

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



Copyright © 2015 Microsoft Corporation. All rights reserved.

PROVISION FROM ACTIVE DIRECTORY

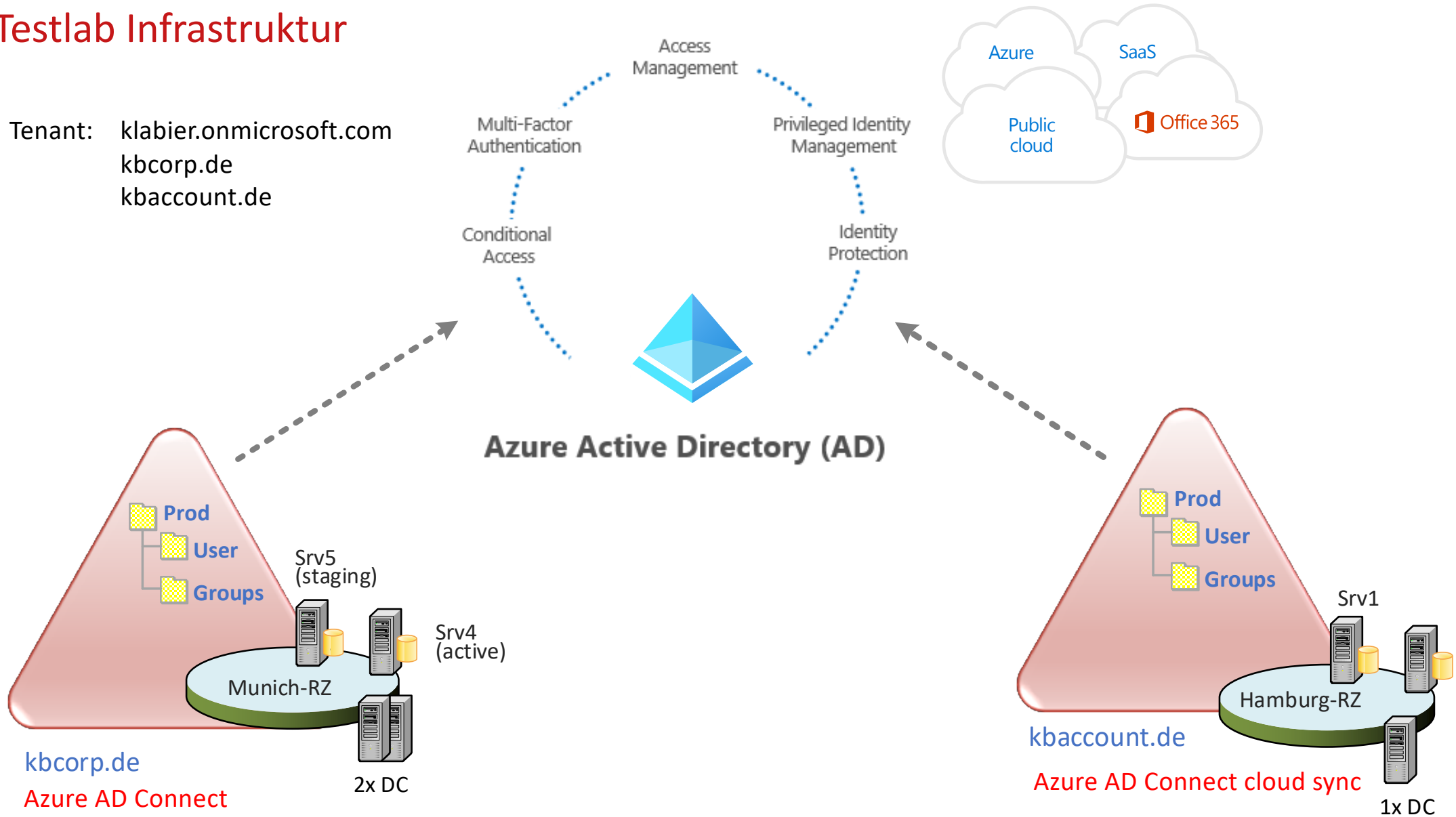


Azure AD cloud sync

This feature allows you to manage sync configurations from the cloud, in addition to syncing Active Directory users and groups from disconnected forests.

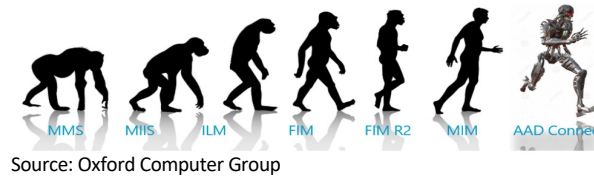
Testlab Infrastruktur

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



Synchronisation – Schaltzentrale einer hybriden Infrastruktur

A long journey:



„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

Schnellste Variante für Setup

Ein Forest (eine Gesamtstruktur)

Password Hash Synchronisation

„Auto Upgrade“ eingeschaltet

Keine Möglichkeit für „staging“ oder „active“

Keine Wahl für Organisationseinheit (OU)

„Source Anchor“ ms-DS-ConsistencyGuid oder objectGUID

„Customize“ Variante

Empfohlene Variante. Import von Konfiguration

Angabe mehrerer Forests

Wahl der Authentifizierung (PHS, PTA, Federation)

„Auto Upgrade“ ist eingeschaltet

Entscheidung über „staging“ oder „active“

Filterung von Domain und OU oder Pilot Gruppe

Wahlweise Abweichung von Standard „Anchor“

Synchronisation – Schaltzentrale einer hybriden Infrastruktur

Optionen für das Azure AD Connect Server Setup

„Customize“ Variante

Empfohlene Variante. Import von Konfiguration möglich

Angabe mehrerer Forests und Entscheidung SQL

Wahl der Authentifizierung (PHS, PTA, Federation)

„Auto Upgrade“ ist eingeschaltet

Entscheidung über „staging“ oder „active“

Filtermöglichkeit von Domain und OU oder Pilot Gruppe

Wahlweise Abweichung vom Standard „Anchor“

„Customize“ Variante mit „staging“

„Muss“ Variante. Import von Konfiguration möglich

Identische Settings zu „active“ zwingend benötigt

Ab v1.5.42.0 (Juli 2020) „Export“ der Konfiguration

Gleiche Einstellungen gewährleistet

Server ist immer „staging“

Keine weiteren Einstellungen möglich

Server ist schnell startklar

Synchronisation – Schaltzentrale einer hybriden Infrastruktur

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



Copyright © 2015 Microsoft Corporation. All rights reserved.

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

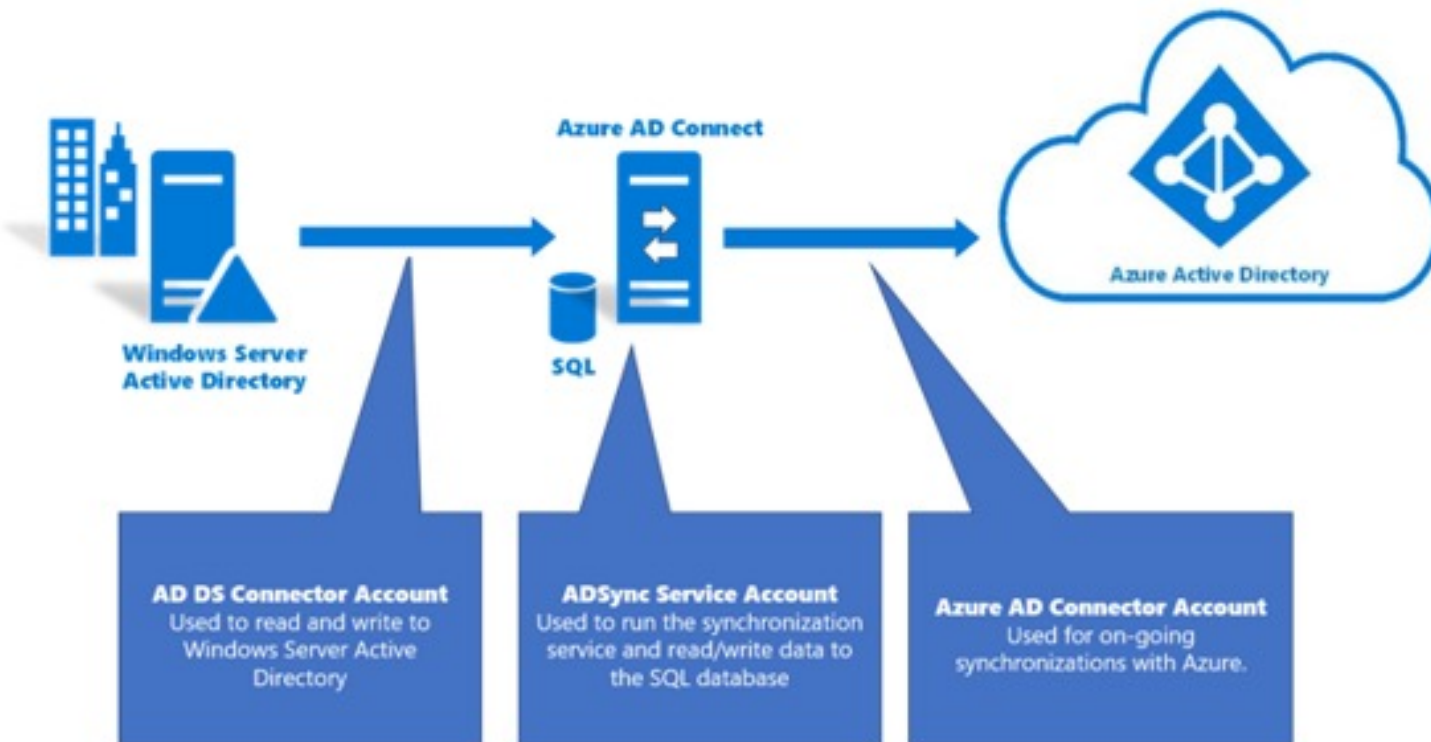
Synchronisation – Schaltzentrale einer hybriden Infrastruktur

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

The screenshot shows the Synchronization Service Manager interface. The main window displays a list of connector operations with columns for Name, Profile Name, Status, Start Time, and End Time. A red text box with a thinking face emoji is overlaid on the list, asking "Was ist das alles?". Below the list, the details for a specific operation are shown, including Step Type, Start Time, End Time, Partition, and Status. The Connection Status is "success" and the Export Errors section is empty.

Name	Profile Name	Status	Start Time	End Time
kbcorp.de	Export	success	07.06.2021 21:21:02	07.06.2021 21:21:02
klabier.onmicrosoft.co...	Export	success	07.06.2021 21:20:53	07.06.2021 21:21:01
klabier.onmicrosoft.co...	Delta Synchronization	success	07.06.2021 21:20:53	07.06.2021 21:20:53
kbcorp.de	Delta Synchronization	success	07.06.2021 21:20:52	07.06.2021 21:20:52
klabier.onmicrosoft.co...	Delta Import	success	07.06.2021 21:20:47	07.06.2021 21:20:52
kbcorp.de	Delta Import	success	07.06.2021 21:20:46	07.06.2021 21:20:47
kbcorp.de	Export	success	07.06.2021 20:51:00	07.06.2021 20:51:00
klabier.onmicrosoft.co...	Export	success	07.06.2021 20:50:52	07.06.2021 20:51:00
klabier.onmicrosoft.co...	Delta Synchronization	success	07.06.2021 20:50:51	07.06.2021 20:50:52
kbcorp.de	Delta Synchronization	success		
klabier.onmicrosoft.co...	Delta Import	success		
kbcorp.de	Delta Import	success		
kbcorp.de	Export	success		
klabier.onmicrosoft.co...	Export	success	07.06.2021 20:20:52	07.06.2021 20:21:01
klabier.onmicrosoft.co...	Delta Synchronization	success	07.06.2021 20:20:52	07.06.2021 20:20:52
kbcorp.de	Delta Synchronization	success	07.06.2021 20:20:51	07.06.2021 20:20:52
klabier.onmicrosoft.co...	Delta Import	success	07.06.2021 20:20:46	07.06.2021 20:20:51
kbcorp.de	Delta Import	success	07.06.2021 20:20:46	07.06.2021 20:20:46
kbcorp.de	Export	success	07.06.2021 20:18:25	07.06.2021 20:18:25
klabier.onmicrosoft.co...	Export	success	07.06.2021 20:18:17	07.06.2021 20:18:25

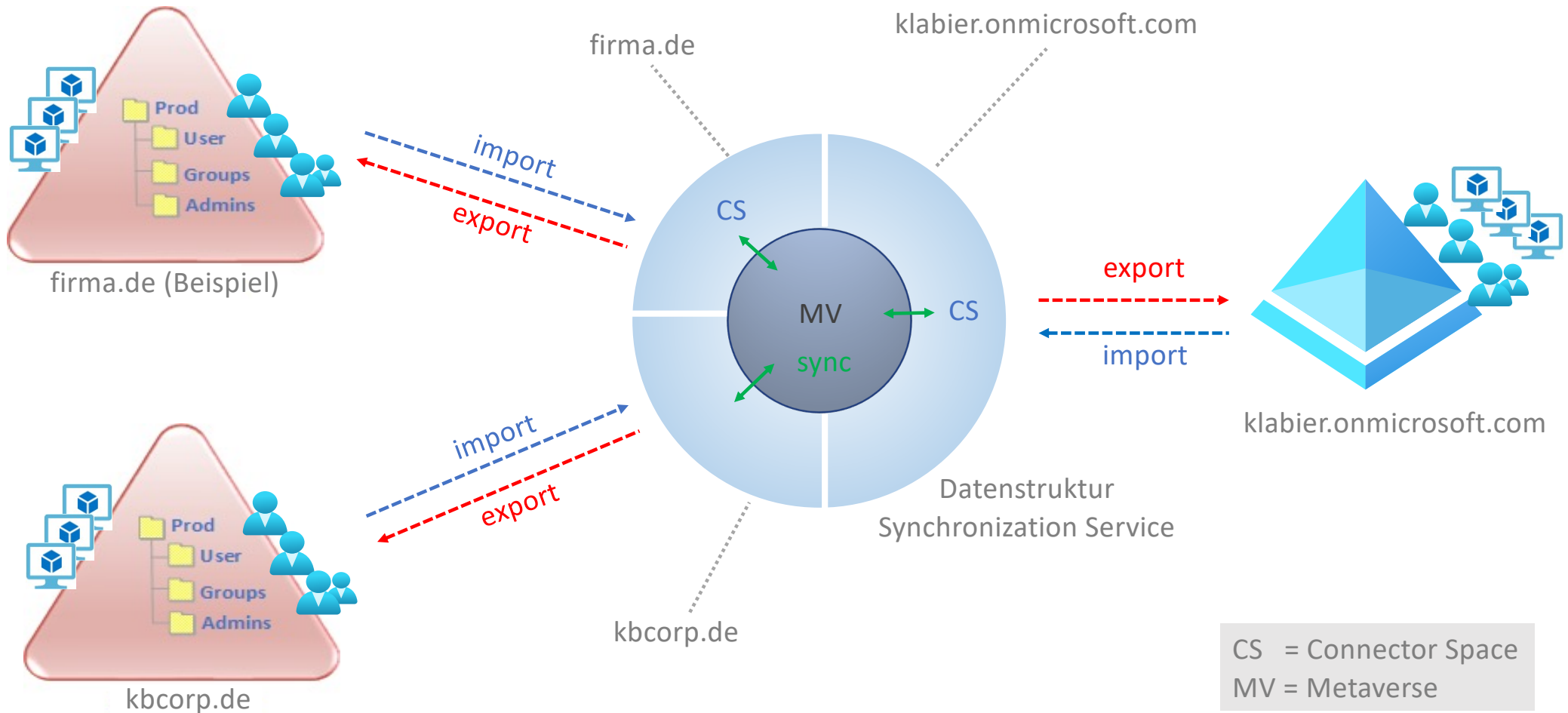
Profile Name: Export User Name: NT SERVICE\ADSync

Step Type: Export **Partition:** DC=kbcorp,DC=de
Start Time: 07.06.2021 21:21:02 **End Time:** 07.06.2021 21:21:02 **Status:** success

Export Statistics		Connection Status	
Adds	0	dc3.kbcorp.de:389	success
Updates	0		
Renames	0		
Deletes	0		
Delete Adds	0		

2022 run(s)

Synchronisation – Schaltzentrale einer hybriden Infrastruktur



Synchronisation – Schaltzentrale einer hybriden Infrastruktur

The screenshot displays the Synchronization Service Manager interface. The main window shows a list of connector operations with columns for Name, Profile Name, Status, Start Time, and End Time. A semi-transparent grey box with the text "OK, verstehe ..." and a smiling face with glasses emoji is overlaid on the table. Below the table, the details for a specific operation are shown, including Step Type, Start Time, Partition, End Time, and Status. A table of Export Statistics and Connection Status is also visible.

Name	Profile Name	Status	Start Time	End Time
kbcorp.de	Export	success	07.06.2021 21:21:02	07.06.2021 21:21:02
klabier.onmicrosoft.co...	Export	success	07.06.2021 21:20:53	07.06.2021 21:21:01
klabier.onmicrosoft.co...	Delta Synchronization	success	07.06.2021 21:20:53	07.06.2021 21:20:53
kbcorp.de	Delta Synchronization	success	07.06.2021 21:20:52	07.06.2021 21:20:52
klabier.onmicrosoft.co...	Delta Import	success	07.06.2021 21:20:47	07.06.2021 21:20:52
kbcorp.de	Delta Import	success	07.06.2021 21:20:46	07.06.2021 21:20:47
kbcorp.de	Export	success	07.06.2021 20:51:00	07.06.2021 20:51:00
klabier.onmicrosoft.co...	Export	success	07.06.2021 20:50:52	07.06.2021 20:51:00
klabier.onmicrosoft.co...	Delta Synchronization	success	07.06.2021 20:50:51	07.06.2021 20:50:52
kbcorp.de	Delta Synchronization	success		
klabier.onmicrosoft.co...	Delta Import	success		
kbcorp.de	Delta Import	success		
kbcorp.de	Export	success		
klabier.onmicrosoft.co...	Export	success	07.06.2021 20:20:52	07.06.2021 20:21:01
klabier.onmicrosoft.co...	Delta Synchronization	success	07.06.2021 20:20:52	07.06.2021 20:20:52
kbcorp.de	Delta Synchronization	success	07.06.2021 20:20:51	07.06.2021 20:20:52
klabier.onmicrosoft.co...	Delta Import	success	07.06.2021 20:20:46	07.06.2021 20:20:51
kbcorp.de	Delta Import	success	07.06.2021 20:20:46	07.06.2021 20:20:46
kbcorp.de	Export	success	07.06.2021 20:18:25	07.06.2021 20:18:25
klabier.onmicrosoft.co...	Export	success	07.06.2021 20:18:17	07.06.2021 20:18:25

Profile Name: Export User Name: NT SERVICE\ADSync

Step Type: Export **Partition:** DC=kbcorp,DC=de
Start Time: 07.06.2021 21:21:02 **End Time:** 07.06.2021 21:21:02 **Status:** success

Export Statistics		Connection Status	
Adds	0	dc3.kbcorp.de:389	success
Updates	0		
Renames	0		
Deletes	0		
Delete Adds	0		

2022 run(s)

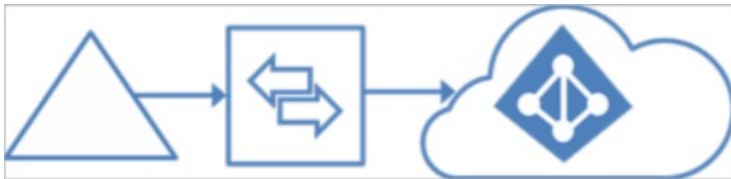
Synchronisation – Schaltzentrale einer hybriden Infrastruktur

Unterstützte Szenarien in einer Gesamtstruktur

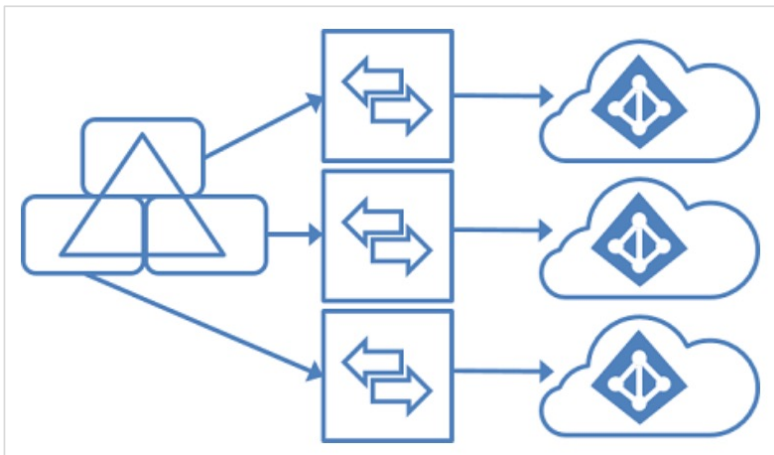
Supported

Unsupported

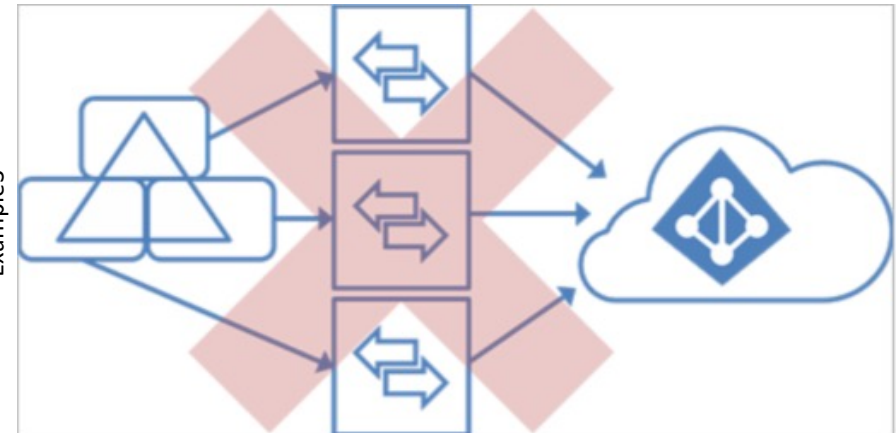
Example1



Example2



Example3

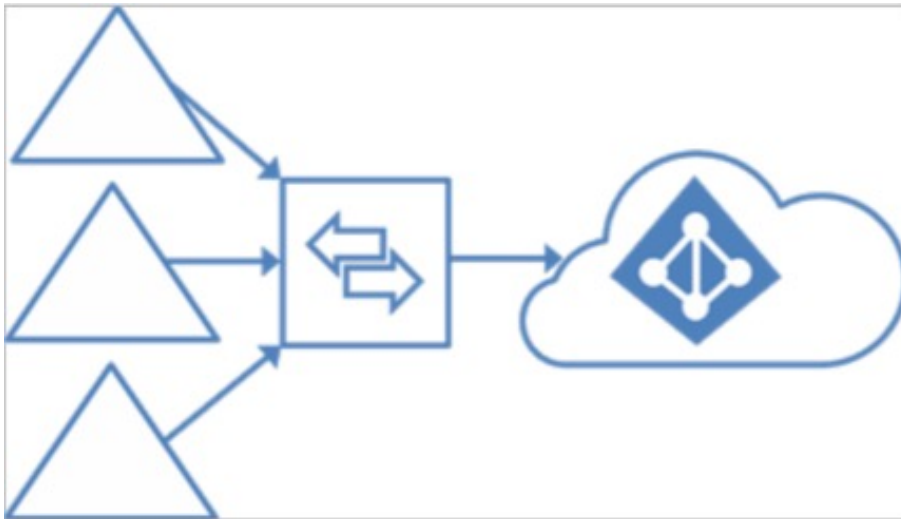


Weitere Details zu unterstützten Szenarien ([link](#))

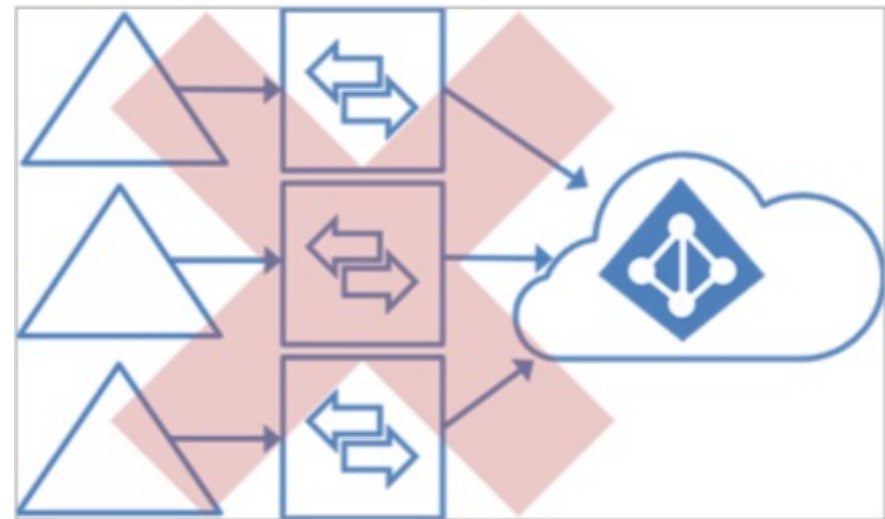
Synchronisation – Schaltzentrale einer hybriden Infrastruktur

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

Selektieren der OUs einer Domäne

Transformieren von Attributen

Filterung auf Basis von Attributen

Azure AD Connect Setup Assistent (Demo 😊)

Azure AD Connect Rule Editor

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:

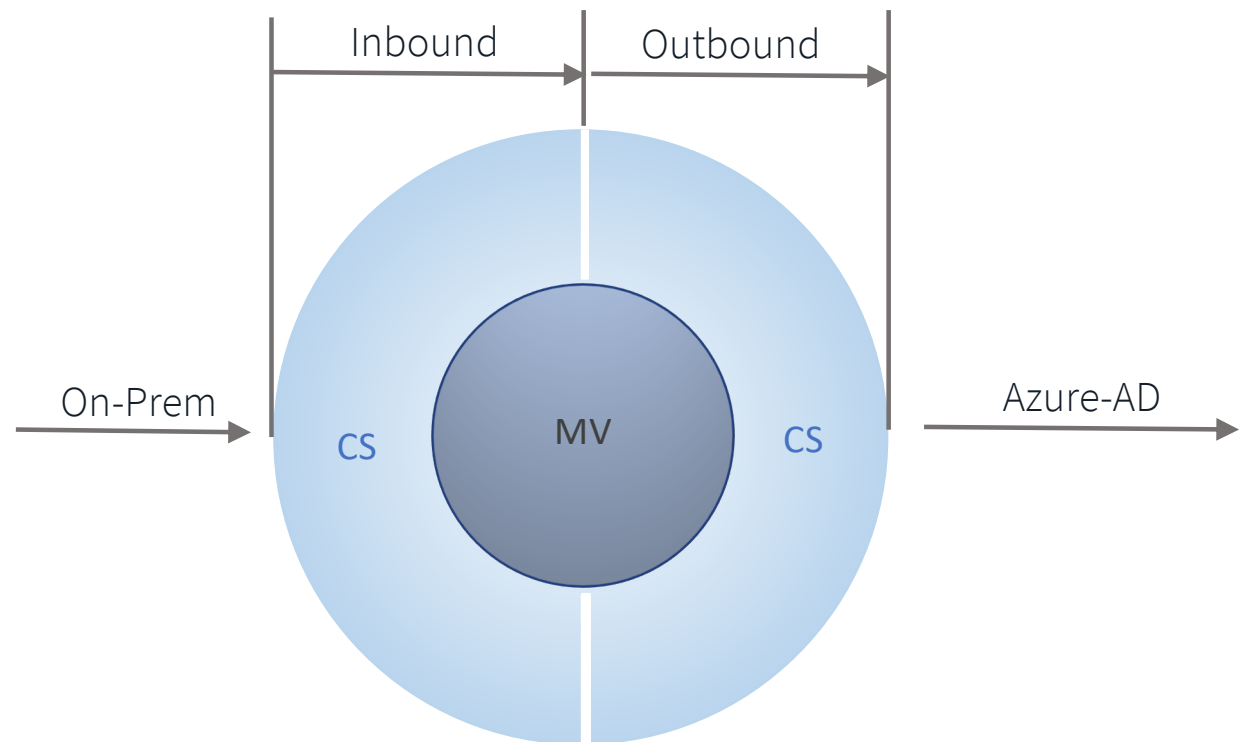
givenName=UCase ([givenName])

Filterung:

MV Attribute:

cloudFiltered = true/false

positiv / negativ möglich



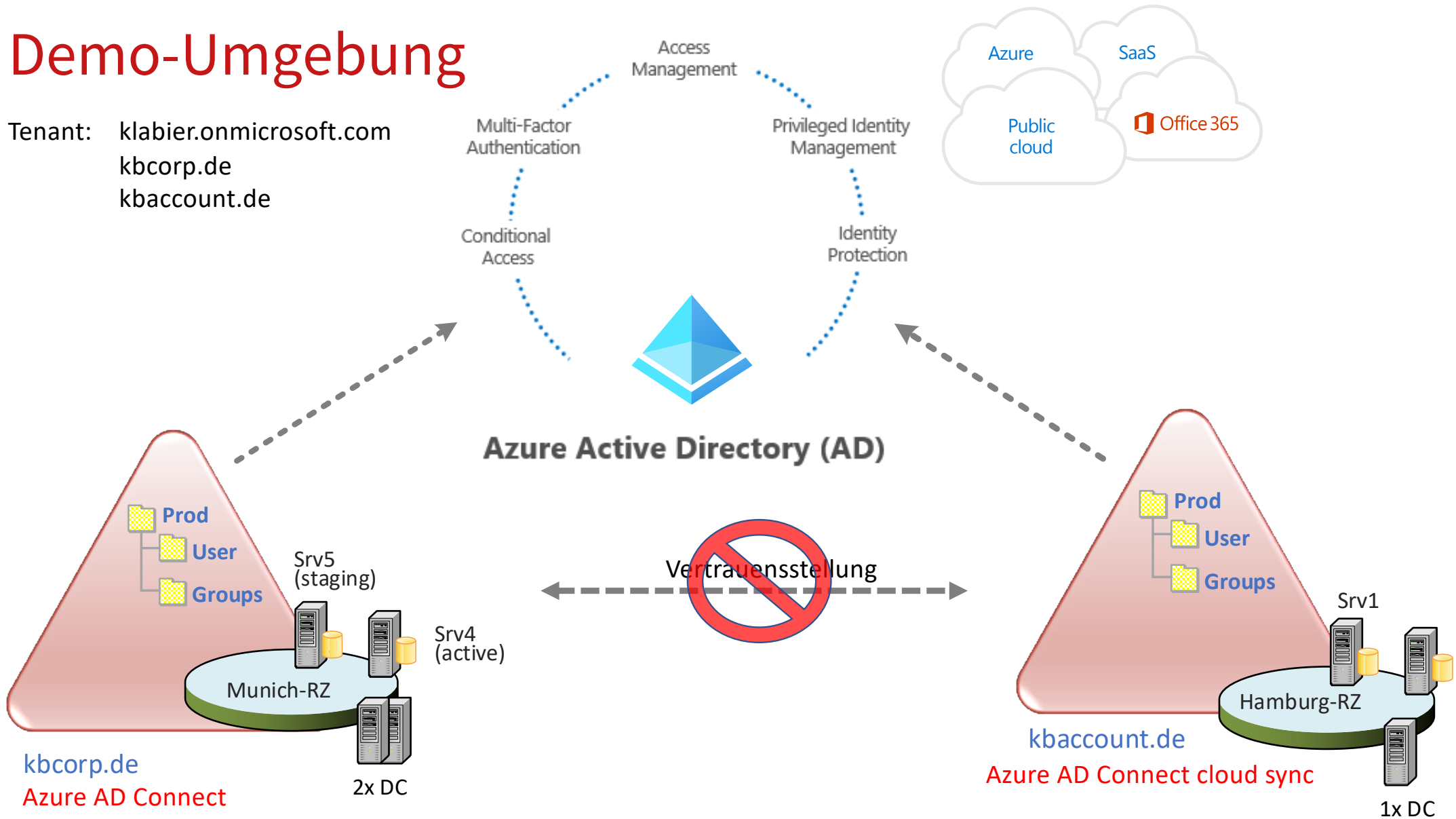
Synchronisation – Schaltzentrale einer hybriden Infrastruktur

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 existing database 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

The screenshot displays the AAD Connect Sync Service Configuration interface. At the top, there are navigation icons and a breadcrumb path: C:\AADDocumenter\Report\KBCORP_Srv5_AppliedTo_KBCORP_Srv4_AADConnectSync_repr. Below this, a list of 'Out to AAD' profiles is shown, including AzureRMS, DynamicsCRM, LyncOnline, and SharePointOnline for both Groups and Users. A 'Run Profiles' section lists various synchronization tasks like Delta Import, Full Import, and Specific Object Export/Import.

AAD Connect Sync Service Configuration

Global Settings

Setting	Value
Microsoft.AADFilter.ApplicationList	ExchangeOnline,Identity,Intune,OfficeProPlus
Microsoft.OptionalFeature.DirectoryExtension	TrueFalse
Microsoft.Synchronize.NextStartTime	Tue, 08 Jun 2021 15:13:52 GMTTue, 08 Jun 2021 15:05:08 GMT
Microsoft.Synchronize.StagingMode	FalseTrue
Microsoft.UserSignIn.DesktopSsoEnabled	TrueFalse

Metaverse Configuration

Metaverse Object Types

person

Attribute	Type	Multi-valued	Indexed	Precedence			Scoping Condition			
				Rank	Connector	Inbound Sync Rule	Source	CS Attribute	Operator	Value
				1	kbcorp.de	NegativeRuleExample	True	description	EQUAL	dontsync
				1	kbcorp.de	In from AD - User Positive Rule Set	False	userPrincipalName	ENDSWITH	@kbcorp.de
								mail	ISNOTNULL	

IF([isPresent([SAMAaccountName]) = False || [SAMAaccountName] =

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

DISTINGUISHEDNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION
CN=Ada Lauritzen,OU=Cust...	user	mail	topleveldomain	lauritzen@kbcorp.local	lauritzen@kbcor...	EDIT
CN=Ada Lauritzen,OU=Cust...	user	targetAddress	blank		SMTP:lauritzen...	REMOVE
CN=Ada Lauritzen,OU=Cust...	user	mailnickname	blank		AdaLauritzen	REMOVE
CN=Adrian Godin,OU=Cust...	user	mailnickname	blank		AdrianGodin	COMPLETE
CN=Adrian Godin,OU=Cust...	user	targetAddress	blank		SMTP:Adrian@...	
CN=Alfred Trice,OU=CustA...	user	mailnickname	blank		AlfredTrice	
CN=Alfred Trice,OU=CustA...	user	targetAddress	blank		SMTP.mail1@k...	
CN=Allan Krebs,OU=CustA...	user	mailnickname	blank		AllanKrebs	
CN=Allan Krebs,OU=CustA...	user	targetAddress	blank		SMTP.mai998l...	EDIT
CN=Alma Rogers,OU=Cust...	user	targetAddress	blank		SMTP.blabla@k...	REMOVE
CN=Alma Rogers,OU=Cust...	user	mailnickname	blank		AlmaRogers	COMPLETE
CN=America Tibbetts,OU=C...	user	mailnickname	blank		AmericaTibbetts	
CN=America Tibbetts,OU=C...	user	targetAddress	blank		SMTP.newmail...	
CN=Amy Martinez,OU=Cust...	user	mailnickname	blank		AmyMartinez	

Query Count: 21 Error Count: 35

Synchronisation – Schaltzentrale einer hybriden Infrastruktur

Microsoft Azure Active Directory Connect

Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure

Uniquely identifying your users

Select how users should be identified in your on-premises directories. ?

- Users are represented only once across all directories.
- User identities exist across multiple directories. Choosing:
 - Mail attribute
 - ObjectSID and msExchMasterAccountSID/msRTCSIP-Original
 - SAMAccountName and MailNickName attributes
 - A specific attribute

Select how users should be identified with Azure AD. ?

- Let Azure manage the source anchor
- Choose a specific attribute
 - mS-DS-ConsistencyGuid

Azure is currently synchronized using mS-DS-ConsistencyGuid and will continue to use this source anchor for your on-premises users. [Learn more](#)

Previous Next

Users are created as individuals in Azure AD Objects are not joined in the metaverse

Default and best option