculty}:{campus=UM_ANN-ARBOR}:{deptId=183000}:
{deptGroup=COLLEGE_OF_LSA}:{deptDescription=LSA Mathematics}:
{deptGroupDescription=College of Lit, Science & Arts}:
{deptVPArea=PRVST_EXC_VP_ACA_AFF}:{jobcode=201000}:{jobFamily=10}:
{emplStatus=A}:{regTemp=R}:{supervisorId=}:{tenureStatus=TEN}:{jobIndicator=P
}
```

HR Reference groups

HR groups by
- department
- department group (college level)
- vp area

17584 HR reference groups



College of Engineering (ref)

College of Engineering - Active (ref)

College of Engineering - Emeritus (ref)

College of Engineering - Faculty (ref)

College of Engineering - Faculty - Active (ref)

College of Engineering - Faculty - On Leave (ref)

College of Engineering - Faculty - Retired (ref)

College of Engineering - On Leave (ref)

College of Engineering - RegularStaff (ref)

College of Engineering - RegularStaff - Active (ref)

College of Engineering - RegularStaff - On Leave (ref)

College of Engineering - RegularStaff - Retired (ref)

College of Engineering - Retired (ref)

College of Engineering - TemporaryStaff (ref)

That’s very nice, but . . .

“I need teaching faculty separated from library faculty”

custom loader?

That’s very nice, but . . .

“I need teaching faculty separated from library faculty”
custom loader?

“I need GSIs separated from the rest of regular staff”
another custom loader?

That’s very nice, but . . .

“I need teaching faculty separated from library faculty”
custom loader?

“I need GSIs separated from the rest of regular staff”
another custom loader?

“Why does temp staff include students?”
and another custom loader?

That’s very nice, but . . .

“I need teaching faculty separated from library faculty”
custom loader?

“I need GSIs separated from the rest of regular staff”
another custom loader?

“Why does temp staff include students?”
and another custom loader?

“I need all supervisors in my unit, but not those who only supervise temps”
😟 is this going to scale?

New Grouper feature

Grouper attribute based access control with scripted groups

Now

- Reduces pre-loaded rollups that might not be used
- You don't need a loader job for each one of these groups
- Any Grouper user could edit the policies if they can READ underlying groups. You can have a UI to help build it and give good error messages
- This solves the issue of composites with any number of factors

Future work:

- The memberships of the ABAC groups are near real time
- Could visualize the policies.

How ABAC will work

HR data table:

subject_id	Category	deptId	deptGroup	job code	job Family	Status	reg/ Temp
Maize	Faculty	183000	COLLEGE_OF_LSA	201000	10	A	R
Maize	Staff	183000	COLLEGE_OF_LSA	106000	28	A	R
Blue	Faculty	465000	SCHOOL_SOCIAL_WORK	202800	13	W	R
Blue	Staff	191250	COLLEGE_OF_LSA	026200	33	A	T
Blue	Faculty	171900	COLLEGE_OF_LSA	202820	13	A	R
Wolverine	Staff	183000	COLLEGE_OF_LSA	101907	210	A	R

How ABAC will work

HR data table:

subject_id	Category	deptId	deptGroup	job code	job Family	Status	reg/ Temp
Maize	Faculty	183000	COLLEGE_OF_LSA	201000	10	A	R
Maize	Staff	183000	COLLEGE_OF_LSA	106000	28	A	R
Blue	Faculty	465000	SCHOOL_SOCIAL_WORK	202800	13	W	R
Blue	Staff	191250	COLLEGE_OF_LSA	026200	33	A	T
Blue	Faculty	171900	COLLEGE_OF_LSA	202820	13	A	R
Wolverine	Staff	183000	COLLEGE_OF_LSA	101568	210	A	R

How ABAC will work

HR data table:

subject_id	Category	deptId	deptGroup	job code	job Family	Status	reg/ Temp
Maize	Faculty	183000	COLLEGE_OF_LSA	201000	10	A	R
Maize	Staff	183000	COLLEGE_OF_LSA	106000	28	A	R
Blue	Faculty	465000	SCHOOL_SOCIAL_WORK	202800	13	W	R
Blue	Staff	191250	COLLEGE_OF_LSA	026200	33	A	T
Blue	Faculty	171900	COLLEGE_OF_LSA	202820	13	A	R
Wolverine	Staff	183000	COLLEGE_OF_LSA	101907	210	A	R
Bigbluebus	Staff	686000	PRKG_TRANSPRT_SRVS	153027	225	A	R

Grouper ABAC

- Add a Grouper config to describe your data, add user-friendly field names, etc.
- Set up a changelog for changes in your data.
- Give group admins some examples of how to use the data in group criteria
- Get rid of reference groups that no one will ever use

Collaboration Topics

Collaboration Topics

- Web services
- New provisioners
- GSH templates to assist with target group setup/naming
- Decentralized use cases
  - Denodo

Developer Engagement

- It has been extremely beneficial for U-M to have direct engagement with the Grouper developers
  - Bug fixes
  - Feature requests
  - Azure provisioner in 2.6.18 reduced full provision time from 45 minutes to 15!
- You need to be on the latest version, so start planning your upgrades now!

Questions?

Thank you!