Help! Entra Connect Cloud Sync is here, All you need to know to boost your migration!

WORKPLACEDUDES

SUMMIT 2024

InSpark

Pim Jacobs

Principal Consultant @ InSpark & Microsoft Security MVP

- Focus on the full Microsoft Entra portfolio
- One of the organisers of the **Dutch Microsoft Entra Community**, join our meetup page!

- Blog: **identity-man.eu**
- Skiing | Soccer | F1 | Family time

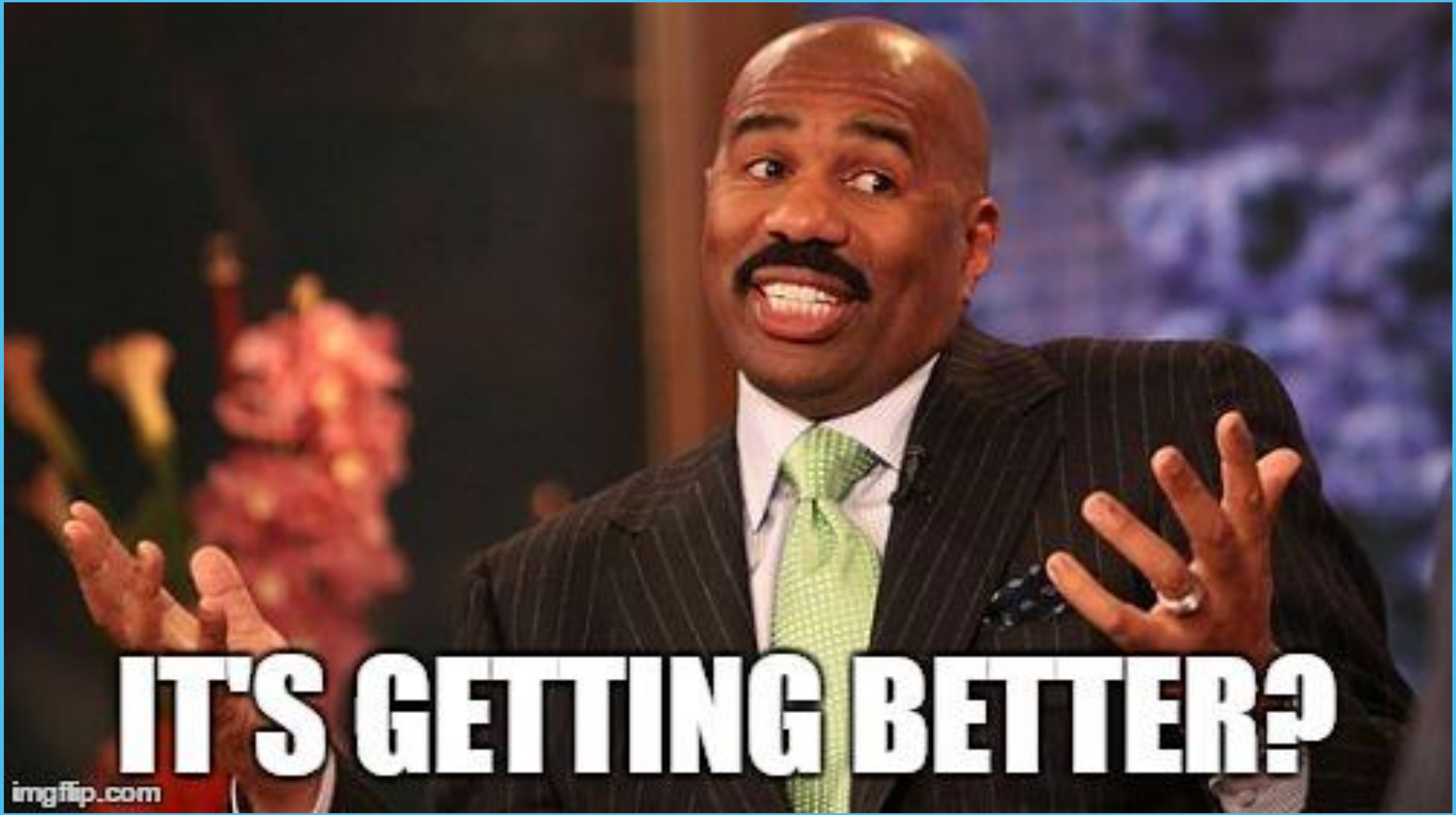
Microsoft® Most Valuable Professional

Agenda

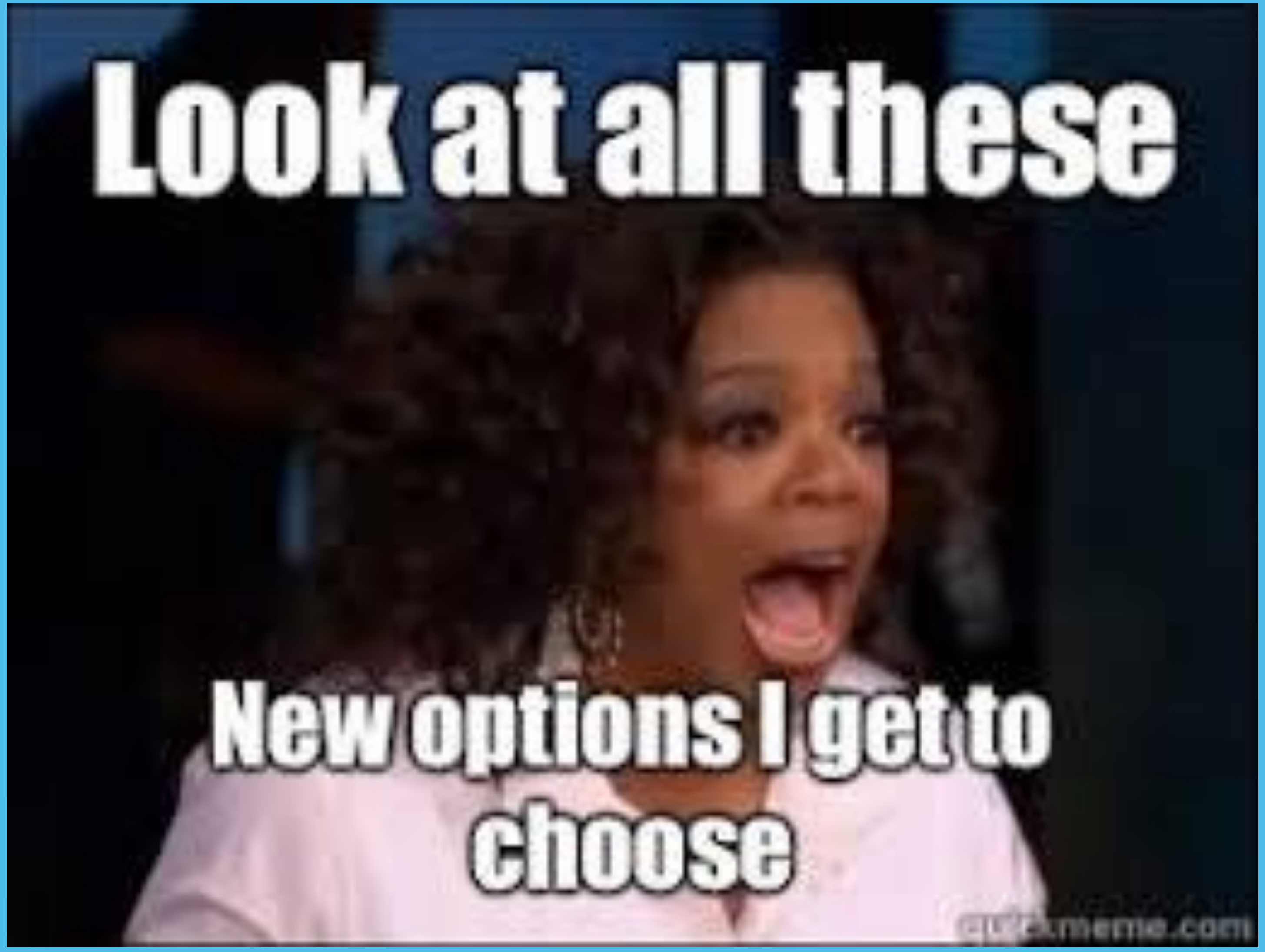
- Why move to Entra Connect Cloud sync?
- Supported Scenarios & Capabilities
- Entra Connect Cloud Sync Architecture
- Configure Entra Connect Cloud Sync to Entra ID
- Migrate to Entra Connect Cloud Sync
- Configure Entra Connect Cloud Sync to Active Directory
- Next Steps & Key takeaways

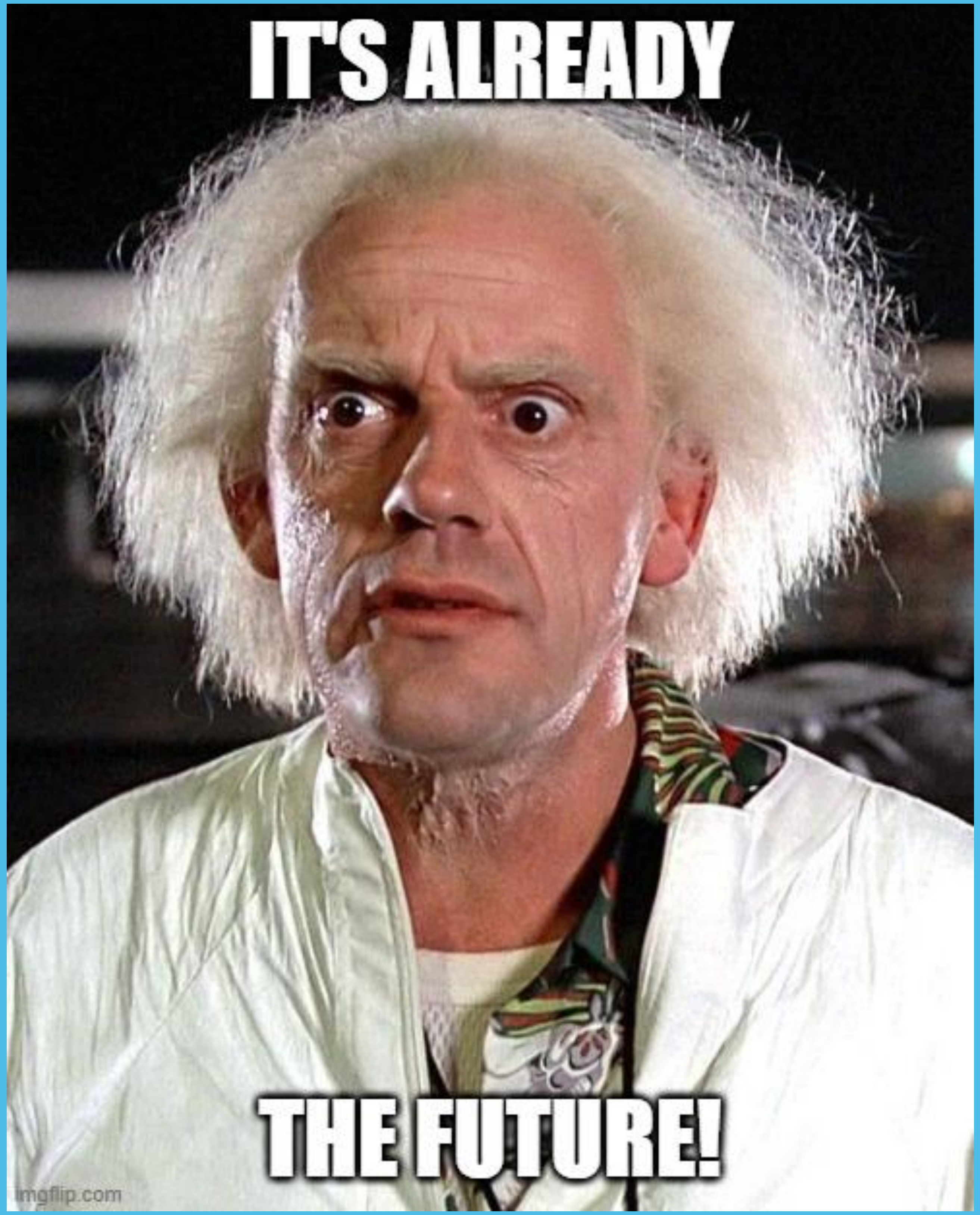
Why move to Entra Connect Cloud sync?

Why move to cloud sync?



Why move to cloud sync?





Supported Scenarios & Capabilities

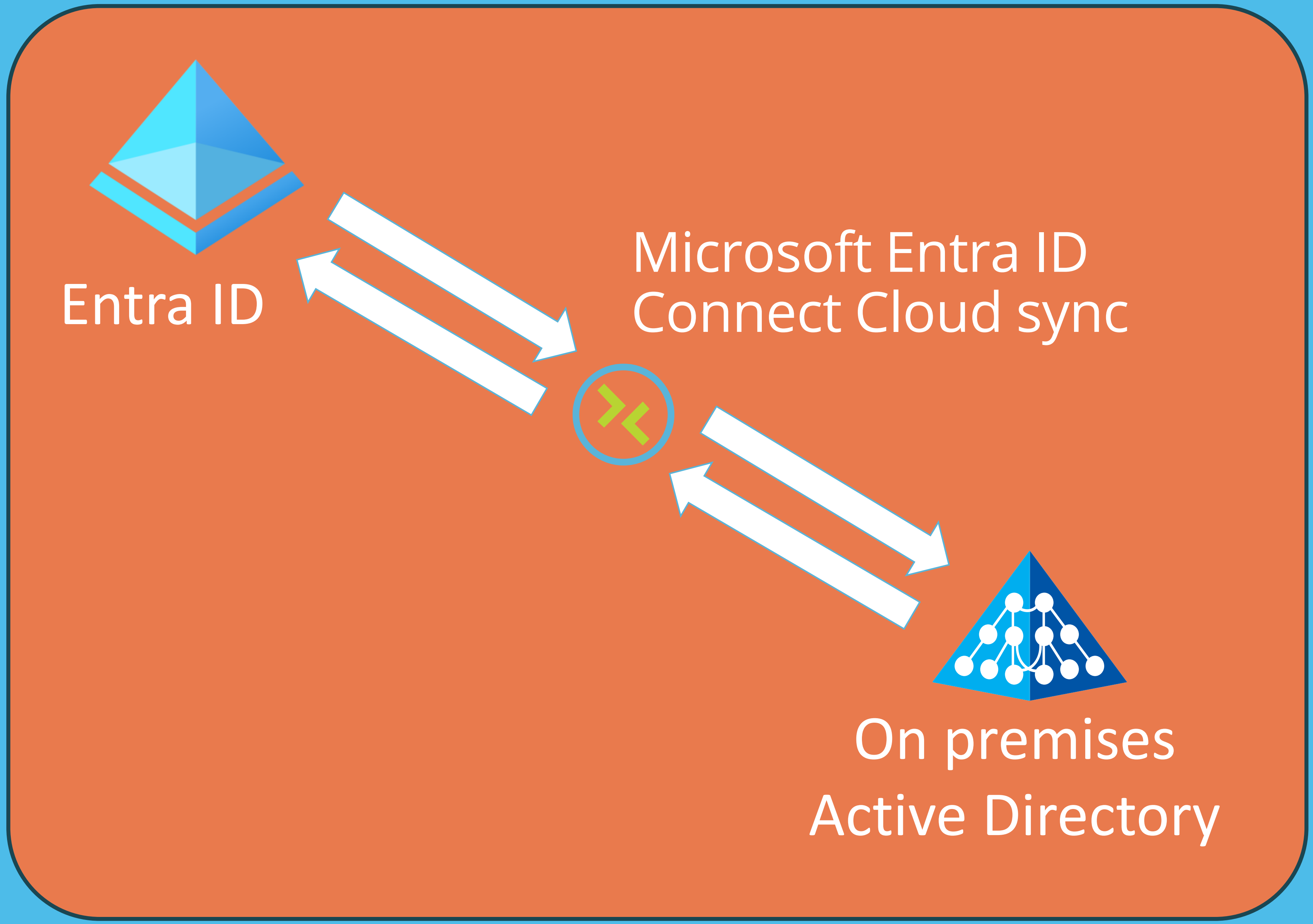
Supported Scenarios

Cost Effective

Quick to deploy

Simple Configuration

Sync in both ways

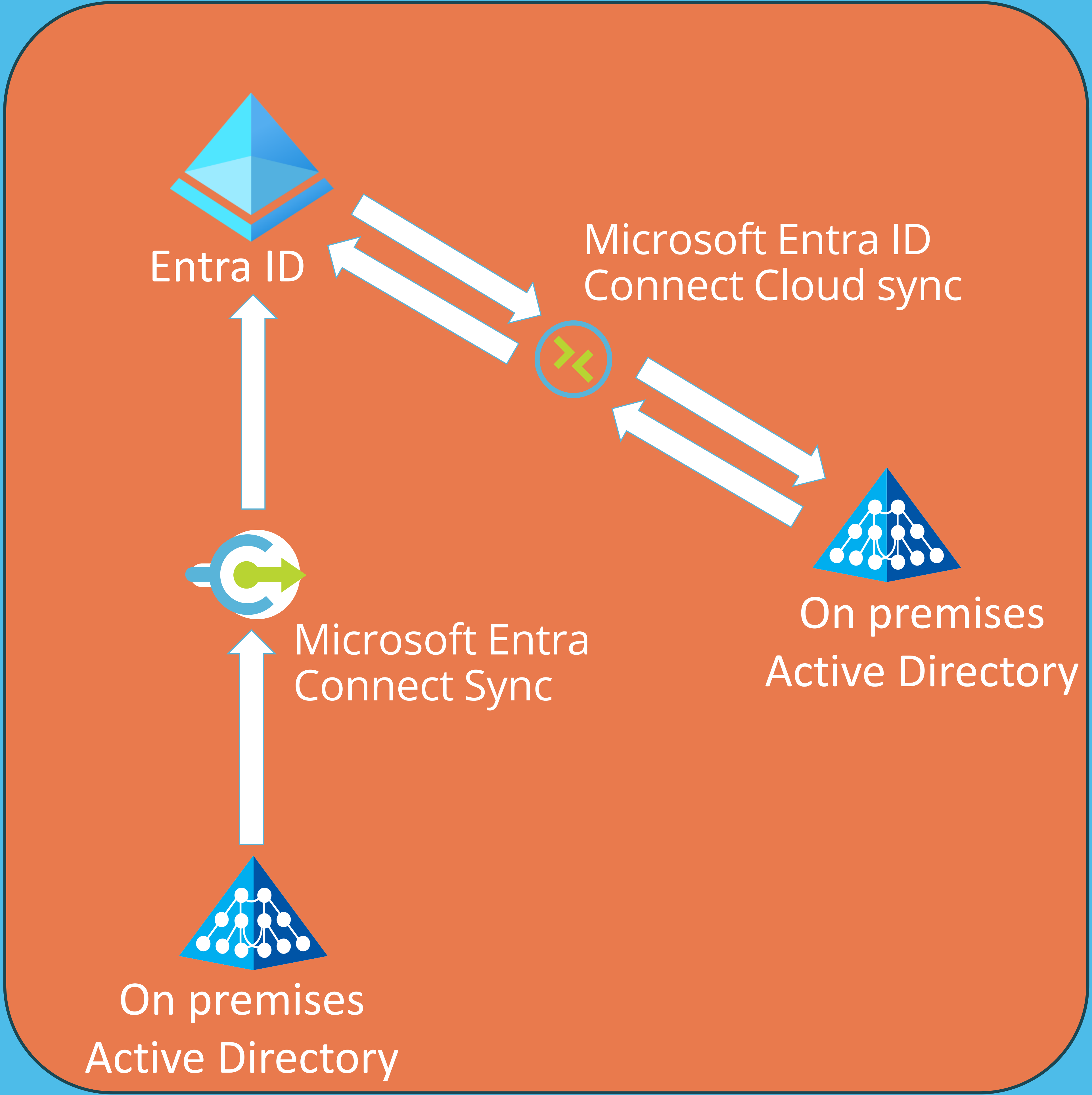


Supported Scenarios

Microsoft Entra Co-existence

Disconnected forest

Resilient architecture



Entra ID
Microsoft Entra ID Connect Cloud sync
Microsoft Entra Connect Sync
On premises Active Directory
On premises Active Directory

InSpark

Current capabilities

Deprecated in connect sync 30 june 2024!

Scenarios & UX

- Users, Contacts, Group & Password sync
- Exchange Hybrid writeback support (also for disconnected forests)
- Directory and custom extension attributes support
- Provision cloud security groups to Active Directory
- Attribute Mapping Experience
- On-demand sync for users
- Accidental Deletes
- Migrate from Connect Sync to Cloud Sync - Steps

Sync Improvements

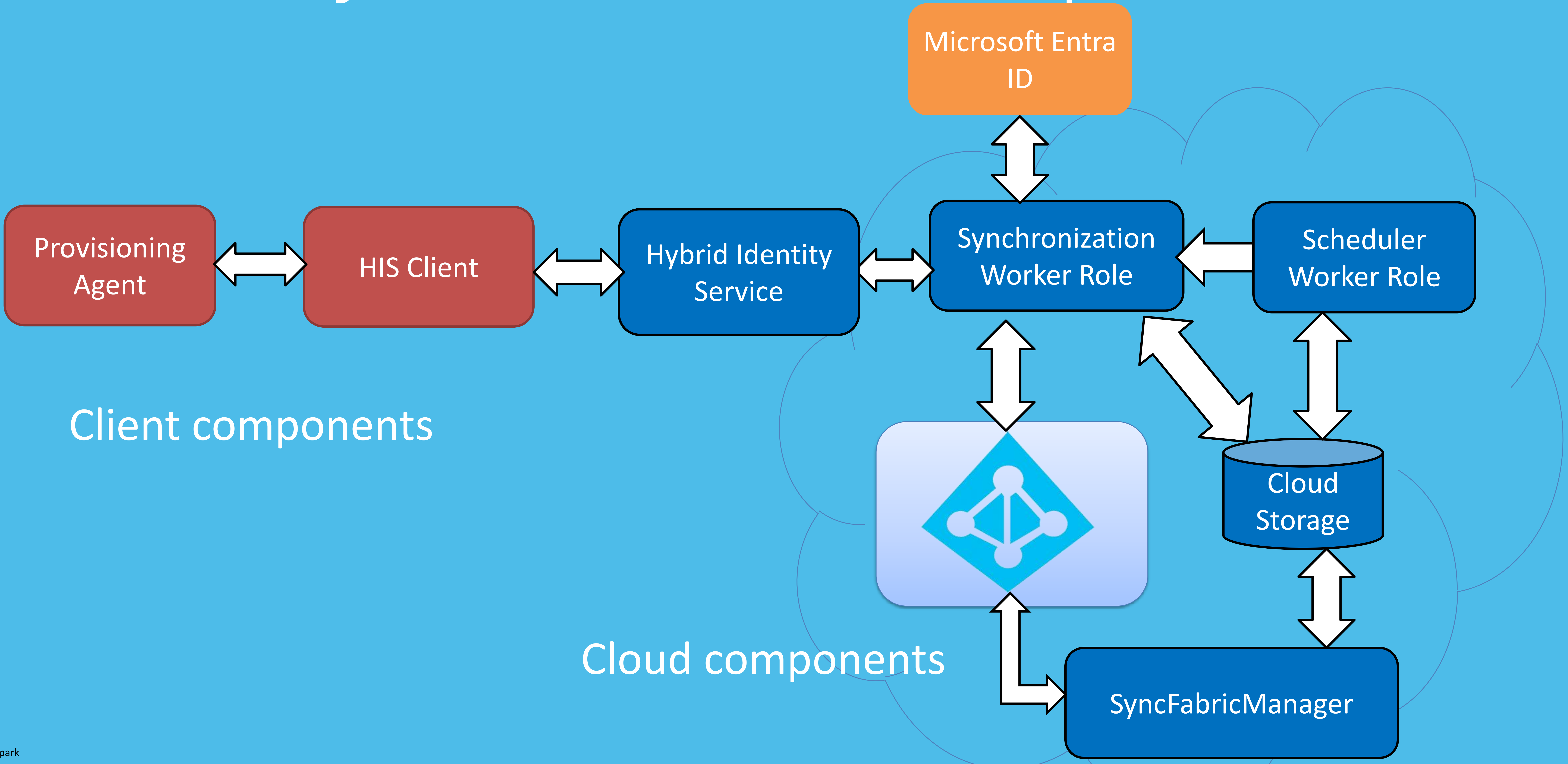
- Support for large object sync (up to 150K AD objects) per domain
- Initial sync time improvements
- Support for groups up to 50k members
- Support for gMSA

Supportability

- Improved Error/Quarantine messages
- UX improvements (Clear Quarantine status, easy copy to clipboard, provisioning insights etc.)
- Easier to provide support
- Self-diagnosis troubleshooting PS toolkit

Entra Connect Cloud Sync Architecture

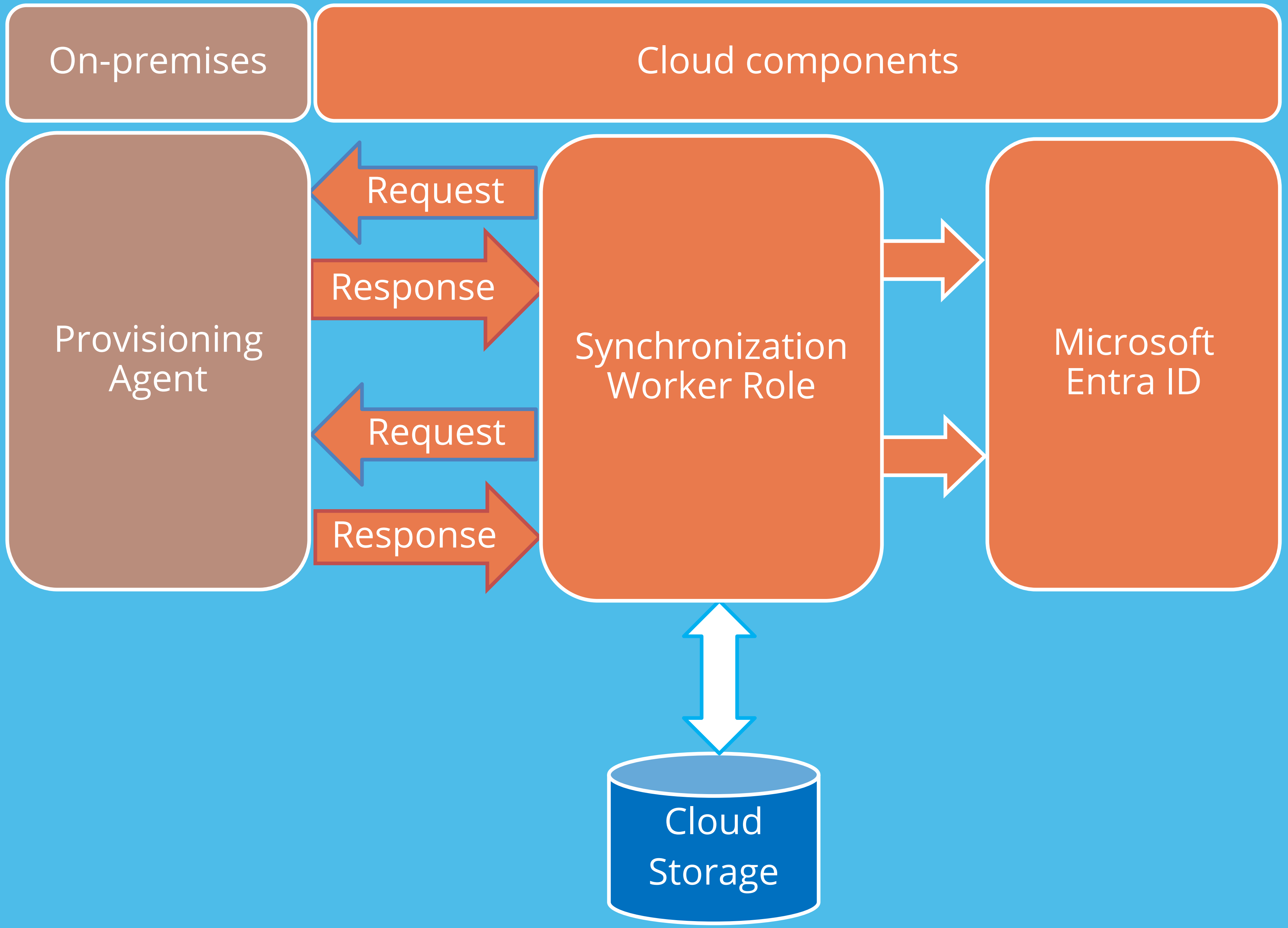
Cloud Sync Architecture & Components



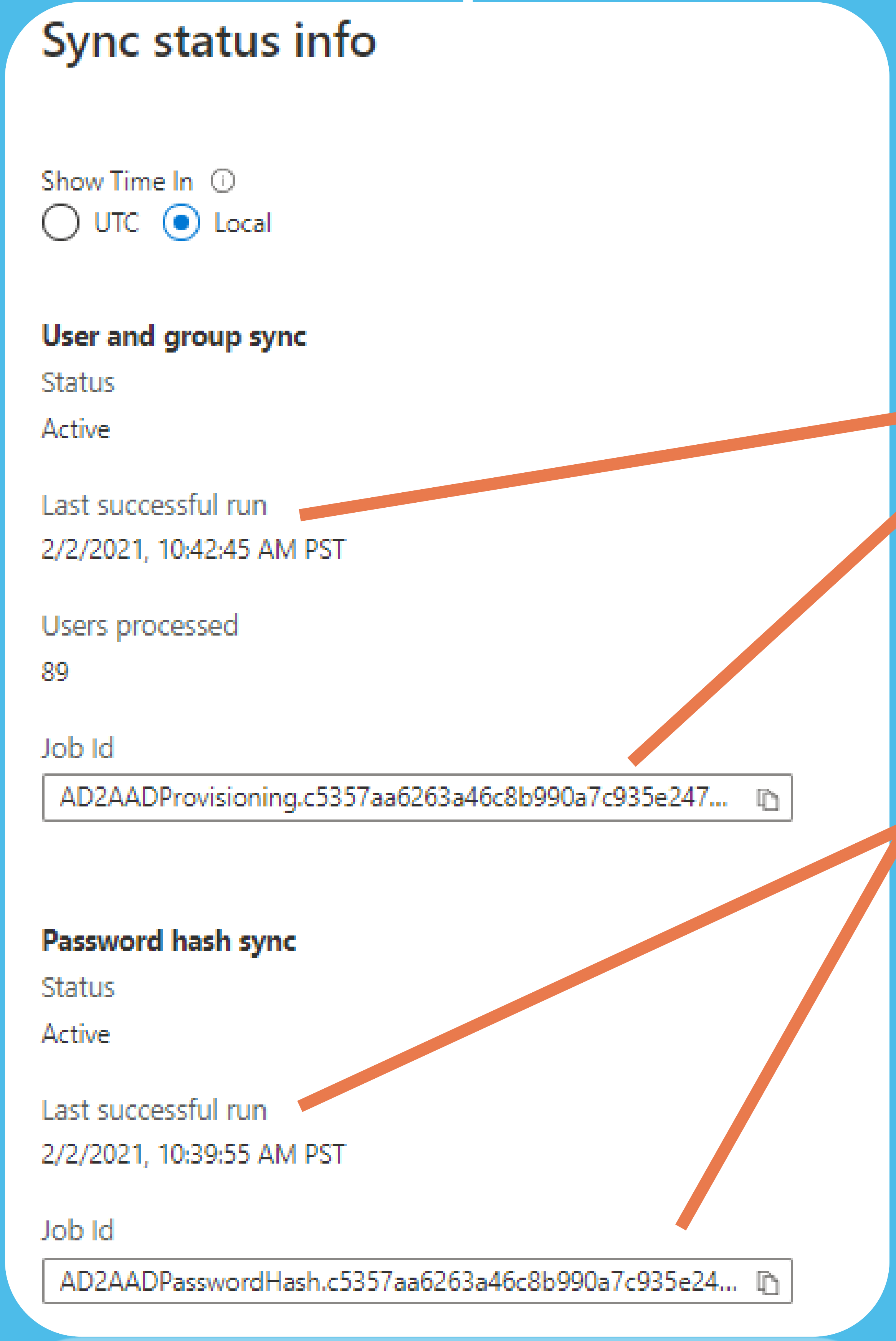
InSpark

Cloud sync cycle explained

- SyncFabric and Agent talk to each through request/response model (config info is sent to Agent with watermark)
- Each cycle is triggered after scheduled RunProfile interval (2 mins)
- Changes not completed in real-time are stored in escrow (data store).
- Cycle reaches quarantine state due to critical issues or hitting escrow threshold limit (40%)
- After repeated quarantine for an hour the RunProfile is tried less often and email is sent out to notify the admin.



Run profiles and Sync cycles | Per domain



Sync status info

Show Time In ⓘ

○ UTC ● Local

User and group sync

Status

Active

Last successful run

2/2/2021, 10:42:45 AM PST

Users processed

89

Job Id

AD2AADProvisioning.c5357aa6263a46c8b990a7c935e247...

Password hash sync

Status

Active

Last successful run

2/2/2021, 10:39:55 AM PST

Job Id

AD2AADPasswordHash.c5357aa6263a46c8b990a7c935e24...

RunProfile

For Object provisioning is created and saved in storage

For PHS (if configured) is created and saved separately in storage

Defines Scoping Filters, Object types, Attributes to read, attribute mappings (identical for both run profiles).

RunProfileIdentifier format: *[Tag].[TenantId].[AD2AAD ApplicationId]*

Sync cycle

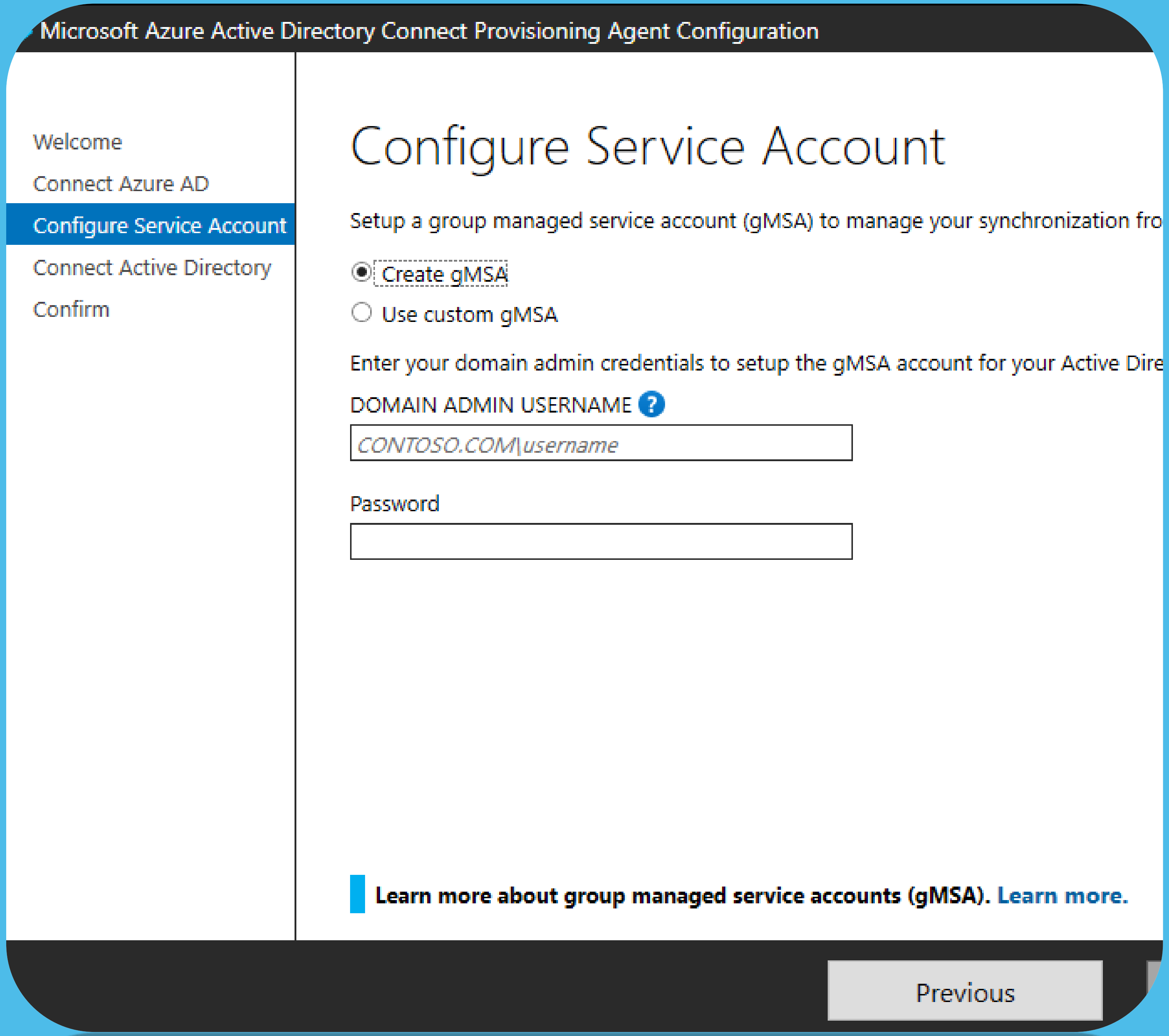
RunProfile for Object provisioning

RunProfile for PHS

Each RunProfile has Full or Delta Sync state - like Entra Connect Sync

Once a Full cycle (Restart sync in UI) has run we move to delta sync

GMSA and the differences



Microsoft Azure Active Directory Connect Provisioning Agent Configuration

Configure Service Account

Setup a group managed service account (gMSA) to manage your synchronization fro

● Create gMSA

○ Use custom gMSA

Enter your domain admin credentials to setup the gMSA account for your Active Dire

DOMAIN ADMIN USERNAME ?

CONTOSO.COM\username

Password

Learn more about group managed service accounts (gMSA). Learn more.

Auto Created GMSA

Created in current domain of local machine

Standard Name: “DomainName\provAgentgMSA$”

Adds Permissions for ALL Domains configured in wizard

Write Permissions to AD added for HR scenarios

Manual created GMSA

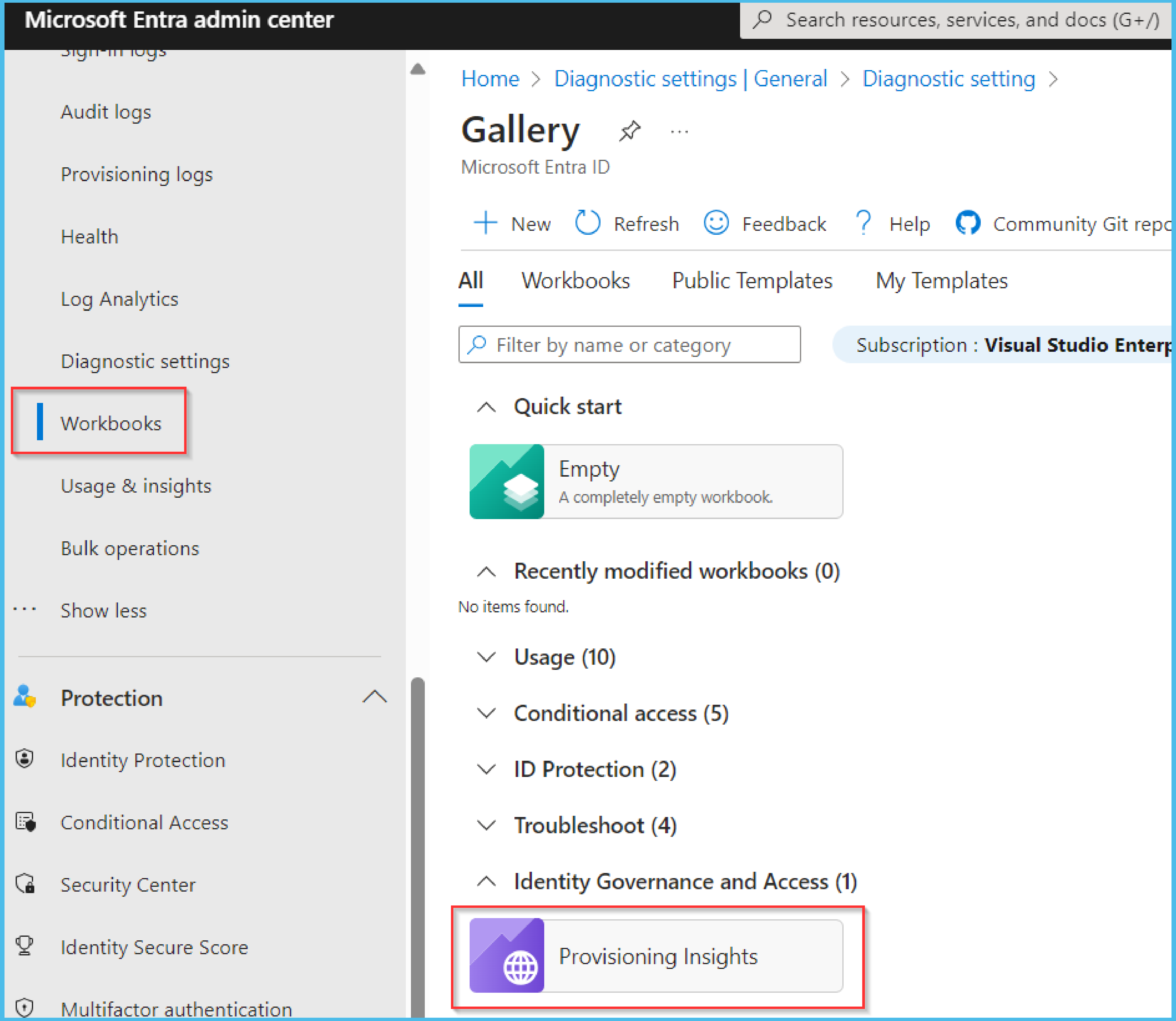
Agent Wizard adds all the same permissions as above

PS Cmdlets available to manage the permissions

- Set-AADCloudSyncPermissions
- Set-AADCloudSyncRestrictedPermissions

[Microsoft Entra provisioning Agent gMSA PowerShell cmdlets - Microsoft Entra ID | Microsoft Learn]()

Microsoft Entra ID Provisioning Logs



Microsoft Entra admin center

Search resources, services, and docs (G+/)

Sign-in logs

Audit logs

Provisioning logs

Health

Log Analytics

Diagnostic settings

Workbooks

Usage & insights

Bulk operations

··· Show less

Protection

Identity Protection

Conditional Access

Security Center

Identity Secure Score

Multifactor authentication

Home > Diagnostic settings | General > Diagnostic setting >

Gallery

Microsoft Entra ID

+ New   Refresh   Feedback   ? Help   Community Git repo

All   Workbooks   Public Templates   My Templates

Filter by name or category

Subscription : **Visual Studio Enterp**

Quick start

Empty

A completely empty workbook.

Recently modified workbooks (0)

No items found.

Usage (10)

Conditional access (5)

ID Protection (2)

Troubleshoot (4)

Identity Governance and Access (1)

Provisioning Insights

Central place for all provisioning logs with advanced search & filtering capabilities

Used for troubleshooting and automation

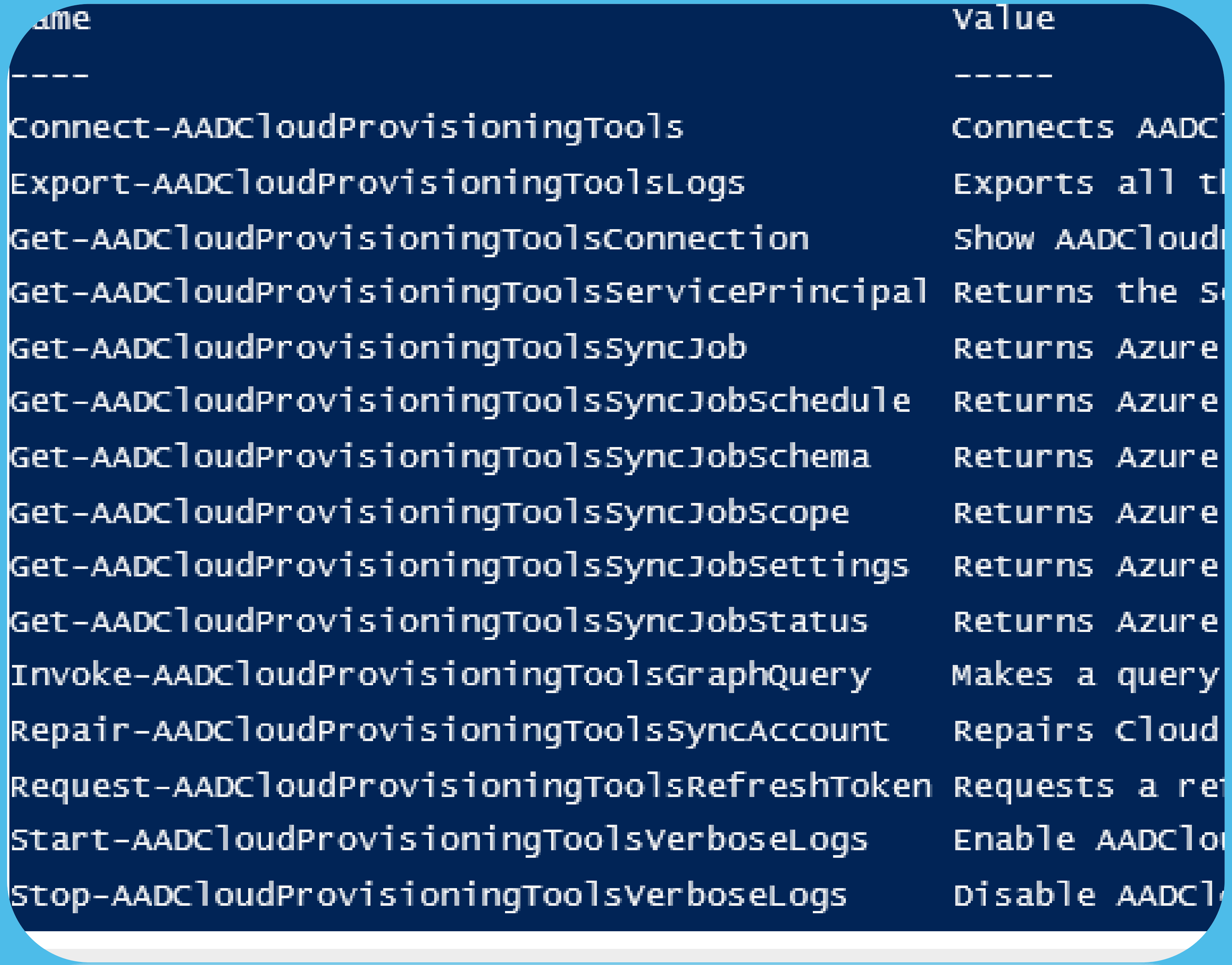
MS Graph API supported

Integrated with Log Analytics

Built-in workbooks and Insights in Entra Portal

Explore synchronization jobs with PowerShell and more

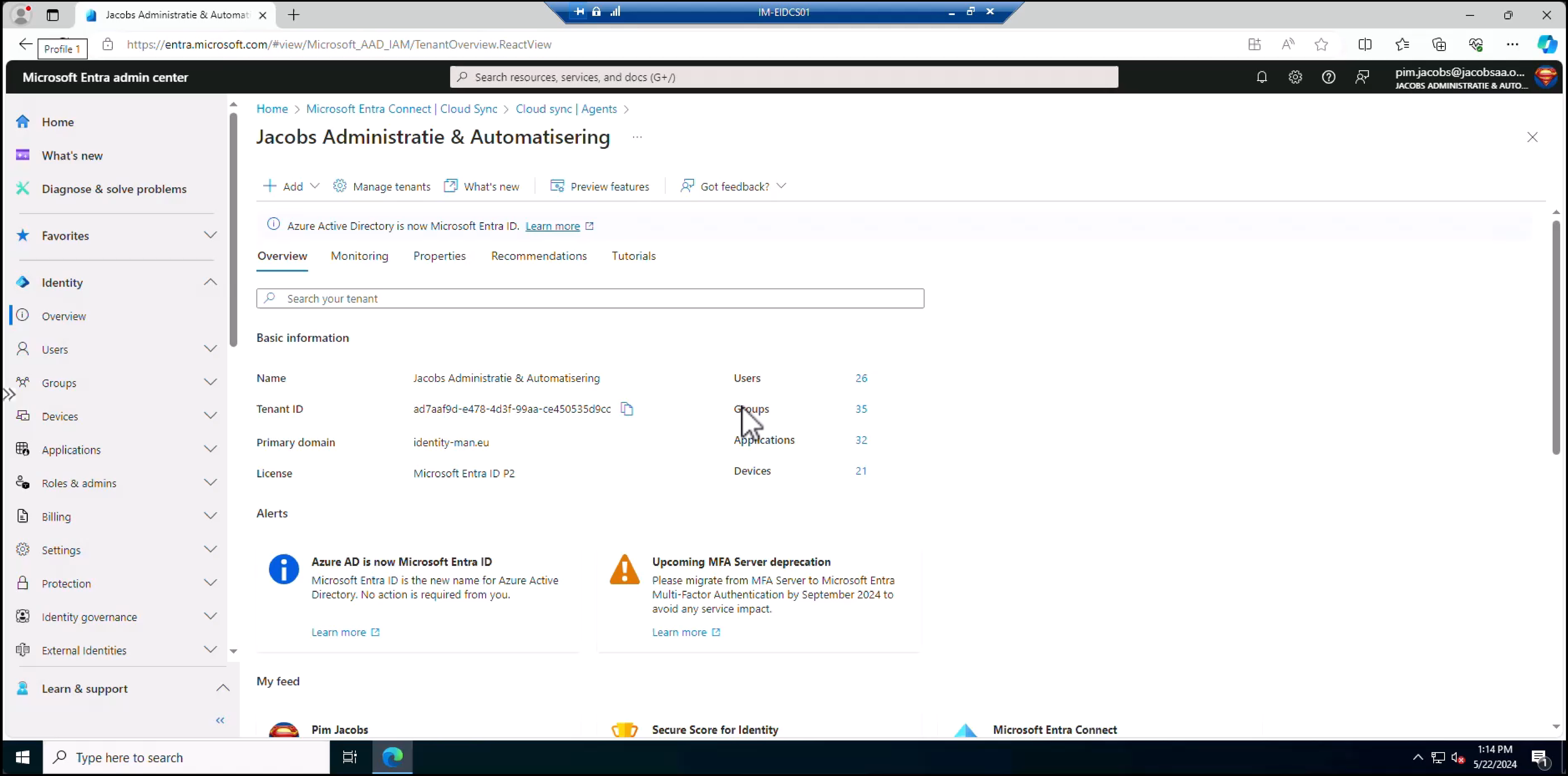
- **Initially introduced to repair sync service account**
- **Expanded to facilitate verbose tracing & reduce dependency on Graph Explorer**
- **Can be used on any machine, except for collecting verbose logs**
- **Use Get-Help <cmdlet>**



```
ame                                          Value
----                                         -----
Connect-AADCloudProvisioningTools            Connects AADC
Export-AADCloudProvisioningToolsLogs         Exports all t
Get-AADCloudProvisioningToolsConnection      Show AADCloud
Get-AADCloudProvisioningToolsServicePrincipal Returns the S
Get-AADCloudProvisioningToolsSyncJob         Returns Azure
Get-AADCloudProvisioningToolsSyncJobSchedule Returns Azure
Get-AADCloudProvisioningToolsSyncJobSchema   Returns Azure
Get-AADCloudProvisioningToolsSyncJobScope    Returns Azure
Get-AADCloudProvisioningToolsSyncJobSettings Returns Azure
Get-AADCloudProvisioningToolsSyncJobStatus   Returns Azure
Invoke-AADCloudProvisioningToolsGraphQuery   Makes a query
Repair-AADCloudProvisioningToolsSyncAccount  Repairs Cloud
Request-AADCloudProvisioningToolsRefreshToken Requests a re
Start-AADCloudProvisioningToolsVerboseLogs   Enable AADClo
Stop-AADCloudProvisioningToolsVerboseLogs    Disable AADCl
```

[AADCloudSyncTools PowerShell module for Microsoft Entra Cloud Sync - Microsoft Entra ID | Microsoft Learn]

DEMO #1
Configure Entra Connect Cloud Sync to Entra ID



Jacobs Administratie & Automatisering

Azure Active Directory is now Microsoft Entra ID. Learn more

Basic information

Name	Jacobs Administratie & Automatisering	Users	26
Tenant ID	ad7aaf9d-e478-4d3f-99aa-ce450535d9cc	Groups	35
Primary domain	identity-man.eu	Applications	32
License	Microsoft Entra ID P2	Devices	21

Alerts

Azure AD is now Microsoft Entra ID
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.
Learn more

Upcoming MFA Server deprecation
Please migrate from MFA Server to Microsoft Entra Multi-Factor Authentication by September 2024 to avoid any service impact.
Learn more

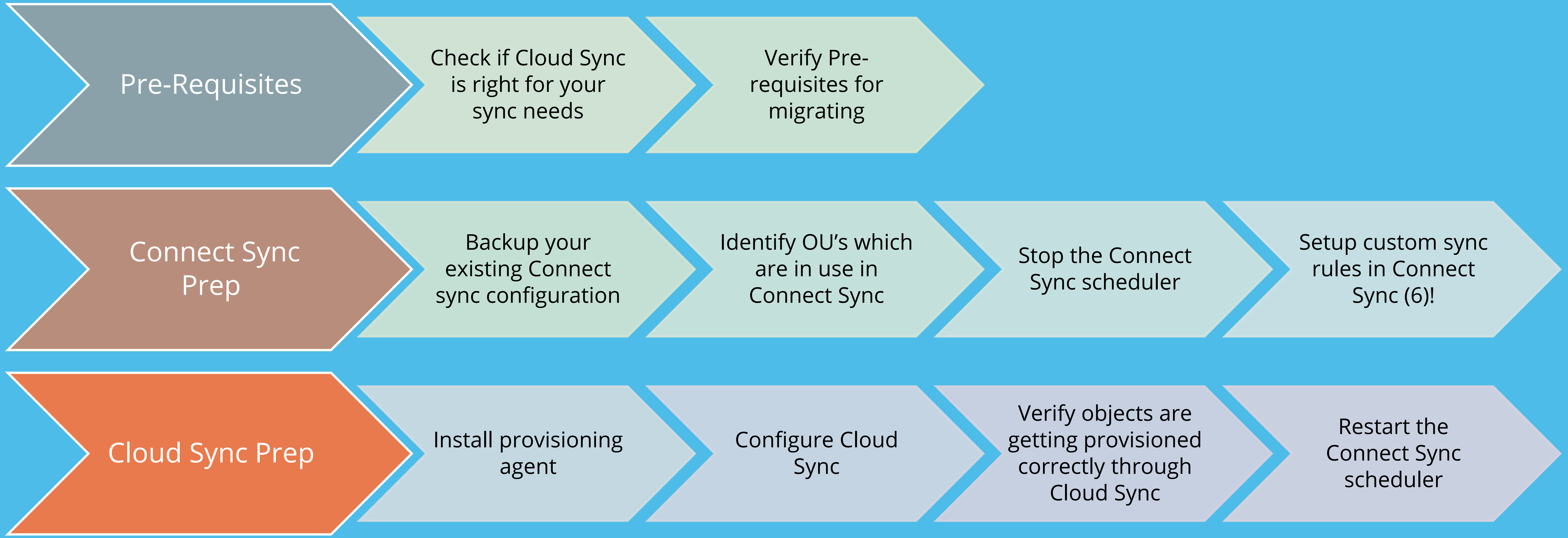
My feed

Pim Jacobs

Secure Score for Identity

Microsoft Entra Connect

Steps to migrate in phased approach to Cloud Sync



Pre-Requisites

- Check if Cloud Sync is right for your sync needs
- Verify Pre-requisites for migrating

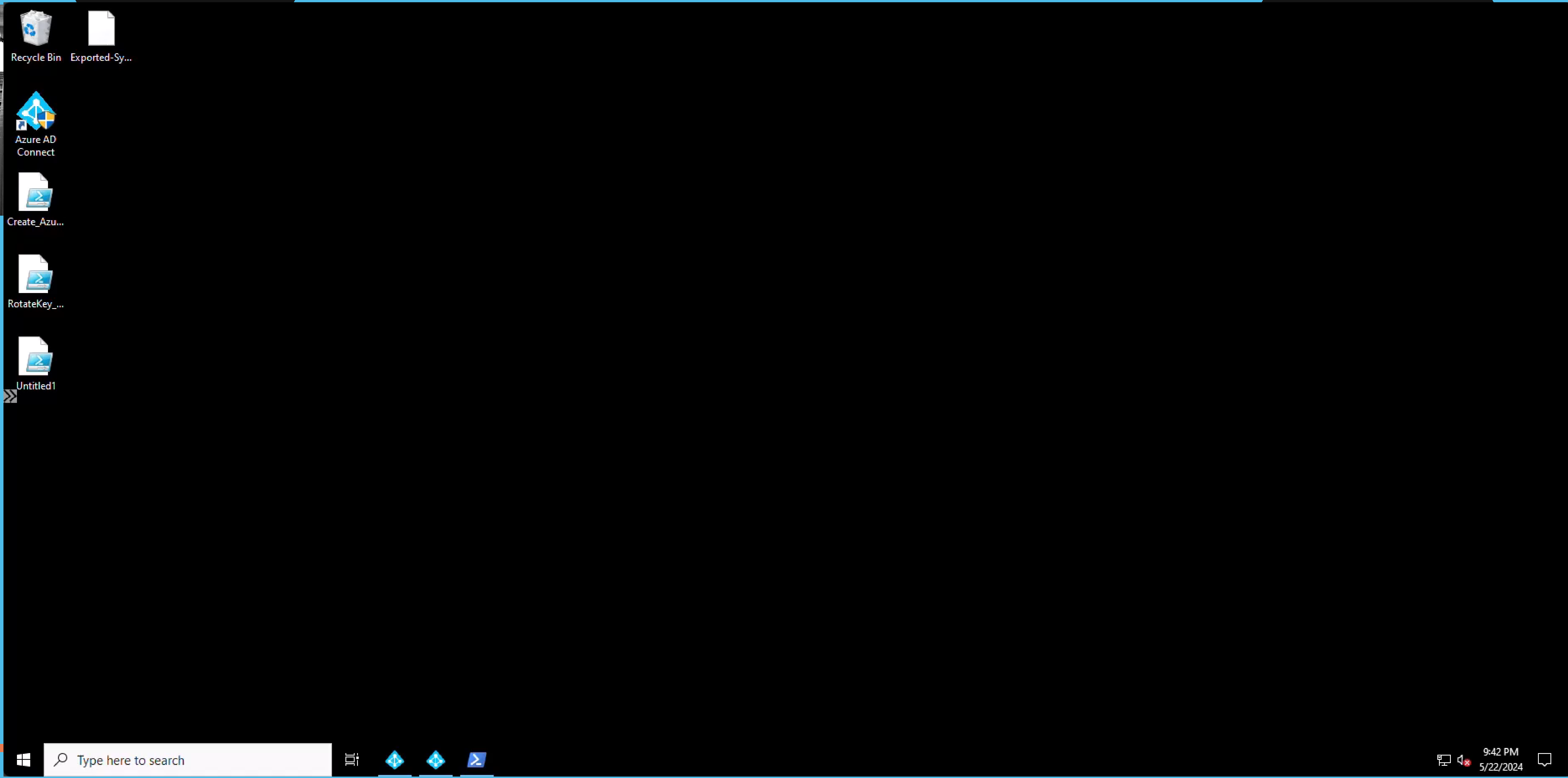
Connect Sync Prep

- Backup your existing Connect sync configuration
- Identify OU's which are in use in Connect Sync
- Stop the Connect Sync scheduler
- Setup custom sync rules in Connect Sync (6)!

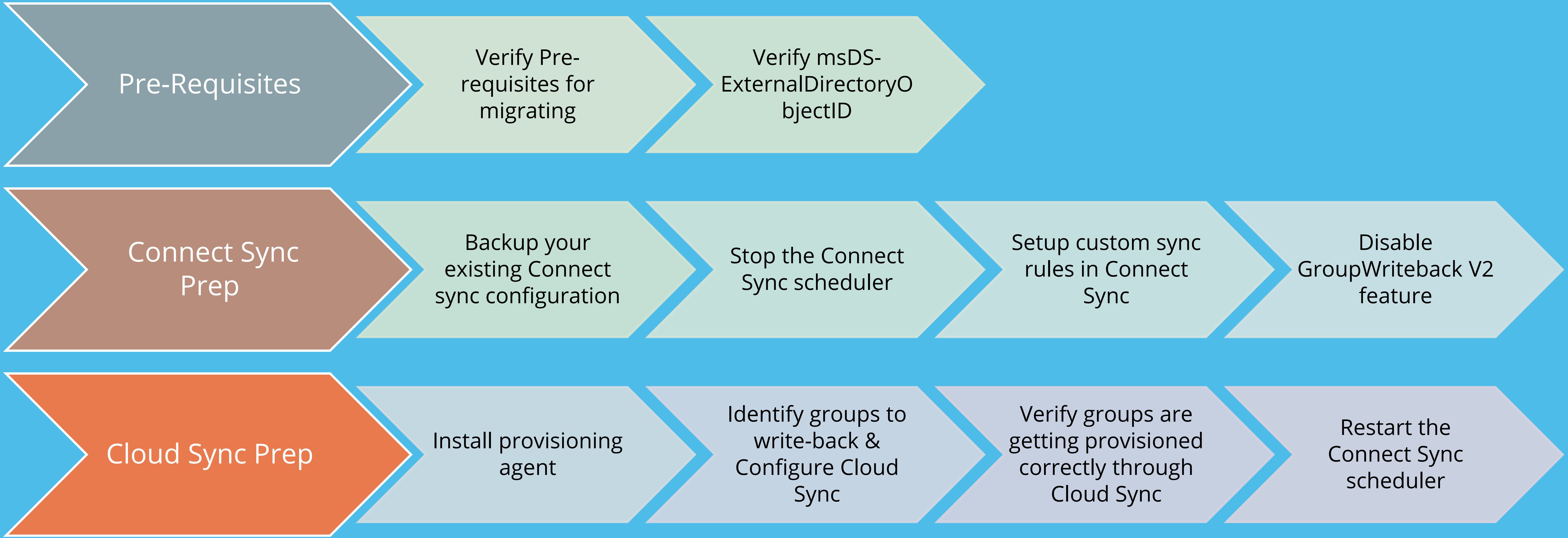
Cloud Sync Prep

- Install provisioning agent
- Configure Cloud Sync
- Verify objects are getting provisioned correctly through Cloud Sync
- Restart the Connect Sync scheduler

DEMO #2 Migrate to Entra Connect Cloud Sync


Recycle Bin
Exported-Sy...
Azure AD Connect
Create_Azu...
RotateKey_...
Untitled1
Type here to search
9:42 PM
5/22/2024

Steps to migrate group write-back to cloud sync



Pre-Requisites

- Verify Pre-requisites for migrating
- Verify msDS-ExternalDirectoryObjectID

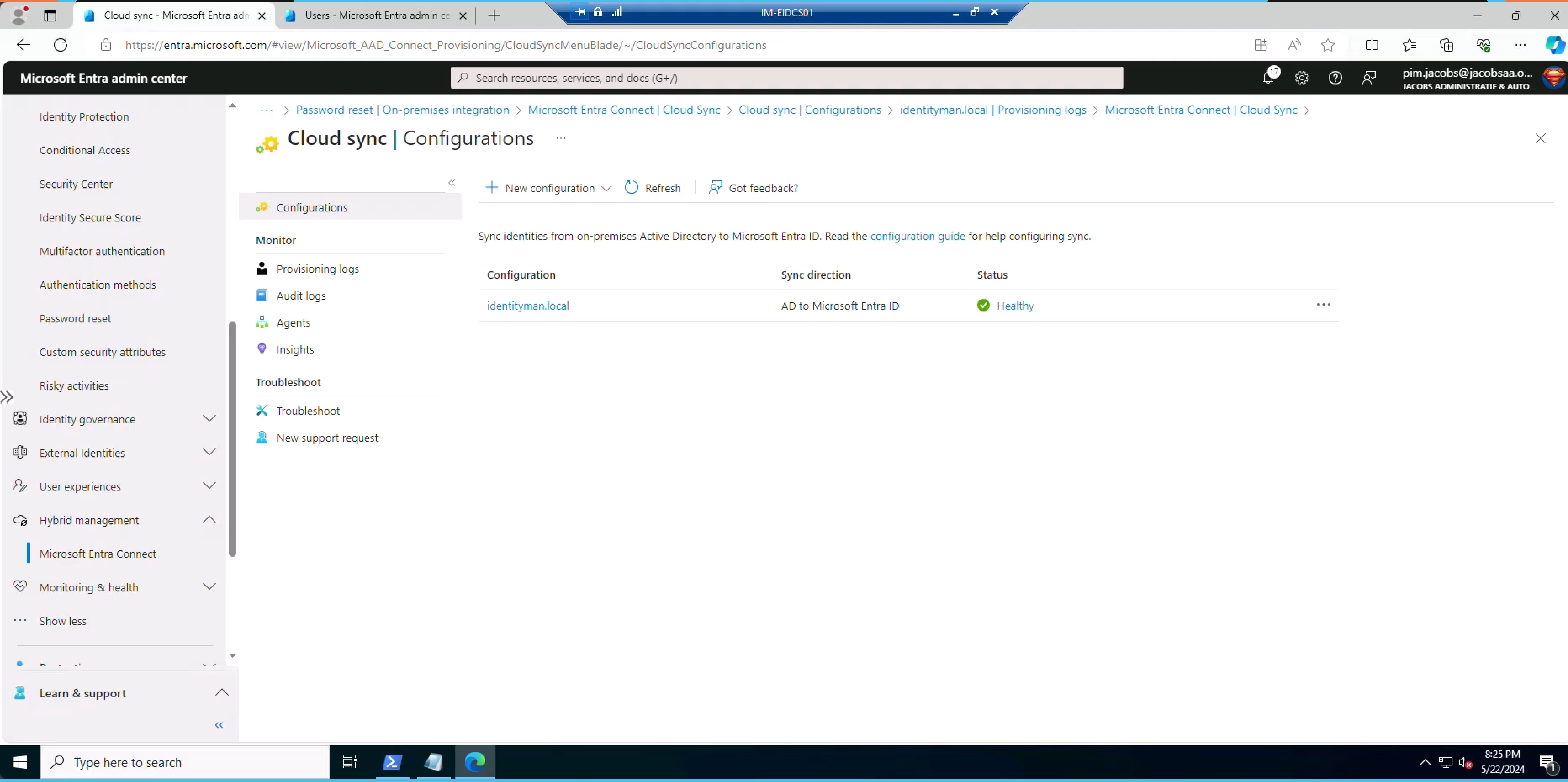
Connect Sync Prep

- Backup your existing Connect sync configuration
- Stop the Connect Sync scheduler
- Setup custom sync rules in Connect Sync
- Disable GroupWriteback V2 feature

Cloud Sync Prep

- Install provisioning agent
- Identify groups to write-back & Configure Cloud Sync
- Verify groups are getting provisioned correctly through Cloud Sync
- Restart the Connect Sync scheduler

DEMO #3 Configure Entra Connect Cloud Sync to Active Directory


Cloud sync - Microsoft Entra adm
Users - Microsoft Entra admin ce
IM-EIDCS01
https://entra.microsoft.com/#view/Microsoft_AAD_Connect_Provisioning/CloudSyncMenuBlade/~/CloudSyncConfigurations
Microsoft Entra admin center
Search resources, services, and docs (G+/)
pim.jacobs@jacobsaa.o...
JACOBS ADMINISTRATIE & AUTO...
Identity Protection
Conditional Access
Security Center
Identity Secure Score
Multifactor authentication
Authentication methods
Password reset
Custom security attributes
Risky activities
Identity governance
External Identities
User experiences
Hybrid management
Microsoft Entra Connect
Monitoring & health
Show less
Learn & support
... > Password reset | On-premises integration > Microsoft Entra Connect | Cloud Sync > Cloud sync | Configurations > identityman.local | Provisioning logs > Microsoft Entra Connect | Cloud Sync >
Cloud sync | Configurations
Configurations
Monitor
Provisioning logs
Audit logs
Agents
Insights
Troubleshoot
Troubleshoot
New support request
New configuration
Refresh
Got feedback?
Type here to search
8:25 PM
5/22/2024

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

Configuration	Sync direction	Status
identityman.local	AD to Microsoft Entra ID	✓ Healthy

Next Steps & Key takeaways

Next Steps

- Install cloud sync
- Use a custom gMSA account with the right permissions!
- Configure or Migrate group writeback first
- Migrate to Connect Sync to Cloud Sync in a phased approach
- Decommission Connect Sync, it’s the legacy of tomorrow!
- Keep an eye out for new features, more is coming!

Key takeaways

- Cloud Sync = The future
- Move object sync over if you can move over!
- Device sync is not available yet!
  For Hybrid Entra Join
- ConsistencyGuid writeback, only used when set otherwise ObjectGuid is being used!
- Cloud sync is / can be used for inbound provisioning as well
- No large group support 250k members
- No support for merging user attributes from multiple domains

Q & A

DANK AAN ONZE SPONSORS

infinity

PATCH MY PC

LIQUIT

Part of RECAST SOFTWARE

veneco

Moving you *forward*