CLOUD DAY 2020

29 OTTOBRE • #CLOUDDAY2020

CENTRALIZE AND SECURE APP SECRETS WITH AZURE KEYVAULT AND AZURE APP CONFIGURATION

Massimo Bonanni
@massimobonanni

Azure Key Vault is a service that enables you to store & manage cryptographic keys, secrets and certificates in one central secure vault!!

Doubts of Devs and IT Pros!!

I want customers to **own and manage** their keys so that I can concentrate on doing what I do best, which is providing the core software features.

I don't want the **responsibility** or potential liability for my customers' tenant keys and secrets.

I want to write an application for Azure that uses keys for **signing** and **encryption**. But I want these keys to be **external** from my application.

I want to make sure that my organization **is in control** of the key lifecycle and can monitor key usage.

Azure KeyVault key features

Secrets Management

Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets

Key Management

Azure Key Vault can also be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.

Certificate Management

Azure Key Vault lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates.

Store secrets backed by Hardware Security Modules

The secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs

Azure KeyVault roles

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.

Use RBAC for permissions.

Vault Consumer

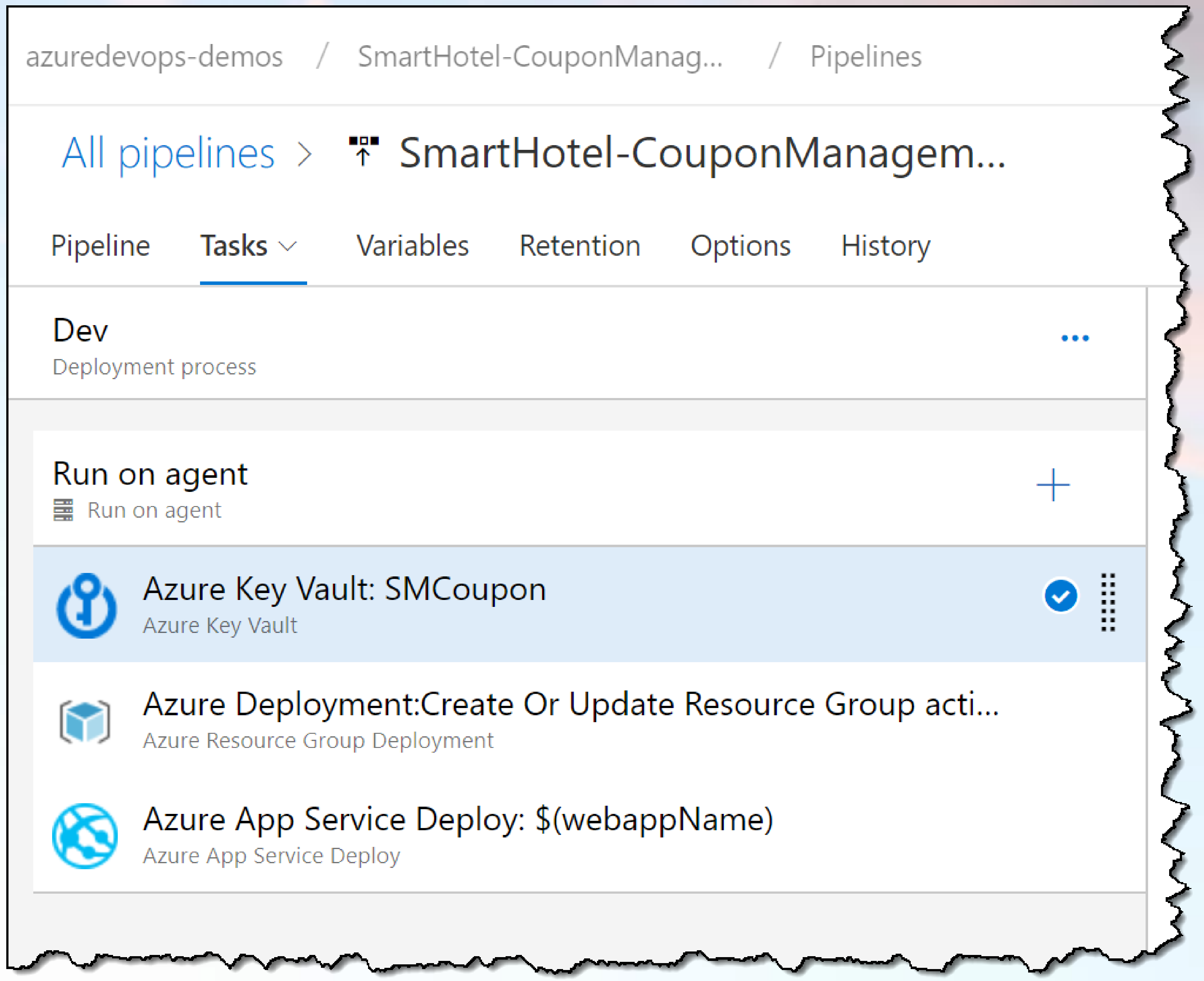
A vault consumer can perform actions on the assets inside the key vault when the vault owner grants the consumer access.

The available actions depend on the permissions granted.

Use KeyVault Access Policy or RBAC (preview) for permissions.

Platform Integration

- Azure Disk Encryption
- Trasparent Data Encryption Azure SQL Database
- Azure App Service
- Storage Account
- ARM Template
- Azure DevOps pipelines
- ...


azuredevops-demos / SmartHotel-CouponManag... / Pipelines
All pipelines > SmartHotel-CouponManagem...
Pipeline
Tasks
Variables
Retention
Options
History
...
+

Dev
Deployment process

Run on agent
Run on agent

Azure Key Vault: SMCoupon
Azure Key Vault

Azure Deployment:Create Or Update Resource Group acti...
Azure Resource Group Deployment

Azure App Service Deploy: $(webappName)
Azure App Service Deploy

Availability and redundancy

The contents of key vault are replicated within the region and to a pair region.

When the region is unavailable, the requests are automatically routed (***failed over***) to a secondary region (read only).

When the primary region is available again, requests are routed back (***failed back***) to the primary region.

Norway West
Norway East
West Europe
UK South
North Europe
UK West
Poland Central
Germany Northeast (Sovereign)
Germany North (Public)
Germany Central (Sovereign)
Germany West Central (Public)
France Central
France South
Italy North
ain Central
Switzerland
Greece
Israel Central
Qatar Central
UAE Central
UAE North
West Indi

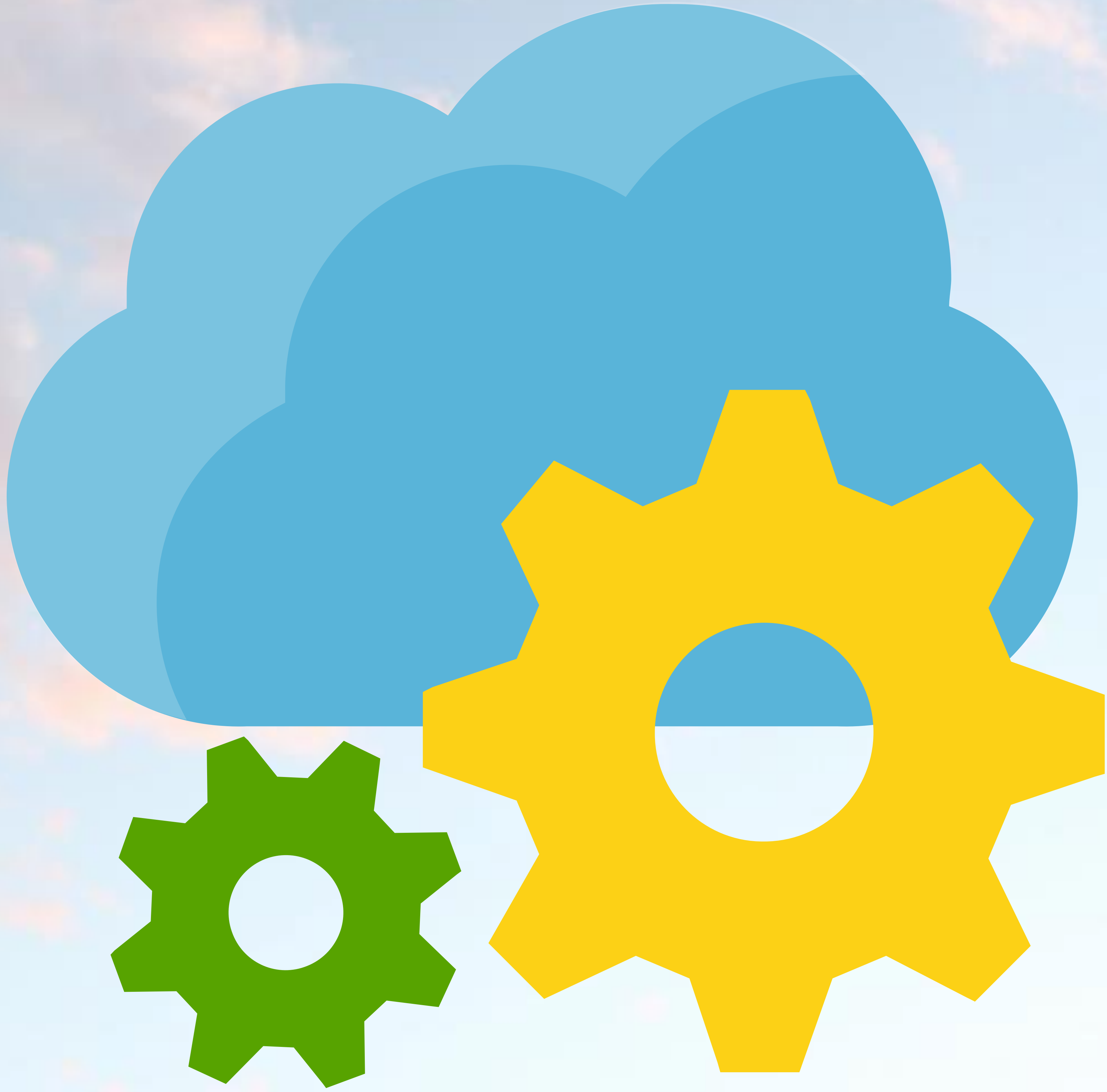
How much?

- Two different plans: Standard and Premium
- Flat rate for transactions
- Pay for renewal of certificates
- Pay for HSM-protected keys

Platform & C# Integration

Why use Azure Key Vault?

1. Centralize application secrets
2. Securely store secrets and keys
3. Monitor access and use
4. Simplified administration of application secrets
5. Integrate with other Azure services



Azure App Configuration provides a service to centrally manage application settings and feature flag

App Configuration Key features

Key-Value store

- Stores configuration data as key-value pairs
- Use label for environments or versions

Point-in-time snapshot

- Maintains a record of changes made to key-value pairs
- You can reconstruct the history of any key-value within the previous seven days

Feature management

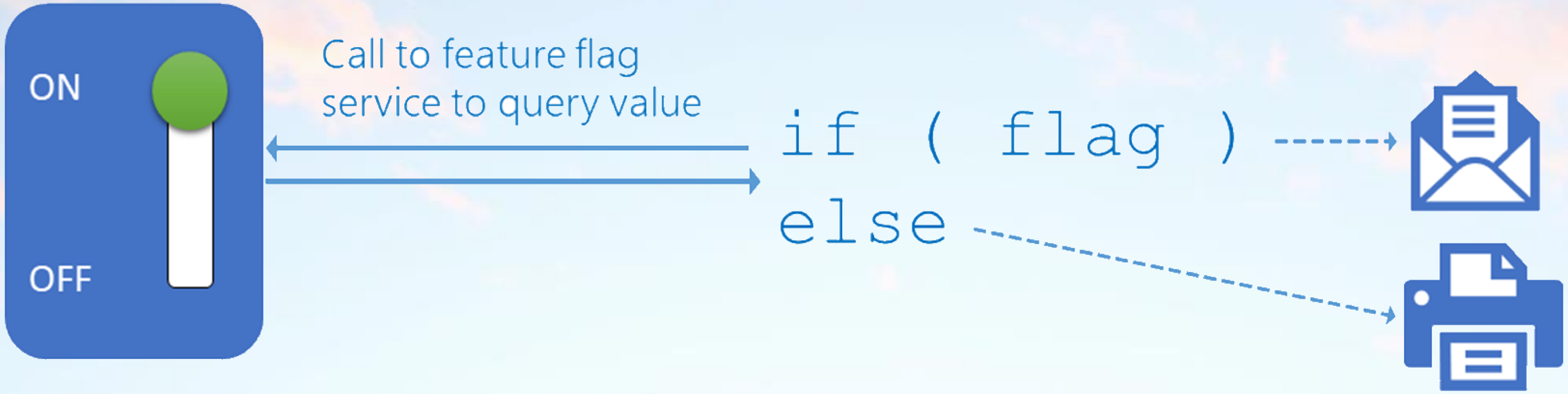
- Decouples feature release from code deployment
- Enables quick changes to feature availability on demand
- AKA ”feature flags”

Security

- Encrypt using customer-managed keys
- Using private endpoints
- Integrate with Azure Managed Identity and Azure KeyVault

What are Feature Flags (FF)?

Feature flags support a customer-first DevOps mindset, to enable (**expose**) and disable (**hide**) features in a solution, even before they are complete and ready for release.



View a feature flag as an **ON | OFF switch** for a specific feature.

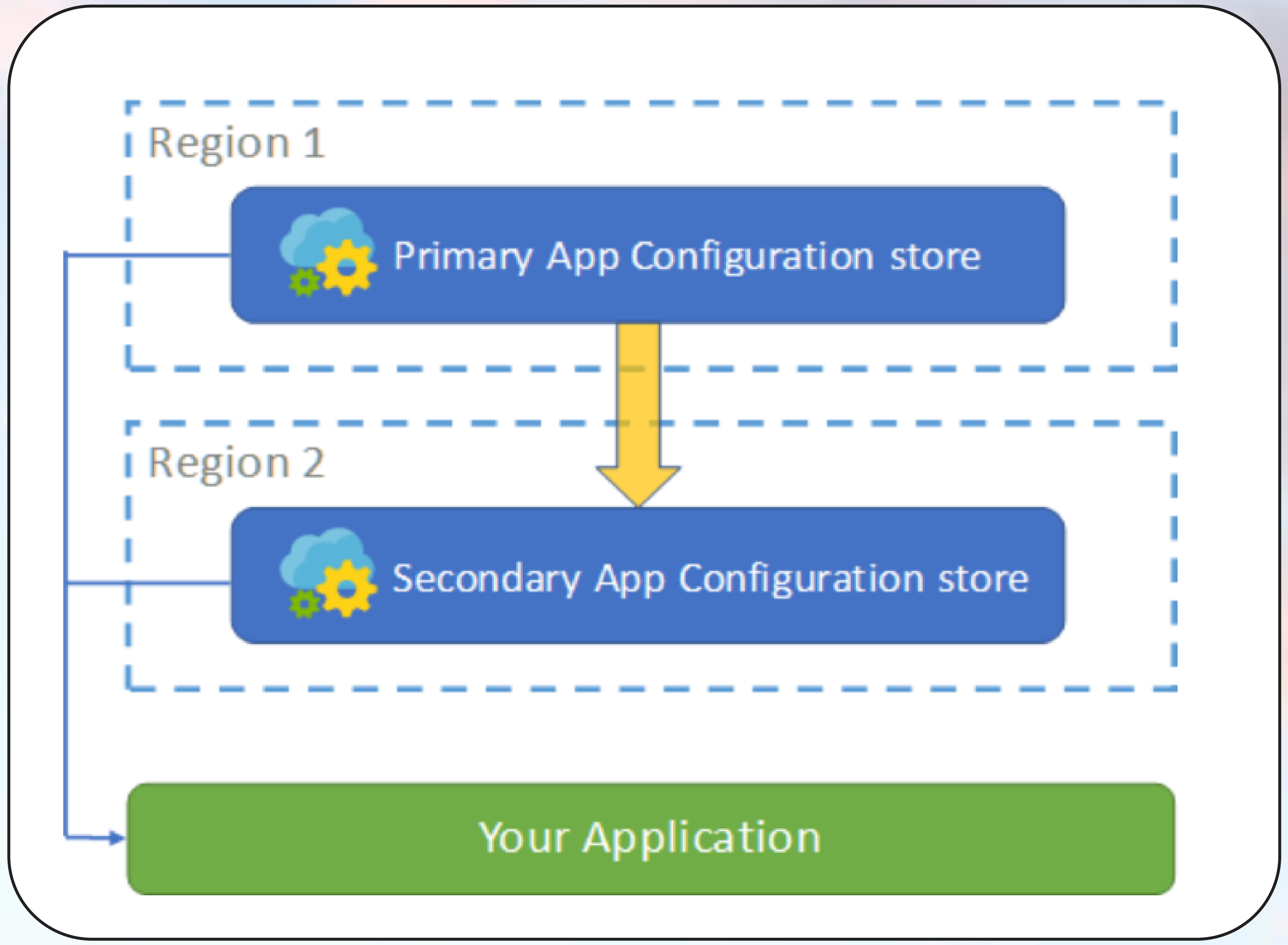
You can, also, use filter to enable feature to specific users.

Resiliency and disaster recovery

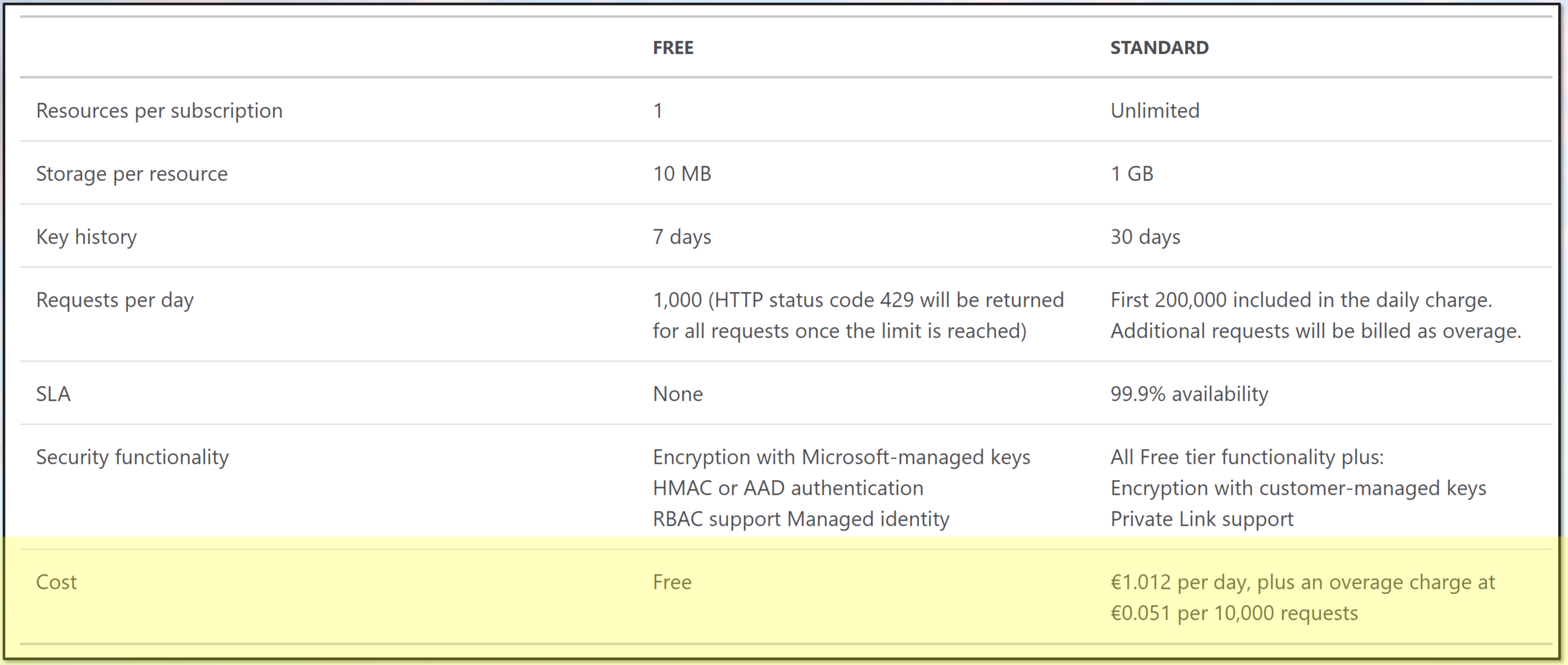
Azure App Configuration is a regional service.

Now, you don’t have any automation for replication between different regions.

Your application loads its configuration from both the primary and secondary stores.


Region 1
Primary App Configuration store
Region 2
Secondary App Configuration store
Your Application

How much?



	FREE	STANDARD
Resources per subscription	1	Unlimited
Storage per resource	10 MB	1 GB
Key history	7 days	30 days
Requests per day	1,000 (HTTP status code 429 will be returned for all requests once the limit is reached)	First 200,000 included in the daily charge. Additional requests will be billed as overage.
SLA	None	99.9% availability
Security functionality	Encryption with Microsoft-managed keys HMAC or AAD authentication RBAC support Managed identity	All Free tier functionality plus: Encryption with customer-managed keys Private Link support
Cost	Free	€1.012 per day, plus an overage charge at €0.051 per 10,000 requests

CLOUD DAY 2020

29 OTTOBRE • #CLOUDDAY2020

Web Site Configuration

Why use App Configuration?

1. Centralize management and distribution of hierarchical configuration data for different environments and geographies
2. Dynamically change application settings without the need to redeploy or restart an application
3. Control feature availability in real-time
4. Enhanced security through Azure-managed identities
5. Encryption of sensitive information at rest and in transit
6. Native integration with popular frameworks

CLOUD DAY 2020

29 OTTOBRE • #CLOUDDAY2020

Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems!

Kevin Mitnic

CLOUD DAY 2020

29 OTTOBRE • #CLOUDDAY2020

Thanks for your attention!!!!!

Connect with me on LinkedIn

linkedin.com/in/massimobonanni/

Massimo Bonanni

Azure Technical Trainer

massimo.bonanni@microsoft.com
@massimobonanni

Microsoft CERTIFIED AZURE FUNDAMENTALS ★
Microsoft CERTIFIED AZURE DATA FUNDAMENTALS ★
Microsoft CERTIFIED AZURE AI FUNDAMENTALS ★
Microsoft CERTIFIED AZURE DEVELOPER ASSOCIATE ★★
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE ★★
Microsoft CERTIFIED AZURE AI ENGINEER ASSOCIATE ★★
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT ★★★
Microsoft CERTIFIED AZURE DEVOPS ENGINEER EXPERT ★★★
Microsoft CERTIFIED AZURE IOT DEVELOPER SPECIALTY
MICROSOFT CERTIFIED TRAINER Microsoft MCT Trainer 2020 - 2021

References

- Azure Key Vault documentation
  https://docs.microsoft.com/en-us/azure/key-vault/
- Azure Key Vault Developer's Guide
  https://docs.microsoft.com/en-us/azure/key-vault/general/developers-guide
- Channel9 - Azure Key Vault with Sumedh Barde
  https://channel9.msdn.com/Shows/Cloud+Cover/Episode-169-Azure-Key-Vault-with-Sumedh-Barde
- Azure App Configuration documentation
  https://docs.microsoft.com/en-us/azure/azure-app-configuration/
- What is Azure App Configuration?
  https://docs.microsoft.com/en-us/azure/azure-app-configuration/overview
- Channel 9 - Introducing Microsoft.FeatureManagement
  https://channel9.msdn.com/Shows/NET-Community-Standups/ASPNET-Community-Standup-May-21st-2019-Introducing-MicrosoftFeatureManagement
- Channel 9 - Getting started with Azure App Configuration
  https://channel9.msdn.com/Shows/Azure-Friday/Getting-started-with-Azure-App-Configuration
- Channel 9 - Azure App Configuration - Making Centralized Configuration Easy
  https://channel9.msdn.com/Events/dotnetConf/NET-Conf-2019/B210
- Secret and Config GitHub Repo
  https://github.com/massimobonanni/azure-att-demo

Kudos

Microsoft

managed/designs

AWS User Group - Italy

AZURE MEETUP MILANO

GDG Cloud Milano