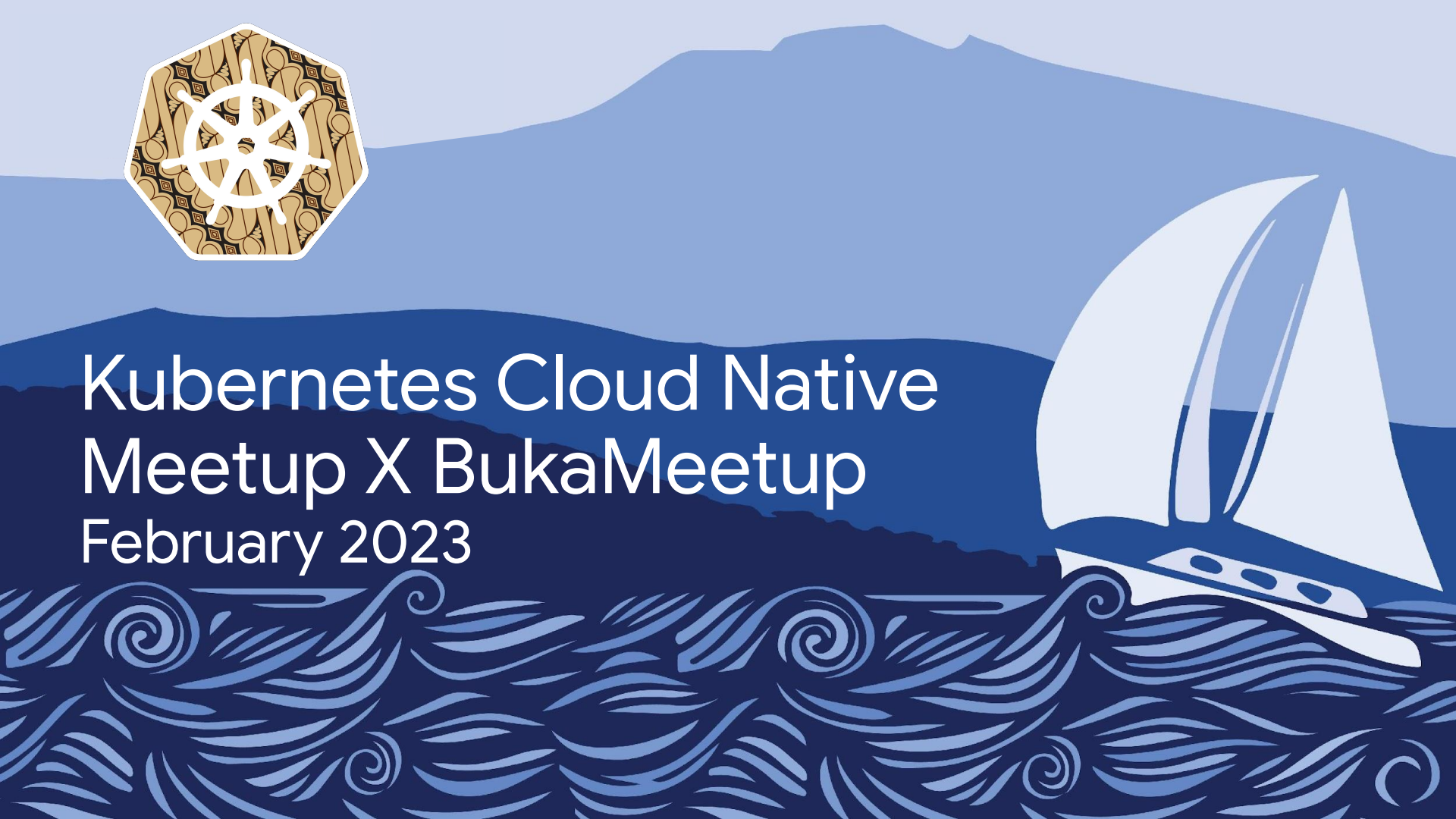

Kubernetes Cloud Native
Meetup X BukaMeetup
February 2023

Agenda

- Kubernetes Community Update
- Opening Speech from Bukalapak
- Talk #1 by **Dewangga Alam @ Bukalapak**
- Talk #2 by **Nicolas Julian @ Jubelio**
- **Q&A**
- Announcements

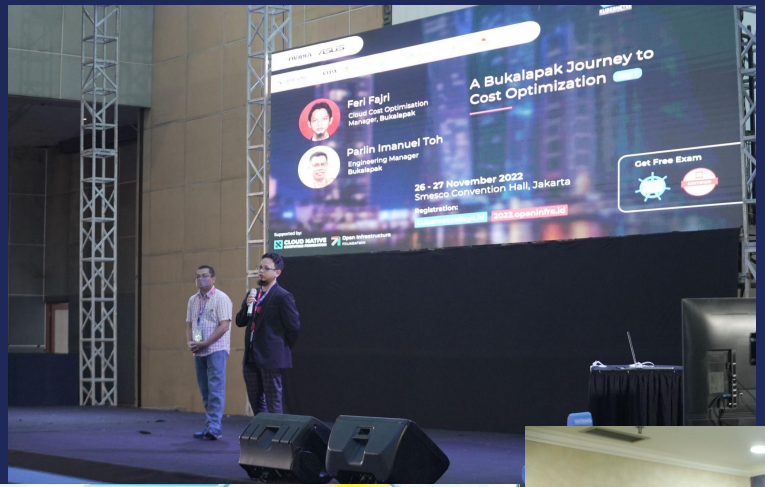
Update from Kubernetes & CloudNative Indonesia

Last Meetup

August 31, 2022

September 24, 2022

Last conference: KCD X IOD Indonesia November 26-27 2022



Last conference: KCD X IOD Indonesia November 26-27 2022

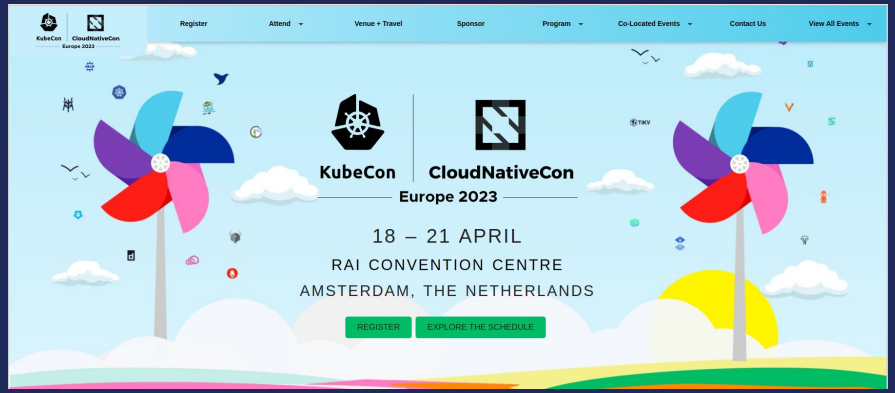
Event Documentation

bit.ly/kcd-x-iod-indonesia-photos

Speakers Talk Playlist

bit.ly/kcd-x-iod-indonesia-playlist

Next Conference: KubeCon | CloudNativeCon Europe 2023

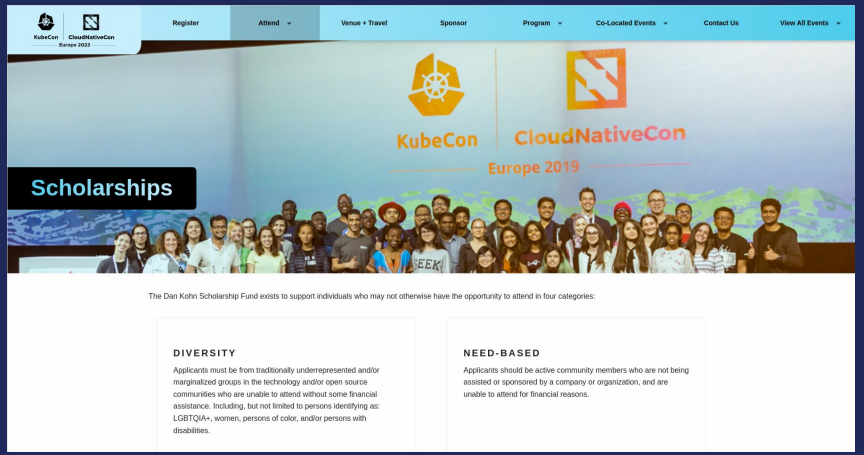


April 18-21, 2023 @ Amsterdam

events.linuxfoundation.org/kubecon-cloudnativecon-europe/

Scholarships

https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/attend/scholarships/



Our Speakers

In partnership with:
bukalapak

Kubernetes Cloud Native Indonesia Meetup Februari 2023

16 Februari 2023 | 19.00 WIB | @Bukalapak HQ
https://online.kubernetescommunity.id

Dewangga Alam
Engineering Manager @Bukalapak
K8s Component Election

Nicolas Julian
DevOps Engineer @Jubelio
Management confidential data with Vault and ArgoCD

Hosted by Kubernetes & Cloud Native Indonesia

CLOUD NATIVE COMPUTING FOUNDATION

bukalapak

Buka Meet Up

February 2023

bukalapak

Opening Speech:

Agung Wijayanto

February 2023

Let's Join With Us!

bit.ly/DevOpsBL

bukalapak

K8s Component Election

Dewangga Alam

Dewangga Alam

dewanggaba@xtremenitro.org
t.me/hostmaster

Working Experience(s) at Bukalapak

- Senior System Engineer (2018-2020)
- Engineering Manager (2020-Now)

Interest at

- Infrastructure
- Internet Security
- Networking

Overview

- Start from early 2010 - Now
- Up to **20 Gbps** traffic
- Up to **118 Terabytes** traffic per month
- **90% Infrastructure as a Code (IAC)**
- **3 different cloud provider**(s) (2 Singapore & 1 Indonesia)

bukalapak

Core Components

- **Security & Policy**
  - Hashicorp Vault
- **Traffic Management**
  - Ingress Nginx
- **Deployment Strategy**
  - Terraform
  - Helm
  - Gitlab CI
  - ArgoCD

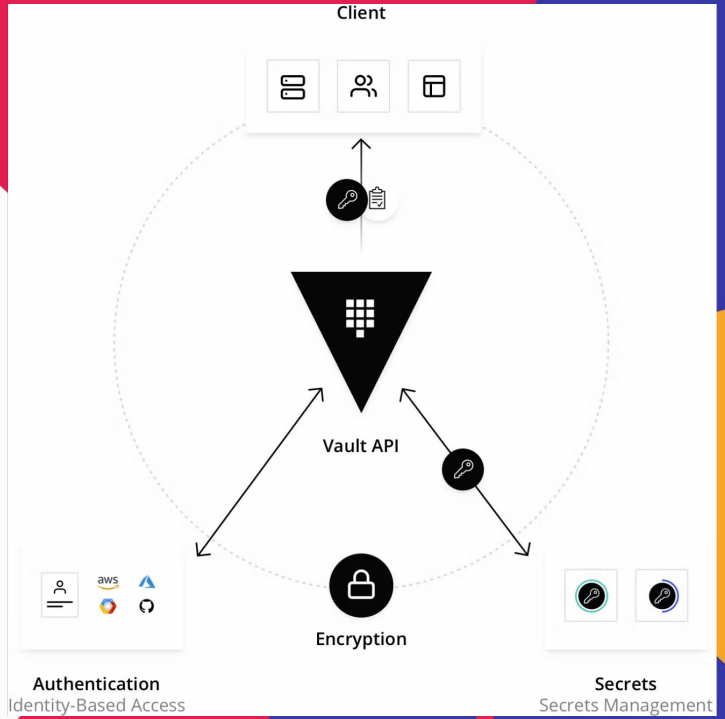
bukalapak

Security & Policy

Hashicorp Vault

It’s agnostic solution for multi-cloud deployment. We can deploy variety workload across cloud provider.

Ref: AWS Secret Manager, Azure Key Vault



bukalapak

Why Hashicorp Vault?

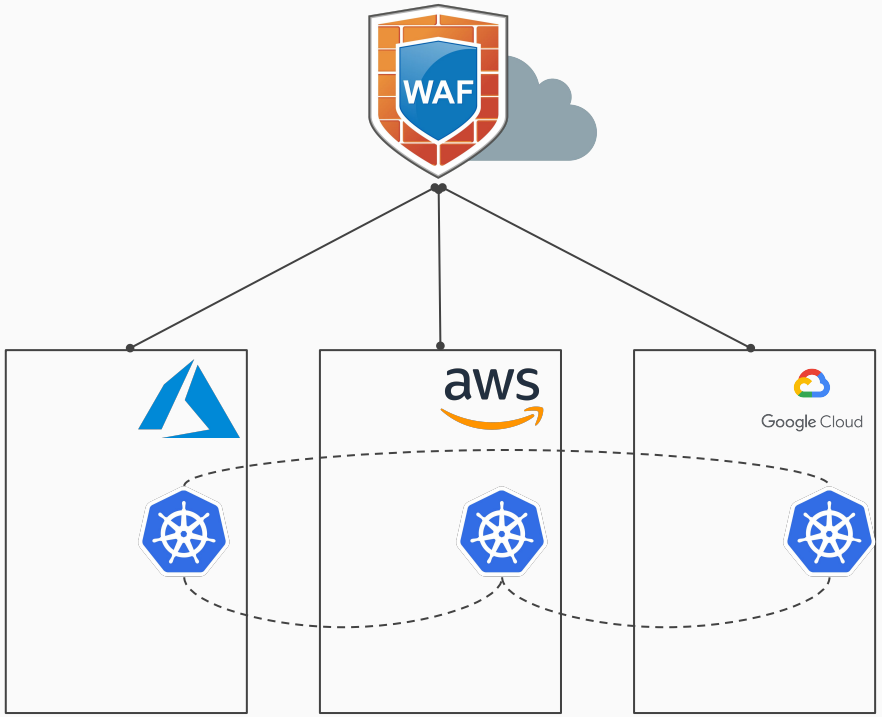
- **Agnostics!**
- Allows dynamic secret (ISO 27001 & PCI Standard)
- RBAC Support
- Self-hosted support

bukalapak

Traffic Management

Ingress Nginx

Just like other ingress, but we trust in LUA for runtime changes.



Why Ingress Nginx?

- “Official” Kubernetes Ingress
- Nginx fork with LUA Support (extra features can easily hooked/called)
- Community support (no vendor lock)
- Open sources!

bukalapak

Deployment Strategy

Terraform

	Source	Cloud	Type	Infrastructure	Language	Agent	Master	Community	Maturity
Chef	Open	All	Config Mgmt	Mutable	Procedural	Yes	Yes	Large	High
Puppet	Open	All	Config Mgmt	Mutable	Declarative	Yes	Yes	Large	High
Ansible	Open	All	Config Mgmt	Mutable	Procedural	No	No	Large	Medium
SaltStack	Open	All	Config Mgmt	Mutable	Declarative	Yes	Yes	Medium	Medium
CloudFormation	Closed	AWS	Provisioning	Immutable	Declarative	No	No	Small	Medium
Heat	Open	All	Provisioning	Immutable	Declarative	No	No	Small	Low
Terraform	Open	All	Provisioning	Immutable	Declarative	No	No	Medium	Low

bukalapak

Src: O'reilly

Deployment Strategy

Terraform (cont)

a This is the number of cookbooks in the Chef Supermarket.
b To avoid false positives for the term “chef”, I searched for “chef engineer”.
c Based on the Puppet Labs JIRA account.
d This is the number of modules in the Puppet Forge.
e To avoid false positives for the term “puppet”, I searched for “puppet engineer”.
f This is the number of reusable roles in Ansible Galaxy.
g This is the number of formulas in the Salt Stack Formulas GitHub account.
h This is the number of templates in the awslabs GitHub account.
i Based on the OpenStack bug tracker.
j I could not find any collections of community Heat templates.
k To avoid false positives for the term “heat”, I searched for “openstack”.
l This is the number of modules in the terraform-community-modules repo.

	Source	Cloud	Contributors	Stars	Commits in Sept	Bugs in Sept	Libraries	StackOverflow	Jobs
Chef	Open	All	477	4,439	182	58	3,052[a]	4,187	5,631[b]
Puppet	Open	All	432	4,158	79	130[c]	4,435[d]	2,639	5,213[e]
Ansible	Open	All	1,488	18,895	340	315	8,044[f]	3,633	3,901
SaltStack	Open	All	1,596	6,897	689	347	240[g]	614	454
CloudFormation	Closed	AWS	?	?	?	?	240[h]	613	665
Heat	Open	All	283	283	83	36[i]	0[j]	52	72[k]
Terraform	Open	All	653	5,732	440	480	40[l]	131	392

bukalapak

Src: O'reilly

Why Terraform?

- Agent-less
- Multi-cloud deployment support in a single workflow
- Community support (no vendor lock)
- Open sources!

bukalapak

How do we choose?

- **Define your goal** at the beginning
- Do the **PoC(s)**
- We prefer **leading edge** than bleeding edge
- Open Source

bukalapak

Conclusion

Know your expectations, deliver it on time, panic nicely.

Thanks!

Our Speakers

In partnership with:
bukalapak

Kubernetes Cloud Native Indonesia Meetup Februari 2023

16 Februari 2023 | 19.00 WIB | @Bukalapak HQ
https://online.kubernetescommunity.id

Dewangga Alam
Engineering Manager @Bukalapak
K8s Component Election

Nicolas Julian
DevOps Engineer @Jubelio
Management confidential data with Vault and ArgoCD

Hosted by Kubernetes & Cloud Native Indonesia

CLOUD NATIVE COMPUTING FOUNDATION

Management confidential data with Vault and ArgoCD

Kulo Sopo ?

Kulo Nicolas Julian

Sekarang bekerja sebagai “Kuli Server” di **Jubelio**.

Latar belakang, Seorang warga sipil bisa yang suka ngopi sambil *sebats*, dan *scrolling* twitter ...

1

Mau Ngomongin Apa ?

Management Secret di Kubernetes dengan bersumber dari Vault ~~di era GitOps ini ..~~

Apa yang bakal didapat dari talk ini ?

- Bagaimana caranya membuat **Custom Plugin** di ArgoCD
- Kelebihan dan Kekurangan dari setiap Secret Operator *(sependek pengetahuan saya)*
- Ideal integrasi secret managemen, “Kondisi di mana semua *confidential data* ter-sentralisasi di satu tempat, dapat di-*consume* oleh semua deployment, dan dapat di-*update* dari satu tempat tersebut”

Kemudahan dan Permasalahan baru yang dibawa GitOps (Yang saya hadapi)

Kemudahan

- Single Sources of truth.
- Make Multi Cluster deployment ezz.
- All your application is reflected from your declarative yaml file in repo.

Permasalahan

- (Sometimes) Hard Coded sensitif value in your repo.

Bagaimana menghindari “Hardcoded sensitif value”

Choose your secret management flow

1. Integrate your Kubernetes with **ExternalSecretOperator** for pulling secret from your vault.
2. Integrate your ArgoCD with **ArgoCD Vault Plugin** for pulling secret from your vault, right before your yaml deployment applied to Kubernetes Cluster.
3. Both is good too!

Apa itu ...

ArgoCD

Continuous Delivery dengan prinsip **GitOps**. (Pull base)

Hasci Vault

Sebuah Secrets Management tools.

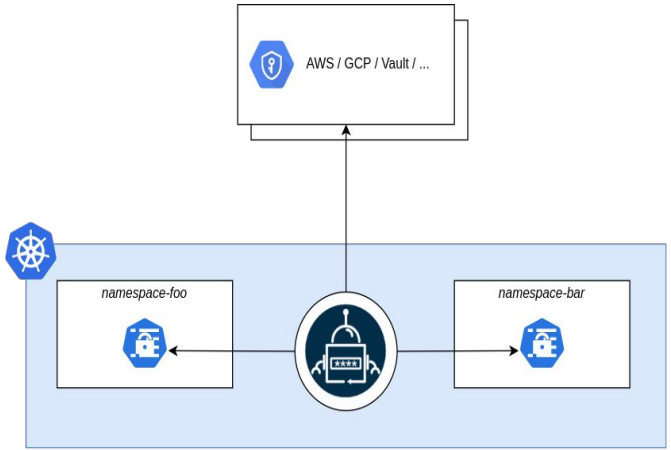
Secret Operator

- External Secret Operator
  - Kubernetes CRD for pulling secret from your vault
- ArgoCD Vault Plugin
  - Tools for filling your template yaml with secret value from vault.

Option 1

External Secret Operator

```
tmux attach -t blog
➜  secret-operator git:(main) kubectl get ns -l eso=test
NAME          STATUS   AGE
kubevirt      Active   82d
prometheus    Active   19d
➜  secret-operator git:(main) cat /tmp/testing-rate.yaml
apiVersion: external-secrets.io/v1beta1
kind: ClusterExternalSecret
metadata:
  name: eso-test
spec:
  namespaceSelector:
   matchLabels:
     eso: test
  externalSecretSpec:
    refreshInterval: "5m"
    secretStoreRef:
      name: vault-backend
      kind: ClusterSecretStore
    target:
      name: eso-test
    dataFrom:
    - extract:
        key: secret/test-secret
➜  secret-operator git:(main) kubectl get secret/eso-test -n kubevirt
NAME       TYPE     DATA   AGE
eso-test   Opaque   5      17m
➜  secret-operator git:(main) kubectl get secret/eso-test -n prometheus
NAME       TYPE     DATA   AGE
eso-test   Opaque   5      17m
➜  secret-operator git:(main)
[blog] 0:nvim- 1:zsh* 2:zsh                                  "MacBook-Pro-MAC.local" 15:42 06-Feb-23
```




Secrets
Access
Policies
demo-secret
➜ /tmp kubectl get ns -l eso=test
NAME STATUS AGE
analytic Active 13h
monitoring Active 27h
➜ /tmp nvim test-eso.yaml
➜ /tmp kubectl apply -f test-eso.yaml
clusterexternalsecret.external-secrets.io/eso-test created
➜ /tmp kubectl get secret/eso-test -n monitoring
NAME TYPE DATA AGE
eso-test Opaque 1 13s
➜ /tmp

Limitasi dari External Secret Operator

Pros

- There's some schedule **RefreshInterval** by design
- More mature project also more wide community
- Multiple namespace management secret by design

Cons

- Only support **Kind=Secret** resources
- You need to recreate the **clusterexternalsecret** if you wanna add new namespace

Contoh *Resources* Selain Secret Yang Memerlukan Sensitif Data

databaseInitSQL	object	DatabaseInitSQL defines a ConfigMap containing custom SQL that will be run after the cluster is initialized. This ConfigMap must be in the same namespace as the cluster.

To fulfil these kind of resources, we can go to **Option 2**

https://access.crunchydata.com/documentation/postgres-operator/v5/references/crd/#postgresclusterspecdatabaseinitsql

Option 2

ArgoCD (Vault) Plugin

+

Why use this plugin?

This plugin is aimed at helping to solve the issue of secret management with GitOps and Argo CD. We wanted to find a simple way to utilize Vault without having to rely on an operator or custom resource definition. This plugin can be used not just for secrets but also for deployments, configMaps or any other Kubernetes resource.

Installation ArgoCD Vault Plugin – Add Backed Vault and InitContainer

```
# Download tools
initContainers:
- name: download-tools
image: registry.access.redhat.com/ubi8
env:
  - name: AVP_VERSION
    value: 1.11.0
command: [sh, -c]
args:
  - >-
    curl -L https://github.com/argoproj-labs/argocd-vault-plugin
    chmod +x argocd-vault-plugin &&
    mv argocd-vault-plugin /custom-tools/
volumeMounts:
  - mountPath: /custom-tools
    name: custom-tools
volumes:
- configMap:
    name: cmp-plugin
  name: cmp-plugin
- name: custom-tools
  emptyDir: {}
```

```
apiVersion: v1
stringData:
  VAULT_ADDR: http://vault.myvaultserver.com
  AVP_AUTH_TYPE: github
  AVP_GITHUB_TOKEN: t0ke3nsecret
  AVP_TYPE: vault
kind: Secret
metadata:
  name: argocd-vault-plugin-credentials
  namespace: argocd
type: Opaque
```

```
containers:
- name: argocd-repo-server
volumeMounts:
- name: custom-tools
  mountPath: /usr/local/bin/argocd-vault-plugin
  subPath: argocd-vault-plugin
envFrom:
  - secretRef:
      name: argocd-vault-plugin-credentials
```

Installation ArgoCD Vault Plugin – Add Cluster Role and Mount SA-Token

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: argocd-repo-server
spec:
  template:
    spec:
      serviceAccount: argocd-repo-server
      serviceAccountName: argocd-repo-server
      automountServiceAccountToken: true
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  # "namespace" omitted since ClusterRoles are not namespaced
  name: argocd-vault
rules:
- apiGroups: [""]
  #
  # at the HTTP level, the name of the resource for accessing Se
  # objects is "secrets"
  resources: ["secrets"]
  verbs: ["get", "watch", "list"]
---
apiVersion: rbac.authorization.k8s.io/v1
# This cluster role binding allows anyone in the "manager" group
kind: ClusterRoleBinding
metadata:
  name: read-secrets-argocd-repo-server
subjects:
- kind: ServiceAccount
  name: argocd-repo-server
  namespace: argocd
roleRef:
  kind: ClusterRole
  name: argocd-vault
  apiGroup: rbac.authorization.k8s.io
```

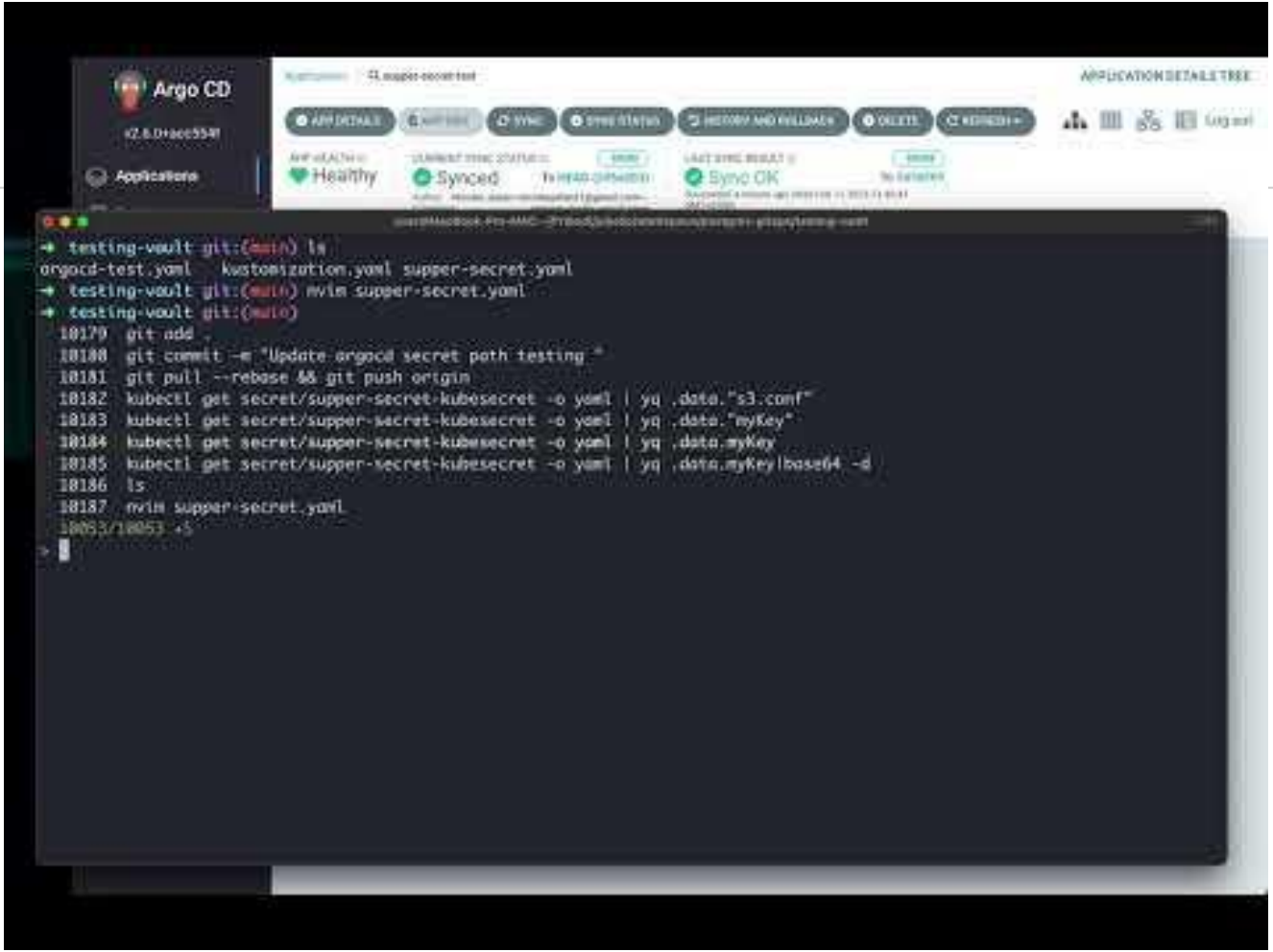
Installation ArgoCD Vault Plugin – Config Plugin

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: cmp-plugin
data:
  avp-kustomize.yaml: |
    ---
    apiVersion: argoproj.io/v1alpha1
    kind: ConfigManagementPlugin
    metadata:
      name: argocd-vault-plugin-kustomize
    spec:
      allowConcurrency: true

      # Note: this command is run _before_ anything is done, therefore the logic is to check
      # if this looks like a Kustomize bundle
      discover:
        fileName: "./kustomization.yaml"
      generate:
        command:
          - sh
          - "-c"
          - "kustomize build . |  argocd-vault-plugin generate --secret-name argocd:argocd-vault-plugin-credentials -"
      lockRepo: false
---
```

https://nicolas.my.id/sebuah-cerita-implementasi-gitops-part-2/

```yaml
# argocd-vault-plugin with Kustomize
- name: avp-kustomize
command: [/var/run/argocd/argocd-cmp-server]
image: quay.io/argoproj/argocd:v2.4.0
securityContext:
  runAsNonRoot: true
  runAsUser: 999
volumeMounts:
  - mountPath: /var/run/argocd
    name: var-files
  - mountPath: /home/argocd/cmp-server/plugins
    name: plugins
  - mountPath: /tmp
    name: tmp
  # Register plugins into sidecar
  - mountPath: /home/argocd/cmp-server/config/plugin.yaml
    subPath: avp-kustomize.yaml
    name: cmp-plugin
  # Important: Mount tools into $PATH
  - name: custom-tools
    subPath: argocd-vault-plugin
    mountPath: /usr/local/bin/argocd-vault-plugin
```


Argo CD
Applications
APPLICATION DETAILS TREE
Healthy
Synced
Sync OK
→ testing-vault git:(main) ls
orgocd-test.yaml kustomization.yaml supper-secret.yaml
→ testing-vault git:(main) nvim supper-secret.yaml
→ testing-vault git:(main)
10179 git add .
10180 git commit -m "Update orgocd secret path testing "
10181 git pull --rebase && git push origin
10182 kubectl get secret/supper-secret-kubesecret -o yaml | yq .data."s3.conf"
10183 kubectl get secret/supper-secret-kubesecret -o yaml | yq .data."myKey"
10184 kubectl get secret/supper-secret-kubesecret -o yaml | yq .data.myKey
10185 kubectl get secret/supper-secret-kubesecret -o yaml | yq .data.myKey|base64 -d
10186 ls
10187 nvim supper-secret.yaml

Limitasi dari ArgoCD Vault Plugin

Pros

- Handle all resources k8s
- ArgoCD Ecosystem

Cons

- **Required hard refresh the application**, if we want to pull new values from vault
- Required third party tools like reflector or create multi application in all wanted namespace where resources contain sensitive data going to deploy

Only choose what you need!

Pilih Solusi Sesuai Kebutuhan, Apabila tidak ada keperluan konfidensial data di luar *Kind=Secret* maka Externalsecret.io operator adalah pilihan paling cocok!

Thanks!

Any questions ?

You can find me at

- nicolas.my.id
- me@nicolas.my.id

QnA

Photo Session

bukalapak

Let's Join With Us!

bit.ly/DevOpsBL

Feedback Form

We love to hear your feedbacks and thoughts for the event by fill out or scan the feedback form!

bit.ly/BLKubernetes_Feedback

Thank You