NIC 2017

nordic infrastructure conference

The premium event for IT-professionals

Feb. 1-3rd in Oslo Spektrum

Andy Malone MVP

Founder: Cybercrime Security Forum

Azure AD Connect Internals:

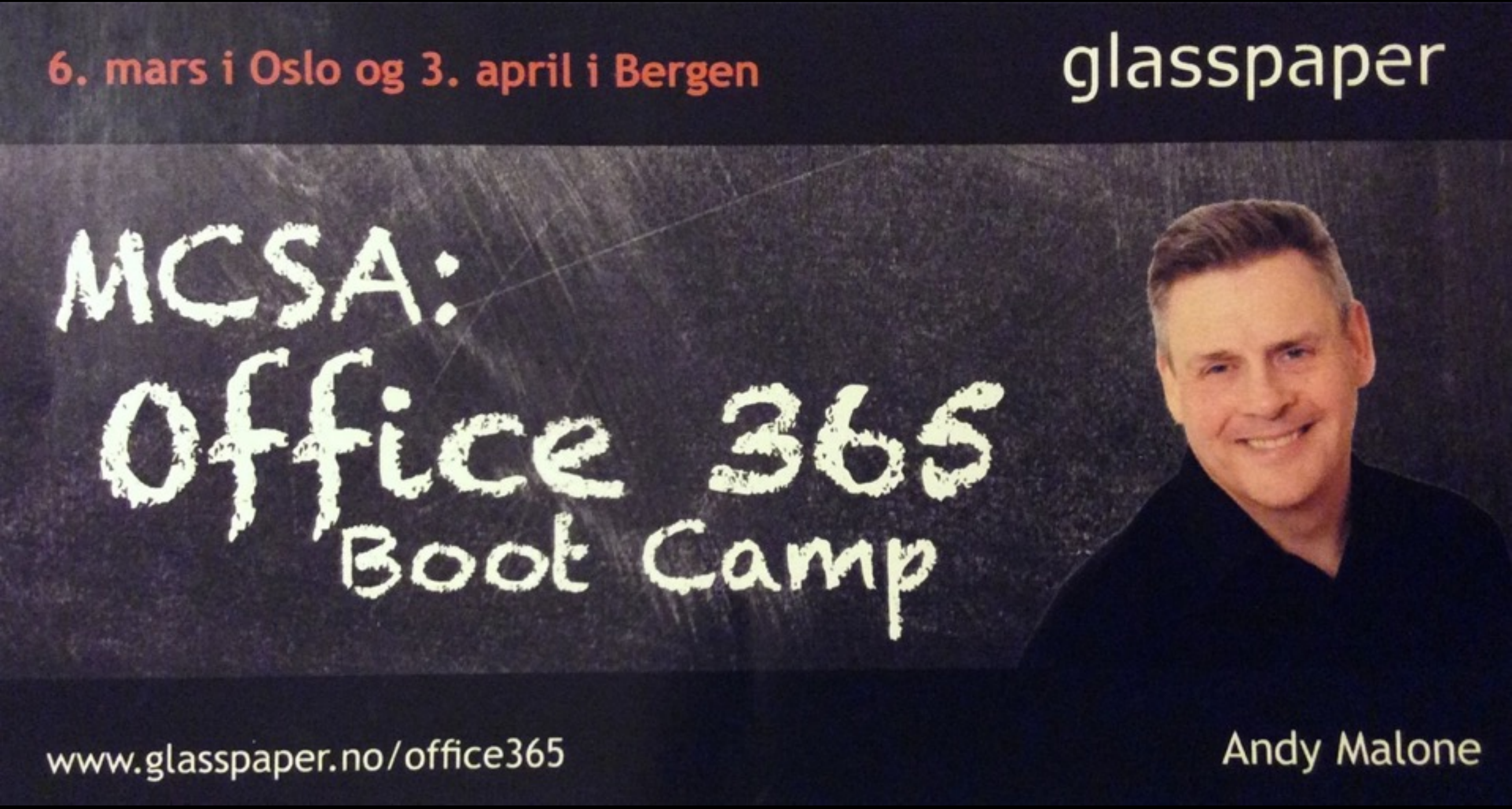
What was I Syncing About?

Follow me on Twitter @AndyMalone

Andy Malone

(United Kingdom)

Microsoft MVP (Enterprise Security)
Microsoft Certified Trainer (20 years)
Founder: Cybercrime Security Forum
Worldwide Event Speaker
Author: The Seventh Day
www.AndyMalone.org



6. mars i Oslo og 3. april i Bergen

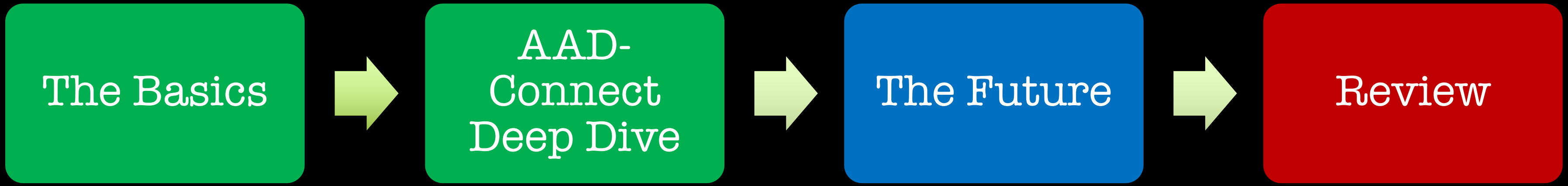
glasspaper

MCSA: Office 365 Boot Camp

www.glasspaper.no/office365

Andy Malone

Session Focus



The Basics

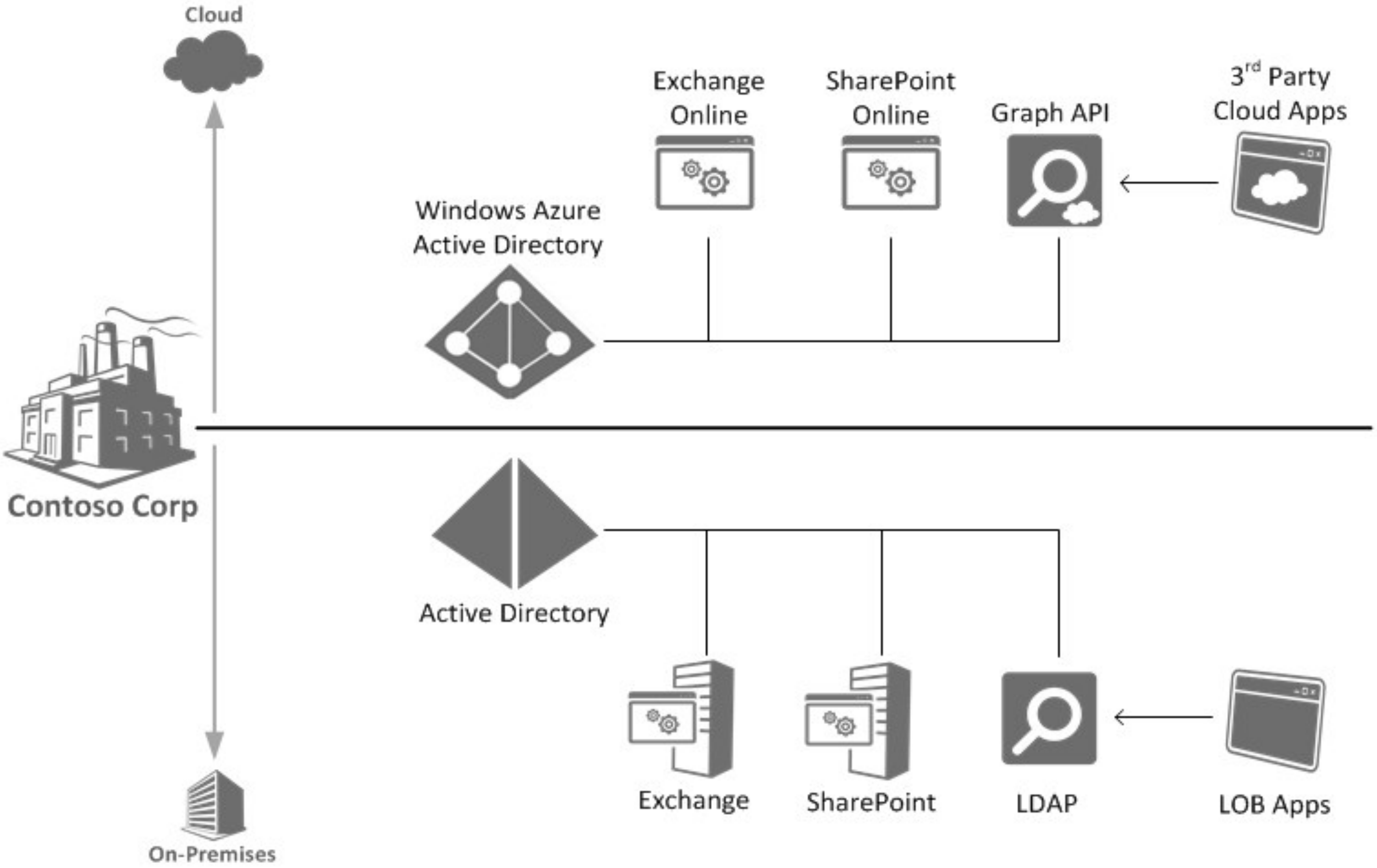
AAD-Connect Deep Dive

The Future

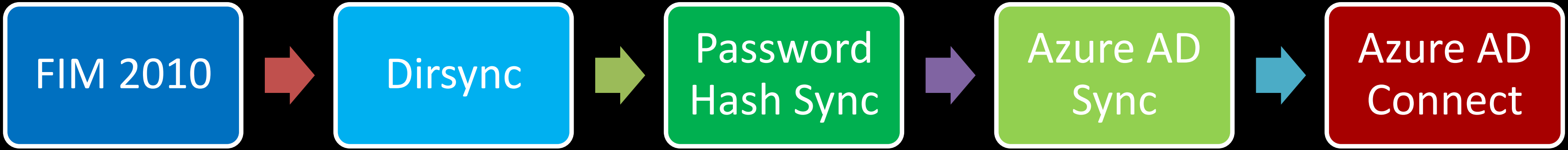
Review

MS Account Vs Azure AD Account

Microsoft account	Azure AD account
The consumer identity system run by Microsoft	The business identity system run by Microsoft
Authentication to services that are consumer-oriented, such as Hotmail and MSN	Authentication to services that are business-oriented, such as Office 365
Consumers create their own Microsoft accounts, such when they sign up for email	Companies and organizations create and manage their own work or school accounts
Identities are created and stored in the Microsoft account system	Identities are created by using Azure or another service such as Office 365, and they are stored in an Azure AD instance assigned to the organization


Cloud
Exchange Online
SharePoint Online
Graph API
3rd Party Cloud Apps
Windows Azure Active Directory
Contoso Corp
Active Directory
Exchange
SharePoint
LDAP
LOB Apps
On-Premises

Synchronization Development



FIM 2010

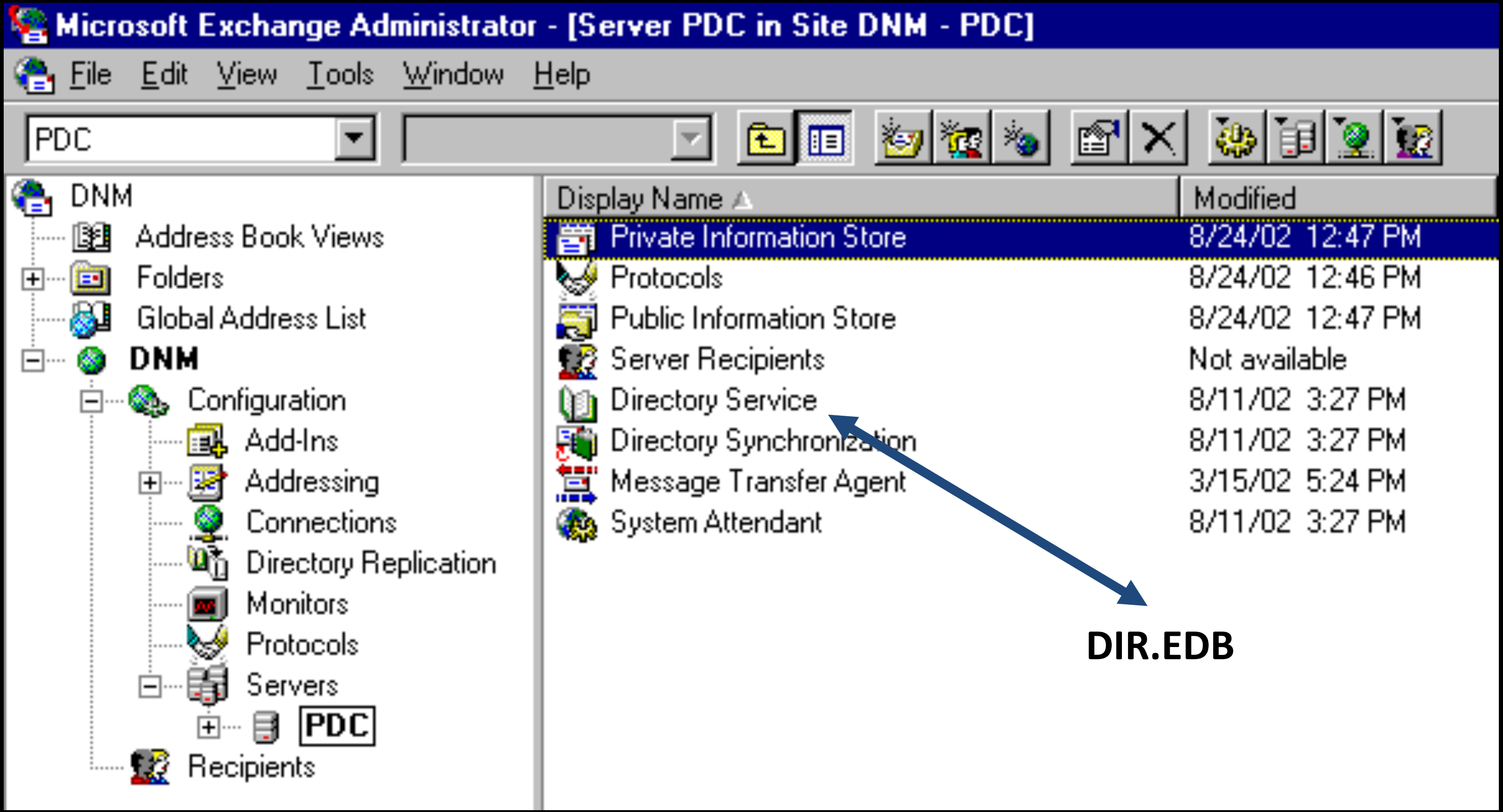
Dirsync

Password Hash Sync

Azure AD Sync

Azure AD Connect

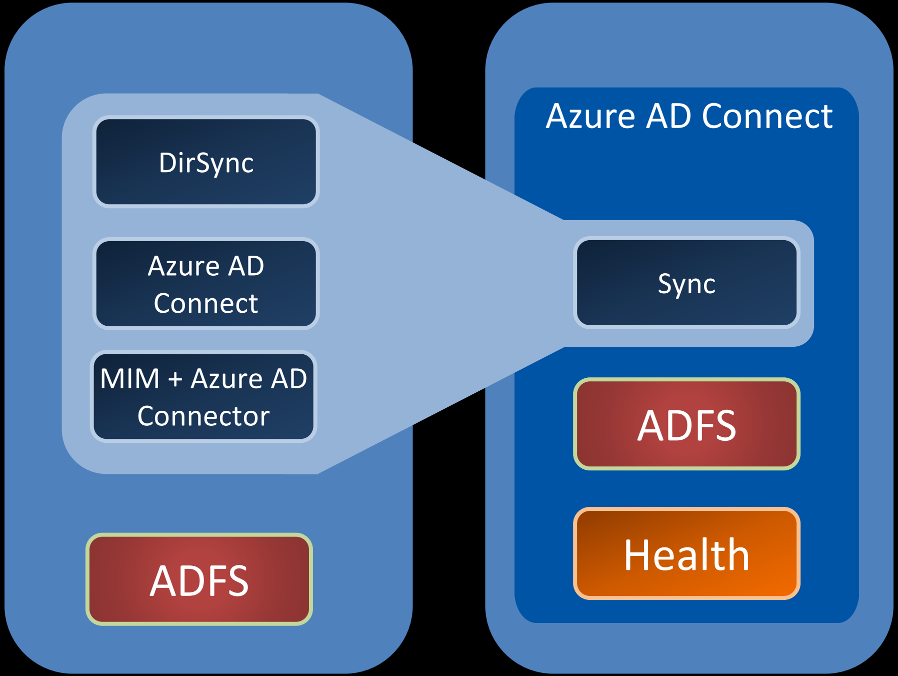
Hey … This all Seems so Familiar!



Display Name	Modified
Private Information Store	8/24/02 12:47 PM
Protocols	8/24/02 12:46 PM
Public Information Store	8/24/02 12:47 PM
Server Recipients	Not available
Directory Service	8/11/02 3:27 PM
Directory Synchronization	8/11/02 3:27 PM
Message Transfer Agent	3/15/02 5:24 PM
System Attendant	8/11/02 3:27 PM

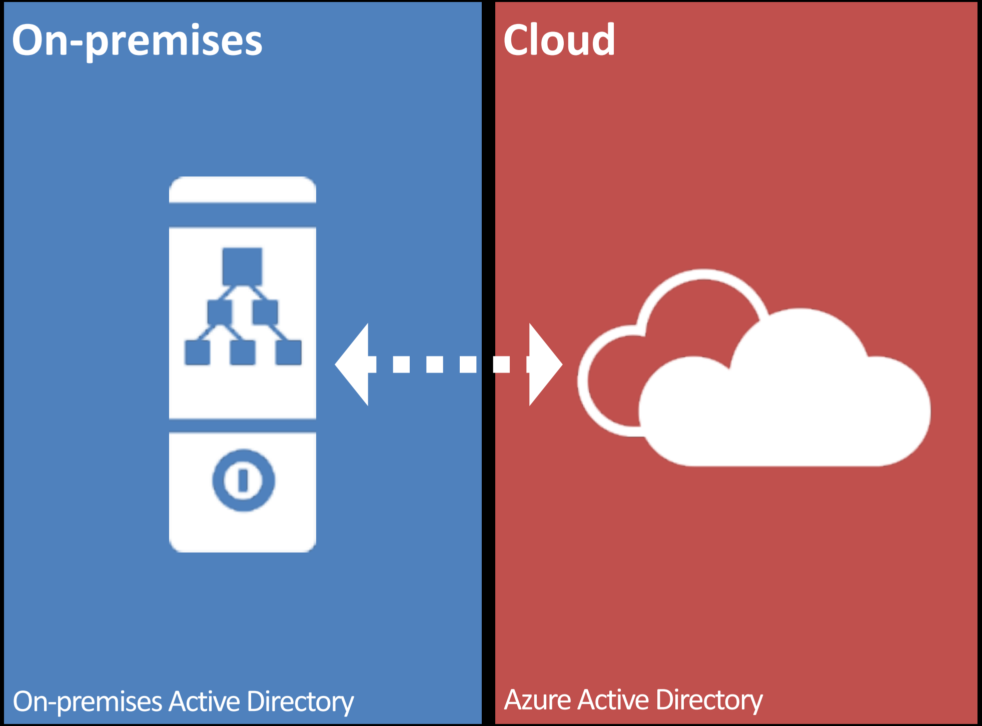
DIR.EDB

What is Azure AD Connect?



- Primary tool to onboard to Azure AD
- Express Settings gets customers connected in a matter of minutes
- Provides install & configuration of password sync/ADFS for sign-in
- All future investments will only be available with Azure AD Connect

AAD-Connect – Why?



On-premises

Cloud

On-premises Active Directory

Azure Active Directory

Why?

Provisions Users, Groups, Mail Enabled Contacts into Azure AD

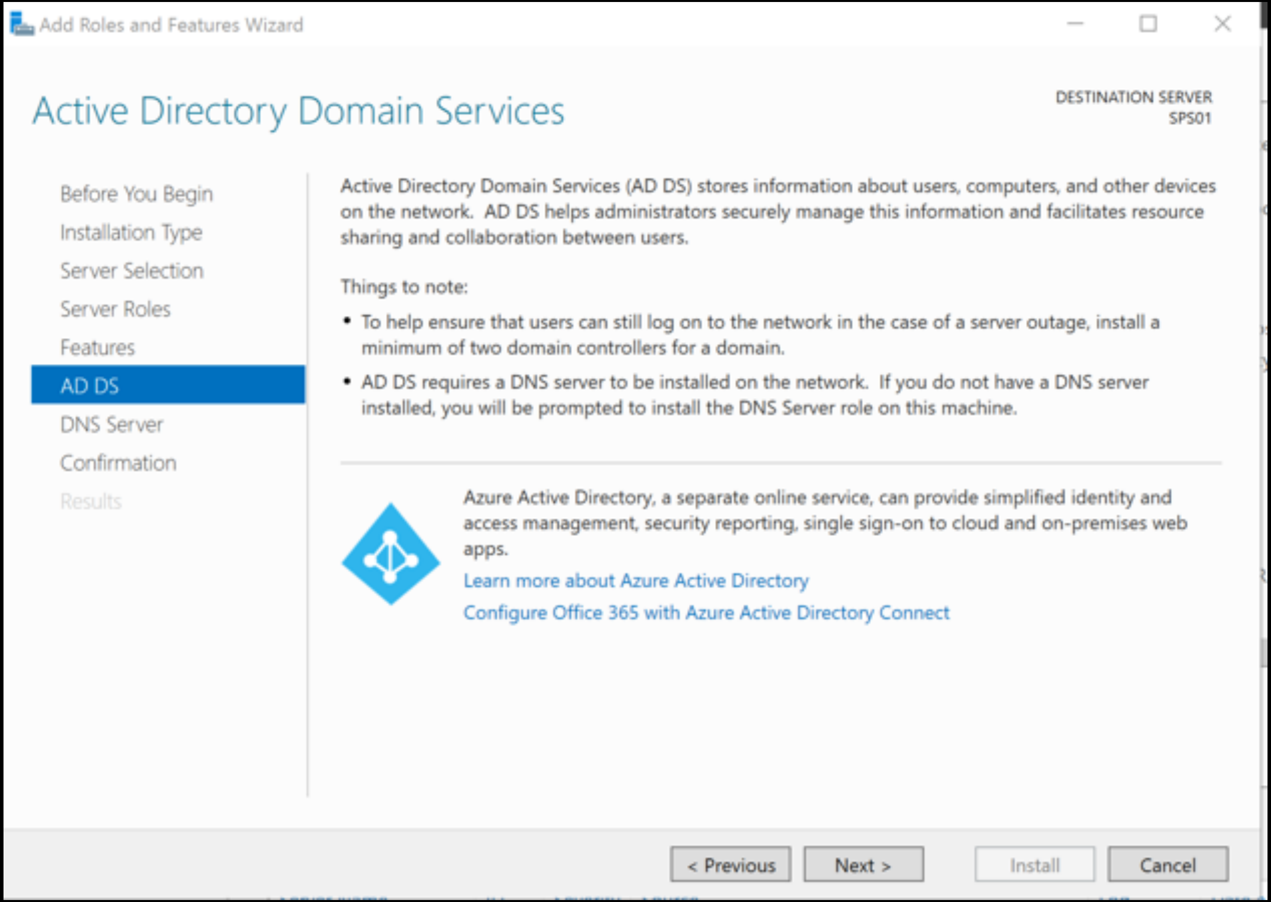
Eliminates the need to manage users and groups in two places

Simplifies user provisioning

Provides Exchange Global Address List (GAL Function)

Enables scenarios such as a hybrid deployment

Windows Server 2016 Azure-AD Integration!



Active Directory Domain Services

DESTINATION SERVER
SPS01

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

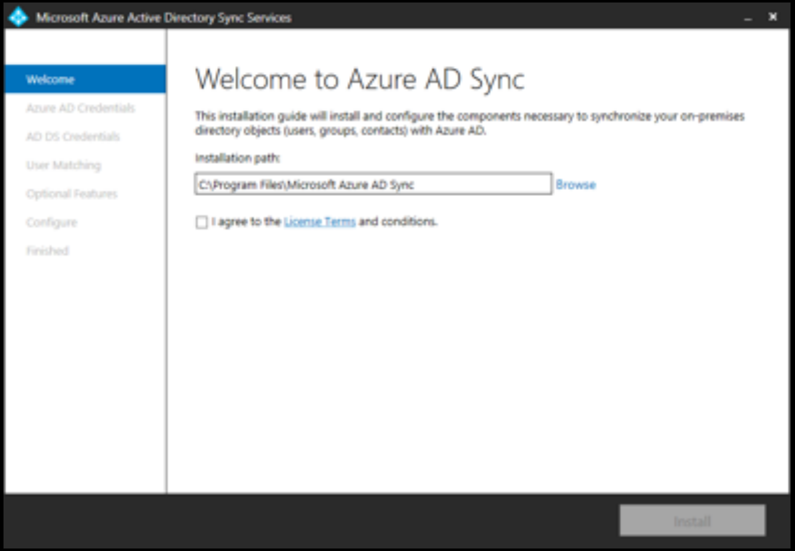
Learn more about Azure Active Directory

Configure Office 365 with Azure Active Directory Connect

How it Works ...

How Sync Works

- Sync's Users – Groups – Mail Enabled Contacts in Azure AD / Office 365
- Copies a Subset of Object App & Device Attributes to Cloud (This is configurable)
- Ignores System & Admin Accounts
- Defaults to Azure AD Basic, Unless Azure Premium AD enabled.



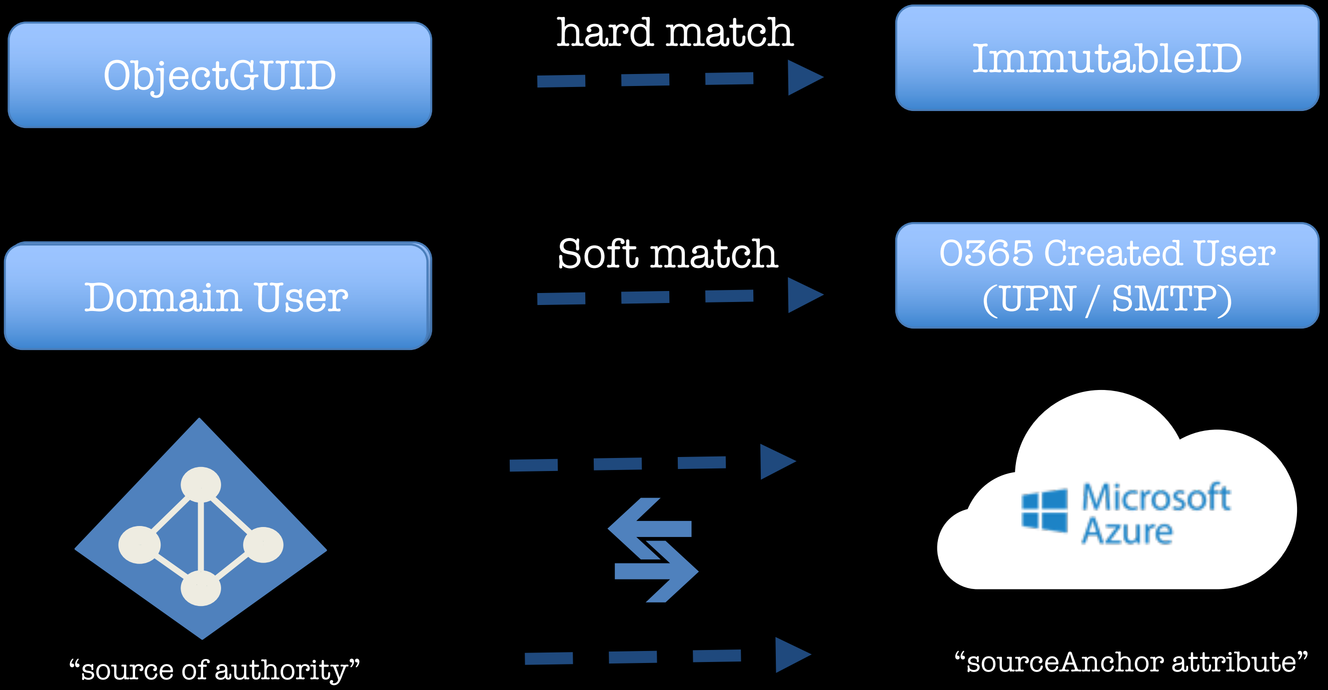
Welcome to Azure AD Sync

This installation guide will install and configure the components necessary to synchronize your on-premises directory objects (users, groups, contacts) with Azure AD.

Installation path: C:\Program Files\Microsoft Azure AD Sync

□ I agree to the License Terms and conditions.

Understanding the Sync Process



ObjectGUID

hard match

ImmutableID

Domain User

Soft match

O365 Created User (UPN / SMTP)

“source of authority”

“sourceAnchor attribute”

Soft-match on UPN

Move from cloud-only identity model to synchronized model used to be a challenge:

- Either set ImmuatbleID on all cloud objects or if you have Exchange Online, soft-match on proxyAddresses

You can now enable soft-match on UPN:

```
Set-MsolDirSyncFeature -Feature EnableSoftMatchOnUpn -Enable $true
```

Allow sync to update UPN

UPNs used to be updateable with PowerShell only

Sync can now update UPN. Enable with:

```
Set-MsolDirSyncFeature -Feature SynchronizeUpnForManagedUsers -Enable $true
```

Does not work if you use federation

Reduced sync errors

UPN and Proxy address conflicts

Need to be unique between two objects in Azure AD

Conflicting objects are not sync'd at all

Attempted on every sync cycle and error reported every time

Forms the majority of the sync errors customers hit

Duplicate Attribute Resiliency

behavior in Azure AD: Sync the conflicting object, but *quarantine* the offending attribute

- UPN Conflict: offending UPN is 'made unique' by adding a 4 digit number to the prefix.
- Proxy Conflict: offending attribute is *quarantined*.

Default behavior for new tenants. Rolled out to existing tenants.

Enabled through following PowerShell cmdlets.

```
Set-MsolDirSyncFeature -Feature DuplicateUPNResiliency -Enable $true
Set-MsolDirSyncFeature -Feature DuplicateProxyAddressResiliency -Enable $true
```

Errors reported once at time of conflict. Available in O365 portal. Viewable through PowerShell.

Azure AD-Connect Prerequisites

Active Directory remediation

- Run IdFix

Verify DNS domains with Office 365

- Add these prior to syncing to preserve UPN

Directories other than Active Directory

- Works with Office 365 – Identity program
- Will be added soon to AAD Sync

One server is most common

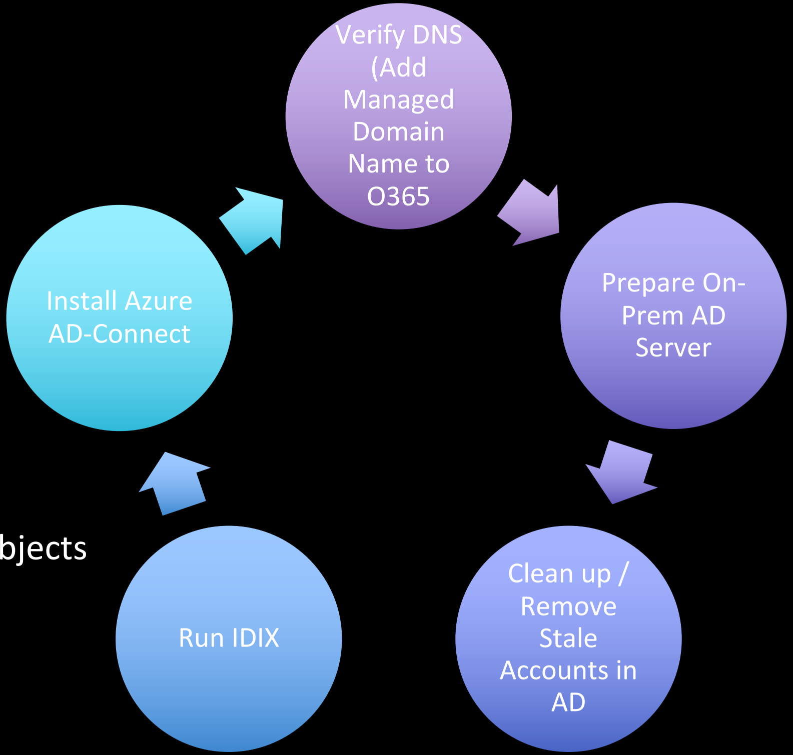
- Domain controller is Okay
- Separate SQL Server is Okay up to 100,000 directory objects
- You can install to Azure IAAS

Migrating from DirSync or MIM / FIM

- Uninstall / Reinstall
- Side by side install with object review

Forest functional level

- Windows Server 2008


Verify DNS (Add Managed Domain Name to O365
Prepare On-Prem AD Server
Clean up / Remove Stale Accounts in AD
Run IDIX
Install Azure AD-Connect

Amending your UPN Suffix

```
Import-Module ActiveDirectory
$oldSuffix = "adatum.local"
$newSuffix = ”MyLiveDomain.com"
$ou = "DC=adatum,DC=com"
$server = "LON-DC1"
Get-ADUser -SearchBase $ou -filter * | ForEach-Object {
$newUpn = $_.UserPrincipalName.Replace($oldSuffix,$newSuffix)
$_ | Set-ADUser -server $server -UserPrincipalName $newUpn
}
```

Script will amend UPN Suffix for all Domain Users from ADATUM.LOCAL to MYLIVEDOMAIN.COM

ID Fix

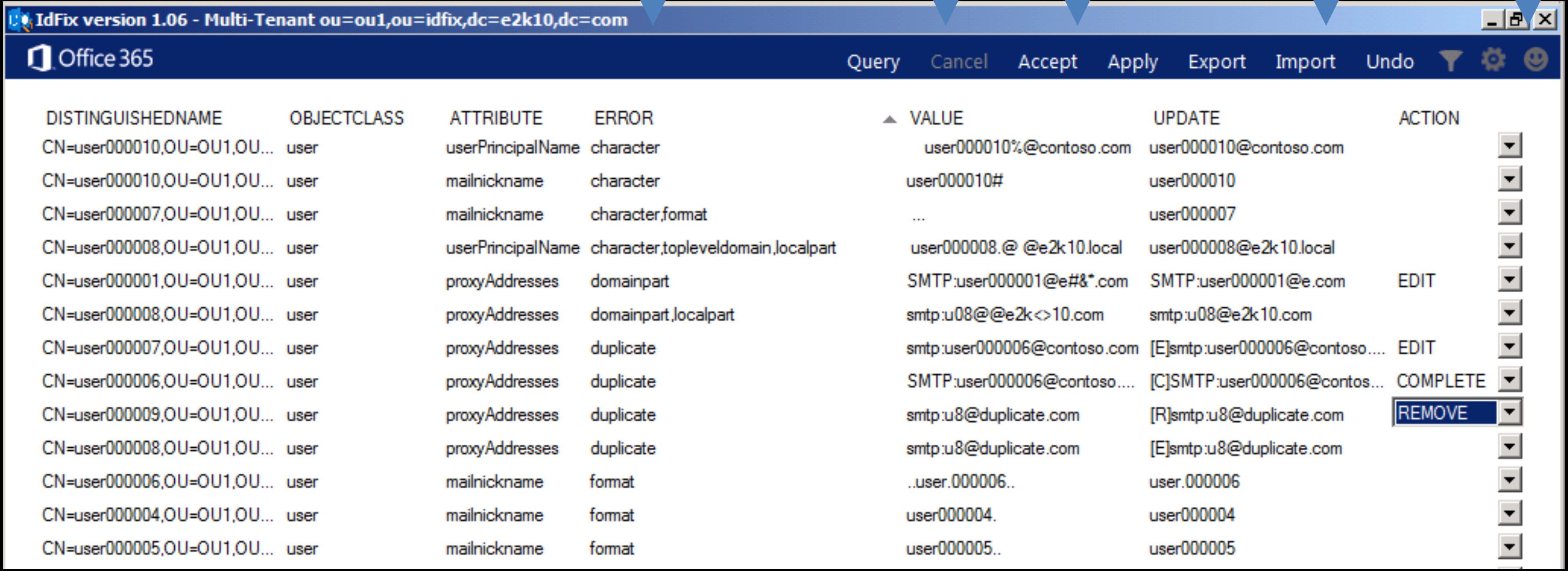
Identifies and remed
that will fail Office 36

Queries all domain
forest via LDAP

Provide
import \

Confirmation of
rollback functioı

Critical system objects are skipped
where editing could cause issues


IdFix version 1.06 - Multi-Tenant ou=ou1,ou=idfix,dc=e2k10,dc=com
Office 365
Query
Cancel
Accept
Apply
Export
Import
Undo

DISTINGUISHEDNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION
CN=user000010,OU=OU1,OU...	user	userPrincipalName	character	user000010%@contoso.com	user000010@contoso.com	
CN=user000010,OU=OU1,OU...	user	mailnickname	character	user000010#	user000010	
CN=user000007,OU=OU1,OU...	user	mailnickname	character,format	...	user000007	
CN=user000008,OU=OU1,OU...	user	userPrincipalName	character,topleveldomain,localpart	user000008.@ @e2k10.local	user000008@e2k10.local	
CN=user000001,OU=OU1,OU...	user	proxyAddresses	domainpart	SMTP:user000001@e#&*.com	SMTP:user000001@e.com	EDIT
CN=user000008,OU=OU1,OU...	user	proxyAddresses	domainpart,localpart	smtp:u08@@e2k<>10.com	smtp:u08@e2k10.com	
CN=user000007,OU=OU1,OU...	user	proxyAddresses	duplicate	smtp:user000006@contoso.com	[E]smtp:user000006@contoso....	EDIT
CN=user000006,OU=OU1,OU...	user	proxyAddresses	duplicate	SMTP:user000006@contoso....	[C]SMTP:user000006@contos...	COMPLETE
CN=user000009,OU=OU1,OU...	user	proxyAddresses	duplicate	smtp:u8@duplicate.com	[R]smtp:u8@duplicate.com	REMOVE
CN=user000008,OU=OU1,OU...	user	proxyAddresses	duplicate	smtp:u8@duplicate.com	[E]smtp:u8@duplicate.com	
CN=user000006,OU=OU1,OU...	user	mailnickname	format	..user.000006..	user.000006	
CN=user000004,OU=OU1,OU...	user	mailnickname	format	user000004.	user000004	
CN=user000005,OU=OU1,OU...	user	mailnickname	format	user000005..	user000005	

Demo

IDFIX

What errors does IdFix look for?

Errors Validated

- Duplicate proxyAddresses
- Invalid characters in attributes
- Over length attributes
- Format errors in attributes
- Use of non-routable domains
- Blank attribute that requires a value

Attributes

- mailNickName
- proxyAddresses
- sAMAccountName
- targetAddress
- userPrincipalName

Demo

Installing Azure AD-Connect

Synchronization Schedules

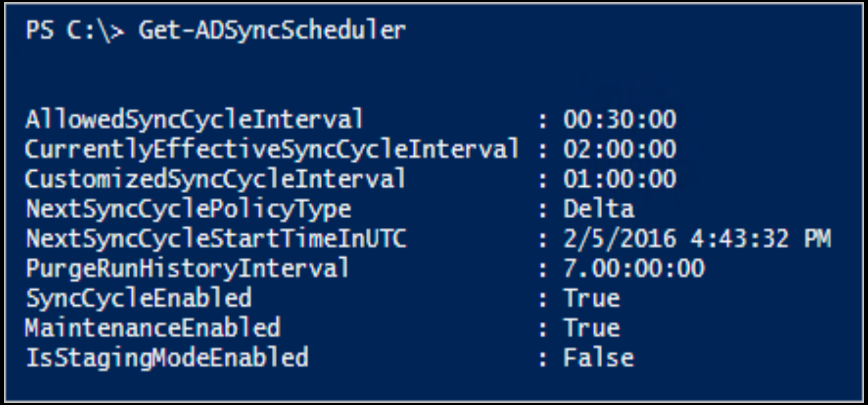
- Full Sync occurs during installation
- Delta Sync Occurs every 30mins by default
- Can be manually Initiated via UI or PowerShell
- Alteration of the Sync Schedule can be done but is NOT Supported
- Once implemented, on-premises AD becomes the “source of authority” for synchronized objects
- Modifications to synchronized objects must occur in the on-premises AD
- Synchronized objects cannot be modified or deleted via the portal unless AAD-Connect is disabled for the tenant
- Imported Object come in as Unlicenced

Scheduler PowerShell Options

- To Initiate a Delta Sync Open a PowerShell prompt and enter the following:
- Start-ADSyncSyncCycle -PolicyType Delta
- To initiate a full sync cycle, run
- Start-ADSyncSyncCycle -PolicyType Initial from a PowerShell prompt. This will start a full sync cycle.

AAD-Connect PowerShell Options

- To see your current configuration settings, go to PowerShell and run **Get-ADSyncScheduler**
- **AllowedSyncCycleInterval**. The most frequently Azure AD will allow synchronizations to occur. You cannot synchronize more frequently than this and still be supported.

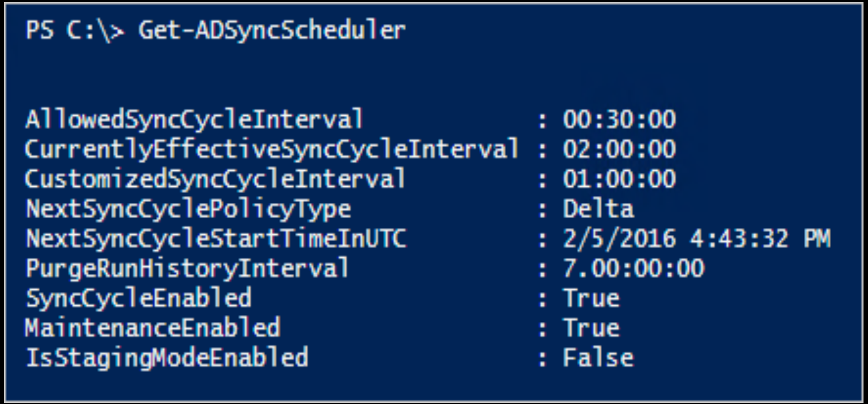


```
PS C:\> Get-ADSyncScheduler


AllowedSyncCycleInterval            : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 02:00:00
CustomizedSyncCycleInterval         : 01:00:00
NextSyncCyclePolicyType             : Delta
NextSyncCycleStartTimeInUTC         : 2/5/2016 4:43:32 PM
PurgeRunHistoryInterval             : 7.00:00:00
SyncCycleEnabled                    : True
MaintenanceEnabled                  : True
IsStagingModeEnabled                : False
```

AAD-Connect PowerShell Options

- **CurrentlyEffectiveSyncCycleInterval**.
- The schedule currently in effect. It will have the same value as CustomizedSyncInterval (if set) if it is not more frequent than AllowedSyncInterval.
- If you change CustomizedSyncCycleInterval, this will take effect after next synchronization cycle.

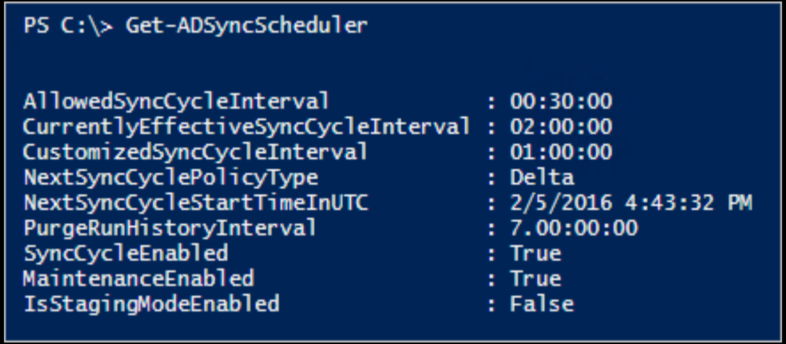


```
PS C:\> Get-ADSyncScheduler


AllowedSyncCycleInterval            : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 02:00:00
CustomizedSyncCycleInterval         : 01:00:00
NextSyncCyclePolicyType             : Delta
NextSyncCycleStartTimeInUTC         : 2/5/2016 4:43:32 PM
PurgeRunHistoryInterval             : 7.00:00:00
SyncCycleEnabled                    : True
MaintenanceEnabled                  : True
IsStagingModeEnabled                : False
```

AAD-Connect PowerShell Options

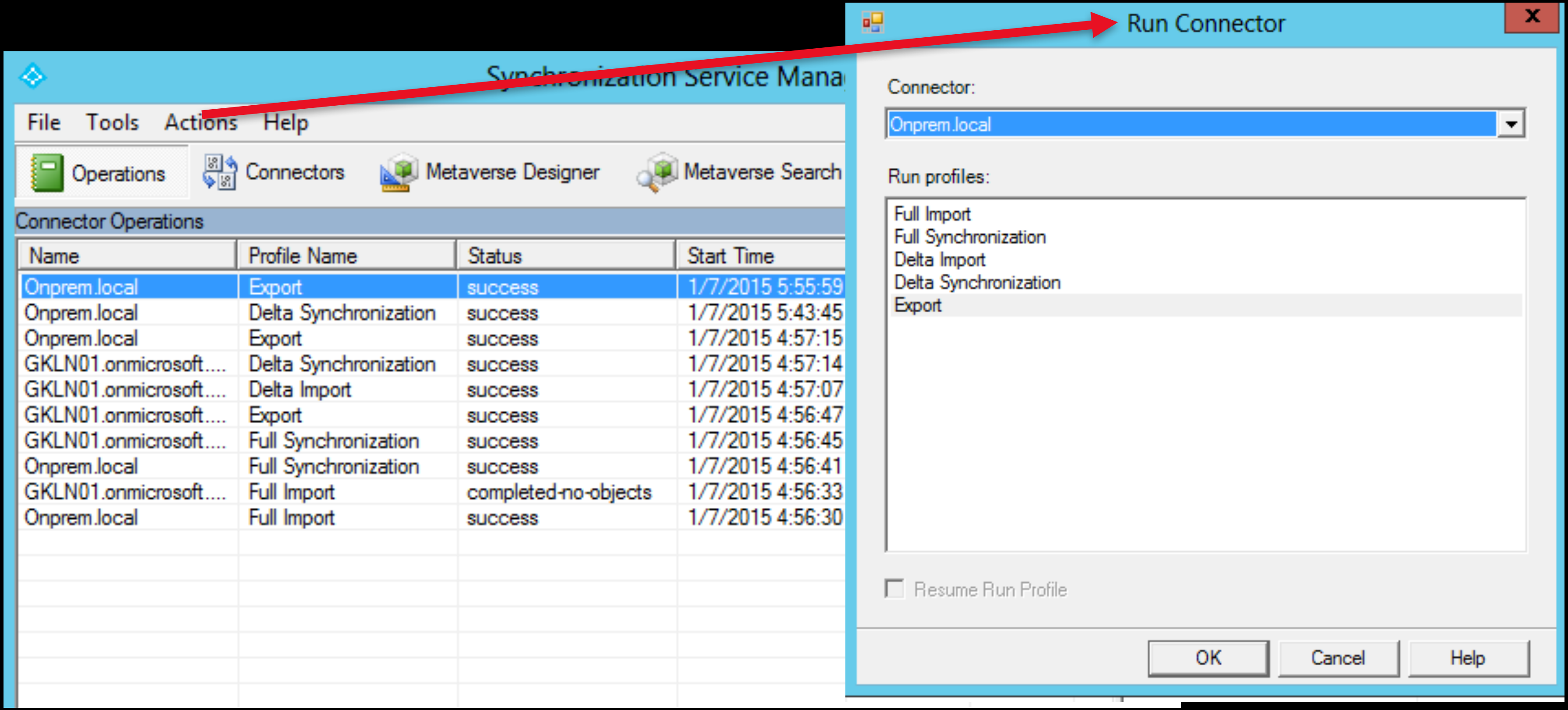
- **CustomizedSyncCycleInterval**.
- If you want the scheduler to run at any other frequency than the default 30 minutes, you will configure this setting.
- In the picture to the right the scheduler has been set to run every hour instead.
- If you set this to a value lower than AllowedSyncInterval, the latter will be used.
- There are more options but these are the main ones



```
PS C:\> Get-ADSyncScheduler


AllowedSyncCycleInterval            : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 02:00:00
CustomizedSyncCycleInterval         : 01:00:00
NextSyncCyclePolicyType             : Delta
NextSyncCycleStartTimeInUTC         : 2/5/2016 4:43:32 PM
PurgeRunHistoryInterval             : 7.00:00:00
SyncCycleEnabled                    : True
MaintenanceEnabled                  : True
IsStagingModeEnabled                : False
```

Sync Service Manager



Connector Operations

Name	Profile Name	Status	Start Time
Onprem.local	Export	success	1/7/2015 5:55:59
Onprem.local	Delta Synchronization	success	1/7/2015 5:43:45
Onprem.local	Export	success	1/7/2015 4:57:15
GKLN01.onmicrosoft....	Delta Synchronization	success	1/7/2015 4:57:14
GKLN01.onmicrosoft....	Delta Import	success	1/7/2015 4:57:07
GKLN01.onmicrosoft....	Export	success	1/7/2015 4:56:47
GKLN01.onmicrosoft....	Full Synchronization	success	1/7/2015 4:56:45
Onprem.local	Full Synchronization	success	1/7/2015 4:56:41
GKLN01.onmicrosoft....	Full Import	completed-no-objects	1/7/2015 4:56:33
Onprem.local	Full Import	success	1/7/2015 4:56:30

Connector: Onprem.local

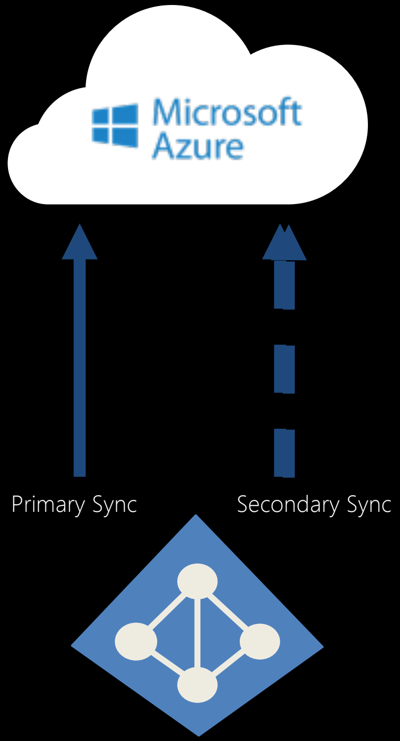
Run profiles:

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

☐ Resume Run Profile

Ok, but tell me Something I don't Know!

- The AAD Sync Engine actually has two Sync Processes, a primary and an undocumented Secondary Process
- For an urgent delta sync, AAD-Connect sends out a secondary sync pulse to check for account deletions, password resets etc
- This is not configurable and cannot be amended
- The Primary sync engine can be edited via PowerShell



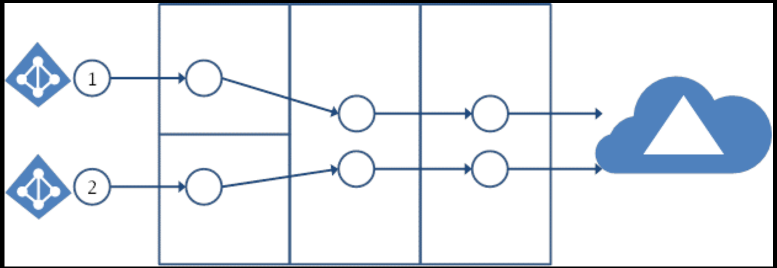
Multi Forrest Scenarios …

Multi Forrest Scenarios

- Separate Topologies
- Full mesh with optional GAL Sync
- Account-Resource Forest

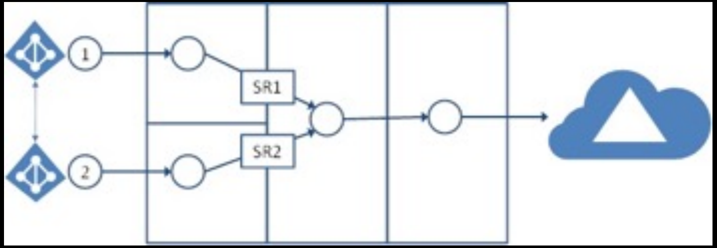
AAD-Connect Scenarios: Separate Topologies

- Forests on-prem treated as separate entities and no user would be present in any other forest
- Each forest has its own Exchange org and there is no GALSync between the forests
- Situation after a merger/acquisition or in an org where each business unit is operating isolated from each other
- Each object in each forest will be represented once in the metaverse and aggregated in the target AAD directory
- Same end-result as having one AAD-Connect server connected to each source AD forest



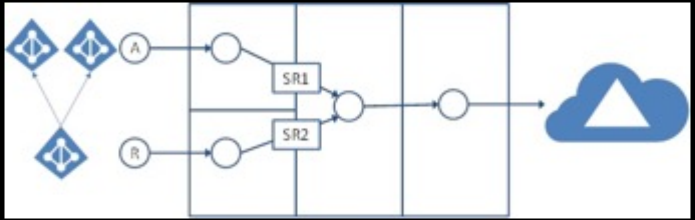
AAD-Connect Scenarios: Full mesh with optional GALSync

- Full meshed topology allows users and resources to be located in any forest and commonly there would be two-way trusts between the forests
- If Exchange is present in more than one forest, there could optionally be a GALSync solution representing a user in one forest as a contact in each other forest
- In this picture we would join on the mail attribute so a user with a mailbox in one forest is joined with the contacts in the other forests
- Distribution and security groups can be found in each forest and can contain a mix of users, contacts, and FSPs (Foreign Security Principals).



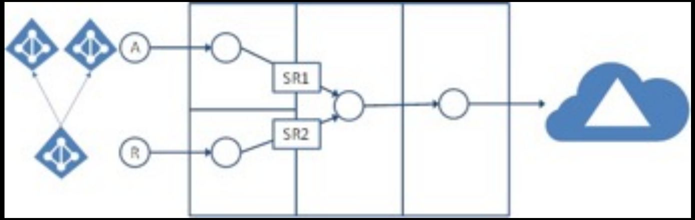
AAD-Connect Scenarios: Account-Resource Forest

- You will have one or more account forests where there are active user accounts
- There will also be one forest trusting all account forests
- This forest will most likely have an extended AD schema with Exchange and Lync
- All Exchange and Lync services as well as other shared services will be located in this forest
- The user will have a disabled user account in this forest and the mailbox will be linked to the account forest
- In the picture below, only one account forest has been represented



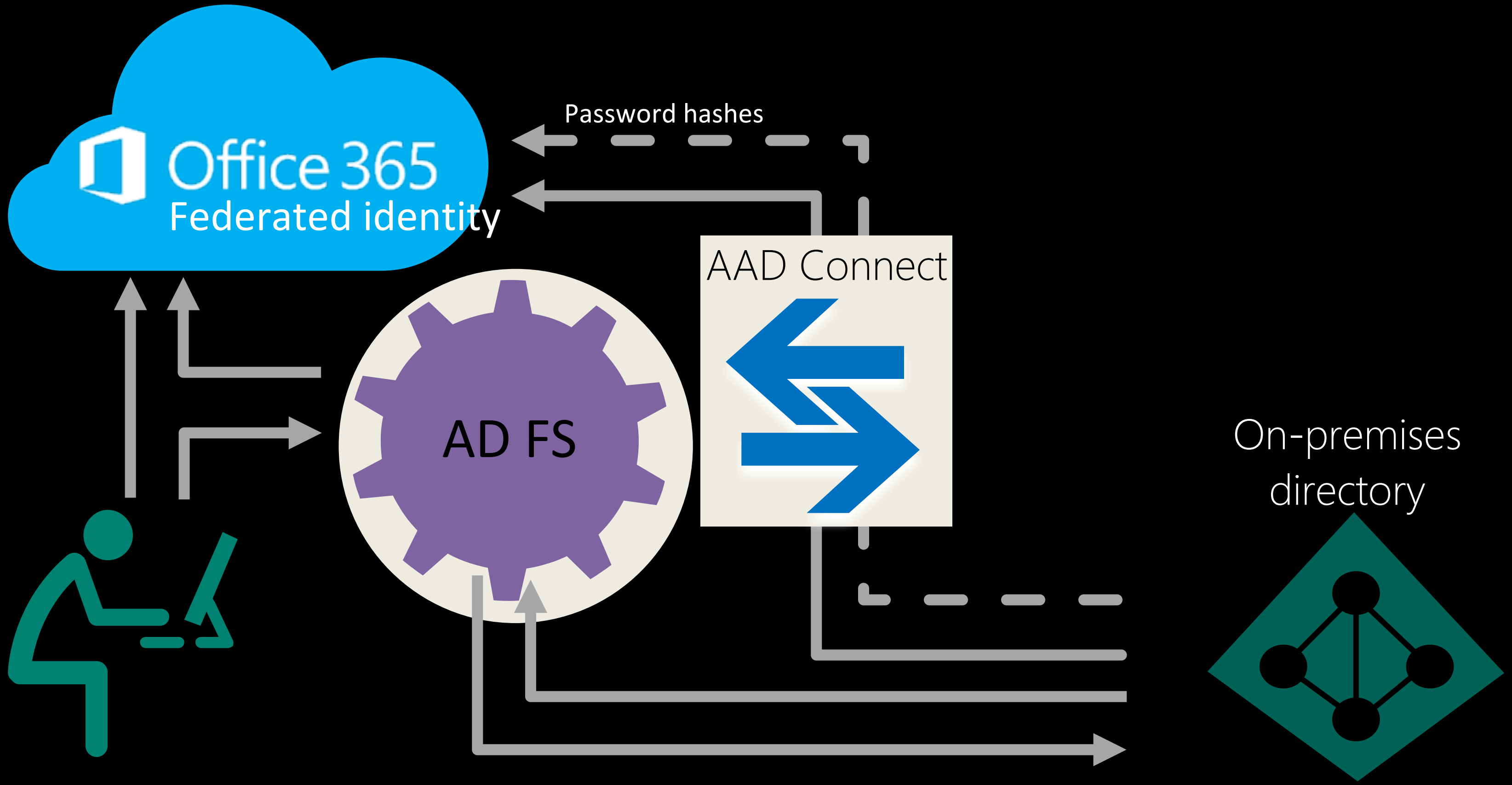
AAD-Connect Scenarios: Account-Resource Forest

- In this picture we would join the enabled user from “A” (Account) with the disabled user in “R” (Resource) using objectSid and msExchMasterAccountSid
- The attributes used for login will come from the account forest with the rules marked SR1 in the picture
- The user and Exchange attributes would come from the resource forest using the rules named SR2
- In the resource forest we would also expect to find distribution groups with the disabled user as the member
- We would also expect to find shared security groups in the resource forest with FSPs to represent the active user in the account forest

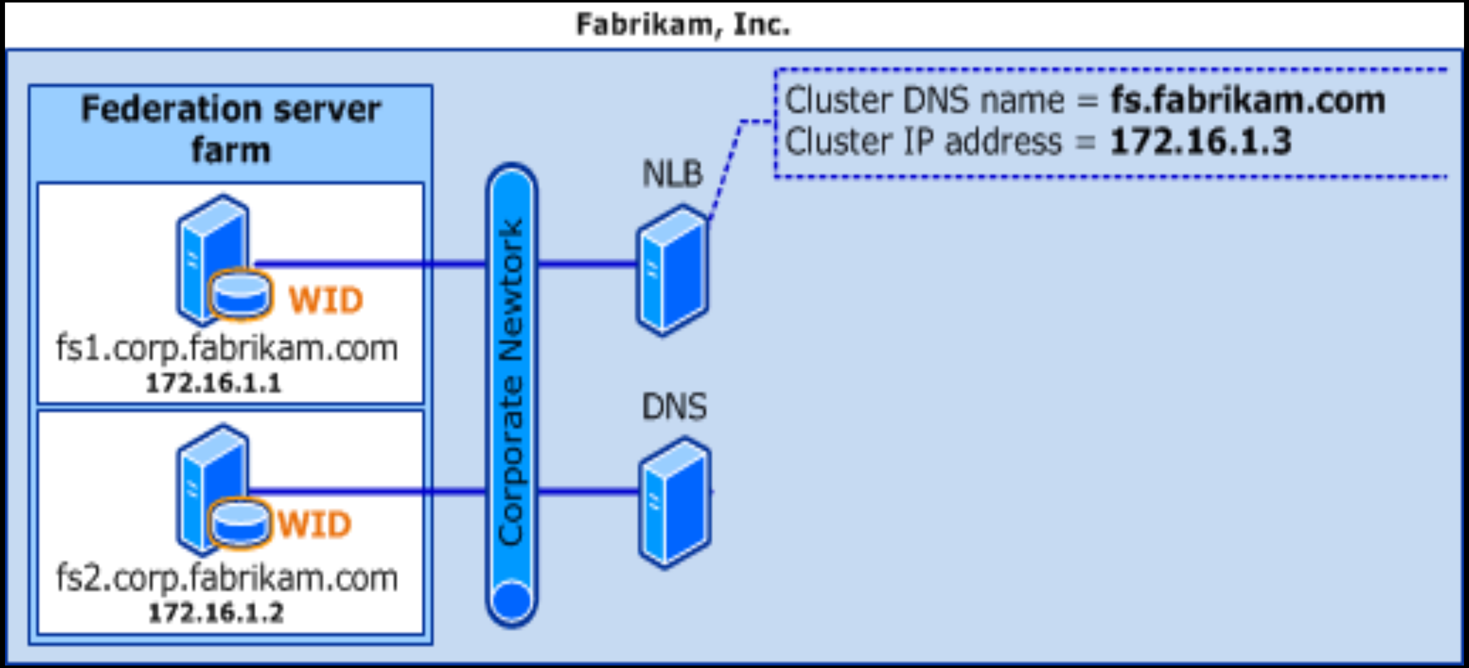


Deploying ADFS Via AzureAD-Connect

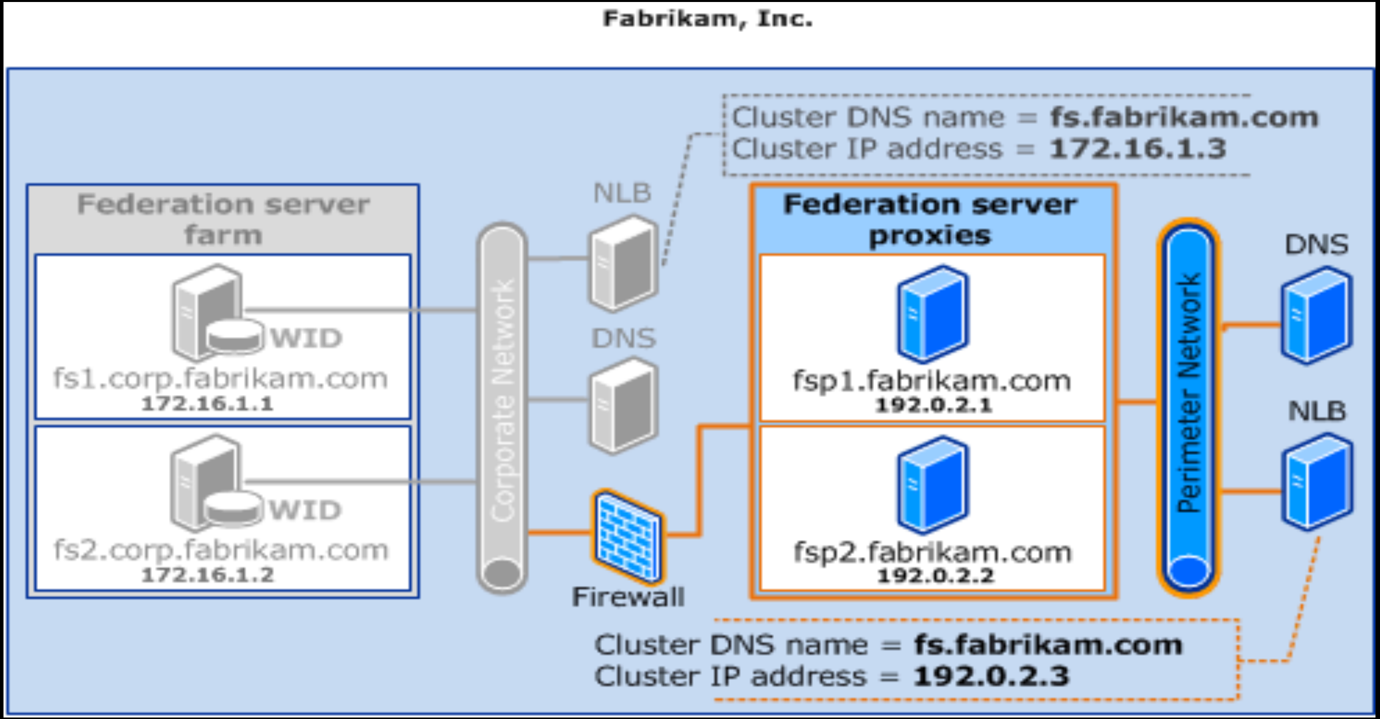
Federated identity model



Deploy a Federation Server Farm

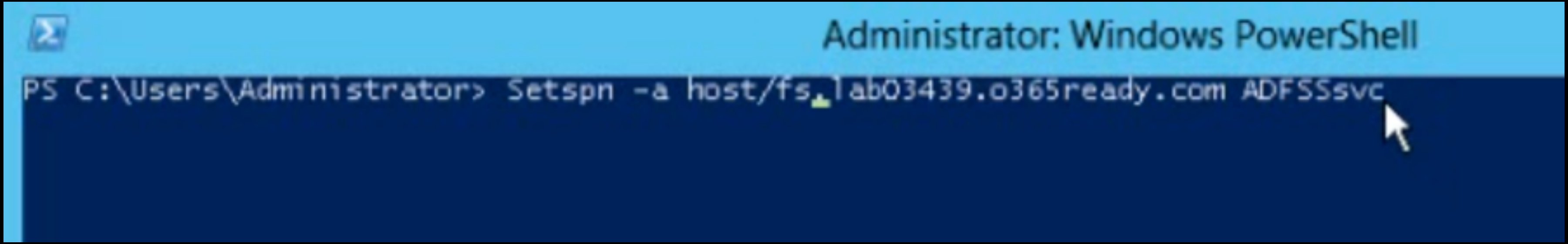


Deploy Federation Server Proxies



ADFS: Prerequisites

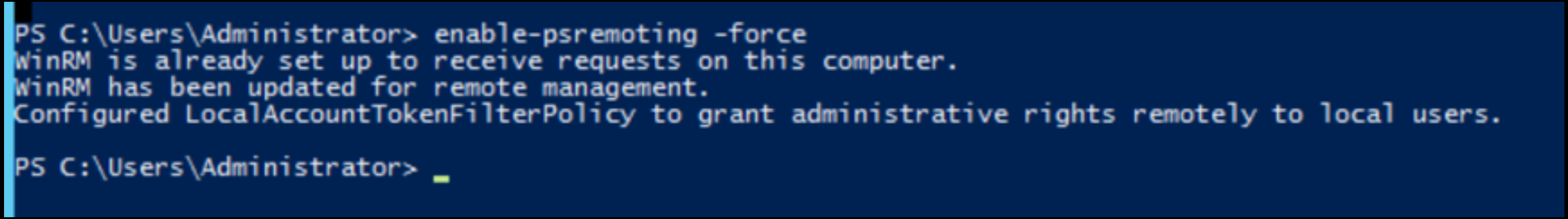
1. Create FS DNS Record in Local & Remote DNS Servers
2. Create User Account in ADUC
3. Grant the user account Service Account permissions before running the wizard



```
PS C:\Users\Administrator> Setspn -a host/fs.lab03439.o365ready.com ADFSSsvc
```

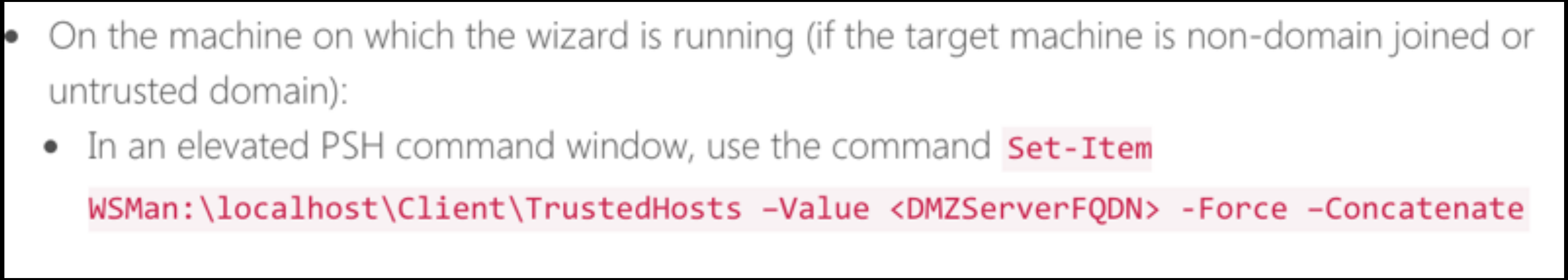
ADFS Proxy: Prerequisites

1. AAD-Connect Requires Windows Server 2012 R2 / 2016
2. Enable PSRemoting



```
PS C:\Users\Administrator> enable-psremoting -force
WinRM is already set up to receive requests on this computer.
WinRM has been updated for remote management.
Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

PS C:\Users\Administrator> _
```



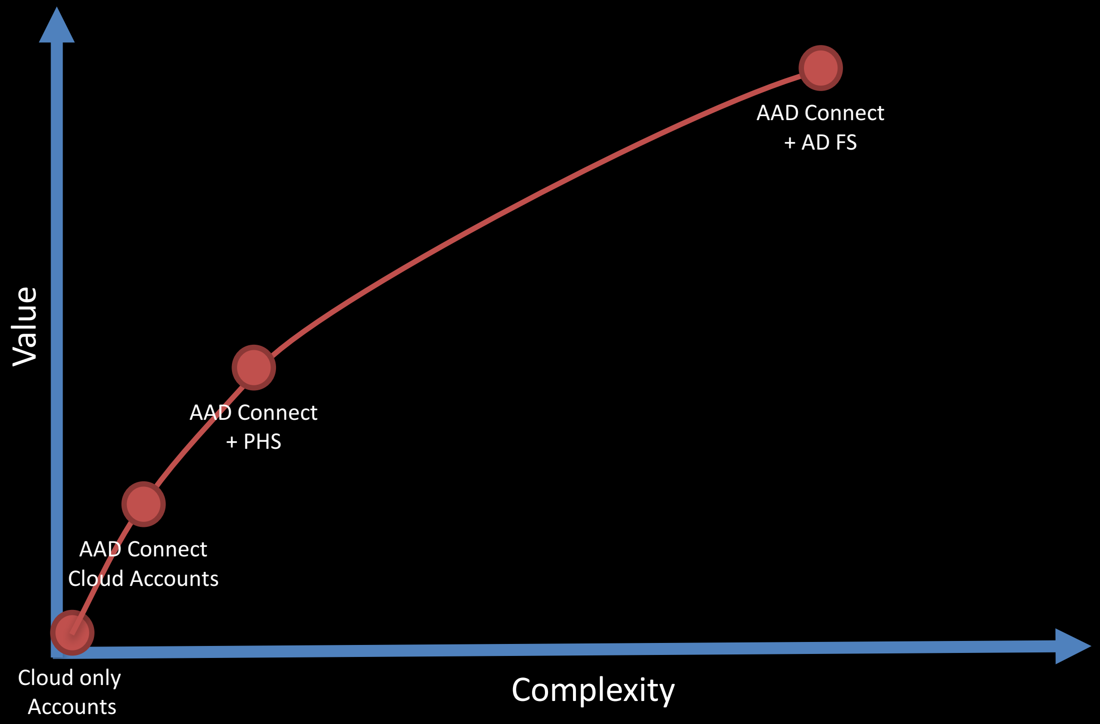
- On the machine on which the wizard is running (if the target machine is non-domain joined or untrusted domain):
  - In an elevated PSH command window, use the command `Set-Item WSMan:\localhost\Client\TrustedHosts –Value <DMZServerFQDN> -Force –Concatenate`

Demo

Deploying ADFS Via AzureAD-Connect

Introducing: Pass Through Authentication (PTA) & Desktop Single Sign On

Sign-in Options today



Demand for Increased Flexibility

Growing Number of Onboarding Requirements

- Need to AuthN against AD on-prem
- Do not wish any passwords Stored on Passed through in the cloud
- No Unauthenticated Endpoints on-prem exposed to internet
- Provide a Simpler SSO solution

Introducing Azure AD Pass-through Authentication

Enables customers to validate password on-premises without the complexity of AD FS

- Allows for on-premises policies to be evaluated such as account disabled, login hours restrictions etc.
- Simple deployment via AAD Connect, no complex DMZ requirements
- Works for single or multi-forest customers

Built on AAD Application Proxy infrastructure

- Securely validates the user's password against on-premises AD
- Customer can deploy multiple agents for HA

Bottom line – Similar benefits to federation without the deployment cost

Desktop SSO

True single sign on without the cost of AD FS

- No additional servers or infrastructure required on premises
- Accelerated deployment

Utilizes existing AD infrastructure

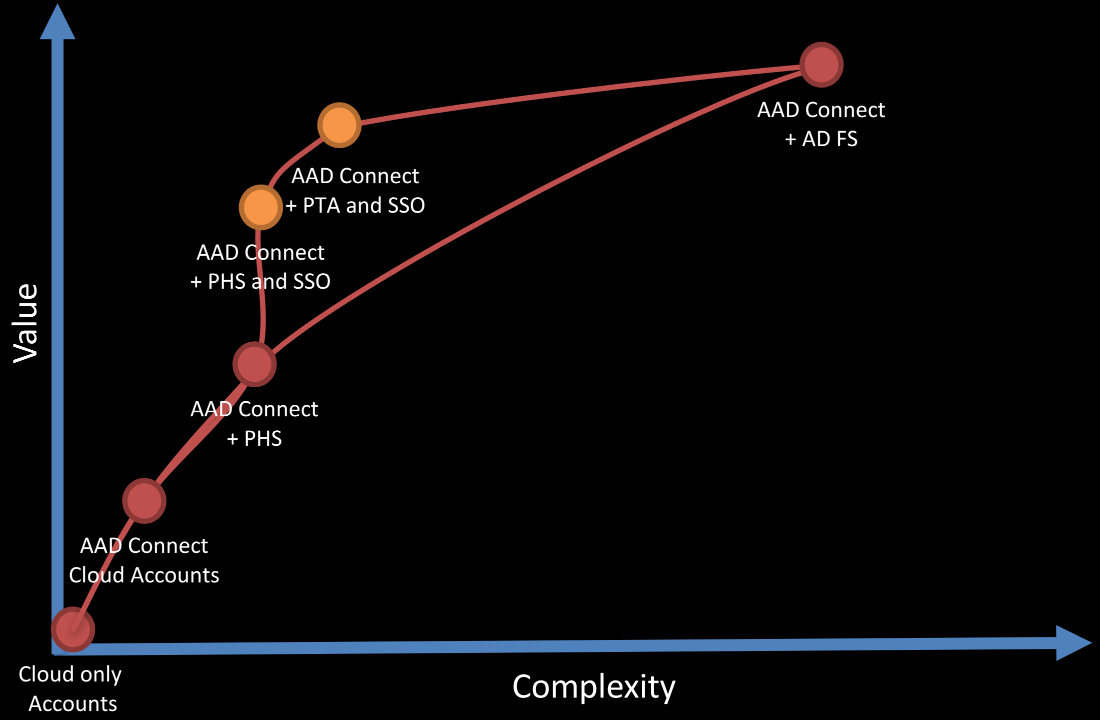
- Inherit support for multiple regions
- Inherit support for finding the closest DC
- Based on Kerberos
- No DR plan outside of existing AD plans

Support for both PTA and PHS customers

- SSO is provide for all domain joined corporate machines with line of sight to a DC

How this will Change your World …

Sign-in Options tomorrow



How this changes deployments

Provides similar services to AD FS

- Forms based authentication for non-domain joined/outside of corp net users (PTA)
- SSO for domain joined users on corp net (SSO)

No need for dedicated servers

- PTA can be installed on existing servers or DC's
- SSO is only a computer account in AD

No load balancers

- PTA automatically uses all available connectors no need to load balance

No DMZ

- All connections are outbound
- No unauthenticated end points on the internet

Less to manage ongoing

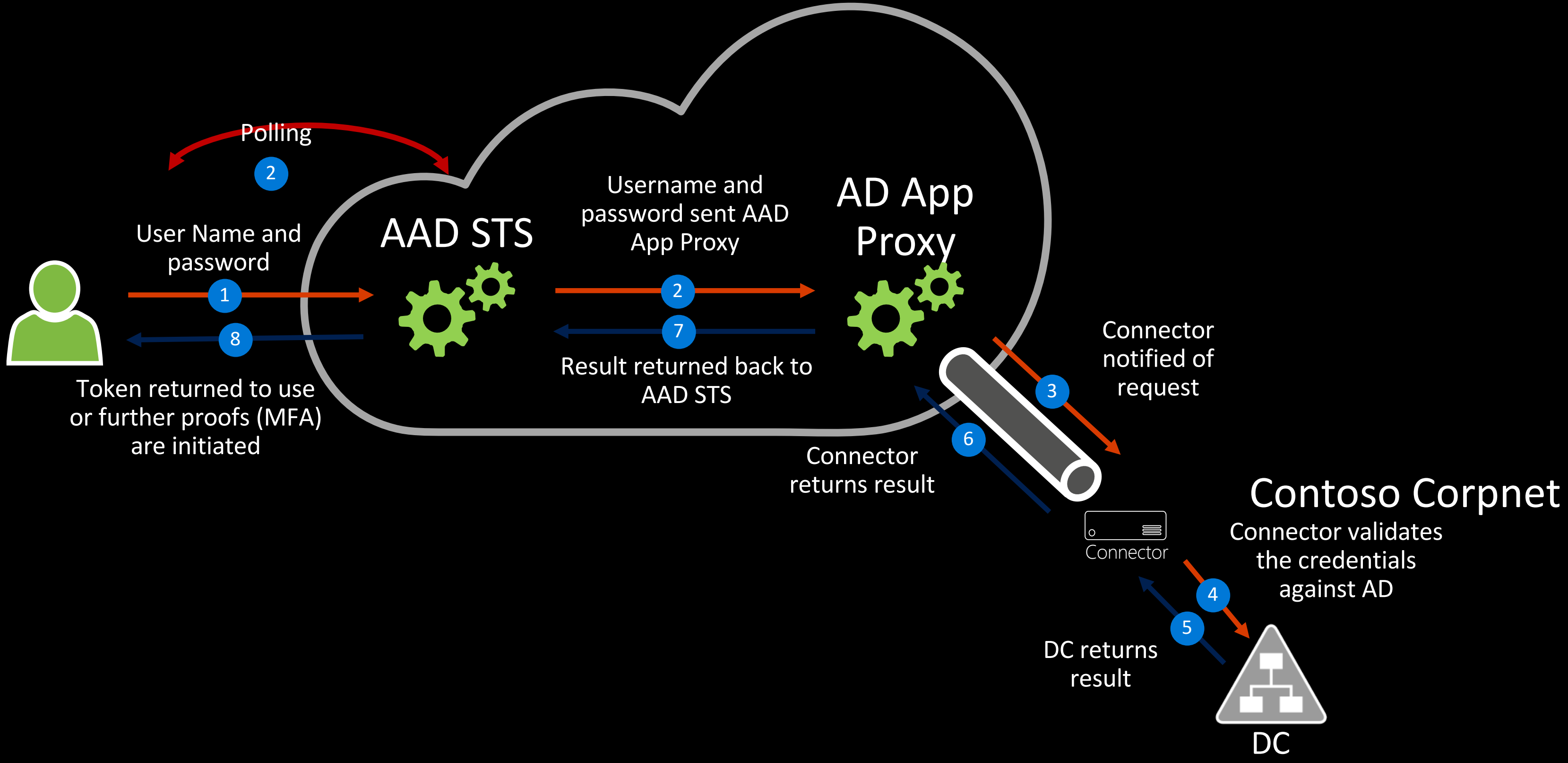
- Simple DR, place connectors where needed
- No certificates to manage

What AD FS offers that PTA and SSO Don’t

- Support for smartcard authentication
- Support for 3rd Party MFA providers
- Passwords are always in your control boundary – i.e. don’t pass through the cloud
- Conditional access rules based on Exchange protocols (e.g. pop, imap etc)
- Support for on-premises device based conditional access (device write back)

How it Works …

PTA – Updated flow


Polling
2
User Name and password
1
8
Token returned to use or further proofs (MFA) are initiated
AAD STS
Username and password sent AAD App Proxy
2
7
Result returned back to AAD STS
AD App Proxy
Connector notified of request
3
6
Connector returns result
Connector
Contoso Corpnet
Connector validates the credentials against AD
4
5
DC returns result
DC

Pass-Through Authentication

Supported Scenarios

- Rich Clients that utilize modern authentication, think ADAL (AD Application Library) enabled
- Browser based passive Web flows

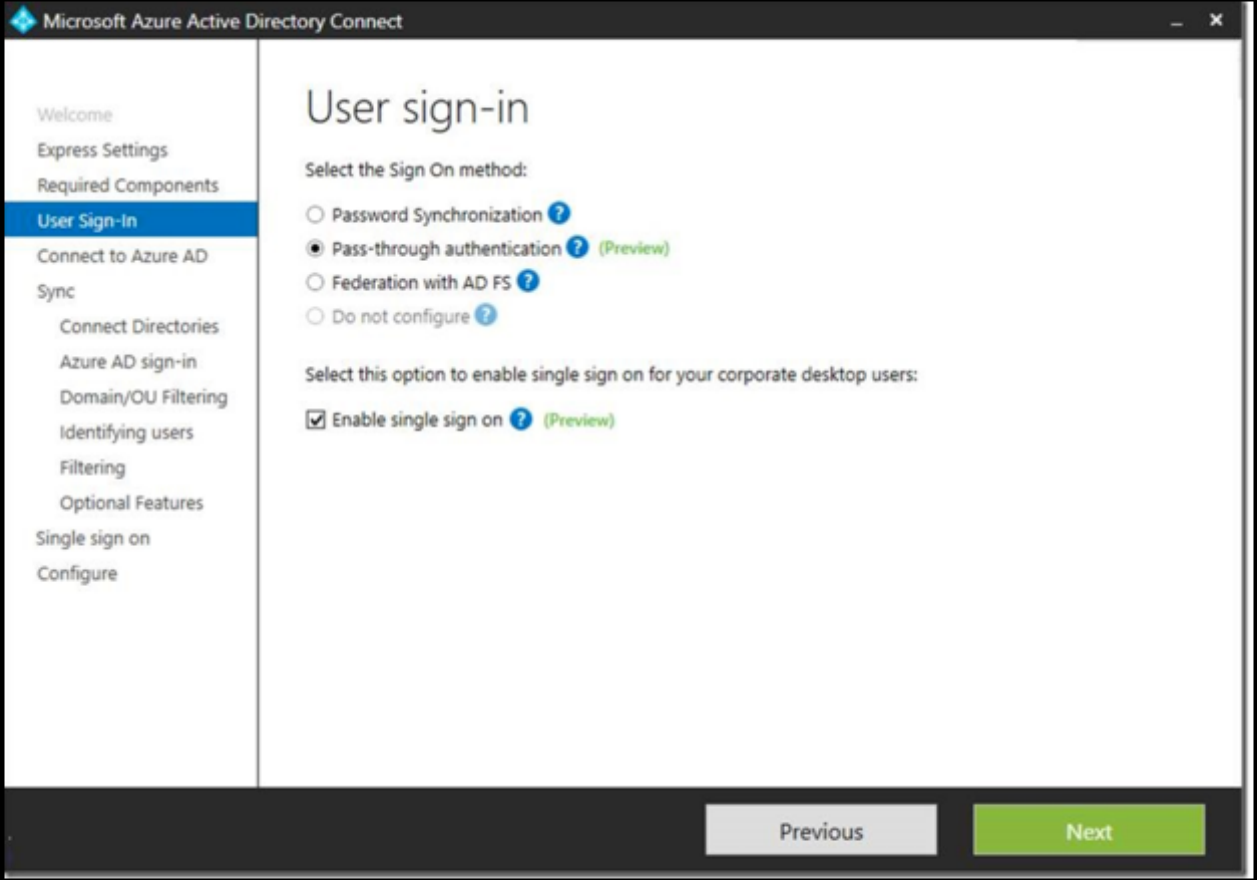
Future Supported Scenarios

- Legacy clients (PowerShell, Lync/Skype, Outlook not using ADAL) – GA
- EAS, native mobile email clients - GA

Until then

- Customers need to use ADAL enabled clients
- Alternatively, use PHS as a fallback

Desktop SSO Requirements



User sign-in

Select the Sign On method:

○ Password Synchronization

● Pass-through authentication (Preview)

○ Federation with AD FS

○ Do not configure

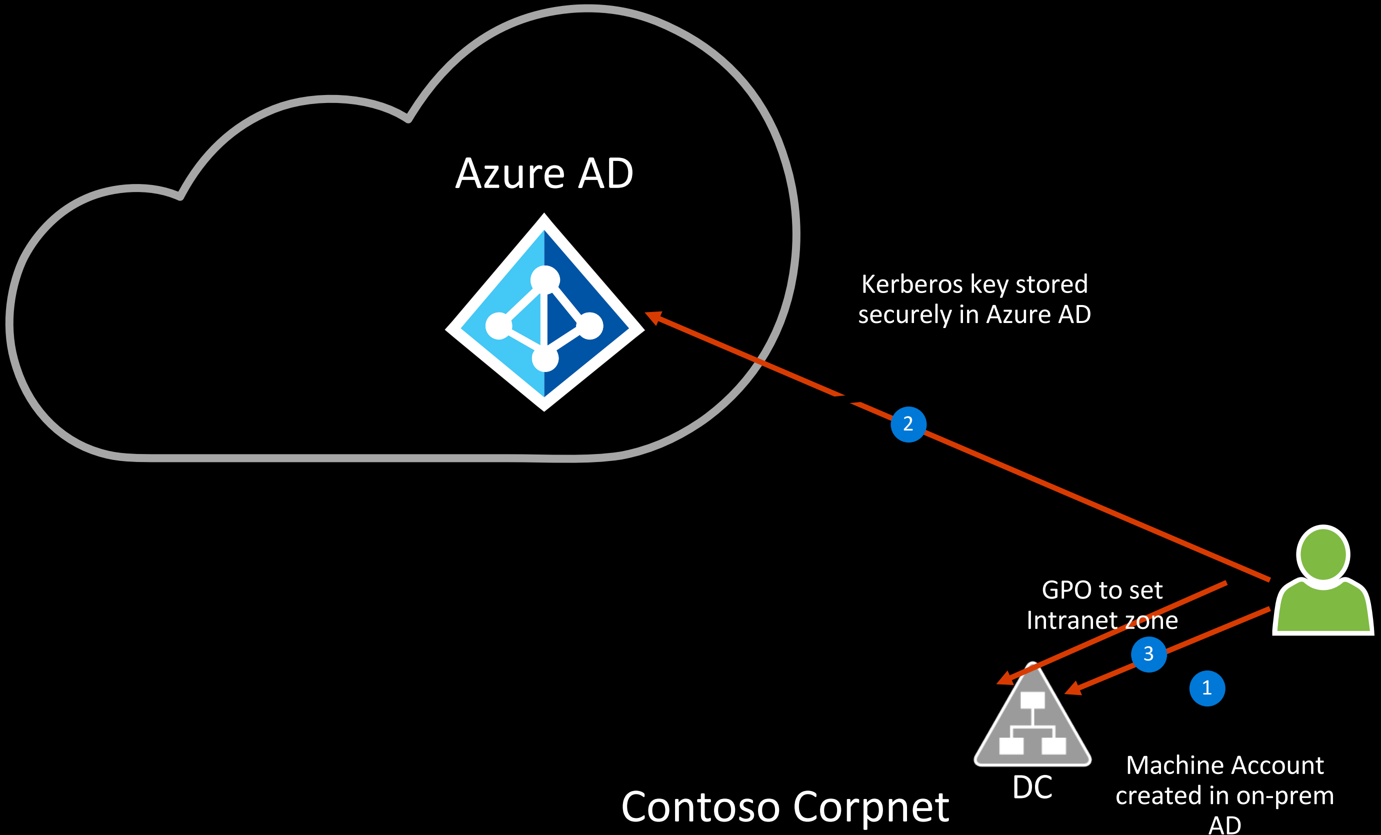
Select this option to enable single sign on for your corporate desktop users:

☑ Enable single sign on (Preview)

Desktop SSO Client Config

- Enabled in Azure Active Directory Connect with either Password hash synchronization or Pass-through authentication.
- Login must occur on a domain joined machine
- Have a direct connection to a domain controller on corpnet or via VPN
- Define the Kerberos end-points in the cloud as part of the browsers Intranet zone
- Supports Win 7,8,10 (No MAC Support (Yet)
- IE, Chrome & Safari Supported (But not Edge)
- Group Policy: User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page and select Site to Zone Assignment
- Value: https://autologon.microsoftazuread-sso.com Data: 1
  Value: https://aadg.windows.net.nsatc.net Data: 1'

How does it work - Setup

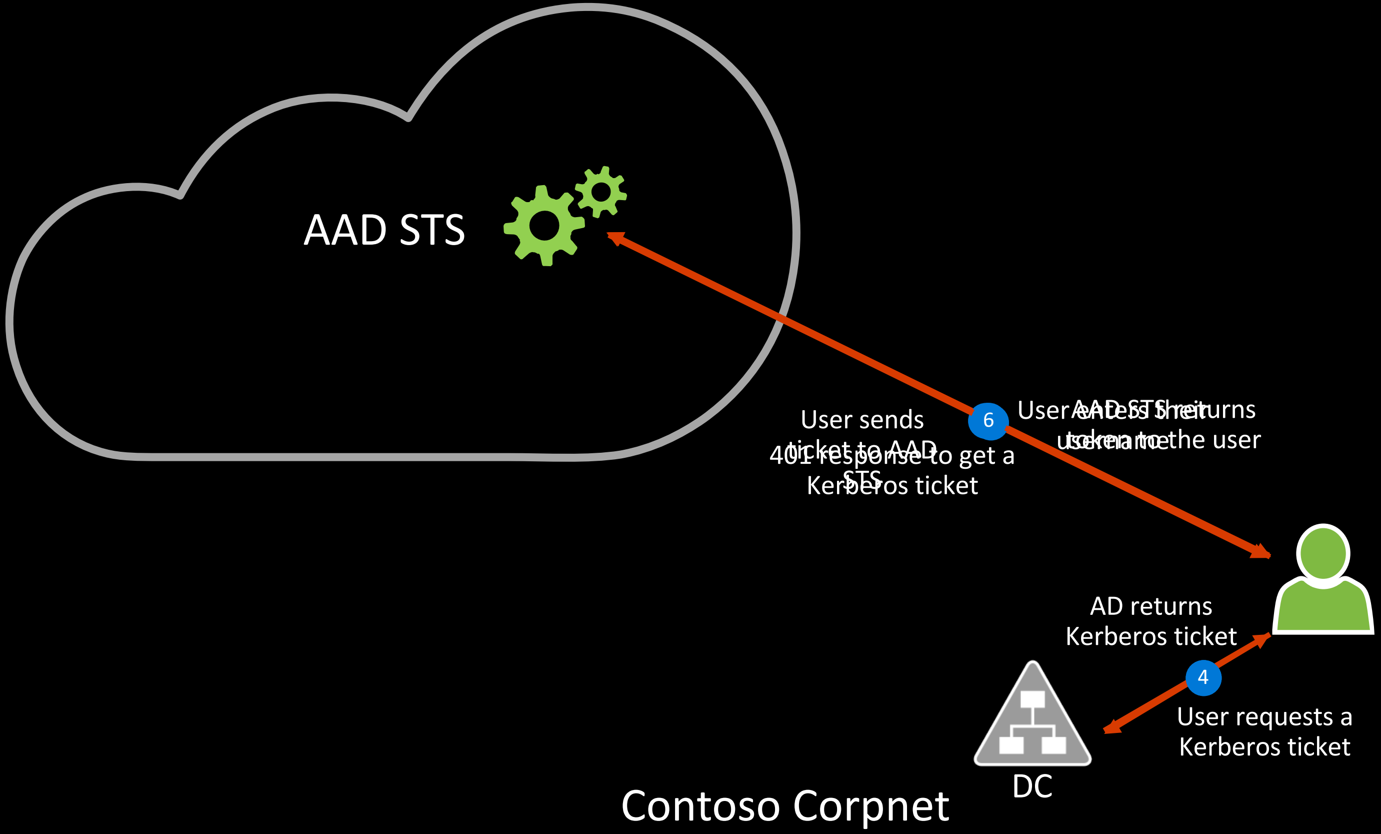


Kerberos key stored securely in Azure AD

GPO to set Intranet zone

Machine Account created in on-prem AD

How does it work - Runtime



AAD STS

User sends ticket to AAD STS

401 response to get a Kerberos ticket

6

User enters their username

AAD STS returns token to the user

AD returns Kerberos ticket

4

User requests a Kerberos ticket

DC

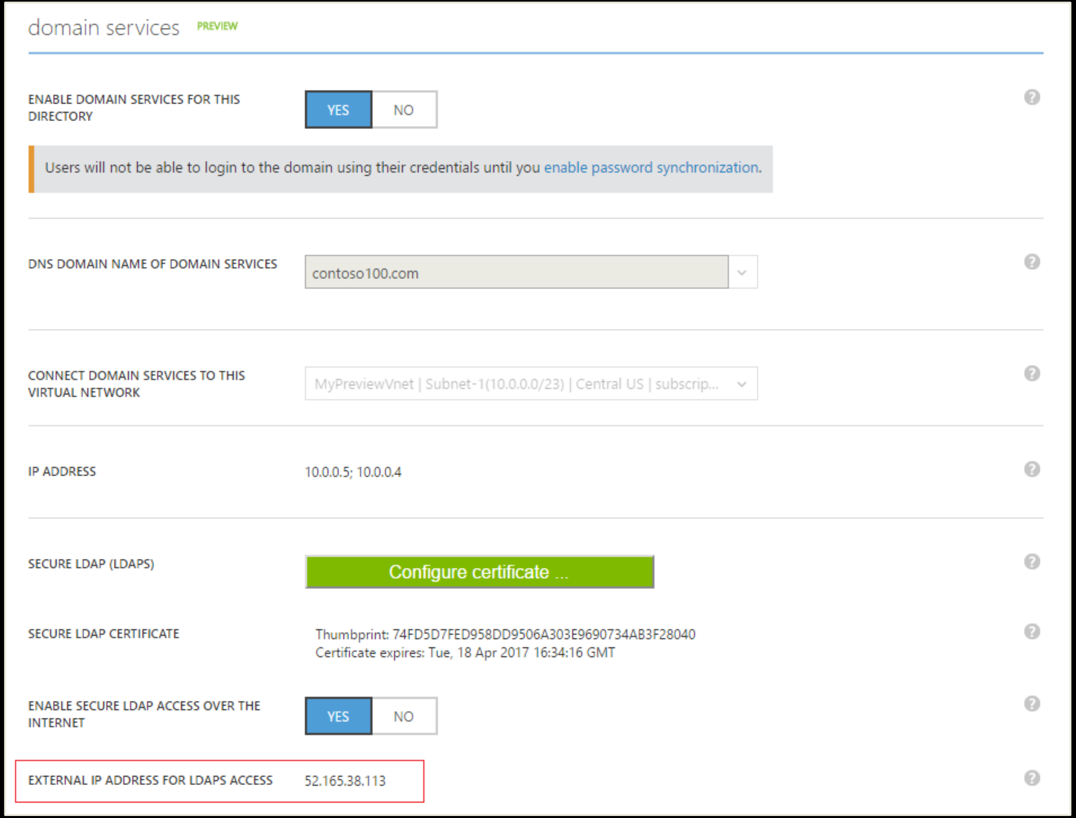
Contoso Corpnet

Demo

Pass Through Authentication & Single Sign On

Other Cool Features …

Secure LDAP



domain services PREVIEW

ENABLE DOMAIN SERVICES FOR THIS DIRECTORY [✓ YES] NO

Users will not be able to login to the domain using their credentials until you enable password synchronization.

DNS DOMAIN NAME OF DOMAIN SERVICES contoso100.com

CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK MyPreviewVnet | Subnet-1(10.0.0.0/23) | Central US | subscrip...

IP ADDRESS 10.0.0.5; 10.0.0.4

SECURE LDAP (LDAPS) Configure certificate ...

SECURE LDAP CERTIFICATE
Thumbprint: 74FD5D7FED958DD9506A303E9690734AB3F28040
Certificate expires: Tue, 18 Apr 2017 16:34:16 GMT

ENABLE SECURE LDAP ACCESS OVER THE INTERNET [✓ YES] NO

EXTERNAL IP ADDRESS FOR LDAPS ACCESS 52.165.38.113

Enable LDAPS access to your managed domain.

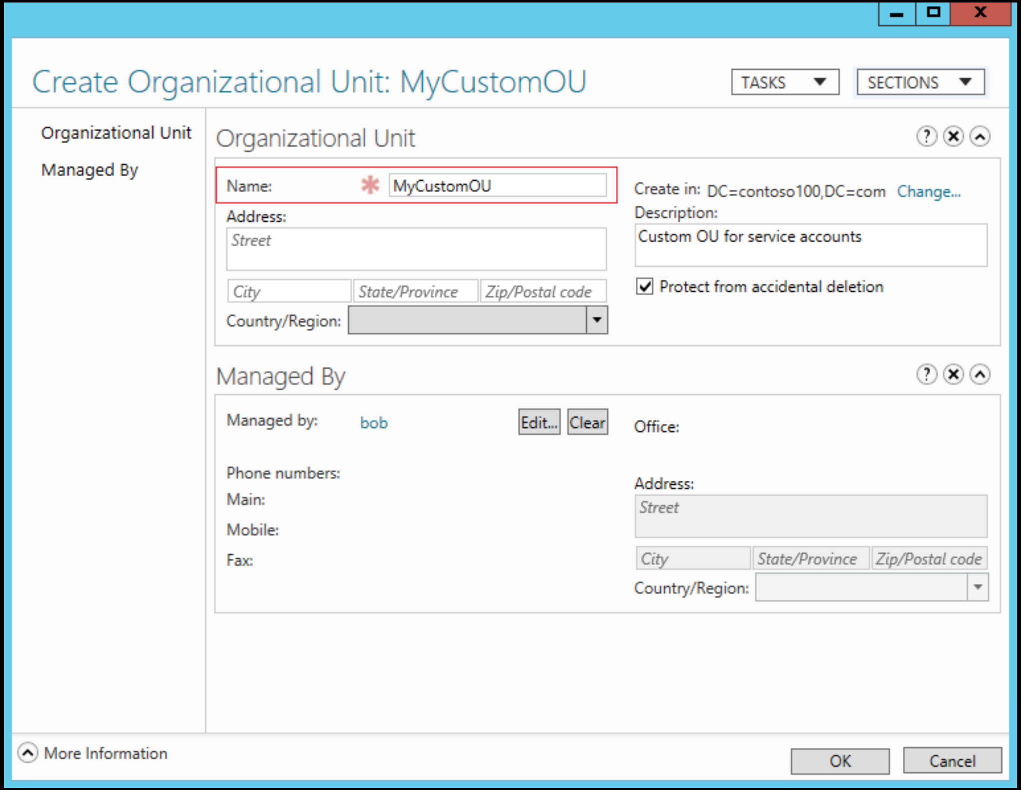
- Default – access within the virtual network.
- Optional – access over the internet.

Easy to configure

- Upload .PFX file containing LDAPS cert.
- Enterprise CA, Public CA or self-signed certificate.

More information

Create Custom OU's on a Managed Domain



Create Organizational Unit: MyCustomOU

Organizational Unit

Name: * MyCustomOU

Create in: DC=contoso100,DC=com

Description: Custom OU for service accounts

☑ Protect from accidental deletion

Managed By

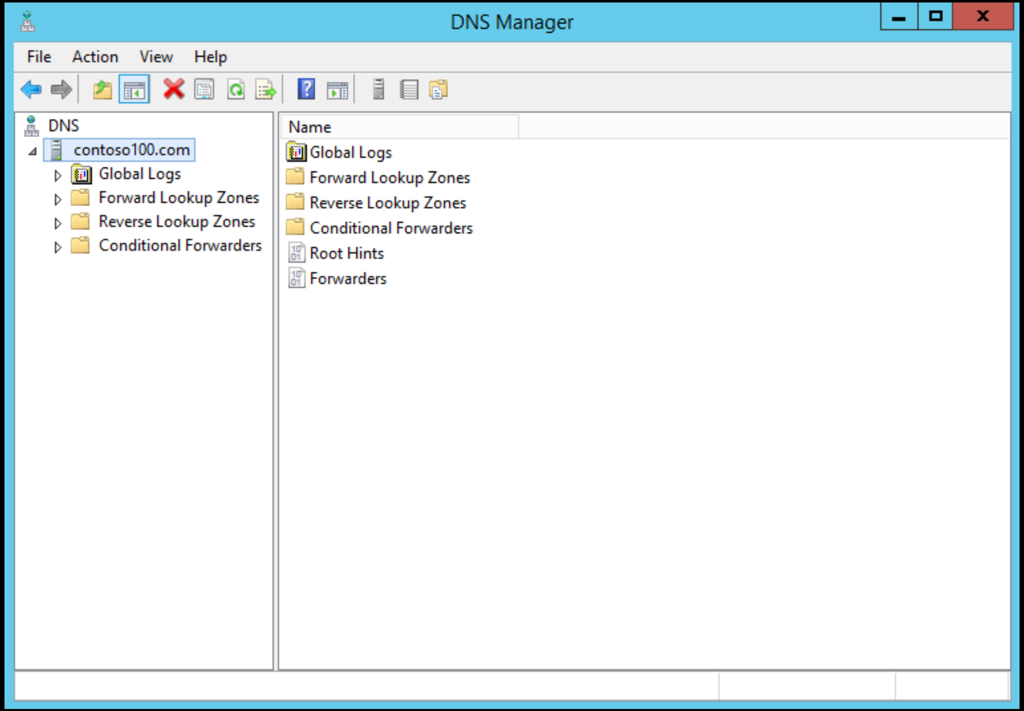
Managed by: bob

Custom OU support

- Members of 'AAD DC Administrators' group can now create custom OUs.
- Creators of the OU have full administrative rights on the OU.
- Use familiar Windows Server AD administration tools (eg. AD Administration Center) to create OU.
- Create service accounts with custom password policies (eg. password-does-not-expire etc.) in custom OU.

More information

Administer DNS on a Manged Domain



Administer DNS

- Members of 'AAD DC Administrators' group can now administer DNS for the managed domain.
- Use familiar Windows DNS administration tools (eg. DNS Manager snap-in).
- Create DNS entries for load-balancers, non-domain joined machines etc. within your virtual network.

More information

Review…

Available Now in Paperback & eBook

www.darknebulapublishing.com

Follow me on Twitter
@AndyMalone

NIC 2017

nordic infrastructure conference

The premium event for IT-professionals

Feb. 1-3rd in Oslo Spektrum