**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**

**CICD系統憑證替換文件**

IBM Confidential

台灣國際商業機器股份­­­­有限公司

目錄

[1 Nexus 替換 https 憑證 3](#_Toc182228746)

[2. Harbor 替換 https 憑證 6](#_Toc182228747)

[3. Jenkins 替換 https 憑證 8](#_Toc182228748)

[4. Gitlab 替換 https 憑證 11](#_Toc182228749)

[5. Redmine 替換 https 憑證 13](#_Toc182228750)

1. [Nexus 替換 https 憑證](#_Nexus_替換_https)
2. Nexus 架構
   * + 瀏覽器 → (Nginx → Nexus)，所以https 憑證是放置在 Nginx 上
3. 認識環境
   * + Nginx 設定檔: /etc/nginx/conf.d/nexus.conf
     + SSL 憑證的路徑: /etc/nexus/ssl/
4. # the server directive is Nginx's virtual host directive
5. server {
6. listen 80;
7. server\_name nexus.brobridge.lab;
8. # redirect http to https www
9. return 301 https://nexus.brobridge.lab$request\_uri;
10. }
11. server {
12. listen 443 ssl;
13. server\_name nexus.brobridge.lab;
14. access\_log /var/log/nginx/nexus.access.log;
15. error\_log /var/log/nginx/nexus.error.log;
16. ssl\_protocols TLSv1.2;
17. ssl\_certificate /etc/nexus/ssl/brobridge.lab.crt;
18. ssl\_certificate\_key /etc/nexus/ssl/brobridge.lab.key;
19. client\_max\_body\_size 128M;
20. location / {
21. proxy\_pass http://127.0.0.1:8081;
22. proxy\_redirect off;
23. proxy\_set\_header Host $host;
24. proxy\_set\_header X-Forwarded-For $remote\_addr;
25. proxy\_set\_header X-Forwarded-Proto https;
26. }
27. }
28. 建立私服器憑證
    * 1. 建立私有鑰匙
         + 私服器金鑰建立時，不要使用密碼。
         + 依據資安要求給於長度即可，先前詢問涵宇是使用 4096。
29. openssl genrsa -out nexus.brobridge.lab.key 4096
    * 1. 建立 CSR
         + 主體(subject)部分依照行方資訊填寫即可。
30. openssl req -sha512 -new \
31. -subj "/C=TW/ST=Taipei/L=Taipei/O=Brobridge/OU=Personal/CN=nexus.brobridge.lab" \
32. -key nexus.brobridge.lab.key \
33. -out nexus.brobridge.lab.csr
    * 1. 準備 v3 格式的設定檔
         + 主要修改 alt\_names，代入私服器 DNS 即可。
34. cat > v3.ext <<-EOF
35. authorityKeyIdentifier=keyid,issuer
36. basicConstraints=CA:FALSE
37. keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
38. extendedKeyUsage = serverAuth
39. subjectAltName = @alt\_names
40. [alt\_names]
41. DNS.1=nexus.brobridge.lab
42. EOF
    * 1. 建立私服器憑證
         + 根據資安要求，修改指定加密格式跟天數即可。
43. openssl x509 -req -sha512 -days 3650 \
44. -CA nexus\_brobridge\_lab\_rootCA.crt -CAkey nexus\_brobridge\_lab\_rootCA.key -CAcreateserial \
45. -in nexus.brobridge.lab.csr \
46. -out nexus.brobridge.lab.crt \
47. -extfile v3.ext
48. 確認私服器憑證包含 SAN

* 檢查憑證內部資訊

1. openssl x509 -in nexus\_brobridge\_lab\_rootCA.crt -noout -text | grep -A 1 "Subject Alternative Name"

* 指定憑證瀏覽(domain 換掉)

1. curl -v https://nexus.brobridge.lab/service/rest/v1/status --cacert ca.crt
2. 憑證配置
   * 將 Server 憑證放在目錄下
3. [root@nexus ssl]# ll /etc/nexus/ssl
4. total 20
5. -rw-------. 1 root root 4588 Apr 10 2023 brobridge.lab.crt
6. -rw-------. 1 root root 1704 Apr 10 2023 brobridge.lab.key
   * 替換新的憑證後，重啓 Nginx:
7. systemctl reload nginx
8. Jenkins 機器測試

以下操作適用 RedHat 系統

* + 將憑證放上 Client 主機; 也可以將內容內容過去。

1. ## 放在這個目錄下，名稱與系統相符即可。
2. cd /etc/pki/ca-trust/source/anchors/
   * 更新憑證信任
3. sudo update-ca-trust

* 用 curl 測試

1. curl -v https://nexus.brobridge.lab/service/rest/v1/status/
2. Trubleshoot

* 確認系統上是否有該憑證

1. trust list | grep nexus

* 指定憑證

1. curl -v https://nexus.brobridge.lab/service/rest/v1/status/ --cacert nexus\_brobridge\_lab\_rootCA.crt

* 忽略憑證

1. curl -v https://nexus.brobridge.lab/service/rest/v1/status/ --insecure
2. 確認私服器憑證包含 SAN（沒有包含也可過）
3. openssl x509 -in nexus\_brobridge\_lab\_rootCA.crt -noout -text | grep -A 1 "Subject Alternative Name"

1. [Harbor 替換 https 憑證](#_Harbor_替換_https_2)
2. 認識環境

* Harbor config位置: /root/kyle/harbor
* Harbor 憑證位置: /root/kyle/harbor/cert
* 設定 harbor.yml 憑證:

1. ... 以上省略 ...
2. https:
3. port: 443
4. certificate: /root/kyle/harbor/cert/harbor.brobridge.lab.crt
5. private\_key: /root/kyle/harbor/cert/harbor.brobridge.lab.key
6. ... 以下省略 ...
7. 建立私服器憑證

* 建立私有鑰匙

1. openssl genrsa -out harbor.brobridge.lab.key 4096

* 建立 CSR

1. openssl req -sha512 -new \
2. -subj "/C=TW/ST=Taipei/L=Taipei/O=Brobridge/OU=Personal/CN=harbor.brobridge.lab" \
3. -key harbor.brobridge.lab.key \
4. -out harbor.brobridge.lab.csr

* 準備 v3 格式的設定檔

1. cat > v3.ext <<-EOF
2. authorityKeyIdentifier=keyid,issuer
3. basicConstraints=CA:FALSE
4. keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
5. extendedKeyUsage = serverAuth
6. subjectAltName = @alt\_names
7. [alt\_names]
8. DNS.1=harbor.brobridge.lab
9. EOF

* 建立私服器憑證

1. openssl x509 -req -sha512 -days 3650 \
2. -CA harbor.brobridge.lab.crt -CAkey ca.key -CAcreateserial \
3. -in harbor.brobridge.lab.csr \
4. -out harbor.brobridge.lab.crt \
5. -extfile v3.ext
6. Harbor 重新載入憑證
7. cd /data/harbor/
8. docker compose down -v
9. ./prepare --with-trivy
10. docker compose up -d
11. Jenkins 機器測試

以下操作適用 RedHat 系統

* 將憑證放上 Client 主機; 也可以將內容內容過去。

1. ## 放在這個目錄下，名稱與系統相符即可。
2. cd /etc/pki/ca-trust/source/anchors/

* 更新憑證信任

1. sudo update-ca-trust

* 用 curl 測試

1. curl -v https://harbor.brobridge.lab/v2/
2. Trubleshoot

* 指定憑證

1. curl -v https://harbor.brobridge.lab/v2/ --cacert harbor.brobridge.lab.crt

* 確認系統上包含該憑證

1. trust list | grep harbor

* 忽略憑證

1. curl -v https://harbor.brobridge.lab/v2/ --insecure
2. 確認私服器憑證包含 SAN（沒有包含也可過）
3. openssl x509 -in harbor.brobridge.lab.crt -noout -text | grep -A 1 "Subject Alternative Name"

1. [Jenkins 替換 https 憑證](#_Jenkins_替換_https_2)

Jenkins 憑證是在啓動時帶入的，所以要在 systemd 服務調整。

1. 建立私服器憑證

* 建立私有鑰匙

1. openssl genrsa -out jenkins.brobridge.lab.key 4096

* 建立 CSR

1. openssl req -sha512 -new \
2. -subj "/C=TW/ST=Taipei/L=Taipei/O=Brobridge/OU=Personal/CN=jenkins.brobridge.lab" \
3. -key jenkins.brobridge.lab.key \
4. -out jenkins.brobridge.lab.csr

* 準備 v3 格式的設定檔

1. cat > v3.ext <<-EOF
2. authorityKeyIdentifier=keyid,issuer
3. basicConstraints=CA:FALSE
4. keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
5. extendedKeyUsage = serverAuth
6. subjectAltName = @alt\_names
7. [alt\_names]
8. DNS.1=jenkins.brobridge.lab
9. EOF

* 建立私服器憑證

1. openssl x509 -req -sha512 -days 3650 \
2. -CA ca.crt -CAkey ca.key -CAcreateserial \
3. -in jenkins.brobridge.lab.csr \
4. -out jenkins.brobridge.lab.crt \
5. -extfile v3.ext

* 將 SSL 憑證轉換成中間過度的 PKCS12 格式的憑證:

1. openssl pkcs12 -export -out jenkins.brobridge.lab.p12 -passout 'pass:brobridge' -inkey jenkins.brobridge.lab.key -in jenkins.brobridge.lab.crt -certfile ca.crt -name jenkins.brobridge.lab

* 將 PKCS12 格式的憑證轉換爲 JKS 格式的憑證:

1. keytool -importkeystore -srckeystore jenkins.brobridge.lab.p12 -srcstorepass 'brobridge' -srcstoretype PKCS12 -srcalias jenkins.brobridge.lab -deststoretype JKS -destkeystore jenkins.brobridge.lab.jks -deststorepass 'brobridge' -destalias jenkins.brobridge.lab
2. 配置私服器憑證

* 透過 systemctl 調整 Jenkins 服務:

1. systemctl edit jenkins.service

* 內容如下:

1. [Service]
2. #WorkingDirectory="/data/jenkins"
3. Environment="JENKINS\_HOME=/data/jenkins"
4. Environment="JENKINS\_PORT=80"
5. Environment="JENKINS\_HTTPS\_PORT=443"
6. Environment="JENKINS\_HTTPS\_LISTEN\_ADDRESS=0.0.0.0"
7. Environment="JENKINS\_HTTPS\_KEYSTORE=/etc/jenkins/ssl/jenkins.brobridge.lab.jks"
8. Environment="JENKINS\_HTTPS\_KEYSTORE\_PASSWORD=brobridge"
9. Environment="JAVA\_OPTS=-Djava.awt.headless=true -Djdk.tls.ephemeralDHKeySize=2048 -Dhudson.model.DirectoryBrowserSupport.CSP=\"default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' 'unsafe-inline' data:;\""
10. AmbientCapabilities=CAP\_NET\_BIND\_SERVICE

* 將 JKS 憑證放到 Jenkins 環境變數位置上:

1. mkdir -p /etc/jenkins/ssl
2. cp jenkins.brobridge.lab.jks /etc/jenkins/ssl
3. chown -R jenkins: /etc/Jenkins
4. chmod 600 /etc/jenkins/ssl/jenkins.brobridge.lab.jks
5. 重啓 Jenkins

重新載入設定，並重啓 Jenkins:

1. systemctl daemon-reload
2. systemctl restart jenkins.service
3. 找他台機器測試

以下操作適用 RedHat 系統

* 憑證生效可能需要一段時間
* 將憑證放上 Client 主機; 也可以將內容內容過去。

1. ## 放在這個目錄下，名稱與系統相符即可。
2. cd /etc/pki/ca-trust/source/anchors/

* 更新憑證信任

1. sudo update-ca-trust

* 用 curl 測試（回傳403爲正常）

1. curl -v https://jenkins.brobridge.lab/api/json/
2. Trubleshoot

* 確認系統上是否有該憑證

1. trust list | grep jenkins

* 指定憑證

1. curl -v https://jenkins.brobridge.lab/api/json/ --cacert jenkins.brobridge.CA.crt

* 忽略憑證

1. curl -v https://jenkins.brobridge.lab/api/json/ --insecure
2. 確認私服器憑證包含 SAN（沒有包含也可過）
3. openssl x509 -in jenkins.brobridge.CA.crt -noout -text | grep -A 1 "Subject Alternative Name"

1. [Gitlab 替換 https 憑證](#_Gitlab_替換_https_1)

Gitlab 是透過 RPM 所安裝，設定檔目錄: /etc/gitlab

1. 建立私服器憑證

* 建立私有鑰匙

1. openssl genrsa -out harbor.brobridge.lab.key 4096

* 建立 CSR

1. openssl req -sha512 -new \
2. -subj "/C=TW/ST=Taipei/L=Taipei/O=Brobridge/OU=Personal/CN=harbor.brobridge.lab" \
3. -key harbor.brobridge.lab.key \
4. -out harbor.brobridge.lab.csr

* 準備 v3 格式的設定檔

1. cat > v3.ext <<-EOF
2. authorityKeyIdentifier=keyid,issuer
3. basicConstraints=CA:FALSE
4. keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
5. extendedKeyUsage = serverAuth
6. subjectAltName = @alt\_names
7. [alt\_names]
8. DNS.1=harbor.brobridge.lab
9. EOF

* 建立私服器憑證

1. openssl x509 -req -sha512 -days 3650 \
2. -CA ca.crt -CAkey ca.key -CAcreateserial \
3. -in harbor.brobridge.lab.csr \
4. -out harbor.brobridge.lab.crt \
5. -extfile v3.ext
6. 配置 Gitlab 憑證

將 gitlab.example.com.key gitlab.example.com.crt 放在 /etc/gitlab/ssl 中:

1. # ll /etc/gitlab/ssl
2. total 32
3. -rw-------. 1 bb bb 4588 Jul 19 2022 brobridge.lab.crt
4. -rw-------. 1 bb bb 1704 Jul 19 2022 brobridge.lab.key
5. 重啓 Gitlab
6. gitlab-ctl restart
7. Jenkins 機器測試

以下操作適用 RedHat 系統

* 將憑證放上 Client 主機; 也可以將內容內容過去。

1. ## 放在這個目錄下，名稱與系統相符即可。
2. cd /etc/pki/ca-trust/source/anchors/

* 更新憑證信任

1. sudo update-ca-trust

* 用 curl 測試(出現 not found 是正常的)，如果要開啓健康檢查功能的話，參考官網文件: <https://docs.gitlab.com/ee/administration/monitoring/health_check.html>

1. curl -v https://gitlab.brobridge.lab/-/liveness
2. Trubleshoot

* 指定憑證

1. curl -v https://gitlab.brobridge.lab/-/liveness --cacert gitlab.brobridge.lab.crt

* 確認系統上包含該憑證

1. trust list | grep gitlab

* 忽略憑證

1. curl -v https://gitlab.brobridge.lab/-/liveness --insecure
2. 確認私服器憑證包含 SAN（沒有包含也可過）
3. openssl x509 -in gitlab.brobridge.lab.crt -noout -text | grep -A 1 "Subject Alternative Name"

1. [Redmine 替換 https 憑證](#_Redmine_替換_https_2)
2. Redmine 架構

瀏覽器 → (Nginx → Redmine)，所以 https 憑證是放置在 Nginx 上

1. 認識環境

* Nginx 設定檔: /etc/nginx/conf.d/redmine.conf
* SSL 憑證的路徑: /etc/redmine/ssl/

1. # the server directive is Nginx's virtual host directive
2. server {
3. listen 80;
4. server\_name redmine.brobridge.lab;
5. # redirect http to https www
6. return 301 https://redmine.brobridge.lab$request\_uri;
7. }
8. server {
9. listen 443 ssl;
10. server\_name redmine.brobridge.lab;
11. access\_log /var/log/nginx/redmine.access.log;
12. error\_log /var/log/nginx/redmine.error.log;
13. ssl\_certificate /etc/redmine/ssl/brobridge.lab.crt;
14. ssl\_certificate\_key /etc/redmine/ssl/brobridge.lab.key;
15. location / {
16. proxy\_pass http://127.0.0.1:3000;
17. proxy\_redirect off;
18. proxy\_set\_header Host $host;
19. proxy\_set\_header X-Forwarded-For $remote\_addr;
20. proxy\_set\_header X-Forwarded-Proto https;
21. }
22. }
23. 建立私服器憑證

建立私有鑰匙

* 私服器金鑰建立時，不要使用密碼。
* 依據資安要求給於長度即可，先前詢問涵宇是使用 4096。

1. openssl genrsa -out redmine.brobridge.lab.key 4096

建立 CSR

* 主體(subject)部分依照行方資訊填寫即可。

1. openssl req -sha512 -new \
2. -subj "/C=TW/ST=Taipei/L=Taipei/O=Brobridge/OU=Personal/CN=redmine.brobridge.lab" \
3. -key redmine.brobridge.lab.key \
4. -out redmine.brobridge.lab.csr

準備 v3 格式的設定檔

* 主要修改 alt\_names，代入私服器 DNS 即可。

1. cat > v3.ext <<-EOF
2. authorityKeyIdentifier=keyid,issuer
3. basicConstraints=CA:FALSE
4. keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
5. extendedKeyUsage = serverAuth
6. subjectAltName = @alt\_names
7. [alt\_names]
8. DNS.1=redmine.brobridge.lab
9. EOF

建立私服器憑證

* 根據資安要求，修改指定加密格式跟天數即可。

1. openssl x509 -req -sha512 -days 3650 \
2. -CA ca.crt -CAkey ca.key -CAcreateserial \
3. -in redmine.brobridge.lab.csr \
4. -out redmine.brobridge.lab.crt \
5. -extfile v3.ext
6. 憑證配置

* 將 Server 憑證放在目錄下

1. [root@redmine conf.d]# ll /etc/redmine/ssl/
2. total 12
3. -rw-------. 1 root root 4588 Oct 28 2022 brobridge.lab.crt
4. -rw-------. 1 root root 1704 Oct 28 2022 brobridge.lab.key

* 替換新的憑證後，重啓 Nginx:

1. systemctl reload nginx
2. Jenkins 機器測試

以下操作適用 RedHat 系統

* 將憑證放上 Client 主機; 也可以將內容內容過去。

1. ## 放在這個目錄下，名稱與系統相符即可。
2. cd /etc/pki/ca-trust/source/anchors/

* 更新憑證信任

1. sudo update-ca-trust

* 用 curl 測試（會出現 401 是正常的）

1. curl -i https://redmine.brobridge.lab/issues.xml
2. Trubleshoot

* 指定憑證

1. curl -v https://redmine.brobridge.lab/issues.xml --cacert redmine.brobridge.lab.crt

* 確認系統上包含該憑證

1. trust list | grep redmine

* 忽略憑證

1. curl -v https://redmine.brobridge.lab/issues.xml --insecure
2. 確認私服器憑證包含 SAN（沒有包含也可過）
3. openssl x509 -in redmine.brobridge.lab.crt -noout -text | grep -A 1 "Subject Alternative Name"