

SECRETS IN KUBERNETES ACROSS THE CLOUD

JHONNATAN GIL CHAVES



LIFE IS SIMPLE, BUT WE INSIST ON MAKING IT COMPLICATED



DO THINGS MORE EFFICIENTLY, TO IMPROVE YOUR LIFE...

AWS-SSM PARAMETER STORE

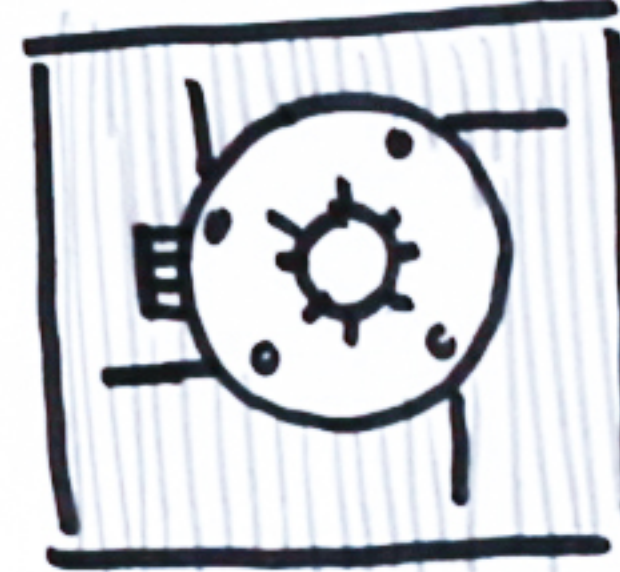
- GENERATE A LOT OF SECRETS LIKE P.W. DATABASE STRINGS & LICENSE CODES



CLOUD RESOURCE CONFIGURATION FILES

BAD PRACTICE TO ADD NAKED/UNENCRYPTED CREDENTIALS DIRECTLY IN THE CONFIG FILES

MANY CURRENT FRAMEWORKS USE VAULTS



- AWS
- ANSIBLE

EXTERNAL SECRETS OPERATOR IS A KUBERNETES OPERATOR - A SW EXTENSION THAT USE CUSTOM RESOURCES TO MANAGE APPS & COMPONENTS

EXTERNAL SECRETS ARCHITECTURE

- 1) DEFINE SECRET IN CLOUD OR LOCAL
- 2) DEPLOY EXTERNAL SECRET WITH HELM →
- 3) CONFIG THE OPERATOR TO USE THE DEPLOYED VAULT
- 4) USE SECRET FROM VAULT TO SECRET IN KUBERNETES & BRING OVER TO VAULT

A CONFIG FILE THAT TELLS THE CLOUD FRAMEWORK HOW TO DEPLOY

HASHICORP-VAULT

VAULTS: SPECIAL CONFIG FILES CONTAINING

VALUE-ATTRIBUTE-PAIRS

PROPERTY

VALUE

VAULTS ARE PROTECTED & CANNOT BE SEEN BY A HACKER

VAULTS ARE ENCRYPTED