**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**

**IBM Cloud Satellite OCP**

**AP 入住 OCP 申請流程**

IBM Confidential

台灣國際商業機器股份­­­­有限公司

目錄

[1. OCP專案填寫 AP 入住申請單(DEV/SIT) 3](#_Toc180409638)

[2. Email帳號資訊 3](#_Toc180409639)

[3. Project 資訊 3](#_Toc180409640)

[4. Service相關資訊及申請 4](#_Toc180409641)

[5. Firewall 對外防火牆資訊 4](#_Toc180409642)

[6. Network Policy 5](#_Toc180409643)

[7. Resource資源申請(Workload / Storage) 5](#_Toc180409644)

[8. 申請 Image 上傳 6](#_Toc180409645)

[9. Service Account申請 6](#_Toc180409646)

[~~10.~~ ~~SCC 資訊~~ 7](#_Toc180409647)

1. OCP專案填寫 AP 入住申請單(DEV/SIT)

根據AP需求填寫以下資訊

* Email 帳號申請資訊：由服務處(Cluster Admin)寄出OCP帳號申請
* Project 資訊 : 由服務處建立 Namespace(project)
* Service 資訊 : 如果有對外服務 (ingress) 申請 DNS Record 及 HTTPS 憑證，由服務處設定 route
* Firewall (對外) 資訊 : 由服務處設定 worker node 對外連線的 firewall policy
* Network Policy
* Resource(Workload /Storage)資訊 : 如果需要 pvc，由服務處設定 pv 並回填到入住申請資料 (參考和資訊服務處討論決議的PV管理辦法 p.10)
* 申請 Image 上傳資訊
* Service Account 申請資訊
* ~~SCC 資訊~~

1. Email帳號資訊

專案開發人員填寫需申請帳號之 Email，由服務處支援科發出邀請

一張含有 文字, 螢幕擷取畫面, 行, 字型 的圖片

自動產生的描述

收到註冊信件後，連線進入 <https://cloud.ibm.com/login>，註冊 IBM Cloud。

詳細申請步驟請參考文件 (上海商銀\_IBM Cloud Satellite\_DEV\_AP OCP帳號申請流程)

1. Project 資訊

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

AP填寫相關資訊，由服務處依照填寫內容進行 Project(Namespace) 建置

1. Gitlab Project Name
2. Namespace名稱
3. 預期部署的 node group 名稱
4. 專案負責人員 (OCP 裡的帳號)
5. Project Template 預設Allow Monitoring：允許 prometheus 所在 namespace 的流量進入
6. 確認是否提供相關 YAML
7. Service相關資訊及申請

依照AP Service 需求填寫相關資訊，若 Service Type 是 Ingress需申請 DNS Record 及 HTTPS 憑證，由服務處設定 Route。

1. DNS record
   * 此DNS record 將對應解析至 HA Proxy ( DEV環境為10.21.107.170 )
   * 命名規則為 <app-name>.<namespace>.ocp.cbs<d/s/p/y>.scsb.com.tw
   * AP 需依照此命名規則填寫，由**服務處支援科**進行申請
2. 憑證
   * 申請名稱需與DNS record名稱相同
   * AP 自行向**研發處**進行申請
3. 防火牆申請
   * DEV環境 OCP對外服務入口端IP為10.21.107.170，443 Port
   * **由服務處向網管進行申請**

一張含有 文字, 數字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

1. Firewall 對外防火牆資訊

填寫AP入住之後、中台對外連線所需防火牆清單，包含Cluster 外部的 firewall。

1. 外部服務的 DNS
2. 外部服務的 IP
3. 外部服務使用的 port number

以上firewall 相關配置需求服務處確認後，由**服務處向網管進行對外防火牆申請**，並確認外部連線服務端是否需額外申請。

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. Network Policy

預設僅允許同一 Namespace 內的通信，無法連接外部。如需對外連線，請填寫 OCP External Network Policy 申請單，申請通過後將由服務處進行設定。

* OCP Internal Network Policy：請填寫需申請特定namespace或應用（使用標籤識別的 Pod）進行東西向(對內)流量交換。
* OCP External Network Policy：請填寫需申請特定namespace或應用（使用標籤識別的 Pod）進行南北向(對外)流量連線。

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. Resource資源申請

依據AP專案需求，填寫所需Project 總資源(CPU/MEM)，以及各Pod數量、單一Workload資源、Workload總資源、Storage 資源。

1. AP填寫所需Namespace(Project)總資源，**由服務處進行 OCP 平台設定上限。**
2. AP填寫Workload各Pod所需資源。

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. Storage資源申請

依據AP專案需求，填寫所需Storage 相關需求，**由服務處配置相關的 PV / PVC**

* + PV/PVC 名稱Default為Workload Name-PV
  + Permission：根據需求選擇對Storage的權限，選擇ROX / RWO / RWX。

一張含有 文字, 數字, 字型, 行 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：

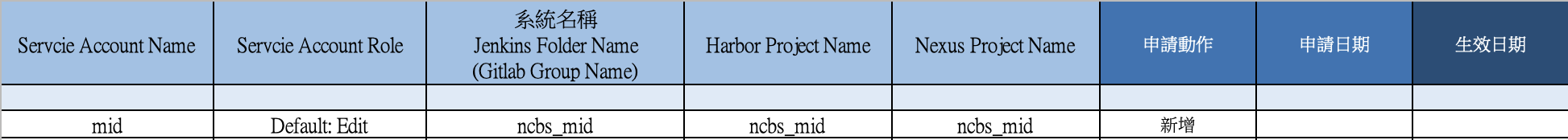
* Base Image（僅能使用RHEL-UBI8:1.0.21，若有其他需求，請向服務處提出申請）。
* 官方整合Image（例如：Redis、Nginx）。
* 自定義 Image

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。
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. Service Account申請

填寫專案的 Service Account Name以及相關系統與專案名稱，確保與現有的 Jenkins、Gitlab、Harbor 和 Nexus 配置一致。



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 Name：同Namespace(Project) Name (EX: mid)
* Service Account 綁定 OCP Role， OCP Role 只能存取自己專案的資源
* OCP Role 預設使用 edit
* Service Account 綁定專案，綁定 Namespace / Project

1. 取得 Service Account Token：申請 Service Account 後，由服務處於OCP中取得 Service Account Token，將此 Token 交由 Jenkins 維運人員設定於Jenkins環境中。
   * DEV Jenkins 維運人員為研發處，STAGE / PROD 為服務處
2. 由服務處將表單中需申請之DNS解析到 HA Proxy (Route)
3. ~~SCC 資訊~~

~~OCP 透過 SCC (SecurityContextConstraints) 機制，來控管 container 可以取得的權限。一般使用者(Normal User)預設套用的 scc 規則為 restricted如下。~~

* ~~不允許設定為特權 (privilege)~~
* ~~不允許設定使用 hostNetwork~~
* ~~只允許少數幾個系統呼叫 (依 OCP 版本而定)~~
* ~~執行程式的 uid 必須符合所在 namespace 限定的範圍內~~
* ~~不允許使用 hostPath~~

~~若AP 需要特殊權限的 SCC 配置，請於~~**~~專案備註欄~~**~~註明所需權限與原因，若需要自訂的 SCC policy，由服務處協助審核與部署。~~

1. ~~SCC 需求（SCC YAML 欄位）：~~

~~• 若填寫為 “N”，表明這些應用尚未有特定的 SCC 定義。需要確定是否所有的應用服務都需要額外的 SCC，或者可以依賴默認的 SCC。~~

~~• 您可以將需要特定權限的應用標示為 “Y”，並根據需求設計對應的 SCC YAML 檔案。~~

1. ~~設置 SCC 名稱（SCC Name 欄位）：~~

~~• 為需要 SCC 的應用指定 SCC 名稱 (SCC Name)。例如，某些應用可能需要使用 privileged 或自定義的 SCC，以滿足特定的運行需求。~~

~~• 如果應用不需要額外的 SCC，可以保持該欄位為空。~~

1. ~~權限類型及原因：若有特定需求下可以申請以下 scc 權限，並說明原因~~

* ~~anyuid : 不限制執行程式的 uid 範圍~~
* ~~hostaccess : 允許使用 hostPath~~
* ~~hostnetwork : 允許使用 hostNetwork~~