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

版本：v2.8 修訂日期：2024/12/18

目錄

1. 前言

- 任何 OCP 專案皆需填寫此 AP 入住申請單，請根據開發需求填寫以下資訊，行方將會根據資訊進行相對應配置與設定。
- 若有其他需配合開發之元件(EX: Redis)，請按照需求填寫 Storage、Image 等需求表單。
- 若有備註事項請填寫於「Project」分頁中的專案備註欄位。
- 提交此入住申請表時請一併附上專案 HTTPS 憑證檔案。

2. Project 資訊

專案基本資訊		
項目名稱	項目說明	填寫欄位
Environment	環境別 (下拉選單)	DEV/SIT
Project Name	Gitlab Project 名稱	ncbs-mid-repo2
Namespace Name		mid
Node Group		mid
Project Admin	專案負責人員	Steven
Project Template	預設為Allow Monitoring	Allow Monitoring

系統提供之 Service Monitor 需求		
項目名稱	項目說明	填寫欄位
使用系統 Service Monitor YAML	Y/N (下拉選單)	Y
使用系統 Dashboards JSON	Y/N (下拉選單)	Y
提供 Alertmanager Rules YAML	Y/N (下拉選單)	N
提供 HPA YAML	Y/N (下拉選單)	N

SCC 是否需申請特權？
若需申請，請說明，若不申請請寫N
N

專案備註
專案特殊要求或備註

請開發人員填寫專案相關資訊，由服務處依照填寫內容進行 Project(Namespace) 建置

1. 環境選擇（DEV/SIT、STAGE、PROD）
2. Gitlab Project Name
3. Namespace 名稱
4. 預期部署的 node group 名稱
5. 專案負責人員 (OCP 裡的帳號)
6. Project Template 預設 Allow Monitoring：允許 prometheus 所在 namespace 的流量進入
7. 確認是否提供相關 YAML
8. 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。
    1. 不允許設定為特權 (privilege)
    2. 不允許設定使用 hostNetwork
    3. 只允許少數幾個系統呼叫 (依 OCP 版本而定)
    4. 執行程式的 uid 必須符合所在 Namespace 限定的範圍內
    5. 不允許使用 hostPath

    若開發人員需要特殊權限的 SCC 配置，需申請並說明權限與原因。

3. Email 帳號資訊

Name	Email	OCP Role Name	申請動作	申請人員	申請日期	執行人員	生效日期
申請人名稱	申請人Email	Admin / Edit / View	新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11	e.g. 芙霧楚	e.g. 2024/11/11
User	user@scsb.com.tw	admin	新增	User	2024/12/18		

1. 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
   - **Stage 及 Prod 環境之 Email 僅能使用上海商銀行內之郵件地址進行申請。**
2. 收到註冊信件後，連線進入 https://cloud.ibm.com/login，註冊 IBM Cloud。
3. 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)

4. Service 相關資訊及申請

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

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。
   - 開發廠商自行向**研發處**進行申請
   - **請開發廠商將憑證檔案附件於此入住申請單交由服務處配置 Route yaml。**
3. OCP 入口端點
   - DEV 環境 OCP 對外服務入口端 IP 為 10.21.107.170，443 Port。
   - 若有需連線進入至 OCP 之外部服務，由使用單位自行根據 DNS 資訊進行申請進入 OCP。

Workload Name	Workload Type	Service 資訊			研發處執行項目	服務處執行項目	申請動作	申請人員	申請日期
		Service Name	Service Type	Service Port	申請 HTTPS 憑證(Y/N)	DNS Record to HA Proxy			
e.g. eg-svc-app	下拉選單	e.g. svc-app	e.g. Ingress	e.g. 443	請研發處進行申請 並附上檔案於申請單	<app-name>.<namespace>. apps.cbs<d/s/p/y>.scsb.com.tw	新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11
mid-cbr-app	Deployment	mid-cbr-app	Ingress	8080	Y	mid-cbr-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-cmn-app	Deployment	mid-cmn-app	Ingress	8080	Y	mid-cmn-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-dep-app	Deployment	mid-dep-app	Ingress	8080	Y	mid-dep-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-gla-app	Deployment	mid-gla-app	Ingress	8080	Y	mid-gla-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-len-app	Deployment	mid-len-app	Ingress	8080	Y	mid-len-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-rem-app	Deployment	mid-rem-app	Ingress	8080	Y	mid-rem-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-remb-app	Deployment	mid-remb-app	Ingress	8080	Y	mid-remb-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-reml-app	Deployment	mid-reml-app	Ingress	8080	Y	mid-reml-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-remm-app	Deployment	mid-remm-app	Ingress	8080	Y	mid-remm-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-rems-app	Deployment	mid-rems-app	Ingress	8080	Y	mid-rems-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28
mid-xau-app	Deployment	mid-xau-app	Ingress	8080	Y	mid-xau-app.mid.apps.cbsd.scsb.com.tw	新增	鄭景文	2024/11/28

5. Firewall 對外防火牆資訊

請開發廠商填寫對外服務連線所需之防火牆清單，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

以上防火牆相關配置需求服務處確認後，由**服務處向網管進行從對外防火牆申請（Worker node 連外）**，並確認外部連線服務端是否需額外申請。

對外連線目標 (Firewall)				申請動作	申請人員	申請日期	執行人員	生效日期
對外服務名稱	DNS	IP	Port	新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11	e.g. 芙霧楚	e.g. 2024/11/11
Oracle DB	SDBSO01.cbsd.scsb.com.tw	10.21.110.110	1521	新增	鄭景文	2024/11/28	李家毓	2024/12/6

6. 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，請開發廠商填寫 OCP External Network Policy 申請單，申請通過後將由服務處進行 Route yaml 配置。

- 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。

Type	Source		Destination		申請動作	申請人員	申請日期	執行人員	生效日期
External	Namespace Name	Label Name	Namespace Name / IP	Label Name / Port	新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11	e.g. 芙霧楚	e.g. 2024/11/11
Internal	mid		mid		新增	鄭景文	2024/11/28	李家毓	預設
External	mid		10.21.110.110	1521	新增	鄭景文	2024/11/28	李家毓	2024/12/6

7. Resource 資源申請

依據專案開發需求，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. 專案所需 Namespace(Project)總資源，**由服務處進行 OCP 平台設定上限。**
2. 請填寫 Workload 各 Pod 所需資源，**由研發處寫入 Deployment yaml**。

Workload Name	Pod 數量	單一 Workload 資源				總和 Workload 資源				於申請單填寫時填寫			設定Deployment yaml後填寫	
		Request		Limit		Request		Limit		申請動作	申請人員	申請日期	執行人員	生效日期
e.g. eg-svc-app	e.g. 1	CPU (m)	Memory (mb)	CPU (m)	Memory (mb)	CPU (m)	Memory (mb)	CPU (m)	Memory (mb)	新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11	e.g. 嚴發儲	e.g. 2024/11/11
mid-cbr-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-cmn-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-dep-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-gla-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-len-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-rem-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-remb-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-reml-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-remm-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-rems-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		
mid-xau-app	2	2000	4000	4000	8000	4000	8000	8000	16000	新增	鄭景文	2024/11/28		

8. Storage 資源申請

依據專案開發需求，請開發廠商填寫所需 Storage 相關需求，**由服務處配置 OCP 相關的 PV / PVC 設定。**

- PV/PVC 命名規則為 Workload Name-pv or Workload Name-pvc
- Permission：根據需求選擇對 Storage 的權限，選擇 ReadOnlyMany（ROX） / ReadWriteOnce（RWO） / ReadWriteMany（RWX）。
- 請開發廠商填寫 PVC 掛載路徑。

Workload Name	Storage					申請動作	申請人員	申請日期	執行人員	生效日期
	G	PV	PVC	Permission	Path					
e.g. eg-svc-app	e.g. 10G	Workload Name-pv	Workload Name-pvc	ROX / RWO / RWX	PVC 掛載路徑	新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11	e.g. 芙霧楚	e.g. 2024/11/11

9. 申請 Image 上傳

依據專案開發需求，請開發廠商依照下列說明填寫需上傳使用之 Image 資訊。

Image Information						Harbor		
Image Type	Base Image Source	是否包含 JDK？	Full Image Name	是否為官方資料？	Image 上傳來源	Harbor Project Name	Harbor Project DIR	驗證碼
下拉選擇	請預設使用 RHEL-UBI8	Base Image 如包含請填寫JDK版本	提供完整 Image名稱	下拉選擇	URL / sftp server		<Project Name_ Service Name>	e.g. SHA1-256

1. 選擇 Image 類型，決定所上傳的 Image 類型，分為兩種：
   - Base Image（預設使用 RHEL-UBI8 最新版本，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
2. 確認 Base Image 是否需包含 JDK
   - 請在此欄位填寫所需 JDK 版本，例如 JDK 11 或 JDK 17。
   - 若無包含請填寫「否」
3. 提供完整 Image 名稱
4. 確認 Image 是否為官方資料來源
5. 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，由服務處在 SFTP server 上，將 Image 透過 Trivy 進行安全掃描
6. 指定 Harbor 專案名稱
7. 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。

8. 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。

10. Service Account 申請

請開發廠商填寫需申請之 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。

Servcie Account Name	CICD 系統			申請動作	申請人員	申請日期
	系統名稱 Jenkins Folder Name (Gitlab Group Name)	Harbor Project Name	Nexus Project Name			
預設權限為 Edit	填寫已申請 CICD 之名稱			新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11
mid	ncbs_mid (MID)	mid		新增	鄭景文	2024/11/28

1. 填寫需申請 OCP Service Account，由服務處協助設定 Service Account，具體流程如下：
    1. Service Account 名稱：與對應的 Namespace (Project) 名稱相同，例如：mid。
    2. Service Account 綁定：
        1. 綁定至指定的 Namespace / Project。
        2. 指定 OCP Role，僅允許存取該專案的資源。
        3. 預設 OCP Role 為 edit。
    3. 申請完成後，由服務處在 OCP 平台中生成該 Service Account 的 Token，並將該 Token 提供給 Jenkins 維運人員設定至 Jenkins 環境中。
2. 填寫相關專案名稱（包括 Jenkins、Harbor、Nexus 等），以便進行統一管理與存檔。

11. OCP Yaml 配置

請開發廠商填寫 AP Service 在 Yaml 檔中的變化參數， 由研發處撰寫 Deployment / ImageStream / ServiceMonitor / service yaml 並進行 OCP 設定部署。

Service yaml	Deployment yaml			ImageStream yaml	ServiceMonitor yaml	申請動作	申請人員	申請日期
Service Name	Image name	readinessProbe.path	livenessProbe.path	DockerImage Name	endpoints path			
EX: mid-cmn-app	mid-cmn-app:1.0.0	/api/cmn/actuator/health/readiness	/api/cmn/actuator/health/liveness	/namespace-name/cmn-app:latest	/api/cmn/actuator/prometheus	新增/刪除	e.g. 嚴發儲	e.g. 2024/11/11

1. Deployment yaml：
    - Image name
    - readinessProbe.path
    - livenessProbe.path
2. ImageStream yaml：
    - DockerImage Name
3. Service yaml：
    - Service Name
4. ServiceMonitor yaml：
    - endpoints path

Route yaml 及 PVC/PV yaml 將由服務處按照 network policy 及 storage 分頁進行 yaml 配置。

12.提交申請

請開發廠商填寫完畢後提交申請單給以下單位

1. 南區研發二處
2. 資訊服務處開放支援科 李家毓 E-MAIL: kurolii@scsb.com.tw

以上流程若有問題請聯繫：資訊服務處開放支援科 李家毓 TEL:(02)6600-8111 ex 6209 / E-MAIL: kurolii@scsb.com.tw