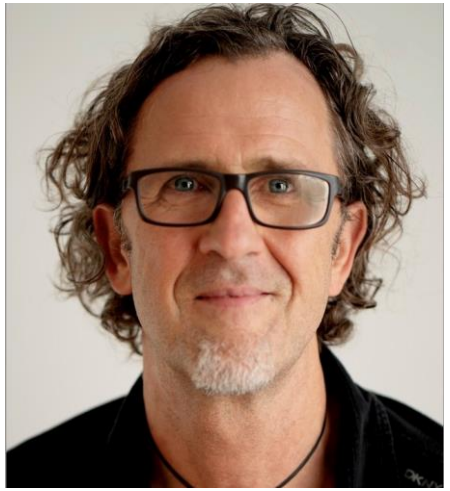
Zero Trust Identity – Administrative Aufgaben schützen

Über mich:



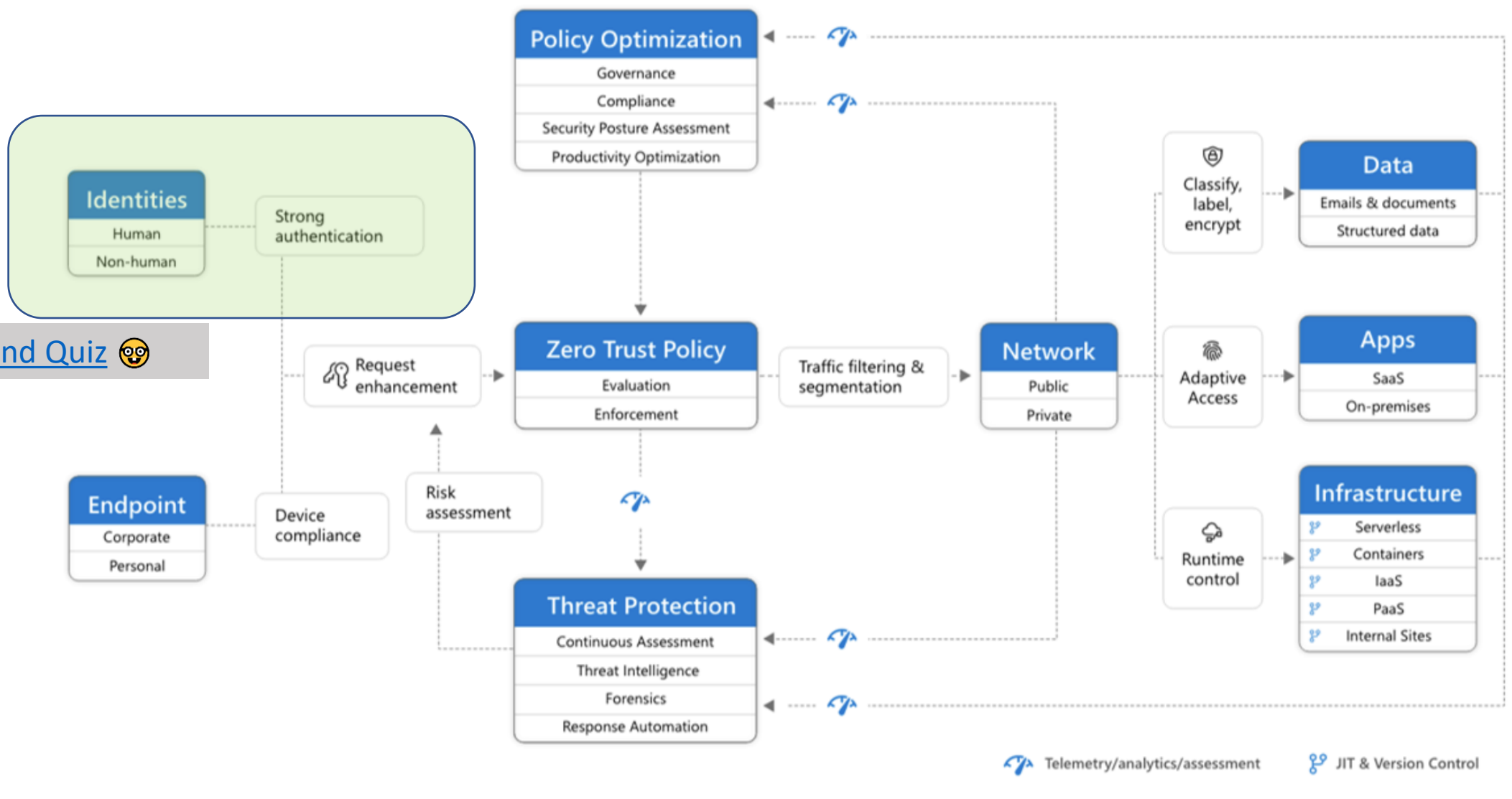
- ➔ Zuhause bin ich in Murnau am Staffelsee (45min südlich von München)
- ➔ Director Consulting Expert bei CGI Deutschland
- ➔ Weitere Stationen: T-Systems International, Wipro
- ➔ Schwerpunkte: Active Directory, Identity im hybriden Kontext, Synchronisation und Zero Trust Identity
- ➔ Wenn es meine Zeit erlaubt publiziere ich Beträge in meinem Blog, in der Fachpresse und in der heise academy

LinkedIn

Blog:
https://nothingbutcloud.net/

Zero Trust Identity – Administrative Aufgaben schützen

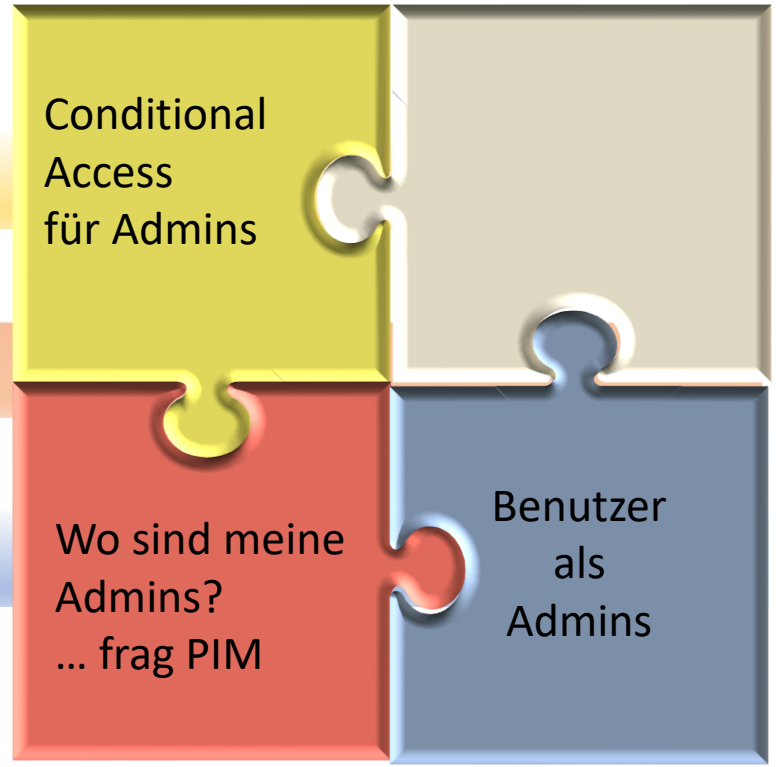
[Mehr Infos und Quiz](#) 🤓



Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

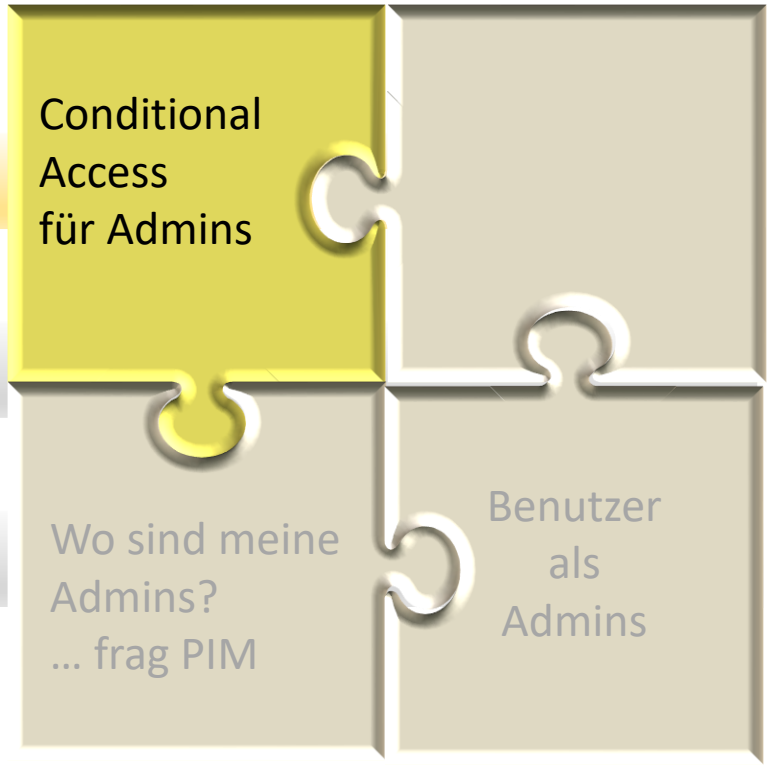
- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken



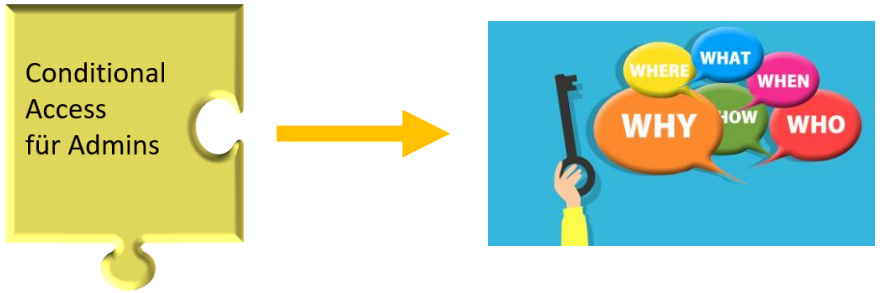
Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken

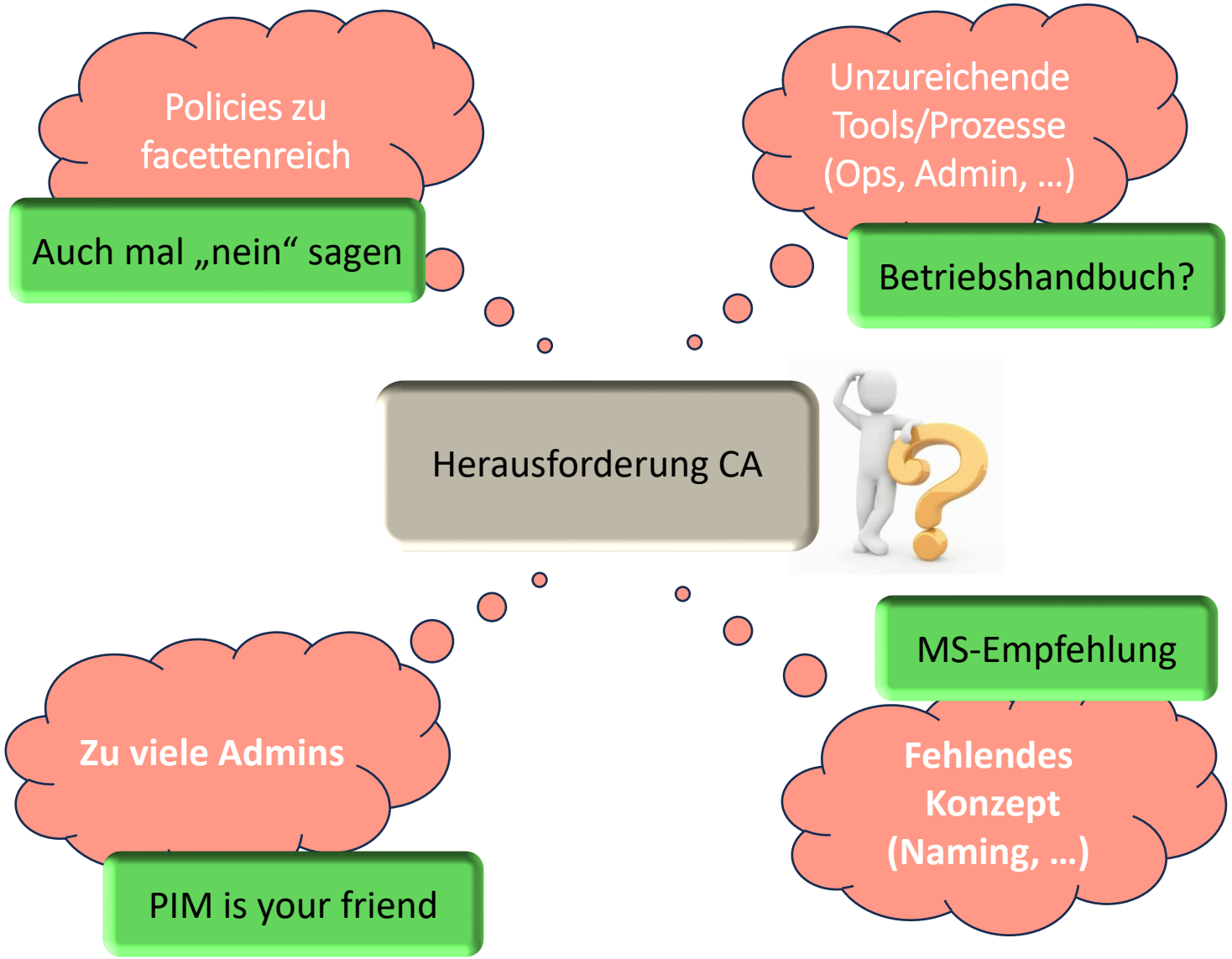


Zero Trust Identity – Administrative Aufgaben schützen



Strategien

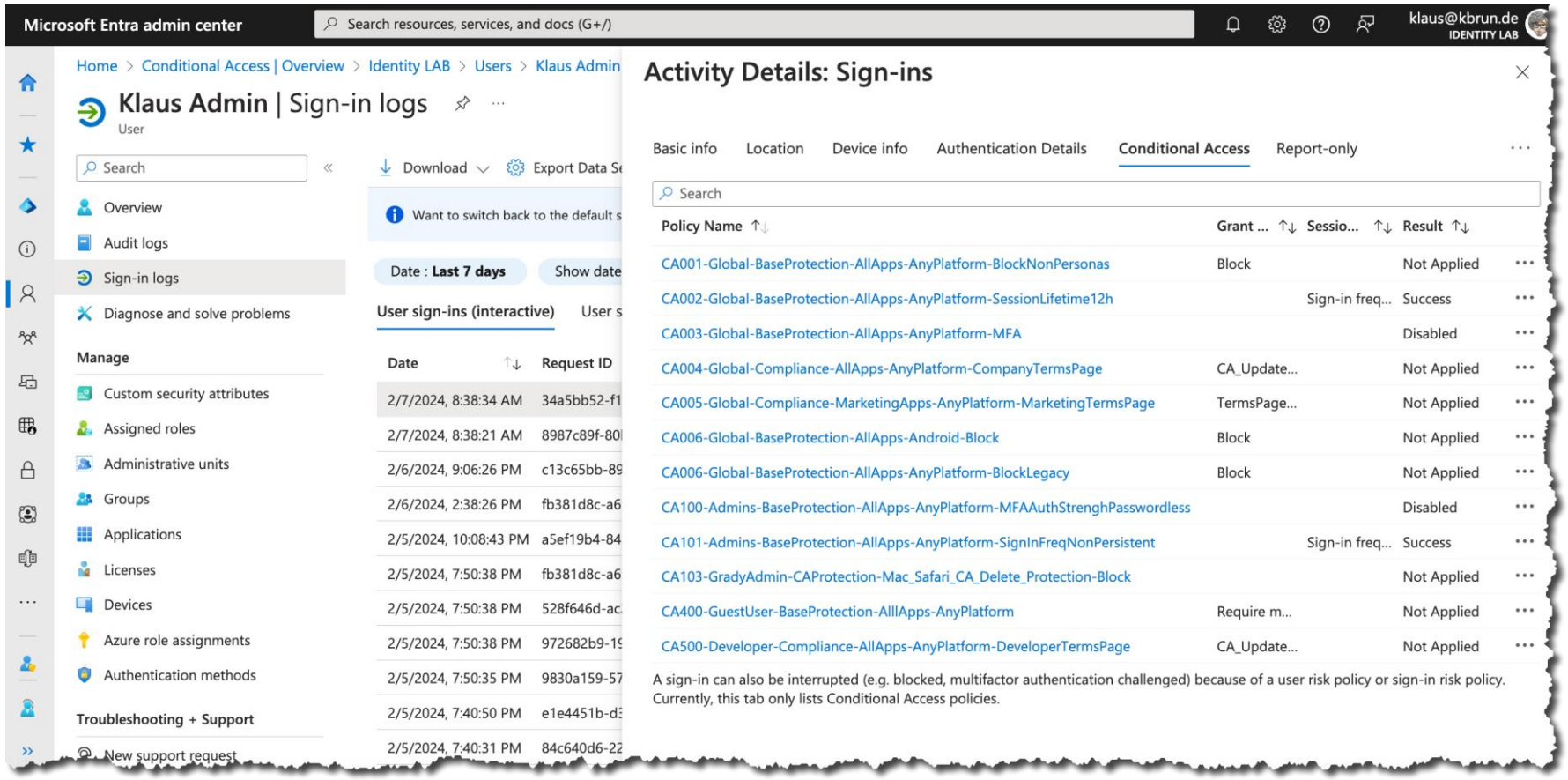
- „Keep it simple“
- Tools: Backup, Vergleich etc.
  z.B. M365DSC, AADInternals
- PIM: Just-in-**time** (JIT)
  just-**enough**-access (JEA)
- Agieren statt reagieren



Zero Trust Identity – Administrative Aufgaben schützen

Conditional Access für Admins

Empfehlung: Gutes „Naming“ ✓



Must read:

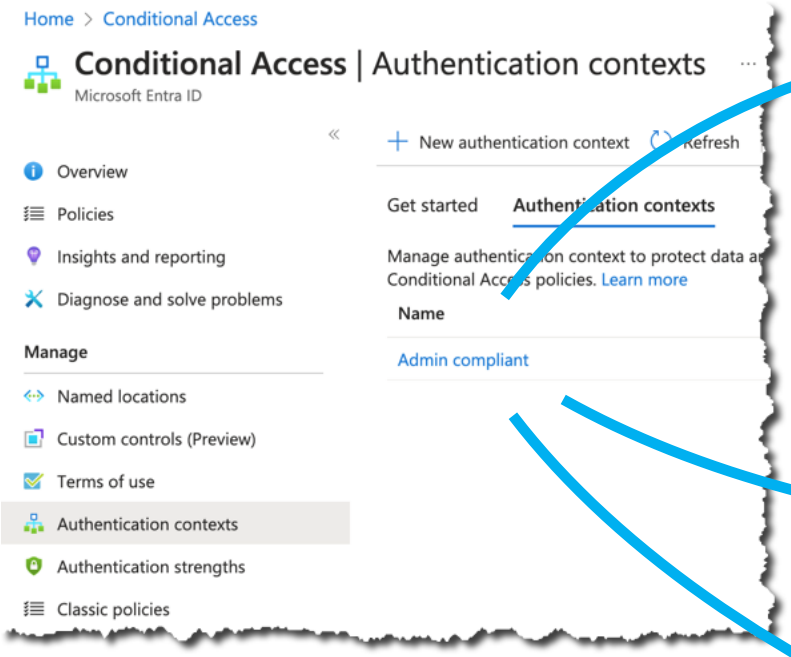
Conditional Access framework and policies - Azure Architecture Center | Microsoft Learn

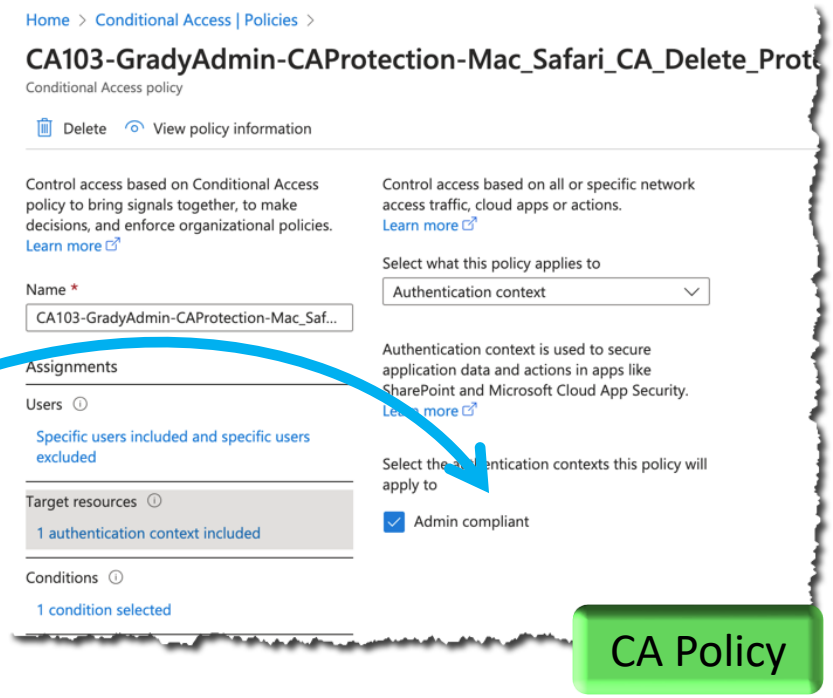
Zero Trust Identity – Administrative Aufgaben schützen

Conditional Access für Admins

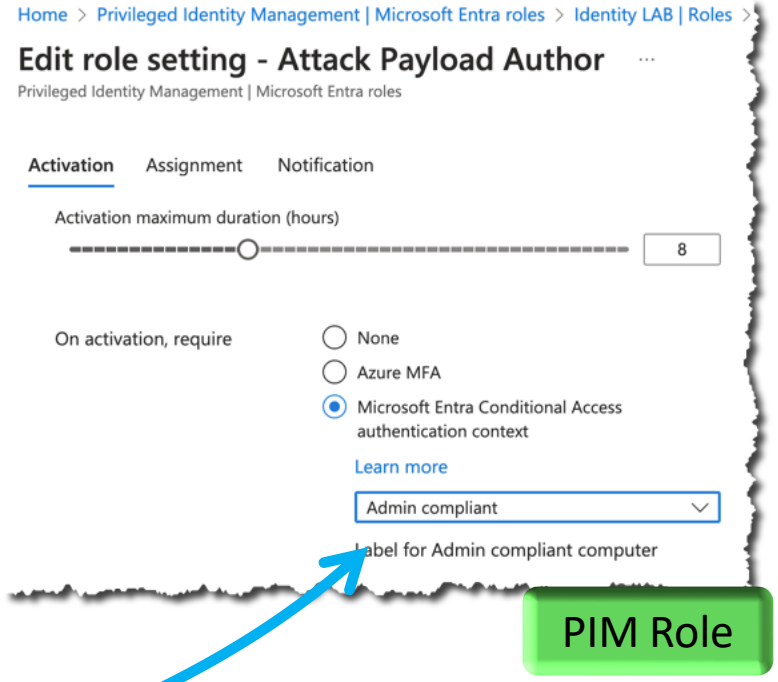
Empfehlung:

Protected Actions ✓

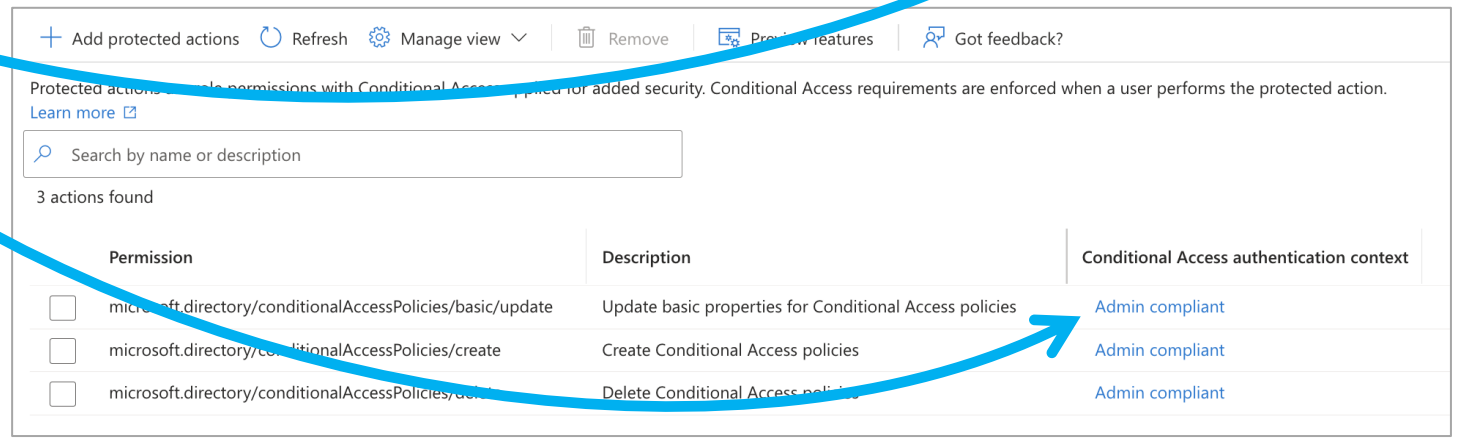




CA Policy



PIM Role



Zero Trust Identity – Administrative Aufgaben schützen

Demo:
Conditional Access Policies for Admins

Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken

Zero Trust Identity – Administrative Aufgaben schützen

Wo sind meine Admins?
… frag PIM

Strategien

PIM - kurz und bündig

- Workflows für Rollen-aktivierung
- Konfig für jede Rolle
- MFA oder Protected Action je Rolle
- Aktivieren über PIM-Dashboard PS / Graph
- P2 für alle User die an PIM teilnehmen
- Integration in Access Reviews
- Umfassende Notification bei Rollen-aktivitäten
- Konfig für Entra Rollen, Gruppen und IaaS
- Analyse kritischer Rollen

Verschiedene Konfig für eine Rolle

PIM for Groups

Analyse / Überblick?

Insights / Alerts

Herausforderung PIM

Aktivieren mehrerer Rollen?

PIM for Groups

Zero Trust Identity – Administrative Aufgaben schützen

Wo sind meine Admins?
… frag PIM

Demo:
PIM for Groups

Zero Trust Identity – Administrative Aufgaben schützen

Agenda:

- Conditional Access Policies und administrative Aspekte
- Was bietet PIM für Kontrolle und Sichtbarkeit von Admins
- Operative Tätigkeiten für „normale“ Benutzer ohne Risiken

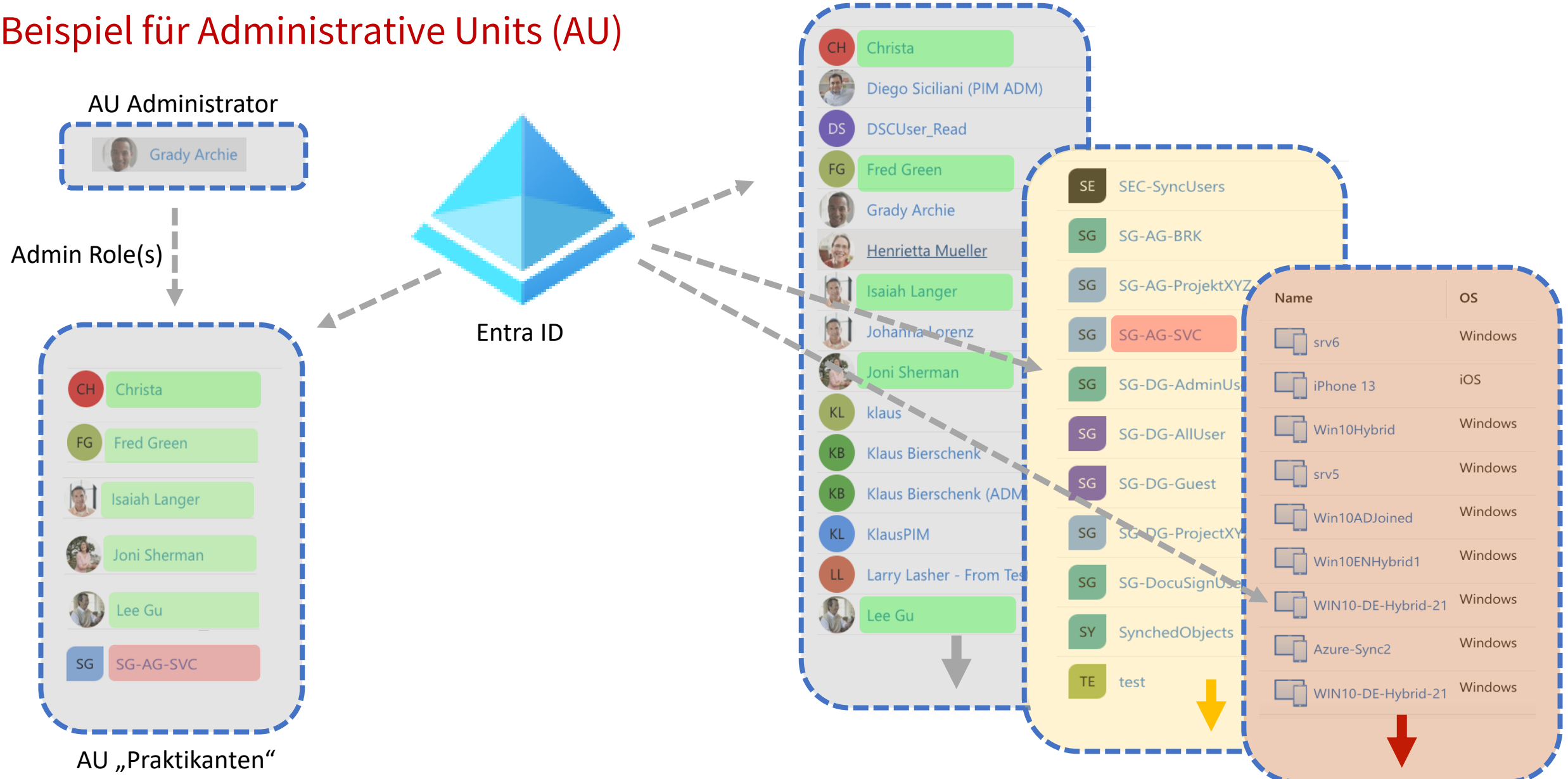
Zero Trust Identity – Administrative Aufgaben schützen

Das Wichtigste rund um „Administrative Units“

- Management auf bestimmte Objekte reduzieren
- Administrativer Kontext für Benutzer, Gruppen und Geräte
- Keine hierarchische Struktur oder Verschachtelung. Keine Vererbung
- PowerShell, Graph API, Entra Admin Center, MyStaff und M365 Admin Portal
- MyStaff bietet „einfache“ administrative Möglichkeiten (PW Reset)
- Objekte können mehreren „Administrative Units“ zugeordnet sein
- Nicht verwechseln mit Organizational Units (OUs) aus den AD Domain Services

Zero Trust Identity – Administrative Aufgaben schützen

Beispiel für Administrative Units (AU)



Zero Trust Identity – Administrative Aufgaben schützen

Demo:
Administrative Units

Zero Trust Identity – Administrative Aufgaben schützen

Die drei wichtigsten Vorteile und Herausforderungen zu „Administrative Units“

Vorteile:

- Administrative Möglichkeit für Benutzer ohne Zugriff auf das Entra Admin Center
- Implementierung ohne viel Aufwand. Gut geeignet für kurzfristigen Zweck (Projekt)
- Management für bestimmte Benutzer (keine Admins) ermöglichen. Einfaches Toolset

Herausforderungen:

- Mehrere AUs werden schnell unübersichtlich. Wer darf was und wo ist schnell unklar
- Nur einige wenige Rollen sind verfügbar. Und nicht alles ist möglich (siehe Link)
- Keine Schachtelung möglich, um Hierarchien aufzubauen

Zero Trust Identity – Administrative Aufgaben schützen

Grundlagen

- Zero Trust Model - Modern Security Architecture | Microsoft Security
- Was ist der bedingte Zugriff in Microsoft Entra ID?
- Was ist Microsoft Entra Privileged Identity Management?
- Administrative UnitVerwaltungseinheiten in Microsoft Entra IDs
- Emergency Access (BGA Accounts)
- Dynamic Group Membership
- MFA - how it works

Weiterführende Informationen

- Framework und Richtlinien für bedingten Zugriff - Azure Architecture Center | Microsoft Learn
- Privileged Identity Management (PIM) für Gruppen
- NothingButCloud: BGA Alerting

Tools

- What is Microsoft365DSC?
- Entra Exporter Tool - Effortlessly Backup Microsoft Entra ID Configurations (o365reports.com)

secIT by heise

HANNOVER 2024

Zero Trust Identity – Administrative Aufgaben schützen

Backup

Zero Trust Identity – Administrative Aufgaben schützen

Empfehlung:

Tools ✓

Microsoft365DSC

- Export, Backup, Vergleich von Einstellungen schwierig
- M365SDC: 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

Zero Trust Identity – Administrative Aufgaben schützen

Conditional Access für Admins

Empfehlung:

Authentication strength ✓