Azure Key Vault

Solve problems

Secrets Management

- Securely store and control access to Tokens, Passwords, Certificates, API keys and Other secrets

Key Management

- Create and control the encryption keys used to encrypt your data

Certificate Management

- Provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates

Why use Azure Key Vault?

- Centralize application secrets
- Securely store secrets and keys
- Monitor access and use
- Simplified administration of application secrets

Basic Concepts and Important Terms

Tenant

- Used to refer to the set of Azure Services

Vault owner

- Can create a key vault and gain full access and control over it.
- Can set up auditing to log who accesses secrets and keys.
- Can control the key lifecycle.
  - Roll to a new version of the key,
  - Back it up

Vault consumer

- Can perform actions on the assets

Resource

- Examples: Virtual machine, Storage Account, Web App, Database, and Virtual Network

Basic Concepts and Important Terms

Resource group	• Holds related resources
Security principal	• A security identity that user-created apps, services, and automation tools use to access specific Azure resources
Azure AD	• Active Directory service • Can have many subscriptions associated
Managed identities	• To authenticate to Key Vault

Keys vs Secrets

- Key
  - A Cryptographic key represented as JWK (JSON Web Key).
  - Example: store A .pfx certificate file that contains a pair of public & private keys
- Secret
  - Key Vault accepts any value and stores it as a binary.
  - Example: A password or API key

Hands-On: Key Vault

Thanks