



Think You Have Entra Backup? Think Again!

Klaus Bierschenk
Director Consulting Expert,
CGI Germany



Meet the Speaker

Klaus Bierschenk

Director Consulting Expert / CGI Germany

- Based in Murnau in Bavaria
- With my Family, two cats and two snakes
- Mountain lover, Ultrarunner



[linkedin.com/in/klabier/](https://www.linkedin.com/in/klabier/)



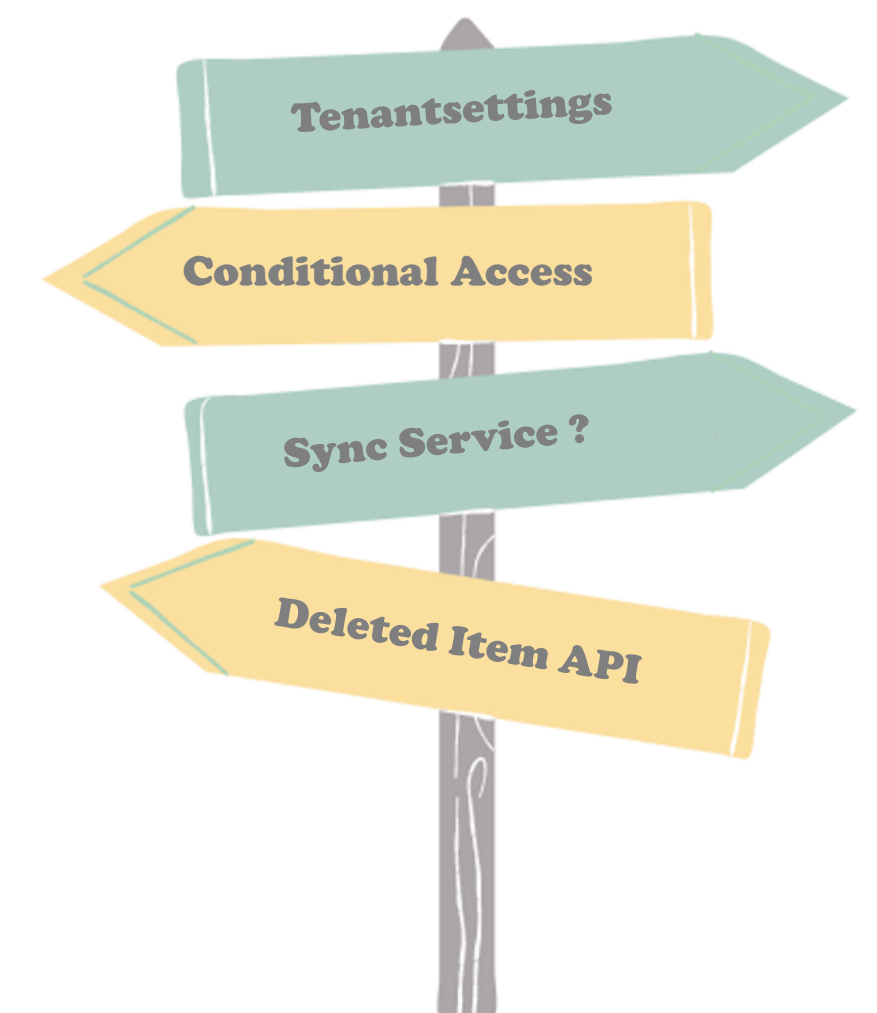
Klaus@nothingbutcloud.net



<https://nothingbutcloud.net>

Trust is good, backup is better... so what's our topic today?

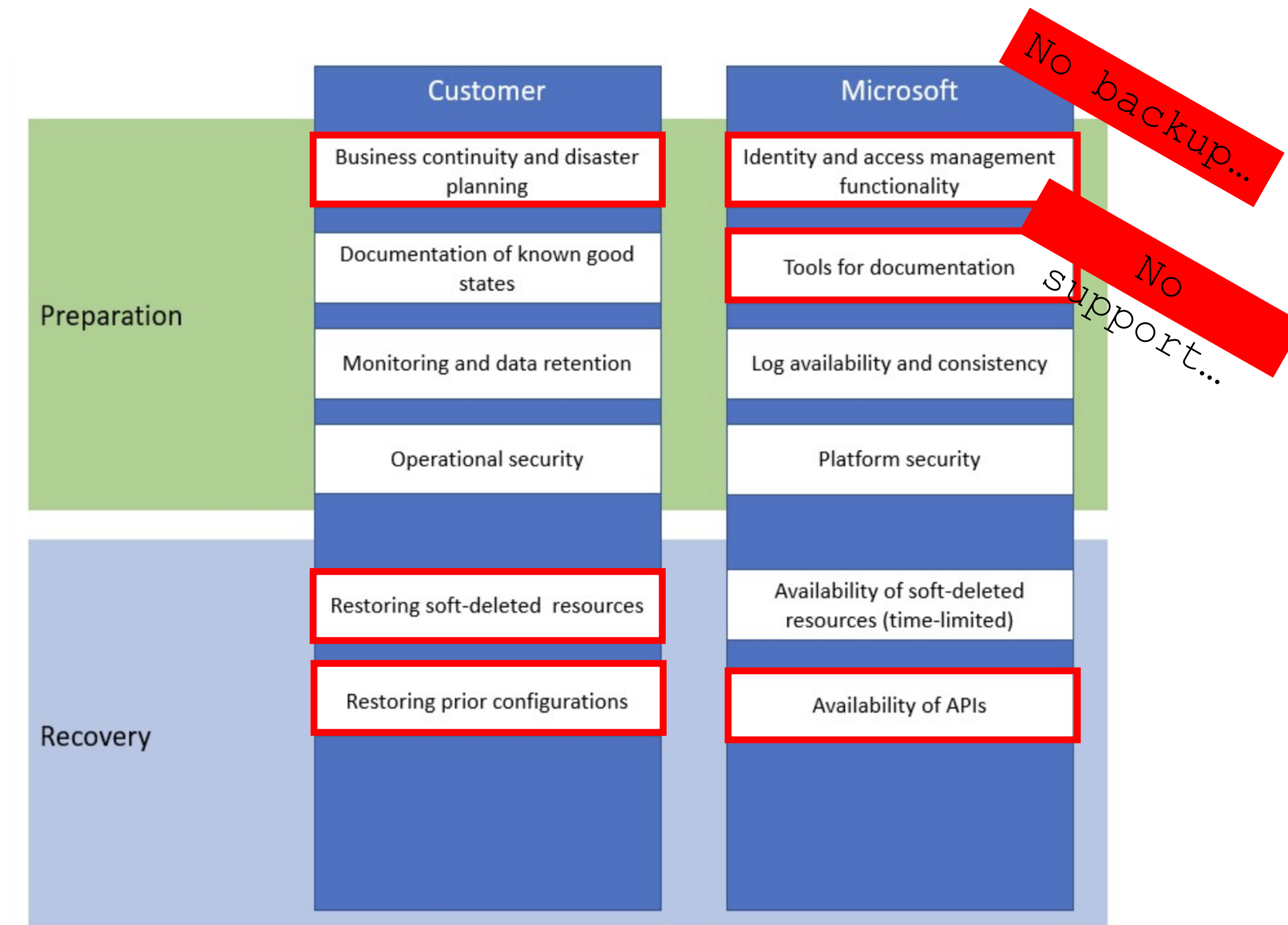
- What is Microsoft's standpoint on backup and restore in Entra ID?
- How can we back up Entra ID — or should we rather ask: What can actually be restored?
- Operational prerequisites: How can we prevent object or configuration loss in Entra ID?



What is Microsoft's standpoint on backup and restore in Entra ID ?

Microsoft provides platform & APIs

Customer responsible for planning & restoring



Source: [Microsoft Learn](#)

Prioritize your crown jewels



- *Know what is really important;* otherwise, a recovery concept becomes difficult
- Sometimes proper documentation is enough, sometimes a backup procedure is the better choice
(... with a tenant of >50 CA policies, documentation alone is not helpful)
- Every company is different, every Entra ID tenant is different — not everything is always equally critical
(... when a tenant has Security Defaults enabled, backing up CAs is not the major topic)



Many settings. Which ones really matter?



User Management & Settings

User roles & permissions
Default sign-in options for users
User lifecycle policies
Locked account policies
User sign-in & session policies
Policies for secondary email addresses
User sign-in logs & auditing
Management of authentication methods
Self-service user registration

Authentication & Security

Multi-Factor Authentication (MFA) policies
Passwordless authentication (FIDO2, Windows Hello)
Certificate-based authentication
Token lifetimes & session configuration
Continuous Access Evaluation (CAE)
Risk-based authentication
Identity risk policies
Authentication strengths for external users
Adaptive authentication policies

Password Policies & Password Protection

Password length & complexity requirements
Password expiration period
Banned password policy (custom deny list)
Smart logout policy (failed sign-in attempts)
Self-Service Password Reset (SSPR) policies
Security questions for SSPR
Temporary Access Pass policies
Advanced password protection policies for on-premises AD

Global Secure Access (GSA)

Network access policies
Conditional Access for network connections
Conditional Access for network segments
Conditional Access for apps

Global Secure Access (GSA)

Assigned Access
Zero Trust Network Access
Web content filtering
DNS security policies
Logging & monitoring for network access



Dynamic group policies
Group-based license assignment
Self-service group management policies
Automatic group membership based on attributes

Guest Users & External Collaboration (B2B/B2C)

Guest invitation settings
External identity providers (Google, Facebook, SAML, OpenID)
B2B collaboration policies
Guest user permission policies
Automate external user deletion
Session policies for guest users

Cloud Sync & Synchronization Settings

Entra ID Cloud Sync & Synchronization Settings
External identity providers (Google, Facebook, SAML, OpenID)
B2B collaboration policies
Guest user permission policies
Automate external user deletion
Session policies for guest users
SCIM synchronization with third-party providers
On-premises directory synchronization (Azure AD Connect)
Custom synchronization rules

Conditional Access & Access Control

Conditional Access & Access Control
Policies for users & groups
Device state & compliance
Session policies
Access control for apps & services
Access control for risk-based rules
Cross-tenant access
Security levels for external identities
Terms of use pages



Security & Monitoring Policies
Security alerts & Identity Protection
Identity protection and risk detection settings
Audit logging for identity activities
Anomaly detection for sign-in attempts
Security assessments & recommendations

Roles & Permissions (RBAC & PIM)

Custom roles & permissions
Least privilege access policies
Time-bound role assignments (Just-In-Time)
Approval workflows for admin roles
Audit logs for privileged roles
Security reviews for highly privileged accounts

Identity Governance & Compliance

Regular reviews
Automated reviews
Compliance management
Automated compliance
Entitlement management
Access control workflows

Device Management & Microsoft Entra Cloud Sync

Register devices in Entra ID (Hybrid Azure AD Join, Azure AD Join)
Device tagging and compliance
Device management for Windows, macOS, iOS, and Android
Enable/disable devices in Entra ID
Device lifecycle management
Configure and manage Entra ID Cloud Sync
Define synchronization filters for groups and users
SCIM synchronization with third-party services
Manage on-premises directory synchronization (Azure AD Connect, Cloud Sync)



Add/remove enterprise applications
Enable Single Sign-On (SSO) for applications
Configure App Proxy for legacy applications
Define OAuth and OpenID Connect policies
Configure third-party identity providers
Manage token lifetimes for applications
Define Conditional Access policies for applications
Configure user and group permissions for apps
Set up managed identities for services

Administrative Units (AUs)

Administrative Units (AUs)
Administrative Units (AUs)
Administrative Units (AUs)

Tenant Settings & Organizational Policies

Manage tenant name and domains
Configure organizational branding
Define privacy policies for identities
Restrictions for multi-tenant organizations
Enable Microsoft Entra ID Governance
Manage Adaptive Application Controls
Conditional Access for tenant-level policies
Control self-service group management

Microsoft Entra Cross-Tenant Access

Policies for cross-tenant collaboration
Manage external access to organizational resources
Define tenant-based authentication rules
Adaptive authentication mechanisms for external users



Just the big picture — not for detailed reading


```

1  {
2    "id": "049fab0d-a309-43b9-a3f9-e2f25aa9caf8",
3    "templateId": null,
4    "displayName": "CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA",
5    "createdDateTime": "2022-07-05T17:05:36.8206457Z",
6    "modifiedDateTime": "2025-07-31T19:38:28.5262738Z",
7    "state": "enabled",
8    "deletedDateTime": null,
9    "partialEnablementStrategy": null,
10   "sessionControls": null,
11   "conditions": {
12     "userRiskLevels": [],
13     "signInRiskLevels": [],
14     "clientAppTypes": [...],
15     "platforms": null,
16     "locations": null,
17     "times": null,
18     "deviceStates": null,
19     "devices": null,
20     "clientApplications": null,
21     "applications": {...},
22     "users": {
23       "includeUsers": [...],
24       "excludeUsers": [
25         "08a644d4-6533-4931-9158-edee7db7fffa",
26         "349c5270-e777-4727-b655-43f99f454dc2"
27       ],
28       "includeGroups": [],
29       "excludeGroups": [
30         "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
31       ],
32       "includeRoles": [],

```






Recover via deletedItems API

GET

v1.0

https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.serviceprincipal

Run query

GET

v1.0

https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.administrativeUnit

Run query

Possible error found in URL near: .graph.administrativeUnit

Request body

Request headers

Modify permissions

Access token

OK - 200 - 193 ms

OK - 200 - 121 ms

Response preview

Response headers

Code snippets

Toolkit component

Adaptive cards

Expand

```

{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#directory/deletedItems/microsoft.graph.administrativeUnit",
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For example: GET directory/deletedItems/microsoft.graph.administrativeUnit?$select=description,displayName",
  "value": [
    {
      "id": "99e94705-e05c-4e45-aa19-9c49f7b1475e",
      "deletedDateTime": "2025-04-06T17:00:00Z",
      "displayName": "Praktikanten",
      "description": "Alle Praktikanten",
    }
  ]
}

```

Supported resources:

- Administrative unit
- Application
- M365 Group
- ServicePrincipal
- user

Additional reading:

<https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.serviceprincipal>

<https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.administrativeUnit>

Recover via deletedItems API



POST v1.0 https://graph.microsoft.com/v1.0/directory/deletedItems/49807c30-fa32-4f17-92ed-d95666262d83/restore Run query

No resource was found matching this query

Request body Request headers Modify permissions Access token

Permissions

One of the following permissions is required to run the query. If possible, consent to the least privileged permission.

OK - 200 - 799 ms

Response preview Response headers Code snippets Toolkit component Adaptive cards Expand

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#directoryObjects/$entity",
  "@odata.type": "#microsoft.graph.servicePrincipal",
  "id": "49807c30-fa32-4f17-92ed-d95666262d83",
  "deletedDateTime": null,
  "accountEnabled": true,
  "alternativeNames": [],
  "appDisplayName": "Microsoft Graph Command Line Tools",
}
```

Permissions and additional reading at [Microsoft Learn](#)



I WANT YOU
To protect your
Entra Crown Jewels

How to create a smart and easy backup?

→ Manually
Code-base

→ PowerShell
Some man

```
$AllPolicies = Get-MgIdentityConditionalAccessPolicy -All

foreach ($Policy in $AllPolicies) {
    # Get the display name of the policy
    $PolicyName = $Policy.DisplayName

    # Convert the policy object to JSON with a depth of 6
    $PolicyJSON = $Policy | ConvertTo-Json -Depth 10

    # Write the JSON to a file in the export path
    $PolicyJSON | Out-File "$BackupFolder\$PolicyName.json" -Force

    # Print a success message for the policy backup
    Write-Host "Successfully backed up CA policy: $($PolicyName)" -ForegroundColor Green
}

Write-host "`nFiles stored in" $($BackupFolder) "`n" -ForegroundColor Green
```



How to create a smart and easy backup?

→ Manually difficult

Code-based approaches are much better

→ PowerShell is your friend

Some manual tweaking... JSON must be precise

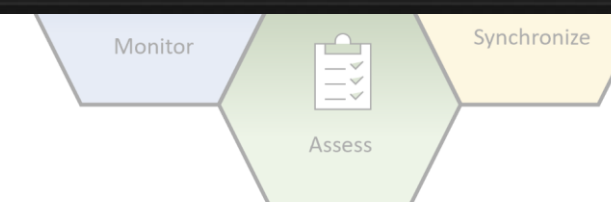
→ EntraExporter is your better friend

Download here: [Open-Source Github](#)

→ M365DSC is another great friend

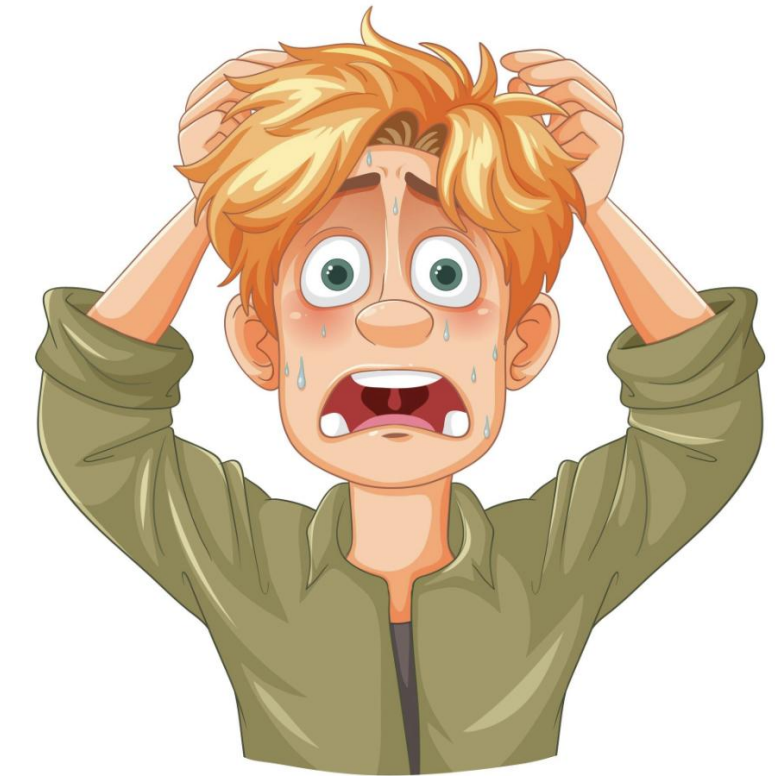
Download here: [Open-Source Github](#)

```
1 {
2   "id": "049fab0d-a309-43b9-a3f9-e2f25aa9caf8",
3   "templateId": null,
4   "displayName": "CA003-Global-BaseProtection-AllApps-AnvPlatform-MFA",
5   "createdDateTime": "2022-07-05T17:05:36.8206457Z",
6   "modifiedDateTime": "2025-07-31T19:38:28.5262738Z",
7   "state": "enabled",
8   "deletedDateTime": null,
9   "partialEnablementStrategy": null,
10  "sessionControls": null,
11  "conditions": {
12    "userRiskLevels": [],
13    "signInRiskLevels": [],
14    "clientAppTypes": [ ...
15  ],
16  ],
17  "platforms": null,
18  "locations": null,
19  "times": null,
20  "deviceStates": null,
21  "devices": null,
22  "clientApplications": null,
23  "applications": { ...
24  },
25  },
26  "users": {
27    "includeUsers": [ ...
28  ],
29    "excludeUsers": [
30      "08a644d4-6533-4931-9158-edee7db7fffa",
31      "349c5270-e777-4727-b655-43f99f454dc2"
32    ],
33    "includeGroups": [],
34    "excludeGroups": [
35      "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
36    ],
37    "includeRoles": [],
38  }
```





Hard deleted? And now what?

- ✓ Object must be recreated
- ✓ Previews JSON export required (EntraExporter)
- ✓ Object will become a new ID
- ✓ Microsoft cannot help
- ✓ Example article on rebuilding a hard-deleted Administrative Unit on my blog → [Read Article](#)



To make sure it never comes down to a restore ...

- ✓ Protect sensitive groups with “PIM Protected Groups” → possible, but should you?
- ✓ AU — Restricted management (GA since June 2025)  Demo ...
- ✓ Protected actions for hard deletions (GA since January 2025)  Demo ...
- ✓ Smart alerting for important resources (samples at the end of the slide deck)



Summary: Back to the agenda questions

- ✓ Microsoft's standpoint is clear
- ✓ It is up to the Tenant Admin to define what is important
- ✓ Regularly reassess your crown jewels — what is truly important — and choose the right backup approach
- ✓ Protective measures against configuration loss: *Who can do what?*
Being proactive instead of reactive saves time and nerves





Further resources ...



Microsoft Learn

[Recoverability best practices](#) (covers Microsoft standpoint in shared responsibility)

[MS Learn: Recover from deletions](#)

[MS Learn: List deleted Item API Objects](#)

[MS Learn: Restore deleted Items and permissions](#)

[MS Learn: Application objects, service principals etc.](#)



Best Practices & Community

[Jorge de Almeida Pinto on HIPConf: Best Practices for Resync AD and Entra ID](#)

[Restricted management administrative units in Microsoft Entra ID](#)



NothingButCloud Blog

[Can I restore deleted Entra objects? Yes? No? Maybe?](#)

[Protecting your Conditional Access Policies: Lean Backup Strategies for Entra ID](#)

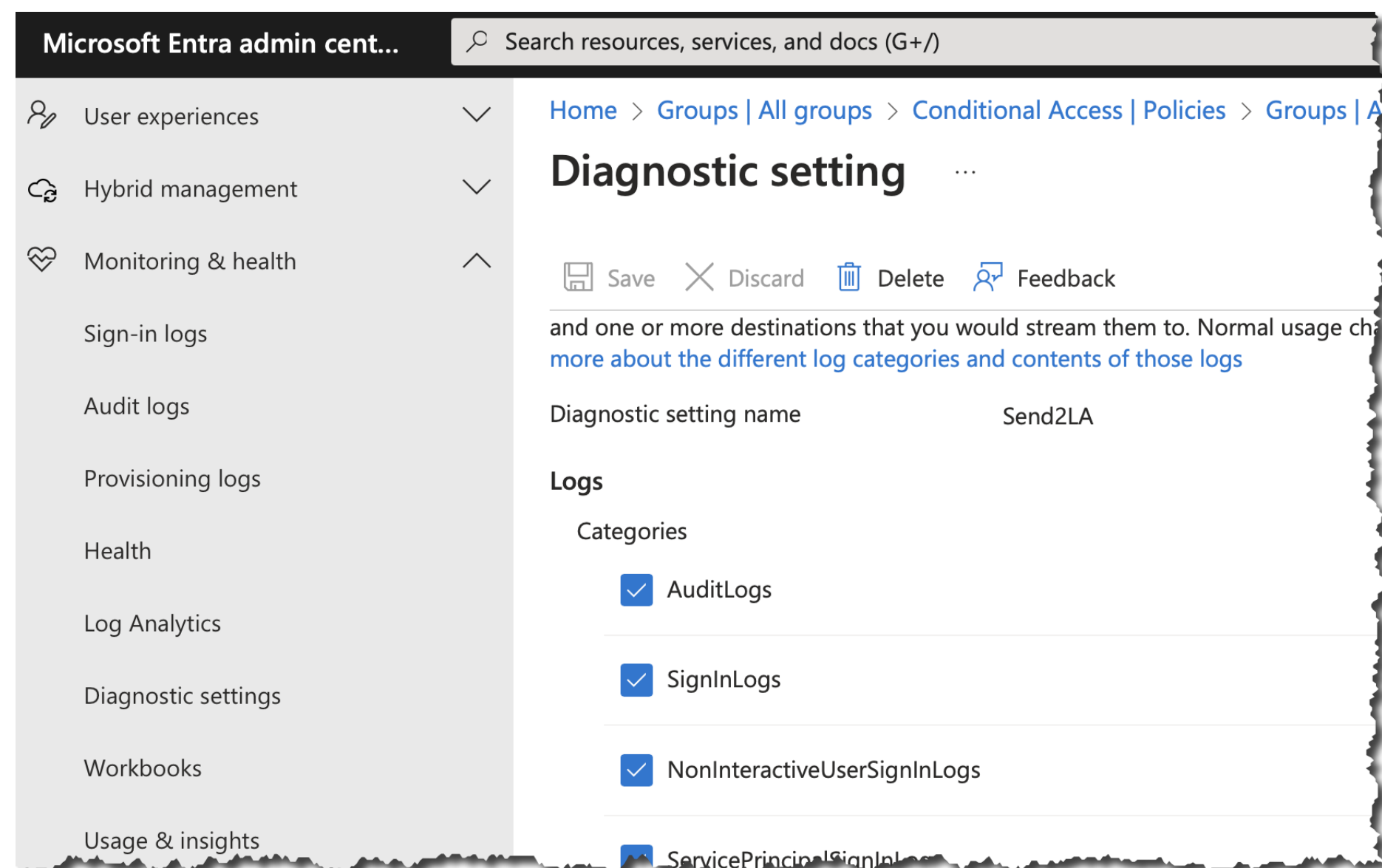
Questions?



Backup slides!

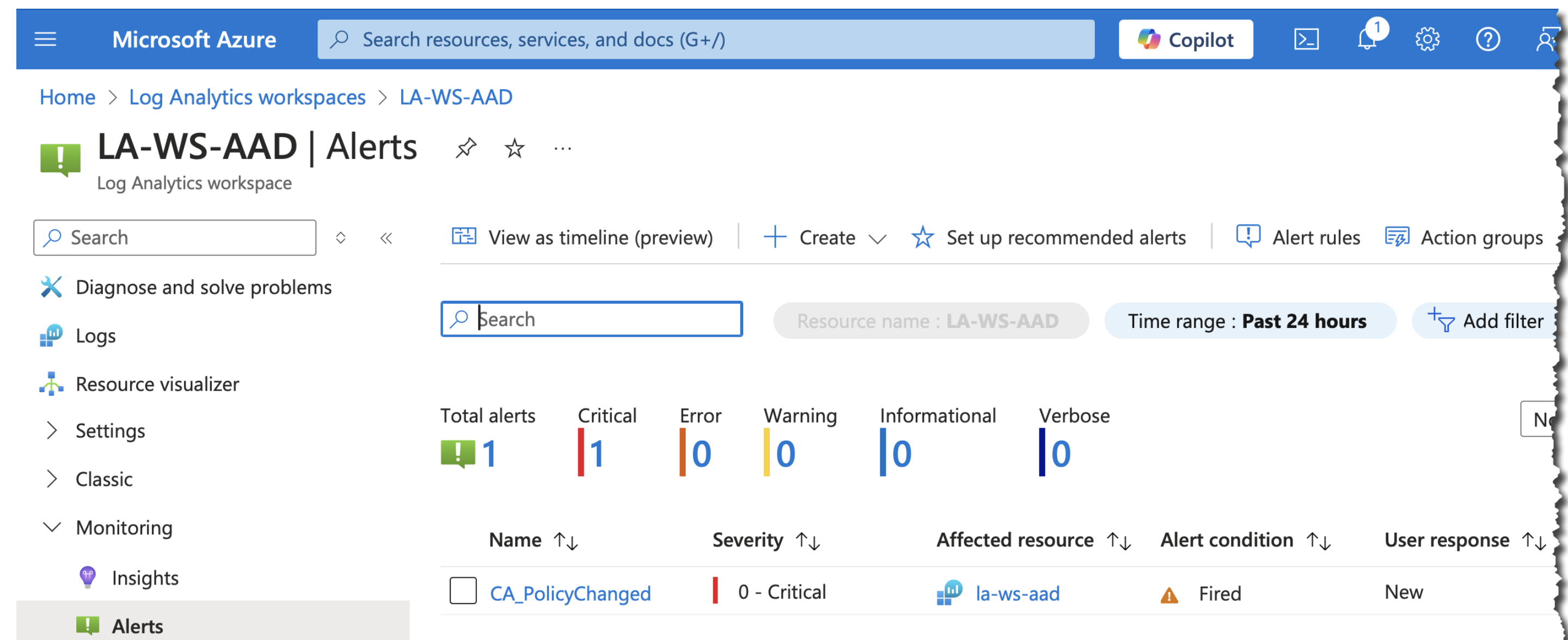
The simple way to alerting (1/2)

Configure diagnostic settings in Entra ID



Logs will be sent to repository

Configure response in Azure Portal



Then set up alert rule and action group →

The simple way to alerting (2/2)

Microsoft Azure Search resources, services, and docs (G+ /) Copilot

Home > Log Analytics workspaces > LA-WS-AAD | Alerts > Alert rules > CA_PolicyChanged >

Edit alert rule

Scope **Condition** Actions Details Tags Review + save

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * ⓘ [See all signals](#)

Define the logic for triggering an alert. Use the chart to view trends in the data. [Learn more](#)

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query *

```
AuditLogs | where ActivityDisplayName == "Update policy"
| project ActivityDateTime, ActivityDisplayName, TargetResources[0].displayName, InitiatedBy.user.userPrincipalName
```

Set up alert rule...

Microsoft Azure Search resources, services, and docs (G+ /) Copilot

Home > Log Analytics workspaces > LA-WS-AAD | Alerts > Alert rules > CA_PolicyChanged > Edit alert rule >

AdminTeamGE

Edit action group

Resource group

Region

Action group name

Display name *

Notifications

Notification type	Name	Status	Selected
Email/SMS message/Push/Voice	Klaus Mail	Subscribed	Email
Email/SMS message/Push/Voice	Klaus Black Phone	Subscribed	SMS message
Email/SMS message/Push/Voice	Klaus Yellow iPhone	Subscribed	SMS message
Email/SMS message/Push/Voice	Azure App	-	Push

...then set up action group



HYBRID
IDENTITY
PROTECTION
conf25

