About me:

I live in beautiful Murnau am Staffelsee, 45min south of Munich

- ➔ Executive Consultant at CGI Deutschland
- ➔ In the industry with experience in Identity and Active Directory for many years
- ➔ Part time technical journalist, technical writer in print and online media
- ➔ Screencast Training published this year at heise Academy „Hybrid Azure AD“ (Level 200-300)
  some chapter since Feb 2022 on Youtube
- ➔ When I am offline, I spend my time in the mountains, doing sports (trailrunning, MTB, etc.)

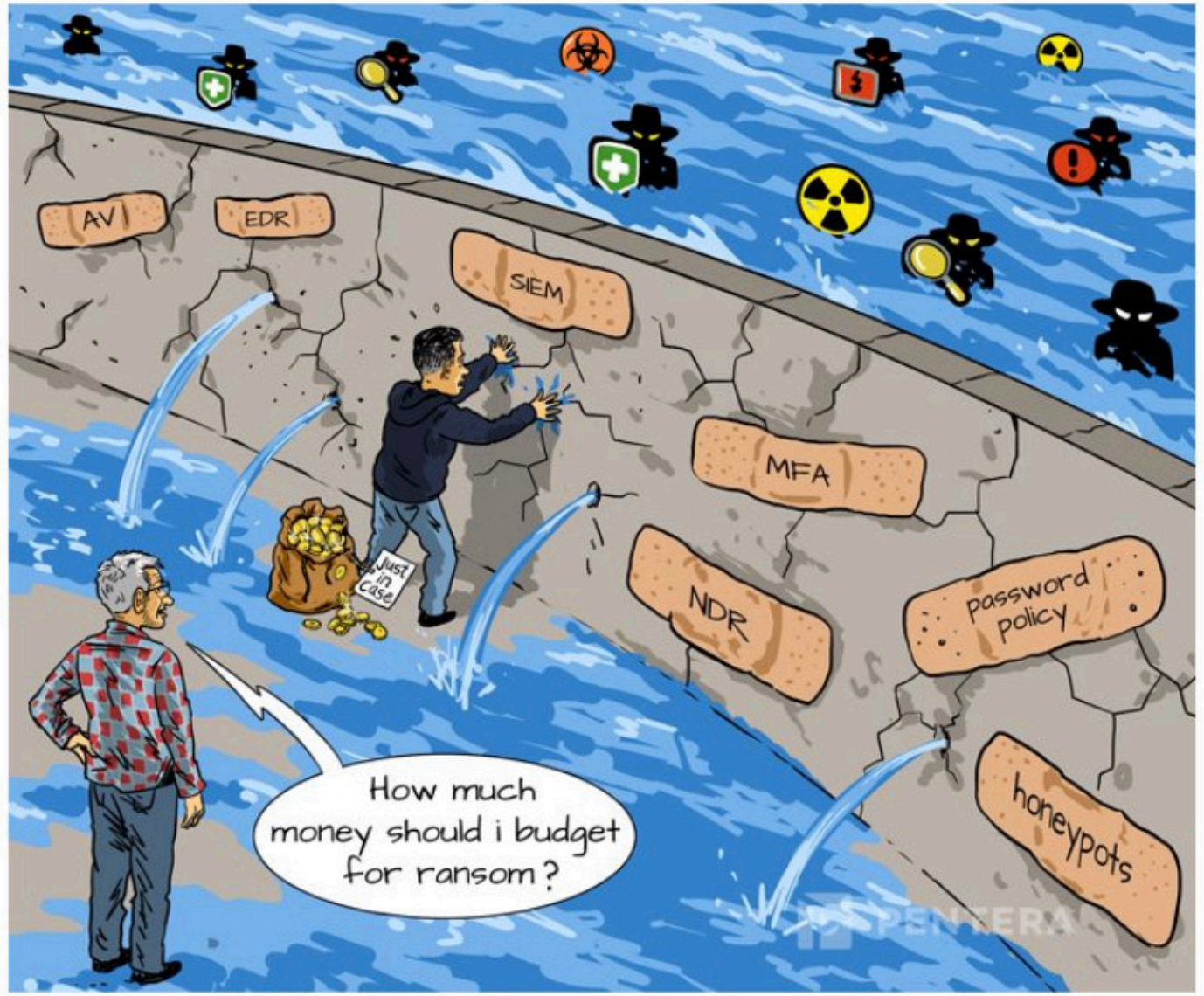
LinkedIn

@KlaBiers

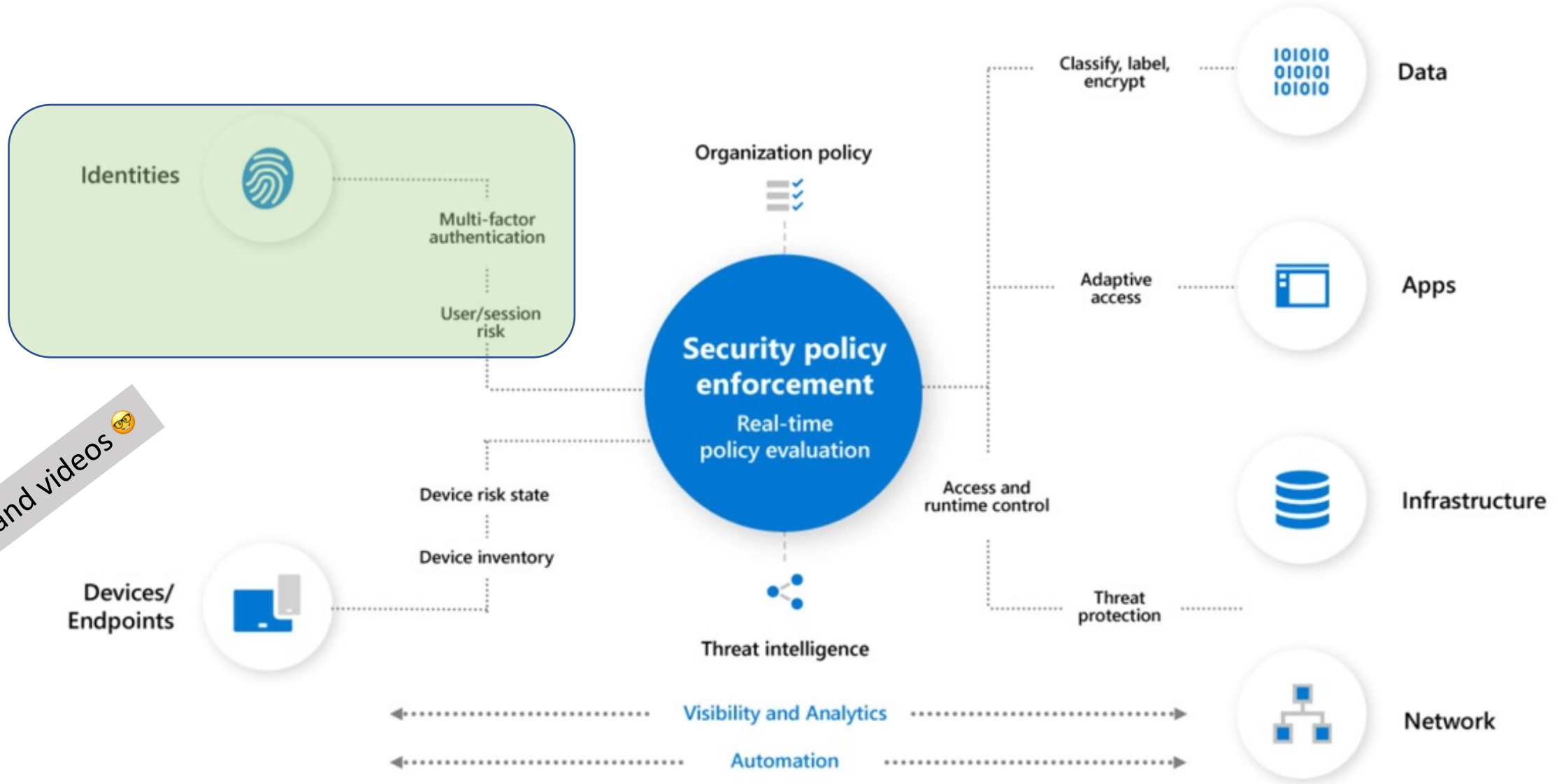
Blog:
https://nothingbutcloud.net/

CYBER TOON

PENTERA



Zero Trust Identity – minor but powerful functionalities



More details and videos

Zero Trust Identity – minor but powerful functionalities

Quick overview on tools

- Agenda and key takeaways -

Privileged Identity Management (PIM)

Conditional Access Policies (CA)

Zero trust - identities

Administrative Units (AU)

Access Reviews

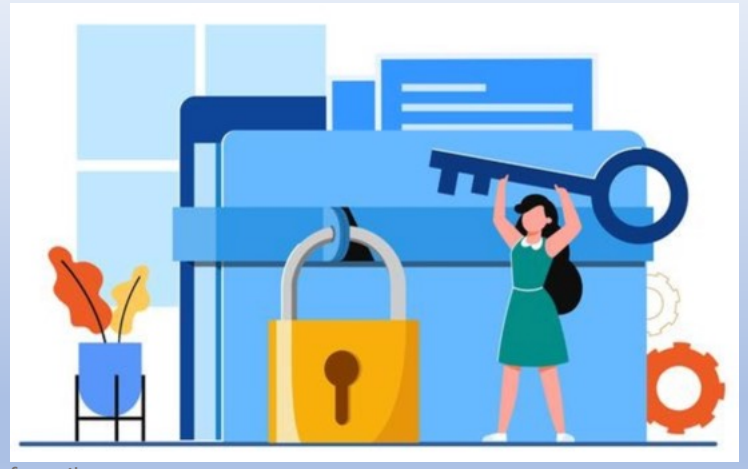
Banned Password Policy

Monitoring (e.g. Alert Rules

Custom Smart Lockout

Identity Protection (IdP)

Dynamic Group Memberships



freepik

Break Glass Accounts (BGA)

Multi Factor Authentication MFA

Zero Trust Identity – minor but powerful functionalities

Privileged Identity Management (PIM)

Conditional Access Policies (CA)

Zero trust - identities

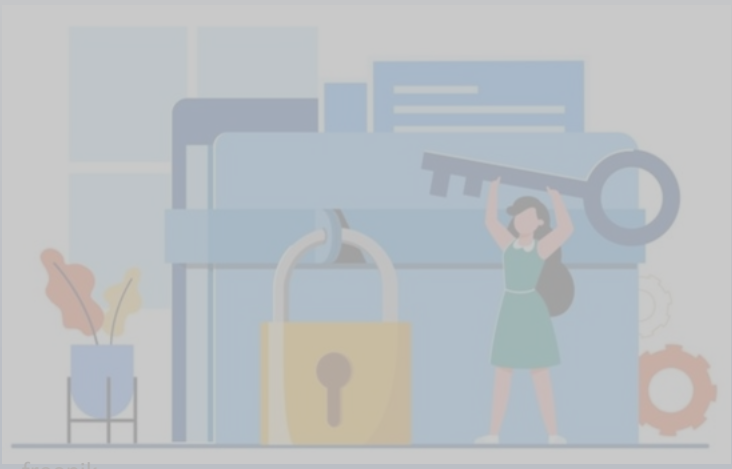
Administrative Units (AU)

Access Reviews

Banned Password Policy

Custom Smart Lockout

Monitoring (e.g. Alert Rules



freepik

Identity Protection (IdP)

Dynamic Group Memberships

Break Glass Accounts (BGA)

Multi Factor Authentication MFA

Zero Trust Identity – minor but powerful functionalities

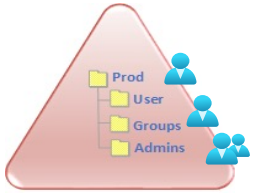
Demo:
Password Protection in the Azure AD Portal

Custom smart lockout

Enter password

Azure Active Directory

Active Directory On-Premises



Error

Password correct ?

no

„Lockout Duration“ running ?

yes

e.g.120 s.

no

1. Attempt after „Lockout“?

yes

no

„Threshold“ reached?

yes

starting „Logout Duration“

no

„Lockout Counter“ reached?

yes

badPwdCount = 0

no

badPwdCount +1

no

Acc. Lockout Threshold reached?

yes

e.g.3x

e.g.60 s.

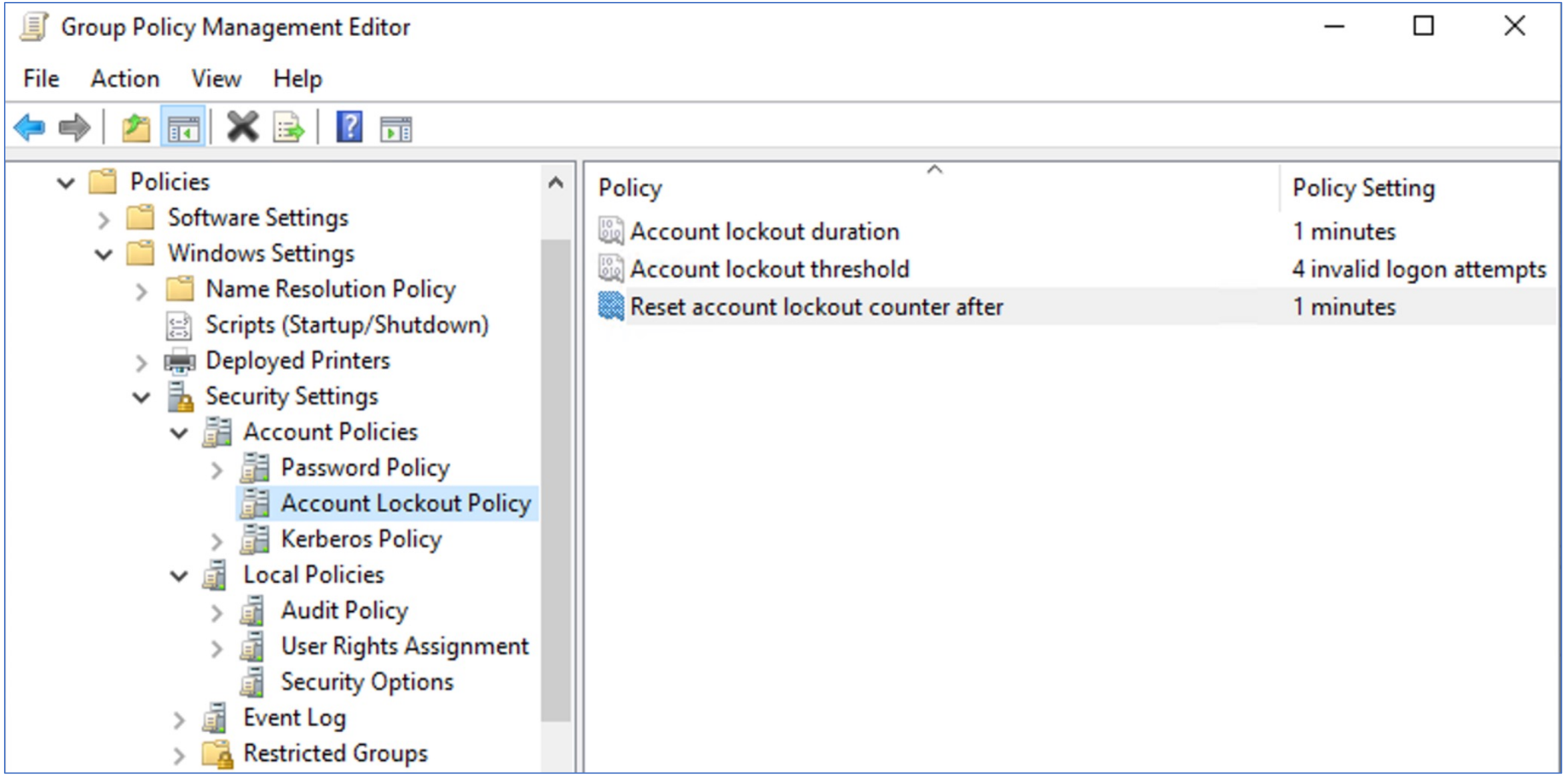
e.g.6x

Threshold in AAD lower then On-Premises

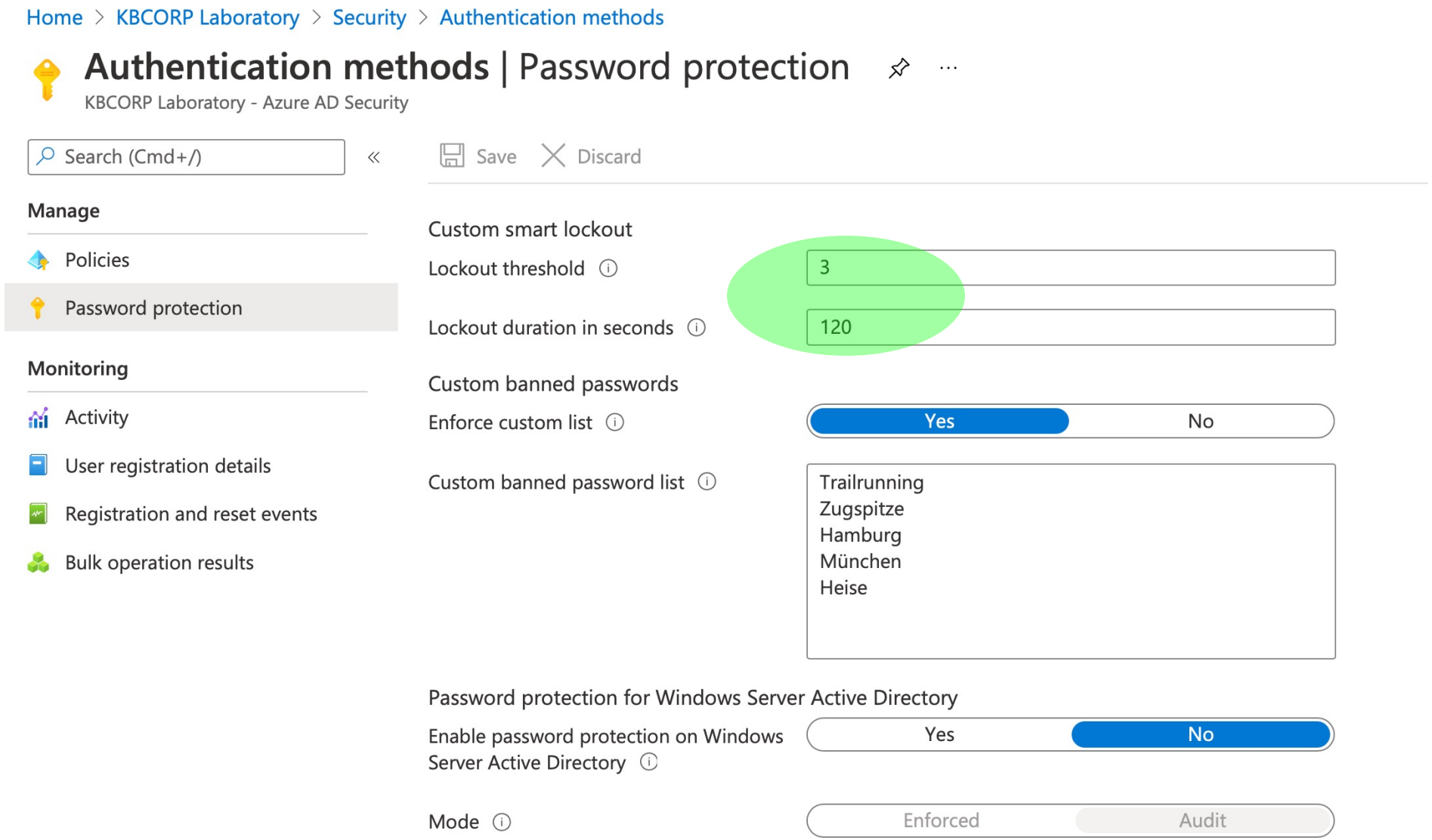
„Duration“ in AAD longer then „Lockout Counter“ On-Prem

Error

Zero Trust Identity – minor but powerful functionalities



Zero Trust Identity – minor but powerful functionalities



Zero Trust Identity – minor but powerful functionalities

Privileged Identity Management (PIM)

Conditional Access Policies (CA)

Zero trust - identities

Administrative Units (AU)

Access Reviews

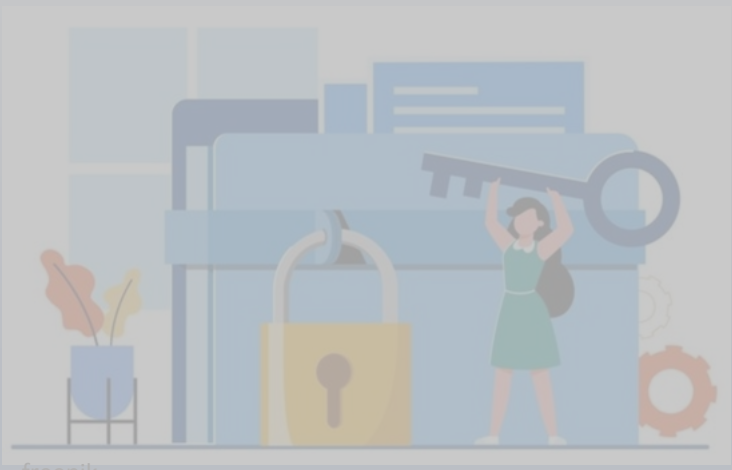
Banned Password Policy

Monitoring (e.g. Alert Rules

Custom Smart Lockout

Identity Protection (IdP)

Dynamic Group Memberships



freepik

Break Glass Accounts (BGA)

Multi Factor Authentication MFA

Zero Trust Identity – minor but powerful functionalities

Demo:
Custom Banned Password Policy

Zero Trust Identity – minor but powerful functionalities

Banned password list – normalization process when changing passwords

Allows to apply a small set of forbidden words to a large set of weak passwords

all letters are converted into lowercase

Character replacements:
@=a $=s 1=i 0=o

Example 1:
blank is in „banned password list“
User entered: Bl@Nk
After normalization: blank
and therefore invalid as password

Example 2:
Zugspitze is in my lab KBCORP in „custom banned password list“
Combinations and variants are also not allowed
Zugpitze1! is invalid.
Valid on the other hand Alpspitze1!

Zero Trust Identity – minor but powerful functionalities

Banned password list – normalization process when changing passwords

Allows to apply a small set of forbidden words to a large set of weak passwords

all letters are converted into lowercase

Character replacements:
@=a $=s 1=i 0=o

Example 3:
$3CureP@$$w0rd8
after normalization becomes
securepassword8
and is therefore rejected as invalid

Example 4:
Combinations of tenant or user names are taken into account:
Kbcorp!christa“
is also invalid and gets rejected

Zero Trust Identity – minor but powerful functionalities

Password strength evaluation algorithm

Final scoring

Each banned word = 1 point

Each unique character = 1 point

At least a score of
5. points is required to pass

Example of valid / invalid password

Zugsp1tzeHe1se98

Scored according to point system:

[zugspitze] + *[heise]* + *[9]* + *[8]*

1 + 1 + 1 + 1 = 4 points = not valid

Zugsp1tze6He1se98

Scored according to point system:

[zugspitze] + *[9]* + *[heise]* + *[9]* + *[8]*

1 + 1 + 1 + 1 + 1 = 5 points = valid

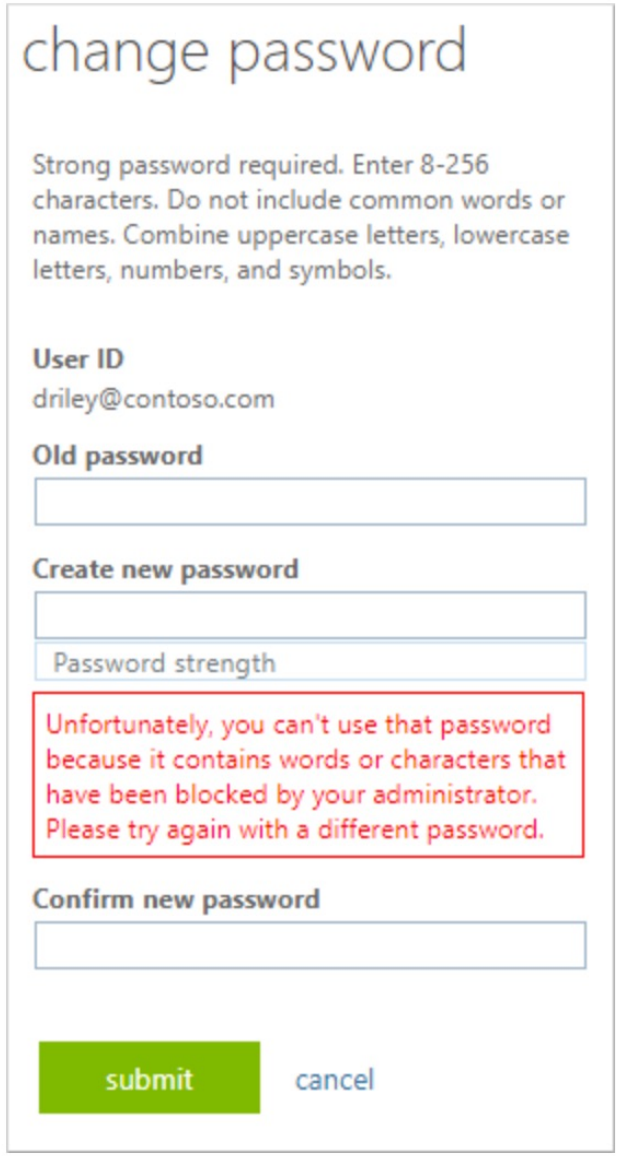
Zero Trust Identity – minor but powerful functionalities

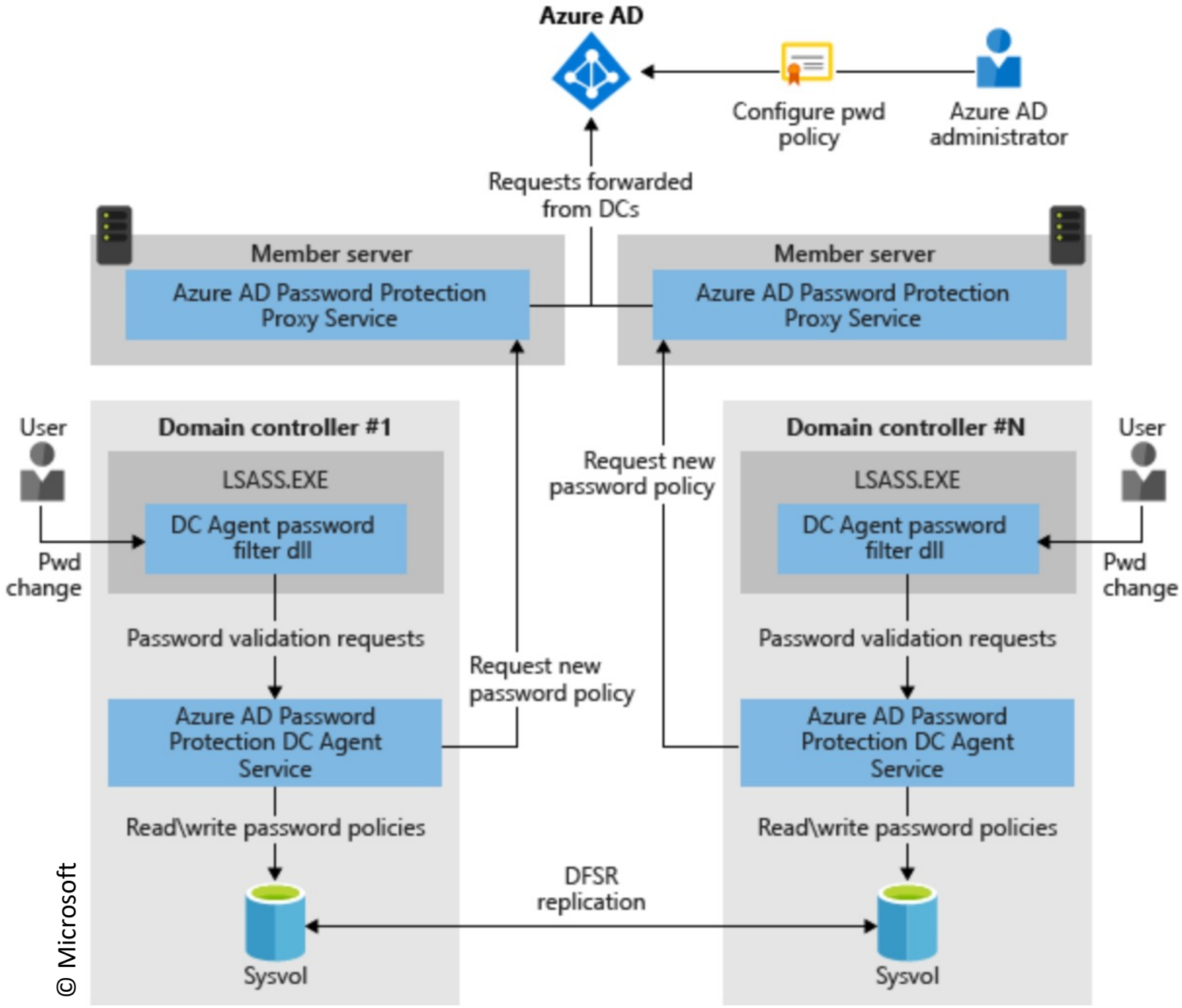
„Banned password list“ im Azure AD

- „Default“ Microsoft „Banned password list“ is not public
- „Custom list“ is a combination and words can be 4-16 char length and max. 1.000 entries
- Regional reference, product names, locations, company-specific abbreviations
- In the hybrid context, the function is extensible to on-premises Active Directory
- combined password list is obtained via proxy and provided to the DCs
- Compatible with existing password filters
- Only basic passwords useful. Normalization detects variations

Zero Trust Identity – minor but powerful functionalities

Password from banned pwd list entered





Key topics

No internet required on DCs

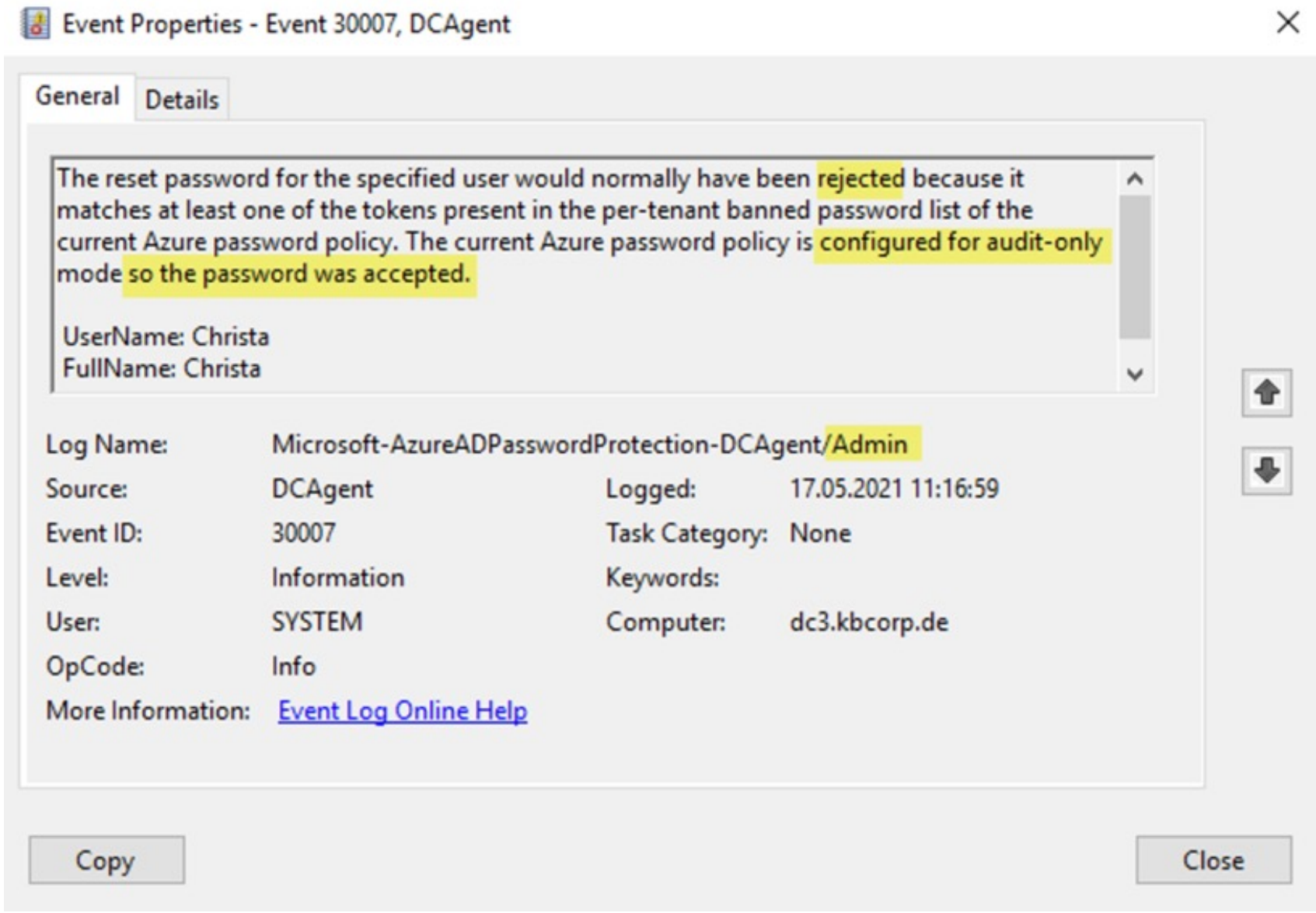
Works with other on-prem password filter dll

Audit mode

„what if“ mode – logs when password would have been rejected

[Microsoft docs article]

Zero Trust Identity – minor but powerful functionalities



Zero Trust Identity – minor but powerful functionalities

Privileged Identity Management (PIM)

Conditional Access Policies (CA)

Zero trust - identities

Administrative Units (AU)

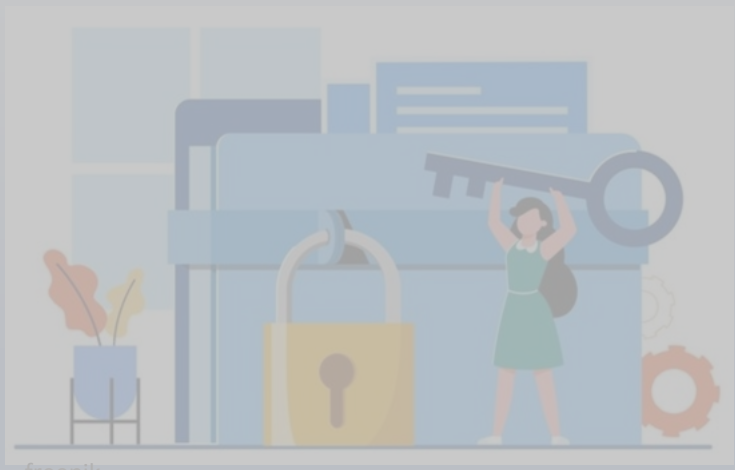
Access Reviews

Banned Password Policy

Monitoring (e.g. Alert Rules

Custom Smart Lockout

Identity Protection (IdP)



freepik

Dynamic Group Memberships

Break Glass Accounts (BGA)

Multi Factor Authentication MFA

Zero Trust Identity – minor but powerful functionalities

Emergency accounts – BGA (Break Glass Accounts)

Locking out of the tenant is possible and represents a nasty scenario

BGAs are an important part of a organization‘s disaster recovery plan

Especially important if PTA is used (requires connection to on-prem agents)

Multiple reasons for an "emergency" are possible:

➔ deleted admin accounts

➔ Incorrect configurations

➔ Policies too restrictive (e. g. Conditional Access)

Zero Trust Identity – minor but powerful functionalities

BGA Design / Implementation

- No synchronized user accounts
- Create "Cloud Only" user accounts (not personalized)
- A dedicated group only for these accounts
- BGA accounts have high privileges (GA)
- BGA accounts are used for exclusions (policies)
- Password considerations: Retention? Shared pwd?
- Risk Analysis required. Wide rights vs. no MFA

Administrative Aspects (ops)

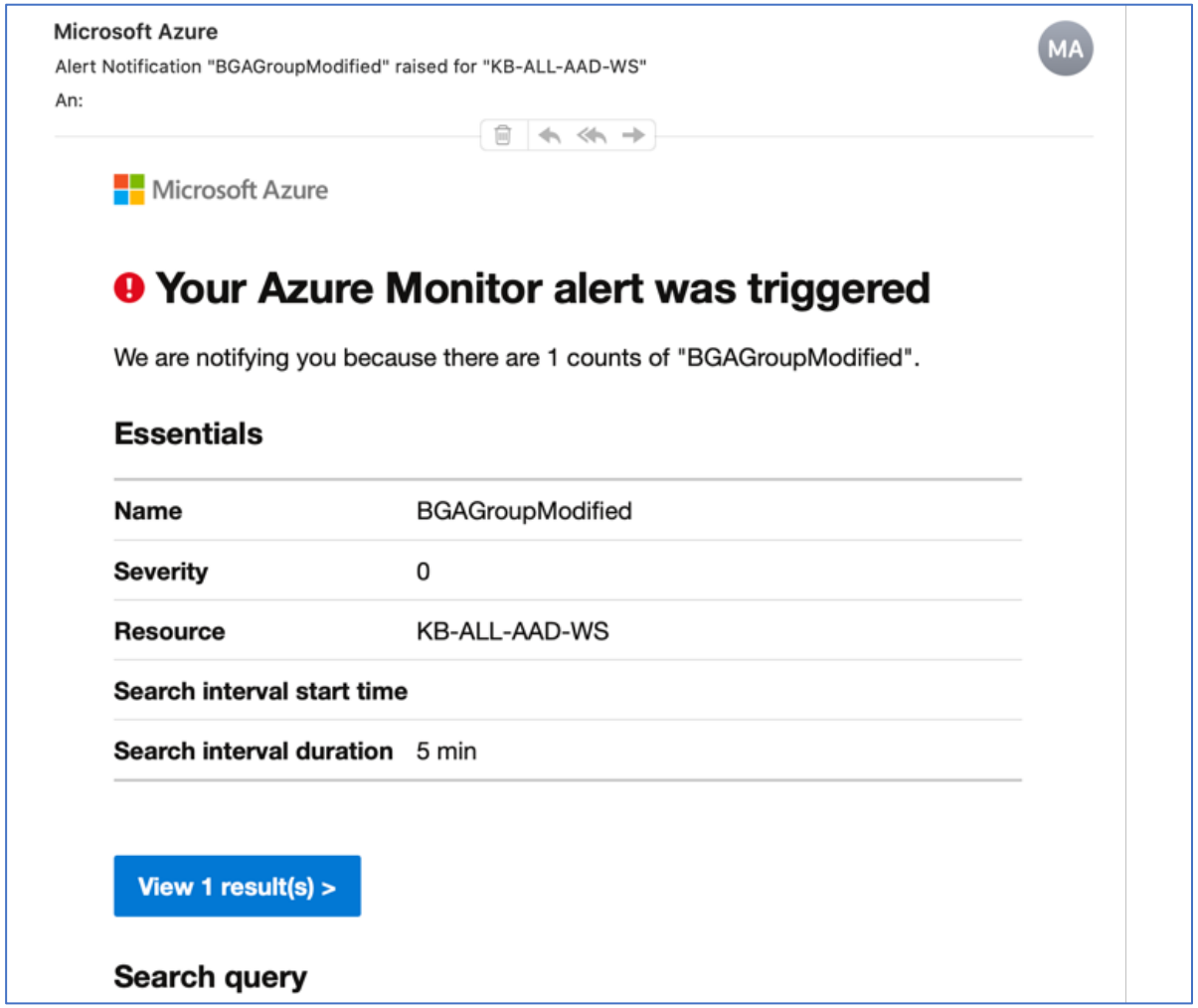
- Document emergency process
- Test regularly with planning. Part of ops man
- Alert rule for BGA login and modification to group
- Does login work? Rights ok? Messages ok?
- Check if "Excludes" fit in the policies
- Regularly check of warning- and alert rules
- Change of pwd in case of MA change in admin team

Zero Trust Identity – minor but powerful functionalities

Demo:
BGA Accounts –
Monitoring and exclusions

Zero Trust Identity – minor but powerful functionalities

Alert rule mail example



Microsoft Azure

Alert Notification "BGAGroupModified" raised for "KB-ALL-AAD-WS"

An:

MA

Microsoft Azure

Your Azure Monitor alert was triggered

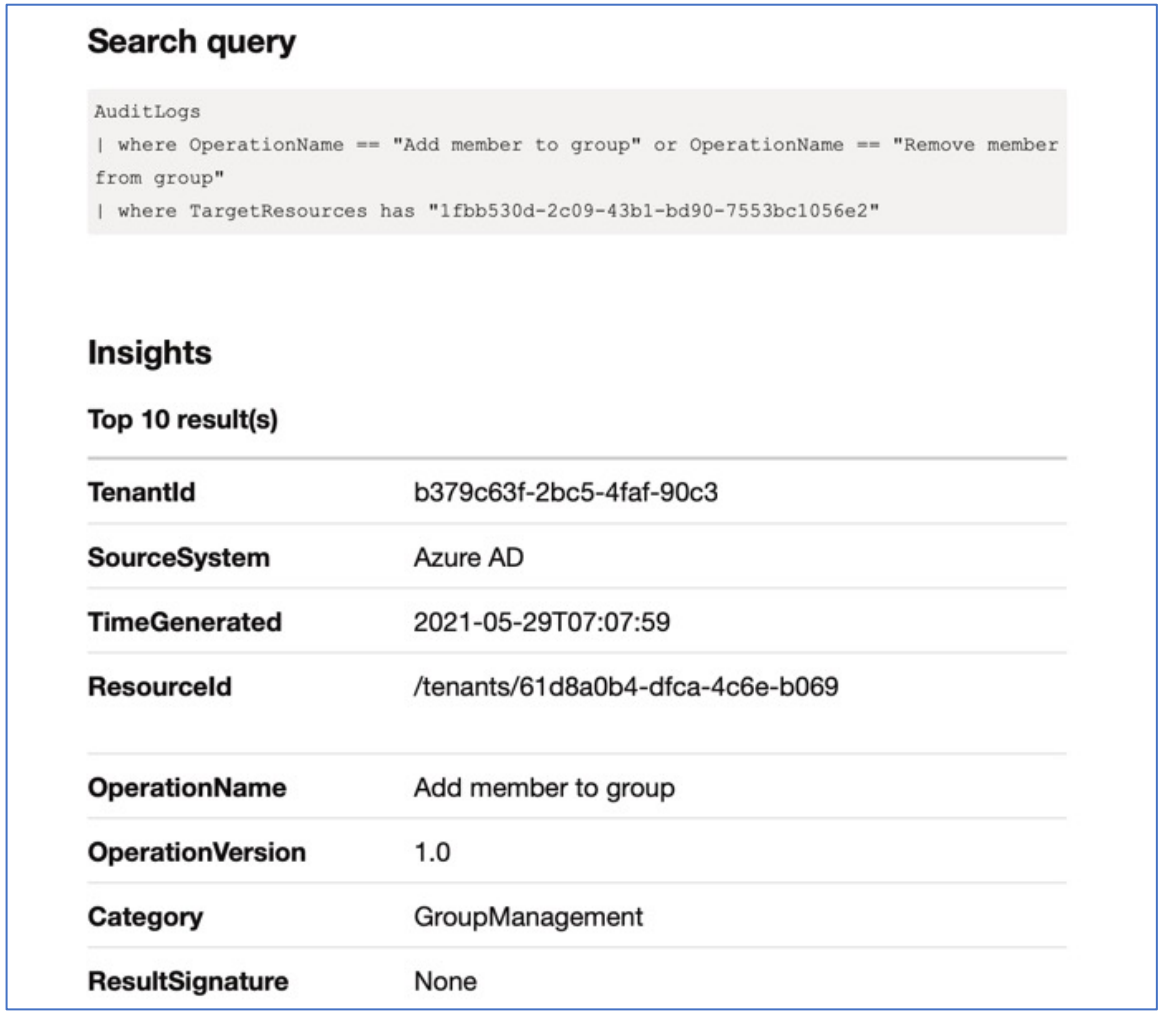
We are notifying you because there are 1 counts of "BGAGroupModified".

Essentials

Name	BGAGroupModified
Severity	0
Resource	KB-ALL-AAD-WS
Search interval start time	
Search interval duration	5 min

View 1 result(s) >

Search query



Search query

```
AuditLogs
| where OperationName == "Add member to group" or OperationName == "Remove member from group"
| where TargetResources has "1fbb530d-2c09-43b1-bd90-7553bc1056e2"
```

Insights

Top 10 result(s)

TenantId	b379c63f-2bc5-4faf-90c3
SourceSystem	Azure AD
TimeGenerated	2021-05-29T07:07:59
ResourceId	/tenants/61d8a0b4-dfca-4c6e-b069
OperationName	Add member to group
OperationVersion	1.0
Category	GroupManagement
ResultSignature	None

Zero Trust Identity – minor but powerful functionalities

Alert rule mail example

InitiatedBy	{"user":{"id":"bdbec5f0-b623-41a4-bdf2-b99bed9d888e","displayName":null,"userPrincipalName":"Klaus-ADM@kbcorp.de","ipAddress":null,"roles":[]}}
LoggedByService	Core Directory
Result	success
TargetResources	[{"id":"f8ae4847-632b-45f8-91b3-ea9d543b1024","displayName":null,"type":"User","userPrincipalName":"christa@kbcorp.de","modifiedProperties":[{"displayName":"Group.ObjectID","oldValue":null,"newValue":"\"1fbb530d-2c09-43b1-bd90-7553bc1056e2\""},{"displayName":"Group.DisplayName","oldValue":null,"newValue":"\"BGAAccounts\""},{"displayName":"Group.WellKnownObjectName","oldValue":null,"newValue":null}],"administrativeUnits":[]},{"id":"1fbb530d-2c09-43b1-bd90-7553bc1056e2","displayName":null,"type":"Group","groupType":"unknownFutureValue","modifiedProperties":[],"administrativeUnits":[]}]
AADTenantId	61d8a0b4-dfca-4c6e-b069-
ActivityDisplayName	Add member to group

Zero Trust Identity – minor but powerful functionalities

Azure AD - regular tasks (examples)

Daily

Check for mail from attached services (Access Reviews, PIM, warning rules, ...)

Weekly

Checking the "Azure AD Connect Health" Dashboard

Check Workbooks “e.g. Failure" statistics in Azure Workbook

Keep an eye on "Identity / Secure Score“

Zero Trust Identity – minor but powerful functionalities

Azure AD - regular tasks (examples)

Monthly:

- Check if a new Azure AD Connect version has been released
- Manually check if exclusions are in place
- Login test with „Break Glass Accounts“ !! Must fire alert rules etc.

Quarterly:

- Change Staging / Active AAD Connect Server
- Check for orphaned objects (Sentinel or PS with LastLogonTimeStamp)

Zero Trust Identity – minor but powerful functionalities

Privileged Identity Management (PIM)

Conditional Access Policies (CA)

Zero trust - identities

Administrative Units (AU)

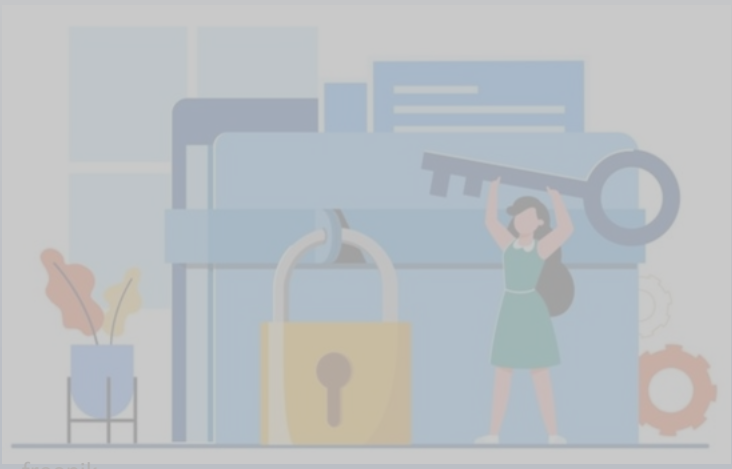
Access Reviews

Banned Password Policy

Monitoring (e.g. Alert Rules

Custom Smart Lockout

Identity Protection (IdP)



freepik

Dynamic Group Memberships

Break Glass Accounts (BGA)

Multi Factor Authentication MFA

Zero Trust Identity – minor but powerful functionalities

Container to bundle objects for administrative purposes

- Administrative structure. Users and groups can be assigned
- No hierarchical structure, no nesting, no Inheritance etc.
- Management via PowerShell, Graph API, Azure Portal
- Possibility to enable management on specific groups / user accounts (project office e. g.)
- Mystaff.microsoft.com offers very "simple" administrative options (PW Reset)
- M365 Admin Portal also possible. More comfortable
- Administered objects can be assigned to multiple "Administrative Units“

Zero Trust Identity – minor but powerful functionalities

Top three advantages and disadvantages of "Administrative units“

Advantages:

- Allows administration to users without giving access to the Azure AD portal
- Implementierung ohne viel Aufwand. Gut geeignet für kurzfristigen Zweck (Projekt)
- Implementation without much effort. Well suited for short term purpose (project)

Disadvantage:

- Multiple units can be confusing. Who may do what and where can be unclear
- Only a few roles are currently available
- Only static assignment of identities to admin units. No dynamic functionality

Zero Trust Identity – minor but powerful functionalities

- Agenda and key takeaways -

Privileged Identity Management (PIM)

Conditional Access Policies (CA)

Zero trust - identities

Administrative Units (AU)

Access Reviews

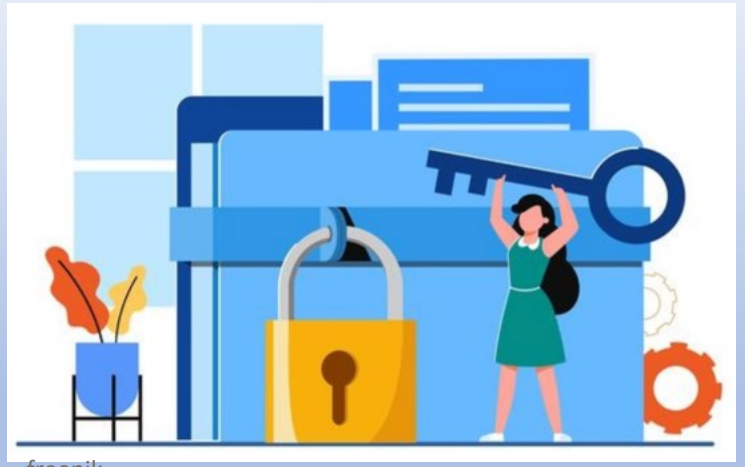
Banned Password Policy

Monitoring (e.g. Alert Rules

Custom Smart Lockout

Identity Protection (IdP)

Dynamic Group Memberships



freepik

Break Glass Accounts (BGA)

Multi Factor Authentication MFA

Zero Trust Identity – minor but powerful functionalities

https://news.microsoft.com/ignite-november-2021-book-of-news/

Zero Trust Identity – minor but powerful functionalities

Quick overview on tools

- Conditional Access policies
- Access Reviews
- Azure AD Monitoring
- Identity Protection
- Privileged Identity Management (PIM)
- Administrative Units
- Password Protection
- Dynamic Group Membership
- Emergency Access (BGA Accounts)
- MFA - how it works

Extended reading covered topics

- Tutorial: Configure Banned Passwords
- Plan and deploy on-premises AAD pwd protection
- How to manage staled devices in Azure AD
- How to manage inactive Users in Azure AD

Nothingbutcloud – 2-5min reading blog posts

- Zero Trust in Azure Identity - Part 1: Tenant Security
- Zero Trust in Azure Identity - Part 2: MFA! Is there a right way?
- Zero Trust in Azure Identity - Part 3: Conditional Access
- Zero Trust in Azure Identity - Part 4: Access Reviews
- Zero Trust in Azure Identity - Part 5: Monitoring critical roles