SIMON MAXWELL-STEWART
SR. SECURITY RESEARCHER @ BEYONDTRUST

From Azure subscription to backdoor intruder

RESTLESS GUESTS

SIMON MAXWELL-STEWART

WHO AM I?

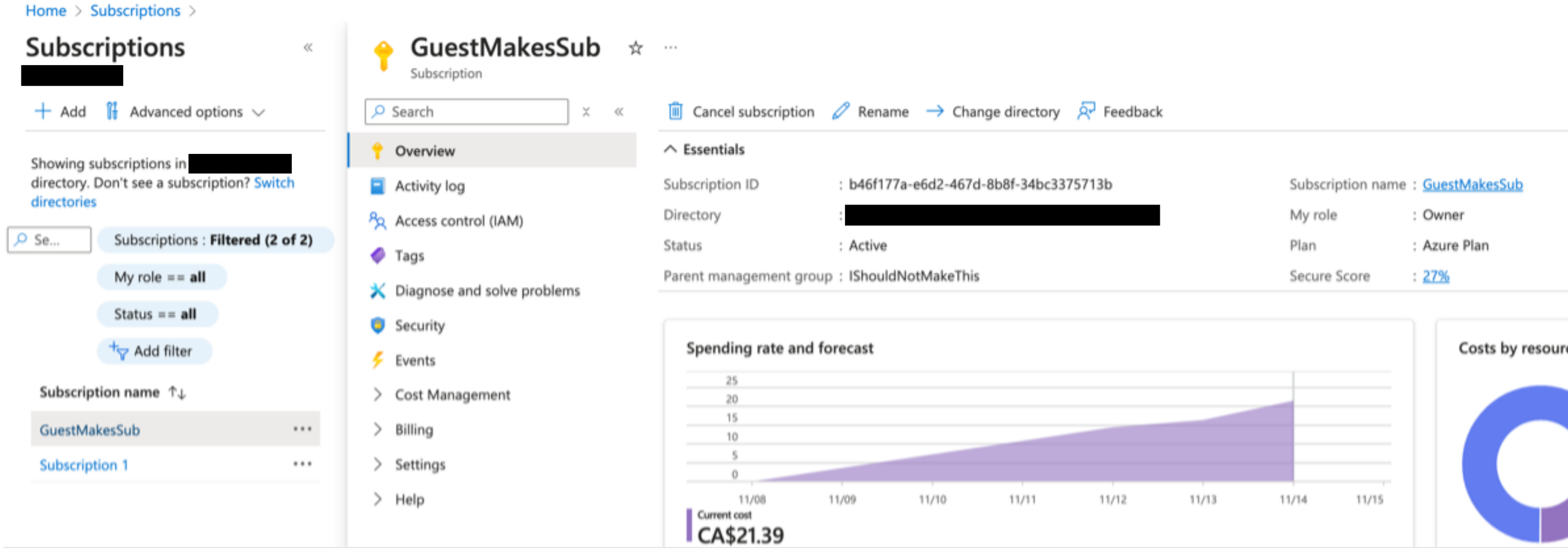
- Physics Undergraduate, University of Oxford
- 8 years in Software and Data Engineering
- 2 years as Lead Data Scientist in Healthcare
- 2 years in Cybersecurity
- Presently resident “graph nerd” at BeyondTrust’s Phantom Labs research team

AGENDA

- INTRO - A mystery!
- Azure
  - Basics
  - In the weeds
  - Undocumented behaviour
- Microsoft’s Position
- Possible ways to abuse
- Defence

LET'S SOLVE A MYSTERY

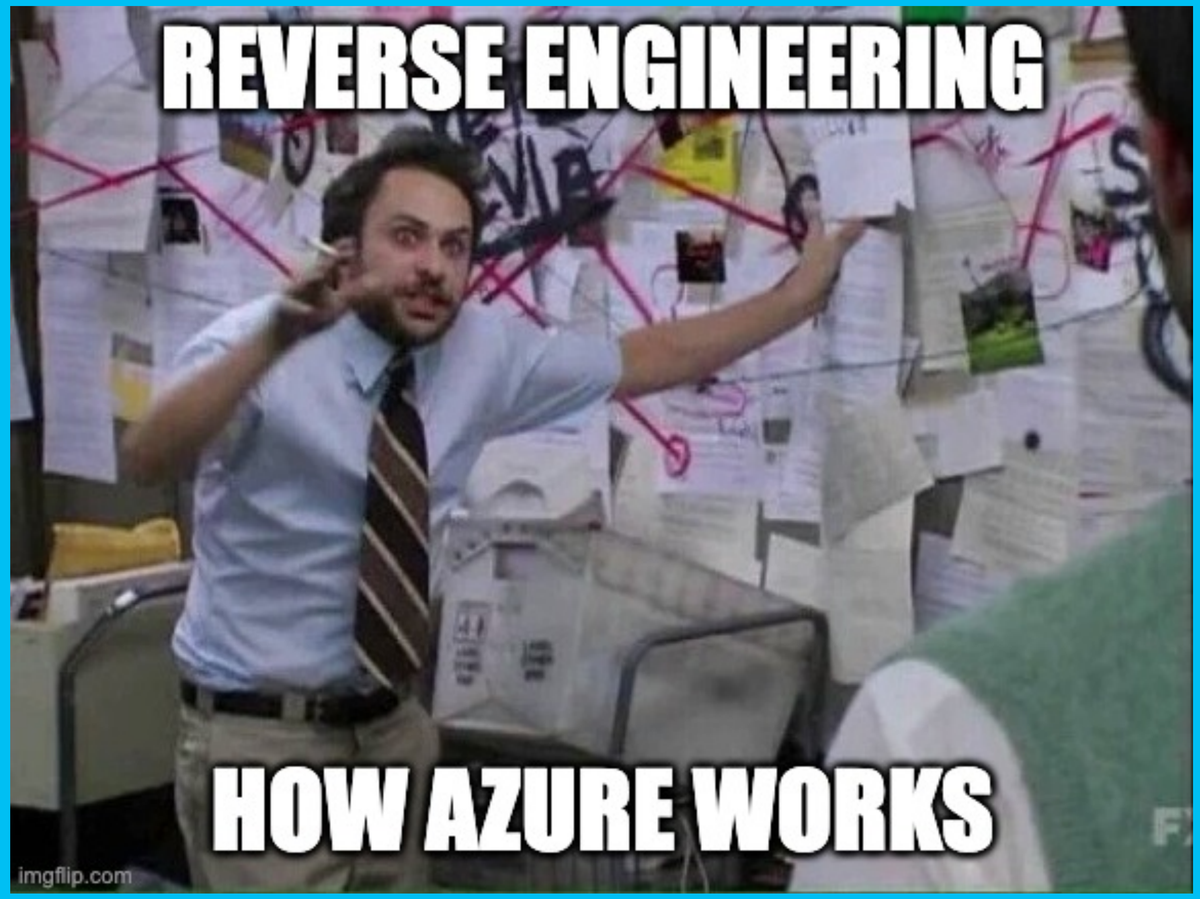
HOW DID A GUEST MAKE A SUBSCRIPTION?!



Guest made subscription!

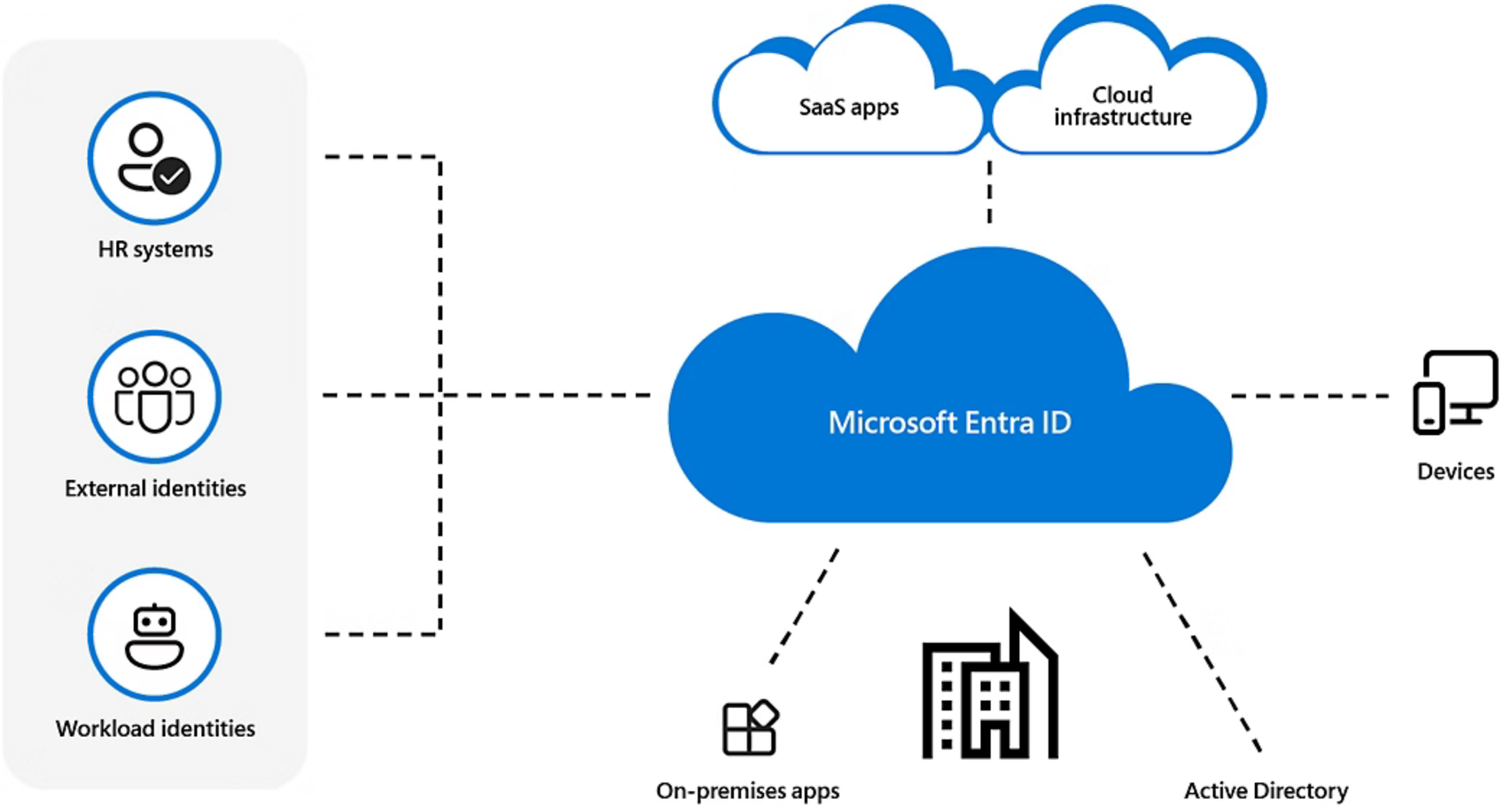
FACTS ABOUT THE CASE

- Entra ID account credentials leaked to the dark web
- Account is a guest B2B user in tenant
- Guest user had no
  - group memberships
  - directory roles
  - RBAC roles
  - permissions granted
- Somehow guest made a subscription?



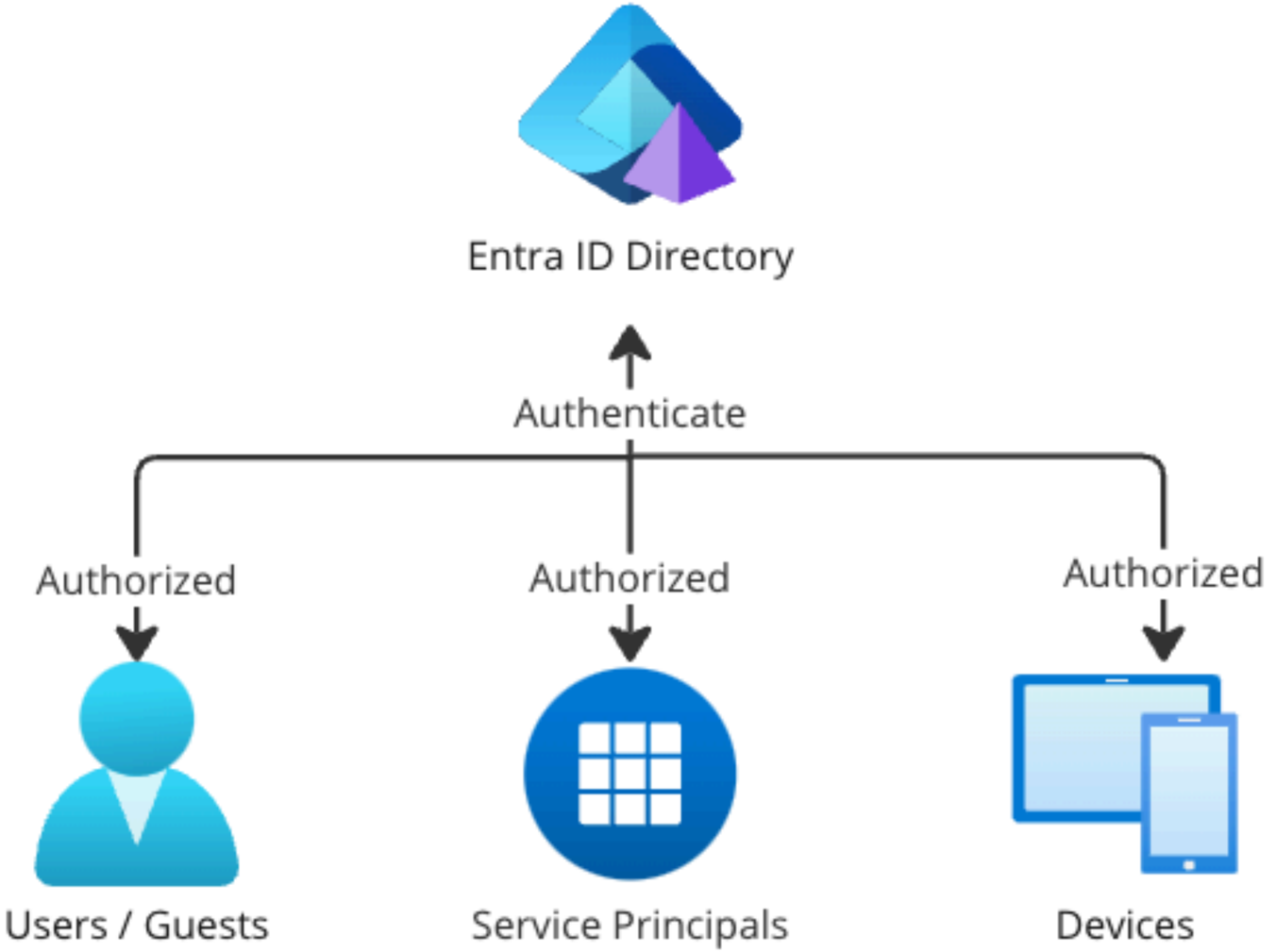
AZURE - BASICS

ENTRA ID

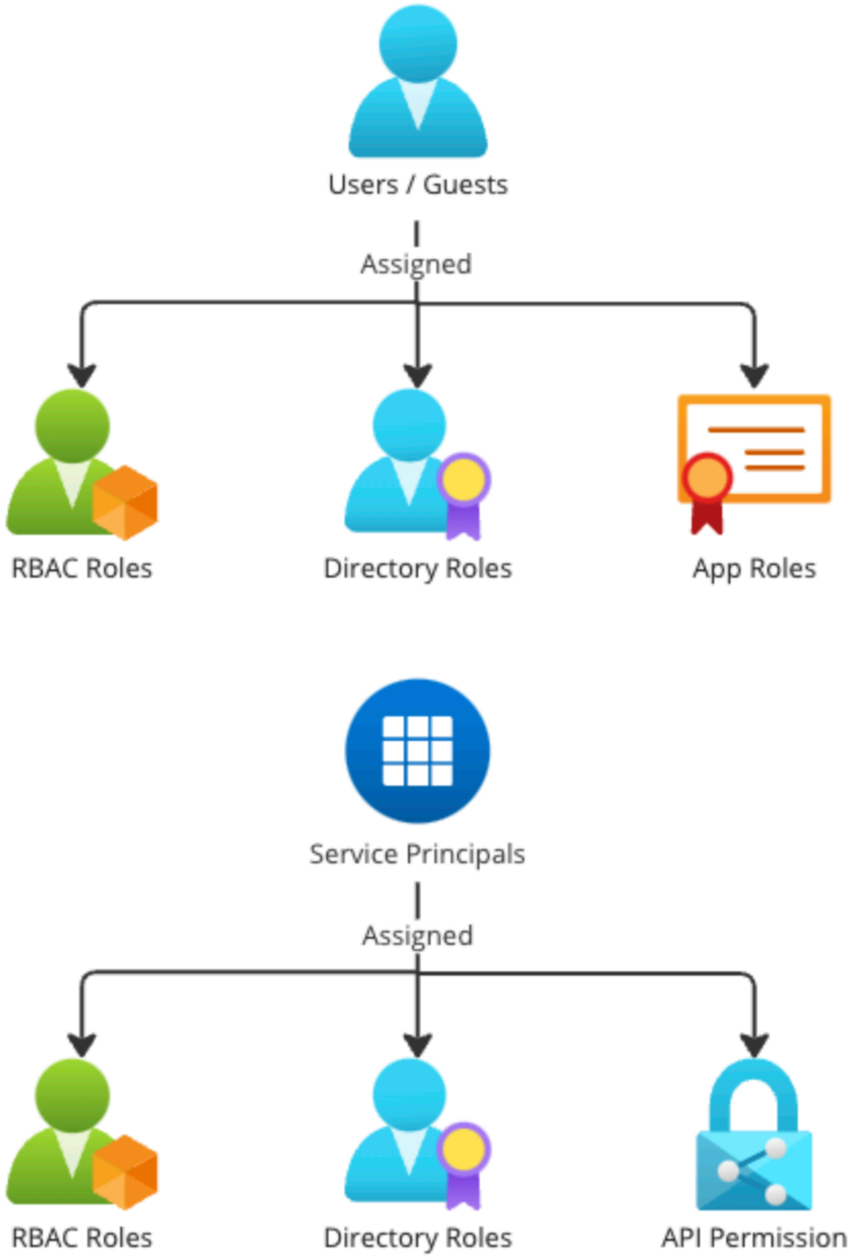


From Microsoft's Entra ID homepage

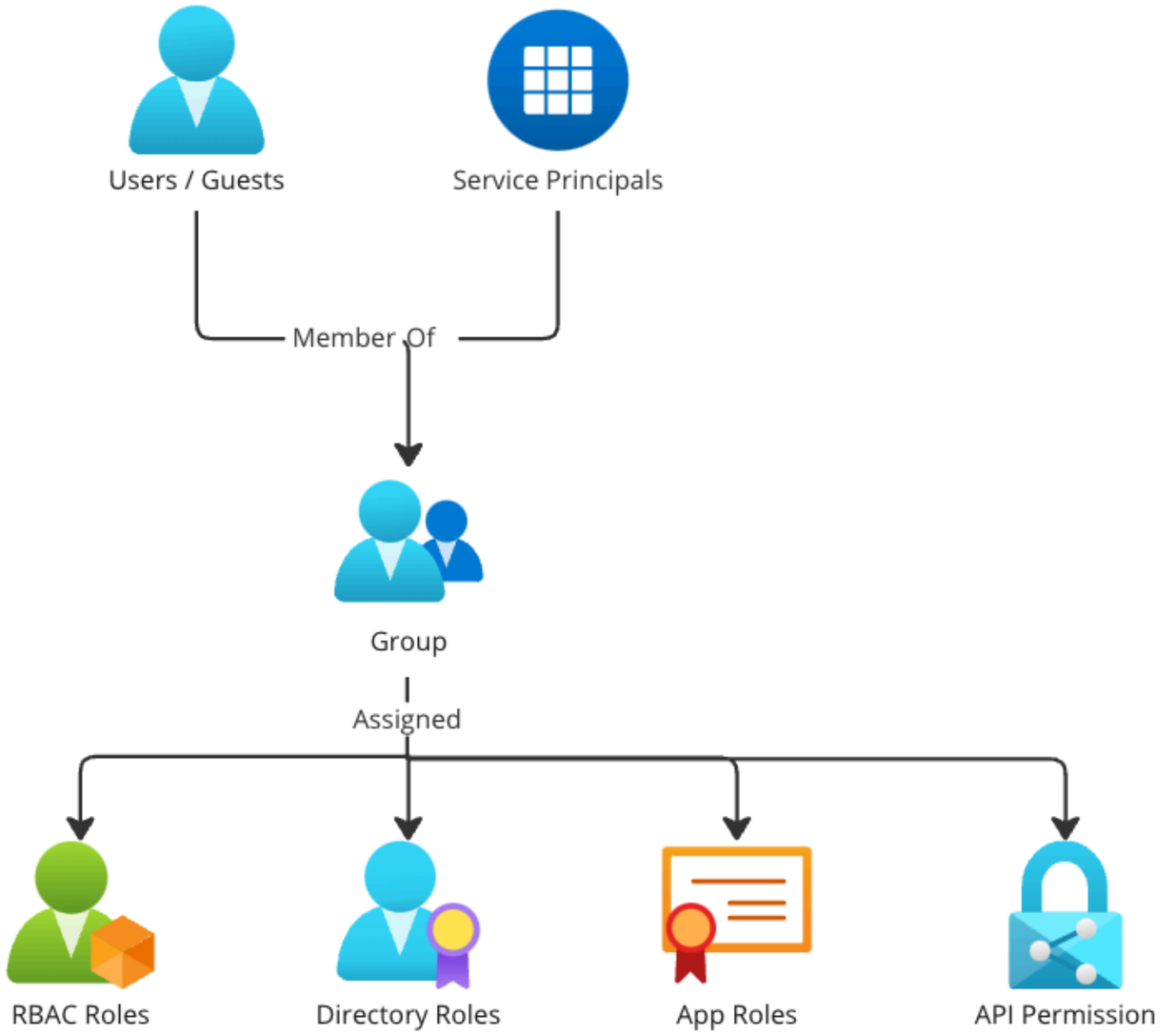
ENTRA ID BASICS



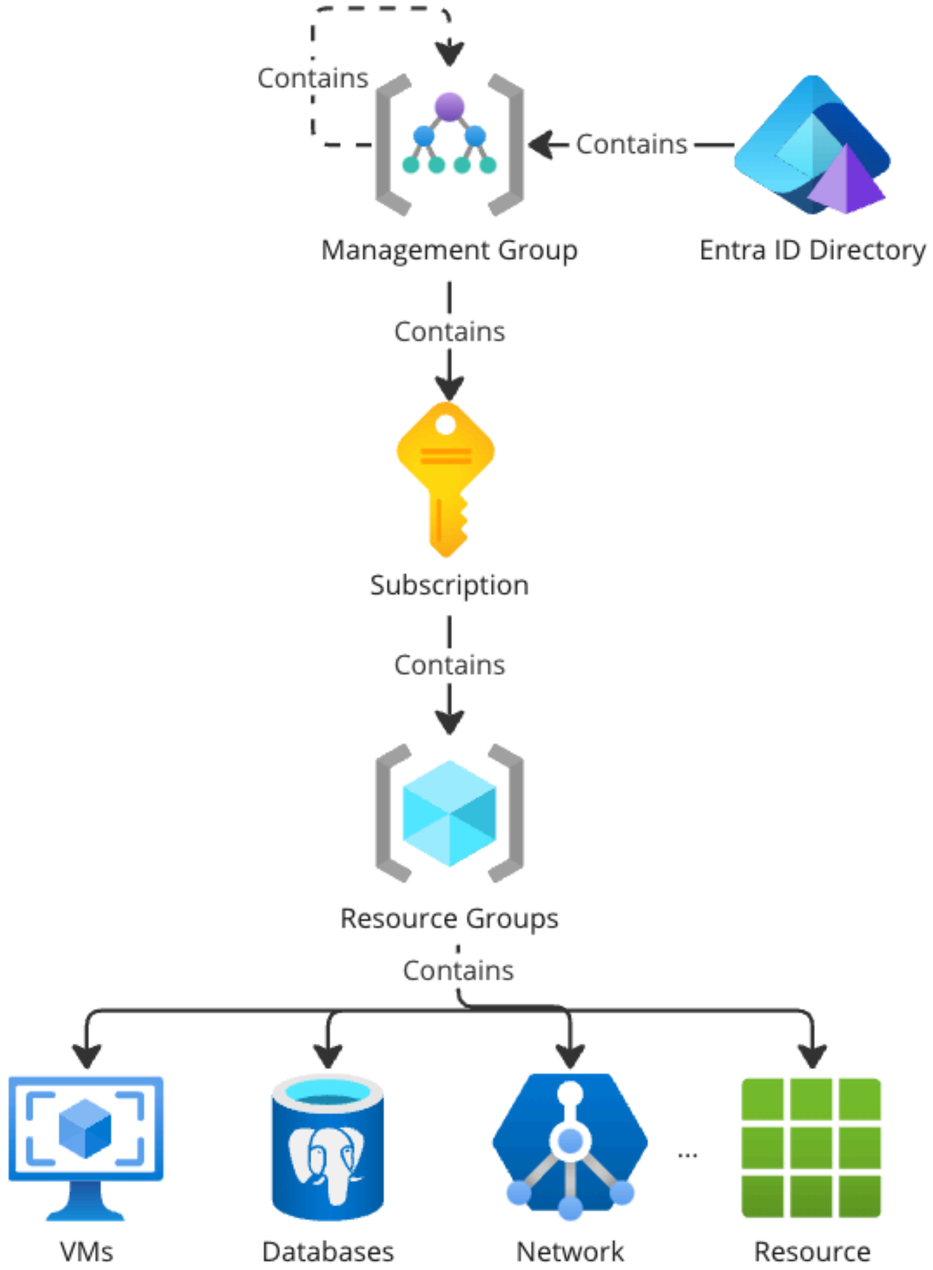
ENTRA ID
BASIC PRIVILEGES



ENTRA ID GROUPS



AZURE RESOURCES BASICS



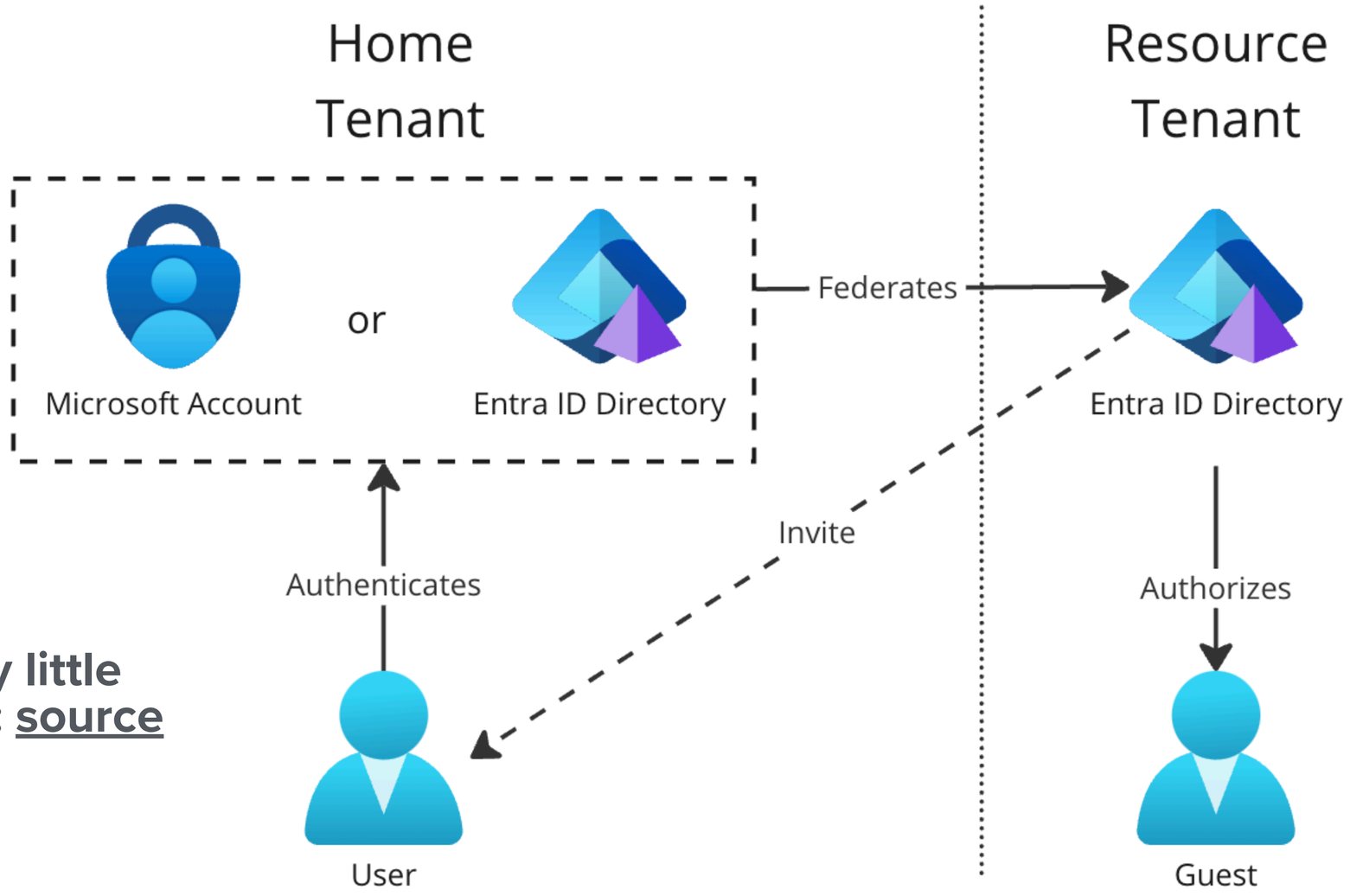
AZURE RESOURCES RBAC ROLES

Built-in role	Description
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 galleries.
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Reservations Administrator	Lets one read and manage all the reservations in a tenant
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure Policy.
User Access Administrator	Lets you manage user access to Azure resources.
Reader	View all resources, but does not allow you to make any changes.

Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

AZURE - INTO THE WEEDS

ENTRA ID B2B GUESTS



- **Guests have very little default privilege: source docs**

Simon Guest

User

Search

- Overview
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Custom security attributes
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods
- New support request

Edit properties | Delete | Refresh | Reset password | Revoke sessions | Manage view | Got feedback?

Overview | Monitoring | Properties

Basic info

SG

Simon Guest

smaxwellstewart[redacted]

Guest

User principal name	smaxwellstewa[redacted]	Group memberships	0
Object ID	9dcc4cb4-cd48-4531-a38a-6647ebe78cd7	Applications	0
Created date time	Nov 7, 2024, 9:13 AM	Assigned roles	0
User type	Guest	Assigned licenses	0
Identities	MicrosoftAccount		

My Feed

Account status

Enabled

Edit

Sign-ins

Last interactive sign-in: Nov 13, 2024, 4:07 PM

Last non-interactive sign-in: Nov 13, 2024, 7:47 PM

See all sign-ins

B2B invitation

Invitation state: Accepted

Reset redemption status

B2B collaboration

Current user is external

Convert to internal user

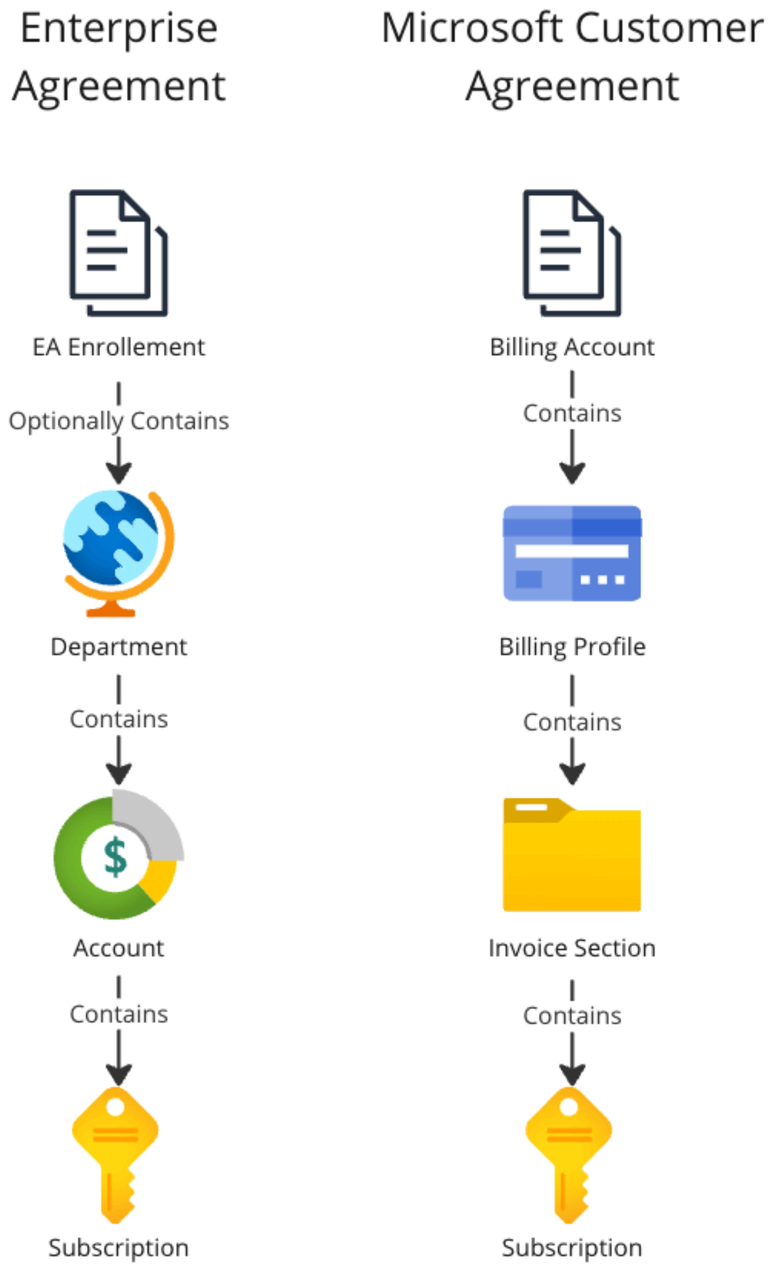
A LESS WELL UNDERSTOOD FEATURE

BILLING AGREEMENTS

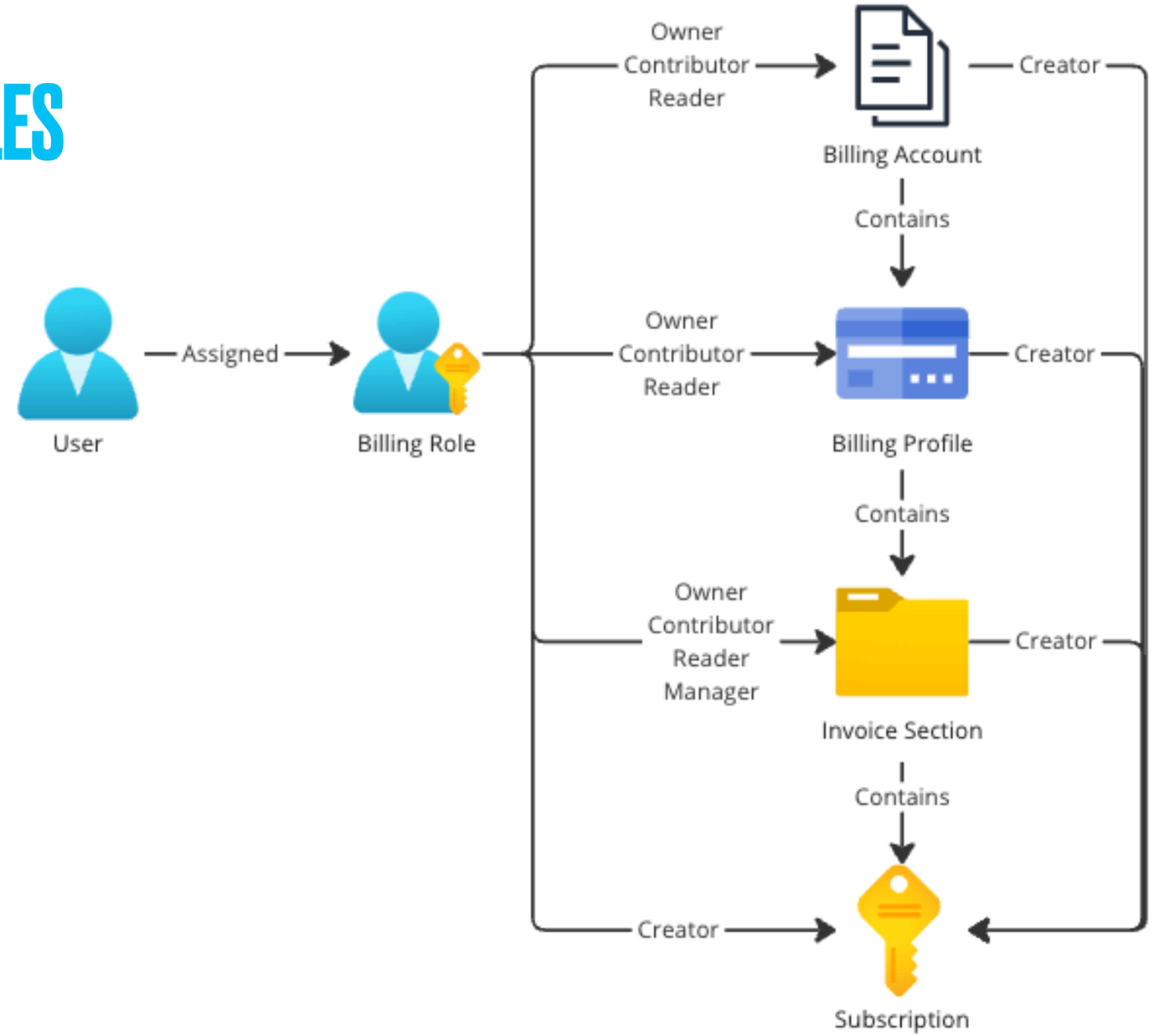
BILLING AGREEMENTS

- **Two ways to be billed for direct agreements**
  - **EA is legacy**
  - **MCA is replacement**

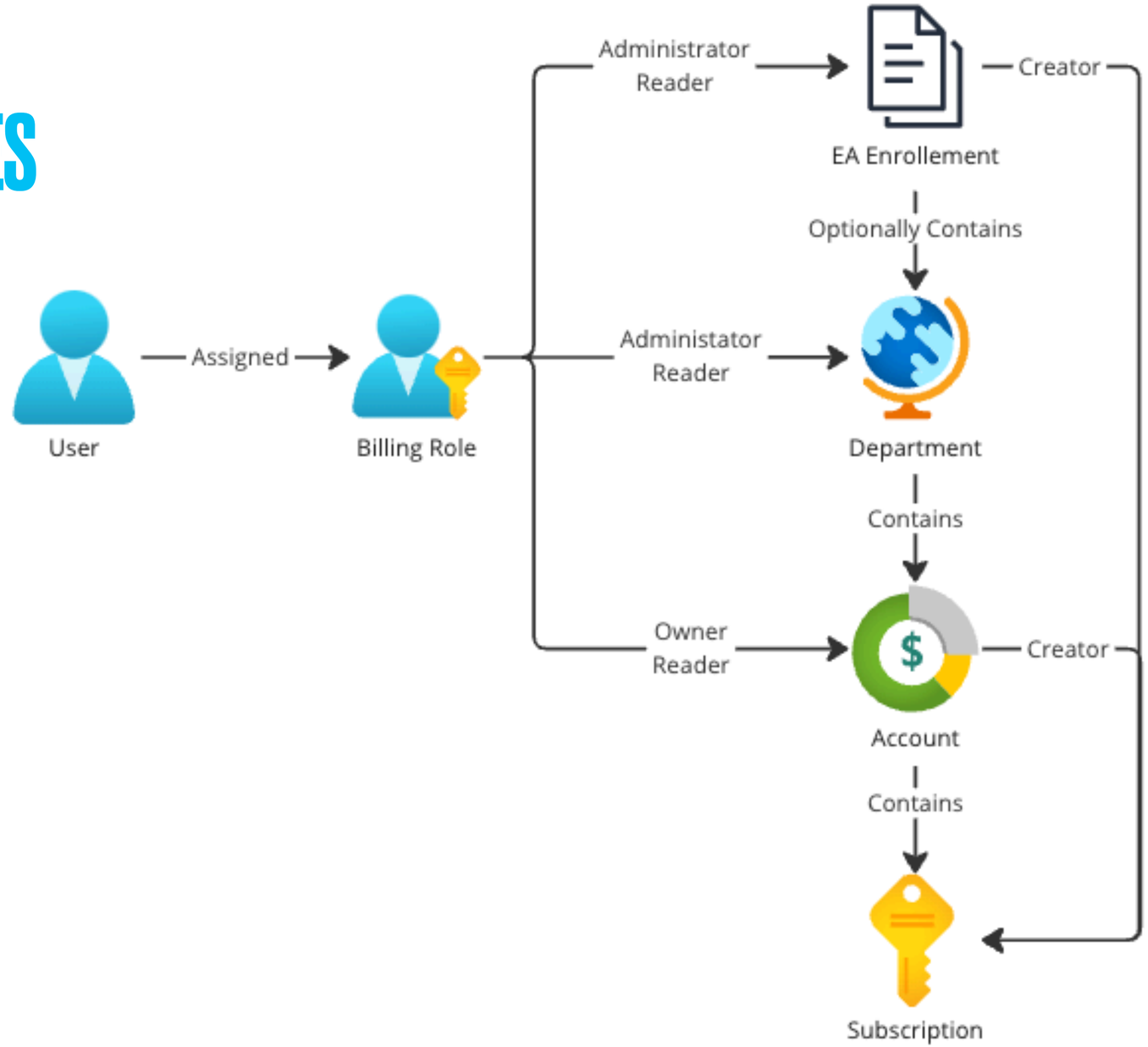
Source: MCA docs, EA docs



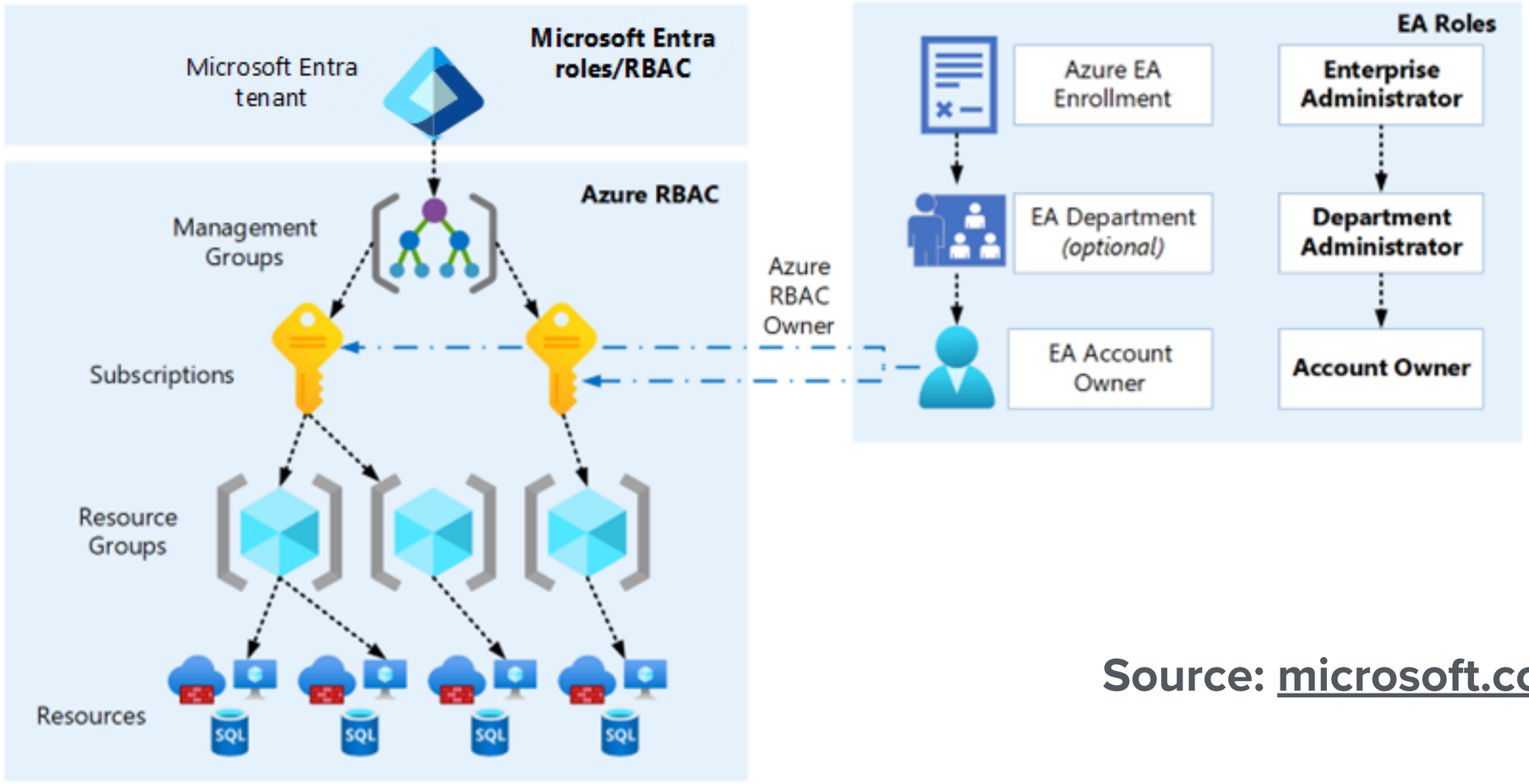
MCA
BILLING ROLES



EA BILLING ROLES



EA VISUALIZED BY MICROSOFT



Source: [microsoft.com]

BILLING ROLES

EA:

- **Enterprise Administrator**
- Enterprise Administrator (read only)
- EA purchaser
- Department Administrator
- Department Administrator (read only)
- **Account Owner**

MCA:

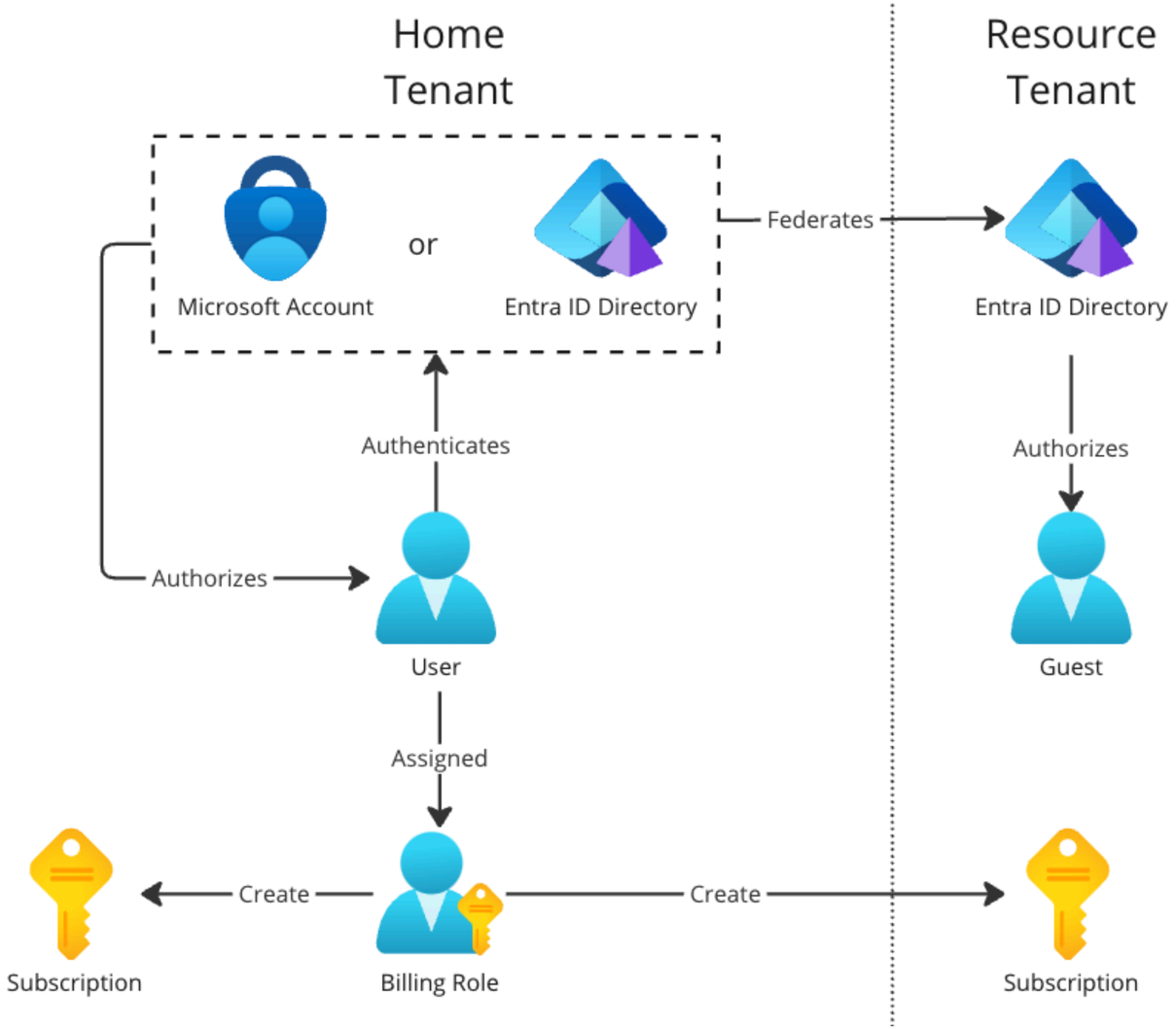
- **Billing account owner**
- **Billing account contributor**
- Billing account reader
- **Billing profile owner**
- **Billing profile contributor**
- Billing profile reader
- Invoice manager
- **Invoice section owner**
- **Invoice section contributor**
- Invoice section reader
- **Azure subscription creator**

AZURE - UNDOCUMENTED BEHAVIOUR

BILLING ROLES ARE WEIRD!

BILLING ROLES GRANT PRIVILEGE ACROSS TENANTS?!

CROSS-TENANT BILLING PRIVILEGES



HOME TENANT

Home > Subscriptions >

Subscriptions

Default Directory

Add | Manage Policies | ...

Global administrators can manage all subscriptions in this list by updating their policy setting here.

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here
Showing subscriptions in Default Directory directory. Don't see a subscription? Switch directories

Se...

Subscriptions : **Filtered (2 of 2)**

My role == **all**

Status == **all**

Add filter

Subscription name ↑↓

Azure subscription 1 ...

Normal Sub ...

Create a subscription ...

Feedback

Basics | **Advanced** | Budget | Tags | Review + create

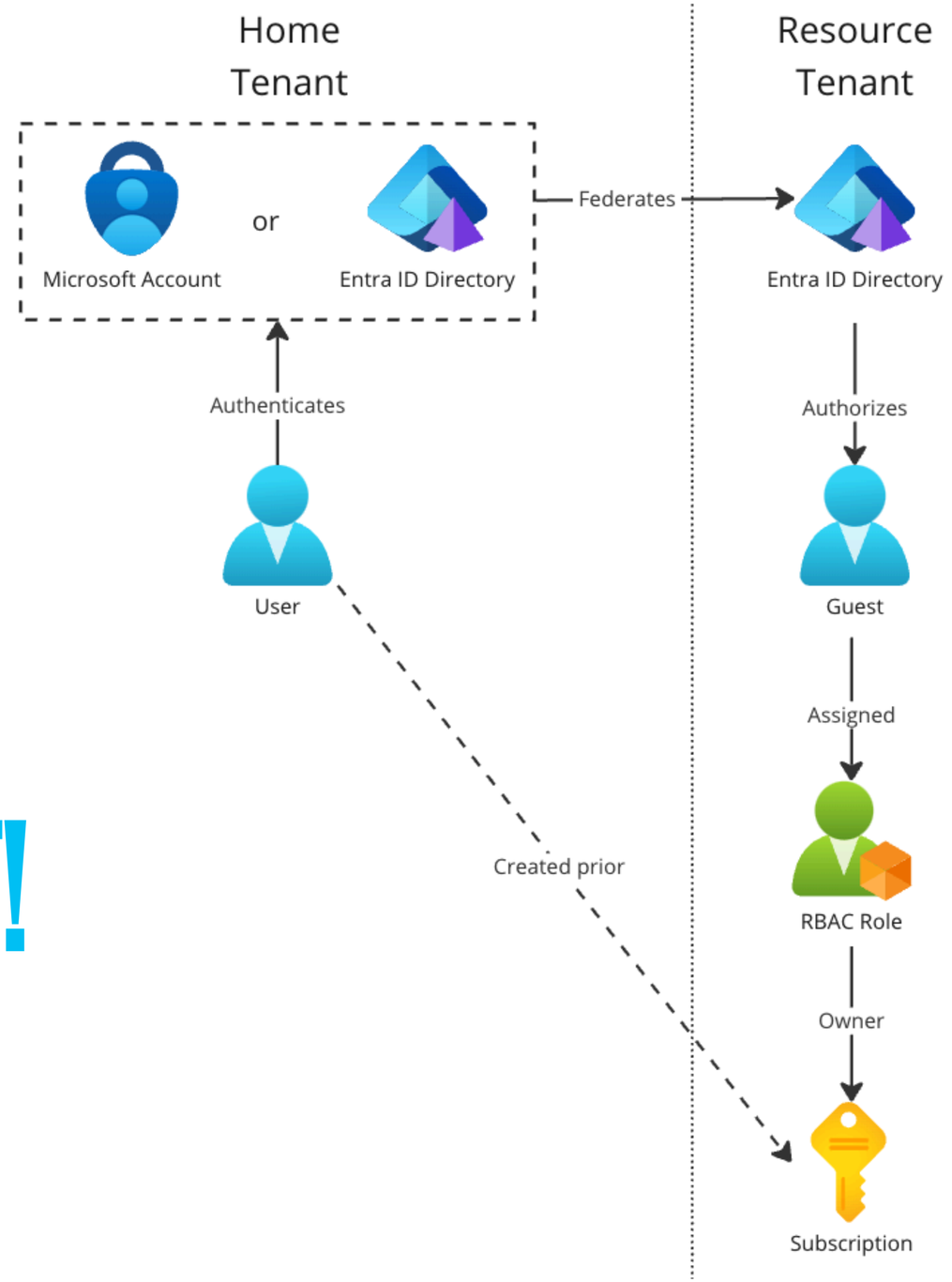
Subscription directory [redacted] Industries [redacted]

Management group: Root management group

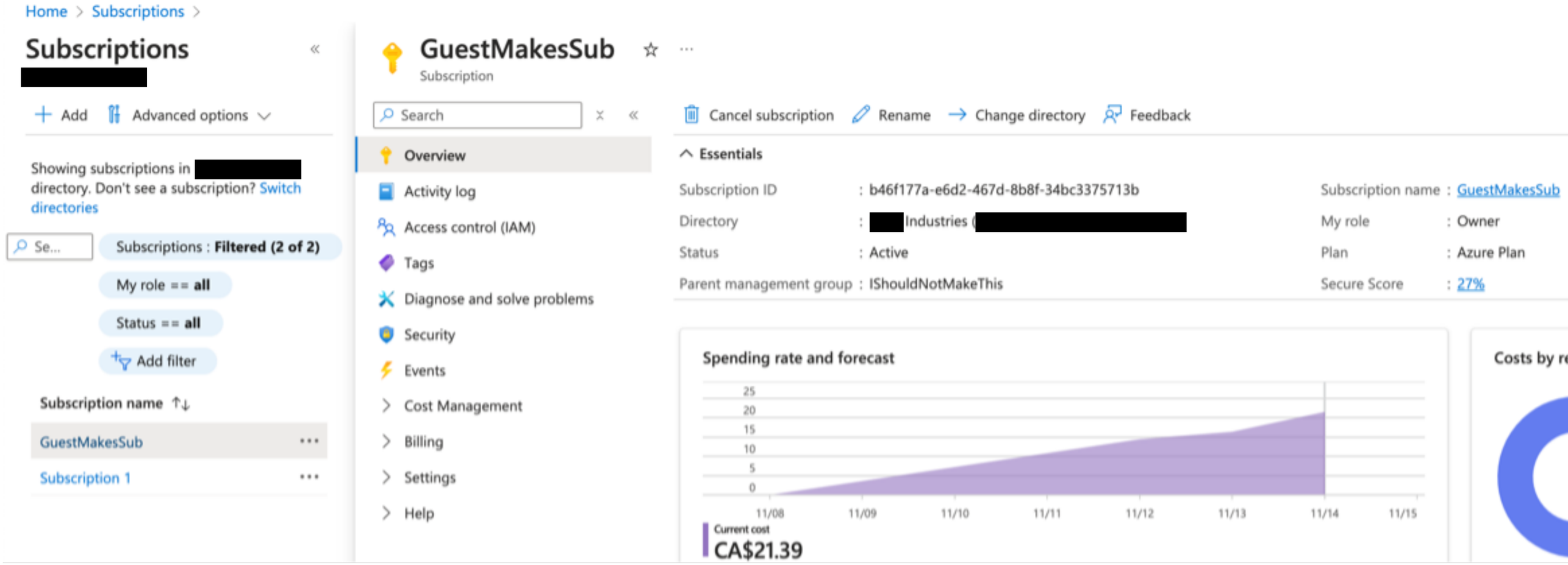
Cannot specify management group since target subscription directory is different than the current directory.

Subscription owner [redacted]

END RESULT!


Home Tenant
Resource Tenant
Microsoft Account
or
Entra ID Directory
Federates
Entra ID Directory
Authenticates
Authorizes
User
Guest
Assigned
Created prior
RBAC Role
Owner
Subscription

RESOURCE TENANT



WHAT WAS MICROSOFT'S VIEW OF THIS?

MICROSOFT'S POSITION

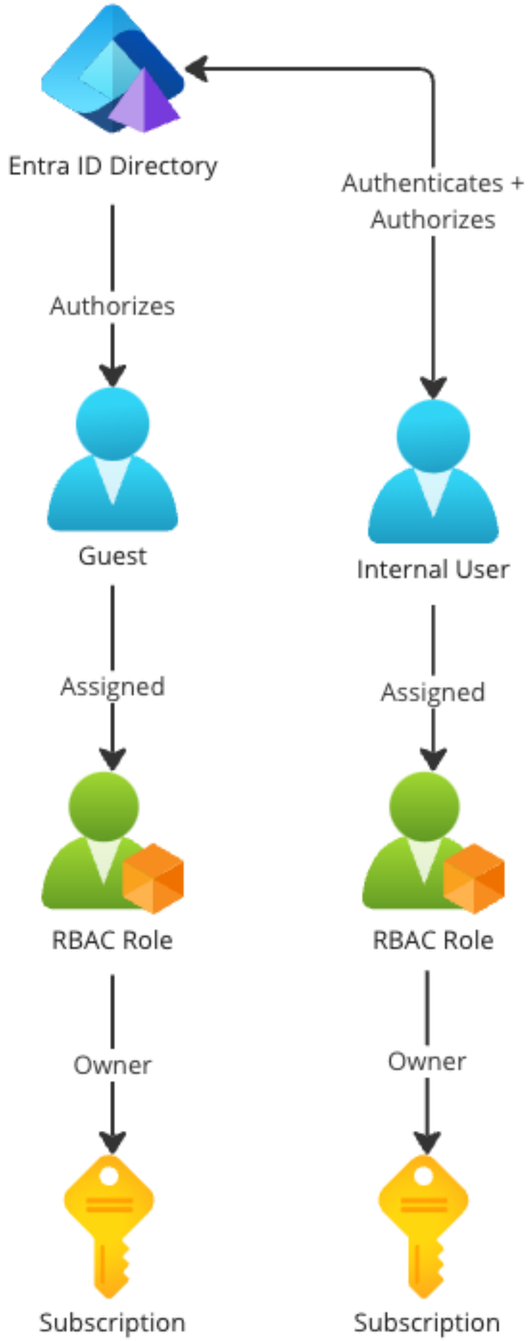
- Confirmed this behaviour was intended as a feature
- No controls exist, at time of meeting, to prevent guests using billing role privilege across tenant.*
- Not a vulnerability as subscriptions are a security boundary in Azure

*This was updated and Microsoft now proposes controls. We will cover at the end.

CAN GUEST MADE SUBSCRIPTIONS BE ABUSED?

UNIQUE PRIVILEGE MODEL

- Guest only has access to their subscription… and it’s empty :(



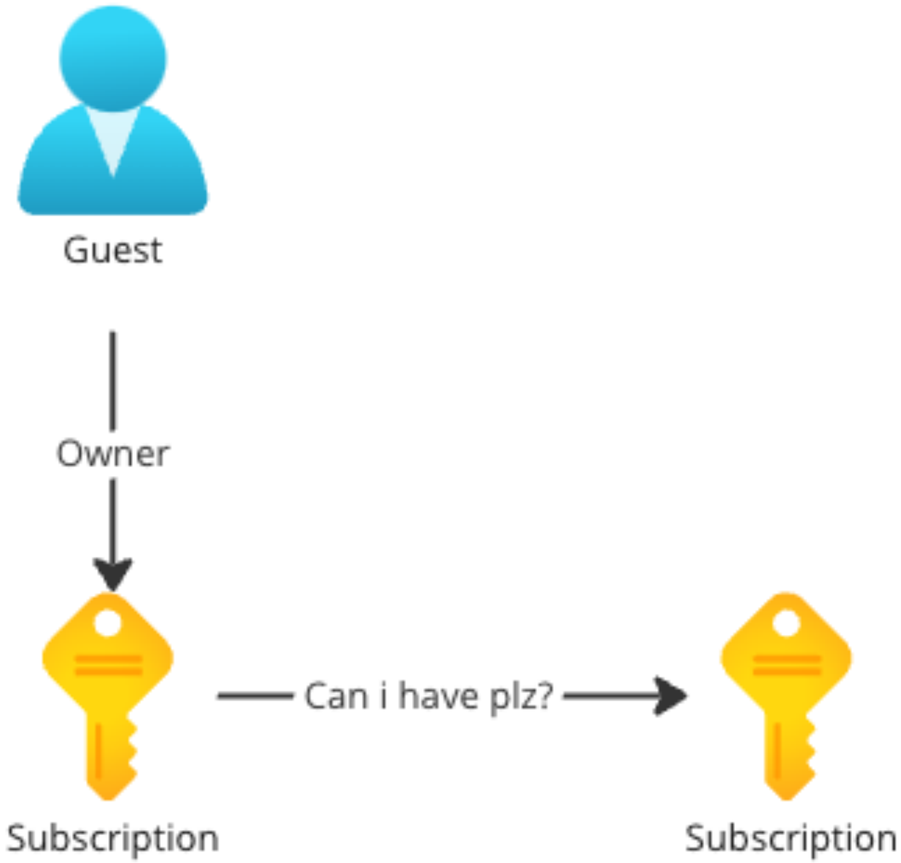
COMPLETELY FAILED ATTEMPTS

BILLING ATTACK?
NO!

- Who ends up paying for this new subscription?
- Guests billing account gets billed for subscription and all resources created inside of it
- No way to use this for guests to offload costs

SUBSCRIPTION TO SUBSCRIPTION? NO!

- Subscriptions purpose is to be logical containers!
- Worst attacker can do: request one subscription transferred to guest controlled one



ENUMERATE THINGS GUESTS NORMALLY CAN'T!

Subscriptions

[redacted]

Add | Manage Policies | ...

Showing subscriptions in [redacted] directory. Don't see a subscription? Switch directories

Se... | Subscriptions : **Filtered (3 of 3)** | My role == **all** | Status == **all** | Add filter

Subscription name

- GuestSub2
- Subscription 1
- GuestMakesSub

GuestSub2 | Access control (IAM)

Subscription

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Resource visualizer
- Events
- Cost Management
- Billing
- Settings
  - Programmatic deployment
  - Billing properties
  - Resource groups
  - Resources
  - Preview features
  - Usage + quotas
  - Policies
  - My permissions
  - Resource providers
  - Deployments

Add | Download role assignments | Edit columns | Refresh | Delete | Feedback

Number of role assignments for this subscription

1 / 4000

Privileged

5

View assignments

Search by name or email | Type : **All** | Role : **All** | Scope : **All scopes** | State : **All** | End time : **All**

All (9) | Job function roles (4) | Privileged administrator roles (5)

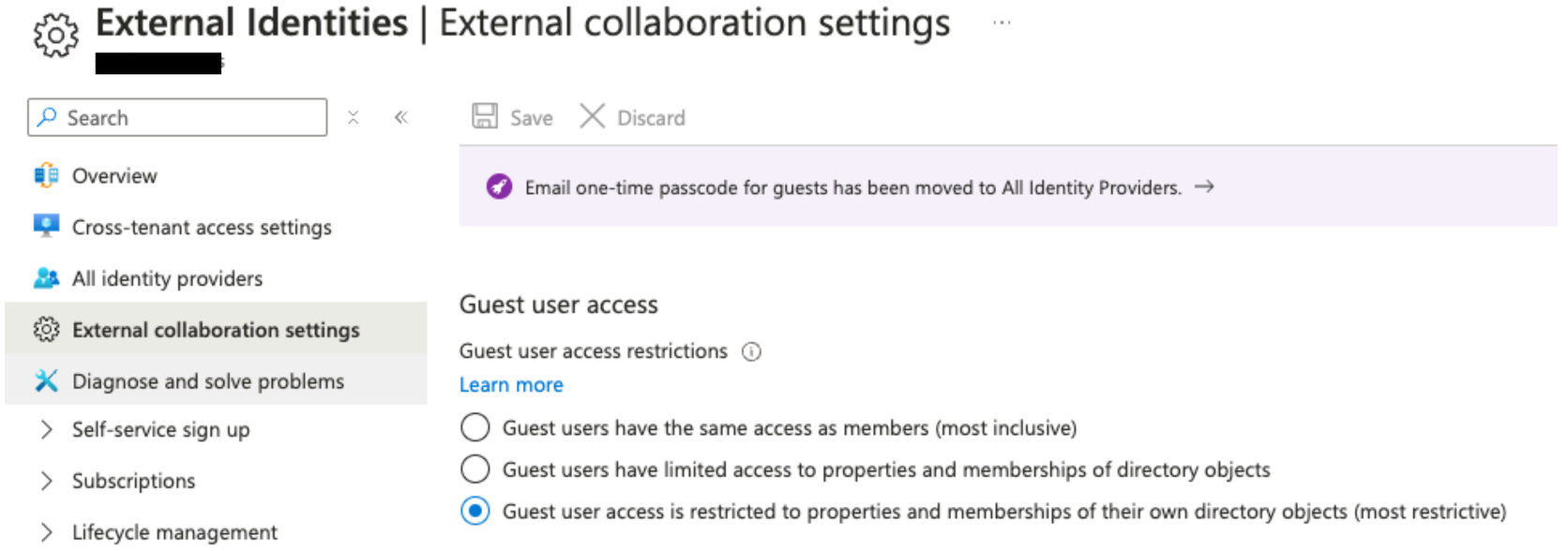
Name	Type	Role	Scope	State	End time
Owner (1)					
SG Simon Guest s[redacted]	User	Owner	This resource	Active permanent	Permanent
Reader (2)					
[redacted]Connector e74d91[redacted]	Service principal	Reader	Management group (I...	Active permanent	Permanent
[redacted]-connector 3f5482[redacted]	Service principal	Reader	Management group (I...	Active permanent	Permanent
AcrDelete (1)					
DM Darth Maul Darth.Maul[redacted]	User	AcrDelete	Management group (I...	Active permanent	Permanent
Key Vault Reader (1)					
[redacted]Connector e74d91d3-[redacted]	Service principal	Key Vault Reader	Management group (I...	Active permanent	Permanent
User Access Administrator (4)					
DM Darth Maul Darth.Maul[redacted]	User	User Access Administrator	Root (Inherited)	Active permanent	Permanent

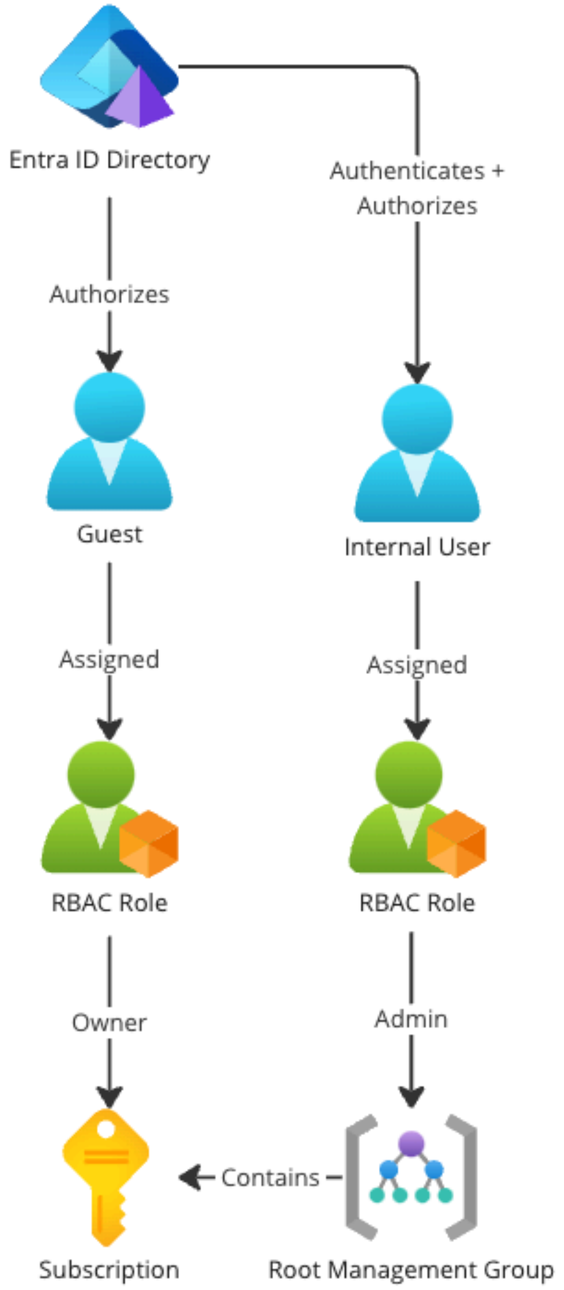
Switch to PowerShell | Restart | Manage files | New session | Editor | Web preview | Settings | Help

```
simon [ ~ ]$ az ad user list --query "[].{displayName:displayName, userPrincipalName:userPrincipalName}"
Insufficient privileges to complete the operation.
```

ENUMERATION? KINDA

- Turns out we can list the root management group admins that our subscription belongs to!
- There is a control to prevent this...





AZURE POLICY

POLICY? KINDA

Home > Policy | Assignments >

Assign policy ...

Basics | Parameters | Remediation | Non-compliance messages | Review + create

Scope

Scope * GuestMakesSub

Learn more about setting the scope

Exclusions GuestMakesSub/GUESTMADE_group

Resource selectors (Expand) Using resource selectors, you can further refine this assignment's applicability by targeting specific subse of resources. Expand to learn more.

Basics

Policy definition * GuestsCompliance

Overrides (Expand) Using overrides, you can change the effects or referenced versions of definitions for all or a subset of resources evaluated by this assignment. Expand to learn more.

Assignment name * GuestsCompliance

Description

Policy enforcement Enabled

Available Definitions

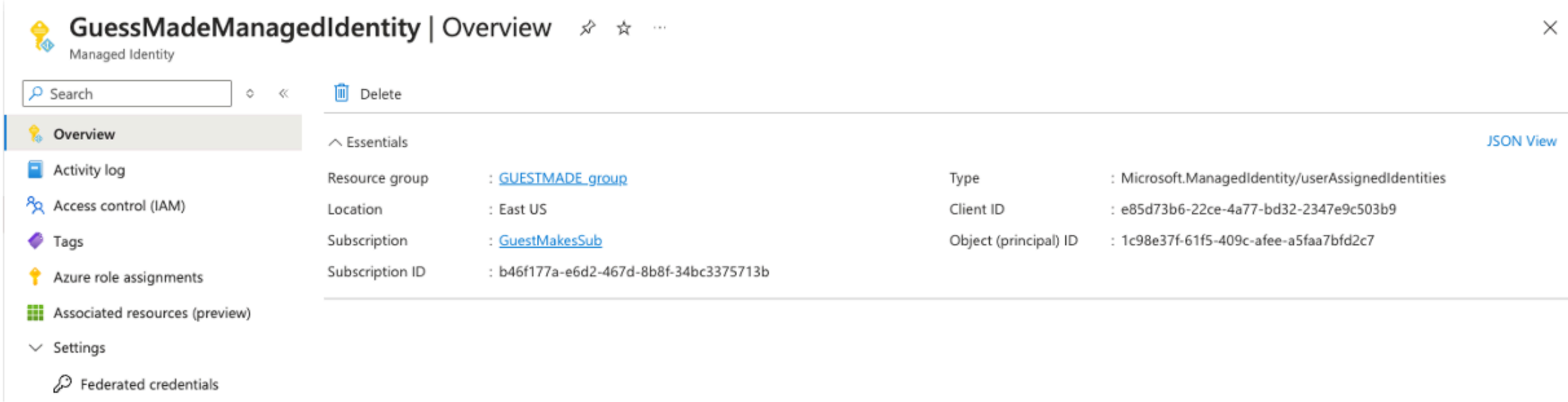
Search | Policy type : All policy types | Category : All categories

Policy name	Latest version (...	Category	Type
Microsoft Managed Control 1158 - Security Auth...	1.0.0	Regulatory Compli...	Static
Bot Service should have local authentication met...	1.0.0	Bot Service	BuiltIn
Review cloud service provider's compliance with ...	1.1.0	Regulatory Compli...	BuiltIn
Enable logging by category group for microsoft.w...	1.0.0	Monitoring	BuiltIn
API Management should have username and pas...	1.0.1	API Management	BuiltIn
Establish usage restrictions for mobile code techn...	1.1.0	Regulatory Compli...	BuiltIn
Deploy export to Log Analytics workspace for Mic...	4.1.0	Security Center	BuiltIn
Microsoft Managed Control 1407 - Maintenance ...	1.0.0	Regulatory Compli...	Static
Keys using elliptic curve cryptography should hav...	1.0.1	Key Vault	BuiltIn
Azure Application Gateway should be deployed w...	1.0.0	Network	BuiltIn
Secure the interface to external systems	1.1.0	Regulatory Compli...	BuiltIn
Observe and report security weaknesses	1.1.0	Regulatory Compli...	BuiltIn
Container registries should have repository scope...	1.0.0	Container Registry	BuiltIn
SQL databases should have vulnerability findings ...	4.1.0	Security Center	BuiltIn
[Preview]: Prevents init containers from being ran ...	1.0.0-preview	Kubernetes	BuiltIn

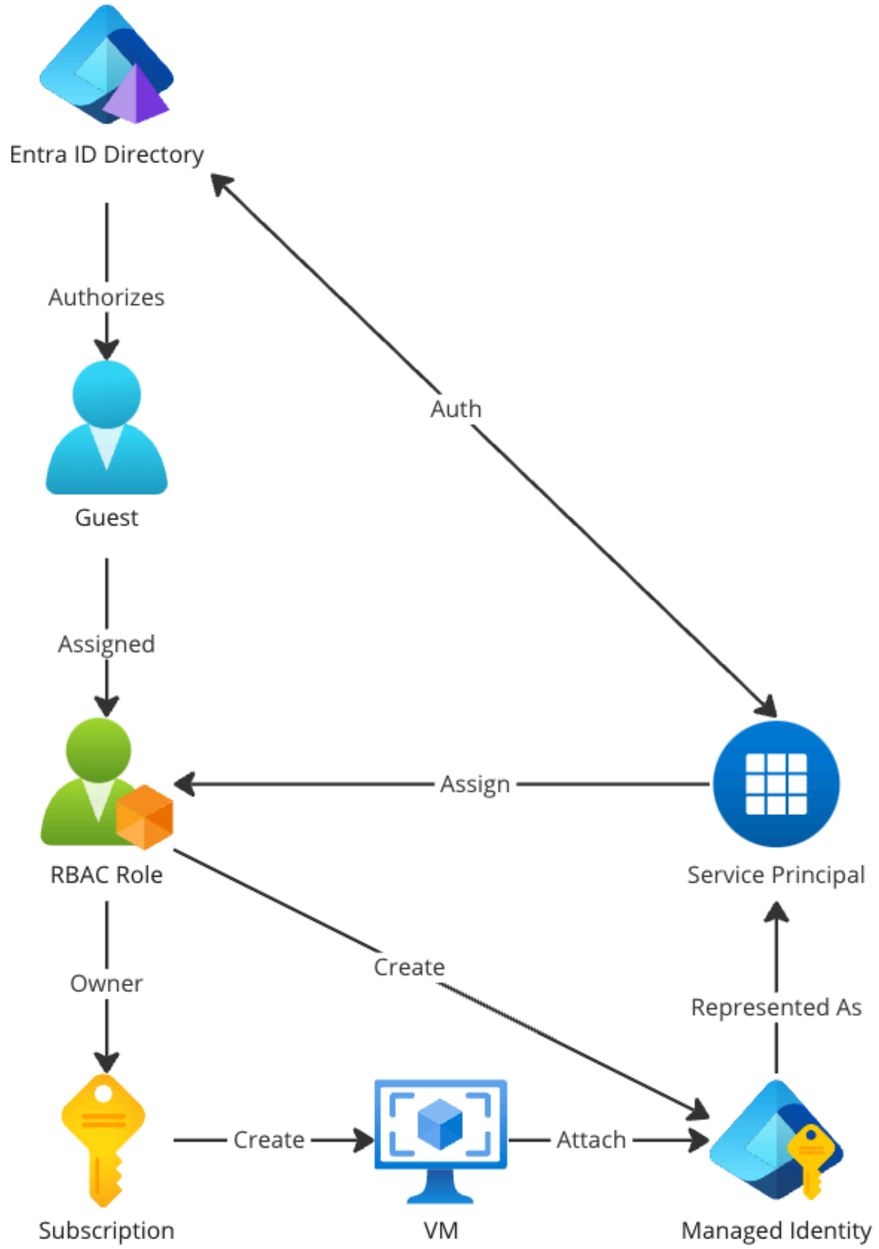
MANAGED IDENTITIES

SUBSCRIPTION TO DIRECTORY? YES!

- Managed Identities are a way we can make Azure Resources that can authenticate against the directory.
- Can be user managed, or follow life cycle of resource
- Inserts Service Principal identity into directory

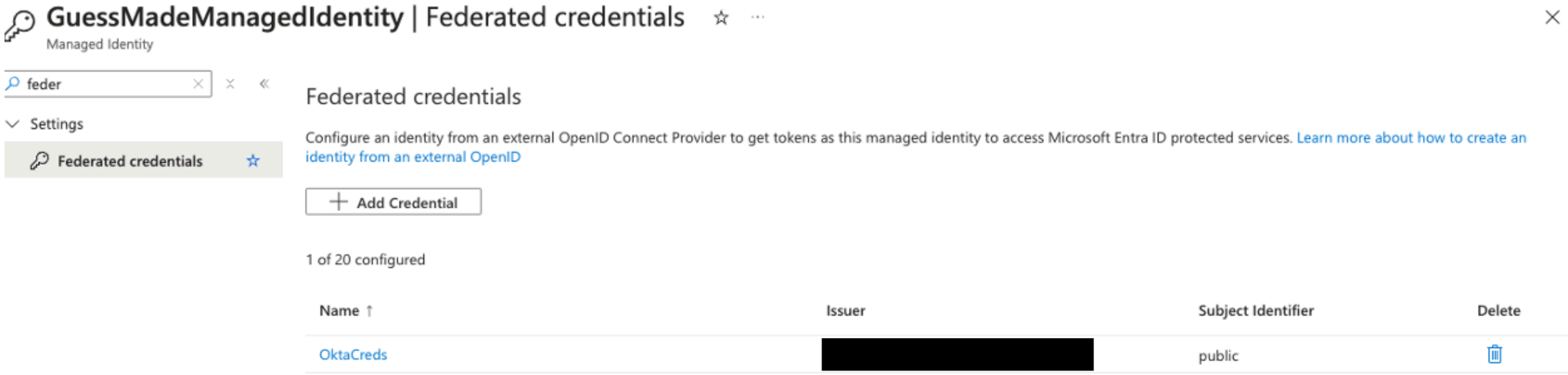


PIVOT!

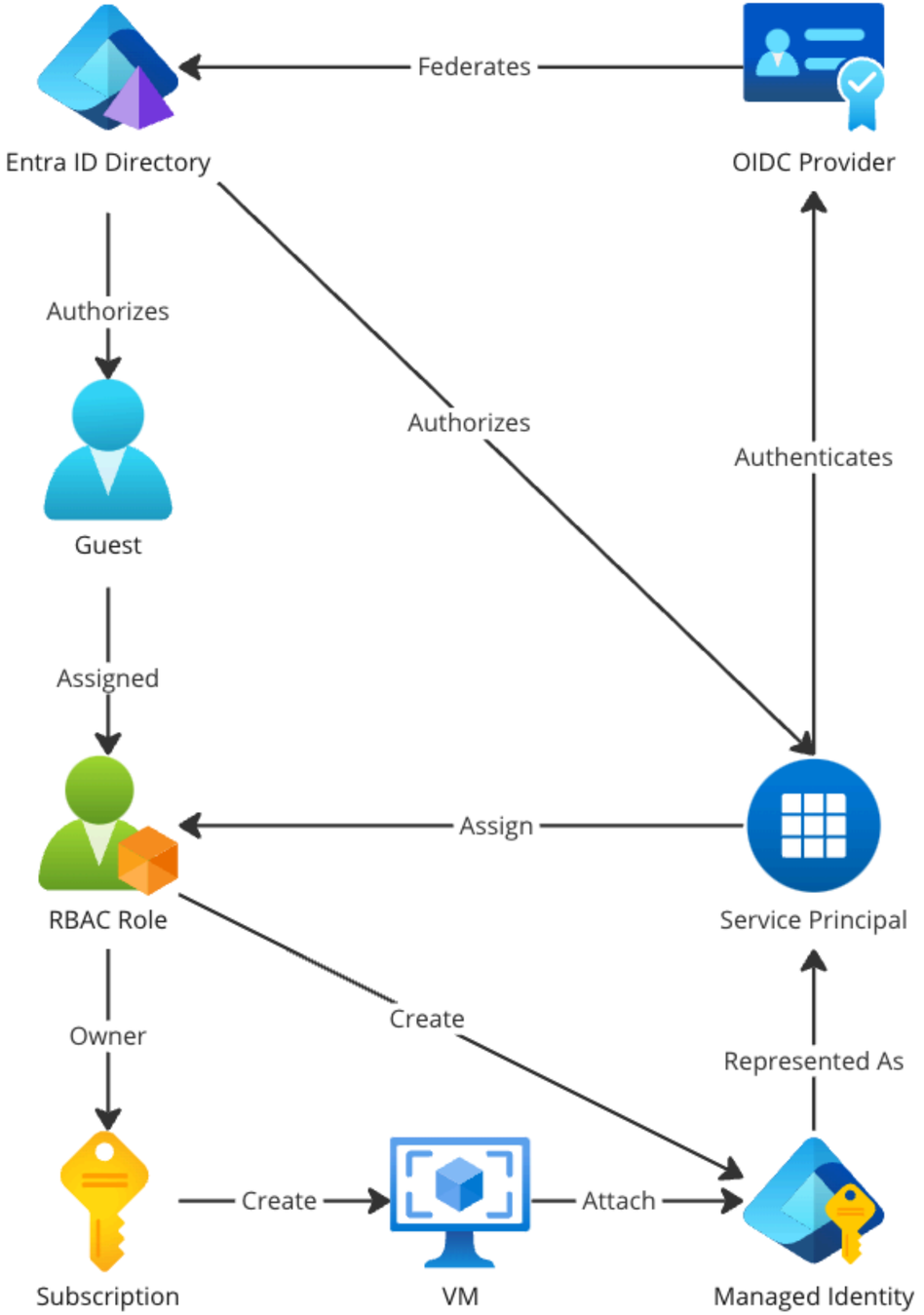

Entra ID Directory
Authorizes
Guest
Auth
Assigned
RBAC Role
Assign
Service Principal
Owner
Create
Represented As
Subscription
Create
VM
Attach
Managed Identity

DEEPEN PERSISTENCE

- We can use a well known technique of adding attacker controlled OIDC federated credentials (source: @dirkjanm)
- Doing this allows us to deepen persistence; attacker controlled identity separate from original guest



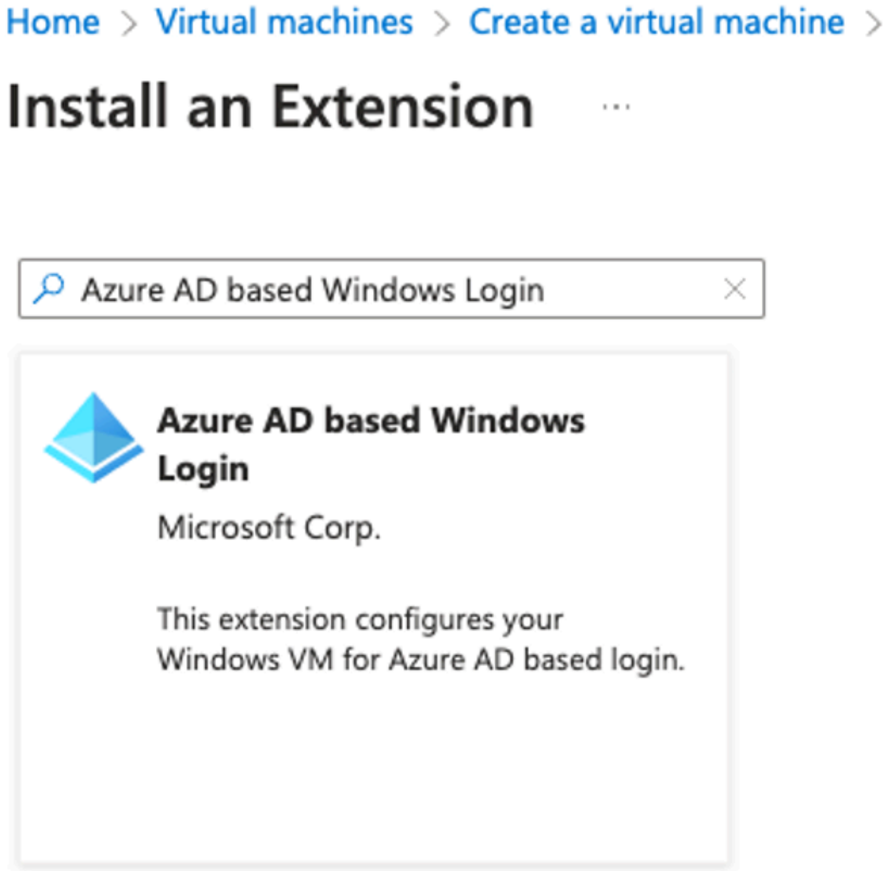
PIVOT!
PIVOT!


Federates
Entra ID Directory
OIDC Provider
Authorizes
Authorizes
Authenticates
Guest
Assigned
Assign
RBAC Role
Service Principal
Owner
Create
Represented As
Create
Attach
Subscription
VM
Managed Identity

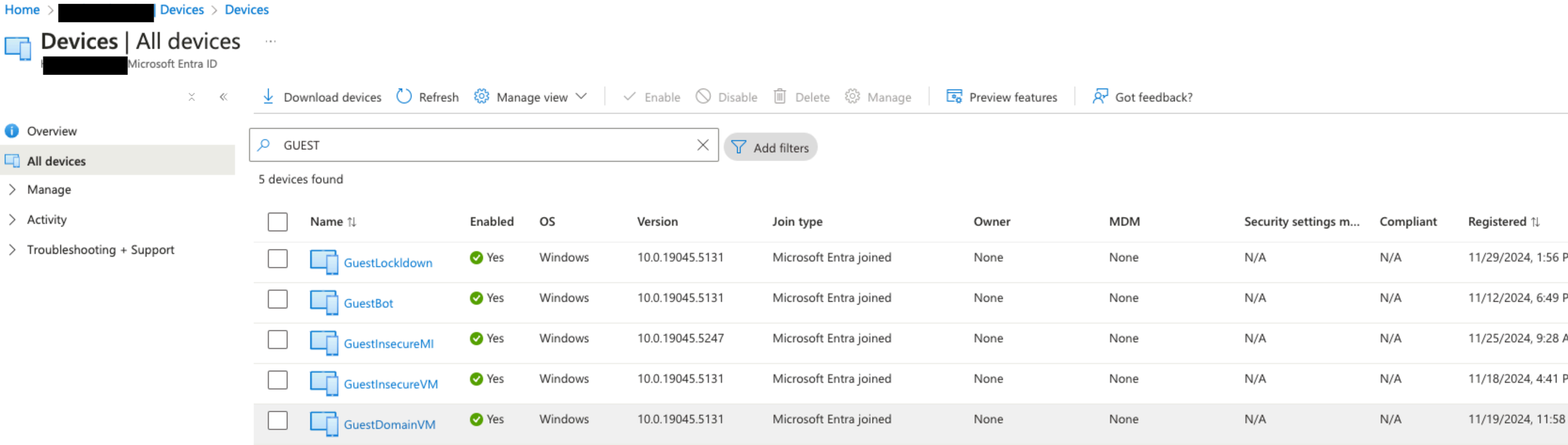
CONDITIONAL ACCESS POLICY

MORE DIRECTORY SHENANIGANS !

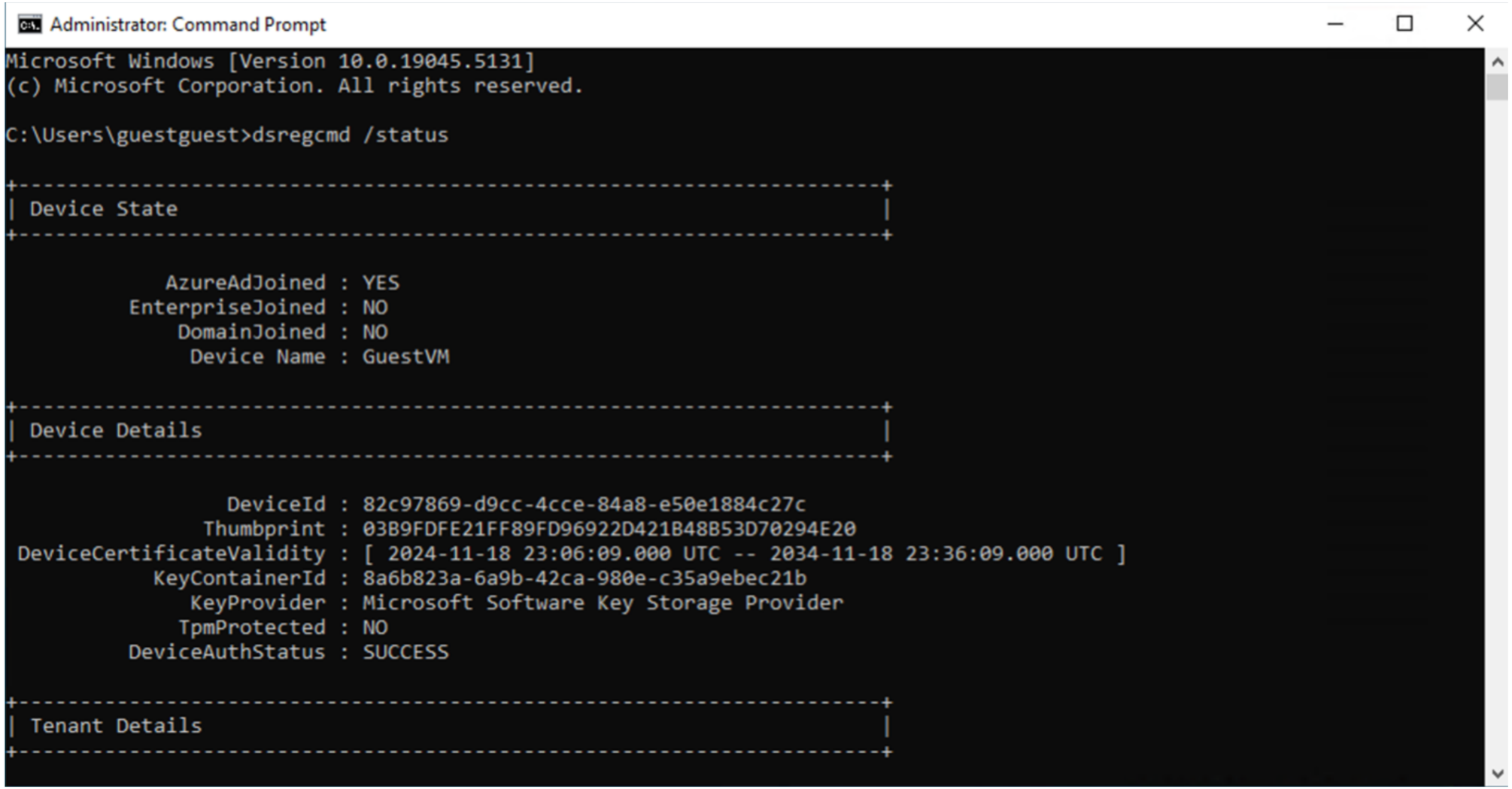
- Device based abused :)



PORTAL VIEW


Home > [redacted] | Devices > Devices
Devices | All devices
[redacted] Microsoft Entra ID
Download devices
Refresh
Manage view
Enable
Disable
Delete
Manage
Preview features
Got feedback?
Overview
All devices
Manage
Activity
Troubleshooting + Support
GUEST
Add filters
5 devices found
Name
Enabled
OS
Version
Join type
Owner
MDM
Security settings m...
Compliant
Registered
GuestLockIdown Yes Windows 10.0.19045.5131 Microsoft Entra joined None None N/A N/A 11/29/2024, 1:56 P
GuestBot Yes Windows 10.0.19045.5131 Microsoft Entra joined None None N/A N/A 11/12/2024, 6:49 P
GuestInsecureMI Yes Windows 10.0.19045.5247 Microsoft Entra joined None None N/A N/A 11/25/2024, 9:28 A
GuestInsecureVM Yes Windows 10.0.19045.5131 Microsoft Entra joined None None N/A N/A 11/18/2024, 4:41 P
GuestDomainVM Yes Windows 10.0.19045.5131 Microsoft Entra joined None None N/A N/A 11/19/2024, 11:58

DEVICE JOINED ENTRA ID!



WHAT'S THE SIGNIFICANCE?

- "Devices (endpoints) are a crucial part of Microsoft's Zero Trust concept. Devices can be Registered, Joined, or Hybrid Joined to Azure AD.

  Conditional Access uses the device information as one of the decisions criteria to allow or block access to services."

https://aadinternals.com/post/devices/

Dr. Nestori Syynimaa aka @DrAzureAD

DYNAMIC DEVICE GROUPS

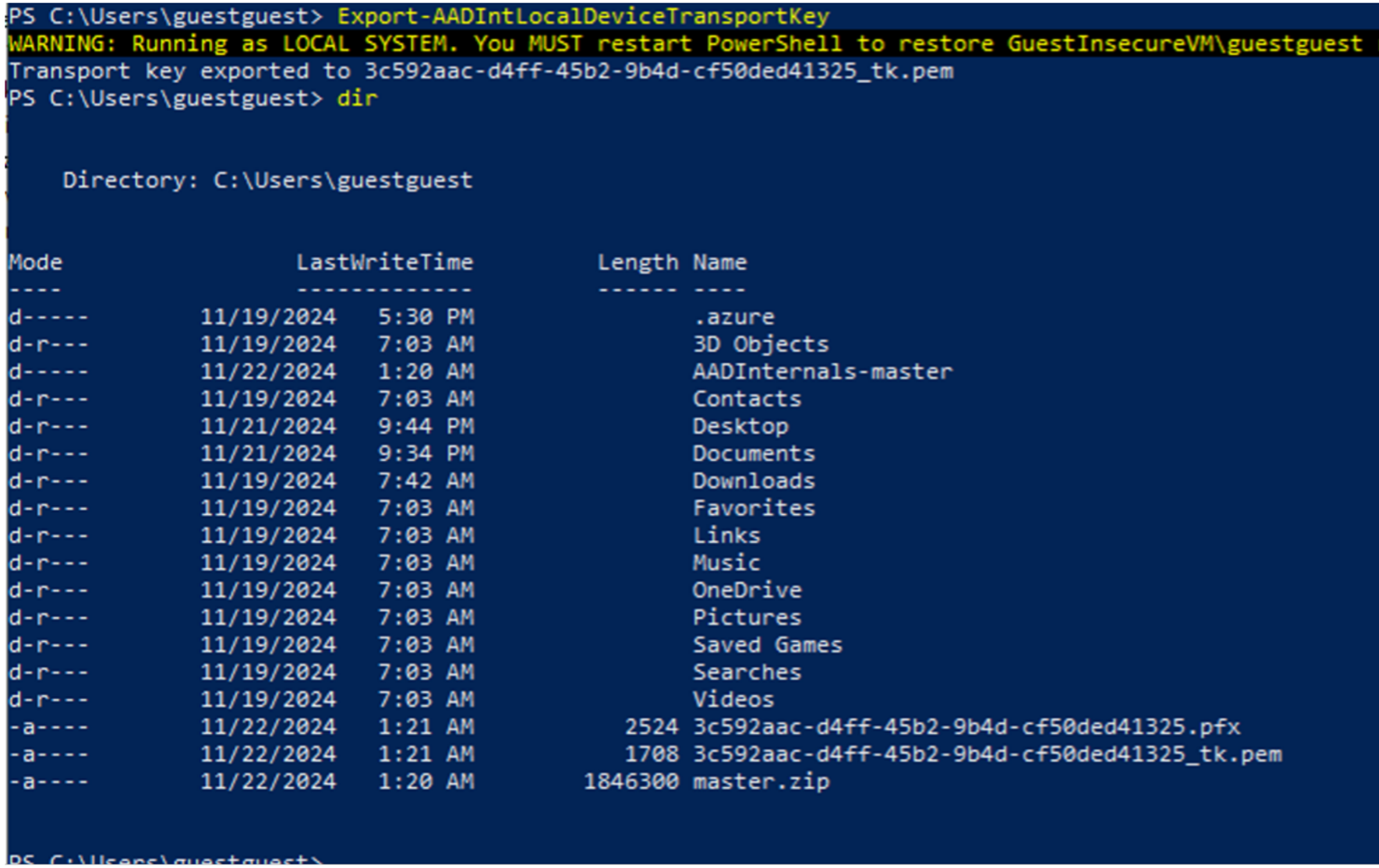
- **Potential security risk: devices can be members of dynamic groups**
- **Similar concept as known dynamic group abuse for users.**
- **For instance, the target organization may have setup conditional access based on dynamic groups like “Windows Workstations”, “VPN Machines” etc.**

Example: (device.displayName -startsWith “AVD”)

STEALING DEVICE IDENTITIES!

“Stealing (and faking) device identities allows threat actors to access the target tenant using the identity of the stolen or faked device. This may allow evading device based Conditional Access (CA) policies, as the compliance of the device is assessed against the original device.”

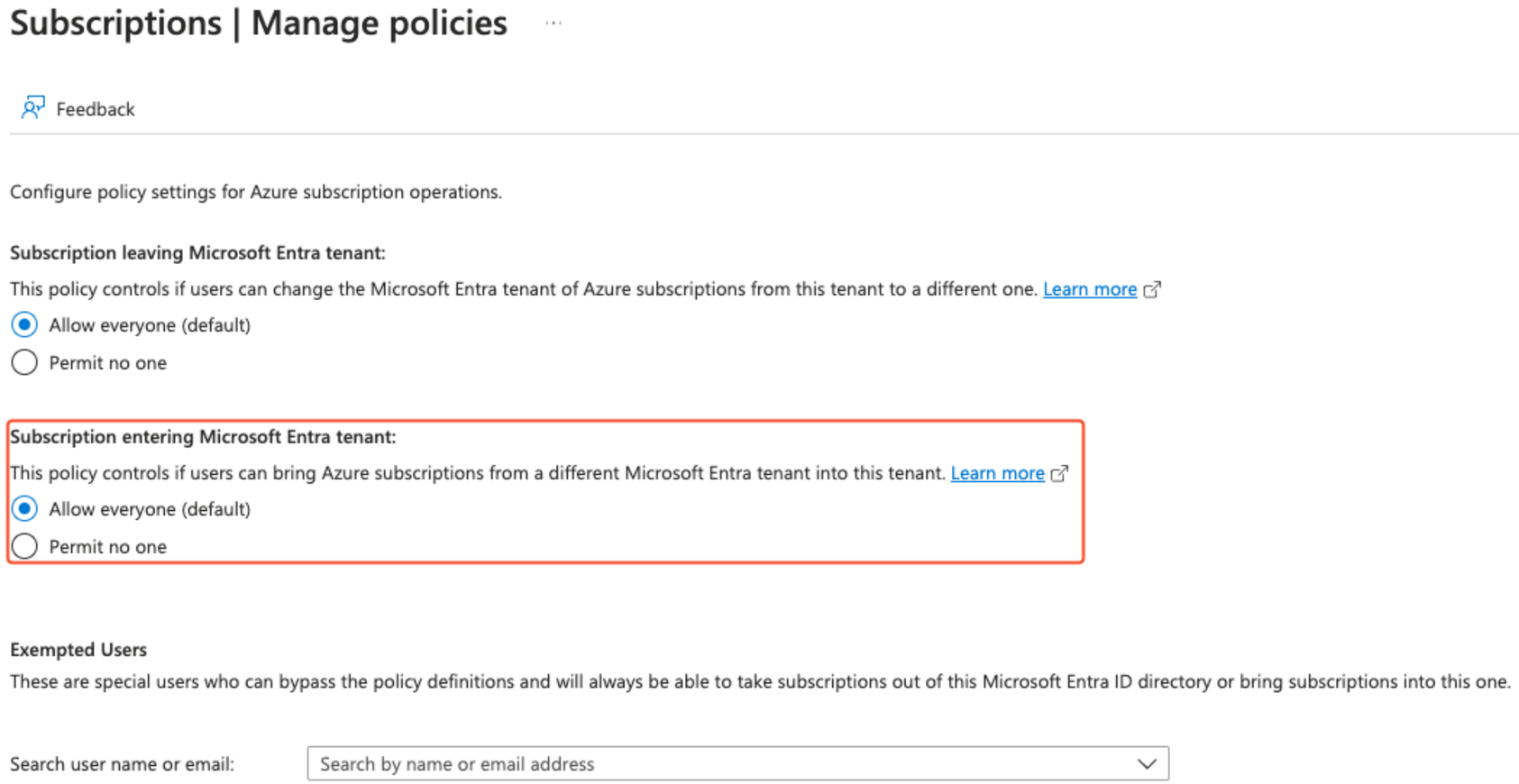
https://aadinternals.com/post/deviceidentity/



BEST DEFENCE

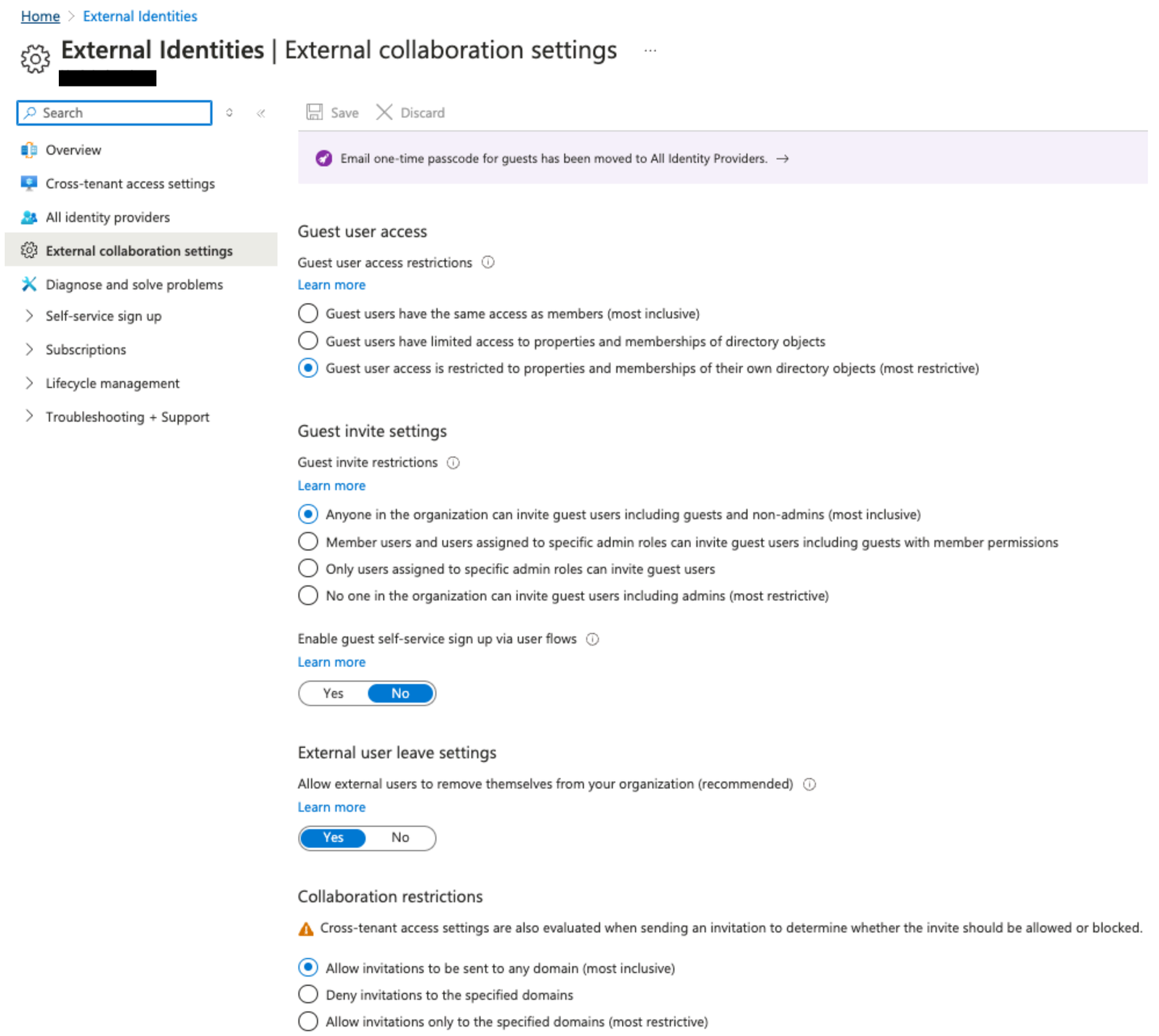
STOP ROOT CAUSE!

- TBD if this works in all cases, some evidence this now works for MCA accounts



CONTROLS!

- Can stop unwanted enumeration attacks
- Generally make guests have as least privilege as possible



BE AWARE!
GUEST API PERMISSION PHISHING

- Malicious collaborators could ask for a privileged API permission to be assigned to a service principal
  - RoleManagement.ReadWrite.Directory

- Guests may have teams access, which threat actor could leverage…
  - “Hey! plz unblock me friend :) just need an admin to grant this app API permission”
  - Attacker can name Managed Identity: “NotSus HR”

- In tenants where this kind of guest collaboration is somewhat routine, ensure admins verify the provenance of all service principals they are being asked to add privileges to

DEFENCE, DEFENCE, DEFENCE!

- Monitoring guest made subscriptions
- Review usage of broad dynamic device groups and conditional access policies of devices
- Some alerts can pop up in Security Center

QUESTIONS?

SIMON MAXWELL-STEWART
SR. SECURITY RESEARCH @ BEYONDTRUST
GITHUB: @KIDTRONNIX