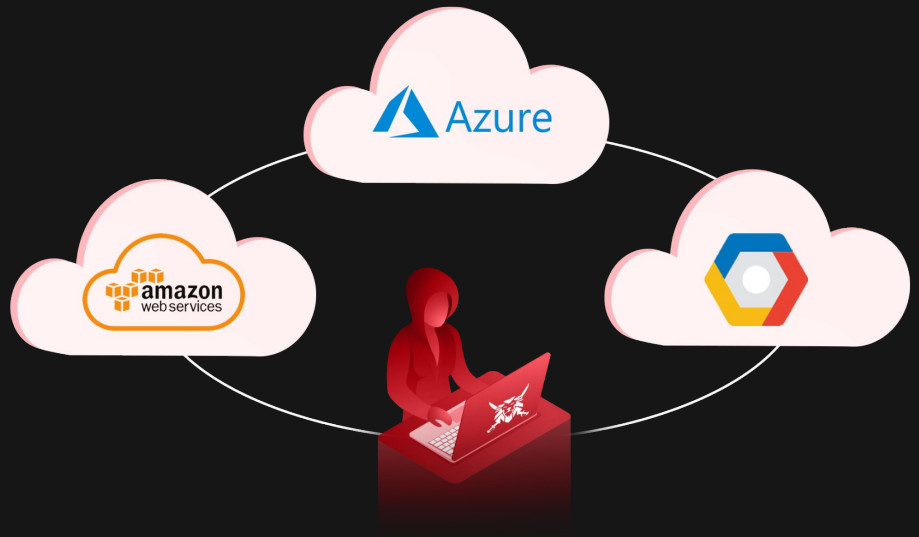
CWL
CyberWarFare Labs

Getting Started with Hybrid Multi-Cloud Red Teaming



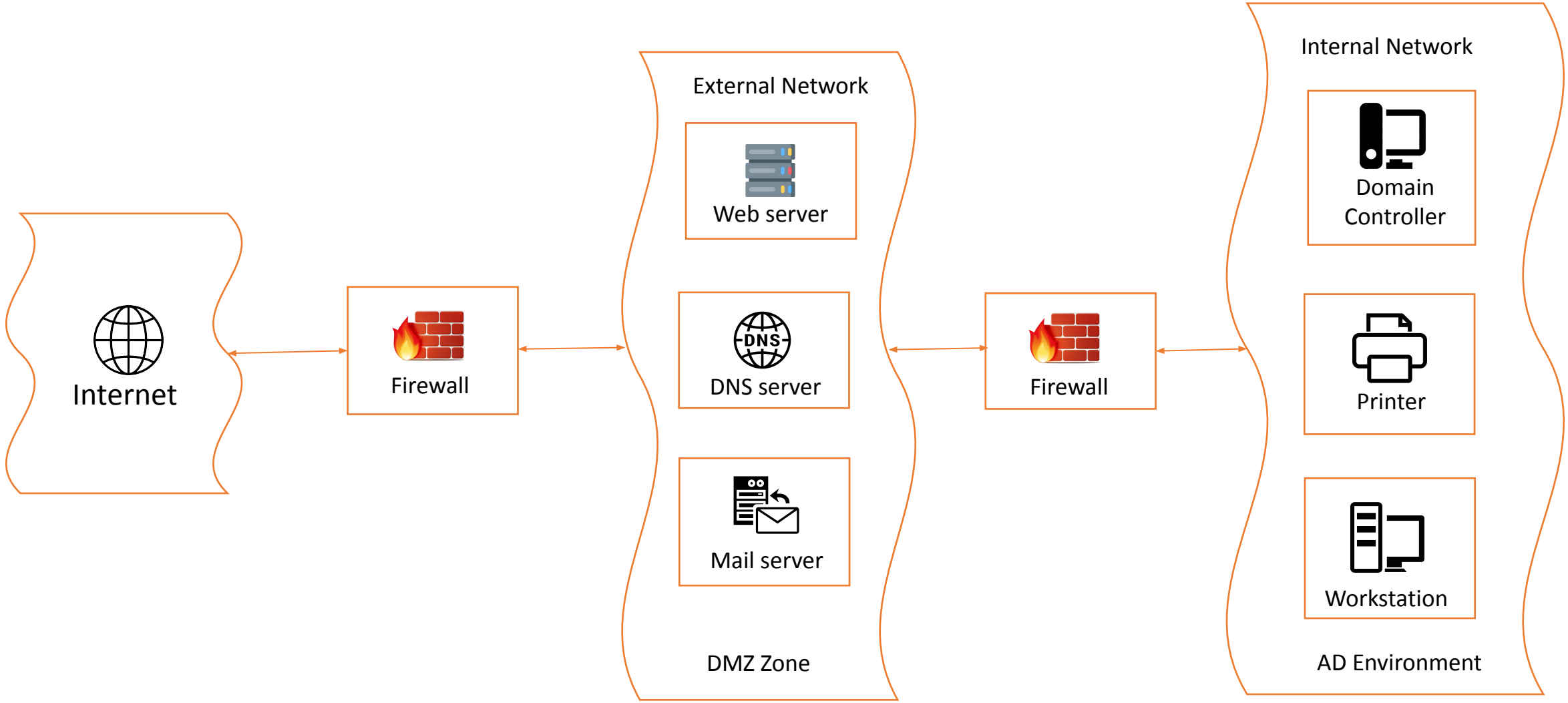
Introduction to Hybrid Multi-Cloud Red Teaming :

- Hybrid Multi Cloud Environment Overview
- AWS Cloud Overview
- Azure Cloud Overview
- Google Cloud Overview
- CTF Exercise

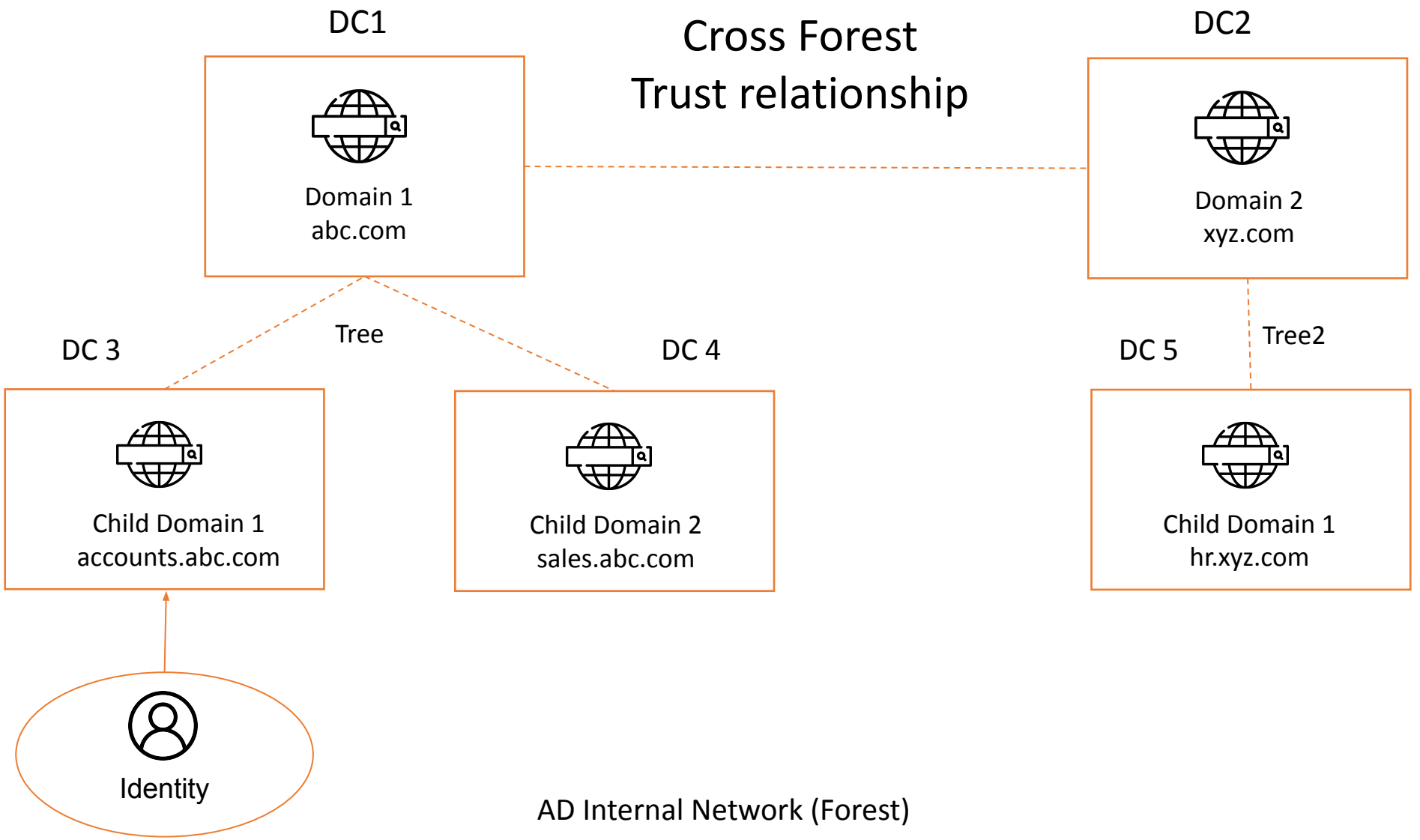
CWL
CyberWarFare Labs

Module - 1 : Hybrid Multi Cloud Environment Overview

Network Architecture of On-Premise Environment

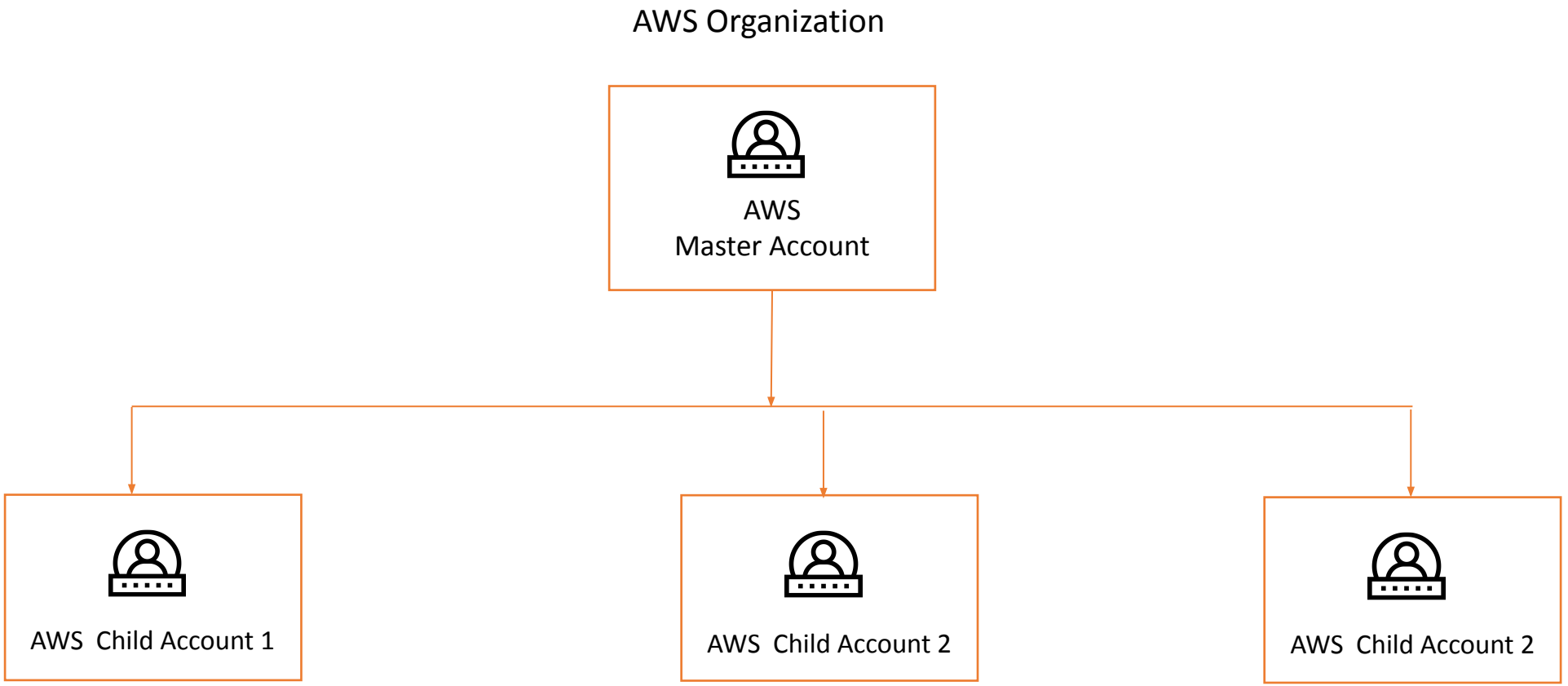


Network Architecture of Active Directory Forest

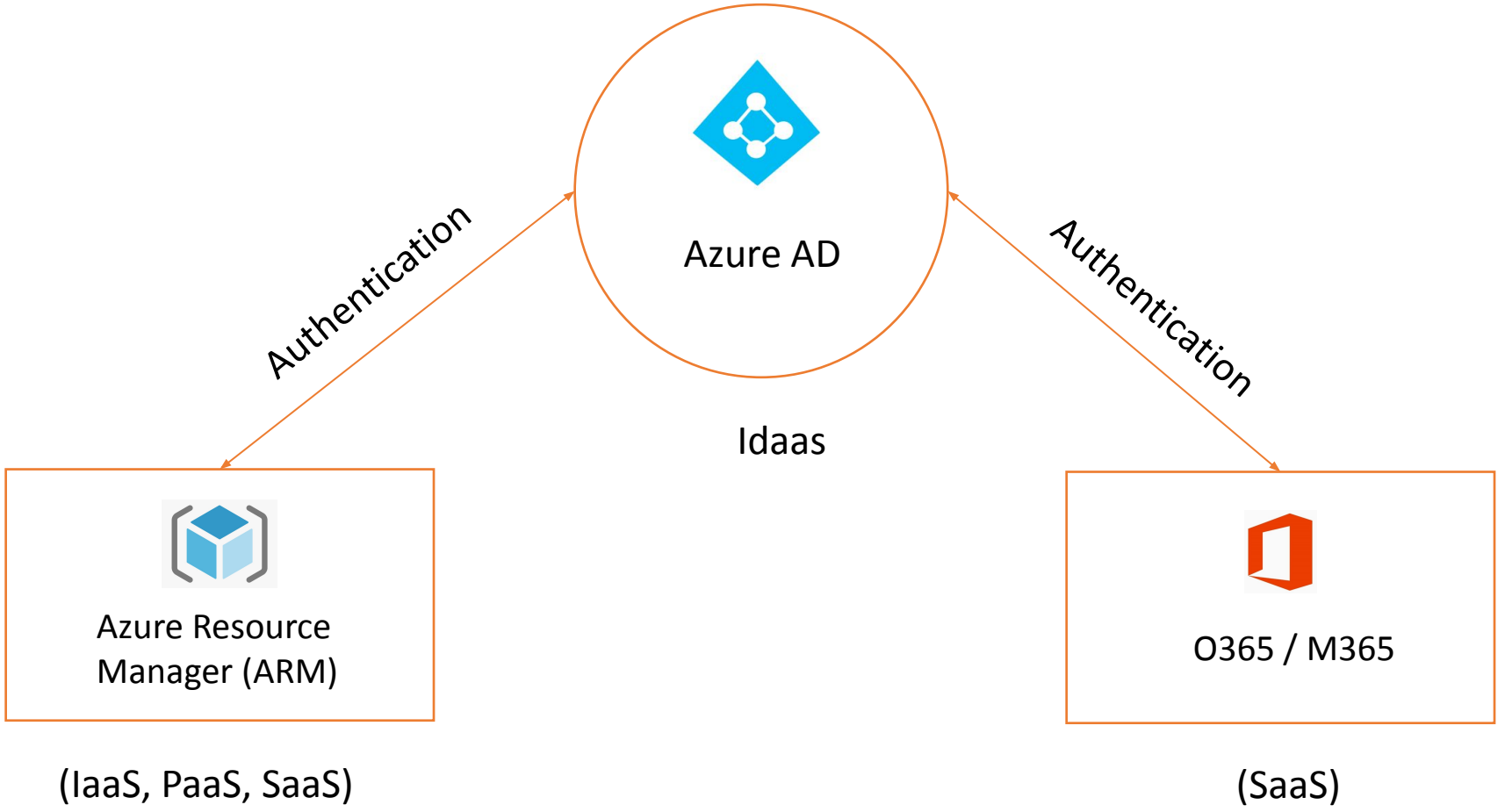


AD Internal Network (Forest)

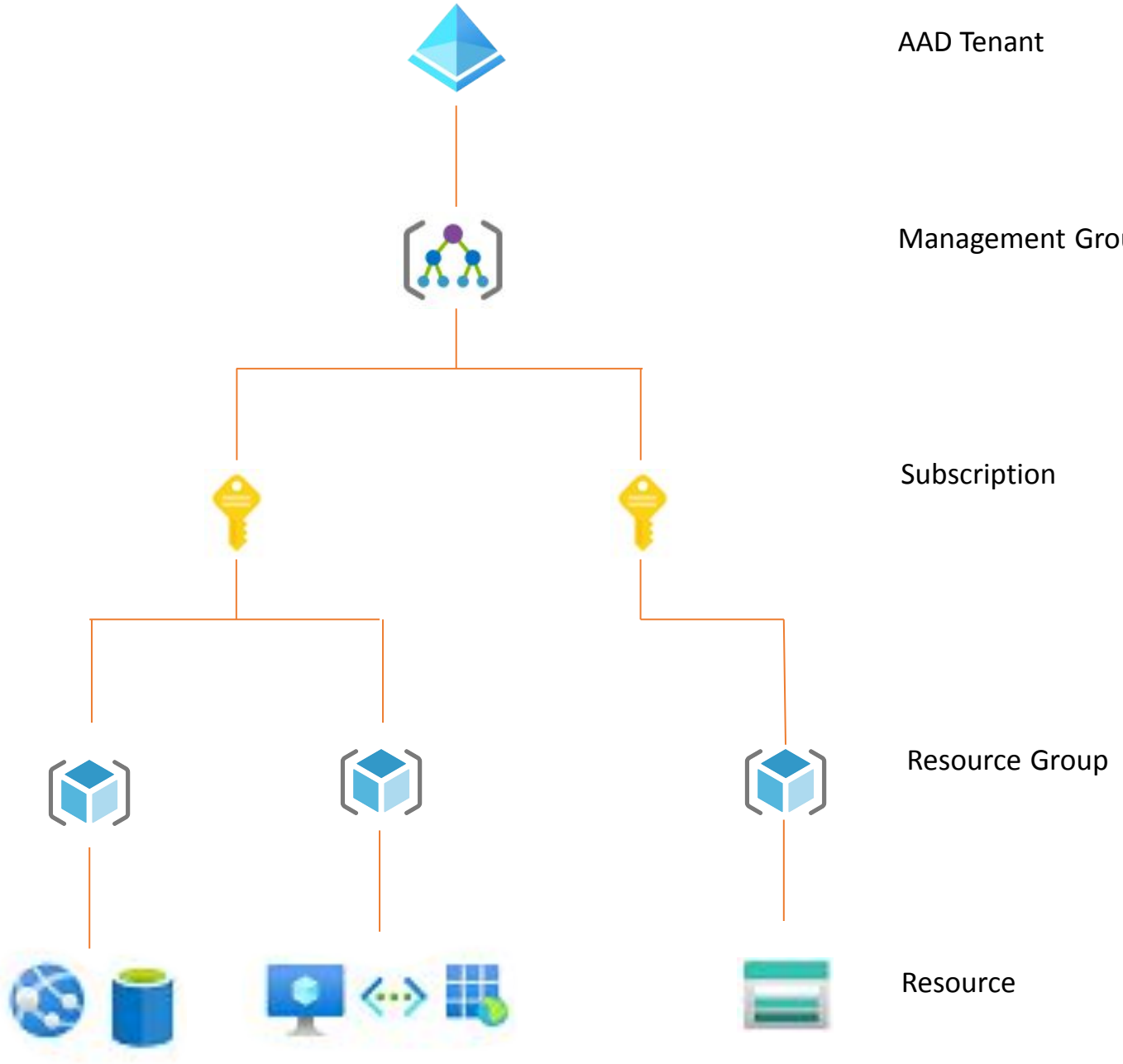
AWS Multi Accounts Architecture



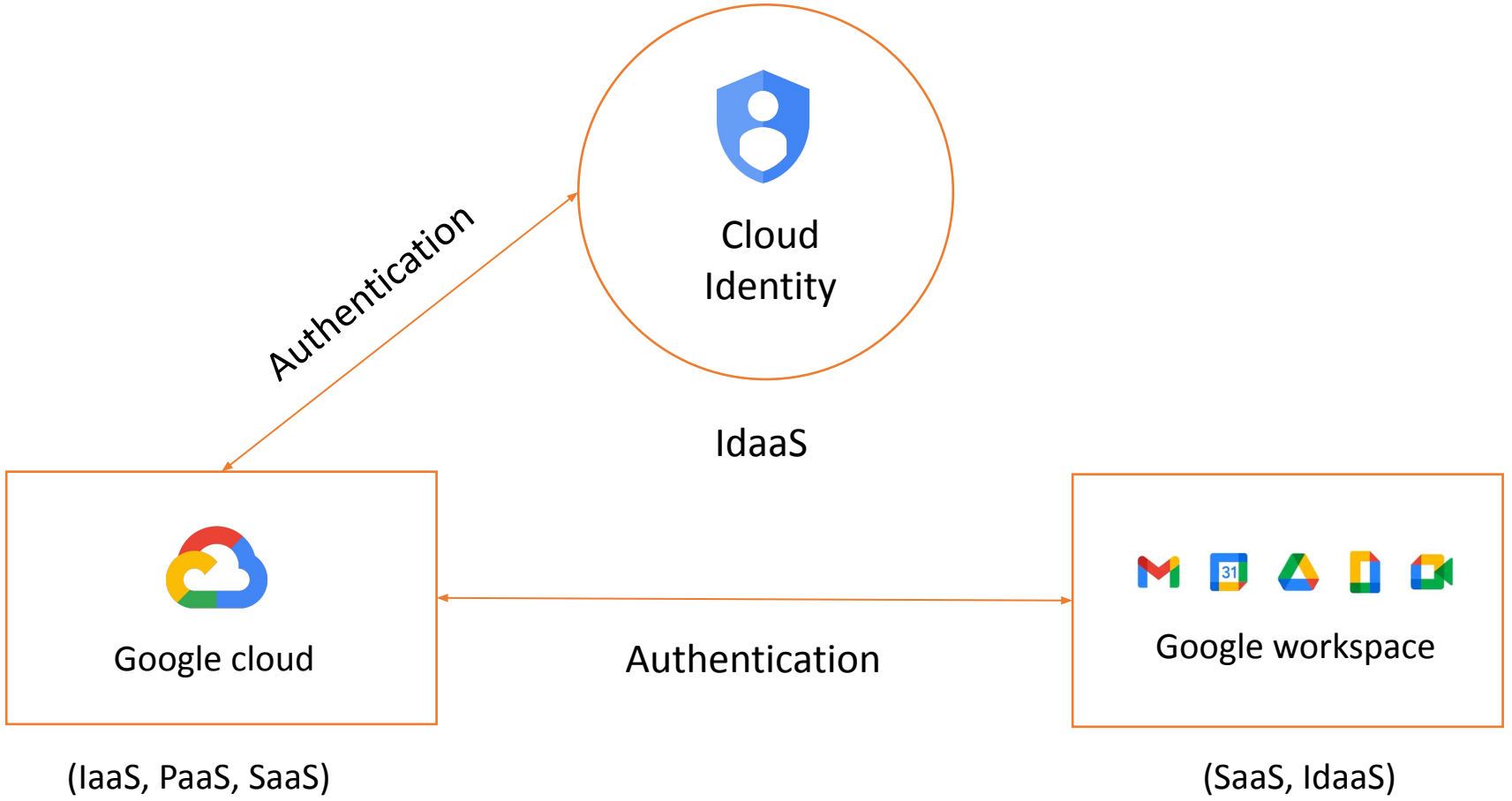
Azure Cloud Working Model



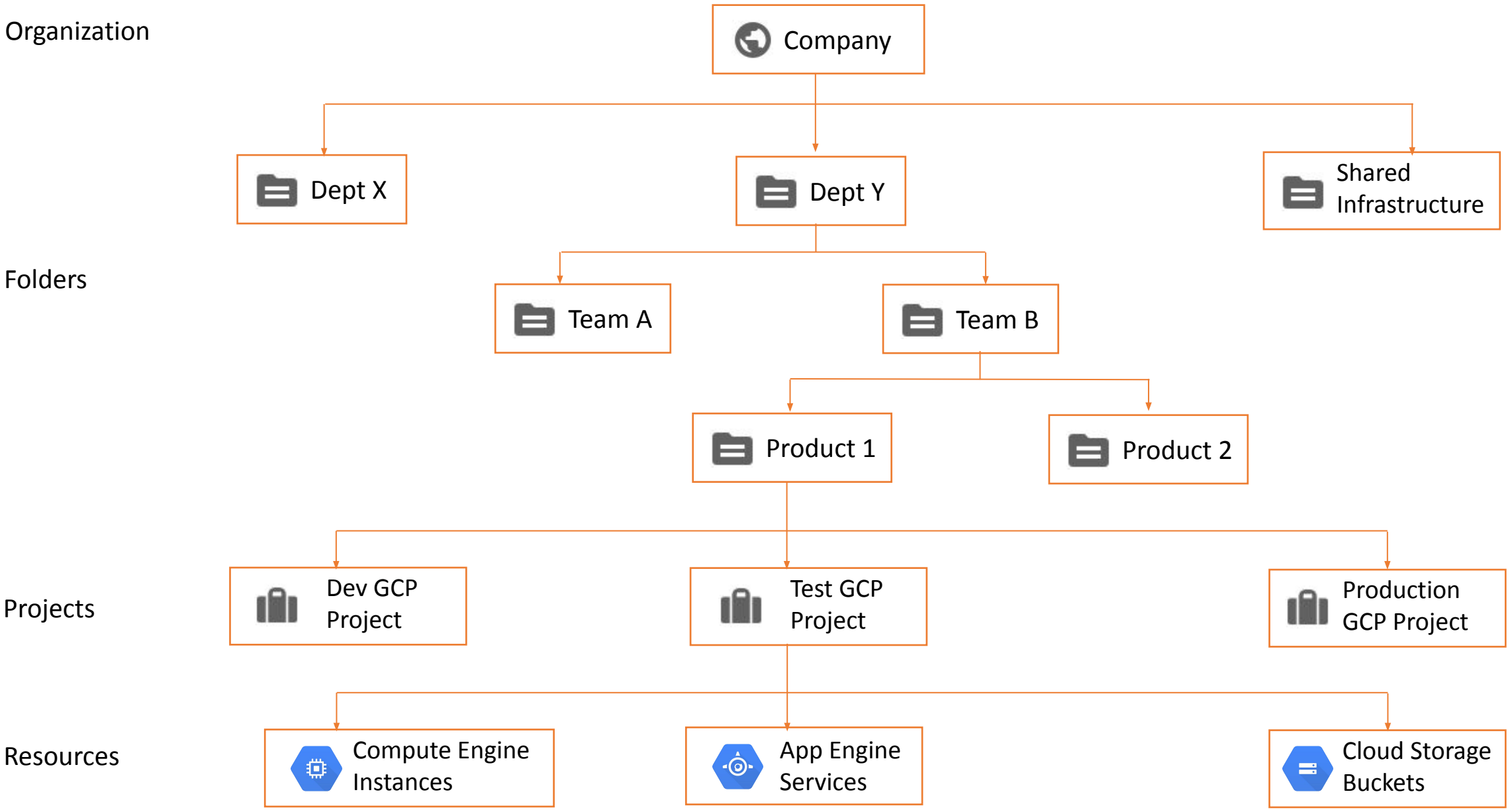
Azure Cloud Hierarchy



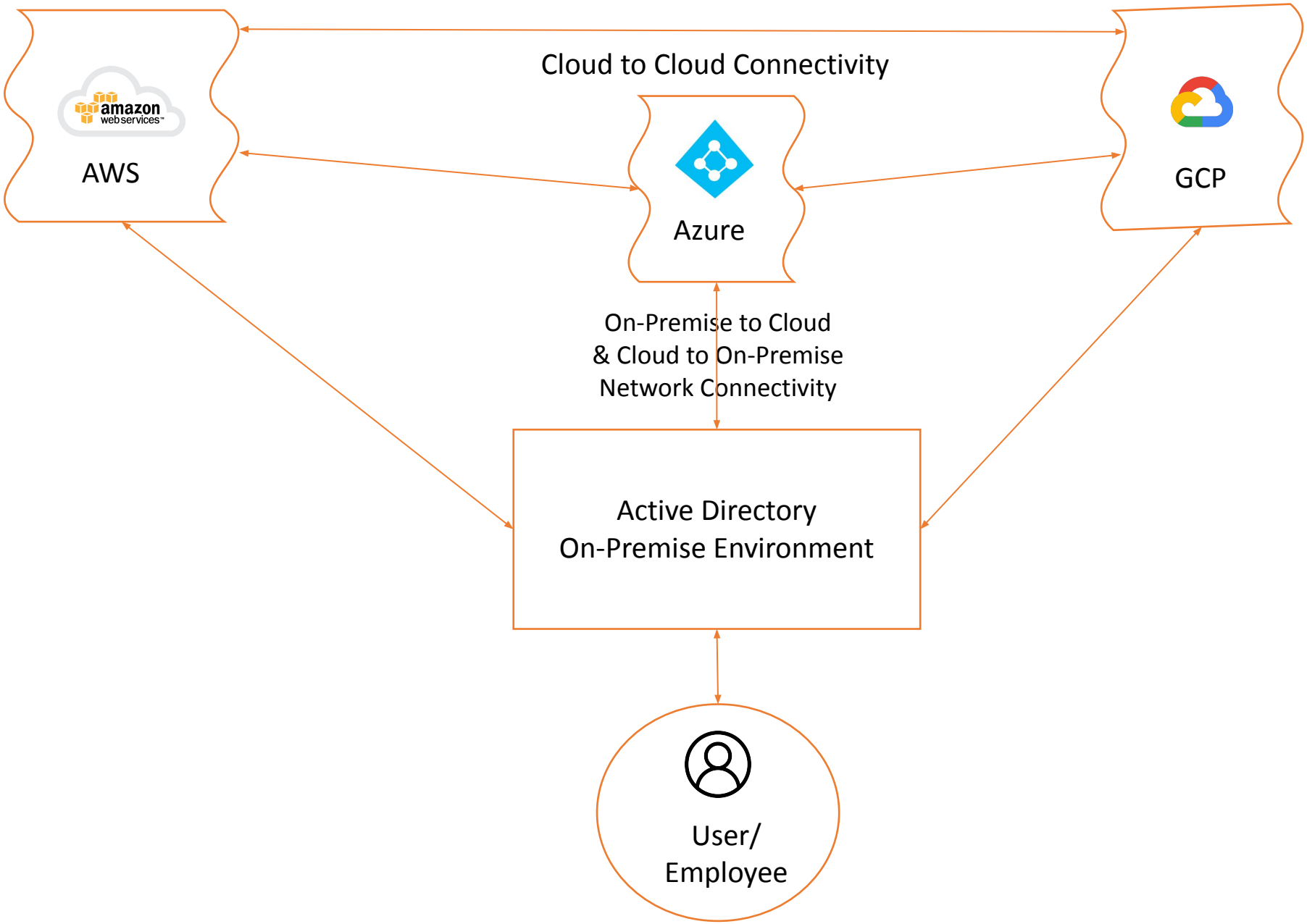
Google Cloud Working Model



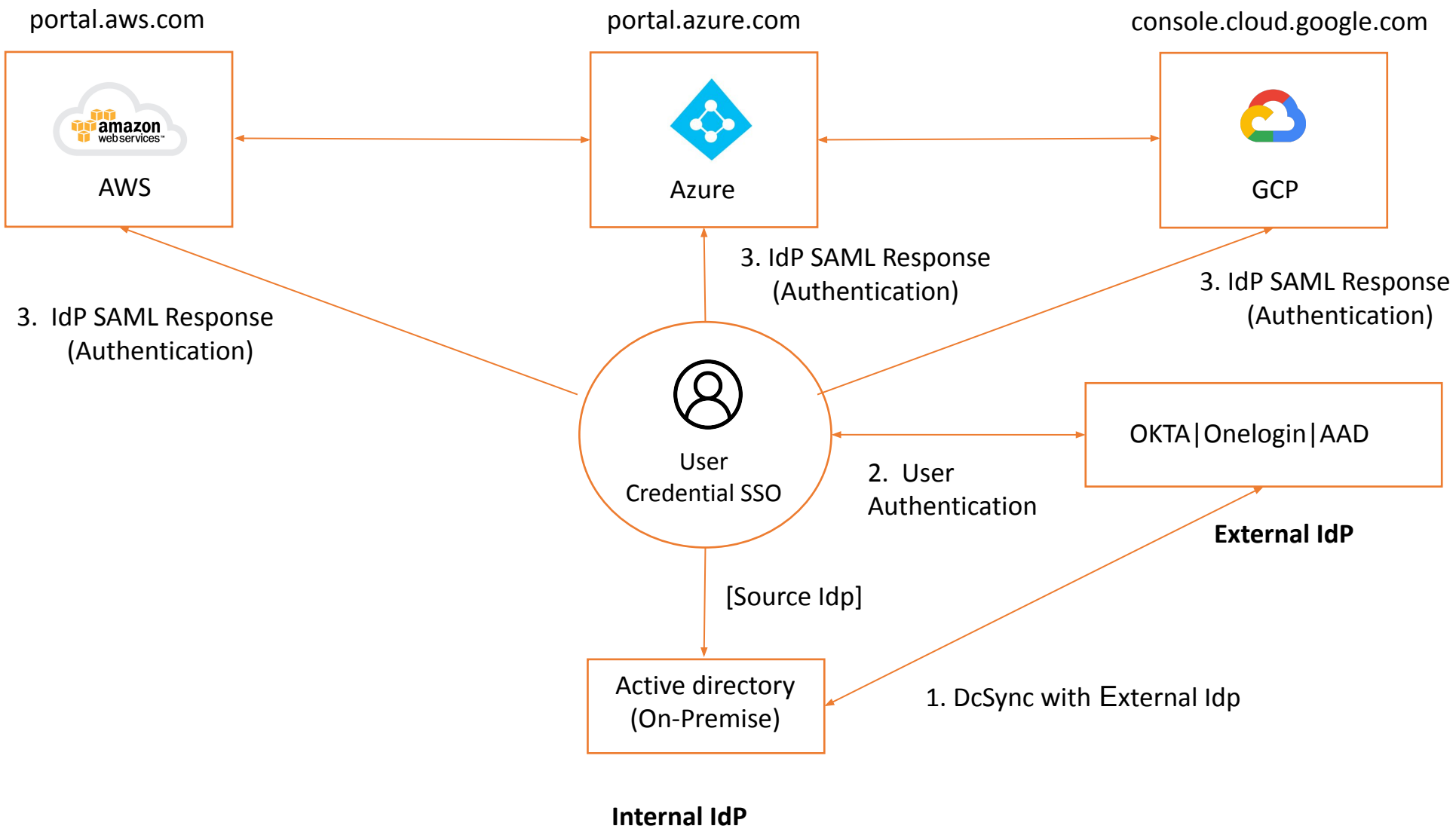
GCP Cloud Hierarchy



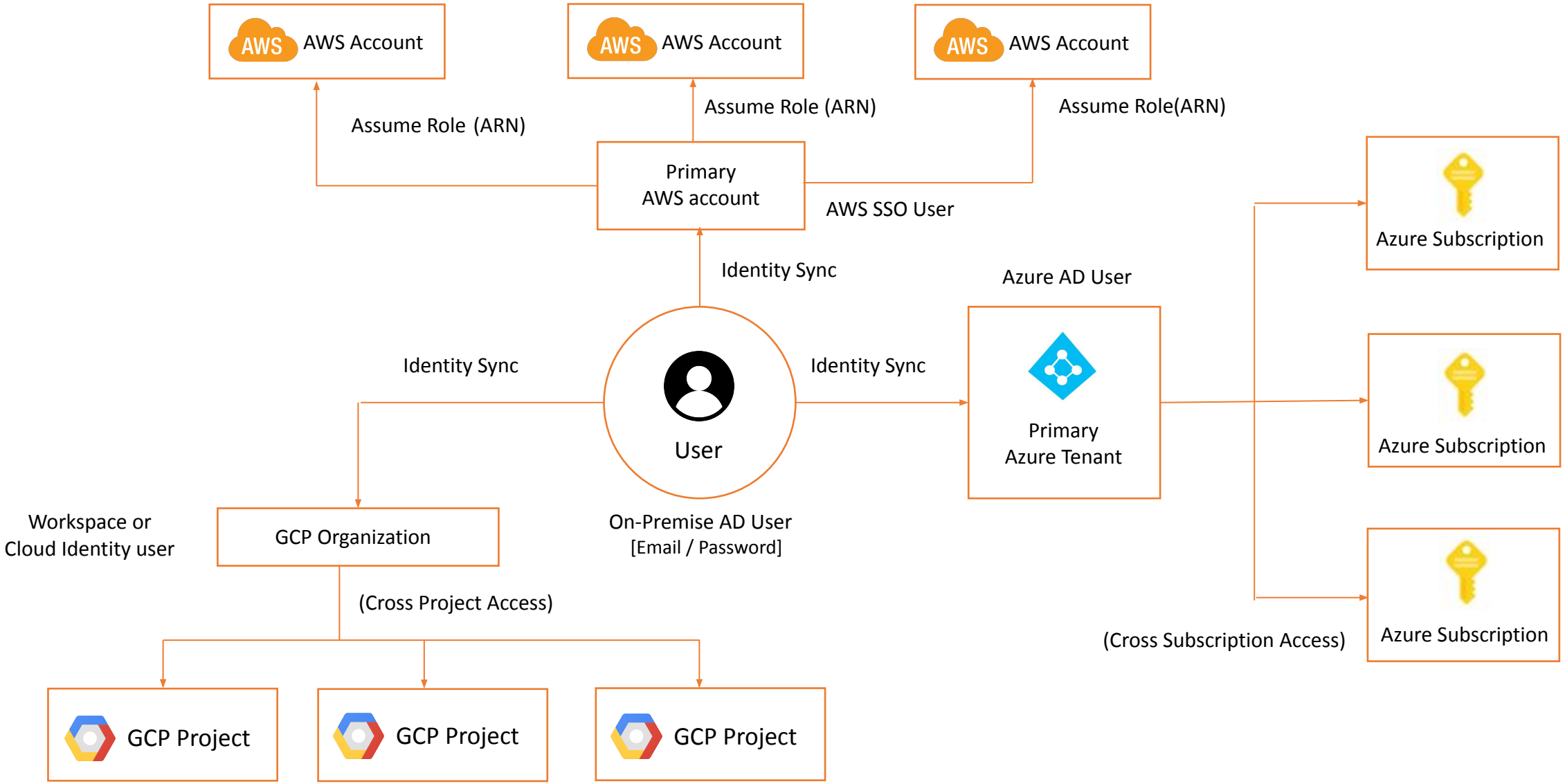
Network Connectivity between Cloud & On-Premise



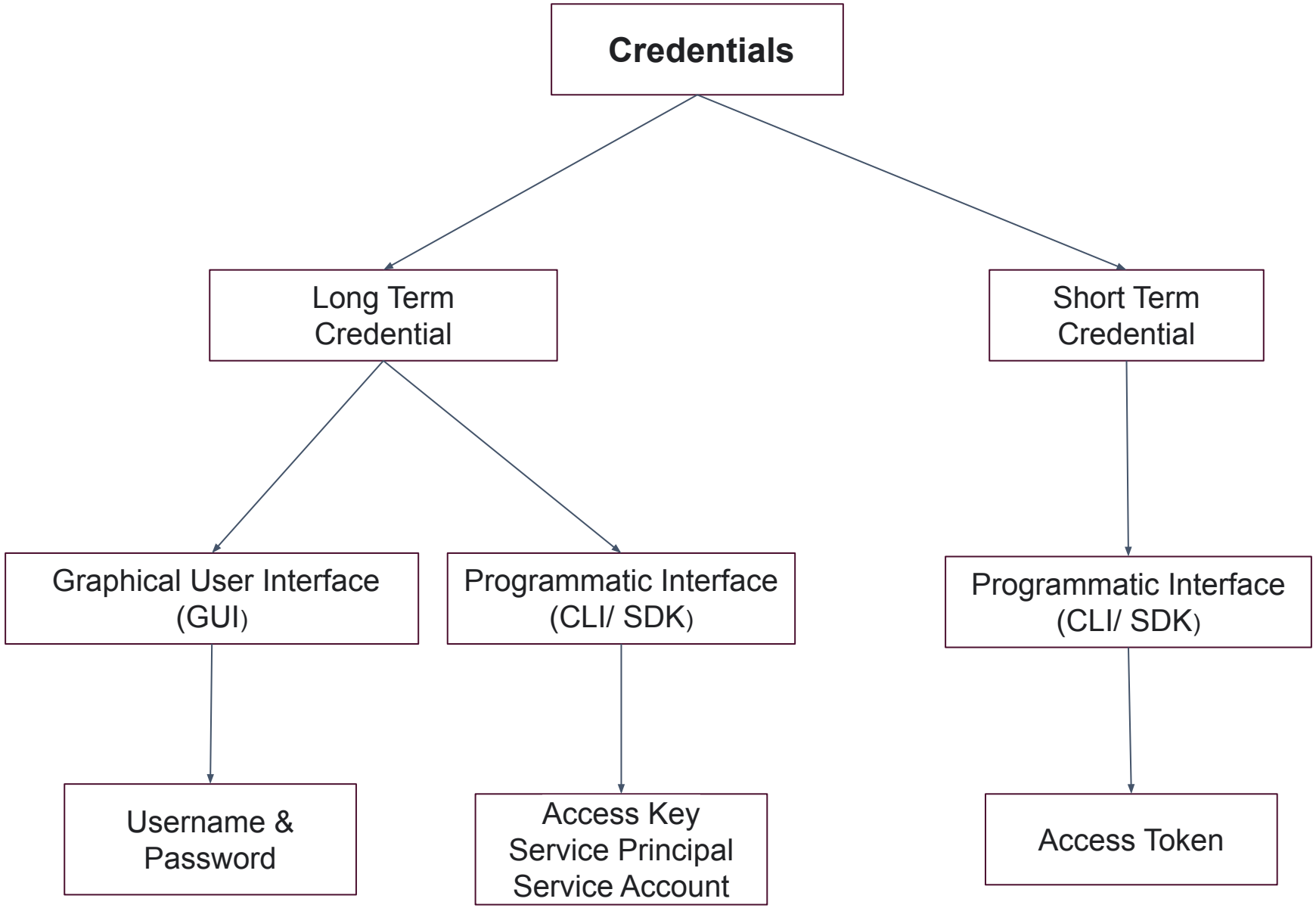
Identity Federation from On-Premise to Cloud



Hybrid Multi Cloud Environment Access

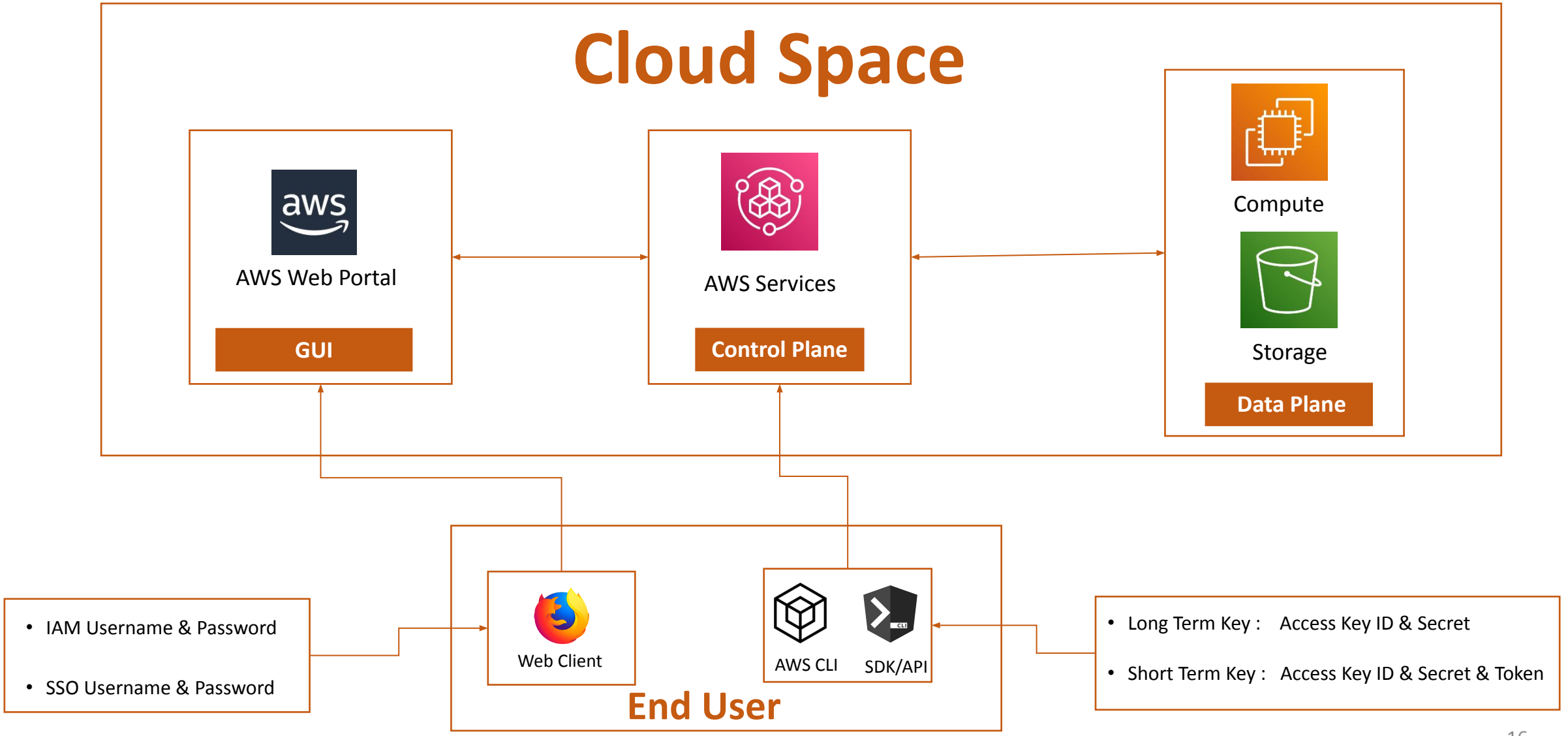


Credentials in Hybrid Multi Cloud Environment



Module - 2 :
AWS Cloud Overview

AWS Cloud Architecture

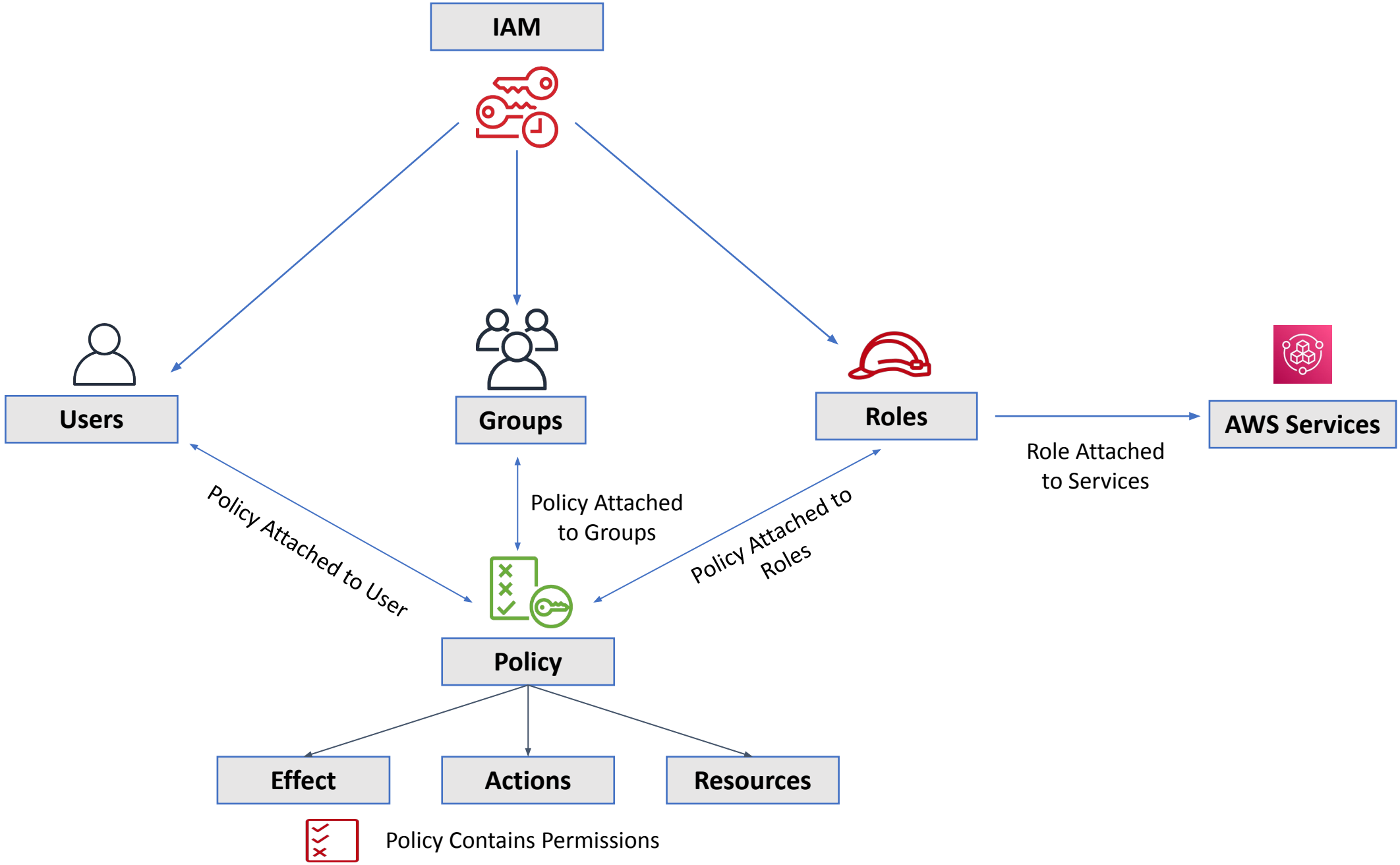


IAM :

- AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely.
- IAM allow you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

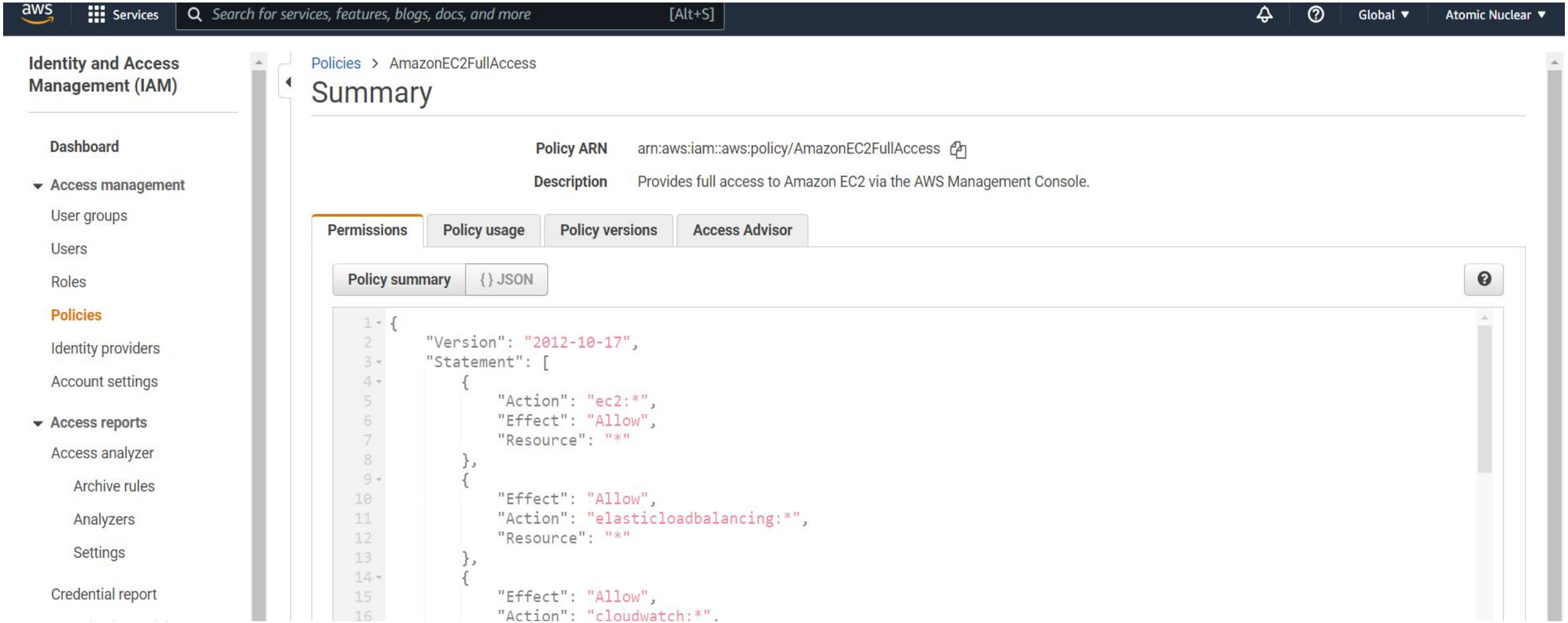
AWS IAM allows:

1. Manage IAM users, groups and their access.
2. Manage IAM roles and their permissions.
3. Manage federated users and their permissions.

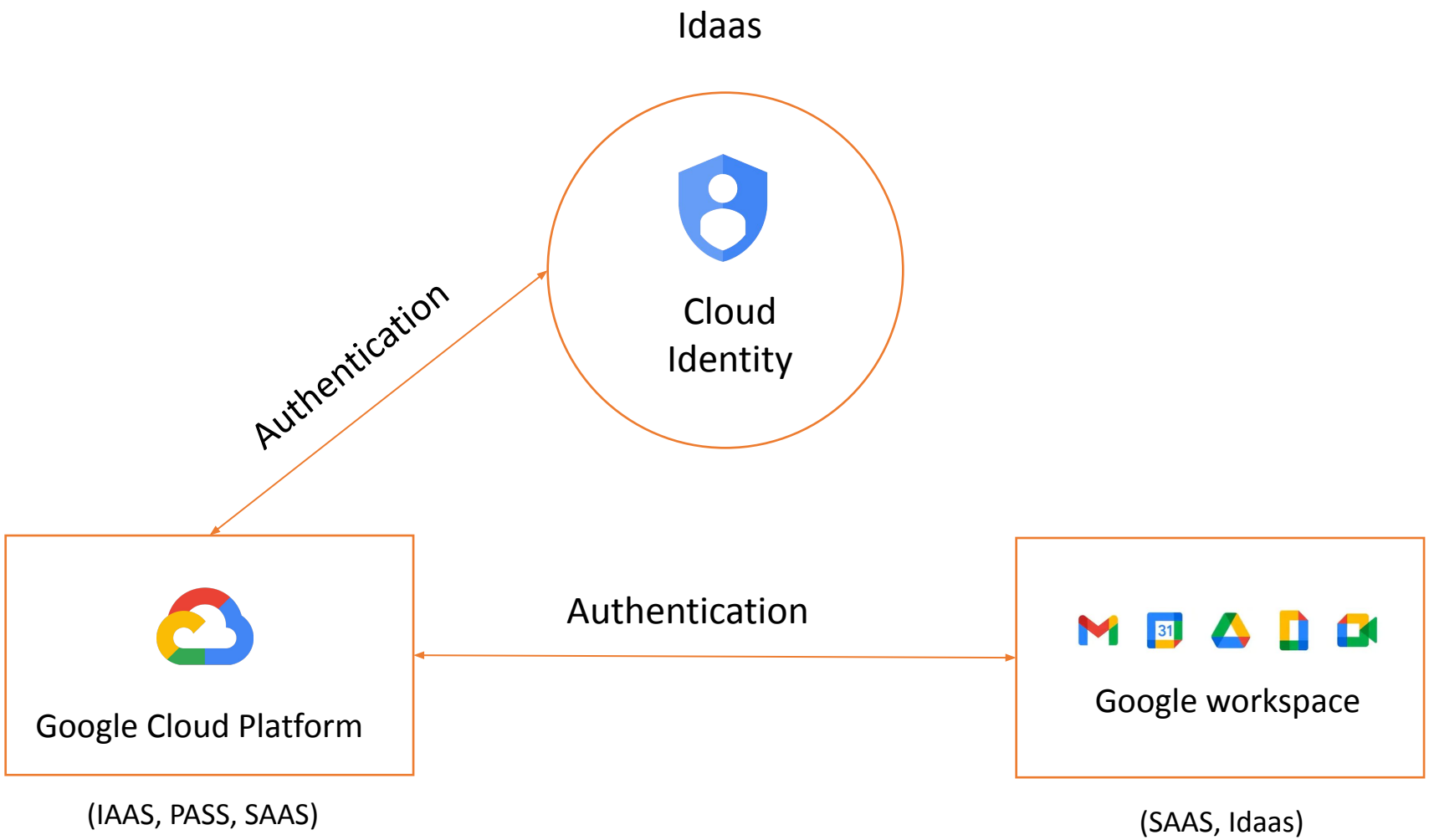

IAM
Users
Groups
Roles
AWS Services
Role Attached to Services
Policy Attached to User
Policy Attached to Groups
Policy Attached to Roles
Policy
Effect
Actions
Resources
Policy Contains Permissions

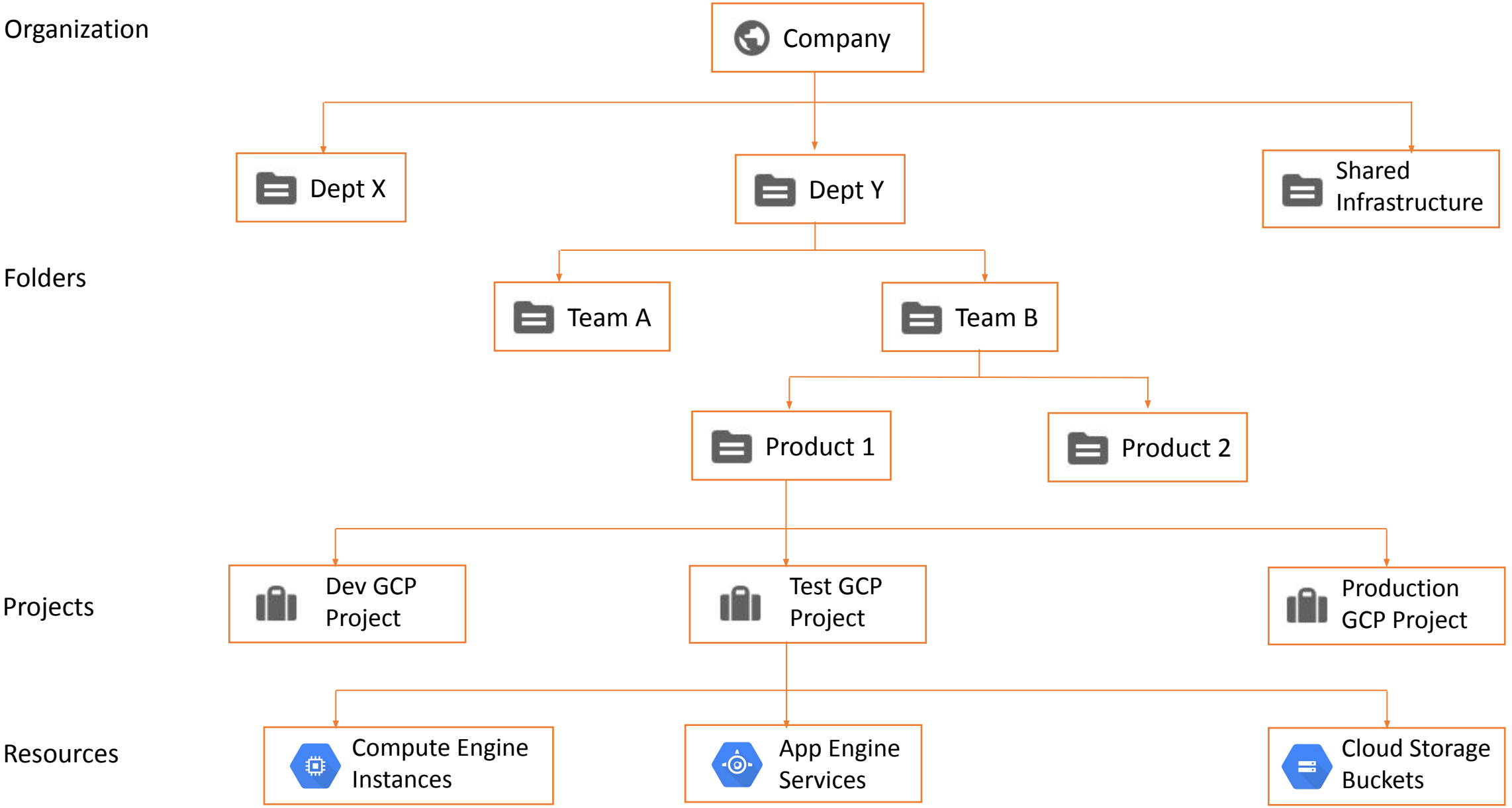
Policy Data :

1. Effect - Use to Allow or Deny Access
2. Action - Include a list of actions (Get, Put, Delete) that the policy allows or denies.
3. Resource - A list of resources to which the actions apply

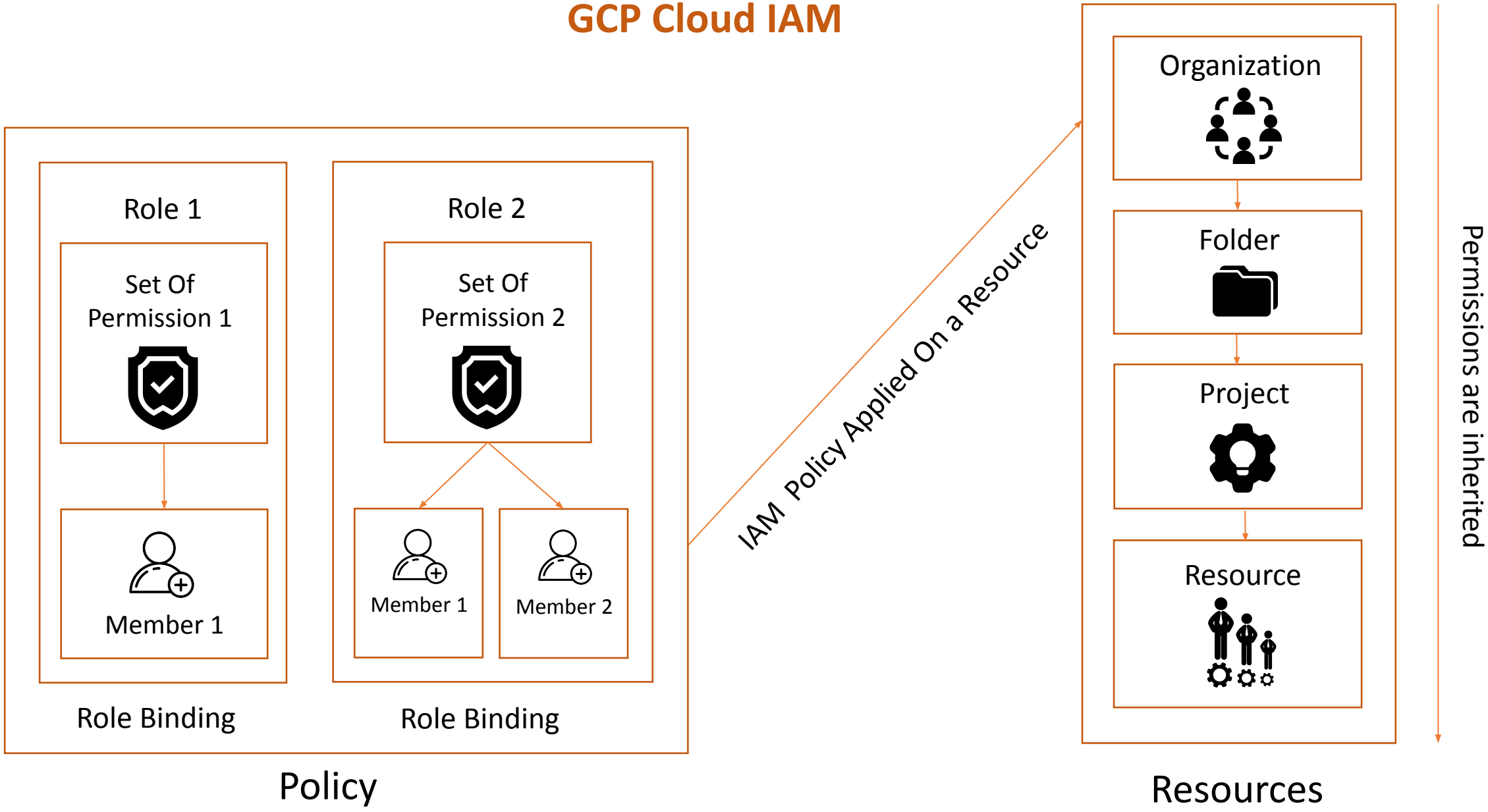


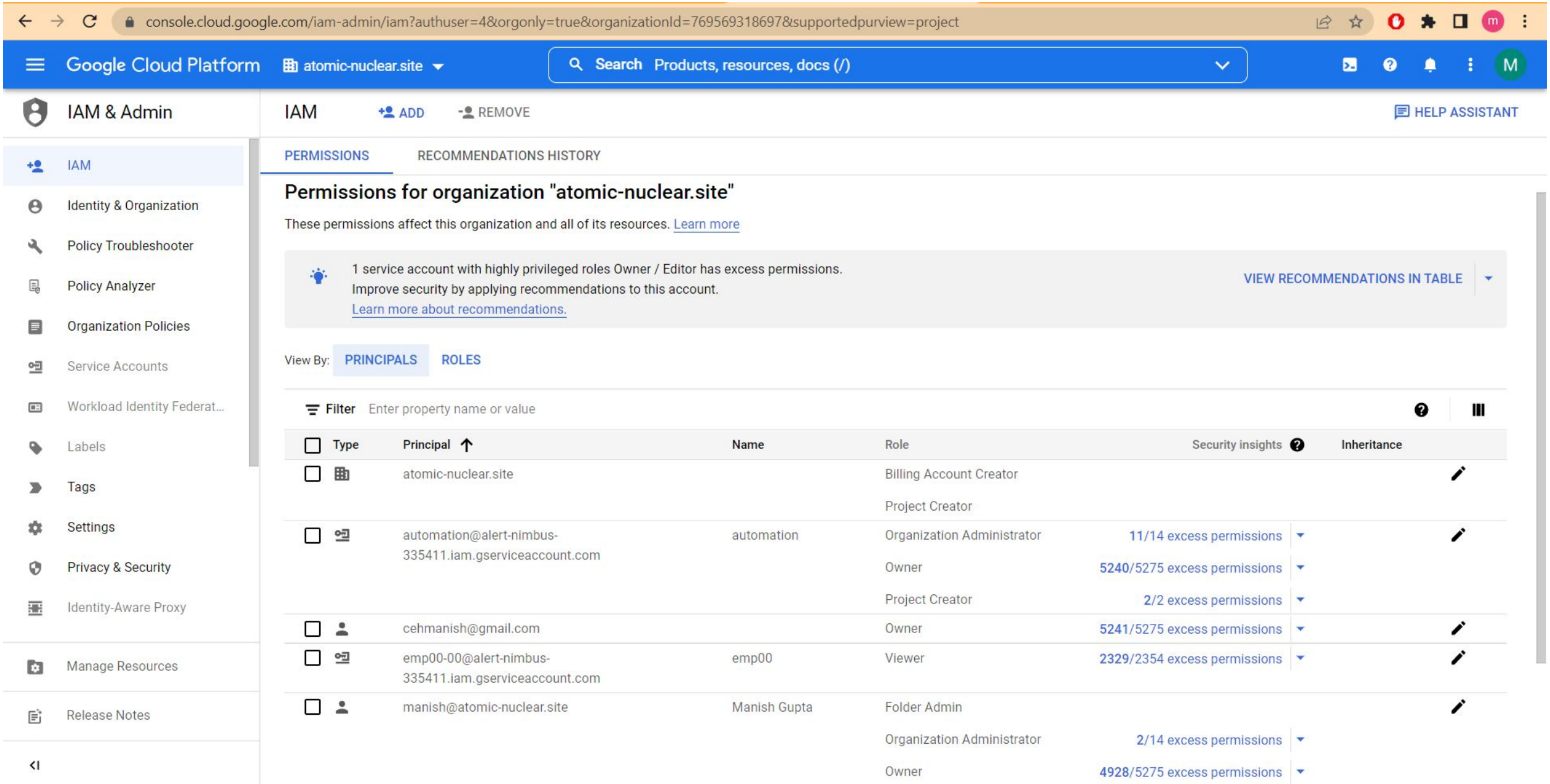
Module - 3 :
Google Cloud Overview


Idaas
Cloud
Identity
Authentication
Google Cloud Platform
(IAAS, PASS, SAAS)
Authentication
Google workspace
(SAAS, Idaas)


Organization
Company
Folders
Dept X
Dept Y
Shared Infrastructure
Team A
Team B
Product 1
Product 2
Projects
Dev GCP Project
Test GCP Project
Production GCP Project
Resources
Compute Engine Instances
App Engine Services
Cloud Storage Buckets

GCP Cloud IAM

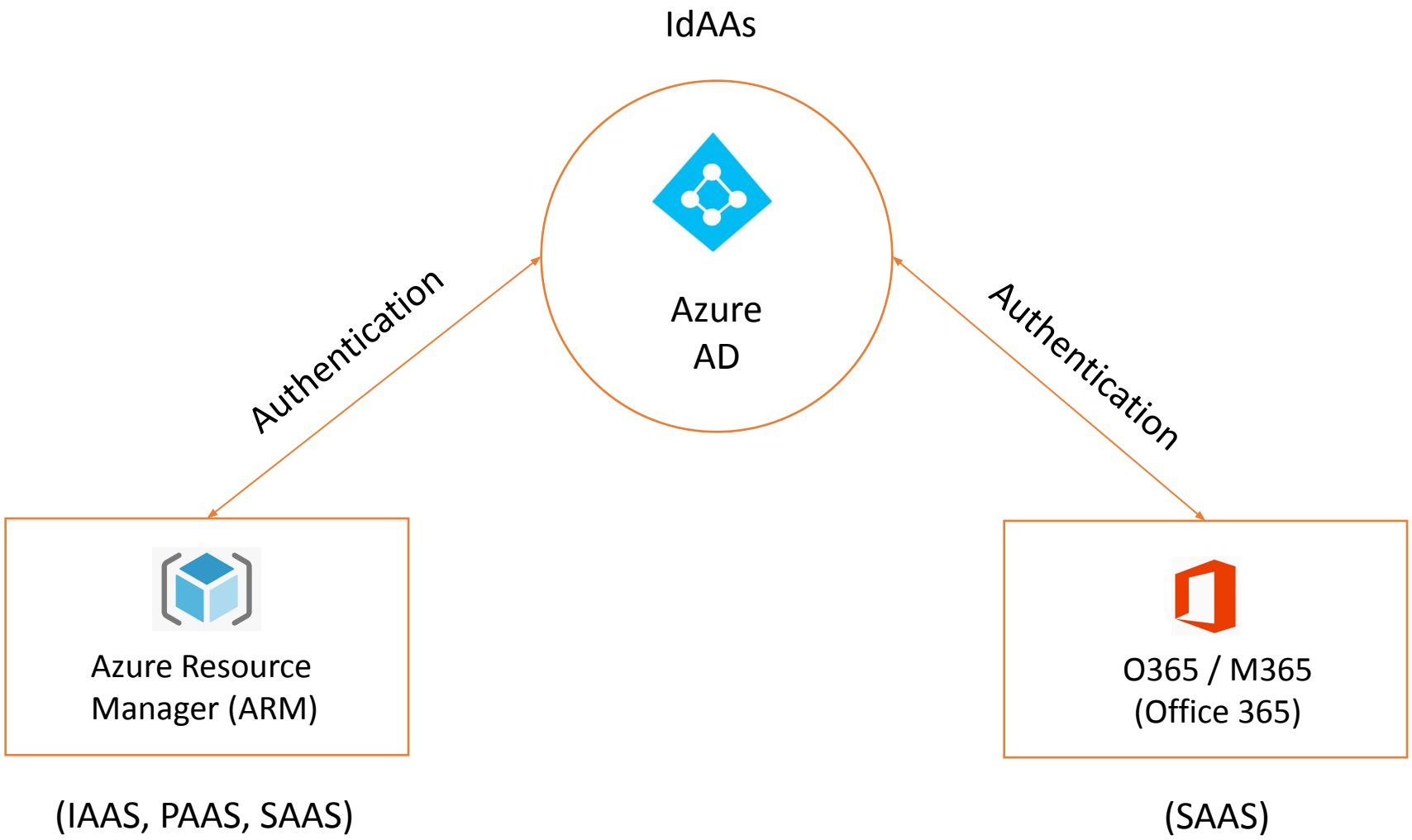




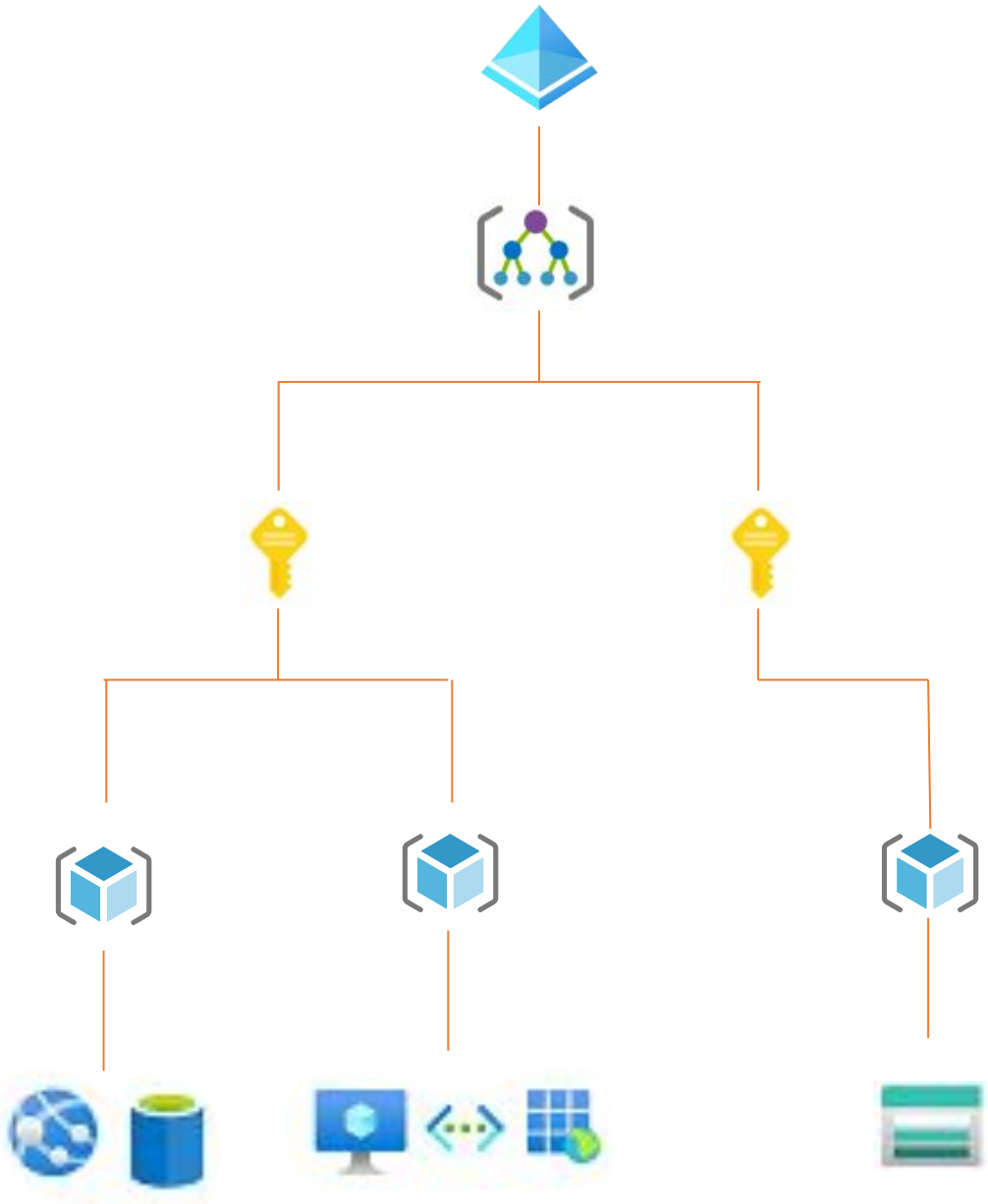
CWL CyberWarFare Labs

IAM Role Binding - Organization Level

Module - 4 :
Azure Cloud Overview


IdAAs
Azure
AD
Authentication
Authentication
Azure Resource
Manager (ARM)
O365 / M365
(Office 365)
(IAAS, PAAS, SAAS)
(SAAS)

Enterprise Global Azure Account



AAD Tenant

Management Group

Subscription

Resource Group

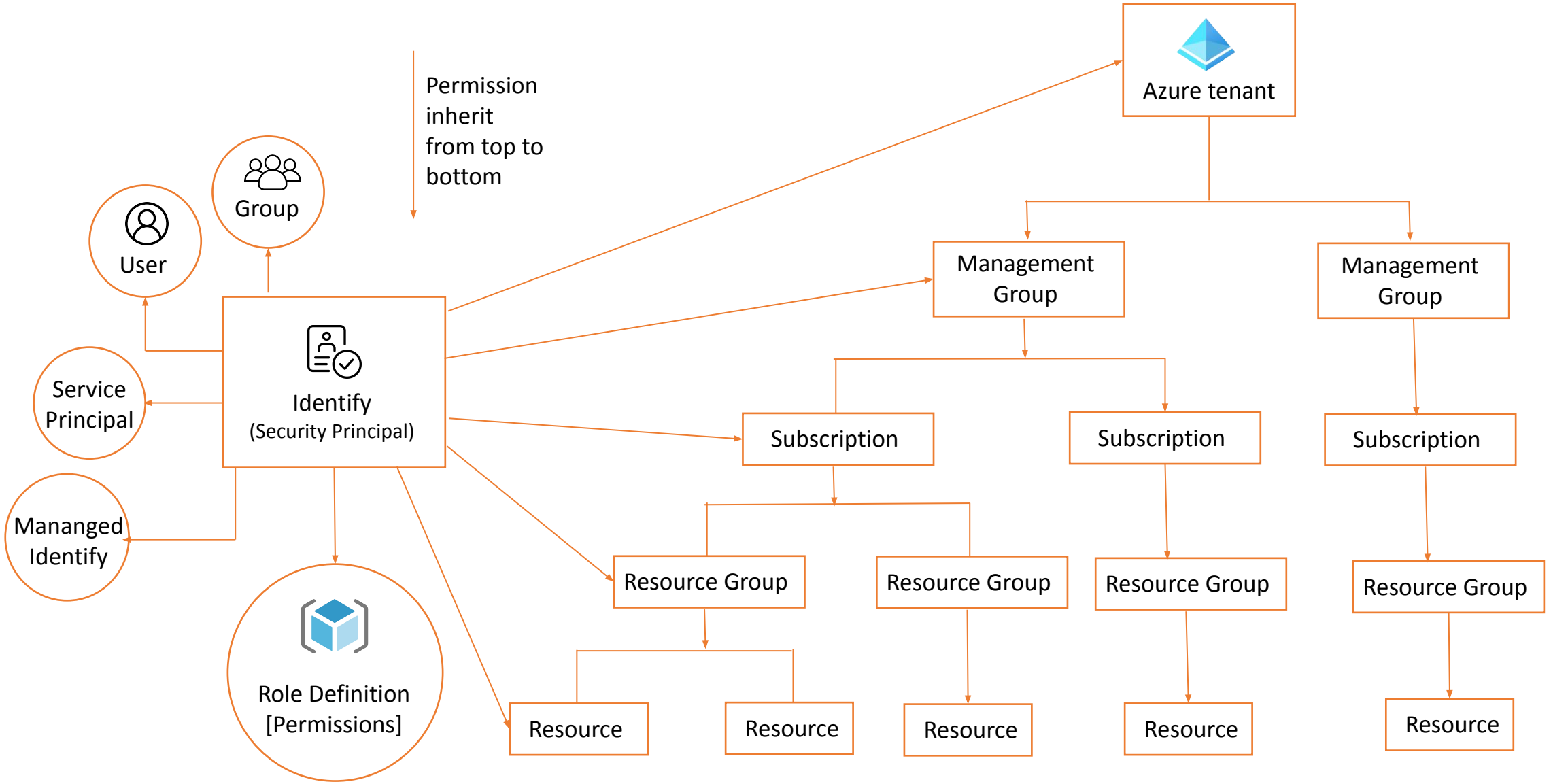
Resource

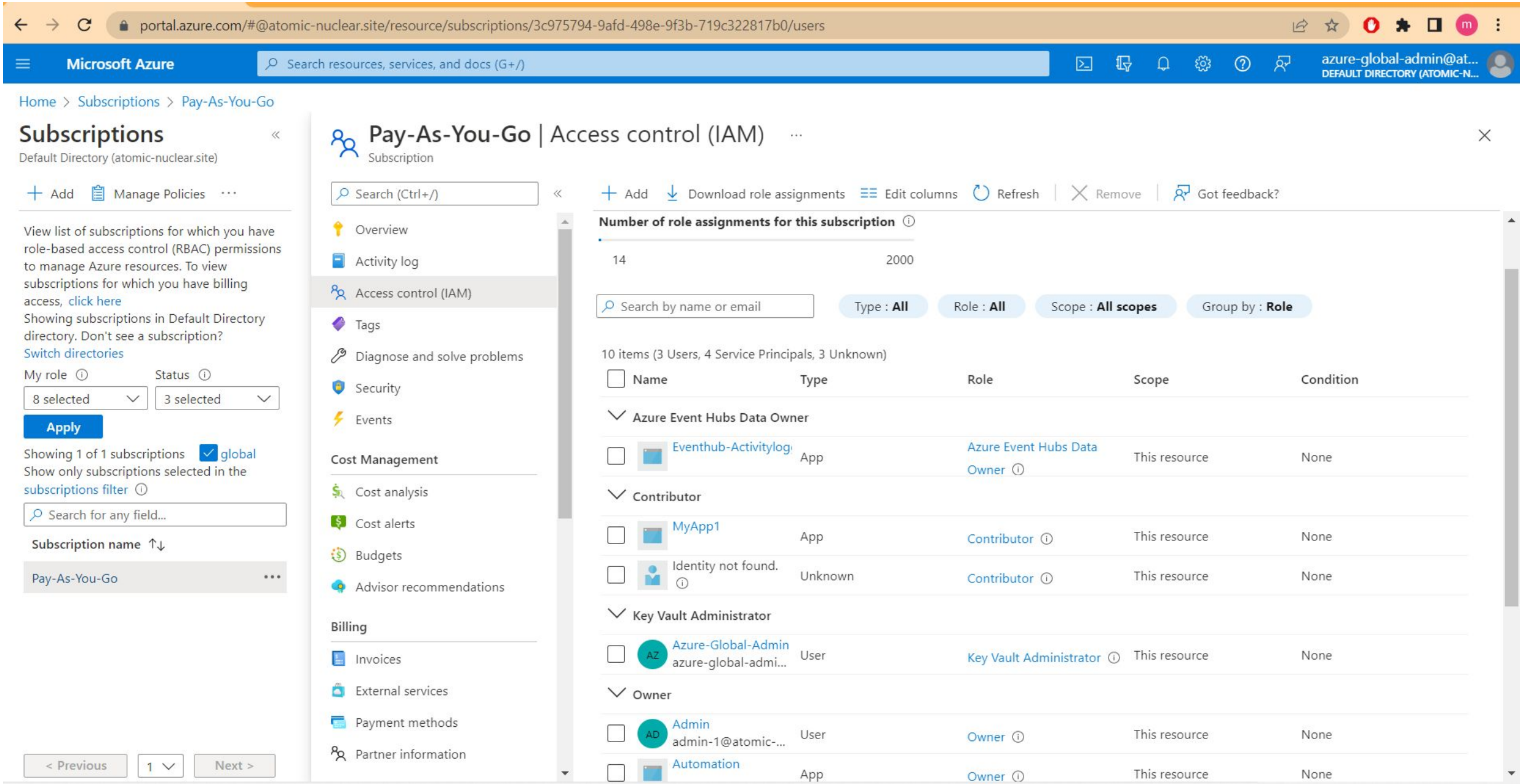
Role Based Access Control (RBAC)

- Azure RBAC is an authorization system built on Azure Resource Manager (ARM) that provides fine-grained access management of Azure resources.

- Role Based Access Control [RBAC] Components -
  - Role Assignment
    - Security principal
    - Scope
    - Roles Definition

Role Assignment Hierarchy




portal.azure.com/#@atomic-nuclear.site/resource/subscriptions/3c975794-9afd-498e-9f3b-719c322817b0/users
Microsoft Azure
Search resources, services, and docs (G+/)
azure-global-admin@at...
DEFAULT DIRECTORY (ATOMIC-N...
Home > Subscriptions > Pay-As-You-Go
Subscriptions
Default Directory (atomic-nuclear.site)
Add
Manage Policies
View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here
Showing subscriptions in Default Directory directory. Don't see a subscription?
Switch directories
My role
8 selected
Status
3 selected
Apply
Showing 1 of 1 subscriptions
global
Show only subscriptions selected in the subscriptions filter
Search for any field...
Subscription name
Pay-As-You-Go
< Previous
1
Next >
Pay-As-You-Go | Access control (IAM)
Subscription
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events
Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations
Billing
Invoices
External services
Payment methods
Partner information
Add
Download role assignments
Edit columns
Refresh
Remove
Got feedback?
Number of role assignments for this subscription
14
2000
Search by name or email
Type : All
Role : All
Scope : All scopes
Group by : Role
10 items (3 Users, 4 Service Principals, 3 Unknown)
Name
Type
Role
Scope
Condition
Azure Event Hubs Data Owner
Eventhub-Activitylog
App
Azure Event Hubs Data Owner
This resource
None
Contributor
MyApp1
App
Contributor
This resource
None
Identity not found.
Unknown
Contributor
This resource
None
Key Vault Administrator
Azure-Global-Admin
azure-global-admi...
User
Key Vault Administrator
This resource
None
Owner
Admin
admin-1@atomic-...
User
Owner
This resource
None
Automation
App
Owner
This resource
None

Thank You !

In case of any difficulties or queries, feel free to mail us at support@cyberwarfare.live

- Follow us on :
  LinkedIn: https://www.linkedin.com/company/cyberwarfare/
  Twitter: https://twitter.com/cyberwarfarelab

- For More Information Visit :
  Enterprise Red / Blue Team Lab : https://cyberwarfare.live
  Red /Blue Team Blog: https://cyberwarfare.live/blog/