Here is a scenario, You are assigned a task to move users from source AD forest to target AD forest where both forests have AADconnect deployed. Did that get you thinking? Well it should, Here is brief summary of what i went through:

As part of office 365 Tenant to Tenant migration; the objective was to migrate users between on-premises Active directory forests first; sync the users so migrated with destination office 365 Tenant and then finally use MigrationWiz (Email Migration tool) to copy emails from source tenant to destination Tenant.

The client used Quest AD migration tool for migrating users accounts from source forest to destination forest, the catch here was that the client did not exclude ‘**MS-DS-ConsistencyGuid**‘ attribute from being copied. Before we dive into why it mattered, lets take a look at the issue we faced after the user was successfully migrated between on-premises forests. Soon after synchronizing the user object with Target tenant AADconnect started throwing an error like:

**“sync-rule-error-function-triggered”**

A similar screenshot from MS article:

Text, table

Description automatically generated

Upon clicking the error and navigating to ‘Synchronization errors’ I was presented with the error: **“Source Anchor attribute has changed”**. Before we drill into the fix lets recap around how the MS-DS-ConsistencyGuid is populated:

To oversimplify things in a standalone forest, ObjectGuid=MS-DS-ConsistencyGuid=ImmutableID ; This is easily the most common configuration depending on the sourceanchor; Without getting into weeds around metaverse etc. AADconnect provisions users in the following manner:

* AADConnect Grabs a users ObjectGuid (on-premises) converts it into Binary and Dumps it into Ms-Ds-consistencyGuid.
* AADconnect stamps the value from ms-ds-consistencyGuid (on-premises) into ImmutableID (in-cloud) post converting it into base 64.

Earlier the equation was simply objectGuid=ImmutableID, Microsoft intelligently introduced Ms-DS-consistencyGuid as a middle man to maintain a sync state in office 365 when a user is moved cross forest and his objectID changes. However, one should carefully examine the impact around choosing to migrate ms-ds-consistencyGuid when a cross forest migration is to be performed. In my case for example the situation was rather weird:

ObjectGuid=ImmutableID ≠Ms-Ds-ConsistencyGuid.

Upon drilling further it was revealed that following two attributes were copied as part of cross-forest user migration using quest: **mS-DS-ConsistencyGuid’ & ‘msDS-ExternalDirectoryObjectId’** which resulted in inconsistent behavior with AADconnect already running in the target forest. AADconnect basically did its own calculation of ms-ds-consistencyGuid based on objectGuid which got overwritten by the ms-ds-consistencyGuid in source forest and thus broke the correlation between the on-premises and the cloud object.

**The Fix:**

In my scenario i had to get from ObjectGuid=ImmutableID ≠Ms-Ds-ConsistencyGuid to ObjectGuid=ImmutableID=Ms-Ds-ConsistencyGuid for about 100 users. The cloud objects had mailboxes associated with them, so i did not had the luxury to start over. Fortunately ms-ds-consistencyGuid is a writeable attribute and all i had to do was match the ms-ds-consistencyGuid with the corresponding objectID for each object. Here are the steps that i followed:

* Disable sync scheduler temporarily: **Set-ADSyncScheduler -SyncCycleEnabled $false**
* Confirm that the immutableID in cloud matches the objectID and not the ms-ds-consistencyGuid. The easiest way is to pull a dump using Ldifde via command prompt on a domain controller:

|  |  |
| --- | --- |
| 1 | ldifde -f export.txt -r "(Userprincipalname=\*)" -l "objectGuid, userPrincipalName, ms-ds-consistencyguid" |

The output from ldifde looked somewhat like this, in a glance it gives you the needed info on-preemies:

Text

Description automatically generatedSample only.

* Next pull out a dump from office 365 to compare what Immutable ID is stamped against the users in office 365:

|  |  |
| --- | --- |
| 1 | Get-msoluser -userprincipalname user1@domain.com | select userprincipalname,ImmutableID |

Once i was sure that the ImmutableID is same as ObjectGuid and i have to just change the Ms-ds-consistencyGuid to match them all, i used the following command to fix all the users in bulk:

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | $f= Import-Csv Useron-premSAM.csv  **foreach**($u **in** $f)  {  $user = Get-ADUser $u.samaccountname  Set-ADUser $user -Replace @{ "ms-Ds-ConsistencyGuid" = $user.ObjectGUID.ToByteArray() }  } |

To use the above command i already had compiled a csv of users that needed fixing based on their SAMaccountName. SamAccountname here is the header in the csv. To run it against a single user you can use:

|  |  |
| --- | --- |
| 1  2 | $brokenuser = Get-ADUser UserSamAccountName  Set-ADUser $brokenUser -Replace @{ "ms-Ds-ConsistencyGuid" = $brokenUser.ObjectGUID.ToByteArray() } |

* Run a full sync: Start-ADSyncSyncCycle -PolicyType Initial
* Turn the sync scheduler back on: Set-ADSyncScheduler -SyncCycleEnabled $True

And that was it !