midPoint in the Cloud
at UC Merced

John Kamminga - IdM Architect
Nick Dugan - Deputy CIO
Colin Thompson - DevOps AWS
How did we get here?

1. Migrated off Sun’s old Waveset.

2. Currently running interim homegrown IdM system.

3. Our plan is to move to the cloud using the TIER platform.
CURRENT IDM

midPoint

IDM ADMIN TOOL

ABILITY TO
PRE-CREATE
EMPLOYEE

AFFILIATE /
GENERIC (IDM)

REST END POINT

REST END POINT

OUTLOOK
DOMAIN LOGINS

UC APPS O365

CAMPUS APPS

APPLICANT /
STUDENT (SIS)

EMPLOYEE
(PPS/UCPATH)

IDM LOADER
ID MATCH
CONVERTED JAVA
CODE

IDENTITY MANAGEMENT
PERSON REGISTRY
ORACLE DATABASE

ODS
OPERATIONAL
DATASTORE

ACCESS MANAGEMENT

ACTIVE
DIRECTORY/ LDAP

SHIBBOLETH
CAS

MIM
(GROUP MGT)

CAMPUS CARD

PHYSICAL
ACCESS
Partnering with Unicon

1. Setup SSO in midPoint with Shibboleth IdP.

2. Setup REST endpoints in midPoint to expose user data for our IdClaim and Password reset Angular pages.
midPoint SSO

application.yml

saml:
  keystorePath:
  keystorePassword:
  privateKeyPassword:
  identityProviderMetadataPath:
  maximumAuthenticationLifetime:
  serviceProviderEntityId:
  serviceProviderMetadataPath:
  forceServiceProviderMetadataGeneration:
  callbackUrl:
  wantAssertionsSigned:
  usernameAttribute:
application.yml

spring:
mail:
port: 443
host: ucmerced.edu
username: rest
password: <pwd>
protocol: smtp
test-connection: true
What’s next?