**SCENARIO**

Customer would like to deploy a Windows Active Directory VM in Azure, connected to their on-premises environment through an Azure VPN.

This is a great scenario for a customer wanting to dip their toes into Azure or see some basics of what things look like and how they are deployed.

**SCENARIO ARCHITECTURE**

* Solution:
  + Deploy a Windows Server 2016 VM running Active Directory
  + Deploy a VPN Gateway
  + Deploy a Connection to connect to the on-premises network
  + Deploy a Virtual Network (vNET) for the VM
  + Deploy a Storage Account for storing the VM’s disk(s)
* How does this architecture meet the customer requirements?
  + Uses Azure Resource Manager (ARM) Template along with PowerShell Desired State Configuration (DSC) to deploy all the required components of the solution along with installing Active Directory on the Windows VM
* What are some limitations of this proposed architecture?
  + VPN Connection to on-premises environment will need to be manually configured after the VPN Gateway is deployed
  + After VPN Connection is established the Windows AD VM will need to have its DNS settings updated to point to at least one on-premises DC
  + After VPN Connection is established the Windows AD VM should have a static private IP address assigned
  + After VPN connection, IP address and DNS settings have been configured, the AD VM can be promoted to a DC
  + In a production environment we would want to deploy 2 AD VMs in an Availability Set
  + Does not enable Azure Security Center

**RESOURCES**

* <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/adds-extend-domain>
* <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/windows-vm>
* <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-plan-design>
* <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-download-vpndevicescript>