Azure Key Vault – Overview

1. Introduction

Azure Key Vault is a cloud service provided by Microsoft Azure to securely store and manage sensitive information such as **secrets, encryption keys, and certificates**. It helps ensure that sensitive data like connection strings, passwords, API keys, and cryptographic keys are protected using secure, centralized management.

2. Key Features

- **Secrets Management**: Store application secrets (e.g., database connection strings, API tokens).
- **Key Management**: Manage and control access to encryption keys.
- **Certificate Management**: Securely store and manage SSL/TLS certificates.
- **Secure Access**: Integrates with Azure Active Directory (Azure AD) for authentication and access control.
- **Logging & Monitoring**: Monitor usage with Azure Monitor and diagnostic logs.

3. Benefits

- **Centralized security**: Single place to manage all sensitive information.
- **Access control**: Define policies for who can access secrets and keys.
- **Integration**: Works seamlessly with Azure services (VMs, App Services, Functions, etc.).
- **Compliance**: Helps meet regulatory standards like GDPR, HIPAA, etc.
- **High availability**: Built-in redundancy across Azure regions.

---

4. Azure Key Vault Components

1. **Vault** – Secure container for keys, secrets, and certificates.
2. **Keys** – Cryptographic keys used for encryption/decryption, signing.
3. **Secrets** – Secure storage of strings like passwords or API keys.
4. **Certificates** – SSL/TLS certificates with lifecycle management.
5. **Access Policies / RBAC** – Control access using Azure AD identities.

---

5. Use Cases

- Storing **application secrets** (database passwords, API keys).
- Managing **encryption keys** for Azure Storage, SQL, or custom apps.
- Securing **certificates** for HTTPS communication.

- Enabling **disk encryption** and **data encryption at rest**.
- Ensuring **compliance** with security standards.

---

6. Hands-On Lab: Create an Azure Key Vault

Prerequisites

- An active Azure subscription
- Access to Azure portal

Steps

1. **Log in to Azure Portal** → https://portal.azure.com
2. **Search for "Key Vault"** in the search bar.
3. Click **Create**.
4. Fill in details:
   - **Subscription**: Select your subscription.
   - **Resource Group**: Create new or use existing.
   - **Key Vault Name**: Unique name.
   - **Region**: Select closest region.
5. Configure **Access Control** (choose role-based or access policies).
6. Click **Review + Create** → then **Create**.

7. After deployment, open the Key Vault.

8. Add a **Secret**:

   - Navigate to *Secrets* → *Generate/Import* → enter secret name and value (e.g., DBPassword).

   - Save it.

9. Retrieve the Secret:

   - Copy the secret's URI (used by apps to access it).

---

7. Security & Best Practices

- Use **Managed Identities** to access Key Vault without hardcoding credentials.

- Restrict access using **Azure RBAC or Access Policies**.

- Enable **Soft Delete and Purge Protection** to prevent accidental loss.

- Regularly **rotate keys and secrets**.

- Enable **logging** to track who accessed the vault.

✅ **Summary**: Azure Key Vault provides a secure, centralized, and compliant way to manage keys, secrets, and certificates in the cloud. It integrates seamlessly with Azure services and enhances application security.