

# Secrets in Kubernetes Across Cloud

**Jhonny Pong (Jhonnatan Gil)**

@jthan24



Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Who is Jhonny Pong (Jhonnatan Gil)



Just a simple human who loves Linux, share knowledge and very passionate about tech in general especially with make more easy every life that needs deploy in local mode and any other environment

**“Life is really simple, but we insist on making it complicated..”**

Confucius

# Contents



**aws-ssm**

**azure-keyvault**

**gcp-secret-manager**

**hashicorp-vault**

**Kubernetes**

**Secrets**

**external secrets**

**demo**

**questions**

**thanks**

A vertical decorative banner on the left side of the slide. It features a blue and white color scheme with various icons: a lightbulb with gears inside, a Wi-Fi signal icon, a grid of dots, and a network diagram with nodes and lines. The background of the banner is a blurred image of a computer keyboard and a monitor.

SIKAC

# AWS - SSM

# AWS - Systems Manager Parameter Store

Parameter Store, a capability of AWS Systems Manager, provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, Amazon Machine Image (AMI) IDs, and license codes as parameter values. You can store values as plain text or encrypted data. You can reference Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the unique name that you specified when you created the parameter.



# AWS - Systems Manager Parameter Store



AWS Systems Manager > Parameter Store > Create parameter

## Create parameter

### Parameter details

Name:

Description — Optional:

Tier:  Standard (Limit of 10,000 parameters. Parameter value size up to 4 KB. Parameter policies are not available. No additional charges) /  Advanced (Can create more than 10,000 parameters. Parameter value size up to 8 KB. Parameter policies are available. Charges)

Type:  String /  StringList /  SecureString (Encrypt sensitive data using KMS)

KMS key source:  My current account (Use the default KMS key for the account) /  Another account (Use a KMS key from another account)

KMS Key ID:

**ⓘ You have selected the default AWS managed key. All users in the current AWS account and Region will have access to this parameter. To restrict access to the parameter, use a customer managed key (CMK) instead. [Learn more](#)**

Value:

Maximum length: 4096 characters.

### My parameters

<input type="checkbox"/>	Name	Tier	Type	Last modified
<input type="checkbox"/>	my-secret-aws	Standard	SecureString	Wed, 15 Sep 2021 00:57:22 GMT

A vertical decorative graphic on the left side of the slide. It features a blue and white color scheme with various icons: a lightbulb with gears inside, a Wi-Fi symbol, a laptop, and a network diagram with nodes and lines. The background has a hexagonal pattern.

SIKAC

# Azure - KeyVault

# Azure - Key Vault Secrets

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. Key Vault service supports two types of containers: vaults and managed hardware security module(HSM) pools. Vaults support storing software and HSM-backed keys, secrets, and certificates. Managed HSM pools only support HSM-backed keys. See Azure Key Vault REST API overview for complete details.





# Azure - Key Vault Secrets



Basics Access policy Networking

Enable Access to:

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ

Home > Key vaults > kv-test-mode >

Project details

Select the subscription to manage your resources.

## Create a secret

Subscription \*

Resource group \*

Instance details

Key vault name \* ⓘ

Region \*

Pricing tier \* ⓘ

Recovery options

Soft delete protection will automatically delete a key vault and secrets for the duration of the retention period within the key vault.

To enforce a mandatory retention period elapsing, you can turn on purge protection by Microsoft.

Soft-delete ⓘ

Days to retain deleted vaults \* ⓘ

Purge protection ⓘ

Upload options

Manual

Name \* ⓘ

my-secret-azure

Value \* ⓘ

.....

Content type (optional)

Set activation date ⓘ

Set expiration date ⓘ

Enabled

Yes No

Tags

0 tags

... publicly, or privately, using a private endpoint.

... create

... and view consolidated billing by applying the same tag to the resource.

Resource
Key vault

A vertical decorative graphic on the left side of the slide. It features a dark blue background with various white and light blue icons and patterns, including a lightbulb with gears inside, a Wi-Fi symbol, a grid of dots, and a network diagram with nodes and lines.

SIKAC

# GCP - Secrets Manager

# GCP - Secret Manager

Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud.



# GCP - Secret Manager



Google Cloud Platform | CamiloTorresUCRutas | secret

Seguridad > Crear secreto

**Administrador de secretos**

- Administrador de riesgos
- Aprobación de acceso
- Web Security Scanner
- Chronicle
- Microsoft AD administrado

### Detalles del Secret

Esta acción creará un Secret con el valor del Secret de la primera versión. [Más información](#)

**Nombre**  
my-secret-gcp

**Valor secreto**  
Ingresar tu valor secreto o impórtalo directamente desde un archivo.

Subir archivo | Tamaño máximo: 64 KiB

**Valor secreto**  
my-secret-gcp

## Secret: "my-secret-gcp"

projects/417425098745/secrets/my-secret-gcp

DESCRIPCIÓN GENERAL | **VERSIONES** | PERMISOS | REGISTROS

Versiones + VERSIÓN NUEVA | HABILITAR | INHABILITAR | DESTRUIR

Versión	Estado	Encriptación	Fecha de creación	Acciones
1	Habilitada	Administrada por Google	15/9/21 01:49	

No se seleccionaron versiones

**Política de replicación**  
Según la configuración predeterminada, Google administra a ubicación en la que se almacena este Secret. Si necesitas ac manual, marca la siguiente casilla para personalizar los ubc nivel mundial a todos. Los Secrets sin importar cómo están re política de replicación no se puede cambiar después de que Secret. [Más información](#)

Administrar ubicaciones de forma manual para este S

**Encriptación**  
Este secreto está encriptado de forma predeterminada con u Google. Si quieres administrar tu encriptación, puedes usar u cliente en su lugar. [Más información](#)

Usar una clave de encriptación administrada por el cli

**Rotación**  
Si configuras un período de rotación, se enviarán notificaciones de rotación a los temas de Pub/Sub. Secret Manager no rotará de forma automática el valor del Secret. [Más información](#)

Establecer periodo de rotación

**Notificaciones**  
Selecciona los temas de Pub/Sub que recibirán notificaciones de eventos cuando se modifique el secreto o una de sus versiones. Estos eventos pueden ser eventos iniciados por el usuario o programados. [Más información](#)

CREAR SECRETO | CANCELAR

A vertical decorative bar on the left side of the slide. It features a dark blue background with various white and light blue icons related to technology and security, including a lightbulb with gears, a Wi-Fi symbol, a laptop, and a network diagram with nodes and lines.

SIKAC

# Hashicorp - Vault

# Hashicorp - Vault

Vault is a tool for securely accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. Vault provides a unified interface to any secret, while providing tight access control and recording a detailed audit log.

Secure Secret Storage: Arbitrary key/value secrets can be stored in Vault. Vault encrypts these secrets prior to writing them to persistent storage, so gaining access to the raw storage isn't enough to access your secrets. Vault can write to disk, Consul, and more.



# Hashicorp - Vault



▼ Secrets Access Policies Tools

▼ Secrets Access Policies Tools Status

## Enable a Secrets Engine

[kv-test-mode](#)

Generic

### Create secret

[kv-test-mode](#) [my](#) [secret](#) [vault](#)

## my/secret/vault

JSON Delete Copy Version 1 Create new version

Key	Value
secret	<span>secret</span>

Consul  Databases

👁 Add

Next Save Cancel

A vertical decorative bar on the left side of the slide. It features a blue and white color scheme with various technology-related icons: a lightbulb with gears inside, a Wi-Fi signal icon, a laptop, and a network diagram with nodes and lines.

SIKAC

# Kubernetes



# What is kubernetes

Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available.





SIKAC

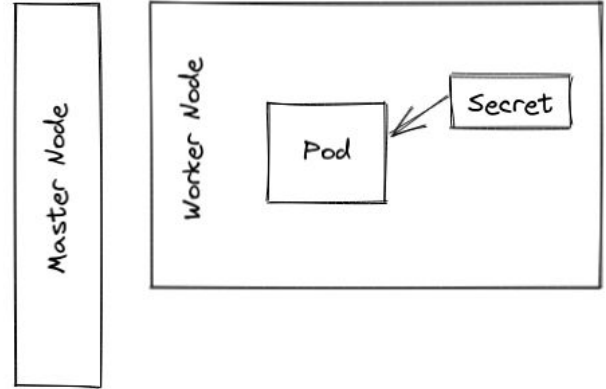
Kubernetes

# Secrets



# What is secret

A Secret is an object that contains a small amount of sensitive data such as a **password**, a **token**, or a **key**. Such information might otherwise be put in a Pod specification or in a container image. Using a Secret means that you don't need to include confidential data in your application code.





SIKAC

# External Secrets



# External Secrets

External Secrets Operator is a Kubernetes operator that integrates external secret management systems like **AWS** Secrets Manager, HashiCorp **Vault**, **Google** Secrets Manager, **Azure** Key Vault and many more. The operator reads information from external APIs and automatically injects the values into a Kubernetes Secret.

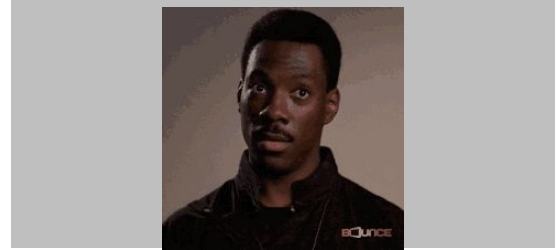


# What, ¿operator?



Operators are software extensions to Kubernetes that make use of custom resources to manage applications and their components. Operators follow Kubernetes principles, notably the control loop

# External Secrets - Architecture



First, define secret in your cloud or on premise (Bare Metal) provider



Second, write your YAML config file to obtain secret.



Third, use the secret in your Cluster.



# Demo Time



**Caution**  
Don't run this on Production

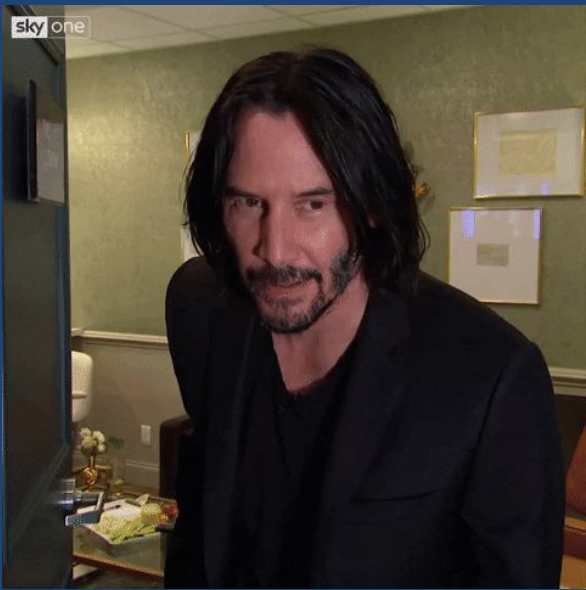






Secrets in Kubernetes Across Cloud - SIKAC

# Thank you!!



Thank you for your time!!

I hope you learn something new!!