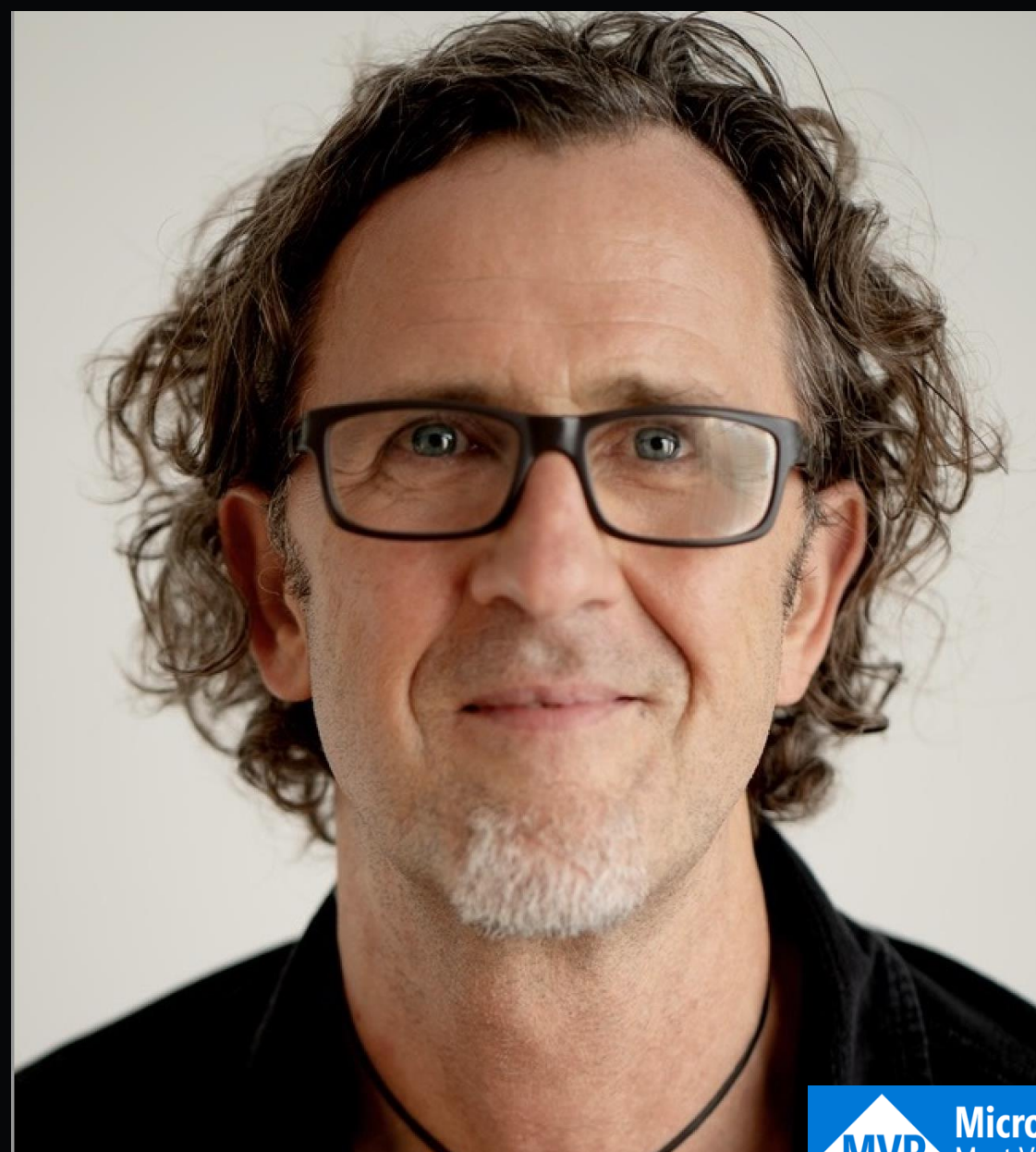




# Think You Have Entra Backup? Think Again!

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/)



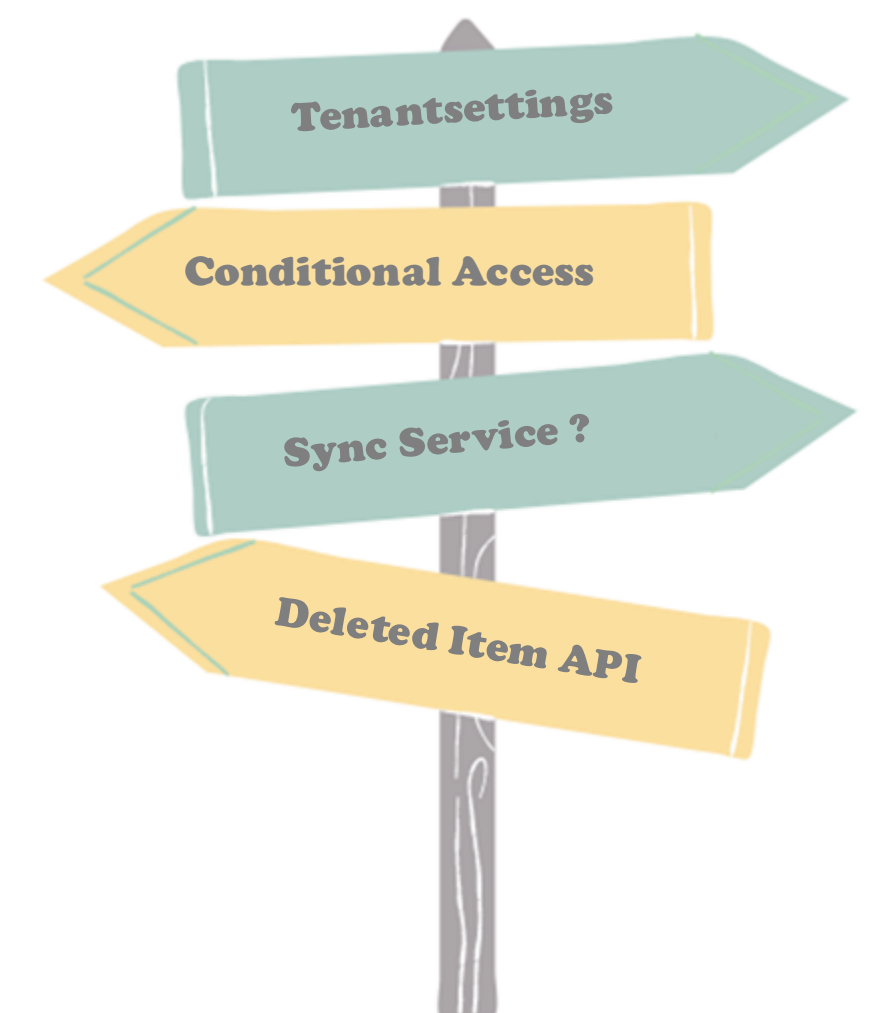
[Klaus@nothingbutcloud.net](mailto:Klaus@nothingbutcloud.net)



<https://nothingbutcloud.net>

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

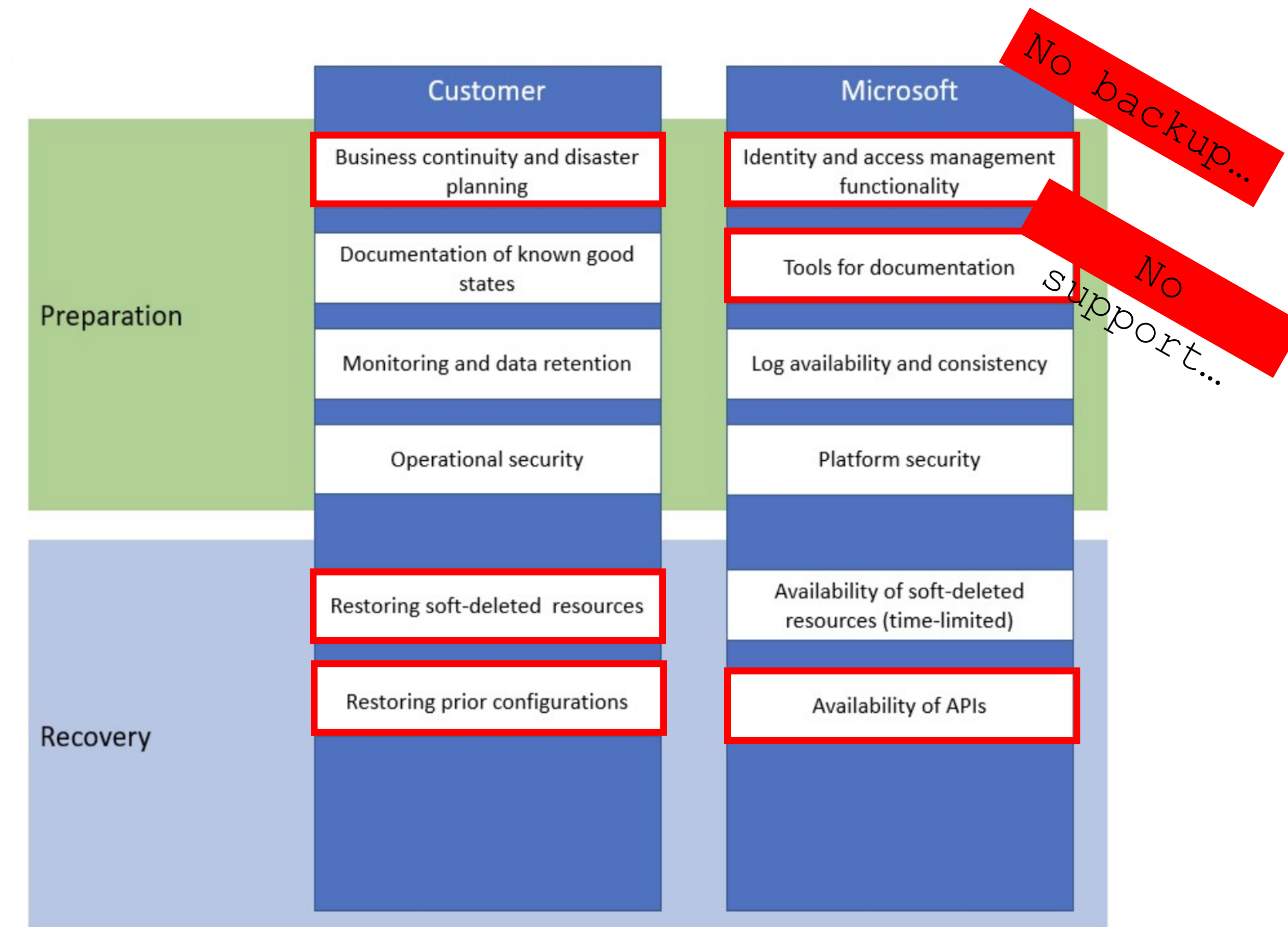
- What is Microsoft's standpoint on backup and restore in Entra ID ?
- How can we back up Entra ID – or should we rather ask: what can actually be restored ?
- Operational prerequisites: How can we prevent object or configuration loss in Entra ID ?



# 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

- *Knowing „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)*






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















# Entra object

Objekttyp	Soft delete	Restore?
User object	✓	 30d Recycle

```
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  },
16  "platforms": null,
17  "locations": null,
18  "times": null,
19  "deviceStates": null,
20  "devices": null,
21  "clientApplications": null,
22  "applications": {...},
23  },
24  "users": {
25    "includeUsers": [...],
26    "excludeUsers": [
27      "08a644d4-6533-4931-9158-edee7db7fffa",
28      "349c5270-e777-4727-b655-43f99f454dc2"
29    ],
30    "includeGroups": [],
31    "excludeGroups": [
32      "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
33    ],
34    "includeRoles": [],
35  },
36  },
37  },
38  },
39  },
40  },
41  },
42  },
43  },
44  }
```

# Entra object restore – reality check

Objektyp	Soft delete	Restore?
User object	✓	 30d Recycle Bin -> Hard deleted
Security group	X	 No restore 
M365 group	✓	 30d Recycle Bin -> Hard deleted
Device object	X	 No restore -> New registration (dsregcmd.exe)
Enterprise Application	✓	 Multi-Tenant -> Deleted Item API  Single-Tenant -> App Reg Recycle Bin
App Registration	✓	 Recycle Bin (Secrets & Certs ✓)
Administrative Unit	✓	 Deleted Item API (30d) -> Hard deleted
Conditional Access	✓	 Deleted Item API (30d) -> JSON export / import







**MARTY, WE HAVE TO GO  
BACK**






# Recover via deletedItems API







GET GET v1.0

GET beta <https://graph.microsoft.com/beta/identity/conditionalAccess/deletedItems/policies>   [Run query](#)

[Request Body](#)  [Request Headers](#)  [Modify Permissions](#)  [Access token](#)

OK - 200 - 242 ms

[Response preview](#)  [Response headers](#)  [Code snippets](#)  [Toolkit component](#)  [Adaptive cards](#)

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#identity/conditionalAccess/deletedItems/policies",
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For example: GET identity/conditionalAccess/deletedItems/policies?$select=conditions,createdDateTime",
  "value": [
    {
      "id": "7bedcea6-9403-450a-8cdb-7e73ee937552",
      "templateId": null,
      "displayName": "CA116-TESTAdmins-ProtectedAction-DeleteCAPolicies-Grant-OnlyGA",
      "createdDateTime": "2025-04-05T11:06:56.8869666Z",
      "modifiedDateTime": "2025-07-31T20:05:11.4691406Z",
      "state": "disabled",
      "deletedDateTime": "2025-09-16T15:18:04Z",
    }
  ]
}
```

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

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

<https://graph.microsoft.com/beta/identity/conditionalAccess/deletedItems/policies>

## Supported resources:

- Administrative unit
- Application
- M365 Group
- ServicePrincipal
- User
- CA Policy **NEW**

# 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-based

→ PowerShell  
Some manual

```
$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*

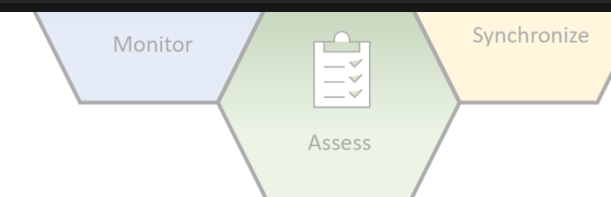
## → EntraExporter is your better friend

*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  "platforms": null,  
17  "locations": null,  
18  "times": null,  
19  "deviceStates": null,  
20  "devices": null,  
21  "clientApplications": null,  
22  "applications": {  
23    "users": {  
24      "includeUsers": [...]  
25    },  
26    "excludeUsers": [  
27      "08a644d4-6533-4931-9158-edee7db7fffa",  
28      "349c5270-e777-4727-b655-43f99f454dc2"  
29    ],  
30    "includeGroups": [],  
31    "excludeGroups": [  
32      "af7e030f-84e5-4edd-827f-8c7a7a1d14be"  
33    ],  
34    "includeRoles": [],  
35  }  
36  }  
37  }  
38  }  
39  }  
40  }  
41  }  
42  }  
43  }  
44  }
```





# How to create a smart and easy Backup?

## → Manually difficult

*Code-based approaches are much better*

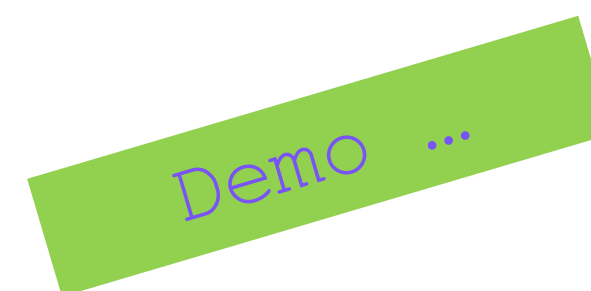
## → PowerShell is your friend

*Some manual tweaking... JSON must be precise – read-only attributes e.g.*



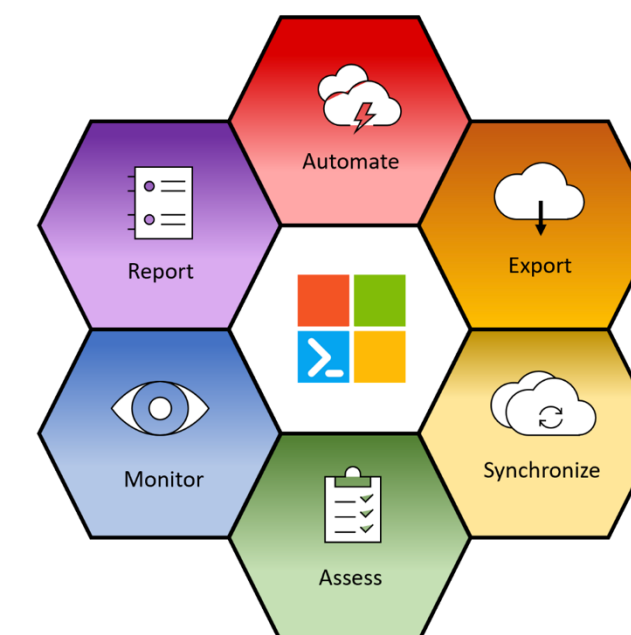
## → EntraExporter is your better friend

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



## → M365DSC is another great friend

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





# *Hard deleted? And now what?*

- ✓ Object must be recreated
- ✓ Previews JSON export required (EntraExporter)
- ✓ Object will become a new ID
- ✓ Microsoft can not 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) 
- ✓ Protected Actions for hard deletions (GA since January 2025) 
- ✓ 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.](#)

[MS Learn: Restore CA Policy](#)    **Public Preview (New)**



### **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?*

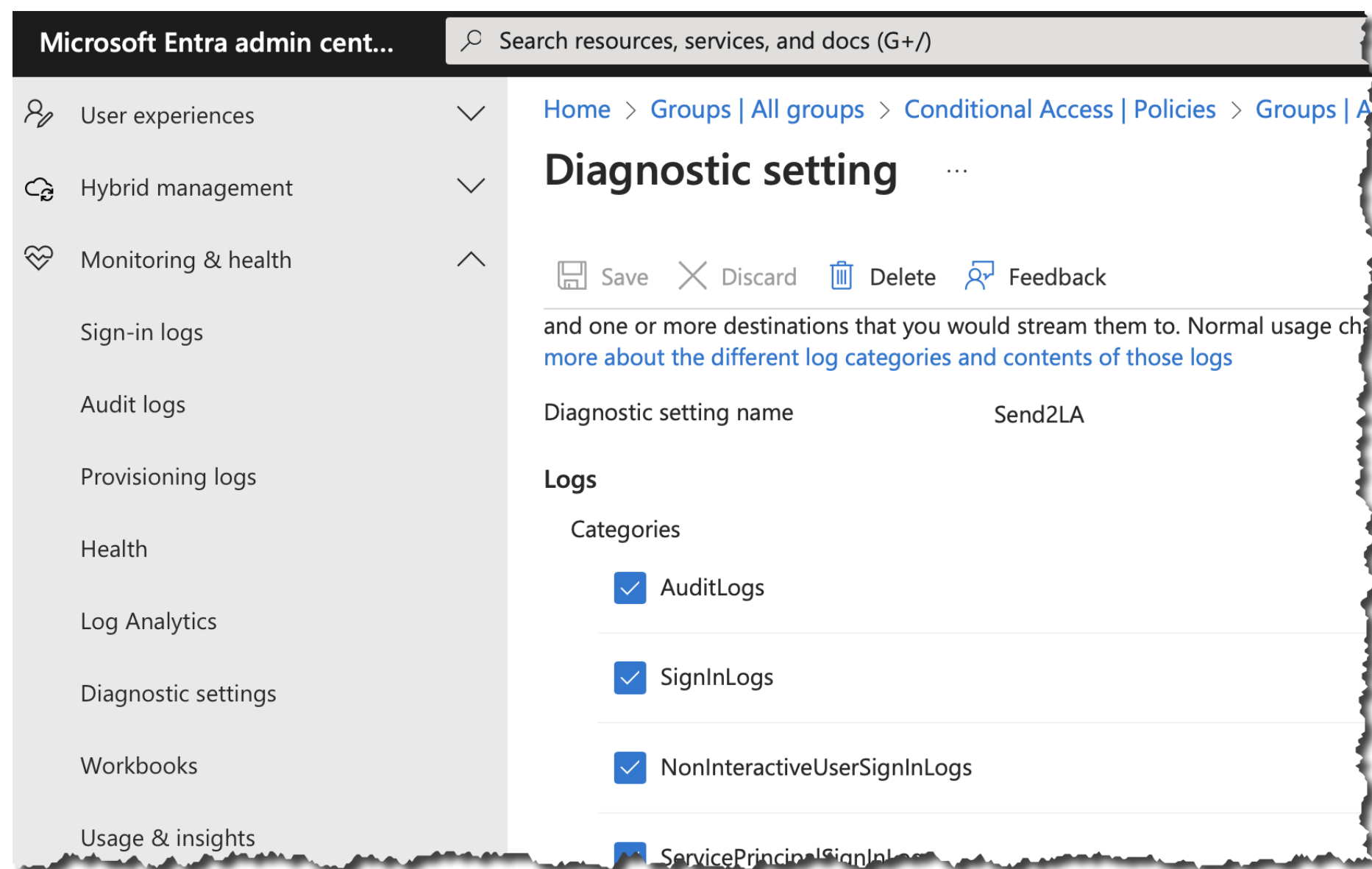




**Backup slides!**

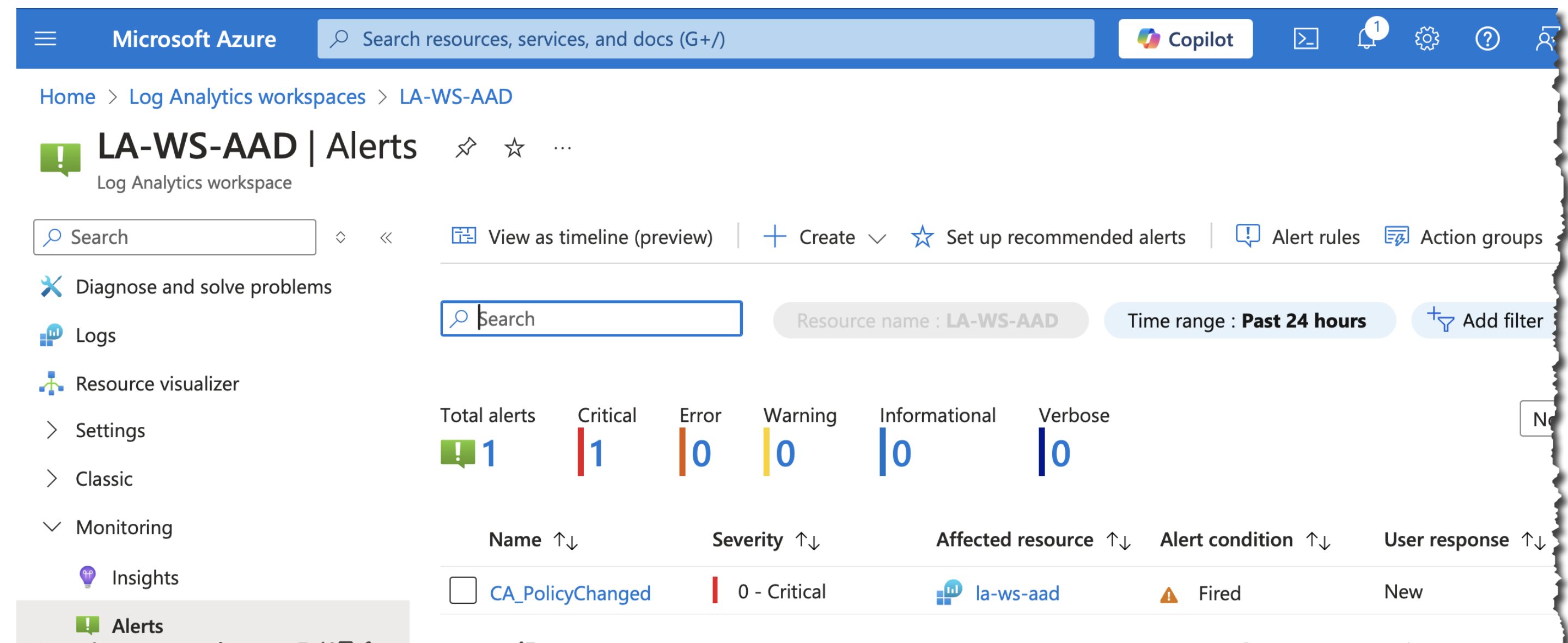
# The simple way to alerting (1/2)

## 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

ScopeConditionActionsDetailsTagsReview + save

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

Signal name \*

Custom log search

[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

Save changes

Test action group

Resource group

KBCORP-Monitoring

Region

Global

Action group name

AdminTeamGE

Display name \*

AdminTeamGE

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