

# Ich sichere mein Entra ID, bloß wie...?

Klaus Bierschenk, Director Expert @ CGI

Ich lebe mit meiner Familie, zwei Schlangen und zwei Katzen in Murnau

Ich bin viel in den Bergen unterwegs und laufe Ultrarennen  
Dies hilft mir sehr bei meinem beruflichen Fokus



<https://bsky.app/profile/klabier.bsky.social>



<http://www.linkedin.com/in/klabier>



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

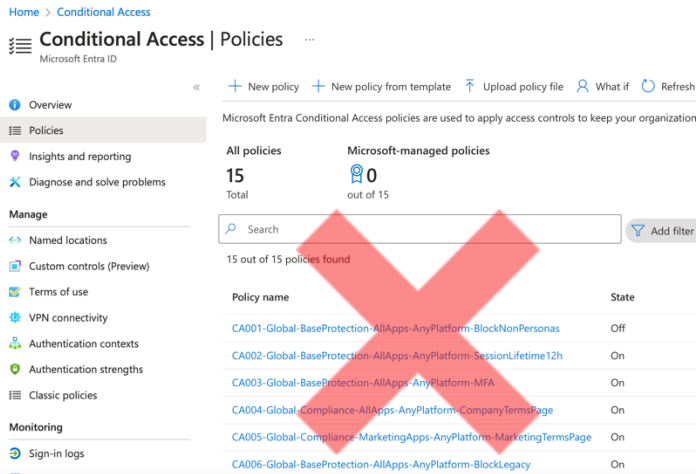
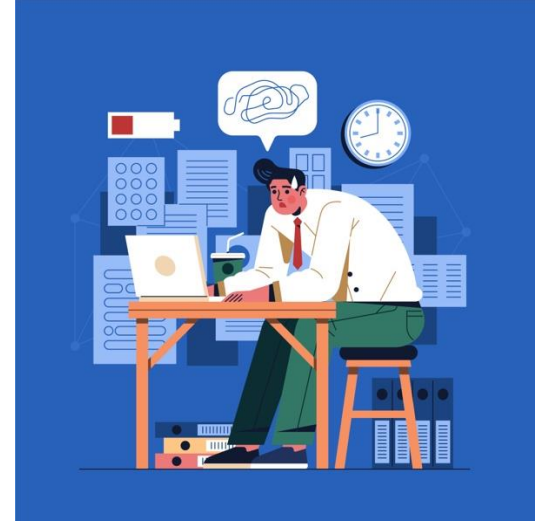


<https://nothingbutcloud.net/>

Vertrauen ist gut, Sicherung ist besser...  
... was ist unser Thema ?

Verlust von  
Konfiguration

Gelöschte Objekte  
in Entra ID





# AGENDA

**Tenantsettings**

**Conditional Access**

**Sync Service ?**

**Deleted Item API**

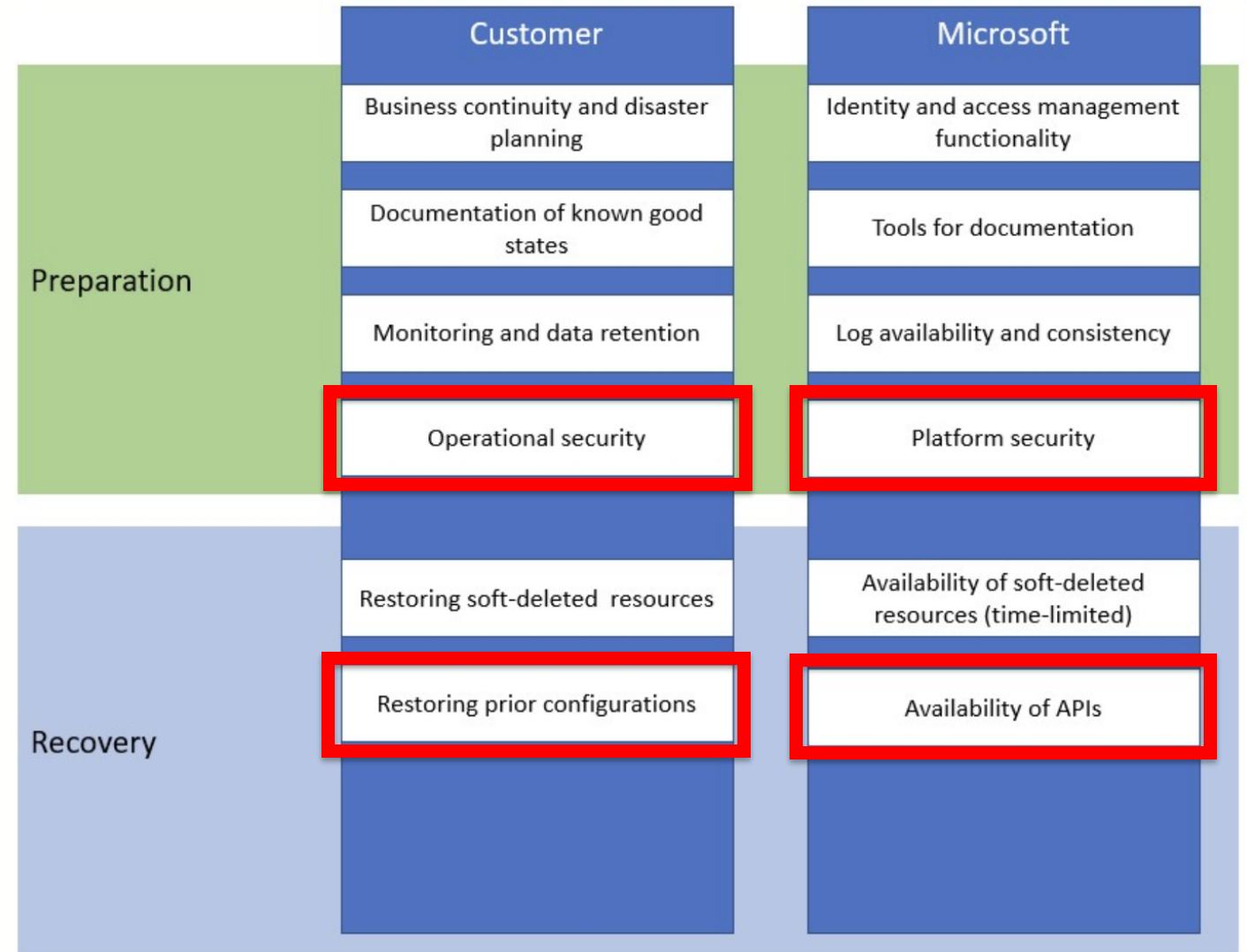
- Was sagt Microsoft zu Backup und Restore in Bezug auf Entra ID?
- „I want you to backup your Entra ID Configuration“ und was ist wichtig dabei?
- Operativ vorausschauen – Restore verhindern
- 💡 **Note:** No commercial tools – just native and open-source.



Vertrauen ist gut, Sicherung ist besser...  
... aber was sagt Microsoft zum Thema Sicherung und Entra ID?

- |   |  |
|---|--|
| ✓ Garantierte Verfügbarkeit des Dienstes            | ✗ Keine Sicherung von Richtlinien, Konfiguration oder Objekten |
| ✓ Authentifizierungsresilienz und Metadaten überall | ✗ Sicherung ist Aufgabe des Admins                             |
| ✓ API-Endpunkte und Doku der Schnittstellen         | ✗ Recoverystrategien in Verantwortung des Kunden               |

# Gemeinsame Verantwortung von Microsoft und Kunde



Quelle: Microsoft [Link](#)

# Konfigurationseinstellungen priorisieren



- „*Was ist wichtig?*“ klären, sonst ist Recovery Konzept schwierig
- Oft reicht gute Dokumentation, manchmal ist Backup die bessere Wahl  
*(... bei einem Tenant mit 50 CA-Policies ist eine Doku nicht wirklich hilfreich)*
- Jedes Unternehmen ist verschieden, jeder Entra ID Tenant ist anders, nicht alles ist immer gleich kritisch  
*(... bei einem Tenant mit Security Defaults spielt eine Sicherung der CA-Policies keine Rolle)*

# Reise durch Richtlinien und Konfigurationen - „Was ist wichtig?“

## Benutzerverwaltung & Einstellungen

- Benutzerrollen & Berechtigungen
- Standard-Anmeldeoptionen für Benutzer
- Benutzer-Lebenszyklusrichtlinien
- Richtlinien für gesperrte Konten
- Anmelde- & Sitzungsrichtlinien für Benutzer
- Richtlinien für sekundäre E-Mail-Adressen
- Benutzeranmeldeprotokolle & Auditing
- Verwaltung von Authentifizierungsmethoden
- Selbstregistrierung für Benutzer

## Authentifizierung & Sicherheit

- Multi-Faktor-Authentifizierung (MFA) Richtlinien
- Passwortlose Authentifizierung (RDO2, Windows Hello)
- Zertifikatsbasierte Authentifizierung
- Token-Laufzeiten & Sitzungskonfiguration
- Continuous Access Evaluation (CAE)
- Risikobasierte Authentifizierung
- Identitätsrisikorichtlinien
- Authentifizierungsstufen für externe Benutzer
- Adaptive Authentifizierungsrichtlinien

## Kennwortrichtlinien & Password Protection

- Kennwortlänge & Komplexitätsanforderungen
- Ablaufzeitraum für Kennwörter
- Banned Password Policy (benutzerdefinierte Sperrliste)
- Smart Lockout Policy (fehlgeschlagene Anmeldeversuche)
- Self-Service Password Reset (SSPR) Richtlinien
- Sicherheitsfragen für SSPR
- Temporäre Access Pass Richtlinien
- Erweiterte Kennwortschutzrichtlinien für lokale Ads

## Global Secure Access (GSA)

- Zugriffsrichtlinien
- Netzwerkverbindungen
- Gerätekonfiguration

## Global Secure Access (GSA)

- Zuweisung
- Zero Trust Network Access
- Web Content Filtering
- DNS-Sicherheitsrichtlinien
- Logging & Monitoring für Netzwerkzugriffe

## Gruppenverwaltung

- Dynamische Gruppenrichtlinien
- Gruppenbasierte Lizenzzuweisung
- Selbstbedienungs-Gruppenmanagement Richtlinien
- Automatische Gruppenzuordnung durch Attribute

## Gastbenutzer & Externe Zusammenarbeit (B2B/B2C)

- Einladungseinstellungen für Gäste
- Externe Identitätsanbieter (Google, Facebook, SAML, OpenID)
- B2B-Kollaborationsrichtlinien
- Richtlinien für Gastbenutzer-Berechtigungen
- Externe Benutzerlöschung automatisieren
- Sitzungsrichtlinien für Gastbenutzer

## Entra Cloud Sync & Synchronisations-einstellungen

- B2B-Kollaborationsrichtlinien
- On-Premises-Verzeichnissynchronisation (Connect)
- Custom Synchronization Rules

## Conditional Access & Zugriffskontrolle

- Richtlinien für Benutzer & Gruppen
- Gerätestatus- & Compliance
- Sitzungsrichtlinien
- Adaptive Richtlinien
- Zugriffsrichtlinien (Cross-Tenant Access)
- Zugriffsrichtlinien für externe Identitäten

## Sicherheits- & Überwachungsrichtlinien

- Sicherheitswarnungen & Identity Protection
- Identitätsschutz- & Risikoerkennungseinstellungen
- Audit-Protokollierung für Identitätsaktivitäten
- Anomalie-Erkennung für Anmeldeversuche
- Sicherheitsbewertungen & Empfehlungen

## Rollen & Berechtigungen (RBAC & PIM)

- Benutzerdefinierte Rollen & Berechtigungen
- Least Privilege Access Richtlinien
- Zeitlich begrenzte Rollenzuweisungen (Just-In-Time)
- Genehmigungs-Workflows für Admin-Rollen
- Audit-Logs für privilegierte Rollen
- Sicherheitsüberprüfung für hochprivilegierte Konten

## Identitäts-Governance & Compliance

- Rollen- & Berechtigungsüberprüfungen
- Audit-Protokollierung für Identitätsaktivitäten
- Automatische Identitätsüberprüfungen
- Entitlementsmanagement
- Zugriffskontroll-Workflows

## Geräteverwaltung & Microsoft Entra Cloud

- Geräte in Entra ID registrieren (Hybrid Azure AD Join, Azure AD Join)
- Geräteerkennung und Compliance
- Geräteverwaltung für Windows, macOS, iOS und Android
- Geräte in Entra ID aktivieren/deaktivieren
- Geräte-Lebenszyklusverwaltung
- Entra ID Cloud Sync einrichten und konfigurieren
- Synchronisationsfilter für Gruppen und Benutzer definieren
- SCIM-Synchronisation mit Drittanbieterdiensten
- On-Premises-Verzeichnissynchronisation verwalten (Azure AD Connect, Cloud Sync)

## Anwendungsverwaltung & Zugriffskontrollen

- Unternehmensanwendungen hinzufügen/löschen
- Single Sign-On (SSO) für Anwendungen aktivieren
- App-Proxy für Legacy-Anwendungen konfigurieren
- OAuth- und OpenID-Connect-Richtlinien festlegen
- Drittanbieter-Identitätsanbieter konfigurieren
- Token-Laufzeiten für Anwendungen verwalten
- Richtlinien für bedingten Zugriff auf Anwendungen definieren
- Benutzer- und Gruppenberechtigungen für Apps konfigurieren
- Managed Identity für Dienste einrichten

## Administrative Units (AUs)

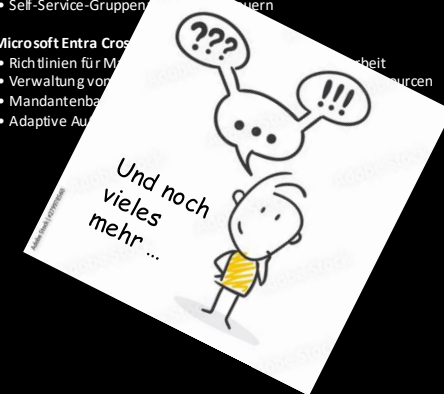
- Administrative Units (AUs)
- Administrative Units (AUs)

## Administrative Units (AUs)

- Mandantenname und Domänen verwalten
- Unternehmensbranding konfigurieren
- Datenschutzrichtlinien für Identitäten festlegen
- Restriktionen für mehrinstanzfähige Organisationen
- Microsoft Entra ID Governance aktivieren
- Adaptive Application Controls verwalten
- Conditional Access für Identitäten-Richtlinien
- Self-Service-Gruppenverwaltung

## Microsoft Entra Cross

- Richtlinien für Multi-Faktor-Authentifizierung
- Verwaltung von Identitätsressourcen
- Mandantenverwaltung
- Adaptive Authentifizierung



# Löschen von Objekten und Ressourcen



Objekttyp	Softdelete	Recovery
Benutzerobjekt	✓	Papierkorb (Soft deleted = recovery, auch hybrid (sync) ; hard deleted neues Objekt)
Computerobjekte	✗	Neuregistrierung – „dsregcmd.exe“ is your friend
Sicherheitsgruppe	✗	Keine Wiederherstellung 😬
M365 Gruppe	✓	Papierkorb
App Registration	✓	Papierkorb (Secret und Zertifikate ✓) Evtl. zugehörige EA wird auch gelöscht und wird mit wiederhergestellt.
Enterprise Application (EA)	✓	Deleted Item API (Multitenant ✓) Zugehörige App Reg wird mit gelöscht; Wiederherstellung <b>über App Reg Papierkorb</b> nicht über Deleted Item API
Administrative Unit	✓	Kein Papierkorb, Wiederherstellung über „Deleted Item API“
Conditional Access Policy	✗	Keine Wiederherstellung 😬



# Recover Applications via deletedItems 1/2



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 - 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",
    }
  ]
}
```

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

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

## Recover Applications via deletedItems 2/2

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",
```



Berechtigungen?  
-> [Link](#)

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



# How to Backup?

→ Manuell schwierig, bis nicht möglich

*Code Varianten besser ...*

→ Powershell is your friend

*Stellenweise Gefruckel ... JSON muss passen, leere Objekte, NULL Objekte etc.*

→ EntraExporter is the better friend



[Open-Source Github](#)

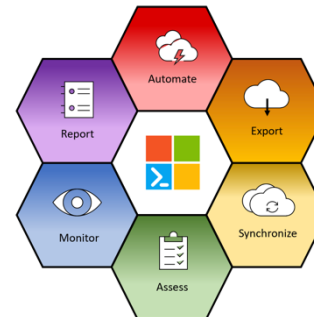
→ M365DSC is another good friend



[Open-Source Github](#)



Demo ...



# How to Backup?

→ Manuell

*Code Variants*

→ Powershell

*Stellenweise Ge*

→ EntraExp



Open-

→ M365DSC is another good friend 🤓



Open-Source Github

```
$AllPolicies = Get-MgIdentityConditionalAccessPolicy -All

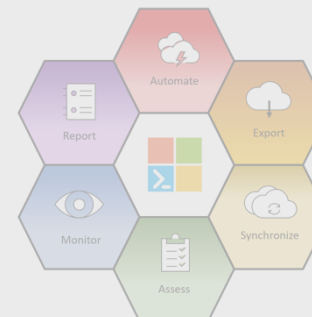
foreach ($Policy in $AllPolicies) {
    # Get the display name of the policy
    $PolicyName = $Policy.DisplayName

    # 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
```



Damit es nicht zum restore kommt...  
*„Smart operations protect against human error“*

- ✓ Gruppen schützen mit „Protected Groups“
- ✓ AU – Restricted Management (Public Preview...)
- ✓ Protected Actions for hard deletions (GA seit Januar 2025)
- ✓ Alarmierung für wichtige Ressourcen (Demo Folien im Anhang)



Demo

Authentication Context in CA konfigurieren

... > Roles and administrators | Protected actions > Add protected actions > Conditional Access

**Conditional Access** | Authentication contexts

Microsoft Entra ID

Overview  
Policies  
Insights and reporting  
Diagnose and solve problems  
Manage  
Named locations  
Custom controls (Preview)  
Terms of use  
VPN connectivity  
**Authentication contexts**  
Authentication strengths  
Classic policies

Get started **Authentication contexts**

Manage authentication context to protect data and actions in your apps. Authentication contexts cannot be deleted when they are referenced by Conditional Access policies. [Learn more](#)

Name	Description
<a href="#">ProtectDeletedItems</a>	
<a href="#">ProtectCAWrites</a>	

1

Eben erstelltes Label (Authentication Context) einer „Protected Action“ zuordnen

... > Add protected actions > Conditional Access | Authentication contexts > Roles and administrators

**Roles and administrators** | Protected actions

Identity LAB

All roles  
**Protected actions**  
Diagnose and solve problems

Protected actions are role permissions with Conditional Access applied for added security. Conditional Access requirements are enforced when a user performs the protected action. [Learn more](#)

Search by name or description

4 actions found

Permission	Description
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/basic/update	Update basic properties
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/create	Create Conditional Access policies
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/delete	Delete Conditional Access policies
<input type="checkbox"/> <b>microsoft.directory/deletedItems/delete</b>	Permanently delete objects

2



## CA132-AdeleV-ProtectedAction-DeletedItems

Conditional Access policy

Delete View policy information View policy impact (Preview)

### Assignments

#### Users

Specific users included and specific users excluded

#### Target resources

1 authentication context included

#### Network

Not configured

#### Conditions

0 conditions selected

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security.

[Learn more](#)

Select the authentication contexts this policy will apply to

☒ ProtectDeletedItems

☐ ProtectCAWrites

Entscheidung  
in CA-Policy

Microsoft Entra Admin Cent...

Nach Ressourcen, Diensten und Dokumenten suchen (G+)

Copilot

AdeleV@kbcorp2021.on...  
IDENTITY LAB (KBCORP2021.ON...

Home > Benutzer | Gelöschte Benutzer > Rollen und Administratoren | Alle Rollen > Adele Vance (Helpdesk) | Zugewiesene

## Benutzer | Gelöschte Benutzer

Identity LAB

Alle Benutzer

Überwachungsprotokolle

Anmeldeprotokolle

Diagnose und  
Problembehandlung

Gelöschte Benutzer

Kennwortzurücksetzung

Benutzereinstellungen

Ergebnisse von Massenvorgängen

Massenwiederherstellung Endgültig löschen Benutzer wiederherstellen

Azure Active Directory ist jetzt Microsoft Entra ID

Benutzer werden 30 Tage nach dem Löschvorgang automatisch dauerhaft gelöscht.

Suchen

Filter hinzufügen

3 Benutzer gefunden

<input type="checkbox"/>	Anzeigenname ↕	Benutzerprinzipalname ↕	Benutzertyp	Datum/Zeit der Löschung ↓	Datum/Zeit
<input type="checkbox"/>	Dominga Soneson	c641a46b79eb4c748d2bf...	Mitglied	10. Apr. 2025, 13:04	10. Mai 2025
<input type="checkbox"/>	Erika Musterfrau	1689cccd3db64271b8e4f...	Mitglied	8. Apr. 2025, 08:59	8. Mai 2025
<input type="checkbox"/>	Max Mustermann	d5ba8e4856e14213a8bd2...	Mitglied	8. Apr. 2025, 08:55	8. Mai 2025

**Fehler beim endgültigen Löschen des Benutzers**

Ungenügende Berechtigungen zum endgültigen Löschen der ausgewählten Benutzer.

[Hilfe bei der Problembehandlung](#)



## Zusammenfassung - Was haben wir gelernt?

→ „known good“ dokumentieren, sichern,  
... pflege ops guide regelmäßige Prozesse



→ Backup Strategie regelmäßig und geplant hinterfragen



→ Schutzmaßnahmen gegen Verlust von Konfiguration  
*Wer darf was? „Proaktiv statt reaktiv“ spart Nerven und Zeit.*

## Weiterführende Informationen:



[MS Learn: Recover from deletions](#)



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



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



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



[Zero Trust in Azure Identity - Part 5: Simple Monitoring Break Glass Accounts](#)



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



[Fortigi - Conditional Access Module](#)





Vielen Dank an unsere Sponsoren!

---

Diamond



---

Platinum



---

Gold





# Bitte gebt uns euer Feedback!

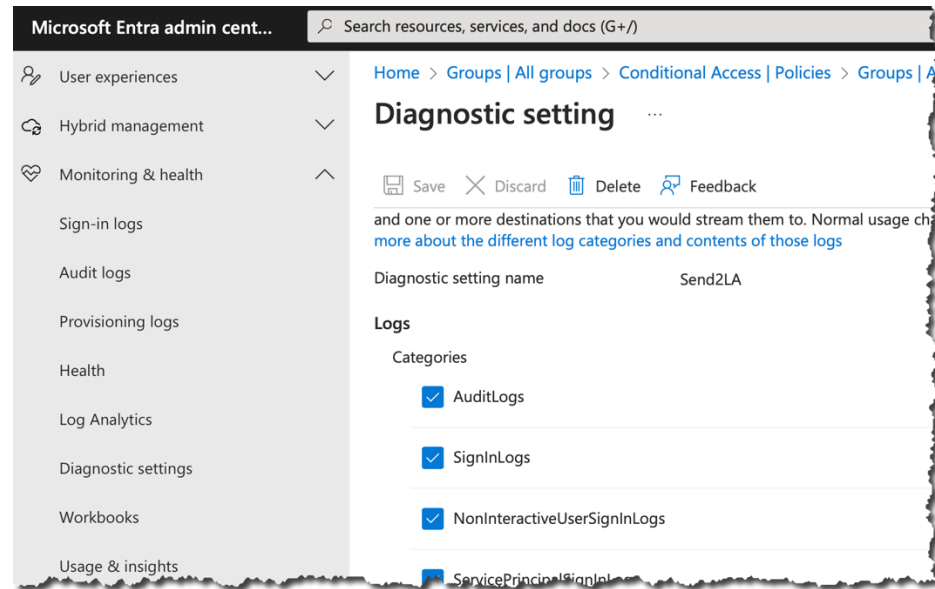
## Feedback geben und Geschenk mitnehmen





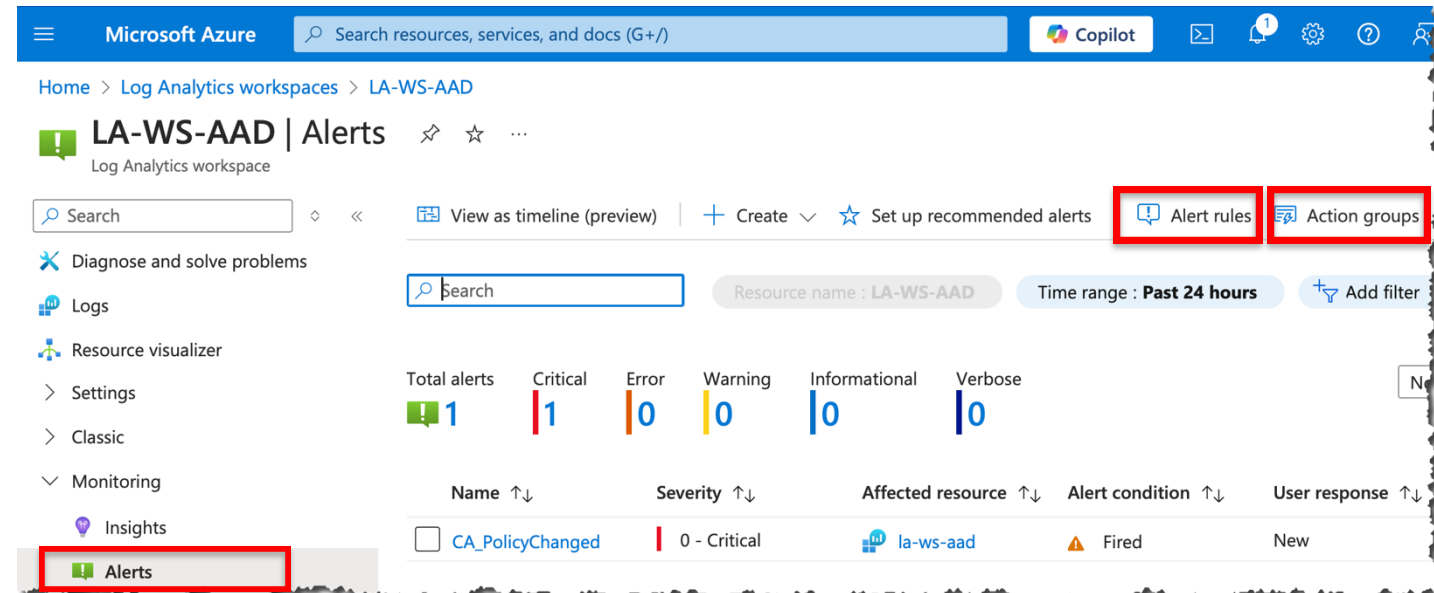
Backup slides!

Konfiguriere Diagnostic Settings in Entra ID



Sende Logs zum  
Repository

Konfiguriere Reaktionen in Azure Portal



Action groups /  
Alert rules

Konfiguriere Diagnostic Settings in Entra ID

Konfiguriere Reaktionen in Azure Portal

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
```

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

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

Sende Logs zum  
Repository



Gartner prognostiziert, dass bis 2025 über 99% der Cloud-Sicherheitsverletzungen auf vermeidbare Fehlkonfigurationen oder Fehler von Endbenutzern zurückzuführen sein werden.

<https://venturebeat.com/business/takeaways-fromgartners-2021-hype-cycle-for-cloud-security-report>





# Microsoft365DSC

- Export, Backup, Vergleich von Einstellungen schwierig
- M365DSC: Sichern, Vergleichen, Automatisieren und mehr ...
- Powershell- und DSC-Kenntnisse sind hilfreich
- Community Lösung mit gutem Support (Github)
- Keine reine Backup / Restore Lösung
- PS-Modul mit ca. 60 Cmdlets

