Microsoft® Entra Connect Cloud Sync is here!

It's time to switch.

All you need to know to boost your migration.

Consultant Modern Identity @ InSpark

Guido Baijense

blog.pentiago365.nl
linkedin.com/in/GuidoBaijense

Agenda

- Identity Synchronization?
- Experiences with Connect Sync
- When to use which tool
- Additional features over Connect Sync
- How does it work?
- Install & Use Cloud Sync
- Migrate to Cloud Sync
- Do’s and don’ts

Identity Synchronization

Microsoft Identity Manager*

- Only advised for very specific use cases
- Requires at least Entra ID P1
- Cool if you want to have Entra ID as the source of authority.

Microsoft Entra Connect Sync

- The tool that everyone uses
- The tool that everyone hates
- Complex

*with the Graph Connector > Valid until January 9, 2029

Identity Synchronization

Microsoft Entra Connect Sync

- The tool that everyone uses
- The tool that everyone hates
- Complex

Microsoft Entra Cloud Sync

- (Not so) new kid on the block
- Microsofts focus
- New features, yeay

Share your (negative) experiences with Connect Sync

Please. Hands in the air.

When to use Cloud Sync or Connect Sync?

Scenario	Supported with Cloud Sync	Supported with Connect Sync
Mergers and acquisitions (disconnected forest)	●	N/A
High availability - latency (I need high availability)	●	N/A
User accounts in one forest / mailboxes in resource forest	N/A	●
Sync large domains with more than 250K objects	N/A	●
Filter directory objects based on attribute values	N/A	●
Microsoft Entra hybrid join	N/A	●
Windows Hello for Business	● (cloud trust)	●

Why move to cloud sync?

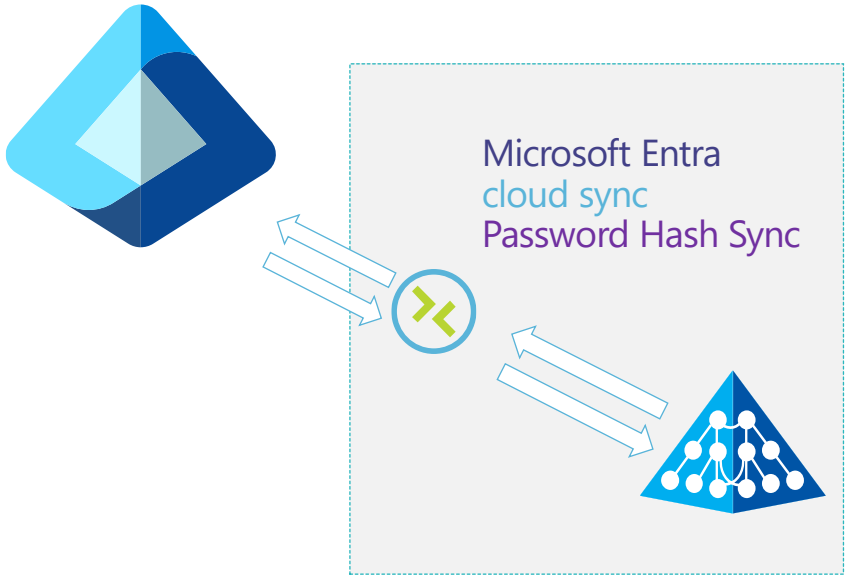
	Microsoft Entra Connect Sync	Microsoft Entra Cloud Sync
Infrastructure	Heavy on-prem footprint	Lightweight agent
Deployment	Requires SQL and larger servers to setup and manage sync configuration	Quick and easy w/ configuration managed from Microsoft Entra ID
AD Consolidation (Disconnected forests)	Requires AD consolidation or requires network connectivity b/w forests	Supports disconnected forests (Mergers and acquisitions)
Resiliency	No high availability	High availability is supported
Cost	Expensive to maintain and support the on-premises infrastructure	Less expensive and low maintenance with minimal on-premises investments.
Performance	Uses sequential syncing when connecting multiple sources thereby increasing sync cycle	Runs parallel sync cycles across multiple sources thereby by reducing sync cycle

*Thanks to **Microsoft** for providing this slide

And those new features

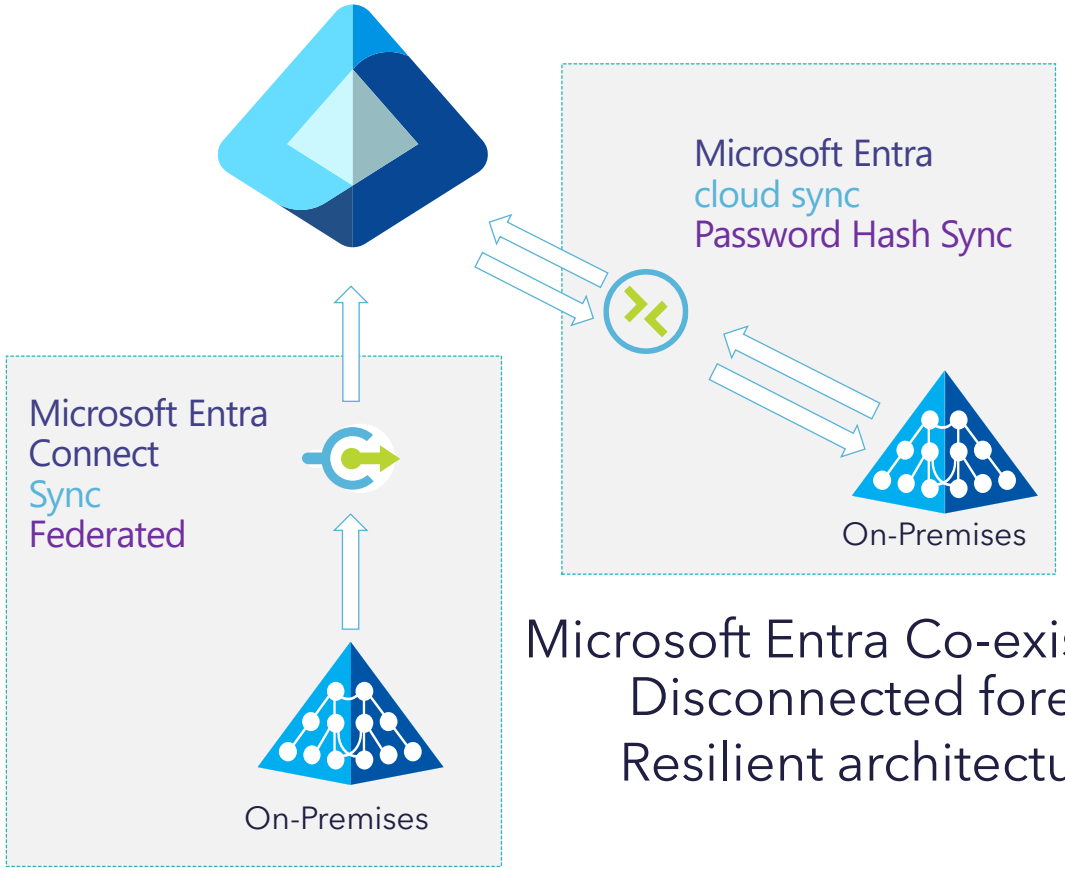
Features?

- Cost Effective
- Quick to deploy
- Simple configuration
- Bi-directional sync for Groups and ***<redacted due to SFI>***



Features?

- Co-Existence
- Disconnected forest
- Resilient architecture



Microsoft Entra Co-existence
Disconnected forest
Resilient architecture

Current capabilities

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 – In a few 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

Current capabilities

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

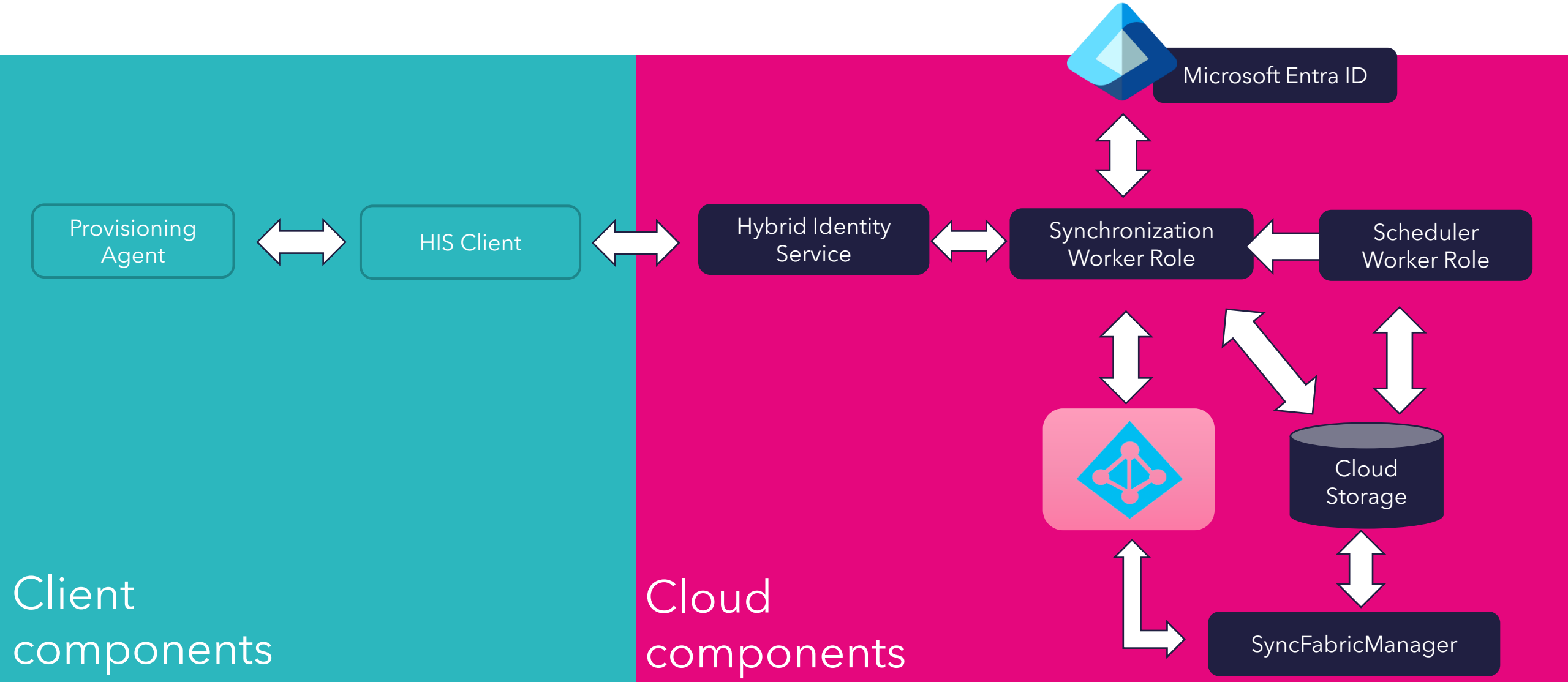
Supportability

- 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

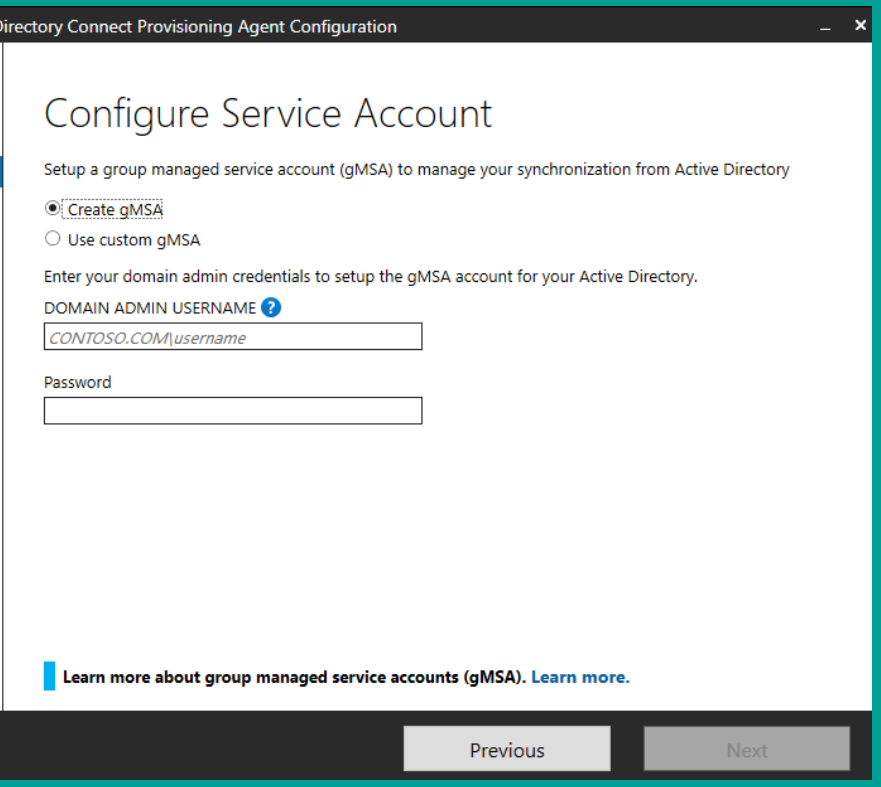
How does it work?

Entra Connect Cloud Sync Architecture

Architecture & Components



GMSA and the differences



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

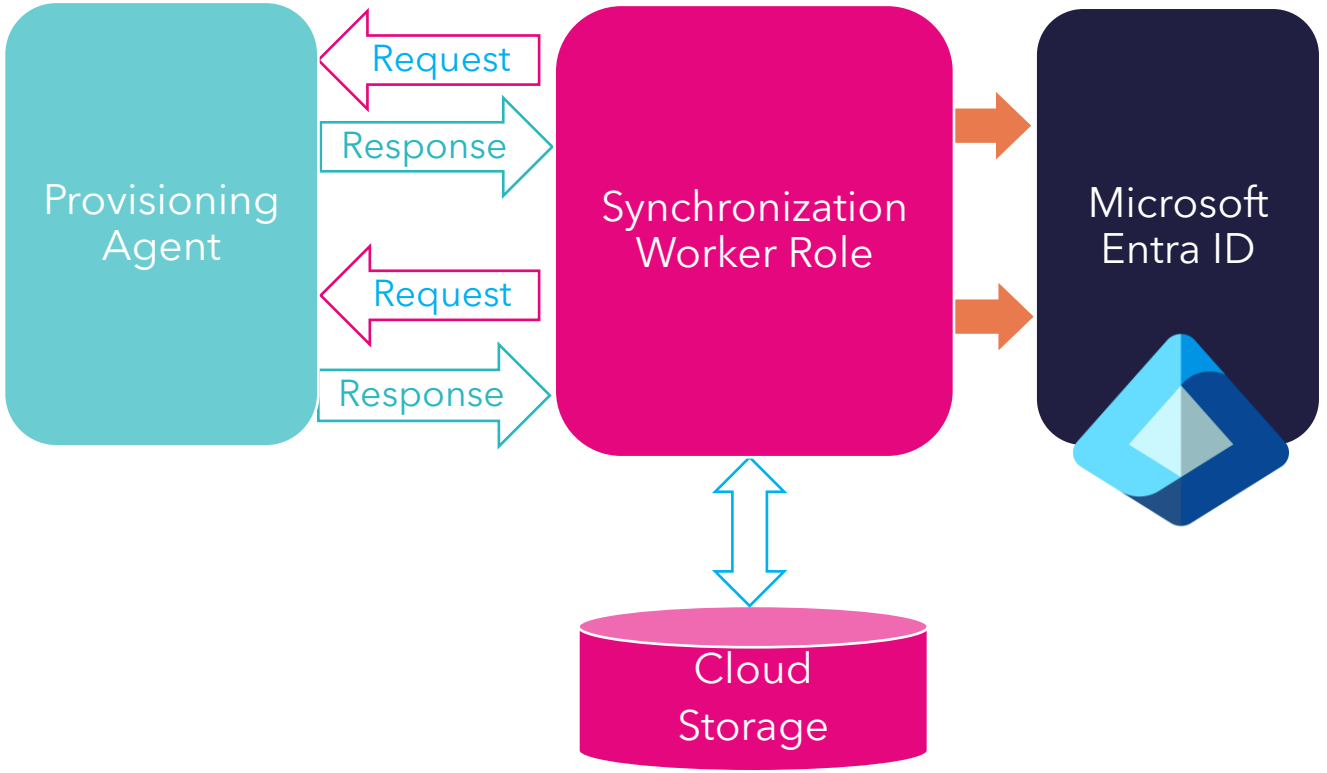
Microsoft Entra provisioning Agent gMSA PowerShell cmdlets - Microsoft Entra ID | Microsoft Learn

Demo

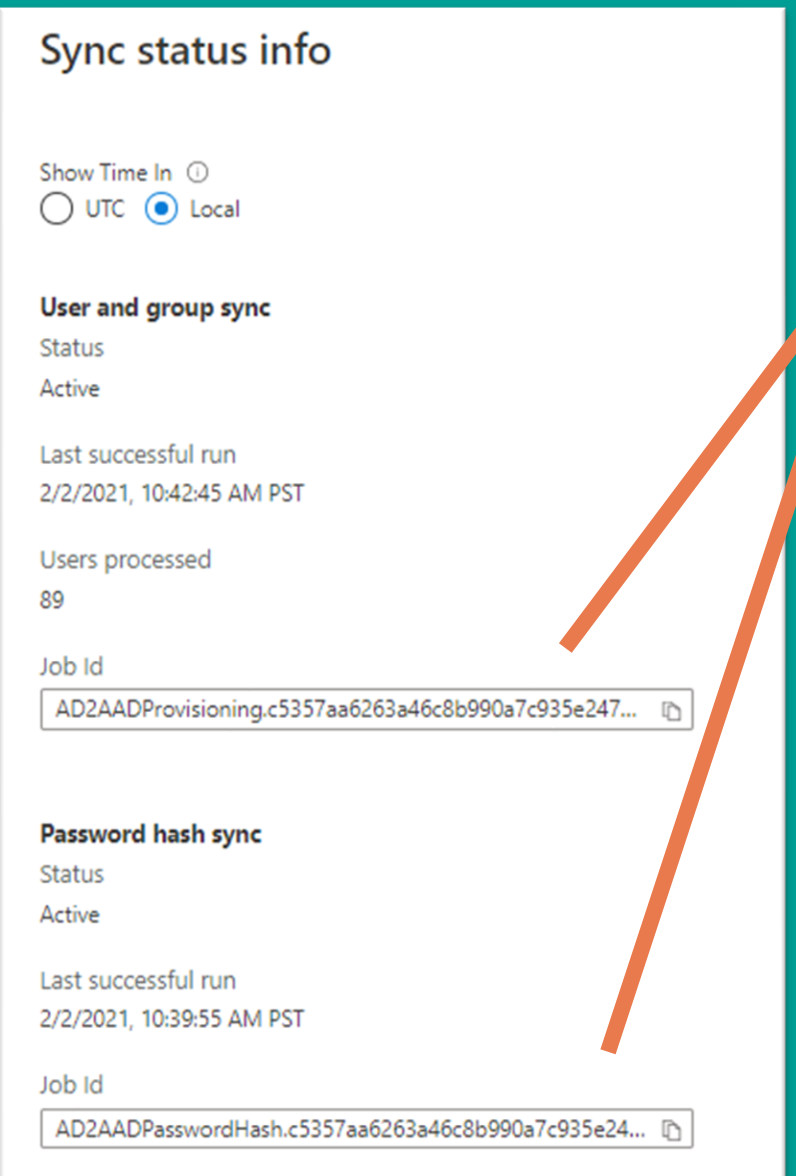
Basic installation and configuration of Entra Cloud Sync – Part 1

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%)



Configuration per domain in portal



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

pentiago.local | Properties

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Single sign-on
Provisioning
Self-service
Custom security attributes

Security

Save | Discard | Delete | Got feedback?

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. Learn more.

If this application resides in your tenant, you can manage additional properties on the application registration.

Enabled for users to sign-in? Yes No

Name * pentiago.local

Homepage URL https://account.activedirectory.windowsazure.com:444/applications/de...

Logo

Select a file

User access URL https://launcher.myapps.microsoft.com/api/signin/

pentiago.local | Overview

Overview
Provision on demand

Manage
Scoping filters
Attribute mapping
Expression builder

Monitor
Provisioning logs
Audit logs
Agents
Insights

Troubleshoot
Troubleshoot
New support request

Review and enable | Restart sync | Delete configuration

Get started | Overview | Properties | Tutorials

Get started provisioning your agent with Cloud Sync

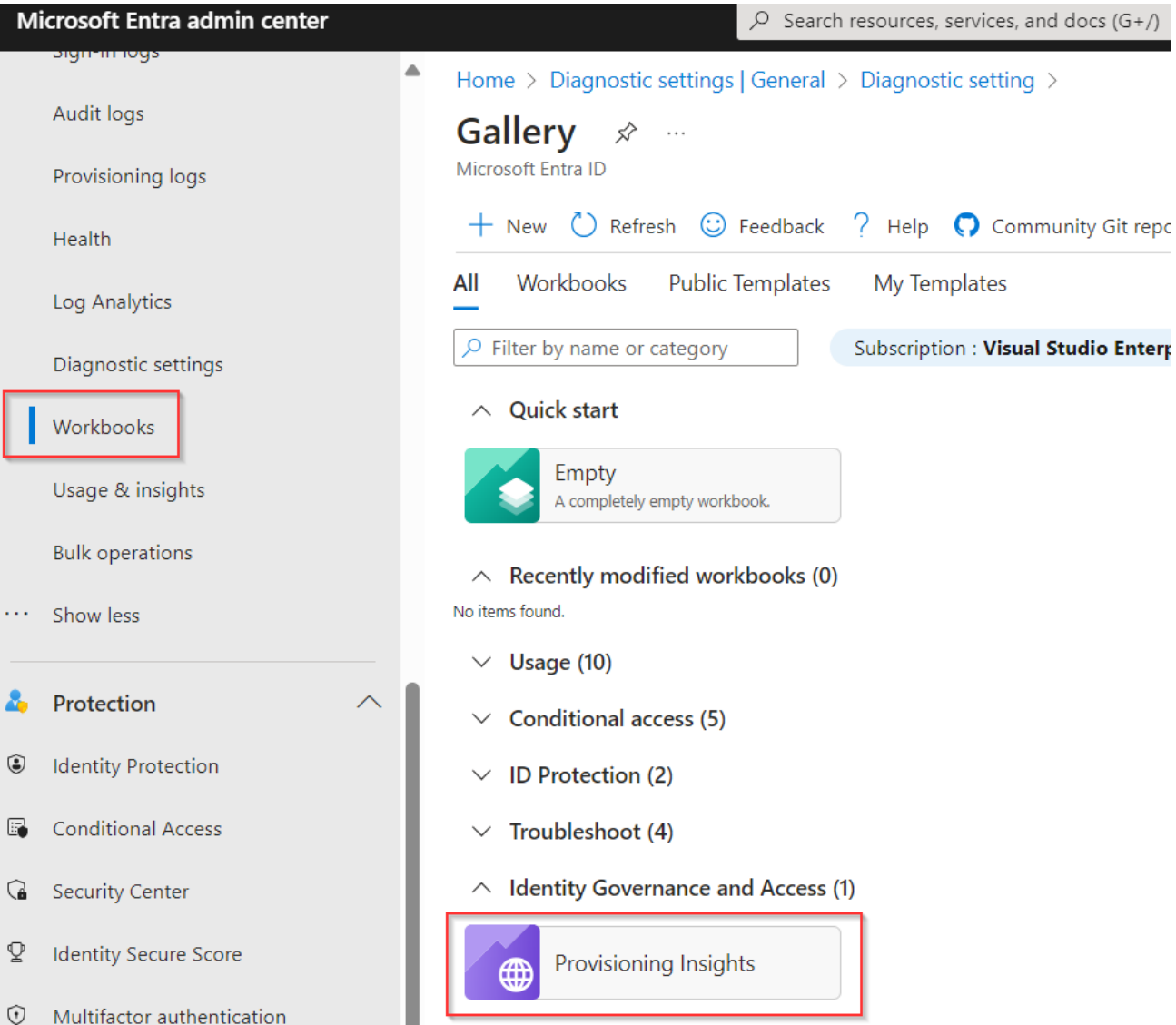
Configure, test and deploy your sync setup using the steps below.

Add scoping filters

Add scoping filters (optional)

By using filtering, you can control which objects appear in Microsoft Entra ID from your on-premises directory. The default configuration takes all objects

Provisioning Logs



- Central place for all provisioning logs with advanced search & filtering capabilities
- Used for troubleshooting
- MS Graph API supported
- Integrated with Log Analytics
- Built-in workbooks and Insights in Entra Portal

Demo

Basic configuration of Entra Cloud Sync - part 2

Explore synchronization jobs with PowerShell and more

e	Value
-	-----
nect-AADCloudProvisioningTools	Connects AADCloudPro
ort-AADCloudProvisioningToolsLogs	Exports all the diag
-AADCloudProvisioningToolsConnection	Show AADCloudProvisi
-AADCloudProvisioningToolsServicePrincipal	Returns the Service
-AADCloudProvisioningToolsSyncJob	Returns Azure AD Clo
-AADCloudProvisioningToolsSyncJobSchedule	Returns Azure AD Clo
-AADCloudProvisioningToolsSyncJobSchema	Returns Azure AD Clo
-AADCloudProvisioningToolsSyncJobScope	Returns Azure AD Clo
-AADCloudProvisioningToolsSyncJobSettings	Returns Azure AD Clo
-AADCloudProvisioningToolsSyncJobStatus	Returns Azure AD Clo
oke-AADCloudProvisioningToolsGraphQuery	Makes a query to Mic
air-AADCloudProvisioningToolsSyncAccount	Repairs Cloud Provis
uest-AADCloudProvisioningToolsRefreshToken	Requests a refresh t
rt-AADCloudProvisioningToolsVerboseLogs	Enable AADCloudProvi
p-AADCloudProvisioningToolsVerboseLogs	Disable AADCloudProv

Initially introduced to repair sync service account

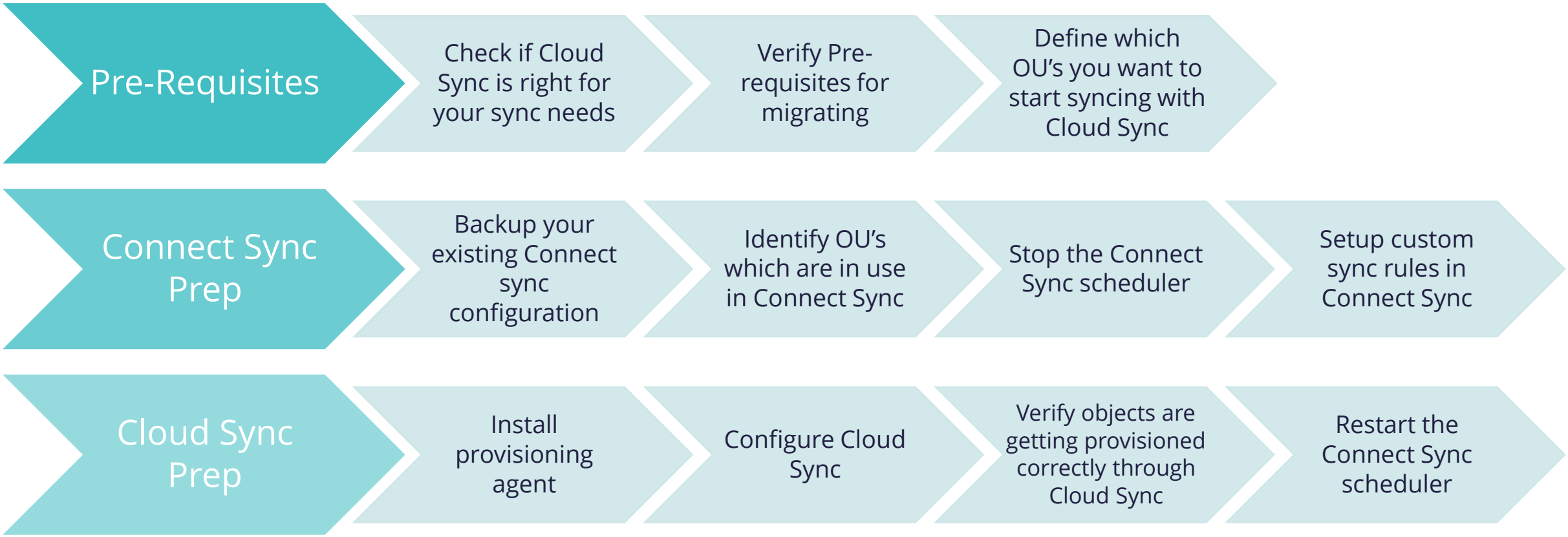
Expanded to facilitate verbose tracing & reduce dependency on Graph Explorer

Can be used on any machine, except for collecting verbose logs

Use Get-Help <cmdlet>

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

Steps to migrate in phased approach to Cloud Sync

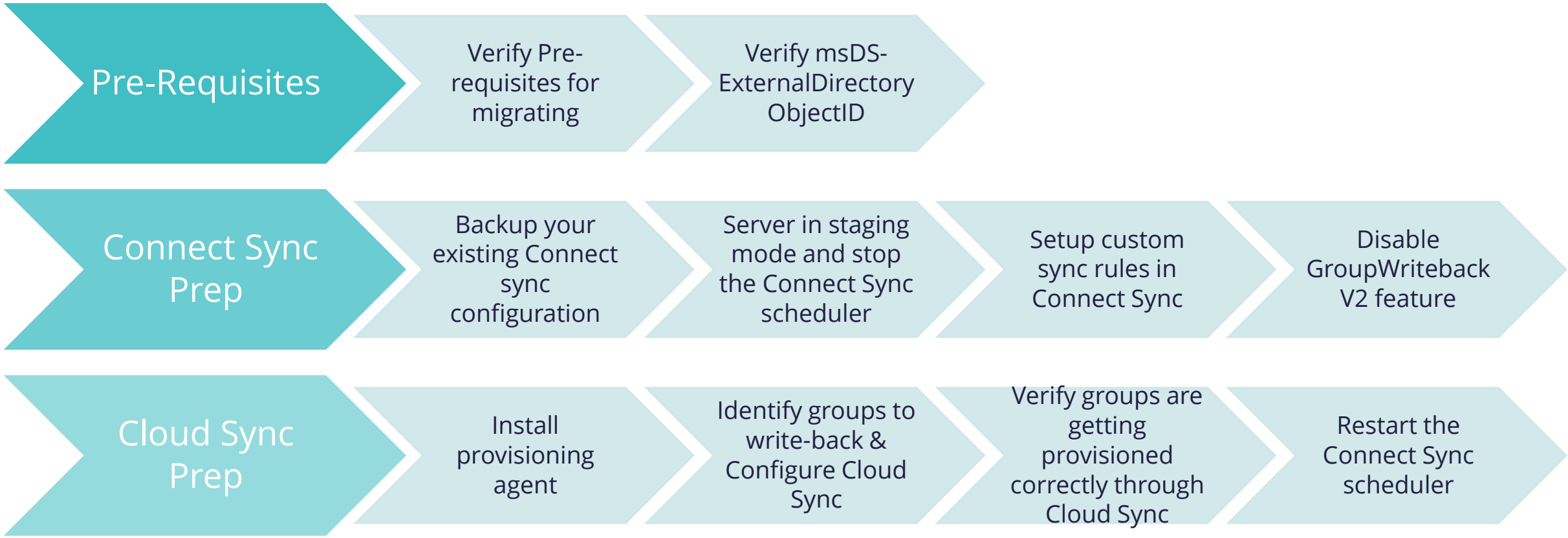


Demo

Migration Scenario’s

The other way around

How to migrate group write-back



Demo

The other way around

Next steps

Install cloud sync…

Next steps

1. Install cloud sync.
2. Use a gMSA with the right permissions.
3. Migrate from Connect Sync to Cloud sync gradually.
4. Decommission Connect Sync – It's old. Like AD FS.
5. Wait patiently for new features

Dont's

- Extending your AD schema and directly enable remote-mailboxes without restarting the sync agents
- Change the sync scope when sync is turned on.

Take aways

Q&A