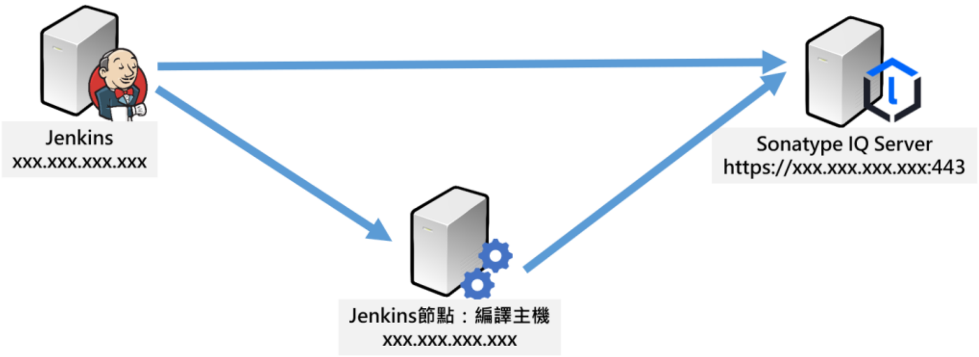
Sonatype-Jenkins CI 整合

※請參考：https://help.sonatype.com/en/sonatype-platform-plugin-for-jenkins.html#sonatype-platform-plugin-for-jenkins---lifecycle

1 整合架構說明

1.1 架構圖



1.2 網路需求

開放以下連線需求：

a. Jenkins 伺服器連至 Sonatype IQ Server

b. Jenkins 節點連至 Sonatype IQ Server

2 插件版本需求與下載位置

2.1 版本相容性

Plugin Version	IQ Server Version	Jenkins Version	Java Runtime
3.20.4 and higher	144 and higher	2.452.0 (LTS) or higher	JDK 17, 21
3.19.0 to 3.20.3	144 and higher	2.361.1 (LTS) or higher	JDK 11, 17
3.16.514 to 3.18.1	144 and higher	2.346.3 (LTS) or higher	JDK 8, 11, 17
3.16.444 to 3.16.510	144 and higher	2.303.3 (LTS) or higher	JDK 8, 11
3.6.20190722-122200.83d1447 to 3.15.438	69 and higher	2.249.1 (LTS) or higher	JDK 8, 11
3.3.20180830-142202.6bdf614 to 3.5.20190425-152158.c63841b	50 and higher	2.249.1 (LTS) or higher	JDK 8, 11
3.0.20180425-130011.728733c to 3.3.20180801-112343.4970c8a	47 and 48	2.249.1 (LTS) or higher	JDK 8, 11
1.1 to 3.0.20180214-134325.e135900	26 - 46	2.249.1 (LTS) or higher	JDK 8

※請參考：https://help.sonatype.com/en/sonatype-platform-plugin-for-jenkins.html#compatibility-253995_body

2.2 下載位置

最新版本：

https://download.sonatype.com/integrations/jenkins/nexus-jenkins-plugin-3.26.0-01.hpi

3 安裝插件

a. 下載插件

b. 登入 Jenkins 伺服器

c. 進入 Manage Jenkins > Plugins 頁面

d. 在左側點選 Advanced Settings

e. 點擊”選擇檔案”，找到已下載的插件檔案(.hpi)

f. 點擊”部署”

4 設定插件

a. 登入 Jenkins 伺服器

b. 進入 Manage Jenkins > System 頁面

c. 捲動至 Sonatype IQ Servers 區塊

d. 點擊”Add Sonatype IQ Server”

甲、Display Name: sonatype-dev (依需求修改)

乙、Server ID: sonatype-dev (依需求修改)

丙、Server URL: http://xxx.xxx.xxx.xxx:443 (依需求修改)

丁、新增 Credential (Jenkins Credential Provider)

i. Kind: Username and password

ii. Scope: Global

iii. Username: xxxxxx (依需求修改)

iv. Password: xxxxxxx (依需求修改)

v. ID: sonatype-lifecycle-scan (依需求修改)

vi. Description: Lifecycle 掃描使用

vii. 點擊”Add”儲存

戊、Credential: 選擇剛設定” Lifecycle 掃描使用”的項目

己、點擊”Test Connection”，確認連線正確

庚、點擊”Save”或”套用”，儲存設定

5 設定 Pipeline 進行掃描

5.1 nexusPolicyEvaluation 語法

```
nexusPolicyEvaluation advancedProperties: '',
        enableDebugLogging: false,
        failBuildOnNetworkError: false,
        iqApplication: selectedApplication('webgoat'),
        iqInstanceId: 'sonatype-dev',
        iqScanPatterns: [[scanPattern: '**/target/*.jar']],
        iqStage: 'build',
        jobCredentialsId: 'sonatype-lifecycle-scan'
```

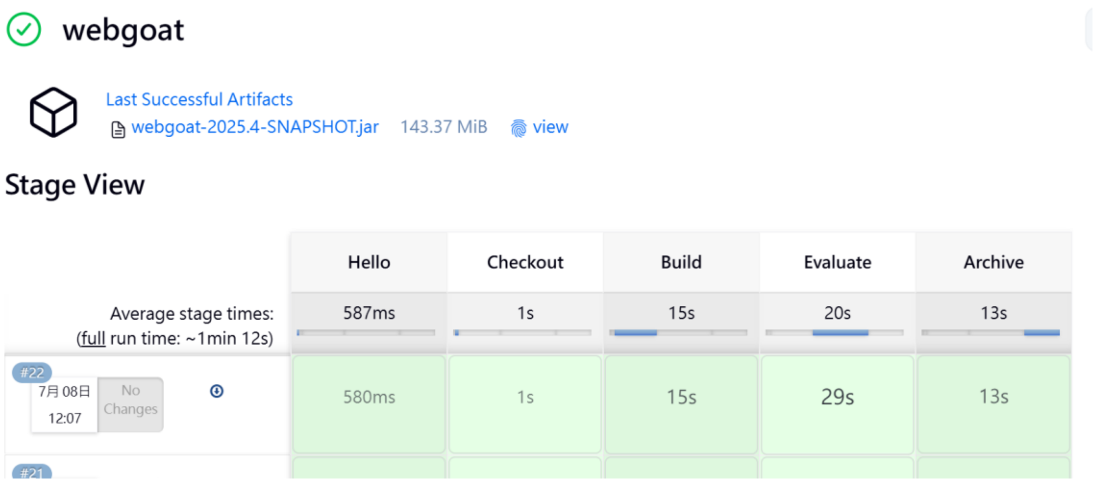
5.2 透過 Pipeline Syntax

a. Sample Step: nexusPolicyEvaluation
    甲、IQ Instance: sonatype-dev (選擇步驟 4 設定的 Server ID)
    乙、Stage: Build (依需求選擇階段)
    丙、Organization: Sandbox-Organization (依需求選擇，需預先設定)
    丁、Application
        i. 點選 “Select an IQ Application”
        ii. Application: Sandbox-Application (依需求選擇，需預先設定)
    戊、Scan Target: **/target/*.jar (依掃描標的設定)
    己、Advanced options
        i. Use job specific credentials: 選擇剛設定” Lifecycle 掃描使用”的項目
        ii. 點擊”Test Connection”

b. 點擊”Generate Pipeline Script”

c. 將產生的內容，複製到 Pipeline 中

5.3 執行結果



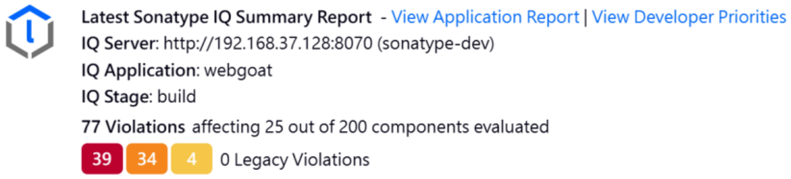
webgoat

Last Successful Artifacts

webgoat-2025.4-SNAPSHOT.jar 143.37 MiB view

Stage View

	Hello	Checkout	Build	Evaluate	Archive
Average stage times: (full run time: ~1min 12s)	587ms	1s	15s	20s	13s
#22 7月 08日 12:07 No Changes	580ms	1s	15s	29s	13s
#21					



Latest Sonatype IQ Summary Report - View Application Report | View Developer Priorities

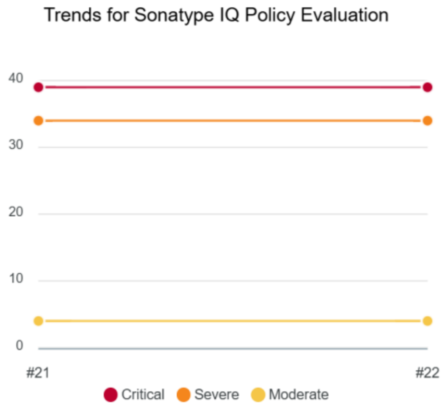
IQ Server: http://192.168.37.128:8070 (sonatype-dev)

IQ Application: webgoat

IQ Stage: build

77 Violations affecting 25 out of 200 components evaluated

39 34 4 0 Legacy Violations



6 Pipeline Sample Script

```
node('st-node') {
        stage('Hello') {
                bat 'hostname'
                bat 'path'
        }
        stage('Checkout') {
                git url: 'https://github.com/WebGoat/WebGoat.git', branch: 'main'
        }
        stage('Build') {
                def mvnHome = tool 'M3'
                env.JAVA_HOME = "D:/Tools/jdk-23.0.2+7"
                bat "mvnw -v"
                bat "${mvnHome}/bin/mvn clean package -DskipTests"
        }
        stage('Evaluate') {
                nexusPolicyEvaluation advancedProperties: '',
                        enableDebugLogging: false,
                        failBuildOnNetworkError: false,
                        iqApplication: selectedApplication('webgoat'),
                        iqInstanceId: 'sonatype-dev',
                        iqScanPatterns: [[scanPattern: '**/target/*.jar']],
                        iqStage: 'build',
                        jobCredentialsId: 'sonatype-lifecycle-scan'
        }
        stage('Archive') {
                step([$class: 'ArtifactArchiver', artifacts: '**/target/*.jar', fingerprint:
true])
        }
}
```