GOTC

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

OPEN SOURCE , OPEN WORLD

「云原生」专场

利用 Tekton + ArgoCD 打造云原生 GitSecOps

马景贺 2021年7月10日

马景贺（小马哥）

LFAPAC 开源布道师/华为云 MVP

ZTE/ LTE 4G开发

IBM/DevOps

中国 DevOps 社区成员、组织者、讲师

云原生社区管委会成员/持续交付 SIG 发起人

01 云原生应用交付之痛

02 痛则思变

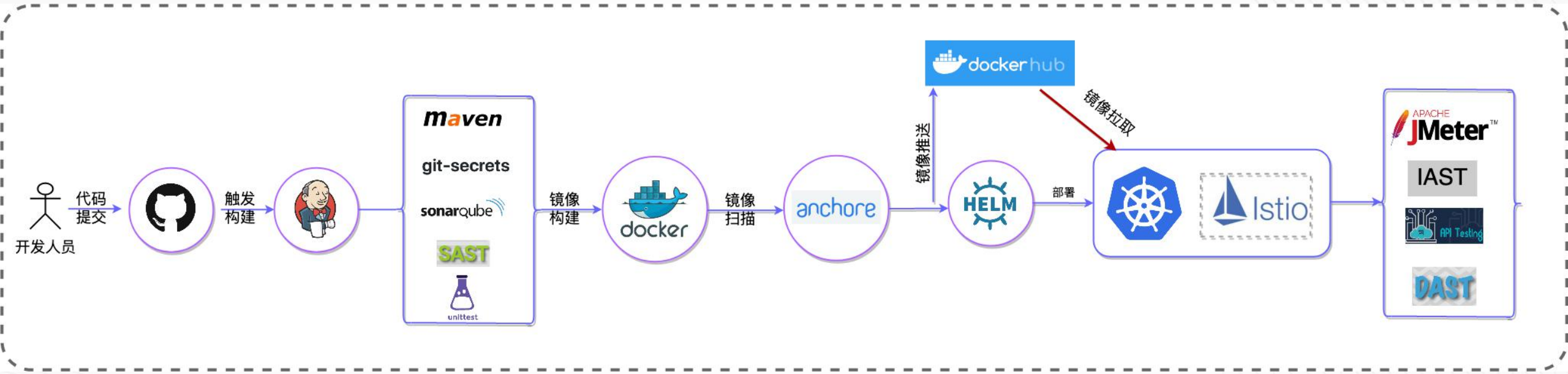
03 GitOps 之殇：敏感信息 & 镜像之谜

04 GitSecOps 体系

05 GitSecOps 之思

01 云原生应用交付之痛

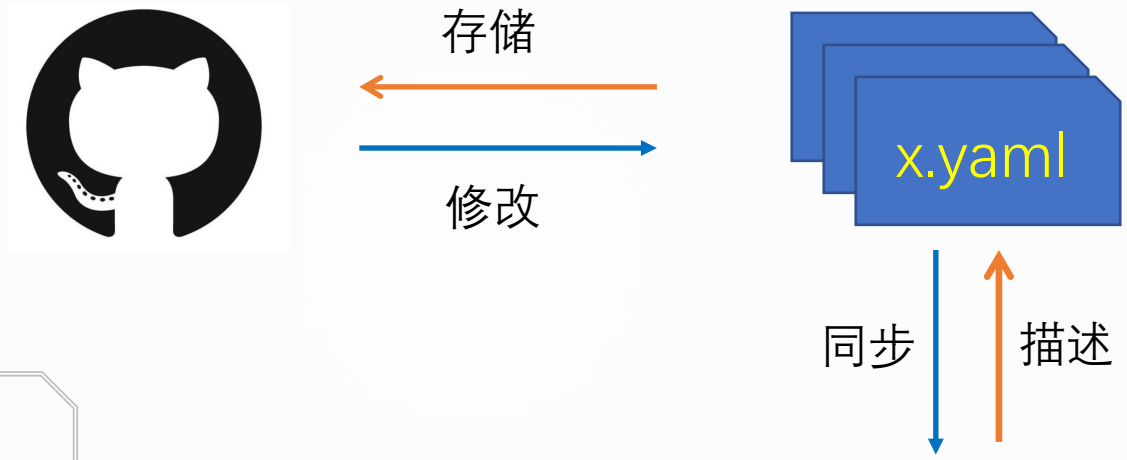
曾经的那些灵魂拷问



- 环境上的信息是什么（资源、环境变量、等）
- 版本相关的信息（发布时间、版本历史）
- 安全相关（具有 kubernetes 集群权限的人员列表，操作权限）
- ……

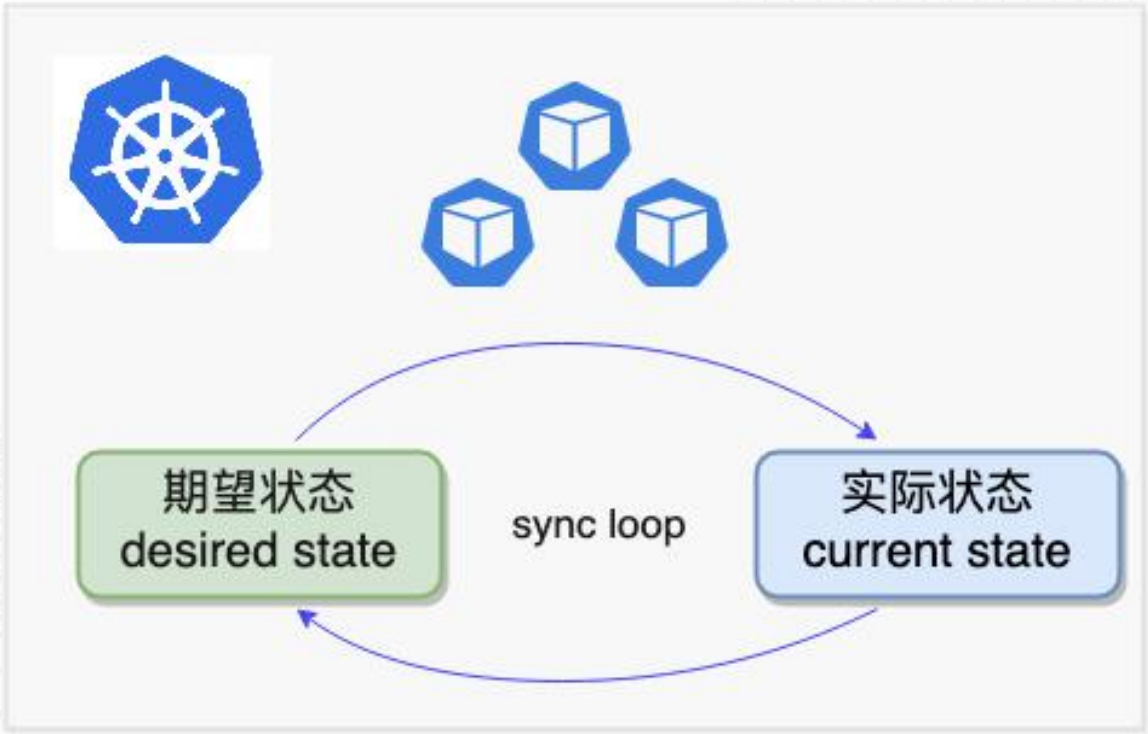
02 痛则思变

痛则思变



GitOps

- ✓ 以声明式系统为基座（典型如k8s）
- ✓ 以Git（GitHub/GitLab）为单一可信源



GitOps 之爽

GOTC

- 用户体验提升（开发、Prod Admin）
- 部署简单
- 回滚快速
- 安全性提高
- 合规审计变得容易

pull request

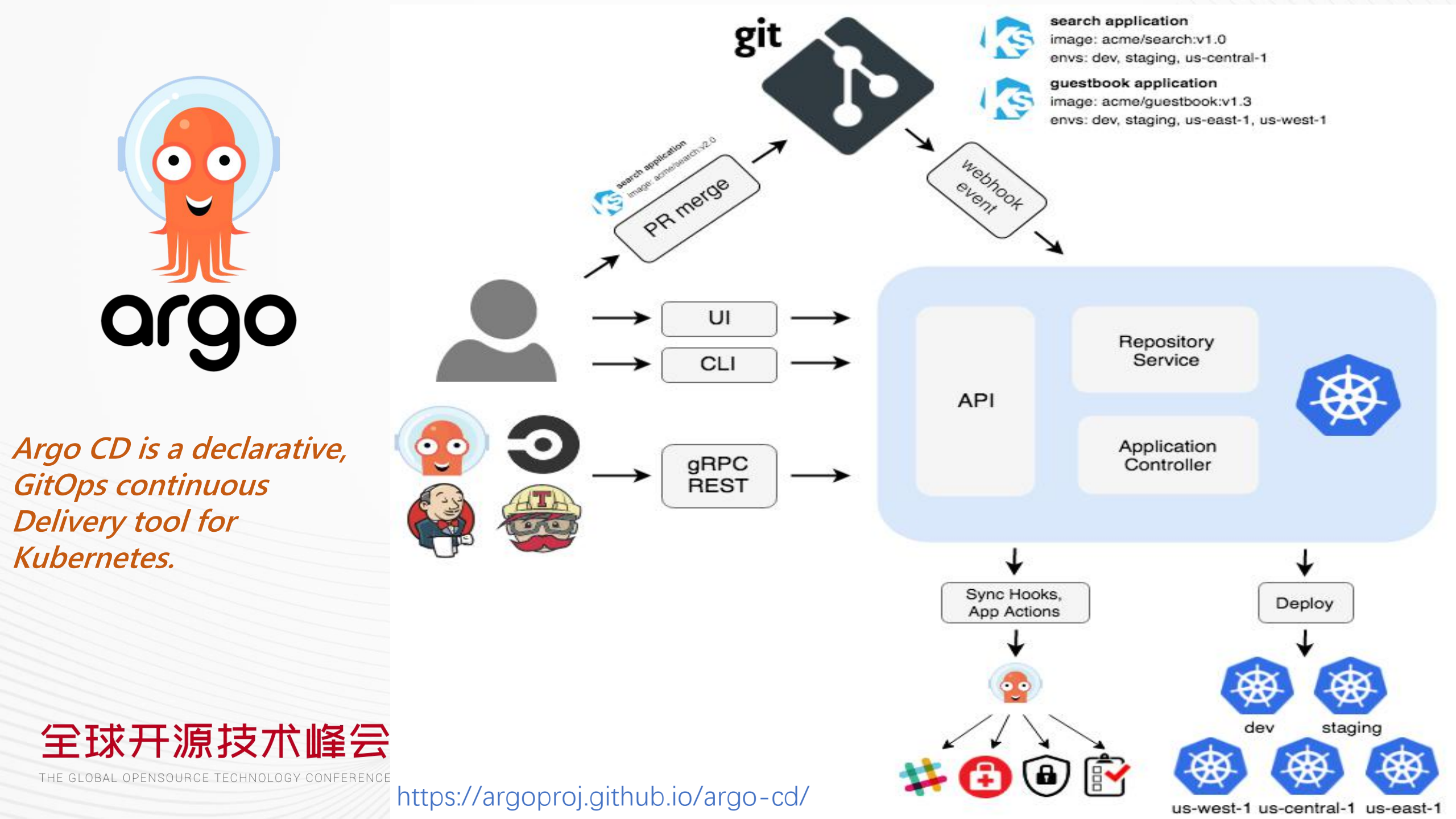
监听

gitops

同步

flux

argo



Argo CD is a declarative, GitOps continuous Delivery tool for Kubernetes.

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

https://argoproj.github.io/argo-cd/

03 GitOps 之殇：敏感信息 & 镜像之谜

敏感信息之殇

GOTC

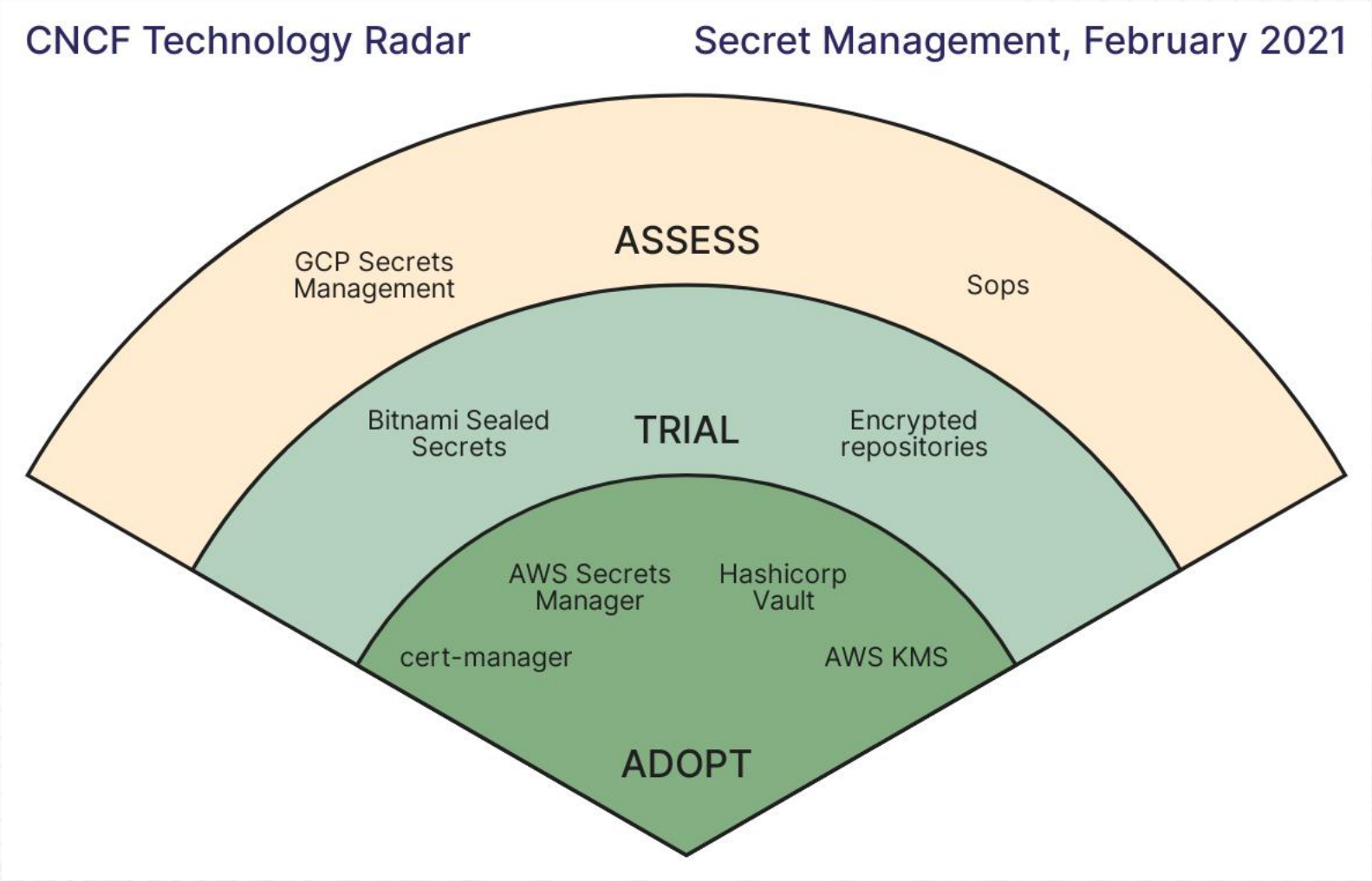
```yaml
apiVersion: v1
kind: Secret
metadata:
  name: senstive-data
data:
  username: xiaomage
  password: Cloud Native DevSecOps
  conference: GOTC
  token: dffwedfedde22

```

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: senstive-data
data:
  username: ENC[AES256_GCM,data:0fayArPrKk0LgLt1//+lya/
  password: ENC[vE10MqKsyhGpMRwbx6MpTLLcmDEHA+43SM0ily
  conference: ENC[gZfNypikkKgHsd7pxPEMcLuL2s1cZQQOKAEtlsaG
  token: ENC[aKdUa3xrQi5UhnUlSgfLjHav6k/Xq

```

敏感信息之殇

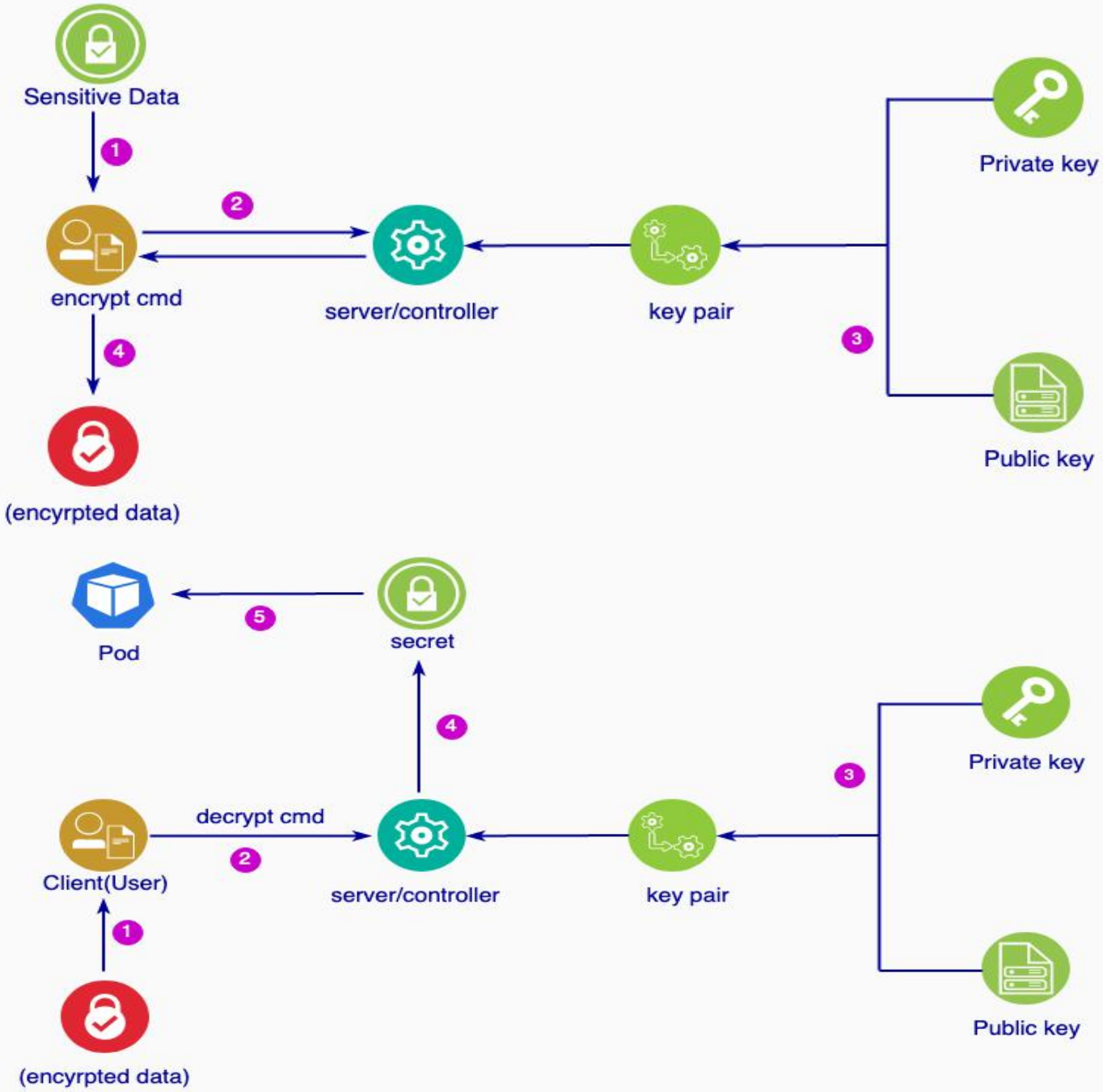

CNCF Technology Radar
Secret Management, February 2021
ASSESS
GCP Secrets Management
Sops
TRIAL
Bitnami Sealed Secrets
Encrypted repositories
AWS Secrets Manager
Hashicorp Vault
cert-manager
AWS KMS
ADOPT

敏感信息之殇

- ✓ Vault
- ✓ Sealed Secrets
- ✓ Helm Secrets
- ✓ Kamus
- ✓ SOPS (gpg)

加密

解密


Sensitive Data
1
2
encrypt cmd
server/controller
key pair
Private key
3
Public key
4
(encyrpted data)
Pod
5
secret
4
3
Private key
decrypt cmd
2
Client(User)
server/controller
key pair
1
Public key
(encyrpted data)

SOPS: Secrets OPerationS

GOTC

```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
bash-3.2$
```

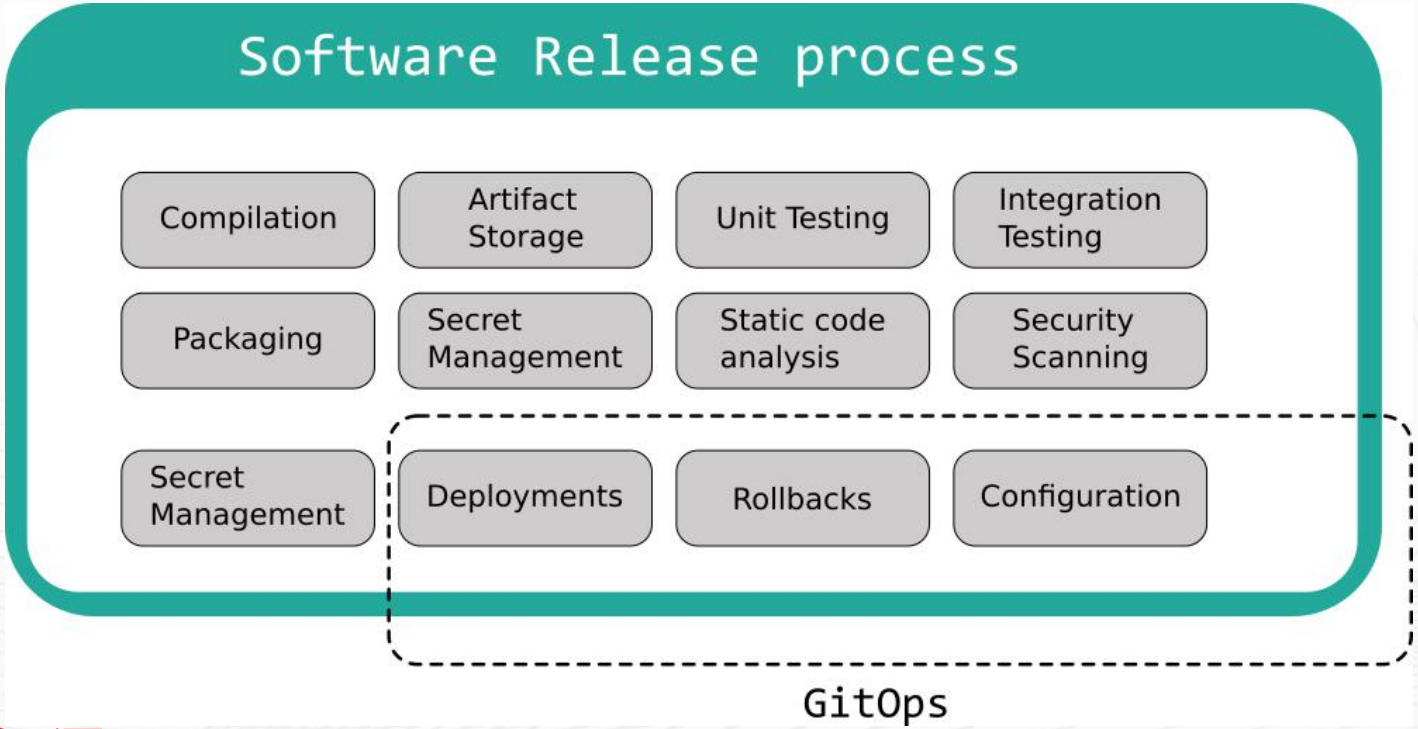

https://github.com/mozilla/sops

镜像之谜

GOTC

有人说：金钱能让人快乐，但是却没说钱从哪儿来；

ArgoCD：给我镜像，能帮你自动部署，但是却不管镜像在哪儿

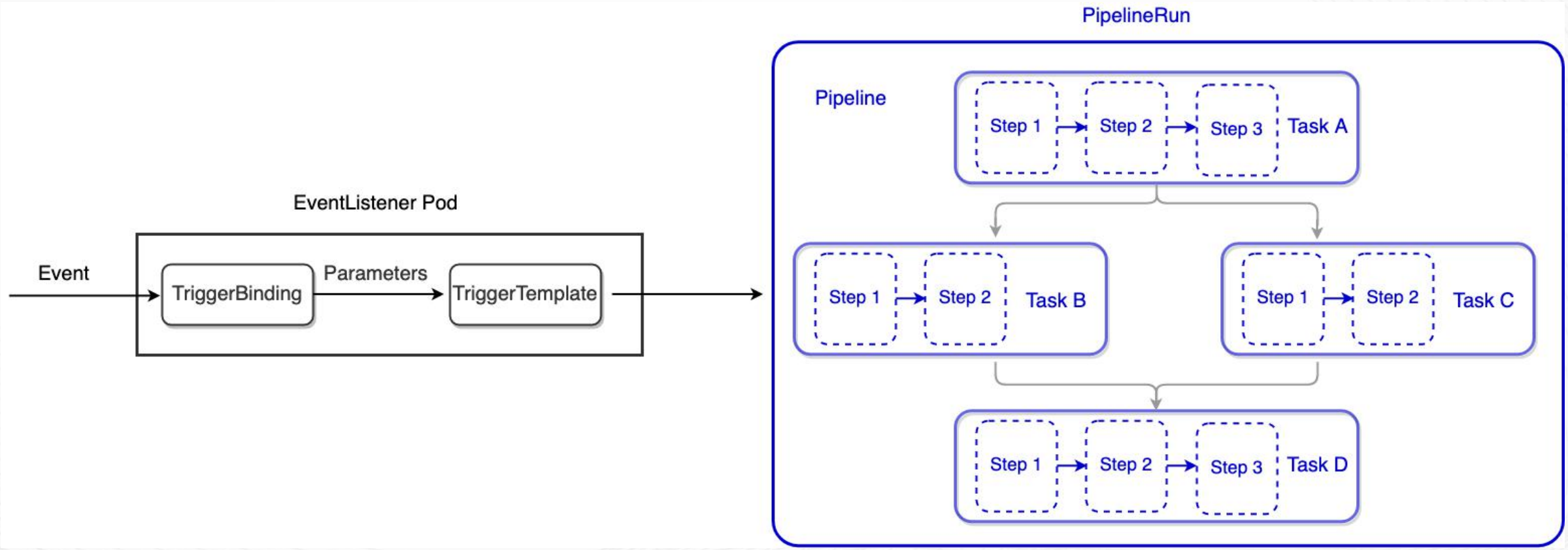


Tekton: 完成源码到镜像的转换

GOTC

Tekton is a powerful and flexible **open-source framework for creating CI/CD systems**, allowing developers to **build, test, and deploy** across cloud providers and on-premise systems

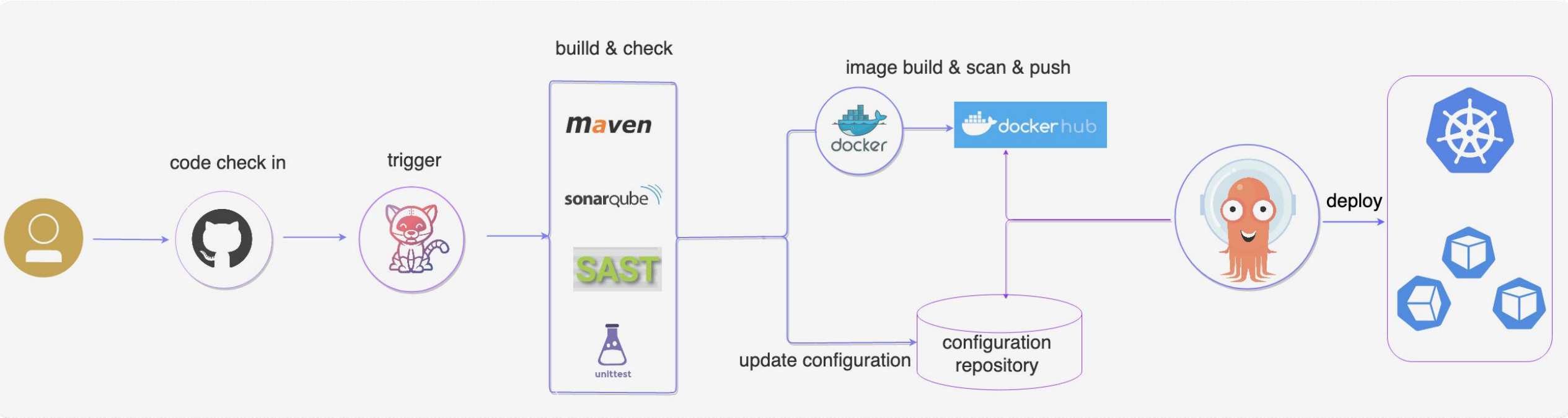
Tekton: 完成源码到镜像的转换



Tekton: 完成源码到镜像的转换

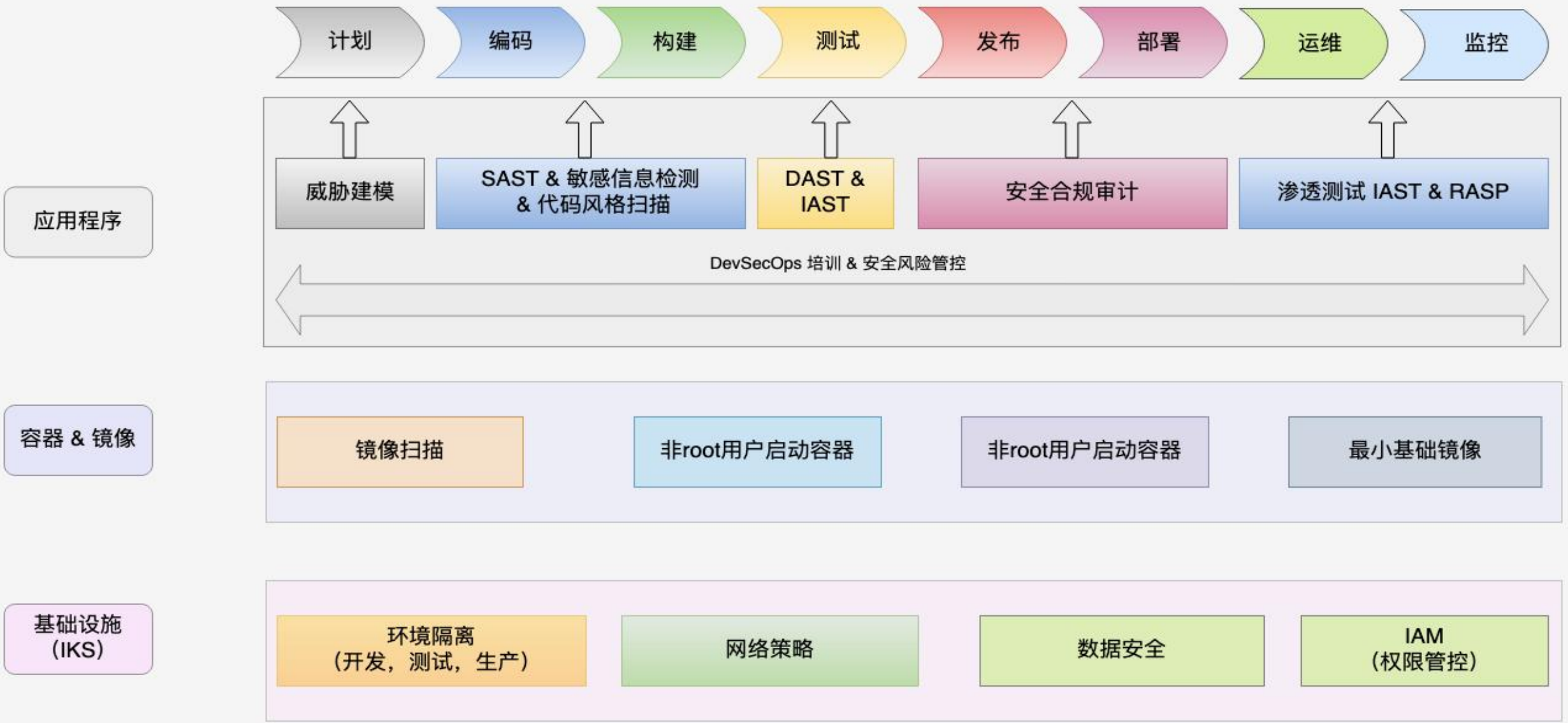

```yaml
resources:
  - name: source-code
    resourceSpec:
      type: git
      params:
        - name: revision
          value: $(tt.params.base_branch)
        - name: url
          value: $(tt.params.gitrepositoryurl)
  - name: docker-image
    resourceSpec:
      type: image
      params:
        - name: url
          value: your/docker/registry/url/$(tt.params.image)
```

```yaml
  - name: image-build-and-push
    image: gcr.io/kaniko-project/executor:v0.17.1
    env:
      - name: "DOCKER_CONFIG"
        value: "/tekton/home/.docker/"
    command:
      - /kaniko/executor
    args:
      - --dockerfile=$(resources.inputs.source-code.path)/Dockerfile
      - --destination=$(resources.outputs.docker-image.url):$(params.image-tag)
      - --context=$(resources.inputs.source-code.path)
```



Tekton + Kustomize + SOPS(gpg) + ArgoCD = GitSecOps

04 GitSecOps 体系


计划
编码
构建
测试
发布
部署
运维
监控
应用程序
威胁建模
SAST & 敏感信息检测
& 代码风格扫描
DAST &
IAST
安全合规审计
渗透测试 IAST & RASP
DevSecOps 培训 & 安全风险管控
容器 & 镜像
镜像扫描
非root用户启动容器
非root用户启动容器
最小基础镜像
基础设施
(IKS)
环境隔离
(开发，测试，生产)
网络策略
数据安全
IAM
(权限管控)

05 GitSecOps 之思

思考

- ✓ 云原生未来已来，开源是其背后的巨大推动力
- ✓ 安全是每个人的责任，需要每个人的参与
- ✓ 没有一劳永逸的安全，只有永不止步的行动
- ✓ Talk is cheap, just show the code

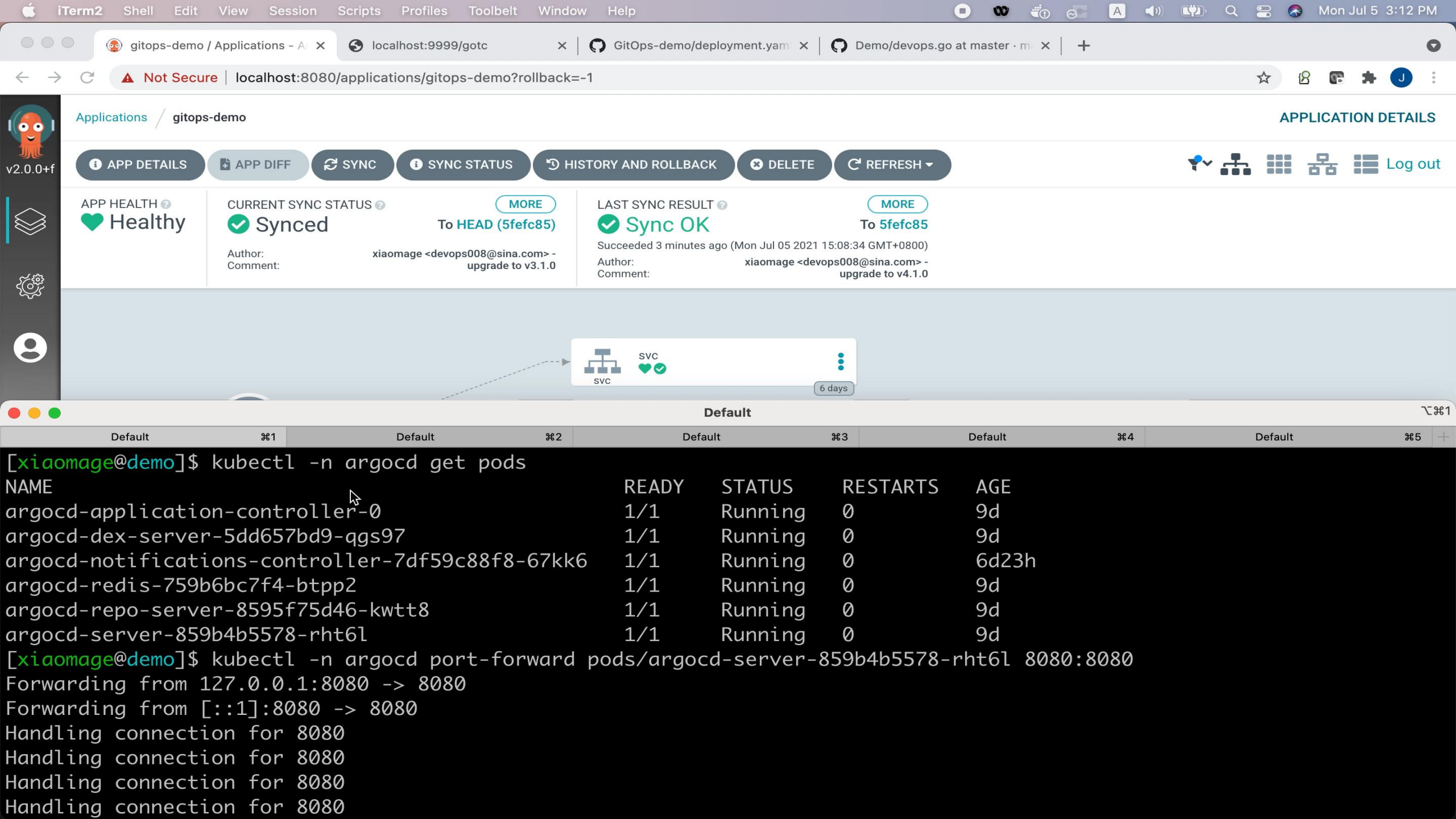
https://github.com/majinghe/argocd-sops.git

https://github.com/majinghe/tekton-demo.git

https://github.com/majinghe/GitOps-demo.git

https://github.com/majinghe/Demo.git

Demo


iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
Mon Jul 5 3:12 PM
gitops-demo / Applications - A
localhost:9999/gotc
GitOps-demo/deployment.yam
Demo/devops.go at master · m
Not Secure
localhost:8080/applications/gitops-demo?rollback=-1
v2.0.0+f
Applications
gitops-demo
APPLICATION DETAILS
APP DETAILS
APP DIFF
SYNC
SYNC STATUS
HISTORY AND ROLLBACK
DELETE
REFRESH
Log out
APP HEALTH
Healthy
CURRENT SYNC STATUS
Synced
MORE
To HEAD (5fefc85)
Author: xiaomage <devops008@sina.com> -
Comment: upgrade to v3.1.0
LAST SYNC RESULT
Sync OK
MORE
To 5fefc85
Succeeded 3 minutes ago (Mon Jul 05 2021 15:08:34 GMT+0800)
Author: xiaomage <devops008@sina.com> -
Comment: upgrade to v4.1.0
SVC
SVC
6 days
Default
⌥⌘1
Default ⌘1
Default ⌘2
Default ⌘3
Default ⌘4
Default ⌘5
[xiaomage@demo]$ kubectl -n argocd get pods
NAME READY STATUS RESTARTS AGE
argocd-application-controller-0 1/1 Running 0 9d
argocd-dex-server-5dd657bd9-qgs97 1/1 Running 0 9d
argocd-notifications-controller-7df59c88f8-67kk6 1/1 Running 0 6d23h
argocd-redis-759b6bc7f4-btpp2 1/1 Running 0 9d
argocd-repo-server-8595f75d46-kwtt8 1/1 Running 0 9d
argocd-server-859b4b5578-rht6l 1/1 Running 0 9d
[xiaomage@demo]$ kubectl -n argocd port-forward pods/argocd-server-859b4b5578-rht6l 8080:8080
Forwarding from 127.0.0.1:8080 -> 8080
Forwarding from [::1]:8080 -> 8080
Handling connection for 8080
Handling connection for 8080
Handling connection for 8080
Handling connection for 8080

GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE