Issue: My organization was using AD connect to sync users to Azure AD. Mentioned bellow settings were in use

- Password Hash Sync
- Password Write Back
- ms-DS-ConsistencyGuid

In a ransomware attack all domain controllers AD sync server and backups are compromised. We rebuilt the domain controllers with same forest and domain names, but the SID is changed. We have recreated the users with same display name and UPN as on the previous domain controller.

We are utilizing M365 for Teams, emails etc.

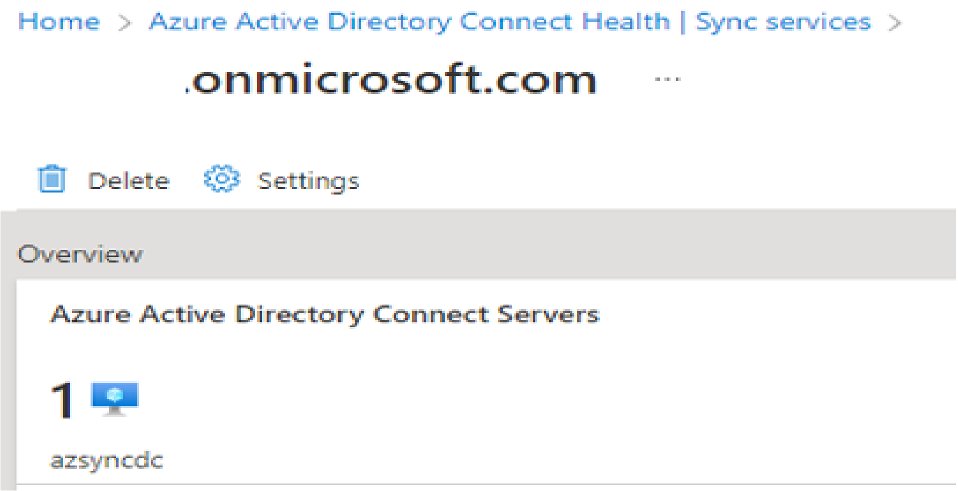
Objective: Restore the syncing of AD users to Azure AD from the newly created domain.

Note: On-prem requirements are not covered on this.

Solution: Solution will be executed in four steps

- Converting Ad Synced users into Cloud Users.
- Hard match for the users that we need to be resynced.
- Running Pilot Sync Batch
- Examine restored M365 services
- Cleanup of old AD Connect Servers

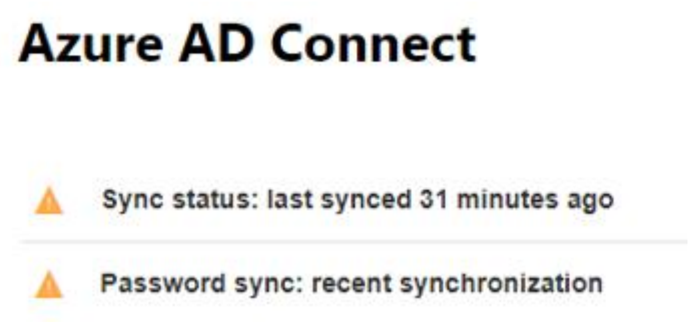
Before starting the resolution steps its important to check and verify the existing state of Azure AD Tenant.


Home > Azure Active Directory Connect Health | Sync services >
.onmicrosoft.com ...
Delete
Settings
Overview

Azure Active Directory Connect Servers

1

azsyncdc



Azure AD Connect

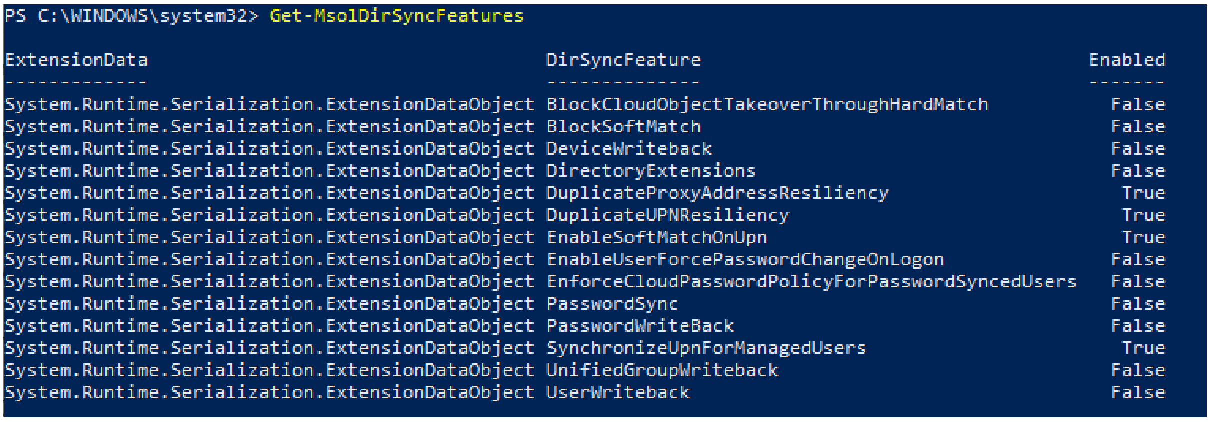
Sync status: last synced 31 minutes ago

Password sync: recent synchronization

ou1user1
ou1user1(
Microsoft 365 E5 Developer (without Windows and Audio

Converting Ad Synced users into Cloud Users.

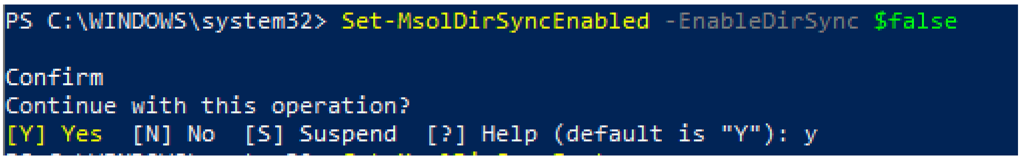
In this step we will disable the AD sync service via PowerShell. It can take up to 72 hours depending on the numbers of users in my lab setup for 5 users it was done under 10 minutes.



```
PS C:\WINDOWS\system32> Get-MsolDirSyncFeatures

ExtensionData                                    DirSyncFeature                                    Enabled
-------------                                    --------------                                    -------
System.Runtime.Serialization.ExtensionDataObject BlockCloudObjectTakeoverThroughHardMatch            False
System.Runtime.Serialization.ExtensionDataObject BlockSoftMatch                                      False
System.Runtime.Serialization.ExtensionDataObject DeviceWriteback                                     False
System.Runtime.Serialization.ExtensionDataObject DirectoryExtensions                                 False
System.Runtime.Serialization.ExtensionDataObject DuplicateProxyAddressResiliency                      True
System.Runtime.Serialization.ExtensionDataObject DuplicateUPNResiliency                               True
System.Runtime.Serialization.ExtensionDataObject EnableSoftMatchOnUpn                                 True
System.Runtime.Serialization.ExtensionDataObject EnableUserForcePasswordChangeOnLogon                False
System.Runtime.Serialization.ExtensionDataObject EnforceCloudPasswordPolicyForPasswordSyncedUsers    False
System.Runtime.Serialization.ExtensionDataObject PasswordSync                                        False
System.Runtime.Serialization.ExtensionDataObject PasswordWriteBack                                   False
System.Runtime.Serialization.ExtensionDataObject SynchronizeUpnForManagedUsers                        True
System.Runtime.Serialization.ExtensionDataObject UnifiedGroupWriteback                               False
System.Runtime.Serialization.ExtensionDataObject UserWriteback                                       False
```

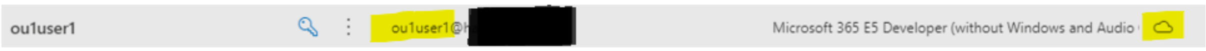
Set-MsolDirSyncEnabled –EnableDirSync $false



```
PS C:\WINDOWS\system32> Set-MsolDirSyncEnabled -EnableDirSync $false

Confirm
Continue with this operation?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
```

After some depending on the numbers of user ad synced accounts will be converted to cloud only accounts and they will keep the same password as of on-prem when they were last synced.

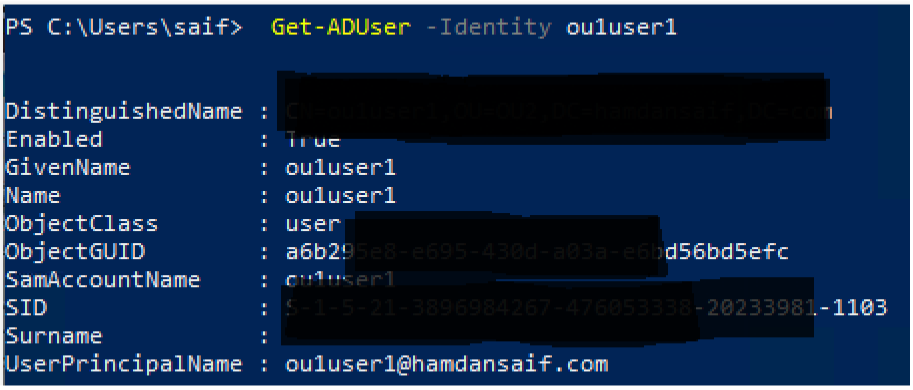


Hard match for the users that we need to be resynced

Install the new AD connect server with required setting and then proceed for Hard Match. Hard match can also be done prior to the new AD connect Installation.

On the Domain Controller open a PowerShell window and run the command Import-Module Active Directory

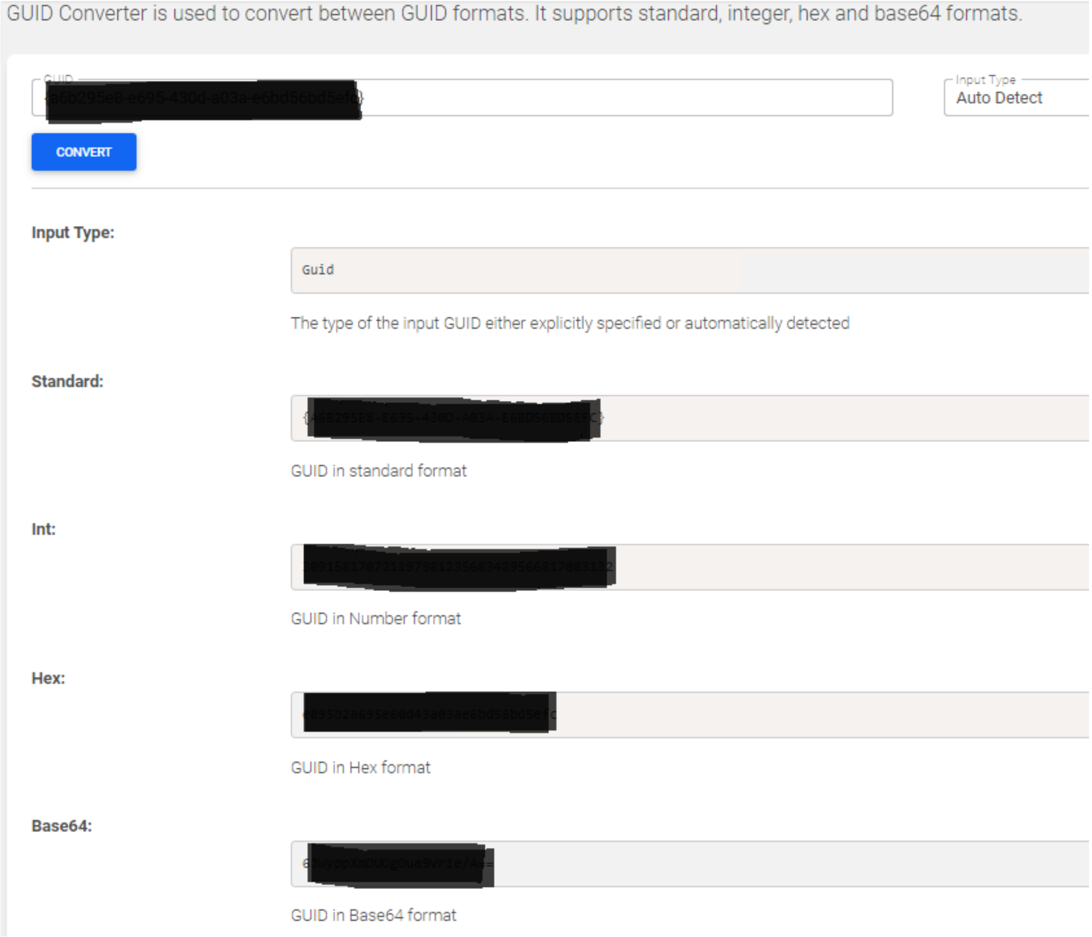
Run the command Get-ADUser -Identity “Enter Local AD logon ID in these quotes” once you run the above command you should be able to see an output like this:



```
PS C:\Users\saif>  Get-ADUser -Identity ou1user1


DistinguishedName : [redacted]
Enabled           : [redacted]
GivenName         : ou1user1
Name              : ou1user1
ObjectClass       : user
ObjectGUID        : a6b29[redacted]d56bd5efc
SamAccountName    : [redacted]
SID               : [redacted]-1103
Surname           :
UserPrincipalName : ou1user1@hamdansaif.com
```

Now copy the object GUID from the output and open the website https://toolslick.com/conversion/data/guid and paste the same on the textbox as shown in the image and click on convert, you should be getting the B64 value and copy the same. Make sure that there are no spaces when you paste the value in the textbox.



GUID Converter is used to convert between GUID formats. It supports standard, integer, hex and base64 formats.

GUID: [redacted]

Input Type: Auto Detect

Input Type: Guid

The type of the input GUID either explicitly specified or automatically detected

Standard: [redacted]

GUID in standard format

Int: [redacted]

GUID in Number format

Hex: [redacted]

GUID in Hex format

Base64: [redacted]

GUID in Base64 format

Although, there are other ways to get the Base64 value from a GUID I recommend this approach as it is simple, you can get the same results from PowerShell.

$user = "ou1user1@-----.com"

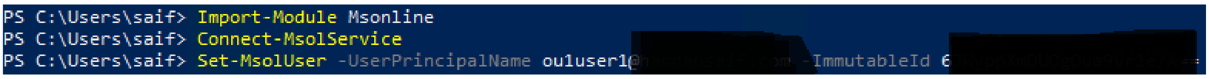
$guid = [guid]((Get-ADUser -Identity "$user").objectGuid)

$immutableId = [System.Convert]::ToBase64String($guid.ToByteArray())

Now in open PowerShell so we connect to cloud & run the command **Import-Module MSOnline**

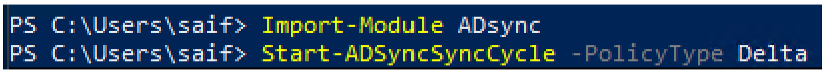
Then run the command **Connect-MSOLService** you should be seeing a prompt to enter credentials, enter the office 365 global admin credentials here.

Once you remove the account run the command **Set-MsolUser -UserPrincipalName user@abc.com -ImmutableId QX00ApTUDEiiEm5kX0WP2w==** , here you need to enter the UPN /Signin address of office 365/azure AD against which you wish to perform a hard match and after the -immutableID flag enter the B64 value that you copied from https://toolslick.com/conversion/data/guid



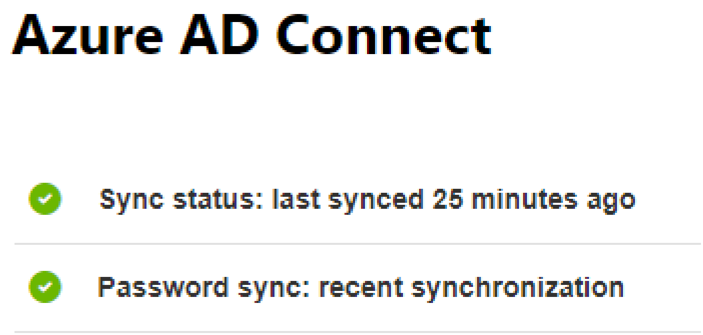
```
PS C:\Users\saif> Import-Module Msonline
PS C:\Users\saif> Connect-MsolService
PS C:\Users\saif> Set-MsolUser -UserPrincipalName ou1user1@[redacted] -ImmutableId 6[redacted]
```

Once this is done run a delta sync



```
PS C:\Users\saif> Import-Module ADsync
PS C:\Users\saif> Start-ADSyncSyncCycle -PolicyType Delta
```

Check AD Connect status

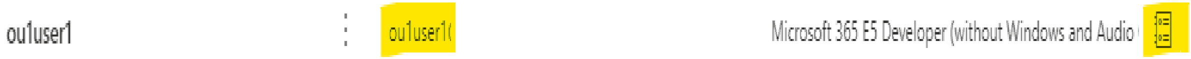


Azure AD Connect

✓ Sync status: last synced 25 minutes ago

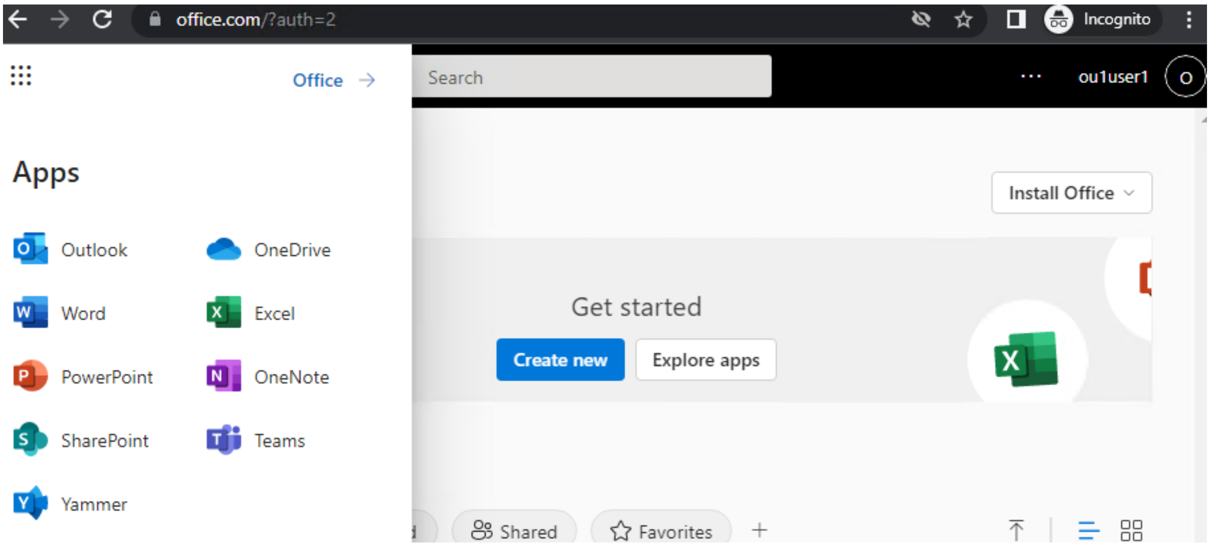
✓ Password sync: recent synchronization

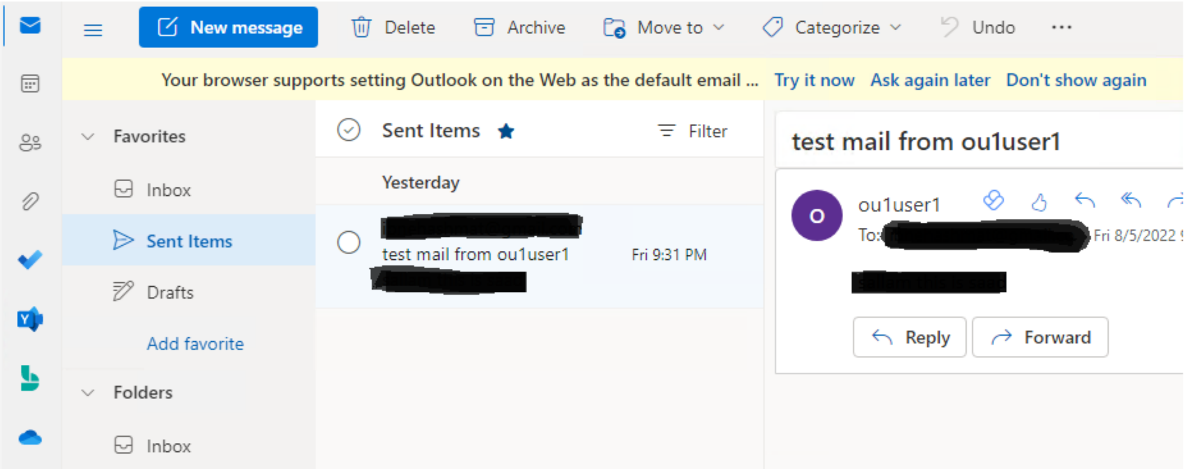
Check the sync status of the user



ou1user1 ⋮ ou1user1(Microsoft 365 E5 Developer (without Windows and Audio

Login into the user account to verify mailbox, Teams etc.





Your browser supports setting Outlook on the Web as the default email ... Try it now Ask again later Don't show again

Sent Items

Yesterday

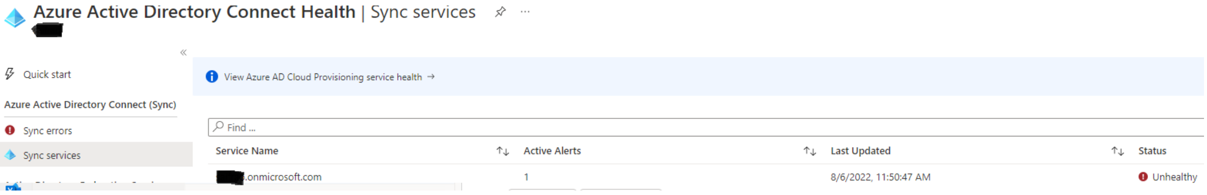
[redacted]
test mail from ou1user1 Fri 9:31 PM
[redacted]

test mail from ou1user1

ou1user1
To: [redacted] Fri 8/5/2022

[redacted]

Go to AD connect in portal.azure to check the sync services health



Azure Active Directory Connect Health | Sync services

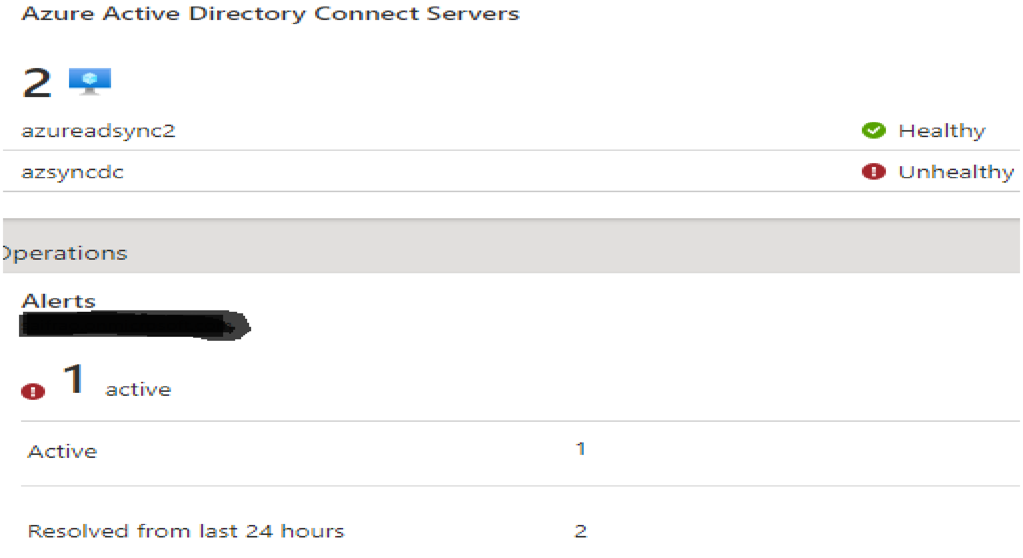
[redacted]

View Azure AD Cloud Provisioning service health →

Find ...

Service Name	Active Alerts	Last Updated	Status
[redacted].onmicrosoft.com	1	8/6/2022, 11:50:47 AM	Unhealthy

We can see both old and new AD connect server listed here. Old one is in unhealthy state.



Azure Active Directory Connect Servers

2

azureadsync2	Healthy
azsyncdc	Unhealthy

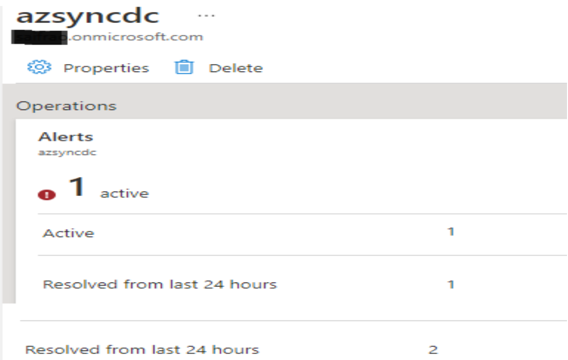
Operations

Alerts
[redacted]

1 active

Active	1
Resolved from last 24 hours	2

We will open the old AD connect and delete it.



azsyncdc
[redacted].onmicrosoft.com

Operations

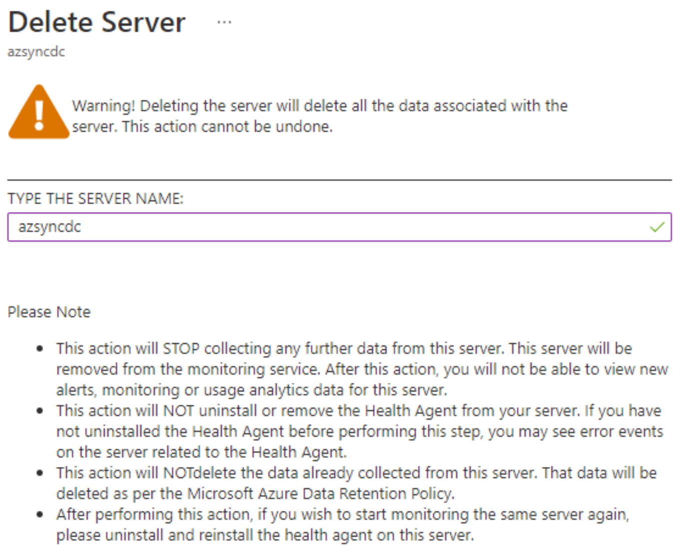
Alerts
azsyncdc

1 active

Active	1
Resolved from last 24 hours	1

Resolved from last 24 hours	2

You will receive a challenge screen when you press the delete icon



Delete Server ···

azsyncdc

Warning! Deleting the server will delete all the data associated with the server. This action cannot be undone.

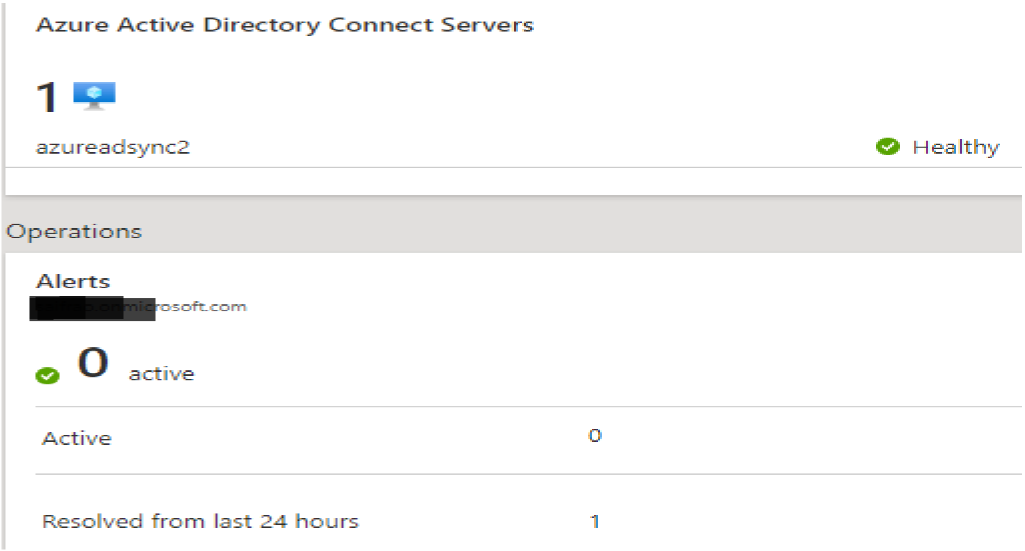
TYPE THE SERVER NAME:

azsyncdc ✓

Please Note

- This action will STOP collecting any further data from this server. This server will be removed from the monitoring service. After this action, you will not be able to view new alerts, monitoring or usage analytics data for this server.
- This action will NOT uninstall or remove the Health Agent from your server. If you have not uninstalled the Health Agent before performing this step, you may see error events on the server related to the Health Agent.
- This action will NOTdelete the data already collected from this server. That data will be deleted as per the Microsoft Azure Data Retention Policy.
- After performing this action, if you wish to start monitoring the same server again, please uninstall and reinstall the health agent on this server.

We can now see the new AD connect listed.



Azure Active Directory Connect Servers

1

azureadsync2 ✓ Healthy

Operations

Alerts

[redacted]rosoft.com

✓ 0 active

Active	0
Resolved from last 24 hours	1