**Azure AD Hybrid Join** **Migration Strat**

**Designed by: Derek Baugh**

1. **Assign Business Premium licenses to necessary accounts in tenant. This allows:**
   1. **Hybrid Azure AD join**
   2. **MDM with both GPOs and Intune**
   3. **Easier device migration (no need for an immediate wipe & Azure AD domain join from start, can ease the device migration. Updating to latest Windows will allow for easier domain and AAD profile integration)**
   4. **Consolidation of credentials used to access Cadre resources.**
   5. **Implement SSO into the majority of SaaS using already known domain passwords.**
2. **Export SAGE 100 data to Right Networks Hosted QuickBooks Desktop.**
3. [**Transfer files**](https://learn.microsoft.com/en-us/sharepointmigration/mm-get-started) **from file shares on DC and VEEAM to Sharepoint.**
4. **Transfer DHCP to local Fortigate:**
   1. **Gradually shorten leases on DC DHCP service so eventually leases are renewing daily (leases are currently set for 1 hour).**
   2. **On cutover, remove DHCP service from on-prem DC. Enable DHCP on f/w. Set correct DNS servers in settings.** 
      1. **Primary set as current DC, secondary as VEEAM server. Will be updated to Azure DC VM as primary & 8.8.8.8 or second Azure server VM as secondary.**
5. **Configure Azure environment:**
   1. **Deploy Fortigate Azure Next Gen F/W ARM** [**Template**](https://github.com/fortinet/azure-templates/tree/main/FortiGate/A-Single-VM) **to setup:**
      1. **1 FortiGate firewall(s) in an active/passive deployment**
      2. **1 VNET(s) containing a protected subnet**
      3. **User Defined Routes (UDR) for the protected subnets**
   2. [**Install/configure Windows Server VM as domain controller**](https://activedirectorypro.com/deploy-domain-controller-azure/) **in protected subnet.**
   3. **Setup** [**site-to-site VPN**](https://docs.fortinet.com/document/fortigate-public-cloud/7.4.0/azure-administration-guide/30680/connecting-a-local-fortigate-to-an-azure-fortigate-via-site-to-site-vpn) **between on-prem Fortigate & Azure Fortigate**
   4. **Join to domain, install AD + DNS services and** [**promote to Domain Controller**](https://lazyadmin.nl/it/add-domain-controller-to-existing-domain/)
   5. **Verify replication (AD structure and DNS zones should be on new DC)**
   6. **Configure DNS entries on servers to reference each other (for round robin setup)**
   7. **Test connection to Azure DC VM by logging into endpoint with domain credentials using static network settings (DNS pointing to Azure VM as primary, 8.8.8.8 or another Win Server VM as secondary)**
   8. **Install Print server service on Azure VM.** [**Transfer configs from old to new server.**](https://4sysops.com/archives/migrate-print-servers-to-windows-server-2019-2022/) **Verify printer connections & GPOs for printer deployment.**
   9. [**Transfer FSMO roles**](https://techencyclopedia.wordpress.com/2020/04/23/how-to-migrate-active-directory-and-dns-from-microsoft-server-2012-to-2019/)
      1. **Move RID master, PDC emulator and Infrastructure Master Roles**
      2. **Move Schema Master role**
      3. **Move Domain Naming Master**
   10. **Set DNS entries on Fortigate to updated server IPs used on test computer.**
   11. [**Demote on-prem DC & disable DNS on Veeam server**](https://lazyadmin.nl/it/demote-domain-controller/)
6. **Clean up AD & OUs.**
7. **Setup AAD sync &** [**Hybrid join devices.**](https://learn.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan) **Other sources:**
   1. [**Resource A**](https://www.orbid365.be/hybrid-azure-ad-join-p1/) **+** [**B**](https://www.orbid365.be/hybrid-azure-ad-join-p2/)
   2. [**Resource C**](https://petri.com/how-to-automatically-hybrid-azure-ad-join-and-intune-enroll-pcs/)
   3. [**Resource D**](https://help.hcltechsw.com/bigfix/10.0/mcm/MCM/Config/automatic_enrollment_of_hybrid_azure_ad_joined_devices.html)
8. **Intune Policy Creation & testing**