By following the Key Vault creation steps outlined, I (almost!) created a Key Vault named “Keyvaultpj” inside a RG named VM-RG. I kept the pricing tier as standard (as opposed to Premium). A standard key vault means that the secrets (keys/certs) will NOT be stored in HSM (Hardware Security Modules) and henceforth will not be FIPS compliant.

I changed the Soft-delete retention policy from 90days to 10days, which means that the secret can be either recovered or permanently deleted for 10 days after the secret is “deleted.” There is however an option to enable purge protection to insure that secrets are retain (but that was left disabled as per the homework instructions).

I enabled “Azure Virtual Machines for deployment” which means that VM’s are allowed to access the key vault. By only checking this option, it appears that neither deployments done via ARM or that hypervisors required to encrypt/decrypt VHD files will have access to the vault.

I ensured that the only user in my subscription “Parker Johnson” (me) can access the key vault, but is restricted to Get, List, Update, Create, and Delete operations on “Key” objects. “Secret” and “Certificate” objects were left at the default settings.

I accepted the defaults for the connectivity method, I.e. “Public endpoint (all networks)”, which I believe means that the key vault can be accessed from any computer out on the internet, which could have some security implications.

No tags were supplied.