



如何實踐品質內建之企業級DevOps流程架構

D.C 玉山商業銀行

 玉山金控 E.SUN FHC



DevOps實行背景

業務發展及心路歷程

01

02

施行痛點及措施

管線流程公版化、快速擴展持續交付、專案管理

安全與高品質交付流程

持續進化邁向DevSecOps、品質內建

03

04

容器安全

實施架構及實行策略

**Fintech時代
創新思維**

**永續發展
數位轉型**

**注重顧客體驗
價值創造**

**快速響應
效率回饋**

問題

業務發展

專案需求眾多，系統建置作業日趨頻繁

系統模組繁複

響應業務需求，取得市場反饋，因而系統模組功能千變萬化

技術債

技術創新快，系統技術債越來越龐大

流程追蹤

軟體開發生命週期過程不夠透明，無法有效管理

挑戰

表單梳理

各種需求、變更及事件單據流程各自為政，勾稽困難

敏捷管理

組織敏捷化，因應各種敏捷管理方法，造就開發方式的轉變

組建公版化

歷史包袱沉重，系統架構五花八門，常有組建及部署的客製化需求

軟體品質

交付速度提升，成品品質卻沒有相應的提升



完善充分的品質管理

自動化的流程，減少手動作業疏失

完整的追蹤紀錄：從需求到版控上線

以維運為考量的開發：架構、Log、監控、自動處理

DevOps
規劃目標

DevOps發展歷程



2017Q4

導入持續整合

2018

CI主從式架構轉換

2019

CI/CD整合
DevOps技術選型

2019Q3

啟動DevOps專案


2020



制定DevOps流程準則及規範
容器化

2021~

推行DevSecOps

OA表單：利用行內表單記錄變更及事件處理流程，並完成資源申請、上線申請。

 JBPM DevOps開發流程: 角色訂定、工具選用(JBPM)

  Jira
系統分析文件、系統設計文件、事件處理知識庫管理，線上編輯、告示，議題關聯，議題管理，以掌管需求開發進度。





PLAN

BUILD

QUALITY ASSURANCE

DEPLOY

OPERATE



統計資料 切換視圖

所有議題
未解決

未解決: 依照

嚴重程度

↓ Low

檢視事件

未解決: 依照負責人

負責人

江文鋒15664

徐育正19486

蔣政道1908

鄭尚倫196

黎嘉倫592

檢視事件

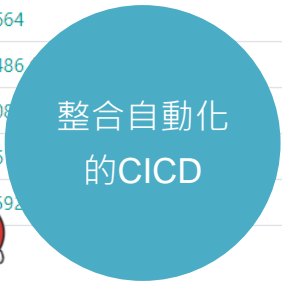
未解決: 由版本

版本

三月版

目前沒有修正版本的問題

檢視事件



我負責的
我報告的

沒有修正版本
未解決

事件 百分比

8

事件 百分比

4 50%

1 13%

3 38%

事件 百分比

1 13%

1 13%

2 25%

1 13%

3 38%

未解決: 由組件

事件

8

未解決: 按議題類型

事件類型

安詩 1 13%

任務 2 25%

故事 4 50%

錯誤 1 13%

事件 百分比

1 13%

2 25%

4 50%

1 13%

檢視事件



相關連結

+ 新增連結

- 尚無連結 -
請點選新增連結

相關附件

上傳檔案

新增待創建的-Jira議題

議題類型 * Jira專案 * 負責人 *

故事 DevOps維運型測試用 SA人員

議題摘要 *

OA轉開之議題

議題描述

測試OA表單流程並且截圖留存

取消 確認

Jira議題

+ 新增項目

編號	類型	摘要	專案	負責人	進度
----	----	----	----	-----	----

- 尚無Jira議題 -



本系統為測試用Jira請使用測試AD登入，若要使用正式Jira請至 <https://esbtrackingp.testesunbank.com.tw/>



DevOps維運型測試用 / **DEVOPS-1079**
OA表單轉開之議題

編輯 留言 指派 更多 更換版本 CANCEL 分派SA人員 挑選來源版本 管理

議題詳情

類型: 故事 狀態: **TO DO** (檢視工作流程)
嚴重程度: Medium 解決方式: 未解決
影響版本: 無 修正版本: 無
模組: 無
標籤: 無

單據資訊 版控資訊 議題進度

選擇Featruce分支來源: 從正在開發版本開立分支

描述

測試OA表單流程並且截圖留存

需求

DEVOPS-1079 OA表單轉開之議題

創建父級 創建子級 連結父級 連結子級 需求樹

人員

負責人: SA人員
指派給我
報告人: 匿名
主要負責人員: SA人員
投票: 0 對這個問題投票
監看者: 1 開始監看這個問題

日期

建立: 5分鐘前
更新: 5分鐘前

敏捷方法開發

在敏捷方法看板中查看

缺陷

未找到相關缺陷。



融斷功能模組開發

留言 敏捷方法看板 更多 開始處理 銷案 管理

匯出

議題詳情

類型: Requirement
 嚴重程度: Medium
 影響版本: 無
 標籤: 無
 狀態: **TO DO** (檢視工作流程)
 解決方式: 未解決
 修正版本: 無

描述

請協助融斷功能模組開發

需求

需求來源

創建父級 創建子級 連結父級 連結子級 需求樹

BSSB02PR-121 融斷功能模組開發

BSSB02PR-122 20201021融斷功能開發

測試案例

測試案例

測試案例總數: 5

創建測試案例 連結測試案例

BBSB02-30 驗證通知訊息之表格顯示規格及瀏覽窗格之資料顯示正確性	BSSB02PR-121	READY	✕
BBSB02-31 測試執行功能鍵	BSSB02PR-121	READY	✕
BBSB02-32 驗證通知訊息知之已讀/未讀訊息顯示方式	BSSB02PR-121	READY	✕
BBSB02-33 驗證週邊系統新增通知訊息之通知信發送時間(即時)及信件提醒內容與系統一致	BSSB02PR-121	READY	✕
BBSB02-37 驗證關鍵字搜尋功能查找具有指定關鍵字之備忘項目(查詢失敗)	BSSB02PR-121	READY	✕

事件連結

開發文件*

- Wiki Page
- ✕ 系統規格書(融斷功能)
- ✕ 系統設計書(融斷功能)

人員

負責人: User A
 報告人: minachen
 投票: 0 對這個問題投票
 監看者: 1 開始監看這個問題

日期

建立: 22/十月/20 12:58 上午
 更新: 現在

敏捷方法開發

在敏捷方法看板中查看

缺陷

問題記錄

關鍵字	問題	優先順序	狀態
BBSB02-74	無法執行功能鍵	↓	DONE
BBSB02-75	驗證失敗	↓	READY TO C...
BBSB02-76	無一致性	↓	DONE
BSSB02PR-3	20201013TDD	↑	ANALYSIS
BSSB02PR-4	201013TDD001	↑	ANALYSIS
BBSB02-273	失敗的單	↑	ANALYSIS



參、非功能需求

[請描述系統之非功能性需求]

(一) 系統備援等級

[例如：系統中斷後，修復時間要求等.....]

系統修復時間：2小時內 4小時內 24小時內 72小時內

(二) 資訊安全要求系統權限控管

[例如：個資遮蔽規則、表單增加浮水印、電子檔下載控管或禁止截取畫面等]

(三) 資料保存期限及備份機制

(四) 語系設定

(五) Timeout與重複登入管理機制

(六) S.T.R.I.D.E 威脅應對機制

[以 S.T.R.I.D.E 威脅模型分析 Abuse Case、威脅面向及防禦應對機制，並以圖及表格說明。若為行動應用程式或遠端服務依法規此項必填。S.T.R.I.D.E 威脅模型參考下表]

代表含意	描述	可因應對策(例)
Spoofing (偽冒)	假冒某人或是某物	身份驗證機制、保護帳密資料
Tampering (竄改)	惡意修改資料	授權機制、數位簽章
Repudiation (否認行為)	使用者否認其行為	數位簽章、稽核軌跡
Information Disclosure (資訊洩漏)	資訊被不預期的方式存取	授權機制、資料加密
Denial of Service (拒絕存取服務)	對使用者拒絕服務	封包過濾/避風頭
Elevation of privilege (權限提升)	未正常授權取得權限能力	以最小權限執行

例如：

Abuse Case	威脅面相	防禦應對機制
阻斷服務	Denial of Service (拒絕存取服務)	壓測、黑名單過濾

*2.問題討論

3 of 3

User A

@陳庭芳17759 請協助說明此部分功能為何?

Edit • Resolve • Like • yesterday at 4:14 PM

UserB

此功能需透過融斷機制進行開發，請 @蔡宜臻20353 協助開發hystrix模組

Edit • Delete • Like • yesterday at 4:26 PM

UserB

已轉開BSSB02PR-121進行追蹤

Edit • Delete • Like • 15 minutes ago

*1.問題標記

其他相關文件



⚡ Epic
10月月版

U UAT_Release
10月_UAT測試單

S SIT_Release
10月_SIT測試單

📄 Story
需求A

📄 Story
需求B

📄 Story
需求C

📄 Story
需求D

🚫 Bug
錯誤A

...

⚡ Epic
11月月版

U UAT_Release
11月_UAT測試單

S SIT_Release
11月_SIT測試單

📄 Story
需求1

📄 Story
需求2

📄 Story
需求3

📄 Story
需求4

🚫 Bug
錯誤1

...



根據需求內容在JIRA建立發布版本

建立新的事件 設置字段

Epic Name* [SG]B2E 通路費用設定(SQL)
在 JIRA Agile 板上用一個簡短的名稱標識此Epic。

摘要* [SG]B2E 通路費用設定(SQL)

標籤 [SG x]

專案管理人員* ESB
輸入使用者名稱, 系統會提供相符的使用者列表供您選擇。

修正版本* GIB.202104.01 x
輸入字元來獲得可能相符的列表, 或點擊下拉列表選擇

版控類型 GitLab

Group(GitLab)* xxx專案 x

Repo(GitLab)*

部署種類 Choose repo...

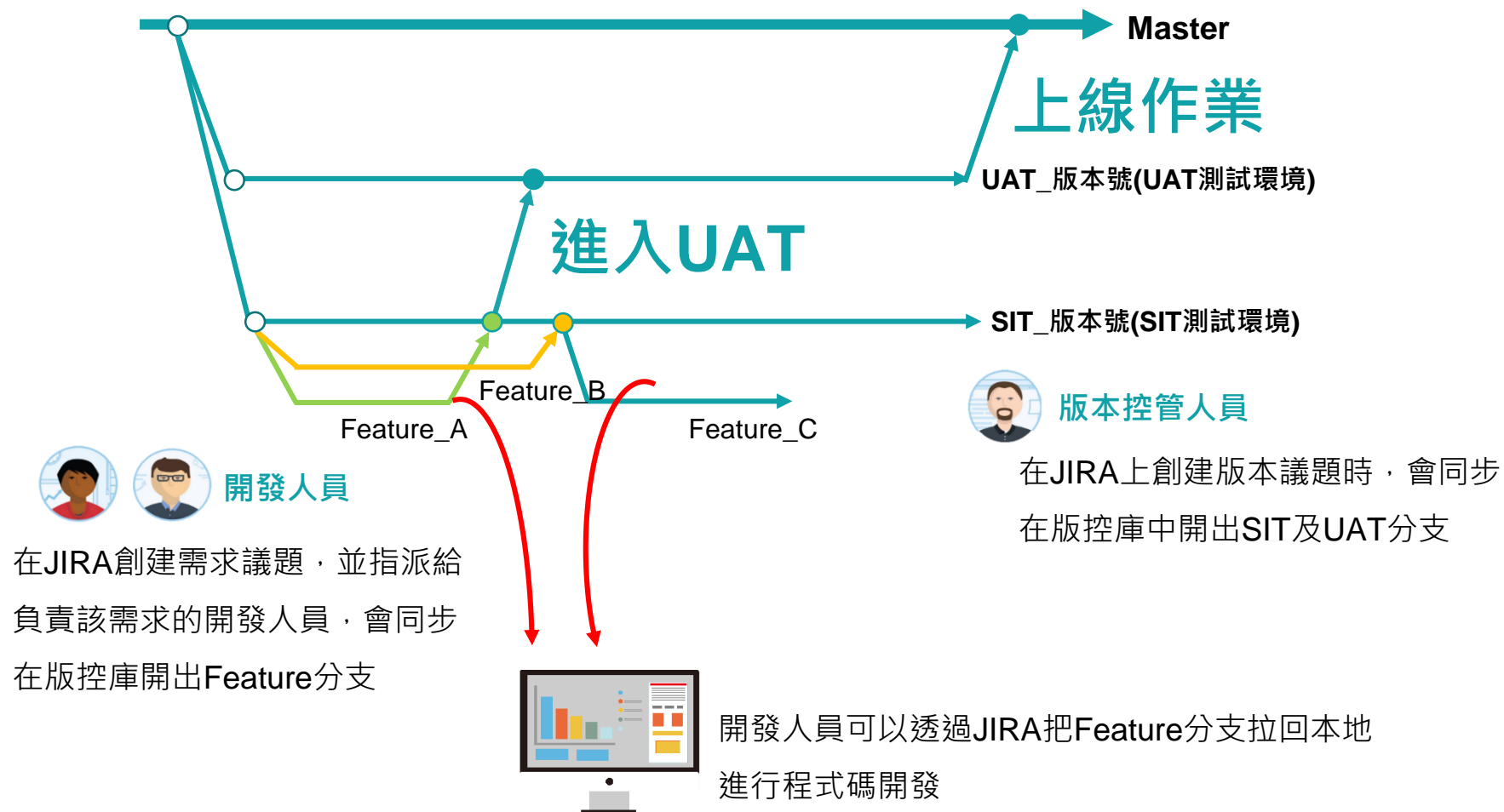
RM人員* GIB_CEO_APP
GIB_REGRESSION_TEST
GIB

是否需要執行週期性* 無
 是
 否

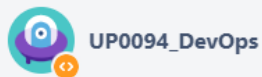
建立另一個 建立 取消

選擇版控來源

版控流程



請以開機帳號進行登入



創建面板

問題

報告

發佈版本

模組

SonarQube Connector

Git提交

需求

測試案例集

測試計劃

需求跟蹤

SynapseRT報告

附加組件

專案連結

添加一個有用的連結資訊給您的團隊。

新增連結



_DevOps / DEVOPS-151

新增【信用卡處向銀行查詢帳戶資料】功能

編輯 留言 指派 更多 更換版本 重新開發 CANCEL 重新創建SIT支線 管理

議題詳情

類型:	S 故事	狀態:	DONE (檢視工作流程)
嚴重程度:	↑ Medium	解決方式:	完成
影響版本:	無	修正版本:	七月大版
標籤:	無		

單據資訊 版控資訊 流水線資訊 程式碼品質 議題進度 需求規格

需求來源單號: 7月版, 之後要補上執工單單號
選擇Featue分支來源: 從正在開發版本開立分支

描述

新增【信用卡處向銀行查詢帳戶資料】功能

需求

測試案例

檔案附件

活動

全部 留言 工作日誌 歷史紀錄 Activity CI Builds Grid History Git收起 Git提交 版本

- JIRA 已增加一個評論 - 09/七月/21 5:04 下午
已創建 Feature_DEVOPS-151 分支,請確認。
- JIRA 已增加一個評論 - 09/七月/21 6:04 下午
User 已創建合併請求從 Feature_DEVOPS-151 到 SIT_七月大版, 請確認。

自動留言提示在上的Git操作

人員

日期

建立: 09/七月/21 4:33 下午
更新: 12/七月/21 11:34 上午
解決: 09/七月/21 6:23 下午

CI Builds

敏捷方法開發

缺陷

Git 源代码

2 提交
上卷

比较代码

分支
Create branch

UAT_七月大版 (后面有 16, 前面有 2)
Feature_DEVOPS-151 (后面有 16, 前面有 1)
SIT_七月大版 (后面有 16, 前面有 4)

Pull requests
Create pull request
Merge requests
Create merge request

版控分支資訊

審核程式碼

版控類型 GitLab

是否建立Temp合併分支
 無
 是
 否

程式碼審核人員

SR

SR人員 - SR@testesunbank.com.tw (SR)

留言

顯示 1 相符的使用者(共 1個)

Visual Text

所有使用者可見

審核程式碼

取消

搜尋

View all issues and filters

第1個議題, 共1098

提交程式碼審核，會自動於 GitLab/AzureDevOps提交分支合併請求

報告人:

Jira

主要負責人員:

SA人員

程式碼審核人員:

SD人員

開發人員:

PG人員

投票:

0 對這個問題投票

監看者:

2 開始監看這個問題

日期

建立:

26/十月/21 3:51 下午

更新:

1分鐘前

敏捷方法開發

[在敏捷方法看板中查看](#)

缺陷

未找到相關缺陷。

Pipeline _JIRA_EMULATION_DEV

合併集成後，進程式碼品質掃描



Stage View

	SCM	BUILD JOB	JUNIT	IQ_SERVER_SCAN	Remove Dev Files
Average stage times: (Average full run time: ~11s)	4s	526ms	355ms		
#88 Nov 09 18:13 49 commits	2s	593ms	346ms		



DevOps維運型測試用 / DEVOPS-1079

OA表單轉開之議題

編輯 留言 Log work 更多 更換版本 無DEV環境 重新開發

議題詳情

類型:	故事	狀態:	READY FOR DEV (檢視工作流程)
嚴重程度:	↑ Medium	解決方式:	未解決
影響版本:	無	修正版本:	202101012
模組:	無		
標籤:	無		

單據資訊 版控資訊 流水線資訊 程式碼品質 議題進度 需求規格

Quality Gate: DEV BUILD PASS DEV LIB PASS

描述
測試OA表單流程並且截圖留存

將結果更新回需求表單



本系統為測試用Jira請使用測試AD登入, 若要使用正式Jira請至 https://esbtrackingp.test

UP0094_DevOps維運型...

All issues Switch filter

Order by 建立

DEVOPS-1165 1125TrainingST01

DEVOPS-1164 1125TrainingST01

DEVOPS-1163 測試用V.1.0.0

DEVOPS-1161 測試用V.1.0.1

DEVOPS-1159 測試用V.1.0.1

DEVOPS-1158 測試用V.1.0.1

DEVOPS-1157 測試用V.1.0.1

DEVOPS-1156 U1_3.14_1_1: [授信帳戶-利率資訊

DEVOPS-1155 U1_3.14_4_1: [授信帳戶-利率資訊

DEVOPS-1154 U1_3.14_3_1: [授信帳戶-利率資訊

DEVOPS-1153 U1_3.14_2_1: [授信帳戶-利率資訊

DEVOPS-1152 U1_3.14_1_1: [授信帳戶-利率資訊

DEVOPS-1151

+ 新增議題

CICD

部署種類 VM

預計部署環境

流水線類型 Jenkins

Views(Jenkins) C105

Jenkins Views

Jobs(Jenkins)* C105_JIRA_SIMULATION_SIT x

Jenkins Jobs

階段環境 SIT

填選單一環境, 例如:SIT、SIT2、UAT、UAT1、UAT_EDLS

預計部署的模組 AP.WEB

用於Jenkins程式過版單的部署模組參數

主要檢核人員* QA

協同測試人員 顯示 1 相符的使用者(共 1個)

QA人員 - QA@testesunbank.com.tw (QA)

輸入使用者名稱, 系統會提供相符的使用者列表供您:

留言 樣式 B I U A

人員

負責人: RM人員

指派給我

報告人: 楊鎧濃22117

RM人員: RM人員

投票: 0 對這個問題投票

監看者: 1 停止監看這個問題

日期

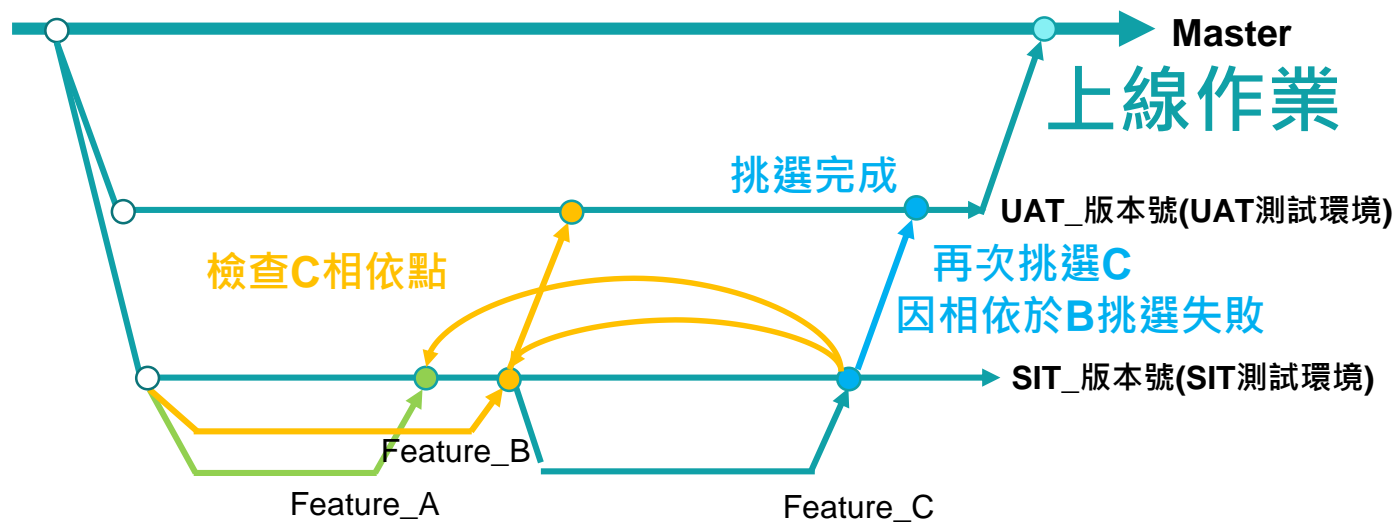
建立: 25/10/21 4:13 下午

更新: 25/10/21 6:18 下午

CICD 取消

第6個議題, 共1100

各個環境都可以自主設定
CICD工作, 並可設定特定檢
核、測試人員



系統分析師

UAT測試時可挑選需求進行差異上板，JIRA會依據相依性檢核挑選的需求，以確保程式完整性

透過JIRA挑選UAT上版需求



挑選需求至UAT 挑選需求上至UAT的需求

UAT需求清單

RM人員

留言

Pick UAT issue in current Version (顯示 3 相符的議題 (共 3個))

- DEVOPS-1045 - [SG]B2E 通路費用設定(SQL)
- DEVOPS-1046 - [HK]B2C 通路費用設定(SQL)
- DEVOPS-1047 - [TW]B2F 通路費用設定(SQL)

Visual Text

所有使用者可見

挑選需求至UAT 取消

挑選需求至UAT 當需求有相依性時提醒使用者

You need take dependency issues: DEVOPS-1045

UAT需求清單

DEVOPS-1047 x

RM人員

RM

輸入使用者名稱, 系統會提供相符的使用者列表供您選擇。

留言

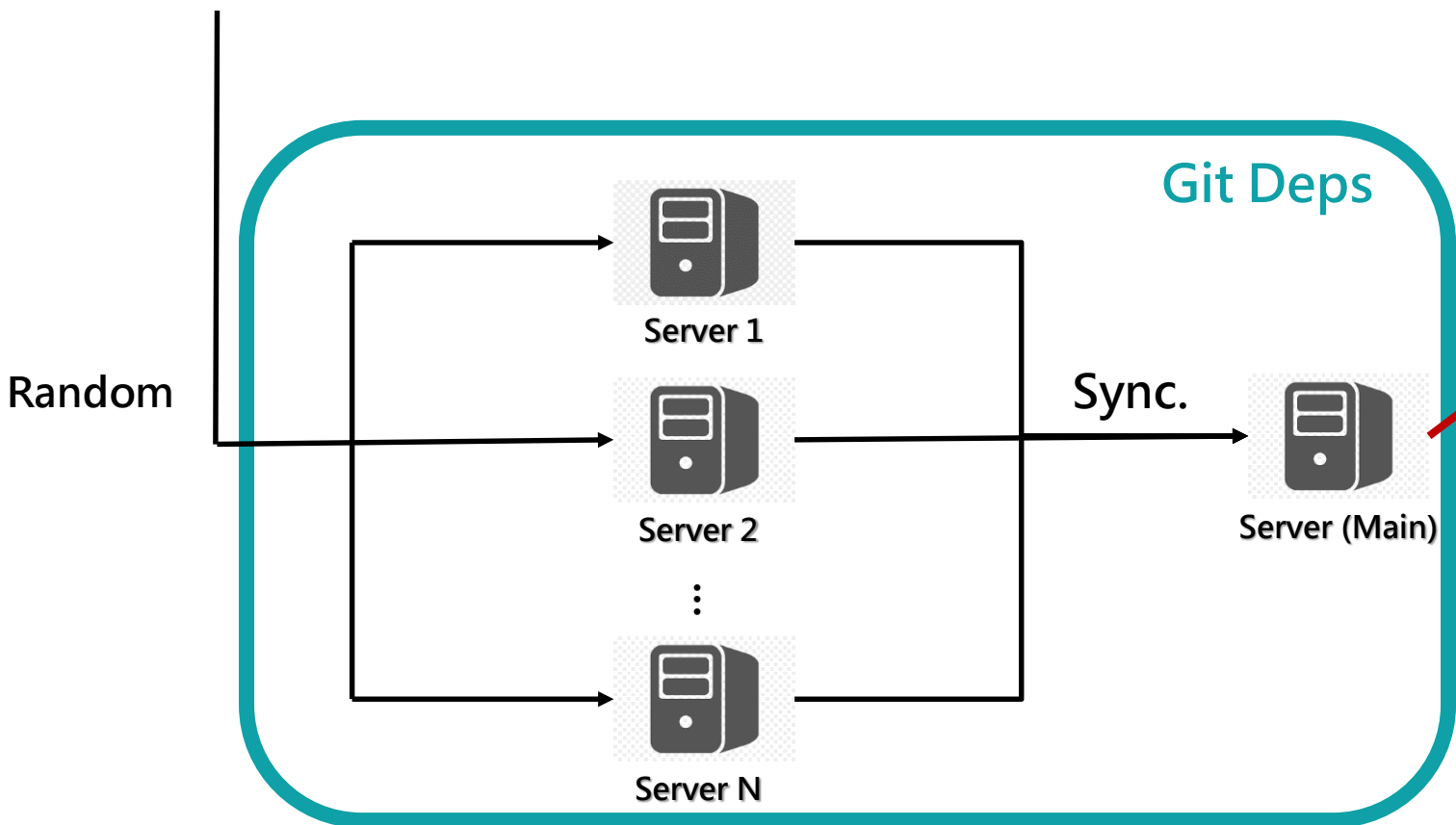
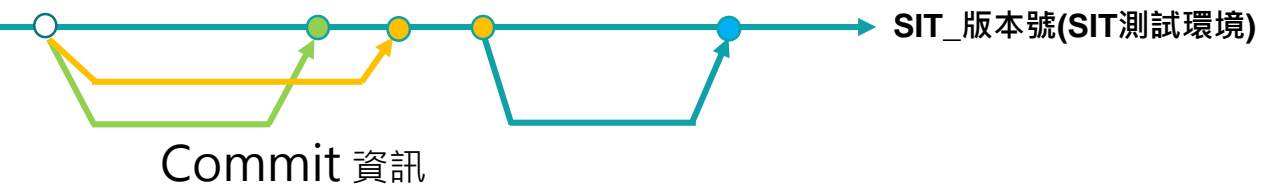
樣式

B I U A

Visual Text

所有使用者可見

挑選需求至UAT 取消



Deps. List

CH0018_EsunMobileBank / EMB-714

[Android] 網銀線下版本包版調整

編輯 留言 指派 更多 更換版本 重新開發 進入DEV 重新創建SIT支線 管理

議題詳情

類型: ■ 錯誤 狀態: CODE REVIEW APP... (檢視工作流程)

嚴重程度: ↑ Medium 解決方式: 未解決

影響版本: 無 修正版本: 202112月版_Android

標籤: 無

單據資訊 版控資訊 流水線資訊 程式碼品質 議題進度 需求規格

版控類型: AzureDevOps

Project(AzureDevOps): EsunMobileBank

Repo(AzureDevOps): EsunMobileBankAndroid

相依性檢查是否完成: 是

是否建立Temp合併分支: 否

Commit ID: 1c32f62883f37ae9efa8546aa9902e83b55aa593

Dependency List:

```

0f3b6b31181c0447a66baf44c778c9425bd5e6bc0284a93a4e68f04f1c9aa6e94eb450d9de63171607a6f26c1167b0a9bc12fabe8ed5
e1c9683fc4384396fc8868b39ce37a7c8042e0111da41ef70b5:555bc83e68bc2351f860642228976133b175b0ef7b8592bb7800383a
9858c6259e33513c75f88d8:0629e16eb07b285737e60c3c7891993307d02a6:1153d3fafac6586a05e7b0f4bb2c631073d3e03b375c3
616de4cd37858feed7146df1a9f52d20ee7:e2000bb4d432772b470091d4dc86ea63b18a1881:0c1b2cf295351c626bfa87995d6080e2a
7cd33aa:776151105eab60d7412e85685e69b989792d52a2:d5c6914dfb777ee4edff475504a50f9a9e1248d:8264fa865c5d37df3a08c2
ba0af245938b6987fb:87a0b46e926f253a250de39d98bcaa4eced6492e:81979d3b99bfe80b7881c7990878aa835eb442e:2ec6e2106f
1807c561643137eb1e58ecddcc13d6:263c01d69babc463873ea4314de1fe64b526d14:9f33c3807e663470d9f05cad4eeb4f95c60c5a2
569224d6daf1139b350777aaa7c32d7188cd691b9:70fc06e08d0487a2f4e650b2790c1de2a3f1559b:8e45f54852c38075ca9e06dbf602
aa007261f485
  
```

議題追蹤及流程控管



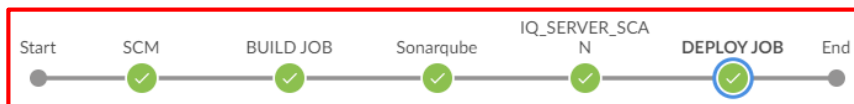
! CH0041_GIB SIT < 593

分支: — 2h 31m 46s 修改人 AtlassianAD-Test, HYT-Jill

提交: — 5 hours ago 由使用者 AtlassianAD-Test 啟動

描述 GIB-2710,GIB-2707,GIB-2706,GIB-2703,GIB-2683,GIB-2637,GIB-2595,GIB-2590,GIB-2574,GIB-2571,GIB-2549,GIB-2536,GIB-2533,GIB-2532,GIB-2531,GIB-2522,GIB-2515,GIB-2500,GIB-2497,GIB-2466,GIB-2460,GIB-2456,GIB-2448,GIB-2442,GIB-2439,GIB-2437,GIB-2435,GIB-2430,GIB-2418,GIB-2407,GIB-2395,GIB-2391,GIB-2388,GIB-2386,GIB-2352,GIB-2351,GIB-2346,GIB-2278,GIB-2277,GIB-2252,GIB-2231,GIB-2216,GIB-2140,GIB-2139,GIB-2138,GIB-2124,GIB-2042,GIB-1869

根據各環境流水線進行CICD



議題詳情

類型: **S** 故事
嚴重程度: ↑ Medium
影響版本: 無
標籤: Benny Merged

狀態: **DONE** (檢視工作流程)
解決方式: 完成
修正版本: GIB.202012.01

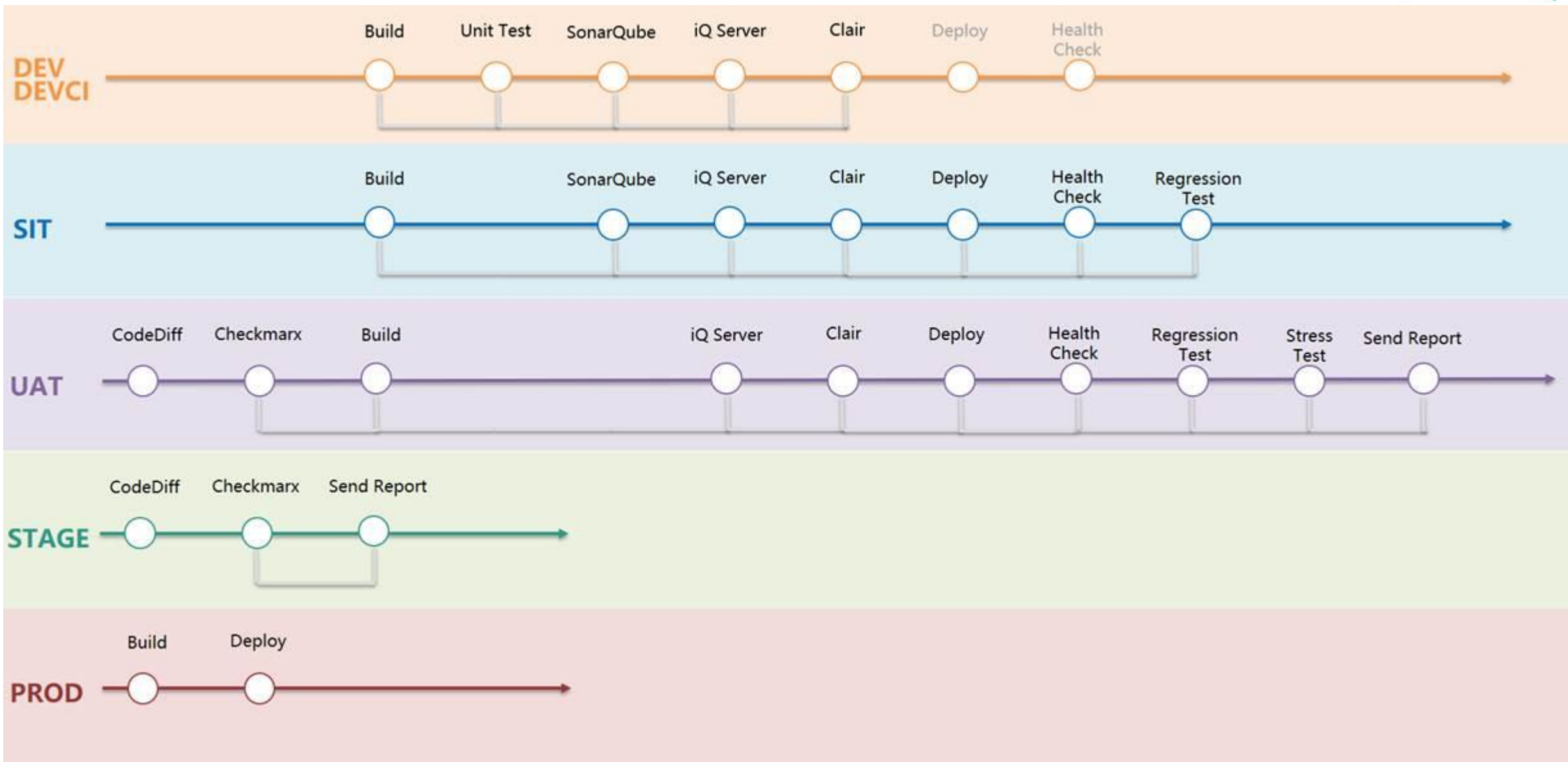
將管線執行結果回寫至JIRA

單據資訊 版控資訊 流水線資訊 程式碼品質 議題進度

Quality Gate:

- DEV BUILD PASS
- DEV LIB PASS
- DEV TEST PASS
- SIT HEALTH PASS
- SIT TEST PASS
- SIT DEPLOY PASS
- SIT REGRESSION PASS
- SIT CODEQUALITY PASS
- SIT LIB PASS
- SIT BUILD PASS
- UAT HEALTH PASS
- UAT TEST PASS
- UAT DEPLOY PASS
- UAT LIB PASS
- UAT BUILD PASS
- UAT REGRESSION PASS
- STAGE SAST PASS
- STAGE REPORT PASS

完整的流水線設計

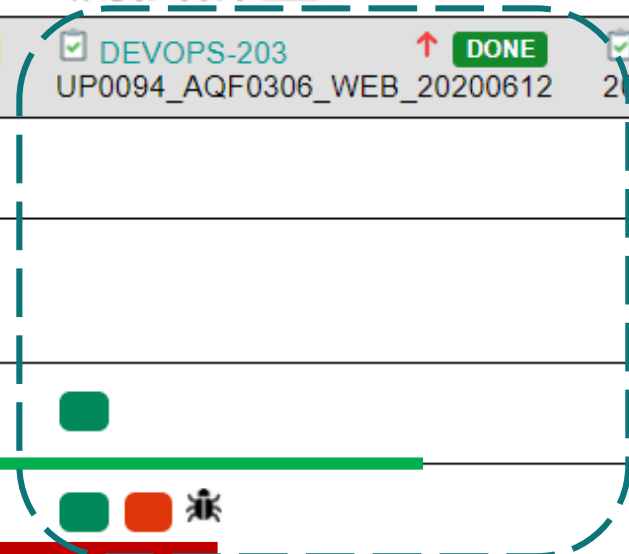




測試計畫

需求	測試案例	DEVOPS-869 20201021Test002	IN PROGRESS	DEVOPS-203 UP0094_AQF0306_WEB_20200612	DONE	DEVOPS-44 20200610WebTP0001
需求 DEVOPS-109 新增【借戶年所得登錄(AQF0306)】功能	DEVOPS-833 CTWTPPTXS-006-001		READY			
	DEVOPS-961 【設定代理-科主管設定同仁】由科主管設定同科內人員互為職務代理		READY			
	DEVOPS-173 TSC00X_TSC00X_4_14		READY			
	DEVOPS-165 TSC00X_TSC00X_4_6		IN PROGRESS			
需求 DEVOPS-107 修改【建檔基本資料(AQF0308)】功能	DEVOPS-172 TSC00X_TSC00X_4_13		READY			
	DEVOPS-168 TSC00X_TSC00X_4_9		READY			
需求 DEVOPS-105 新增【建檔基本資料(AQF0308)】功能	DEVOPS-172 TSC00X_TSC00X_4_13		READY			
	DEVOPS-168 TSC00X_TSC00X_4_9		READY			

測試案例



Defect



UAT 環境

測試進度

Key	Created	Jira測試週期名稱	測試開始日期	測試結束日期	總工作天數	已工作天數	測試案例總數	已測試案例總數 (Passed&Failed)	已通過案例總數	未通過案例總數	不適用案例總數	測試執行率	測試通過率	測試產度	已達進度	測試達成率
ICC-3568	Nov 09, 2021	UAT Round1	2021-11-01	2021-11-19	15	7	2304	688	479	209	15	30.06%	69.62%	46.67%	20.93%	44.84%
ICC-3543	Nov 08, 2021	UAT Round1	2021-11-01	2021-11-19	15	6	2304	490	364	126	5	21.31%	74.29%	40.00%	15.83%	39.58%
ICC-3542	Nov 08, 2021	UAT	2021-11-01	2021-11-19	15	6	2304	490	360	127	5	20.97%	74.60%	40.00%	15.66%	39.15%

Defect開立數量

	1 Nov 2021	2 Nov 2021	3 Nov 2021	4 Nov 2021	5 Nov 2021	6 Nov 2021	7 Nov 2021	8 Nov 2021	9 Nov 2021	10 Nov 2021	11 Nov 2021	12 Nov 2021	13 Nov 2021	14 Nov 2021	15 Nov 2021	16 Nov 2021	17 Nov 2021	18 Nov 2021	19 Nov 2021	20 Nov 2021	21 Nov 2021	22 Nov 2021	23 Nov 2021
UAT Round1	3	11	8	7	16	-	-	4	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Total (Issues)	3	11	8	7	16	0	0	4	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0

自動化測試(Defect狀態)

狀態	ANALYSIS	TO DO	POSTPONE	IN PROGRESS	READY TO CONFIRM	DONE	CANCEL	READY	Total
UAT Round1	30	2	-	6	12	13	2	-	65
Total (Issues)	30	2	0	6	12	13	2	0	65

自動化測試(Defect嚴重程度)

嚴重程度	Highest	High	Medium	Low	Lowest	Total
UAT Round1	2	14	31	3	-	50
Total (Issues)	2	14	31	3	0	50

SIT環境

測試進度

Key	Created	測試開始日期	測試結束日期	總工作天數	已工作天數	測試案例總數	已測試案例總數 (Passed&Failed)	已通過案例總數	未通過案例總數	不適用案例總數	測試執行率	測試通過率	測試產度	已達進度	測試達成率
ICC-3460	Oct 26, 2021	2021-08-24	2021-10-22	44	44	89	88	74	14	1	100.00%	84.09%	100.00%	84.09%	84.09%
ICC-3452	Oct 22, 2021	2021-08-24	2021-10-22	44	44	89	71	65	6	1	80.68%	91.55%	100.00%	73.86%	73.86%
ICC-3438	Oct 21, 2021	2021-08-24	2021-10-22	44	43	89	66	59	7	1	75.00%	89.39%	97.73%	67.05%	68.60%

Defect開立數量

	1 Nov 2021	2 Nov 2021	3 Nov 2021	4 Nov 2021	5 Nov 2021	6 Nov 2021	7 Nov 2021	8 Nov 2021	9 Nov 2021	10 Nov 2021	11 Nov 2021	12 Nov 2021	13 Nov 2021	14 Nov 2021	15 Nov 2021	16 Nov 2021	17 Nov 2021	18 Nov 2021	19 Nov 2021	20 Nov 2021	21 Nov 2021	22 Nov 2021	
SIT_1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Total (Issues)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

自動化測試(Defect狀態)

狀態	ANALYSIS	TO DO	POSTPONE	IN PROGRESS	READY TO CONFIRM	DONE	CANCEL	Total
SIT_1	-	-	-	2	2	177	-	181
Total (Issues)	0	0	0	2	2	177	0	181

自動化測試(Defect嚴重程度)

嚴重程度	Highest	High	Medium	Low	Lowest	Total
SIT_1	-	-	4	-	-	4
Total (Issues)	0	0	4	0	0	4



應達/實達比			
議題追蹤			
標籤類別	應達百分比	實達百分比	議題數量
開發	74.78%	60.15%	61
周邊系統	25.79%	18.02%	22
SD文件	42.65%	50.00%	2
DEV資源	100.00%	.00%	1
SIT資源	100.00%	8.33%	3
UAT資源	.00%	.00%	0
Prod資源	.00%	.00%	0
功能測試	85.01%	78.46%	13
SIT測試	21.15%	10.00%	2
UAT測試	.00%	.00%	0
壓力測試	50.00%	50.00%	2
安全測試	.00%	.00%	0
教育訓練	.00%	.00%	0
上線作業	.00%	.00%	0
結案	.00%	.00%	0
總共	33.29%	18.33%	106

1 issue Refresh

正在進行	即將過期	超出預計完成時間
<div style="border: 2px solid green; border-radius: 15px; padding: 10px; text-align: center;"> <p>Unresolved</p> <p>20</p> </div> <p>Chart By: 解決方式 Count: Issues Total: 20</p>	<div style="display: flex; justify-content: space-around;"> <div style="border: 2px solid orange; border-radius: 15px; padding: 10px; text-align: center;"> <p>Unresolved</p> <p>6</p> </div> <div style="border: 2px solid blue; border-radius: 15px; padding: 10px; text-align: center;"> <p>完成</p> <p>4</p> </div> </div> <p>Chart By: 解決方式 Count: Issues Total: 10</p>	<div style="border: 2px solid red; border-radius: 15px; padding: 10px; text-align: center;"> <p>Unresolved</p> <p>10</p> </div> <p>Chart By: 解決方式 Count: Issues Total: 10</p>

負責人議題

B08大個金顧客通知平台 (RACE) 任務, 故事

Status: All 發案修19592 - k83142917-195...

Contains text... Search Show JQL

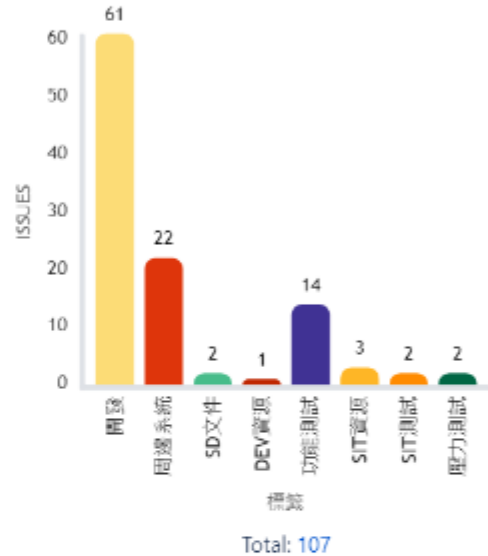
21 issues found



狀態	Issues	%
TO DO	4	19%
IN PROGRESS	1	4.8%
IN DEVELOPMENT	1	4.8%
DEV CICD	0	0%
READY TO CONFIRM	0	0%
DONE	15	71.4%

需求階段總攬

柱狀圖 統計需求於各階段環境 開發 SIT UAT 議題種類及數量



每周完成議題數

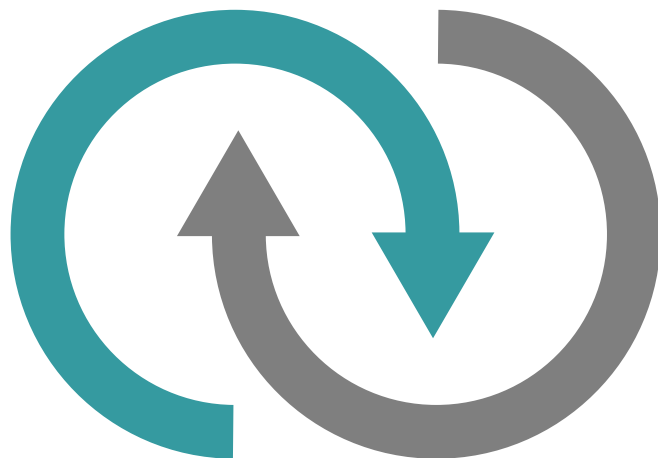


邁向DevSecOps



交付速度

導入DevOps後，產出速度加快，但交付時間及品質卻未明顯提升



交付品質

導入安全檢測及套件掃描工具，並導入自動化測試框架，制定準入準出原則，以提升交付品質。



測試



- 人工測試耗時
- 紀錄追蹤不易



資安



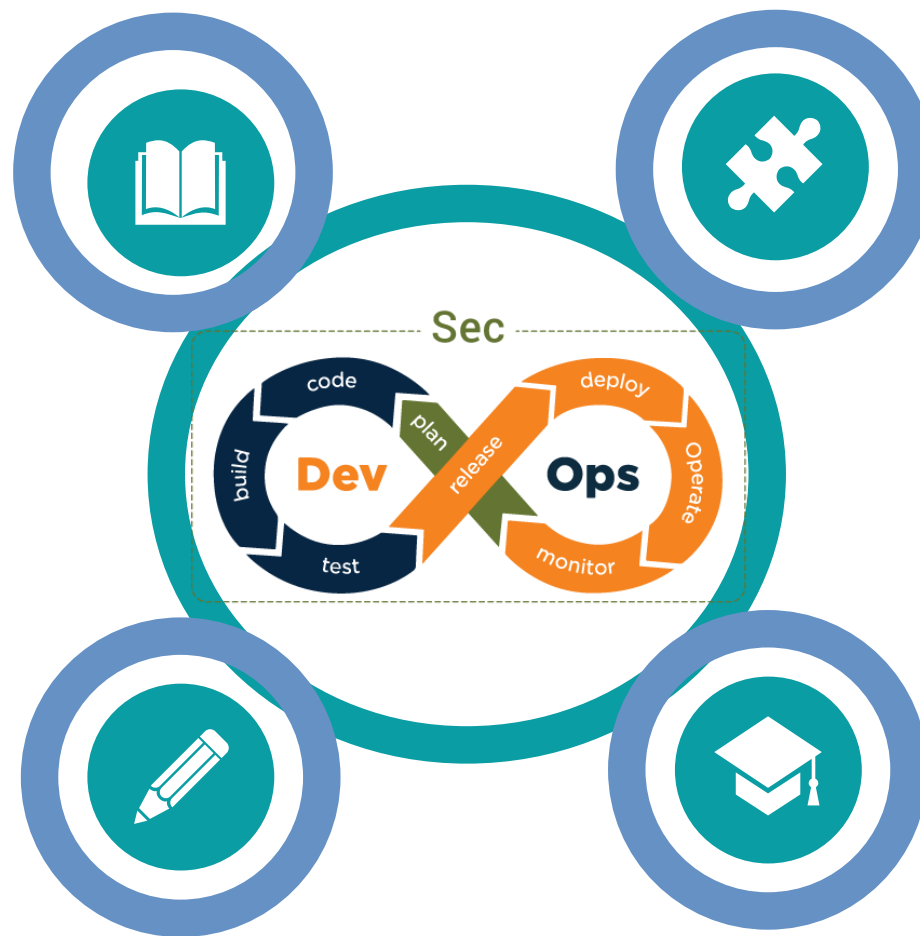
- 查驗流程耗時
- 潛在風險發現不及時
- 函式庫授權、弱點檢測及管理不完整





完整流水線

- ✓ 定義各環境流水線、程式碼組建部署及品質檢測
- ✓ 定義準入準出原則



議題追蹤&流程控管

- ✓ 透過統一介面進行溝通、開發及測試，完善流程狀態的追蹤

角色切分

- ✓ 劃分流程中角色(PG、SA、SD、PM、BA、QA、RM)
- 自動化測試人員協助測試
- 資安人員制定規範，確保各階段如質如期地進行

落實安全

- 落實各階段品質卡控，強化資安效益。
- 即時通知機制，提升問題排障及時性。

E.SUN 安全機制



 **Checkmarx**
靜態程式安全

sonarqube
程式碼品質

 **Nexus Container**
黑箱容器安全

 **HCL AppScan**
黑箱測試

 **clair**
靜態容器安全

 **Nexus Lifecycle**
開源套件安全





分析風險

- 重複程式碼比例
- 程式維護、技術債比例
- 安全性漏洞
- 系統測試覆蓋率

DevOps Rename

Conditions ?

Conditions on New Code

Metric	Operator	Value
Duplicated Lines (%)	is greater than	60.0%
Maintainability Rating	is worse than	D
Vulnerabilities	is greater than	0
Reliability Rating	is worse than	D

若程式碼品質檢測出現下述項目之一，則須進行修復或提出說明

- A. 重複程式碼百分比大於 60%
- B. 維護比例大於 50%
- C. 出現違反可靠性阻擋標準之項目



版控資訊 流水線資訊 程式碼品質

Quality Gate:

✔ SIT BUILD PASS

❌ SIT CODEQUALITY FAIL

Resources should be closed

Java

5



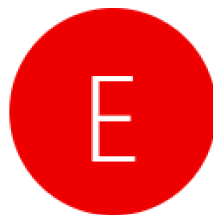
GIB-2770

Size



2,616,507 lines of code

Reliability



bugs

Security



vulnerabilities

Maintainability



60,900 code smells
2269d technical debt
1.4% technical debt ratio



CH0041_GIB / GIB-2770

Resources should be closed



編輯



留言

指派

更多 ▾

進入開發

議題詳情

類型:

B 錯誤

嚴重程度:

↑ Medium

影響版本:

無

標籤:

無

版控資訊

議題進度

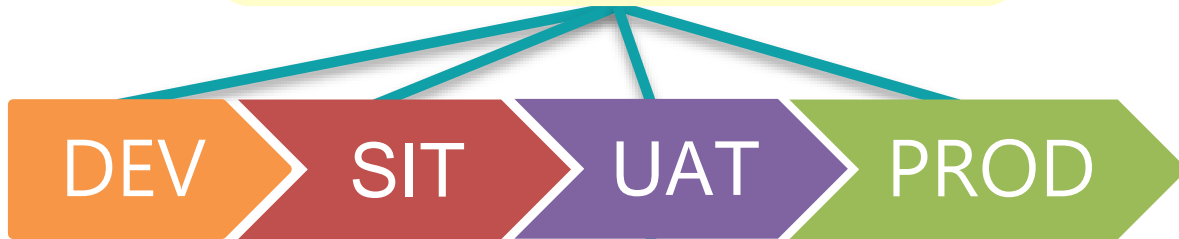
相依性檢查是否完成: 否

描述

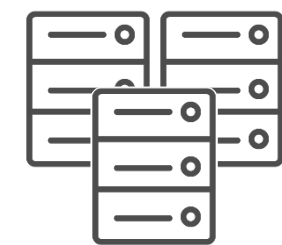
Go to check your issues to SonarQube project: GIB



開發、編譯過程透過
Nexus RM 抓取套件



編譯成品掃描



外部來源



開發人員



檢查 CVE, License



Nexus Lifecycle
by sonatype



套件放行 or 隔離



Nexus Repository
by sonatype



Nexus Firewall
by sonatype



✓ 上版/上線前整合自動掃描

	SCM	DEPLOY JOB	CODE_DIFF	CHECKMARX_ALL	REPORT_NOTIFY
Average stage times: (Average full run time: ~2min 34s)	6s	34ms	2s	2min 5s	1s
#7 Apr 14 15:32 80 commits	6s	34ms	2s	2min 5s	1s

✓ 每周/每月例行掃描

	SCM	TS0129_GTS_JP	TS0129_GTS_JP	ABR_HK	ERLC_Report_E
Average stage times:	11s	9min 4s	0ms	3h 11min	8s
#211 May 08 00:00 609 commits	19s	33s	29s	32min 36s	8s
#210 May 01 00:00 17 commits	6s	28s	28s	40min 28s	8s
#209 Apr 24 00:00 104 commits	12s	1h 20min	6min 33s	40min 52s	7s

✓ 於掃描後寄信通知

2020/12/12 (週六) 上午 08:01

esbcidevops@testesunbank.com.tw
SIT_Checkmarx - Build # 190 - SUCCESS!

收件者 [] [] [] []

按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

ScanReport.pdf
.pdf 檔案

BUILD

Build URL: https://_____ .testesunbank.com.tw/job/

Project: SIT_Checkmarx

Date of build: Sat, 12 Dec 2020 00:00:00 +0800

Build duration: 8 hr 1 min and counting

Build cause: Started by timer

Build description:

Built on:

```
[Cx-Info]: Uploading zip file
[Cx-Info]: Temporary file deleted
[Cx-Info]: Sending SAST scan request
[Cx-Info]: SAST Scan created successfully. Link to project st
[Cx-Info]: _____Get CxSAST Results:_____
[Cx-Info]: Waiting for CxSAST scan to finish.
[Cx-Info]: Waiting for SAST scan results. Elapsed time: 00:00
[Cx-Info]: Waiting for SAST scan results. Elapsed time: 00:00
[Cx-Info]: Waiting for SAST scan results. Elapsed time: 00:01
[Cx-Info]: Waiting for SAST scan results. Elapsed time: 00:01:21. 16% processed. Status: Scanning.
[Cx-Info]: Waiting for SAST scan results. Elapsed time: 00:01:41. 16% processed. Status: Scanning.
[Cx-Info]: Waiting for SAST scan results. Elapsed time: 00:02:01. 99% processed. Status: Finished.
[Cx-Info]: SAST scan finished successfully.
[Cx-Info]: Retrieving SAST scan results
[Cx-Info]: Waiting for server to generate xml report. 4990 seconds left to timeout
[Cx-Info]: _____Checkmarx Scan Results(CxSAST):_____
[Cx-Info]: High severity results: 0
[Cx-Info]: Medium severity results: 1
[Cx-Info]: Low severity results: 0
[Cx-Info]: Information severity results: 0
[Cx-Info]:
[Cx-Info]: Scan results location: https:// _____ esunbank.com.tw/CxWebClient/ViewerMain.aspx?scanId= _____ &Projec
[Cx-Info]: _____
```



安全規章: ISMS



資安種子



KM文件

(三) 資安檢測：

泛指為確認是否存在資訊安全風險或技術脆弱性議題，進而針對程式碼、主機設備、網站伺服器等標的進行之檢測作業，依檢測頻率可分為週期性檢測及臨時性檢測。

本作業要點所涵蓋之資安檢測類型如下：

1. 程式碼檢測

Case 1	
事件系統	AU
上架日期	2020
經辦	柯
資安種子	陳
Checkmarx 版本	8.9.0.210 HF5

OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)

CGI Reflected XSS All Clients\路徑 1:

嚴重程度： 中風險
 結果狀態： 校驗
 線上結果 [https:// esunbank.com.tw/CxWebClient/ViewerMain.aspx?scanid=&projectid=&pathid=](https://esunbank.com.tw/CxWebClient/ViewerMain.aspx?scanid=&projectid=&pathid=)
 狀態 新的

在Gener...oller.java文件的行號388中，找到未經驗證的輸入。在println的行號 388中，找到了跨網站指令碼(Cross-site scripting,XSS)的可能開發。

	來源	目的地
檔案	Gener ontroller.java	Gener ontroller.java
行	390	390
物件	getUserInfo	println

代碼片斷
檔案名稱
方法

```

Gener... C
ontroller.java
public ModelAndView data(@ModelAttribute("model") AssetTransFormBean form)
{
    ....
    390.
        System.out.println("form.getUserInfo().getUserMst().getBankNo()="+
        form.getUserInfo().getUserMst().getBankNo());
  
```

解決方式

容器安全

實施架構

容器架構的導入，建立CI流水線進行准入准出控制



實行策略

導入容器策略管理，節省實施政策及規則管理的時間

Admission Control (阻擋部署)

DLP Sensors (資訊、資料阻擋)



事件記錄

事件留存記錄
快速查找變更軌跡

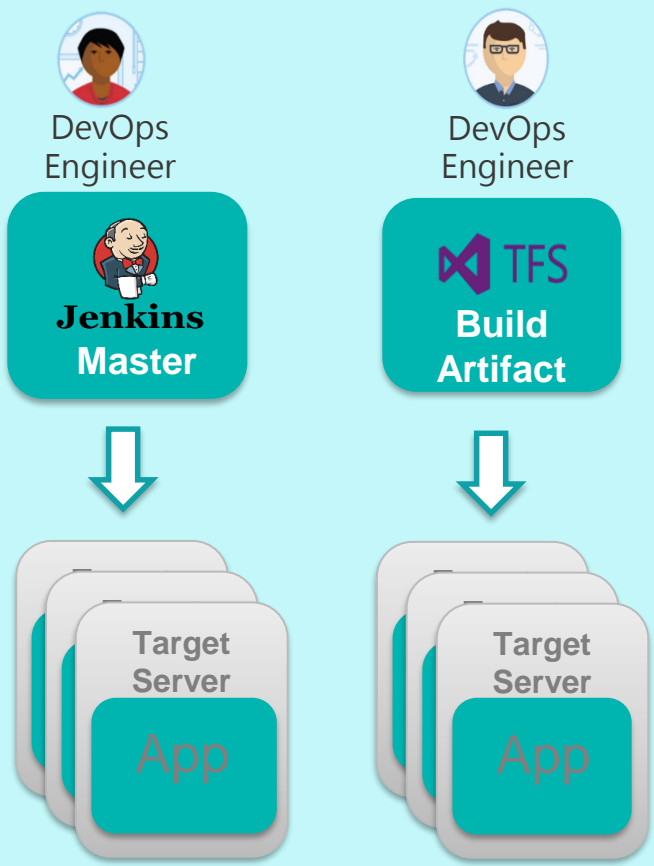


持續監控

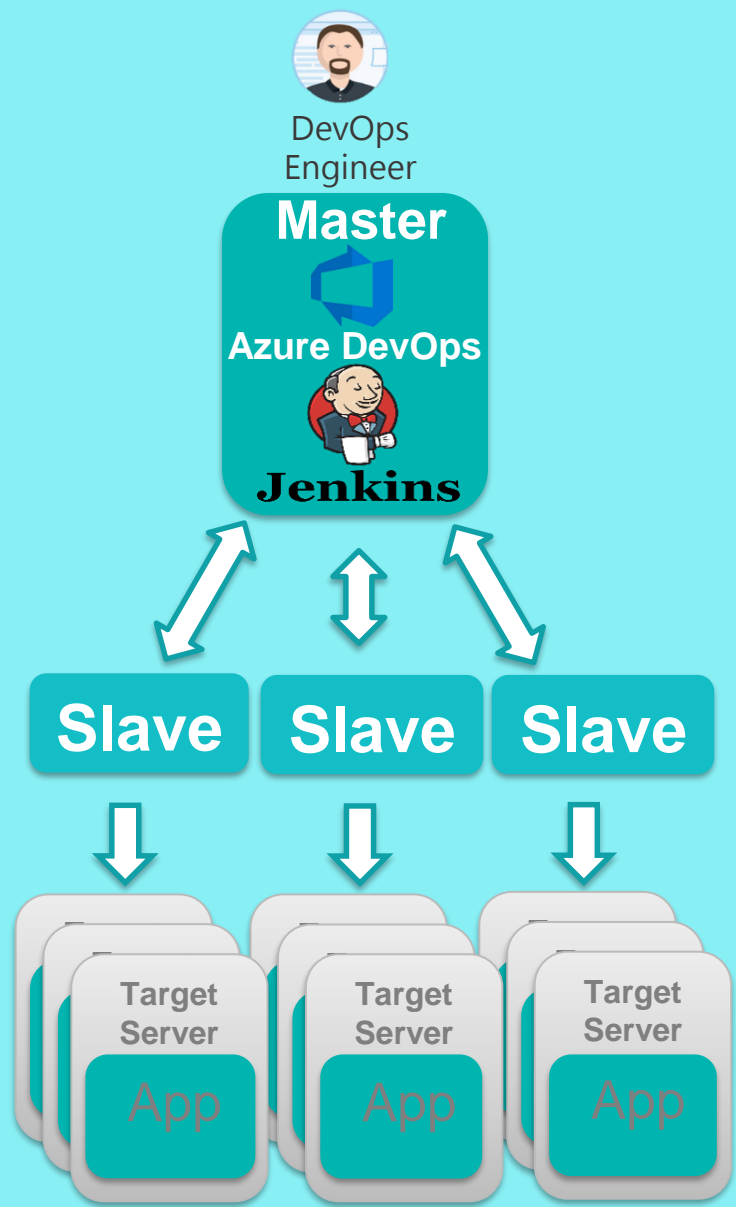
Dashboard檢視容器安全狀態
即時監控L7網路流量



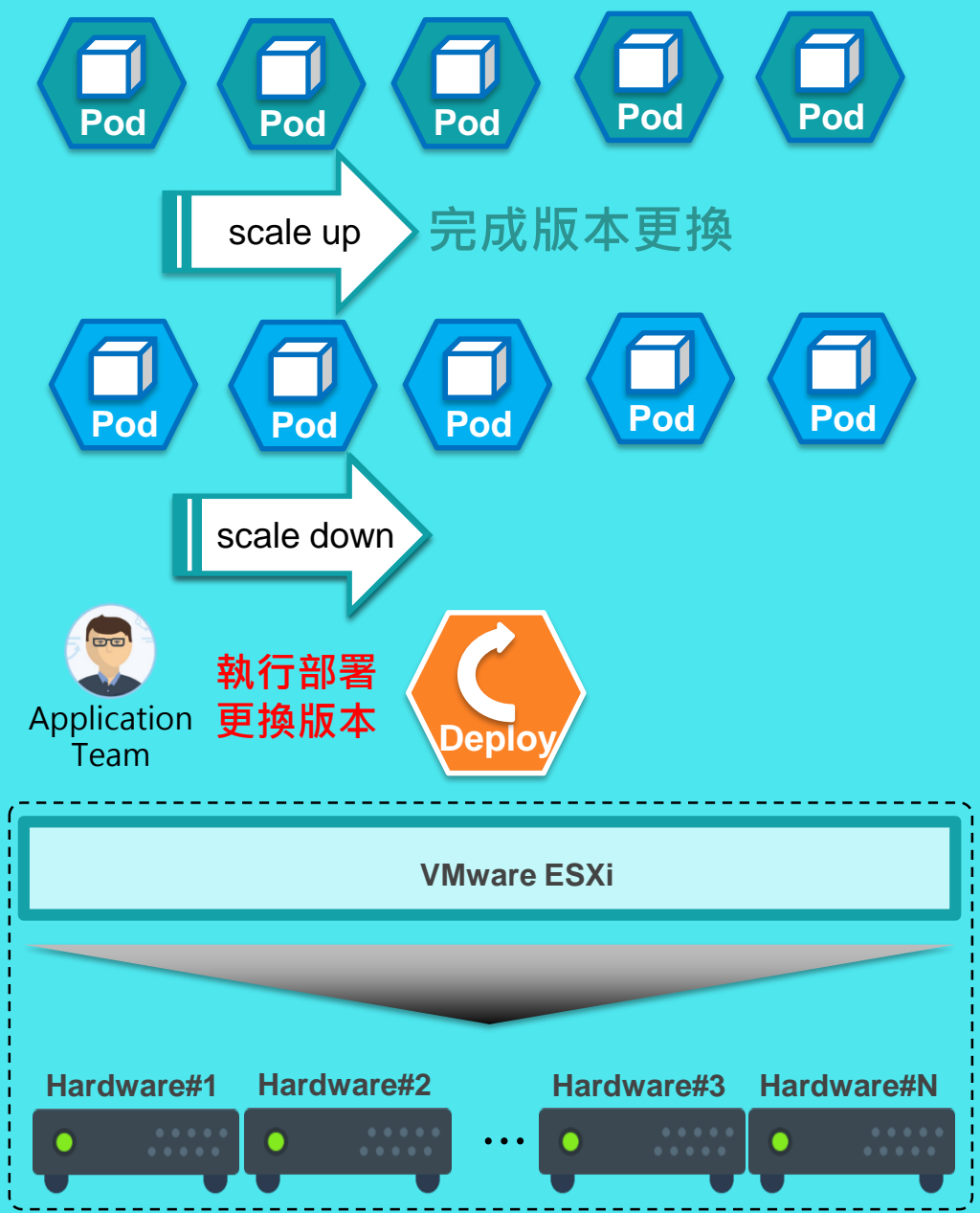
單體式



主從式



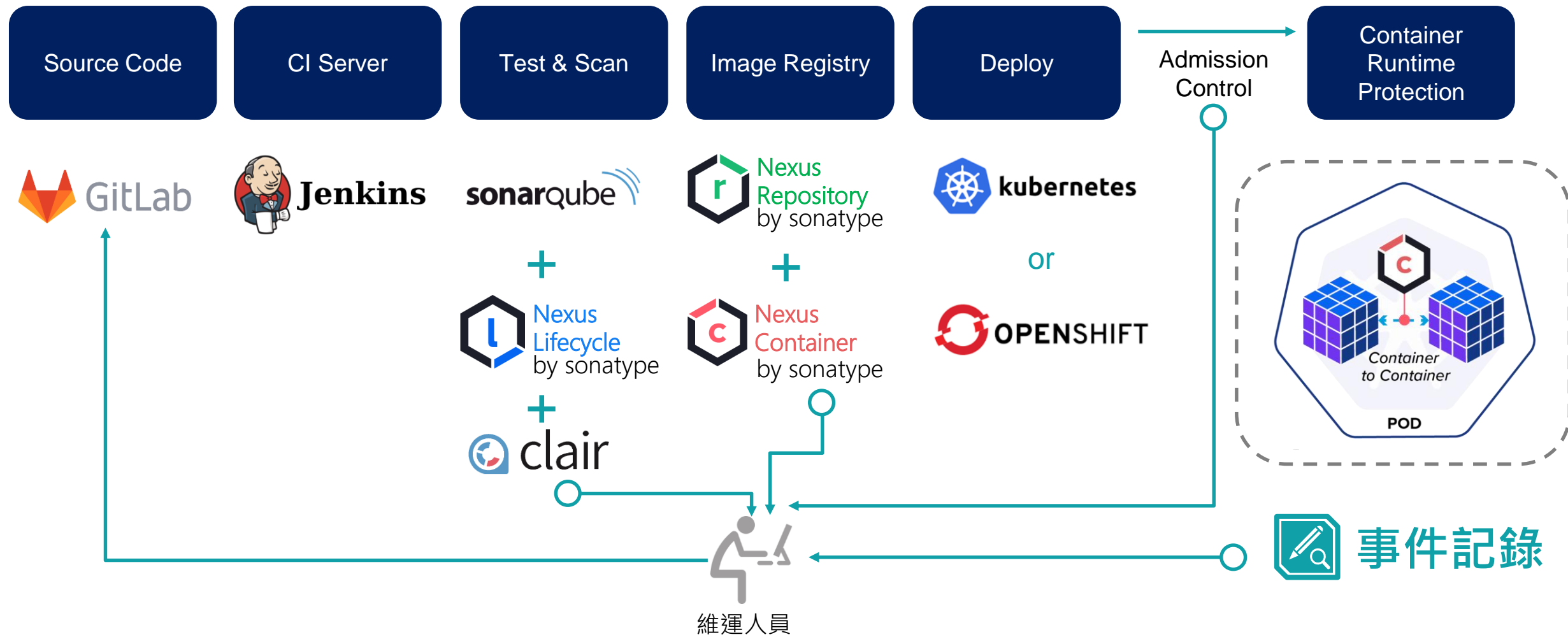
容器化



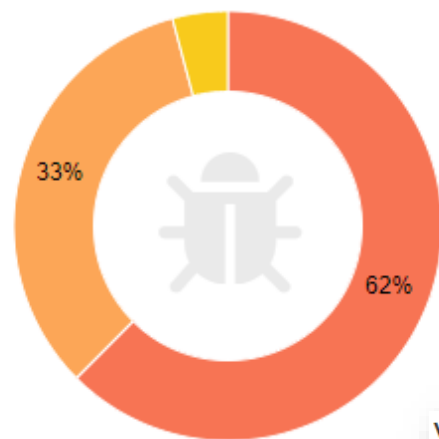
實施架構

實行策略

持續監控



實行策略 – Image Scan (鏡像安全)



Quay Security Scanner has detected **24** vulnerabilities.
Patches are available for **24** vulnerabilities.

- 15** High-level vulnerabilities.
- 8** Medium-level vulnerabilities.
- 1** Low-level vulnerabilities.

Vulnerabilities

CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION
▶ RHSA-2020:2852	High	nodejs-full-i18n	1:10.24.0-1.module+el8.3.0+10166+b07ac28e	1:12.18.2-1.module+el8.2.0+7233+61d664c1
▶ RHSA-2021:0734	High	nodejs-full-i18n	1:10.24.0-1.module+el8.3.0+10166+b07ac28e	1:12.21.0-1.module+el8.3.0+10191+34fb5a07
▶ RHSA-2021:0744	High	nodejs-full-i18n	1:10.24.0-1.module+el8.3.0+10166+b07ac28e	1:14.16.0-2.module+el8.3.0+10180+b92e1eb6
▶ RHSA-2021:1024	High	openssl-libs	1:1.1.1g-12.el8_3	1:1.1.1g-15.el8_3
▶ RHSA-2021:1024	High	openssl-devel	1:1.1.1g-12.el8_3	1:1.1.1g-15.el8_3

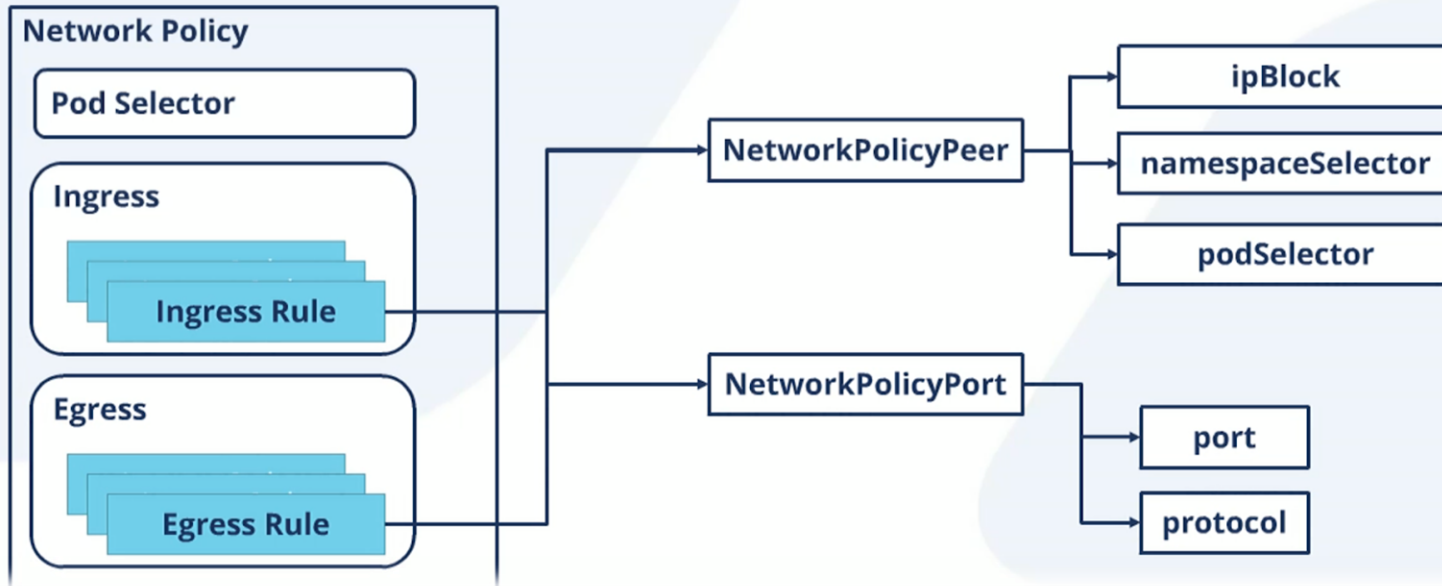


SDN: Software Defined Network



Network Policy Definitions

- Rules contain peers (the other side of the connection) and ports



- 禁止訪問指定服務
- 限制訪問指定服務
- 放行訪問限制
- 禁止 namespace 中非白名單流量
- 禁止其他 namespace 流量
- 運行所有 namespace 流量
- 指定 namespace 訪問服務
- 允許其他 namespace 的指定 pod 的流量
- 允許外網訪問服務
- 允許應用固定埠流量
- 多標籤限制
- 禁止應用的出口流量
- 禁止命名空間非白名單流量



持續監控 – Dashboard檢視容器安全狀態



即時監控安全風險

Security Risk Score

25
FAIR

Nodes	Pods
4	39

Service Connection Risk

Discover	0
Monitor	14
Protect	1

Ingress/Egress Exposure Risk

Discover	0
Threats	0
Violations	1

[Improve your score](#)

Vulnerability Exploit Risk

Discover	0
Monitor	942
Protect	211

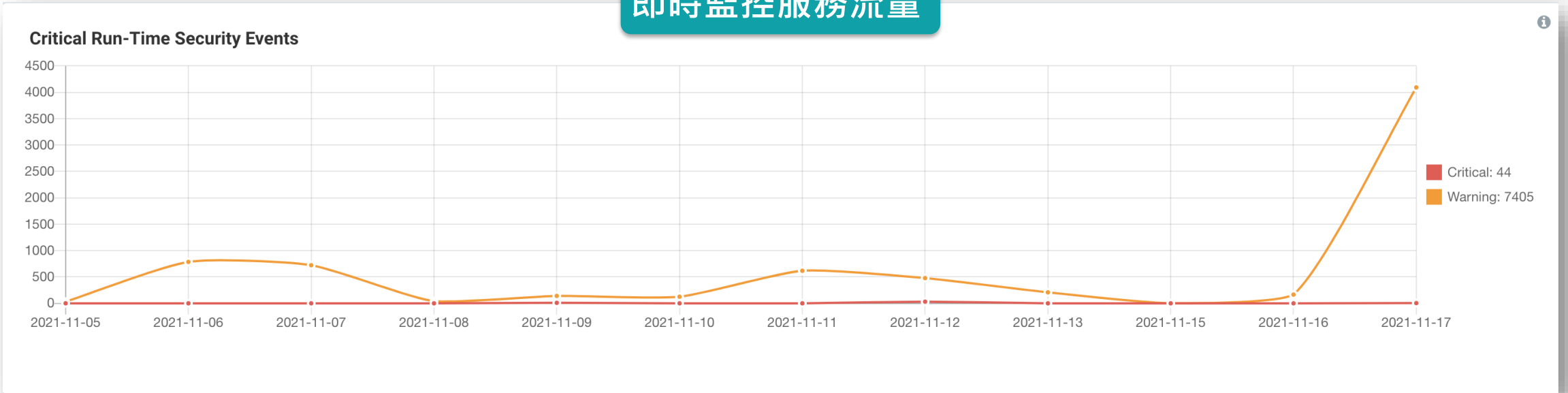
CVE DB Version: 2.493
(Nov 16, 2021)

How to Improve Your Score

Your overall security score is **FAIR**, please review the individual risk scores and follow the recommendations to reduce the overall risk.

[Improve your score](#)

即時監控服務流量



持續監控 – 即時監控L7網路流量



Network Activity

ACTIONS ▾

Add Group/NS

ALL ▾ ⚙ VIEW ▾ ↻ REFRESH

ingress → nginx-pod-6dfc668b5-shgrn

Application	Client IP	Server IP	Protocol...	Bytes	Rule	Ac...	Time
DLPall	HTTP	172.22.172.192	172.22.117.201	tcp/80	5.5 KB	10030 Allow	Sep 03, 2021 21:22:02

Session Count: 1

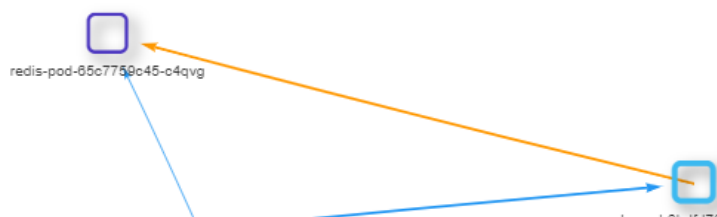
Packet Capture → nginx-pod-6dfc668b5-shgrn

Start Time	Status	File Size	Stop Time
Sep 03, 2021 21:21:00	stopped	3.2 KB	Sep 03, 2021 21:21:10

Set Capture duration

10 minutes

▶



- Alias
- Active Sessions
- Packet Capture
- Quarantine
- Expand
- Focus
- Collapse Namespace
- Collapse All Namespaces
- Collapse Group
- Collapse All Groups
- Discover
- Monitor
- Protect

SUMMARY

Name: node-pod-6bdfd769f5-hs589

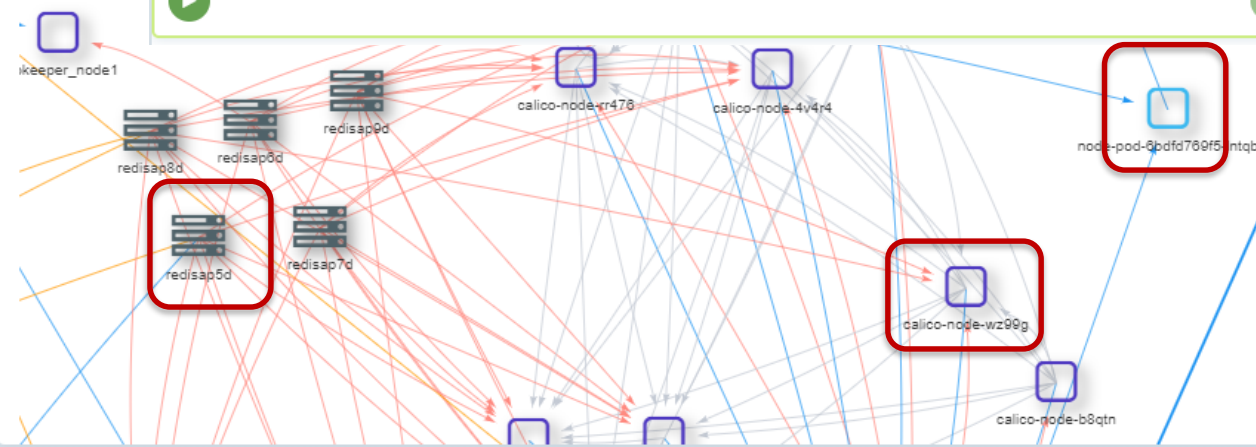
Namespace: demo

Service: node-pod.demo

State: discover

On Node: redisap5d

Vulnerabilities



各節點網路規則有無隱藏
安全性問題





事件記錄



nexus container by sonatype | POWERED BY NeuVector

admin admin

Events CSV REFRESH

298 events found Advanced Filter Filter...

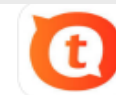
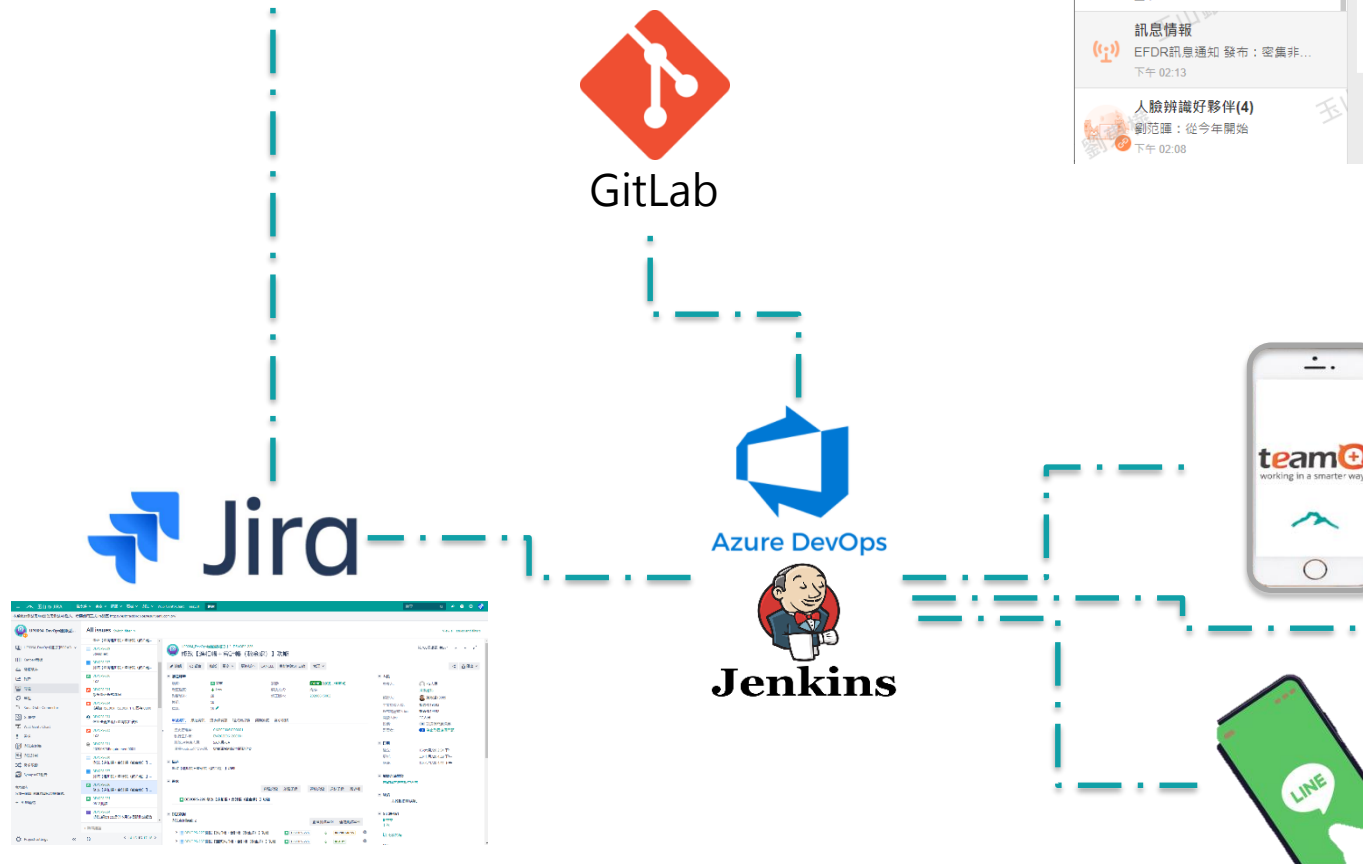
Name	Level	User	Location	Time
RESTful.Write	Info	User Name : admin User Roles : admin(Global)	Node : redisap2d	Sep 06, 2021 10:32:08
RESTful.Write	Info	User Name : admin User Roles : admin(Global)	Node : redisap2d	
RESTful.Write	Info	User Name : admin User Roles : admin(Global)	Node : redisap2d	Sep 06, 2021 10:26:36
<div style="border: 2px solid #008080; border-radius: 15px; padding: 10px;"> <p>Message Configure dlp group from 10.10.10.5</p> <p>REST Request: PATCH - https://neuvector-svc-controller.neuvector:10443/v1/dlp/group/demo</p> <p>REST Body: {"config":{"name":"demo","replace":[{"action":"deny","name":"all"}, {"action":"deny","name":"demo"}],"status":true}}</p> </div>				
User.Login	Info	User Name : admin User Roles : admin(Global)	Node : redisap2d	Sep 06, 2021 10:21:13
User.Login.Failed	Warning	User Name : admin	Node : redisap2d	Sep 06, 2021 10:21:10

© 2021 - Sonatype
Powered by NeuVector
Version - v4.2.2

查看事件、執行來源IP，確認事件描述，查找變更軌跡



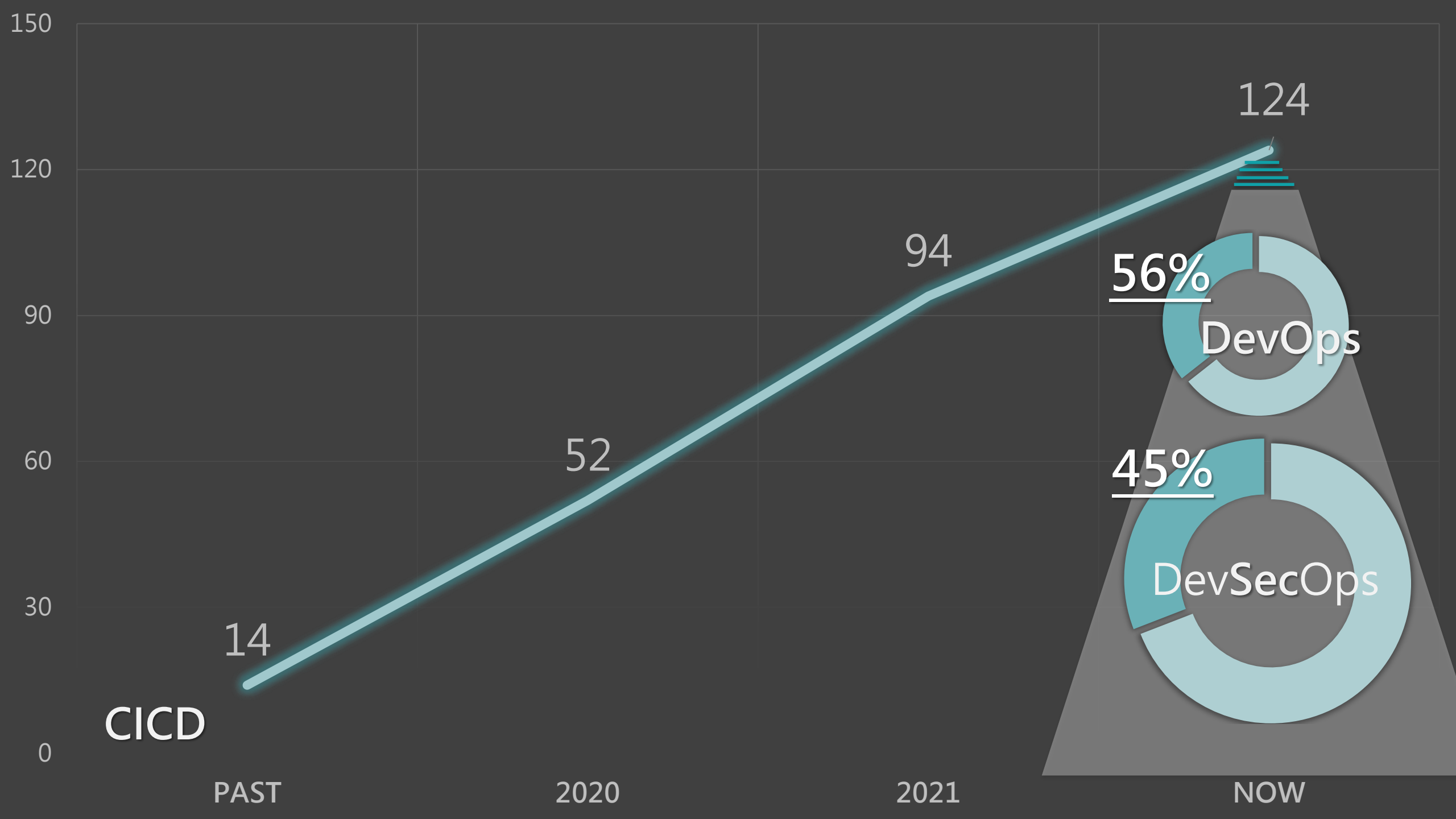
串接Team+ 進行通知



DevOps平台訊息通知
2021/02/09 16:42:10
...

行動銀行執行部署成功!





成熟度分析(1/2)



Level 1

- 局部嘗試導入DevOps，獲得初期成效

Level 2

- 較大範圍推行DevOps，使局部效率提升

Level 3

- 全面推行DevOps，貫穿軟體生命週期，並使整體效率提升

Level 4

- 全面落實DevOps，並能最佳化整體效率

Level 5

- 形成持續改進的文化，並不斷推展DevOps效益



成熟度分析(2/2)



軟體生命週期

- 提升測試的覆蓋率、執行效率，缺陷有效性

應用設計

- 制定更符合DevOps流程的架構設計準則

安全及風險管理

- 提升自動化監控的覆蓋範圍

組織結構

- 落實敏捷角色、塑造持續改善的文化，讓組織更加敏捷



感謝聆聽 敬請指教