Objective: Create Azure (Entra) Connect AD Connect server in stagging mode.

Equipment:

Keepass

Member server

Admin access to all required resources to perform required work in on-prem Windows Active Directory, member server, and entra.microsoft.com MS Entra Admin Portal.

Procedures:

1. Click on app and select install, agree, and click on Customize. Refer to figure 1.0.

| mponent will be r federation with AD |
|--|
| mponent will be r federation with AD |
| r federation with AD |
| r federation with AD |
| r federation with AD |
| |
| ed for deployment |
| ange what data is |
| |
| |
| |
| |
| |
| |
| |

Figure 1.0 Initial setup

- 2. When Azure AD Connect app comes up, click on Customize. Refer to figure 1.1.
- 3. From "Install required components" GUI, click on Import synchronization settings. Refer to figure 1.2.
- 4. Browse to your downloads area for the Exported-SynchronizationPolicy, then click on Install. Refer to figure 1.2.

| Welcome | install required components | | | | | | |
|---|---|--|--|--|--|--|--|
| Express Settings Required Components Jser Sign-In | No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. ? | | | | | | |
| | Specify a custom installation location Use an existing SQL Server | | | | | | |
| | Use an existing service account Specify custom sync groups | | | | | | |
| | ✓ Import synchronization settings SETTINGS LOCATION | | | | | | |
| | C:\Exported-SynchronizationPolicy-20240110-090235.json Browse | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Figure 1.2 Import SynchronizationPolcy from non-stagging AADC server

Notes: install process is creating Azure local groups and local services. For ADSyncAdmins, verify correct domain groups are in there for this to work. Do a comparison with other AADC production servers.

5. From the "User sign-in" GUI, select Password Has Synchronization and click Next. Refer to figure 1.3.



Figure 1.3 Password Has Synchronization

6. From the "Connect to Azure AD" GUI, enter specific user credentials and click Next. Refer to figure 1.4.



Figure 1.4 Enter specific user credentials

7. From "Connect your directories" GUI, click on Change Credentials. Refer to figure 1.5.



Figure 1.5 Change Credentials

8. From AD forest account GUI, specific credentials and click OK. Refer to figure 1.6.

AzureADConnectStaggingServer-Public

| Welcome | Con | nect your directories | | | | |
|--|---|--|---------------------------|--|--|--|
| Express Settings Required Components User Sign-In Connect to Azure AD Sync | Enter co DIRECTC Active FOREST | AD forest account AD forest account An AD account with sufficient permissions is required for periodic s connect can create the account for you. Alternatively, you may pro- | synchronization. Azure AD | | | |
| Connect Directories | ms.ccsf | the required permissions. Learn more about managing account permissions. | | | | |
| Configure | CONFIGI ms. : | The first option is recommended and requires you to enter Enterpr Select account option. O Create new AD account O Use existing AD account DOMAIN USERNAME T PASSWORD T T T T T T T T T T T T T | ise Admin credentials. | | | |
| | | ок | Cancel | | | |

Figure 1.6 Use existing AD account

9. From "Connect your directories" GUI, verify Configured Directories area is green and click Next. Refer to figure 1.7.



Figure 1.7 Configured Directories is green

10. From "Ready to configure" GUI, verify 2 displayed parameters are select and click Install. Refer to figure 1.8.



Figure 1.8 AADC stagging mode

11. Wait for install to complete and verify similar to figure 1.9 is displayed, then click Exit.



Figure 1.9 Complete

- 12. From stagging server, bring up computer management.
- 13. Go to Groups, then click on ADSync Admins.
- 14. Verify your setup matches what is displayed from figure 2.0.

| ADSyncAdmins Properties ? X | | | | | | |
|---|--------------------------|-----------------------------------|--|------------------------|-----------|--|
| General | | | | | | |
| ADSyncAdmins | | | | | | |
| Description: | ADSyncAdm | nins | | | | |
| Members: | | | | | | |
| Sector S | rise Admins onnectDir | | | | | |
| Add | Remove | Changes are not e user logs | to a user's group ffective until the r on. | nembers next time t | hip he | |
| (| ОК | Cancel | Apply | He | elp | |

Figure 2.0 members of ADSync Admins

- 15. Reboot server.
- 16. RDC into stagging server when it is up again.
- 17. Check on services and verify "Microsoft Azure AD Sync" is running. If is not enter the password for it, and restart the service.
- 18. From the server, check Azure AD Connect Synchronization Service is running by click on More, then Run as administrator. Refer to figure 2.1

| Synchronization Se | rvice Manager on T | F-AZRSYNC-01 | | | - C |) × |
|---|---|--|---|---|----------|-----|
| Operations | Connectors 🧕 Me | taverse Designer | 🚇 Metaverse Search | | | |
| onnector Operations | | | • | | | |
| Name | Profile Name | Status | Start Time | End Time | | |
| citycollegesf onmicros | Delta Synchronization | success | 1/11/2024 10:05:53 AM | 1/11/2024 10:05:53 AM | | |
| onmicros | Delta Synchronization Delta Import Pull Synchronization Full Synchronization Full Import Full Import | SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS | 1/11/2024 10:05:52 AM 1/11/2024 10:05:48 AM 1/11/2024 10:05:47 AM 1/11/2024 9:34:07 AM 1/11/2024 9:32:40 AM 1/11/2024 9:31:50 AM 1/11/2024 9:31:18 AM | 1/11/2024 10:05:53 AM 1/11/2024 10:05:52 AM 1/11/2024 10:05:48 AM 1/11/2024 9:34:43 AM 1/11/2024 9:34:06 AM 1/11/2024 9:32:39 AM 1/11/2024 9:31:50 AM | | |
| rofile Name: Delta Synchr Step Type: Delta Syn Start Time: 1/11/202 Synchronization Statistics | onization User Name: I chronization 4 10:05:53 AM | NT SERVICE\ADSyn | c Partition: default End Time: 1/11/2024 1 Connection Status | 10:05:53 AM Status: success | | |
| Inbound Synchronizal Projections Joins Filtered Disconnectors Disconnectors Connectors with Flow Upd Connectors without Flow Filtered Connectors Deleted Connectors Metaverse Object Deletes | tion 0 0 19 dates 0 Updates 0 0 0 5 0 | | Flow Errors | | | |
| | | | | | Q = m(a) | 62 |

Figure 2.1 Azure AD Connect Synchronization Service Manager

- 19. Bring up MS Edge web browser and access <u>https://entra.microsoft.com/</u>
- 20. From left side object tree, select Protection.
- 21. Click on Identity governance.
- 22. Click on Privileged identity Management->My Roles
- 23. From Eligible assignments, under Actions, click on Activate.
- 24. Enter reason and click on Activate.
- 25. Wait for activation cycle to complete.
- 26. From the Microsoft Entra admin center search bar, type in Microsoft Entra Connect and press Enter.
- 27. Scroll down to Health And Analytics, and click on Entra Connect Health.
- 28. Click on Sync services.
- 29. Hover over roll associated with Service Name and click on it. Refer to figure 2.2.

| 🗧 🖸 🕼 https://extramicrosoft.com/feature.msslp=trueHview/Microsoft_Azure_AOHybridtesth/Autigridtesith@ade/serviceNiane/AutigridTevice-itycalegesfannicrosoft.com/s 🔠 🗚 🏠 🛱 🍲 🎕 | | | | | | | |
|--|---------------------------------------|--------|--|---|---|-------------------------------------|--|
| Ν | ficrosoft Entra admin center | | $\mathcal P$ -Search resources, services, and docs (6+,5 | ରେ ପ | 00 R . | | |
| ħ | Home | j | Home > Microsoft Entry Convect > Microsoft Entry Connect Health Sync services > Lonmicrosoft.com | | | × | |
| * | Favorites | ř | 🕄 Delete 💿 Settings | | | | |
| ٠ | Identity | ~ | Overview | | | | |
| 4 | Protection | × | Microsoft Entra Connect Servers | | | | |
| 8 | Identity governance Dashboard | ^ | 3 | | | O Healthy O Healthy O Healthy | |
| a | Access reviews Privileged identity | | Operations | | | • • • • • • • | |
| 6 0 | Management Lifecycle workflows | | Aints Openingentermitisecturer | Last expert to Microsoft Entra ID checkpedemicrostrate | Sync Error Auti-inclusion clacologieto | | |
| | Verified ID | \sim | Adive 0 | | 2 | | |
| • | Permissions Management | | | | 2 | | |

Figure 2.2 Microsoft Entra Connect Servers. CCSF-AzrSync-01 (w2k22) with AADC 2.3.2.0 Stagging is good.

Notes:

Can have multiple stagging servers, but you can only have one syncing server.

Microsoft Entra Connect: Next steps and how to manage Microsoft Entra Connect - Microsoft Entra ID | Microsoft Learn Microsoft Entra Connect: Enabling device writeback - Microsoft Entra ID | Microsoft Learn