



CLOUD IDENTITY SUMMIT '21

Identity Integration Track

“Error-free with hybrid
synchronization”

Klaus Bierschenk (CGI Deutschland)

Community Event



Error-free with hybrid synchronization

About me:

I live in beautiful Murnau am Staffelsee, 45min south of Munich

- Executive Consultant at CGI Deutschland
- Part time technical journalist, technical writer in print and online media
- In the industry with experience in Identity and Active Directory for many years
- When I am offline, I spend my time in the mountains, with some kind of sports (trailrunning, MTB, etc.)



  @KlaBiers

Blog:
<https://nothingbutcloud.net/>



Error-free with hybrid synchronization

Agenda and key takeaways

- Technology overview and components
- Update Information
- Sources of error in synchronization
- Precautions - ensure that an sync environment stays healthy
- Free tools that make your life easier
- Demos...



Error-free with hybrid synchronization

Technology overview and components



Azure AD Connect

Copyright © 2015 Microsoft Corporation. All rights reserved.

- Azure AD Connect server
- On-Premises on specific boxes
- Multiple components; Security; SQL; Accounts; Synchronization

Full sync functionality

Troubleshooting is challenging

PROVISION FROM ACTIVE DIRECTORY



Azure AD cloud sync

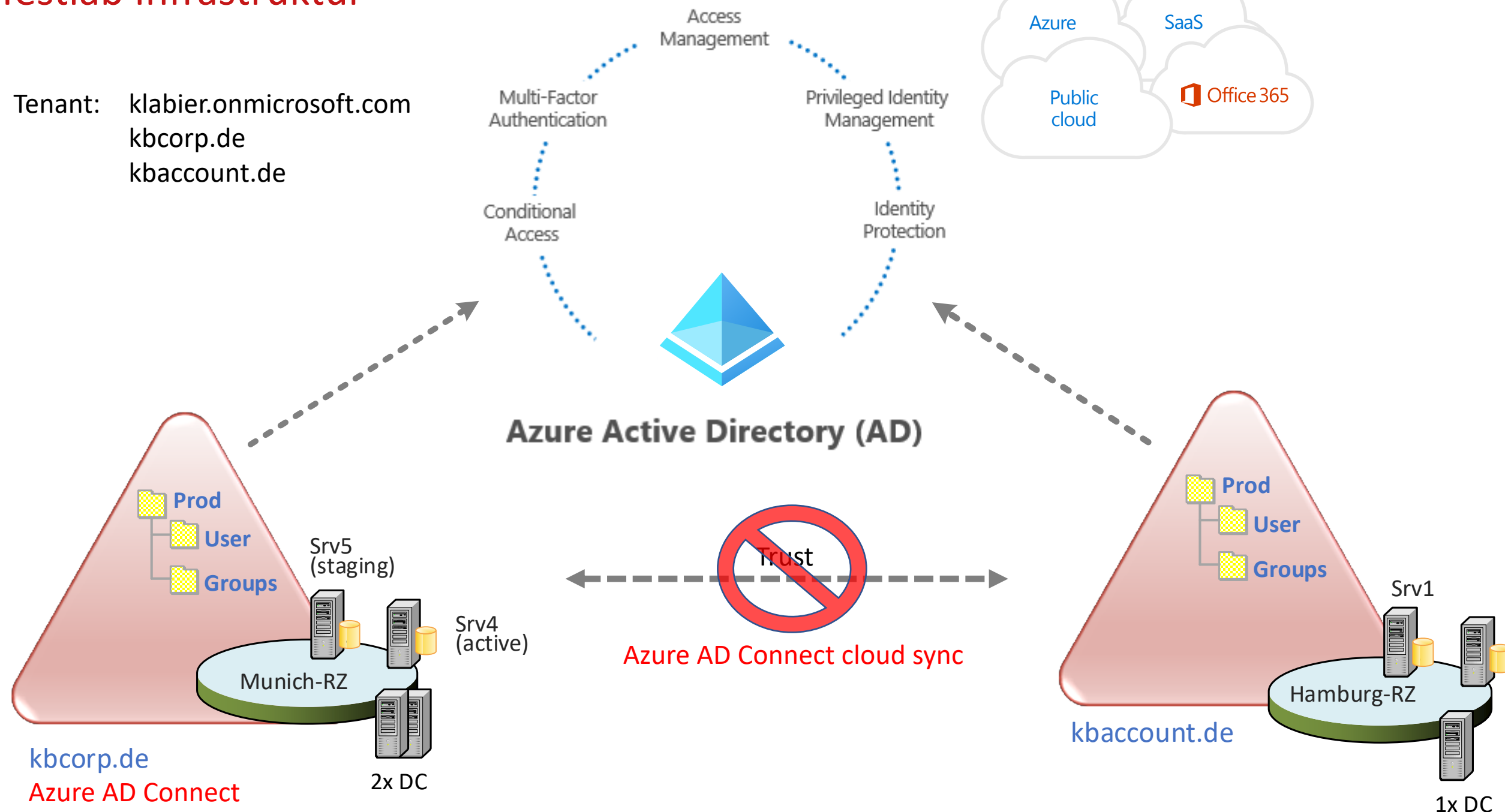
- Relatively new technology (GA 2020)
- Just simple agent On-Premises
- Management from the cloud (Azure AD Portal)

Subset of sync functionalities

Troubleshooting less complex

Testlab Infrastruktur

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



Error-free with hybrid synchronization

Function	Azure AD Connect	AAD cloud sync
Where is Configuration stored?	Locale Server (SQL)	Azure
Is Central management from the Azure Portal possible		✓
Support for disconnected forests		✓
Filtering on attribute level	✓	
"Simple" filtering based on group membership		✓
Write back from Azure AD (password, groups (Exch. Online), devices)	✓	
On-Premises Agent is highly available		✓
Synchronization of custom-specific attributes	✓	
Installing the on-prem agents on a domain controller	✓	✓
Support for Pass-Thru Authentication (PTA)	✓	
Powershell Support	✓	✓

Error-free with hybrid synchronization

Keep it up to date – multiple updates a year

AAD Connect Server

Azure AD Connect Server update (no Agent update)

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-version-history>

manually possible

Azure AD Connect Health

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-health-version-history>

Azure AD Pass-through Authentication agent

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-pta-version-history>

Cloud sync

Azure AD Connect cloud provisioning agent

<https://docs.microsoft.com/de-de/azure/active-directory/cloud-sync/reference-version-history>

Error-free with hybrid synchronization

AAD Connect Server V2 update

Update very simple; In-Place possible (W2K16)

Enable TLS 1.2 on Server manually

MSAL instead of ADAL

No changes with functionalities but:

- Windows Server 2016+ is required and
- SQL Server 2019 Local DB part of the setup

AADC V2 is still free but Health still requires P1

To consider ... 🤔

AADC V1 retired 22/08, ADAL support end in 22/06

SQL Server 2012 components remains on box

Consider fresh new box with JSON import from V1

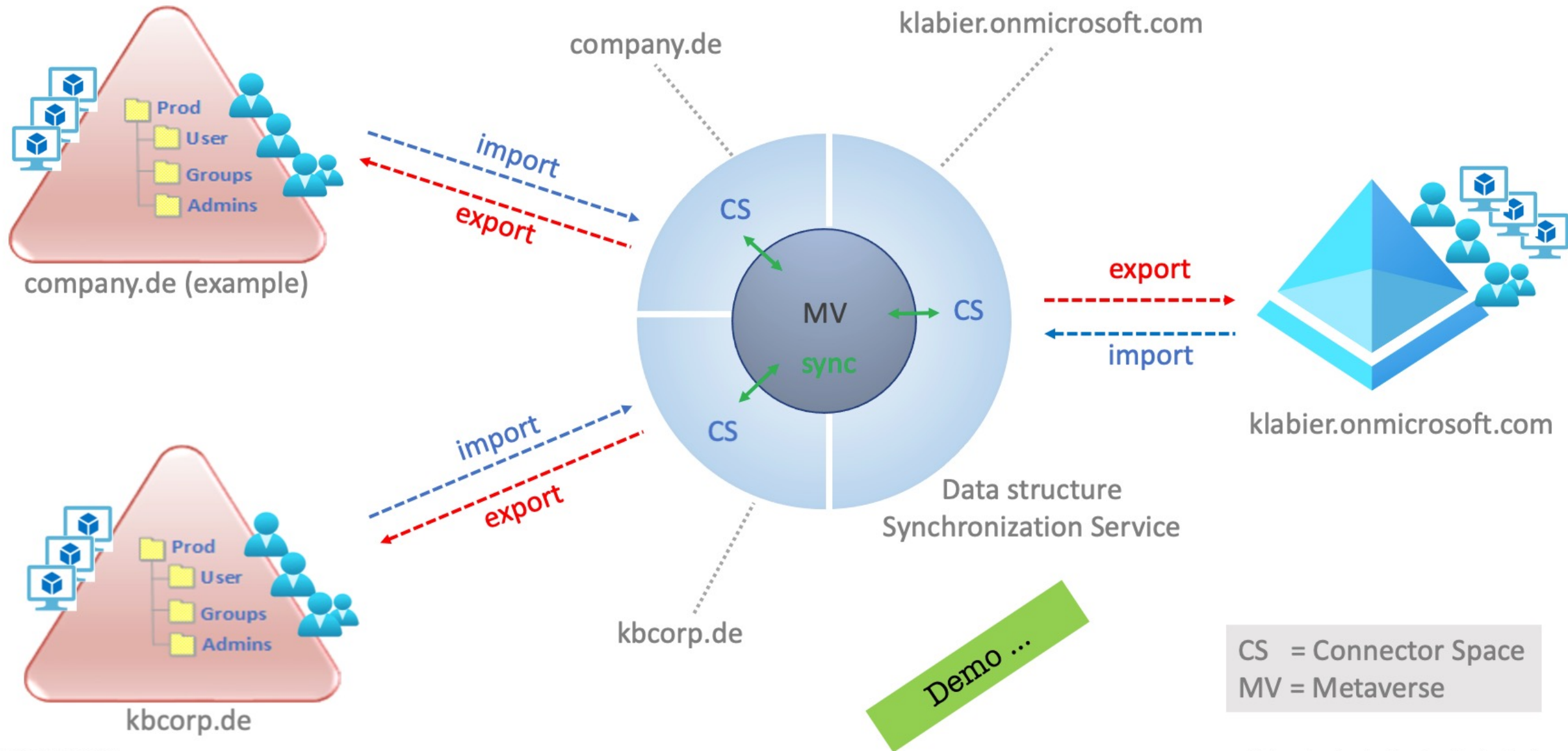
Export config on v1.x and import in v2.x

Upgrade from any AAD Connect Version possible

No automatic update, even when Autoupgrade=on

main article as starting point can be found [here](#)

Error-free with hybrid synchronization



Error-free with hybrid synchronization

Sources of errors – update and switch staging / active



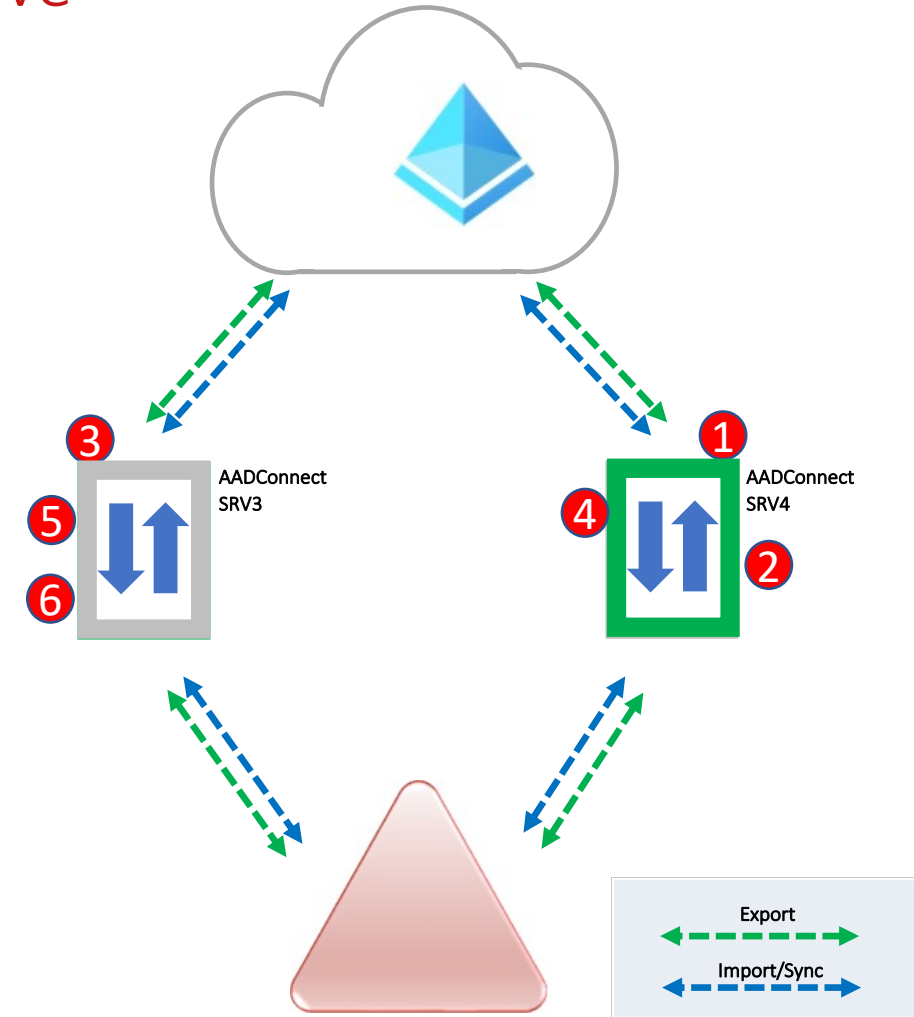
Key facts - staging and config

- ✓ Each AADC has own config
 - AADC Setup Wizard
 - Filtering rules
- ✓ Multiple staging possible
- ✓ Sync cycles independent
- ✓ Staging procedures in ops guide
- ✓ Extra staging for rules developpe

Swing Migration ...

- 1 Update Staging
- 2 Health Check of updated staging
- 3 Make active a Staging viceversa
- 4 Make some export check
- 5 Update „new“ staging
- 6 Don't forget a final health check

demo



Error-free with hybrid synchronization

Sources of errors – switch staging, pending exports



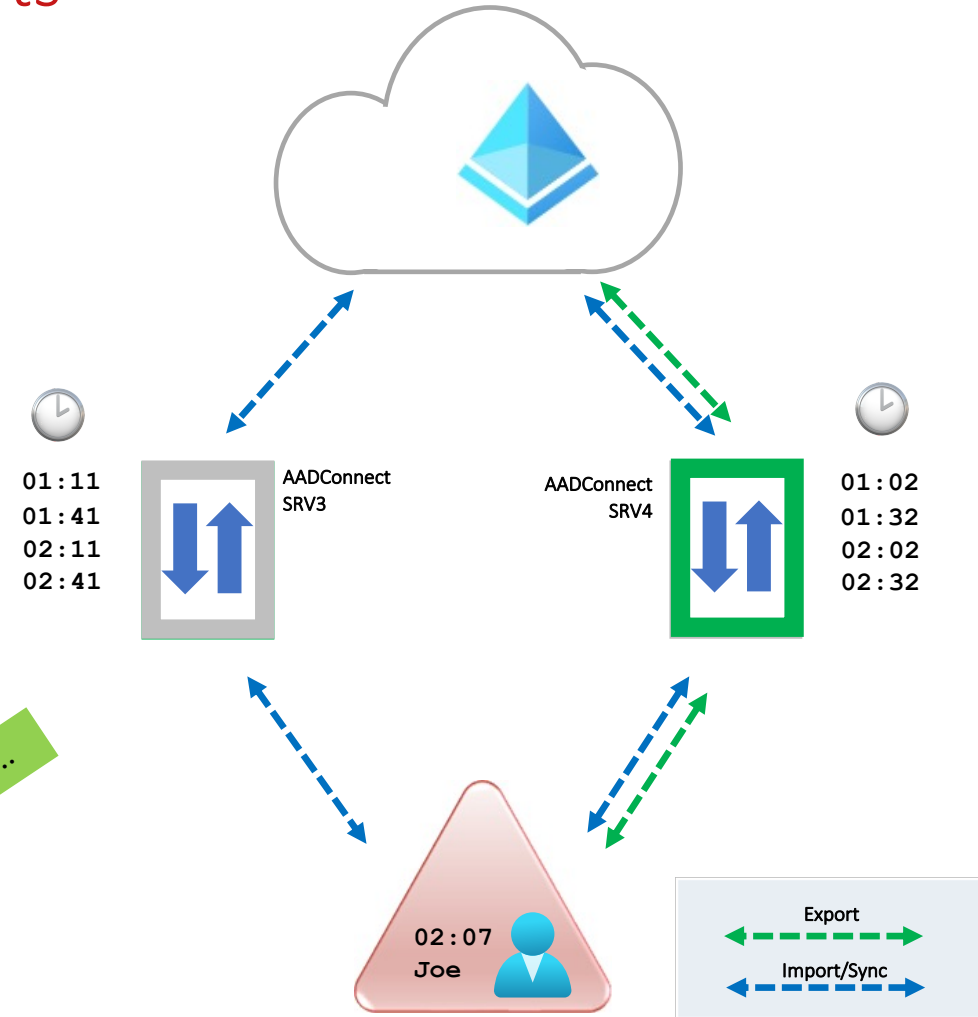
Key facts - staging and config

- ✓ Each AADC has own config
 - AADC Setup Wizard
 - Filtering rules
- ✓ Multiple staging possible
- ✓ Sync cycles independent
- ✓ Staging procedures in ops guide
- ✓ Extra staging for rules developpe

Pending export example ...

02:02 - srv4 run sync
02:07 – User Joe is created in AD
02:11 – srv3 run sync
Object „Joe“ is pending
02:32 - srv4 run sync
02:41 – srv3 run sync
**„Joe“ imported from AAD
and not longer pending**

Demo ...



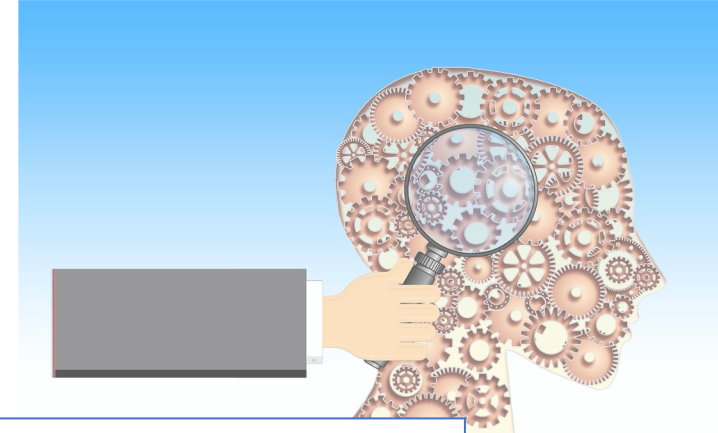
Error-free with hybrid synchronization

Sources of errors – identifying errors and diagnostics

AAD Connect Dashboard check as first option – both AADC & cloud sync

Demo ...

Powershell is your friend to find details – e.g. `Invoke-ADSyncDiagnostics`



Home > KBCORP Laboratory > Azure Active Directory Connect Health > klabier.onmicrosoft.com > SRV4 >

Azure Active Directory Connect (Sync) Alerts

klabier.onmicrosoft.com

🕒 Time Range

Name	Type	Scope	Raised	Last Detected	Resolved
Active Alerts					
No data found.					
Resolved Alerts					
No data found.					
Others					
Password Hash Synchronization heart...	❗ Error	SRV4	24.9.2021, 23:40:18	28.9.2021, 09:22:24	28.9.2021, 11:11:08

Error-free with hybrid synchronization

Sources of errors – identifying errors and diagnostics

Check errors on service level

Invoke-ADSyncDiagnostics

Demo ...

Eventvwr.msc



```
PS C:\Users\administrator.KBCORP> Invoke-ADSyncDiagnostics -PasswordSync

=====
Password Hash Synchronization General Diagnostics
=====

AAD Tenant - klabier.onmicrosoft.com
Password Hash Synchronization cloud configuration is enabled

False

AD Connector - kbcorp.de
Password Hash Synchronization is enabled
Latest Password Hash Synchronization heartbeat is detected at: 09/28/2021 09:08:42 UTC

Directory Partitions:
=====
Directory Partition - kbcorp.de
Password Hash Synchronization agent is continuously getting failures for domain "kbcorp.de"
Please check 611 error events in the application event logs for details
The latest 611 error event for the domain "kbcorp.de" is generated at: 09/28/2021 08:06:40 UTC

True
AD Connector account had a Password Hash Synchronization permission problem for the domain "kbcorp.de" at: 09/28/2021 08:06:40 UTC
Please see: https://go.microsoft.com/fwlink/?linkid=847234
Please check 611 error events in the application event logs for details

False
False
Last successful attempt to synchronize passwords from this directory partition started at: 9/28/2021 9:14:42 AM UTC and ended at: 9/28/2021 9:14:43 AM UTC

Only Use Preferred Domain Controllers: False
Checking connectivity to the domain...
Domain "kbcorp.de" is reachable

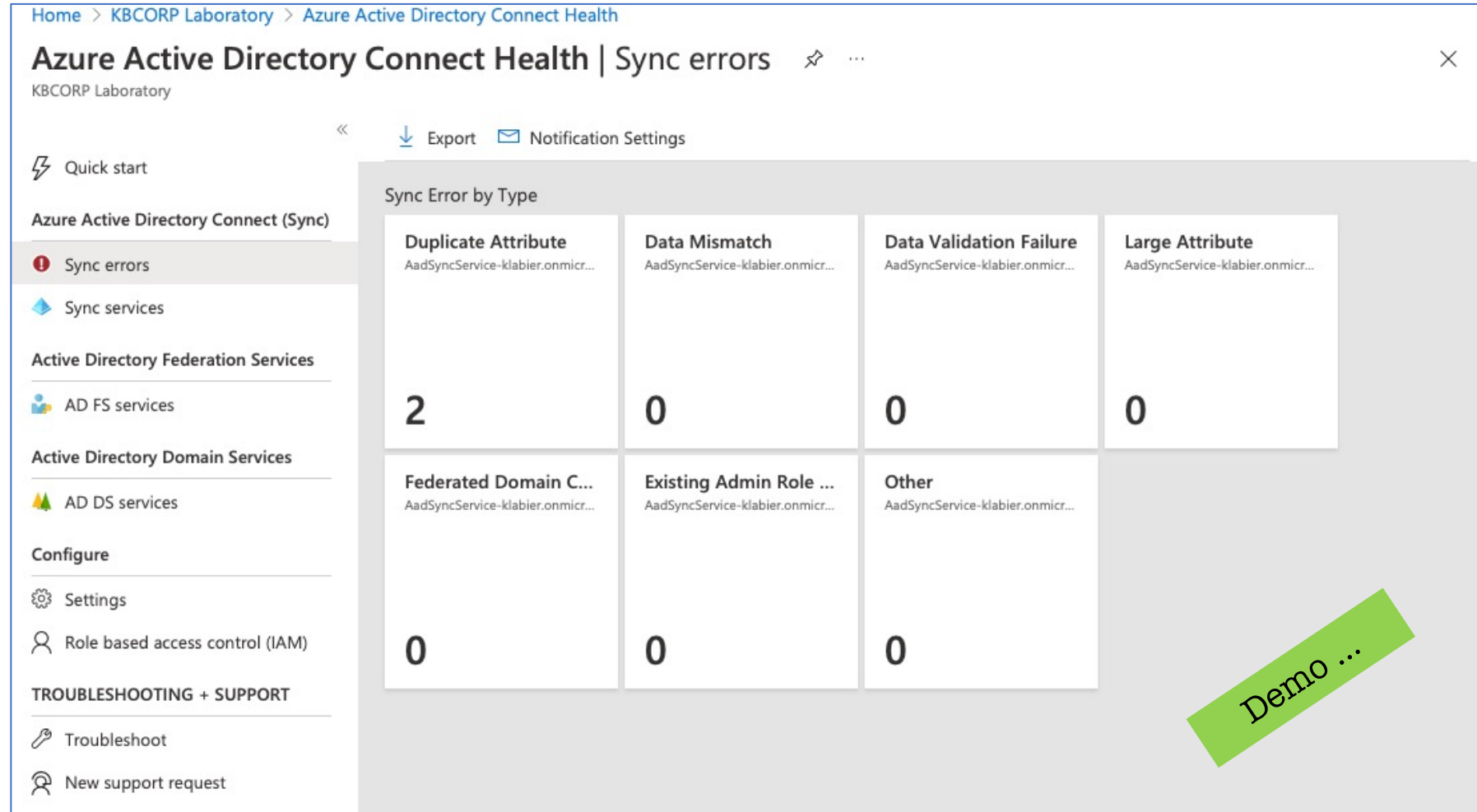
Did you find Password Hash Sync General Diagnostics helpful? [y/n]:
```

Error-free with hybrid synchronization

Sources of errors – synchronization errors / identities

Check errors on sync level

Errors must be fixed on object level



The screenshot shows the Azure Active Directory Connect Health interface for 'KBCORP Laboratory'. The main heading is 'Azure Active Directory Connect Health | Sync errors'. The left sidebar contains navigation options: Quick start, Azure Active Directory Connect (Sync), Active Directory Federation Services, Active Directory Domain Services, Configure, and TROUBLESHOOTING + SUPPORT. The 'Sync errors' section is active, showing a 'Sync Error by Type' table.

Sync Error by Type	Count
Duplicate Attribute	2
Data Mismatch	0
Data Validation Failure	0
Large Attribute	0
Federated Domain C...	0
Existing Admin Role ...	0
Other	0

A green diagonal banner in the bottom right corner of the screenshot reads 'Demo ...'.



Error-free with hybrid synchronization

Free tools which makes your life easier: AADConnectDocumenter

Compares two server configurations

Create dump: `Get-ADSyncServerConfiguration -Path "<CompletePathToOutputFolder>"`

Mandatory before switching from Staging to Active

Good understanding of Sync Engine terminology is desirable to understand report

Good options to export/transfer sync rules

Well suited for document AAD Connect Server

Download and Whitepaper:

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

Error-free with hybrid synchronization

The screenshot shows the AAD Connect Config tool interface. At the top, there's a file explorer path: C:\AADDocumenter\Report\KBCORP_Srv5_AppliedTo_KBCORP_Srv4_AADConnectSync_repr. Below this, there are several red text links for 'Out-to-AAD' configurations for different groups and users. A 'Run Profiles' section lists various synchronization profiles like 'Delta Import', 'Delta Synchronization', 'Export', 'Full Import', 'Full Synchronization', 'Specific Object Export', and 'Specific Object 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 GMT Tue, 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	

IIF(IsPresent([sAMAccountName]) = False || [sAMAccountName] =

Demo ...

Error-free with hybrid synchronization

Free tools which makes your life easier: idFix

Checks objects (on-prem) with error report, to identify what can cause problems in Azure AD / M365

Changes directly in the GUI ...

... or via CSV import

Be careful with bulk updates

... but context of the ops user can be changed

Each write operation creates LDIF for undo

Verbose report with details to write activities

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

Error-free with hybrid synchronization

Frequent tasks - ensure that an sync environment stays healthy

Always update

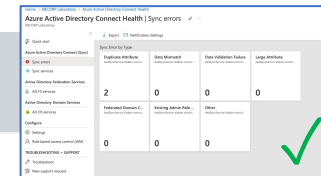
Integrate Sync into monitoring solution

Switch staging and active regularly-> You will not forget when you have it in the operational manual

Check the dashboard to see if there is an unnormal number of synchronization issues

Integrating Azure AD Connect Documenter checks also into frequent operational procedures

Check and play with the Powershell modules for learning and to find new helpful cmdlets ...



Error-free with hybrid synchronization

Continue reading...

General:

[Azure AD Pricing \(AAD Connect / Health included\)](#)

[Azure AAD Connect V2 - major changes](#)

Setup:

[Use existingdatabase switch - install Database](#)

[Use existingdatabase switch - Move Database](#)

[Supported Scenarios](#)

[Endpoint Update with not AADC V2](#)

[Swing Migration Update Method](#)

[Move Azure AD Connect database from SQL Server Express](#)

Security:

[AADConnectConfigDocumenter](#)

[Hardening Service Accounts from AADConnect - Account permissions](#)

[Hardening Service Accounts from AADConnect - connector accounts](#)

[Check for pending exports](#)

Troubleshooting:

[Supported scenarios](#)

[Troubleshooting object synchronization](#)

Cloud sync

[Start to find out what is possible with Cloud provisioning](#)

[Troubleshooting cloud sync](#)

Utilities:

[IdFix: Guide and Download](#)

[AADConnectConfigDocumenter](#)

Azure AD Connect 1.5.30.0 – V2 API Deployment

[Azure AD Connect sync V2 endpoint API](#)

Bonbon

[FIM/MIM Link Collection \(Huge list! Not totally new but perfect to understand FIM/MIM/Sync\)](#)



CLOUD IDENTITY SUMMIT '21

Your Feedback is Important!

<http://feedback.identitysummit.cloud/>

Community Event by



Azure Meetup

BONN

Follow us on Twitter



@identitysummit

The graphic features a central blue cloud with a white fingerprint icon. Below it, the text 'CLOUD IDENTITY SUMMIT '21' is displayed in white on a purple background. A blue banner below that contains the text 'Ask Me Anything (AMA)'. At the bottom, white text on a dark background invites attendees to a lounge session. The background is dark blue with several semi-transparent video call windows showing stylized avatars of people with various hair colors and styles. Some windows have speech bubbles or call icons. The overall theme is digital identity and community interaction.

CLOUD IDENTITY SUMMIT '21

Ask Me Anything (AMA)

JOIN THE CLOUD IDENTITY LOUNGE AT 8:00 PM (CEST)

Roundtable discussion and Q&A
on experiences from the field, current trends and more!
Interactive session to bring your questions and use the opportunity to
meet the speakers or exchange with members of the community!

Error-free with hybrid synchronization

Sources of errors – synchronization errors / is the object cloud filtered?

Do you know all your filtering rules?

Can be heavily complex. Want to learn more? Check [this](#) as a starting point

You miss an object in AAD?

Maybe it is filtered from synchronization

Demo ...

Filtering:

MV Attribute:

cloudFiltered = true/false

positive / negative possible



Error-free with hybrid synchronization

High availability with Azure AD Connect Server / Data storage

Is high availability really necessary?

No farm setup!! Each AAD Connect Server has own separate config

What actually happens when an AAD Connect server fails?

Staging Server concept -> Demo 😊 / check „pending exports“ before switch

Staging server challenge! Same Config important. AADConnectDocumenter in the backup slides

High availability for SQL can make sense

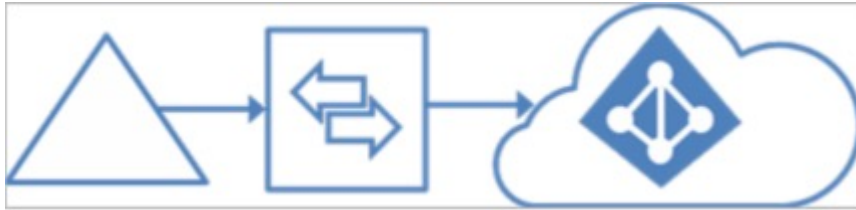
Setup with „*useexistingdatabase*“ switch (MS Docs link)

Error-free with hybrid synchronization

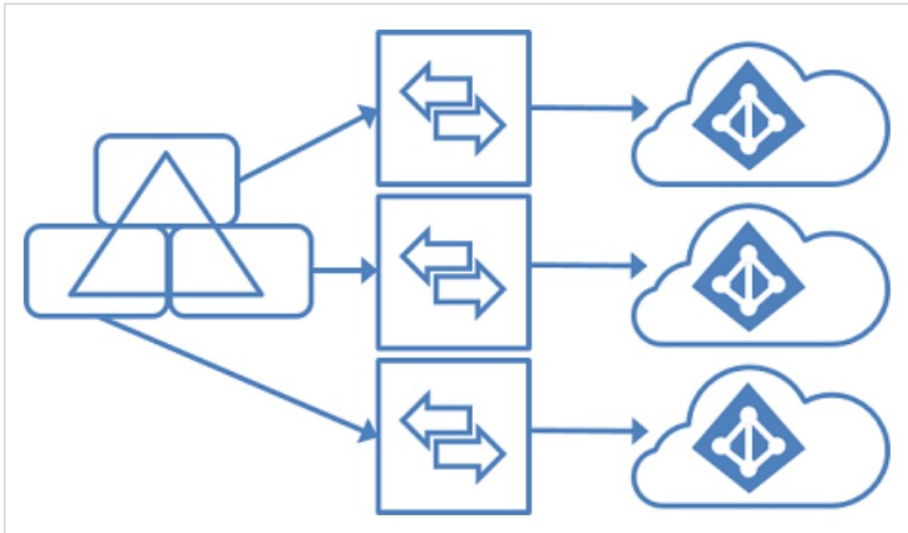
Supported and unsupported scenarios (one forest)

Supported

Example1

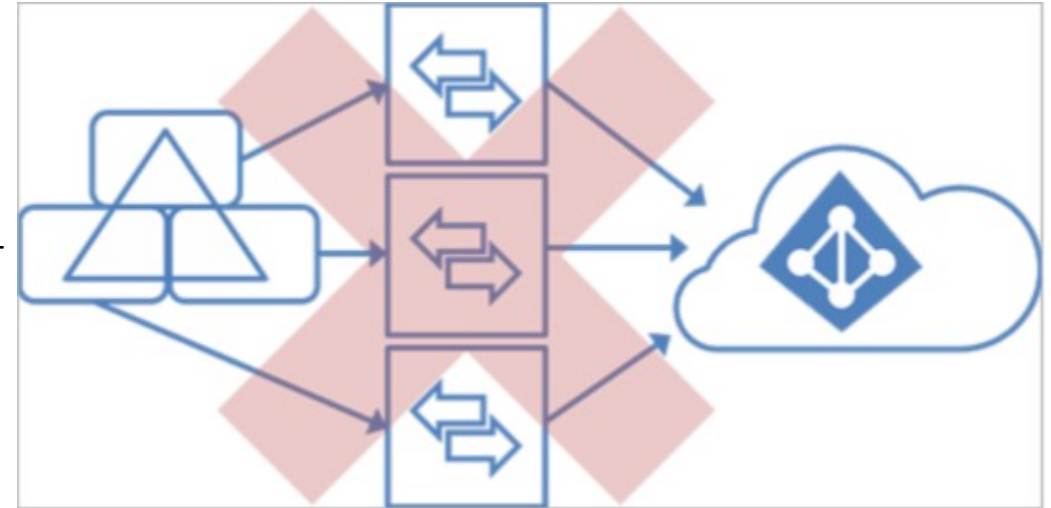


Example2



Unsupported

Example3

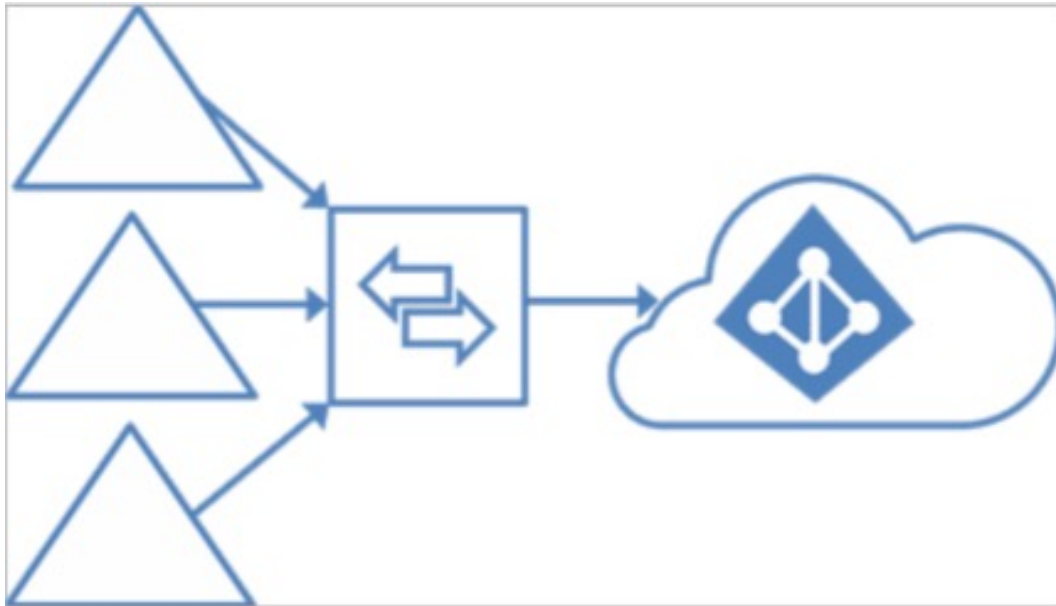


More details [link](#))

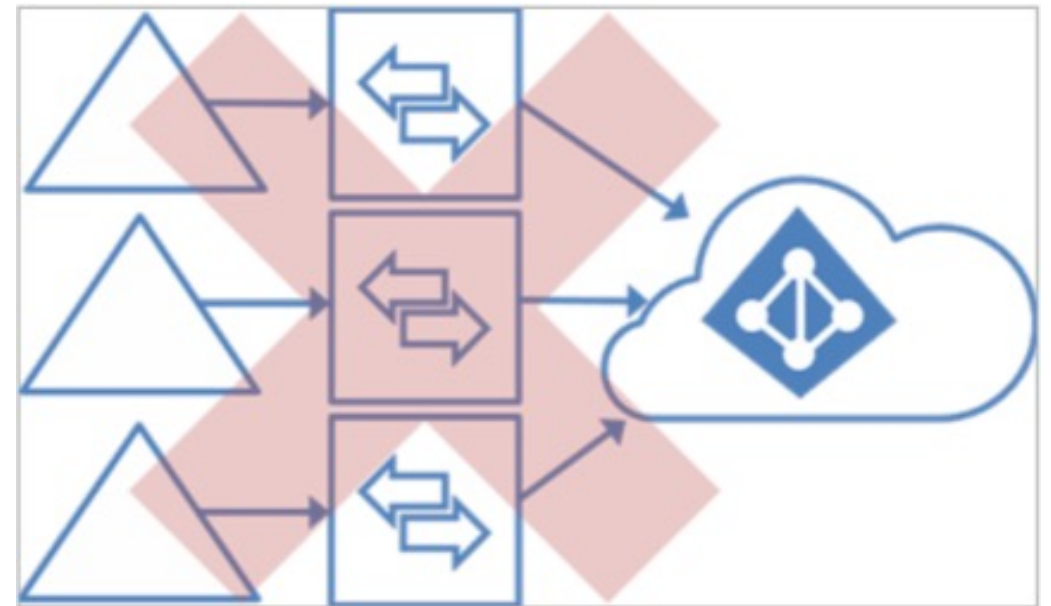
Error-free with hybrid synchronization

Supported and unsupported scenarios (multiple forest)

Supported



Unsupported



More details ([link](#))

Error-free with hybrid synchronization

The screenshot shows the 'Identifying users' step in the Microsoft Azure Active Directory Connect configuration wizard. The left sidebar contains navigation options: Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering, Identifying users (highlighted), Filtering, Optional Features, and Configure. The main content area is titled 'Uniquely identifying your users' and contains two sections. The first section, 'Select how users should be identified in your on-premises directories', has three radio button options: 'Users are represented only once across all directories.' (selected), 'User identities exist across multiple directories. Using:', and a third option. Under the second option, there are four sub-options: 'Mail attribute' (selected), 'ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginalSource' (disabled), 'SAMAccountName and MailNickName attributes' (disabled), and 'A specific attribute' (disabled). A dropdown menu is shown below these options. A red callout bubble points to the 'Users are represented only once across all directories.' option with the text: 'Users are created as individuals in Azure AD. Objects are not joined in the metaverse'. The second section, 'Select how users should be identified with Azure AD', has two radio button options: 'Let Azure manage the source anchor' and 'Choose a specific attribute' (selected). A dropdown menu below shows 'mS-DS-ConsistencyGuid'. A red callout bubble points to this dropdown with the text: 'Default and best option'. At the bottom, a status bar indicates: 'Azure is currently synchronized using mS-DS-ConsistencyGuid and will continue to use this as the source anchor for your on-premises users. Learn more'. Navigation buttons for 'Previous' and 'Next' are at the bottom right.

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. Using:
 - Mail attribute
 - ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginalSource
 - 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 as the source anchor for your on-premises users. [Learn more](#)

Previous Next

Error-free with hybrid synchronization

images in that slides are license free and from
Pixabay.com