

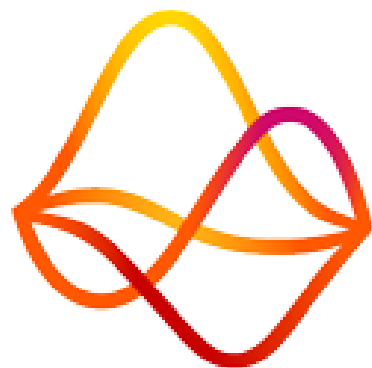


Azure Meetup

07/05/2020



Our sponsor



avanade





Keep your secrets and configurations safe in Azure!



«I am **Massimo, Massimo Bonanni**,
Keymaster of Gozer. Volguus Zildrohar,
Lord of the Sebouillia.

Are you the *Gatekeeper*?»



**Are you using
Azure
KeyVault?**

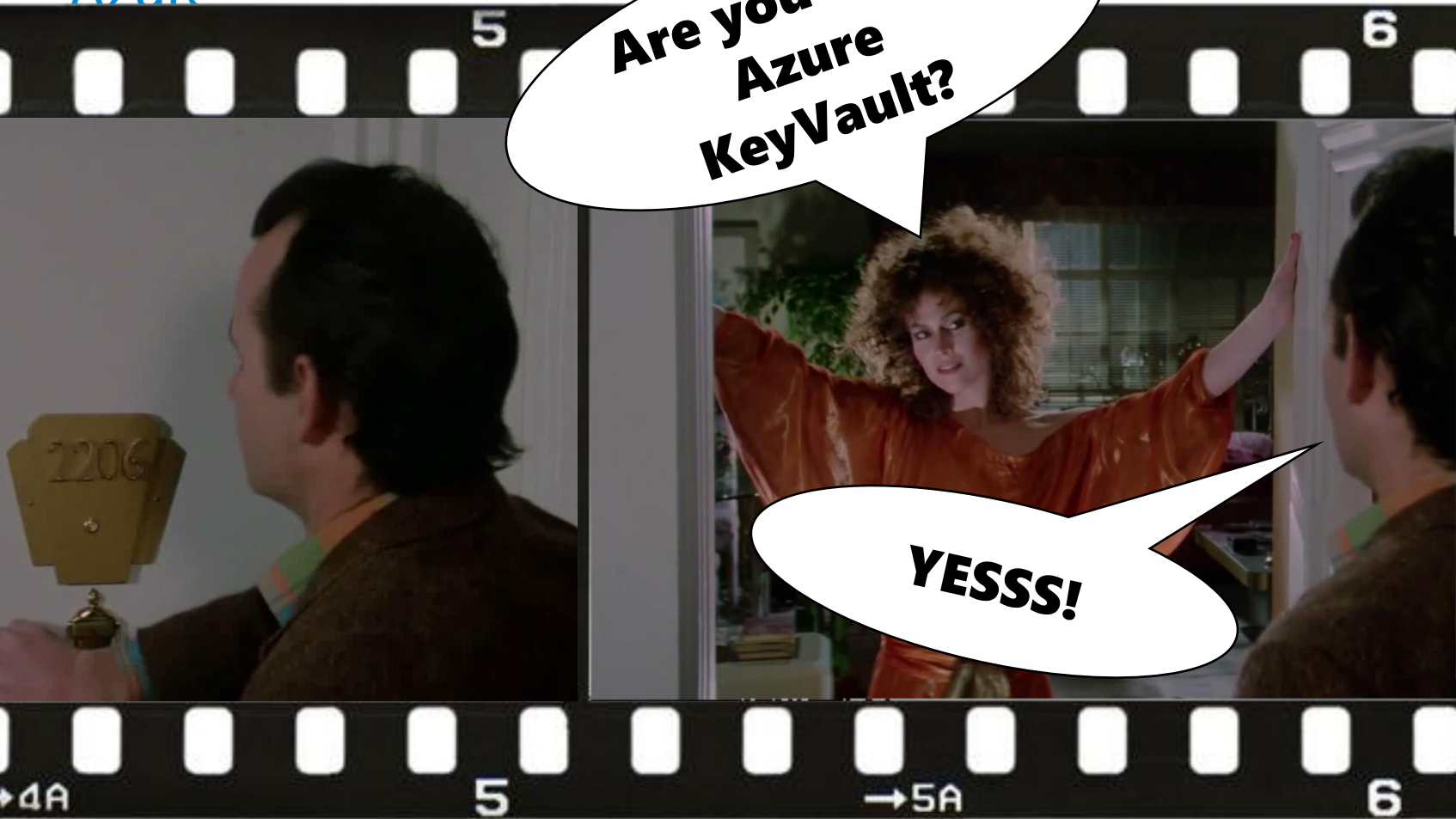
No!





**Are you using
Azure
KeyVault?**

YESSS!



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





The doubts of the IT Professionals!!

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 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 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 actors



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.
 - Can roll to a new version of the key, back it up, and do related tasks.



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.

Access model overview

Management Interface

- The management plane is where you manage Key Vault itself
- Operations in this plane include creating and deleting key vaults, retrieving Key Vault properties, and updating access policies
- Uses Azure Active Directory (Azure AD) for authentication
- Uses role-based access control (RBAC) for authorization

Data Interface

- The data plane is where you work with the data stored in a key vault
- You can add, delete, and modify keys, secrets, and certificates
- Uses Azure Active Directory (Azure AD) for authentication
- Uses a Key Vault access policy for authorization

Hardware Security Module (HSM)

A **hardware security module** (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

A hardware security module contains one or more secure cryptoprocessor chips.

HSM modules are typically certified to internationally recognized standards such as **Common Criteria** or **FIPS 140**.





Platform Integration



Azure Disk Encryption



The always encrypted in Azure SQL Database



Azure App Service



Storage Account



ARM Template



...

Add/Edit application setting

Key Name:

Value:

☐ Deployment slot setting

Key Vault Reference Details

Vault Name	maxkeyvaultdemo
Secret Name	mySecretKey
Secret Version	289a8a0bfd624752a722592e3f6a78b4
Identity	System assigned managed identity
Status	Resolved



DEMO

Create a KeyVault and Platform Integration





Supported programming and scripting languages

REST Api



.NET



Java



Node.js



Python



Powershell



Azure CLI



DEMO

C# Integration



Why use Azure Key Vault?



Centralize application secrets



Securely store secrets and keys



Monitor access and use



Simplified administration of application secrets



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

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



App Configuration benefits

A fully managed service that can be set up in minutes

Flexible key representations and mappings

Tagging with labels

Point-in-time replay of settings

Dedicated UI for feature flag management




Comparison of two sets of configurations on custom-defined dimensions

Enhanced security through Azure-managed identities

Encryption of sensitive information at rest and in transit

Native integration with popular frameworks

Feature Management

-  Shipping a new application feature requires a complete redeployment of the application itself.
-  Testing a feature often requires multiple deployments of the application.
-  Each deployment may change the feature or expose the feature to different customers for testing.

Feature management is a modern software-development practice that decouples feature release from code deployment and enables quick changes to feature availability on demand.

It uses a technique called *feature flags* (also known as *feature toggles*, *feature switches*, and so on) to dynamically activate/disactivate a feature.

Point-in-time snapshot



Azure App Configuration keeps records of the precise times when a new key-value pair is created and then modified.



These records form a complete timeline in key-value changes.



An App Configuration store can reconstruct the history of any key value and replay its past value at any given moment, up to the present.



With this feature, you can “time-travel” backward and retrieve an old key value.

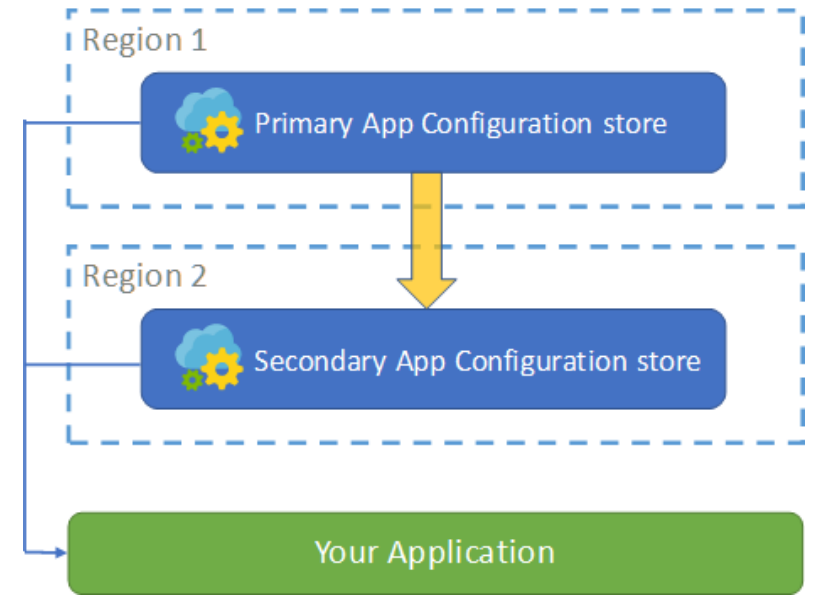


Resiliency & disaster recovery

- ☁️ Azure App Configuration is a regional service.
- ☁️ To realize cross-region redundancy, you need to create multiple App Configuration stores in different regions.
- ☁️ Your application loads its configuration from both the primary and secondary stores in parallel.

```
public static IWebHostBuilder CreateWebHostBuilder(string[] args) =>
    WebHost.CreateDefaultBuilder(args)
        .ConfigureAppConfiguration((hostingContext, config) =>
        {
            var settings = config.Build();
            config.AddAzureAppConfiguration(settings["ConnectionString_SecondaryStore"], optional: true)
                .AddAzureAppConfiguration(settings["ConnectionString_PrimaryStore"], optional: true);
        })
        .UseStartup<Startup>();
```

- ☁️ You can use the **Export** function in App Configuration to copy data from the primary store to the secondary on demand



```
C:\>az appconfig kv export --destination appconfig --name PrimaryStore --dest-name SecondaryStore
```



DEMO

Configuration Management



Why use App Configuration?



Centralize management and distribution of hierarchical configuration data for different environments and geographies



Dynamically change application settings without the need to redeploy or restart an application



Control feature availability in real-time



Enhanced security through Azure-managed identities



Encryption of sensitive information at rest and in transit



Native integration with popular frameworks

"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 Mitnick



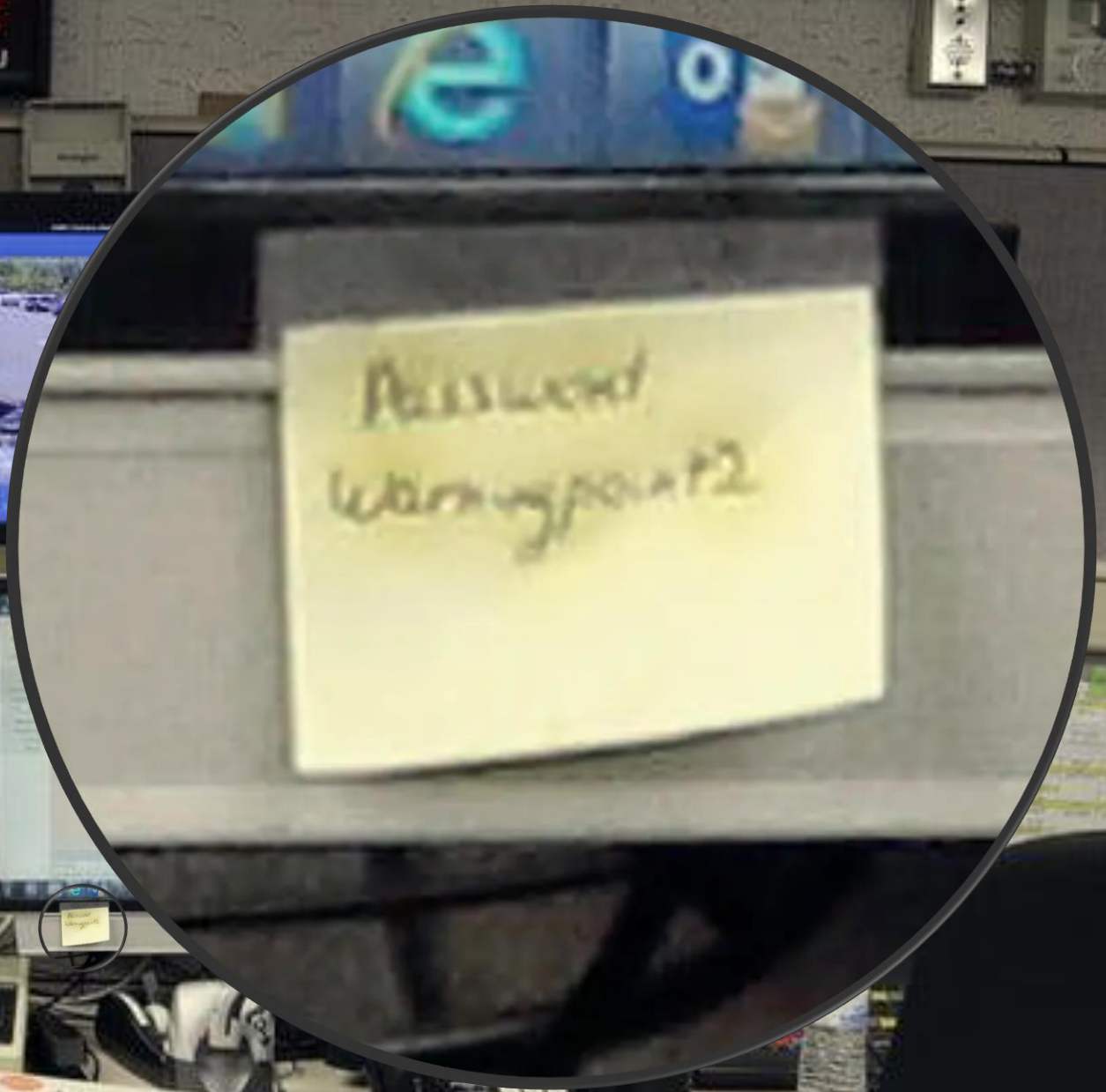


05:39
GUAM

09:39
HONOLULU

5:39
ASH D.C.

19:39
GMT / ZULU



Missed
Warning point 2



Thanks for your attention!!!!



Massimo Bonanni



Azure Technical Trainer @ Microsoft

massimo.bonanni@microsoft.com

@massimobonanni





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>