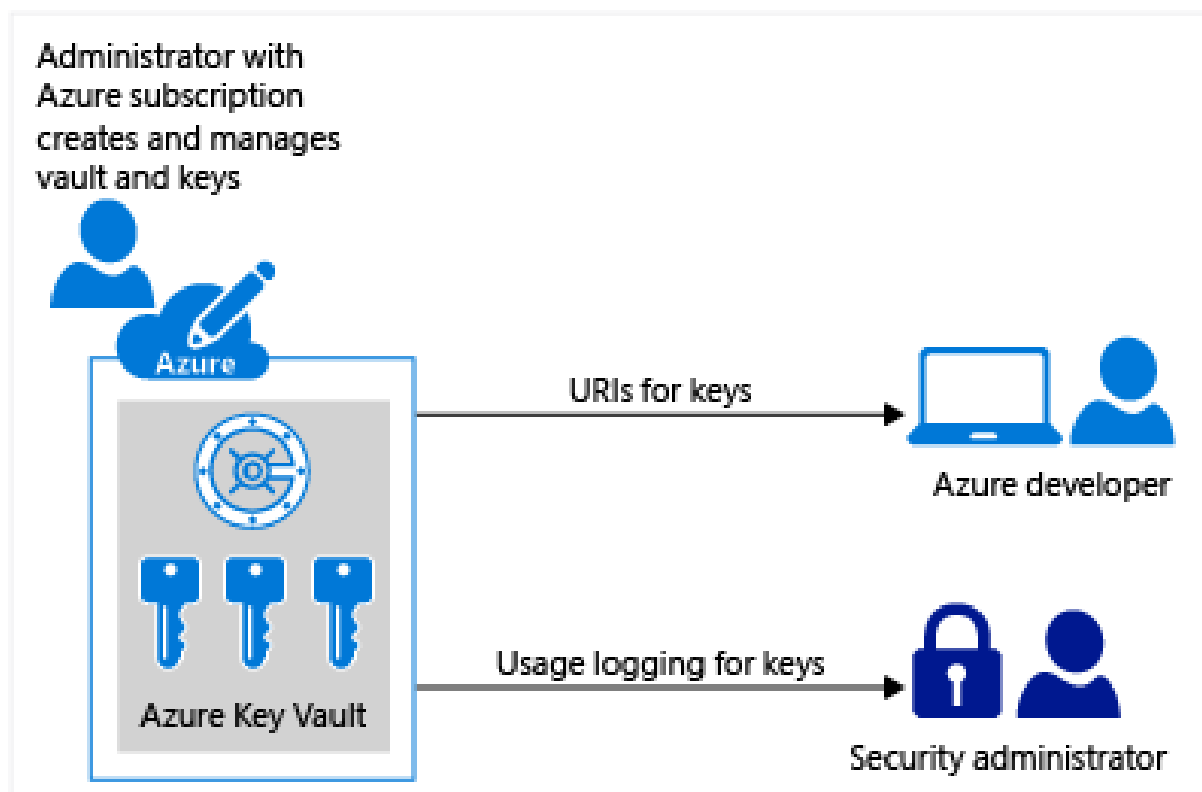# Stories : Azure Key Vault Service

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

1. **Secrets Management:**

   - Azure Key Vault enables you to store and retrieve sensitive information such as API keys, connection strings, and passwords securely.

- You can manage these secrets centrally, and they can be versioned, so you can keep track of changes over time.

2. **Key Management:**

- It provides a secure and scalable way to create, import, and control access to cryptographic keys used by cloud applications and services.

- Supports operations like key generation, encryption, decryption, signing, and verification.

3. **Certificate Management:**

- You can securely store and manage X.509 certificates and their associated private keys.

- Azure Key Vault can automate the renewal of certificates, reducing the manual effort required to maintain certificates.

4. **Access Control:**

- Azure Key Vault integrates with Azure Active Directory (Azure AD) for authentication and authorization.

- Role-Based Access Control (RBAC) is used to control who can perform operations on the key vault and its contents.

5. **Audit Logging:**

- Azure Key Vault provides detailed audit logs, allowing you to monitor access and actions performed on the stored secrets, keys, and certificates.
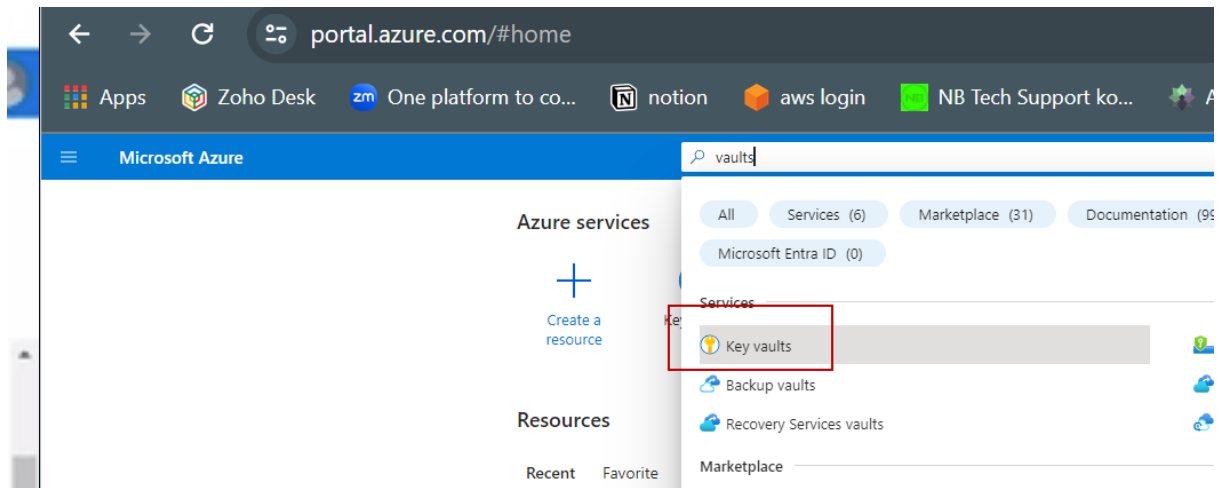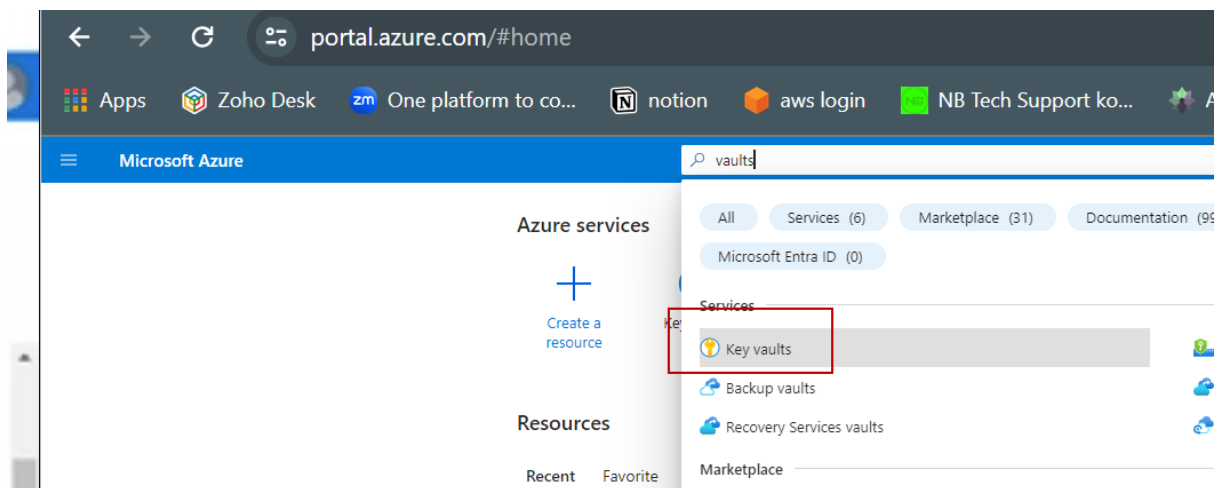
Object of Key Vaults

keys
Certificates
Secrets

Lab : Create a Key vault service and assign role to it

Create a key vault

Create a vault input a unique name

Create a key vault ...

Basics   Access configuration   Networking   Tags   Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * | Azure subscription 1 |

    Resource group * | azure715amRG |
                                     Create new

Instance details

Key vault name * ⓘ | mubKeyvault   ✓ |

Region * | East US |

Pricing tier * ⓘ | Standard |

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete

[Previous]   [Next]   [Review + create]

Assign policy to access current user

Home > Key vaults >
Show portal menu
Create a key vault ...

Permission model

Grant data plane access by using a Azure RBAC or Key Vault access policy

◯ Azure role-based access control (recommended) ⓘ
⦿ Vault access policy ⓘ

Resource access

☐ Azure Virtual Machines for deployment ⓘ
☐ Azure Resource Manager for template deployment ⓘ
☐ Azure Disk Encryption for volume encryption ⓘ

Access policies

Access policies enable you to have fine grained control over access to vault items. Learn more

+ Create   ✎ Edit   🗑 Delete

☑ Name ↑↓	Email ↑↓	Key Permissions	Secret Permissions	Certificate Permissions
∨ USER				
☑ dl devops	dldevops2024_outlook.com#EXT#@dldevops2024outlook.o...	Get, List, Update, Create, Import, Delete, Recover, Backup, R...	Get, List, Set, Delete, Recover, Backup, Restore	Get, List, Update, Create

Provide the level of access to network ALL or Particular Network as per requirement

Home > Key vaults >

Create a key vault ...

Basics   Access configuration   **Networking**   Tags   Review + create

You can connect to this key vault either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Enable public access   ☑

Public Access

Allow access from: ◉ All networks
                            ○ Selected networks

                            ⓘ Traffic from all public networks can access this resource. This is not recommended
                               for private applications or environments. Learn more

Private endpoint

Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the key vault or private li
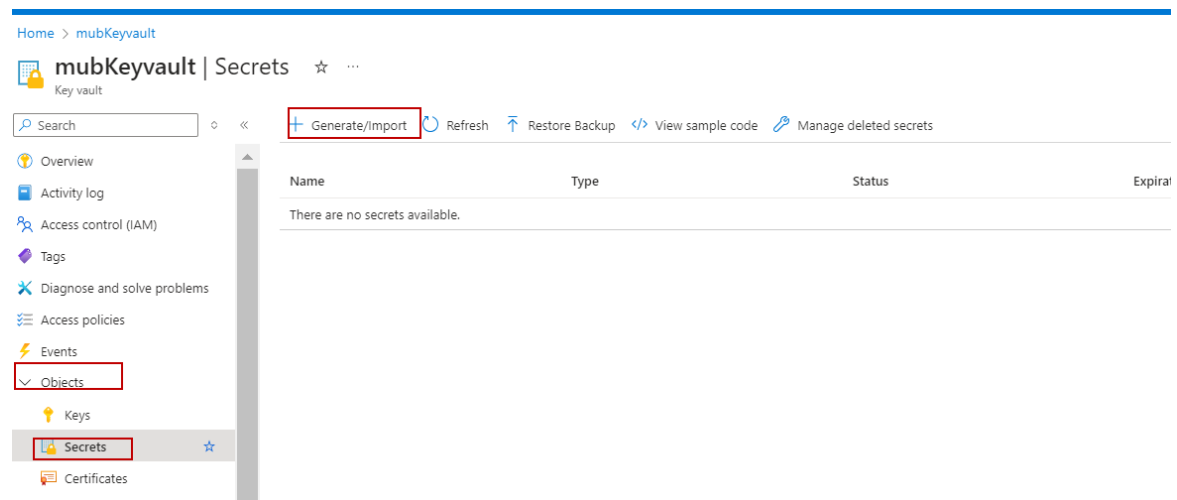
＋ Create a private endpoint

Name	Subscription	Resource group	Region	Subnet
Click on add button to add private endpoint				

Previous   Next   Review + create

now add object to key vault from objects Section

adding a username and password to vault

Home > mubKeyvault

mubKeyvault | Secrets ☆ ⋯
Key vault

🔍 Search «   + Generate/Import ↻ Refresh ↑ Restore Backup </> View sample code 🔑 Manage deleted secrets

- 🎯 Overview
- 📋 Activity log
- 🔑 Access control (IAM)
- 🏷️ Tags
- 🔧 Diagnose and solve problems

ℹ️ The secret 'azureuser' has been successfully created.

Name	Type	Status	Expiration date
azureuser	mynexus user password details	✓ Enabled	

Click on the credentials which has been created and access it

Home > mubKeyvault | Secrets > azureuser >

4683c08940ac44238d4281dea3362b0b 📌 ⋯
Secret Version

Properties

Created	5/10/2024, 8:52:40 AM
Updated	5/10/2024, 8:52:40 AM
Secret Identifier	https://mubkeyvault.vault.azure.net/secrets/azureuser/4683c0... 📋

Settings

Set activation date ℹ️ ☐

Set expiration date ℹ️ ☐

Enabled [Yes][No]

Tags 0 tags

Secret

Content type (optional) mynexus user password details

Show Secret Value

Secret value •••••••••••• 📋