CLOUD IDENTITY SUMMIT '21

Identity Integration Track

"Error-free with hybrid synchronization"

Klaus Bierschenk (CGI Deutschland)

Azure Meetup BONN

Error-free with hybrid synchronization

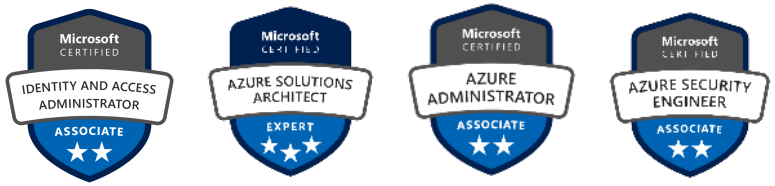
About me:

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…

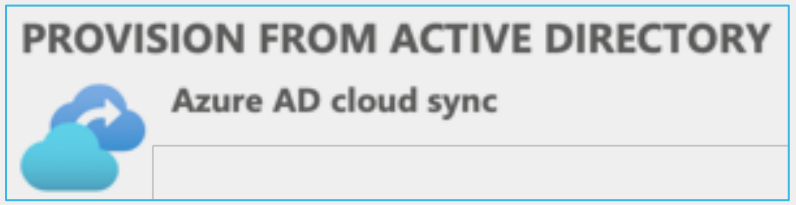
Error-free with hybrid synchronization

Technology overview and components

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

Full sync functionality

Troubleshooting is challenging



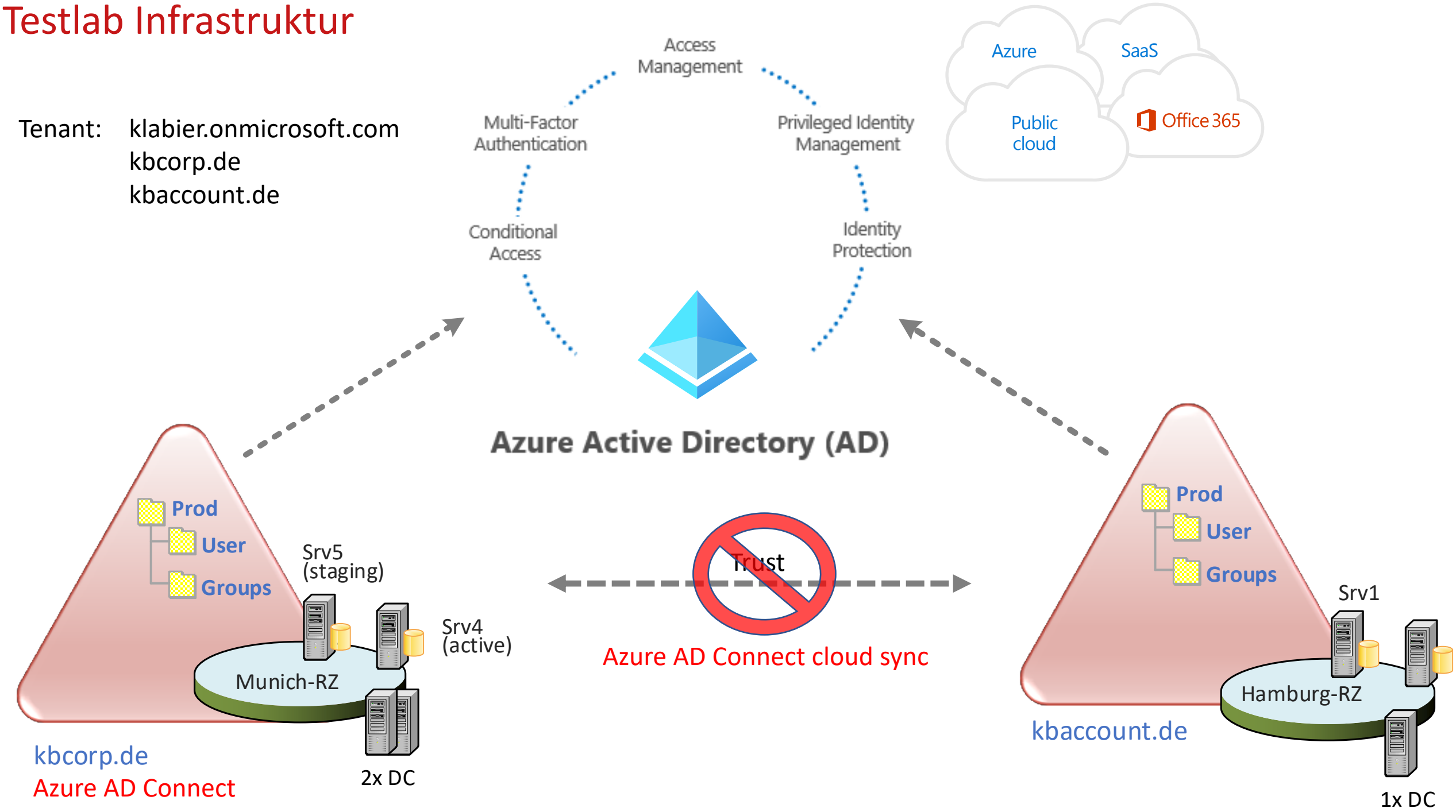
- Relatively new technology (GA 2020)
- Just simple agent On-Premises
- Management from the cloud (Azure AD Portal)

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)

manually possible

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

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

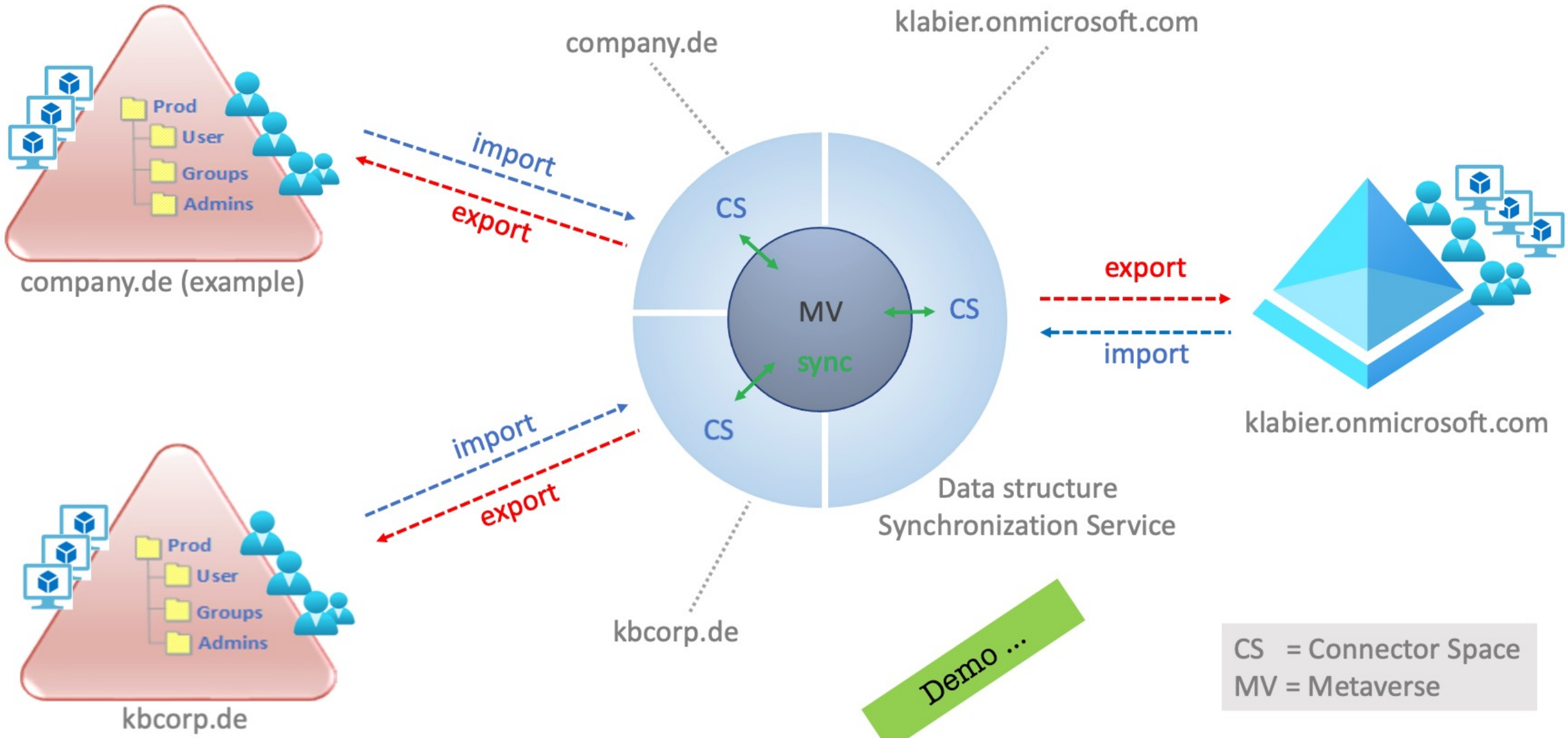
AAD Connect Server V2 update

- 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

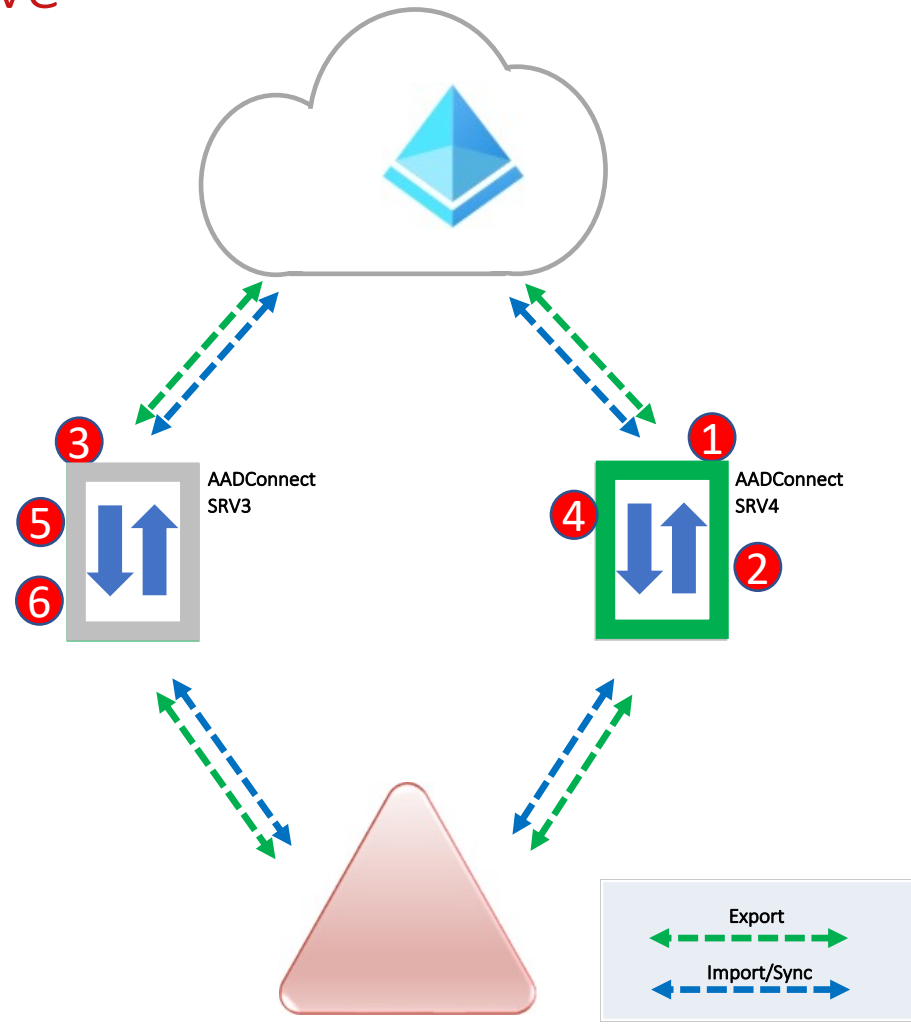
Key facts - staging and config

- ✓ 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 develope

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 develope

Pending export example …

02:02 - srv4 run sync

02:07 – User Joe is created in AD

02:11 – srv3 run sync

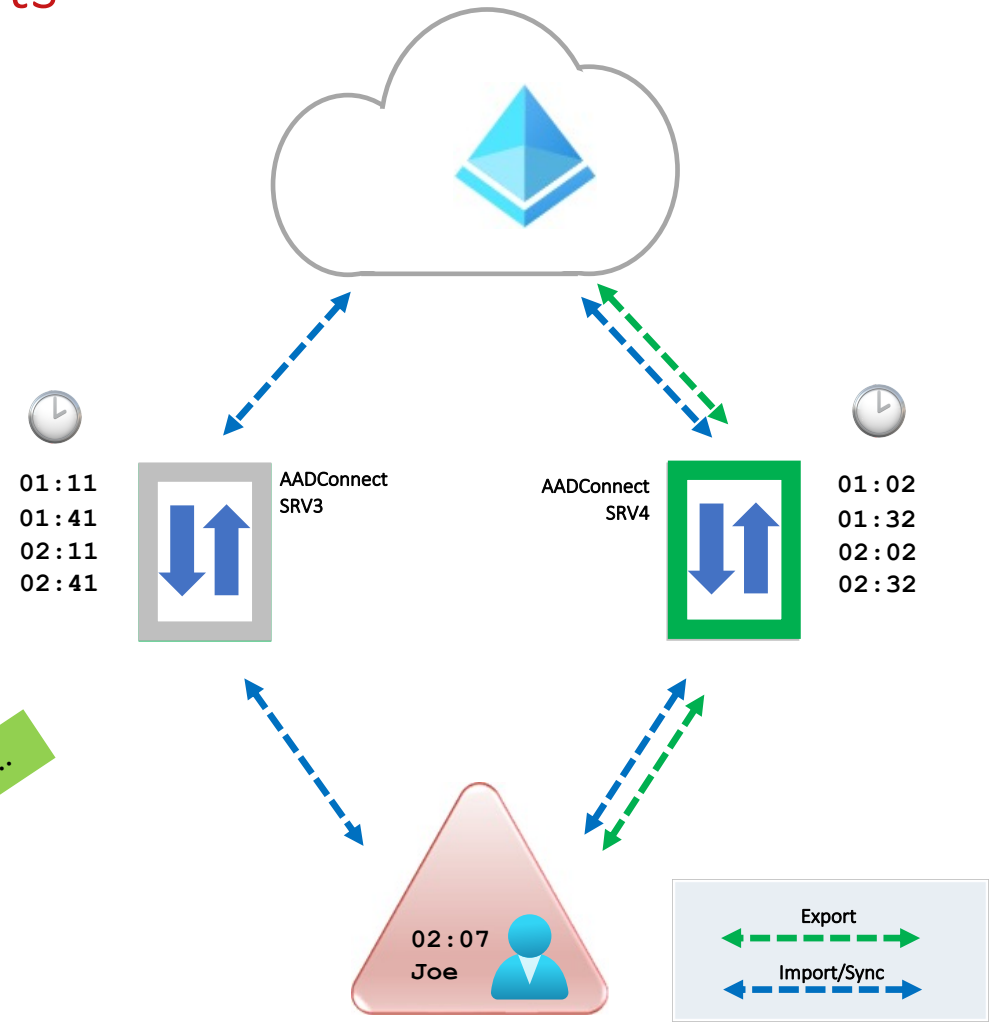
Object „Joe“ is pending

02:32 - srv4 run sync

02:41 – srv3 run sync

„Joe“ imported from AAD and not longer pending

Demo …

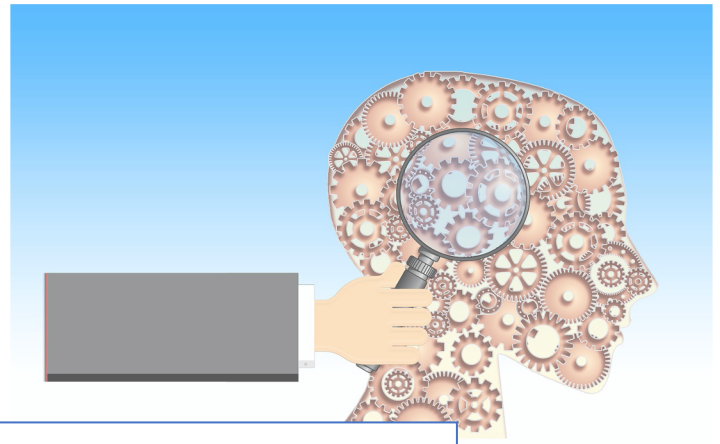


Error-free with hybrid synchronization

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

Find …

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`

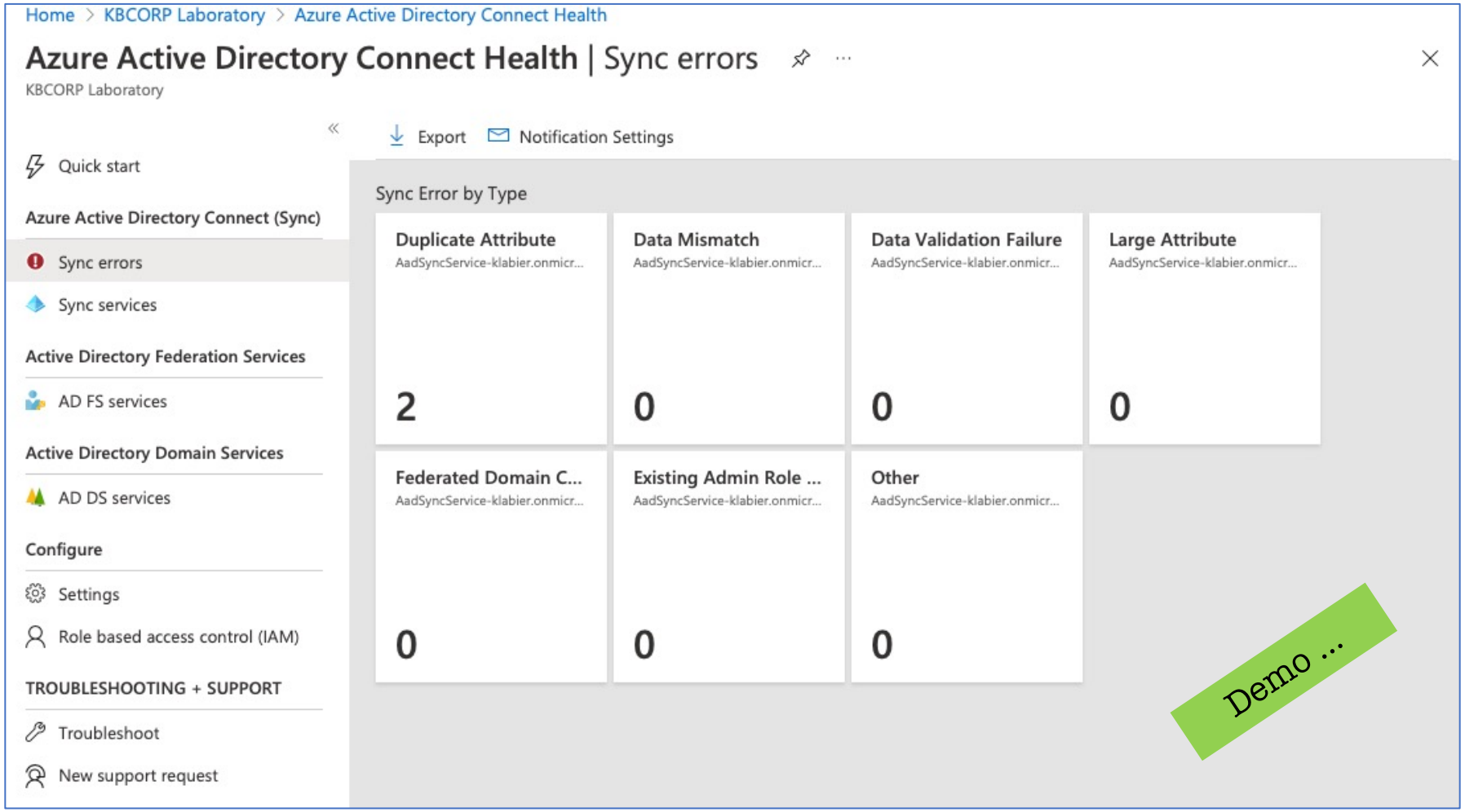
```
PS C:\Users\administrator.KBCORP> Invoke-ADSyncDiagnostics -PasswordSync

================================================================
=                                                              =
=          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 fixed on objectlevel



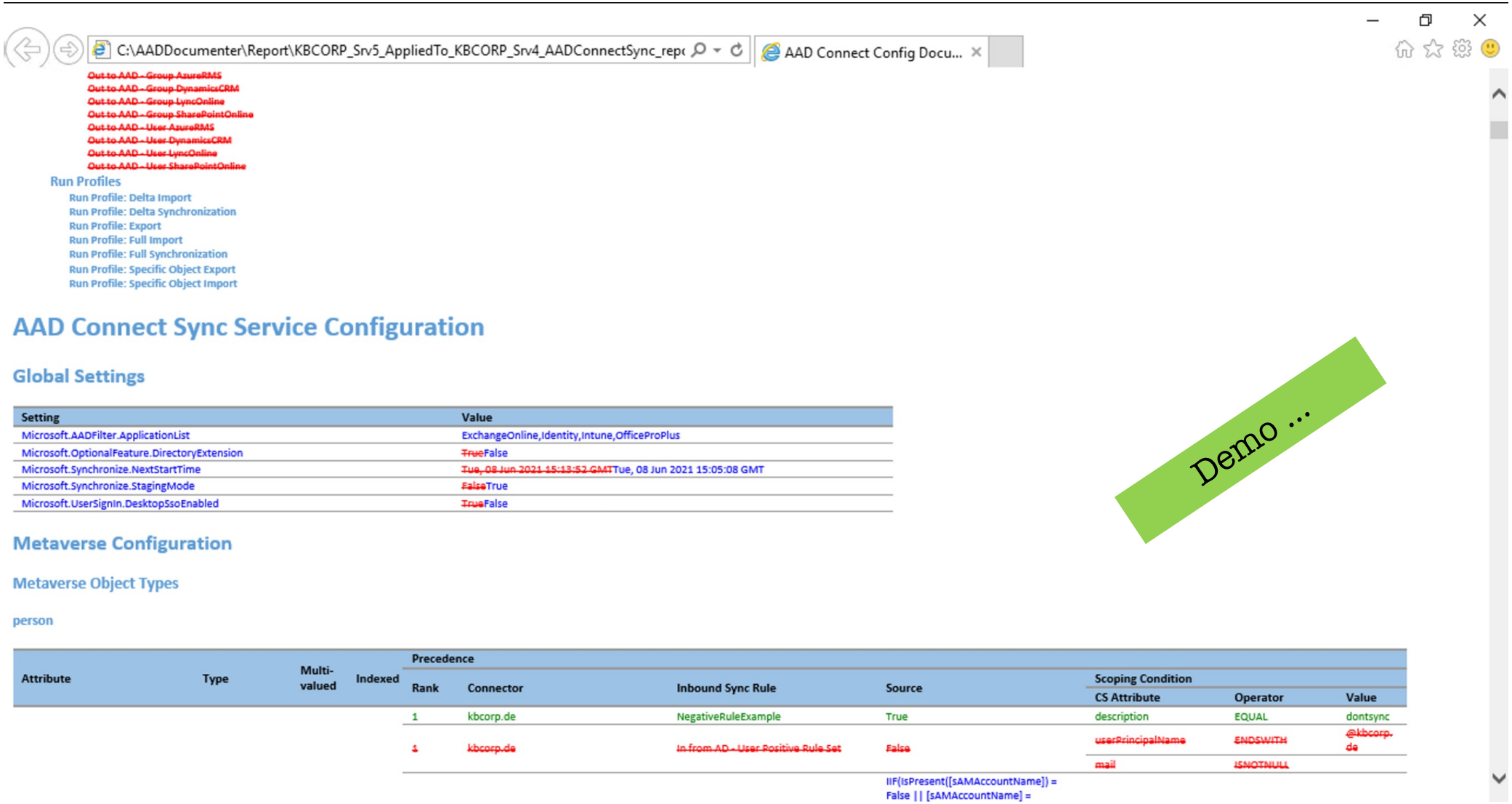
Error-free with hybrid synchronization

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



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 ...

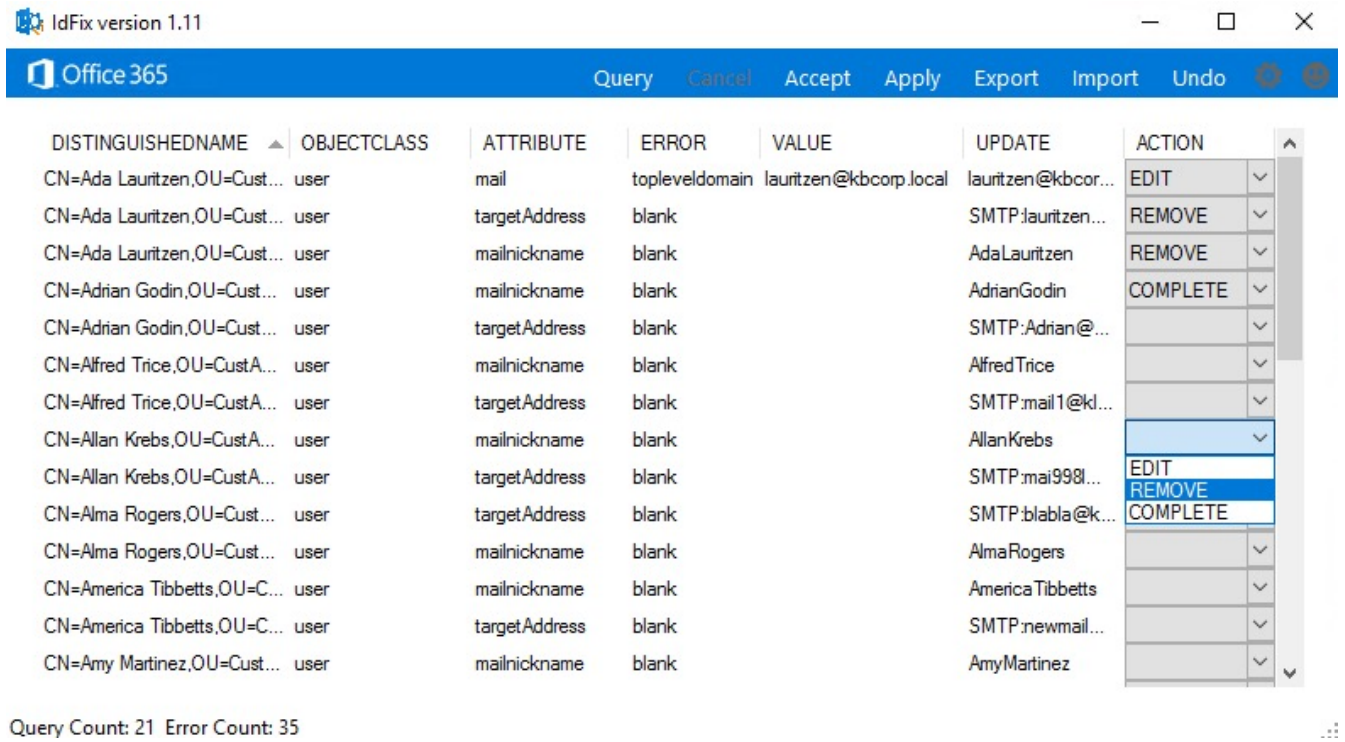
... or via CSV import

Be careful with bulk updates

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

Each write operation creates LDIF for undo

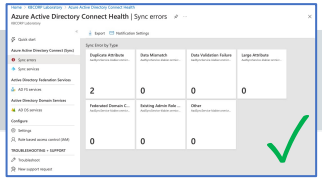
Verbose report with details to write activities



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 szenarios
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


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

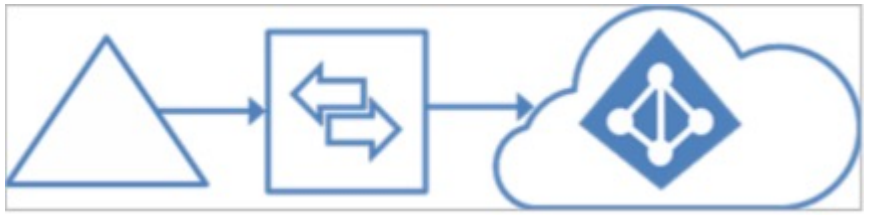
- Is high availability really necessary?
- No farm setup!! Each AAD Connect Server has own separate config
- What actually happens when an AAD Connect server fails?
- Staging Server concept -> Demo 😀 / check „pending exports“ before switch
- Staging server challenge! Same Config important. AADConnectDocumenter in the backup slides
- High availability for SQL can make sense
- Setup with *„useexistingdatabase“* switch (MS Docs link)

Error-free with hybrid synchronization

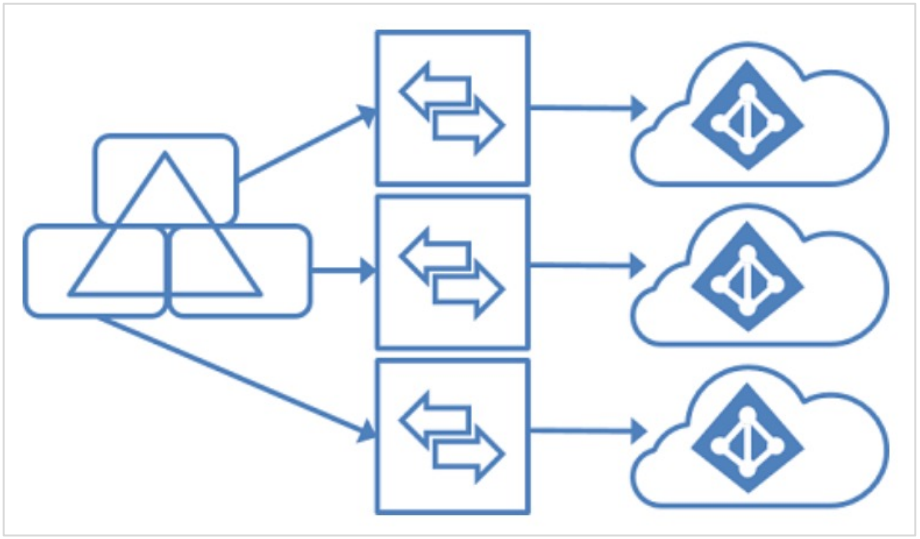
Supported and unsupported scenarios (one forest)

Supported	Unsupported

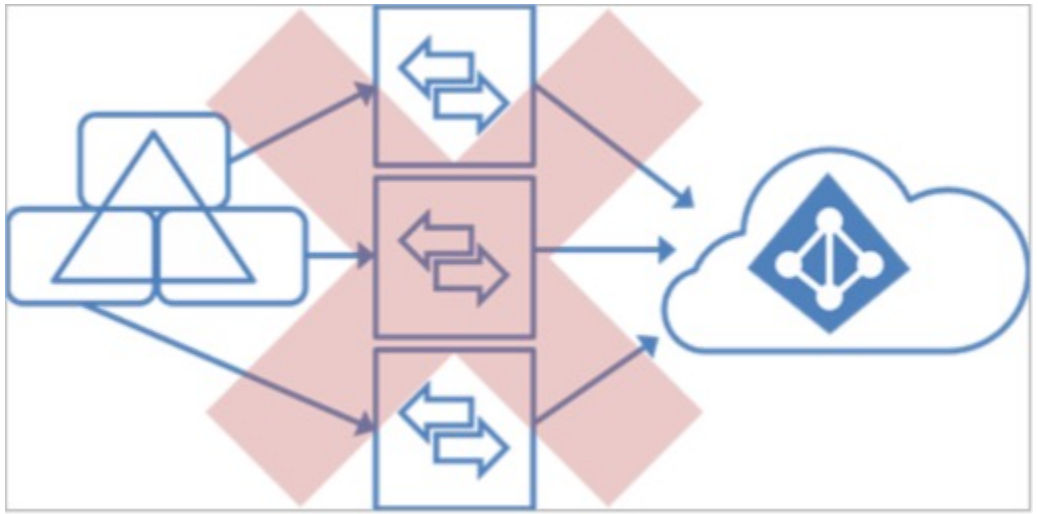
Example1



Example2



Example3

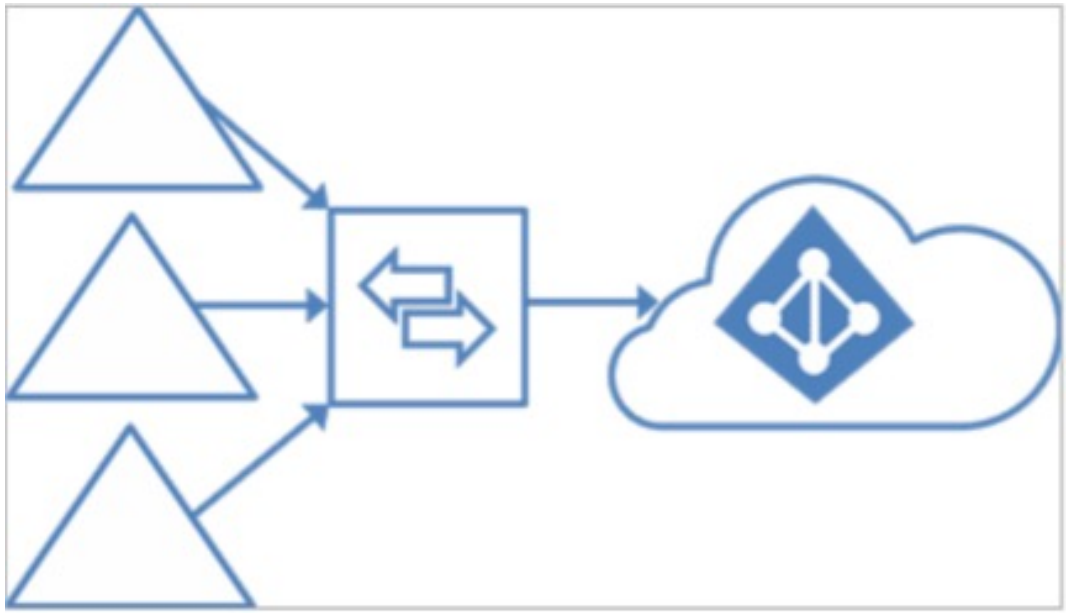


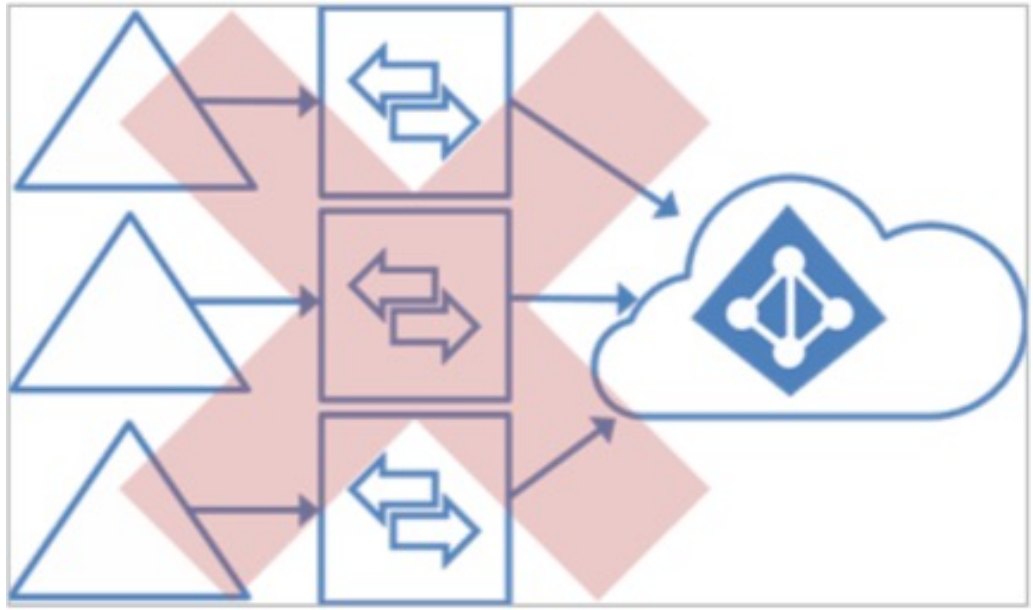
More details link)

Error-free with hybrid synchronization

Supported and unsupported scenarios (multiple forest)

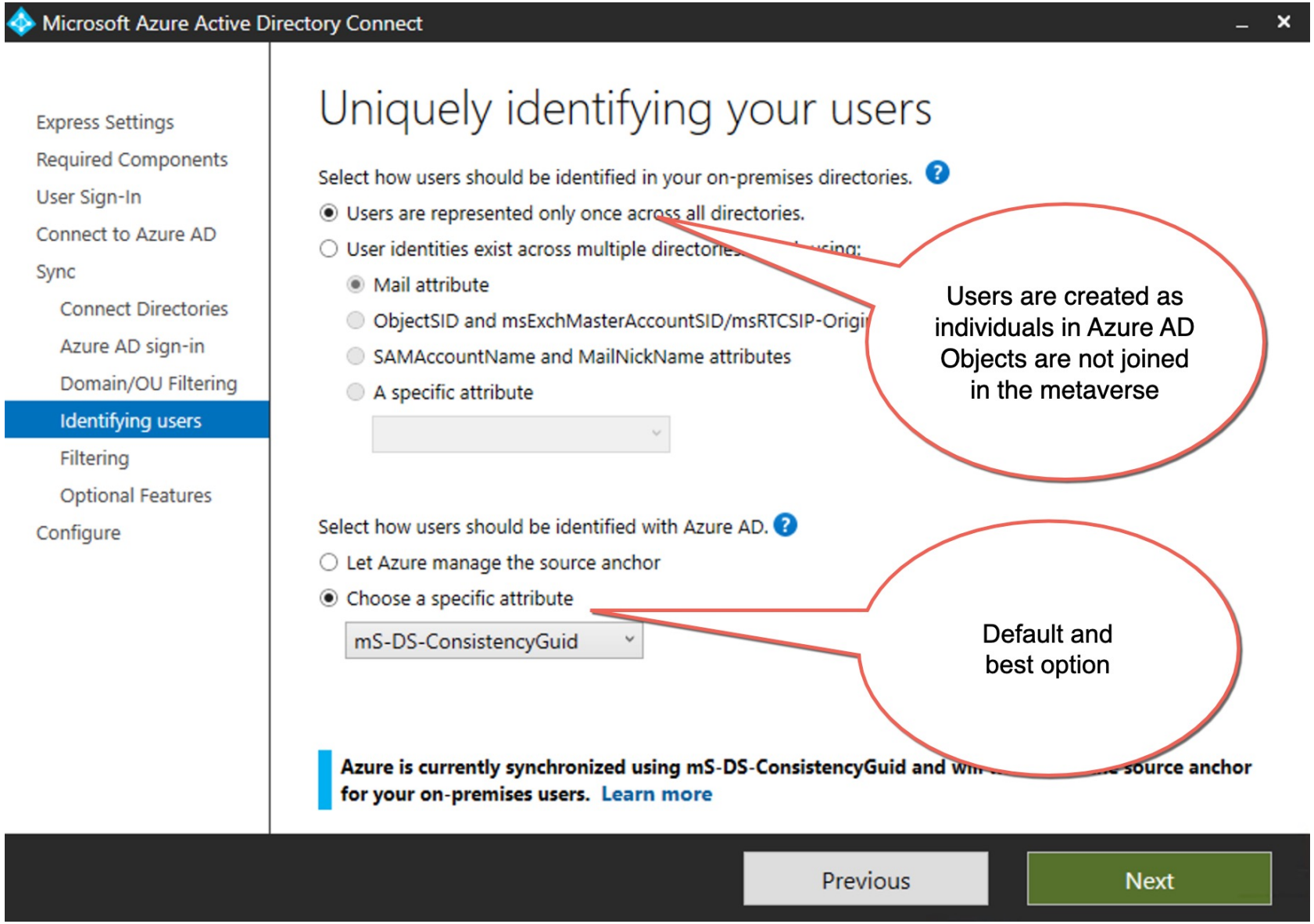
Supported	Unsupported





More details (link)

Error-free with hybrid synchronization



Error-free with hybrid synchronization

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