**Key Vaults**

**Vault URI** :

Unique name

Uri ends with “vault.azure.net”

Directory name is the name of the tenant.

**Soft delete**: When a key or secret is soft deleted, it allows us to recover them within a period of 7-90 days depending on what is set up.

To permanently delete an object, first it needs to be deleted and then purged.

**Purge protection**: Purge access policy is not granted by default to any service principal including the key vault and subscription owner and must be set deliberately.

**Access policies**: These can be created for Key, Secret, Permissions. These can be assigned to principal which can be objectId, name or email and also optionally to application that are part of the AAD.

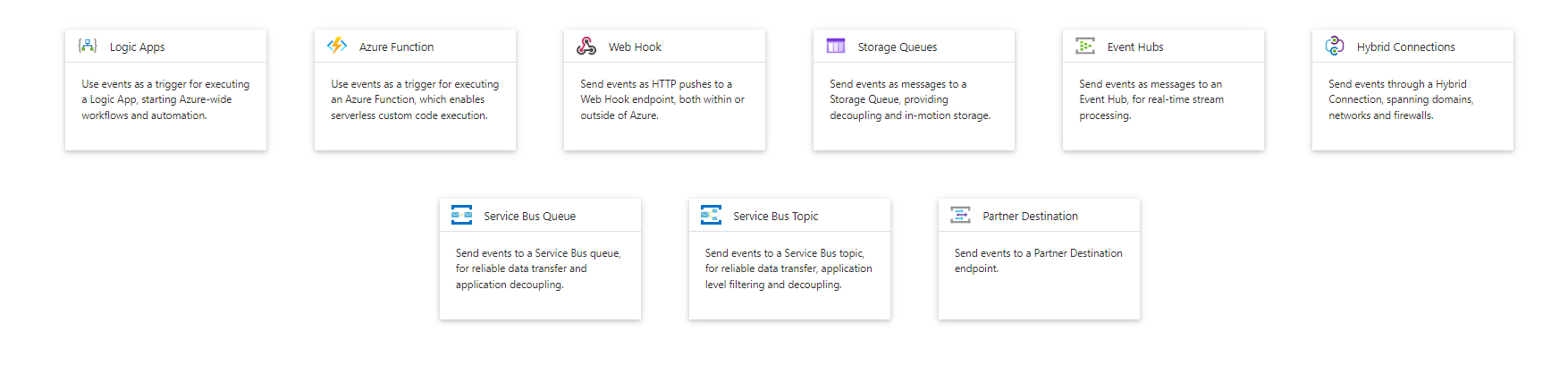
**Events**:

Different events that occur on a key vault can be captured and necessary actions can be taken on the same. The events that occur on a key vault are shown in the following screenshot:

Graphical user interface, text, application, email

Description automatically generated

These events can be captured/delivered by/to a variety of azure and non-azure resources as shown below:

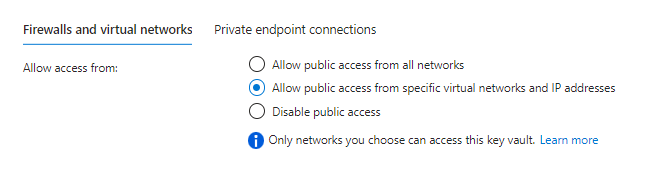


**Networking & Firewall**:

By default, Key vault firewall is disabled. So, all applications can access the key vault and send requests.

Public access does not mean any user can perform operation on the key vault. This would require Azure Active Directory authentication and access policy permissions.

When firewall is enabled,



**Working with key vault API’s**:

Key vault REST API error codes: [REST API error codes - Azure Key Vault | Microsoft Learn](https://learn.microsoft.com/en-us/azure/key-vault/general/rest-error-codes)