www.workplaceninjas.us

Is Entra Connect Sync Still the Best Choice? Let's Sync About It!

Workplace Ninjas

Thank you Sponsors

Gold Sponsors

Microsoft

RECAST SOFTWARE

control up

robopack

empowered by SOFTWARE CENTRAL

DEVICIE

PATCH MY PC

nerdio

Silver Sponsors

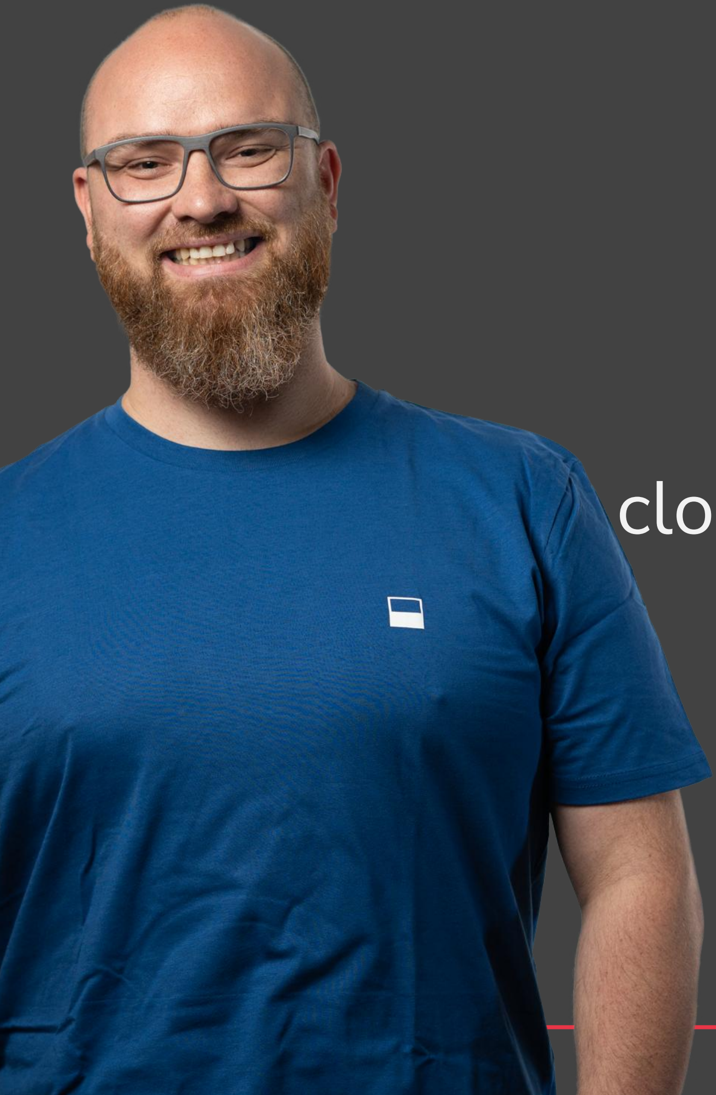
numecent®

CLOUDPAGING DELIVERS

CONTRAFORCE

Rimo3

About us



Fabian Bader		Chris Brumm
@fabian_bader	𝕏	@cbrhh
/in/fabianbader	in	/in/christopherbrumm
cloudbrothers.info	⌂	chris-brumm.com

Cyber Security Architects

@

glueck kanja

Microsoft MVPs

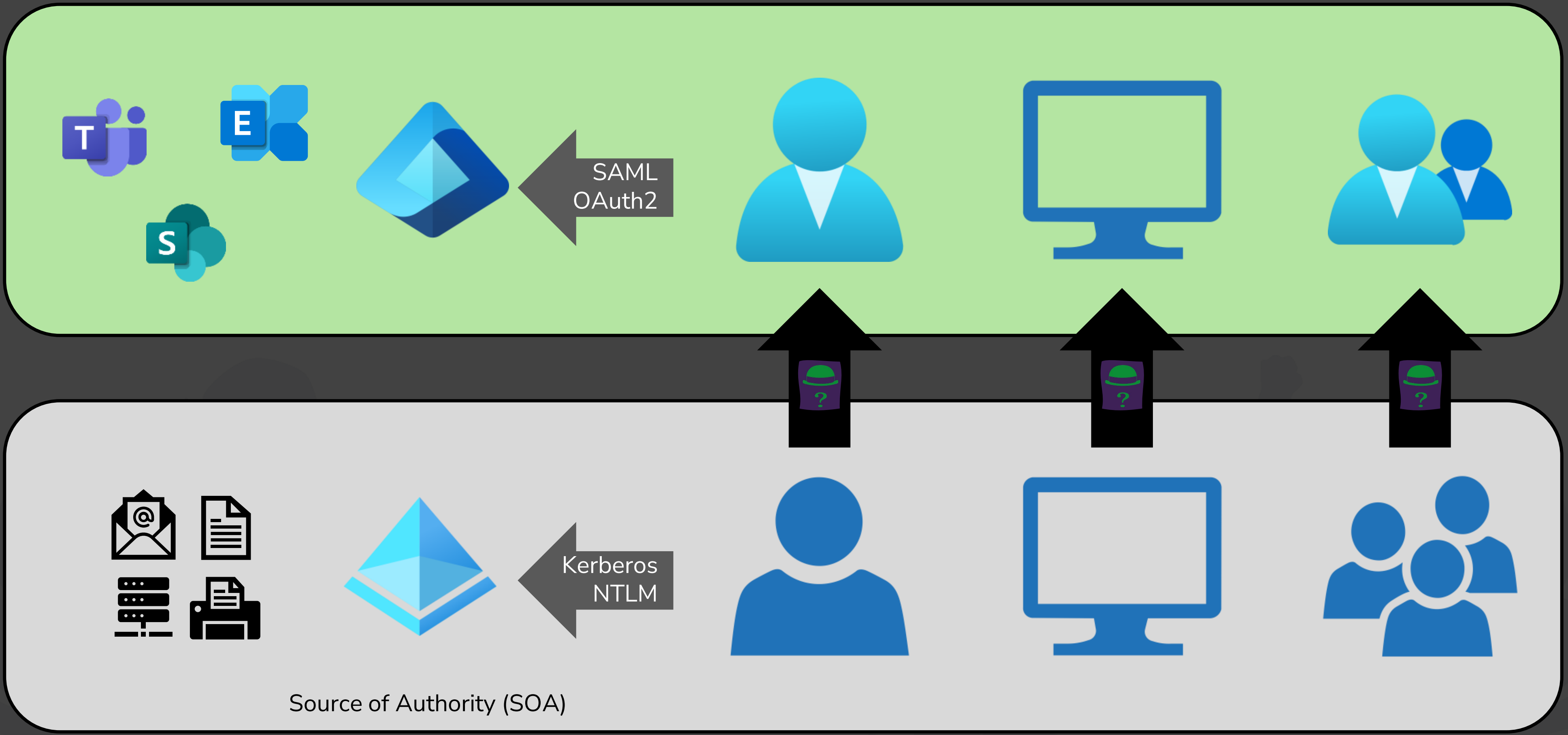
Object limitations

Entra Clouds Sync
supports
only
150.000 objects

Agenda

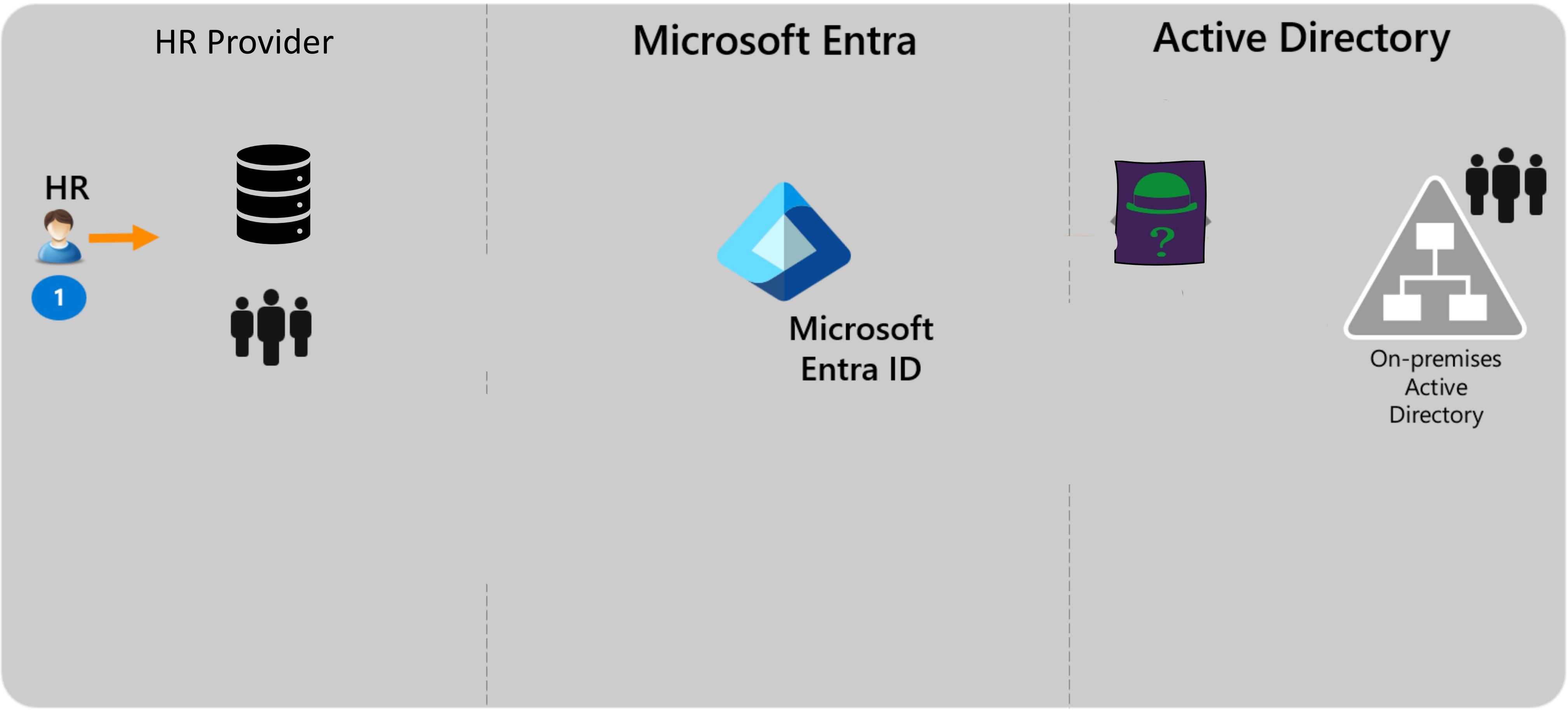
- Hybrid Identities - The tale of two sync engines
- Key differences
- Migration
- Coexistence
- Change of Source of Authority
- Security Implications

Introduction to Hybrid Identities



Source of Authority (SOA)

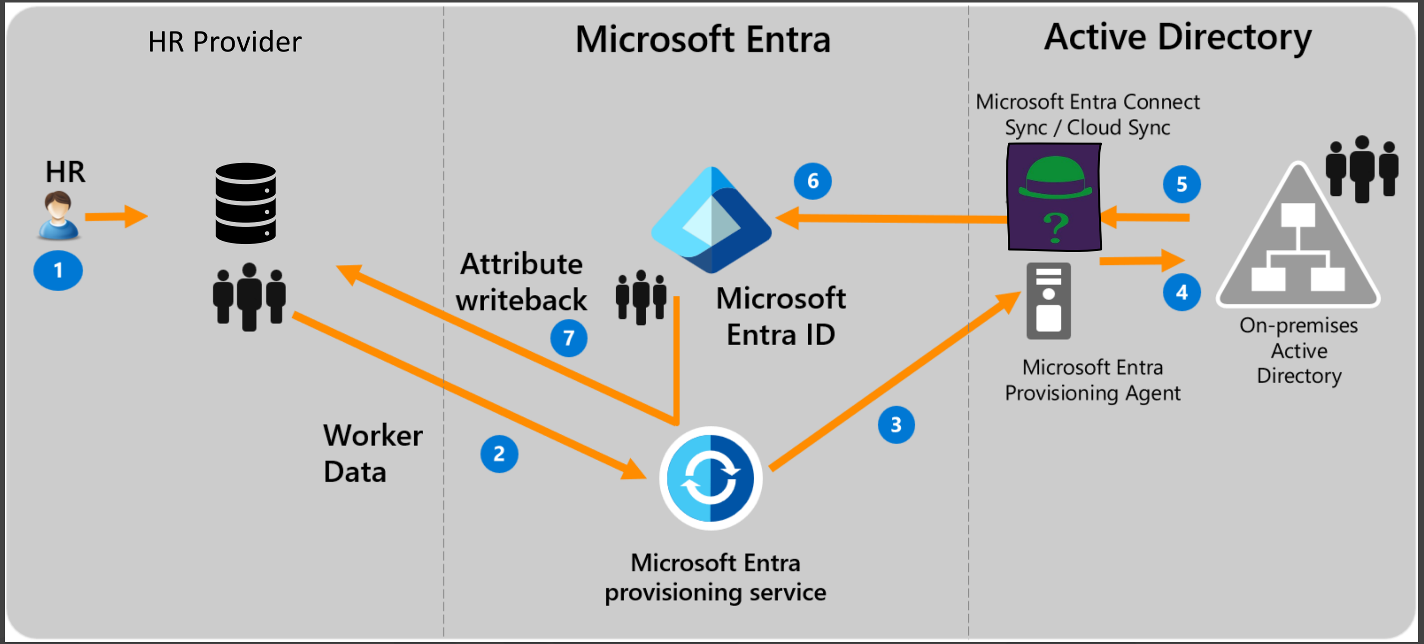
External HR provider



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)

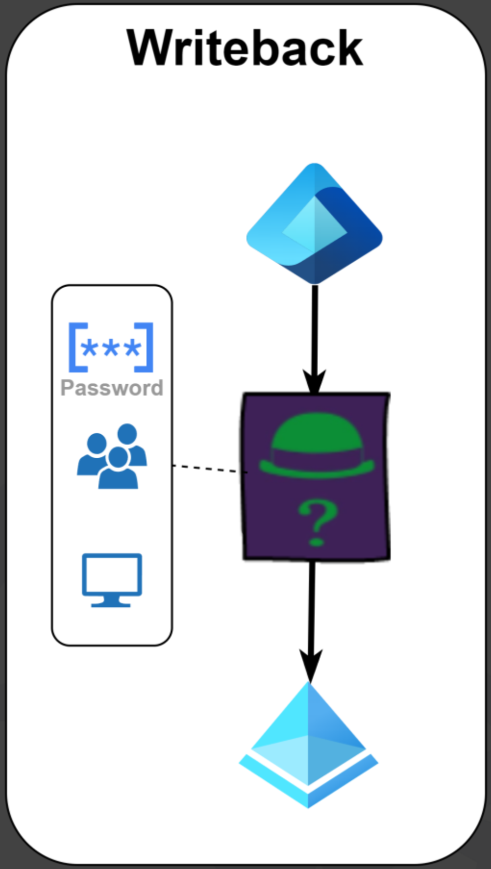


HR Provider
Microsoft Entra
Active Directory
HR
1
Microsoft Entra Connect Sync / Cloud Sync
6
5
4
Attribute writeback
7
Microsoft Entra ID
Microsoft Entra Provisioning Agent
On-premises Active Directory
Worker Data
2
3
Microsoft Entra provisioning service

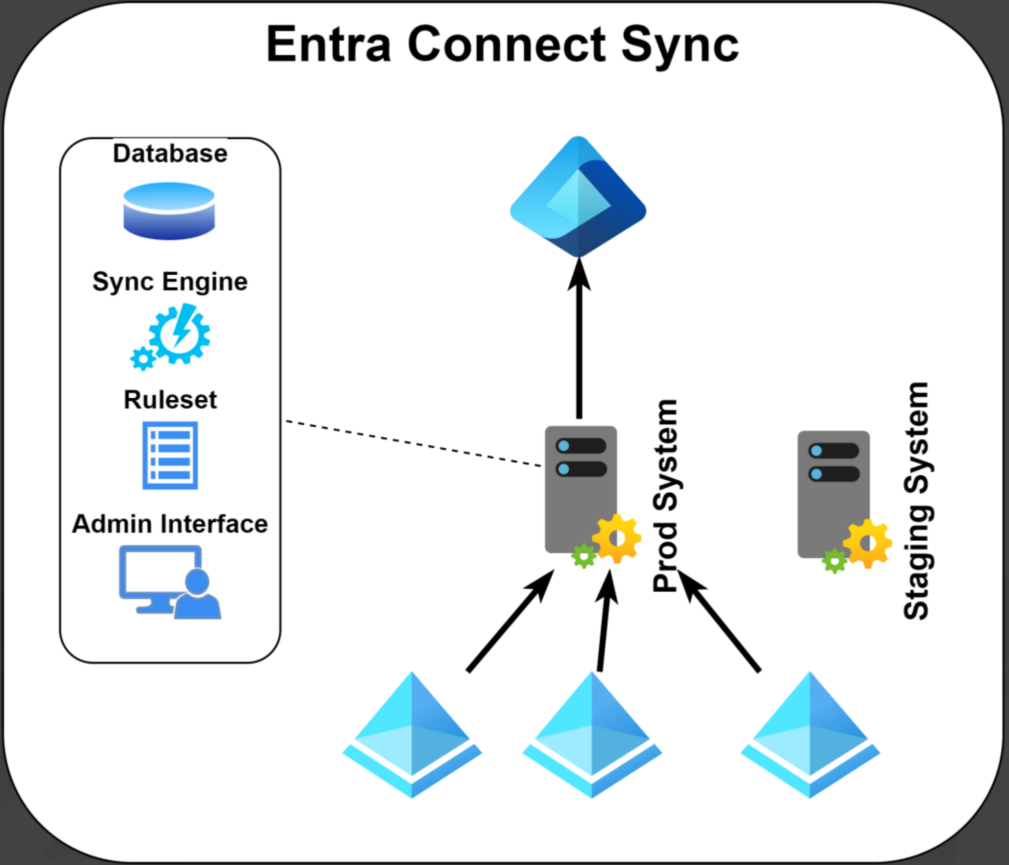
Attribute or object writeback

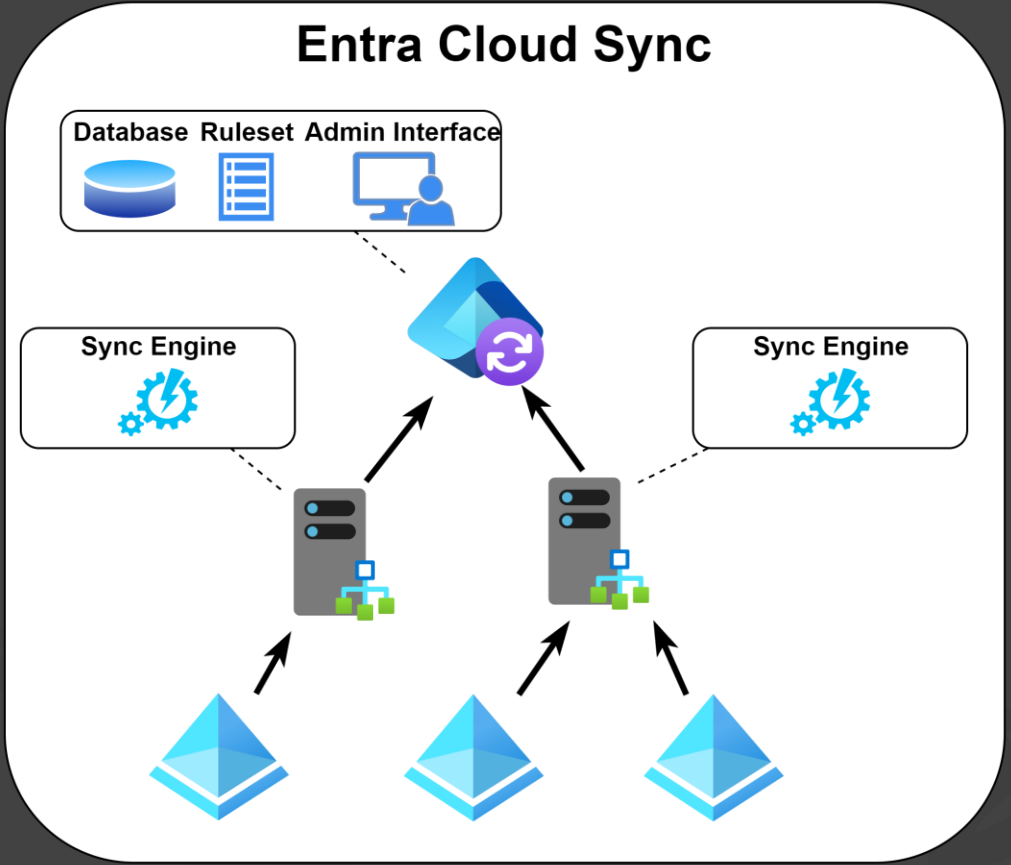
- Password attribute writeback
- ms-ds-consistencyGUID attribute writeback

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

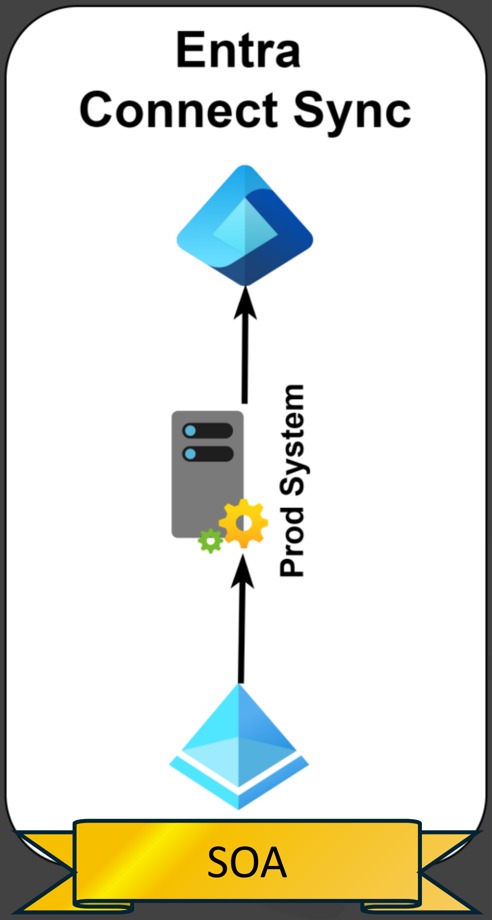


Methods to manage hybrid identities

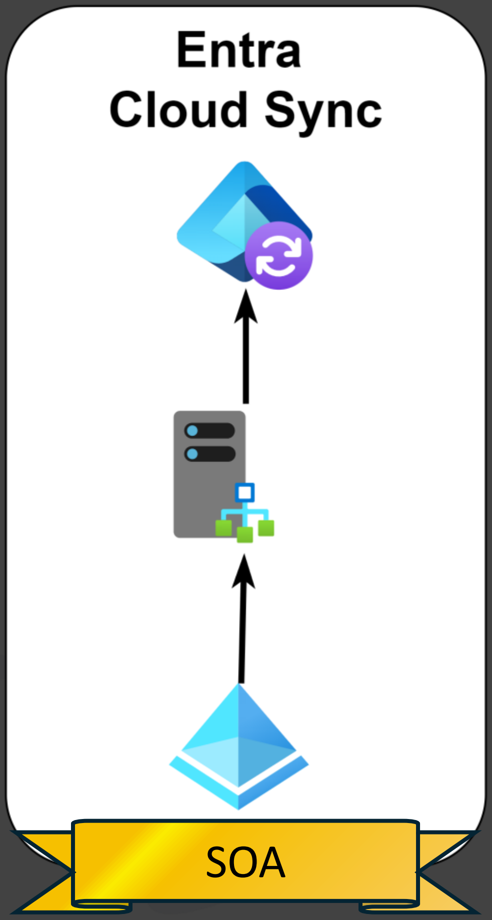




What are key difference in the tools



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

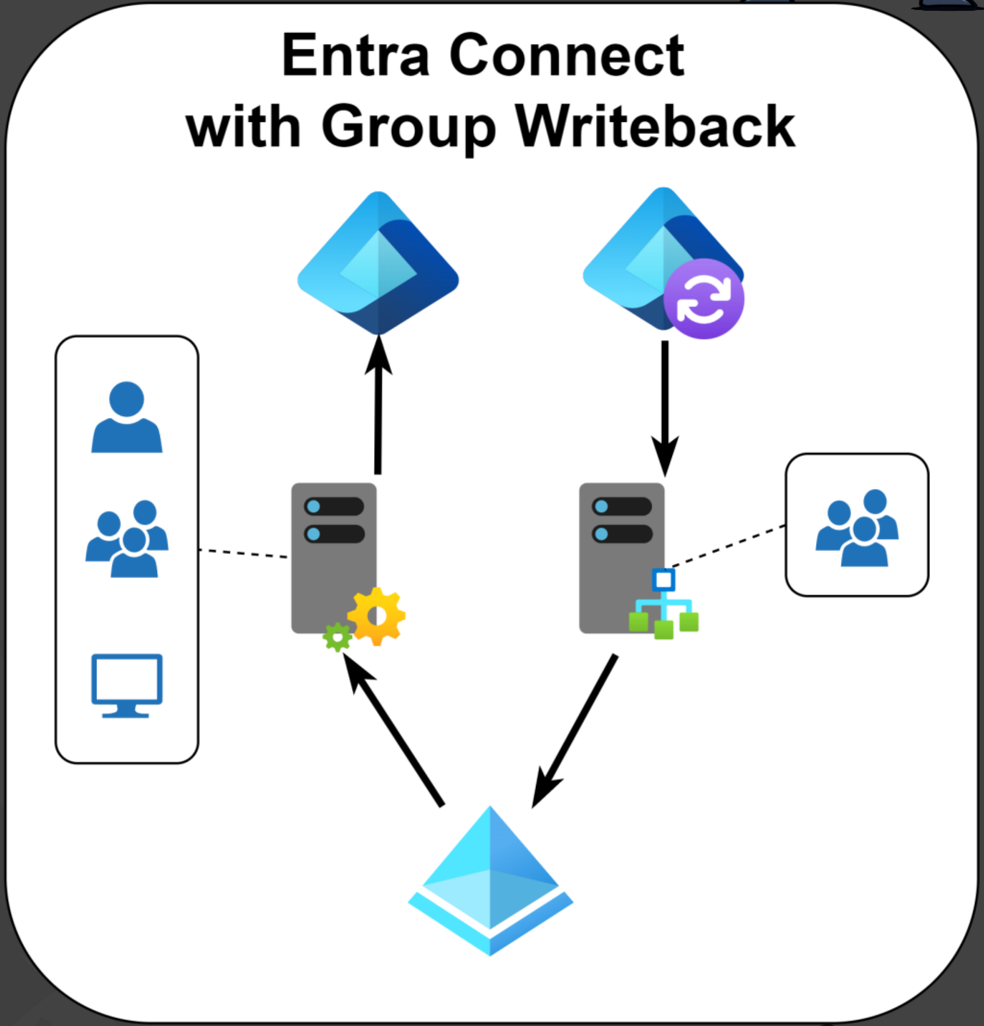
> *We are investing all the new capabilities in Cloud Sync moving forward and the goal is to have one Sync Client for all our customers.*
>
> ***And that’s Cloud Sync […]***
>
> *- Dhanyah K, Microsoft PM for Entra Connect/Cloud Sync*

ENTRA. CHAT
Dhanyah K, Microsoft PM for Entra Connect/Cloud Sync
We are investing all the new
Watch full episode @ https://entra.chat

Coexistence Scenario #1

Add Cloud Sync to use Group Writeback

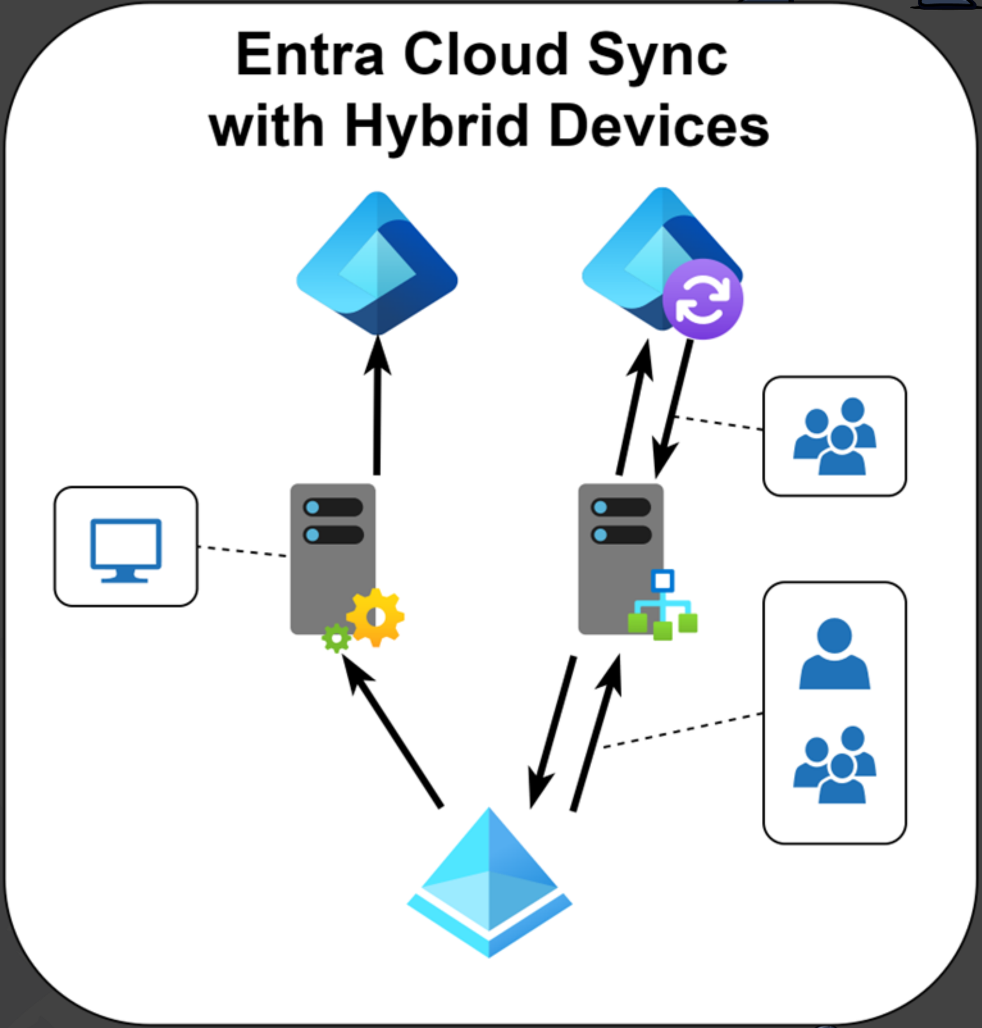
(until my migration blocker is solved)



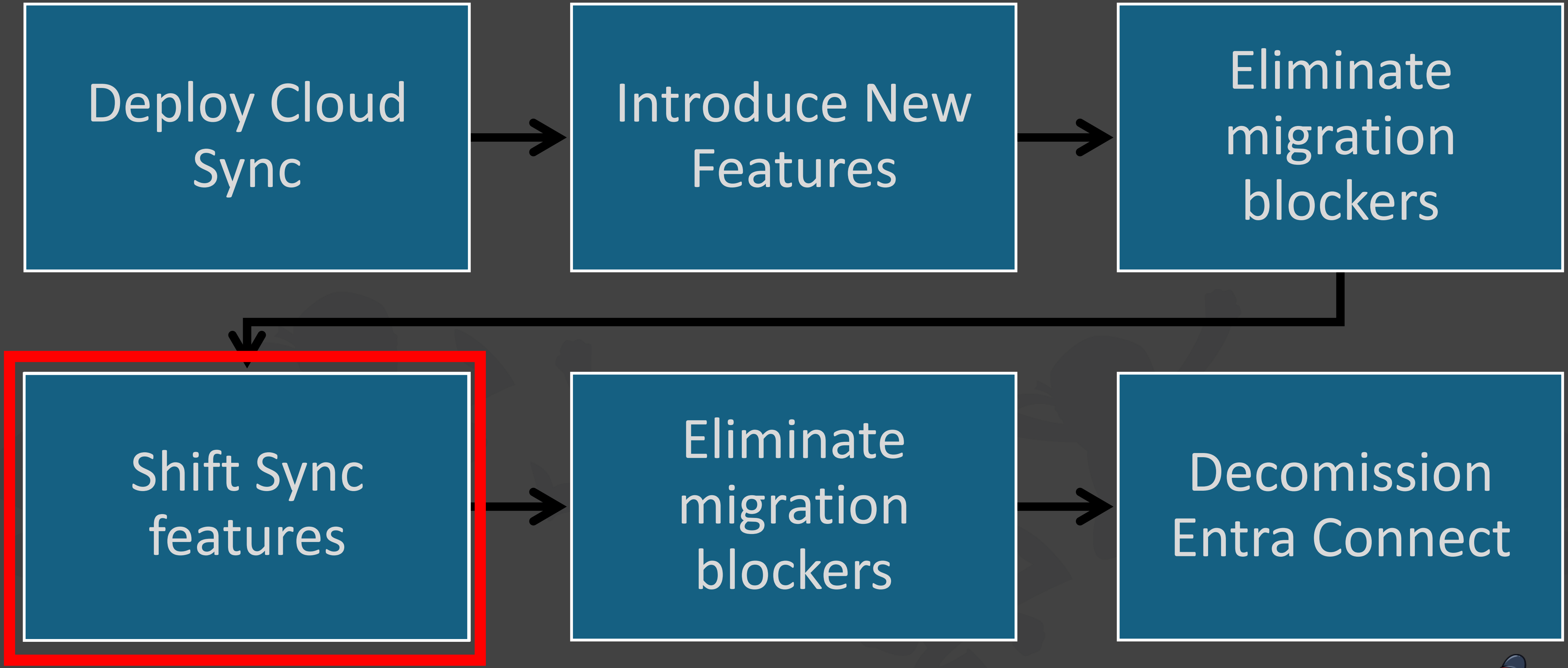
Coexistence Scenario #2

Keep Connect Sync for Hybrid-Joined Devices

(until my migration blocker is solved)



Migration Path



Deploy Cloud Sync

Introduce New Features

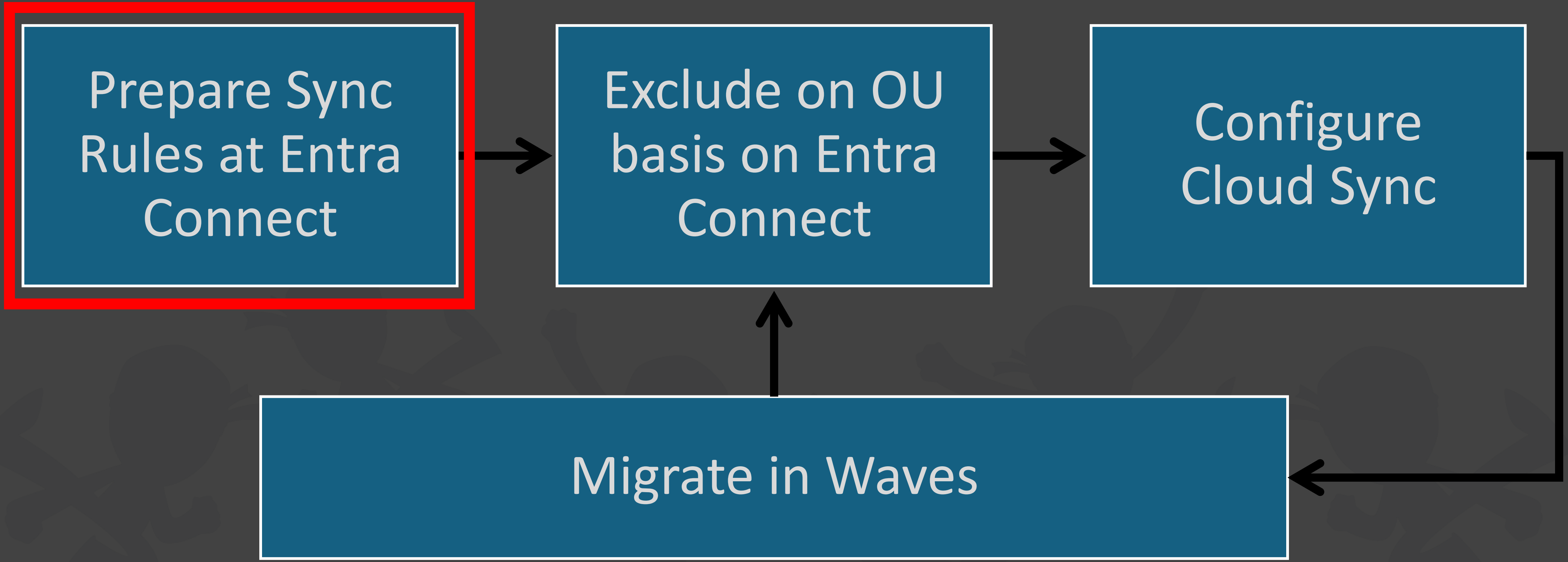
Eliminate migration blockers

Shift Sync features

Eliminate migration blockers

Decomission Entra Connect

Shift Sync features



Prepare Sync Rules at Entra Connect

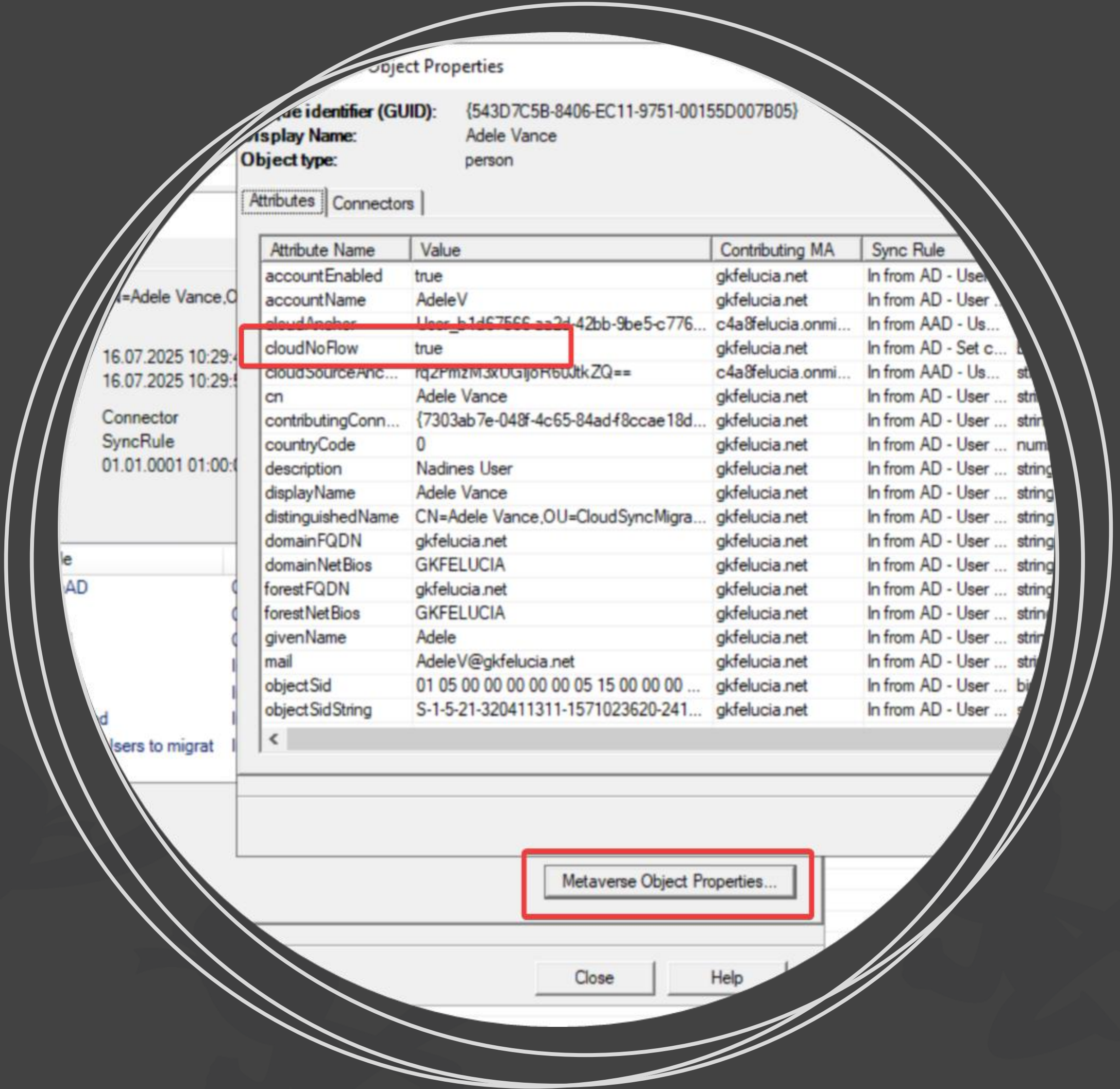
Exclude on OU basis on Entra Connect

Configure Cloud Sync

Migrate in Waves

cloudNoFlow

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



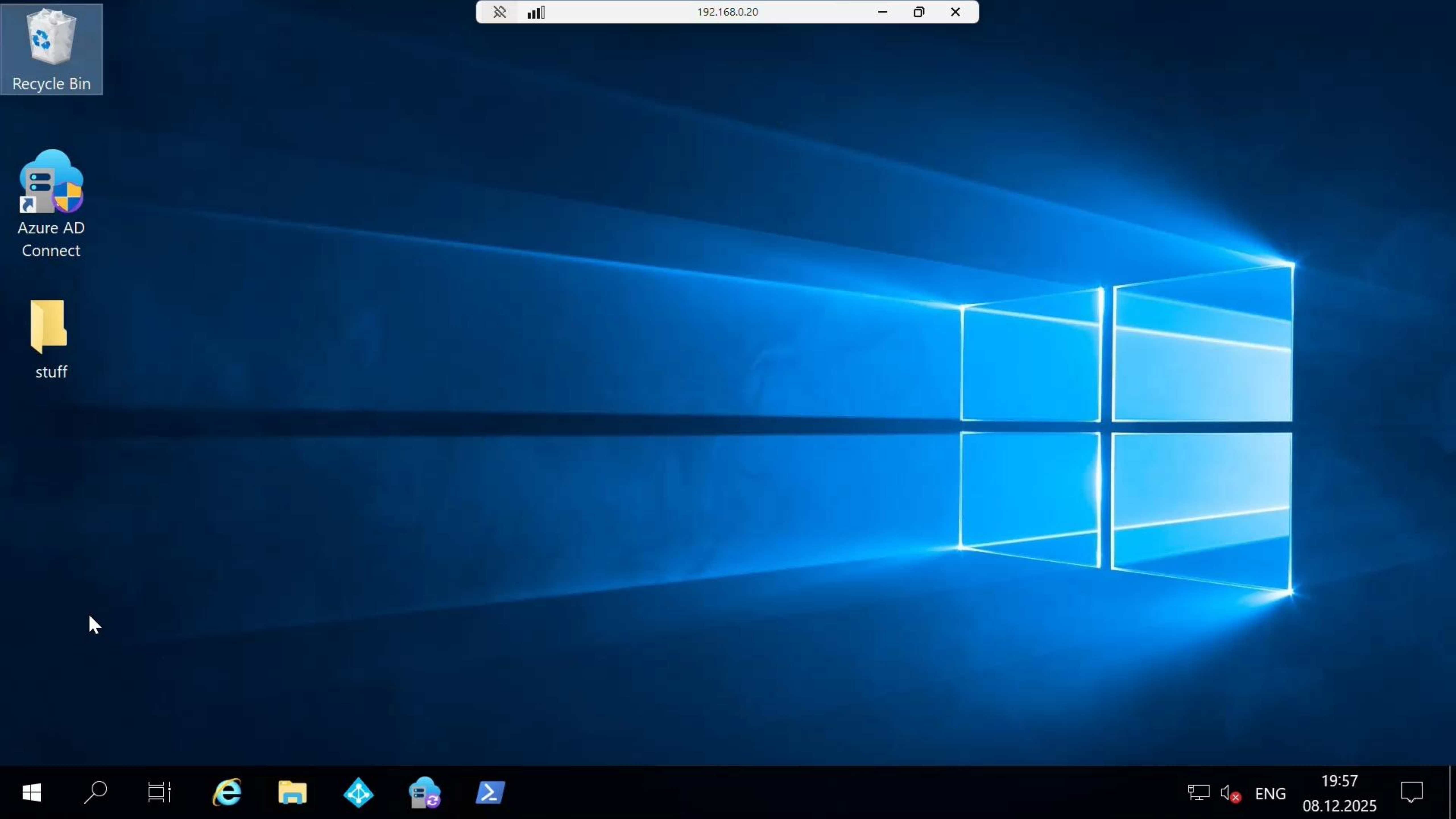
bject Properties

que identifier (GUID): {543D7C5B-8406-EC11-9751-00155D007B05}
isplay Name: Adele Vance
Object type: person

Attribute Name	Value	Contributing MA	Sync Rule
accountEnabled	true	gkfelucia.net	In from AD - User
accountName	AdeleV	gkfelucia.net	In from AD - User ...
cloudAnchor	User_b1d67566-aa2d-42bb-9be5-c776...	c4a8felucia.onmi...	In from AAD - Us...
cloudNoFlow	true	gkfelucia.net	In from AD - Set c...
cloudSourceAnc...	rq2PmzM3xUGIjoR6UJtkZQ==	c4a8felucia.onmi...	In from AAD - Us...
cn	Adele Vance	gkfelucia.net	In from AD - User ...
contributingConn...	{7303ab7e-048f-4c65-84ad-f8ccae18d...	gkfelucia.net	In from AD - User ...
countryCode	0	gkfelucia.net	In from AD - User ...
description	Nadines User	gkfelucia.net	In from AD - User ...
displayName	Adele Vance	gkfelucia.net	In from AD - User ...
distinguishedName	CN=Adele Vance,OU=CloudSyncMigra...	gkfelucia.net	In from AD - User ...
domainFQDN	gkfelucia.net	gkfelucia.net	In from AD - User ...
domainNetBios	GKFELUCIA	gkfelucia.net	In from AD - User ...
forestFQDN	gkfelucia.net	gkfelucia.net	In from AD - User ...
forestNetBios	GKFELUCIA	gkfelucia.net	In from AD - User ...
givenName	Adele	gkfelucia.net	In from AD - User ...
mail	AdeleV@gkfelucia.net	gkfelucia.net	In from AD - User ...
objectSid	01 05 00 00 00 00 00 05 15 00 00 00 ...	gkfelucia.net	In from AD - User ...
objectSidString	S-1-5-21-320411311-1571023620-241...	gkfelucia.net	In from AD - User ...

Demo

The cloudNoFlow


192.168.0.20
Recycle Bin
Azure AD Connect
stuff
ENG
19:57
08.12.2025

Migration Takeaways

Never deselect OUs in Entra Connect while migration!

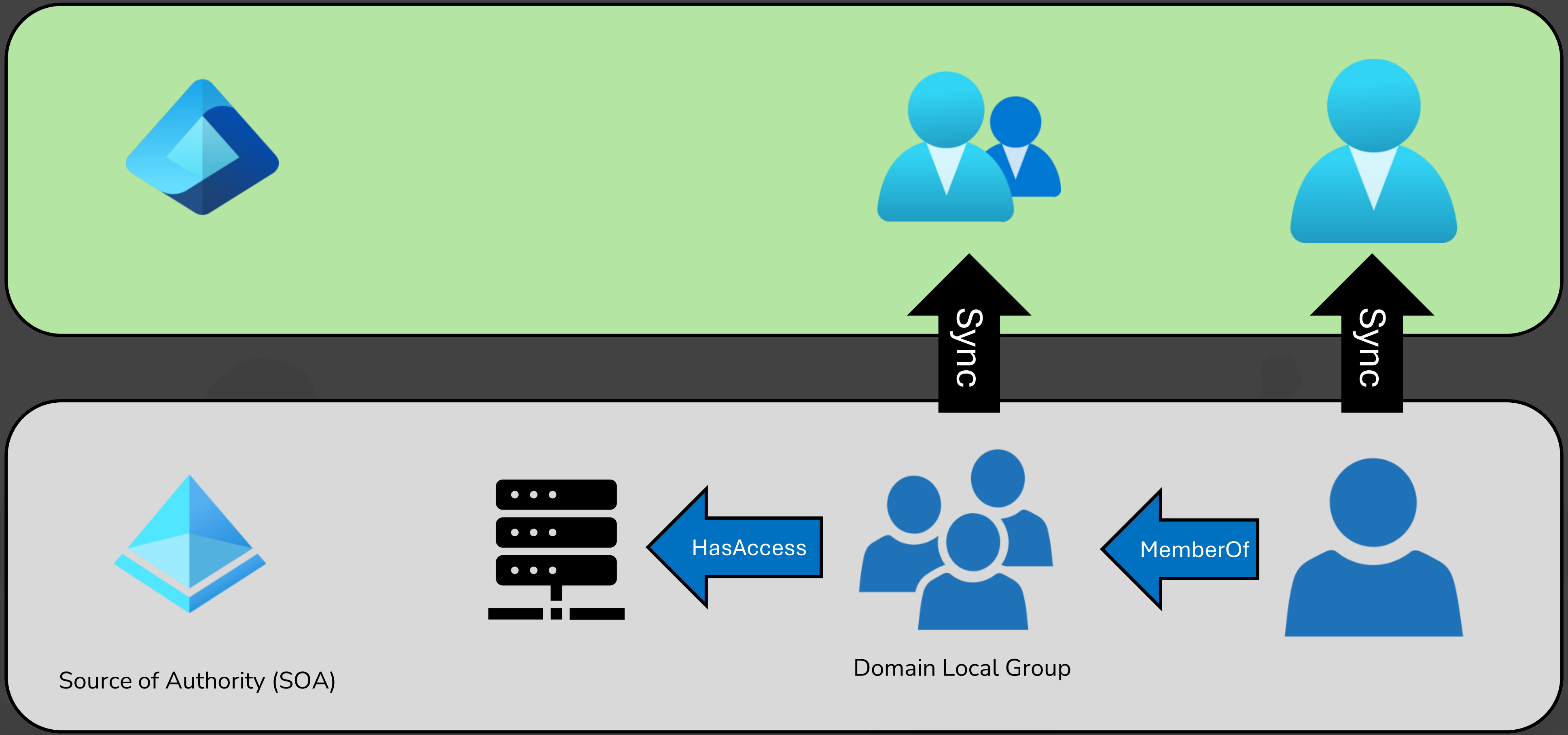
More Migration Takeaways

- ✓ 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 🚀

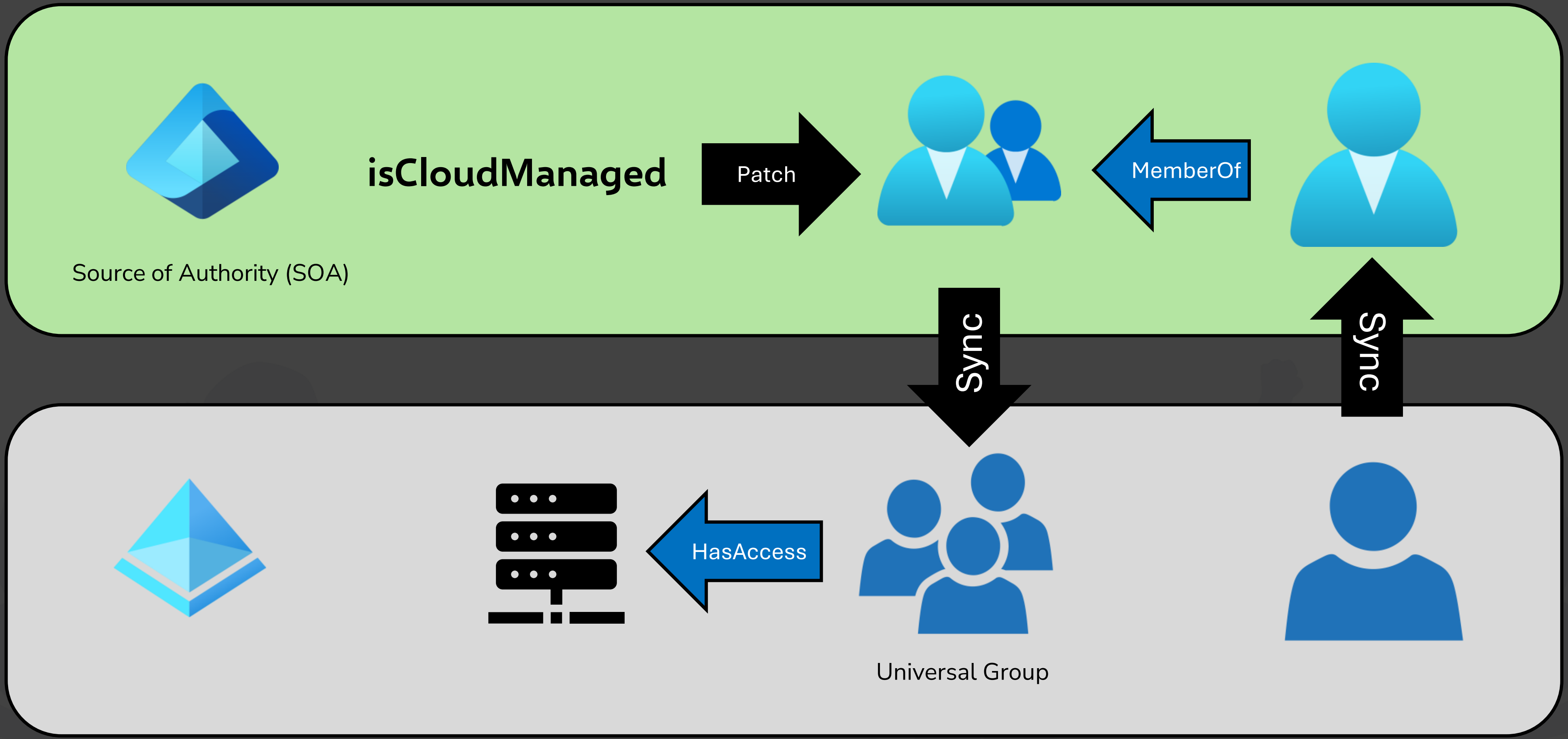
Change of Source of Authority

Migrate groups to cloud-based management with write-back

Classic hybrid group management



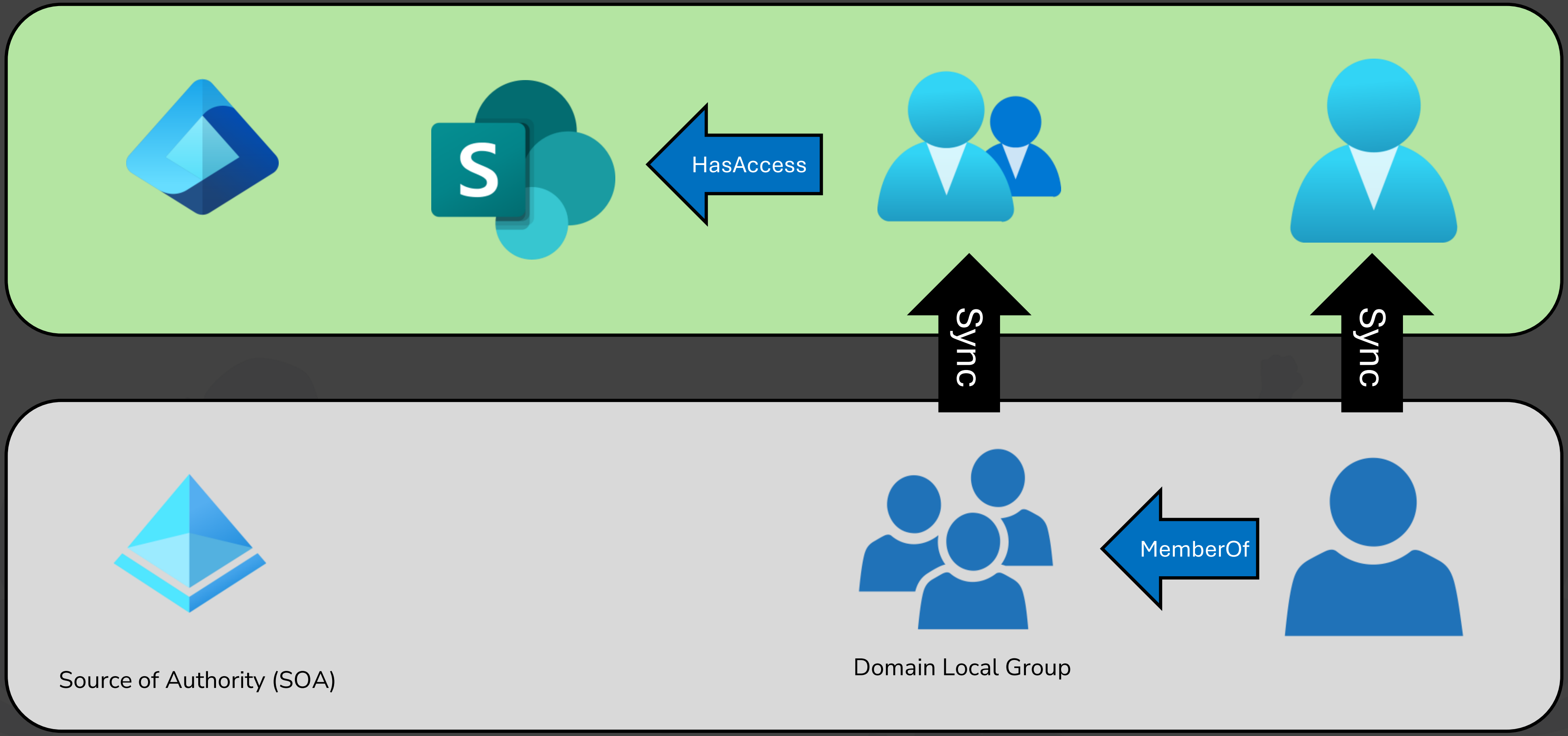
Change of Source of Authority #1



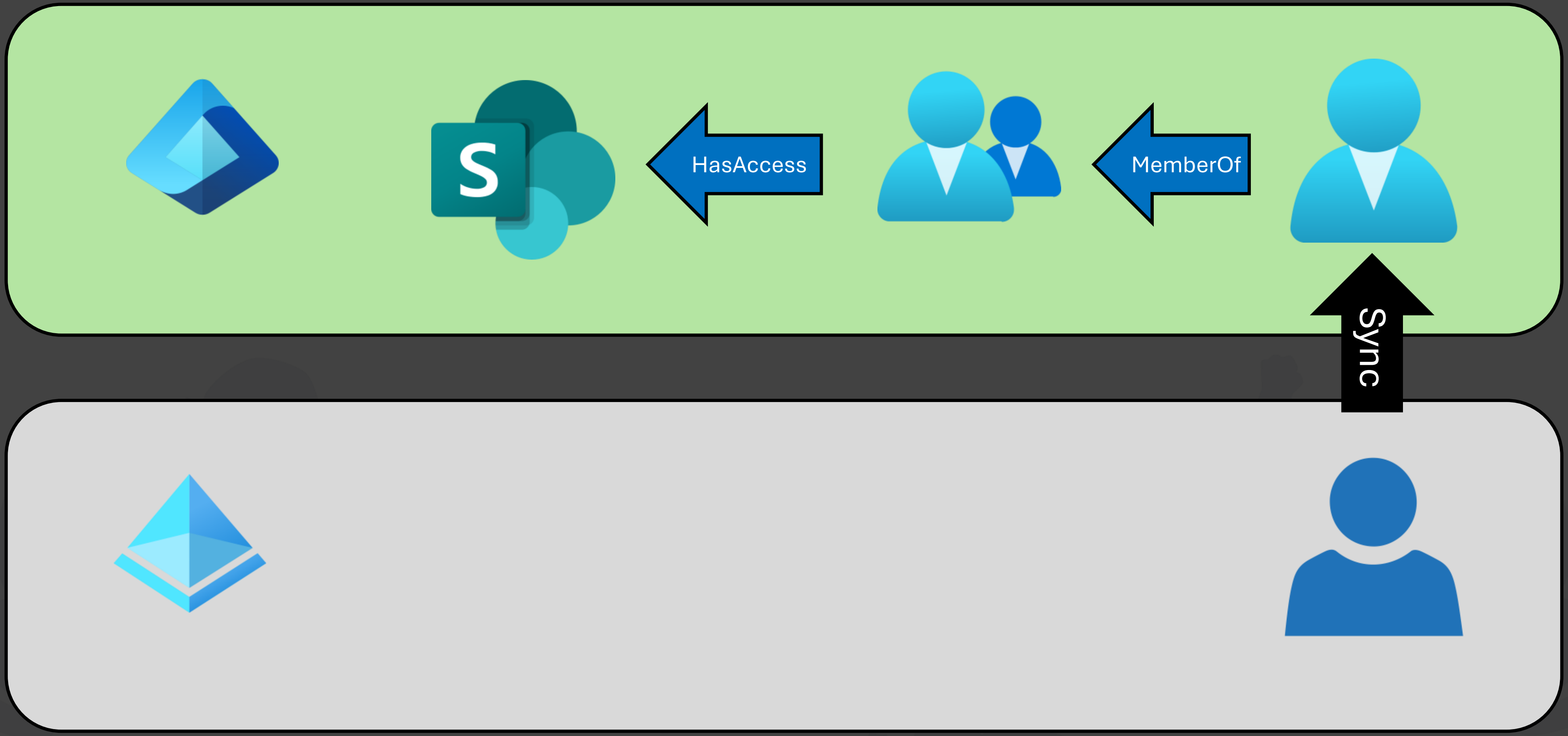
Scenario #2

Move to fully cloud managed

Cloud hybrid group management

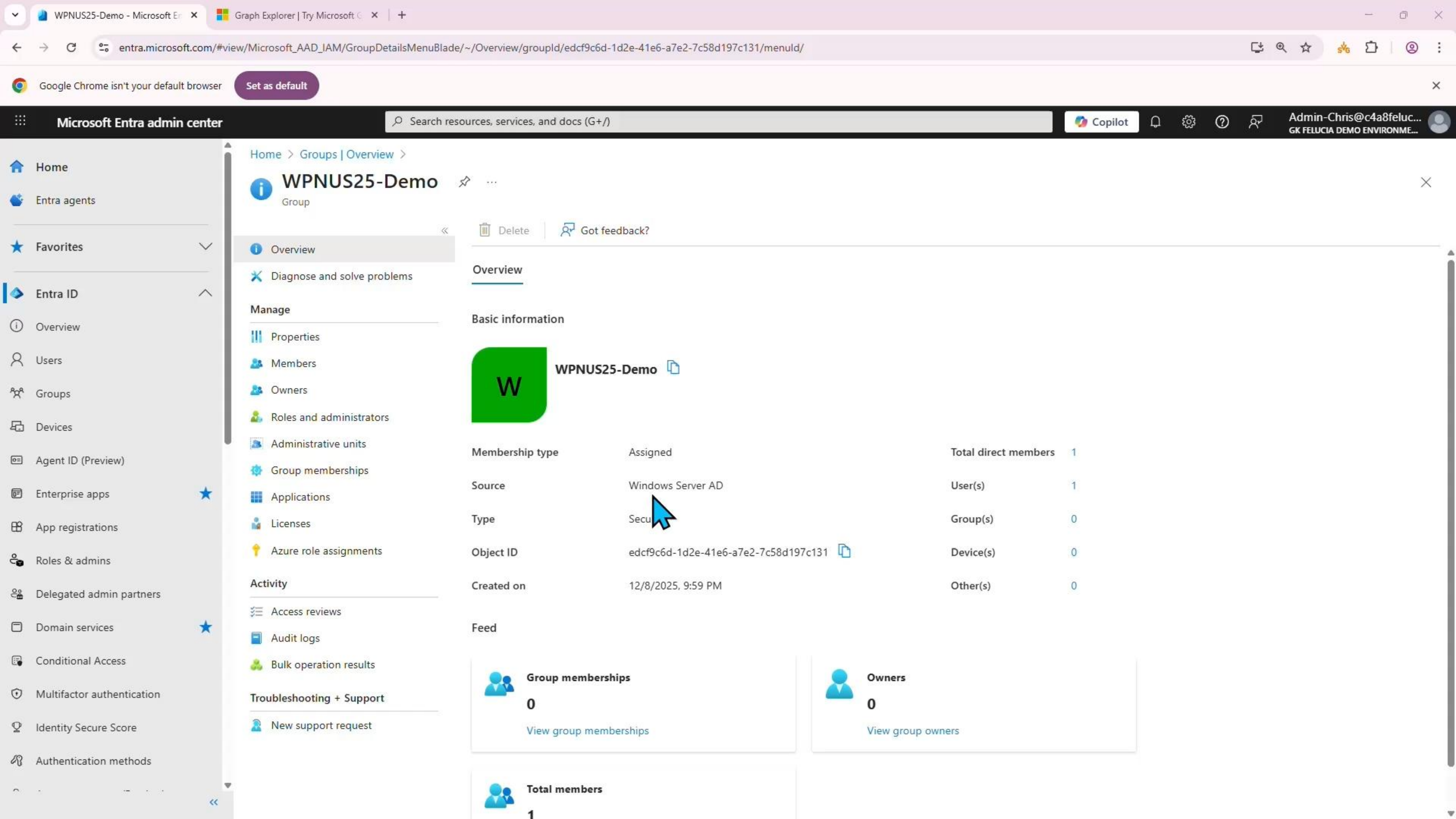


Change of Source of Authority #2



Demo

isCloudManaged



Basic information

W

WPNUS25-Demo

Membership type	Assigned	Total direct members	1
Source	Windows Server AD	User(s)	1
Type	Secu	Group(s)	0
Object ID	edcf9c6d-1d2e-41e6-a7e2-7c58d197c131	Device(s)	0
Created on	12/8/2025, 9:59 PM	Other(s)	0

Feed

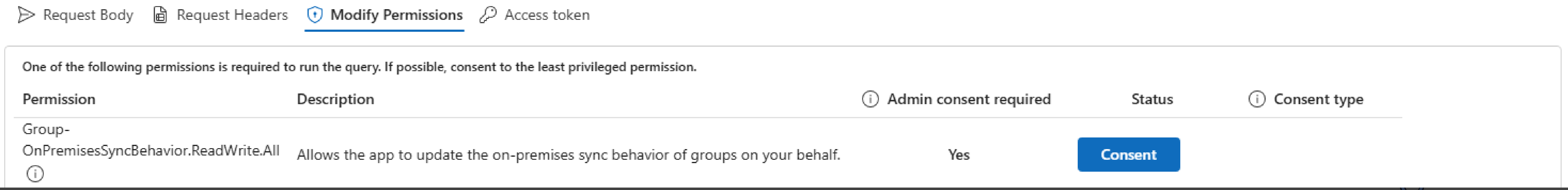
Group memberships
0
View group memberships

Owners
0
View group owners

Total members
1

Group 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



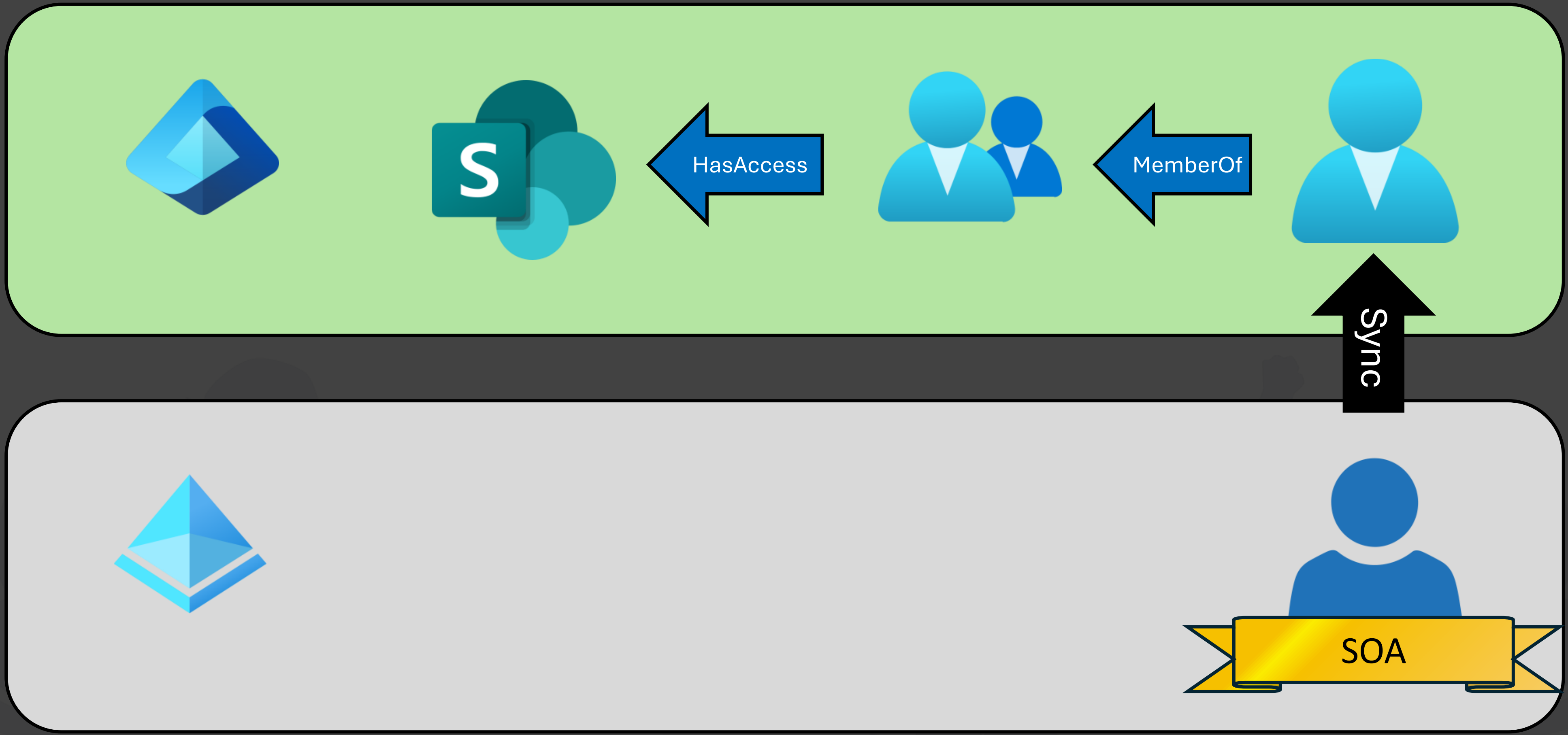
One of the following permissions is required to run the query. If possible, consent to the least privileged permission.

Permission	Description	Admin consent required	Status	Consent type
Group-OnPremisesSyncBehavior.ReadWrite.All	Allows the app to update the on-premises sync behavior of groups on your behalf.	Yes	Consent	

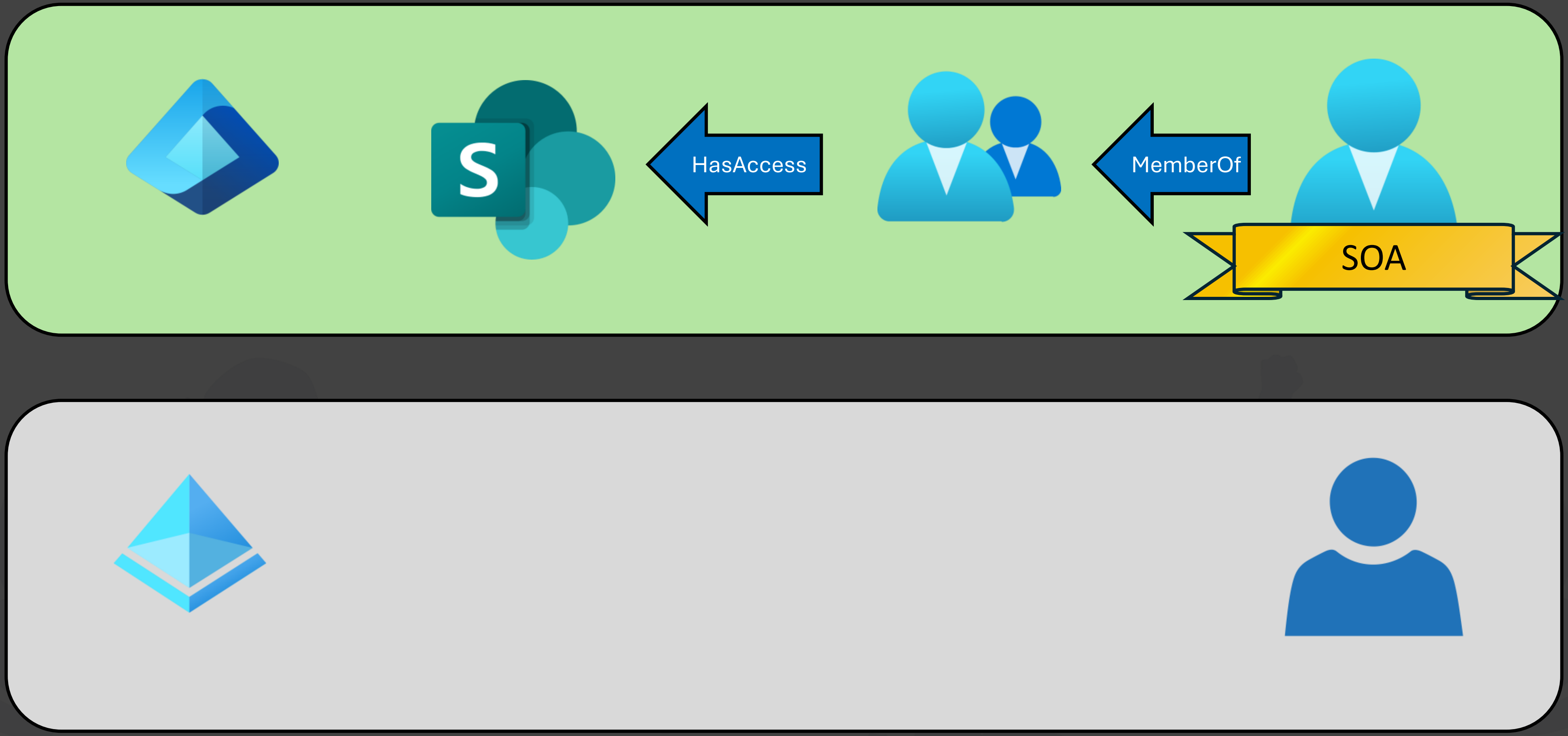
Change of Source of Authority

Migrate users and contacts to cloud-based management ~~with write-back~~

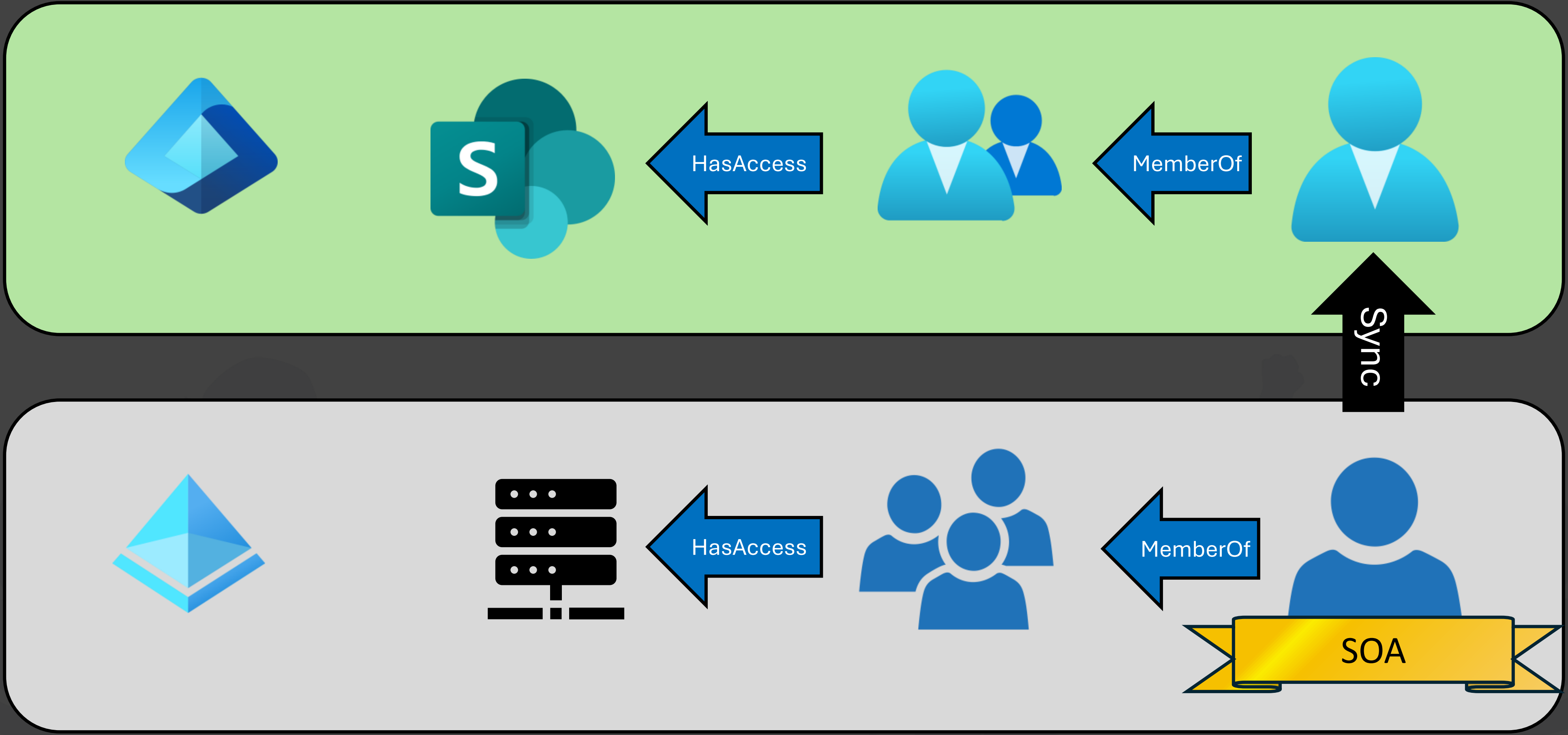
Change of Source of Authority #1



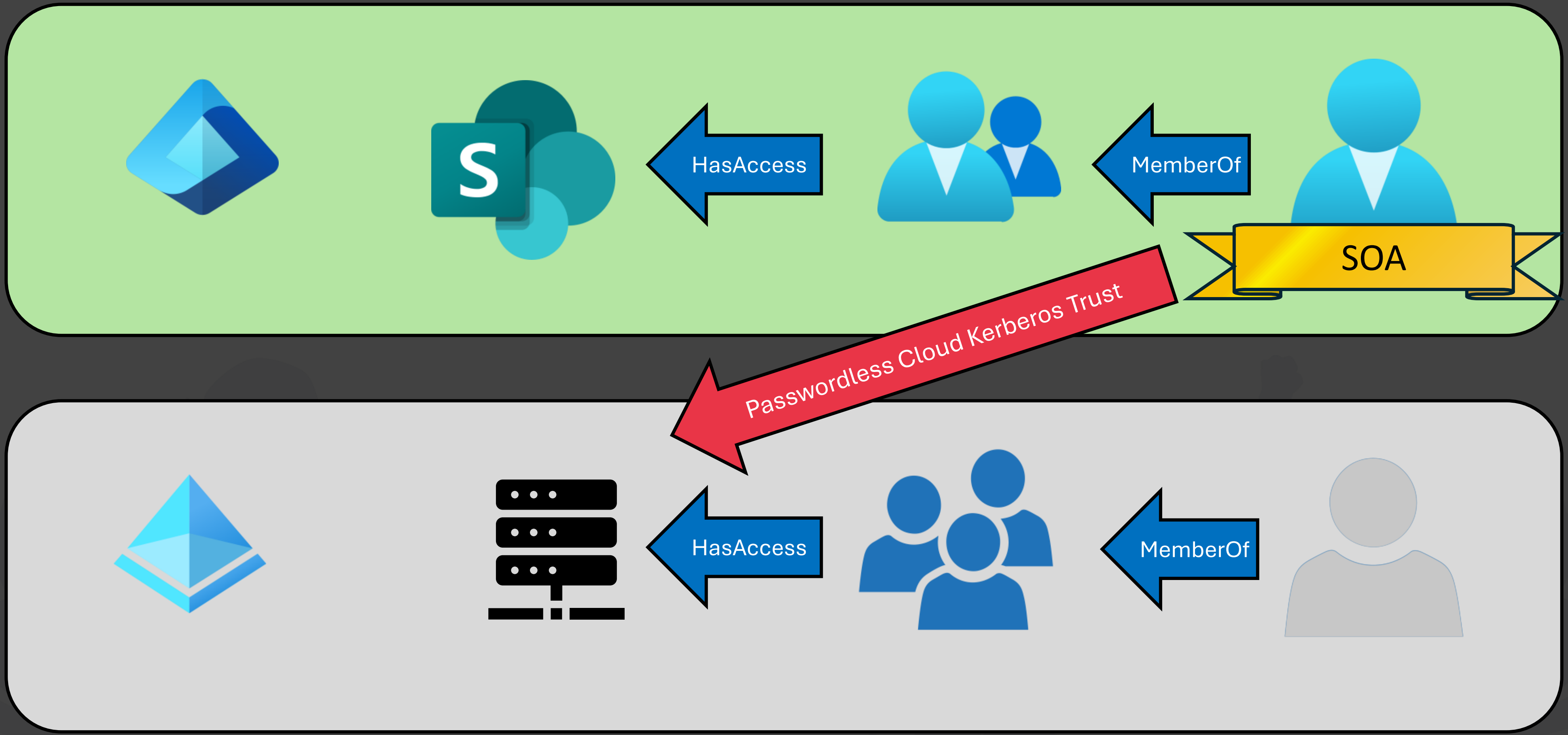
Change of Source of Authority #1



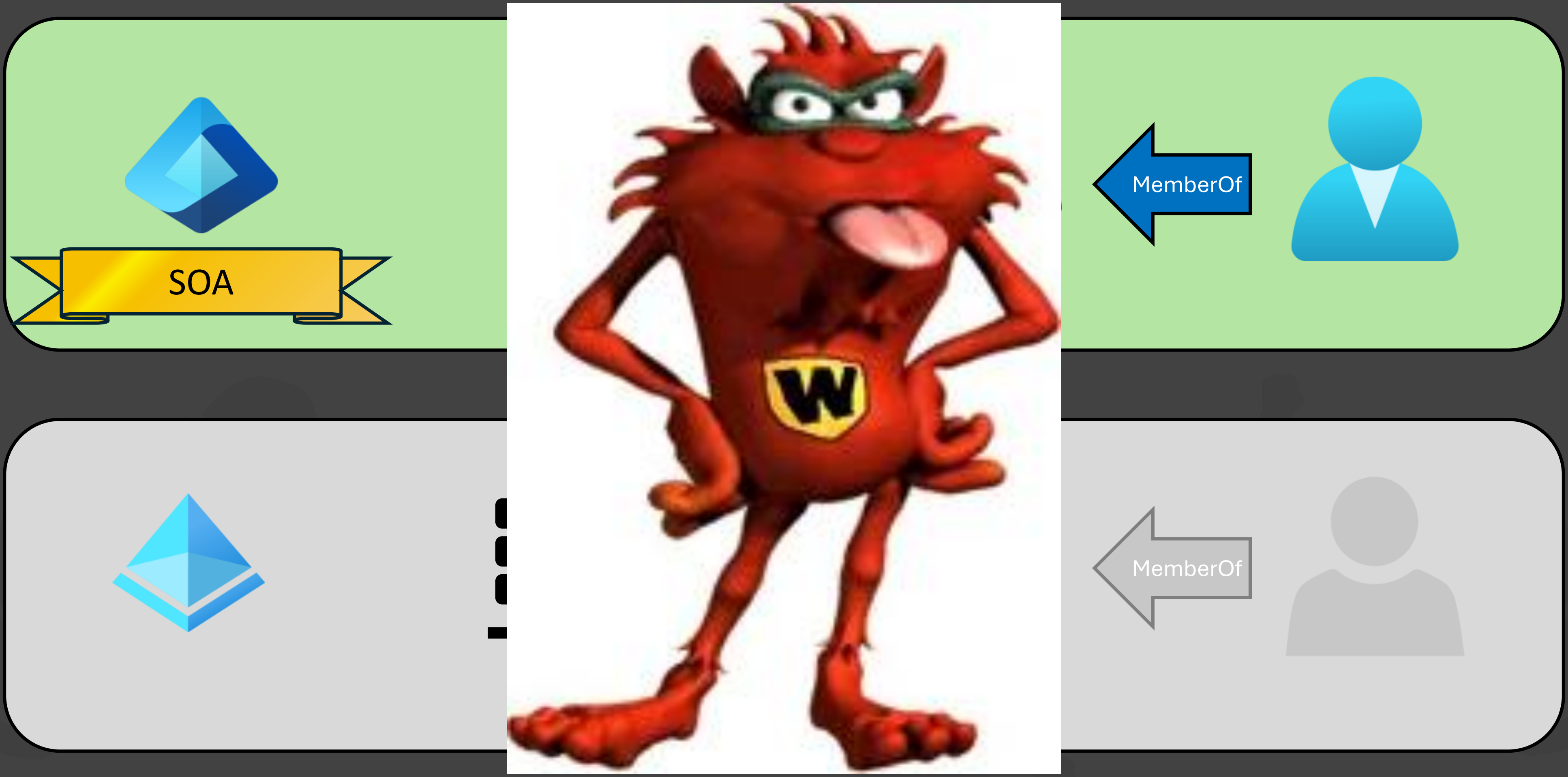
Change of Source of Authority #2



Change of Source of Authority #2



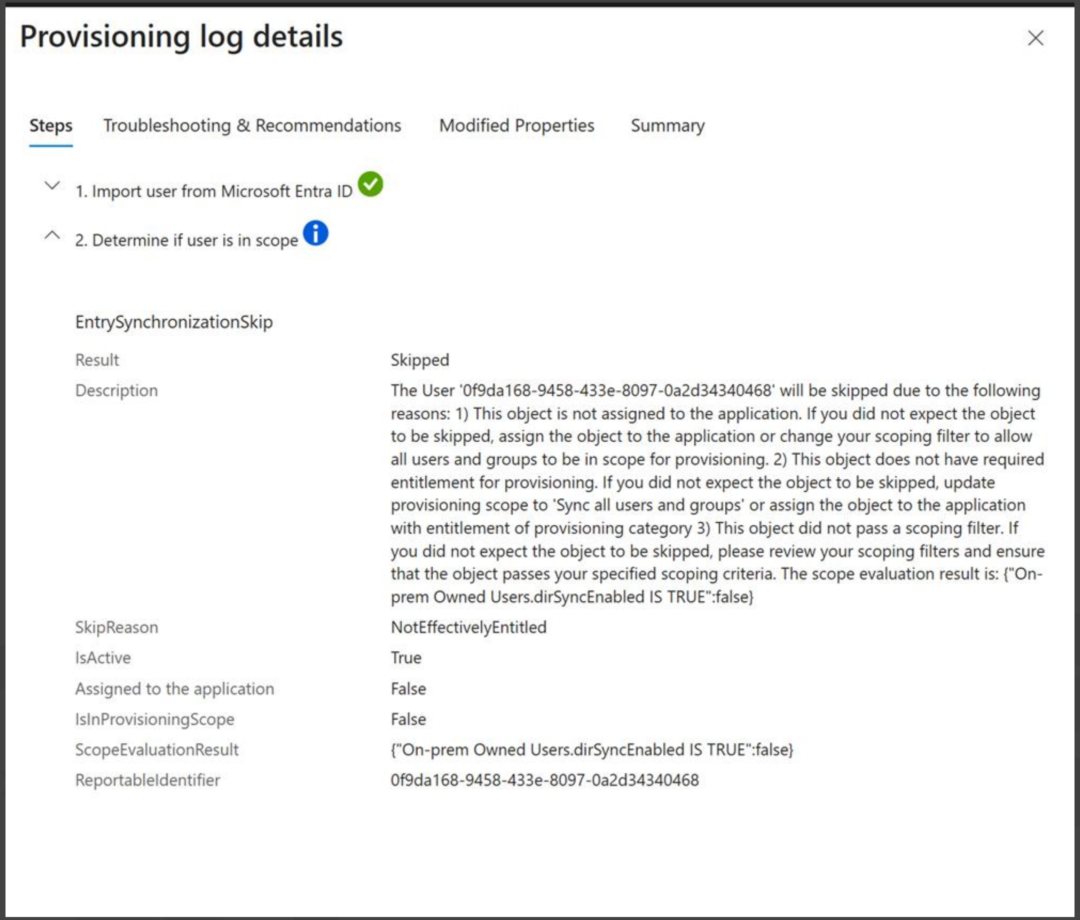
Combination of User + Group SOA



WE SUPPORT
USER SOA SWITCH NOW!
YEAH - LET'S COMBINE
IT WITH GROUP WRITEBACK!
IT WORKS WITH
GROUP WRITEBACK... RIGHT?
imgflip.com

The user change of SOA problem

- After the SOA change the user is 100% cloud
- Cloud users cannot be added to on-premises groups by group writeback
- Already existing group memberships in cloud managed groups will be removed



Provisioning log details

1. Import user from Microsoft Entra ID ✓

2. Determine if user is in scope ⓘ

EntrySynchronizationSkip

Result: Skipped

Description: The User '0f9da168-9458-433e-8097-0a2d34340468' will be skipped due to the following reasons: 1) This object is not assigned to the application. If you did not expect the object to be skipped, assign the object to the application or change your scoping filter to allow all users and groups to be in scope for provisioning. 2) This object does not have required entitlement for provisioning. If you did not expect the object to be skipped, update provisioning scope to 'Sync all users and groups' or assign the object to the application with entitlement of provisioning category 3) This object did not pass a scoping filter. If you did not expect the object to be skipped, please review your scoping filters and ensure that the object passes your specified scoping criteria. The scope evaluation result is: {"On-prem Owned Users.dirSyncEnabled IS TRUE":false}

SkipReason: NotEffectivelyEntitled

IsActive: True

Assigned to the application: False

IsInProvisioningScope: False

ScopeEvaluationResult: {"On-prem Owned Users.dirSyncEnabled IS TRUE":false}

ReportableIdentifier: 0f9da168-9458-433e-8097-0a2d34340468

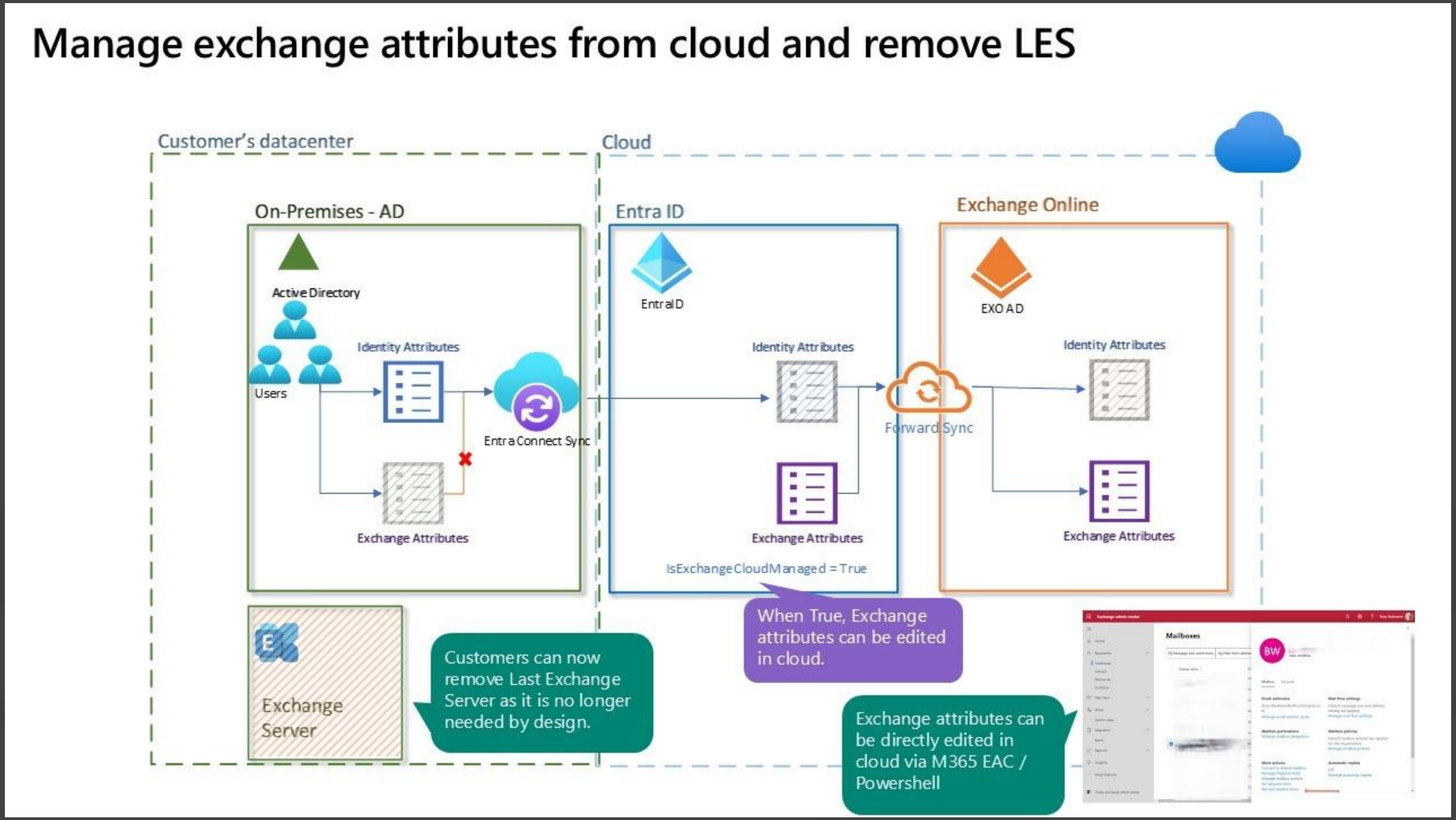
User SOA Takeaways

- ✓ The user must use a PWless authentication method to access OnPrem resources.
  - ✓ Windows Hello for Business
  - ✓ Passkey/FIDO2 authentication
- ✓ All on-prem Auth must use either Kerberos or NTLM
- ✓ LDAP based authentication is no longer supported
- ✓ Converted users will be removed from group-writeback enabled groups, even if the AD users is still existent

Special case

Last Exchange Server

Cloud-Managed Remote Mailboxes



Manage exchange attributes from cloud and remove LES

When True, Exchange attributes can be edited in cloud.

Customers can now remove Last Exchange Server as it is no longer needed by design.

Exchange attributes can be directly edited in cloud via M365 EAC / Powershell

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

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

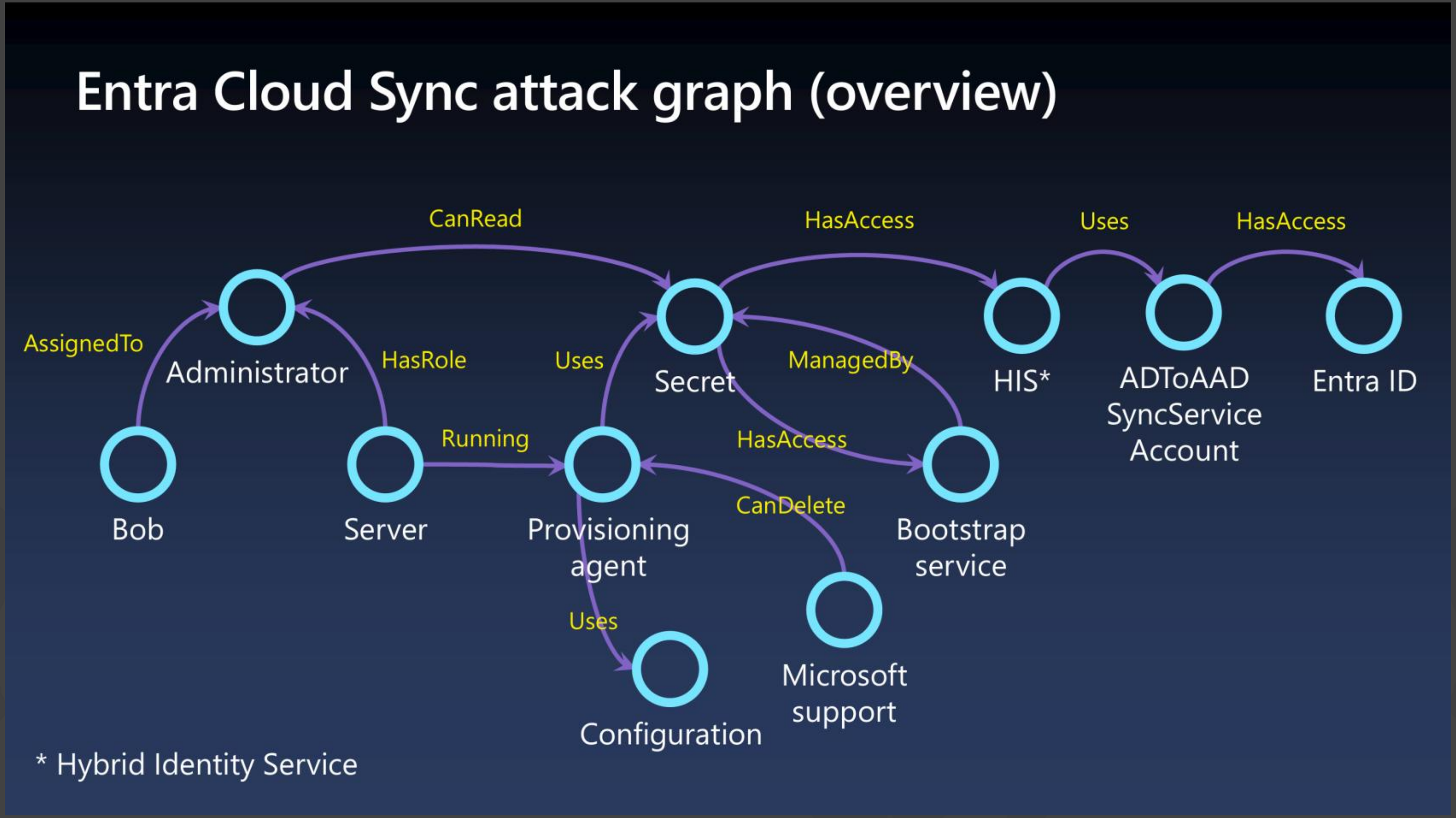
- UserGroupCreateDelete

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 an asseration is still possible
    - without TPM replacing the certificate as a backdoor is possible
- 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, for a compromise the attacker also needs:

- 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 😅

GO MIGRATE
WEEKEND UPDATE WEEKEND UPDATE WEEKEND UPDATE
SNL

Thank You!