EUROPEAN CLOUD SUMMIT 2024

Identities are everywhere. A challenge for user management and workflows

Klaus Bierschenk

Technology Consultant @ CGI Germany
Author, Speaker, Identity Enthusiast

Find me blogging at nothingbutcloud.net

EUROPEAN CLOUD SUMMIT

Microsoft run events

AURUM AvePoint CoreView dox42

EasyLife 365 resco veeam

adesso business. people. technology. Allied Global ASCENT BCC DE CIX devoteam

empowerID FPT Software glueck kanja Jabra GN kaspersky LightningTools

nintex Rencore ShareGate: Spot by NetApp SysCloud Syskit WEBCON LOW-CODE, BUT BETTER.

Use ECS Coins for Swag!

Top 3 win an Atari 2600+

1 Get the app

2 Visit sessions and sponsors, rate sessions

3 Earn ECS Coins

4 Spend ECS Coins

csmmt.eu/app

run events

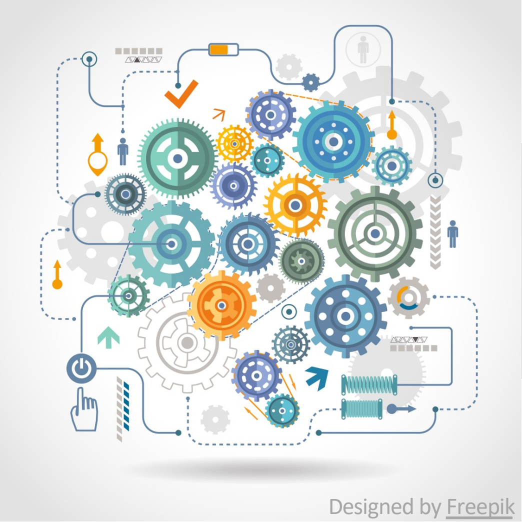
Agenda and key takeaways

➔ What technology for which scenario?

➔ When to use Cloud Connect or Cloud Sync?
What‘s next?

➔ Group Writeback

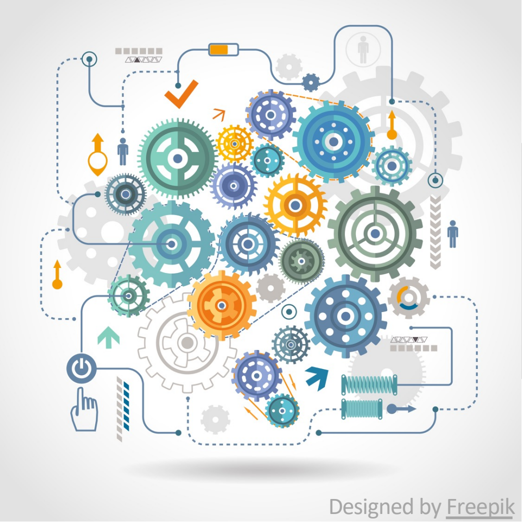
➔ Lifecycle Workflows


Designed by Freepik

➔ Other synchronization topics… App Sync, Cross Tenant Sync, API Driven Provisioning, …

Agenda and key takeaways

- ➔ What technology for which scenario?
- ➔ When to use Cloud Connect or Cloud Sync? Whats next?
- ➔ Group Writeback
- ➔ Lifecycle Workflows
- ➔ Other synchronization topics… App Sync, Cross Tenant Sync, API Driven Provisioning, …



Designed by Freepik

Synchronisation Technologies - Overview

Identities everywhere - a challenge for management

Entra Connect Sync
formerly Azure AD Connect Server

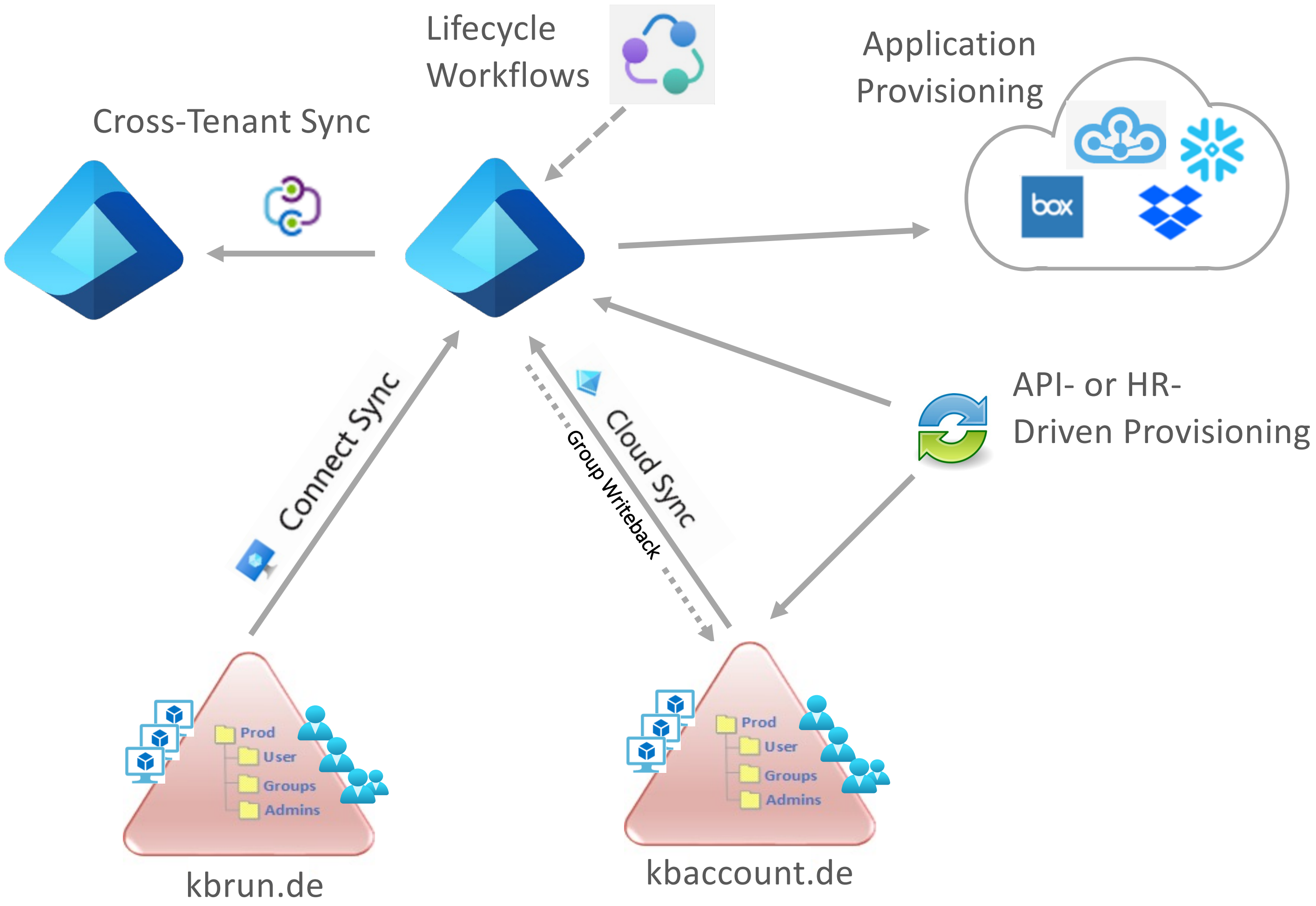
Entra Cloud Sync
formerly Azure AD Cloud Sync

Lifecycle Workflows
Joiner, mover, leaver actions

Application Provisioning
Publish identities for SaaS Apps

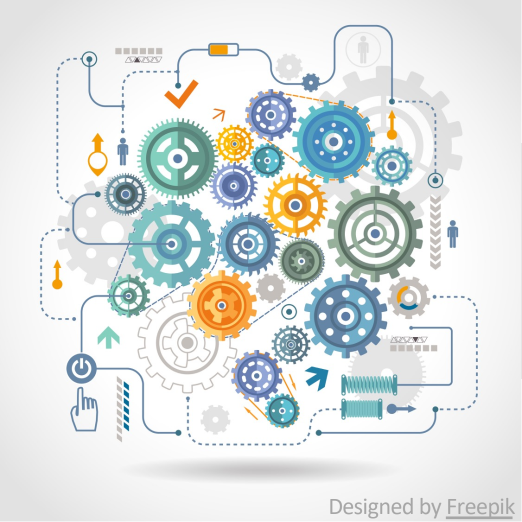
Cross-Tenant Sync
B2B the easy way

API- / HR-Driven Provisioning
flexible API for Provisioning



Agenda and key takeaways

- ➔ Which technology for which scenario?
- ➔ When to use Cloud Connect or Cloud Sync? Whats next?
- ➔ Group Writeback
- ➔ Lifecycle Workflows
- ➔ Other synchronization topics… App Sync, Cross Tenant Sync, API Driven Provisioning, …



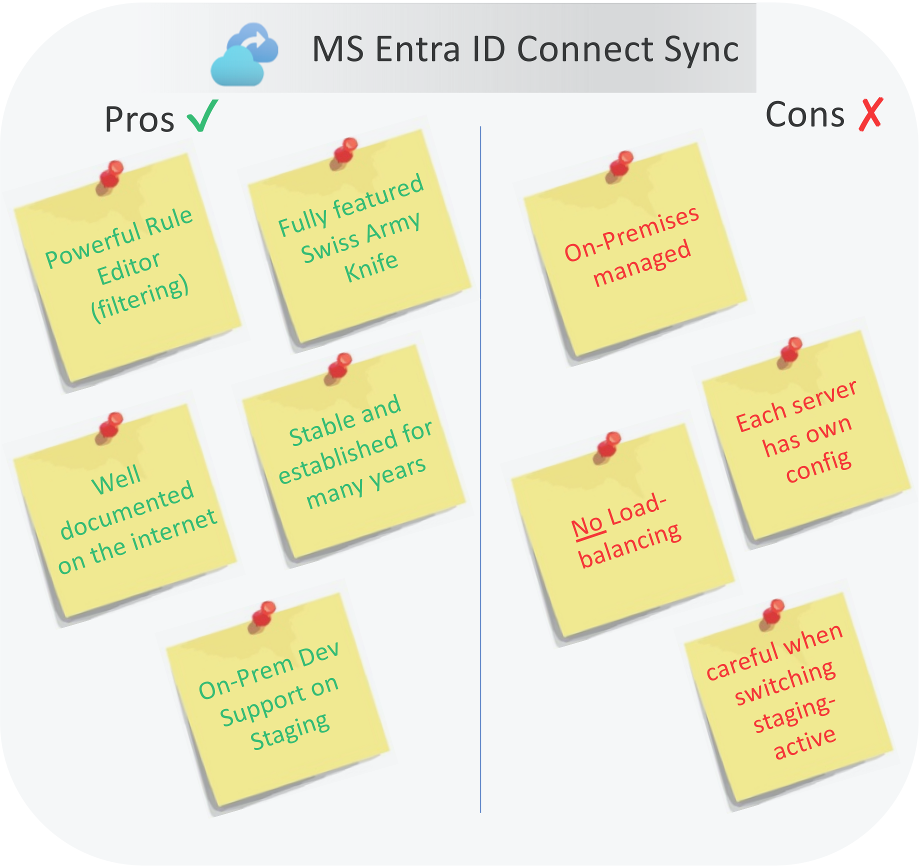
Designed by Freepik

Connect Sync vs. Cloud Sync – Comparison 1/2

What is it ?

The better question is…

… what is it not?



MS Entra ID Connect Sync

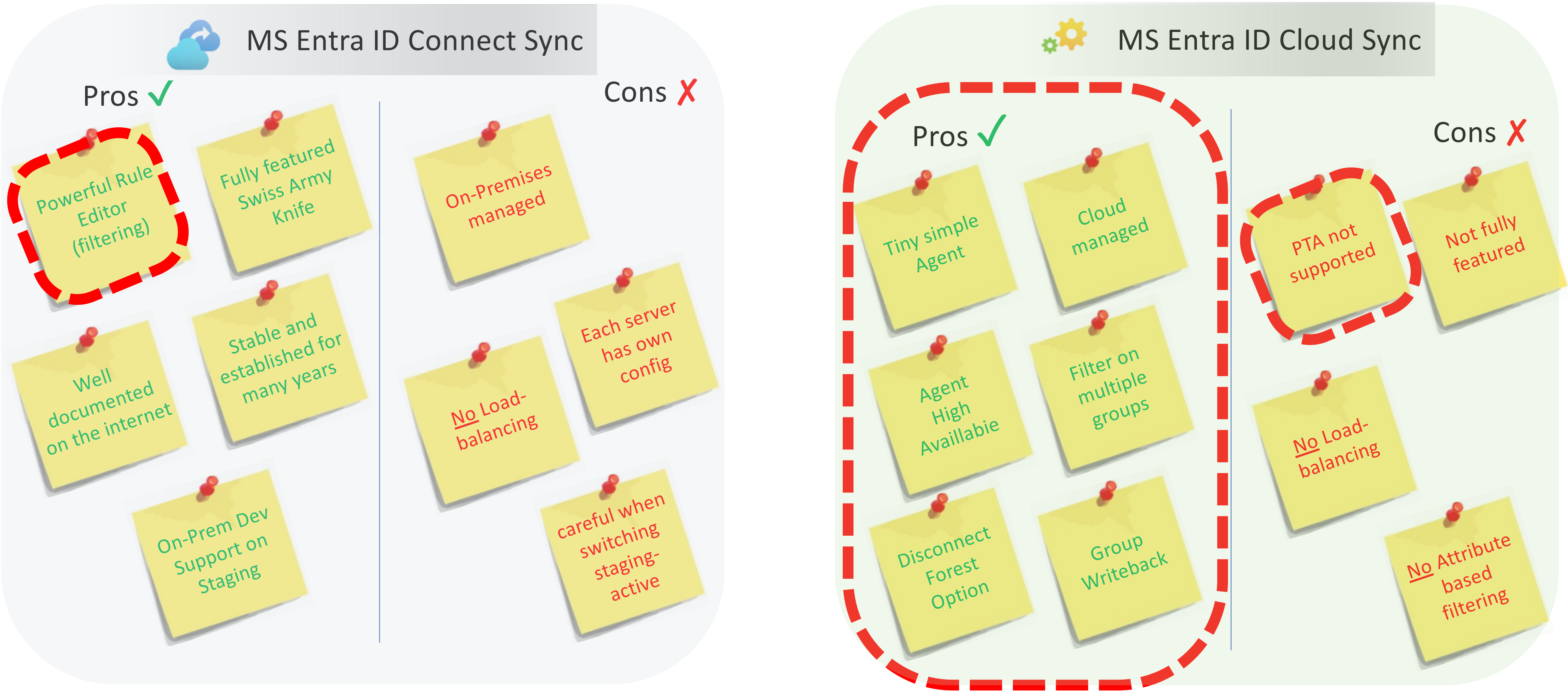
Pros ✓

- Powerful Rule Editor (filtering)
- Fully featured Swiss Army Knife
- Well documented on the internet
- Stable and established for many years
- On-Prem Dev Support on Staging

Cons ✗

- On-Premises managed
- Each server has own config
- No Load-balancing
- careful when switching staging-active

Connect Sync vs. Cloud Sync – Comparison 2/2



MS Entra ID Connect Sync

Pros ✓

- Powerful Rule Editor (filtering)
- Fully featured Swiss Army Knife
- Well documented on the internet
- Stable and established for many years
- On-Prem Dev Support on Staging

Cons ✗

- On-Premises managed
- Each server has own config
- No Load-balancing
- careful when switching staging-active

MS Entra ID Cloud Sync

Pros ✓

- Tiny simple Agent
- Cloud managed
- Agent High Availlabie
- Filter on multiple groups
- Disconnect Forest Option
- Group Writeback

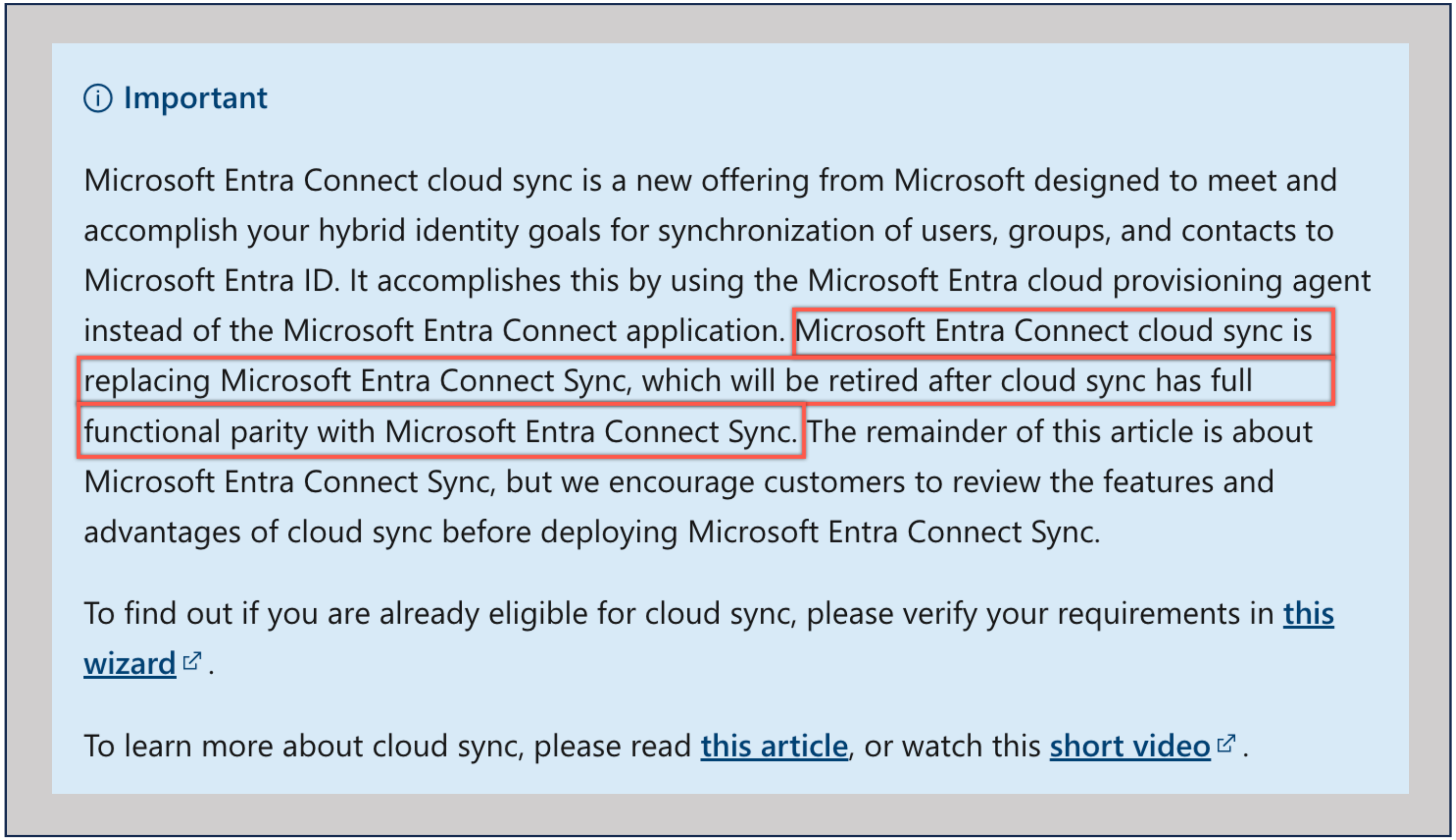
Cons ✗

- PTA not supported
- Not fully featured
- No Load-balancing
- No Attribute based filtering

Synchronisation Technologies – Entra Cloud Connect vs. Cloud Sync

Cloud connect sync is not officially depricated, but …

… found this at Microsoft (link)



ⓘ **Important**

Microsoft Entra Connect cloud sync is a new offering from Microsoft designed to meet and accomplish your hybrid identity goals for synchronization of users, groups, and contacts to Microsoft Entra ID. It accomplishes this by using the Microsoft Entra cloud provisioning agent instead of the Microsoft Entra Connect application. Microsoft Entra Connect cloud sync is replacing Microsoft Entra Connect Sync, which will be retired after cloud sync has full functional parity with Microsoft Entra Connect Sync. The remainder of this article is about Microsoft Entra Connect Sync, but we encourage customers to review the features and advantages of cloud sync before deploying Microsoft Entra Connect Sync.

To find out if you are already eligible for cloud sync, please verify your requirements in **this wizard**.

To learn more about cloud sync, please read **this article**, or watch this **short video**.

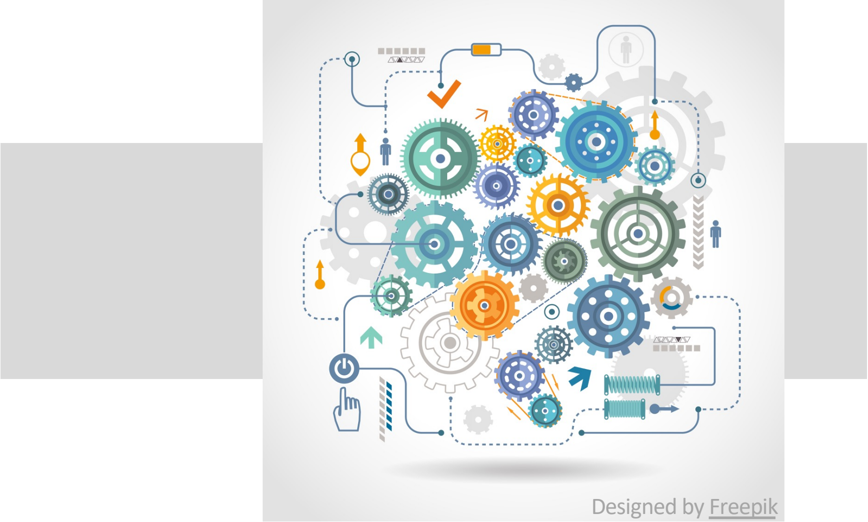
Synchronisation Technologies – Lab

Demo:
Entra Cloud Sync

Designed by Freepik

Agenda and key takeaways

- ➔ Which technology for which scenario?
- ➔ When to use Cloud Connect or Cloud Sync? Whats next?
- ➔ Group Writeback
- ➔ Lifecycle Workflows
- ➔ Other synchronization topics… App Sync, Cross Tenant Sync, API Driven Provisioning, …



Designed by Freepik

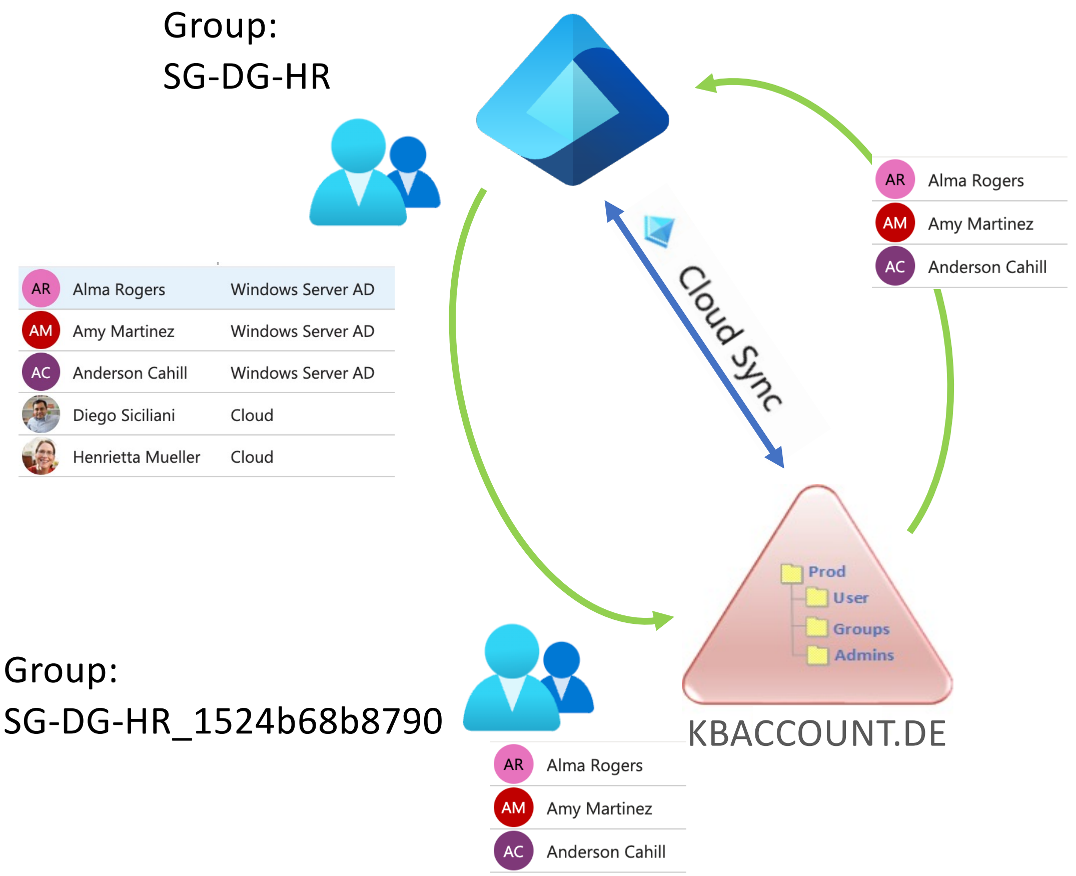
Synchronisation Technologies – Cloud Sync / Group Writeback

What it is … ✓

- → Replacement of the Connect Group Writeback v2
- → Synchronize Cloud Groups to On-Prem AD
- → Extended functionality in Entra Cloud Sync
- → Empowers AD DS to use dynamic groups
- → Creates group as universal in AD

What it is not … ✗

- → No user accounts are created in On-Premises AD
- → On-Prem Groups cannot be used
- → It‘s not longer possible with Connect Sync



Group:
SG-DG-HR

AR	Alma Rogers	Windows Server AD
AM	Amy Martinez	Windows Server AD
AC	Anderson Cahill	Windows Server AD
	Diego Siciliani	Cloud
	Henrietta Mueller	Cloud

AR	Alma Rogers
AM	Amy Martinez
AC	Anderson Cahill

Group:
SG-DG-HR_1524b68b8790

AR	Alma Rogers
AM	Amy Martinez
AC	Anderson Cahill

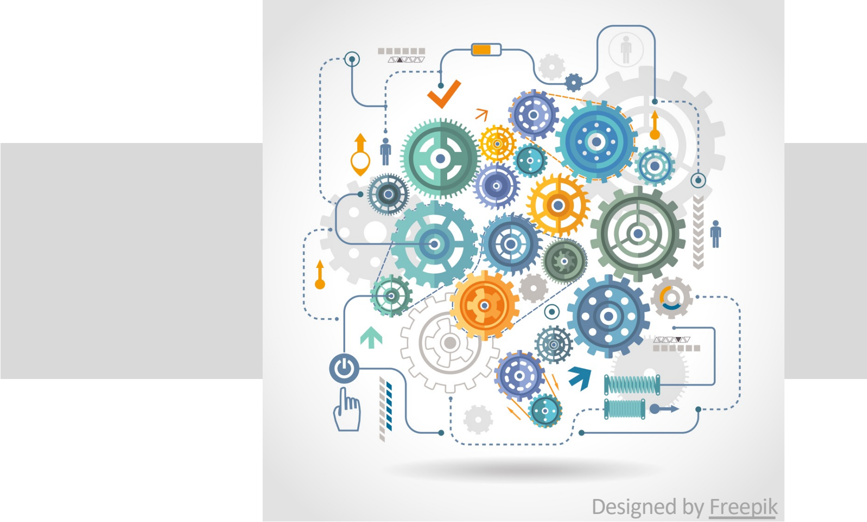
Synchronisation Technologies – Lab

Demo:
Group Writeback

Designed by Freepik

Agenda and key takeaways

- ➔ Which technology for which scenario?
- ➔ When to use Cloud Connect or Cloud Sync? Whats next?
- ➔ Group Writeback
- ➔ Lifecycle Workflows
- ➔ Other synchronization topics… App Sync, Cross Tenant Sync, API Driven Provisioning, …



Designed by Freepik

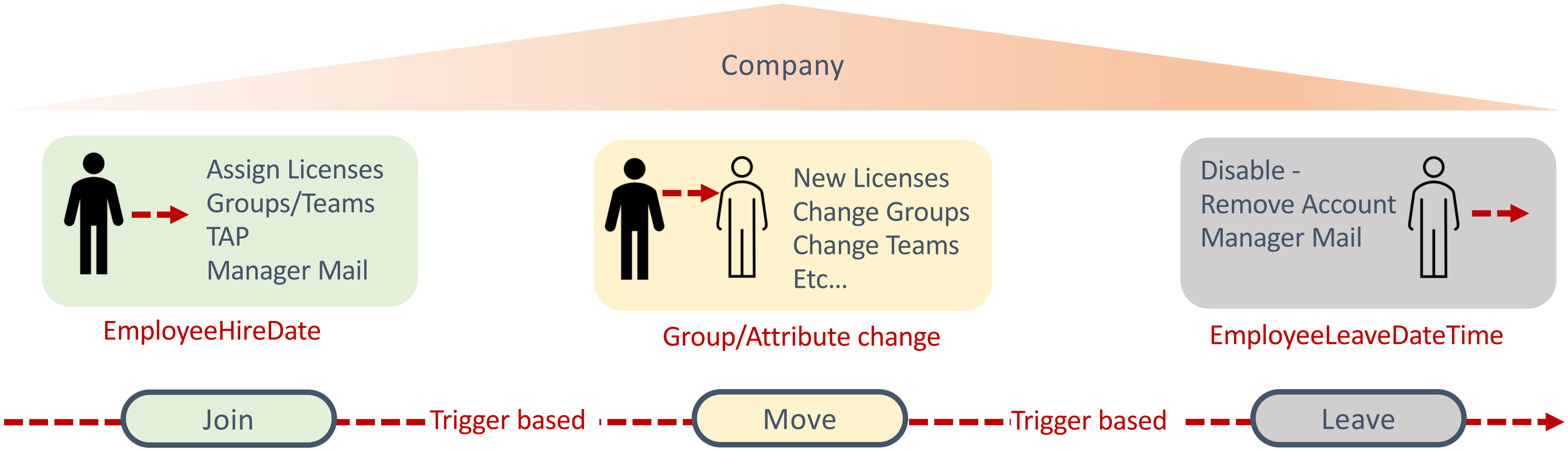
Lifecycle Workflows – a trigger based solution

Admin working manually on daily identity tasks

Designed by Freepik

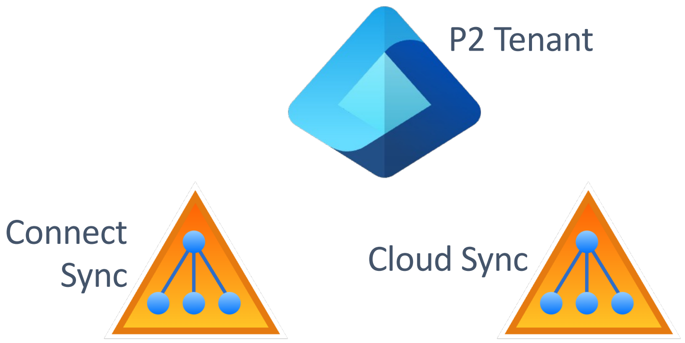
Admin using Lifecycle Workflows

Lifecycle Workflows – a trigger based solution



ExtensionAttribute1 =
EmployeeHireDate

ExtensionAttribute2 =
EmployeeLeaveDateTime

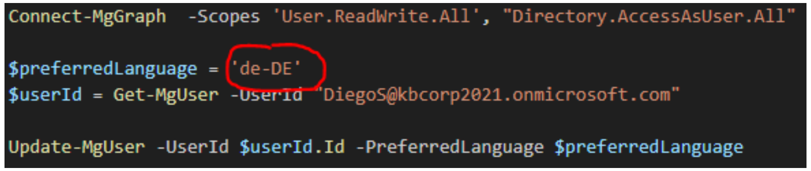


Additional Infos:

- No error handlin
- No On-Premi ation out of the stom extension
- Default sc e 3h
- Language support

DEMO

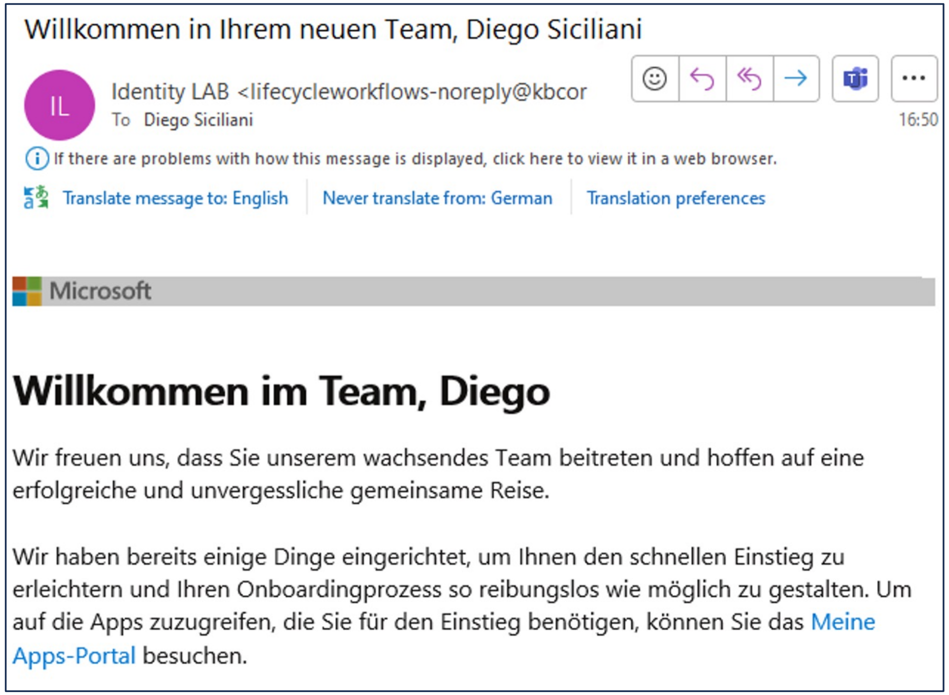
Lifecycle Workflows – a trigger based solution



```
Connect-MgGraph  -Scopes 'User.ReadWrite.All', "Directory.AccessAsUser.All"

$preferredLanguage = 'de-DE'
$userId = Get-MgUser -UserId "DiegoS@kbcorp2021.onmicrosoft.com"

Update-MgUser -UserId $userId.Id -PreferredLanguage $preferredLanguage
```



Willkommen in Ihrem neuen Team, Diego Siciliani

IL Identity LAB <lifecycleworkflows-noreply@kbcor

To Diego Siciliani

16:50

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

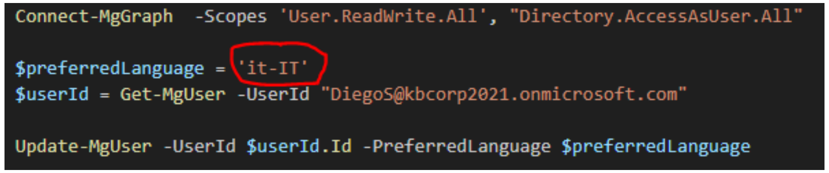
Translate message to: English | Never translate from: German | Translation preferences

Microsoft

Willkommen im Team, Diego

Wir freuen uns, dass Sie unserem wachsendes Team beitreten und hoffen auf eine erfolgreiche und unvergessliche gemeinsame Reise.

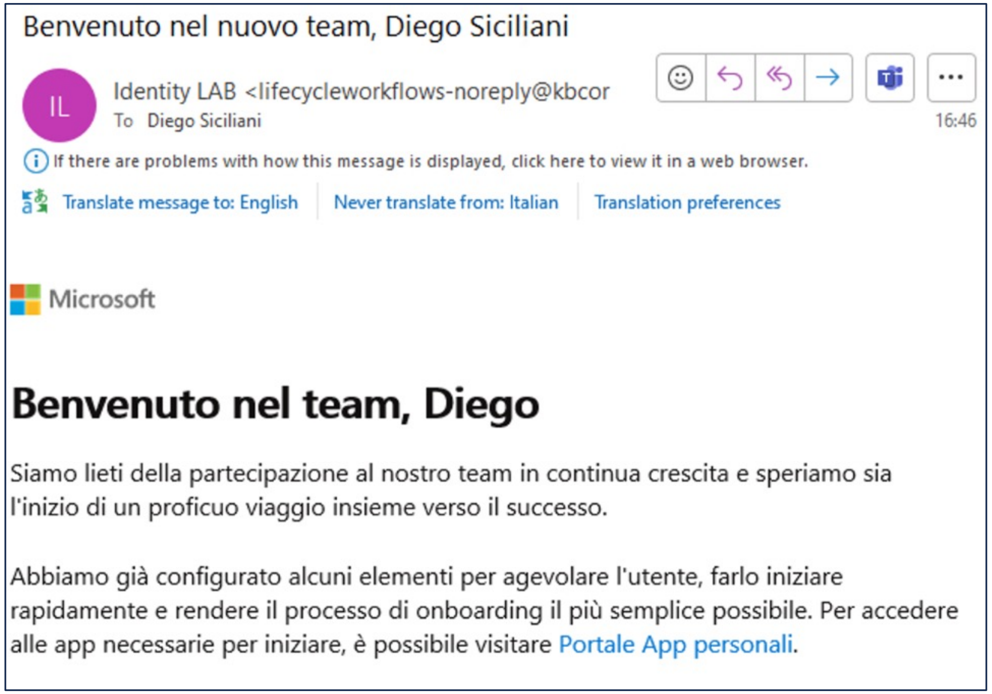
Wir haben bereits einige Dinge eingerichtet, um Ihnen den schnellen Einstieg zu erleichtern und Ihren Onboardingprozess so reibungslos wie möglich zu gestalten. Um auf die Apps zuzugreifen, die Sie für den Einstieg benötigen, können Sie das Meine Apps-Portal besuchen.



```
Connect-MgGraph  -Scopes 'User.ReadWrite.All', "Directory.AccessAsUser.All"

$preferredLanguage = 'it-IT'
$userId = Get-MgUser -UserId "DiegoS@kbcorp2021.onmicrosoft.com"

Update-MgUser -UserId $userId.Id -PreferredLanguage $preferredLanguage
```



Benvenuto nel nuovo team, Diego Siciliani

IL Identity LAB <lifecycleworkflows-noreply@kbcor

To Diego Siciliani

16:46

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

Translate message to: English | Never translate from: Italian | Translation preferences

Microsoft

Benvenuto nel team, Diego

Siamo lieti della partecipazione al nostro team in continua crescita e speriamo sia l'inizio di un proficuo viaggio insieme verso il successo.

Abbiamo già configurato alcuni elementi per agevolare l'utente, farlo iniziare rapidamente e rendere il processo di onboarding il più semplice possibile. Per accedere alle app necessarie per iniziare, è possibile visitare Portale App personali.

Lifecycle Workflows – a trigger based solution - important attributes

Cloud Only Attributes

→ **EmployeeHireDate**
Direct edit possible (Cloud Only Identity)

→ **EmployeeLeaveDateTime**
No direct edit.
Changes via Sync tools or Graph API

Be careful with the format.
It must be:
YYYY-MM-DDThh:mm:ssZ

On-Prem and Cloud

→ **Manager**
Ensure that attribute is not empty. Otherwise workflow will fail (mail)

→ **preferredLanguage**
Can be used for translated mails (Only default mail templates)

Lifecycle Workflows – a trigger based solution – additional infos

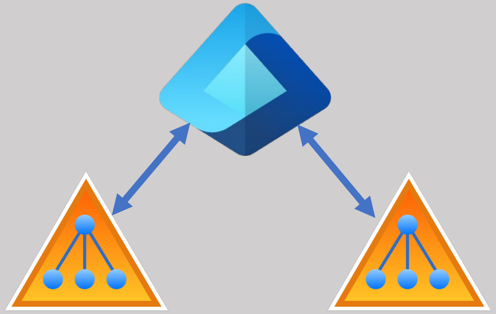
On-Premises: one more challenge

→ Cloud based solution

→ No AD On-Premises integration, it is not hybrid

→ No rocket science, but more effort required

- Custom extensions, Logic App
- Automation account
- Hybrid worker
- Permissions to act in AD DS
- …



→ Find more reading and links to step-by-step guides at the references slide

Lifecycle Workflows – updates and news from the last few weeks

➔ General Availability - Maximum workflows limit in Lifecycle workflows is now 100

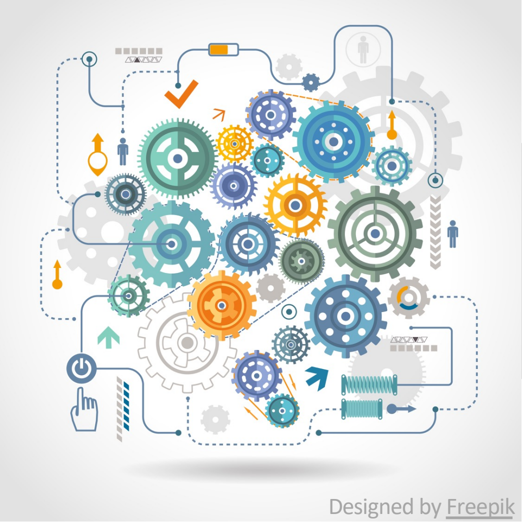
➔ General Availability - Lifecycle Workflows: Export workflow history data to CSV files

➔ Public Preview - Configure custom workflows to run mover tasks when a user's job profile changes (link)

➔ General Availability - API driven inbound provisioning

Agenda and key takeaways

- ➔ Which technology for which scenario?
- ➔ When to use Cloud Connect or Cloud Sync? Whats next?
- ➔ Group Writeback
- ➔ Lifecycle Workflows
- ➔ Other synchronization topics… App Sync, Cross Tenant Sync, API Driven Provisioning, …



Designed by Freepik

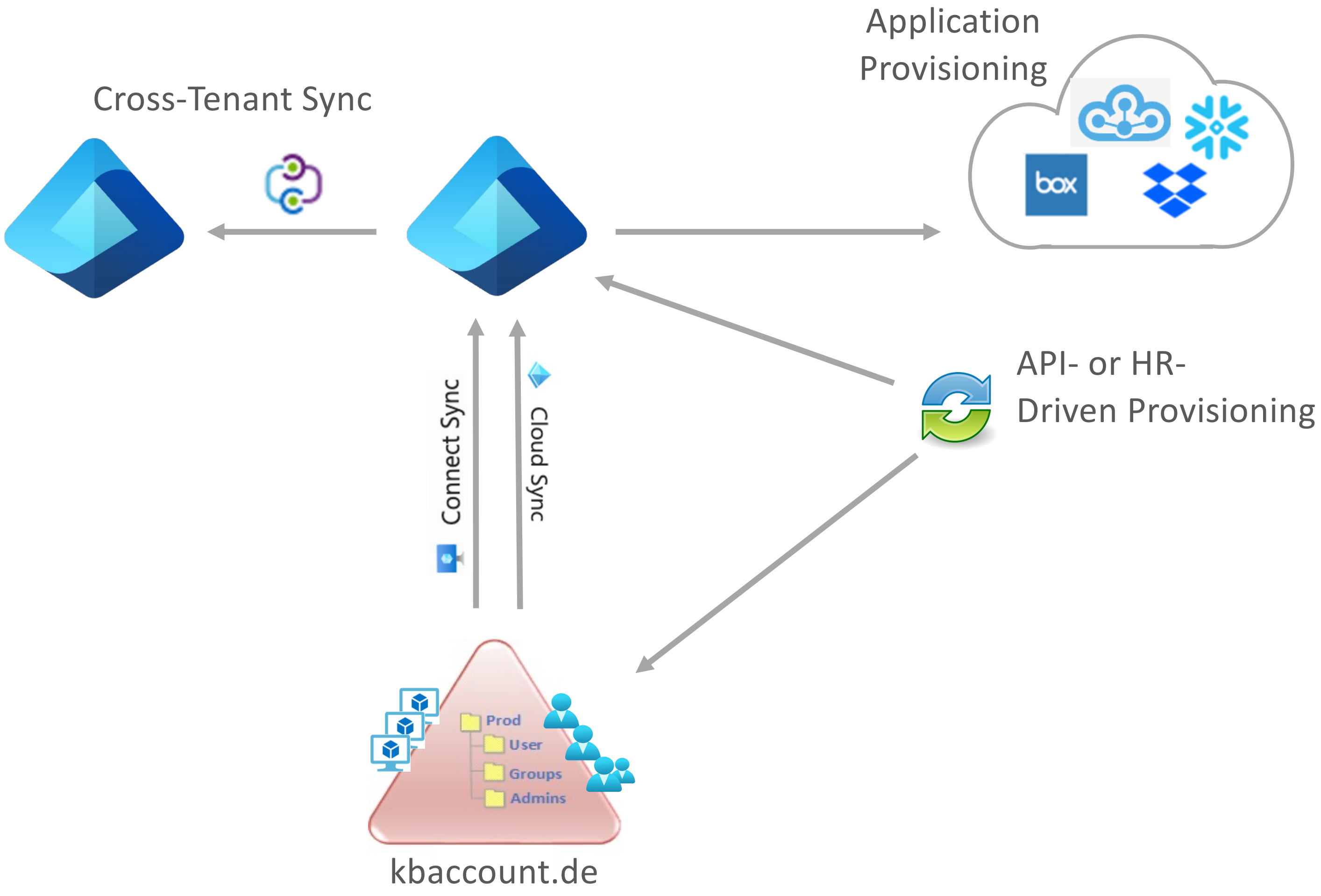
Synchronisation Technologies – Individual provisioning

Individual provisioning:

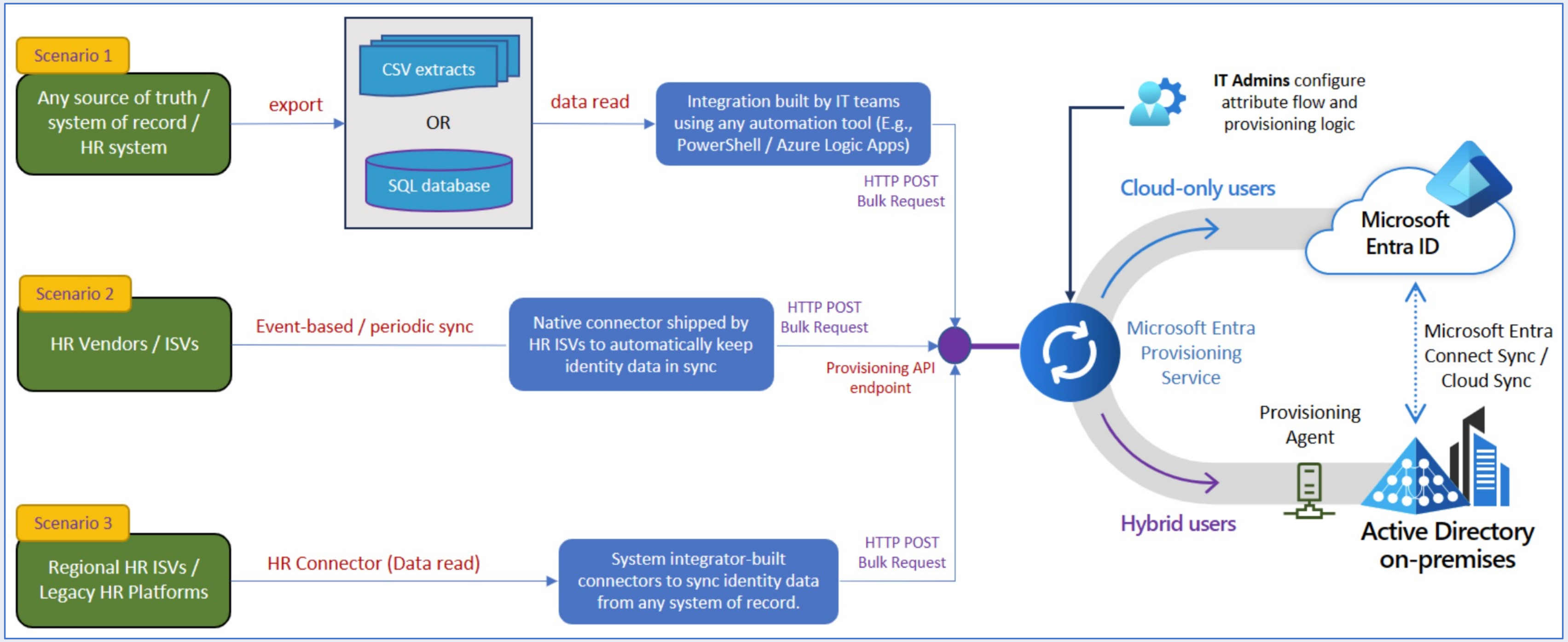
→ Various setups possible

→ Scenario specific

→ Application specific

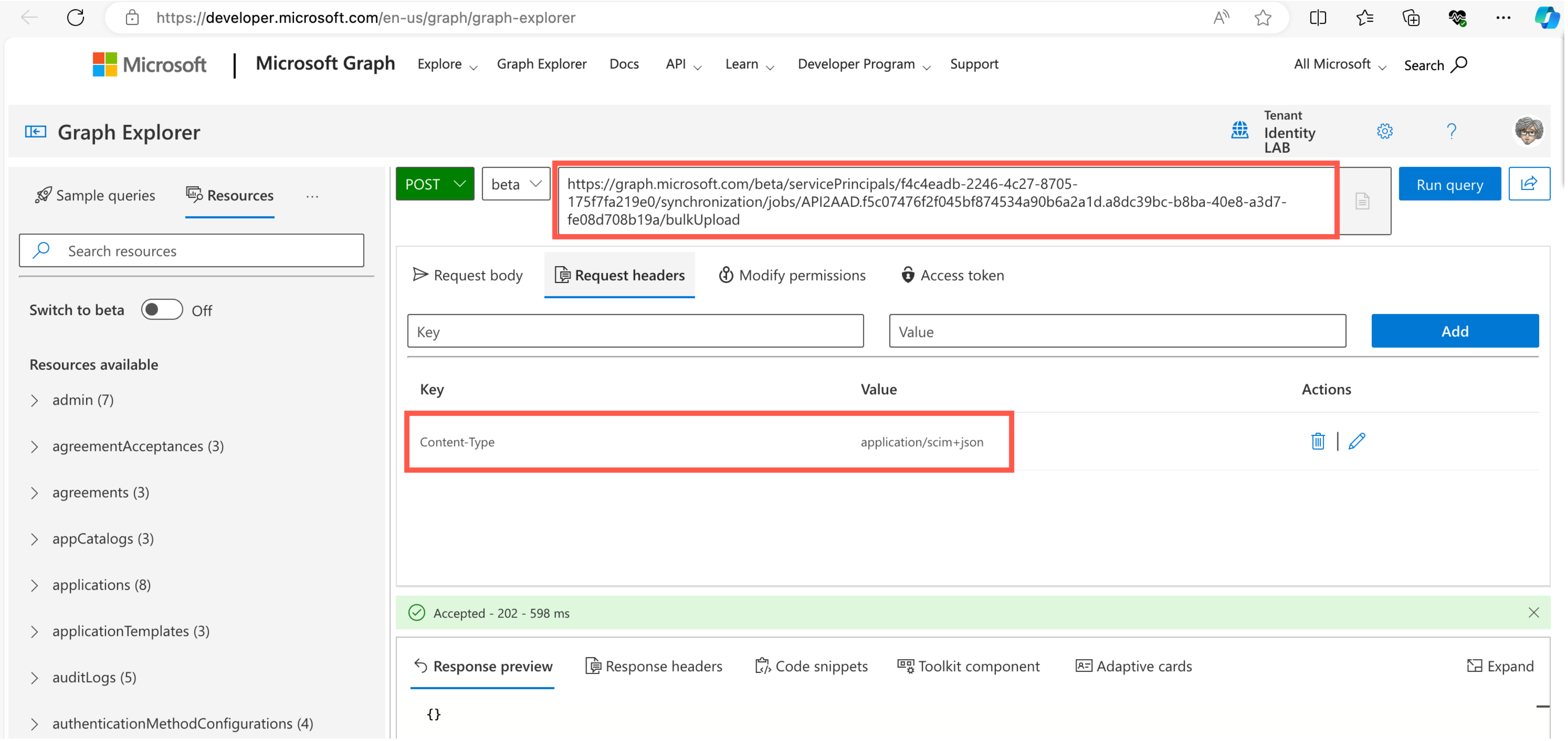


API-driven inbound provisioning


Scenario 1
Any source of truth / system of record / HR system
export
CSV extracts
OR
SQL database
data read
Integration built by IT teams using any automation tool (E.g., PowerShell / Azure Logic Apps)
HTTP POST Bulk Request
Scenario 2
HR Vendors / ISVs
Event-based / periodic sync
Native connector shipped by HR ISVs to automatically keep identity data in sync
HTTP POST Bulk Request
Provisioning API endpoint
Scenario 3
Regional HR ISVs / Legacy HR Platforms
HR Connector (Data read)
System integrator-built connectors to sync identity data from any system of record.
HTTP POST Bulk Request
IT Admins configure attribute flow and provisioning logic
Cloud-only users
Microsoft Entra ID
Microsoft Entra Provisioning Service
Microsoft Entra Connect Sync / Cloud Sync
Provisioning Agent
Hybrid users
Active Directory on-premises

Source: [Microsoft Link]
Quickstart guides availlable; cURL, Postman, Powershell, Graph Explorer, Azure Logic Apps

Additional Infos … API-driven provisioning



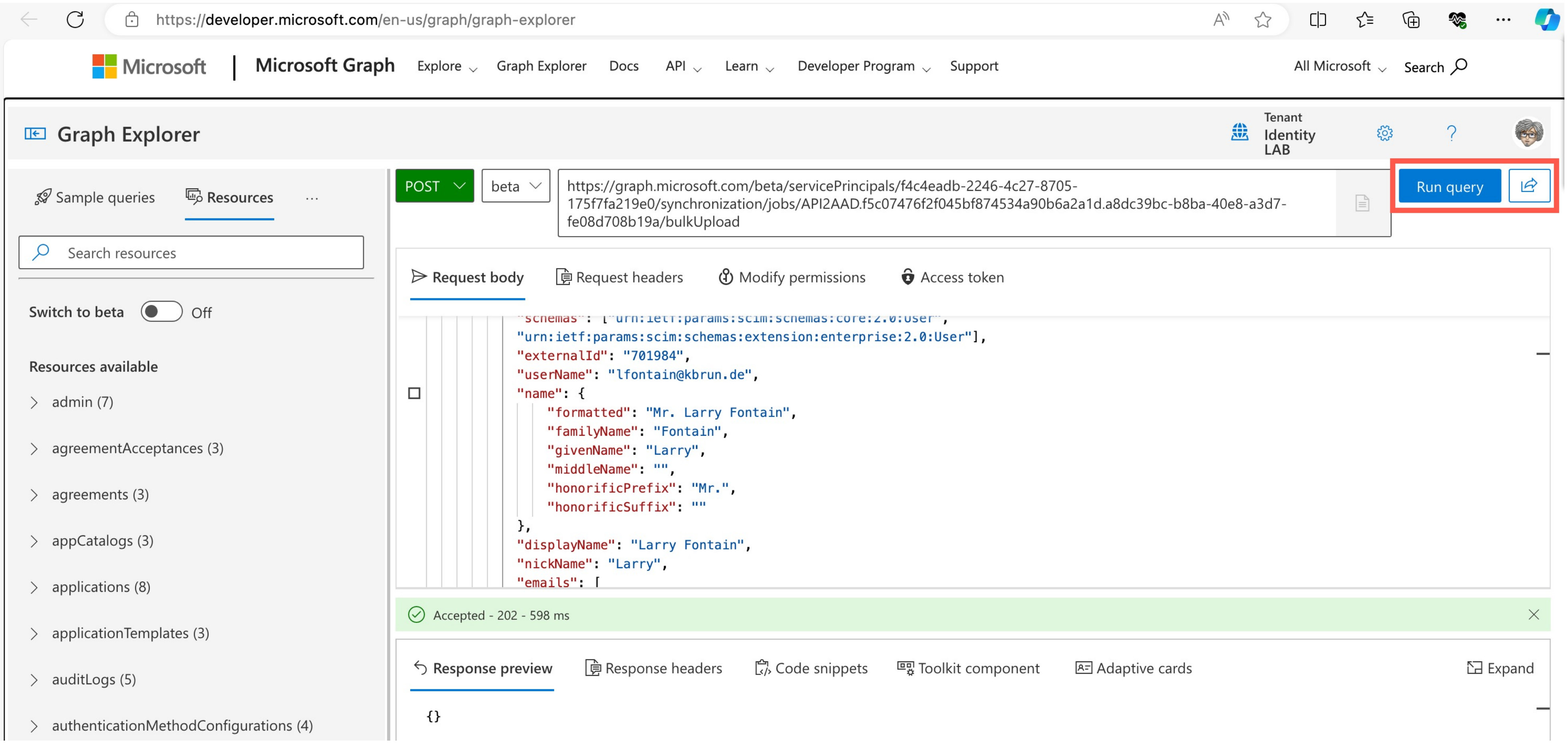
POST beta https://graph.microsoft.com/beta/servicePrincipals/f4c4eadb-2246-4c27-8705-175f7fa219e0/synchronization/jobs/API2AAD.f5c07476f2f045bf874534a90b6a2a1d.a8dc39bc-b8ba-40e8-a3d7-fe08d708b19a/bulkUpload

Key	Value	Actions
Content-Type	application/scim+json	

Accepted - 202 - 598 ms

```
{}
```

Additional Infos … API-driven provisioning



POST https://graph.microsoft.com/beta/servicePrincipals/f4c4eadb-2246-4c27-8705-175f7fa219e0/synchronization/jobs/API2AAD.f5c07476f2f045bf874534a90b6a2a1d.a8dc39bc-b8ba-40e8-a3d7-fe08d708b19a/bulkUpload

```
"schemas": ["urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"],
"externalId": "701984",
"userName": "lfontain@kbrun.de",
"name": {
    "formatted": "Mr. Larry Fontain",
    "familyName": "Fontain",
    "givenName": "Larry",
    "middleName": "",
    "honorificPrefix": "Mr.",
    "honorificSuffix": ""
},
"displayName": "Larry Fontain",
"nickName": "Larry",
"emails": [
```

Accepted - 202 - 598 ms

```
{}
```

Agenda and key takeaways

➔ When to use Cloud Connect or Cloud Sync?
What‘s next?

Go for Cloud Sync! If not possible today, wait or plan carefully. Consider migration …

➔ Group Writeback

Very powerful, but be careful with dynamic groups

➔ Lifecycle Workflows

Can hugely reduce admin effort in daily identity tasks. Check reference links for deep dive

Additional information, continue reading …

Lifecycle Workflows (On-Prem topics):

[Lifecycle Workflows example series (including On-Premises integration) - Pim Jacobs]

[Automated Lifecycle Workflows for Privileged Identities with Azure AD Identity Governance - Thomas Naunheim]

[Customize emails sent from workflow tasks - Microsoft Entra ID Governance | Microsoft Learn]

Additional Microsoft docs:

[Exchange hybrid writeback with cloud sync - Microsoft Entra ID | Microsoft Learn]

[Read this]

[Application provisioning documentation | Microsoft Learn]

[What is HR driven provisioning with Microsoft Entra ID? | Microsoft Learn]

[What is automated app user provisioning in Microsoft Entra ID | Microsoft Learn]

[How to use single sign-on with cloud sync - Microsoft Entra ID | Microsoft Learn]

Additional topics/docs Cloud Connect:

[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 sync V2 endpoint API]

Security:

[Hardening Service Accounts from AADConnect - Account permissions]

[Hardening Service Accounts from AADConnect - connector accounts]

[Check for pending exports]

THANK YOU,
YOU ARE AWESOME ❤️

PLEASE RATE THIS SESSION
IN THE MOBILE APP.

in LinkedIn

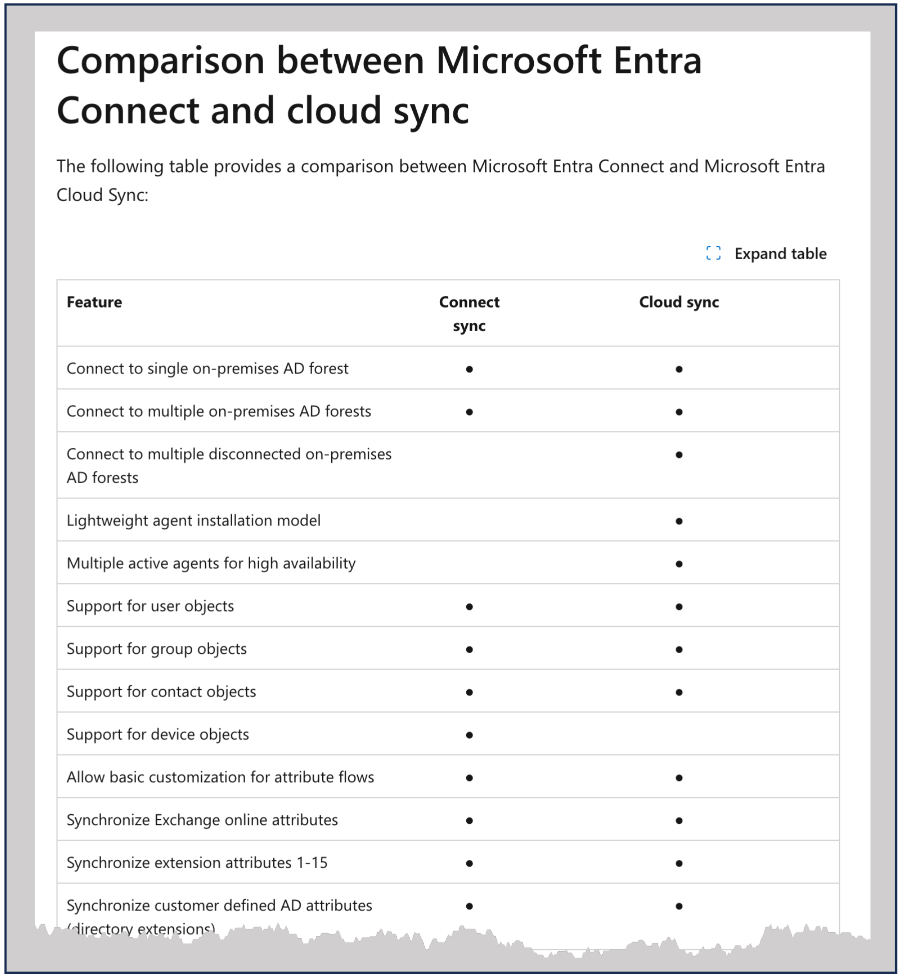
Blog:
https://nothingbutcloud.net/

Backup slides

EUROPEAN CLOUD SUMMIT

Additional Infos: full comparision list connect sync vs. Cloud sync

Find the complete comparison list in this article



Comparison between Microsoft Entra Connect and cloud sync

The following table provides a comparison between Microsoft Entra Connect and Microsoft Entra Cloud Sync:

⛶ Expand table

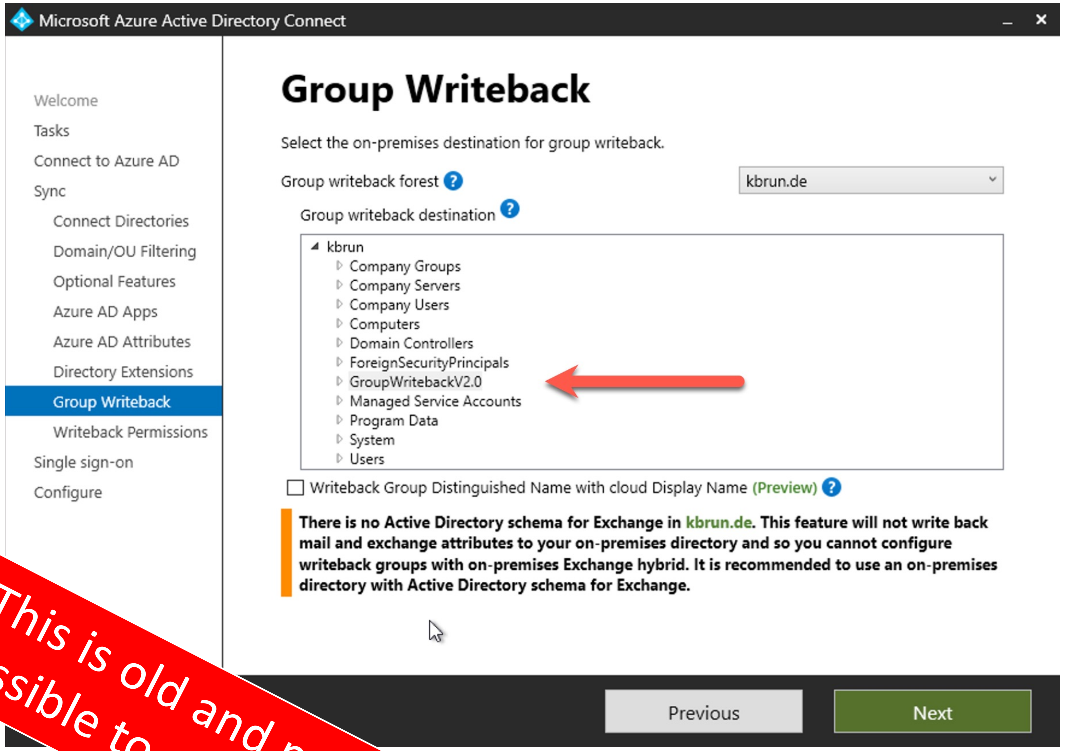
Feature	Connect sync	Cloud sync
Connect to single on-premises AD forest	●	●
Connect to multiple on-premises AD forests	●	●
Connect to multiple disconnected on-premises AD forests		●
Lightweight agent installation model		●
Multiple active agents for high availability		●
Support for user objects	●	●
Support for group objects	●	●
Support for contact objects	●	●
Support for device objects	●	
Allow basic customization for attribute flows	●	●
Synchronize Exchange online attributes	●	●
Synchronize extension attributes 1-15	●	●
Synchronize customer defined AD attributes (directory extensions)	●	●

Synchronisation Technologies – Cloud Sync / Group Writeback

Are you using Group Writeback v2?
… as a setup option in Entra Cloud Connect?

➔ Support will end 30. June 2024

➔ It is moved to Entra Cloud Sync Group Writeback



Group Writeback

Select the on-premises destination for group writeback.

Group writeback forest: kbrun.de

Group writeback destination

□ Writeback Group Distinguished Name with cloud Display Name (Preview)

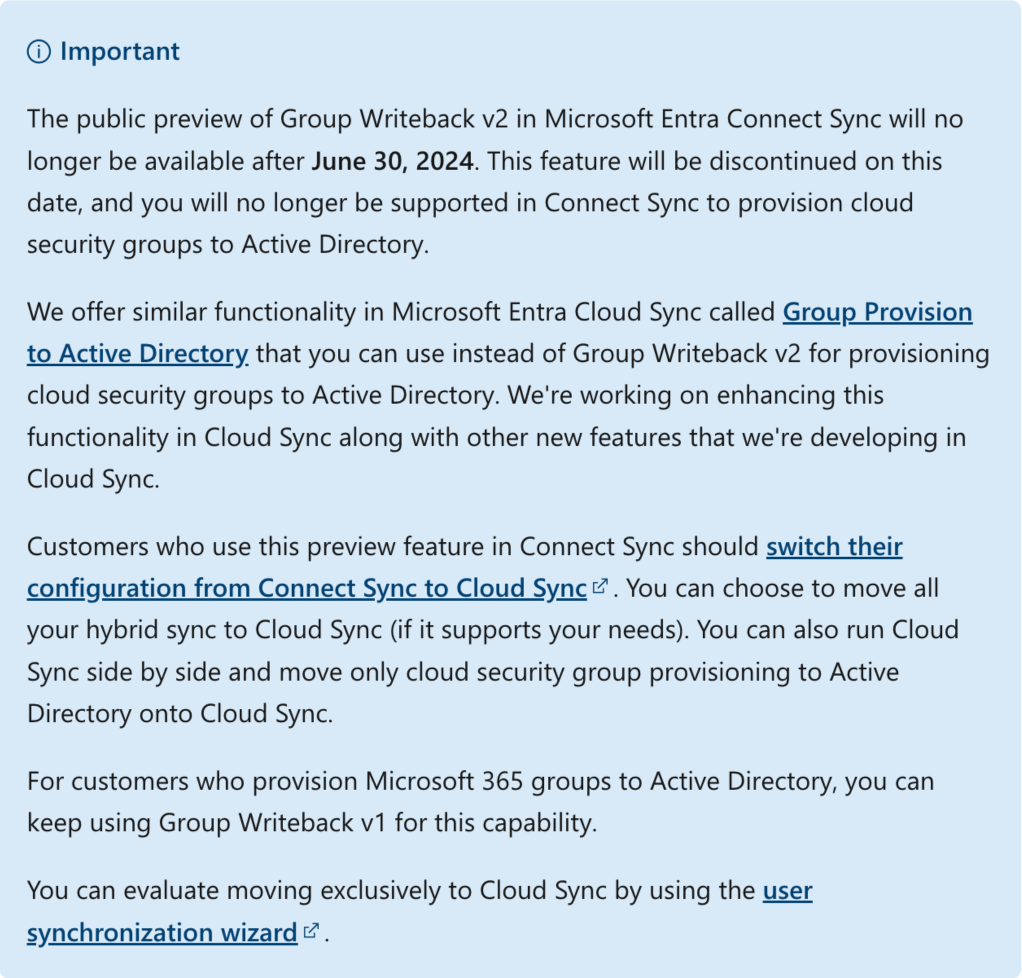
There is no Active Directory schema for Exchange in kbrun.de. This feature will not write back mail and exchange attributes to your on-premises directory and so you cannot configure writeback groups with on-premises Exchange hybrid. It is recommended to use an on-premises directory with Active Directory schema for Exchange.

This is old and not possible to edit here

Additional Infos …

Found this here:

Migrate Microsoft Entra Connect Sync group writeback V2 to Microsoft Entra Cloud Sync - Microsoft Entra ID | Microsoft Learn



ⓘ **Important**

The public preview of Group Writeback v2 in Microsoft Entra Connect Sync will no longer be available after **June 30, 2024**. This feature will be discontinued on this date, and you will no longer be supported in Connect Sync to provision cloud security groups to Active Directory.

We offer similar functionality in Microsoft Entra Cloud Sync called **Group Provision to Active Directory** that you can use instead of Group Writeback v2 for provisioning cloud security groups to Active Directory. We're working on enhancing this functionality in Cloud Sync along with other new features that we're developing in Cloud Sync.

Customers who use this preview feature in Connect Sync should **switch their configuration from Connect Sync to Cloud Sync**. You can choose to move all your hybrid sync to Cloud Sync (if it supports your needs). You can also run Cloud Sync side by side and move only cloud security group provisioning to Active Directory onto Cloud Sync.

For customers who provision Microsoft 365 groups to Active Directory, you can keep using Group Writeback v1 for this capability.

You can evaluate moving exclusively to Cloud Sync by using the **user synchronization wizard**.

Additional Infos … keep it up to date – multiple updates per 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://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/reference-version-history