semperis

TROOPERS CONFERENCE IN 2023

TROOPERS

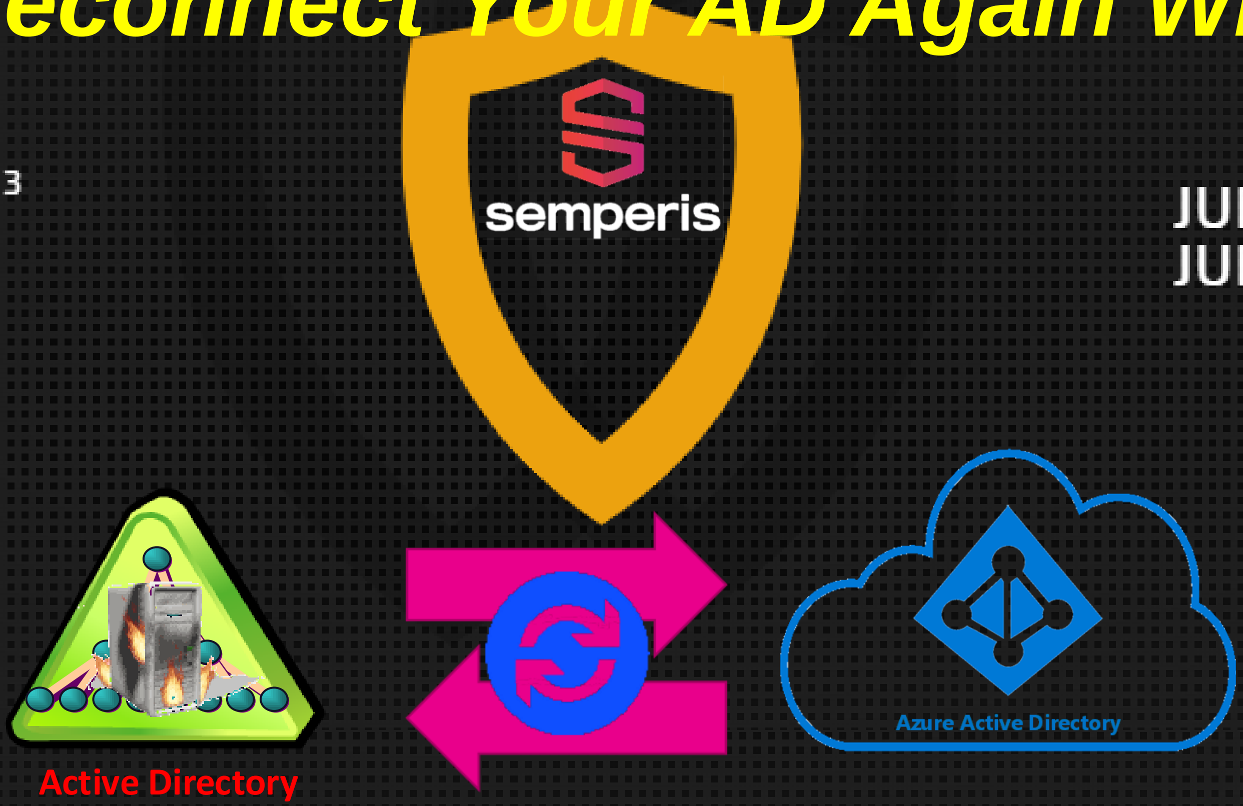
JUNE 26TH TO
JUNE 30TH, 2023

So You Performed A Forest Recovery
How Do You Reconnect Your AD Again With Azure AD

TROOPERS CONFERENCE IN 2023

TROOPERS

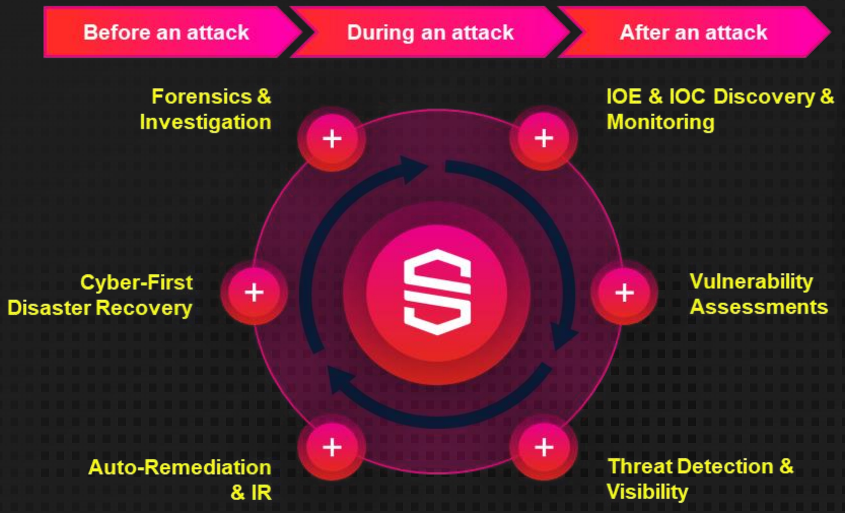
JUNE 26TH TO
JUNE 30TH, 2023



Jorge de Almeida Pinto
Senior Solutions Architect
Senior Incident Response Lead

Me, Myself And I! ...And Semperis

semperis


Before an attack
During an attack
After an attack
Forensics & Investigation
IOE & IOC Discovery & Monitoring
Cyber-First Disaster Recovery
Vulnerability Assessments
Auto-Remediation & IR
Threat Detection & Visibility

ABOUT SEMPERIS

We're Mission-Driven to Be a Force for Good

At Semperis, our workforce across all departments is part of a bigger mission to be a force for good. We fight every day to stop cyber criminals and curb the funding of evil.

Microsoft MVP Most Valuable Professional

Jorge de Almeida Pinto Senior Solutions Architect Senior Incident Response Lead	
LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter
Website	https://www.semperis.com/
Blog	https://www.semperis.com/blog/
Podcast	https://hipconf.libsyn.com/
Contact	jorged@semperis.com

- ✓ Architecting, designing, implementing and maintaining secure identity solutions
- ✓ Technology Focus: Identity, Security And Recovery
- ✓ Product Focus: AD, ADFS, AAD Connect, FIM/MIM, Azure AD Technologies.

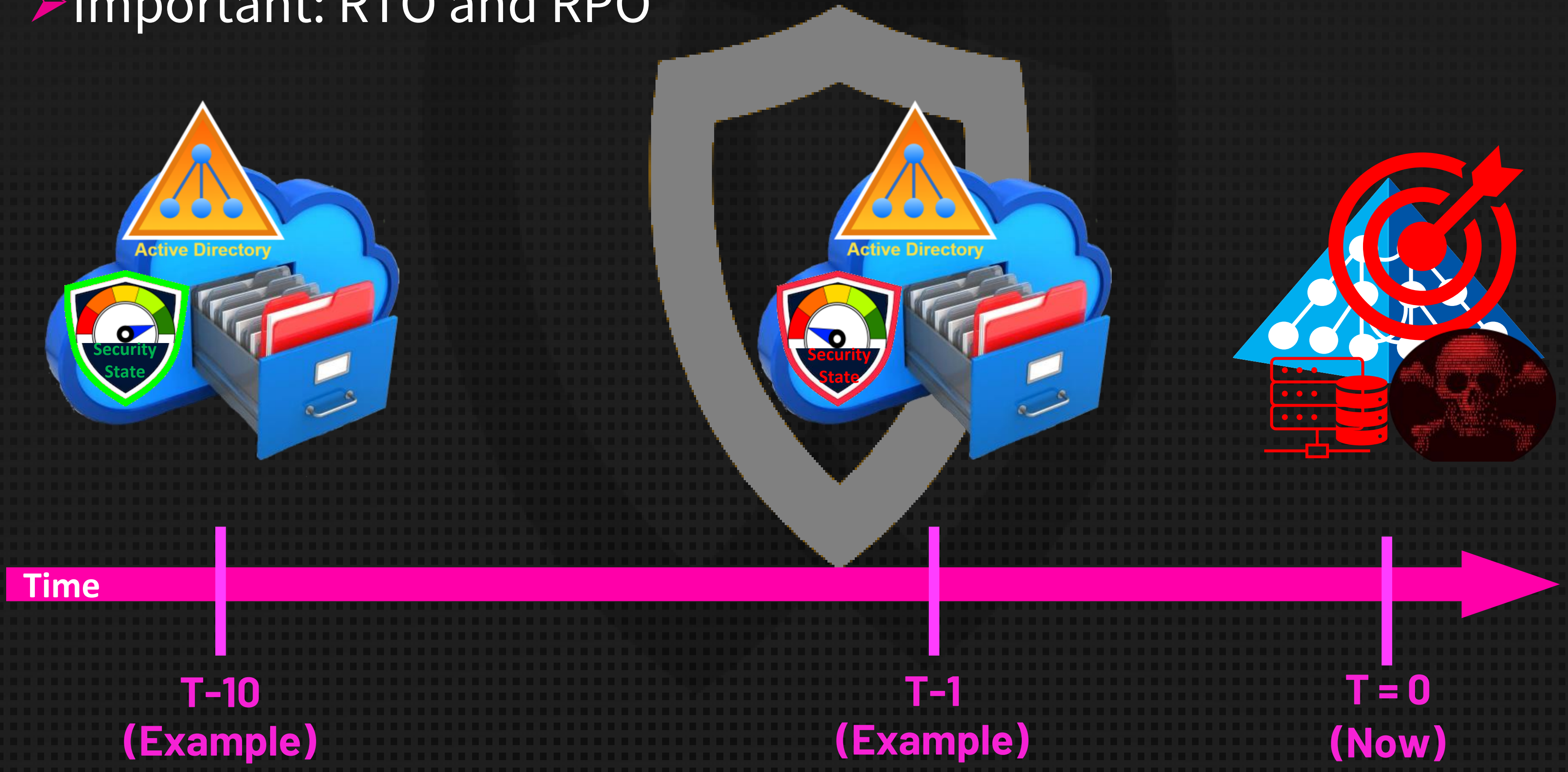
Agenda

1. Forest Recovery – What Happens?
2. Authentication Mechanisms
3. Risk/Impact Mitigating Actions – AuthN & Sync
4. Architecture Of Connect Sync & Cloud Sync
5. Reconnecting With Azure AD – Sync
6. Take Aways

Forest Recovery – What Happens?

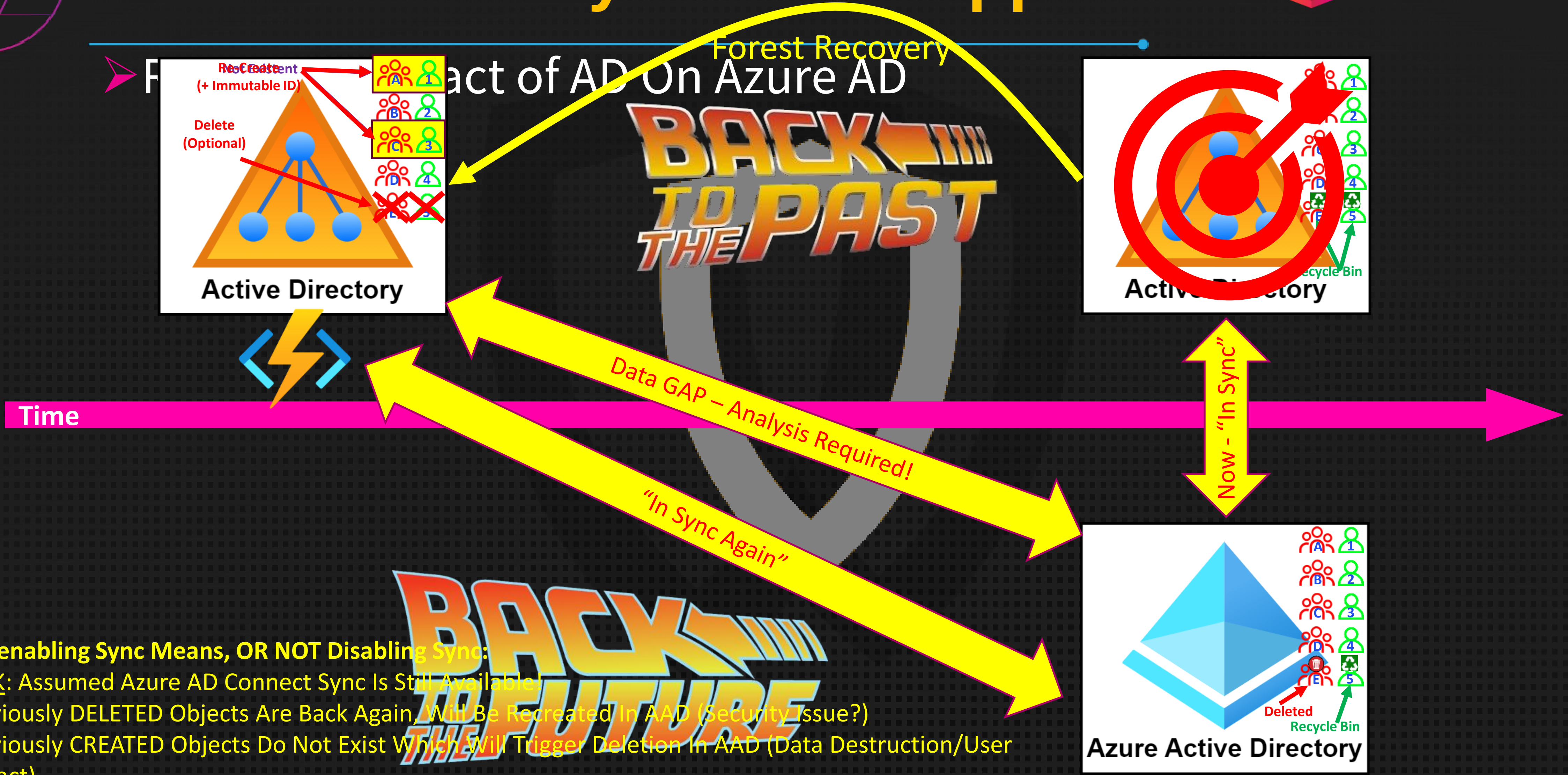
Forest Recovery – What Happens?

- The Preferred Backup
  - Important: RTO and RPO



Forest Recovery – What Happens?

- F act of AD On Azure AD



JUST Reenabling Sync Means, OR NOT Disabling Sync:

REMARK: Assumed Azure AD Connect Sync Is Still Available!

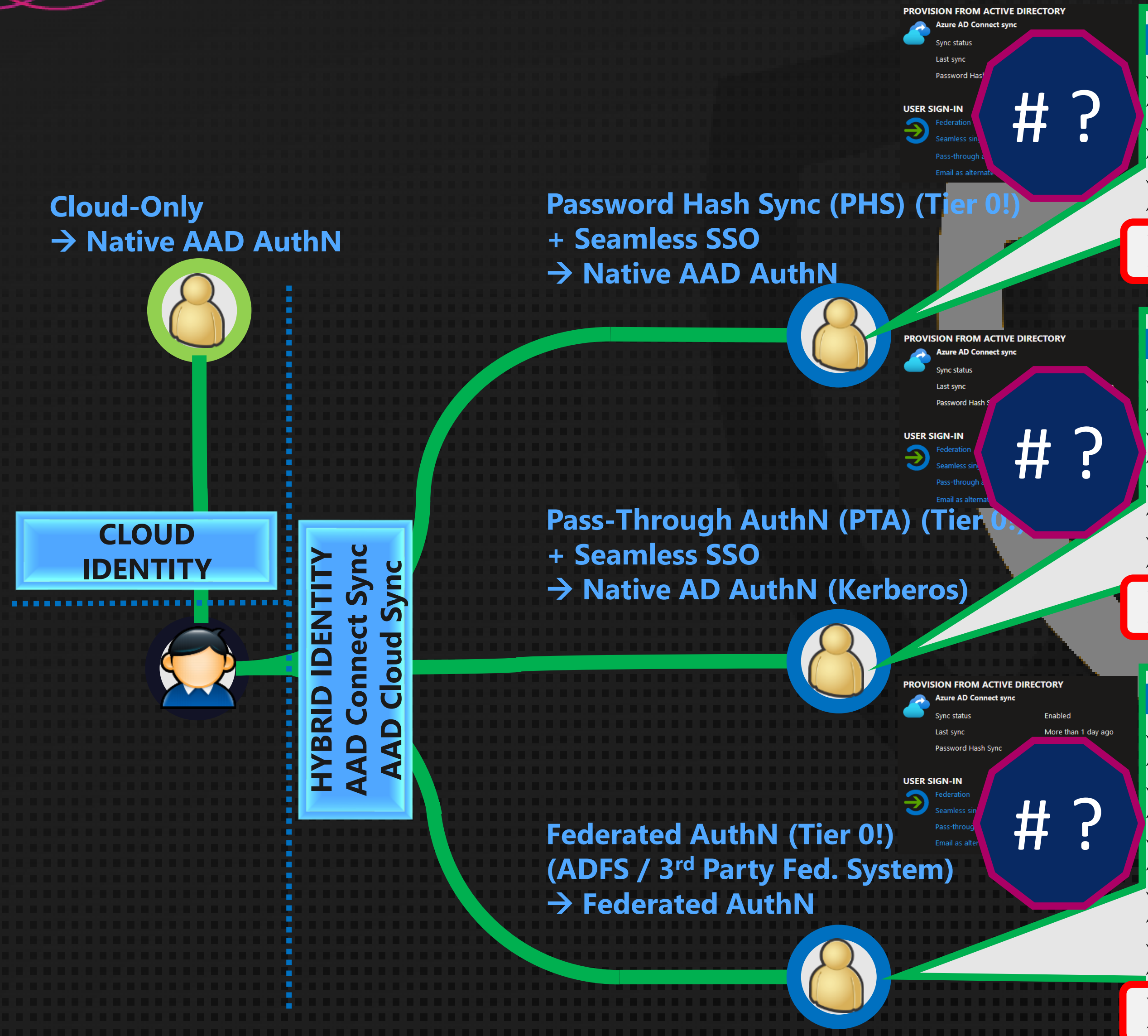
- Previously DELETED Objects Are Back Again, Will Be Recreated In AAD (Security Issue?)
- Previously CREATED Objects Do Not Exist Which Will Trigger Deletion In AAD (Data Destruction/User Impact)
- Members re-added (security issue?)/removed (loss of functionality) from synched groups

THEREFORE: Disable Sync (Connect Sync) Or Disable Configuration (Cloud Sync) Prior To Forest Recovery!

Authentication Mechanisms

Authentication Mechanisms

semperis



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect sync

Sync status

Last sync

Password Hash

USER SIGN-IN

Federation

Seamless sin

Pass-through a

Email as alternate

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect sync

Sync status

Last sync

Password Hash S

USER SIGN-IN

Federation

Seamless sin

Pass-through

Email as alterna

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect sync

Sync status Enabled

Last sync More than 1 day ago

Password Hash Sync

USER SIGN-IN

Federation

Seamless sin

Pass-throug

Email as alter

Password Hash Sync + Seamless SSO

- ➢ Least Deployment Effort
- ➢ Azure AD Clould MFA + 3rd Party Cloud MFA
- ➢ Leaked Credential Report/Protection
- ➢ NO Real-Time On-Prem Dependency For AuthN

Pass-Through AuthN + Seamless SSO

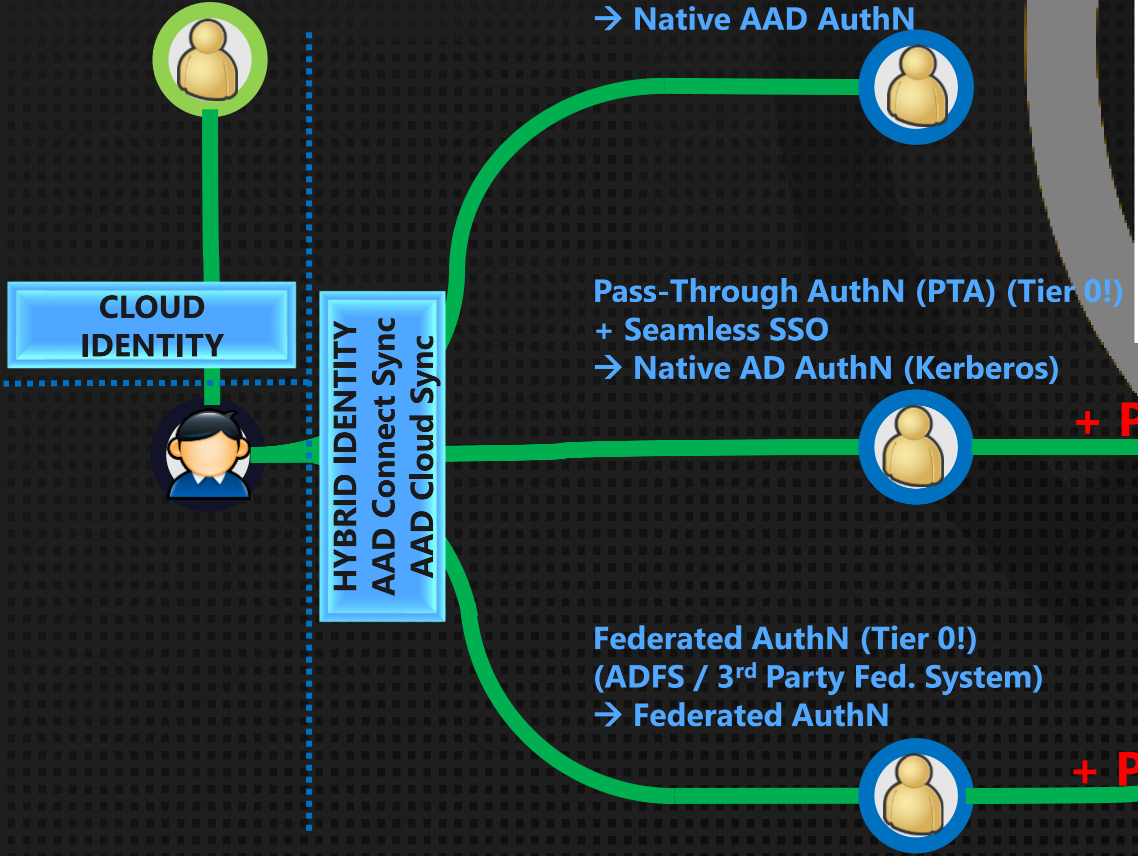
- ➢ Re-Use AD AuthN Policies
- ➢ Light-Weight PTA Agents Deployed On-Prem
- ➢ No Inbound Networking
- ➢ Azure AD Clould MFA + 3rd Party MFA
- ➢ HAS Real-Time On-Prem Dependency For AuthN

Federated AuthN

- ➢ Rich Feature Set / Heavy-Weight Deployment
- ➢ Lots Flexibility In Transform Rules
- ➢ Smartcard & Certificate AuthN
- ➢ Azure AD Clould MFA + 3rd Party MFA
- ➢ Azure AD On-Prem Server MFA (Deprecated)
- ➢ HAS Real-Time On-Prem Dependency For AuthN

Authentication Mechanisms

semperis



Cloud-Only
→ Native AAD AuthN

Password Hash Sync (PHS) (Tier 0!)
+ Seamless SSO
→ Native AAD AuthN

Pass-Through AuthN (PTA) (Tier 0!)
+ Seamless SSO
→ Native AD AuthN (Kerberos)

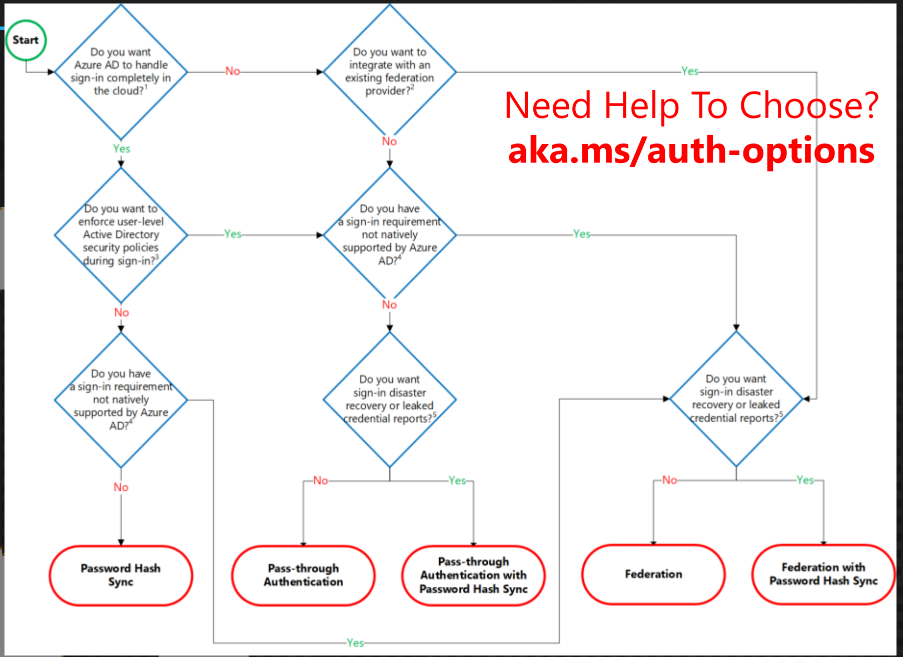
+ PHS

- Disaster Recovery For AuthN
- Leaked Credential Report/Protection

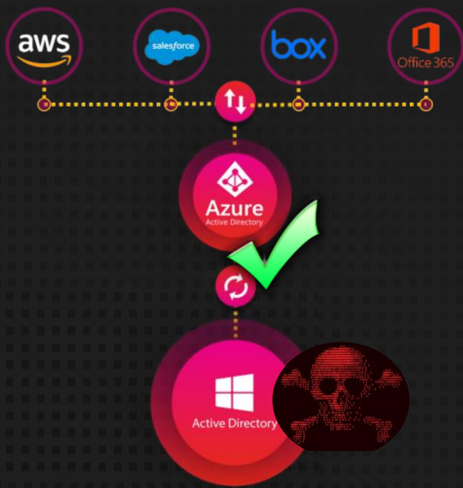
Federated AuthN (Tier 0!)
(ADFS / 3rd Party Fed. System)
→ Federated AuthN

+ PHS

- Disaster Recovery For AuthN
- Leaked Credential Report/Protection


Start
Do you want Azure AD to handle sign-in completely in the cloud?1
No
Yes
Do you want to integrate with an existing federation provider?2
Yes
No
Do you want to enforce user-level Active Directory security policies during sign-in?3
Yes
No
Do you have a sign-in requirement not natively supported by Azure AD?4
Yes
No
Do you have a sign-in requirement not natively supported by Azure AD?4
No
Yes
Do you want sign-in disaster recovery or leaked credential reports?5
No
Yes
Do you want sign-in disaster recovery or leaked credential reports?5
No
Yes
Password Hash Sync
Pass-through Authentication
Pass-through Authentication with Password Hash Sync
Federation
Federation with Password Hash Sync

Need Help To Choose?
aka.ms/auth-options

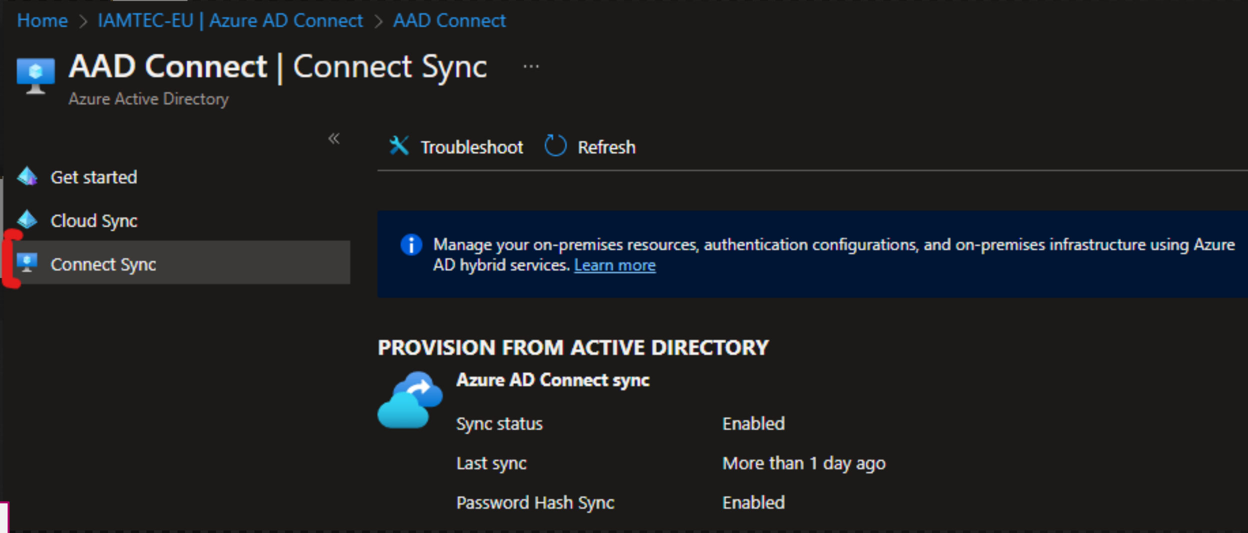


Risk/Impact Mitigating Actions – AuthN & Sync

Risk/Impact Mitigating Actions – AuthN & Sync

When AD Is Down… (Synchronization)

- Azure AD CONNECT Sync
  - Still Up-And-Running (i.e., NOT down/ransomwared)?
    - DISABLE The AAD Connect SCHEDULER
  - Running Or Not…
    - DO NOT DISABLE Sync IN AAD!



Home > IAMTEC-EU | Azure AD Connect > AAD Connect

AAD Connect | Connect Sync

Azure Active Directory

Manage your on-premises resources, authentication configurations, and on-premises infrastructure using Azure AD hybrid services. Learn more

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect sync

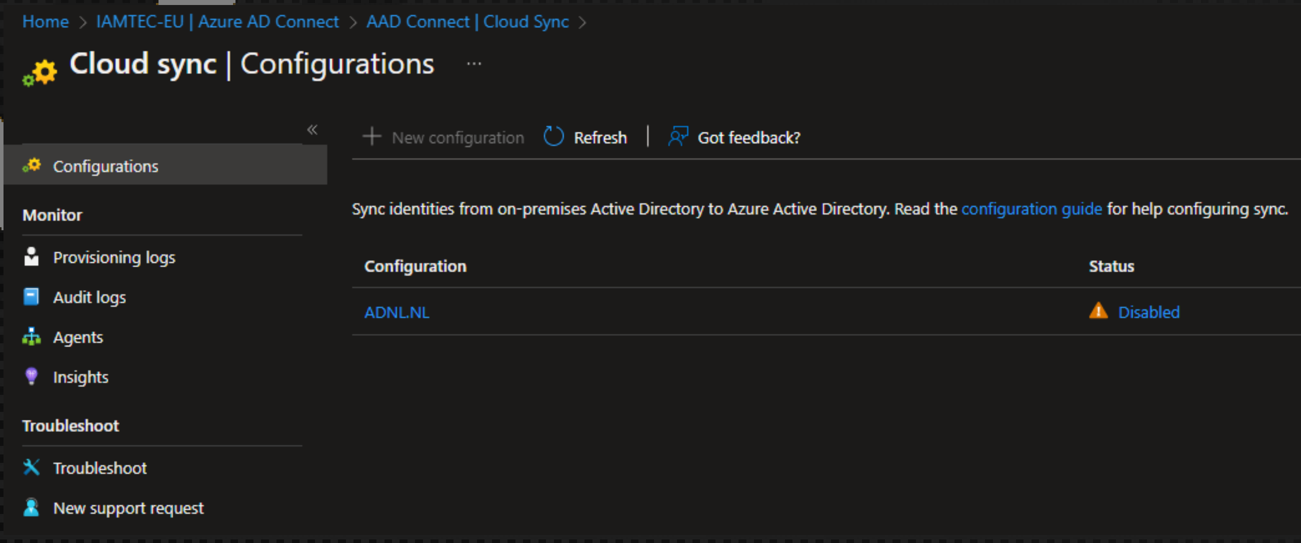
Sync status	Enabled
Last sync	More than 1 day ago
Password Hash Sync	Enabled

- ➢ Set-ADSyncScheduler -SyncCycleEnabled $false
- ➢ Get-ADSyncScheduler

Risk/Impact Mitigating Actions – AuthN & Sync

When AD Is Down… (Synchronization)

- Azure AD CLOUD Sync
  - DISABLE The AAD Cloud Sync Configuration (Requires Global Admin "BreakGlass")
  - DO NOT DELETE The AAD Cloud Sync Configuration



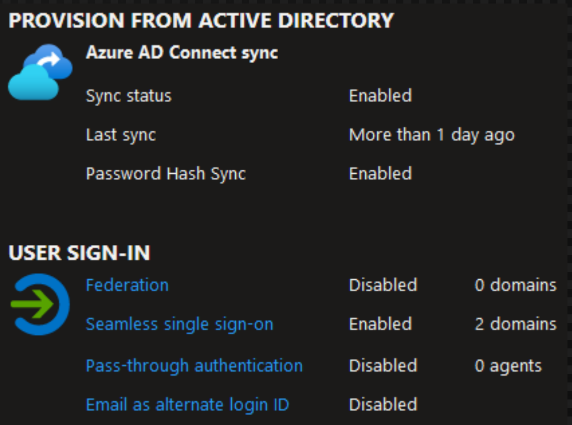
Sync identities from on-premises Active Directory to Azure Active Directory. Read the configuration guide for help configuring sync.

Configuration	Status
ADNL.NL	⚠ Disabled

Risk/Impact Mitigating Actions – AuthN & Sync

When AD Is Down… (Authentication (AuthN))

- Password Hash Sync (PHS)
  - Nothing To Do Here!
  - AuthN Against AAD Will Continue To Work!



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect sync

Sync status	Enabled
Last sync	More than 1 day ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	2 domains
Pass-through authentication	Disabled	0 agents
Email as alternate login ID	Disabled	

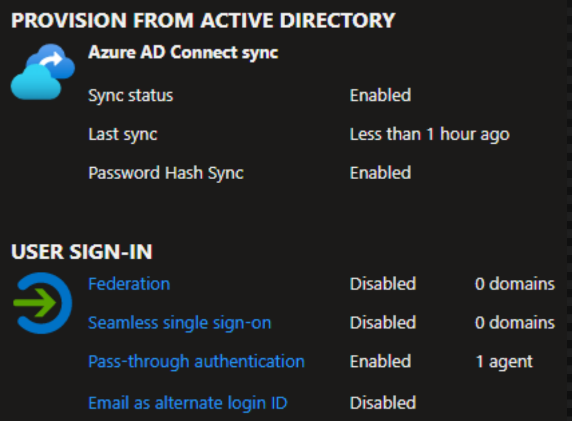
Risk/Impact Mitigating Actions – AuthN & Sync

When AD Is Down… (Authentication (AuthN))

- Pass-Through Authentication (PTA)
  - No PHS As Backup? → This WILL Hurt!
  - PHS Enabled & Synched? → Disable PTA In AAD
    - Download PTA Agent ("AADConnectAuthAgentSetup.exe")
    - Exec (Requires Global Admin "BreakGlass"):

```
CD "C:\Program Files\Microsoft Azure AD Connect Authentication Agent"
Import-Module ".\Modules\PassthroughAuthPSModule"
Get-PassthroughAuthenticationEnablementStatus
Disable-PassthroughAuthentication
```

Azure AD Identity...



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect sync

Sync status	Enabled	
Last sync	Less than 1 hour ago	
Password Hash Sync	Enabled	

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	1 agent
Email as alternate login ID	Disabled	

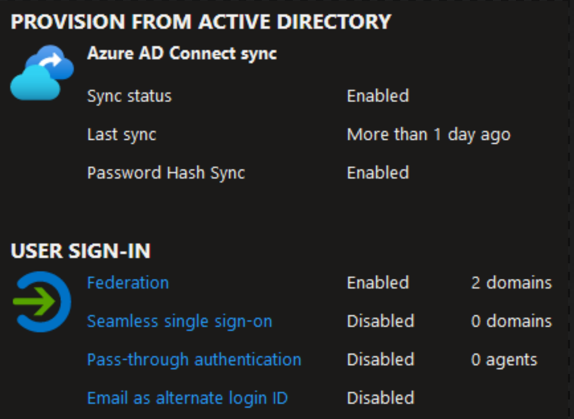
Risk/Impact Mitigating Actions – AuthN & Sync

When AD Is Down… (Authentication (AuthN))

- Federated Authentication
  - No PHS As Backup? → This WILL Hurt!
  - PHS Enabled & Synched? → Convert Domain In AAD
    - Exec (Requires Global Admin “BreakGlass”):

```
$aadGlobalAdmCreds = Get-Credential
Import-Module MSONLINE
Connect-MSOLService -Credential $aadGlobalAdmCreds
$fedDomInAAD = Get-MSOLDomain | ?{$_.Status -eq "Verified" -And
$_.Authentication -eq "Federated" -And !$($_.RootDomain)}
$fedDomInAAD | %{Set-MsolDomainAuthentication -DomainName $($_.Name) -
Authentication Managed}
```

Azure AD Identity...



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect sync

Sync status	Enabled
Last sync	More than 1 day ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Enabled	2 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents
Email as alternate login ID	Disabled	

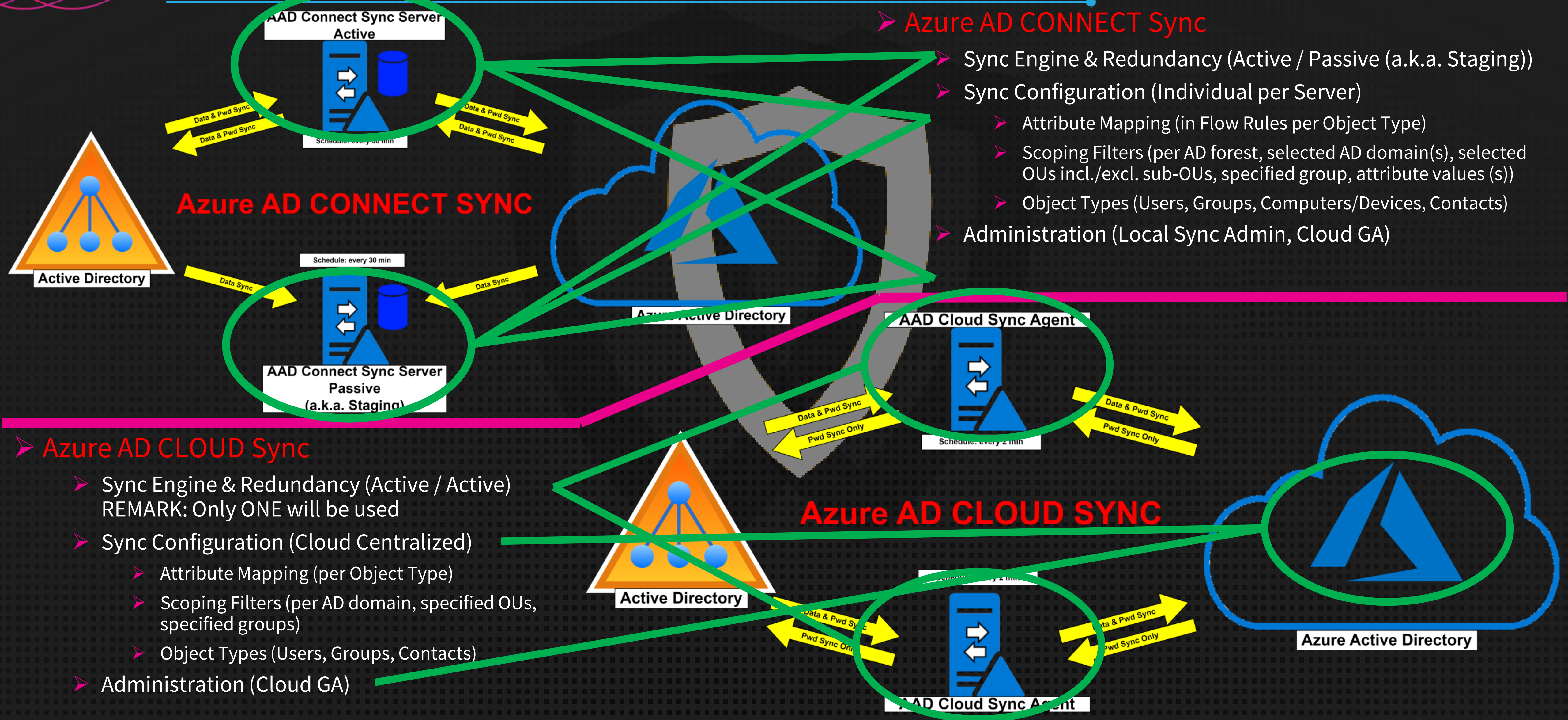
Risk/Impact Mitigating Actions – AuthN & Sync

After Everything Is Back To “Normal” Again

- If Reconfigured, Revert Back To Previous AuthN Mechanism (PHS→PTA Or PHS→FED Or Keep PHS!)
- Watch Out For Password Changes In AAD After Reconfiguring PTA Or Fed AuthN
- Remember, AD Went Back In Time, Watch Out For Password Differences

Architecture Of Connect Sync And Cloud Sync

Architecture Of Connect Sync And Cloud Sync



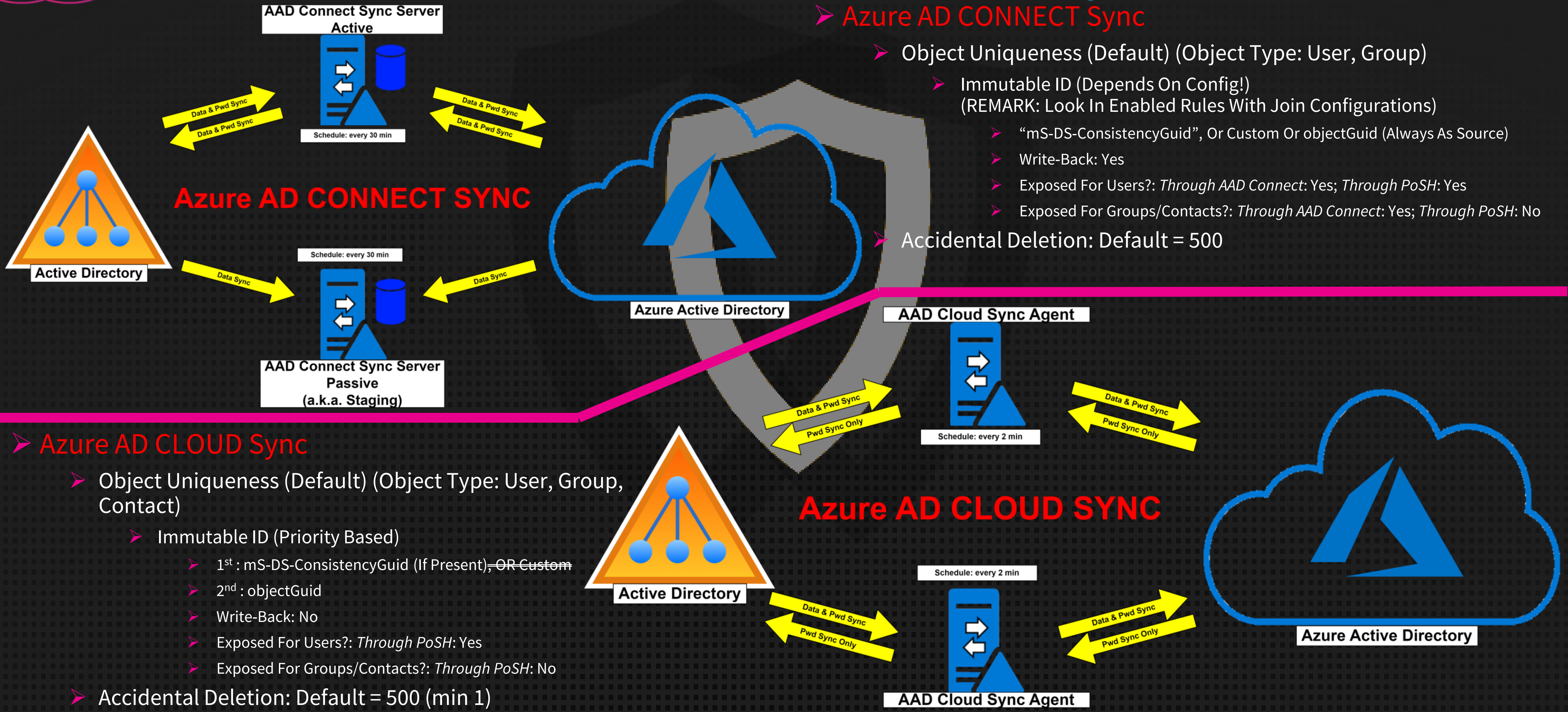
- Azure AD CONNECT Sync
  - Sync Engine & Redundancy (Active / Passive (a.k.a. Staging))
  - Sync Configuration (Individual per Server)
    - Attribute Mapping (in Flow Rules per Object Type)
    - Scoping Filters (per AD forest, selected AD domain(s), selected OUs incl./excl. sub-OUs, specified group, attribute values (s))
    - Object Types (Users, Groups, Computers/Devices, Contacts)
  - Administration (Local Sync Admin, Cloud GA)

- Azure AD CLOUD Sync
  - Sync Engine & Redundancy (Active / Active)
    REMARK: Only ONE will be used
  - Sync Configuration (Cloud Centralized)
    - Attribute Mapping (per Object Type)
    - Scoping Filters (per AD domain, specified OUs, specified groups)
    - Object Types (Users, Groups, Contacts)
  - Administration (Cloud GA)

Architecture Of Connect Sync And Cloud Sync

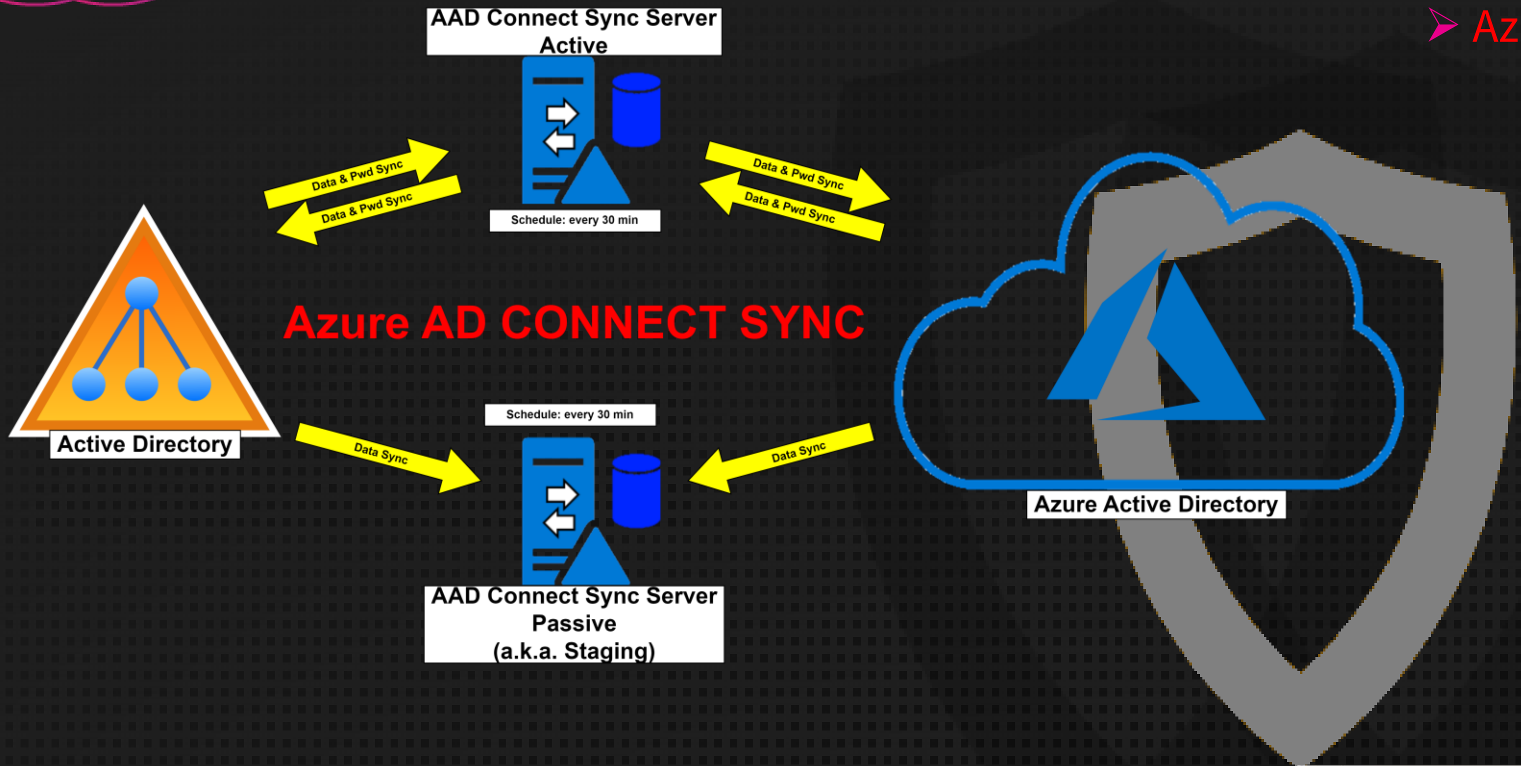
- Azure AD CONNECT Sync
  - Object Uniqueness (Default) (Object Type: User, Group)
    - Immutable ID (Depends On Config!)
      (REMARK: Look In Enabled Rules With Join Configurations)
      - "mS-DS-ConsistencyGuid", Or Custom Or objectGuid (Always As Source)
      - Write-Back: Yes
      - Exposed For Users?: *Through AAD Connect*: Yes; *Through PoSH*: Yes
      - Exposed For Groups/Contacts?: *Through AAD Connect*: Yes; *Through PoSH*: No
  - Accidental Deletion: Default = 500

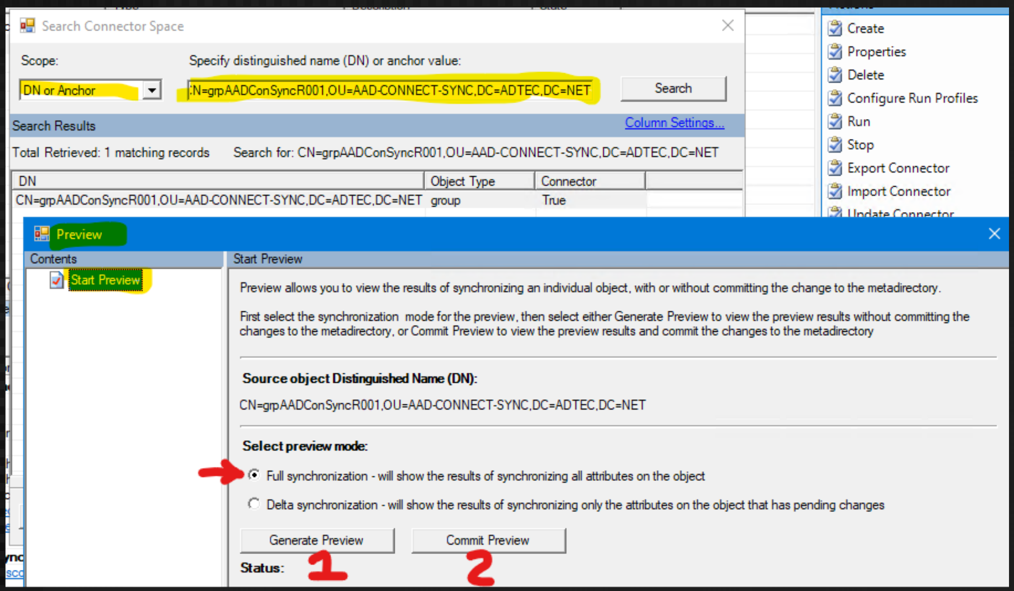
- Azure AD CLOUD Sync
  - Object Uniqueness (Default) (Object Type: User, Group, Contact)
    - Immutable ID (Priority Based)
      - 1st : mS-DS-ConsistencyGuid (If Present)~~, OR Custom~~
      - 2nd : objectGuid
      - Write-Back: No
      - Exposed For Users?: *Through PoSH*: Yes
      - Exposed For Groups/Contacts?: *Through PoSH*: No
  - Accidental Deletion: Default = 500 (min 1)



Architecture Of Connect Sync And Cloud Sync

- Azure AD CONNECT Sync
  - Manual Checks Before EXPORT: Individual/All objects




Search Connector Space

Scope: DN or Anchor

Specify distinguished name (DN) or anchor value: :N=grpAADConSyncR001,OU=AAD-CONNECT-SYNC,DC=ADTEC,DC=NET

Search Results

Total Retrieved: 1 matching records   Search for: CN=grpAADConSyncR001,OU=AAD-CONNECT-SYNC,DC=ADTEC,DC=NET

DN	Object Type	Connector
CN=grpAADConSyncR001,OU=AAD-CONNECT-SYNC,DC=ADTEC,DC=NET	group	True

Preview

Start Preview

Preview allows you to view the results of synchronizing an individual object, with or without committing the change to the metadirectory.

First select the synchronization mode for the preview, then select either Generate Preview to view the preview results without committing the changes to the metadirectory, or Commit Preview to view the preview results and commit the changes to the metadirectory

Source object Distinguished Name (DN):

CN=grpAADConSyncR001,OU=AAD-CONNECT-SYNC,DC=ADTEC,DC=NET

Select preview mode:

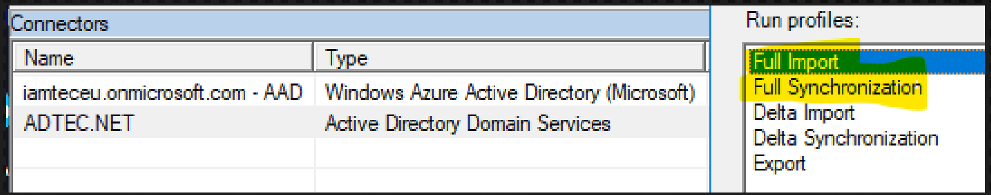
● Full synchronization - will show the results of synchronizing all attributes on the object

○ Delta synchronization - will show the results of synchronizing only the attributes on the object that has pending changes

1 Generate Preview

2 Commit Preview

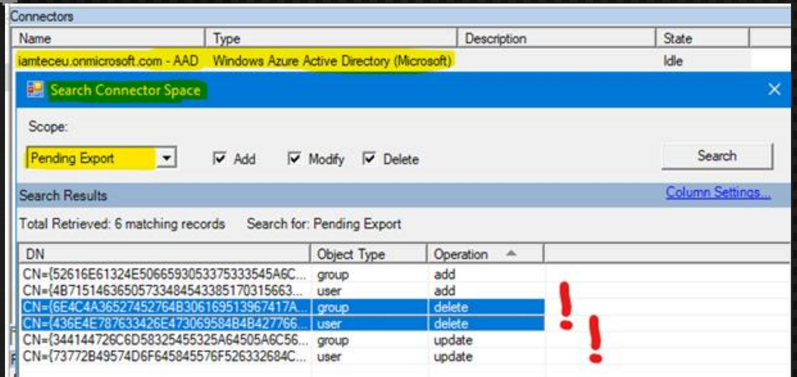
Status:


Connectors

Name	Type
iamteceu.onmicrosoft.com - AAD	Windows Azure Active Directory (Microsoft)
ADTEC.NET	Active Directory Domain Services

Run profiles:

- Full Import
- Full Synchronization
- Delta Import
- Delta Synchronization
- Export


Connectors

Name	Type	Description	State
iamteceu.onmicrosoft.com - AAD	Windows Azure Active Directory (Microsoft)		Idle

Search Connector Space

Scope: Pending Export   ☑ Add ☑ Modify ☑ Delete

Search Results

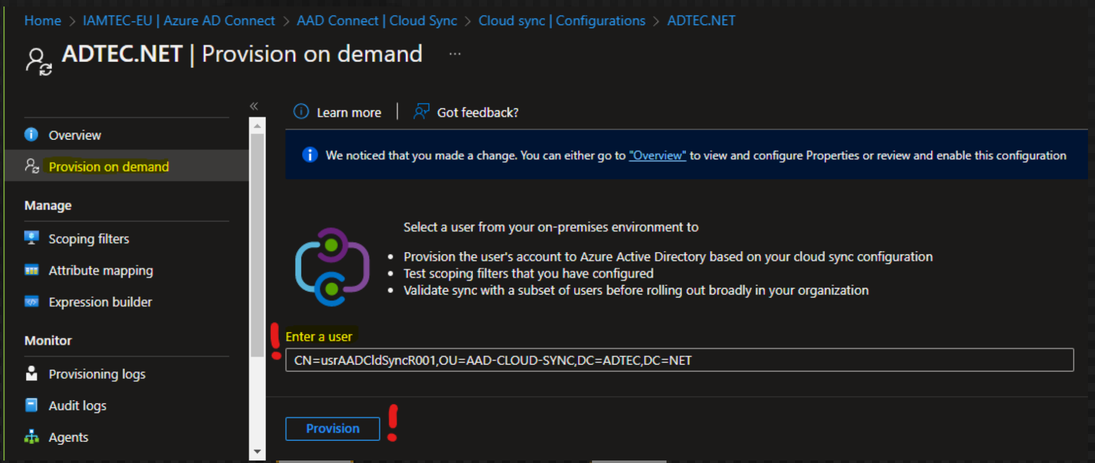
Total Retrieved: 6 matching records   Search for: Pending Export

DN	Object Type	Operation
CN={52616E61324E5066593053375333545A6C...	group	add
CN={4B71514636505733484543385170315663...	user	add
CN={6E4C4A36527452764B306169513967417A...	group	delete
CN={436E4E787633426E473069584B4B427766...	user	delete
CN={344144726C6D58325455325A64505A6C56...	group	update
CN={73772B49574D6F645845576F526332684C...	user	update

! !

Architecture Of Connect Sync And Cloud Sync

- Azure AD CLOUD Sync
  - Manual Checks Before EXPORT: NONE



Home > IAMTEC-EU | Azure AD Connect > AAD Connect | Cloud Sync > Cloud sync | Configurations > ADTEC.NET

ADTEC.NET | Provision on demand ...

We noticed that you made a change. You can either go to "Overview" to view and configure Properties or review and enable this configuration

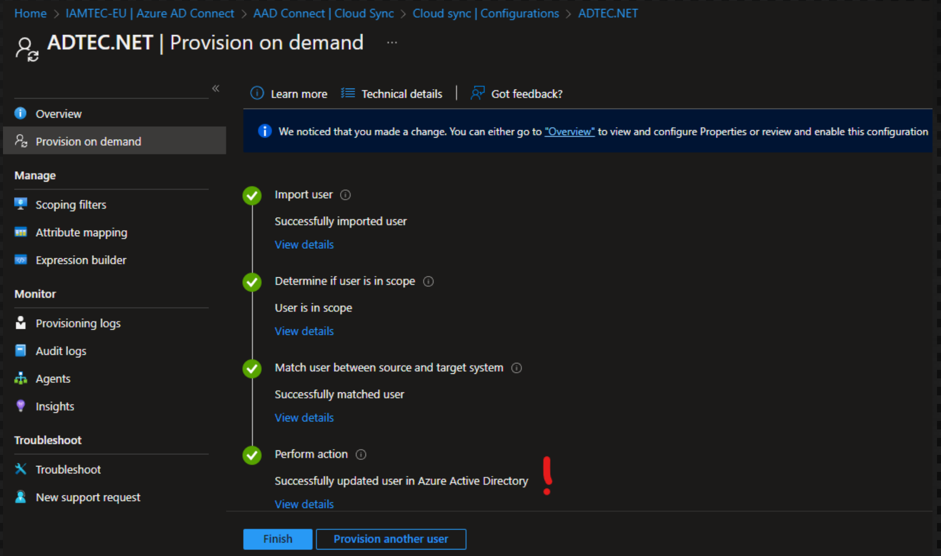
Select a user from your on-premises environment to

- Provision the user's account to Azure Active Directory based on your cloud sync configuration
- Test scoping filters that you have configured
- Validate sync with a subset of users before rolling out broadly in your organization

Enter a user

CN=usrAADCldSyncR001,OU=AAD-CLOUD-SYNC,DC=ADTEC,DC=NET

Provision



Home > IAMTEC-EU | Azure AD Connect > AAD Connect | Cloud Sync > Cloud sync | Configurations > ADTEC.NET

ADTEC.NET | Provision on demand ...

We noticed that you made a change. You can either go to "Overview" to view and configure Properties or review and enable this configuration

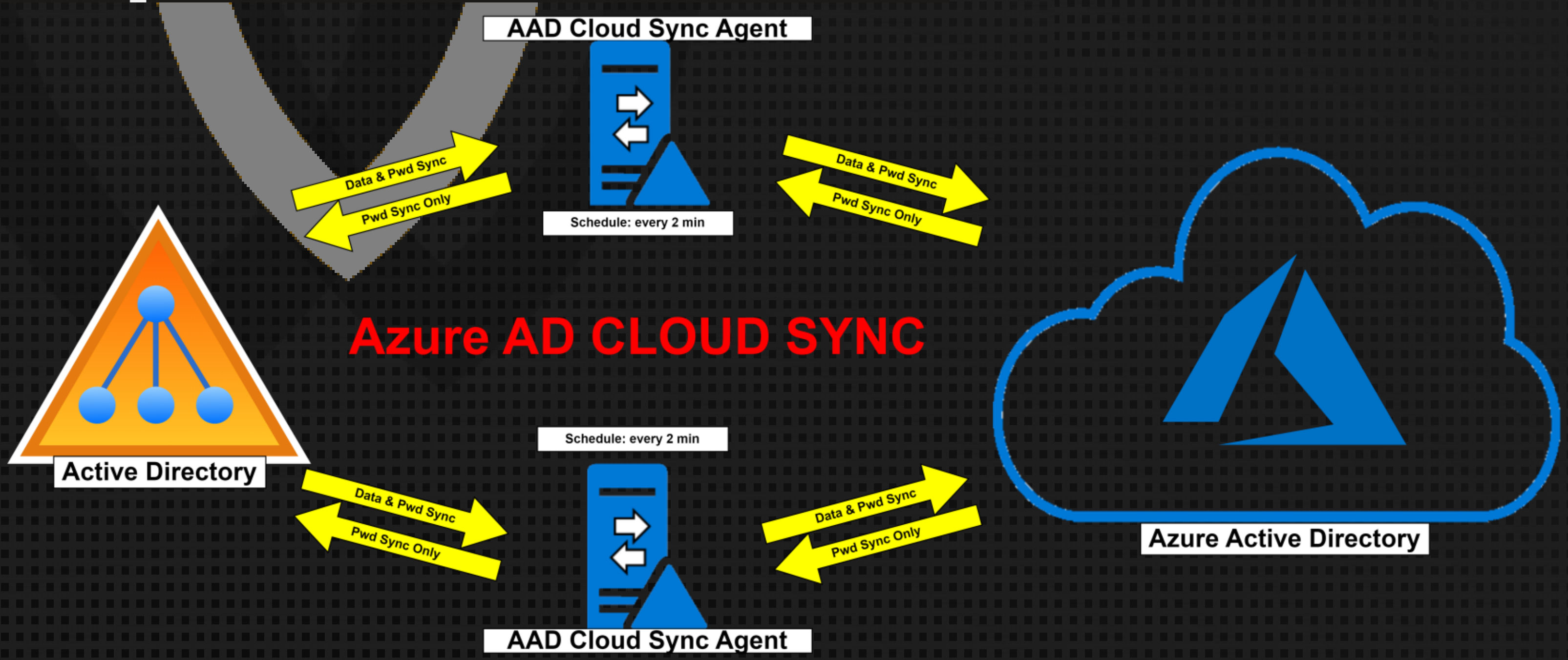
Import user
Successfully imported user
View details

Determine if user is in scope
User is in scope
View details

Match user between source and target system
Successfully matched user
View details

Perform action
Successfully updated user in Azure Active Directory
View details

Finish | Provision another user



Reconnecting With Azure AD - Sync

Reconnecting With Azure AD - Sync

semperis

- What Is Being Used?
  - Azure AD CONNECT Sync

    Or
  - Azure AD CLOUD Sync
- Assumed Starting Point
  - AD Has Been Recovered
  - AD Back To Production
  - AD Needs To Be Needs To Be “Fixed” To Match AAD
  - AAD Connect Sync Server(s), Or AAD Cloud Sync Provisioning Agent(s) May Need To Be Fixed (If Down)

Reconnecting With Azure AD - Sync

semperis

- Azure AD CONNECT Sync (Preparation Tasks)…
  - Down? → Need To Rebuild!
    - Config Export Available?
    - No Config Export?
      - Selected OUs By Querying Synched AAD Objects Against AD And Creating Unique List Of Parent Objects (The OUs) In Canonical Format!
      - Enabled Features? → Hope You Have Good Memory Or Docs
      - Sync Rules? → Hopefully Using Default, Otherwise Good Luck!
  - Up?
    - Scheduler Disabled?

Reconnecting With Azure AD - Sync

semperis

- Azure AD CONNECT Sync (Preparation Tasks)…
  - Which Attribute For "Immutable ID"?
    - When Down? → Scan AD For "Immutable ID" Attribute In AD
    - When Up? → Check Server Config AND Check Sync Rules With Join Criteria On AD And AAD Side (Per Object Type!)

Reconnecting With Azure AD - Sync

semperis

- Azure AD CONNECT Sync (Preparation Tasks)…

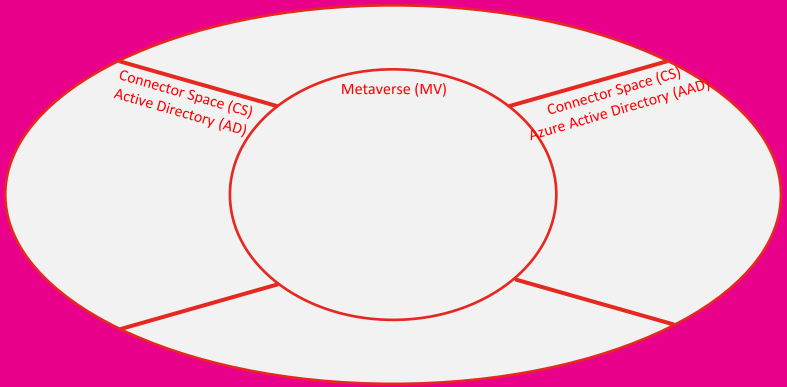
  https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/plan-connect-design-concepts#how-to-enable-the-consistencyguid-feature---existing-deployment

  - “Immutable ID” Attribute In AD = objectGuid?
    - Upgrade To Latest AAD Connect Version FIRST
    - Migrate Immutable ID To “ms-DS-ConsistencyGuid” Attribute
    - Using Federation? → Update Claim Rules!
      - ADFS Managed Through AAD Connect Wizard → Automatically
      - ADFS NOT Managed Through AAD Connect Wizard Or 3rd Party Federation → Fix Manually
    - DO NOT Enable Sync At The End Of The AAD Connect Wizard Configuration (Re)Configuration!!!

Reconnecting With Azure AD - Sync

- Azure AD CONNECT Sync (Preparation Tasks)…
  - Review Sync Rules (**“User” Objects**)

Rule Name (AD)	CS AD Attribute(s)	MV Attribute	CS AAD Attribute	Rule Name (AAD)
JOIN RULES				
In From AD - User Join	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary		
		sourceAnchor	sourceAnchor	In from AAD - User Join

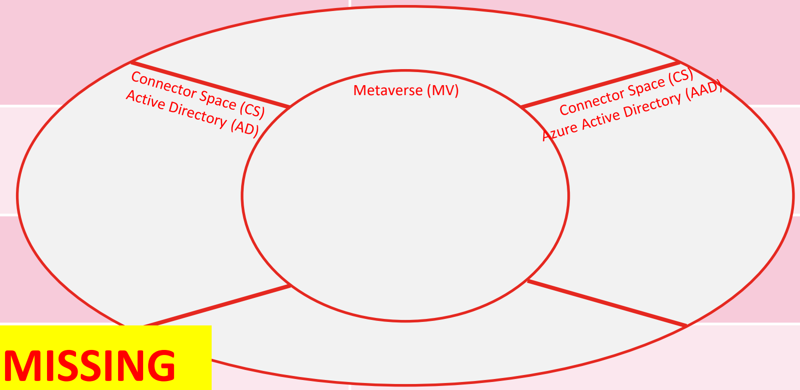


Reconnecting With Azure AD - Sync

➢Azure AD CONNECT Sync (Preparation Tasks)…

➢Review Sync Rules (**“Group” Objects**)

Rule Name (AD)	CS AD Attribute(s)	MV Attribute	CS AAD Attribute	Rule Name (AAD)
JOIN RULES				
In From AD - Group Join	1) ms-DS-ConsistencyGuid 2) objectGUID ↔	sourceAnchorBinary		
		sourceAnchor ↔	sourceAnchor	In from AAD - Group Join
TRANSFORMATION(S)				
In From AD - Group Join	1) ms-DS-ConsistencyGuid 2) objectGUID →	sourceAnchorBinary		
In from AD - Group Common	1) ms-DS-ConsistencyGuid 2) objectGUID →	sourceAnchorBinary		
In from AD - Group Common	1) ms-DS-ConsistencyGuid (Base64) 2) objectGUID (Base64) →	sourceAnchor		
Out to AD - Group ImmutableId	ms-DS-ConsistencyGuid ←	sourceAnchorBinary	← MISSING	



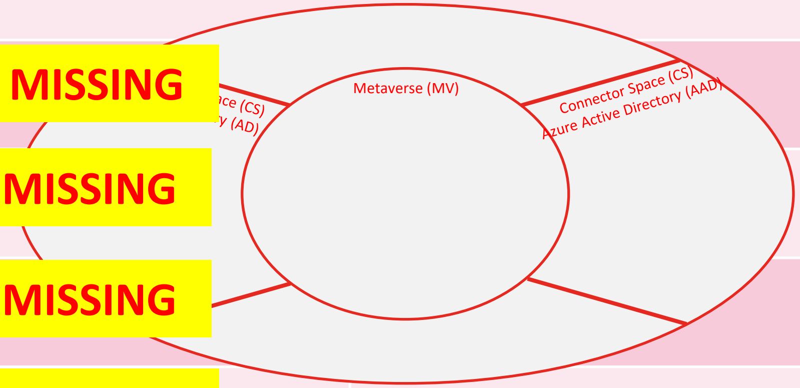
Reconnecting With Azure AD - Sync

semperis

➢Azure AD CONNECT Sync (Preparation Tasks)…

➢Review Sync Rules (**“Contact” Objects**)

Rule Name (AD)	CS AD Attribute(s)	MV Attribute	CS AAD Attribute	Rule Name (AAD)
		JOIN RULES		
In From AD - Contact Join	1) ms-DS-ConsistencyGuid 2) objectGUID Mail	↔ sourceAnchorBinary Mail	← MISSING	
		sourceAnchor ↔	sourceAnchor	In from AAD - Contact Join
		TRANSFORMATION(S)		
In From AD - Contact Join	1) ms-DS-ConsistencyGuid 2) objectGUID	→ sourceAnchorBinary	← MISSING	
In from AD - Contact Common	1) ms-DS-ConsistencyGuid 2) objectGUID	→ sourceAnchorBinary	← MISSING	
In from AD - Contact Common	1) ms-DS-ConsistencyGuid (Base64) 2) objectGUID (Base64)	→ sourceAnchor	← MISSING	
Out to AD - Contact ImmutableId	ms-DS-ConsistencyGuid	← sourceAnchorBinary	← MISSING	



Reconnecting With Azure AD - Sync

- Azure AD CLOUD Sync (Preparation Tasks)…
  - Configuration(s) Disabled In AAD?

Reconnecting With Azure AD - Sync

semperis

- GAP Analysis Between AAD And AD
  - Get Synched Objects From AAD (OnPremisesSyncEnabled = True) & Check Existence In AD (Using GC!) (REMARK: Watch Out For Multiple AD Domains!)
    - Users/Groups → I.e., "OnPremisesSecurityIdentifier" In AAD Against "objectSid" In AD
    - Contacts → I.e., "Mail" In AAD Against "mail" In AD
    - Others? → Check For Usable Attributes
  - For Groups, Also Evaluate The Memberships In AAD Against AD (To Prevent Deleted members)

Reconnecting With Azure AD - Sync

- Fixing Objects In AD
  - Recreate MISSING Users/Groups/Contacts In AD Using Data From AAD
  - Re-Establish MISSING Group Memberships In AD Using Data From AAD

Reconnecting With Azure AD - Sync

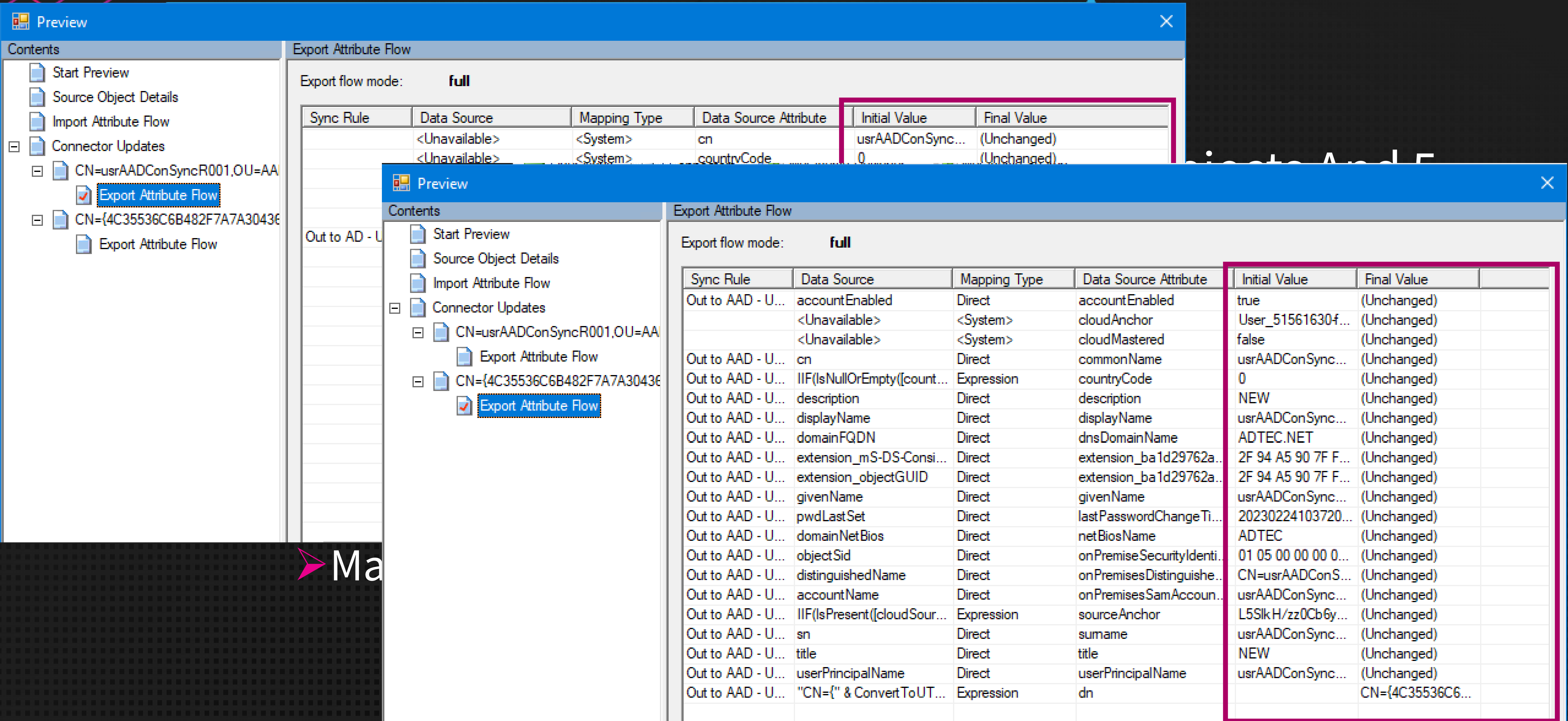
semperis

- Populating “Immutable ID” Values (SourceAnchor)
  - MSFT (AAD And Graph) PoSH And “Immutable ID”:
    - Exposed For Users
    - NOT Exposed For Groups
  - Azure AD Connect Sync And “Immutable ID”:
    - Exposed For Users AND Groups
    - Query AAD Connector Space Or Use AADInternals PoSH Module (= Non-MSFT!)
  - Using Azure AD Cloud Sync?
    - Use AADInternals PoSH Module (= Non-MSFT!)

Reconnecting With Azure AD - Sync

- Reenabling Sync Between AD And AAD (*Applicable For Azure AD CONNECT Sync!*)
  - Manual Full Import On AD Connector
  - Manual Full Import On AAD Connector

Reconnecting With Azure AD - Sync



Preview

Contents

- Start Preview
- Source Object Details
- Import Attribute Flow
- Connector Updates
  - CN=usrAADConSyncR001,OU=AA
    - Export Attribute Flow
  - CN={4C35536C6B482F7A7A30436
    - Export Attribute Flow

Export Attribute Flow

Export flow mode: **full**

Sync Rule	Data Source	Mapping Type	Data Source Attribute	Initial Value	Final Value
	<Unavailable>	<System>	cn	usrAADConSync...	(Unchanged)
	<Unavailable>	<System>	countryCode	0	(Unchanged)
Out to AD - U					

Preview

Contents

- Start Preview
- Source Object Details
- Import Attribute Flow
- Connector Updates
  - CN=usrAADConSyncR001,OU=AA
    - Export Attribute Flow
  - CN={4C35536C6B482F7A7A30436
    - Export Attribute Flow

Export Attribute Flow

Export flow mode: **full**

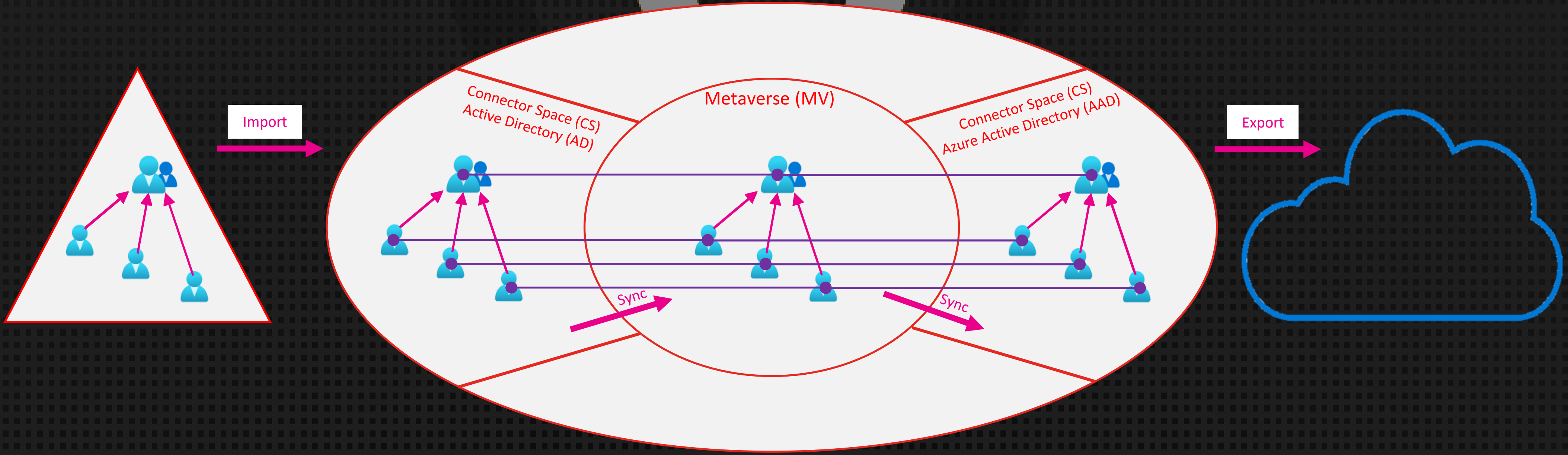
Sync Rule	Data Source	Mapping Type	Data Source Attribute	Initial Value	Final Value
Out to AAD - U...	accountEnabled	Direct	accountEnabled	true	(Unchanged)
	<Unavailable>	<System>	cloudAnchor	User_51561630f...	(Unchanged)
	<Unavailable>	<System>	cloudMastered	false	(Unchanged)
Out to AAD - U...	cn	Direct	commonName	usrAADConSync...	(Unchanged)
Out to AAD - U...	IIF(IsNullOrEmpty([count...	Expression	countryCode	0	(Unchanged)
Out to AAD - U...	description	Direct	description	NEW	(Unchanged)
Out to AAD - U...	displayName	Direct	displayName	usrAADConSync...	(Unchanged)
Out to AAD - U...	domainFQDN	Direct	dnsDomainName	ADTEC.NET	(Unchanged)
Out to AAD - U...	extension_mS-DS-Consi...	Direct	extension_ba1d29762a...	2F 94 A5 90 7F F...	(Unchanged)
Out to AAD - U...	extension_objectGUID	Direct	extension_ba1d29762a...	2F 94 A5 90 7F F...	(Unchanged)
Out to AAD - U...	givenName	Direct	givenName	usrAADConSync...	(Unchanged)
Out to AAD - U...	pwdLastSet	Direct	lastPasswordChangeTi...	20230224103720...	(Unchanged)
Out to AAD - U...	domainNetBios	Direct	netBiosName	ADTEC	(Unchanged)
Out to AAD - U...	objectSid	Direct	onPremiseSecurityIdenti...	01 05 00 00 00 0...	(Unchanged)
Out to AAD - U...	distinguishedName	Direct	onPremisesDistinguishe...	CN=usrAADConS...	(Unchanged)
Out to AAD - U...	accountName	Direct	onPremisesSamAccoun...	usrAADConSync...	(Unchanged)
Out to AAD - U...	IIF(IsPresent([cloudSour...	Expression	sourceAnchor	L5SlkH/zz0Cb6y...	(Unchanged)
Out to AAD - U...	sn	Direct	surname	usrAADConSync...	(Unchanged)
Out to AAD - U...	title	Direct	title	NEW	(Unchanged)
Out to AAD - U...	userPrincipalName	Direct	userPrincipalName	usrAADConSync...	(Unchanged)
Out to AAD - U...	"CN={" & ConvertToUT...	Expression	dn		CN={4C35536C6...

➤Ma

Reconnecting With Azure AD - Sync

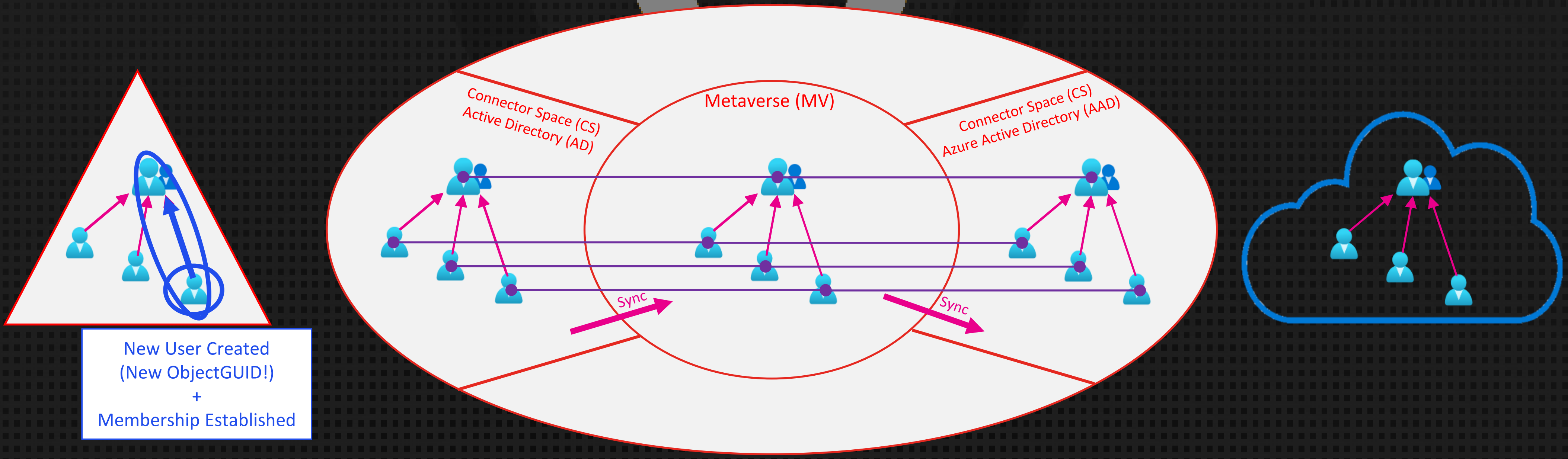
semperis

- Reenabling Sync Between AD And AAD (*Applicable For Azure AD CONNECT Sync!*)
  - For Linked Attributes (e.g. member) You COULD See Weird Behavior That Can Be Explained Due To "Referential Integrity"



Reconnecting With Azure AD - Sync

- Reenabling Sync Between AD And AAD (*Applicable For Azure AD CONNECT Sync!*)
  - For Linked Attributes (e.g. member) You COULD See Weird Behavior That Can Be Explained Due To "Referential Integrity"

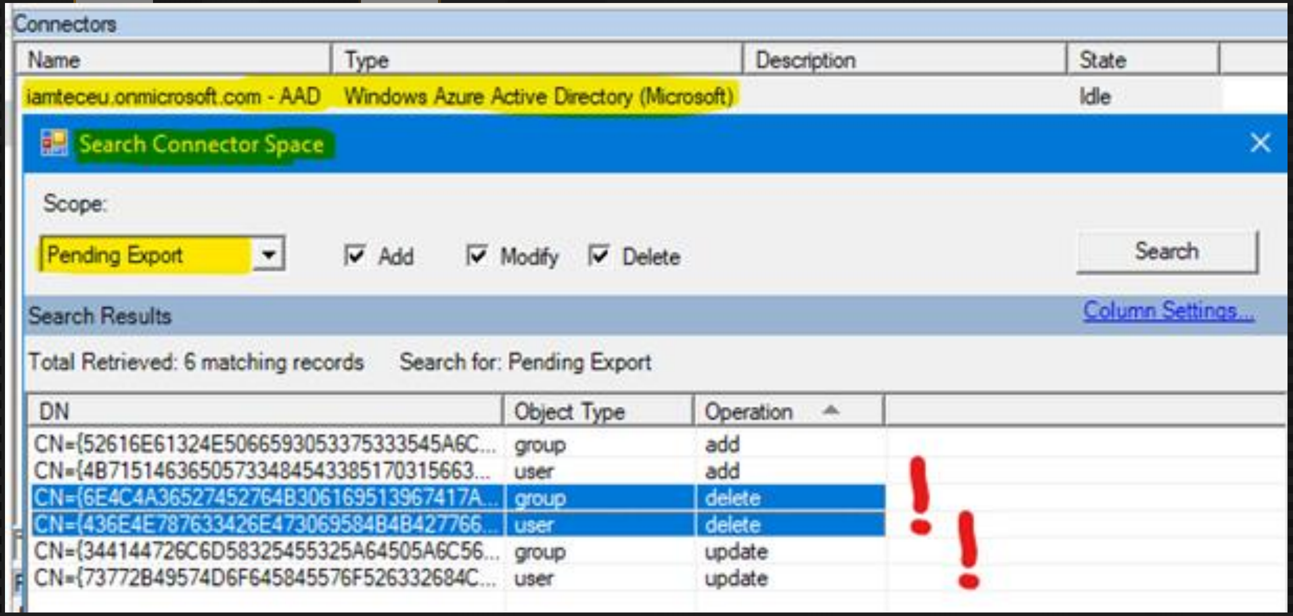


New User Created
(New ObjectGUID!)
+
Membership Established

Reconnecting With Azure AD - Sync

semperis

- Reenabling Sync Between AD And AAD (*Applicable For Azure AD CONNECT Sync!*)
  - Manual Full Synchronization On AD Connector
  - On AAD Connector, Evaluate Pending Exports (Add, Modify, Delete)



Connectors

Name	Type	Description	State
iamteceu.onmicrosoft.com - AAD	Windows Azure Active Directory (Microsoft)		Idle

Search Connector Space

Scope: Pending Export ☑ Add ☑ Modify ☑ Delete

Search Results

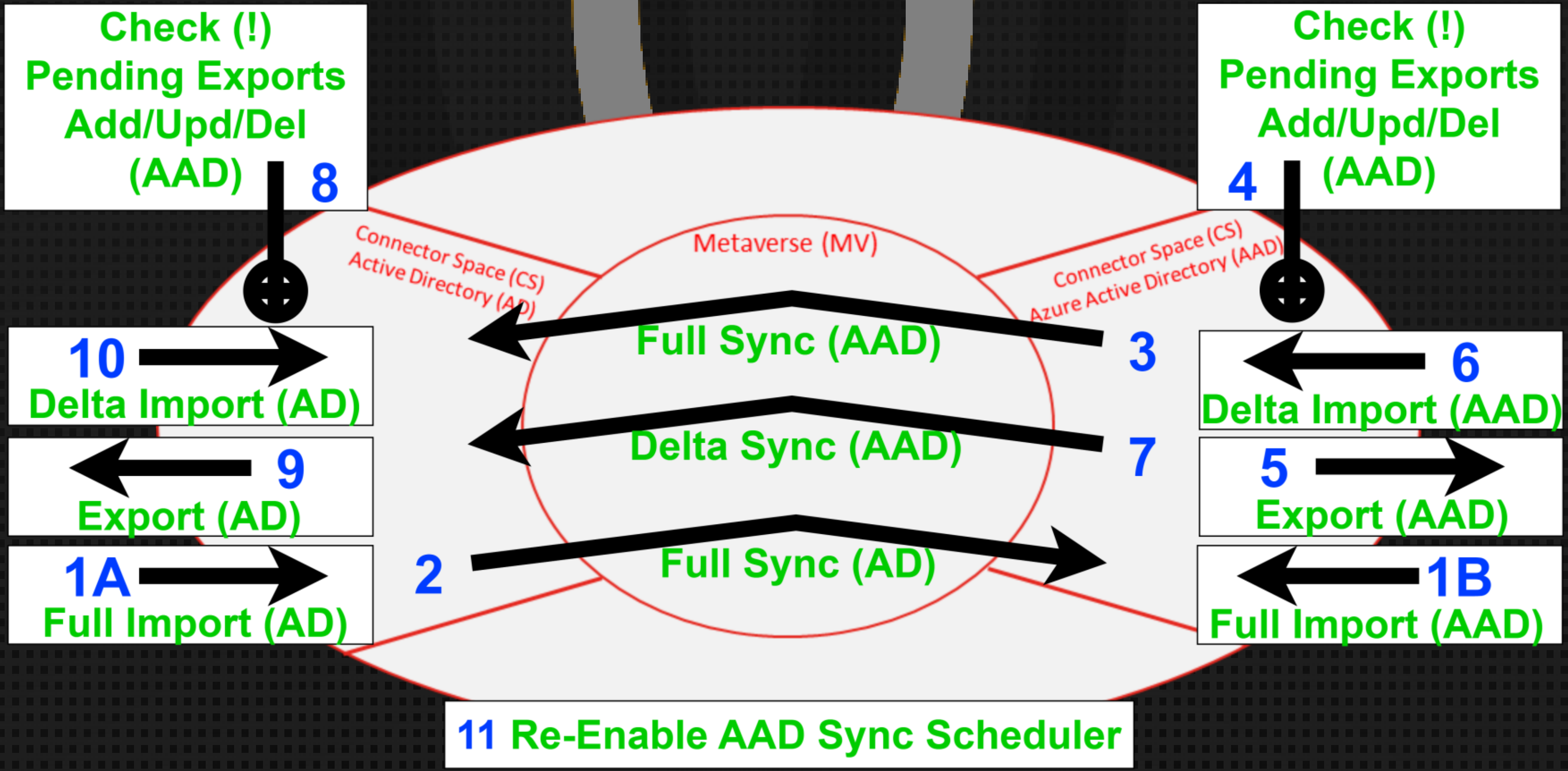
Total Retrieved: 6 matching records   Search for: Pending Export

DN	Object Type	Operation
CN={52616E61324E50665930533753333545A6C...	group	add
CN={4B7151463650573348454338517031566 3...	user	add
CN={6E4C4A36527452764B30616951396741 7A...	group	delete
CN={436E4E787633426E473069584B4B427766...	user	delete
CN={344144726C6D58325455325A64505A6C56...	group	update
CN={73772B49574D6F645845576F526332684C...	user	update

Reconnecting With Azure AD - Sync

semperis

- Reenabling Sync Between AD And AAD (*Applicable For Azure AD CONNECT Sync!*)
  - When All OK, Perform Controlled (Manual) Full Cycle



Reconnecting With Azure AD - Sync

- Reenabling Sync Between AD And AAD (*Applicable For Azure AD CLOUD Sync!*)
  - Reenable Azure AD Cloud Configuration(s)!
  - For Each Config: Restart Sync
  - …AND PRAY ALL IS OK!

Take Aways

Take Aways!

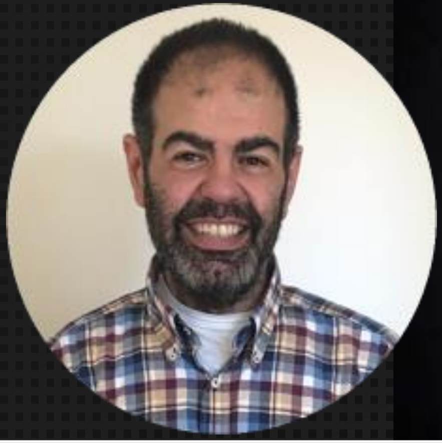
semperis

- The DR Plan Should NOT ONLY Care About AD. But ALSO EVERYTHING Depending On Or Related To AD (e.g. ADFS, AAD Con/Cld Sync, etc)
  - Do Not Forget About Possible/Immediate Pre-Actions (e.g. Impact/Risk-Mitigation) Or Post-Actions (e.g. Improve Security) Required
- Make Sure To Have PHS!
  - Other AuthN And PHS As Backup? → Be Prepared To Change/Convert

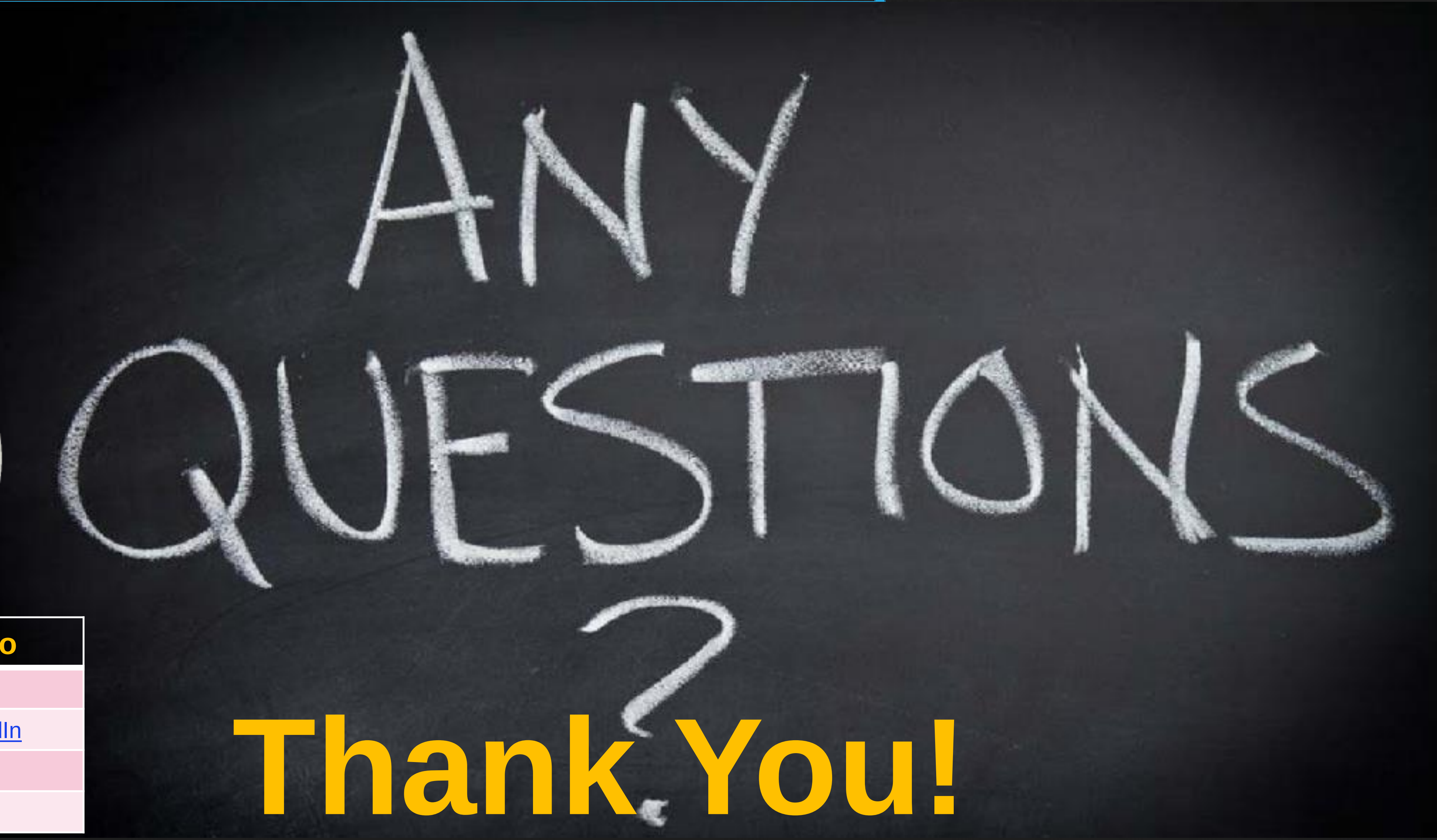
Take Aways!

- For AAD Connect
  - Still Using “ObjectGUID”? → “Migrate To “ms-DS-ConsistencyGuid” As Immutable ID For User/Group/Contact Objects
  - Fix And Update Sync Rules To Correctly Support The Immutable ID “ms-DS-ConsistencyGuid”
- Regularly Export & Secure Config(s) of AADC/ADFS/Others
- !!! AUTOMATE – AUTOMATE – AUTOMATE !!!

Questions? – Get In Touch!



Jorge de Almeida Pinto	
Contact	jorged@semperis.com
LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter



Thank You!