CLOUD IDENTITY SUMMIT '25

Identity Management Track

Is Entra Connect Still the Best Choice?

Fabian Bader + Chris Brumm (glueckkanja AG)

Community Event by Azure Meetup BONN

About us

Fabian Bader **Chris Brumm**

@fabian_bader @cbrhh

/in/fabianbader /in/christopherbrumm

cloudbrothers.info chris-brumm.com

Cyber Security Architects

@

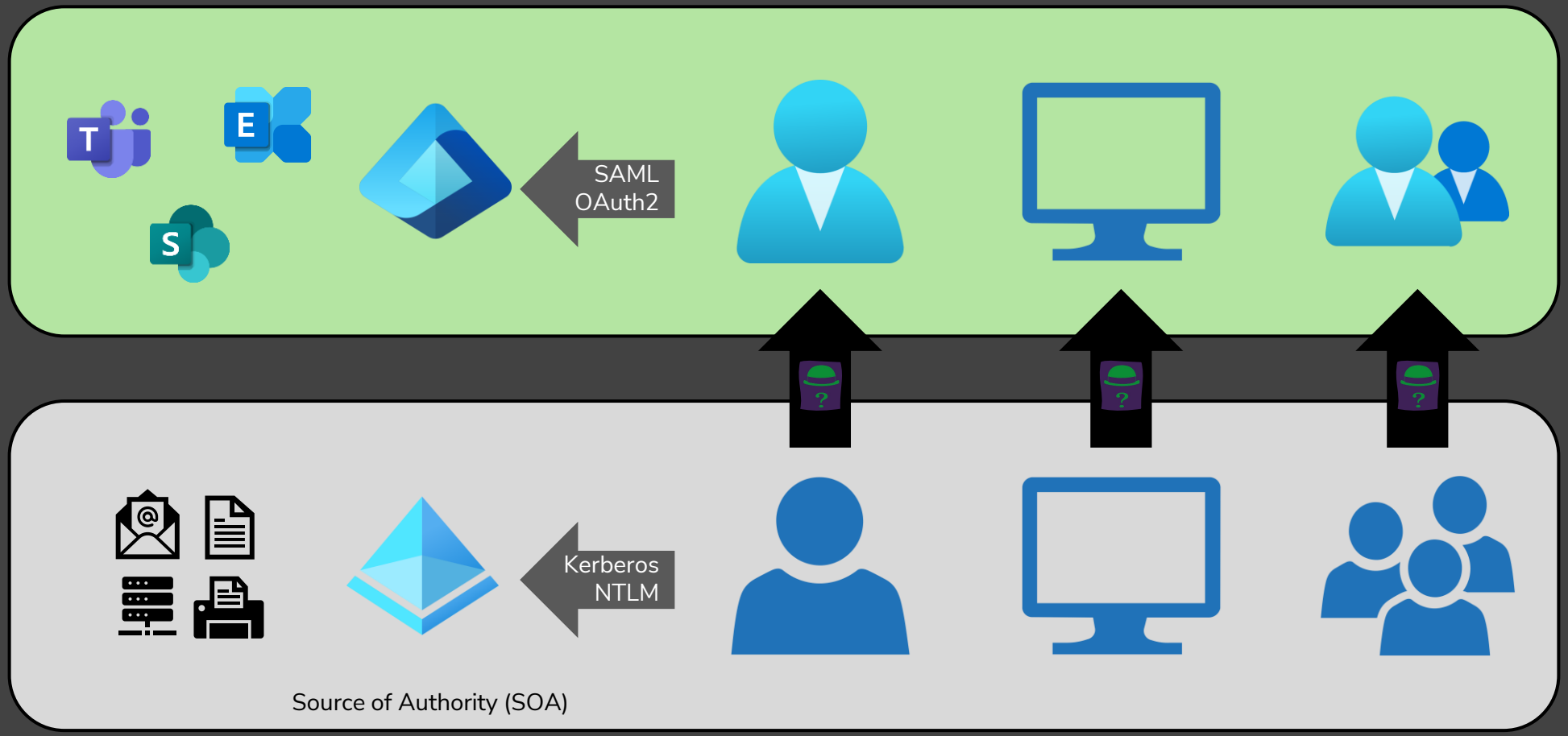
glueck kanja

Microsoft MVPs

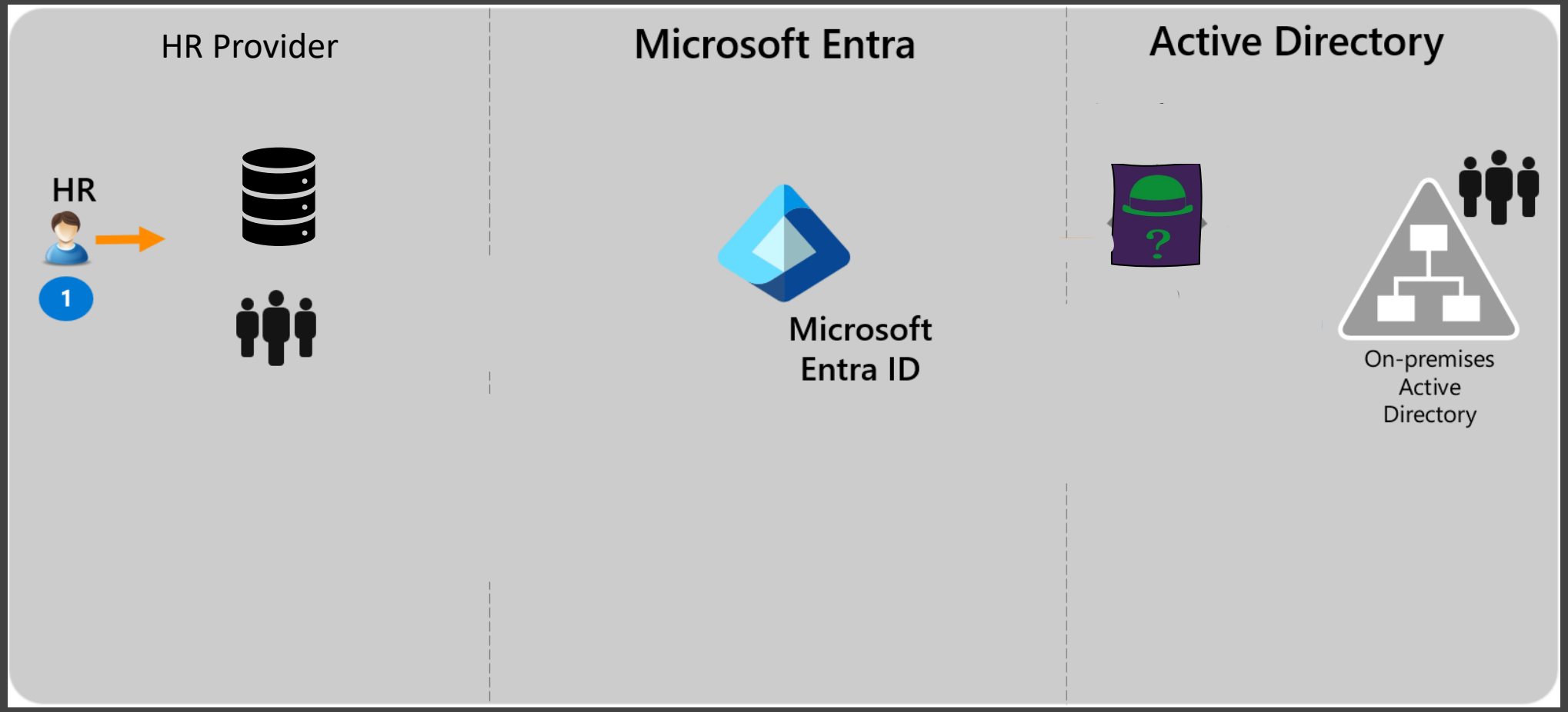
Agenda

- Hybrid Identities - The tale of two sync engines
- Key differences
- Migration
- Coexistence
- Change of Source of Authority
- Security Implications

Introduction to Hybrid Identities



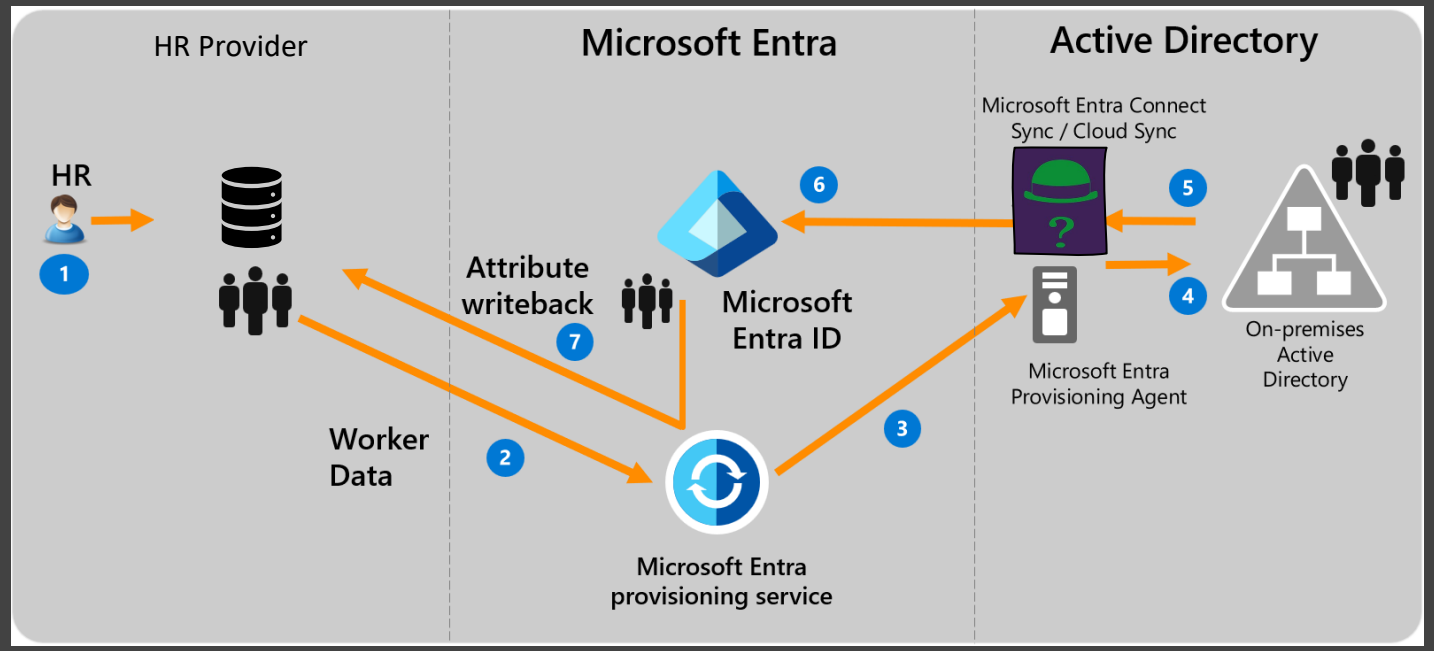
External HR provider



Source: https://learn.microsoft.com/en-us/entra/identity/saas-apps/workday-inbound-tutorial#solution-architecture

Source of Authority responsibilities

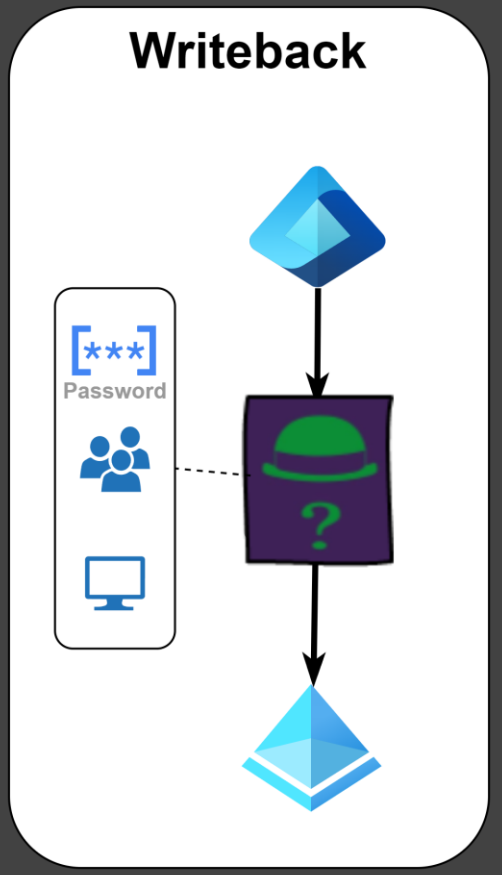
- CRUD actions
- Password management
- Password verification
  - Password-hash sync
  - Pass-Through Authentication
  - Federation (AD FS)
- Authentication method exchange
  - Seamless SSO (Kerberos TGS -> (SAML) -> OAuth2 Token)
  - Cloud Kerberos Trust (Cloud Kerberos -> Kerberos TGT)
  - Kerberos Constrained Delegation SSO (OAuth2 -> TGS)



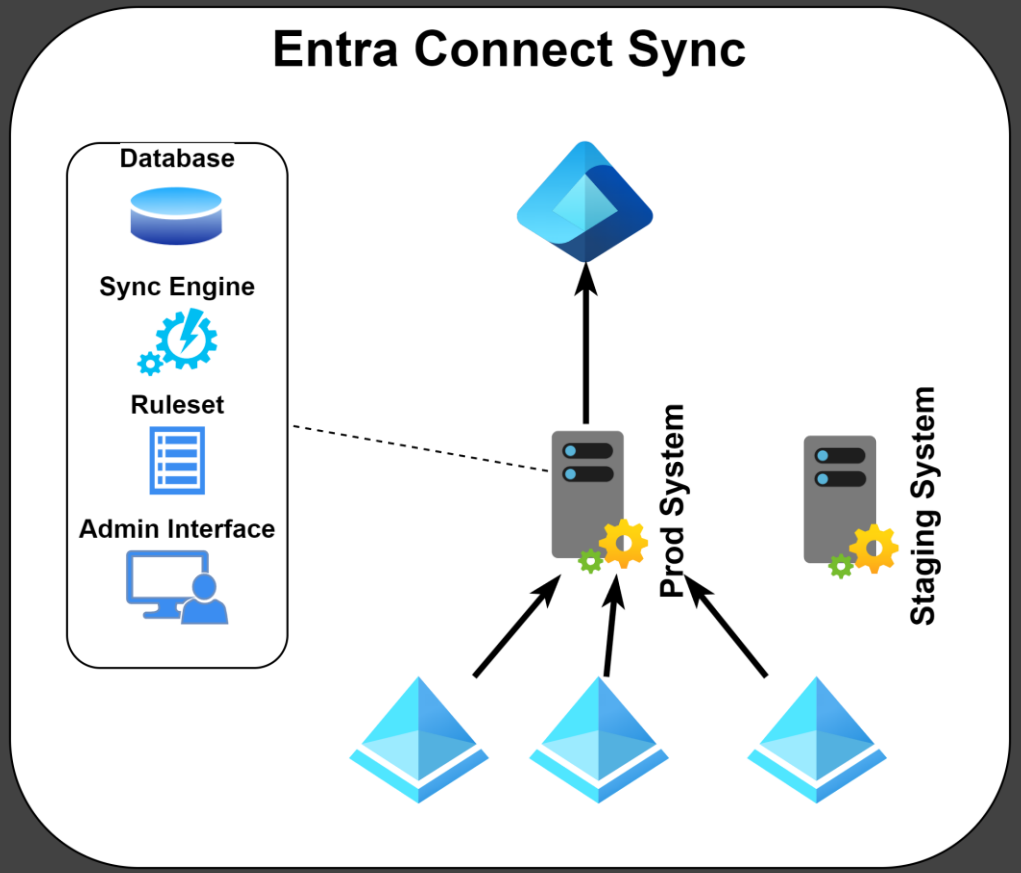
Attribute or object writeback

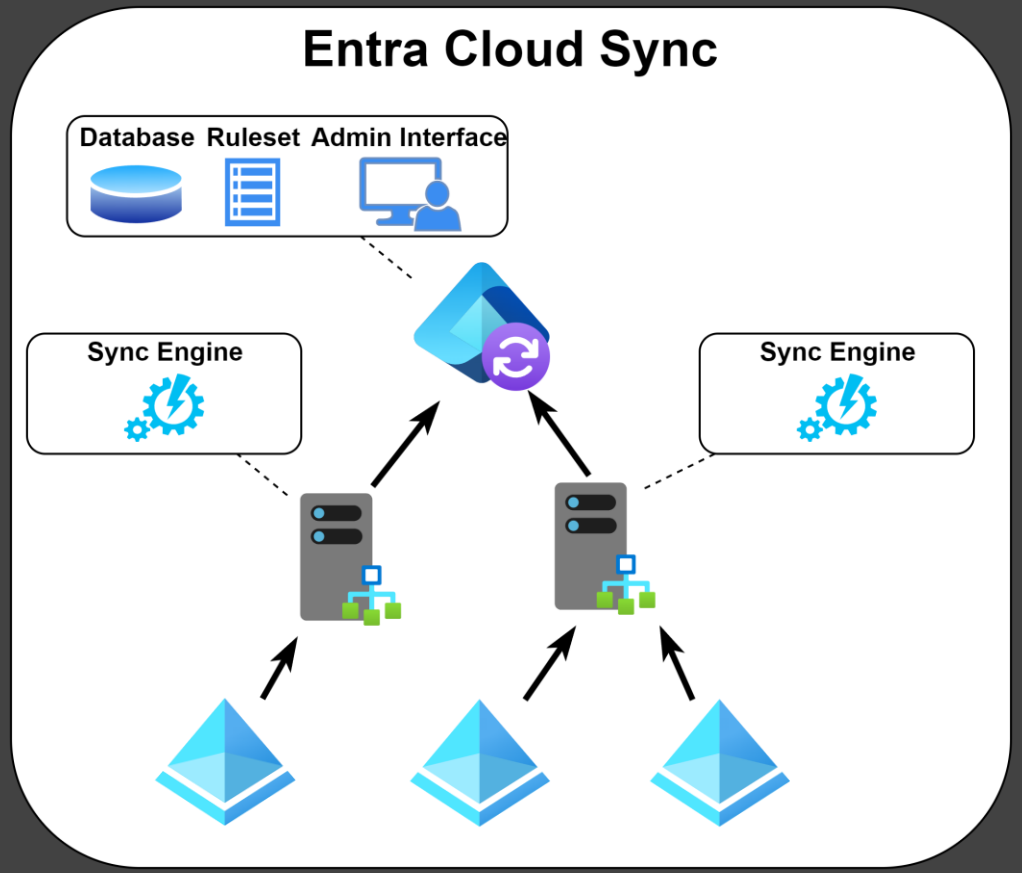
- Password attribute writeback
- ms-ds-consistencyGUID attribute writeback

- Device object writeback
- Group object writeback
- ~~User object writeback~~

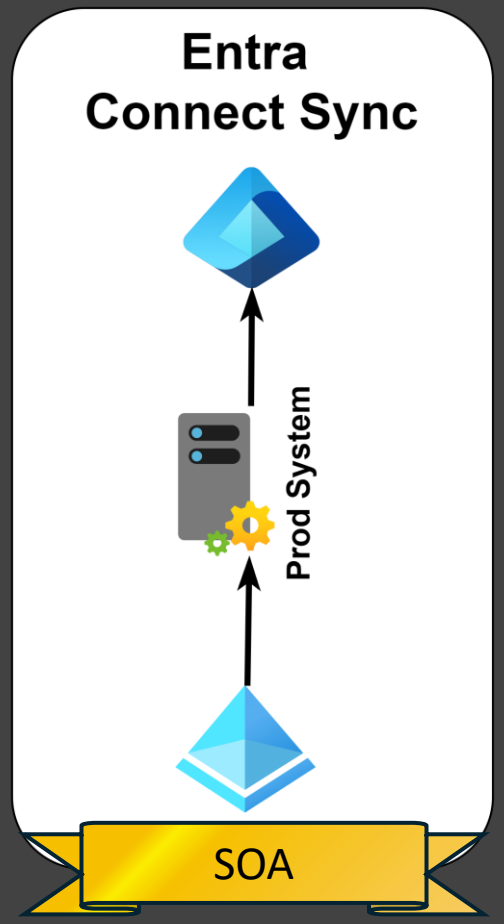


Methods to manage hybrid identities

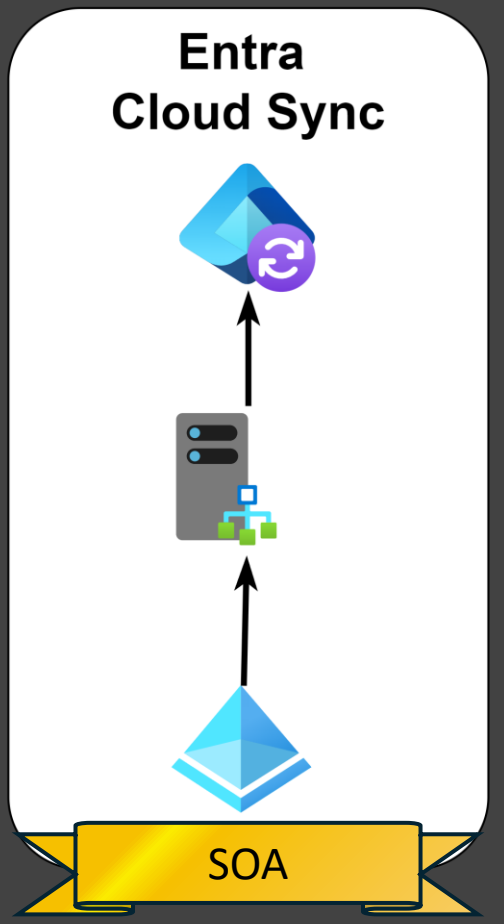




What are key difference in the tools



OnPrem Footprint	
Heavy	Light
Config and Database	
OnPrem	Cloud
Architecture	
Monolithic	Agentbased
Redundancy	
Hot Standby	Active-Active
Schedule	
every 30 Minutes	every 2 Minutes



Signature moves

Connect Sync

- Device Sync/Writeback
- Active / Passive (Staging)
- Pass-Trough Authentication
- Attribute Filter, Transformation, Customization
- Resource Forest
- Entra Domain Services
- Authenticate to Microsoft Entra ID using Application Identity
- ms-DS-ConsistencyGuid writeback

Cloud Sync

- Group Writeback
- High Availability (Active/Active)
- Disconnected environments
- Change of Authority (Preview)
- Provision on demand

Migration Blocker

- PTA / AD FS Deployment
  - **Solution: Use Password-Hash-Sync!**
- Windows Hello for Business
  - Key Trust & Certificate trust
  - **Solution: Cloud Kerberos Trust**
- Hybrid Devices
  - **Solution: Entra joined Clients and AVD/W365**
- Merging of two identities from different domains
  - **Solution: Move to a single user object**

but remember…


Why don’t we have both?
imgflip.com

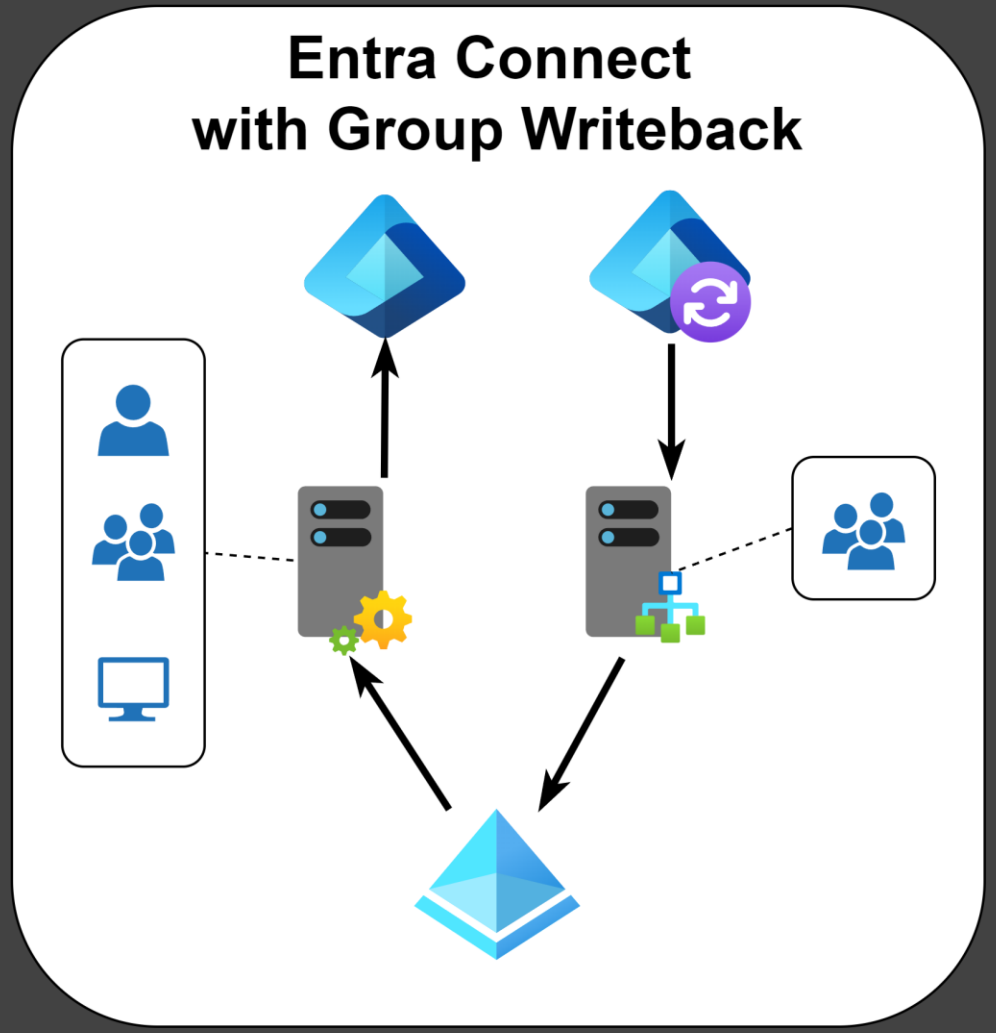
That’s why not both forever

> *We are investing all the new capabilities in Cloud Sync moving forward and the goal is to have one Sync Client for all our customers.*
>
> ***And that’s Cloud Sync […]***
>
> *- Dhanyah K, Microsoft PM for Entra Connect/Cloud Sync*

Coexistence Scenario #1

Add Cloud Sync to use Group Writeback

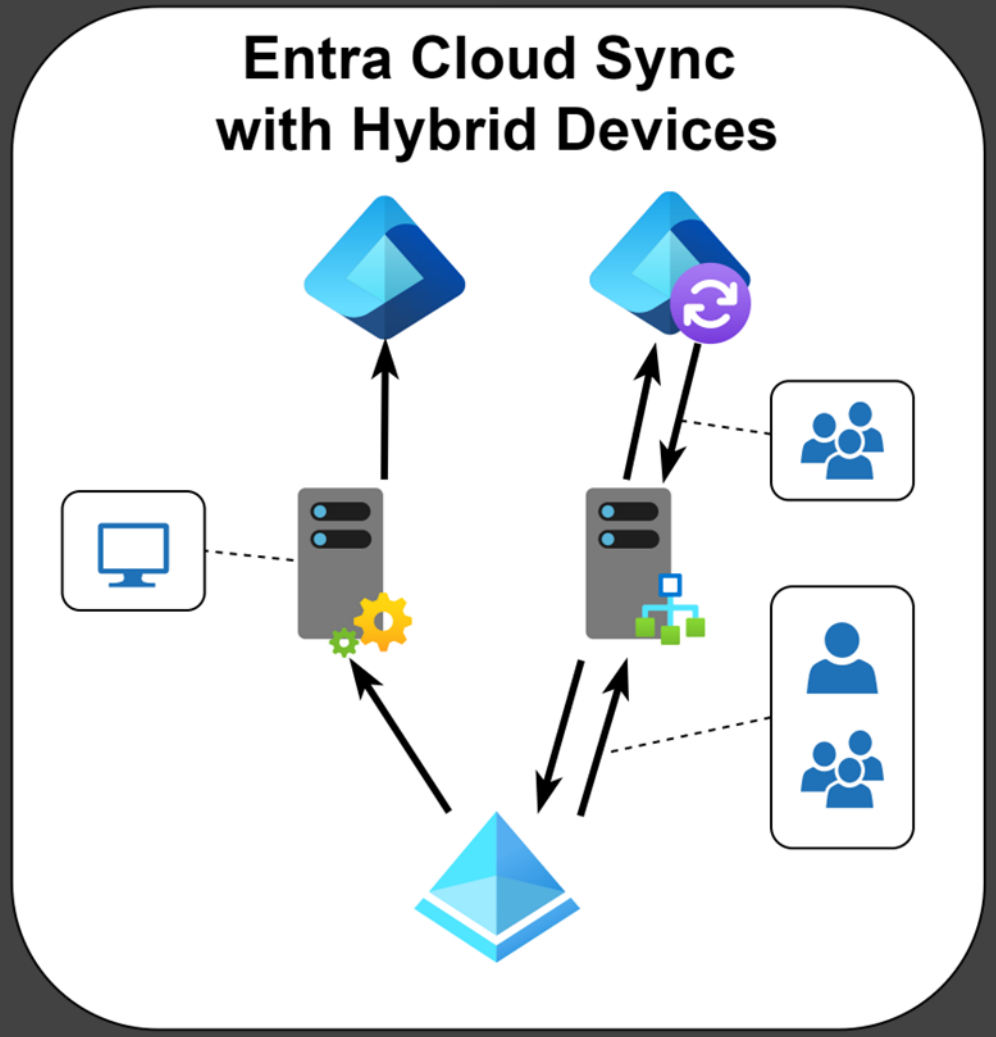
(until my migration blocker is solved)



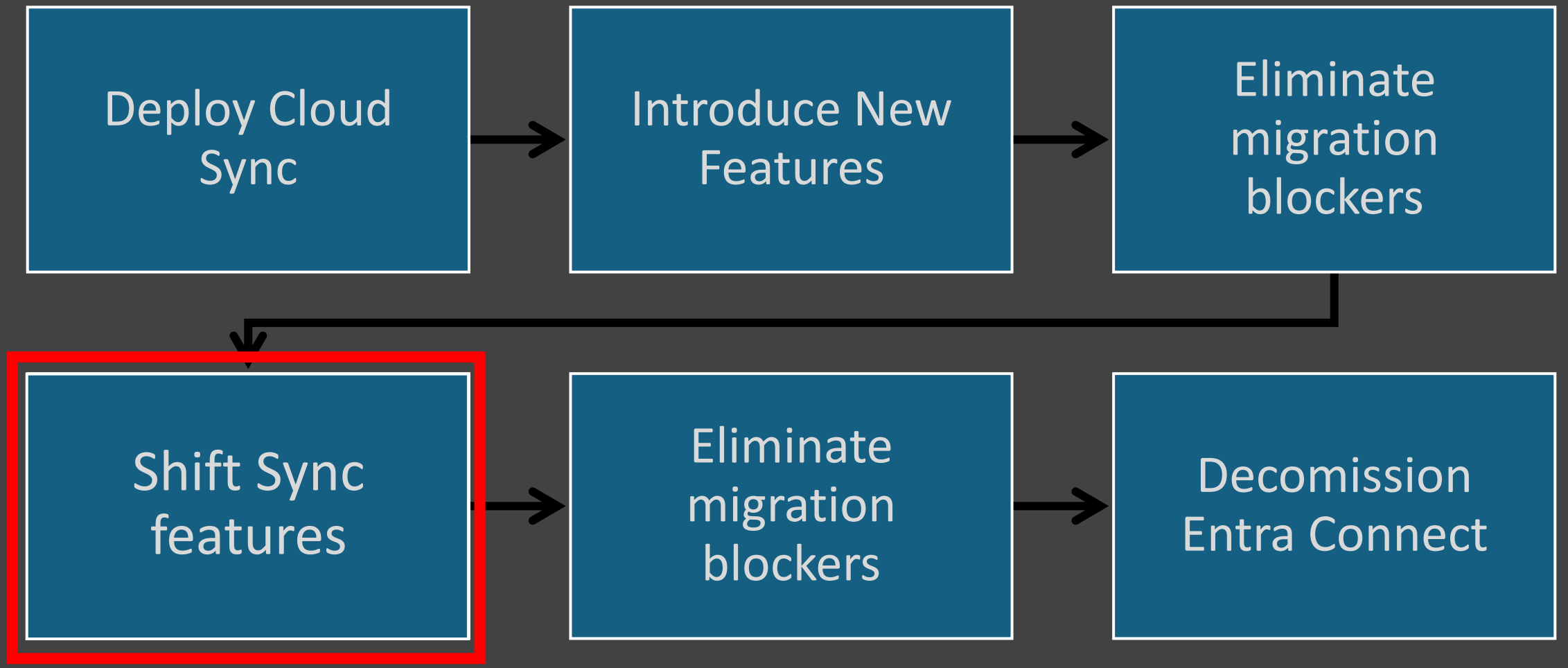
Coexistence Scenario #2

Keep Connect Sync for Hybrid-Joined Devices

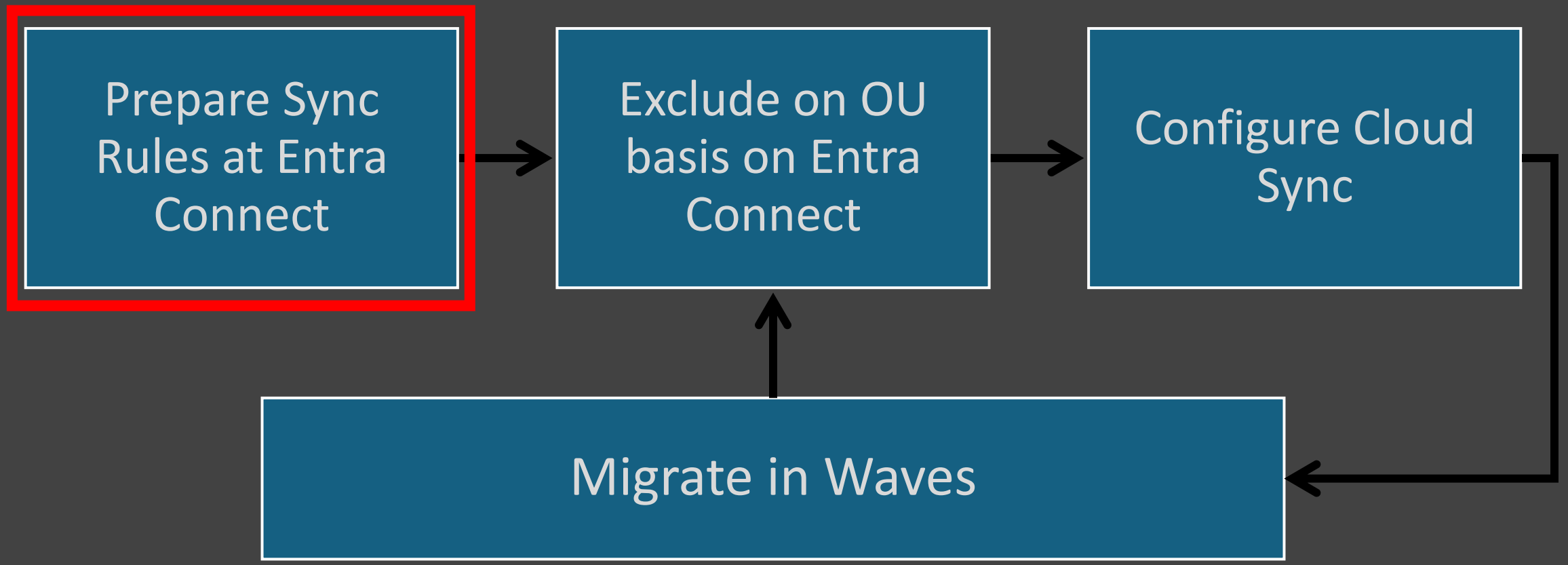
(until my migration blocker is solved)



Migration Path

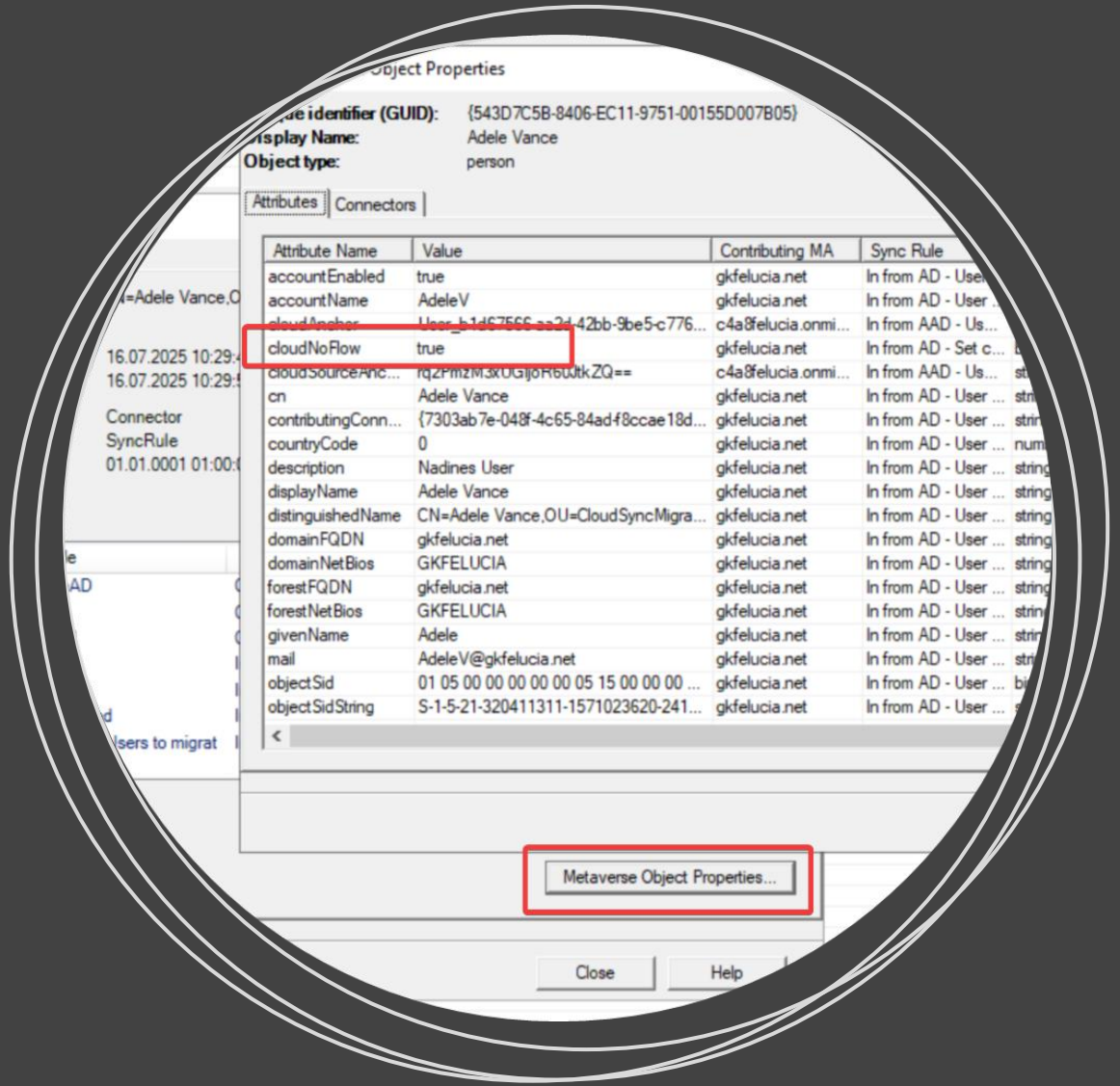


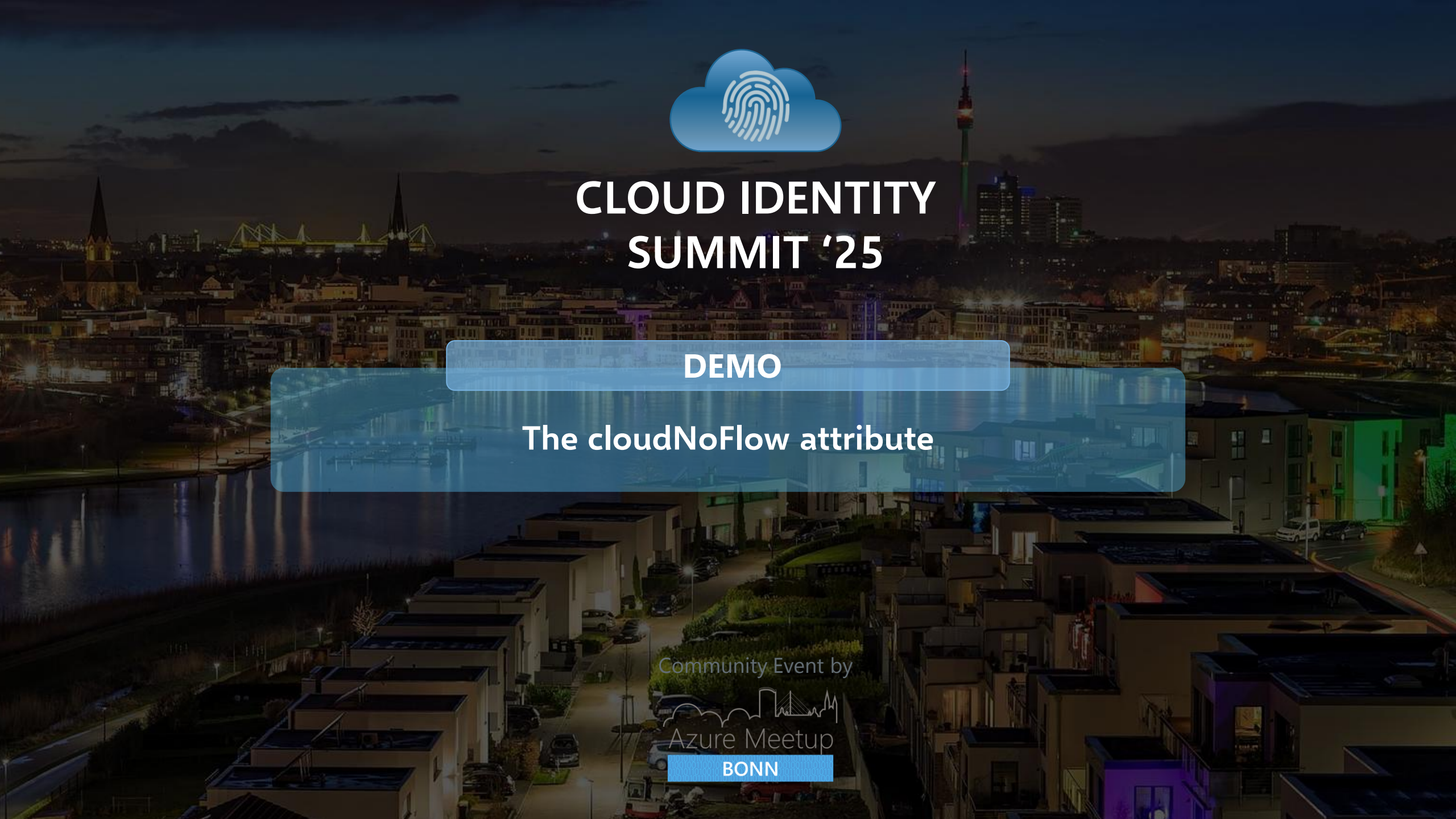
Shift Sync features



cloudNoFlow

- Special attribute
- Prevents change sync to Entra ID
- Exceptions:
  Attributes of type “Reference”
  - memberOf
  - manager
  - …





CLOUD IDENTITY SUMMIT ‘25

DEMO

The cloudNoFlow attribute

Community Event by

Azure Meetup BONN

Migration Takeaways

Never deselect OUs in Entra Connect while migration!

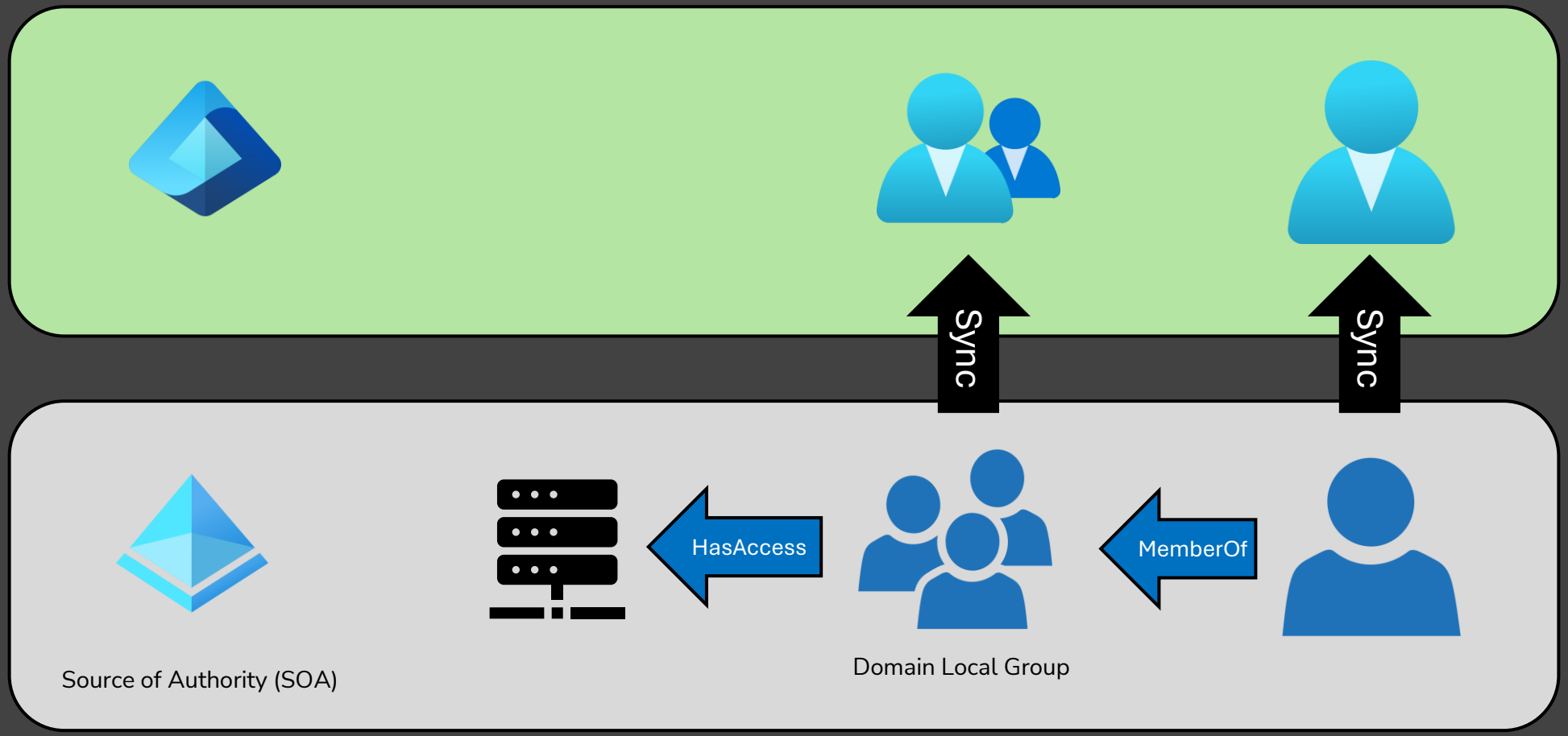
More Migration Takeaways

- ✓ The “shift sync feature” phase should be short
  - ✓ The necessary changes are unintuitive and error-prone
  - ✓ The changes made by Entra Connect are not switched off completely (References)
- ✓ Entra Cloud Sync has no exclude option for OUs
  - ✓ Consider to sync the whole directory
  - ✓ Consider to rearrange your OU structure (yeah – I know…)
- ✓ After config changes you should “restart provisioning” aka Full Sync
- ✓ A sync is now done every two minutes 🚀

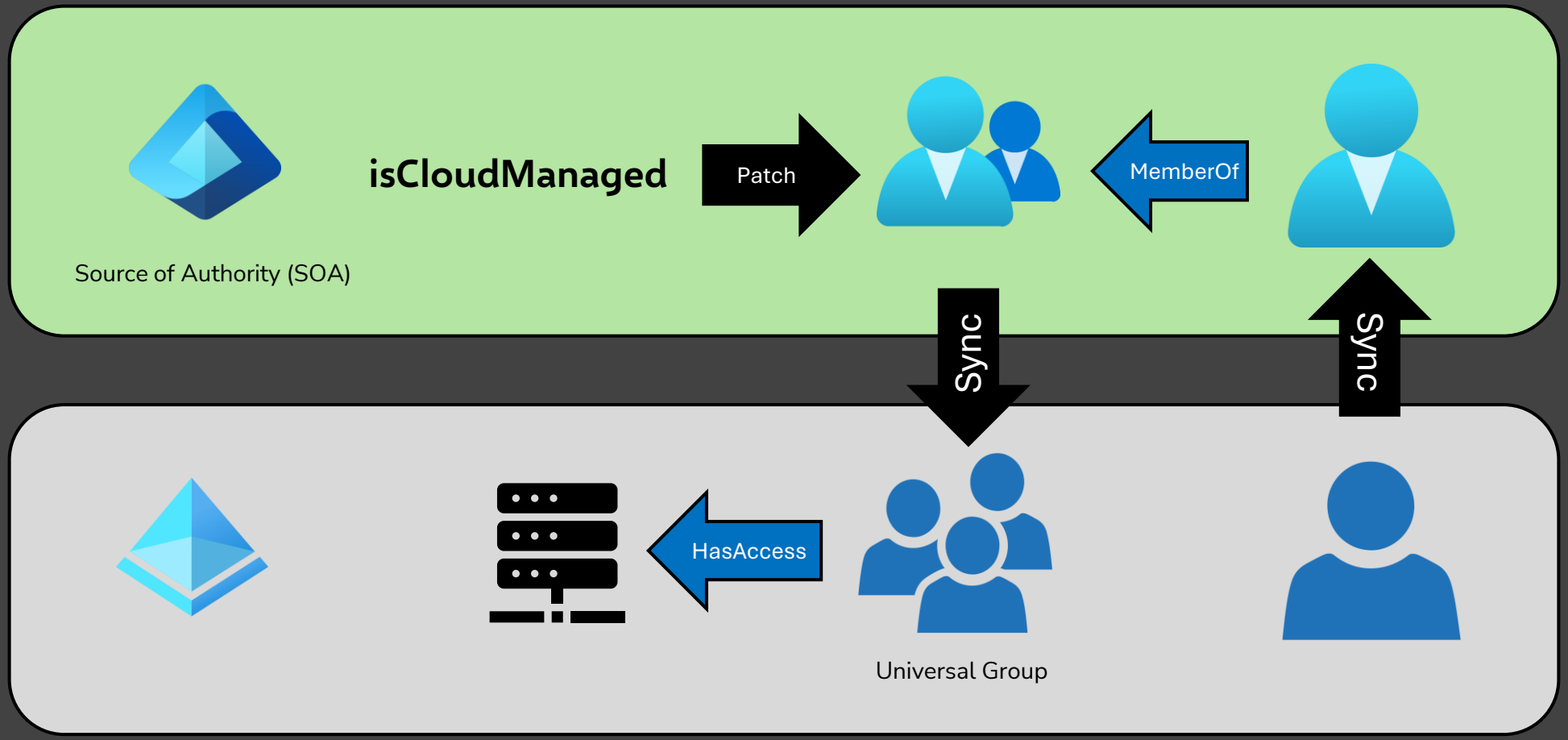
Change of Source of Authority

Migrate to cloud-based management with write-back

Classic hybrid group management



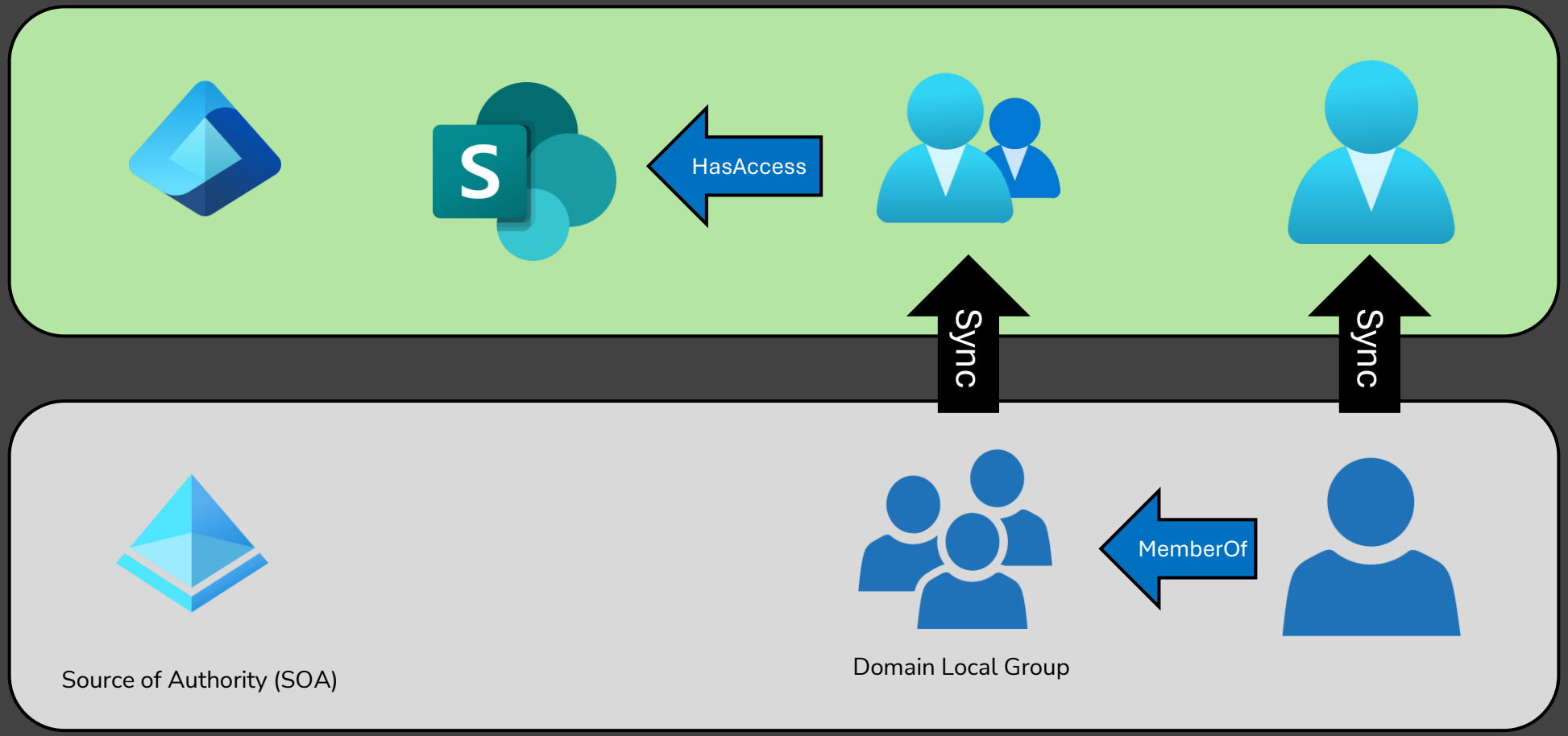
Change of Source of Authority #1



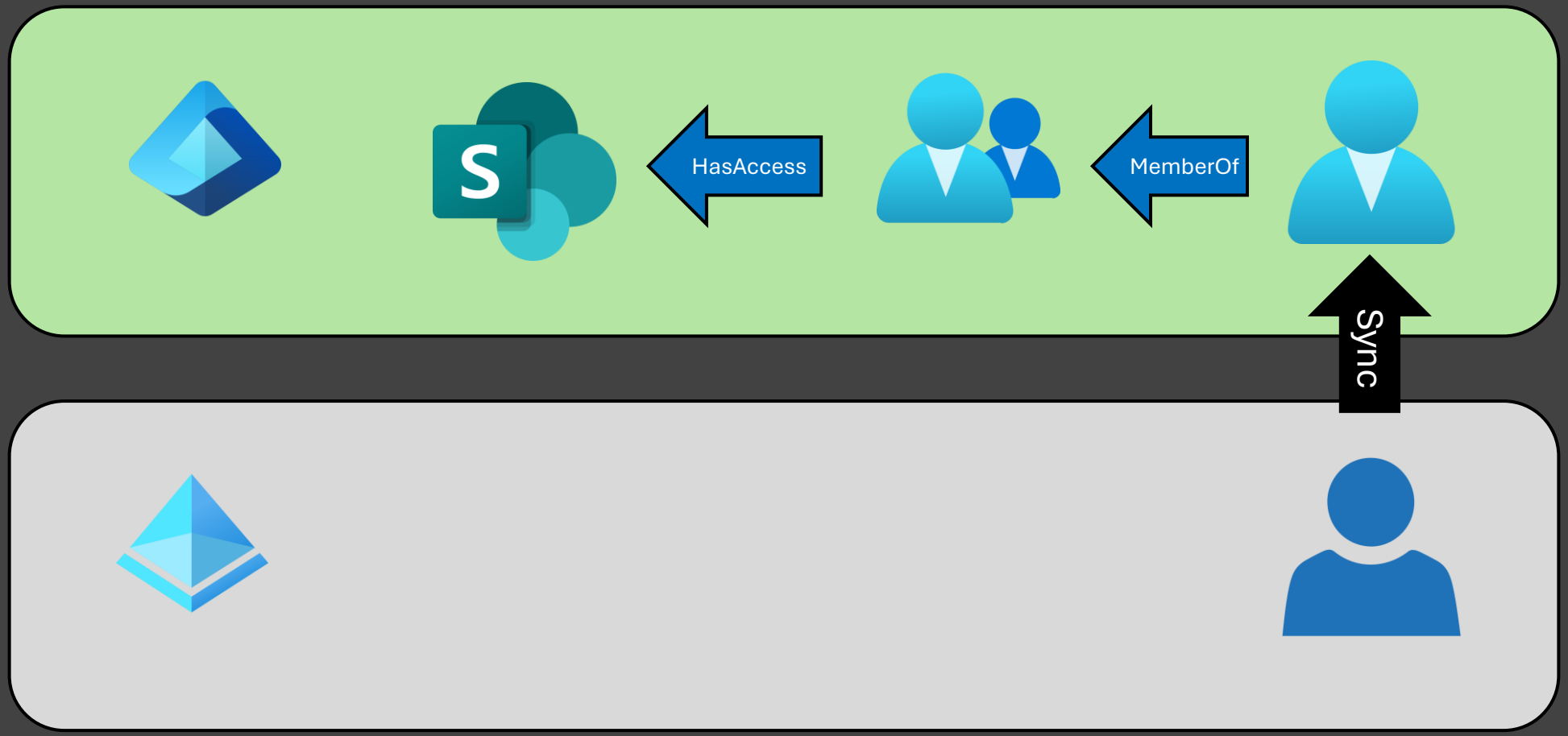
Scenario #2

Move to fully cloud managed

Cloud hybrid group management



Change of Source of Authority #2



CLOUD IDENTITY SUMMIT ‘25

DEMO

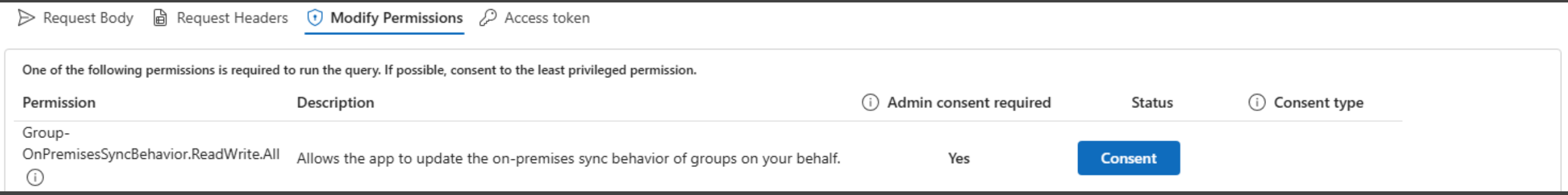
The isCloudManaged attribute

Community Event by

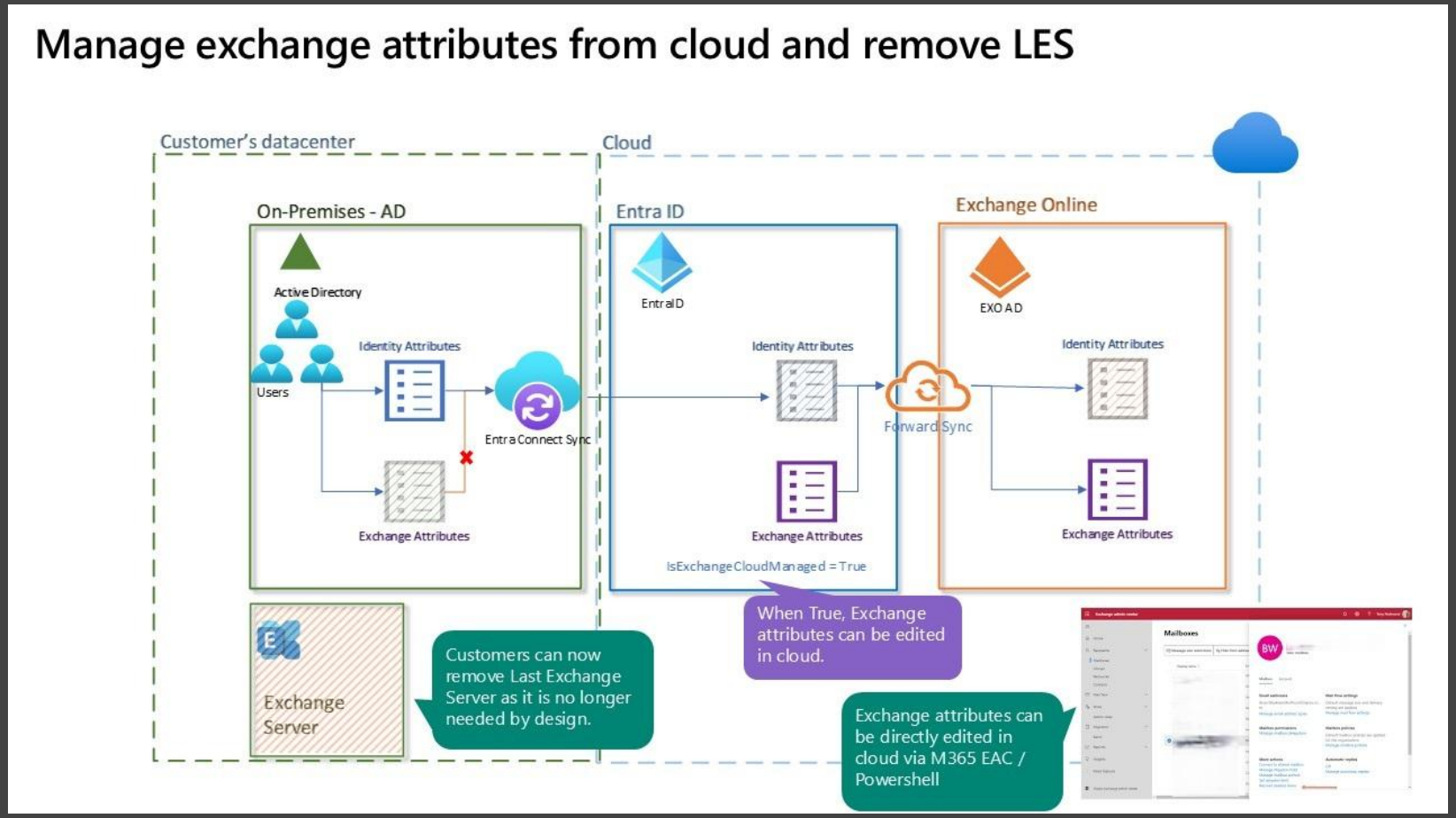
Azure Meetup BONN

SOA Takeaways

- ✓ Convert groups that need write-back to Universal
- ✓ Make sure the write-back scope can access the group or the group is moved
- ✓ There is no indication of the change on-prem.
  Delete the group as soon as possible if no longer needed
- ✓ You can revert the change by setting IsCloudManaged = false
- ✓ Graph Permission Consent required



Cloud-Managed Remote Mailboxes



Source: https://learn.microsoft.com/en-us/exchange/hybrid-deployment/enable-exchange-attributes-cloud-management#identity-exchange-attributes-and-writeback

Cloud-Managed Remote Mailboxes

- New attribute: IsExchangeCloudManaged
- Replacement for Last Exchange Server on-prem
- Only 23 Exchange attributes support write-back
  - 20x ExtensionAttributes
  - msExchRecipientDisplayType
  - msExchRecipientTypeDetails
  - proxyAddresses
- It’s the exception from the “Entra Cloud Sync First” rule
  - Currently: Only Entra ID Connect
  - Future: Entra Cloud Sync
- No solution for a local mail relay

THE SENDMAN

SAY GOODNIGHT TO YOUR LAST EXCHANGE SERVER

Sendman Private Preview Signup

Let’s talk security

Security - Authentication

- Entra Connect
  - On-premises
    - Legacy service user with password stored in the Connect database
  - Cloud
    - User and password stored in the Connect database
    - Certificate based authentication with TPM support (since 2025)
- Entra Cloud Sync
  - On-premises
    - Group Managed Service Account
  - Cloud
    - Hybrid Identity Service (HIS) Registration Service
    - Certificate based authentication

Security - AD least privileged

Entra Connect

- ms-DS-ConsistencyGuid
- **Password hash sync**
- Password writeback
- Exchange hybrid
- Exchange Mail Public Folder
- Device writeback

Entra Cloud Sync

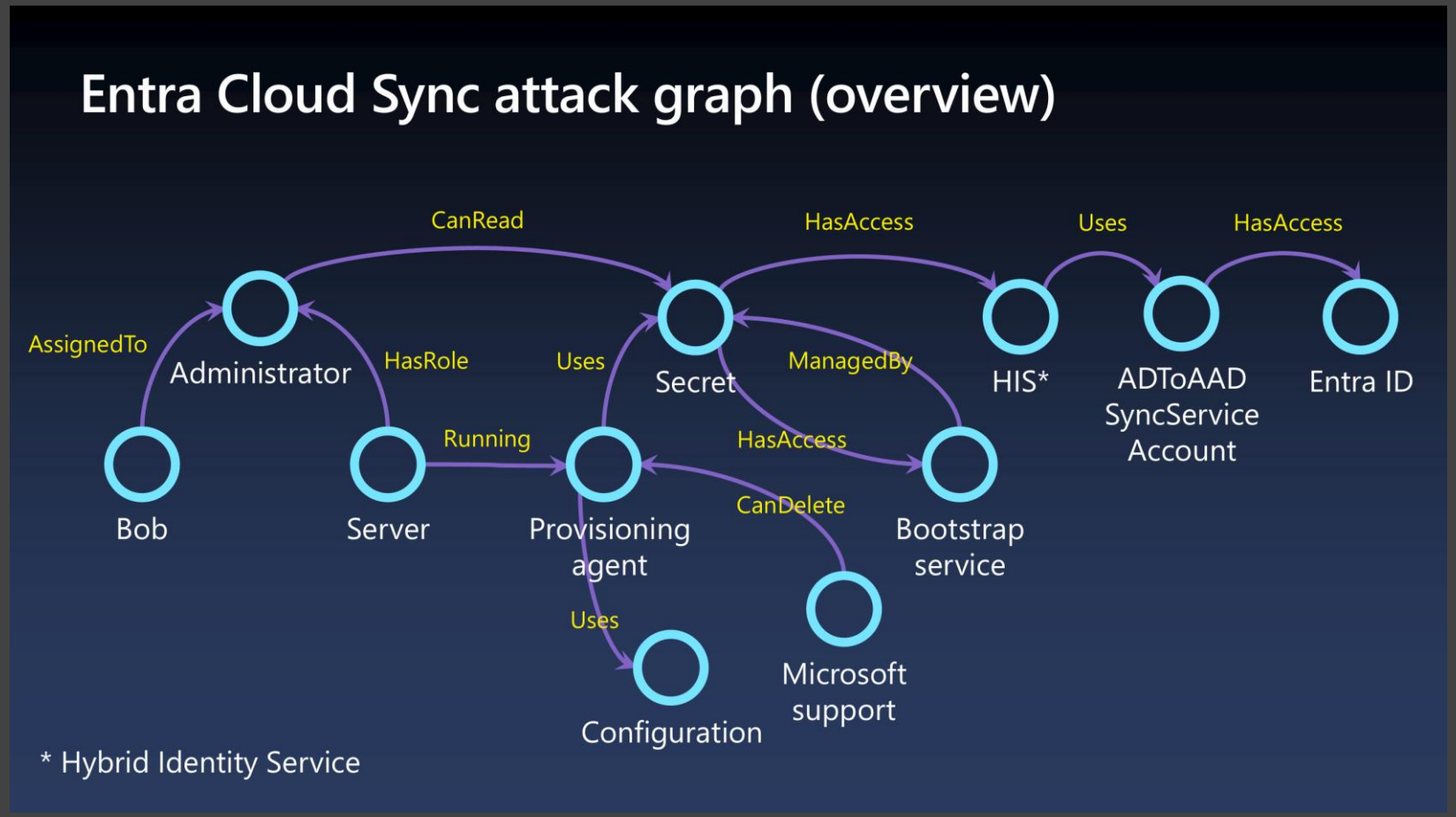
- BasicRead
- **Password hash sync**
- Password writeback
- Exchange hybrid
- Exchange Mail Public Folder
- UserGroupCreateDelete

https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/how-to-gmsa-cmdlets#using-set-aadcloudsyncpermissions
https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-accounts-permissions

Security - Attack points

- Entra Connect
  - Local user and password stored in DB
  - Cloud user and password stored in DB
  - Certificate can be protected in TPM / HSM
    Signing a asseration is still possible, allows to add new certificate as a backdoor
- Entra Cloud Sync
  - Local agent certificate can be extracted and used to plant a backdoor agent
  - gMSA is bound to the device, no attack known

Cloud Sync - Attack paths



Source: Dr. AzureAD

Sync compromise == Entra compromise ?

Since the last hardening measures of Microsoft, you need in addition:

- Synced Admins
- No or partial MFA (or device) enforcement

Sync compromise == AD compromise ?

Depending on the privileges of the gMSA:

- PHS = Full compromise
- Connect Sync = All Domains
- Cloud Sync = maybe only a subset

Security - Remediation

- Entra Connect
  - Rotate password of local user account
  - Rotate password of cloud sync account
  - Remove unknown certificates from service principal
  - Rotate certificate for cloud sync service principal
- Entra Cloud Sync
  - Call **Microsoft** to request removal of the malicious agent
  - Recreate the group managed service account

Security - Recommendations

- Protect all Sync Servers like any other tier 0 system
- Onboard those systems to Defender for Identity
- Minimize lateral movement paths
  - Don’t sync users that have privileged roles in Entra ID
  - Don’t sync users that have any privileged role in any RBAC system
  - Enforce MFA: everytime, everywhere
  - Enforce compliant devices
  - Use PAW devices for privileged accounts
- Adopt your detection for certificate based Entra Connect

- Unrelated but: Disable Seamless Single Sign On 😅

An Outlook from the Exchange Team

Object-Level SOA for Users, Groups, and Contacts

We are in the process of developing Object-Level SOA management for `Users`, `Groups`, and `Contacts`. This functionality is intended to assist organizations seeking to decommission both on-premises Exchange Servers and Active Directory. With this feature, the SOA of individual objects - such as `Users`, `Groups`, and `Contacts` - can be migrated to the cloud at the object level. Comprehensive support for User SOA, Group SOA, and Contact SOA will enable full cloud-based management of entities originally created on-premises, once migration is complete. Although `User` and `Contacts` SOA are not yet available, `Group` SOA - which enables you to migrate the SOA of an entire group to the cloud - is now available for you to try.

Source: https://learn.microsoft.com/en-us/exchange/hybrid-deployment/enable-exchange-attributes-cloud-management#identity-exchange-attributes-and-writeback


GO MIGRATE

CLOUD IDENTITY SUMMIT '25

Thanks to our sponsors

Gold Sponsors

adesso

e·on

glueck kanja

TOKEN swiss made software

Silver Sponsors

Omada

SOFTWARE CENTRAL_TENANTMGR

Bronze Sponsors

MSC Cyber Guard GmbH

water IT Security & Defense

CLOUD IDENTITY SUMMIT '25

Ask Me Anything (AMA)

Roundtable discussion and Q&A
on experiences from the field and current trends!

Meet the speakers and exchange
with members of the community!

4:30 PM @Community and Sponsor Area

Community Event by

Azure Meetup
BONN

CLOUD IDENTITY SUMMIT ‘25

Your Feedback is Important!

https://www.identitysummit.cloud/feedback/

Community Event by

Azure Meetup BONN