


- Preparing Your On-Prem AD for Microsoft Entra Connect (formerly Azure AD Connect)



Clean Before You Sync – Real-World Checklist for Hybrid Identity

- Perparim Abdullahu – AZ-305 Certified | SC-300 in Progress







Why Cleaning Up Is Critical

Before syncing your on-prem domain with Microsoft Entra ID (formerly Azure AD), do a health check. Dirty AD = sync failures, identity mismatches, and hours of cleanup later.



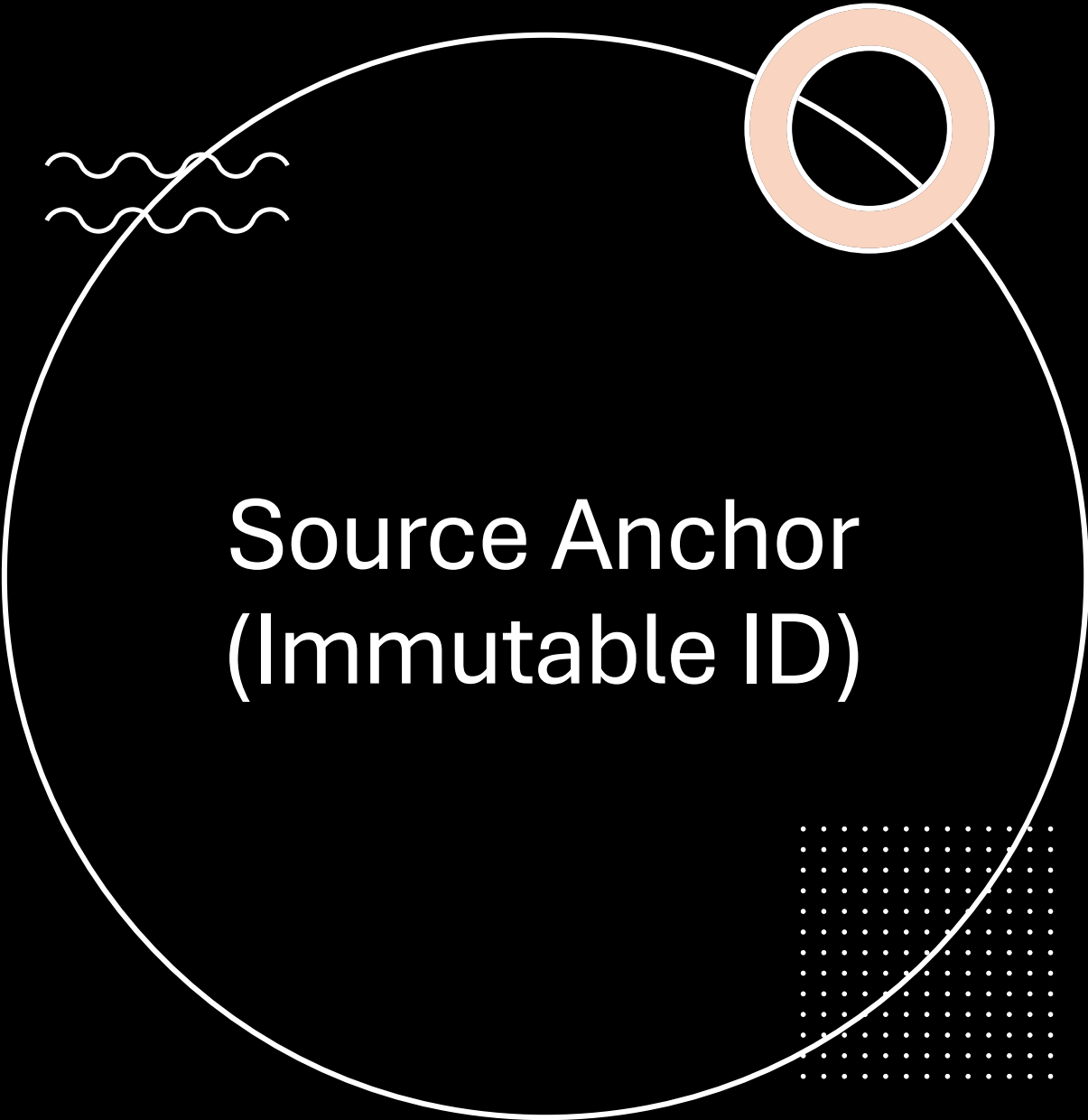
```
mirror_mod = modifier_ob.  
# Add mirror object to mirror  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
  
# Selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob.  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
  
print("please select exactly  
  
-- OPERATOR CLASSES ----  
  
types.Operator):  
on X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
  
context):  
context.active_object is not
```

Tools to Use Before Syncing

-  **IDFix** – detects illegal characters, duplicates, UPN issues
-  **dcdiag** / AD logs – checks for replication or sync errors
-  Remove stale users, computer accounts, groups, and service accounts
-  Focus on last **100 days** of errors (Microsoft's recommendation)

Plan for Failover – Don't Risk a Single Point of Failure

- Only **1 active Microsoft Entra Connect (formerly AAD Connect) server** allowed
- Add a **Staging Mode Server** as passive standby
- Or use **virtualization + live migration**
- Staging mode is enabled during setup (checkbox in the wizard)



Source Anchor (Immutable ID)

🔗 On-prem + cloud users must be matched.

Source Anchor = unchangeable ID that links both sides.

- Typically: ms-DS-ConsistencyGuid
- Chosen during Microsoft Entra Connect (formerly AAD Connect) setup
- Ensures consistent sync even after failover



UPN Matters Too

UPN (email-style login)
must also match across
environments.

Example:
jdoe@perparimlab.com

Fix broken/missing
UPNs before syncing

Use custom UPN
suffixes if needed

Final Checklist Before You Sync

- ✓ Run IDFix
- ✓ Review event logs
- ✓ Remove stale accounts
- ✓ Choose Source Anchor
- ✓ Enable staging mode server (optional but recommended)
- ✓ Align UPNs for all users



My Takeaway

- In real-world hybrid identity rollouts, cleanup **before** sync is critical. A few hours of prep avoids days of headaches.

- Perparim Abdullahu – AZ-305-Certified | SC-300 in Progress