自己的DevOps開源工具自己做

我是周育緯

- 資策會正工程師
- 7 年 System, DevOps 與 Backend 開發與維護經驗
- 擅長於: Kubernetes, OpenStack, Python
- 資策會及工研院 Kubernetes 講師
- Github: https://github.com/demoyuw

源起

用VM跑DevOps的痛點

- DevOps環境毀了，無法保證能快速重建。
- 跑一次好花時間，沒法跟上開發團隊 Push code的速度。
- 版本升級對VM而言是一大挑戰 ➔ 從做VM映像檔開始重新測試。
- 客戶的Infrastructure 跟我們的不一樣(VMWare, OpenStack, KVM, Virtualbox)。

用傳統Jenkins設定的痛點

- Jenkins一堆設定要用UI設。
- 我的CI script不會自動備份。
- 改壞的時候，忘了上次正確測試的script。

因為測試困難

- 所以沒完整測試就上線 ➔ 結果凌晨四點在機房維護線上環境

發現

發現能夠寫CI YAML，跟發現新大陸一樣

- CI YAML 跟著開發Source code走，全部script也一併納入程式碼版控。
- 誰改壞YAML 跟script都有紀錄
- 有程式碼版控紀錄多久我都能rollback

發現環境採用Kubernetes，快又方便

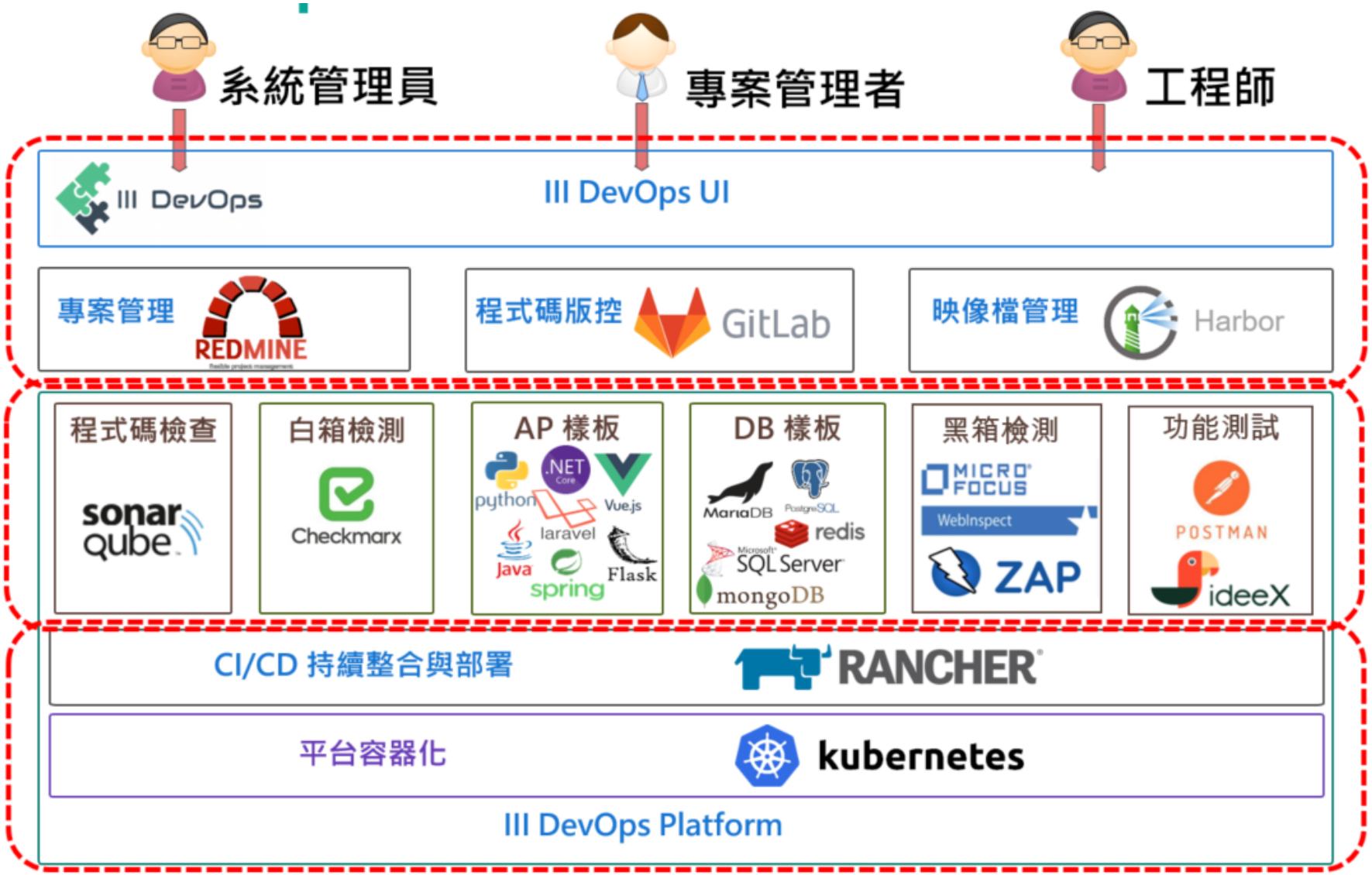
- Kubernetes排程及資源限制，省了手動資源調整。
- Kubernetes監測pod健康，Pod crash自動restart。
- Kubernetes保有rollback靈活性，幫你保存image，讓你能夠隨時rollback。
- 工具與測試環境皆部屬在k8s上 ➔ 系統工程師只需專注維護k8s。
- 流量需求增加 ➔ 增加k8s節點，增加deploymet的replicas

目標

- 做一套開源DevOps工具供跨團隊使用
- 以地端開源軟體組成
- 以Kubernetes為平台
- 可快速安裝，獨立部屬。

部屬

元件全部容器化


系統管理員
專案管理者
工程師
III DevOps
III DevOps UI
專案管理
REDMINE
程式碼版控
GitLab
映像檔管理
Harbor
程式碼檢查
sonarqube
白箱檢測
Checkmarx
AP 樣板
python
.NET Core
Vue.js
laravel
Java
spring
Flask
DB 樣板
MariaDB
PostgreSQL
redis
Microsoft SQL Server
mongoDB
黑箱檢測
MICRO FOCUS
WebInspect
ZAP
功能測試
POSTMAN
ideeX
CI/CD 持續整合與部署
RANCHER
平台容器化
kubernetes
III DevOps Platform

好用的開源軟體納進來

- 選定自己的開源軟體授權 ➔ 我們用Apache 2.0
- 檢查各家開源軟體license，避免後續衍生法律問題。
- 制定開源貢獻者條款

採用開源條款特別注意事項

- XPL 類
  - GPLv2 ➔ 無法獨立運行，你的軟體也會被渲染成GPL
  - LGPL v3 ➔ 要開源你介接該軟體的client 端程式碼
  - Eclipse Public license v1 ➔ 無法獨立運行，你要開源的程式碼。不過你可以自行選擇你的開源license。
- Apache 2.0, MIT
  - 聲明出處

版控與CI工具 webhook ➔難自動化

- GitLab root token ➔ 新版API不支援，只能從UI產生
- Rancher pipeline webhook 採用OAuth2.0 ➔ 只能從UI點擊確認
- 解決方法: 全部專案皆放在root下，在進行權限進行區隔

Rancher pipeline - 優點

- CI YAML 簡單好理解
- CI而已，還不想面對K8s授權問題。

Rancher pipeline - 缺點

- 產品不夠完善，有時需要進pod裡面看logs
- Rancher 新版本已棄用。

As of Rancher v2.5, Git-based deployment pipelines are now deprecated. We recommend handling pipelines with Rancher Continuous Delivery powered by Fleet, available in Cluster Explorer.

NOTICE:
Fleet does not replace Rancher pipelines; the distinction is that Rancher pipelines are now powered by Fleet.

Pipeline

提供pipeline測試紀錄

開發進度 / Pipelines

yuwei-test-1216

最終更新：2021-12-21 17:28:41

項次	狀態 / 測試項目	分支 / Commit	上傳訊息 / 處理訊息	最終更新
43	Finished (5/11)	develop 586a29d	UI 編輯 .rancher-pipeline.yaml 啟用停用分支	2 小時前
40	Finished (1/11)	develop fe586e9	Add this is develop branch	4 天前
39	Failed (1/11)	master 1f3ce9b	Update .rancher-pipeline.yml Got FAILED status in 'Test--SonarQube source code scan' stage	4 天前
38	Failed (1/11)	master 328c15e	Update .rancher-pipeline.yml Got FAILED status in 'Test--SonarQube source code scan' stage	5 天前
37	Failed (0/11)	master 50d72c8	UI 編輯 .rancher-pipeline.yaml 啟用停用分支 Got FAILED status in 'Test--SonarQube source code scan' stage	5 天前
35	Finished (1/11)	master 0caa182	Update .rancher-pipeline.yml	5 天前

共 6 項 1

測試細節 UI 編輯 .rancher-pipeline.yaml 啟用停用分支

1 Create connection by issue_id and git commit message	Success
2 Test--SonarQube source code scan	Skipped
3 Test--Checkmarx source code scan	Skipped
4 Deploy--Set Web environment variables	Success
5 Build--Build and push docker image	Success
6 Deploy--Web	Success
7 Deploy--Wait Web deployment	Success
8 Test--ZAP	Skipped
9 Test--WebInspect	Skipped
10 Test--Postman	Skipped
11 Test--SideeX	Skipped

Deploy--Wait Web deployment

```
+ rancher login ******** -t ******** --skip-verify
time="2021-12-21T07:51:49Z" level=info msg="Only 1 project available: Default"
time="2021-12-21T07:51:49Z" level=info msg="Saving config to /root/.rancher/cli2.json"
+ bash /app/run.sh
yuwei-test-1216-develop-serv-dpy 1/1 1 1 6s
yuwei-test-1216-develop-serv deployed!
```

k8s namespace

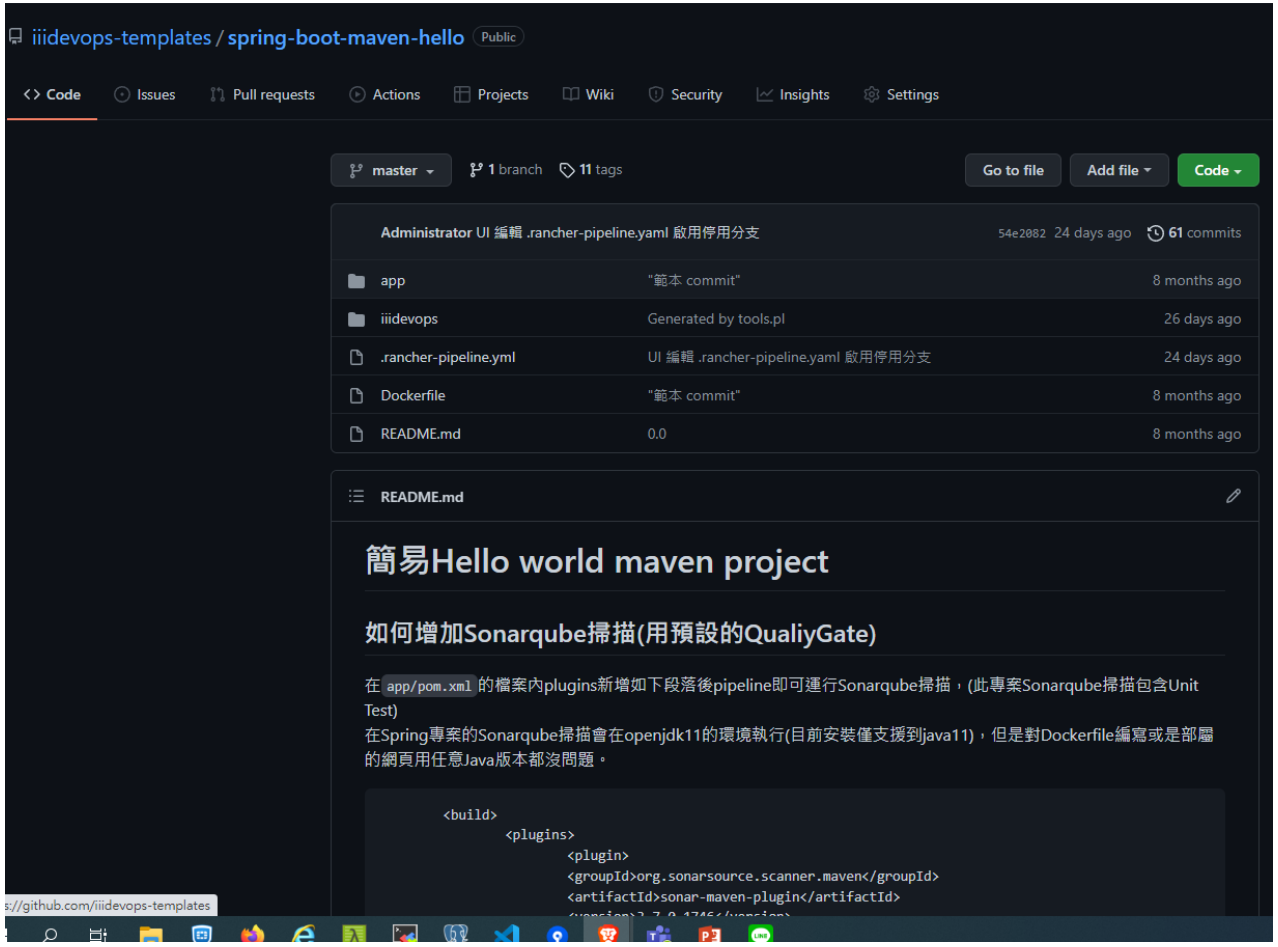
- 權限區隔
- 資源量限制 (CPU, Memory, k8s 資源限制)

VMWare Harbor

- Project進行權限區隔
- Image可用儲存空間也可依Project調整
- 建立mirror project，避免直接向Docker Hub pull image。

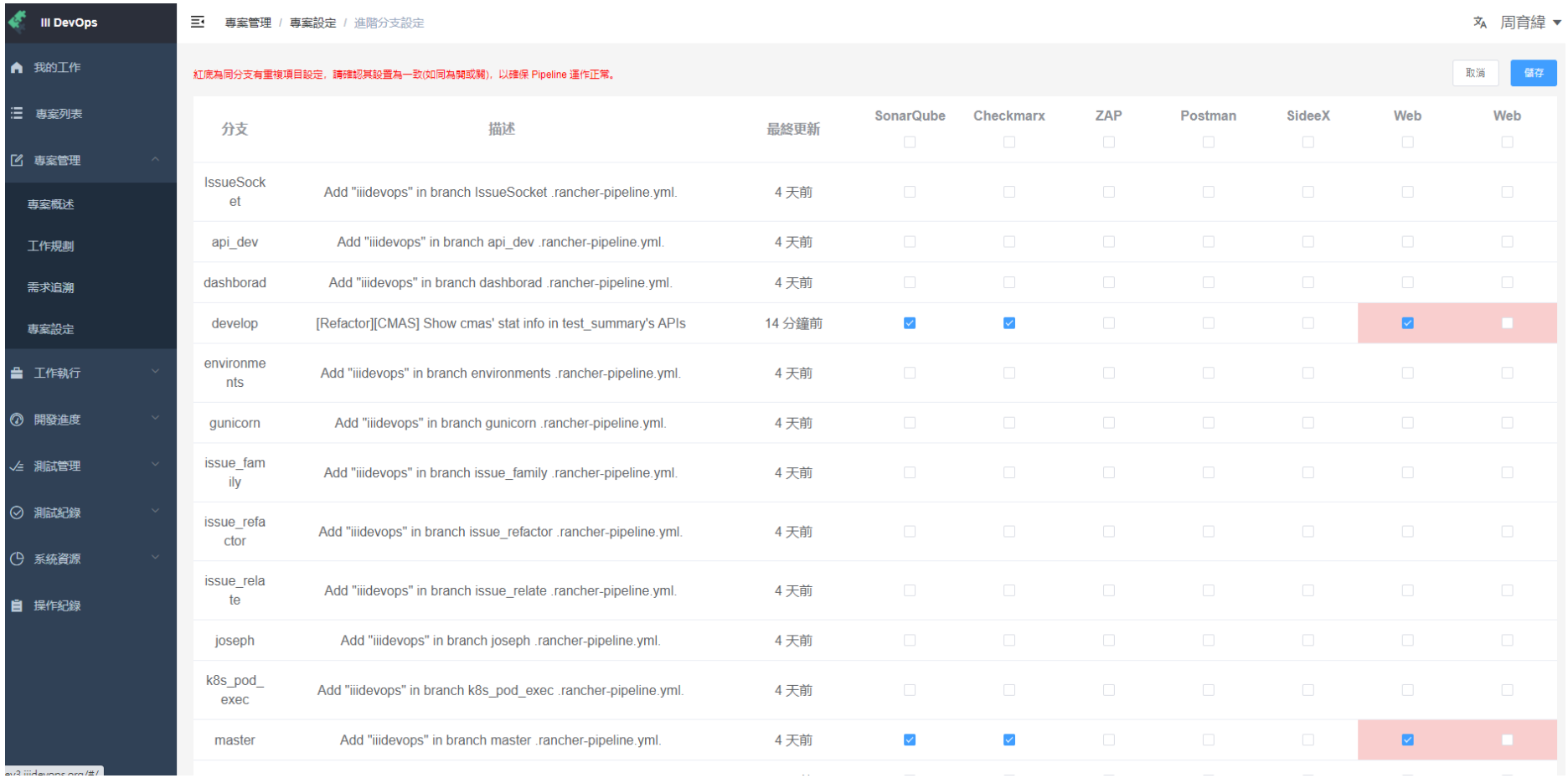
讓不會寫CI YAML 的RD 也能用 -1

- CI YAML 範本 ➔ 一鍵用範本建立專案



讓不會寫CI YAML 的RD 也能用 -2

- UI 對YAML 做變更 ➔ Enable/Disable branch



測試步驟寫成Helm chart

- 複雜邏輯在chart裡面進行，降低YAML複雜度，增加可讀性。
- 越容易撰寫的CI，可變化性也越差。
- 方便後續版本升級

```
- name: Test--Checkmarx source code scan
  iiidevops: checkmarx
  steps:
  - applyAppConfig:
      answers:
        git.branch: ${CICD_GIT_BRANCH}
        git.commitID: ${CICD_GIT_COMMIT}
        git.repoName: ${CICD_GIT_REPO_NAME}
        git.url: ${CICD_GIT_URL}
        harbor.host: harbor-dev3.iiidevops.org
        pipeline.sequence: ${CICD_EXECUTION_SEQUENCE}
      catalogTemplate: cattle-global-data:iii-dev-charts3-scan-checkmarx
      name: ${CICD_GIT_REPO_NAME}-${CICD_GIT_BRANCH}-cmx
      targetNamespace: ${CICD_GIT_REPO_NAME}
      version: 0.2.0
  when:
    branch:
      include:
      - skip-master
```

Helm chart code

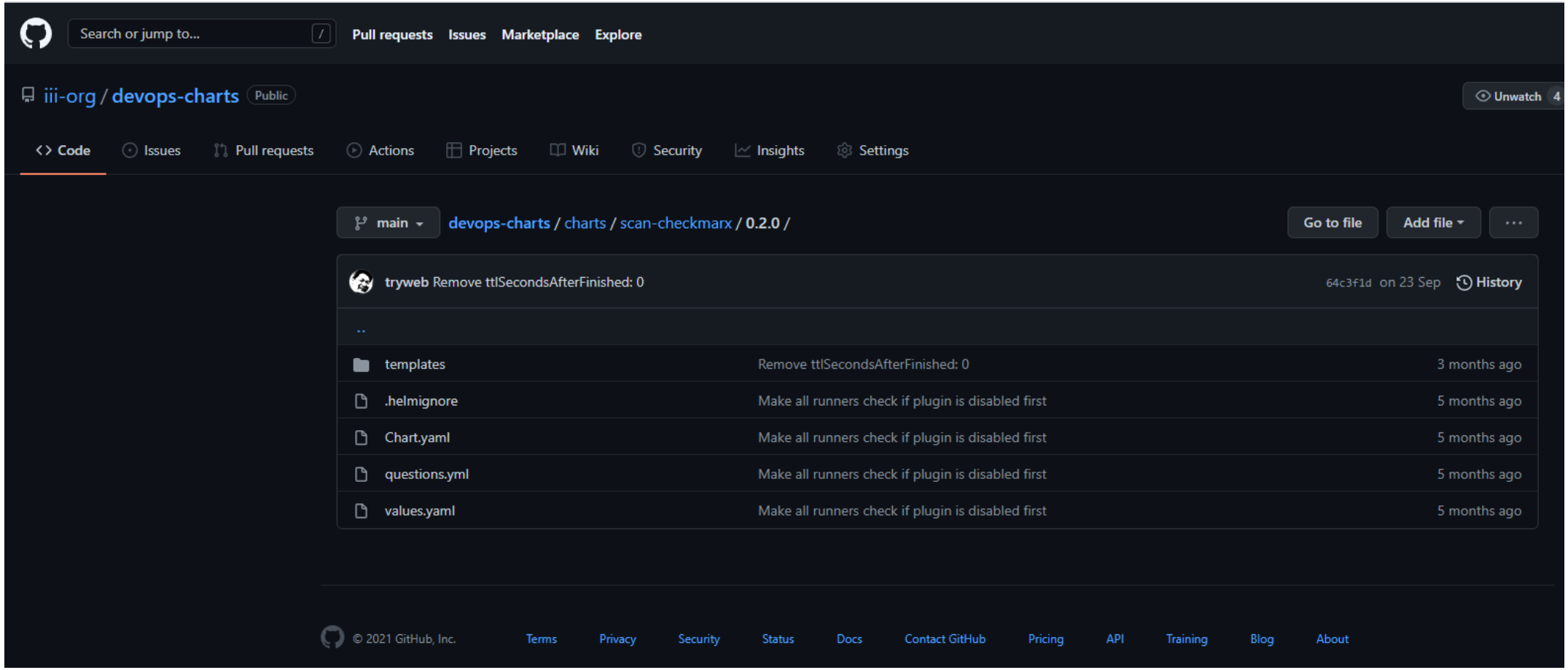


Chart repository

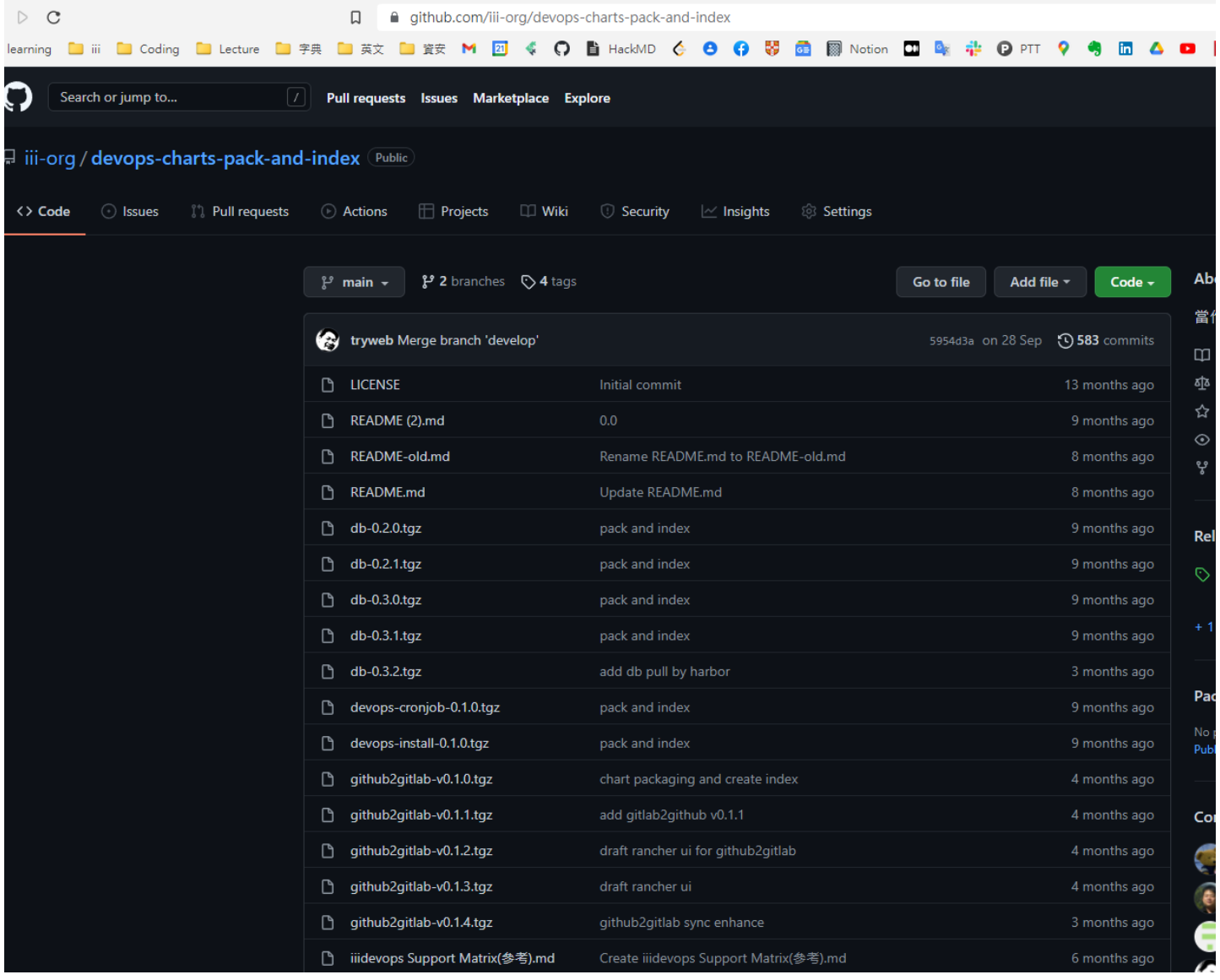
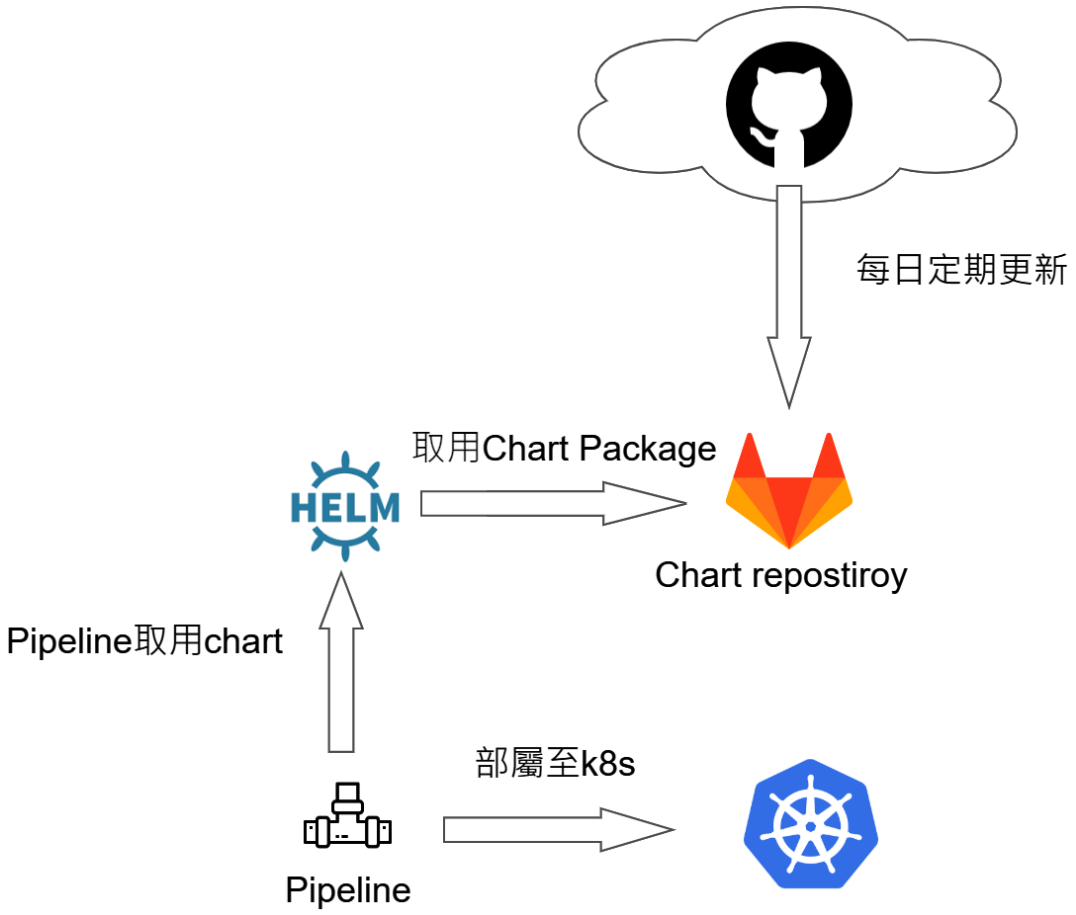


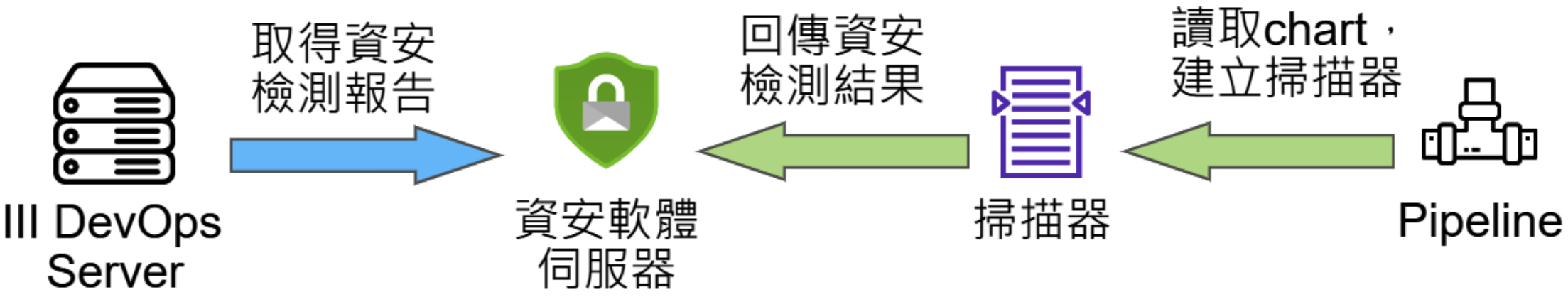
Chart upgrade



掃描/測試工具

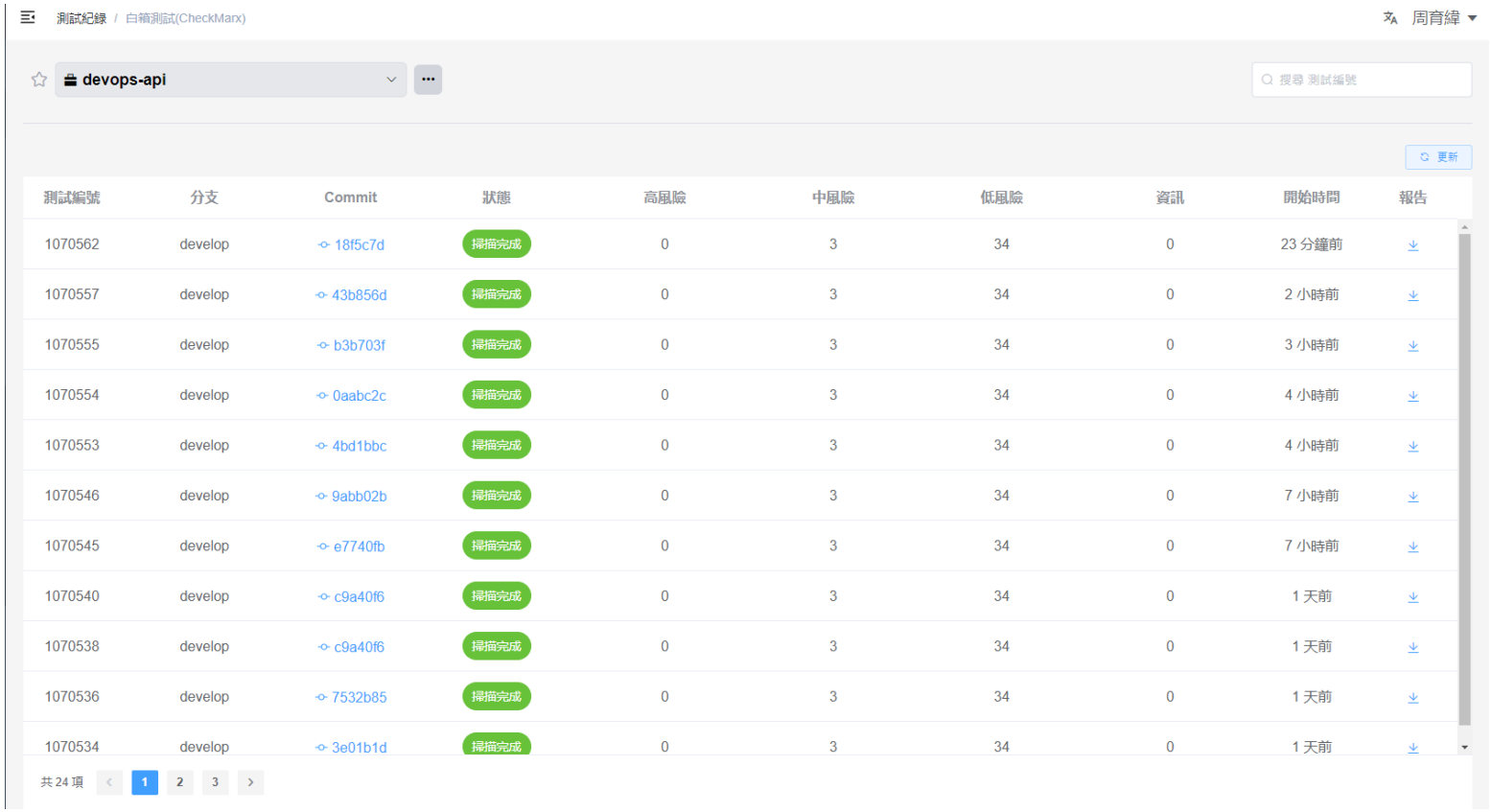
掃描/測試 工具 – 1

- SonarQube, CheckMarx, Fortify WebInspect



CheckMarx

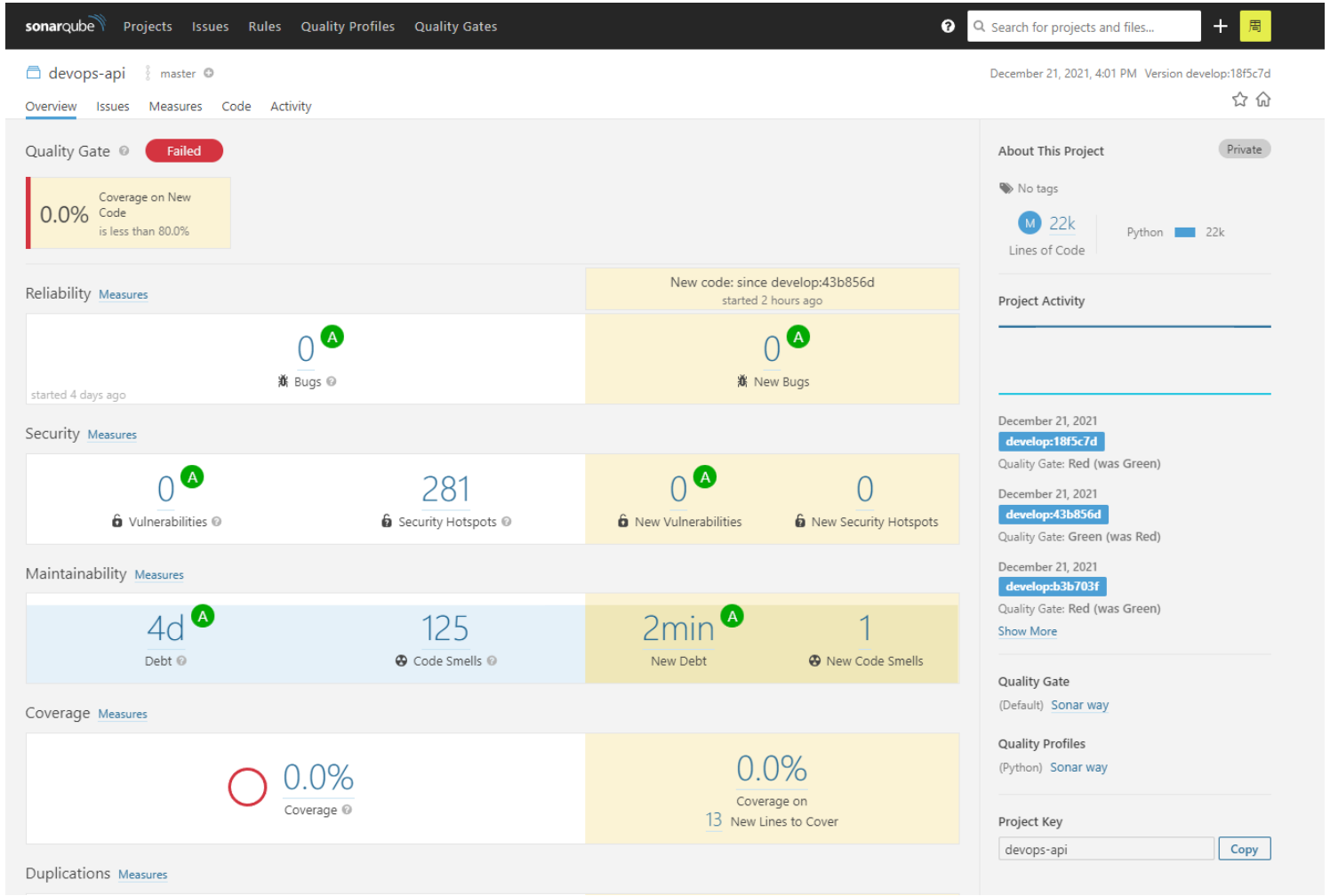
- UI 呈現趨勢總覽
- 下載pdf資安檢測報告



測試編號	分支	Commit	狀態	高風險	中風險	低風險	資訊	開始時間	報告
1070562	develop	18f5c7d	掃描完成	0	3	34	0	23 分鐘前	
1070557	develop	43b856d	掃描完成	0	3	34	0	2 小時前	
1070555	develop	b3b703f	掃描完成	0	3	34	0	3 小時前	
1070554	develop	0aabc2c	掃描完成	0	3	34	0	4 小時前	
1070553	develop	4bd1bbc	掃描完成	0	3	34	0	4 小時前	
1070546	develop	9abb02b	掃描完成	0	3	34	0	7 小時前	
1070545	develop	e7740fb	掃描完成	0	3	34	0	7 小時前	
1070540	develop	c9a40f6	掃描完成	0	3	34	0	1 天前	
1070538	develop	c9a40f6	掃描完成	0	3	34	0	1 天前	
1070536	develop	7532b85	掃描完成	0	3	34	0	1 天前	
1070534	develop	3e01b1d	掃描完成	0	3	34	0	1 天前	

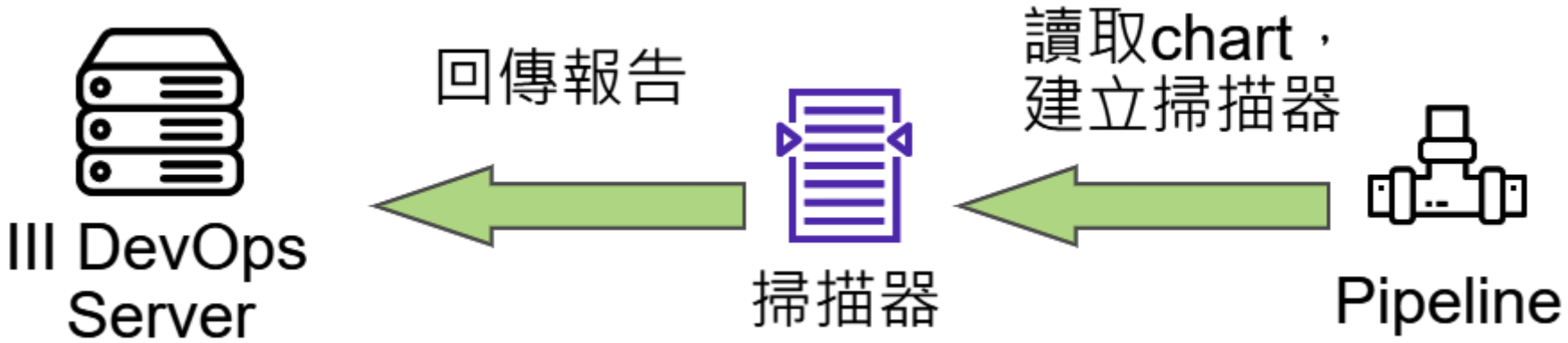
SonarQube

- 也依專案進行權限區分



掃描/測試 工具 - 2

- OWASP ZAP, Postman, SideeX



掃描以後呢

- 當掃描不是問題後，教人怎麼看報告，怎麼修改才是問題。
- 掃描速度與行數成等比 ➔ 不要把library code也全都commit進來。

描述

Hardcoded Password in Connection String\路徑 1:

嚴重程度：	中風險
結果狀態：	校驗
線上結果	https://checkmarx.labad.org/CxWebClient/ViewerMain.aspx?scanid=1070553&projectid=32663&pathid=33
狀態	反覆出現的問題

應用程式包含寫死的連線詳細資訊，存在於apis/resources/rancher.py的第108行中的""password""。這個連線字串包含寫死的密碼，在apis/resources/rancher.py的rc_get_pipe_log_websocket第204行的create_connection用來連接資料庫，這可能會暴露資料庫密碼，以及阻礙適當的密碼管理。

	來源	目的地
檔案	apis/resources/rancher.py	apis/resources/rancher.py
行	111	217
物件	""password""	create_connection

代碼片斷

檔案名稱 apis/resources/rancher.py

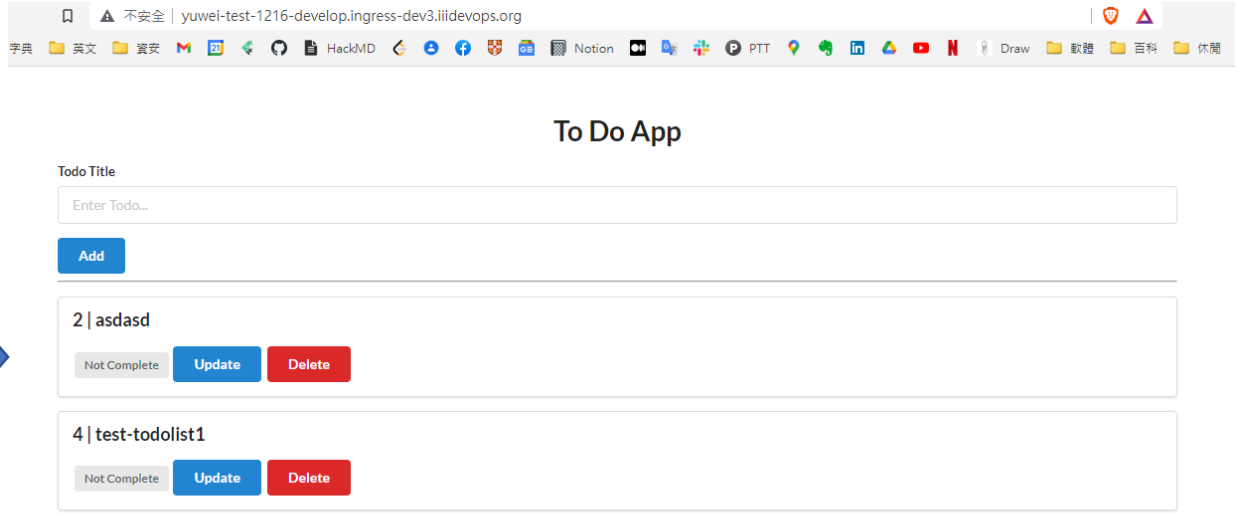
方法 def __generate_token(self):

```
....
111.            "password": config.get('RANCHER_ADMIN_PASSWORD')
```

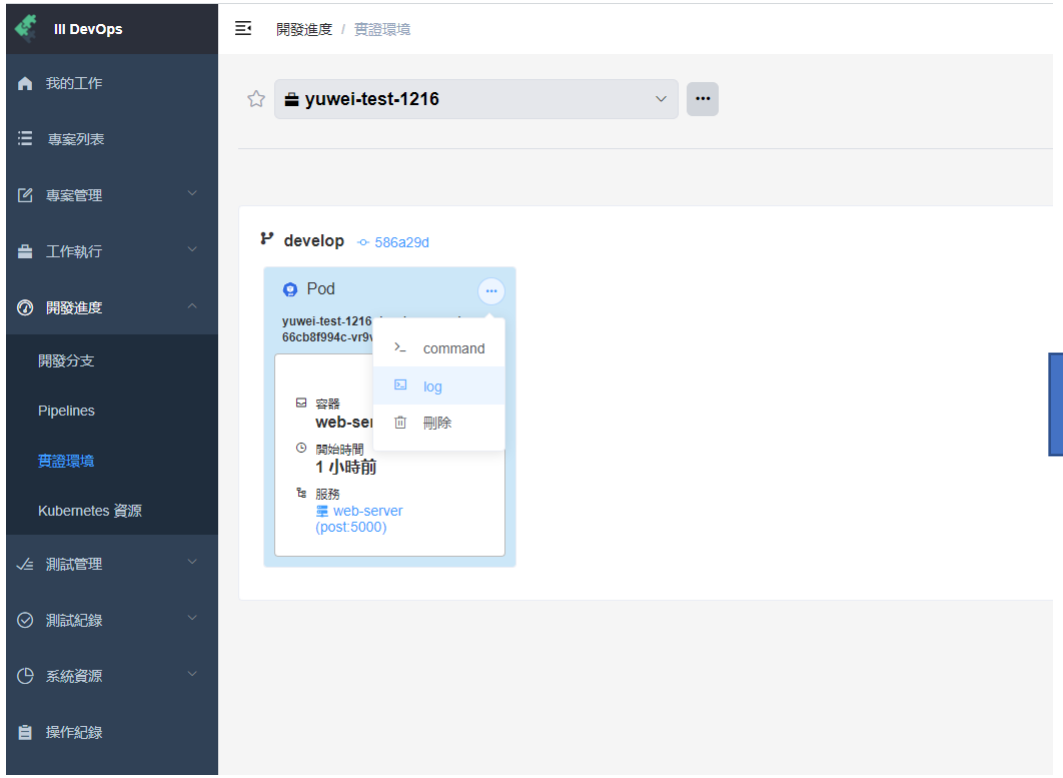
測試環境

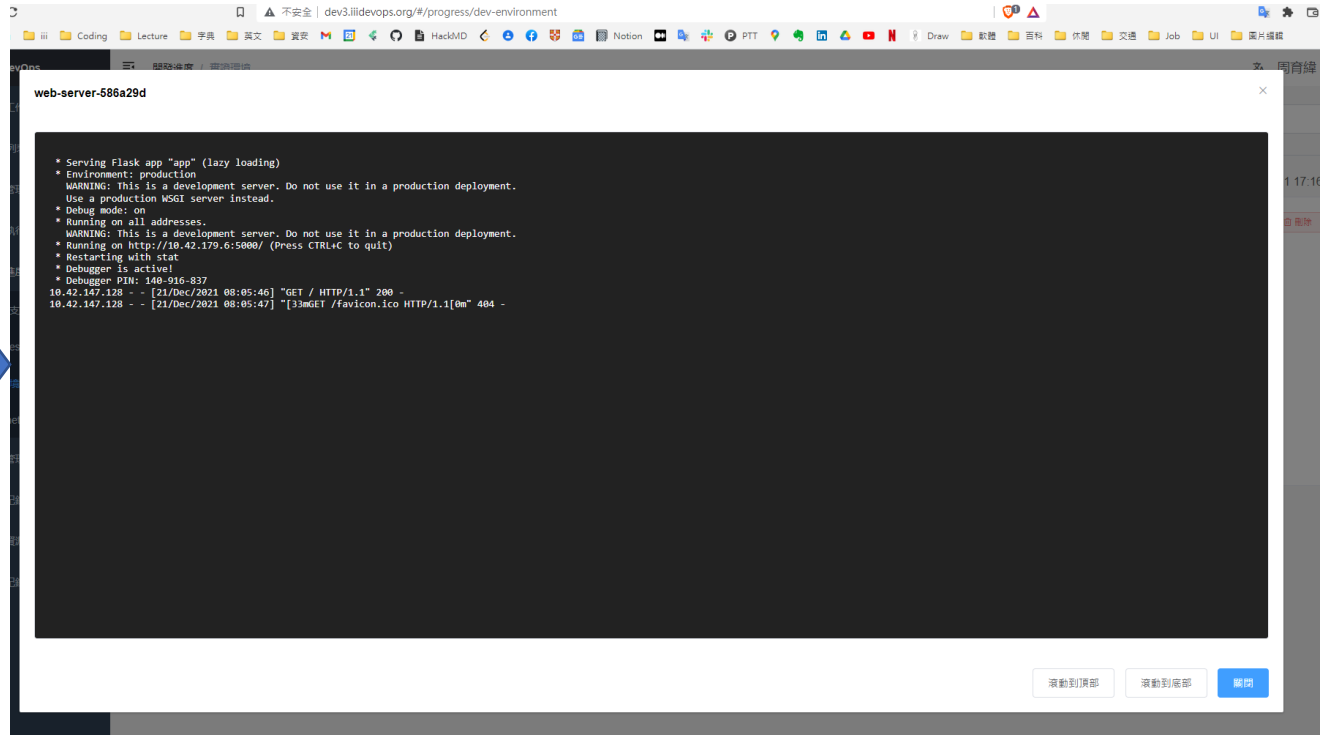
提供UI 供RD連入測試環境

- K8s service + ingress 導入測試環境

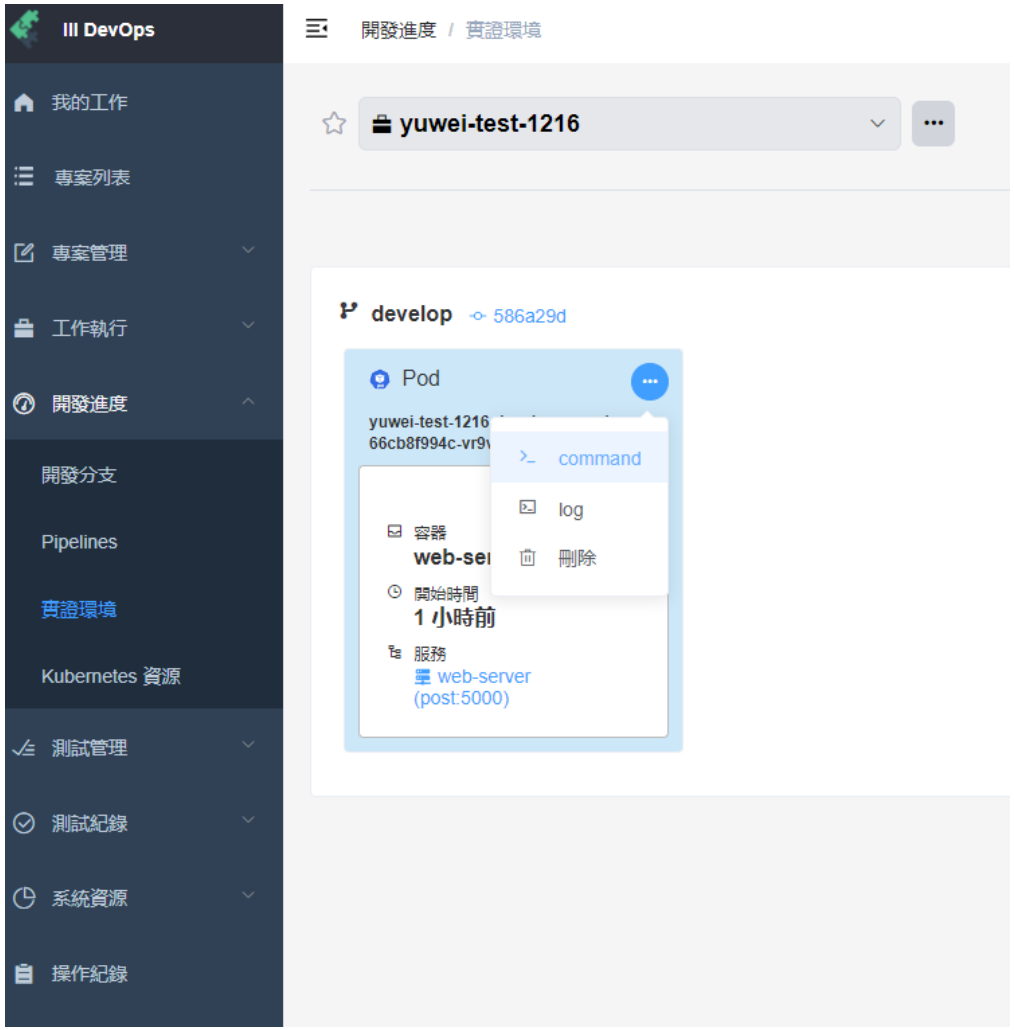


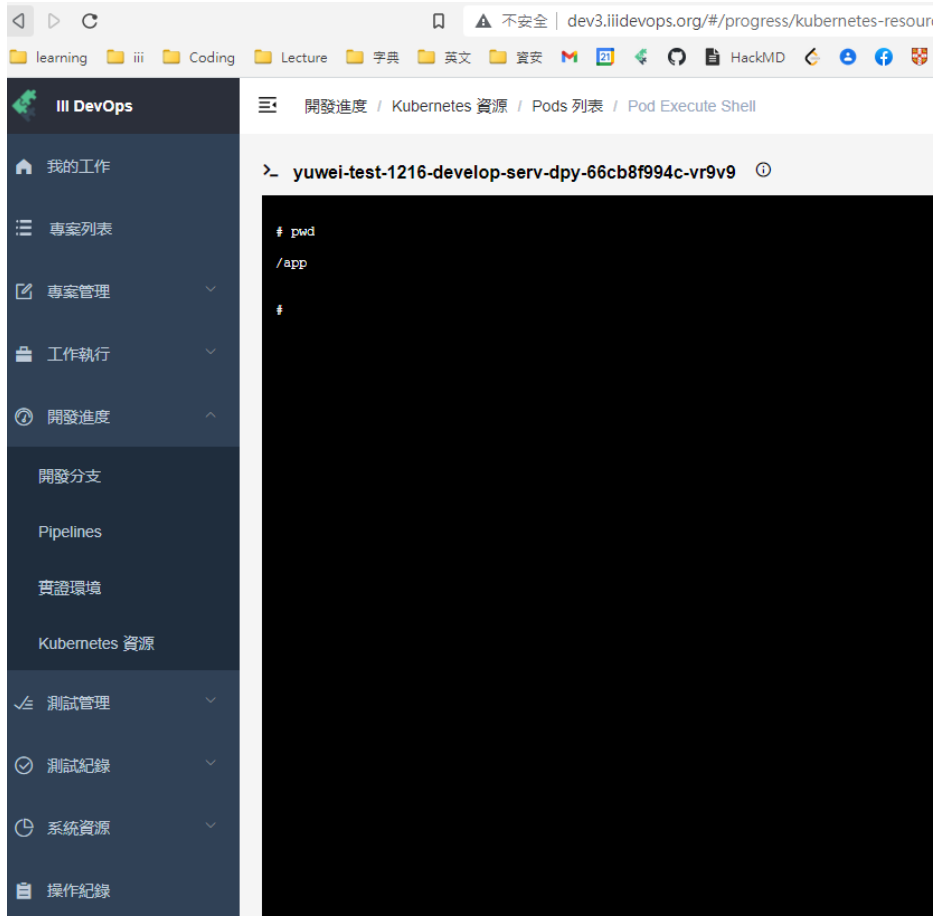
提供UI 供RD 進pod 看 logs





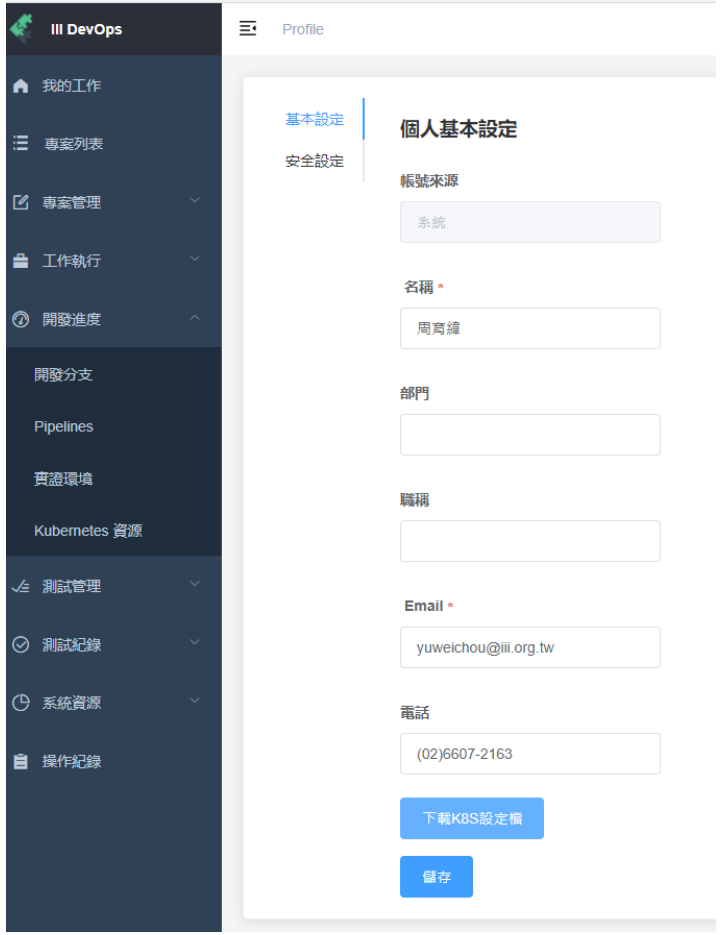
提供UI 供RD 進pod exec進行操作





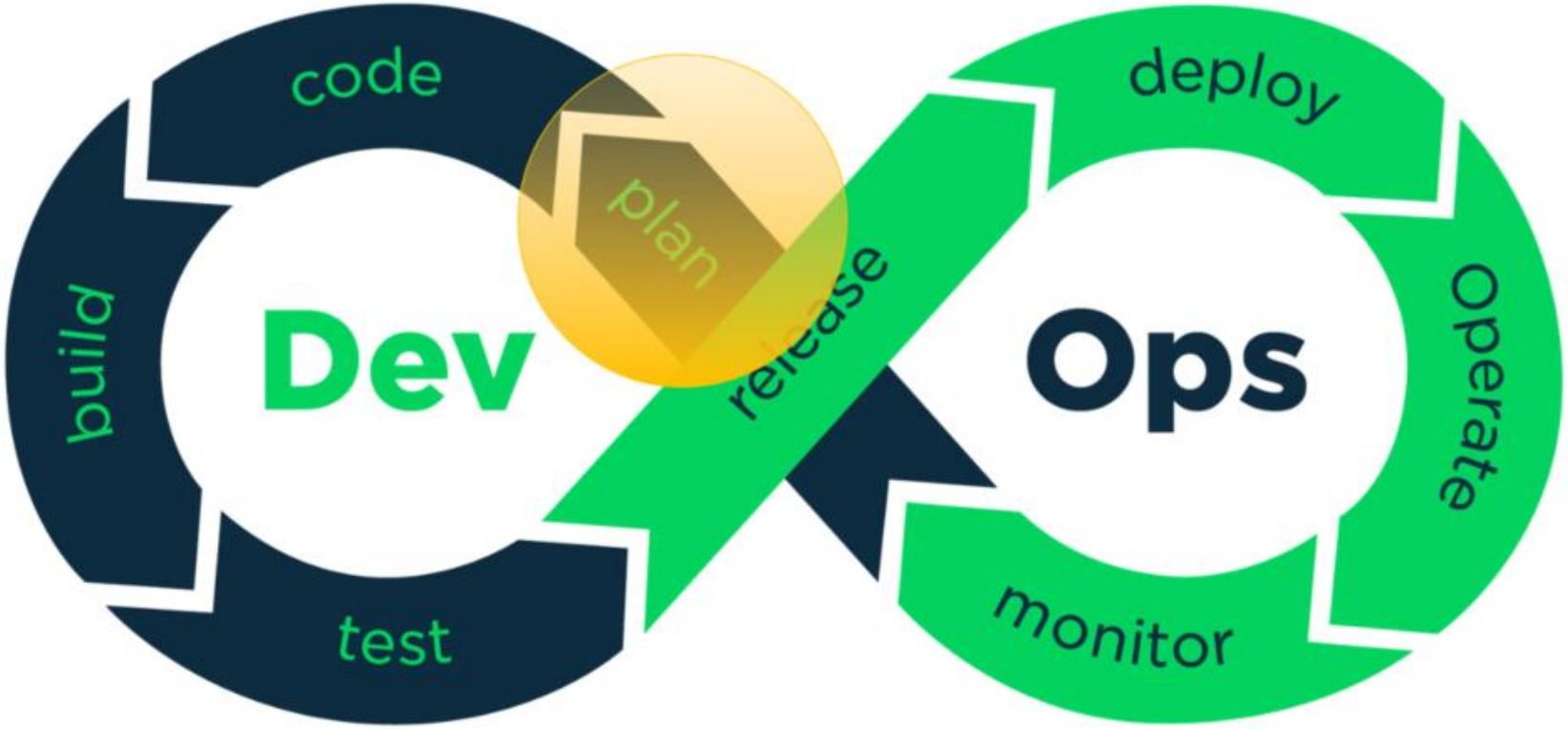
至少也要有

- 提供kubeconfig file 供User下指令進行操作

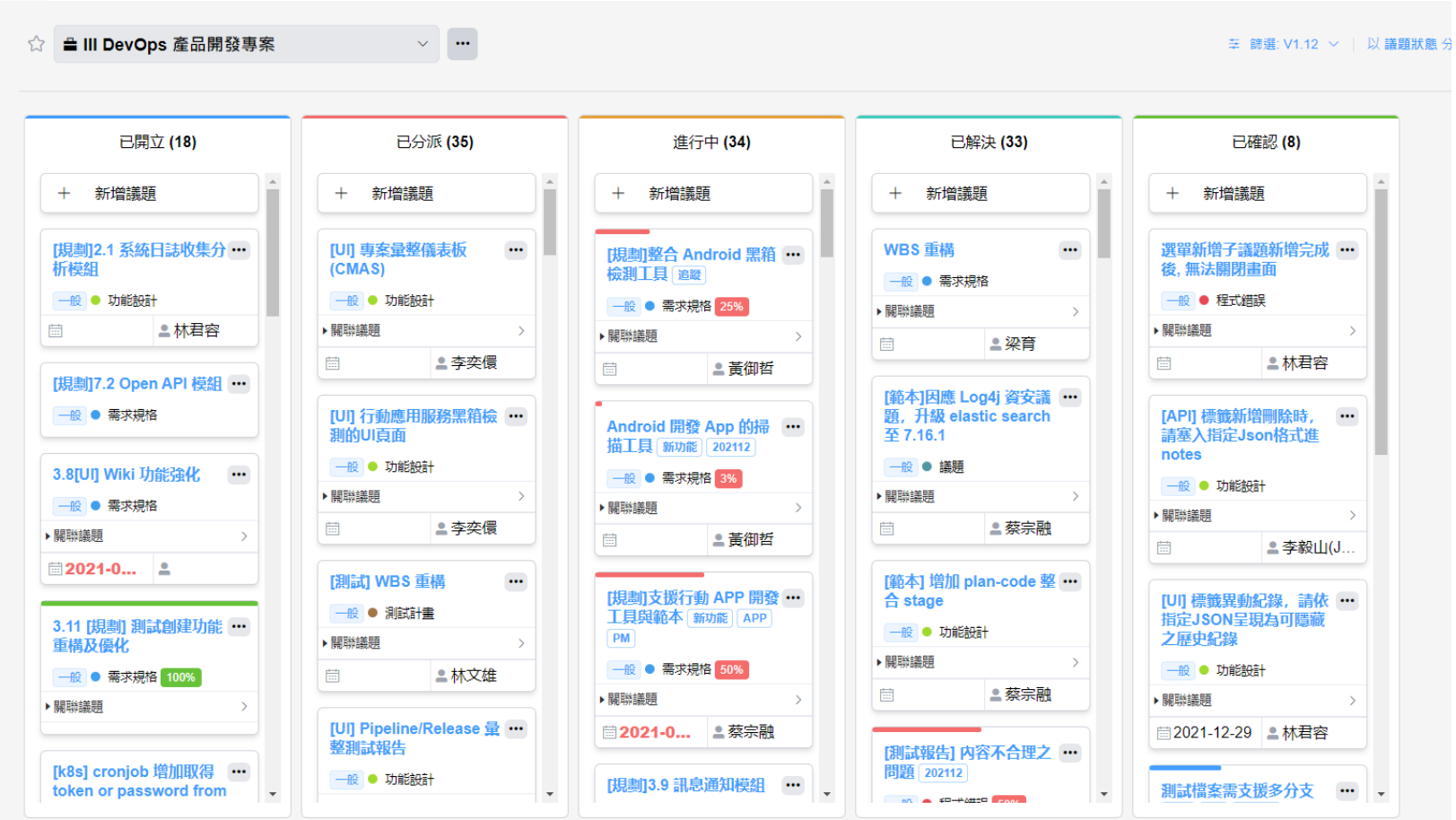


專案管理

PM問: plan在哪?


code
plan
build
Dev
release
test
deploy
Ops
operate
monitor

Build Scrum board for Redmine



就是有人愛條列式

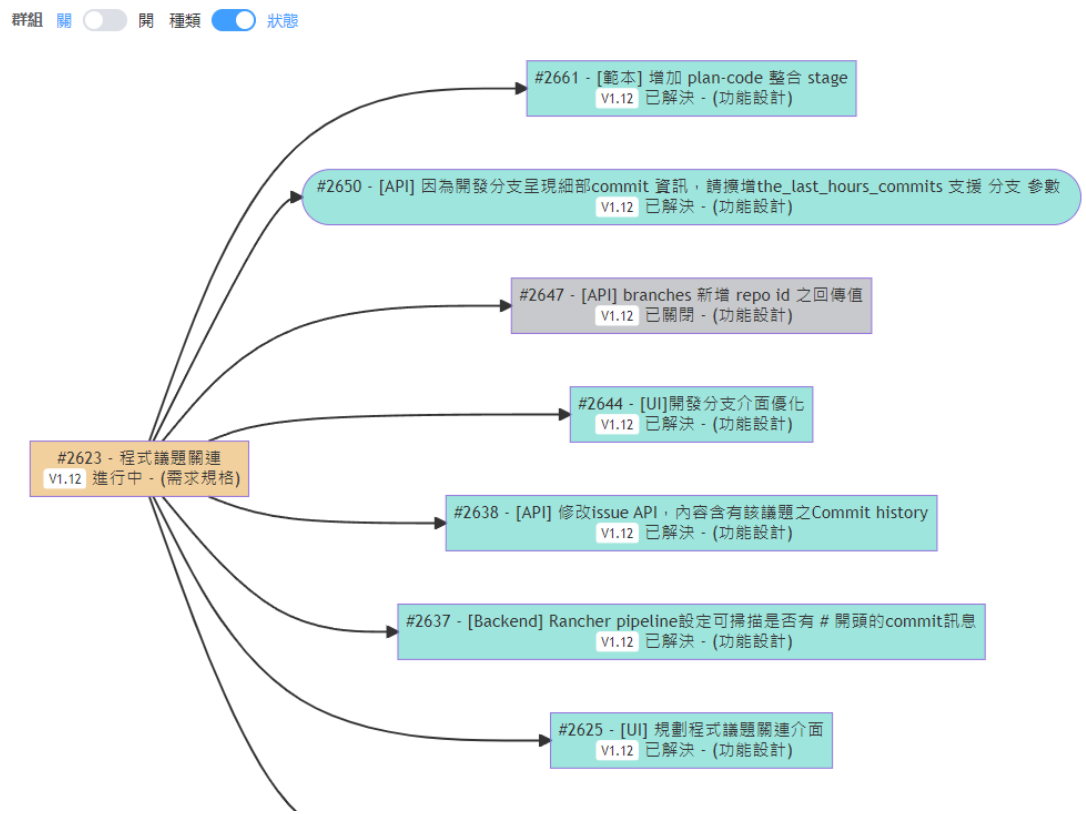
III DevOps 產品開發專案 ··· + 新增議題 篩選 搜尋

種類	議題編號 / 議題名稱	優先權	狀態	受分配者
功能設計	#2678 [UI] 專案彙整儀表板(CMAS)	一般	已分派	李奕儇 (noitseuq)
測試計畫	#2677 [測試] WBS 重構	一般	已分派	林文雄 (asher)
功能設計	#2672 [UI] Pipeline/Release 彙整測試報告	一般	已分派	李奕儇 (noitseuq)
議題	#2671 ISO V1.12.x 更新 images	一般	已分派	黃堤瑋 (twhuang)
變更請求	#2670 因為 Log4j 議題 SonarQube 7.9 需要升級至 8.9	一般	已分派	蔡宗融 (jonathan)
議題	#2669 檢查與修復所有套件有 Log4j 的弱點問題	一般	已開立	蔡宗融 (jonathan)
程式錯誤	#2666 系統管理者-儀表板大螢幕尺寸顯示異常	一般	已分派	梁育 (webster)
功能設計	#2665 [合規][UI] 匯入查檢表範例文字調整	緊急	已解決	林文雄 (asher)
程式錯誤	#2664 [合規][UI] 查檢表匯入後操作按鈕好像消失了	緊急	進行中	林文雄 (asher)
功能設計	#2663 [UI] 行動應用服務黑箱檢測的UI頁面	一般	已分派	李奕儇 (noitseuq)

共 219 項 1 2 3 4 5 6 ··· 22

議題關聯

議題關聯圖(#2650 - [API] 因為開發分支呈現細部commit 資訊，請擴增the_last_hours_commits 支援 分支 參數)



所遇到的困難

工程團隊不願意搬遷 ➔ 秀牛肉

- Code push 以後➔ 就有白箱掃描，源碼掃描結果
- 無償得到一套測試環境

未來挑戰

- 成功了，等於接下全公司所有開發團隊DevOps的工作。
- 支援CD
- 不支援Windows Solution ➔ 跑windows container，現只支援ASP.NET Core on linux。