BANZAICLOUD

Detecting and Blocking Vulnerable Containers in K8s

Nándor **Krácser**
Péter **Balogh**

Mar 28, 2019

Who are we?

“We are building the operating system
for your containers and clouds”

“Based on Kubernetes, we take care of all the detail
that makes developers ecstatic, ops people a little less grumpy,
and your finance guy feel like he's a rock star”

https://banzaicloud.com/

How can we improve image security of K8s?

Strategies for preventing vulnerable containers:

- Use only trusted images
- Scan images in deploy time

Image scanning tools:

- CoreOS Clair
- OpenScap
- Anchore-engine

What are we doing?

- Installing minikube or other K8s environment if it doesn’t exist in your machine
- Installing Helm if it doesn’t exist in your machine
- Deploying Anchore-engine as a vulnerability scanner
  - using helm
- Deploying *Validating Webhook* in K8s cluster
  - using helm
- Deploying test deployments in K8s and waiting for results

K8s Dynamic Admission Control

- Kubernetes can be easily extended via *Admission Webhooks*
- There are two types of admission webhooks:
  - Validating
  - Mutating
- https://banzaicloud.com/blog/k8s-admission-webhooks/

What are we using?

Anchore-engine

https://github.com/anchore/anchore-engine

Helm chart:

https://github.com/helm/charts/blob/master/stable/anchore-engine/

Banzaicloud's anchore-image-validator as a Validating Webhook:

https://github.com/banzaicloud/anchore-image-validator

Helm chart:

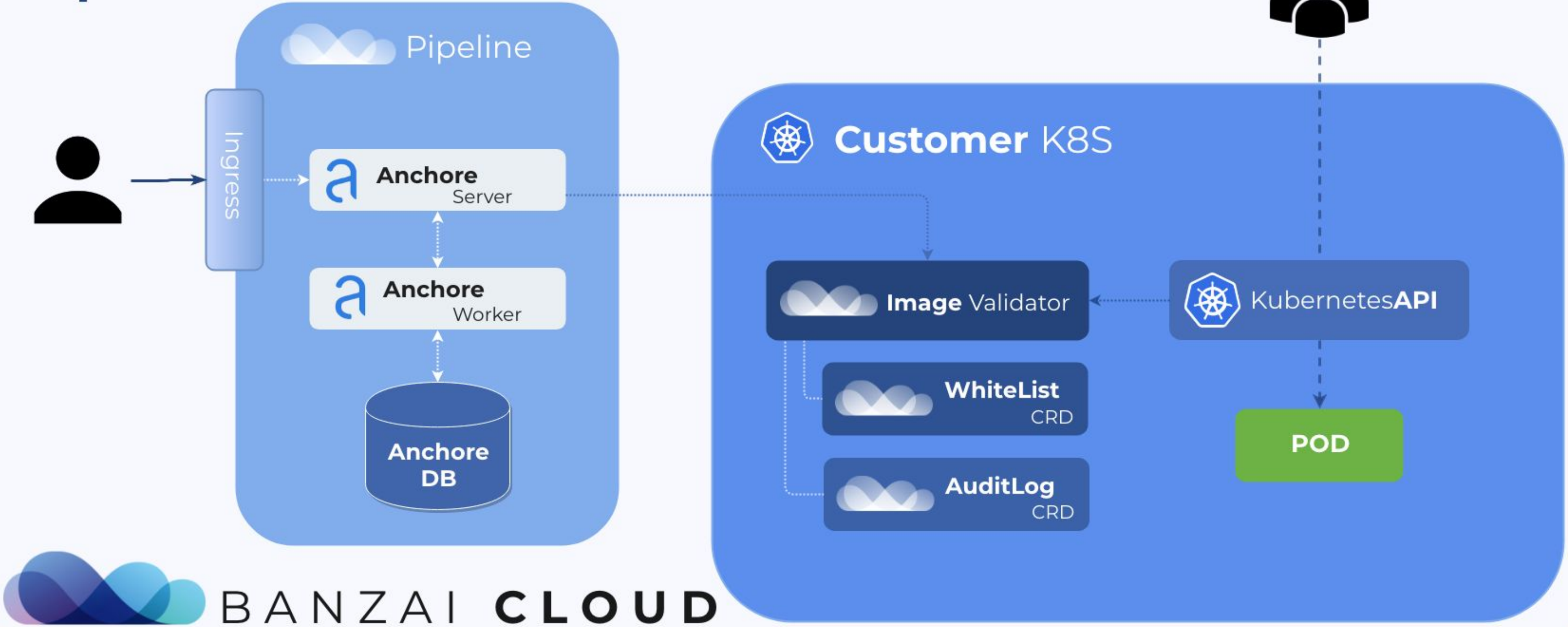
https://github.com/banzaicloud/banzai-charts/tree/master/anchore-policy-validator

Workshop repo:

https://github.com/pbalogh-sa/bsidesbud-workshop

How does it work?

Image Security Flow with **Pipeline**



BANZAI CLOUD

https://banzaicloud.com/blog/anchore-image-validation/

Running K8s in local environment

Mac

- Minikube
- Docker-for-desktop
- Kind
- PKE

Virtualizations:

- VirtualBox, Hyperkit
- HyperKit
- HyperKit, Docker
- Vagrant, Virtualbox

Windows

- Minikube
- Docker-for-desktop
- PKE

Virtualizations:

- VirtualBox, Hyper-V
- Hyper-V
- Vagrant, Virtualbox

GNU/Linux

- Minikube
- Kind
- PKE

Virtualizations:

- VirtualBox, KVM
- Docker
- Vagrant, Virtualbox

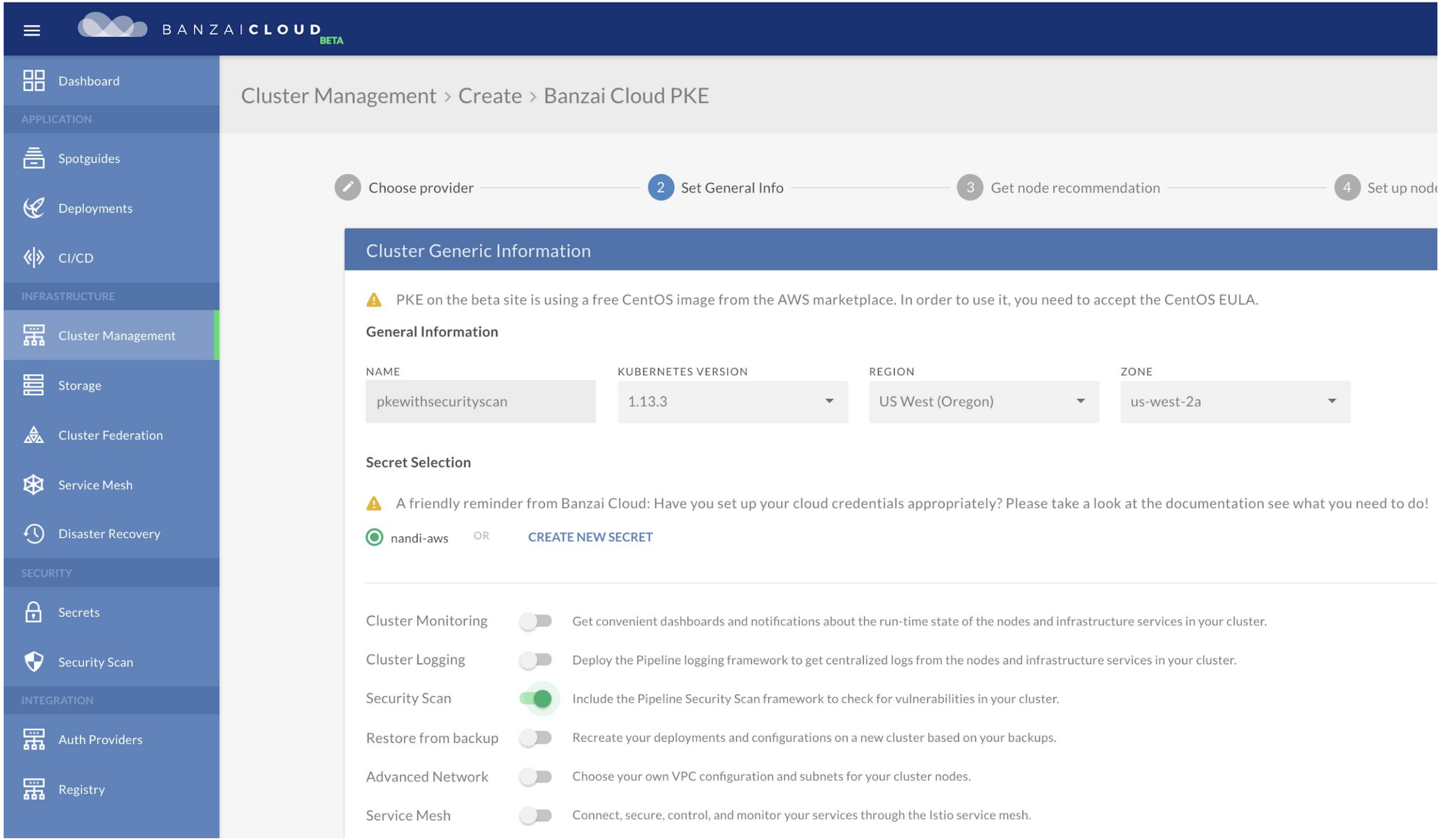
https://github.com/banzaicloud/pke

BANZAI CLOUD

The proof of the pudding is in the eating.

https://github.com/pbalogh-sa/bsidesbud-workshop

It works out of the box in Pipeline: https://beta.banzaicloud.io



Cluster Management > Create > Banzai Cloud PKE

Choose provider — 2 Set General Info — 3 Get node recommendation — 4 Set up node

Cluster Generic Information

⚠ PKE on the beta site is using a free CentOS image from the AWS marketplace. In order to use it, you need to accept the CentOS EULA.

General Information

NAME	KUBERNETES VERSION	REGION	ZONE
pkewithsecurityscan	1.13.3	US West (Oregon)	us-west-2a

Secret Selection

⚠ A friendly reminder from Banzai Cloud: Have you set up your cloud credentials appropriately? Please take a look at the documentation see what you need to do!

● nandi-aws OR CREATE NEW SECRET

Cluster Monitoring	Off	Get convenient dashboards and notifications about the run-time state of the nodes and infrastructure services in your cluster.
Cluster Logging	Off	Deploy the Pipeline logging framework to get centralized logs from the nodes and infrastructure services in your cluster.
Security Scan	On	Include the Pipeline Security Scan framework to check for vulnerabilities in your cluster.
Restore from backup	Off	Recreate your deployments and configurations on a new cluster based on your backups.
Advanced Network	Off	Choose your own VPC configuration and subnets for your cluster nodes.
Service Mesh	Off	Connect, secure, control, and monitor your services through the Istio service mesh.

Questions?!

BANZAI **CLOUD**