**上海商業銀行股份有限公司**

**新核心系統INFRA**

**軟硬體設備建置專案服務**

**CI/CD 部署至OCP上版流程**

IBM Confidential

台灣國際商業機器股份­­­­有限公司

目錄

[一、前置作業 3](#_Toc178773041)

[1. OCP 帳號權限申請 3](#_Toc178773042)

[2. 申請Image上傳 3](#_Toc178773043)

[3. Jenkins 腳本開發 3](#_Toc178773044)

[二、 CI/CD上版流程 3](#_Toc178773045)

[1. DEV環境上版 3](#_Toc178773046)

[1.1 DEV本地開發 3](#_Toc178773047)

[1.2 DEV環境-推上DEV Branch 4](#_Toc178773048)

[1.3 DEV環境- Jenkins 部署 5](#_Toc178773049)

[1.4 DEV環境- 研發處測試人員驗測 5](#_Toc178773050)

[1.5 DEV環境- Merge Request 到 Main Branch 5](#_Toc178773051)

[2. DEV to STAGE 過版 6](#_Toc178773052)

[2.1 DEV to STAGE 審核申請 6](#_Toc178773053)

[2.2 DEV to STAGE -同步比對 6](#_Toc178773054)

[3. STAGE環境上版 6](#_Toc178773055)

[3.1 STAGE環境 Jenkins 上版 6](#_Toc178773056)

[3.2 STAGE環境 - Jenkins 上版部署程式選擇 7](#_Toc178773057)

[3.3 STAGE環境 - Jenkins 卡控點 7](#_Toc178773058)

[3.4 STAGE環境 – 驗收確認 8](#_Toc178773059)

[4. STAGE to PROD 過版 8](#_Toc178773060)

[4.1 STAGE to PROD– 審核申請 8](#_Toc178773061)

[5. PROD環境上版 8](#_Toc178773062)

[5.1 PROD環境 Jenkins 上版 8](#_Toc178773063)

[三、 CI/CD退版流程 9](#_Toc178773064)

[1. DEV 環境退版 9](#_Toc178773065)

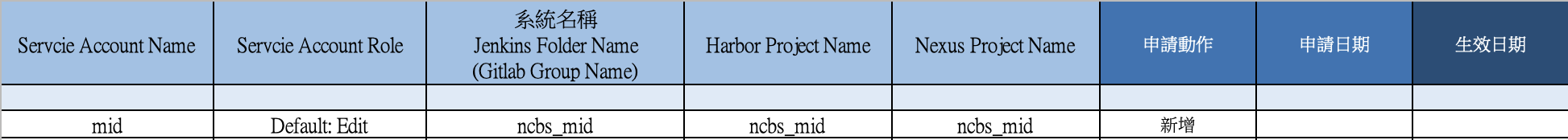
[2. STAGE 環境退版 9](#_Toc178773066)

[3. PROD 環境退版 9](#_Toc178773067)

一、前置作業

1. OCP 帳號權限申請

於AP 入住申請單中，填寫需申請之Service Account以及CI/CD系統Project Name。



1. 申請 OCP Service Account (CI/CD 部署到 OCP 的帳號)，， **由服務處設定Service Account**

* Service Account Naming Rule：同Namespace(Project) Name (EX: mid)
* 由OCP管理人員將Service Account設定於OCP中並綁定權限及Namespace / Project
  + - Service Account 綁定 OCP Role (預設使用 edit)
    - Service Account 綁定Namespace / Project

1. 取得 Service Account Token

* 申請 Service Account 後，由OCP管理人員於OCP中取得 Service account Token，將此 Token 交由 Jenkins 維運人員設定於Jenkins環境中。

1. 由OCP管理人員將表單中需申請之DNS 解析到 HA Proxy (Route)

一張含有 文字, 螢幕擷取畫面, 數字, 字型 的圖片

自動產生的描述

1. 申請Image上傳

一張含有 文字, 數字, 行, 字型 的圖片

自動產生的描述

1. 選擇Image類型，決定所上傳的Image類型，分為兩種：

* Base Image（僅能使用RHEL-UBI8:1.0.21，若有其他需求，請向服務處提出申請）。
* 官方整合Image（例如：Redis、Nginx）。
* 自定義 Image

1. 提供完整Image名稱
2. 確認 Image是否為官方資料來源。
3. 提供 Image來源
   * 官方整合Image：提供官方有效網址

* 自定義 Image：由AP自行上傳至 SFTP server (獨立VM or Nexus存放image？)，由服務處在SFTP server上將Image透過Trivy進行安全掃描 **需透過資安認可**

1. 指定Harbor專案名稱。
2. 設定Harbor專案目錄
   * 根據專案名稱及服務名稱來命名 Harbor 專案目錄（命名規則：<Project Name\_Service Name>，如表格中的 mid\_cbr-app）。
   * 由服務處負責從SFTP server將Image放置Harbor 專案目錄。
   * 由研發處Harbor 專案目錄中的Image進行安全掃描。
3. 提供驗證碼 (SHA1-256)：
   * Image上傳後，需提供Image的 SHA1-256 驗證碼，以確保完整性與一致性。
4. Jenkins 腳本開發

開發人員根據 AP系統需求參照文件 (上海商銀\_OCP CICD\_Jenkins 腳本範本) 進行腳本撰寫開發。

1. CI/CD上版流程
2. DEV環境上版
   1. DEV本地開發
3. 依照開發需求資訊建立系統異動單(Notes)。
4. 依照開發需求資訊建立Redmine單。

一張含有 文字, 字型, 行, 螢幕擷取畫面 的圖片

自動產生的描述

1. Clone Branch 進行開發 Git Clone URL

一張含有 文字, 電子產品, 螢幕擷取畫面, 軟體 的圖片

自動產生的描述

1. Git Checkout Prod Tag

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

1. Git create local Branch 進行開發：git checkout –b issue branch

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

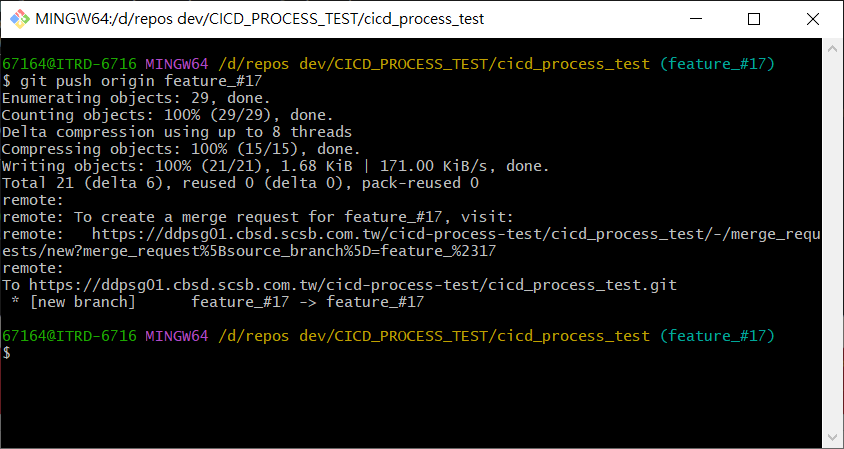
自動產生的描述

1. **Push local Branch To Remote**
   1. 提交 : git add . 和 git commit –m “Feature\_#17”

一張含有 文字, 螢幕擷取畫面, 軟體, 電腦 的圖片

自動產生的描述

* 1. Push 至遠端 Gitlab : git push origin feature\_#17



* 1. DEV環境-推上DEV Branch

開發主管 Code Review，確認是否合併

一張含有 文字, 螢幕擷取畫面, 軟體, 網頁 的圖片

自動產生的描述

* 1. DEV環境- Jenkins 部署
* 透過 Jenkins 建置新版應用程式，並使用oc apply部署到 DEV 環境的 OCP。
* 部署腳本請參照文件 (上海商銀\_OCP CICD\_Jenkins 腳本範本)。

一張含有 螢幕擷取畫面, 軟體, 文字, 電腦圖示 的圖片

自動產生的描述

* 透過 Jenkins 整合工具進行安全性掃描
  + Checkmarx： 自動化掃描 source code。
  + Dependency check：掃描AP中的第三方相依儲存庫，檢測是否存在已知的安全漏洞。例：當檢測到高風險（High Level）漏洞超過五個時，系統將會停止繼續進行。
  1. DEV環境- 研發處測試人員驗測
* 若測試有問題，與開發主管確認問題原因，需修改程式時，通知研發處開發人員修改。
  + 研發處開發人員直接使用(2.)建立的開發分支進行修改，不需要重新建立新的開發分支。
  + 研發處開發人員從(3.) 開始做到此步驟，請測試人員進行測試。
* 若測試沒問題，通知開發主管可以上版到STAGE。
  1. DEV環境- Merge Request 到 Main Branch

1. 確認測試沒問題，由開發主管發起 MR 到 main 分支。
2. 以 Main Branch建立 Tag。
3. 送申請單到 STAGE 審核

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

1. DEV to STAGE 過版
   1. DEV to STAGE 審核申請

* 資管科人員 確認 開發主管 傳來的申請單(Notes)
* 若無問題，資管科人員則手動進行 Compare list 動作
* 確認 DEV 與 STAGE 環境程式碼都無問題，資管科人員再手動操作 Jenkins 上版。
  1. DEV to STAGE -同步比對
* 同步 DEV 環境的 Gitlab 專案到 STAGE 環境
* 檢驗 Tag 是否存在
* 寄送比對結果 Email，給開發主管以及資管科人員。

1. STAGE環境上版
   1. STAGE環境 Jenkins 上版

由資管科人員手動啓用 Jenkins 流程

一張含有 螢幕擷取畫面, 文字, 軟體 的圖片

自動產生的描述

* 1. STAGE環境 - Jenkins 上版部署程式選擇

由資管科人員根據提單需求手動選擇 Jenkins 上版程式

一張含有 文字, 螢幕擷取畫面, 數字, 字型 的圖片

自動產生的描述

* 1. STAGE環境 - Jenkins 卡控點

資管人員確認部署Tag版本，點選 Proceed 進行部署。

一張含有 文字, 螢幕擷取畫面, 字型, 行 的圖片

自動產生的描述

* 1. STAGE環境 – 驗收確認

1. 資管人員收到主管覆核的系統異動申請單/需求問題處理單（Notes）單後，依據Tag資訊進行STAGE過版。
2. 手動執行Jenkins STAGE過版 job。
3. 過版完成後，資管人員登錄 Notes 單、紀錄過版job編號，進行簽核。
4. STAGE 一天至多上版一次，緊急修正hotfix除外。
5. STAGE to PROD 過版
   1. STAGE to PROD– 審核申請

資管科審核人員確認申請單後，手動啓用 Jenkins 進行上版。

1. PROD環境上版
   1. PROD環境 Jenkins 上版

一張含有 文字, 螢幕擷取畫面, 軟體 的圖片

自動產生的描述

1. CI/CD退版流程
2. DEV 環境退版

此環境僅作開發上版，不做退版動作。

1. STAGE 環境退版

* CICD流程會拉取舊版的 Yaml
* OCP 部署時，Yaml 會抓舊的 Image
* CICD流程應把 Yaml 檔推到 Nexus-prod

**操作流程**

* 1. 資管人員 向系統開發人員 確認退版的版號
  2. STAGE – Jenkins 資管人員操作上版
  3. 驗收人員檢查

一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述

1. PROD 環境退版

* PROD 上版是直接指定 UAT 包好的版本
  + 例如: v20240724-bbg
* 確定退版的話，退版時建議指定版本重新上版即可
* 先前討論是由資管科人員操作
* 部署 Yaml 都放在 Gitlab 做版控，Jenkins 會去 Nexus 拉取。

**操作流程**

1. 資管人員確認退版的版號
2. PROD - Jenksin 資管人員操作上版
3. 驗收人員檢查

一張含有 文字, 螢幕擷取畫面, 字型, 標誌 的圖片

自動產生的描述