ENDLICH KONTROLLE ÜBER IHRE KOMPLEXEN MICROSOFT-BERECHTIGUNGEN

Berechtigungen im AD, NTFS Filesystem, Exchange, Sharepoint, Entra ID & Co. übersichtlich darstellen und Missstände automatisiert erkennen

René Leitz, Product Manager daccord

daccord

Vorbemerkungen

Wer kennt es nicht, dieses sorgenvolle Gefühl, wenn es um Berechtigungsvergaben im Active Directory und um Zugriffsrechte auf Dateiservern geht?

Je größer die Umgebung wird, desto unübersichtlicher kann es schnell werden.

Wie schnell könnten beispielsweise unerlaubte Zugriffe über verwaiste Konten zu schwerwiegenden Folgen führen? Hier den Überblick zu behalten und wirklich sicher zu sein, ist mit Bordmitteln oftmals eine große Herausforderung.

ZUM ERKLÄRVIDEO

daccord

Berechtigungen in Microsoft-Umgebungen

- Ein Frontend zur Analyse aller Microsoft Berechtigungen
- Durch „Integrationspakete“ wie z.B. Active Directory, MS Fileserver, Entra ID, Exchange erweiterbar
- Sofortige Erkennung von Missständen durch mitgelieferte „Richtlinien“
- Historische Speicherung aller Veränderungen
- Spezielle „Effektive-Rechte-Sichtweisen“ zur Beantwortung der Frage: Was darf Max Mustermann?

daccord

Was sind Richtlinien?

- Vorgefertigte Analysen Ihrer Daten wie z.B.
  - gibt es im Active Directory mit sich selbst verschachtelte Gruppen
  - gibt es ausgeschiedene Mitarbeiter mit noch aktiven Benutzerkonten
- Schwachstellen werden direkt nach der Installation angezeigt
- Beurteilung der Daten auf Basis von Schwellenwerten und Einstufung des Missstandes in verschiedene Risikolevel
- Zeitgesteuerte Ausführung um einen historischen Verlauf abzubilden (Verbesserung oder Verschlechterung)
- Individuelle Richtlinien nach Kundenanforderung möglich

daccord

Anwendungsfälle

Anwendungsfall 1:
Was darf Peter Walk?

Anwendungsfall 2:
Richtlinienverstoß im MS Fileserver

Anwendungsfall 3:
Gibt es fehlerhafte Gruppenverschachtelungen (Loops) im Active Directory?

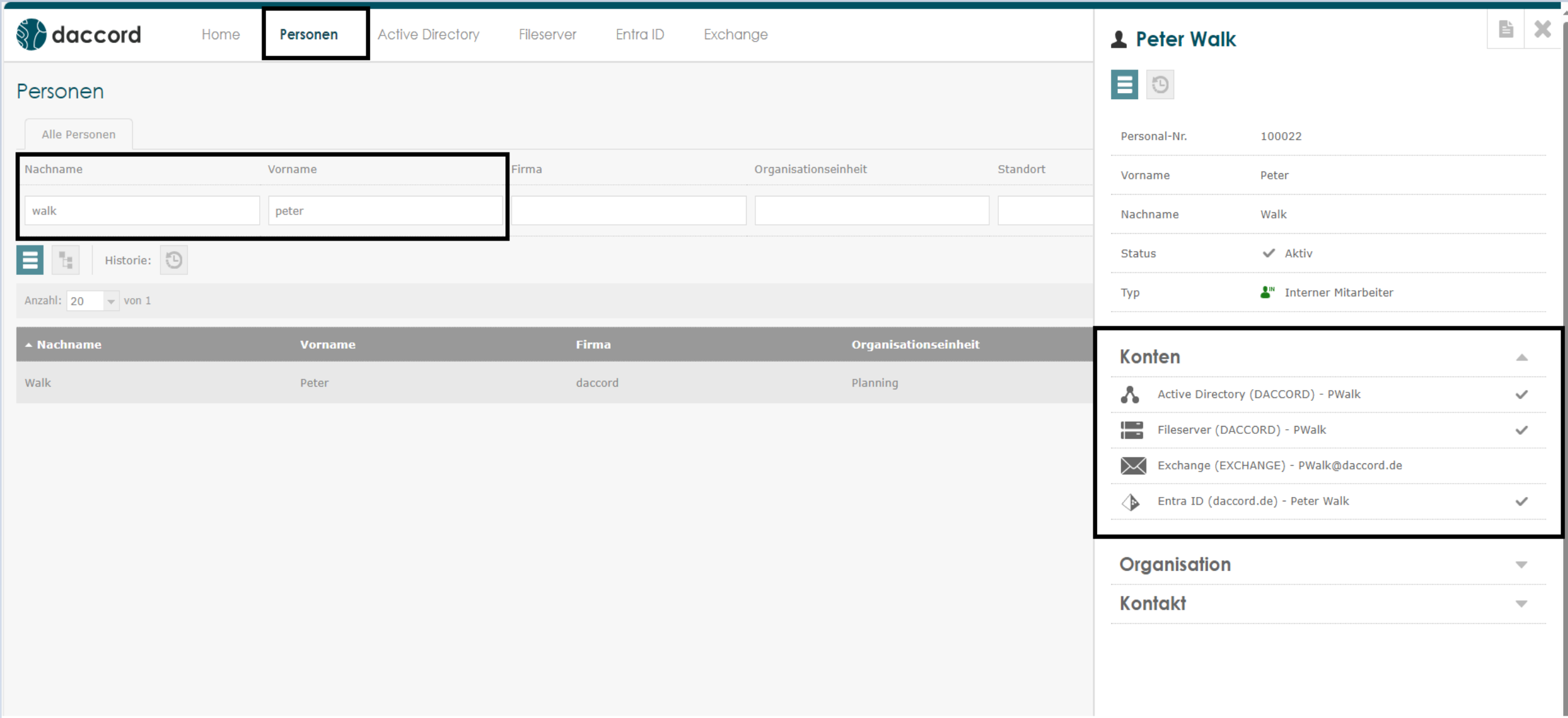
Anwendungsfall 4:
Gab es Änderungen in der Domain Admin-Gruppe im Active Directory?

daccord

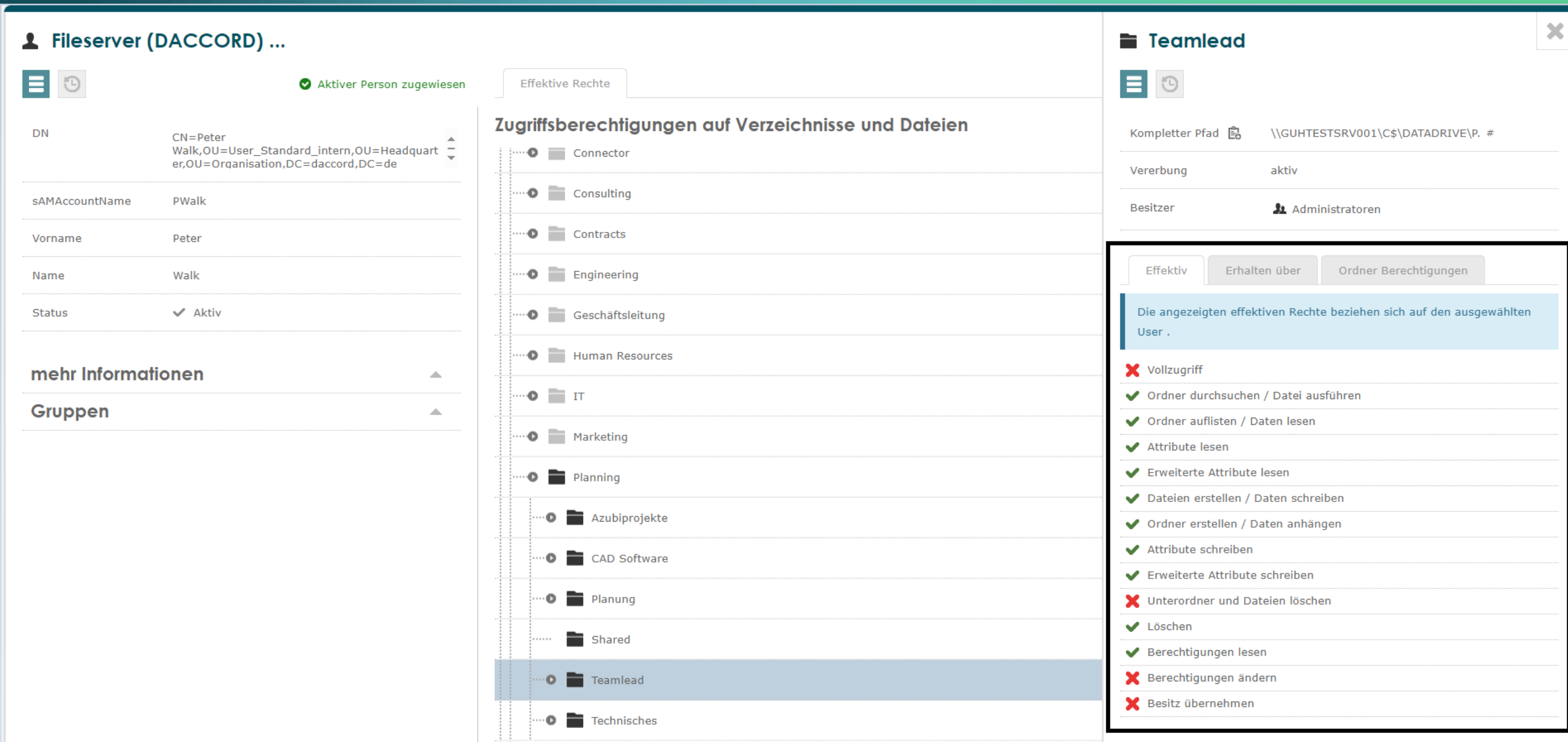
ANWENDUNGSFALL 1:

WAS DARF PETER WALK?

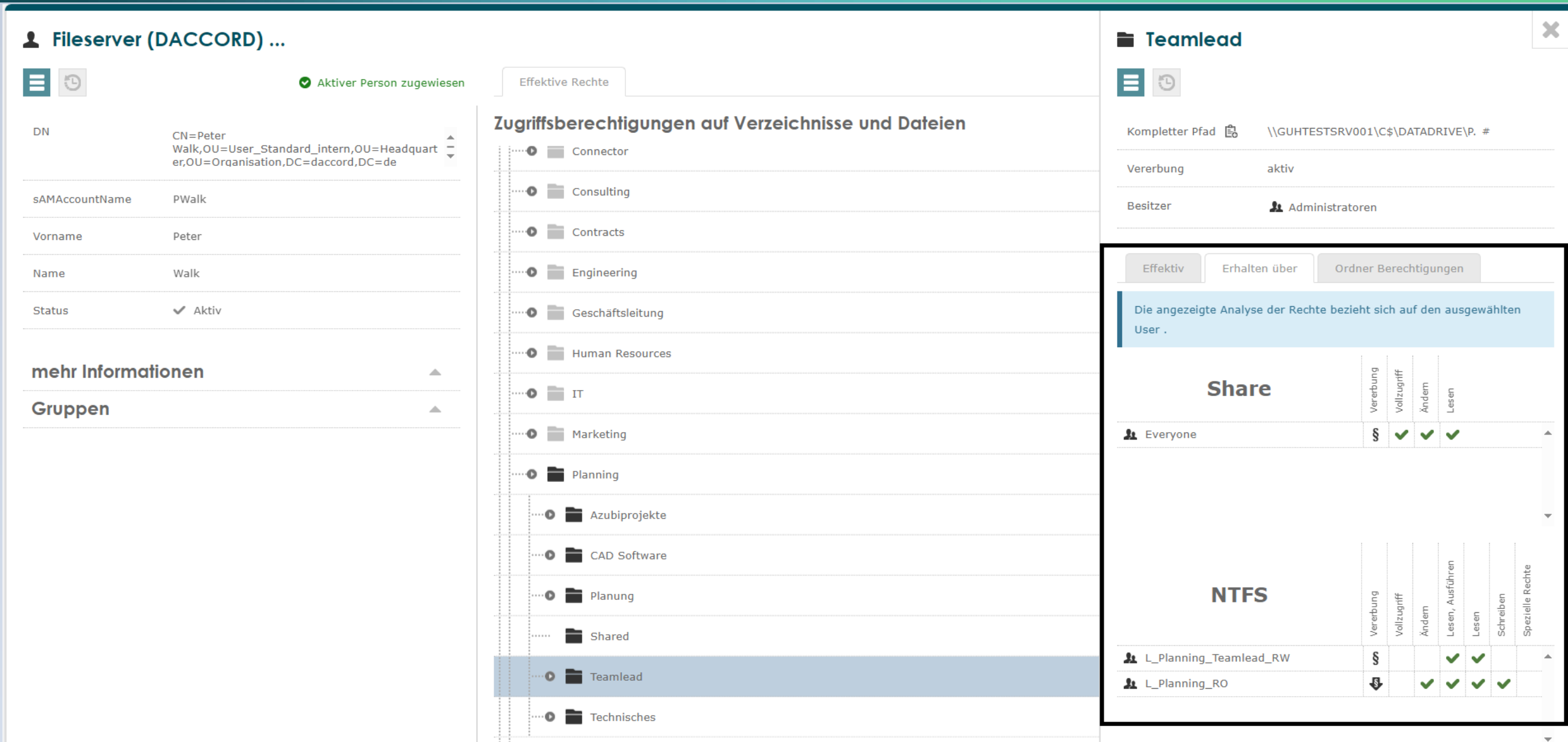
Anzeige aller Benutzerkonten einer Person



MS Fileserver Berechtigungen



MS Fileserver Berechtigungen



MS Exchange Berechtigungen

Exchange (EXCHANGE) -...

Aktiver Person zugewiesen

Mailbox ID	PWalk@daccord.de
sAMAccountName	PWalk
Name	PWalk@daccord.de
Anzeigename	Peter Walk
Besitzer	PWalk
Exchange System	EXCHANGE
Kategorie	UserMailbox
Datenbank	DB1

E-Mail Adressen

Weitere Attribute

Berechtigungen

Berechtigungen auf diese Mailbox

	Vollzugriff	Ändern	Berechtigungen lesen	Senden als	Senden im Auftrag von	Sonst. Berechtigungen
CJuanez	✓				✓	
CRocker	✓				✓	
PWalk	✓		✓			

Mailbox Berechtigungen

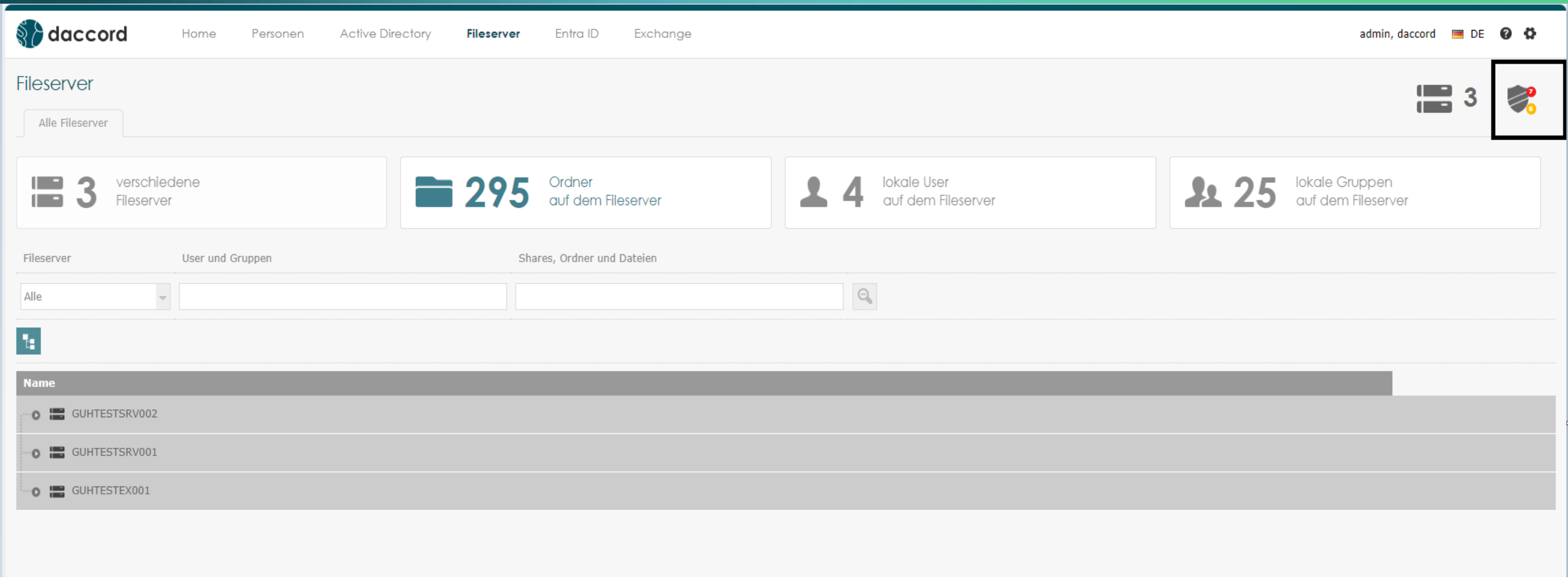
Zugriffsberechtigungen auf Mailboxen

	Vollzugriff	Besitzer ändern	Berechtigungen ändern	Berechtigungen lesen	Senden als	Senden im Auftrag von	Sonst. Berechtigungen
PWalk@daccord.de	✓			✓			
PKinzinger@daccord.de	✓					✓	
Planung@daccord.de	✓				✓		
AYariz@daccord.de					✓		
hgverkn@daccord.de	✓						

ANWENDUNGSFALL 2:

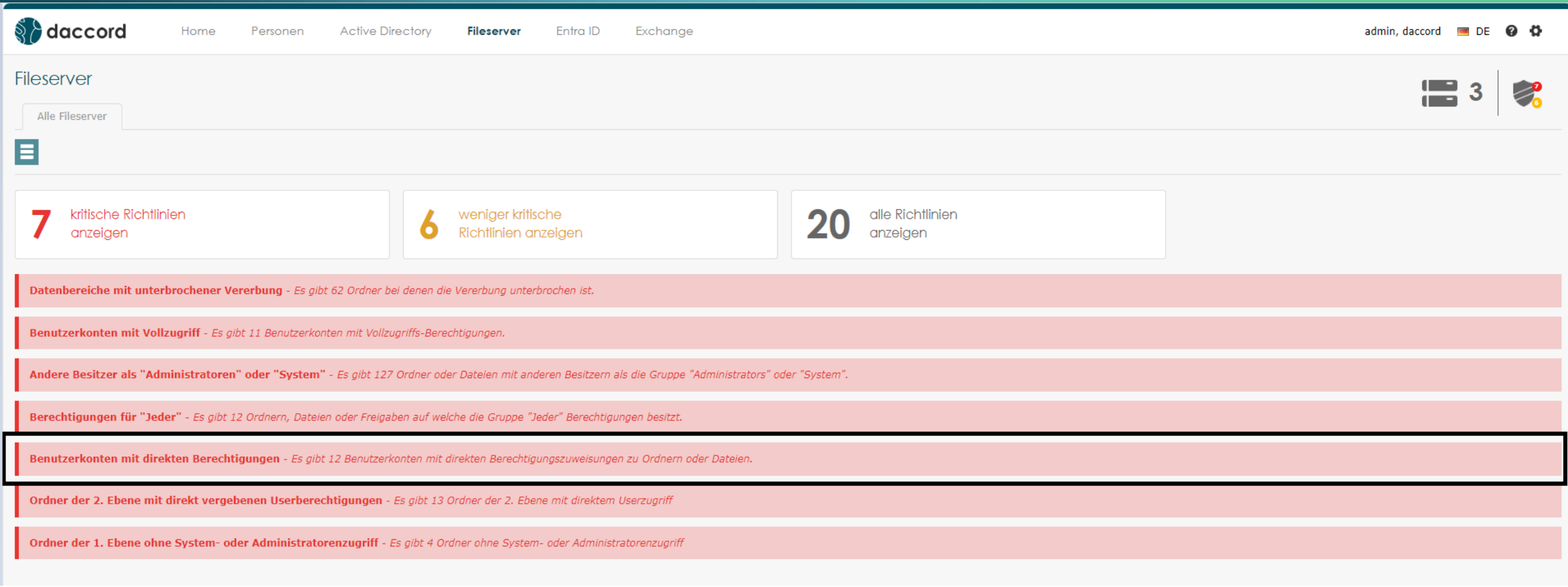
RICHTLINIENVERSTOSS IM MS FILESERVER

MS Fileserver: Hinweis zum Richtlinienverstoß



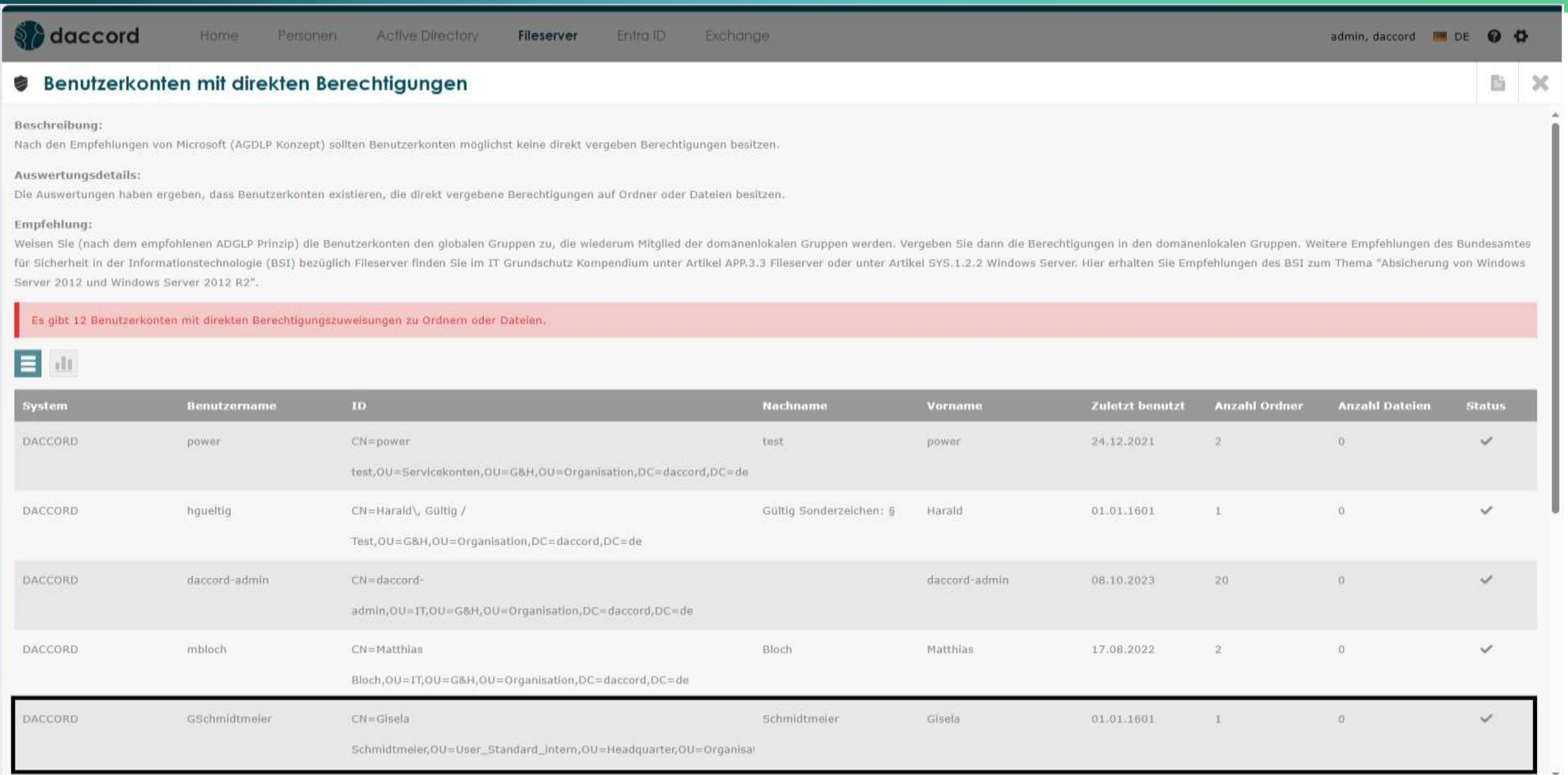
daccord

MS Fileserver: Kritische Richtlinien

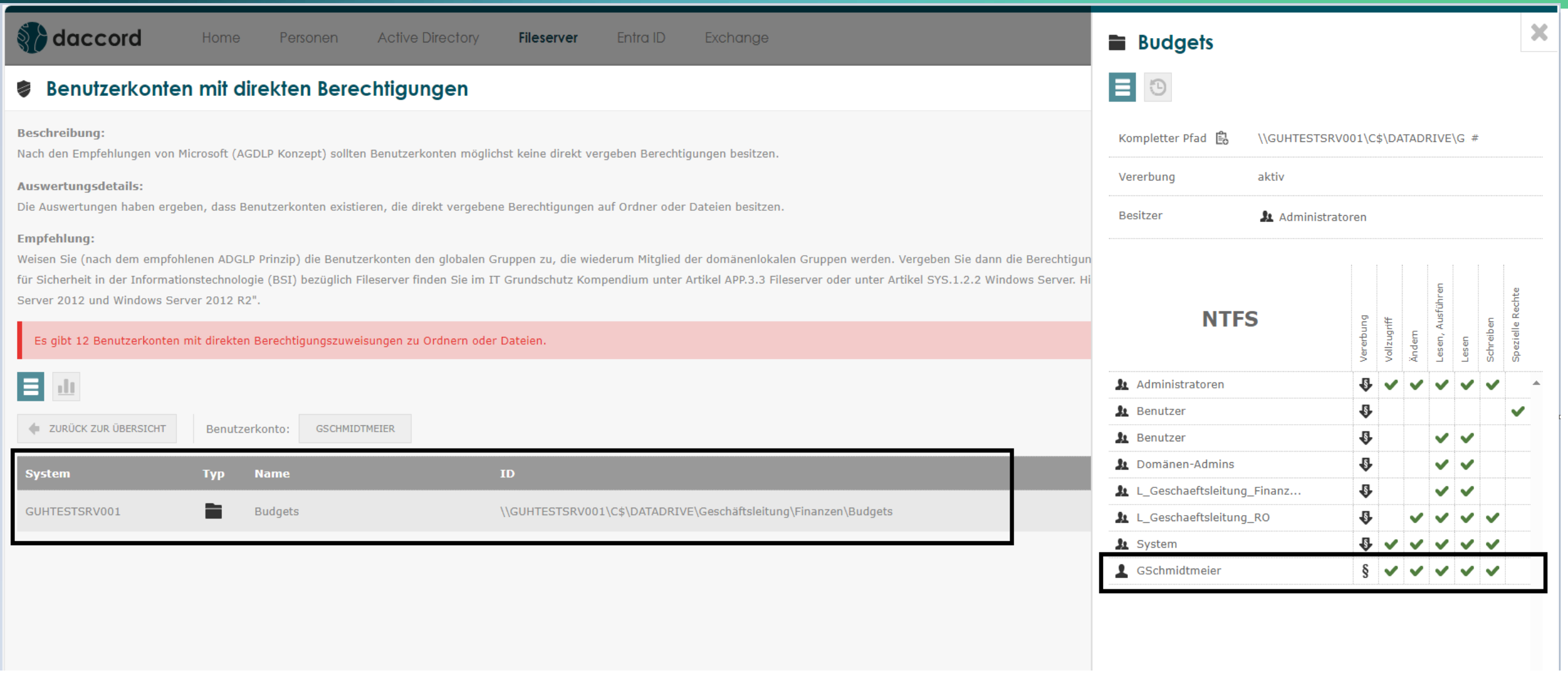


daccord

MS Fileserver: Richtlinien-Auswertung

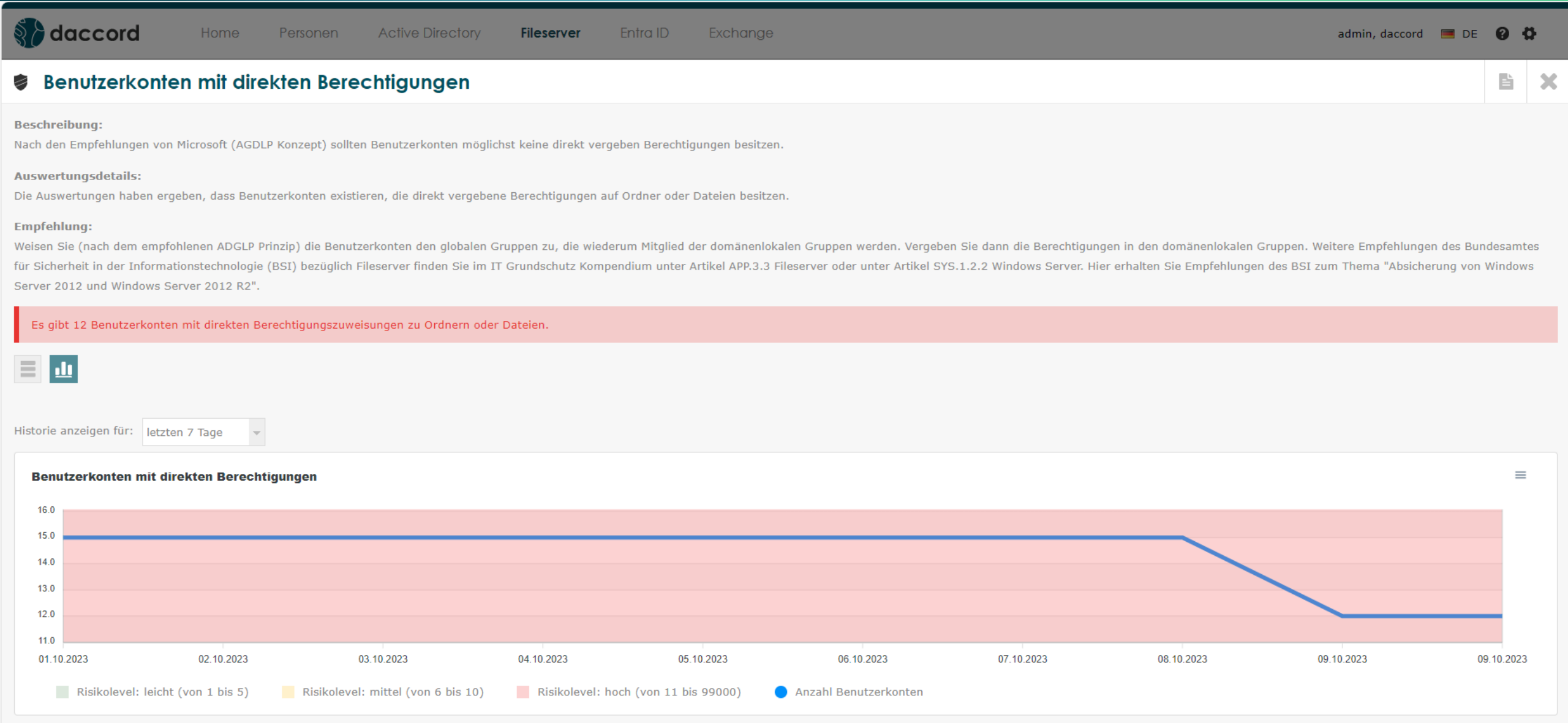


MS Fileserver: Richtlinien-Auswertung



daccord

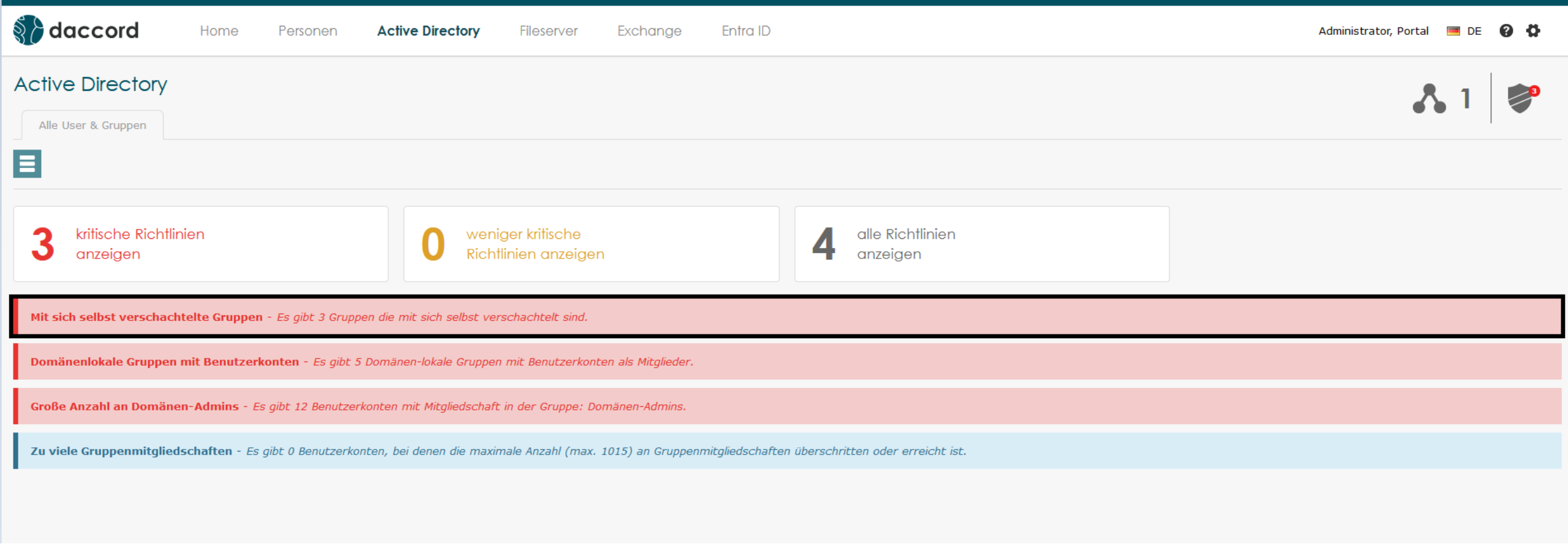
Historischer Verlauf



ANWENDUNGSFALL 3:

GIBT ES FEHLERHAFTE GRUPPENVERSCHACHTELUNGEN (LOOPS) IM ACTIVE DIRECTORY?

Fehlerhafte Gruppenverschachtelungen (Loops)



daccord

Fehlerhafte Gruppenverschachtelungen (Loops)

Mit sich selbst verschachtelte Gruppen

Beschreibung:
Active Directory Gruppen, welche mit sich selbst verschachtelt sind, können innerhalb von Anwendungen oder Scripten zu Problemen in Form von Abstürzen, unendlichen Schleifen und ungewollten Fehlermeldungen führen. Zirkuläre Verschachtelungen sind aus diesem Grund möglichst zu vermeiden.

Auswertungsdetails:
Im Active Directory System gibt es Gruppen, die mit sich selbst verschachtelt sind.

Empfehlung:
Überprüfen Sie Ihre Gruppenkonstellation und beheben Sie die zirkuläre Verschachtelung.

Es gibt 3 Gruppen die mit sich selbst verschachtelt sind.

Gruppenname	ID	Domain	Scope	Kategorie	Anzahl Verschachtelung
ROL_Purchasing-Employees	CN=ROL_Purchasing-Employees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_Trainees	CN=ROL_Trainees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_TEMP	CN=ROL_TEMP,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1

daccord

Fehlerhafte Gruppenverschachtelungen (Loops)

Mit sich selbst verschachtelte Gruppen

Beschreibung:
Active Directory Gruppen, welche mit sich selbst verschachtelt sind, können innerhalb von Anwendungen oder Scripten zu Problemen in Form von Abstürzen, unendlichen Schleifen und ungewollten Fehlermeldungen führen. Zirkuläre Verschachtelungen sind aus diesem Grund möglichst zu vermeiden.

Auswertungsdetails:
Im Active Directory System gibt es Gruppen, die mit sich selbst verschachtelt sind.

Empfehlung:
Überprüfen Sie Ihre Gruppenkonstellation und beheben Sie die zirkuläre Verschachtelung.

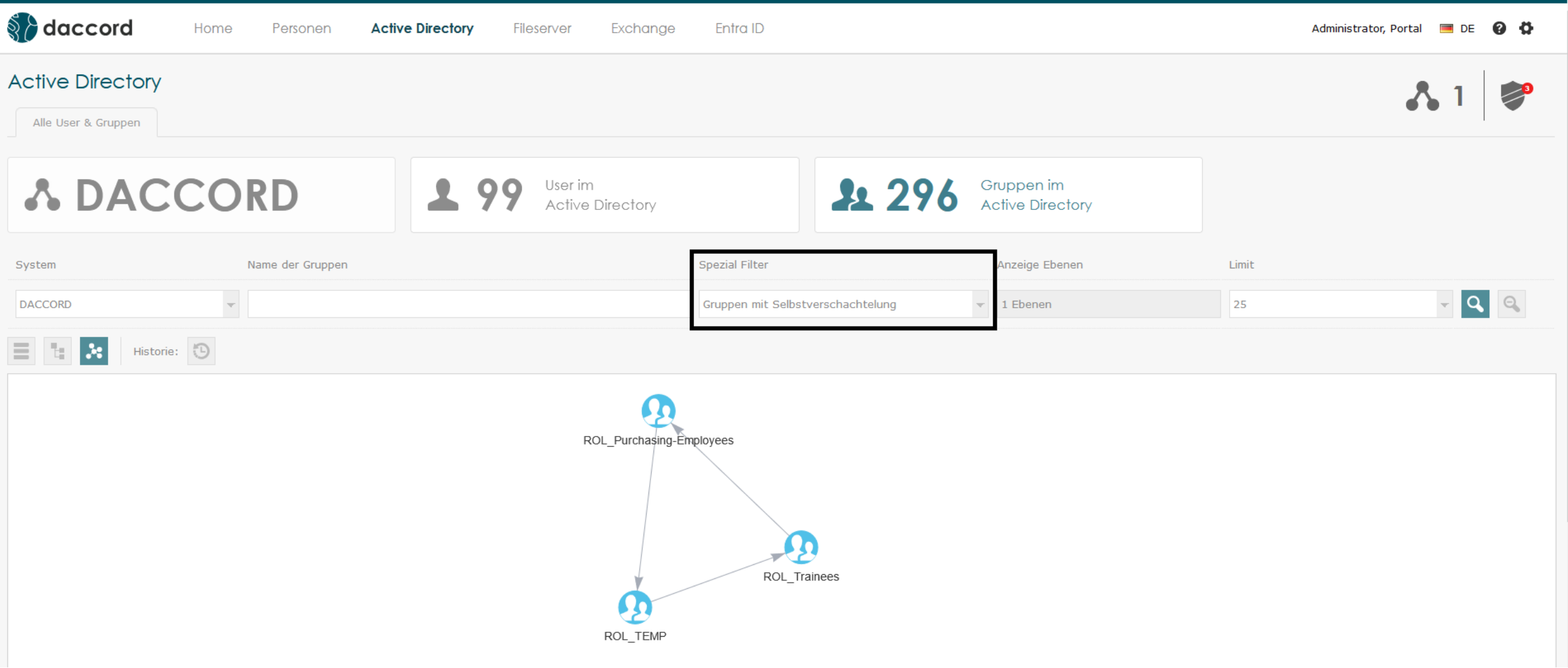
Es gibt 3 Gruppen die mit sich selbst verschachtelt sind.

ZURÜCK ZUR ÜBERSICHT | Gruppe: ROL_PURCHASING-EMPLOYEES

Gruppenname	ID	Domain	Scope	Kategorie	Reihenfolge
ROL_TEMP	CN=ROL_TEMP,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_Trainees	CN=ROL_Trainees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	1
ROL_Purchasing-Employees	CN=ROL_Purchasing-Employees,OU=global,OU=Gruppen,OU=Zentrale,OU=Organisation,DC=daccord,DC=de	DACCORD	Global	Sicherheit	2

daccord

Fehlerhafte Gruppenverschachtelungen (Loops)

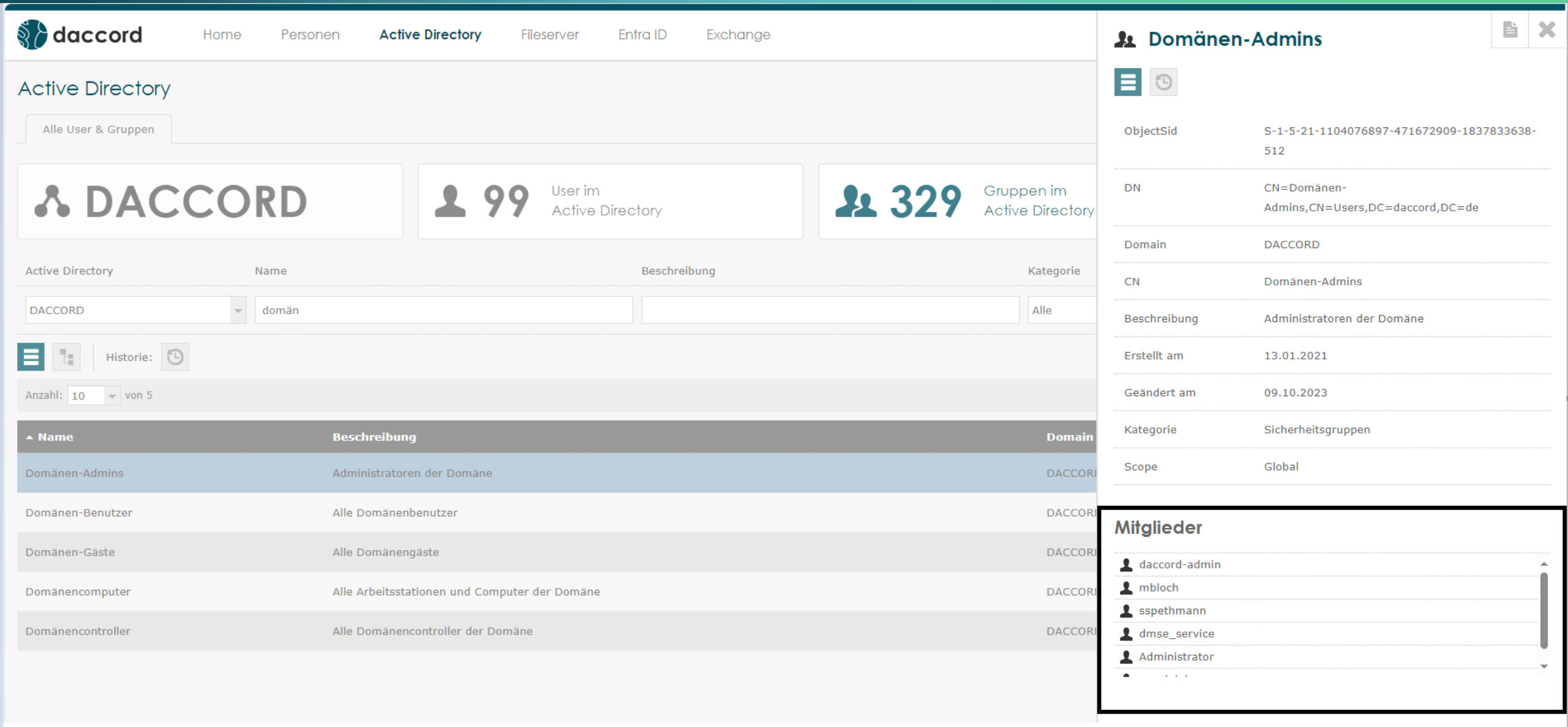


daccord

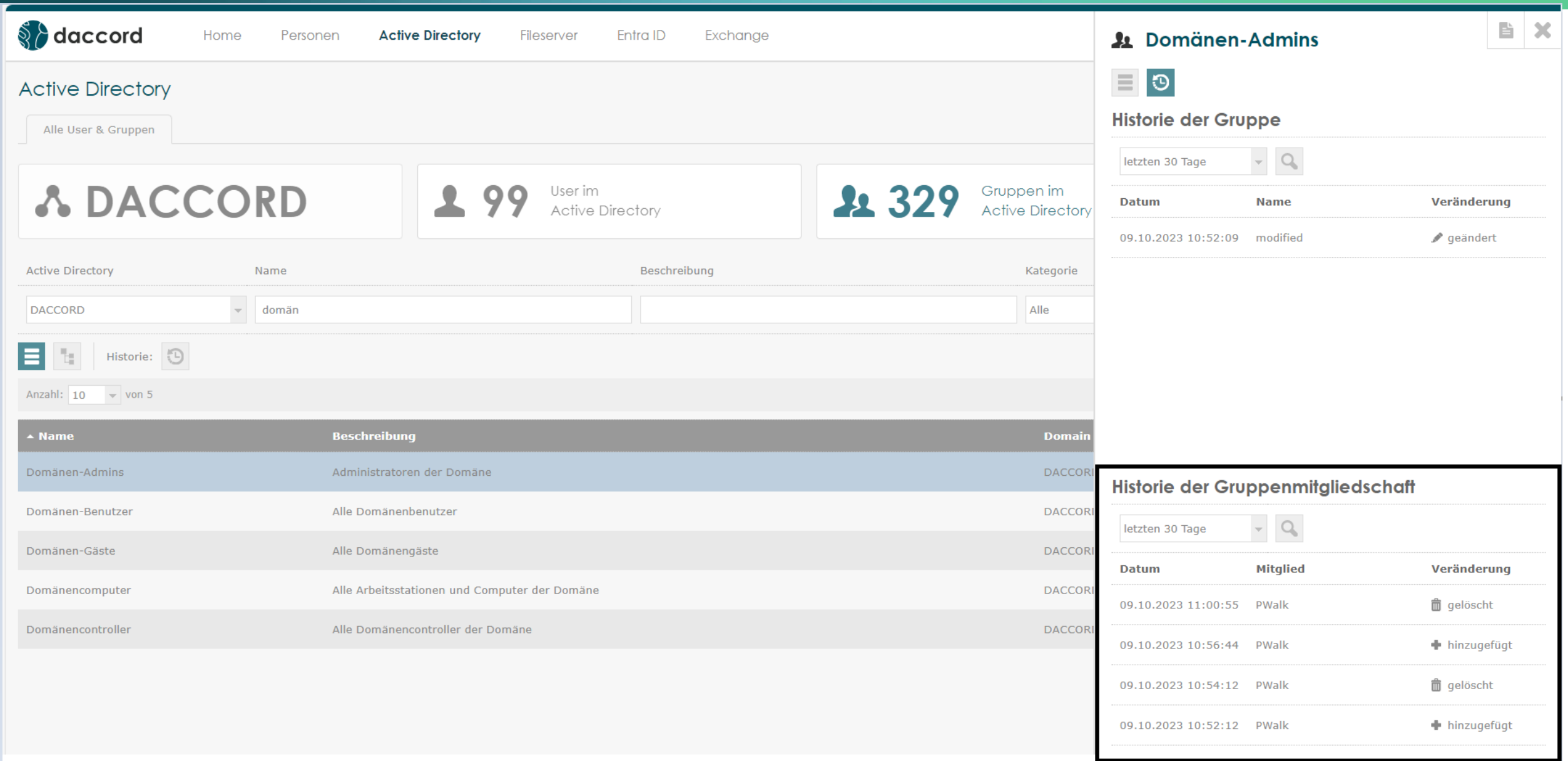
ANWENDUNGSFALL 4:

GAB ES ÄNDERUNGEN IN DER DOMAIN ADMIN GRUPPE IM ACTIVE DIRECTORY?

Gruppe Domänen-Admins



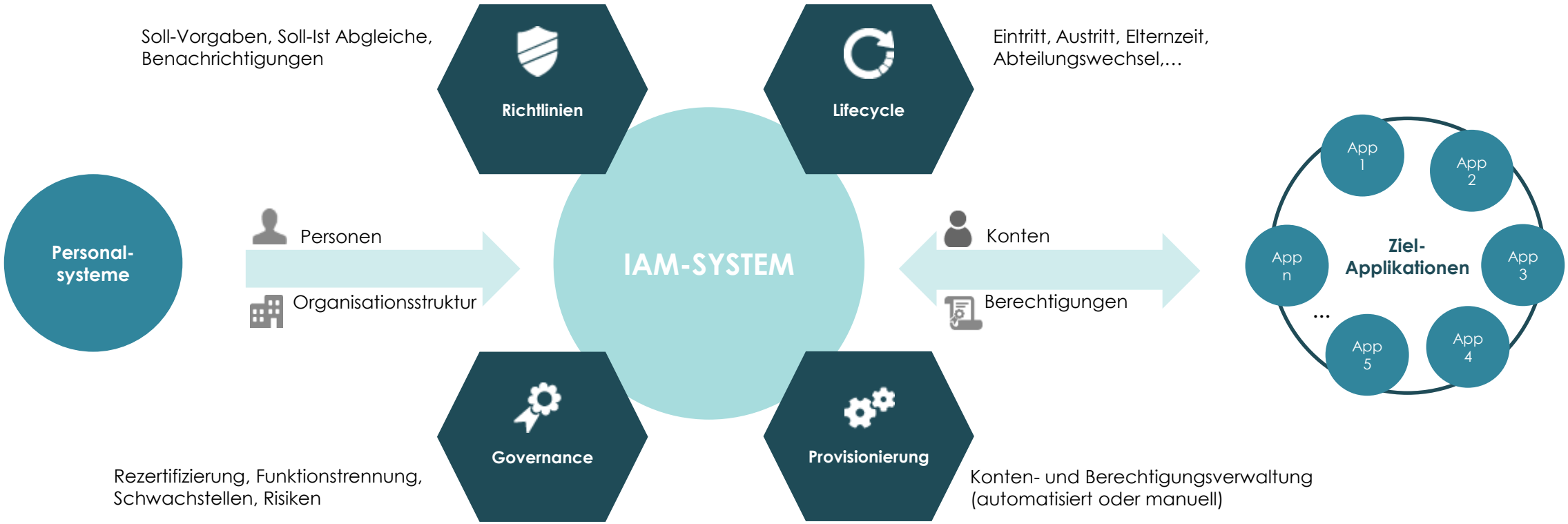
Gruppe Domänen-Admins Historie



DACCORD NEXT GEN

daccord Next Gen

daccord Next Gen versteht sich als **DIE** zentrale Anlaufstelle für Ihr Identity & Access Management.



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Sie finden uns hier in Halle 7 am Stand 349!