CDW Documentation

Deploy Azure Key Vault

Deploy Azure Key Vault

Creating an Azure Key Vault

1. Login to the correct subscription.
2. In the Search Bar search for Key Vault and select Key Vaults
3. Click Create in upper left
4. Select the correct subscription and resource group, which has to already exist.
5. Enter Key Vault name, Select Region, and select pricing tier (normally Standard)
6. Choose days to retain deleted vault based on needs.
7. Choose to enable or disable purge protection based on needs.
8. Click Next
9. Choose permission model (should be Azure Role-Based access control)
    1. Select Resource Access as needed
    2. Click Next
10. Configure Networking as needed, either Public (normally no) or Private Endpoint, which requires a preexisting network.
11. Click next if you want to configure tags, if not click Review + Create
12. This will create the Key Vault and when done you can click Go To Resource
13. Click on Access Control (IAM) and configure users or roles to access the vault
    1. At a minimum the role has to have Get capabilities for the Key Vault.
14. Click on Objects and create either Keys, Secrets, or Certificates as needed.
15. Test retrieval via the selected method be it VM, CLI, or deployment.
    1. Easiest test is from the CLI.
    2. Login: az login –tenant siriusazuretest.onmicrosoft.com (for AI Lab)
    3. Select the right tenant from the list
    4. Run key vault retrieval command: az keyvault secret show –vault-name don-secret-vault-of-gold –name donsecret
    5. Use your secret in the desired way.

AI Knowledge