Module 2: Integrating with Azure AD Connect

Lab Overview

In this module, we cover all aspects of Active Directory integration with Azure Active Directory, by using Azure AD Connect. The lab exercise covers the following:

- Registration of an additional Azure Tenant domain name, reflecting the organization's public namespace
- Installation of Azure AD Connect – Express Settings
- Synchronization of on-premises AD users/groups to Azure AD, from Azure AD Connect
- Guidelines on AADConnect troubleshooting
- Azure AD Health Portal

Prerequisites

In order to execute the steps in this demo, the following should be set up and configured 'behind the scenes':

a) In the on-premises Active Directory, create a handful of users and groups; these objects will be used later on in other demos as well

Lab Steps

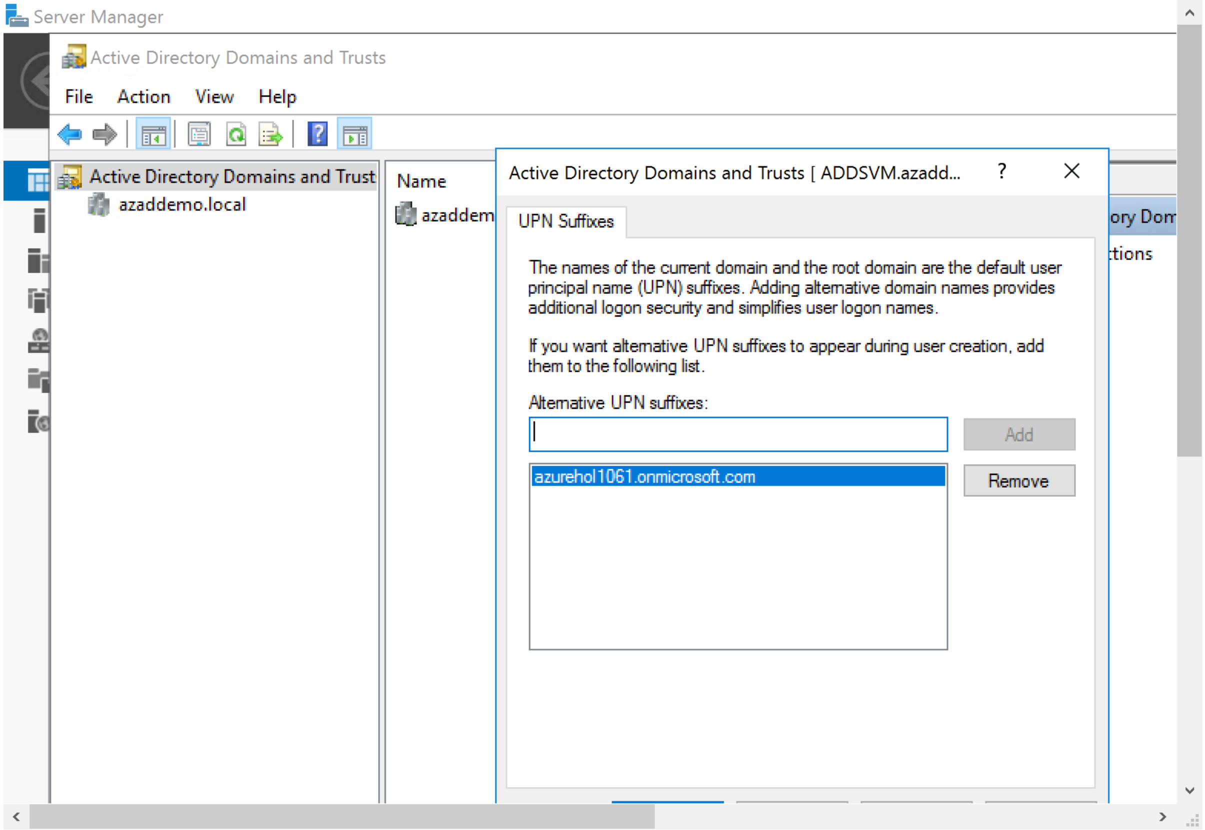
Exercise 1: Verify public DNS namespace to Azure AD

1. Connect to https://portal.azure.com
2. Log on with the admin@tenant.onmicrosoft.com account credentials
3. From the Azure Portal, browse to Azure Active Directory section
4. From the Settings blade, select "custom domain names", and notice the <tenant>.onmicrosoft.com domain. Here you would add your custom public domain namespace, which we assume is not available for this lab exercise.

Note: Since you don't have a public DNS domain name available for this lab, update the UPN Suffix on the local Active Directory domain to match the one from Azure AD <tenant.onmicrosoft.com>. This to avoid issues in the AAD Connect sync later on.

1. From the Azure Portal, browse to Virtual Machines; select the ADDSVM; select Connect to open the RDP Remote Management session to this VM.
2. Use the following credentials user = labadmin; pw = L@BadminPa55w.rd
3. From the Start Menu, search for Active Directory Domains and Trusts
4. From within the Active Directory Domains and Trusts management console, select Active Directory Domains and Trusts (=the highest level in the tree)

5. Right click and select Properties; this opens the UPN suffixes tab
6. Add the Azure Active Directory namespace here (<tenant.onmicrosoft.com>)


Server Manager
Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trust
azaddemo.local
Name
azaddem
ory Dom
tions

Active Directory Domains and Trusts [ADDSVM.azadd...

UPN Suffixes

The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

azurehol1061.onmicrosoft.com

This completes the setup and configuration of a public DNS name space as additional domain in Azure Active Directory.

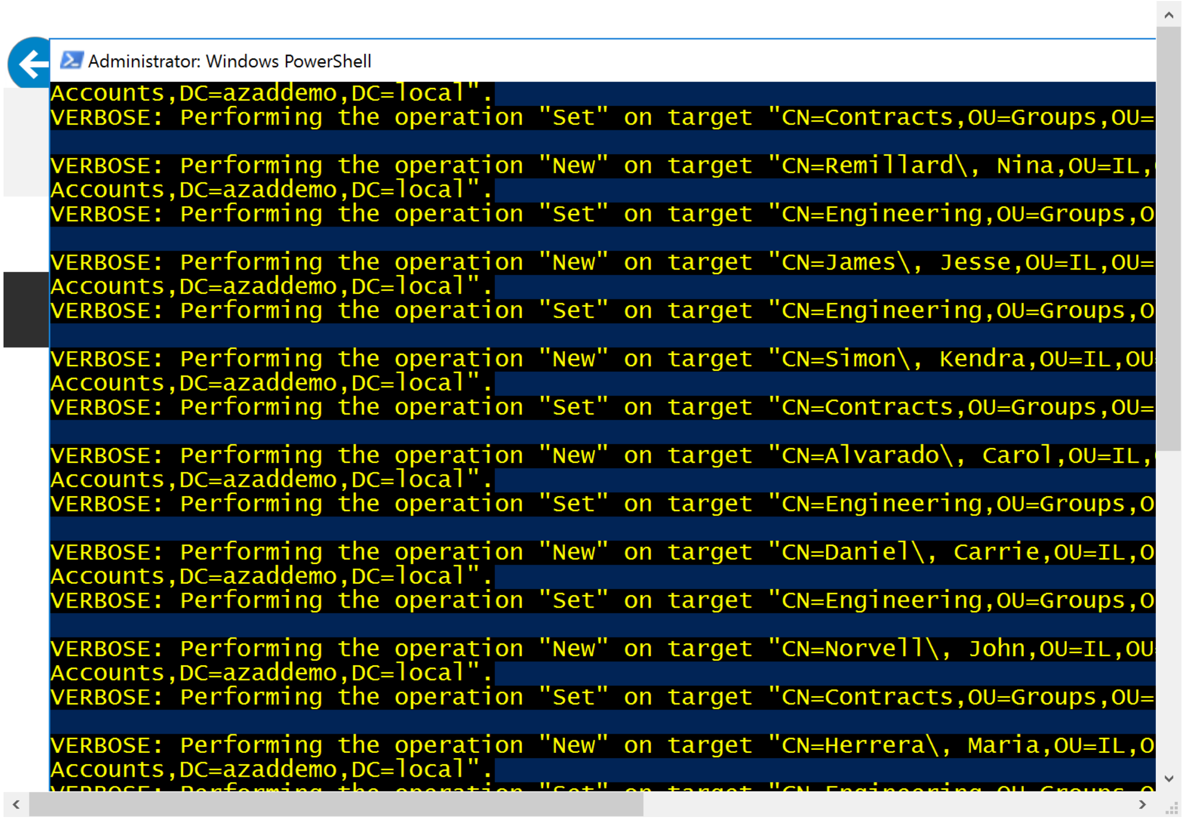
Exercise 2: Deploying Azure AD Connect in the on-premises Active Directory domain

Run this exercise from within the ADDSVM, to ease the download of the Azure AD Connect tool.

1. First, we are going to populate our on-premises Active Directory domain with departments, User groups and User accounts. Connect to the following URL: https://pdtitlabsstorage.blob.core.windows.net/templates/createdemousers/CreateDemoUsers.zip

   And download the CreateDemoUsers.zip file to your Active Directory Domain Controller VM.

2. Extract the downloaded file, and run the CreateDemoUsers.ps1 PowerShell script, by right clicking on it and selecting “Run with PowerShell”.



```
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Contracts,OU=Groups,OU=

VERBOSE: Performing the operation "New" on target "CN=Remillard\, Nina,OU=IL,
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Engineering,OU=Groups,O

VERBOSE: Performing the operation "New" on target "CN=James\, Jesse,OU=IL,OU=
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Engineering,OU=Groups,O

VERBOSE: Performing the operation "New" on target "CN=Simon\, Kendra,OU=IL,OU
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Contracts,OU=Groups,OU=

VERBOSE: Performing the operation "New" on target "CN=Alvarado\, Carol,OU=IL,
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Engineering,OU=Groups,O

VERBOSE: Performing the operation "New" on target "CN=Daniel\, Carrie,OU=IL,O
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Engineering,OU=Groups,O

VERBOSE: Performing the operation "New" on target "CN=Norvell\, John,OU=IL,OU
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Contracts,OU=Groups,OU=

VERBOSE: Performing the operation "New" on target "CN=Herrera\, Maria,OU=IL,O
Accounts,DC=azaddemo,DC=local".
VERBOSE: Performing the operation "Set" on target "CN=Engineering,OU=Groups,O
```

3. From the Start Menu, open Active Directory Users and Computers, and notice a “Demo Accounts” Organization Unit got created, with several sub-OUs and User accounts.

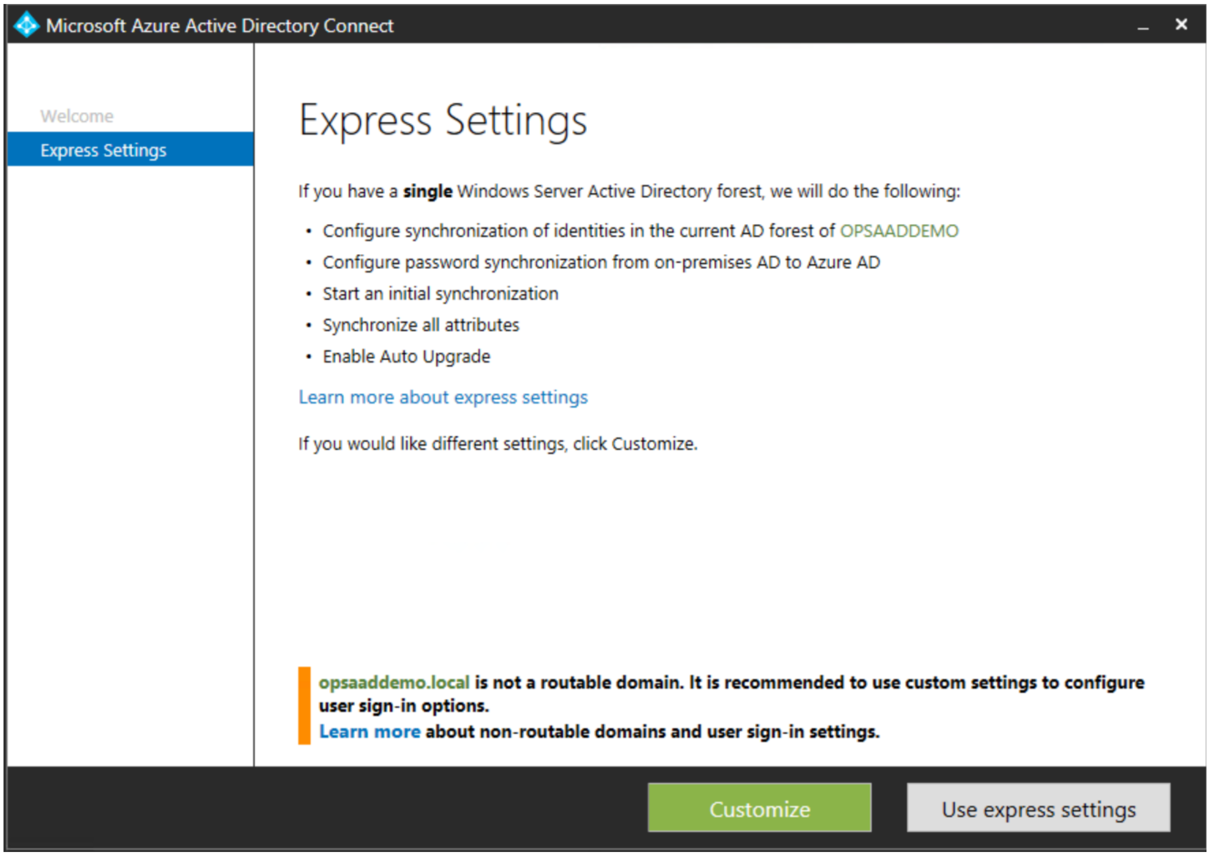
4. Wait for the PowerShell script to complete successfully (it should close automatically when finished).

5. Log on to the Azure Portal using your Azure subscription admin credentials.

6. From the Azure AD Connect section in the Azure AD settings, Click the "Download Azure AD Connect" link, to download the Azure AD Connect tool. (FYI, the direct link is this one: https://www.microsoft.com/en-us/download/details.aspx?id=47594)

7. Start the installation of the Azure AD Connect tool on the Virtual Machine domain controller in Azure. While this is not a requirement out of Azure AD Connect to be installed on a domain controller, we do this in this lab, to minimize needed resources in the Azure trial subscription.

   Overall functionality remains the same, whether AADConnect runs on a DC instead of on a member server.



Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

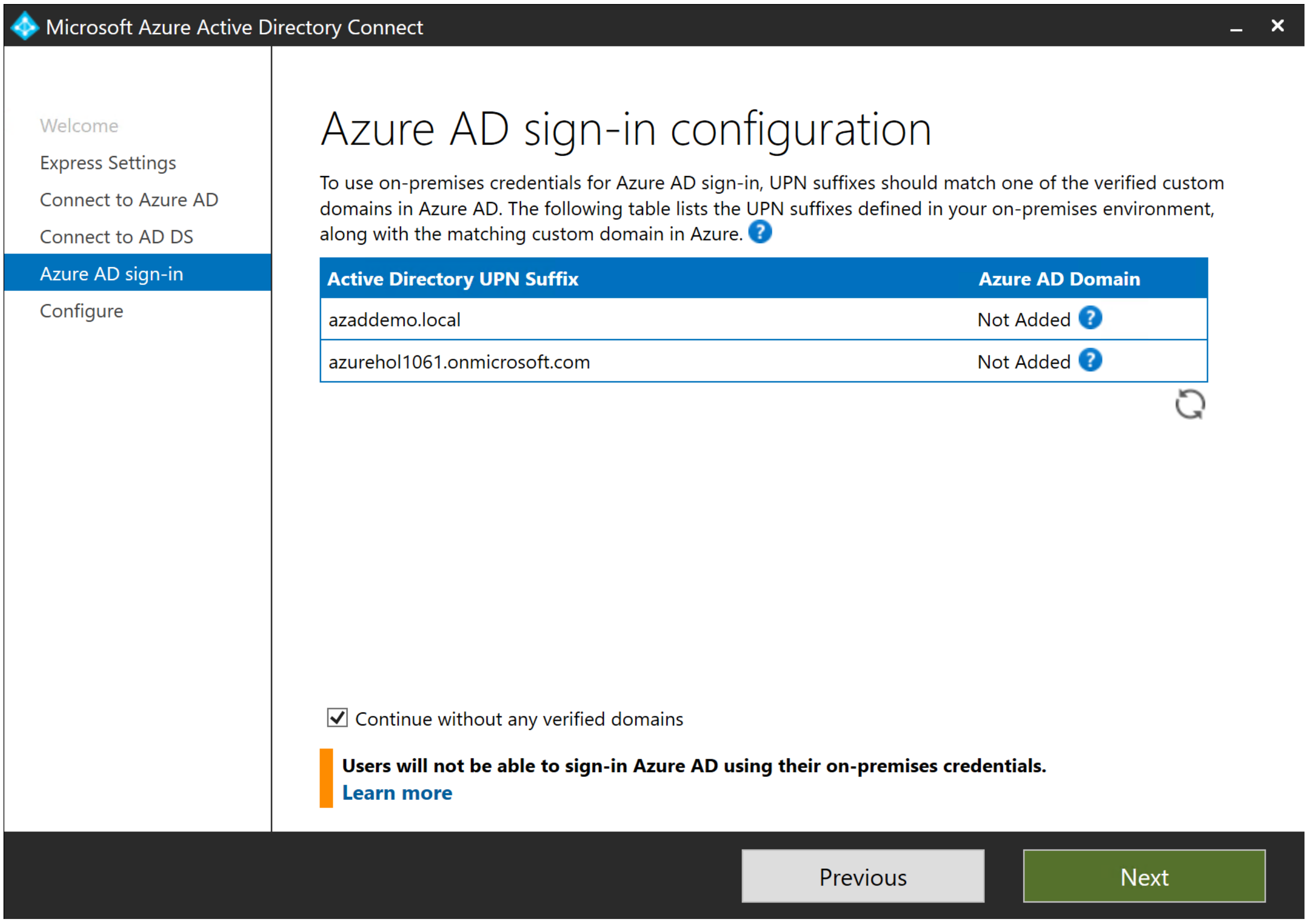
- Configure synchronization of identities in the current AD forest of OPSAADDEMO
- Configure password synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

opsaaddemo.local is not a routable domain. It is recommended to use custom settings to configure user sign-in options.
Learn more about non-routable domains and user sign-in settings.

8. Since you are running temporary demo domains in Azure Active Directory, AD Connect will warn you about using non-verified domains. Confirm this is by selecting the "Continue without any verified domains".



Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

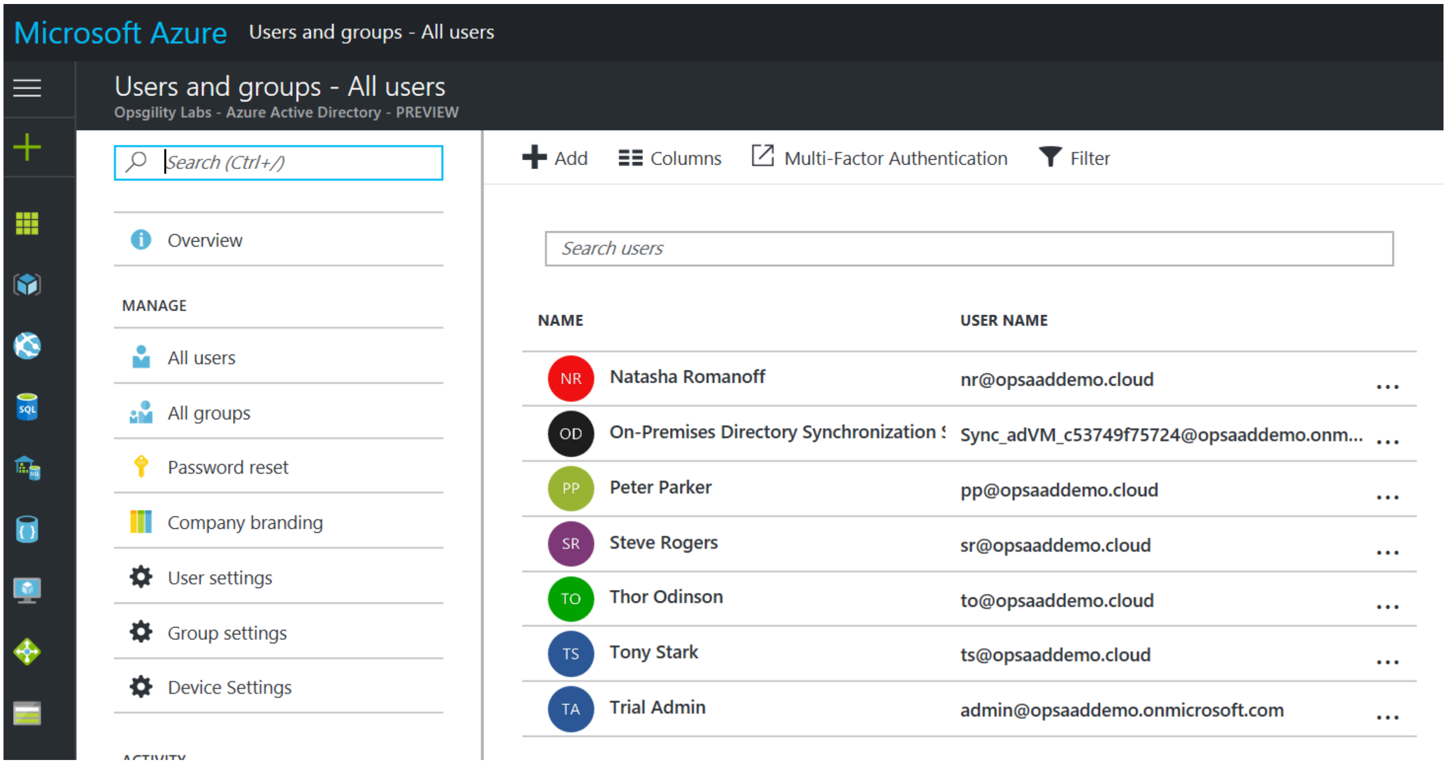
Active Directory UPN Suffix	Azure AD Domain
azaddemo.local	Not Added
azurehol1061.onmicrosoft.com	Not Added

☑ Continue without any verified domains

Users will not be able to sign-in Azure AD using their on-premises credentials.
Learn more

9. Continue the setup wizard using the default settings. Note the default behavior where Password Hash sync is set up.

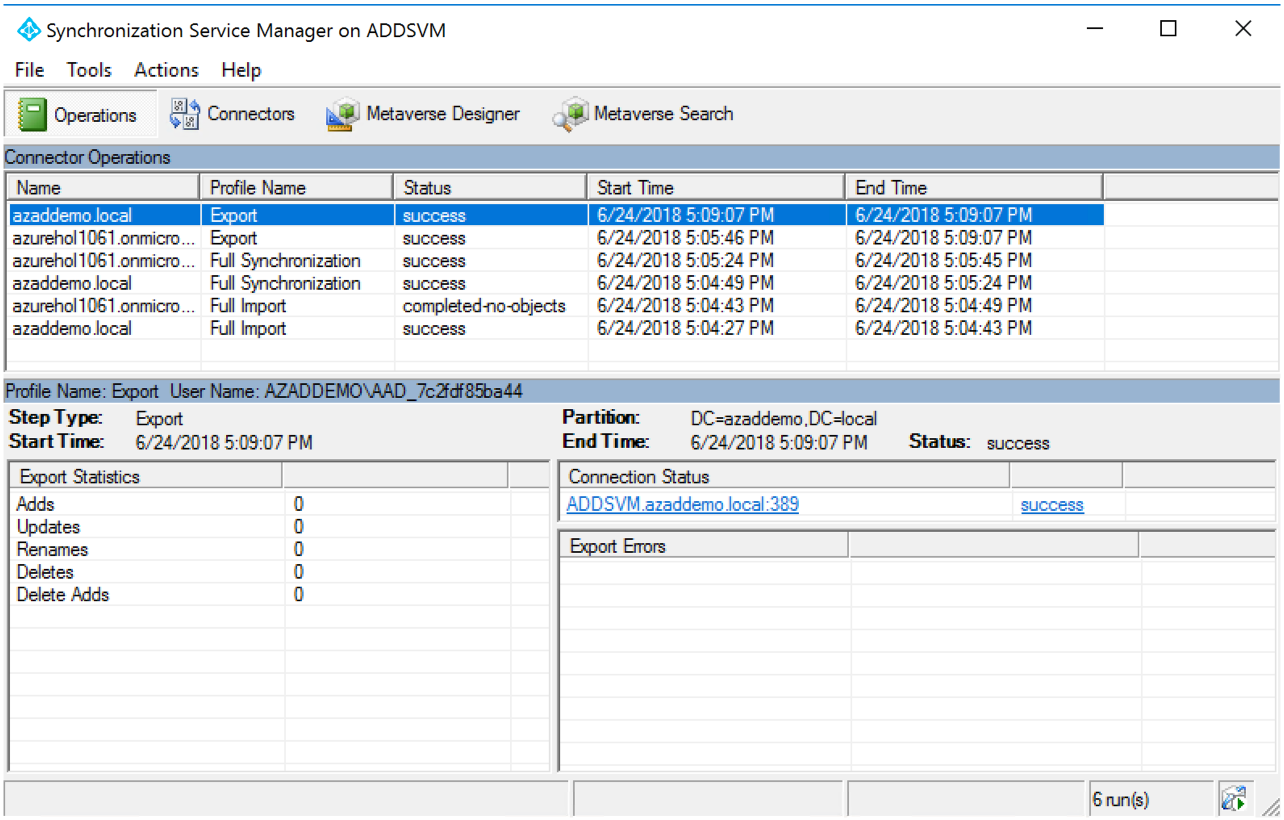
10. Finish the Express Settings, and wait for the synchronization to occur and complete. Verify from the Azure AD Portal, the users have been synchronized successfully to Azure AD



	NAME	USER NAME	
NR	Natasha Romanoff	nr@opsaaddemo.cloud	...
OD	On-Premises Directory Synchronization	Sync_adVM_c53749f75724@opsaaddemo.onm...	...
PP	Peter Parker	pp@opsaaddemo.cloud	...
SR	Steve Rogers	sr@opsaaddemo.cloud	...
TO	Thor Odinson	to@opsaaddemo.cloud	...
TS	Tony Stark	ts@opsaaddemo.cloud	...
TA	Trial Admin	admin@opsaaddemo.onmicrosoft.com	...

11. Go back to the AADConnect Server, where you will use the AADConnect Synchronization Service, which is unknown for many admins, but yet very powerful and helpful when needing to troubleshoot synchronization.

12. Start this tool from the following path: C:\Program Files\Microsoft Azure AD Sync\UIShell and start the miisclient.exe



Name	Profile Name	Status	Start Time	End Time
azaddemo.local	Export	success	6/24/2018 5:09:07 PM	6/24/2018 5:09:07 PM
azurehol1061.onmicro...	Export	success	6/24/2018 5:05:46 PM	6/24/2018 5:09:07 PM
azurehol1061.onmicro...	Full Synchronization	success	6/24/2018 5:05:24 PM	6/24/2018 5:05:45 PM
azaddemo.local	Full Synchronization	success	6/24/2018 5:04:49 PM	6/24/2018 5:05:24 PM
azurehol1061.onmicro...	Full Import	completed-no-objects	6/24/2018 5:04:43 PM	6/24/2018 5:04:49 PM
azaddemo.local	Full Import	success	6/24/2018 5:04:27 PM	6/24/2018 5:04:43 PM

Profile Name: Export User Name: AZADDEMO\AAD_7c2fdf85ba44

Step Type: Export
Start Time: 6/24/2018 5:09:07 PM
Partition: DC=azaddemo,DC=local
End Time: 6/24/2018 5:09:07 PM **Status:** success

Export Statistics	
Adds	0
Updates	0
Renames	0
Deletes	0
Delete Adds	0

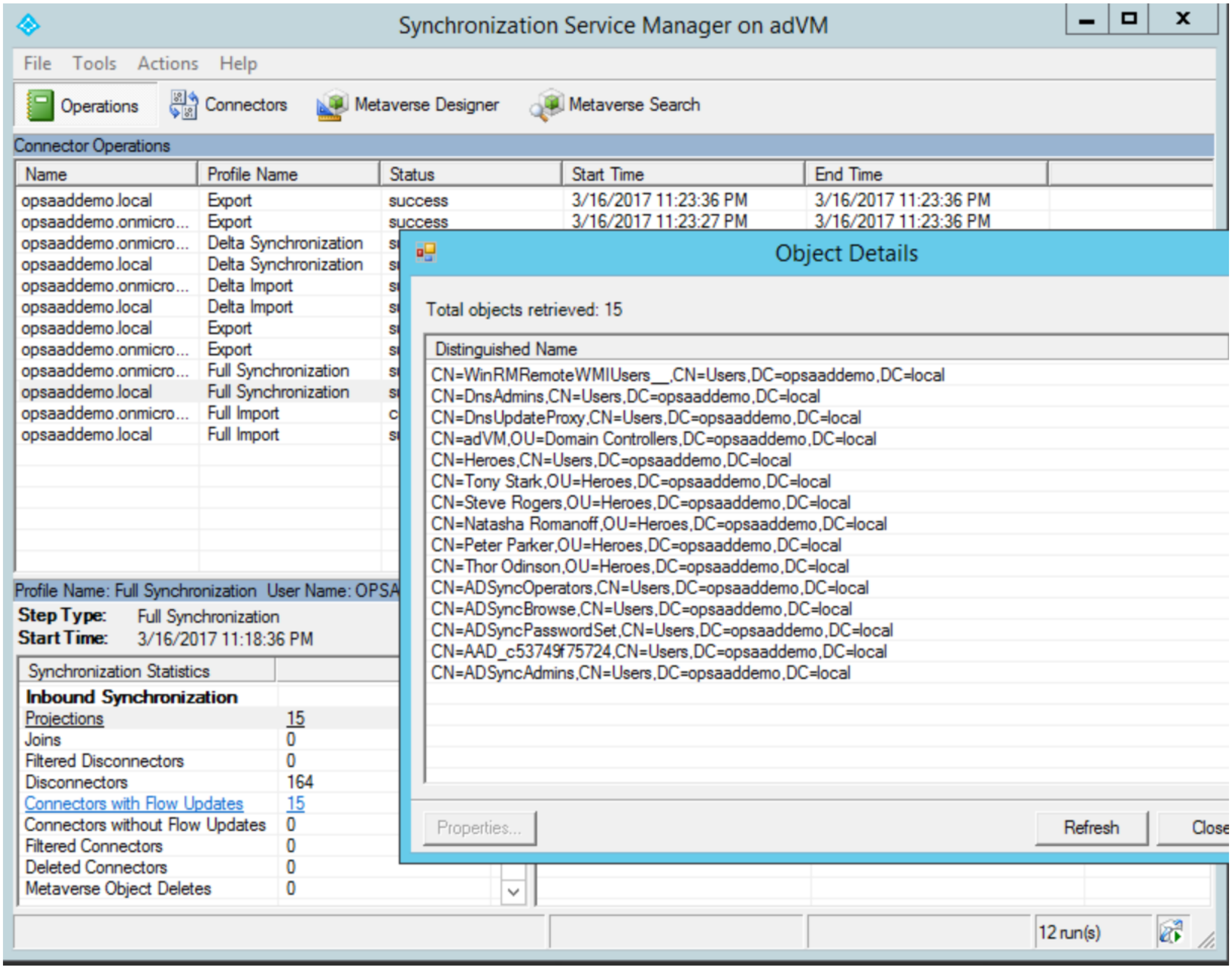
Connection Status	
ADDSVM.azaddemo.local:389	success

Export Errors

6 run(s)

- Explore the different sync cycles, like Full Import at the initial deployment, followed by intermediate delta import and sync jobs.

13. Select any of the line items having updates (number of changes) linked to it. In my demo setup, the full synchronization job had 15 updates, based on the AD Object I was having already



Connector Operations

Name	Profile Name	Status	Start Time	End Time
opsaaddemo.local	Export	success	3/16/2017 11:23:36 PM	3/16/2017 11:23:36 PM
opsaaddemo.onmicro...	Export	success	3/16/2017 11:23:27 PM	3/16/2017 11:23:36 PM
opsaaddemo.onmicro...	Delta Synchronization	s		
opsaaddemo.local	Delta Synchronization	s		
opsaaddemo.onmicro...	Delta Import	s		
opsaaddemo.local	Delta Import	s		
opsaaddemo.local	Export	s		
opsaaddemo.onmicro...	Export	s		
opsaaddemo.onmicro...	Full Synchronization	s		
opsaaddemo.local	Full Synchronization	s		
opsaaddemo.onmicro...	Full Import	c		
opsaaddemo.local	Full Import	s		

Profile Name: Full Synchronization User Name: OPSA

Step Type: Full Synchronization
Start Time: 3/16/2017 11:18:36 PM

Synchronization Statistics	
Inbound Synchronization	
Projections	15
Joins	0
Filtered Disconnectors	0
Disconnectors	164
Connectors with Flow Updates	15
Connectors without Flow Updates	0
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0

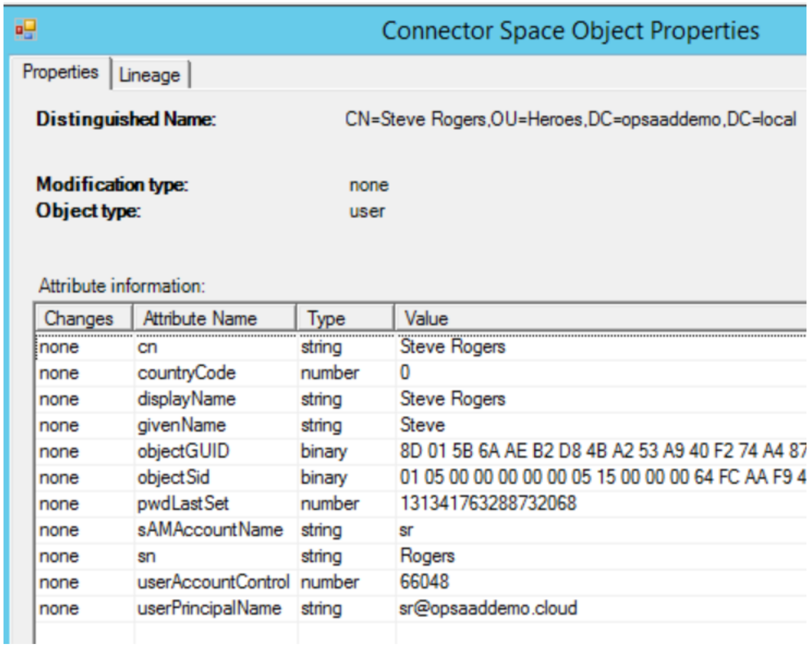
Object Details

Total objects retrieved: 15

Distinguished Name
CN=WinRMRemoteWMIUsers__,CN=Users,DC=opsaaddemo,DC=local
CN=DnsAdmins,CN=Users,DC=opsaaddemo,DC=local
CN=DnsUpdateProxy,CN=Users,DC=opsaaddemo,DC=local
CN=adVM,OU=Domain Controllers,DC=opsaaddemo,DC=local
CN=Heroes,CN=Users,DC=opsaaddemo,DC=local
CN=Tony Stark,OU=Heroes,DC=opsaaddemo,DC=local
CN=Steve Rogers,OU=Heroes,DC=opsaaddemo,DC=local
CN=Natasha Romanoff,OU=Heroes,DC=opsaaddemo,DC=local
CN=Peter Parker,OU=Heroes,DC=opsaaddemo,DC=local
CN=Thor Odinson,OU=Heroes,DC=opsaaddemo,DC=local
CN=ADSyncOperators,CN=Users,DC=opsaaddemo,DC=local
CN=ADSyncBrowse,CN=Users,DC=opsaaddemo,DC=local
CN=ADSyncPasswordSet,CN=Users,DC=opsaaddemo,DC=local
CN=AAD_c53749f75724,CN=Users,DC=opsaaddemo,DC=local
CN=ADSyncAdmins,CN=Users,DC=opsaaddemo,DC=local

14. Select “Projections”, which opens up the list of objects retrieved. Notice you recognize the user accounts from the AD OU, by their CommonName.

15. Selecting any of the line items / Properties, shows the detailed parameters for the given object



Distinguished Name: CN=Steve Rogers,OU=Heroes,DC=opsaaddemo,DC=local

Modification type: none
Object type: user

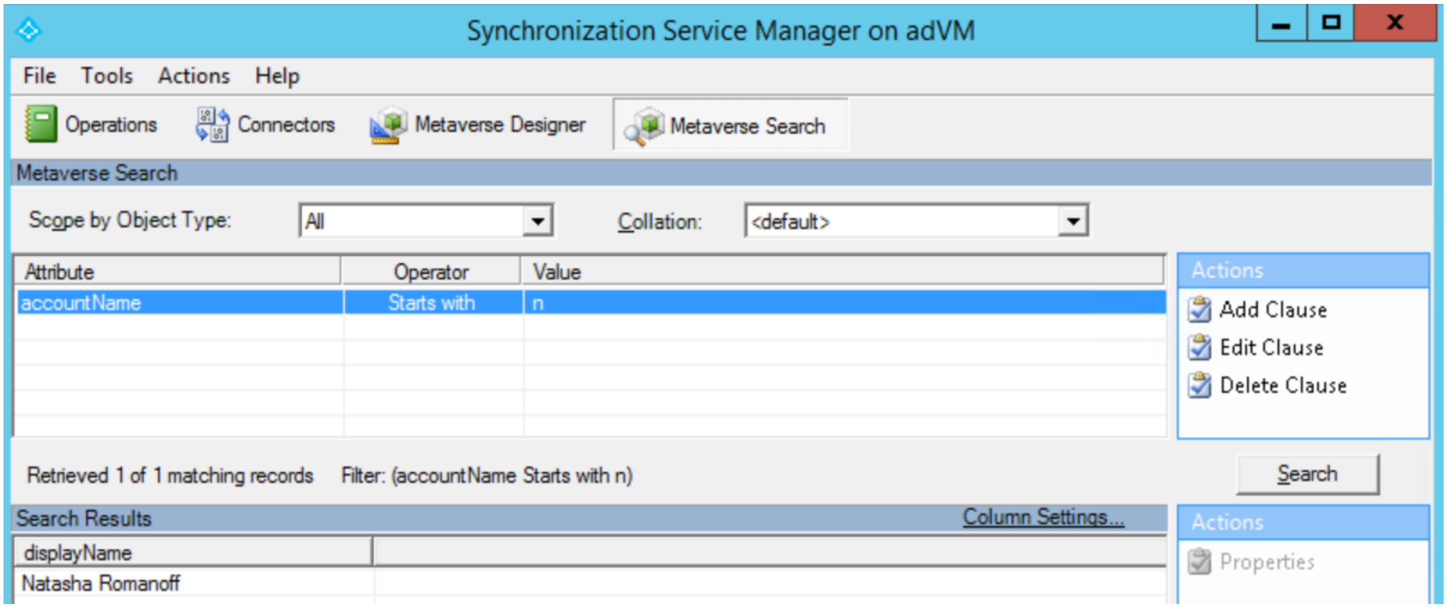
Attribute information:

Changes	Attribute Name	Type	Value
none	cn	string	Steve Rogers
none	countryCode	number	0
none	displayName	string	Steve Rogers
none	givenName	string	Steve
none	objectGUID	binary	8D 01 5B 6A AE B2 D8 4B A2 53 A9 40 F2 74 A4 87
none	objectSid	binary	01 05 00 00 00 00 00 05 15 00 00 00 64 FC AA F9 4
none	pwdLastSet	number	131341763288732068
none	sAMAccountName	string	sr
none	sn	string	Rogers
none	userAccountControl	number	66048
none	userPrincipalName	string	sr@opsaaddemo.cloud

16. Close the popup windows, until you are back at the home screen of the Synchronization Service tool. Here, click on the “Metaverse Search” button, followed by selecting Ädd Clause”. In the conditions,

- select attribute=accountname;
- operator = starts with
- value = n

The result will show all users starting with a “n” in their displayName filed, out of my demo environment.



Scope by Object Type: All

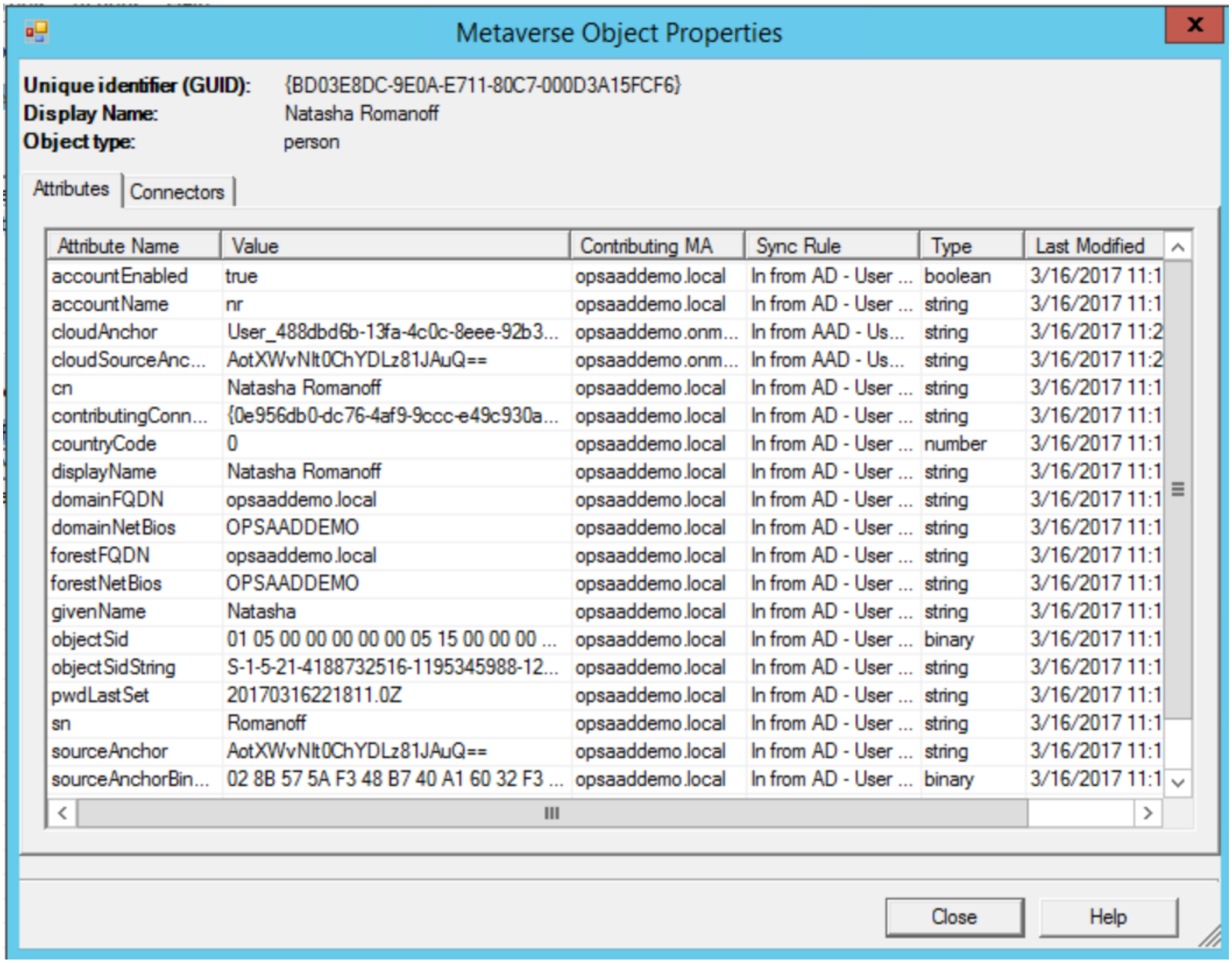
Collation: <default>

Attribute	Operator	Value
accountName	Starts with	n

Retrieved 1 of 1 matching records Filter: (accountName Starts with n)

displayName
Natasha Romanoff

17. Select the user / properties, which will expose more detailed parameters for the given user account:



Unique identifier (GUID): {BD03E8DC-9E0A-E711-80C7-000D3A15FCF6}
Display Name: Natasha Romanoff
Object type: person

Attributes | Connectors

Attribute Name	Value	Contributing MA	Sync Rule	Type	Last Modified
accountEnabled	true	opsaaddemo.local	In from AD - User ...	boolean	3/16/2017 11:1
accountName	nr	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
cloudAnchor	User_488dbd6b-13fa-4c0c-8eee-92b3...	opsaaddemo.onm...	In from AAD - Us...	string	3/16/2017 11:2
cloudSourceAnc...	AotXWvNIt0ChYDLz81JAuQ==	opsaaddemo.onm...	In from AAD - Us...	string	3/16/2017 11:2
cn	Natasha Romanoff	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
contributingConn...	{0e956db0-dc76-4af9-9ccc-e49c930a...	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
countryCode	0	opsaaddemo.local	In from AD - User ...	number	3/16/2017 11:1
displayName	Natasha Romanoff	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
domainFQDN	opsaaddemo.local	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
domainNetBios	OPSAADDEMO	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
forestFQDN	opsaaddemo.local	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
forestNetBios	OPSAADDEMO	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
givenName	Natasha	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
objectSid	01 05 00 00 00 00 00 05 15 00 00 00 ...	opsaaddemo.local	In from AD - User ...	binary	3/16/2017 11:1
objectSidString	S-1-5-21-4188732516-1195345988-12...	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
pwdLastSet	20170316221811.0Z	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
sn	Romanoff	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
sourceAnchor	AotXWvNIt0ChYDLz81JAuQ==	opsaaddemo.local	In from AD - User ...	string	3/16/2017 11:1
sourceAnchorBin...	02 8B 57 5A F3 48 B7 40 A1 60 32 F3 ...	opsaaddemo.local	In from AD - User ...	binary	3/16/2017 11:1

Emphasize again how this operation can help in pinpointing the reason why a given user / users are not being synchronized to Azure AD.

This completes the exercise of Module 2, in which you learned about Azure AD Connect.