Carnegie Mellon University
Software Engineering Institute

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

Carnegie Mellon University Software Engineering Institute

DEVSECOPS DAYS

Contents

SIKAC

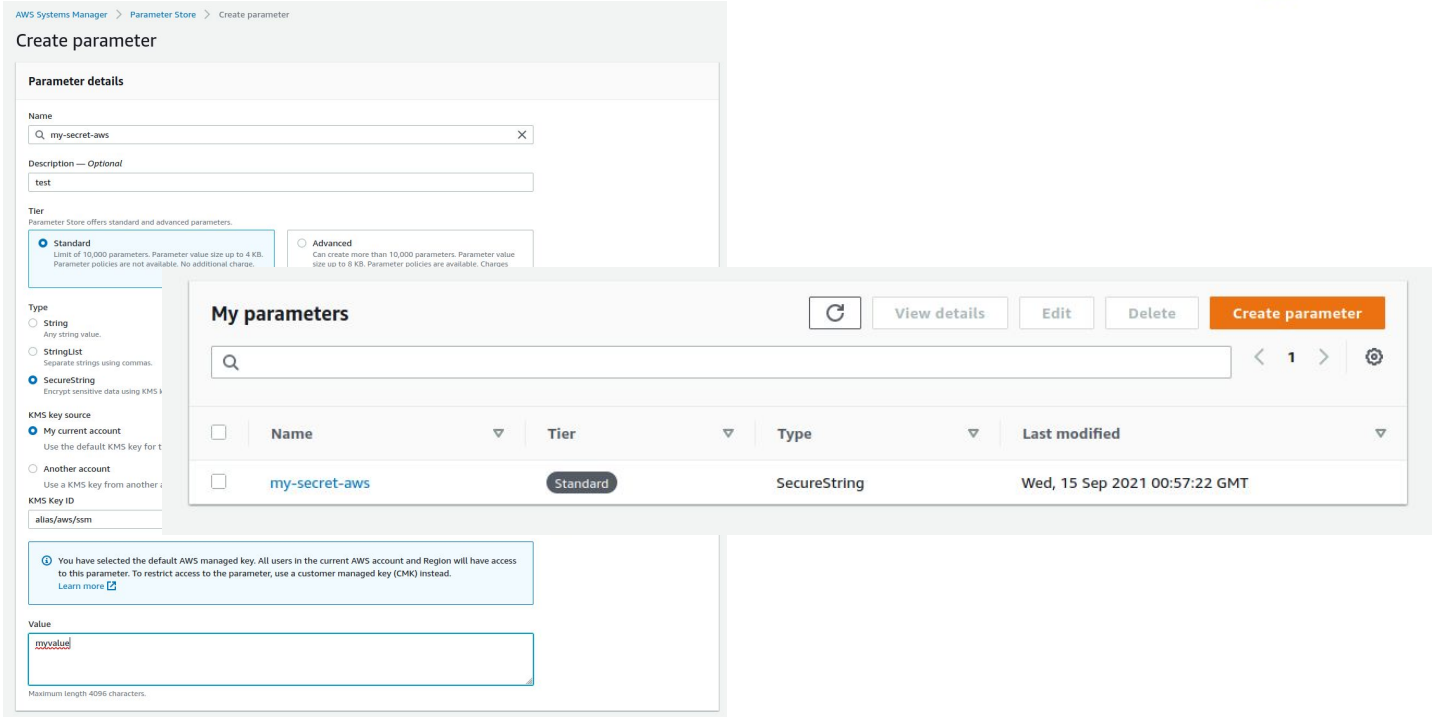
AWS - SSM

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.

https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html

AWS - Systems Manager Parameter Store



Carnegie Mellon University Software Engineering Institute

DEVSECOPS DAYS LOS ANGELES

SIKAC

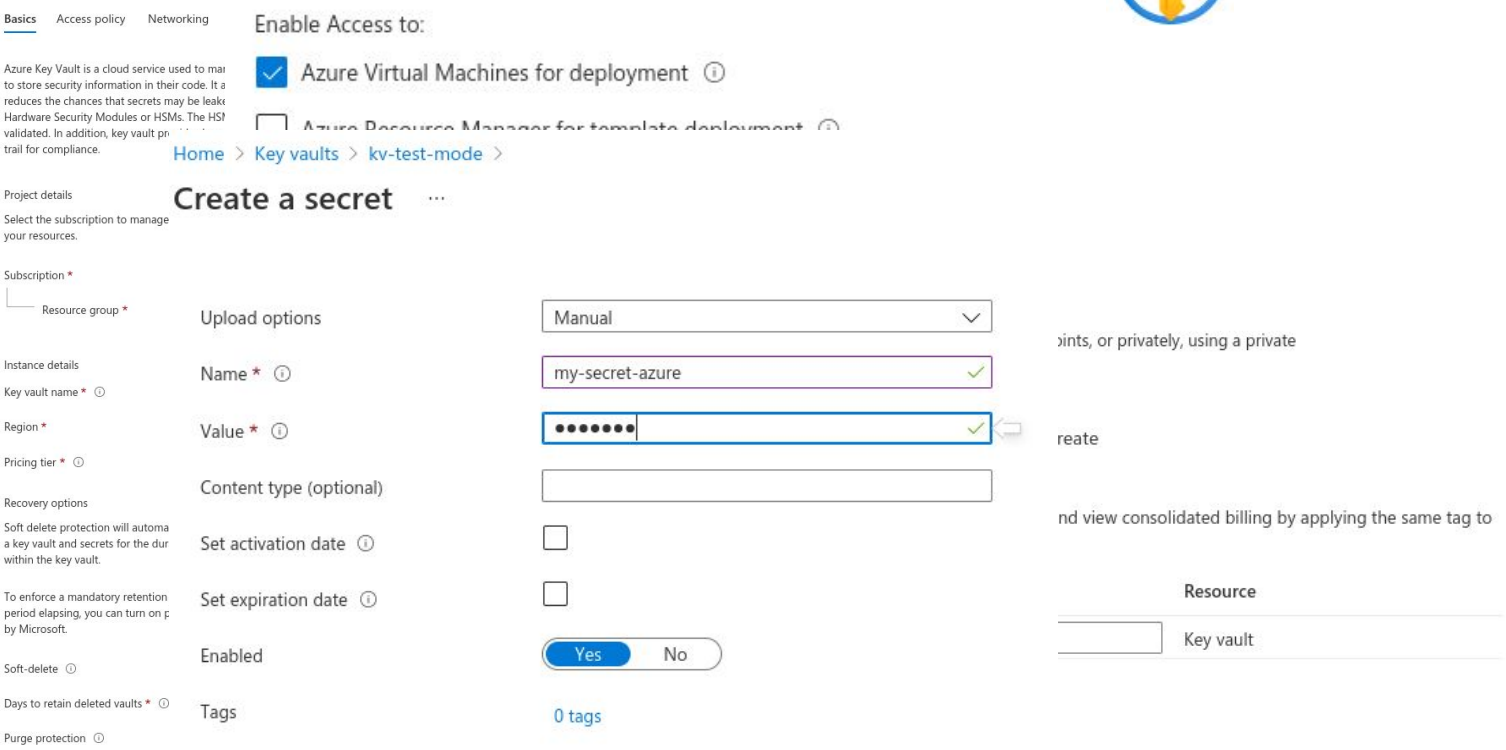
Azure - KeyVault

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.

https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts

Azure - Key Vault Secrets



Carnegie Mellon University Software Engineering Institute

DEVSECOPS DAYS LOS ANGELES

SIKAC

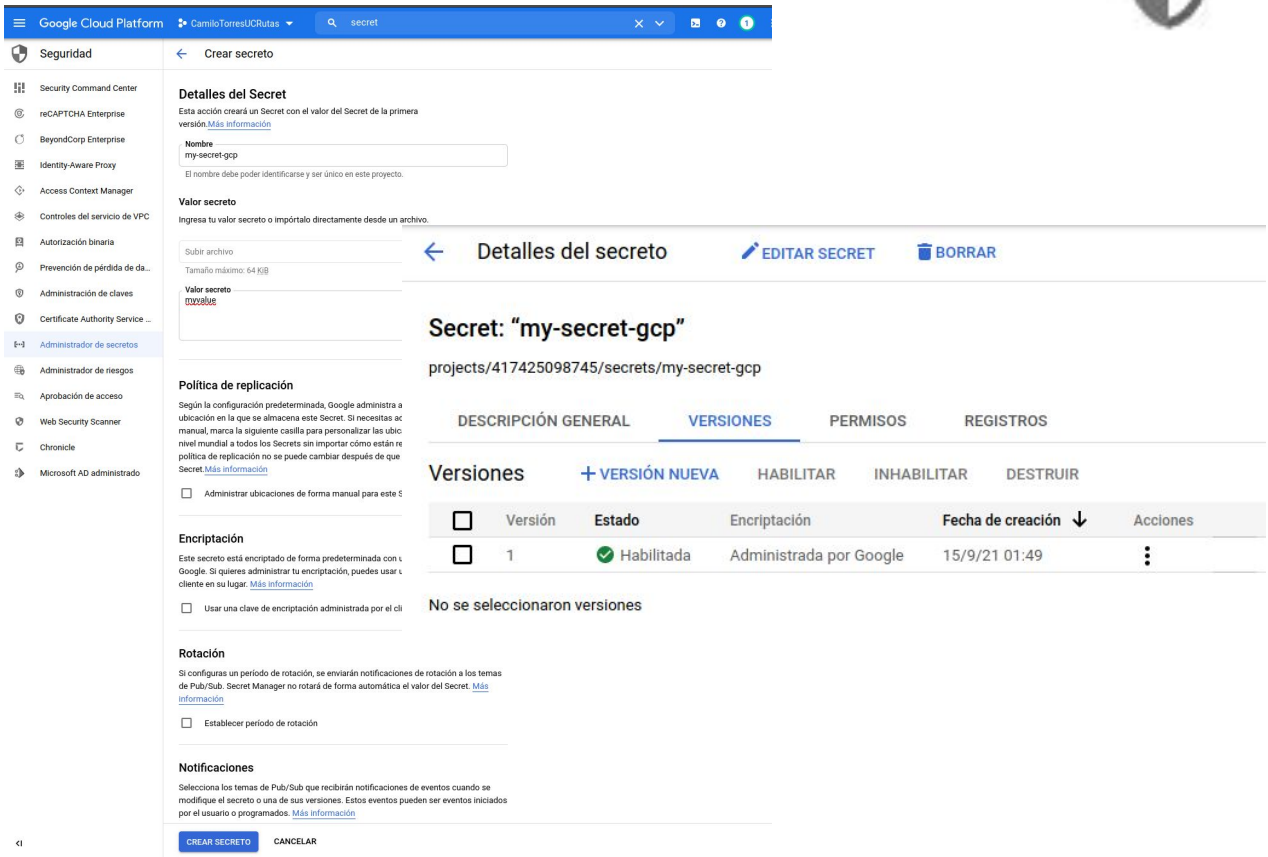
GCP - Secrets Manager

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.

https://cloud.google.com/secret-manager

GCP - Secret Manager



SIKAC

Hashicorp - Vault

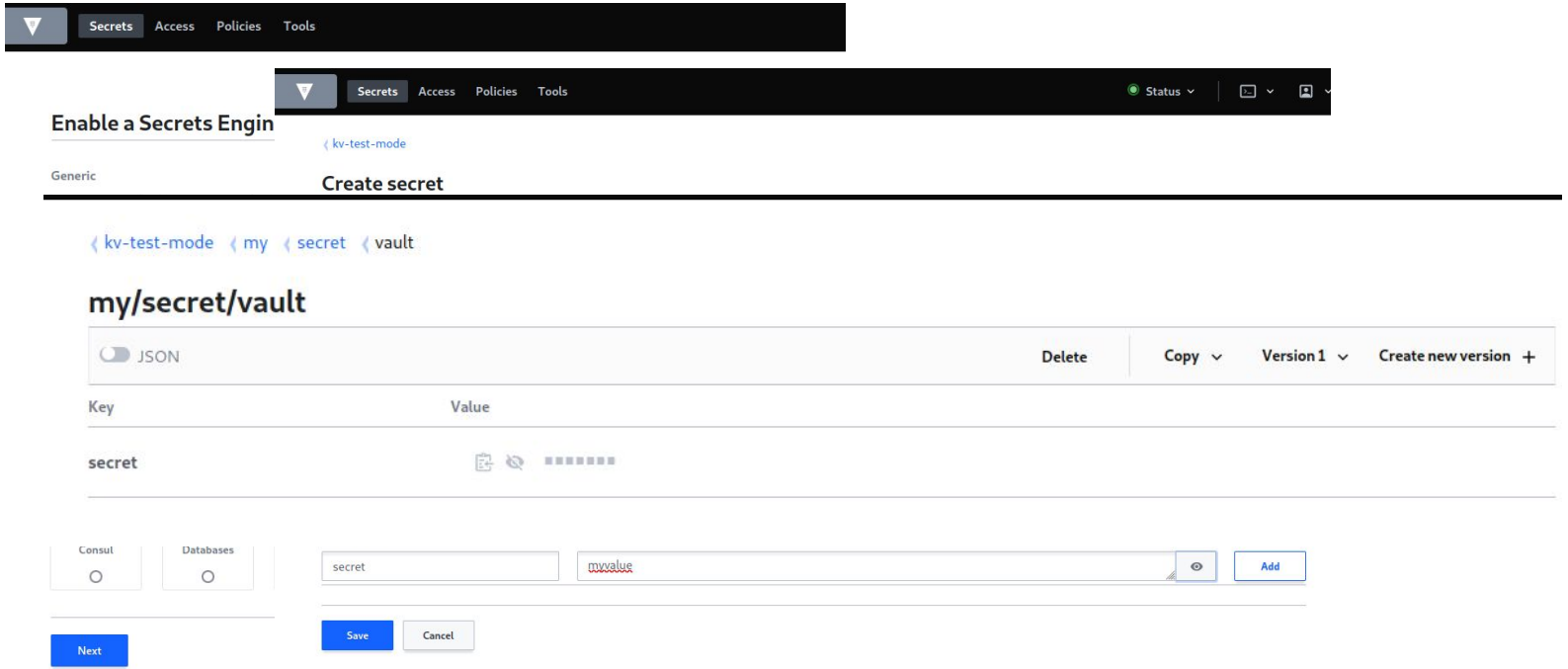
Hashicorp - Vault

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.

https://www.vaultproject.io/docs/what-is-vault

Hashicorp - Vault



Carnegie Mellon University Software Engineering Institute

DEVSECOPS DAYS LOS ANGELES

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.

https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/

Carnegie Mellon University Software Engineering Institute

DEVSECOPS DAYS LOS ANGELES

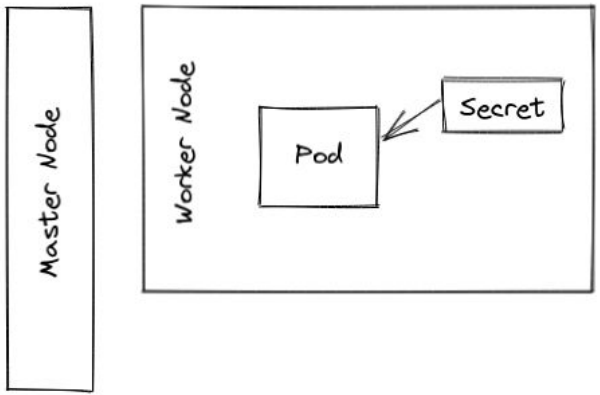
SIKAC

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.



https://kubernetes.io/docs/concepts/configuration/secret/

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.

https://external-secrets.io/

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

https://kubernetes.io/docs/concepts/extend-kubernetes/operator/

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.

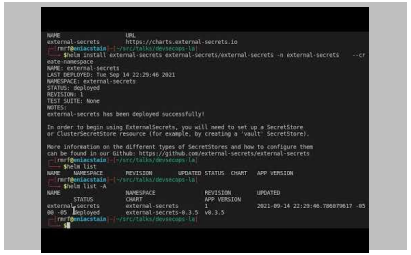
Carnegie Mellon University
Software Engineering Institute

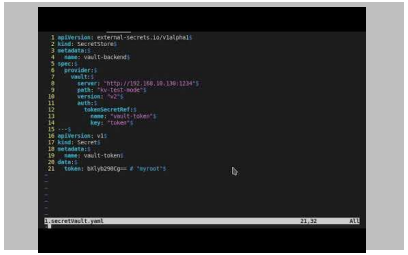
Demo Time

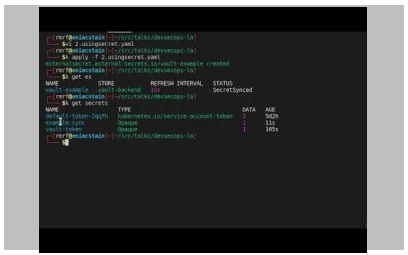
Caution
Don’t run this on Production

Flow in this demo

Back to slide 14







First create a secret in vault.

Second deploy external secrets with helm in Kubernetes cluster.

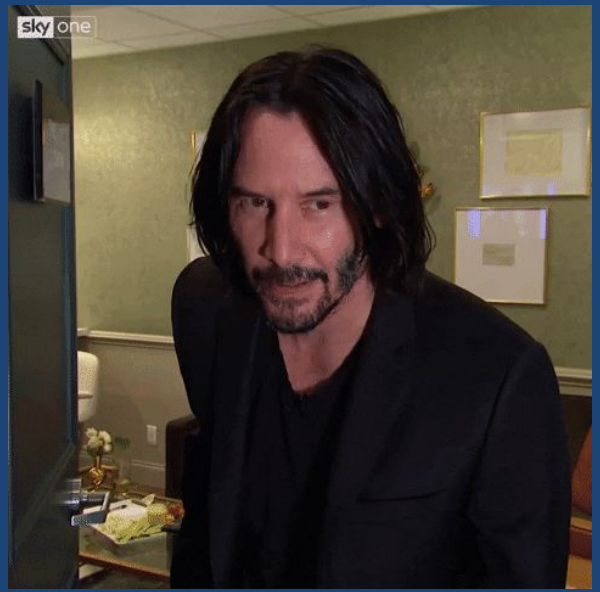
Third using external secrets operator for configure vault.

Fourth sync secret from vault to secret in kubernetes.

Questions ¿?

Carnegie Mellon University Software Engineering Institute

Thank you!!



Thank you for your time!!

I hope you learn something new!!

https://github.com/jthan24/devsecops-la