# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Zu meiner Person:

Ich lebe in Murnau am Staffelsee, 45min südlich von München,
und arbeite als Executive Consultant bei CGI

Ich habe eine Passion für das Active Directory sowie
das Azure Active Directory und angrenzender Technologien

- ➔ Microsoft zertifiziert seit Windows Server Active Directory Version im Jahr 2000
- ➔ 20-jährige Projekthistorie im Enterprise Kundenumfeld - im Bereich von Identity Technologien
- ➔ Nebenbei tätig als Fachjournalist. Mitarbeit an Fachlektoraten und Veröffentlichen von Fachartikeln in Print- und Onlinemedien
- ➔ Coming soon 😳 heise Academy Screencast Kurs „Hybrid Azure AD“

LinkedIn Profil

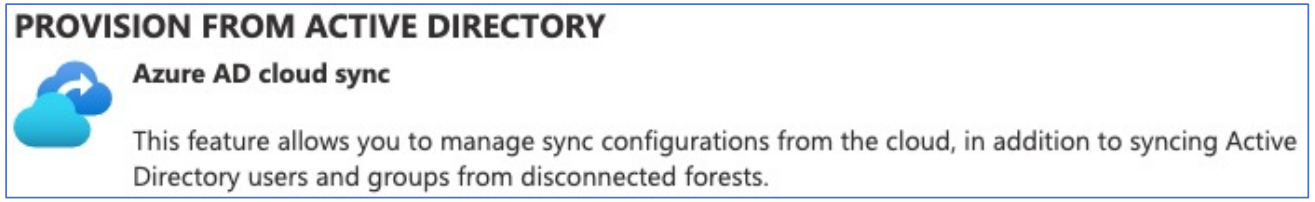
@KlaBiers

Blog:
https://nothingbutcloud.net/

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

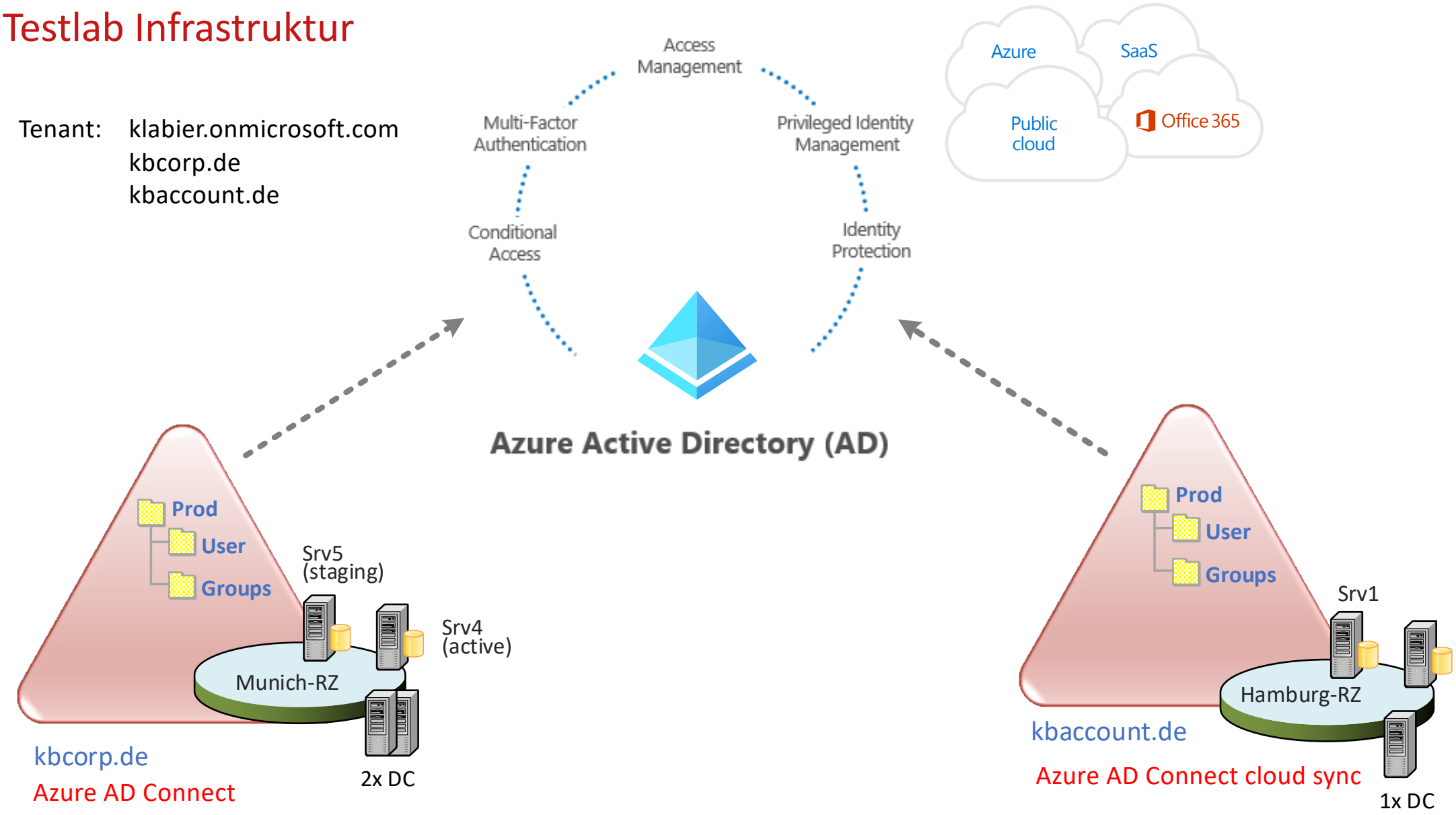
## Agenda:

- Historische Aspekte (ILM, FIM, MIM)
- Azure AD Connect (Komponenten, Architektur, Setup, Security, unterstützte Szenarien, …)
- Kleine Pause … (10 min)
- Azure AD Connect cloud sync (wann und warum?)
- Demos zu Azure AD Connect / Azure AD cloud sync

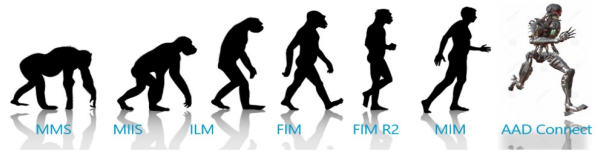
# Testlab Infrastruktur

Tenant: klabier.onmicrosoft.com
kbcorp.de
kbaccount.de



# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## A long journey:



Source: Oxford Computer Group

„Synchronization Service“ ist Teil von Azure AD Connect mit einer langen Historie im Microsoft Identity Portfolio

MMS (1999), MIIS (2003), ILM (2007), FIM (2010), FIM R2, MIM (2015 … bis heute)

Identity Suite mit diversen Technologien: Self-Service Portal, Zertifikatsverwaltung, RBAC Mgmt, etc.

„Synchronization Service“ kann ohne MIM eingesetzt werden und ohne Hybrid Setup…

DirSync (2009), Azure AD Sync (2014), Azure AD Connect

Herzstück der Identity Suite ist „Synchronization Service“ der sich unter der Haube von AAD Connect befindet

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Optionen für das Azure AD Connect Server Setup

| „Express“ Variante | „Customize“ Variante |
| --- | --- |
| Schnellste Variante für Setup | Empfohlene Variante. Import von Konfiguration |
| Ein Forest (eine Gesamtstruktur) | Angabe mehrerer Forests |
| Password Hash Synchronisation | Wahl der Authentifizierung (PHS, PTA, Federation) |
| „Auto Upgrade“ eingeschaltet | „Auto Upgrade“ ist eingeschaltet |
| Keine Möglichkeit für „staging“ oder „active“ | Entscheidung über „staging“ oder „active“ |
| Keine Wahl für Organisationseinheit (OU) | Filterung von Domain und OU oder Pilot Gruppe |
| „Source Anchor“ ms-DS-ConsistencyGuid oder objectGU | Wahlweise Abweichung von Standard „Anchor“ |

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Optionen für das Azure AD Connect Server Setup

| „Customize“ Variante | „Customize“ Variante mit „staging“ |
| --- | --- |
| Empfohlene Variante. Import von Konfiguration möglich | „Muss“ Variante. Import von Konfiguration möglich |
| Angabe mehrerer Forests und Entscheidung SQL | Identische Settings zu „active“ zwingend benötigt |
| Wahl der Authentifizierung (PHS, PTA, Federation) | Ab v1.5.42.0 (Juli 2020) „Export“ der Konfiguration |
| „Auto Upgrade“ ist eingeschaltet | Gleiche Einstellungen gewährleistet |
| Entscheidung über „staging“ oder „active“ | Server ist immer „staging“ |
| Filtermöglichkeit von Domain und OU oder Pilot Gruppe | Keine weiteren Einstellungen möglich |
| Wahlweise Abweichung vom Standard „Anchor“ | Server ist schnell startklar |

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Was befindet sich nach dem Setup alles auf dem Azure AD Connect Server?


- Azure AD Connect (Setupmodul, Desktop)
- Synchronization Rules Editor (Filterung basierend auf Attributen, Transformationen)
- Powershellmodule ADSync (**`get-command –module adsync`**)
- SQL Server 2012 Express LocalDB (10GB limitation)
- Synchronization Service (Admin Console, miisclient.exe)
- ADSyncConfig.psm1 (link) (ist auch Teil von **`Invoke-ADSyncDiagnostics`**)
- Monitoring und Health Komponenten


(c) Klaus Bierschenk – klaus@nothingbutcloud.net

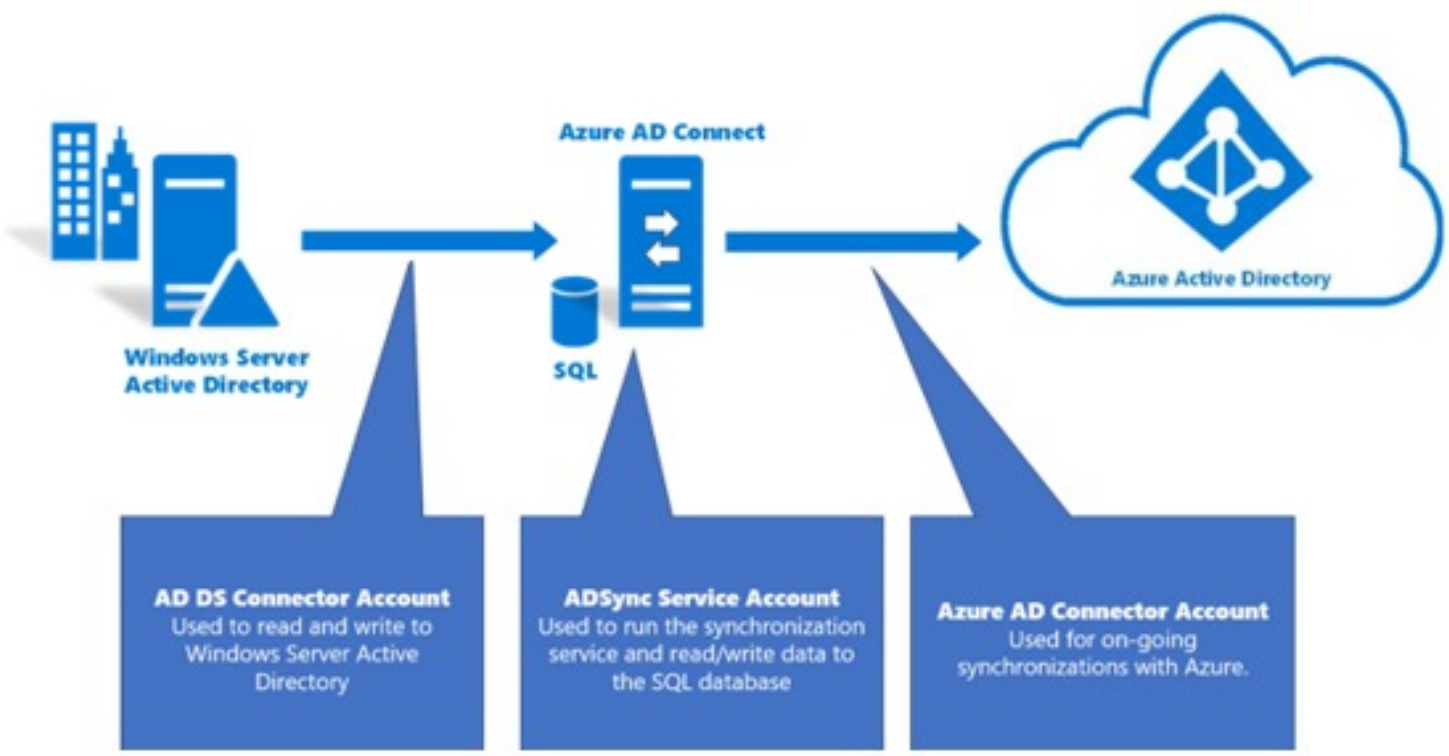
# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Was befindet sich nach dem Setup auf dem AAD Connect Server?

<< Demo: AAD Connect Server Komponenten>>

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Was befindet sich nach dem Setup auf dem AAD Connect Server?

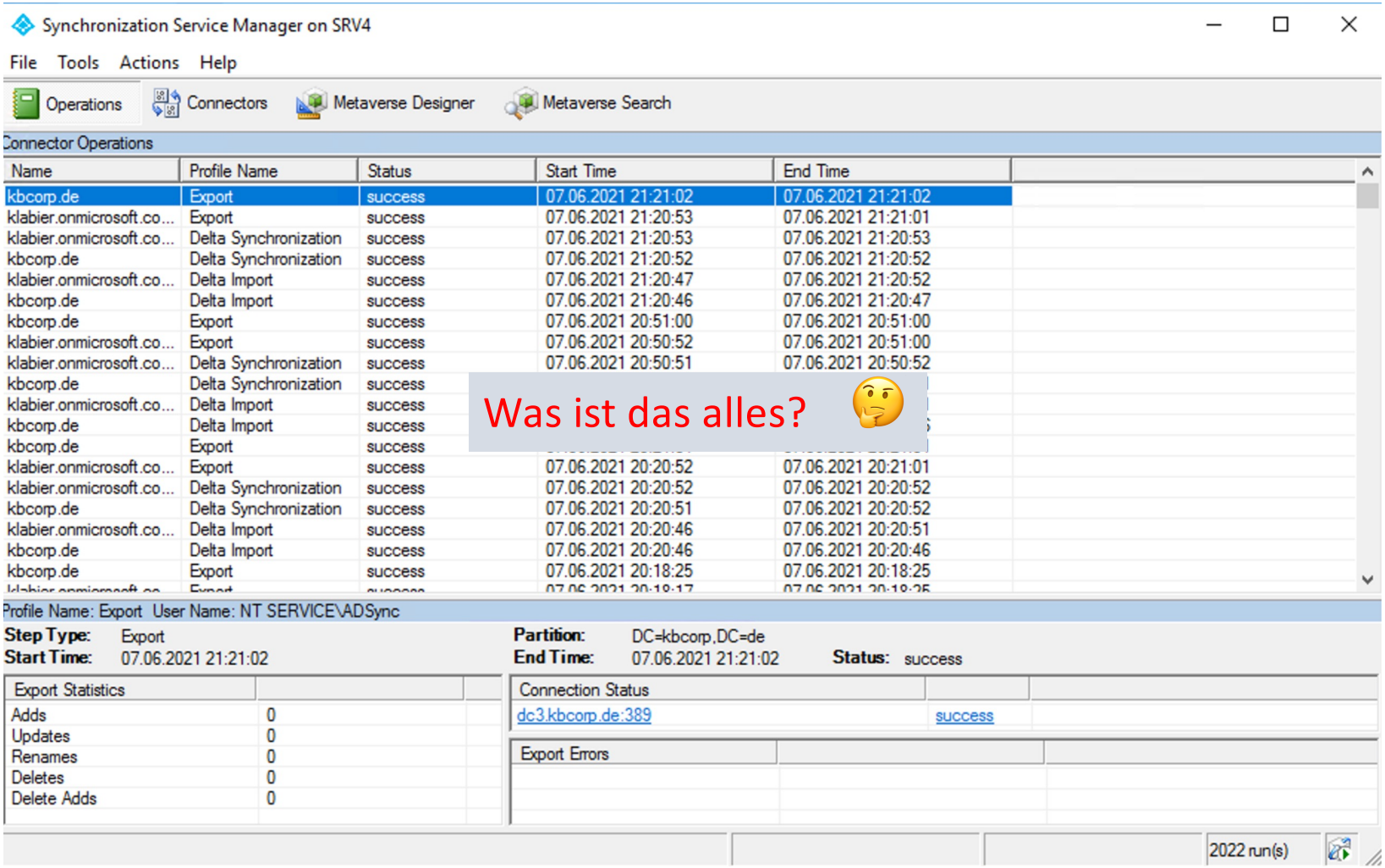



Must check/read:

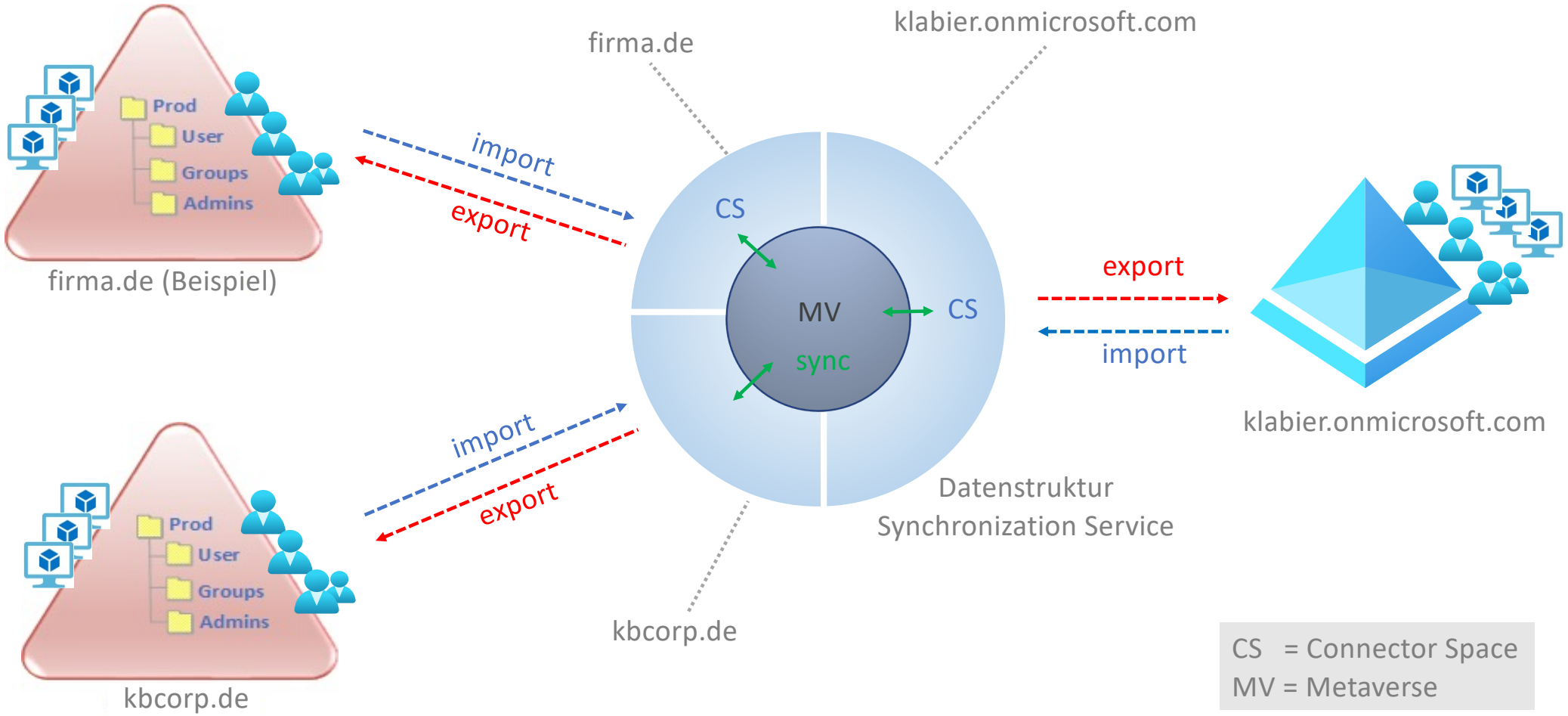
Konfigurieren ADConnector Berechtigungen (link)

ADSync-Dienstkonto (link)

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

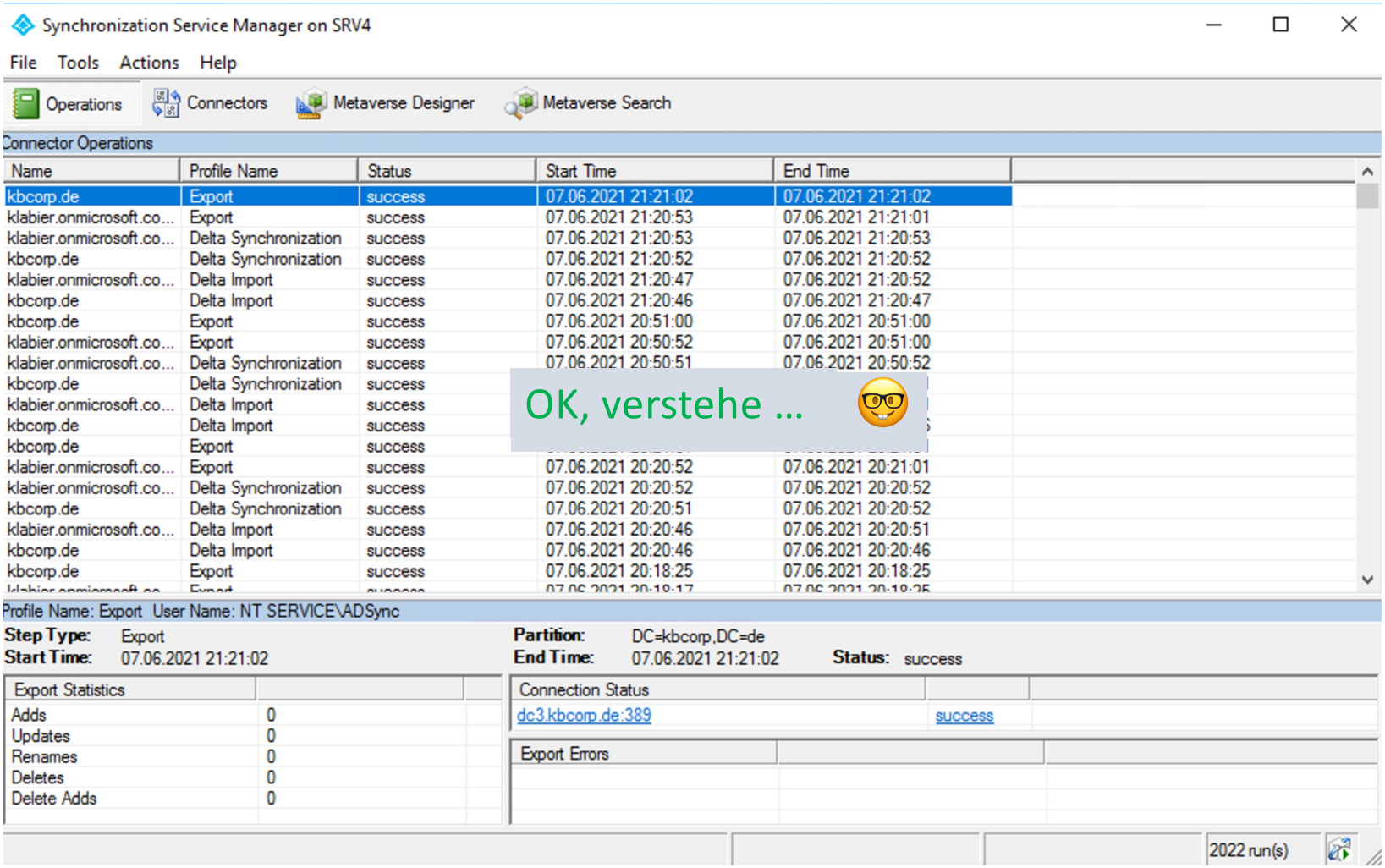


# Synchronisation – Schaltzentrale einer hybriden Infrastruktur




CS = Connector Space
MV = Metaverse

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

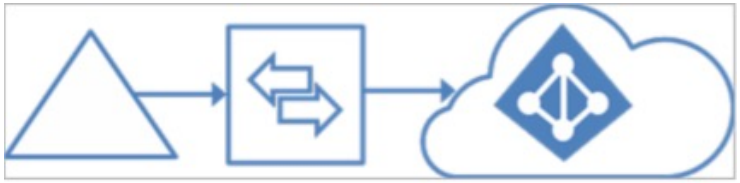


# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

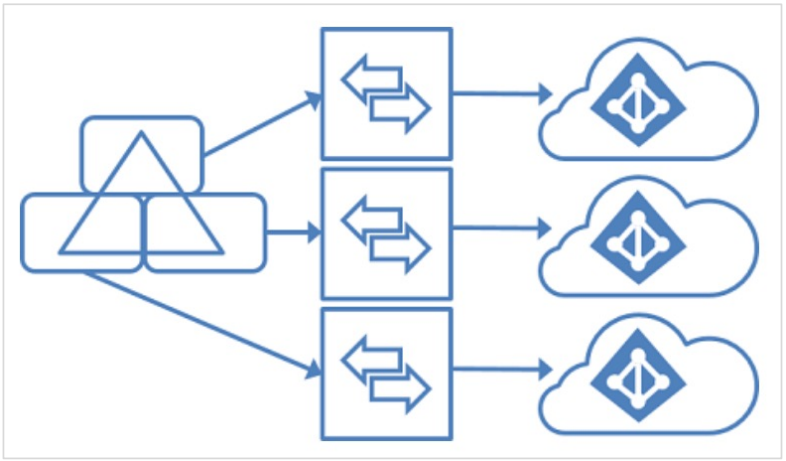
## Unterstützte Szenarien in einer Gesamtstruktur

| Supported | Unsupported |
| --- | --- |

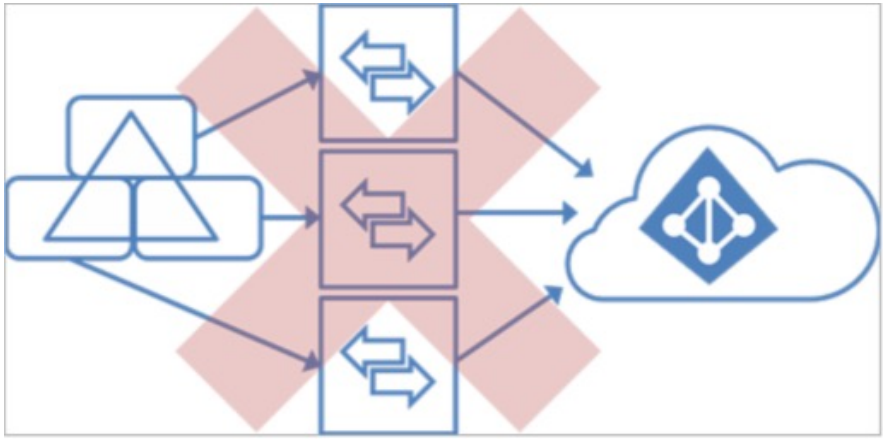
Example1



Example2



Example3

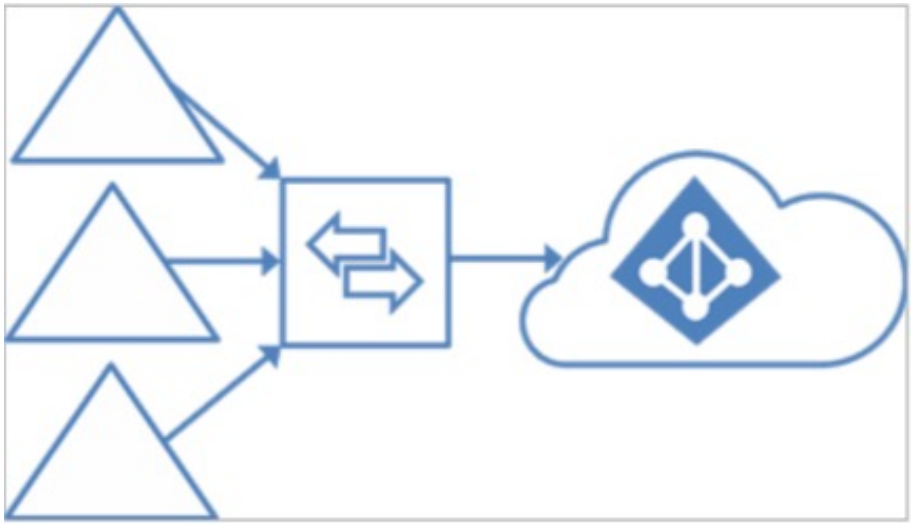


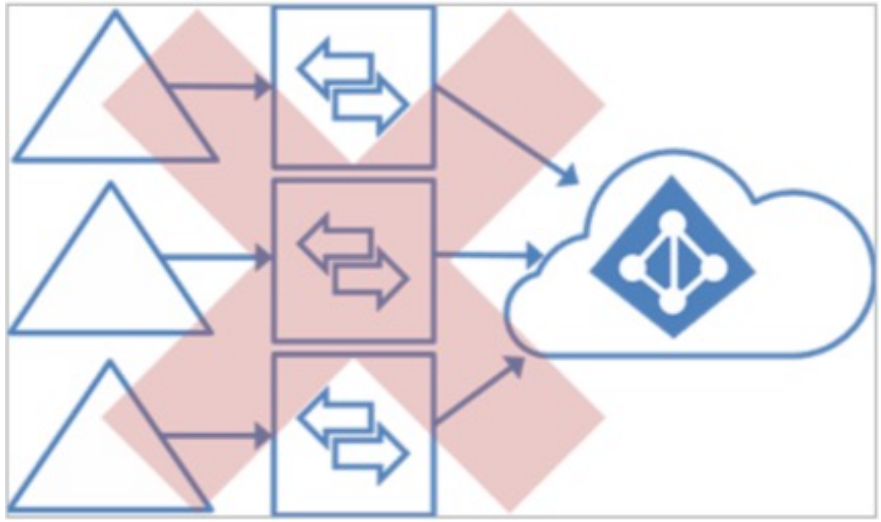
Weitere Details zu unterstützten Szenarien (link)

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Unterstützte Szenarien mit mehreren Gesamtstrukturen

| Supported | Unsupported |
| --- | --- |





Weitere Details zu unterstützten Szenarien (link)

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Hochverfügbarkeit von Azure AD Connect Server / Datenspeicherung

- Ist Hochverfügbarkeit wirklich notwendig?
- Kein Farmsetup! Jeder AAD Connect Server hat seine eigene Konfiguration
- Was passiert den eigentlich wenn ein AAD Connect Server ausfällt?
- Staging Server Konzept -> Demo 😀 / „pending exports“ vor Wechsel prüfen
- Staging Server Herausforderung! Gleiche Config wichtig. AADConnectDocumenter in den Backup Folien
- Hochverfügbarkeit für SQL kann Sinn machen
- Setup mit *„useexistingdatabase“* switch (MS Docs link)

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Regeleditor – Filtern und Transformieren von der Objekten

| *Anforderung* | *Filterung erfolgt durch* |
| --- | --- |
| Definieren der Domänen aus einem Forest | Azure AD Connect Setup Assistent (Demo 😀) |
| Selektieren der OUs einer Domäne | |
| Transformieren von Attributen | Azure AD Connect Rule Editor |
| Filterung auf Basis von Attributen | |

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Regeleditor – Filtern und Transformieren von der Objekten

<< Demo Filterung AAD Connect Setup und miisclient.exe >>

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Regeleditor – Filtern und Transformieren von der Objekten

Erfüllt zwei Aufgaben:

Transformationen:

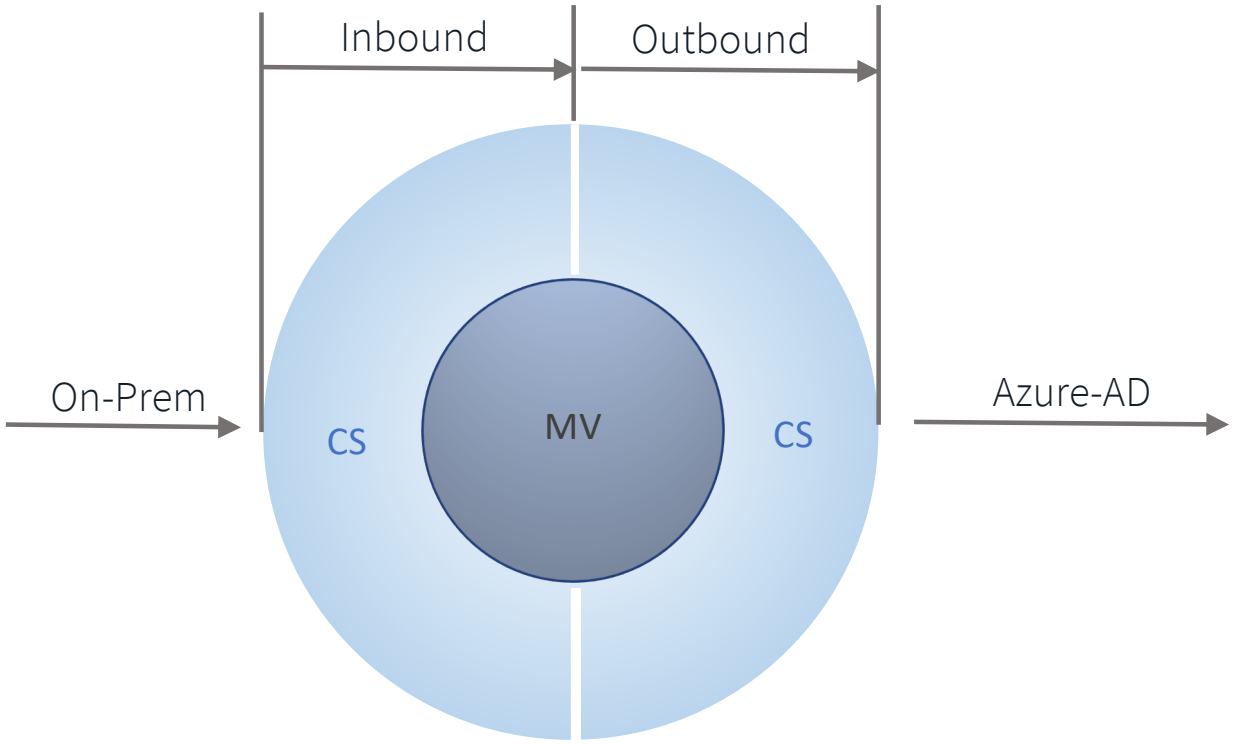
Fixe Zuweisung:
**`Company= "KBCORP Lab"`**

Ausdruck:
**`givenName=UCase([givenName])`**

Filterung:

MV Attribute:
**`cloudFiltered = true/false`**

positiv / negativ möglich



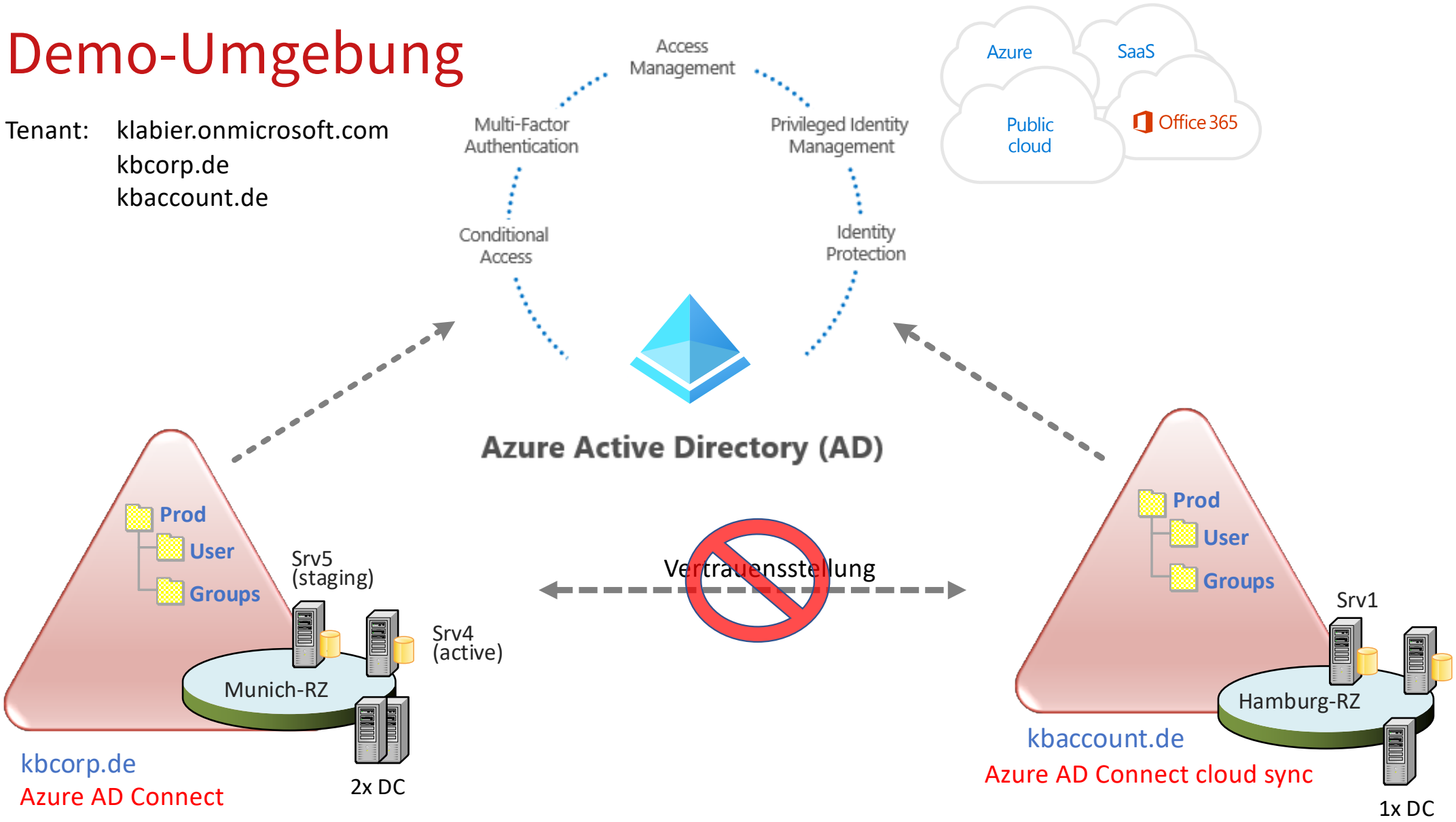
# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Regeleditor – Filtern und Transformieren von der Objekten

<< Demo Filterung mit Regeleditor >>

# Demo-Umgebung

Tenant: klabier.onmicrosoft.com
kbcorp.de
kbaccount.de



# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Übersicht Azure AD Connect cloud sync

- Relativ neue Alternative zu AAD Connect (Public Preview ab MS Ignite 2019 und GA seit Ende 2020)
- „Derzeit“ kein Ersatz für Azure AD Connect
- Co-Existenz der Technologien ist möglich
- Minimale On-Premises Komponenten
- Management in der Cloud. Konfiguration erfolgt ausschließlich im Azure Portal
- Bei neuen Installationen ist abzuwägen welche Technologie vorzuziehen ist
- Mehrere Server/Agents – Hochverfügbar (kein Lastenausgleich)

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

| Funktion | Azure AD Connect | AAD cloud sync |
|---|---|---|
| Konfiguration wird wo gespeichert? | Lokaler Server (SQL) | Azure |
| Zentrales Management aus dem Azure Portal möglich | | ✓ |
| Unterstützung für nicht verbundene Forests | | ✓ |
| Filterung auf Ebene von Attributen | ✓ | |
| „Einfache“ Filterung basierend auf Gruppenmitgliedschaft | | ✓ |
| Zurückschreiben aus dem Azure AD (Password, Gruppen, Geräte) | ✓ | |
| On-Premises Agent Hochverfügbarkeit | | ✓ |
| Synchronisation benutzerspezifischer Attribute | ✓ | |
| Installation der Agenten auf einem Domänen Controller | ✓ | ✓ |
| Unterstützung für „Pass-Thru Authentication“ | ✓ | |
| Powershell Unterstützung | ✓ | ✓ |

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Regeleditor – Filtern und Transformieren von der Objekten

<< Demo cloud sync Portal und Agent Server >>

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Versionen und Update check

Azure AD Connect Server
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/reference-connect-version-history#:~:text=April%202024%20werden%20die%20Versionen,einen%20optimalen%20Support%20zu%20erhalten.

Azure AD Connect cloud sync Agent
https://docs.microsoft.com/de-de/azure/active-directory/cloud-sync/reference-version-history

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

FIM/MIM Link Collection (Huge list! Not totally new but perfect to understand FIM/MIM/Sync)
https://social.technet.microsoft.com/wiki/contents/articles/3610.fim-2010-mim-2016-related-wiki-articles.aspx#FIM_Understanding_Article

It is actually possible to synchronize different portions of AD to different tenants too. See this article for limitations of this approach.
https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-topologies#each-object-only-once-in-an-azure-ad-tenant

IdFix: Guide (also included in Download)
https://docs.microsoft.com/en-us/office365/enterprise/install-and-run-idfix
https://microsoft.github.io/idfix/

AADConnectConfigDocumenter
https://github.com/Microsoft/AADConnectConfigDocumenter

Custom setup
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-install-custom

Azure AD Connect – V2 API DEployment
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-endpoint-api-v2#deployment-guidance
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account

Fehlersuche mit einzelnen Objekten
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/tshoot-connect-object-not-syncing

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

AADConnectConfigDocumenter
https://github.com/Microsoft/AADConnectConfigDocumenter

Azure AD Pricing (AAD Connect / Health included)
https://azure.microsoft.com/en-us/pricing/details/active-directory/

Hardening Service Accounts from AADConnect
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account

Supported Scenarios
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#each-object-only-once-in-an-azure-ad-tenant

Use existingdatabase switch
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-install-existing-database
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-install-move-db

Start to find out what is possible with Cloud provisioning
https://docs.microsoft.com/en-us/azure/active-directory/cloud-provisioning/

Check for pending exports
https://docs.microsoft.com/de-de/azure/active-directory/hybrid/tshoot-connect-object-not-syncing

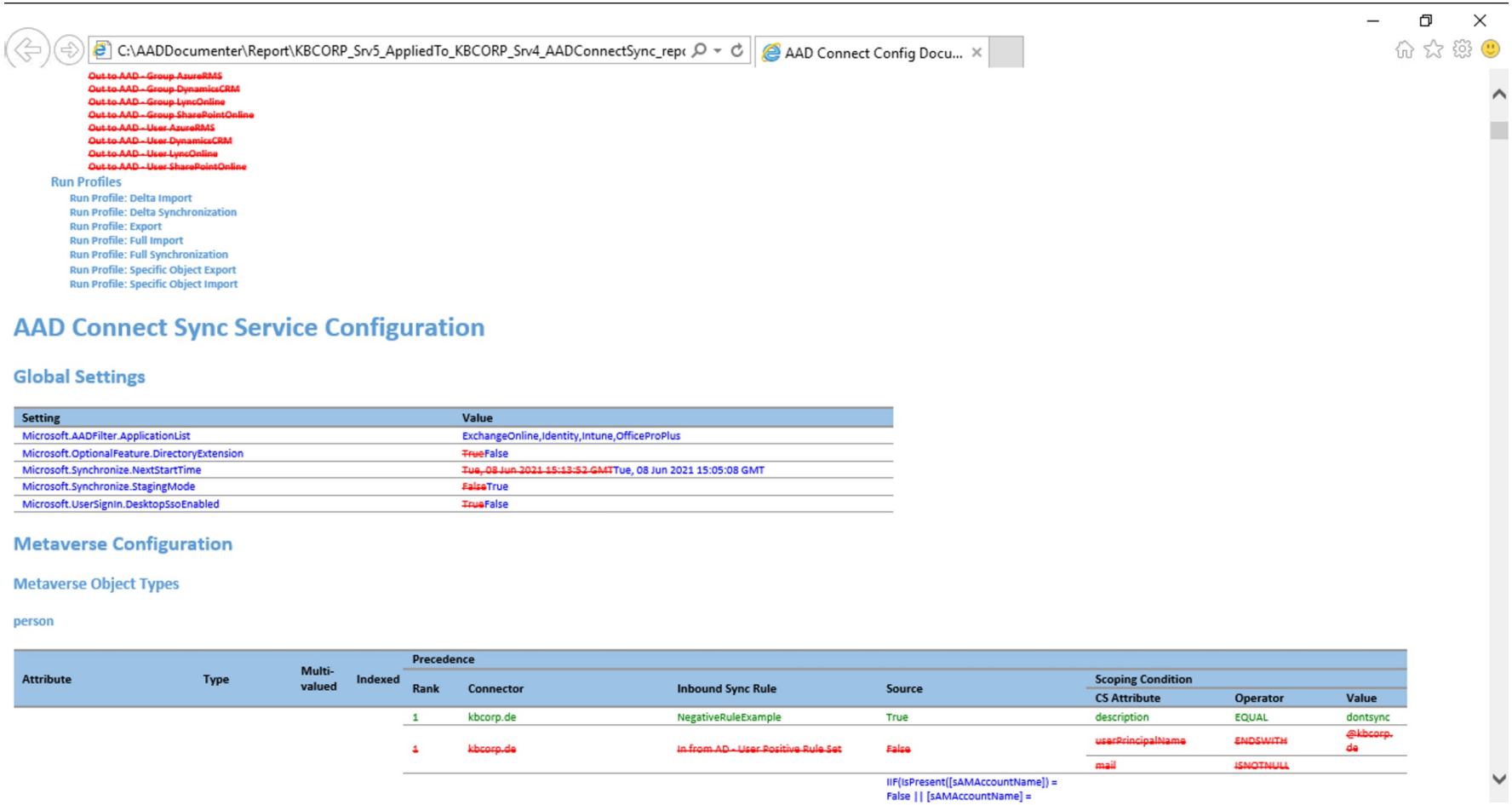
# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## Dokumentation und Vergleich: Staging vs. Active Server

- Vergleicht zwei Server Konfigurationen
- Dump erstellen: `Get-ADSyncServerConfiguration -Path "<CompletePathToOutputFolder>"`
- Zwingend notwendig vor Wechsel von Staging zu Active
- Gute Kenntnis der Terminologie der Sync Engine wünschenswert um Report zu verstehen
- Gute Möglichkeit Sync Rules zu exportieren/transferieren
- Gut geeignet um AAD Connect Server zu dokumentieren

Download und Dokumentation:
https://github.com/Microsoft/AADConnectConfigDocumenter

# Synchronisation – Schaltzentrale einer hybriden Infrastruktur



# Synchronisation – Schaltzentrale einer hybriden Infrastruktur

## idFix: Aufräumen für intakte zu synchronisierende Datenbasis

Prüft Objekte (on-Prem) mit Fehlerreport was im Azure AD / M365 zu Prüblemen führen kann

Änderungen direkt in der GUI …

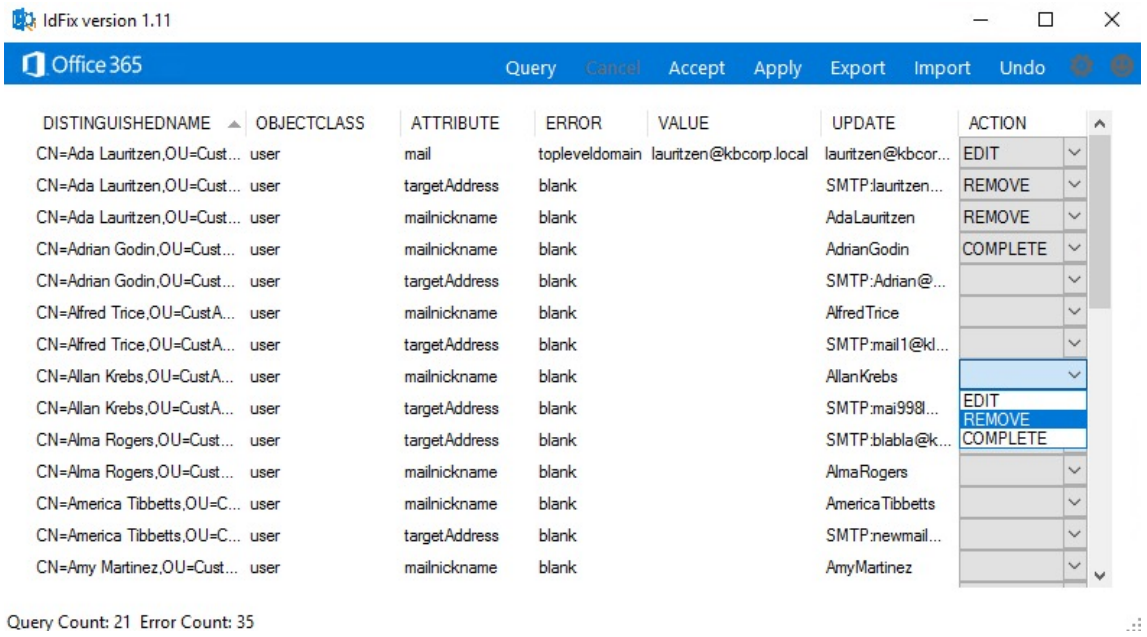
… oder auch per CSV

Vorsichtig! Bulk updates

… jedoch lässt sich Kontext des Users ändern

Jeder Schreibvorgang erstellt LDIF für Undo

Verbose report mit Details zu Vorgängen



# Synchronisation – Schaltzentrale einer hybriden Infrastruktur