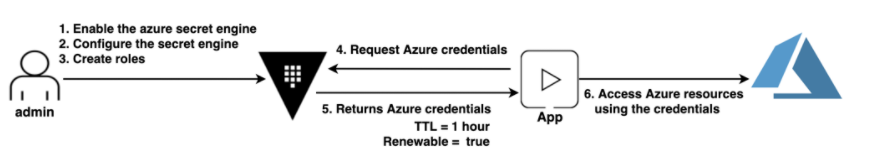
This is intended to be done on a home lab and to replace deprecated steps found here [Azure Secrets Engine | Vault](https://learn.hashicorp.com/tutorials/vault/azure-secrets)



This illustration shows the admin persona interfacing with the Vault to do the initial configurations. Then the Vault leverages the Vault app role that is mapped to Azure SPN. This allows the app to request credentials from the Vault who negotiates a new token from Azure.

This lab is intended for a Linux environment running on your personal lab.

Prereq’s: <https://learn.hashicorp.com/tutorials/vault/getting-started-install#install-vault> , <https://docs.microsoft.com/en-us/cli/azure/install-azure-cli> , <https://portal.azure.com>

You need to have vault, azure cli, and a working azure account with active subscription.

1. Start here [create azure SPN and RG](https://learn.hashicorp.com/tutorials/vault/azure-secrets#create-an-azure-service-principal-and-resource-group) . The steps from there until step 17 are good. Once you reach step 17 please refer back to this guide for supplemental information.
2. If you have run az login then you can use the commands below to set your tenant and subscription IDs. You can use the client id and client secret commands once you have created a SPN.
3. Set variables for azure data (subscription ID, tenant ID, client/app ID, client secret).
   1. TENANT\_ID=$(az account list --query '[].tenantId' -o tsv)
   2. SUBSCRIPTION\_ID=$(az account list --query '[].id' -o tsv)
   3. CLIENT\_ID=$(az ad app list --query "[?displayName=='Azure\_TF\_Vault\_app'].appId" -o tsv)
   4. CLIENT\_SECRET=$(az ad app credential reset --id $CLIENT\_ID --append --query 'password' -o tsv)
4. After reaching step 17 we deviate from the guide. This is due to Azure AD Graph API being deprecated. We will be using Microsoft Graph API.
5. From step 17 under API permissions we will use Microsoft Graph instead of Azure AD Graph. We will assign application permissions of Application.ReadWrite.All and Directory.ReadWrite.All , after they are assigned grant admin consent.
6. Navigate back to azure home and then to subscriptions, then click on IAM and add your application ‘education’ to to owner role.
7. Navigate back to azure home and then to Azure AD, select the roles and administrators blade, assign the application administrator role to ‘education’
8. Navigate back to azure home then select resource groups, create a new group named ‘vault-education’
9. You can resume the walkthrough here [Start Vault](https://learn.hashicorp.com/tutorials/vault/azure-secrets#start-vault) I would note that you will have issues trying to reuse a root vault token
10. Create the two vault policies shown at the start of the hashicorp walkthrough
11. The rest of the the hashicorp walkthrough is valid.