



B A N Z A I **C L O U D**

Biztonsági megoldások automatizálása Kubernetes környezetben

Balogh Péter



- RBAC
- Titok tárolás
- Konténer képfájl megbízhatóság
- Alkalmazás biztonság
- Hálózat biztonság
- Admission plugin
- Audit log
- Node biztonság



- RBAC
- Titok tárolás
- Konténer képfájl megbízhatóság
- Alkalmazás biztonság
- Hálózat biztonság
- Admission plugin
- Audit log
- Node biztonság



Autentikáció

- X509 kliens tanúsítvány
- Statikus token file
- Bootstrap token
- Statikus jelszó file
- ServiceAccount token
- OpenID Connect token
- Webhook token autentikáció
- Autentikációs proxy

Autorizáció

- node - a kubelet API kéréseinek autorizációja
- ABAC - Attribute-based access control
(felváltotta az RBAC)
- RBAC - Role-based access control
- Webhook - HTTP callback



Saját K8s cluster esetén

- OpenID connect token

```
--oidc-issuer-url=<openid-issuer>  
--oidc-client-id=<client-id>  
--oidc-ca-file=<CA-cert>  
--oidc-username-claim=<JWT-claim-to-username>  
--oidc-groups-claim=<JWT-claim-to-groups>
```

- Webhook token autentikáció

authn

```
--authentication-token-webhook-config-file=<authn-config-file>  
--authentication-token-webhook-cache-ttl=<access-cache-timeout>
```

- Webhook mód autorizáció

authz

```
--authorization-webhook-config-file=<authz-config-file>
```



Provider managed K8s cluster esetén

- Kubernetes API szerver hozzáférés hiánya
- Áthidaló megoldás OpenID felhasználásával
- Dex - OpenID connect provider
- Banzai Cloud jwt-to-rbac

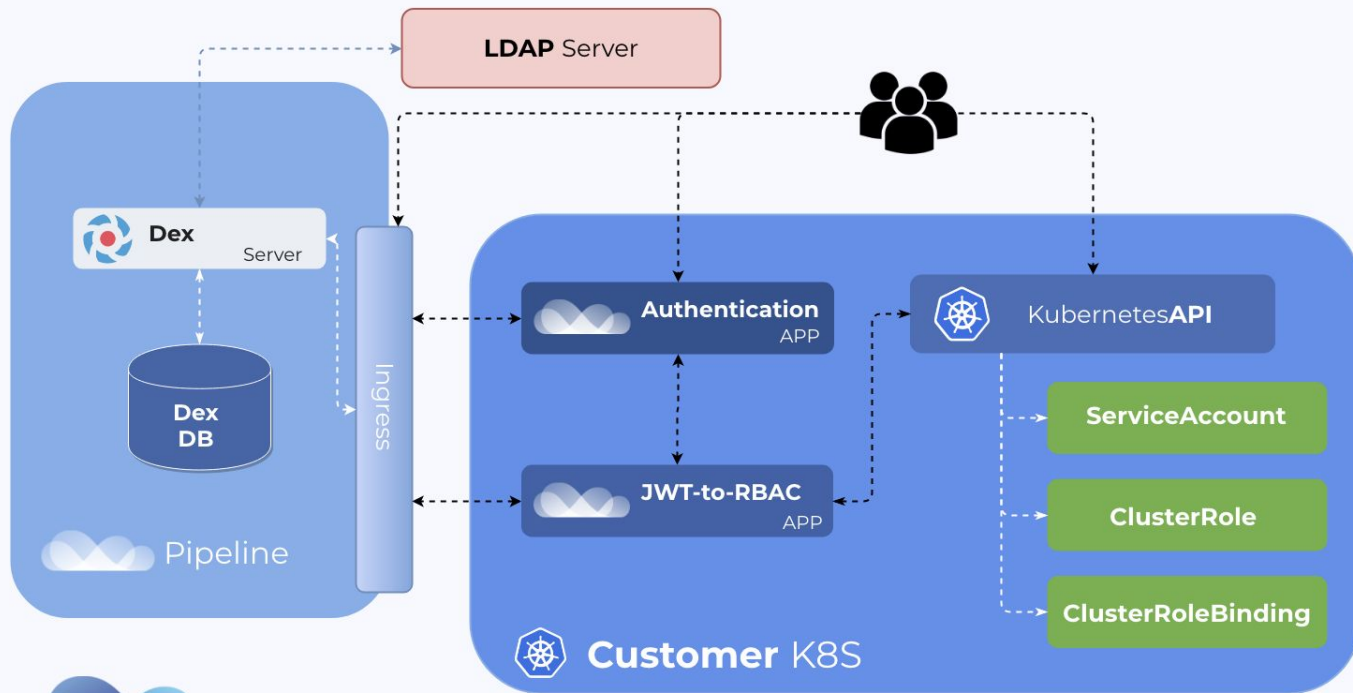
<https://github.com/dexidp/dex>

<https://github.com/banzaicloud/jwt-to-rbac>

<https://banzaicloud.com/blog/k8s-rbac/>



JWT-to-RBAC Flow





Bank Vaults (Vault svájci bicska és operátor)

Automata unseal, token megújítás

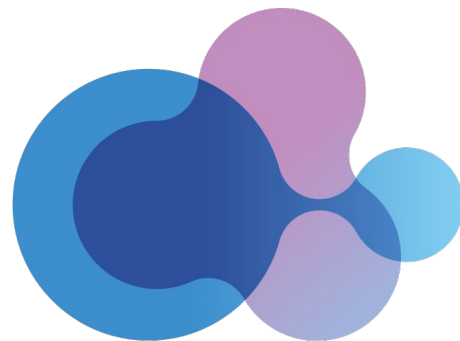
Kubernetes támogatás

Titok injektálás (mutating webhook)

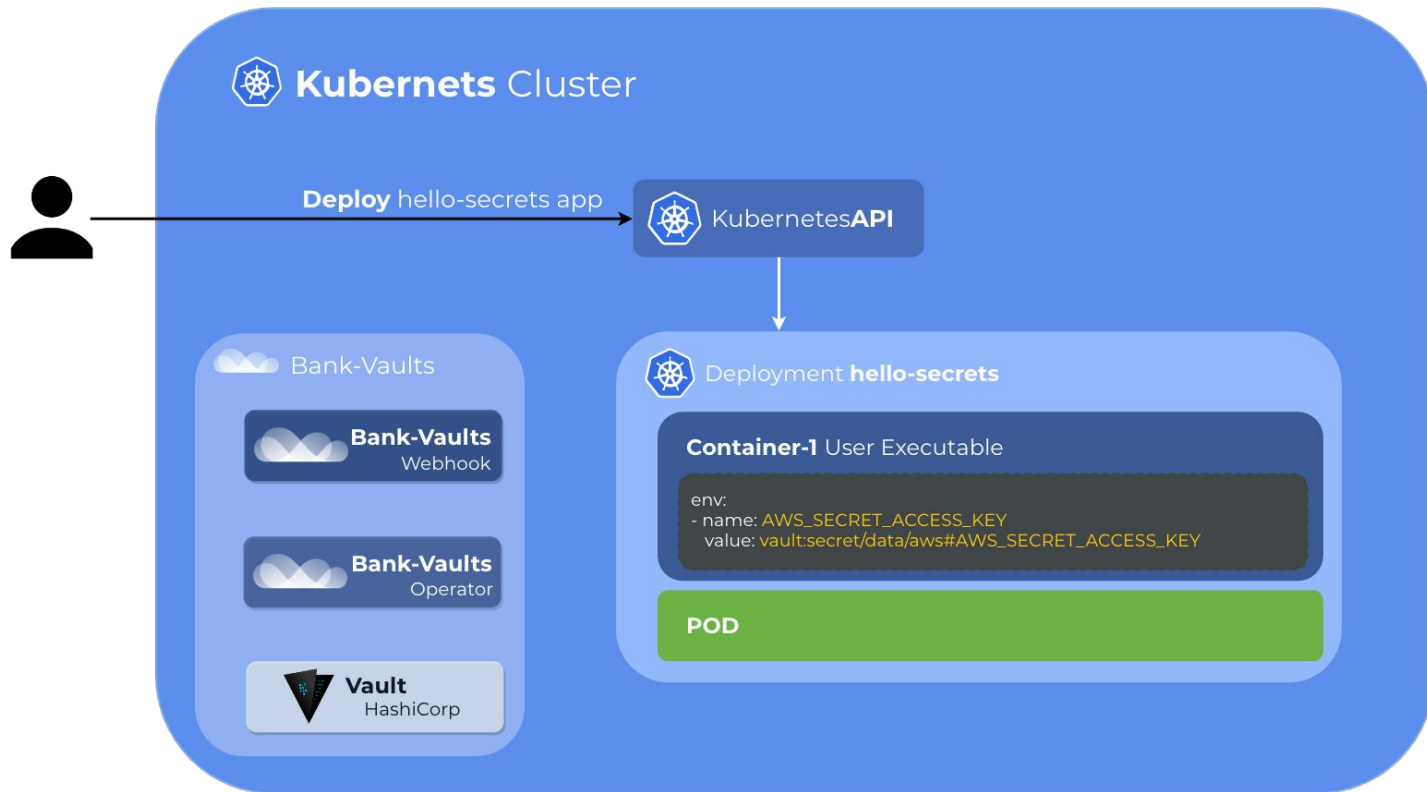
<https://www.vaultproject.io/>

<https://github.com/banzaicloud/bank-vaults>

<https://banzaicloud.com/tags/bank-vaults/>



bank-vaults
BY BANZAICLOUD





Konténer képfájlok sérülékenység vizsgálata

Egy meghatározott policy alapján ad vissza eredményt

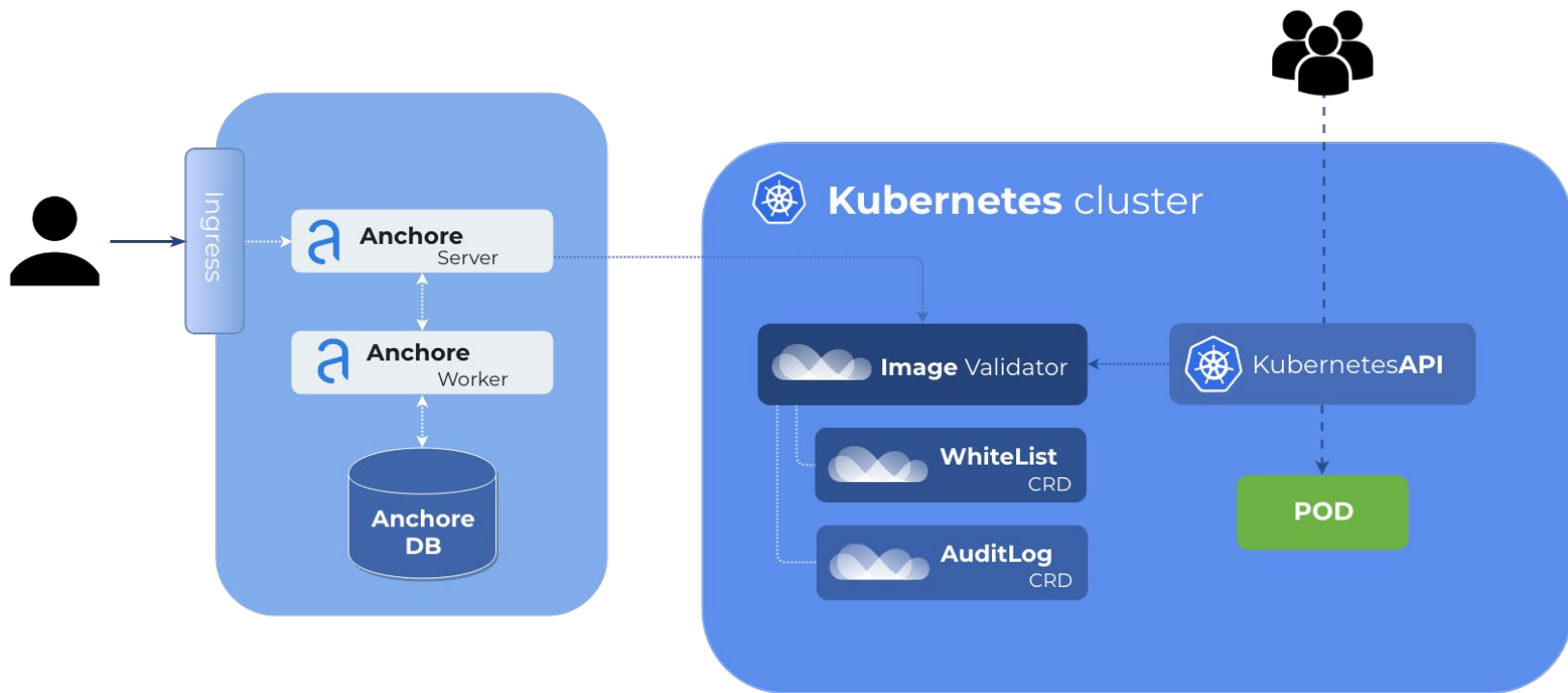
Automatikus vizsgálat megvalósítása egy alkalmazás
telepítése során



<https://anchore.com/opensource/>

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

<https://banzaicloud.com/tags/vulnerability/>





Banzaicloud DAST operátor

OWASP Zed Attack Proxy felhasználásának automatizálása

<https://github.com/zaproxy/zaproxy>

<https://github.com/banzaicloud/dast-operator>

<https://banzaicloud.com/tags/dast/>





CustomResource alapján (operátor)

- OWASP Zed Attack Proxy telepítés K8s környezetbe
- meghatározott URL alapján indítja a tesztet

Service annotációi alapján (operátor)

- elindítja a service vizsgálatát
- API vizsgálat indítása OpenAPI definíció alapján

Ingress annotációi alapján (webhook)

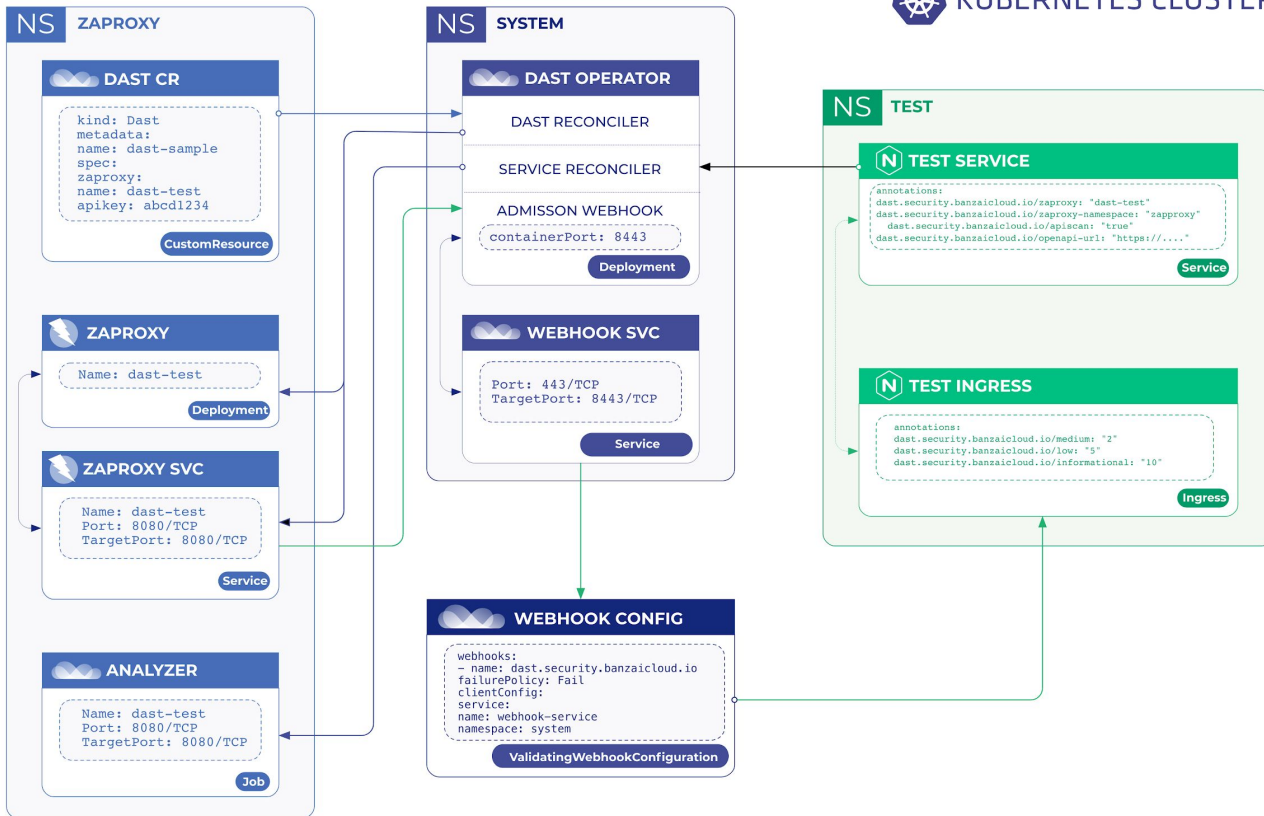
- megkeresi az ingress mögött lévő serviceket
- azok teszt eredményeit elkéri a ZAPProxy-tól
- annotáció alapján engedi/nem engedi létrehozni az ingress objektumot

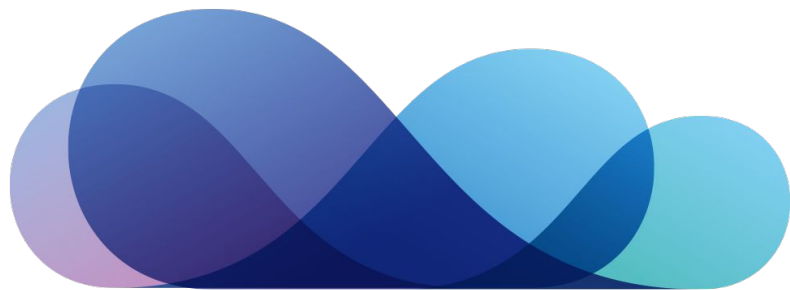


DAST operator



KUBERNETES CLUSTER





BANZAI **CLOUD**