CVSHealth

DACOE PRESENTATION

Demystifying Identity and Access Management

- Saicharan Sirangi [Data Science Lead]

What is Identity?

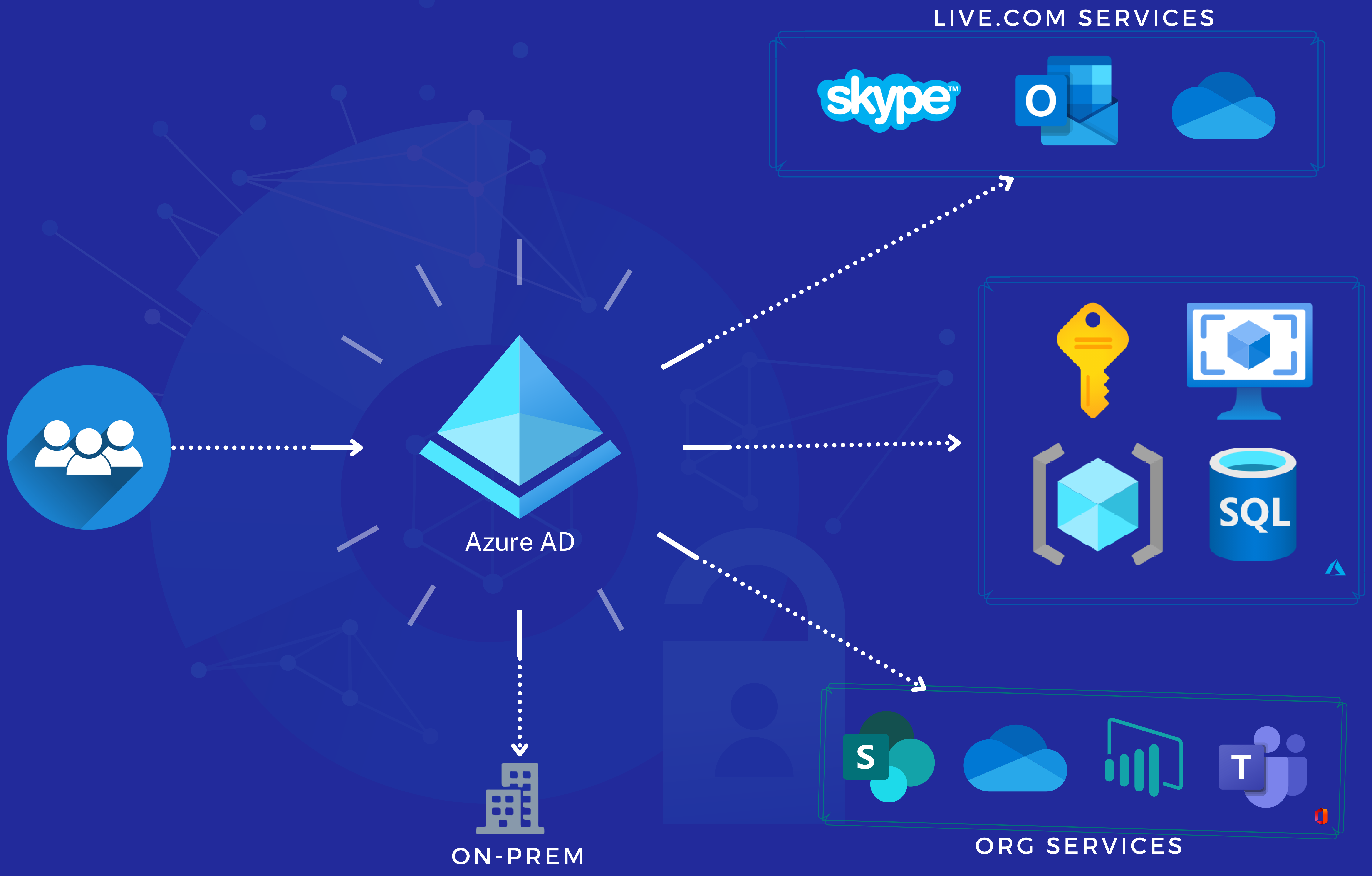
A thing that can get authenticated.

Can be a user with a username and password.

Also applications or other servers with secret keys or certificates.

Access Management

"The Process of controlling, verifying, tracking and managing access to authorized users and applications"



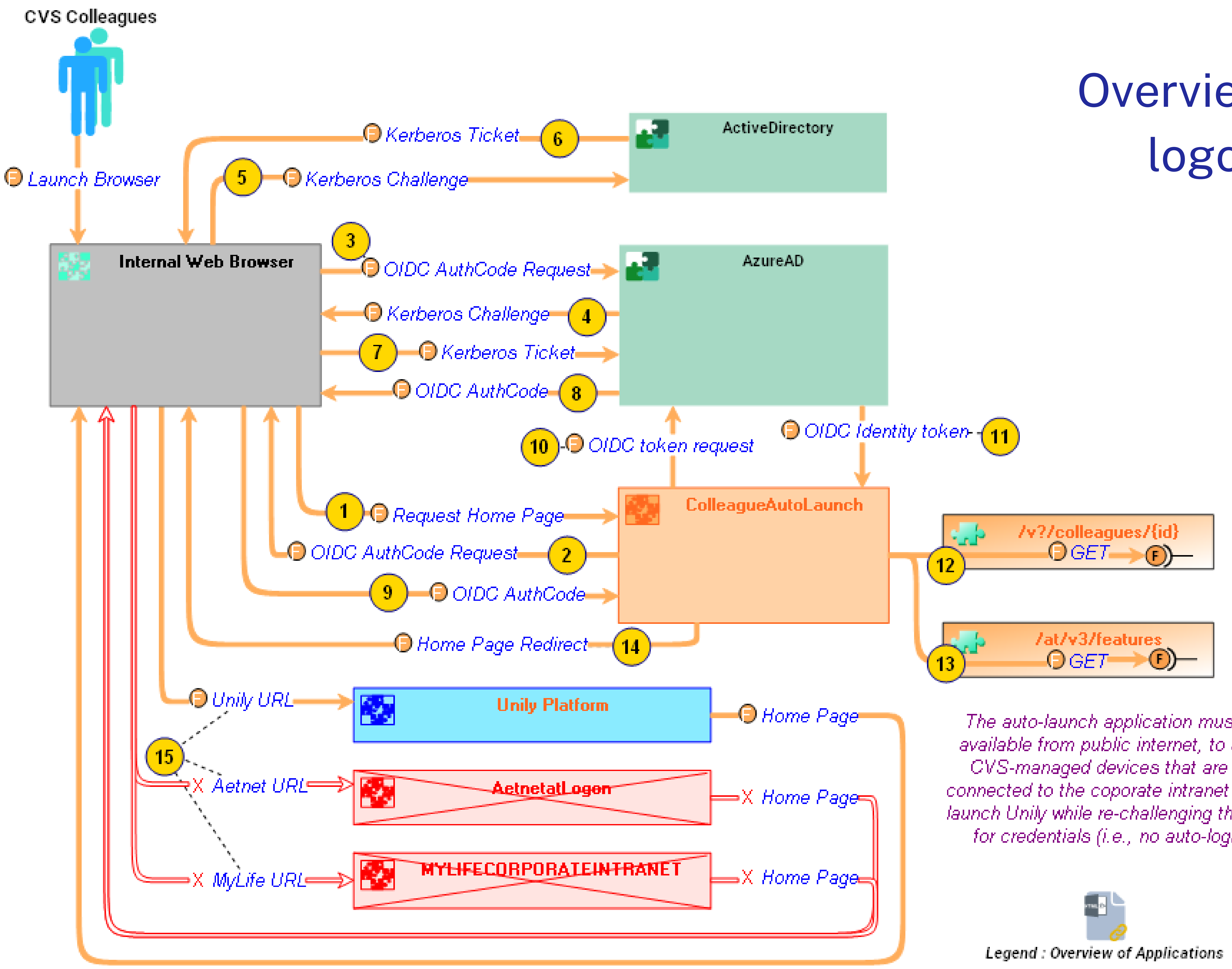
LIVE.COM SERVICES

Azure AD

ON-PREM

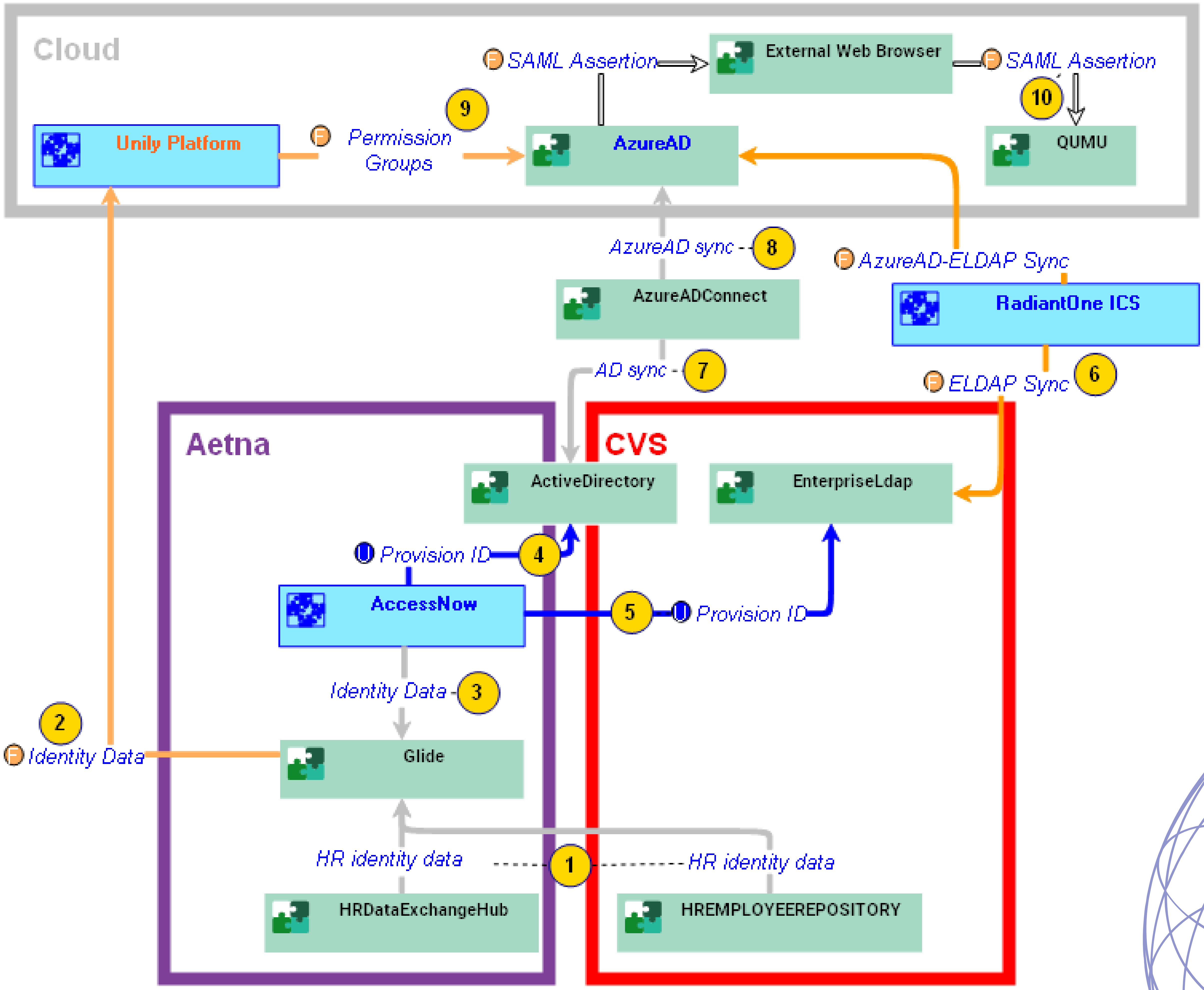
ORG SERVICES

Overview of Applications :Unily logon from CVS network



The auto-launch application must be available from public internet, to allow CVS-managed devices that are not connected to the coporate intranet to still launch Unily while re-challenging the user for credentials (i.e., no auto-login).

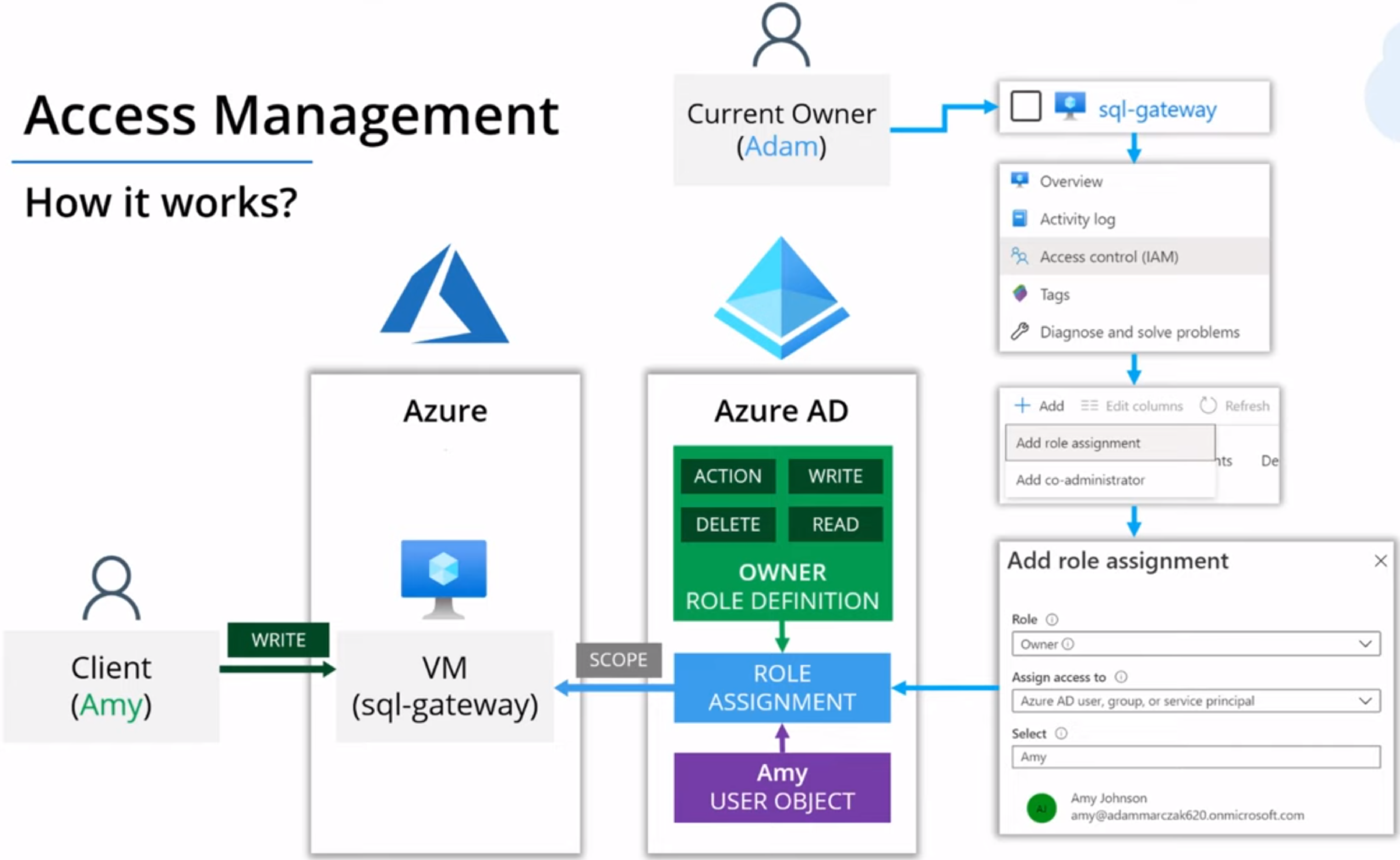
Colleague Azure AD Synchronization



sync shall include profile data as well as id/password

Access Management

How it works?



Add role assignment

Role: Owner

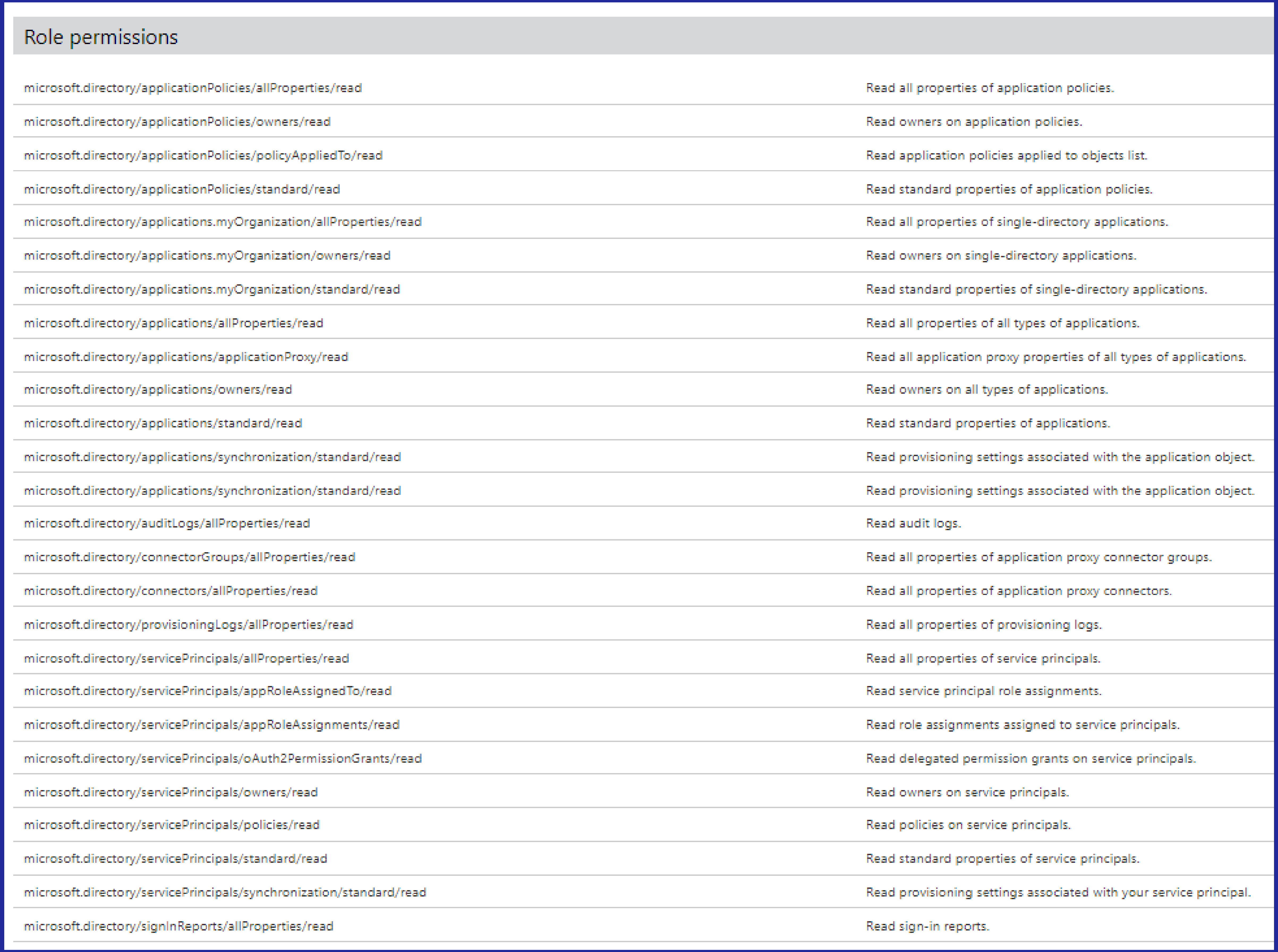
Assign access to: Azure AD user, group, or service principal

Select: Amy

Amy Johnson
amy@adammarczak620.onmicrosoft.com

Ideally get Universal Read Access

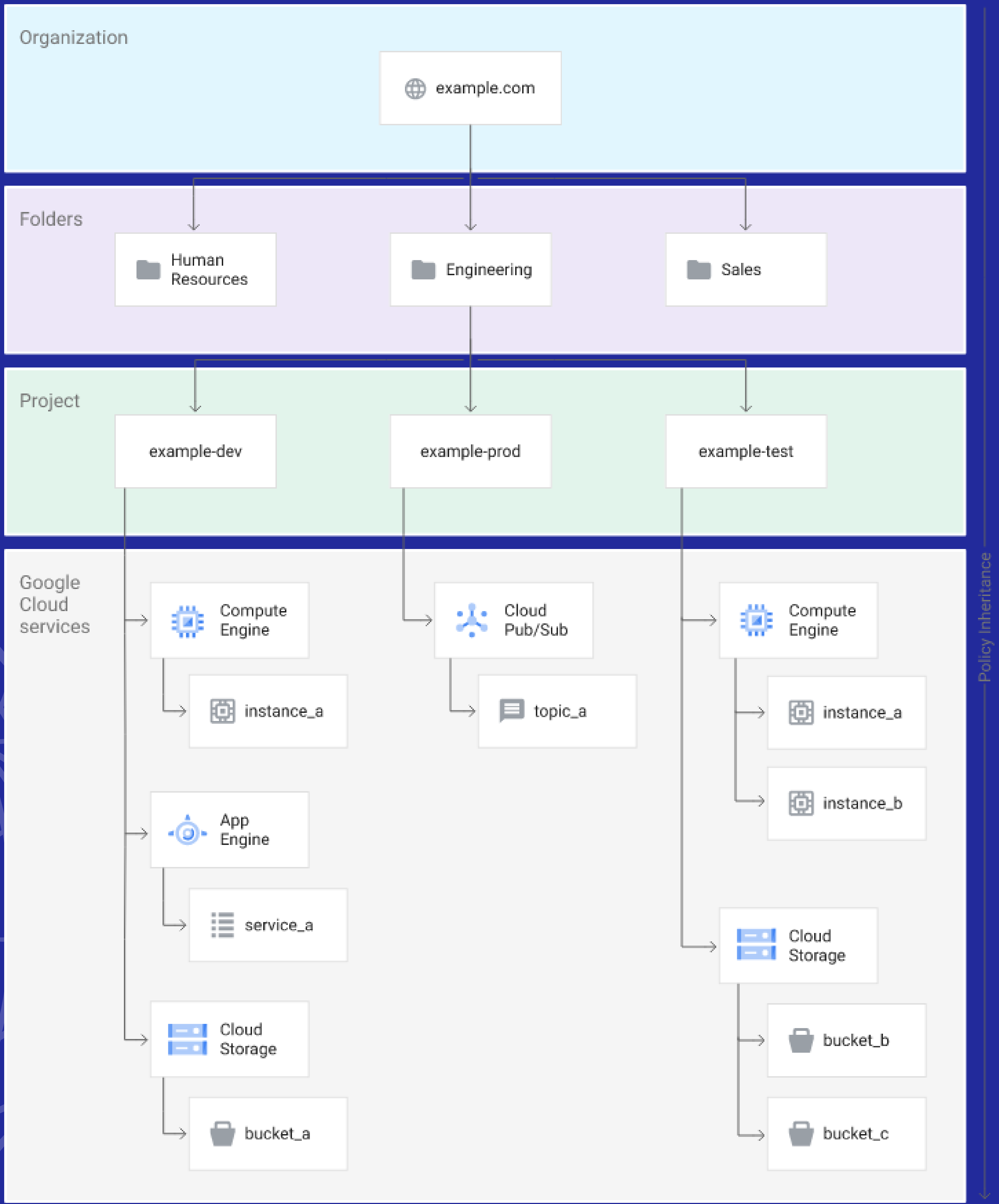
Permissions needed:

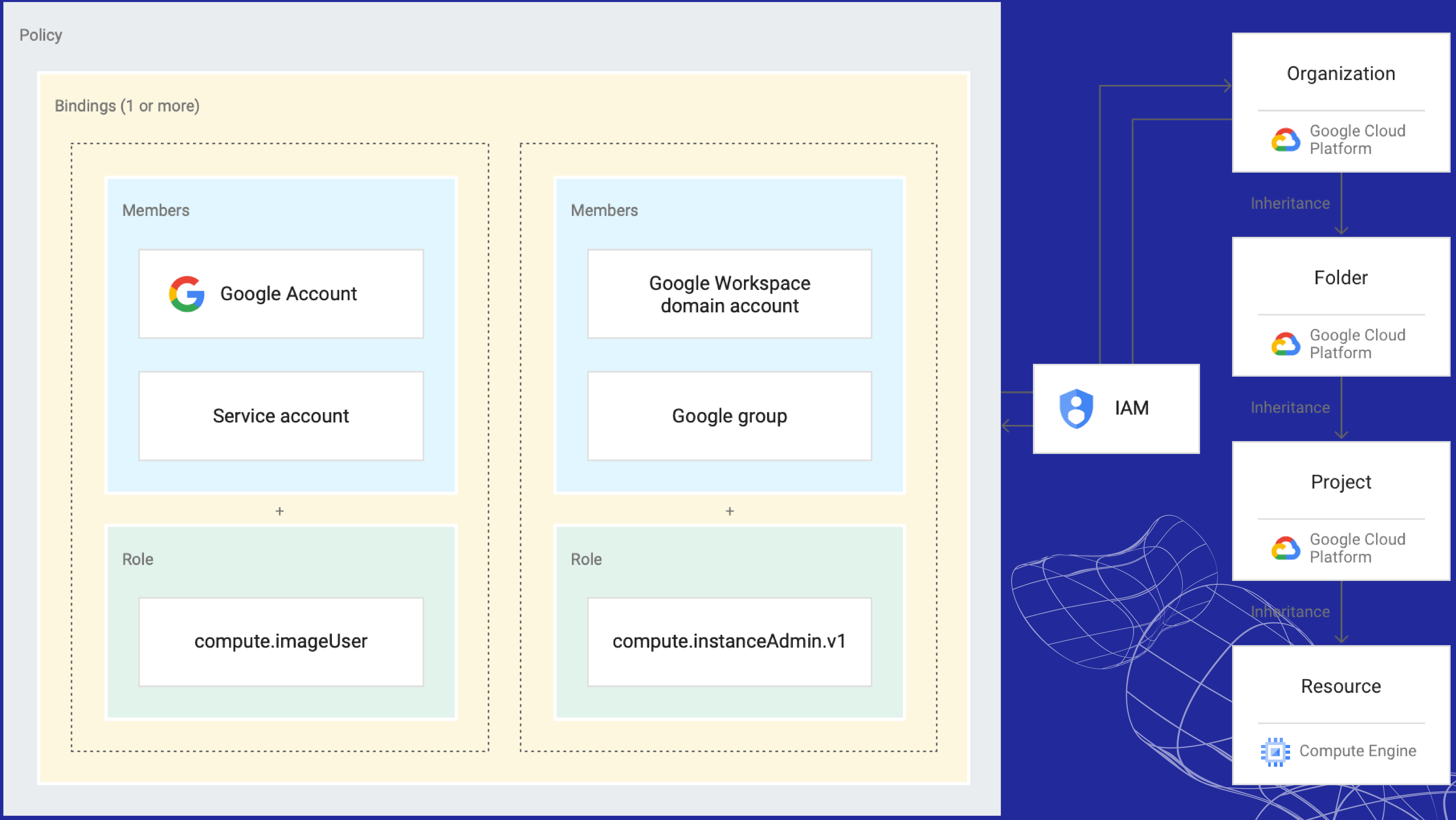


Role permissions

microsoft.directory/applicationPolicies/allProperties/read	Read all properties of application policies.
microsoft.directory/applicationPolicies/owners/read	Read owners on application policies.
microsoft.directory/applicationPolicies/policyAppliedTo/read	Read application policies applied to objects list.
microsoft.directory/applicationPolicies/standard/read	Read standard properties of application policies.
microsoft.directory/applications.myOrganization/allProperties/read	Read all properties of single-directory applications.
microsoft.directory/applications.myOrganization/owners/read	Read owners on single-directory applications.
microsoft.directory/applications.myOrganization/standard/read	Read standard properties of single-directory applications.
microsoft.directory/applications/allProperties/read	Read all properties of all types of applications.
microsoft.directory/applications/applicationProxy/read	Read all application proxy properties of all types of applications.
microsoft.directory/applications/owners/read	Read owners on all types of applications.
microsoft.directory/applications/standard/read	Read standard properties of applications.
microsoft.directory/applications/synchronization/standard/read	Read provisioning settings associated with the application object.
microsoft.directory/applications/synchronization/standard/read	Read provisioning settings associated with the application object.
microsoft.directory/auditLogs/allProperties/read	Read audit logs.
microsoft.directory/connectorGroups/allProperties/read	Read all properties of application proxy connector groups.
microsoft.directory/connectors/allProperties/read	Read all properties of application proxy connectors.
microsoft.directory/provisioningLogs/allProperties/read	Read all properties of provisioning logs.
microsoft.directory/servicePrincipals/allProperties/read	Read all properties of service principals.
microsoft.directory/servicePrincipals/appRoleAssignedTo/read	Read service principal role assignments.
microsoft.directory/servicePrincipals/appRoleAssignments/read	Read role assignments assigned to service principals.
microsoft.directory/servicePrincipals/oAuth2PermissionGrants/read	Read delegated permission grants on service principals.
microsoft.directory/servicePrincipals/owners/read	Read owners on service principals.
microsoft.directory/servicePrincipals/policies/read	Read policies on service principals.
microsoft.directory/servicePrincipals/standard/read	Read standard properties of service principals.
microsoft.directory/servicePrincipals/synchronization/standard/read	Read provisioning settings associated with your service principal.
microsoft.directory/signInReports/allProperties/read	Read sign-in reports.

Hierarchy


Organization
example.com
Folders
Human Resources
Engineering
Sales
Project
example-dev
example-prod
example-test
Google Cloud services
Compute Engine
instance_a
App Engine
service_a
Cloud Storage
bucket_a
Cloud Pub/Sub
topic_a
Compute Engine
instance_a
instance_b
Cloud Storage
bucket_b
bucket_c
Policy inheritance



Policy

Bindings (1 or more)

Members

Google Account

Service account

+

Role

compute.imageUser

Members

Google Workspace domain account

Google group

+

Role

compute.instanceAdmin.v1

IAM

Organization

Google Cloud Platform

Inheritance

Folder

Google Cloud Platform

Inheritance

Project

Google Cloud Platform

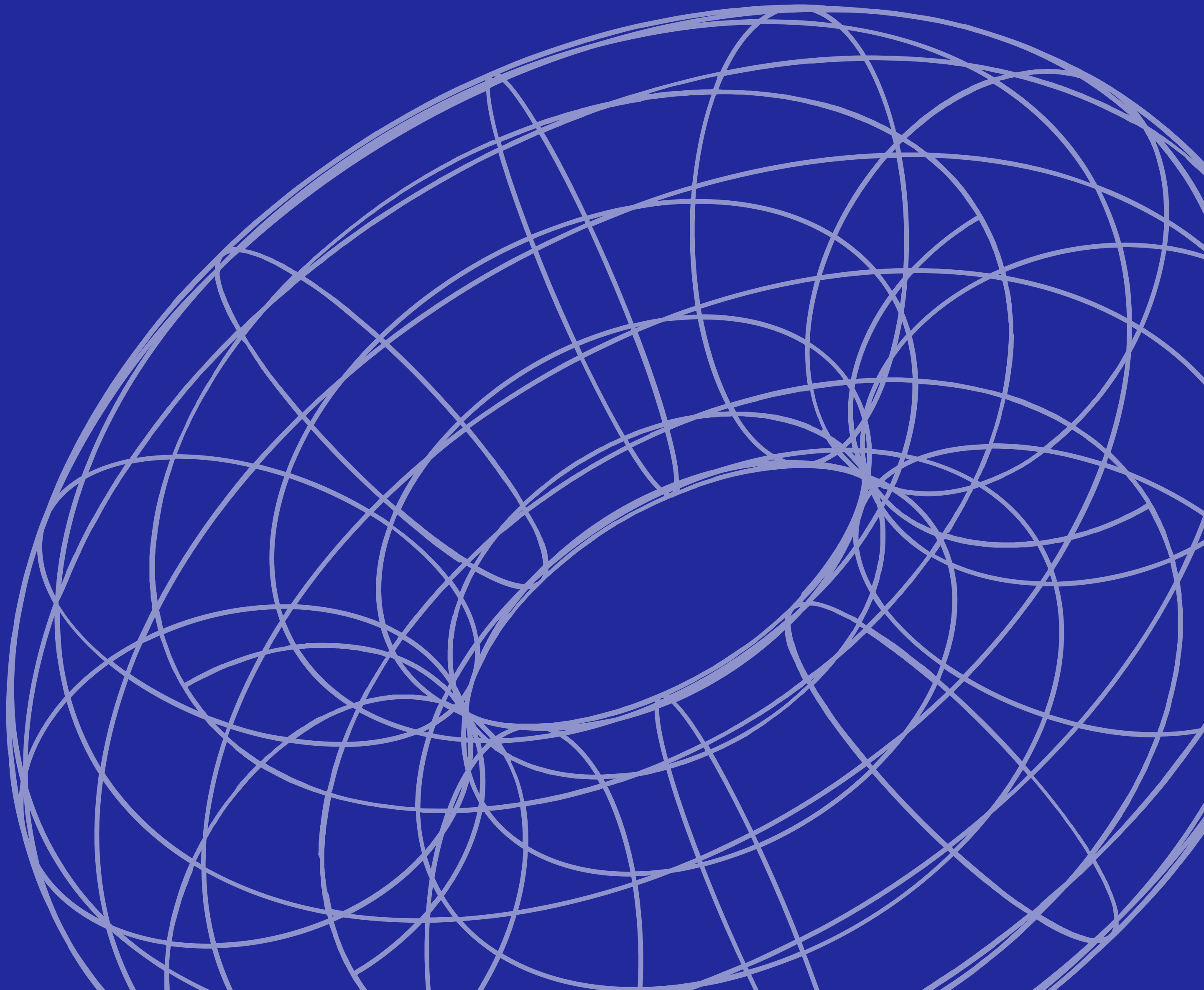
Inheritance

Resource

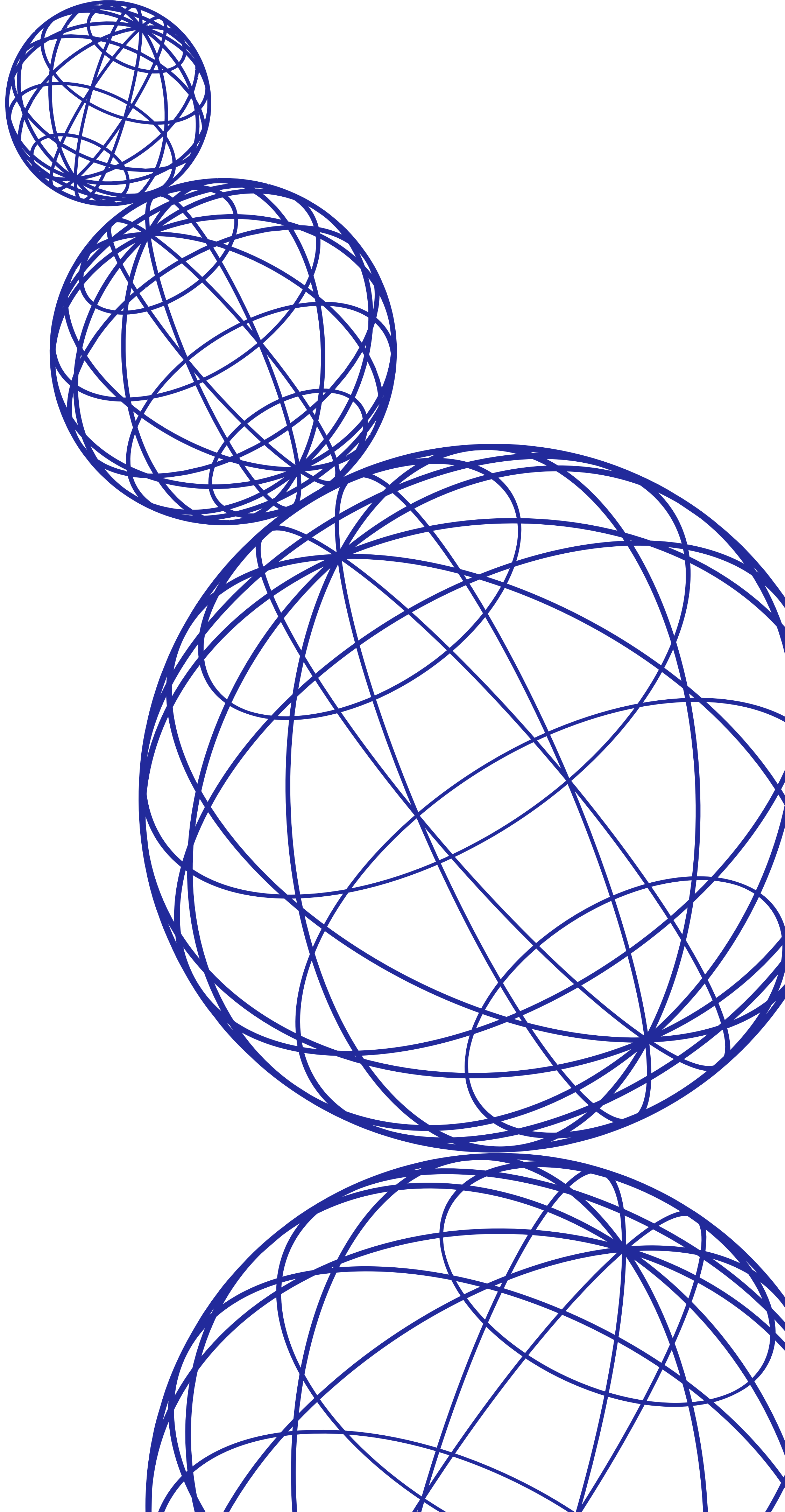
Compute Engine

IAM - Areas of interest

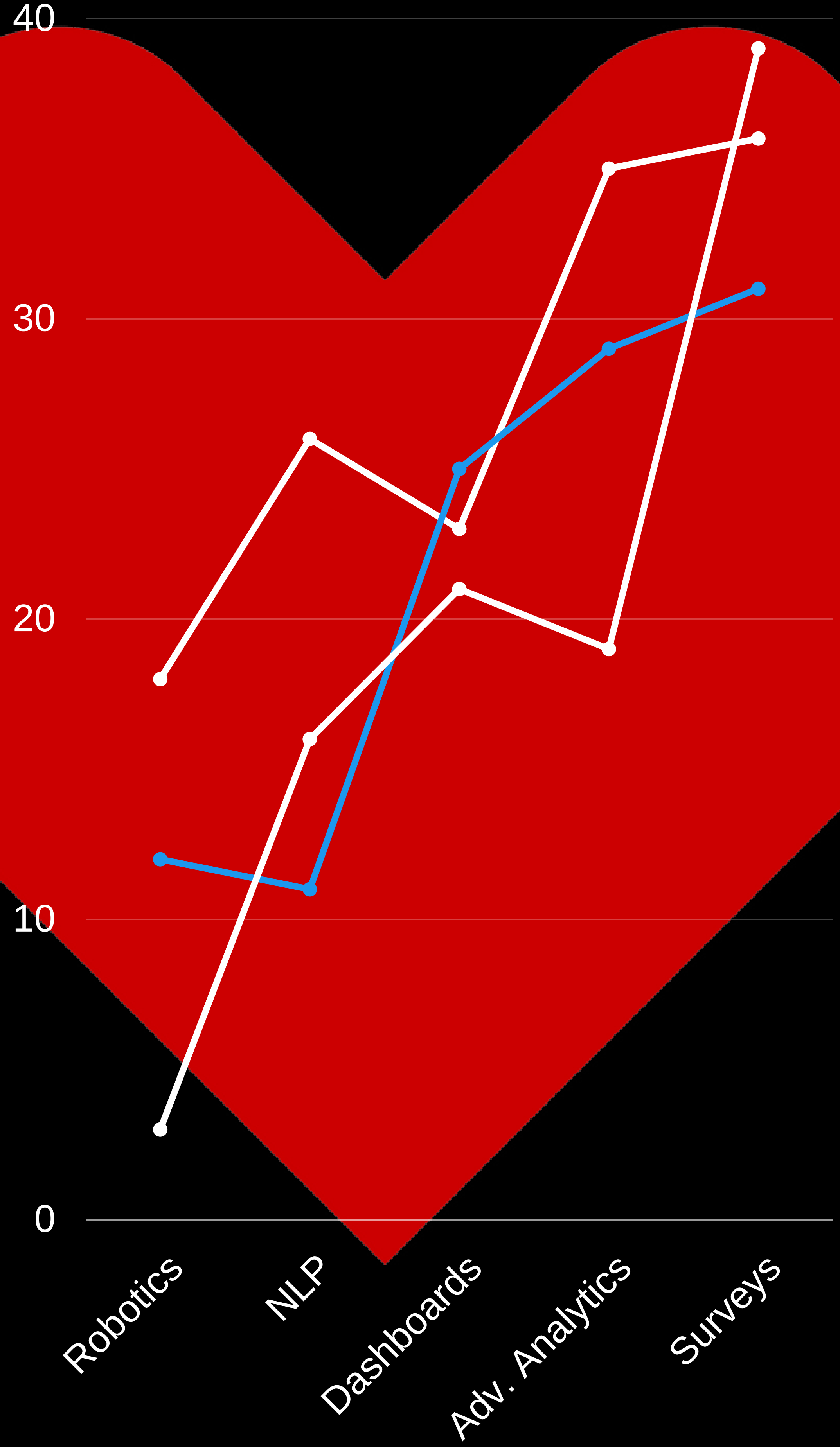
- Privilege Identity Management . Just in time Access
- Automated Provisioning and De-provisioning activity
- Single Sign-on, Multi-factor authentication, and PAM methods
- Safeguards For Privilege -Inheritance
- Federated Access
- Custom Roles & Conditional Policies
- Cross Cloud Protocols & recent gcp migration
- Automatic and Customizable Password Management
- Use of standard core protocols for Change management
- AD DS, Azure AD, Azure AD DS
- How Least privilege access is ensured

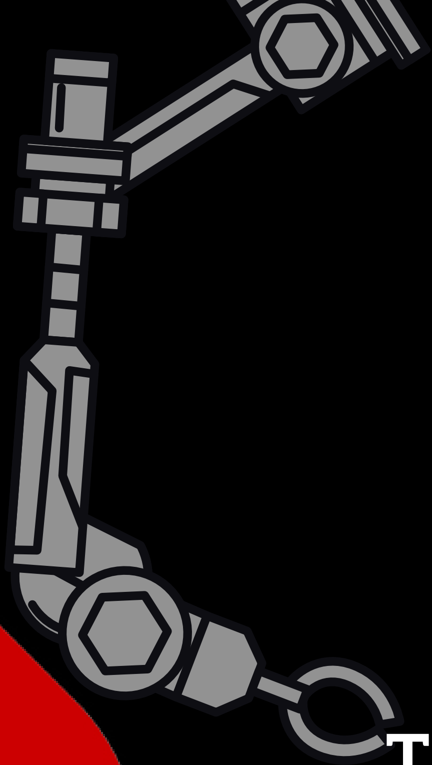


Do you have any questions?



ITDACOE@AETNA.COM





TALK TO US:

Data Science Development

MICHAEL FRITZ

Supervisor

SAICHARAN SIRANGI

Lead