2023 INTERNET2 TECHNOLOGY exchange

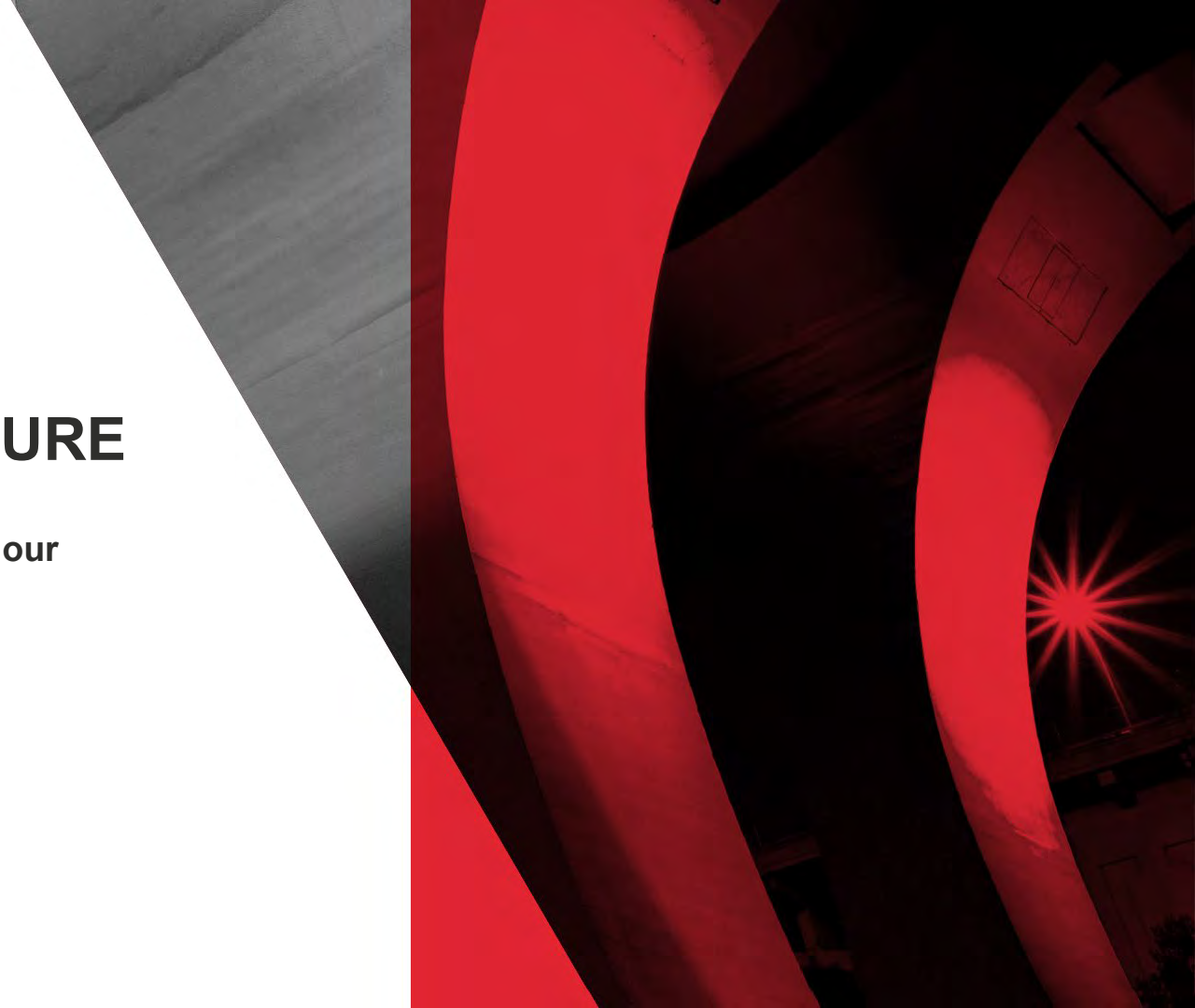
Can Your API Do This?
Cloud APIs and SSO

Leveraging enterprise IAM to access cloud platforms

Erik Coleman, IAM Architect, University of Illinois at Urbana-Champaign
Keith Wessel, Principal IAM Specialist, University of Illinois at Urbana-Champaign

OUR IAM INFRASTRUCTURE

Some background on our setup

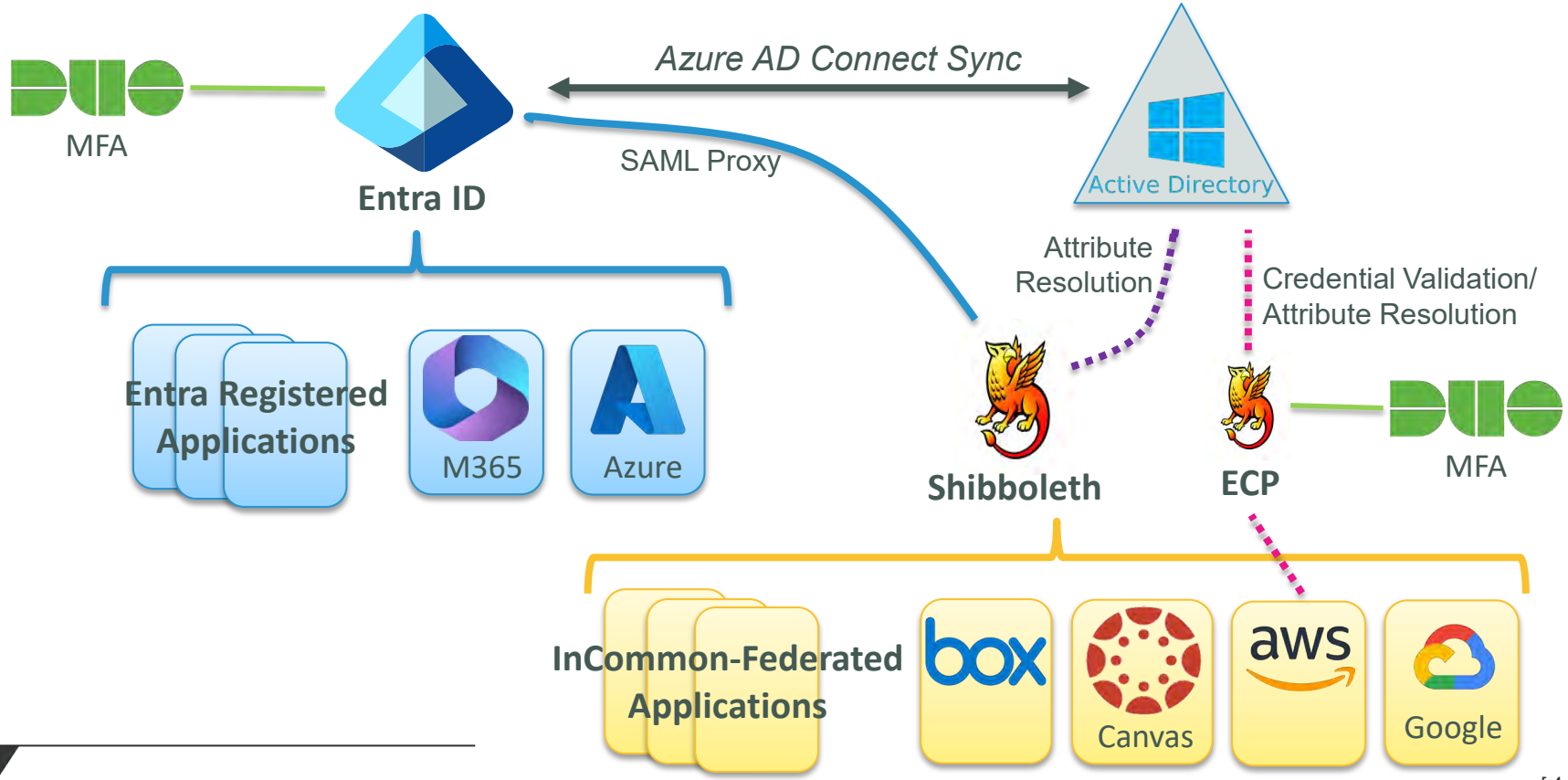


Linked SSOs: Shibboleth plus Entra ID

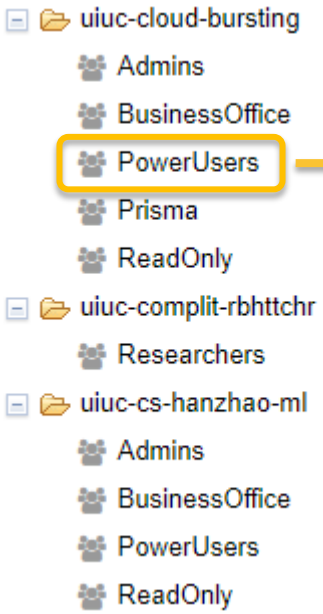
- Consistent browser login experience
- Shibboleth proxies authentication to Entra ID
- Gain benefits of each SSO system with one login
- Entra ID maintains the user session
- Special magic to signal when MFA is needed by Shib
- Shib continues to rely on AD for attribute lookup
- Shib Enhanced Client or Proxy (ECP) still does its own authN

- Link to the Incommon Linking SSOs Working Group Report: http://doi.org/10.26869/TI.171.1

Linked SSOs: Shibboleth and Entra ID



Leveraging Grouper for Authorization



AD LDAP Group

`CN=urb_app_aws_123456789_PowerUsers`

IDP-generated XML

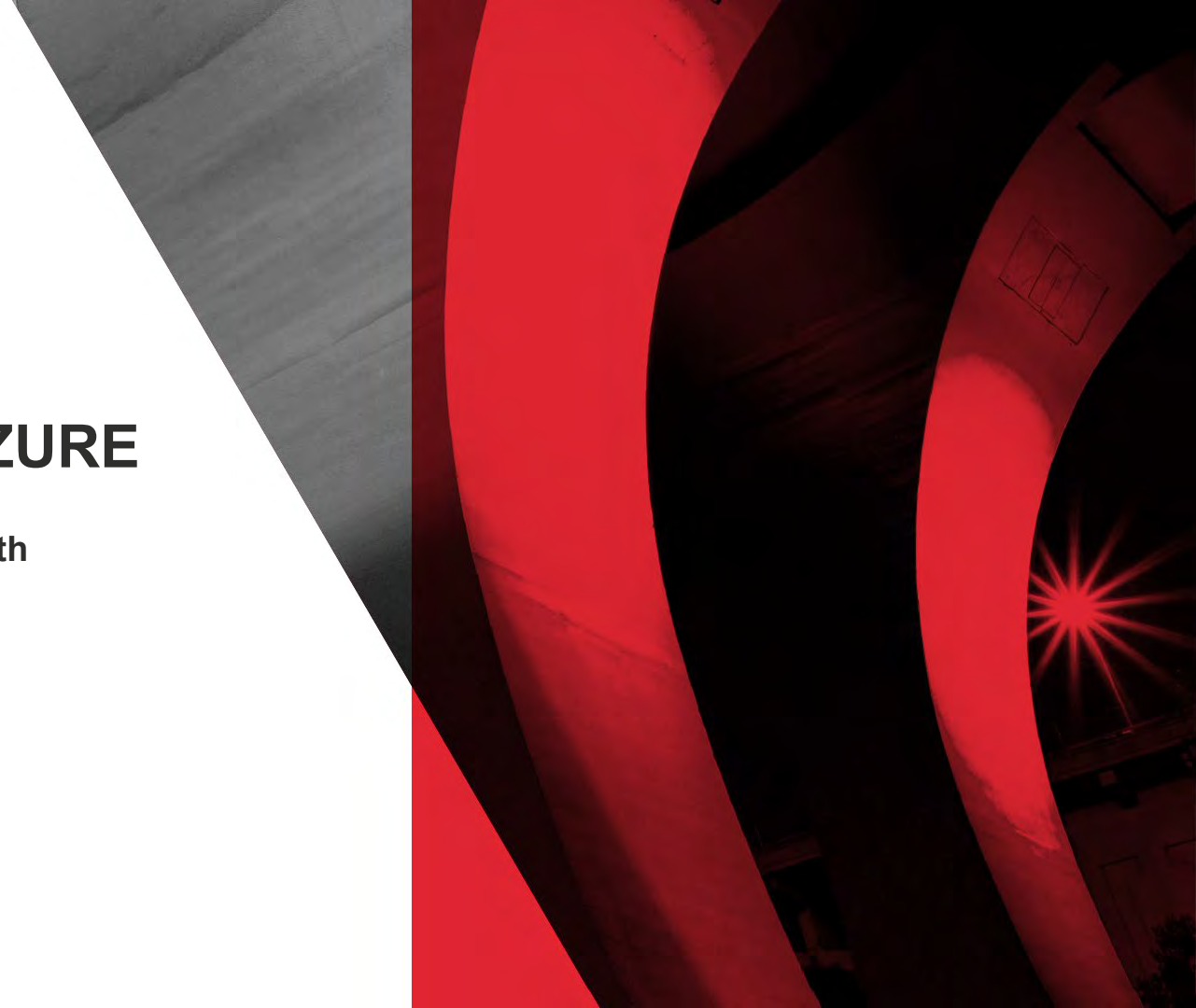
```
<AttributeValue>
   arn:aws:iam::123456789:saml-provider/shibboleth.Illinois.edu,
   arn:aws:iam::123456789:role/PowerUsers
</AttributeValue>
```

Putting the infrastructure to work

- Leverage SSO for cloud platform authentication when possible
- Leverage enterprise groups/access policies for cloud roles
- Structure your roles: driven by application, not the cloud platform
- Reuse pieces across clouds as much as possible to improve scalability
  - SSO attributes
  - Grouper groups

MICROSOFT AZURE

SSO Capabilities with Console and CLI



Microsoft Azure (Cloud)

- Entra ID (formerly Azure AD) provides a “directory tenant”
- Not to be confused with the Azure resource subscriptions themselves
- Tightest integration of IAM among the 3 major public clouds
- Cloud-reimagined “Active Directory” provides AuthN and AuthZ
- Supports both SAML and Open ID Connect
- Azure Subscriptions have built-in trust relationship to Entra ID
- Supports application “registration” and Service Principal Names (SPNs)
- Azure “App Gallery” provides pre-configured apps that can be registered

Azure CLI Browser Sign-in

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\ecc> az login
A web browser has been opened at https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue the login in the web browser. If no web
browser is available or if the web browser fails to open, use device code flow with `az login --use-device-code`.
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "44467e6f-462c-4ea2-823f-7800de542323",
    "id": "3f6706b3-f76a-4e6e-b95c-965d1f854545",
    "isDefault": true,
    "managedByTenants": [],
    "name": "urbana-itp-test",
    "state": "Enabled",
    "tenantId": "44467e6f-462c-4ea2-823f-7800de546868",
    "user": {
      "name": "ecc@illinois.edu",
      "type": "user"
    }
  },
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "44467e6f-462c-4ea2-823f-7800de542323",
    "id": "615eb75a-6afa-412b-8a9d-077e95503535",
    "isDefault": false,
    "managedByTenants": [],
    "name": "urbana-business-test",
    "state": "Enabled",
    "tenantId": "44467e6f-462c-4ea2-823f-7800de543636",
    "user": {
      "name": "ecc@illinois.edu",
      "type": "user"
    }
  }
]
```

Demo of Azure Authentication

You have logged into Microsoft Azure!

You can close this window, or we will redirect you to the Azure CLI documentation in 1 minute.

Announcements

[Windows only] Azure CLI is collecting feedback on using the Web Account Manager (WAM) broker for the login experience.

You may opt-in to use WAM by running the following commands:

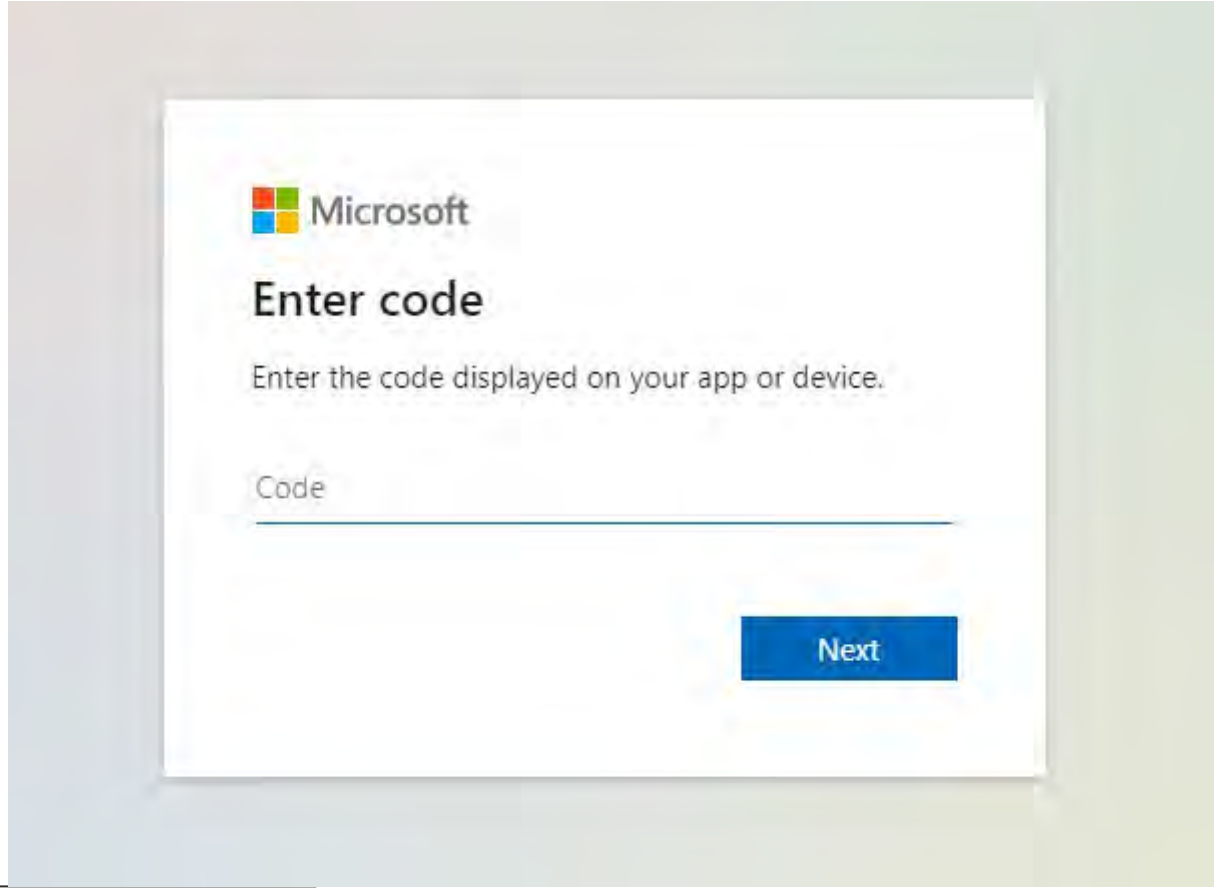
```
az config set core.allow_broker=true
az account clear
az login
```

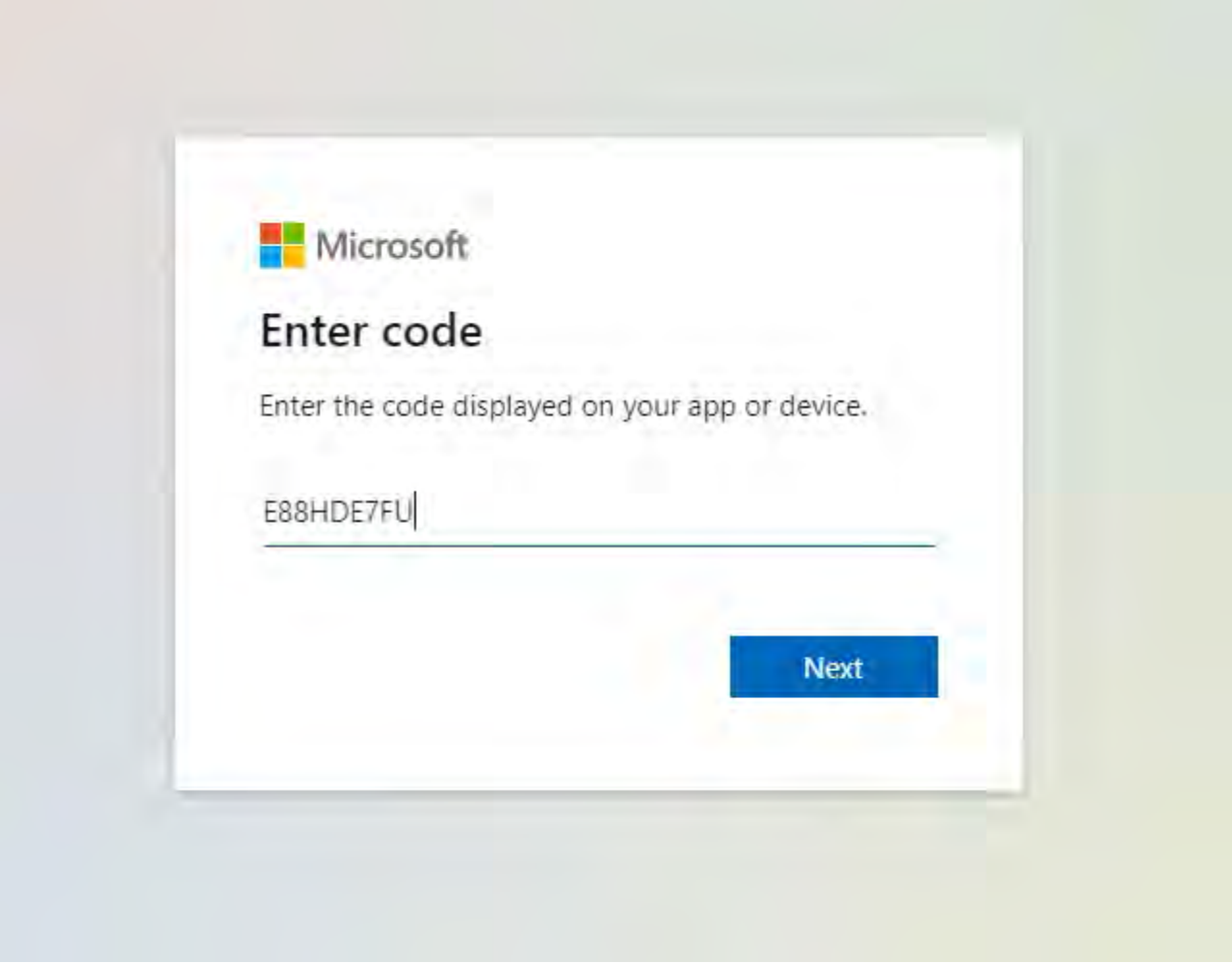
Azure CLI Sign-in Using Device Code

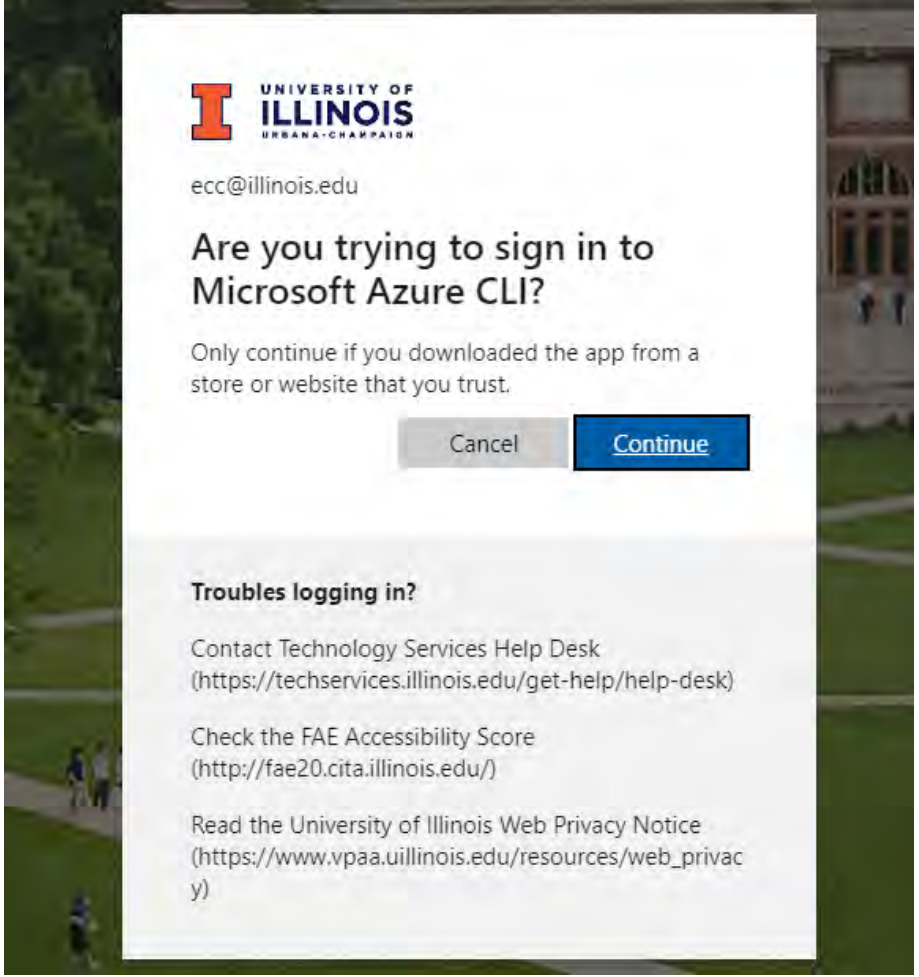
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\ecc> az login --use-device-code --tenant 44467e6f-462c-4ea2-823f-
7800de542626
To sign in, use a web browser to open the page https://microsoft.com/devicelogin
and enter the code E88HDE7FU to authent
icate.
```


Microsoft
Enter code
Enter the code displayed on your app or device.
Code
Next


Microsoft
Enter code
Enter the code displayed on your app or device.
E88HDE7FU
Next


UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN
ecc@illinois.edu
Are you trying to sign in to Microsoft Azure CLI?
Only continue if you downloaded the app from a store or website that you trust.
Cancel
Continue
Troubles logging in?
Contact Technology Services Help Desk (https://techservices.illinois.edu/get-help/help-desk)
Check the FAE Accessibility Score (http://fae20.cita.illinois.edu/)
Read the University of Illinois Web Privacy Notice (https://www.vpaa.uillinois.edu/resources/web_privacy)

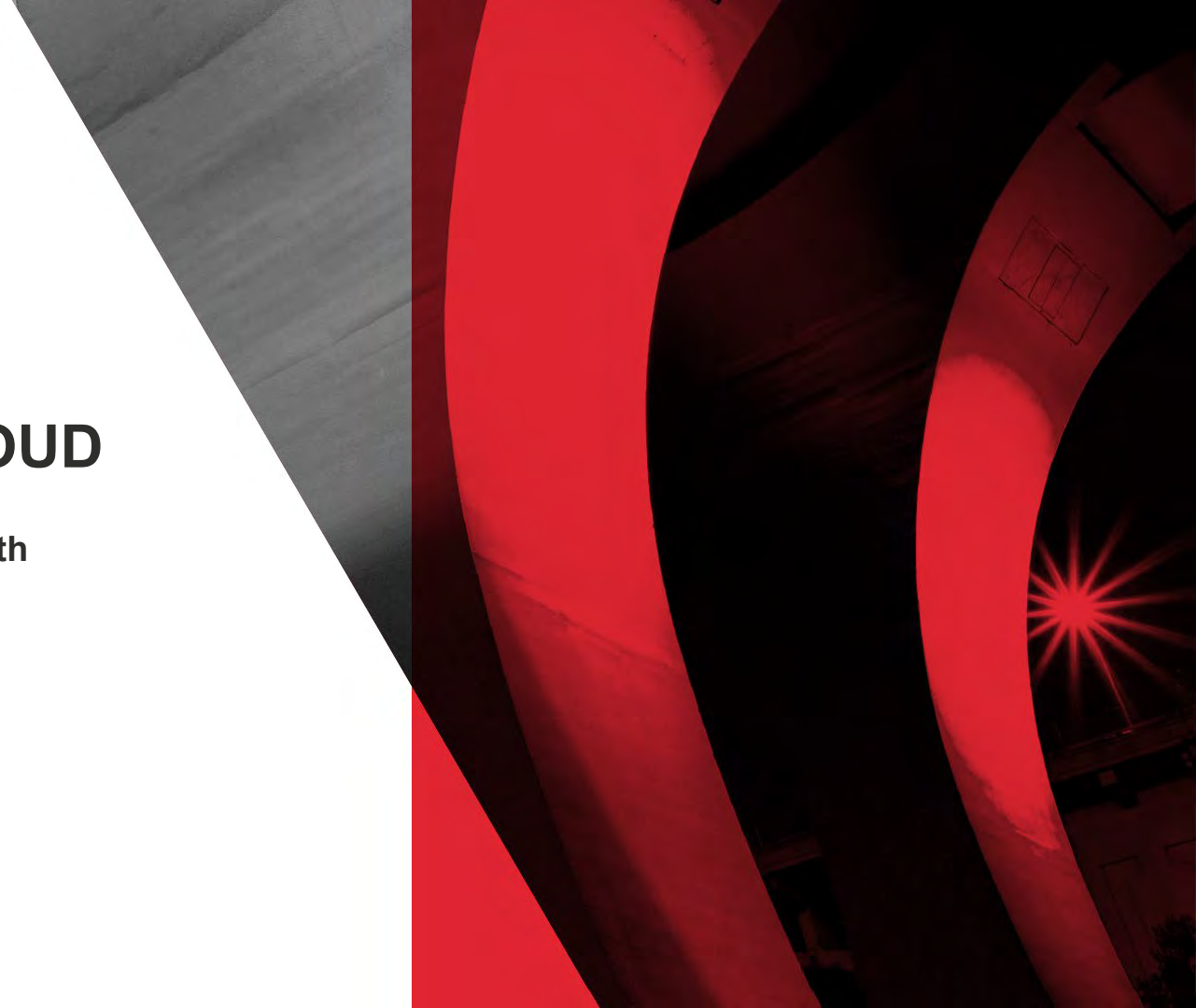

Microsoft
Microsoft Azure Cross-platform Command Line Interface
You have signed in to the Microsoft Azure Cross-platform Command Line Interface application on your device. You may now close this window.

Azure CLI login complete

```
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code E88HDE7FU to authenticate.
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "44467e6f-462c-4ea2-823f-7800de542323",
    "id": "3f6706b3-f76a-4e6e-b95c-965d1f854545",
    "isDefault": true,
    "managedByTenants": [],
    "name": "urbana-itp-test",
    "state": "Enabled",
    "tenantId": "44467e6f-462c-4ea2-823f-7800de546868",
    "user": {
      "name": "ecc@illinois.edu",
      "type": "user"
    }
  },
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "44467e6f-462c-4ea2-823f-7800de542323",
    "id": "615eb75a-6afa-412b-8a9d-077e95503535",
    "isDefault": false,
    "managedByTenants": [],
    "name": "urbana-business-test",
    "state": "Enabled",
    "tenantId": "44467e6f-462c-4ea2-823f-7800de543636",
    "user": {
      "name": "ecc@illinois.edu",
      "type": "user"
    }
  }
]
```

GOOGLE CLOUD

SSO Capabilities with Console and CLI



Google's `gcloud` CLI

- GCloud supports API/CLI authN using OpenID Connect
- User runs something like "gcloud auth application-default login"
- Similar to Azure, browser window opens, or prompts for URL with a code
- After authentication, gcloud gets access and refresh tokens

Using SSO with GCP

- By default, gcloud authn uses provisioned Google account
- Google IAP (Identity Aware Proxy) bridges external auth
- IAP connects to Google Identity Platform
- Identity platform can talk to external SAML or OIDC provider
- Not needed if your org's Google Workspace already uses SSO
- In that case, Google account login will already direct to your IdP

Demo of gcloud Browser Sign-in

```
ecc@TECH-P10E74838:~$ gcloud init
Welcome! This command will take you through the configuration of gcloud.

Your current configuration has been set to: [default]

Network diagnostic detects and fixes local network connection issues.
Checking network connection...done.
Reachability Check passed.
Network diagnostic passed (1/1 checks passed).
You must log in to continue. Would you like to log in (Y/n)?  Y

Go to the following link in your browser:

https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=32555940589.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fsdk.cloud.google.com%2Fauthcode.html&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fsqlservice.login+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=cUb3ZaUC4i9DJdvg8EZiUHNrJq2oC7&prompt=consent&access_type=offline&code_challenge=zes5yAbu4eo3Z4xGAQqXHDMp4HcFsYLxtJobJ9hoAZA&code_challenge_method=S256

Enter authorization code: 4/0AfJohXmVLF3NpxcChof80V1vgj_-Eb5ZMP8d_uZSS7n1PxkGWcl7VGt2Ydtz3OP5FDbeMg
You are logged in as: [ecc@illinois.edu].

Pick cloud project to use:
 [1] iron-pottery-198521
 [2] Enter a project ID
 [3] Create a new project
Please enter numeric choice or text value (must exactly match list item):  1

Your current project has been set to: [iron-pottery-198521].
```

AMAZON WEB SERVICES

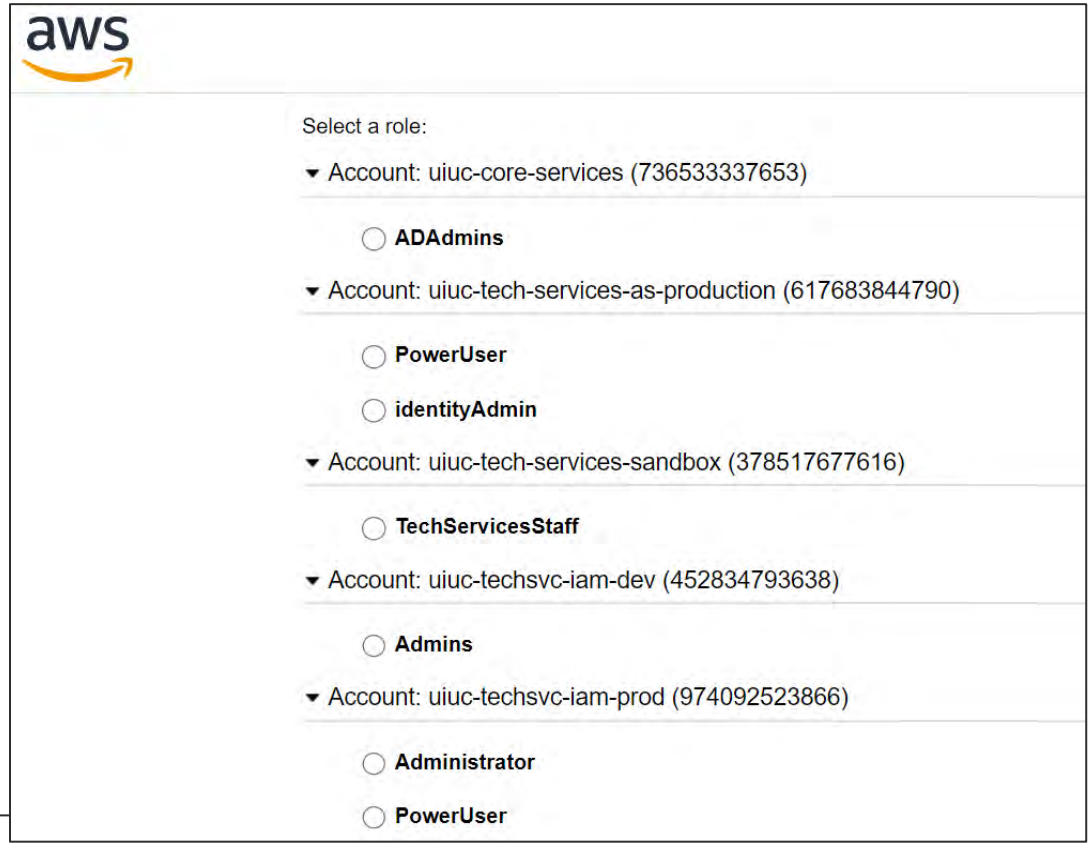
SSO Capabilities with Console and CLI

Quick demo of AWS Console (Shib roles)

- Roles managed in AuthMan Groups; pushed to Active Directory
- ** NEED Grouper group naming convention **
- Shibboleth maps eligible roles in SAML response

```
<AttributeValue>
    arn:aws:iam::account-number:saml-provider/provider-name,
    arn:aws:iam::account-number:role/role-name1
</AttributeValue>
```

AWS Web Console Login



AWS CLI Module: awscli-login

- Allows non-browser authN using Shibboleth ECP
- Supports MFA request to user if configured in IdP
- Stores Shib IdP ‘cookie’ as a local file for re-use
- Parses eligible IAM roles from IdP SAML response
- Prompts user to select appropriate role (or can be set in variable or in-line)
- Sends SAML response with selected role to AWS ACS endpoint
- AWS stores the resulting credentials in normal fashion

Installation of awscli-login

```
ecc@TECH-P10E74838:~$ pip install awscli-login
Processing
./.cache/pip/wheels/3a/1c/d9/79817785aa6a5d8dc25b5d64167c4344e4e0e5b94245aea3de/awscli_lo
gin-0.2b1-py3-none-any.whl
Requirement already satisfied: six>=1.5 in /usr/lib/python3/dist-packages (from python-
dateutil<3.0.0,>=2.1->botocore->awscli-login) (1.14.0)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from
rsa<4.8,>=3.1.2->awscli->awscli-login) (0.4.2)
Installing collected packages: awscli-login
Successfully installed awscli-login-0.2b1
ecc@TECH-P10E74838:~$ aws configure set plugins.login awscli_login
ecc@TECH-P10E74838:~$ aws login configure
ECP Endpoint URL [None]: https://shibboleth.illinois.edu/idp/profile/SAML2/SOAP/ECP
Username [None]:
Enable Keyring [False]:
Duo Factor [None]:
Role ARN [None]:
ecc@TECH-P10E74838:~$
```

Logging in with awscli-login

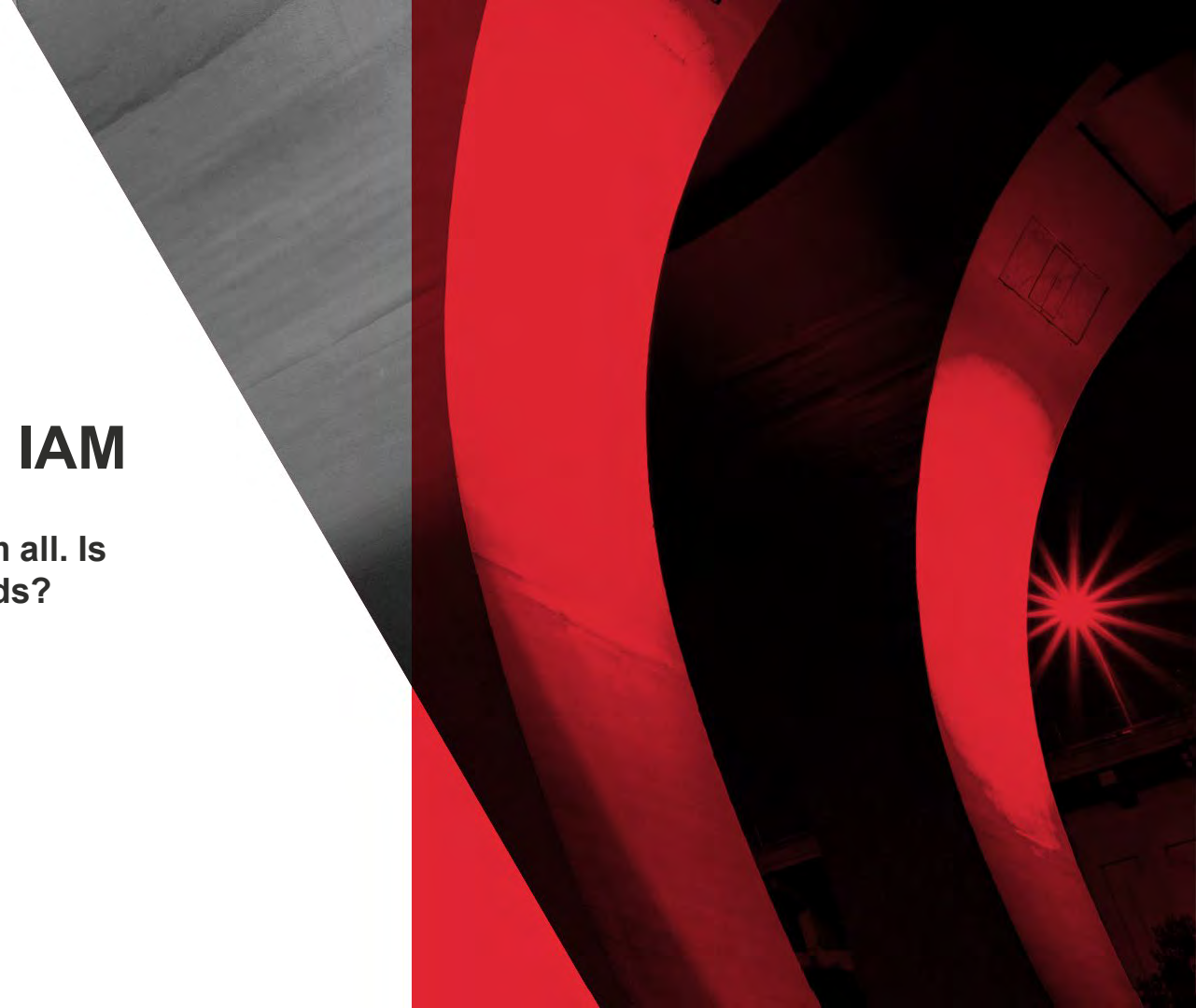
```
ecc@TECH-P10E74838:~$ aws login
Username [ecc]:
Password:
Factor: passcode
Code: 695697
Please choose the role you would like to assume:
     Account: 378517623416
         [ 0 ]: TechServicesStaff
     Account: 452834734538
         [ 1 ]: Admins
     Account: 477657812392
         [ 2 ]: Administrator
         [ 3 ]: PowerUser
     Account: 617683845690
         [ 4 ]: PowerUser
         [ 5 ]: identityAdmin
     Account: 736533367853
         [ 6 ]: ADAdmins
     Account: 974092554666
         [ 7 ]: Administrator
         [ 8 ]: PowerUser
Selection: 8
ecc@TECH-P10E74838:~$
```

Use awscli-login with AWS CLI v2

```
ecc@TECH-P10E74838:~$ which aws
/home/ecc/.local/bin/aws
ecc@TECH-P10E74838:~$ which aws2
/usr/local/bin/aws2
ecc@TECH-P10E74838:~$ aws login
Username [ecc]:
Please choose the role you would like to assume:
     Account: 378517623416
         [ 0 ]: TechServicesStaff
     Account: 452834734538
         [ 1 ]: Admins
     Account: 477657802292
         [ 2 ]: Administrator
         [ 3 ]: PowerUser
     Account: 617683856790
         [ 4 ]: PowerUser
         [ 5 ]: identityAdmin
     Account: 736533367853
         [ 6 ]: ADAdmins
     Account: 974092578966
         [ 7 ]: Administrator
         [ 8 ]: PowerUser
Selection: 3
ecc@TECH-P10E74838:~$ aws s3 ls
2022-02-08 14:59:48 cloudfront-content-public-us-east-2-477657802292
2021-10-27 15:09:26 config-bucket-477657802292
2022-02-02 15:46:26 log-us-east-2-477657802292
2021-11-03 15:46:57 uiuc-techsvc-iam-test
ecc@TECH-P10E74838:~$ aws2 s3 ls
2022-02-08 14:59:48 cloudfront-content-public-us-east-2-477657802292
2021-10-27 15:09:26 config-bucket-477657802292
2022-02-02 15:46:26 log-us-east-2-477657802292
2021-11-03 15:46:57 uiuc-techsvc-iam-test
ecc@TECH-P10E74838:~$
```

CROSS-CLOUD IAM

Use Entra ID to rule them all. Is it as crazy as it sounds?



Entra ID Integrated with AWS & Google Cloud

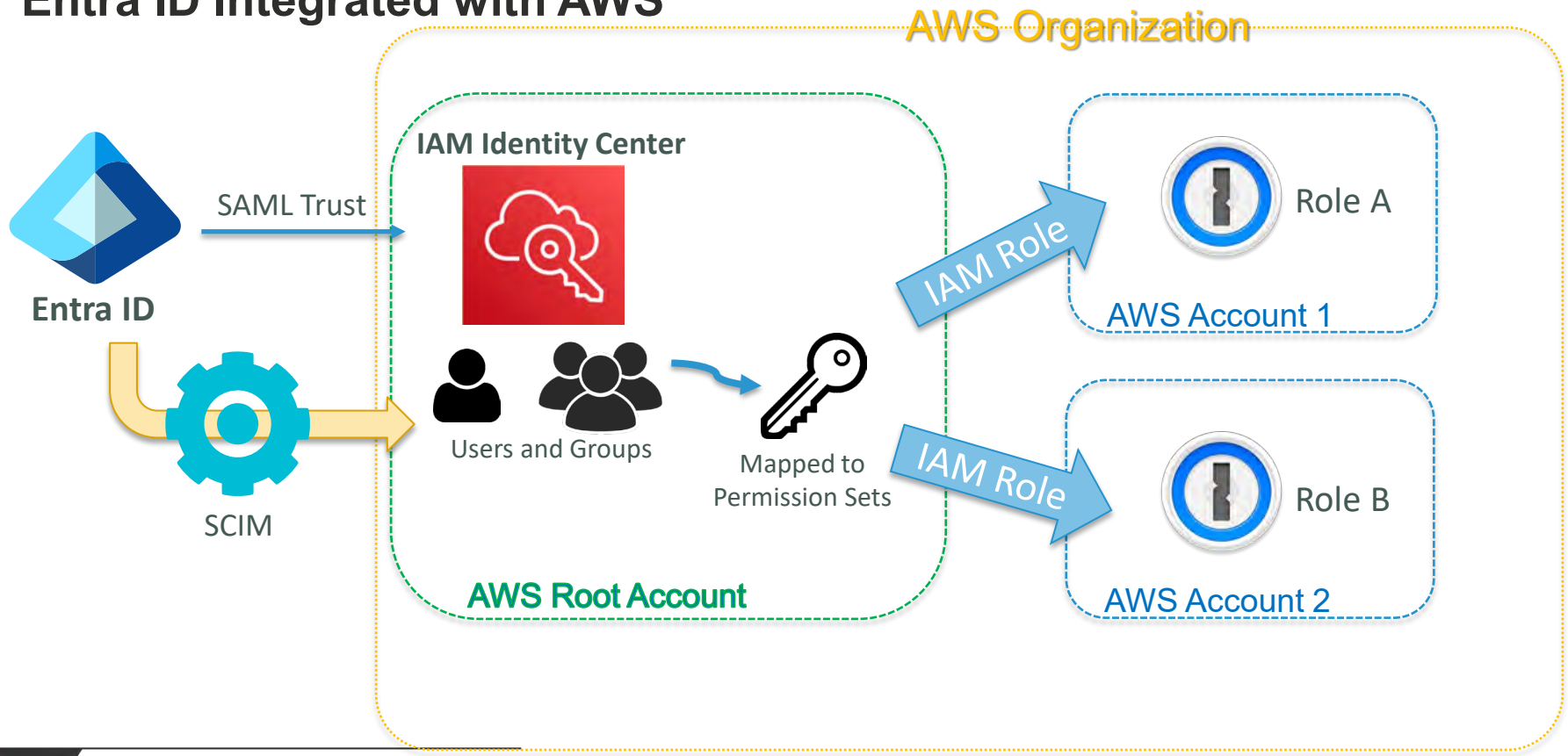
- For authN: Entra ID is well-established industry leader
- We're already using Entra ID SSO for console logins now

Advantages

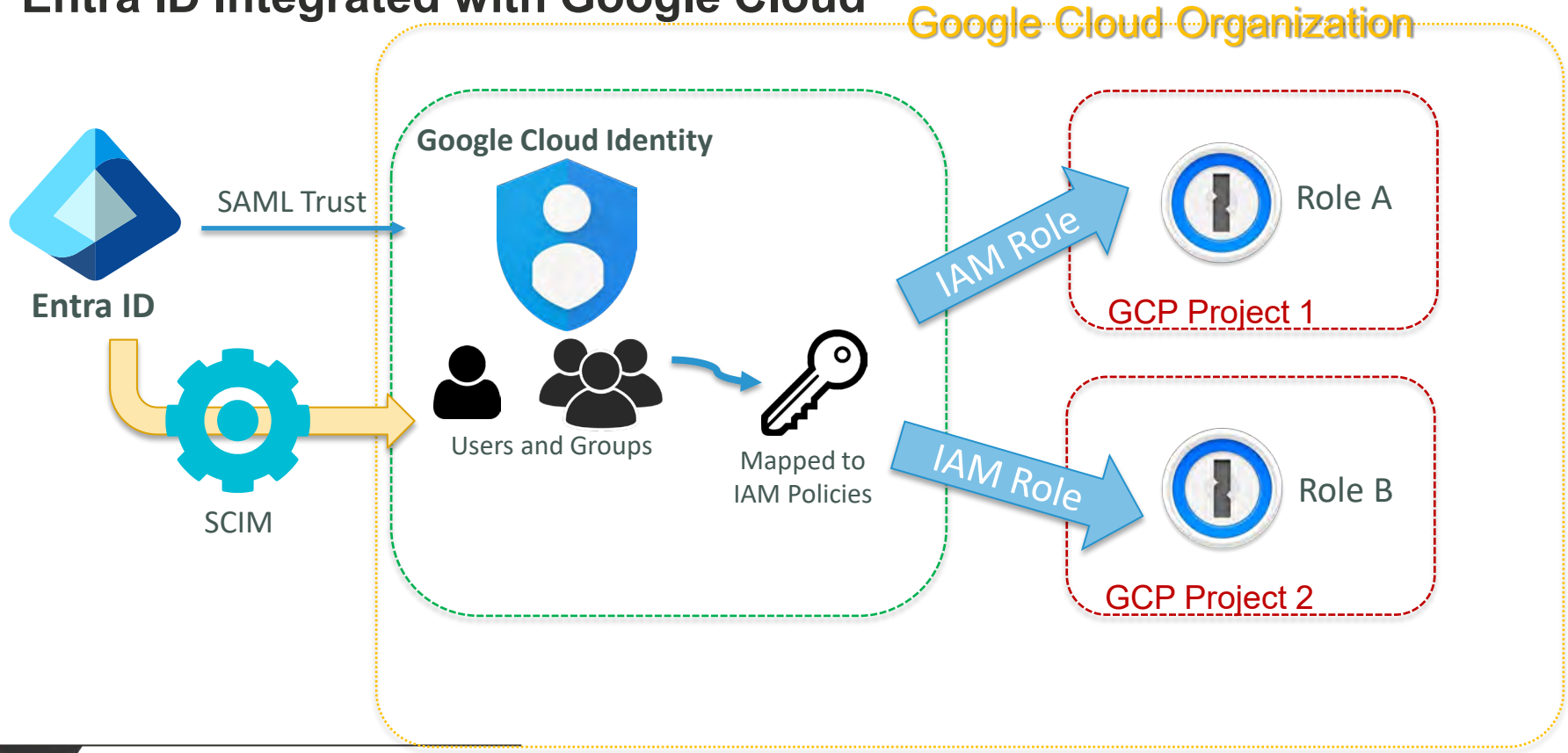
- Users SCIM provisioned from Entra ID as source (JIC vs. JIT)
- Central mapping of groups to roles/permission sets
- Entra ID Security Groups could be sourced from Grouper

- Cloud Infrastructure Entitlement Management (CIEM) like Microsoft Entra Permissions Management can have unified visibility into all resource permissions
- Central management and auditing: one source of truth for consistency

Entra ID Integrated with AWS



Entra ID Integrated with Google Cloud



WHAT ABOUT YOU?

Share with us your cloud SSO experiences