2025 DevSecOps 환경 구축 가이드

상징, 로고, 폰트, 원이(가) 표시된 사진

자동 생성된 설명

Korea IT DevSecOps

2025. 02. 20

# 서론

**2025 DevSecOps 환경 구축 가이드**는 DevSecOps 방식을 통해 개발, 운영, 보안을 효과적으로 통합하여 CI/CD 프로세스를 최적화하고 시스템의 안전성을 강화하는 방법을 제시합니다. 특히, Jenkins, SonarQube, Docker, Kubernetes와 Wazuh을 활용하여 소스 코드 품질을 개선하고 보안 자동화를 구현하는 구체적인 접근법을 제공합니다.

이 문서는 다음을 목표로 합니다:

1. 개발 산성 증대

CI/CD 파이프라인 자동화를 통해 효율적인 빌드 및 배포 프로세스 구현.

2. 보안 내재화

코드 분석 및 취약점 점검 도구를 활용하여 개발 초기 단계에서부터 보안을 강화.

3. 안정적인 환경 구축

Kubernetes 기반 확장 가능하고 안정적인 애플리케이션 실행 환경 설계.

4. 실시간 모니터링 및 분석

Wazuh를 사용하여 시스템 로그, 보안 이벤트를 통합 관리하고, 빠른 문제 분석과 대응지원.

5. 협업화 촉진

개발, 운영, 보안 팀 간의 긴밀한 협력을 통해 조직 전반의 보안 인식 제고.

본 가이드는 실무적인 설정 및 적용 사례를 중심으로 DevSecOps 환경을 단계적으로 구축하는 방법을 설명하며, 이를 통해 안전하고 효율적인 소프트웨어 개발, 운영, 그리고 보안을 제공합니다.

# 팀 소개

|  |  |
| --- | --- |
| 상징, 로고, 폰트, 원이(가) 표시된 사진  자동 생성된 설명  Team DevSecOps | 기획  정재호 장진영 박진우 안정훈 지윤정 |
| 개발  배준성 윤광혁 최민재 장태경 |
| 운영  김범준 김지홍 노윤서 손혜영 이주원 |

# Lab Git Repository

<https://github.com/jinyeong001/DevSecOps.Full-Project.git>

<https://github.com/GH6679/web_wargamer.git>

목차

[2025 DevSecOps 환경 구축 가이드 1](#_Toc187665766)

[서론 1](#_Toc187665767)

[팀 소개 2](#_Toc187665768)

[Lab Git Repository 2](#_Toc187665769)

[1. DevSecOps 5](#_Toc187665770)

[1.1. DevSecOps 란? 5](#_Toc187665771)

[1.2. DevSecOps의 이점 6](#_Toc187665772)

[2. 사전 준비 사항 7](#_Toc187665773)

[2.1 사전 요구 사항 (필요 설치 파일) 7](#_Toc187665774)

[2.2 사전 요구 사항 설치 7](#_Toc187665775)

[3. yaml 작성법 9](#_Toc187665776)

[3.1 yaml 이란? 9](#_Toc187665777)

[3.2 주요 필드 9](#_Toc187665778)

[3.3 워커 노드 추가 10](#_Toc187665779)

[3.4 기타 필드 11](#_Toc187665780)

[4. Kubernetes 14](#_Toc187665781)

[4.1 Kubernetes 란? 14](#_Toc187665782)

[4.2 DevSecOps에서 Kubernetes의 역할 15](#_Toc187665783)

[4.3 kind 15](#_Toc187665784)

[4.4 오류 발생 또는 충돌 시 18](#_Toc187665785)

[5. Jenkins 19](#_Toc187665786)

[5.1 Jenkins 란? 19](#_Toc187665787)

[5.2 DevSecOps에서의 Jenkins의 역할 19](#_Toc187665788)

[5.3 Jenkins worker node 생성 20](#_Toc187665789)

[5.4 Jenkins worker node 실행 23](#_Toc187665790)

[6. Wazuh 25](#_Toc187665791)

[6.1 Wazuh 란? 25](#_Toc187665792)

[6.2 Wazuh의 역할 25](#_Toc187665793)

[6.3 Wazuh 사용계획 및 기대되는 이점 25](#_Toc187665794)

[7. Web 구축 26](#_Toc187665795)

[7.1. WebPage 소스코드 26](#_Toc187665796)

[7.2. Web worker node 생성 27](#_Toc187665797)

[7.3 Web worker node 실행 31](#_Toc187665798)

# 1. DevSecOps

### 1.1. DevSecOps 란?

DevSecOps는 개발(Development), 보안(Security), 운영(Operations)을 통합하여 소프트웨어 개발의 전 과정에서 보안을 자동화하고 내재화하는 방법론입니다. 기존 DevOps 모델은 개발과 운영 간 협업에 초점을 맞췄으나, 보안은 종종 후순위로 다뤄졌습니다. 이에 반해 DevSecOps는 초기 설계 단계부터 배포, 운영에 이르기까지 보안을 모든 과정에 포함시키며, 이를 통해 **보안은 모두의 책임**이라는문화를 강조합니다.

DevSecOps의 주요 원칙은 다음과 같습니다:

* **자동화된 보안 통합**: CI/CD 파이프라인에 보안 도구를 통합하여 코드 분석, 취약점 점검, 종속성 관리를 자동화합니다.
* **보안 중심의 협업**: 개발, 운영, 보안 팀이 협력하여 보안 문제를 조기에 발견하고 해결합니다.
* **지속적인 개선**: 위협 모델링과 실시간 모니터링으로 보안을 지속적으로 강화합니다.

우리는 DevSecOps 구현을 위해 Jenkins와 같은 CI/CD 도구를 기반으로 SonarQube로 코드 품질 및 보안 점검을 수행하며, Wazuh를 활용해 시스템 로그를 분석하고 이상 행동을 탐지합니다. 또한, Docker와 Kubernetes로 컨테이너 보안을 강화하고, Falco 등의 런타임 보안 도구로 운영 환경의 보안성을 유지합니다.

이러한 접근법은 보안을 단순한 방어 전략이 아닌 개발과 운영의 핵심 요소로 자리 잡게 합니다. 이를 통해 조직 내 보안 문화가 정착되고, 빠르고 안전한 소프트웨어 배포가 가능해집니다.

### 1.2. DevSecOps의 이점

DevSecOps를 채택하면 다양한 이점을 누릴 수 있습니다. 먼저, CI/CD 파이프라인에서 자동화된 보안 테스트와 취약점 분석 도구를 활용함으로써 개발 초기부터 보안을 강화할 수 있습니다. 보안이 개발 초기 단계에 통합되면, 후반 단계에서 보안 취약점을 수정하는 데 드는 비용을 크게 절감할 수 있습니다. 이는 보안 문제를 사전에 식별하고 해결하는 데 중요한 역할을 하며, 전반적인 개발 비용 절감으로 이어집니다.

또한, DevOps의 자동화와 속도를 유지하면서도 보안 검사를 주기적으로 수행할 수 있습니다. 이를 통해 안전한 코드 배포가 보장되며, 지속적인 통합 및 배포(CI/CD)를 지원하는 보안 관행이 자연스럽게 형성됩니다. 주기적인 보안 점검을 통해 개발과 배포 과정에서 발생할 수 있는 보안 리스크를 사전에 최소화할 수 있습니다.

DevSecOps에서는 보안이 단지 보안 팀의 책임만이 아닙니다. 개발자와 운영 팀도 보안에 대한 책임을 공유하고 협업하는 문화가 필요합니다. 이를 통해 조직 내 보안 인식 수준이 높아지고, 더 빠르고 효율적인 보안 대응이 가능합니다. 또한, 위협 모델링과 모니터링을 통해 실시간으로 보안을 관리하고, 발생할 수 있는 보안 문제를 예방할 수 있습니다. 이러한 방식은 다양한 산업에서 요구하는 보안 표준과 규제를 준수하는 데도 유효합니다.

이와 같은 이유로 우리는 DevSecOps를 채택하여 개발, 보안, 운영이 유기적으로 협력하고 효율적으로 관리될 수 있도록 하는 통합 프로젝트를 추진하고 있습니다. DevSecOps 환경을 통해 보안을 강화하면서도 개발과 운영의 효율성을 유지할 수 있는 시스템을 구축할 수 있습니다.

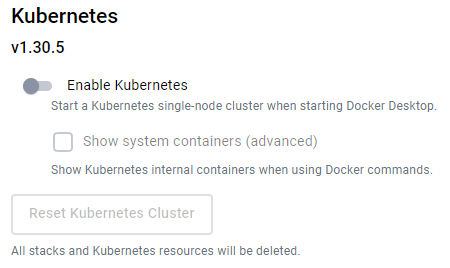
# 2. 사전 준비 사항

### 2.1 사전 요구 사항 (필요 설치 파일)

* WSL(WSL2)
* Docker Desktop(Kind)
* Git
* Chocolatey
* Kuberctl
* 구축파일(.yaml)
* localtunnel

본 프로젝트의 작업은 바탕화면에서 진행됩니다.

Docker Desktop 설치 후 설정에서 Kubernetes 해제 필요 (기본 설정)



### 2.2 사전 요구 사항 설치

Window PowerShell 관리자 권한으로 실행

1) WSL(Windows Subsystem for Linux) 설치

Windows에서 Linux 환경을 구축할 수 있게 해주는 핵심 기능을 한다.

# WSL 설치

1. dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart
2. dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart

# WSL2 기본 버전으로 설정

1. wsl –set-default-version 2

2) Chocolatey 설치

Chocolatey는 Windows용 패키지 관리자 도구이다.

# Chocolatey 패키지 관리자 설치

1. Set-ExecutionPolicy Bypass -Scope Process -Force
2. [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.ServicePointManager]::SecurityProtocol -bor 3072
3. iex ((New-Object System.Net.WebClient).DownloadString('https://community.chocolatey.org/install.ps1'))

3) Git 설치

Github 및 Jenkins를 통한 자동화 핵심 기능을 한다.

# Git 기본 패키지 설치

1. choco install git -y

4) Docker Desktop, kubectl 및 kind 설치

Kind(Kubernetes IN Docker)는 Docker 컨테이너를 사용하여 Kubernetes 클러스터를 쉽게 배포하고 관리할 수 있게 해주는 도구이다..

# Docker Desktop 설치

1. choco install docker-desktop -y

# kubectl과 kind 설치

1. choco install kubernetes-cli -y
2. choco install kind -y

5) Localtunnel 설치

localtunnel 설명 추가

# node.js 다운로드

1. <https://nodejs.org/ko/>

Window cmd 관리자 권한 실행

# localtunnel 다운로드

1. npm install -g localtunnel

Localtunnel 사용 방법

# Window cmd 관리자 권한 실행

1. lt –subdomain <도메인 이름> --port <사용될 포트>

# 터널 비밀번호

1. <https://loca.lt/mytunnelpassword>

# 3. yaml 작성법

### 3.1 yaml 이란?

YAML은 "YAML Ain't Markup Language"의 약자로, 데이터 직렬화에 사용되는 가볍고 사람이 읽기 쉬운 형식입니다. JSON이나 XML과 비교해 간결하고 이해하기 쉬운 구문을 제공하며, 설정 파일이나 데이터 저장에 자주 활용됩니다. YAML은 들여쓰기를 통해 데이터 구조를 정의하며, 주로 다음과 같은 특징이 있습니다.

* **간결성**: 태그나 괄호 없이 간단한 텍스트 기반 형식.
* **유연성**: 다양한 데이터 타입과 구조를 지원.
* **사람이 읽기 쉬움**: 들여쓰기로 계층 구조를 표현.

### 3.2 주요 필드

이 작성법은 DevSecOps 환경에서 사용되는 주요 필드(apiVersion, kind, metadata, spec)와 Kubernetes 워커 노드를 추가하는 방법을 중심으로 작성되었습니다.

1) apiVersion

* 뜻: API 버전을 지정합니다. Kubernetes 리소스 종류마다 지원하는 API 버전이 다를 수 있습니다.
* 사용 목적: Kubernetes가 리소스를 처리할 때 올바른 API를 호출하도록 지시합니다.
* 예시: 여기서 apps/v1은 Deployment와 같은 애플리케이션 관련 리소스를 정의할 때 사용합니다.

apiVersion: apps/v1

2) kind

* 뜻: YAML 파일이 정의하는 리소스의 유형을 지정합니다.
* 사용 목적: Kubernetes에서 정의된 리소스 종류(Deployment, Pod 등)를 나타냅니다.
* 예시: 여기서 Deployment는 애플리케이션 배포를 정의함을 의미합니다.

kind: Deployment

3) metadata

* 뜻: 리소스에 대한 메타데이터를 정의합니다. 리소스 이름, 라벨, 주석 등을 포함합니다.
* 사용 목적: 리소스를 식별하거나 관리할 때 사용되는 정보를 제공합니다.
* 주요 필드:
  + name: 리소스의 이름
  + labels: 리소스에 태그를 추가하여 그룹화하거나 필터링에 사용
* 예시

metadata:

name: exmple-deployment

labels: app: example

4) spec

* 뜻: 리소스의 동작 방식과 구성 세부 사항을 정의합니다.
* 사용 목적: Pod 탬플릿, 컨테이너 정의, 서비스 포트 등을 지정합니다.
* 주요 필드:
  + replicas: Pod 복제본 수
  + containers: 실행할 컨테이너 이미지와 설정
* 예시

spec:

replicas: 3

selector:

matchLabels:

app: example

template:

metadata:

labels:

app: example

spec:

containers:

- name: nginx

image: nginx:1.21.6

ports:

- containerPort: 80

### 3.3 워커 노드 추가

1) kind-config.yaml 파일

워커 노드 설정은 nodes 필드에 추가합니다.

kind: Cluster

apiVersion: kind.x-k8s.io/v1alpha4

nodes:

- role: control-plane

- role: worker

labels:

node-type: webserver

purpose: apache-php

- role: worker

labels:

node-type: database

purpose: mysql

* role: worker: 워커 노드로 역할을 지정
* labels: 각 워커 노드에 태그를 추가하여 특정 워크노드에 연결

2) Deployment에서 워커 노드 참조

특정 노드에서 실행되도록 nodeSelector를 사용합니다.

spec:

template:

spec:

nodeSelector:

node-type: webserver

3) 노드 상태 확인

Windows PowerShell 실행 후, 명령어를 통해 클러스트 상태 확인.

1. kubectl get nodes -–show-labels

### 3.4 기타 필드

1) status

* 뜻: 리소스의 현재 상태를 나타냅니다.
* 사용 목적: 리소스가 배포된 후 Kubernetes가 관리하는 동적인 상태 정보를 기록합니다. 사용자가 수동으로 설정할 필요는 없습니다.
* 예시: 현재 3개의 Pod 중 2개가 정상적으로 실행되고 있음을 나타냅니다.

status:

replicas: 3

availableReplicas: 2

2) selector

* 뜻: 리소스를 특정 레이블을 기준으로 연결합니다.
* 사용 목적: Deployment와 같은 리소스가 Pod를 선택하거나 Service가 대상 Pod를 식별할 때 사용됩니다.
* 예시: app: example 레이블이 포함된 리소스를 선택합니다.

selector:

matchLabels:

app: example

3) template

* 뜻: 리소스가 생성할 객체(Pod 등)의 템플릿을 정의합니다.
* 사용 목적: Deployment, DaemonSet 등의 리소스에서 사용되며, 생성할 Pod의 세부 설정을 포함합니다.
* 예시: app: example 레이블을 가진 Pod를 생성하며, nginx 컨테이너를 실행합니다.

template:

metadata:

labels:

app: example

spec:

containers:

- name: nginx

image: nginx:1.21.6

4) volumes

* 뜻: 컨테이너에서 사용할 볼륨을 정의합니다.
* 사용 목적: 데이터의 영속성을 보장하거나 컨테이너 간 데이터를 공유할 때 사용됩니다.
* 예시: Persistent Volume Claim(PVC)을 참조하여 데이터를 영구 저장합니다.

volumes:

- name: example-volume

persistentVolumeClaim:

claimName: example-pvc

5) resources

* 뜻: 컨테이너에서 사용할 CPU와 메모리 리소스를 제한하거나 요청합니다.
* 사용 목적: 클러스터의 리소스를 효율적으로 관리합니다.
* 예시:
  + limits: 컨테이너가 사용할 수 있는 최대 리소스 설정
  + requests: 컨테이너가 요청하는 최소 리소스 설정

resources:

limits:

memory: "512Mi"

cpu: "500m"

requests:

memory: "256Mi"

cpu: "250m"

6) env

* 뜻: 컨테이너 내에서 사용할 환경 변수를 정의합니다.
* 사용 목적: 동적인 환경 설정을 제공하거나 비밀 값을 주입합니다.
* 예시: 데이터베이스 호스트와 포트를 환경 변수로 정의합니다.

env:

- name: DB\_HOST

value: "example-database"

- name: DB\_PORT

value: "3306"

7) ports

* 뜻: 컨테이너가 노출하는 네트워크 포트를 정의합니다.
* 사용 목적: 외부 네트워크와의 통신 경로를 설정합니다.
* 예시: 컨테이너의 80번 포트를 외부로 노출합니다.

ports:

- containerPort: 80

8) nodeSelector

* 뜻: 특정 노드에서 리소스를 실행하도록 지정합니다.
* 사용 목적: 지정된 레이블을 기준으로 Pod가 실행될 노드를 선택합니다.
* 예시: node-type=database 레이블이 설정된 노드에서 Pod가 실행되도록 지정합니다.

nodeSelector:

node-type: database

9) affinity

* 뜻: Pod 배치 전략을 정의합니다.
* 사용 목적: 특정 노드에 Pod을 배치하거나, 특정 노드에서 실행되지 않도록 제약 조건을 설정합니다.
* 예시: node-type=webserver 노드에만 Pod가 배치되도록 지정합니다.

affinity:

nodeAffinity:

requiredDuringSchedulingIgnoredDuringExecution:

nodeSelectorTerms:

- matchExpressions:

- key: node-type

operator: In

values:

- webserver

# 4. Kubernetes

### 4.1 Kubernetes 란?

Kubernetes(쿠버네티스)는 **컨테이너화된 애플리케이션을 쉽고 빠르게 배포 및 확장하며 관리를 자동화**해주는 오픈소스 오케스트레이션 플랫폼입니다. 애플리케이션의 안정적이고 효율적인 운영을 지원하며, 클라우드와 온프레미스 환경 모두에서 사용할 수 있습니다.

Kubernetes는 다양한 구성 요소를 통해 컨테이너화된 애플리케이션을 관리합니다. 주요 개념은 다음과 같습니다:

1. **컨테이너(Container)**

* Docker와 같은 컨테이너 기술을 해 애플리케이션을 격리된 환경에서 실행합니다.
* Kubernetes는 이러한 컨테이너의 배포와 관리를 담당합니다.

2. **노드(Node)**

* Kubernetes 클러스터를 구성하는 서버 단위입니다.
* **마스터 노드**는 클러스터를 관리하고, **워커 노드**는 컨테이너를 실행합니다.

3. **클러스터(Cluster)**

* Kubernetes가 관리하는 시스템 단위로 여러 노드로 구성됩니다.
* 작업을 노드 간에 분배하여 효율적인 리소스 활용을 지원합니다.

4. **파드(Pod)**

* Kubernetes에서 가장 작은 배포 단위로, 하나 이상의 컨테이너가 포함됩니다.
* 동일한 네트워크 및 스토리지를 공유하며 함께 작동합니다.

5. **디플로이먼트(Deployment)**

* 애플리케이션 배포 및 관리를 담당하며, 원하는 상태(예: 컨테이너 수)를 정의합니다.
* Kubernetes는 이 상태를 유지하도록 자동으로 조정합니다.

6. **서비스(Service)**

* 파드 간의 통신을 가능하게 하며, 외부 네트워크와의 연결을 제공합니다.

7. **이벤트 기반 관리**

* 애플리케이션 상태를 지속적으로 모니터링하며, 필요 시 재배치, 재시작, 확장을 수행합니다.

따라서 우리는 Kubernetes의 주요개념을 기반으로 DevSecOps 환경을 효율적으로 관리할 계획입니다. 컨테이너를 통해 애플리케이션을 격리된 환경에서 실행하고, 노드와 클러스터를 활용해 리소스를 최적화하며 안정적인 시스템 운영을 지원합니다.

파드와 디플로이먼트를 이용해 애플리케이션을 유연하게 배포하고, 서비스를 통해 내부 및 외부 네트워크 통신을 원활히 처리합니다. 또한, Kubernetes의 이벤트 기반 관리 기능을 활용해 애플리케이션 상태를 지속적으로 모니터링하고, 필요 시 자동으로 확장하거나 복구하는 방안을 적용할 것입니다.

### 4.2 DevSecOps에서 Kubernetes의 역할

우리가 Kubernetes를 사용하는 이유는 DevSecOps 환경에서 애플리케이션을 효율적이고 안정적으로 관리하기 위함입니다. Kubernetes는 리소스를 최적화하여 비용을 절감하고, 빠른 배포와 자동 복구를 통해 운영 안정성을 제공합니다.

또한, 클라우드와 온프레미스 환경을 모두 지원하며, 애플리케이션 확장과 멀티 클라우드 통합이 가능해 유연성과 확장성이 뛰어납니다. CI/CD 도구와의 손쉬운 통합으로 보안을 강화할 수 있어 우리의 프로젝트에 필수적인 플랫폼입니다.

Kubernetes를 사용함으로써 DevSecOps 환경에서 생산성과 안정성을 동시에 향상시킬 수 있습니다. 자동화된 배포와 리소스 최적화를 통해 개발 및 운영 시간을 단축하고 비용을 절감할 수 있습니다. 장애 발생 시 자동 복구와 중단 없는 업데이트를 제공하여 시스템 가용성과 사용자 경험을 크게 개선합니다.

또한, 멀티 클라우드 및 하이브리드 환경을 지원해 유연한 인프라 구성이 가능하며, 애플리케이션의 확장성을 확보할 수 있습니다. Jenkins, SonarQube, Wazuh 등 다양한 DevSecOps 도구와의 통합으로 파이프라인 전반의 보안과 효율성을 강화할 수 있어, 전체적인 운영 관리가 간소화되고 보안 위험이 최소화됩니다. 이를 통해 안정적이고 신뢰할 수 있는 애플리케이션 서비스를 제공할 수 있습니다.

### 4.3 kind

우리는 kind(Kubernetes IN Docker)를 사용하여 클러스터를 구성하고 노드를 설치 및 관리합니다. kind는 Docker 컨테이너 내에서 Kubernetes 클러스터를 실행할 수 있어, 간편하고 빠르게 개발 및 테스트 환경을 구축할 수 있다는 장점이 있습니다.

1) Kind 설치 및 환경설정

Window PowerShell 관리자 권한 실행

# KIND 다운로드

1. Invoke-WebRequest -Uri "https://kind.sigs.k8s.io/dl/v0.20.0/kind-windows-amd64" -OutFile "$env:USERPROFILE\kind.exe"

# bin 디렉토리 생성 및 이동

1. New-Item -Path "$env:USERPROFILE\bin" -ItemType Directory -Force
2. Move-Item -Path "$env:USERPROFILE\kind.exe" -Destination "$env:USERPROFILE\bin"

# 환경변수 설정

1. $env:Path += ";$env:USERPROFILE\bin"
2. [Environment]::SetEnvironmentVariable('Path', $env:Path, 'User')

# 설치 확인

1. kind –-version

2) kind-config.yaml 생성

kind-config.yaml 파일은 쿠버네티스에서 어떠한 클러스터를 생성할지 설정하는 파일이다.

DevSecOps폴더에 k8s-yaml폴더 생성 및 kind-config.yaml 파일 생성 후, 아래 코드 작성

kind: Cluster

apiVersion: kind.x-k8s.io/v1alpha4

nodes:

# 컨트롤 플레인

- role: control-plane

extraPortMappings:

- containerPort: 30080 #DevSecOps Web

hostPort: 30080

listenAddress: "0.0.0.0"

protocol: TCP

# 워커 노드 1: 테스트 웹서버

- role: worker

labels:

node-type: webserver

purpose: apache-php

3) 클러스터 생성 및 학인

Window PowerShell 관리자 권한 실행

※ Docker Desktop 실행 필요

# DevSecOps\k8s폴더로 이동

#(컴퓨터 설정에 따라 Users폴더 안 사용자 폴더이름 변경 필요)

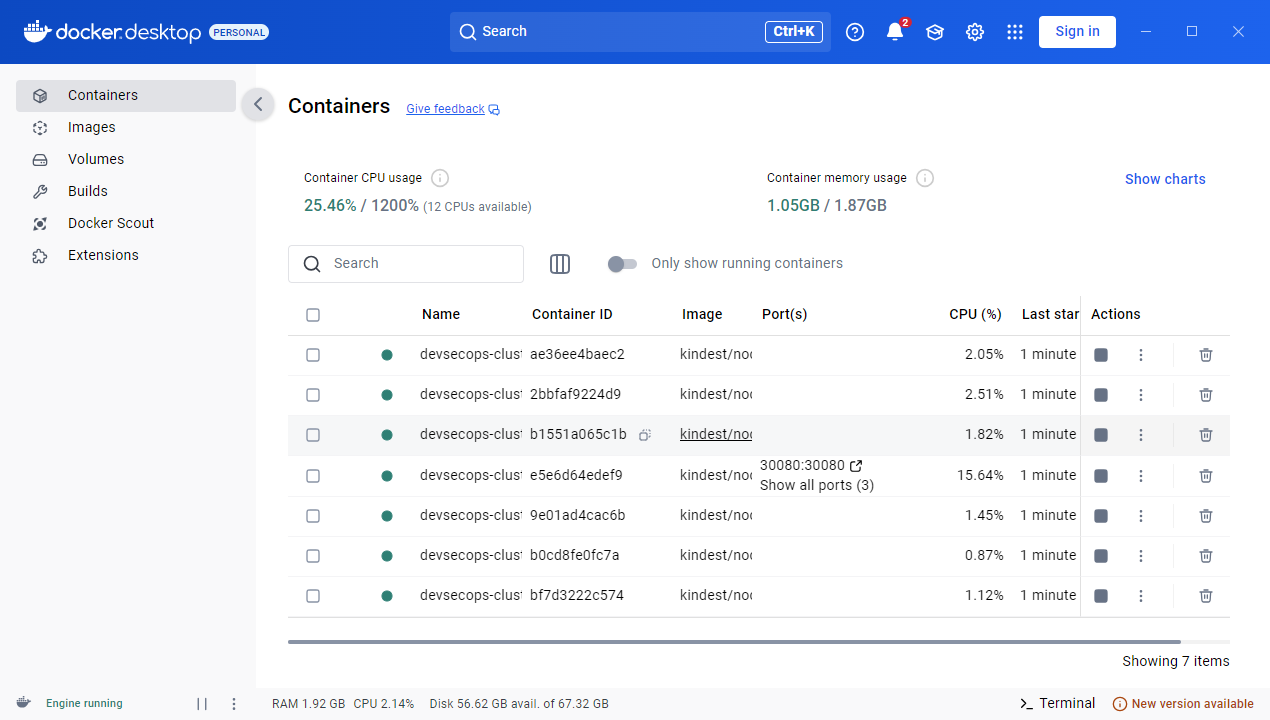
1. cd C:\Users\Administrator\Desktop\DevSecOps\k8s\

# kind 명령어로 새 클러스터 생성

1. kind create cluster --config kind-config.yaml --name devsecops-cluster

# 클러스터 생성 확인

1. Kind get clusters



Docker Desktop 화면

kind-config.yaml 파일에서 설정한 각 노드들이 컨테이너로 실행되고 있는 것을 볼 수 있다.

### 4.4 오류 발생 또는 충돌 시

1) 클러스터 삭제 및 Docker Desktop 재실행

Window PowerShell 관리자 권한 실행

# 모든 클러스터 삭제

1. kind delete clusters -–all

2) Docker Desktop 재실행 후, kindest/node 이미지 삭제

1. Docker Desktop 해당 이미지의 Delete 버튼(휴지통) 클릭



2. Docker Desktop 터미널에서 명령어 입력

# Docker Image 삭제

1. docker rmi <Image ID>

# 5. Jenkins

### 5.1 Jenkins 란?

Jenkins는 CI/CD를 위한 오픈소스로 도구로, 다양한 플러그인을 지원하여 코드 변경 사항이 발생할 때마다 **자동으로 빌드, 테스트, 배포 과정을 수행할 수 있는 도구**입니다.  
이를 통해 개발팀은 소프트웨어 개발 및 배포 과정을 효율적으로 관리할 수 있으며, 반복 작업을 자동화하여 개발 생산성을 크게 향상시킬 수 있습니다.

**CI/CD란 무엇인가?**

* **CI (지속적 통합, Continuous Integration)**: 개발자들이 각자 작업한 코드 변경 사항을 중앙 저장소에 정기적으로 통합하고, 이를 자동화된 빌드와 테스트를 통해 검증하는 프로세스입니다. 이를 통해 코드 품질을 유지하고, 통합 시 발생할 수 있는 문제를 조기에 발견할 수 있습니다.
* **CD (지속적 배포, Continuous Deployment)**: CI 과정에서 통합된 코드가 자동으로 프로덕션 환경에 배포되기까지의 전 과정을 자동화하는 것을 의미합니다. 이로 인해 새로운 기능과 수정 사항이 사용자에게 빠르고 안정적으로 전달될 수 있습니다.

Jenkins는 이러한 CI/CD 프로세스를 손쉽게 구축하고 관리할 수 있는 도구로, 소프트웨어 개발과 배포의 효율성을 크게 향상시킵니다.

### 5.2 DevSecOps에서의 Jenkins의 역할

Jenkins는 DevSecOps 환경에서 **자동화의 핵심 도구**로 활용됩니다.

* 코드 변경 시 **자동으로 빌드하고 테스트하여 오류를 빠르게 발견**할 수 있습니다.
* **수천 개의 플러그인을 통해 다양한 기능**을 추가하여 복잡한 요구 사항을 충족시킬 수 있습니다.
* **배포 파이프라인을 코드로 정의하고 관리**할 수 있어, 재사용성과 유지보수성을 극대화합니다.
* **보안 검증, 취약점 스캔**과 같은 DevSecOps 요구사항도 Jenkins 파이프라인에 통합하여 자동화할 수 있습니다.

이러한 기능을 통해 Jenkins는 DevSecOps의 핵심 원칙인 **자동화, 통합, 보안**을 구현하는 데 중요한 역할을 수행합니다.

### 5.3 Jenkins worker node 생성

1) jenkins-deployment.yaml 생성

jenkins-deployment.yaml 파일은 jenkins worke node 설정 파일이다.

k8s-yaml 폴더에 jenkins-deployment.yaml 파일 생성 후, 아래 코드 작성

apiVersion: apps/v1

kind: Deployment

metadata:

name: jenkins

labels:

app: jenkins

spec:

replicas: 1

selector:

matchLabels:

app: jenkins

template:

metadata:

labels:

app: jenkins

spec:

nodeSelector:

purpose: jenkins

securityContext:

runAsUser: 0

fsGroup: 0

initContainers:

- name: init-jenkins-home

image: busybox

command: ['sh', '-c', 'mkdir -p /var/jenkins\_home && chown -R 1000:1000 /var/jenkins\_home']

volumeMounts:

- name: jenkins-home

mountPath: /var/jenkins\_home

containers:

- name: jenkins

image: jenkins/jenkins:lts

ports:

- containerPort: 8080

name: http

- containerPort: 50000

name: jnlp

volumeMounts:

- name: jenkins-home

mountPath: /var/jenkins\_home

env:

- name: JAVA\_OPTS

value: "-Xmx2048m"

resources:

limits:

memory: "2Gi"

cpu: "1000m"

requests:

memory: "1Gi"

cpu: "500m"

startupProbe:

httpGet:

path: /login

port: 8080

failureThreshold: 30

periodSeconds: 10

readinessProbe:

httpGet:

path: /login

port: 8080

initialDelaySeconds: 60

timeoutSeconds: 5

periodSeconds: 10

livenessProbe:

httpGet:

path: /login

port: 8080

initialDelaySeconds: 60

timeoutSeconds: 5

periodSeconds: 10

volumes:

- name: jenkins-home

persistentVolumeClaim:

claimName: jenkins-pvc

2) kind-config.yaml 수정

Jenkins 클러스터를 생성하기 위해 kind-config.yaml 파일 수정, 아래 코드 추가

kind: Cluster

apiVersion: kind.x-k8s.io/v1alpha4

nodes:

# 컨트롤 플레인

# Jenkins 웹 인터페이스 포트

# - CI/CD 파이프라인 관리 웹 UI

# - 빌드 및 배포 모니터링

# - 호스트 접근: http://localhost:8080

- containerPort: 30800

hostPort: 8080

listenAddress: "0.0.0.0"

protocol: TCP

# Jenkins JNLP 에이전트 포트

# - Jenkins 워커 노드 연결

# - 분산 빌드 에이전트 통신

# - 호스트 접근: localhost:50000

- containerPort: 30850

hostPort: 50000

listenAddress: "0.0.0.0"

protocol: TCP

# 워커 노드 2: Jenkins

- role: worker

labels:

node-type: auto

purpose: jenkins

3) Jenkins-pv.yaml 생성

PV(Persistent Volume)와 PVC(Claim)은 쿠버네티스에서 영구 스토리지를 관리하기 위한 핵심 리소스이다.

apiVersion: v1

kind: PersistentVolume

metadata:

name: jenkins-pv

labels:

type: local

spec:

storageClassName: manual

capacity:

storage: 10Gi

accessModes:

- ReadWriteOnce

hostPath:

path: "/data/jenkins-volume"

---

apiVersion: v1

kind: PersistentVolumeClaim

metadata:

name: jenkins-pvc

spec:

storageClassName: manual

accessModes:

- ReadWriteOnce

resources:

requests:

storage: 10Gi

4) Jenkins-service.yaml 생성

jenkins worker node의 연동을 위한 파일

apiVersion: v1

kind: Service

metadata:

name: jenkins

labels:

app: jenkins

spec:

type: NodePort

ports:

- port: 8080

targetPort: 8080

nodePort: 30800

name: http

- port: 50000

targetPort: 50000

nodePort: 30850

name: jnlp

selector:

app: Jenkins

### 5.4 Jenkins worker node 실행

1) kind 클러스터 재생성

Window PowerShell 관리자 권한 실행

# DevSecOps폴더로 이동

1. cd C:\Users\Administrator\Desktop\DevSecOps

# kind 클러스터 생성

1. kind create cluster --name devsecops-cluster --config k8s-yaml/kind-config.yaml

# 노드 상태 확인

1. kubectl get nodes --show-labels

디플로이먼트와 서비스 배포

# deployment, service yaml 파일 배포

1. kubectl apply -f k8s-yaml/jenkins-deployment.yaml
2. kubectl apply -f k8s-yaml/jenkins-services.yaml

# 배포 상태 확인

1. kubectl get pods -o wide
2. kubectl get services

2) Jenkins 관리자 암호

Jenkins worker node로부터 초기 관리자 암호 추출

# Jenkins Administrator Password에 필요한 패스워드값 출력

1. kubectl exec -it $(kubectl get pods -l app=jenkins -o jsonpath='{.items[0].metadata.name}') -- cat /var/jenkins\_home/secrets/initialAdminPassword

3) 웹 페이지 접속

browser 주소창: localhost:8080 or <http://Windows> Host IP:8080

4) localtunnel을 이용한 도메인 연결

Window cmd 관리자 권한 실행

1. lt --subdomain jenkins1234 --port 8080

# 6. SonarQube

### 6.1 SonarQube란?

SonarQube는 지속적인 코드 품질 관리를 위한 오픈소스 정적 코드 분석 플랫폼입니다. 다양한 프로그래밍 언어를 지원하며, 코드의 품질, 버그, 취약점 등을 자동으로 분석하여 개발팀이 더 나은 소프트웨어를 만들 수 있도록 도와주는 도구입니다.

SonarQube의 주요 기능은 무엇인가?

* 코드 품질 분석: 소스 코드의 버그, 취약점을 감지하고, 중복 코드, 코딩 표준, 단위 테스트, 코드 커버리지, 복잡도 등을 분석하여 전반적인 코드 품질을 평가합니다.
* 지속적 통합: CI/CD 파이프라인과 통합되어 자동화된 코드 분석을 제공하며, Jenkins, GitHub Actions 등 다양한 CI 도구와 연동이 가능합니다.
* 다중 환경 지원: Java, Python, JavaScript, C# 등 30개 이상의 프로그래밍 언어를 지원하며, Linux, Windows, Mac 등 다양한 환경에서 구동이 가능합니다.

SonarQube는 이러한 기능들을 통해 개발팀이 코드 품질을 지속적으로 모니터링하고 개선할 수 있도록 도와주며, 소프트웨어의 전반적인 품질 향상에 크게 기여합니다.

### 6.2 SonarQube yaml 파일 생성

DevSecOps 폴더에 SonarQube 폴더 생성 후 yaml 설정 파일 생성

Window PowerShell 관리자 권한 실행

1) postgres-deployment.yaml 생성

apiVersion: apps/v1

kind: Deployment

metadata:

  name: sonar-postgres

spec:

  replicas: 1

  selector:

    matchLabels:

      app: sonar-postgres

  template:

    metadata:

      labels:

        app: sonar-postgres

    spec:

      nodeSelector:

        node-type: jenkins

        purpose: jenkins

      containers:

      - name: postgres

        image: postgres:12

        env:

        - name: POSTGRES\_DB

          value: sonar

        - name: POSTGRES\_USER

          value: sonar

        - name: POSTGRES\_PASSWORD

          value: sonarpass

        ports:

        - containerPort: 5432

        volumeMounts:

        - name: postgres-data

          mountPath: /var/lib/postgresql/data

      volumes:

      - name: postgres-data

        emptyDir: {}

2) sonarqube-deployment.yaml 생성

apiVersion: apps/v1

kind: Deployment

metadata:

  name: sonarqube

spec:

  replicas: 1

  selector:

    matchLabels:

      app: sonarqube

  template:

    metadata:

      labels:

        app: sonarqube

    spec:

      nodeSelector:

        node-type: jenkins

        purpose: jenkins

      initContainers:

      - name: init-sysctl

        image: busybox:1.28

        command:

        - sysctl

        - -w

        - vm.max\_map\_count=262144

        securityContext:

          privileged: true

      containers:

      - name: sonarqube

        image: sonarqube:8.9.9-community

        ports:

        - containerPort: 9000

        env:

        - name: SONAR\_JDBC\_USERNAME

          value: sonar

        - name: SONAR\_JDBC\_PASSWORD

          value: sonarpass

        - name: SONAR\_JDBC\_URL

          value: jdbc:postgresql://sonar-postgres:5432/sonar

        volumeMounts:

        - name: sonar-data

          mountPath: /opt/sonarqube/data

        - name: sonar-extensions

          mountPath: /opt/sonarqube/extensions

      volumes:

      - name: sonar-data

        emptyDir: {}

      - name: sonar-extensions

        emptyDir: {}

3) services.yaml 생성

apiVersion: v1

kind: Service

metadata:

  name: sonarqube

spec:

  type: NodePort

  ports:

  - port: 9000

    targetPort: 9000

    nodePort: 30900

  selector:

    app: sonarqube

---

apiVersion: v1

kind: Service

metadata:

  name: sonar-postgres

spec:

  ports:

  - port: 5432

  selector:

    app: sonar-postgres

### 6.3 SonarQube node 실행

1) 디플로이먼트와 서비스 배포

Window PowerShell 관리자 권한 실행

# SonarQube 폴더로 이동

1. cd C:\Users\Administrator\Desktop\DevSecOps\SonarQube

# deployment, service yaml 파일 배포

1. kubectl apply -f k8s\postgres-deployment.yaml
2. kubectl apply -f k8s\sonarqube-deployment.yaml
3. kubectl apply -f k8s\services.yaml

# 배포 상태 확인

1. kubectl get pods -o wide
2. kubectl get services

2) 웹 페이지 접속

browser 주소창: localhost:30900

3) localtunnel을 이용한 도메인 연결

Window cmd 관리자 권한 실행

1. lt --subdomain sonarqube1234 --port 30900

# 7. CI/CD 자동화 구축

### 7.1 Github Web hook 설정

Github Repository -> Settings -> Code and automation -> Webhooks -> Add webhook 클릭

**Payload URL**: 3입력

**Current type**: application/json 설정

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

### 7.2 Github Access Token 생성

Github Profile -> Settings -> Developer settings -> Personal access tokens -> Tokens(classic) -> Generate new token (classic) 클릭

**Note**: jenkins\_token 입력

**Select scopes**: repo, workflow, write:packges, admin:repo\_hook 체크

텍스트, 스크린샷, 폰트이(가) 표시된 사진

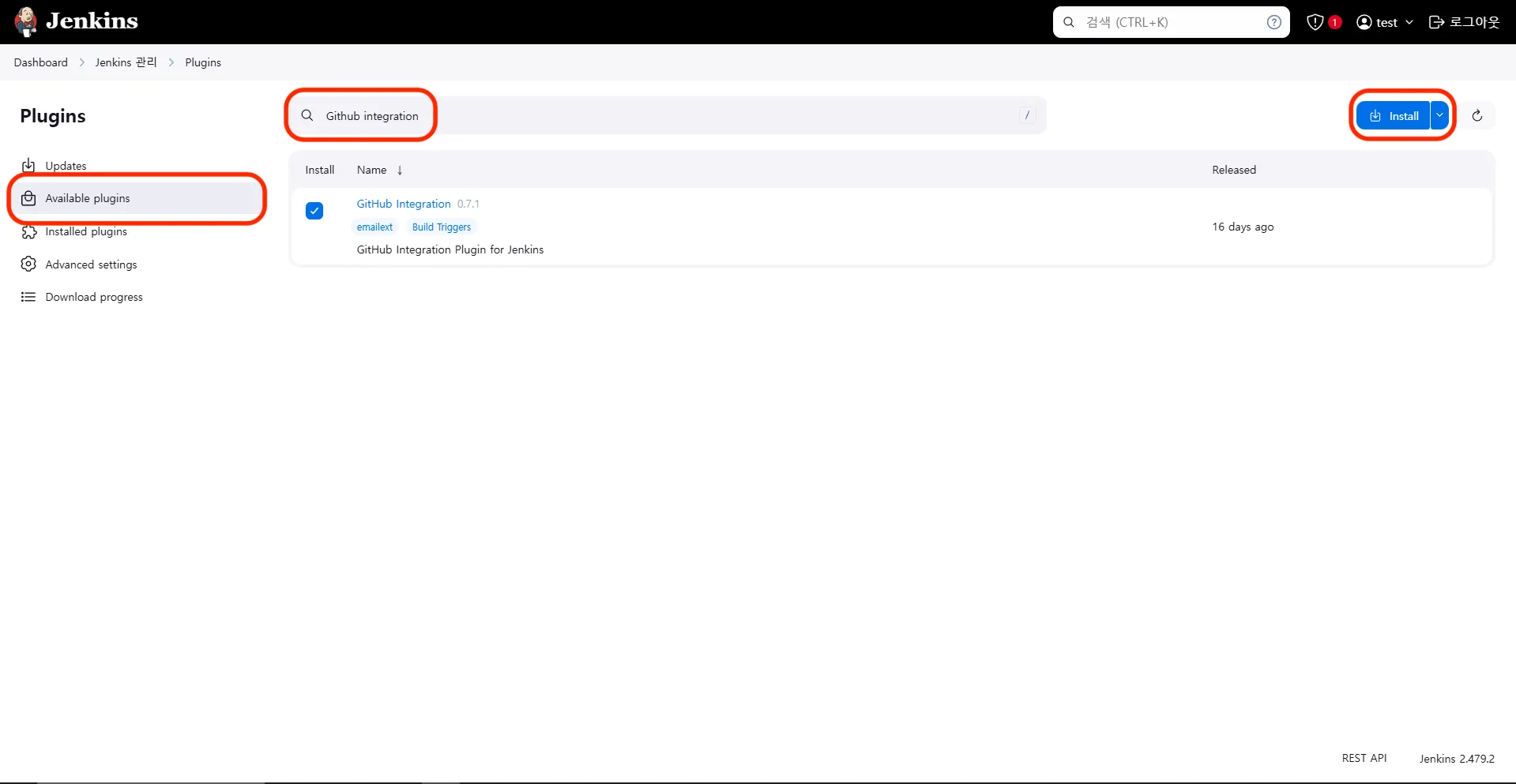
자동 생성된 설명

### 7.3 Jenkins Github 연동

1) Plugin 다운

Dashboard -> Jenkins 관리 -> Plugins -> Available plugins 클릭

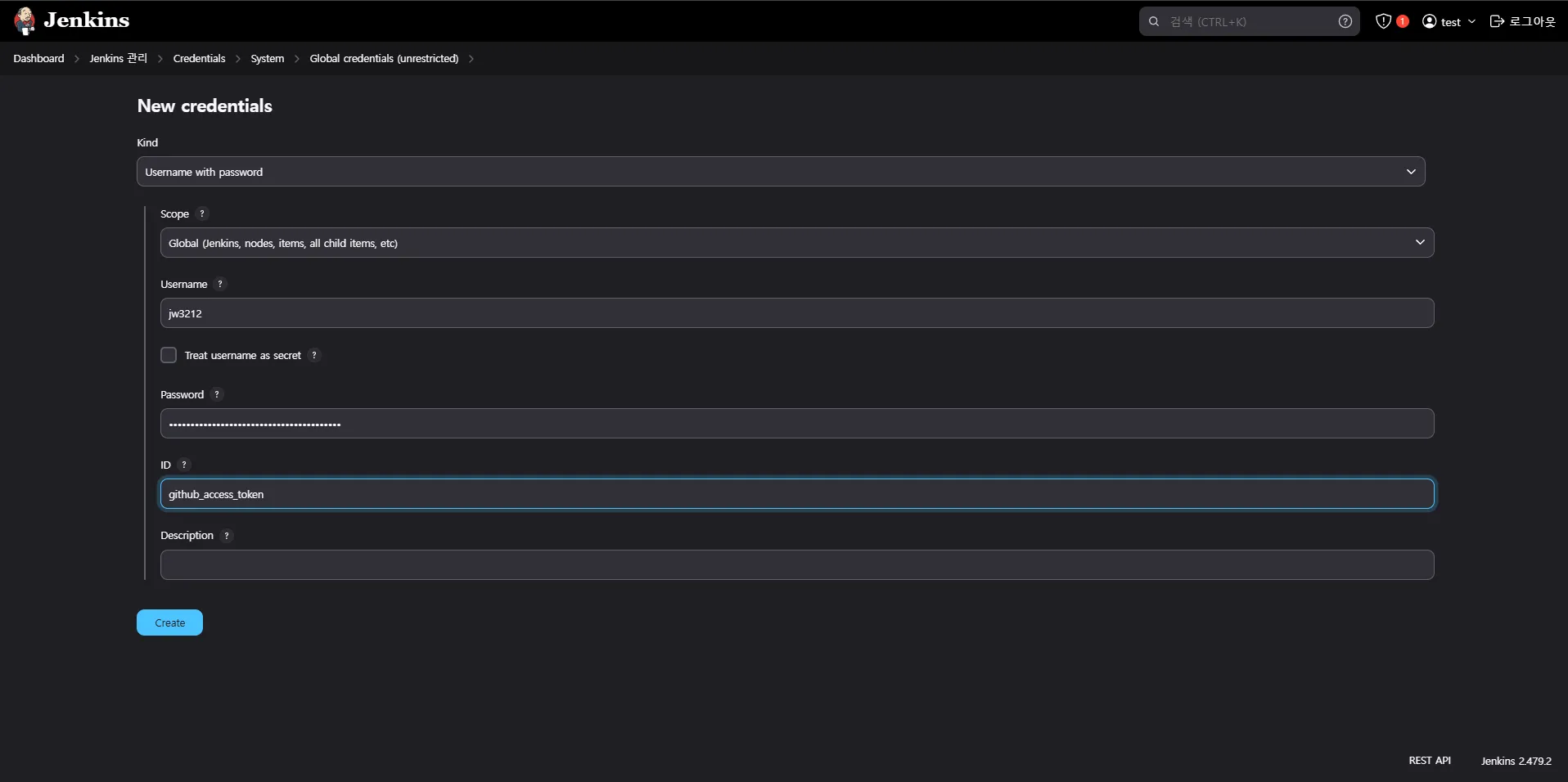
* github integration
* SonarQube Scanner
* Sonar Quality Gates
* Docker
* Docker pipeline



2) Github, Jenkins 연동

Credentials → System → Global credentials에서 Add Credentials 클릭

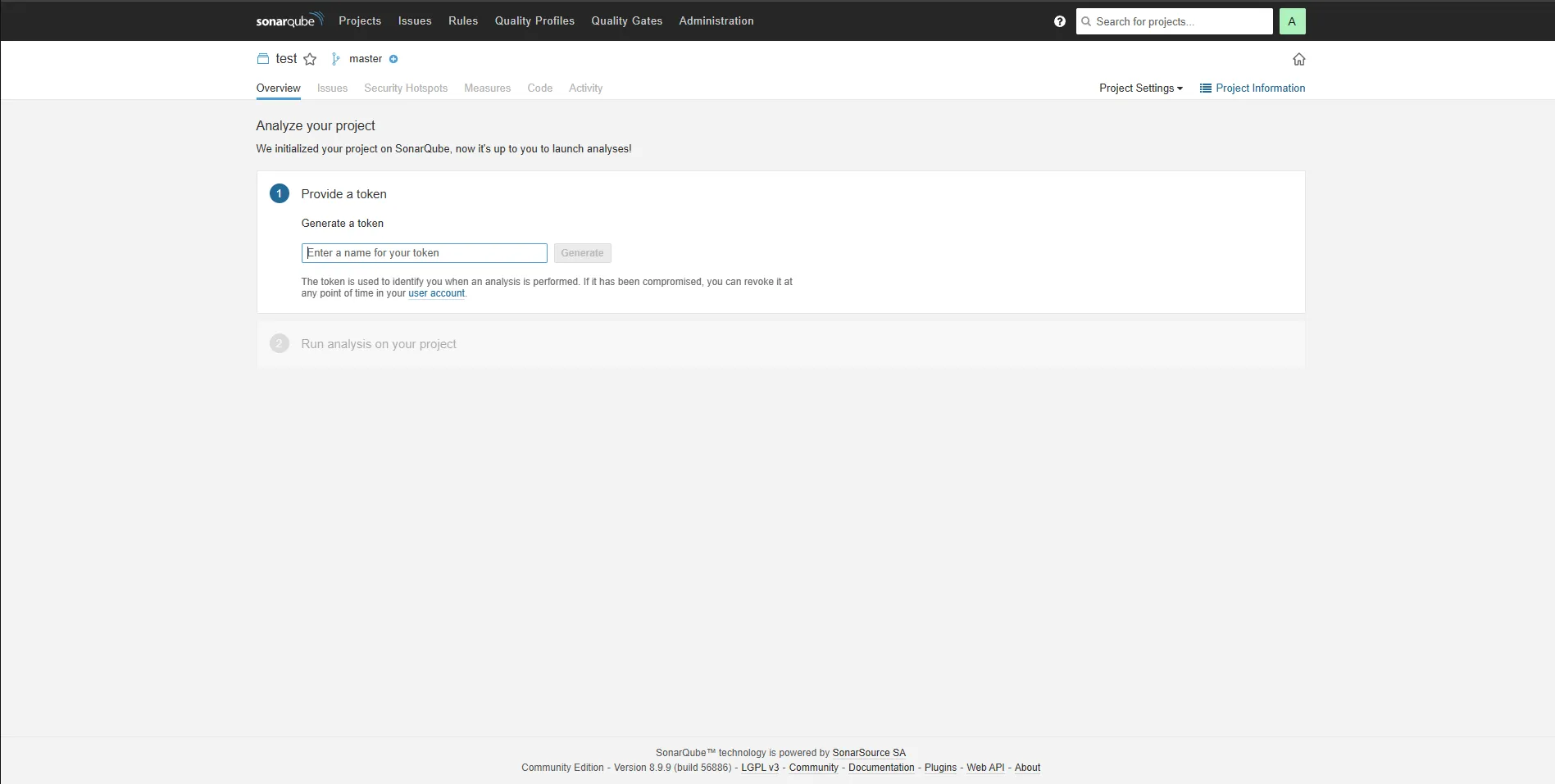
* Username에는 github Username을 입력
* Password에는 github access token을 입력



### 7.4 Sonarqube, Jenkins 연동

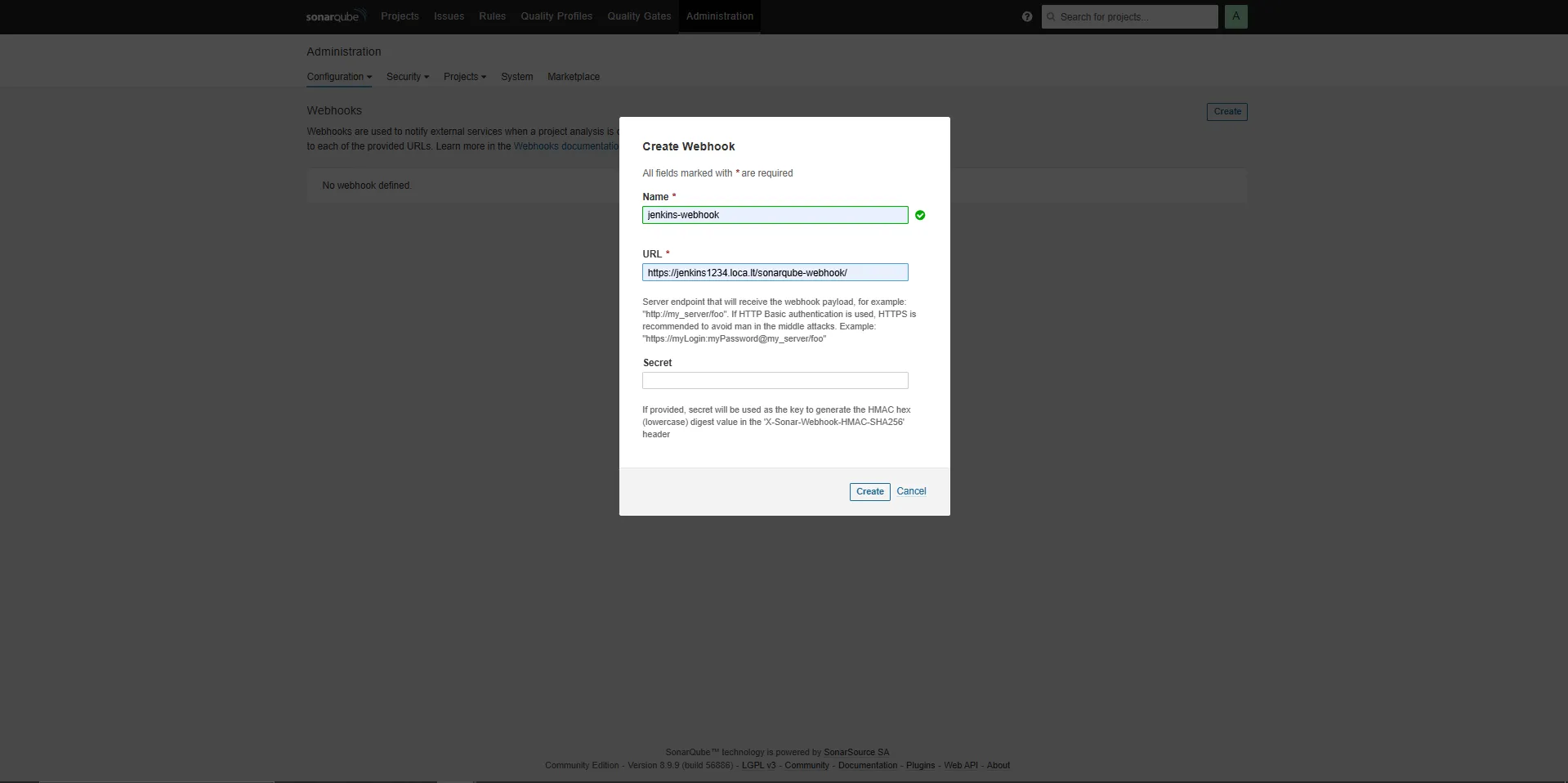
1) Sonarqube Project 생성 및 token 생성

Add a project -> Manually 클릭 -> Project 생성 -> 임의의 값을 사용하여 token 생성



2) Sonarqube, Jenkins Webhook 연동

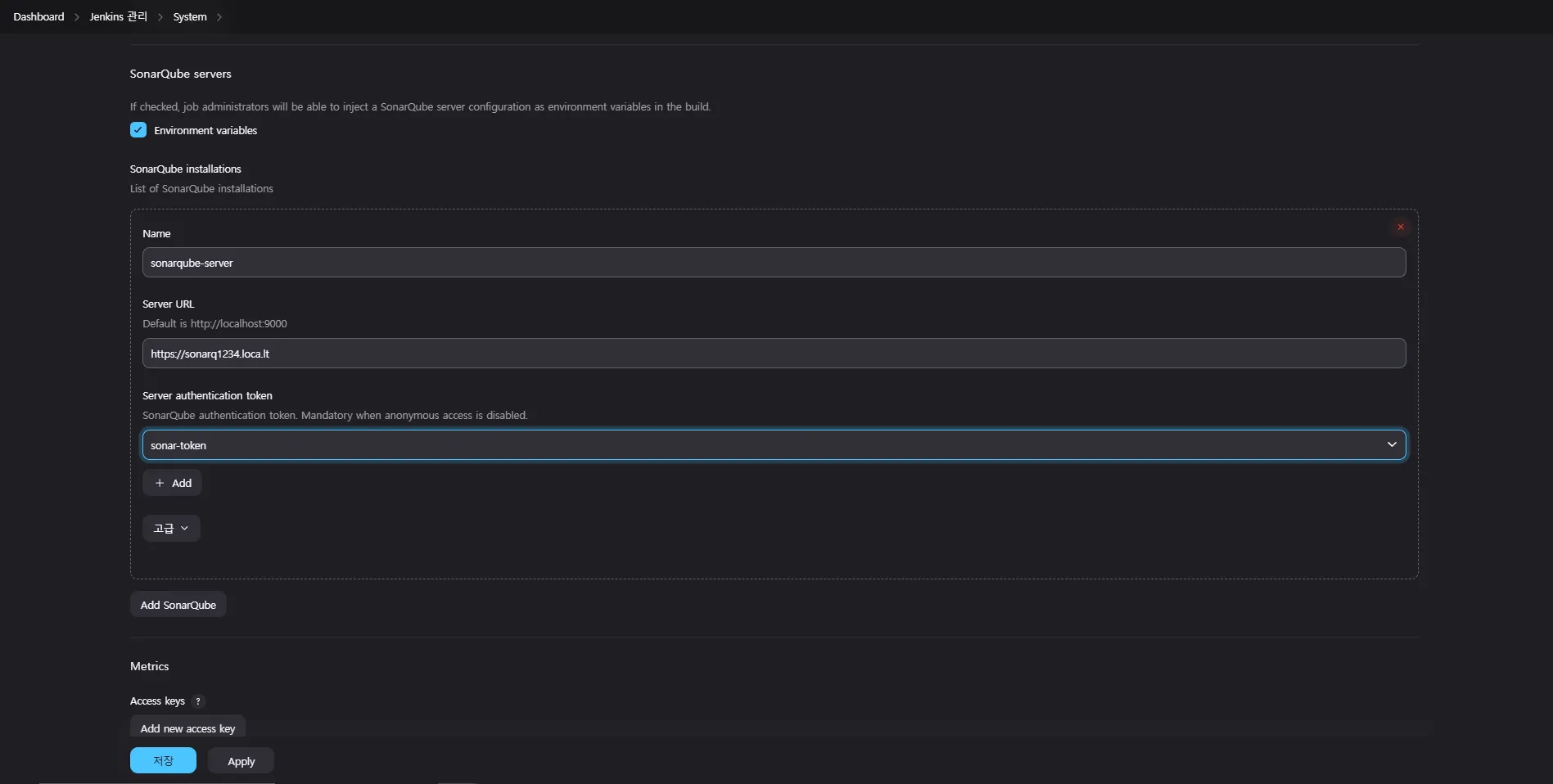
Administration → Configuration → Webhook -> Create 클릭



3) Jenkins, Sonarqube 연동 설정

Dashboard → Jenkins 관리 → System 클릭

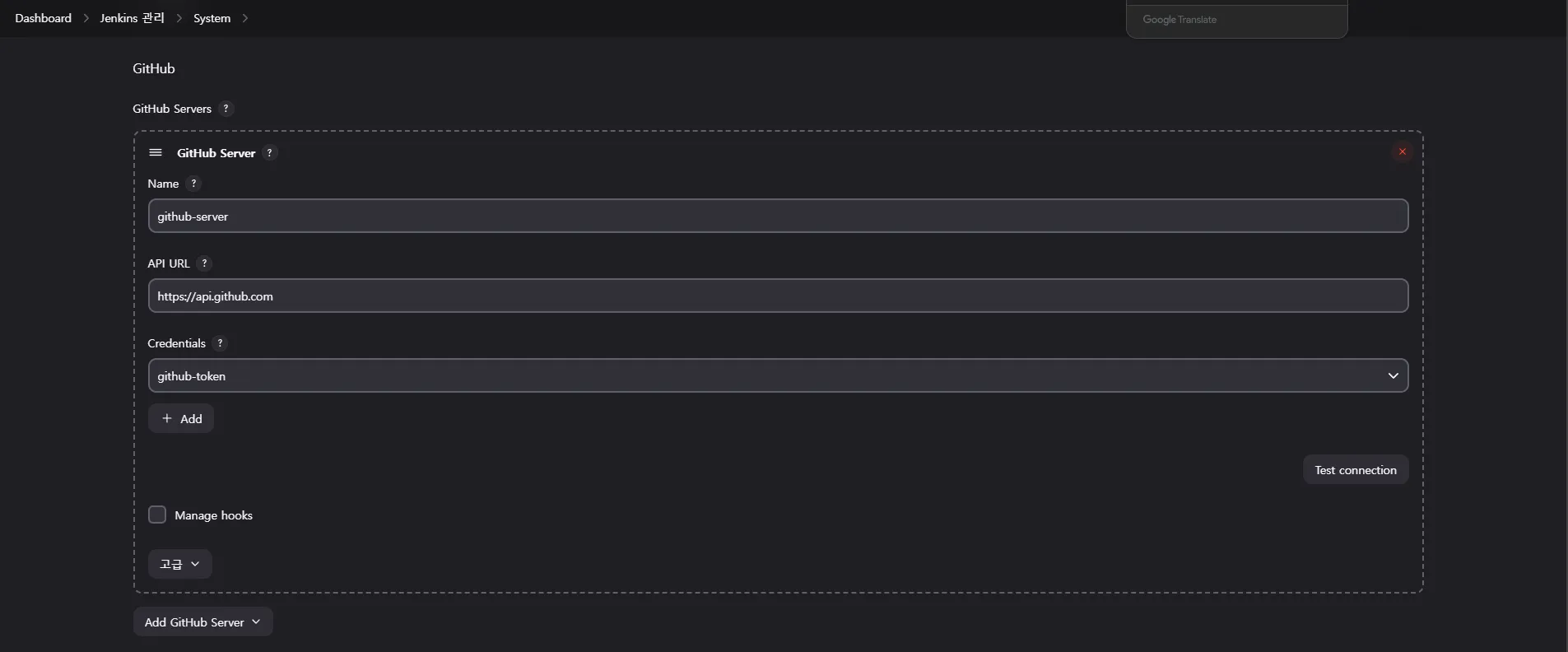
* SonarQube server 설정
* Github server 설정



* Environment variables 체크
* Name 입력
* Server URL 입력
* Server Authentication token add를 클릭하여 생성



* Kind : Secret text 선택
* Secret : Sonarqube에서 생성한 token값을 입력



* API URL : <https://api.github.com> 입력
* Crednetials는 Add를 클릭하여 생성

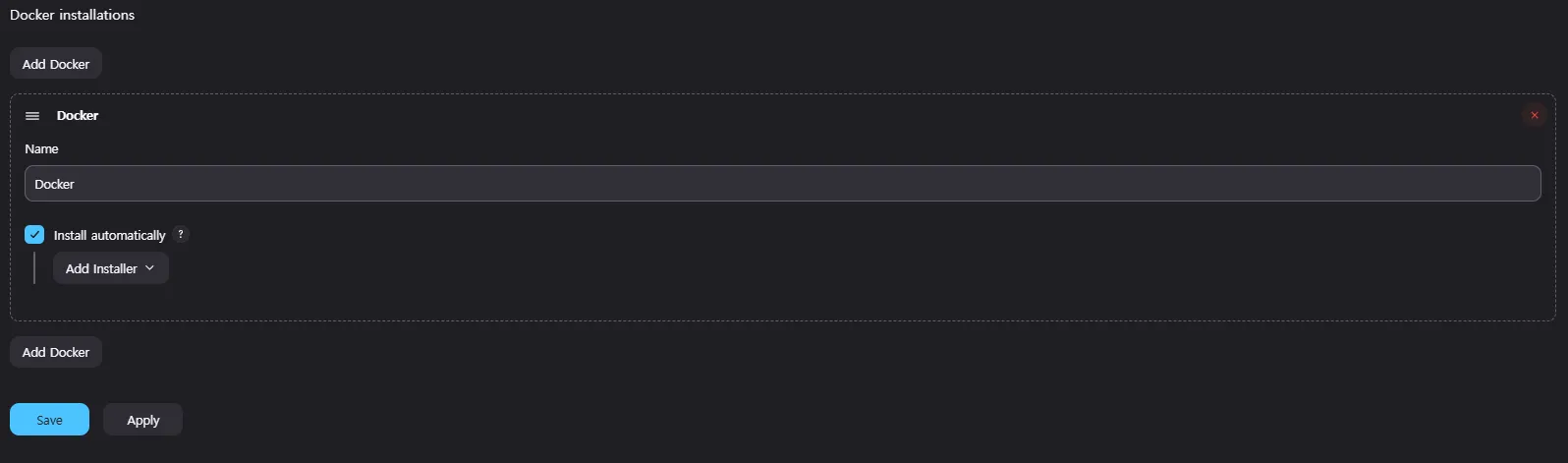


* Kind : Secret text 선택
* Secret : github access token 입력

4) CI/CD에서 사용 될 tool 설정

Dashboard → Jenkins 관리 → Tools 클릭

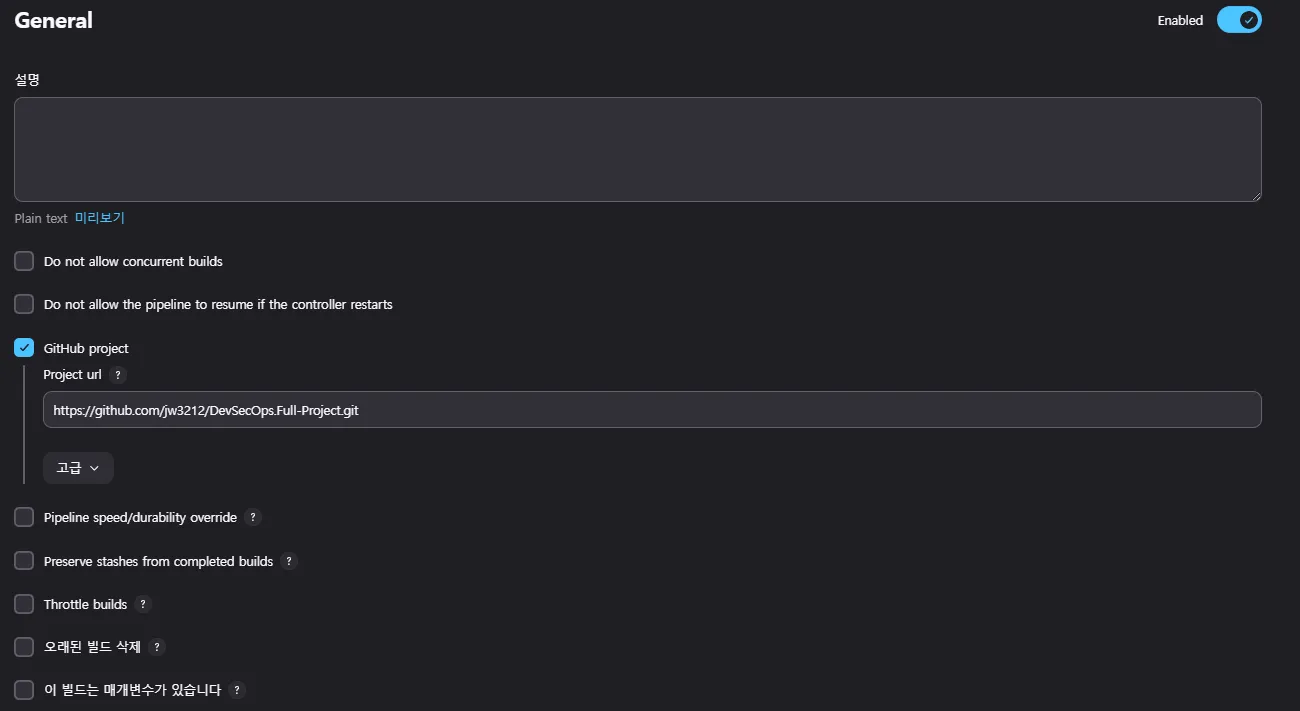
* Sonarqube Scanner installations
* Maven installations
* Docker installations



* Docker는 Install automatically를 체크해 줍니다.

5) Jenkins Project 생성, Pipeline 스크립트 설정 및 테스트

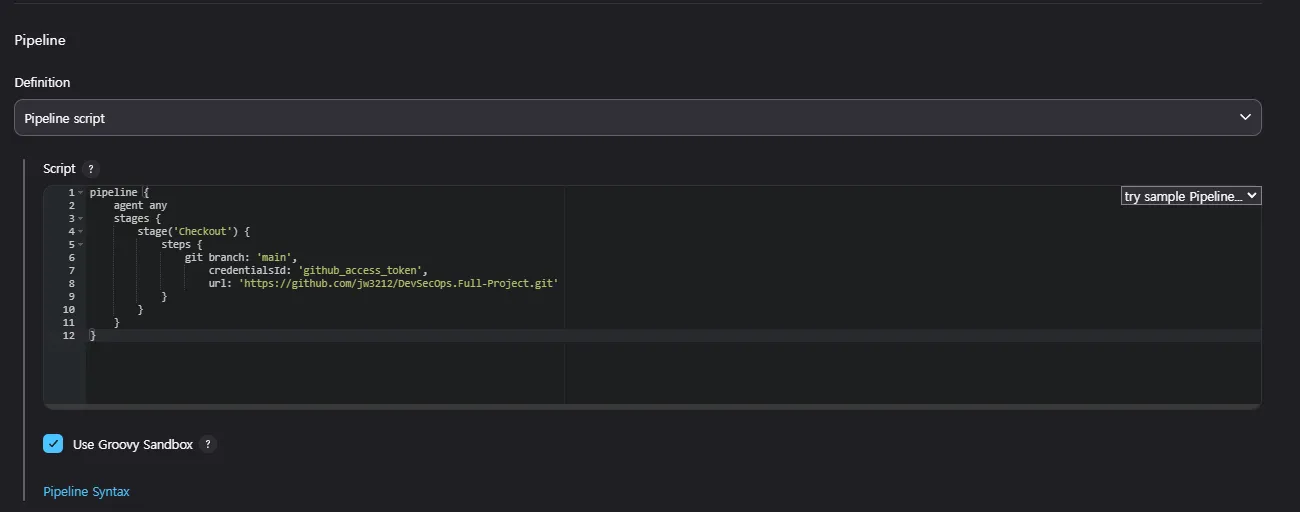
Dashboard -> Create a job -> Pipeline 선택



* Github project 체크
* Project url : github에 Clone using the web URL.의 URL 입력



* GitHub hook trigger for GITScm polling 체크



* Pipeline script 입력

pipeline {

agent any

stages {

stage('Checkout') {

steps {

git branch: 'main',

credentialsId: 'github\_access\_token',

url: 'https://github.com/jw3212/DevSecOps.Full-Project.git'

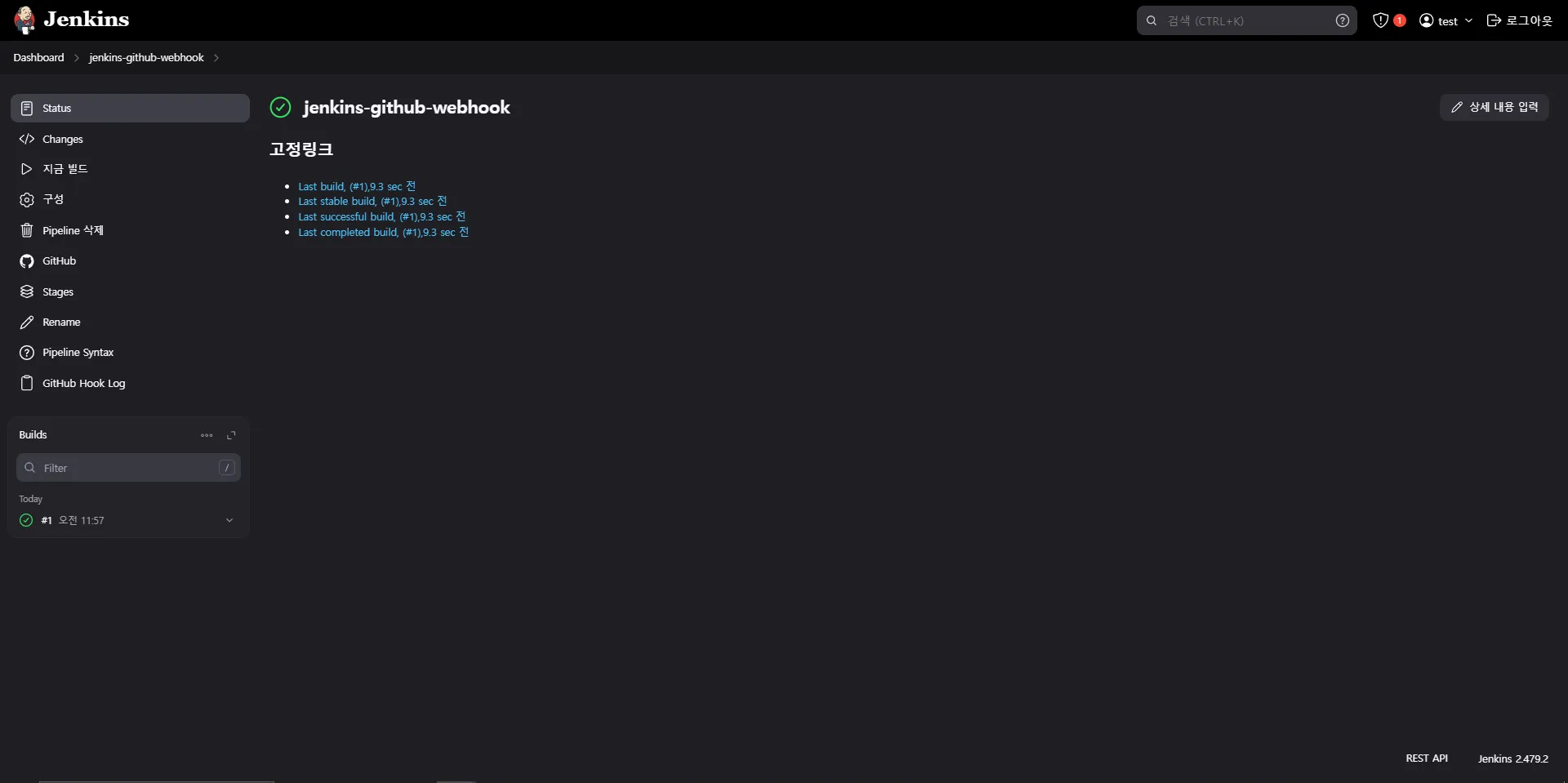
// URL을 본인의 github url로 변경해주시면 됩니다.

}

}

}

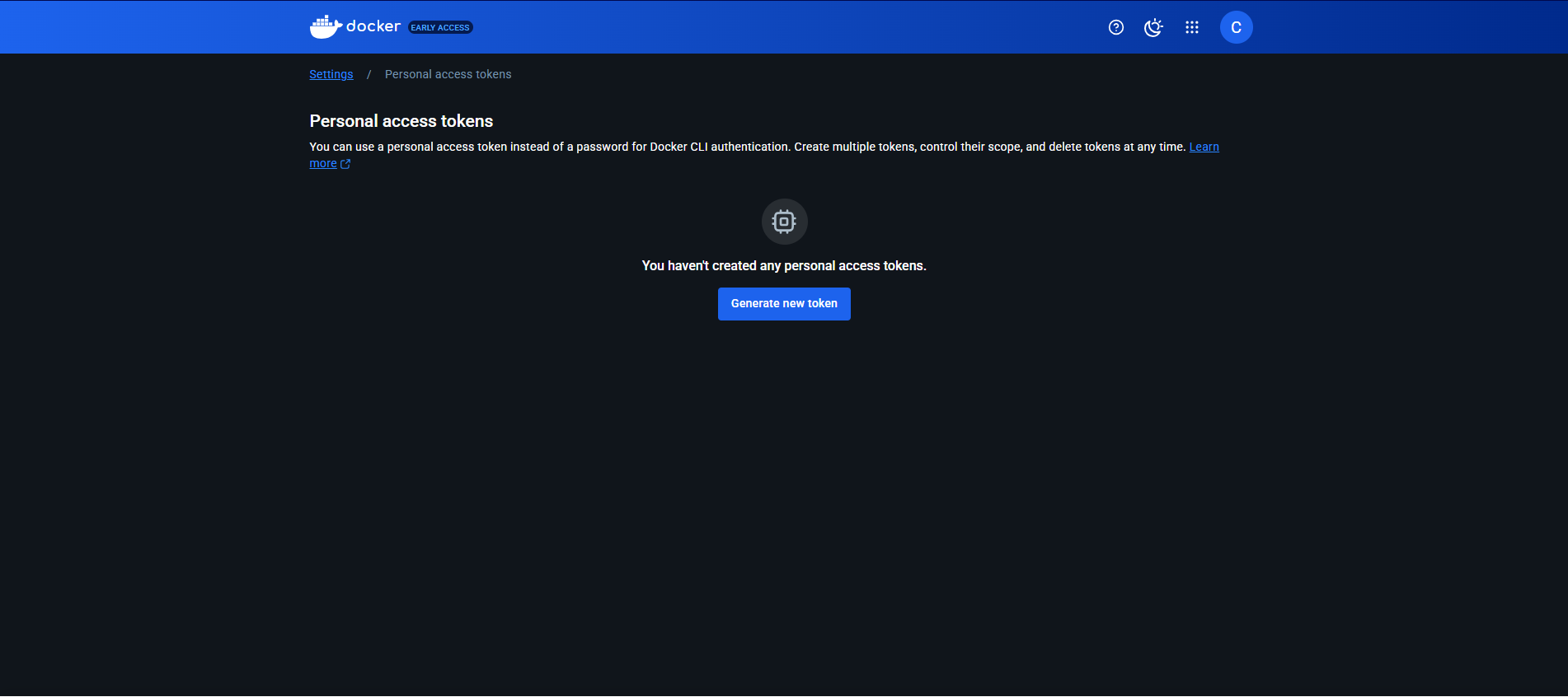
}



* 지금 빌드를 눌러 Jenkins와 Github의 연동 테스트

6) Docker Access token 생성

Profile 클릭 -> Account setting → Personal Access token → Generate new token



* Access token 생성

7) Jenkins pod에 Docker 설치 및 레지스터 설정

Powershell 관리자 권한 실행

# pod 상태 확인

kubectl get pods -o wide



* Jenkins의 IP 확인

# worker node2 접속

# worker node2의 이름은 따로 적으셔야 합니다.

kubectl exec -it jenkins-6b68fb88c9-6s9tf -- /bin/bash

* Jenkins pod에 접속

# 사전 패키지 설치

apt-get update

apt-get install -y apt-transport-https ca-certificates curl gnupg lsb-release

* Docker 설치에 필요한 패키지 설치

# Docker GPG 키 추가

curl -fsSL https://download.docker.com/linux/debian/gpg | gpg --dearmor -o /etc/apt/keyrings/docker.gpg

* Docker GPG 키 추가

# Debian Docker 저장소 추가

echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/debian bookworm stable" | tee /etc/apt/sources.list.d/docker.list > /dev/null

* Docker 저장소 추가

# 패키지 목록 업데이트

apt-get update

# Docker 설치

apt-get install -y docker-ce docker-ce-cli containerd.io

* Docker 설치

apt install -y vim

# 파일 열기

vi /etc/init.d/docker

# 62번째 줄을 찾아 다음과 같이 수정

# 기존: ulimit -Hn 524288

# 수정: ulimit -n 524288

# PowerShell로 하면 수정을 했을 때, 사라지는데 이는 배경색과 글자색이

# 같아져서 생기는 일이기에 걱정하지 않으셔도 됩니다.

ls -l /var/run/docker.sock

* Docker의 실행과 docker.sock의 생성 확인

docker run -d -p 5000:5000 --restart=always --name registry registry:2

* 레지스트리를 5000포트로 실행

# 본인의 Jenkins IP 입력 (포트 변경X)

mkdir -p /etc/docker

echo '{

"insecure-registries": ["10.244.6.2:5000"],

"storage-driver": "vfs"

}' > /etc/docker/daemon.json

* 레지스트리 설정

service docker restart

# 본인의 Jenkins IP 입력 (포트 변경X)

curl http://10.244.6.2:5000/v2/\_catalog

* 레지스트리 적용 여부 확인

# Docker 소켓 권한 설정

chmod 666 /var/run/docker.sock

* Docker 소켓 권한 설정

mkdir -p /etc/systemd/system/docker.service.d

vi /etc/systemd/system/docker.service.d/docker-options.conf

# 아래 내용 추가

# 본인의 Jenkins IP 입력 (포트 변경X)

--insecure-registry=10.244.4.2:5000

8) web workernode에 Docker 설치 및 레지스터 설정

Powershell 관리자 권한 실행

# worker 노드 접속

kubectl debug node/devsecops-cluster-worker -it --image=ubuntu -- chroot /host bash

* Worker node 접속

# 본인의 Jenkins IP 입력 (포트 변경X)

mkdir -p /etc/docker

echo '{

"insecure-registries": ["10.244.4.2:5000"],

"storage-driver": "vfs"

}' > /etc/docker/daemon.json

* Daemon 설정

# kubelet 설정

# 본인의 Jenkins IP 입력 (포트 변경X)

mkdir -p /etc/kubernetes/registries

echo '{

"apiVersion": "kubelet.config.k8s.io/v1",

"kind": "CredentialProviderConfig",

"providers": [{

"name": "registry-credentials",

"matchImages": ["10.244.4.2:5000/\*"],

"defaultCacheDuration": "12h"

}]

}' > /etc/kubernetes/registries/config.json

* Kubelet 설정

# 네트워크 설정

echo "NO\_PROXY=10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,.svc,localhost,127.0.0.1" >> /etc/environment

echo "no\_proxy=$NO\_PROXY" >> /etc/environment

* 네트워크 설정

mkdir -p /etc/containerd

# 본인의 Jenkins IP 입력 (포트 변경X)

cat > /etc/containerd/config.toml << EOF

version = 2

[plugins."io.containerd.grpc.v1.cri".registry]

[plugins."io.containerd.grpc.v1.cri".registry.mirrors]

[plugins."io.containerd.grpc.v1.cri".registry.mirrors."10.244.4.2:5000"]

endpoint = ["http://10.244.4.2:5000"]

[plugins."io.containerd.grpc.v1.cri".registry.configs]

[plugins."io.containerd.grpc.v1.cri".registry.configs."10.244.4.2:5000".tls]

insecure\_skip\_verify = true

EOF

* 레지스트리 endpoint 설정

# containerd 재시작

systemctl restart containerd

# worker 노드 접속

kubectl debug node/devsecops-cluster-worker -it --image=ubuntu -- chroot /host bash

# kubelet 재시작

systemctl restart kubelet

# worker 노드 접속

kubectl debug node/devsecops-cluster-worker -it --image=ubuntu -- chroot /host bash

# 본인의 Jenkins IP 입력 (포트 변경X)

curl <http://10.244.4.2:5000/v2/_catalog>

* Containerd, kubelet 재시작 및 설정 적용
* 레지스트리 확인

9) CI/CD Pipeline script 설정

pipeline {

agent any

tools {

maven 'Maven'

}

triggers {

githubPush()

}

stages {

stage('Checkout') {

steps {

git branch: 'main',

credentialsId: 'github\_access\_token',

url: 'https://github.com/jw3212/DevSecOps.Full-Project.git'

// 본인의 github URL 입력

}

}

stage('Install Dependencies') {

steps {

sh '''

curl -LO "https://dl.k8s.io/release/$(curl -L -s https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl"

chmod +x kubectl

mv kubectl /usr/local/bin/

# Docker 데몬 설정 (sudo 제거)

# 본인의 Jenkins IP 입력 (포트 변경X)

mkdir -p /etc/docker

echo '{

"insecure-registries": ["10.244.2.2:5000"],

"storage-driver": "vfs"

}' > /etc/docker/daemon.json

# Docker 소켓 권한 설정 (sudo 제거)

chmod 666 /var/run/docker.sock

'''

}

}

stage('SonarQube analysis') {

steps {

dir('web\_wargamer-master') {

withSonarQubeEnv('sonarqube-server') {

sh "mvn sonar:sonar \

-Dsonar.projectKey=test \

-Dsonar.host.url=http://192.168.1.3:30900/ \

-Dsonar.login=d2420266aa0ccade726b9c7ddeee326c8b2cafc0\

-Dsonar.sources=. \

-Dsonar.java.binaries=."

// SonarQube에서 얻은 Maven을 넣으면 됩니다.

}

}

}

}

stage('Build Docker Image') {

steps {

dir('web\_wargamer-master') {

sh """

# Docker 데몬 상태 확인

if ! docker info > /dev/null 2>&1; then

dockerd &

sleep 5

fi

# 이미지 빌드

docker build -t wargame-web:latest .

# 이미지 태그 및 푸시

# 본인의 Jenkins IP 입력 (포트 변경X)

docker tag wargame-web:latest 10.244.2.2:5000/wargame-web:latest

docker push 10.244.2.2:5000/wargame-web:latest

"""

}

}

}

stage('Create Registry Secret') {

steps {

sh """

# 본인의 Jenkins IP 입력 (포트 변경X)

# docker-username에는 자기 docker 계정이름 적기

# docker-password는 위에서 얻은 docker token 넣기

kubectl create secret docker-registry registry-secret \

--docker-server=10.244.2.2:5000 \

--docker-username=codepj \

--docker-password=dckr\_pat\_gWjzaJribM8rnxdhVfr2Jr6j8N4 \

--dry-run=client -o yaml | kubectl apply -f -

"""

}

}

stage('Deploy to Kubernetes') {

steps {

script {

// 기존 설정 적용

sh """

kubectl apply -f web\_wargamer-master/k8s/db-init-configmap.yaml

kubectl apply -f web\_wargamer-master/k8s/db-deployment.yaml

kubectl apply -f web\_wargamer-master/k8s/web-deployment.yaml

kubectl apply -f web\_wargamer-master/k8s/services.yaml

"""

// Deployment 롤링 업데이트 강제 실행

sh """

kubectl rollout restart deployment wargame-web

kubectl rollout status deployment wargame-web

"""

}

}

}

}

}

# 8. Wazuh

### 8.1 Wazuh 란?

**Wazuh**는 오픈소스 기반의 보안 플랫폼으로, **호스트 기반 침입 탐지 시스템(HIDS)** 역할을 수행하며, **위협 탐지, 규정 준수, 보안 모니터링**을 제공합니다. Wazuh는 에이전트와 서버, 대시보드로 구성되어 있으며, 클라우드 및 온프레미스 환경에서 모두 효율적으로 작동합니다.

### 8.2 Wazuh의 역할

DevSecOps 환경에서 Wazuh는 다음과 같은 주요 역할을 수행합니다:

* **보안 이벤트 모니터링:** 호스트와 컨테이너에서 발생하는 이벤트를 실시간으로 수집하고 분석하며, 로그, 시스템 호출, 네트워크 트래픽을 기반으로 위협을 탐지합니다.
* **취약점 관리:** 에이전트가 설치된 서버와 애플리케이션의 취약점을 스캔하며, 알려진 CVE(Common Vulnerabilities and Exposures)를 감지하고 경고를 제공합니다.
* **규정 준수 보고:** ISO 27001, GDPR, HIPAA 등 다양한 규정을 준수하는지 확인합니다.감사(Audit) 데이터를 수집하고 상세 보고서를 생성합니다.
* **파일 무결성 모니터링(FIM):** 중요한 파일 및 디렉토리의 변경 사항을 추적합니다. 예상치 못한 변경 감지 시 경고 알림을 보냅니다.
* **컨테이너 및 클라우드 보안:** Docker 및 Kubernetes와의 통합을 통해 컨테이너의 보안 상태를 점검합니다. 클라우드 환경(AWS, GCP, Azure)의 보안 설정을 검사합니다.
* **중앙 집중식 관리:** 모든 에이전트를 중앙에서 관리하며, 대시보드를 통해 전체 시스템 상태를 모니터링합니다.

### 8.3 Wazuh 사용계획 및 기대되는 이점

DevSecOps 환경에서 Wazuh 활용 방식은 다음과 같습니다.

1. **설치 및 배포**

* Kubernetes 클러스터 내에 Wazuh 서버 및 에이전트를 설치합니다.
* Docker를 활용하여 Wazuh 컨테이너를 배포하고 구성합니다.

2. **통합 및 모니터링**

* Jenkins, SonarQube, 애플리케이션 서버와 통합합니다.
* 시스템 및 애플리케이션 로그를 Wazuh로 전송하여 분석합니다.

3. **경고 및 보고**

* 보안 위협 감지 시 경고를 설정합니다.
* DevSecOps 파이프라인 단계별 보안 상태 리포트를 생성합니다.

4. **실시간 대시보드 활용**

* Kibana를 통해 실시간 보안 데이터 시각화합니다.
* 취약점 및 규정 준수 상태 확인합니다.

Wazuh는 다양한 플랫폼을 지원하며, Linux, Windows, macOS, Docker와 같은 환경에서 효과적으로 동작합니다. 수천 개의 노드에서도 원활히 작동할 수 있는 확장성을 제공하며, Slack, 이메일, 웹훅 등을 통한 알림 시스템을 갖추고 있습니다. 또한, ELK(Elasticsearch, Logstash, Kibana) 스택과의 통합을 통해 실시간 보안 데이터 시각화를 지원하며, 오픈소스 기반으로 무료로 사용이 가능합니다.

Wazuh를 사용함으로써 DevSecOps 환경에서 보안을 크게 강화할 수 있습니다. CI/CD 파이프라인 전체의 보안 상태를 실시간으로 모니터링하고, 취약점과 위협을 사전에 탐지 및 제거하여 보안 위험을 최소화합니다. 또한, ISO 27001, GDPR, HIPAA 등 다양한 규정 준수를 자동화된 방식으로 지원함으로써 감사 및 규정 준수 보고가 간소화됩니다. 중앙 집중식 관리 대시보드를 통해 모든 에이전트를 효율적으로 관리할 수 있어 운영 효율성도 향상됩니다.

Wazuh는 이러한 기능을 통해 DevSecOps 파이프라인 전반에서 신뢰성과 보안성을 확보하는 강력한 도구로 자리 잡습니다.

# 9. Web 구축

### 9.1. WebPage 소스코드

방법 1) 직접 생성

1. DevSecOps폴더에 Web폴더 생성 후, 웹 소스코드 복사

Practice Web Source code: [DevSecOps Team Web Source code](https://github.com/GH6679/web_wargamer)

2. Github의 특수문자를 허용하기 위한 설정

Window PowerShell 관리자 권한 실행

# DevSecOps\Web폴더로 이동

1. cd C:\Users\Administrator\Desktop\DevSecOps\Web

# Github 특수문자 허용

2. git config core.protectNTFS false

3. DevSecOps폴더에 k8s-yaml 폴더 생성

방법 2) Window PowerShell 사용

Window PowerShell 관리자 권한 실행

# DevSecOps폴더 이동

1. cd C:\Users\Administrator\Desktop\DevSecOps

# 소스코드 클론

2. git clone <https://github.com/GH6679/web_wargamer.git>

3. cd web\_wargamer

# 깃허브 안에 있는 특수문자들 허용으로 설정

4. git config core.protectNTFS false

5. cd ..

# k8s-yaml 디렉토리 생성

6. mkdir k8s-yaml

### 9.2. Web worker node 생성

1) web-deployment.yaml 생성

web-deployment.yaml 파일은 웹 worker node 설정 파일이다.

k8s-yaml 폴더에 web-deployment.yaml 파일 생성 후, 아래 코드 작성

apiVersion: apps/v1

kind: Deployment

metadata:

name: wargame-web

spec:

selector:

matchLabels:

app: wargame-web

template:

metadata:

labels:

app: wargame-web

node-type: webserver

spec:

nodeSelector:

node-type: webserver

containers:

- name: wargame-web

image: wargame-web:latest

imagePullPolicy: Never

ports:

- containerPort: 80

env:

- name: DB\_HOST

value: "wargame-db-service"

- name: DB\_PORT

value: "3307"

- name: DB\_DATABASE

value: "LED\_WG"

- name: DB\_USERNAME

value: "root"

- name: DB\_PASSWORD

value: "1234"

volumeMounts:

- name: web-storage

mountPath: /var/www/html

resources:

limits:

memory: "512Mi"

cpu: "500m"

requests:

memory: "256Mi"

cpu: "250m"

volumes:

- name: web-storage

persistentVolumeClaim:

claimName: web-pvc

2) db-deployment.yaml 생성

db-deployment.yaml 파일은 웹 데이터베이스 worker node 설정 파일이다.

k8s-yaml 폴더에 db-deployment.yaml 파일 생성 후, 아래 코드 작성

apiVersion: apps/v1

kind: Deployment

metadata:

name: wargame-db

spec:

selector:

matchLabels:

app: wargame-db

template:

metadata:

labels:

app: wargame-db

node-type: web-db

spec:

nodeSelector:

node-type: web-db

containers:

- name: mariadb

image: mariadb:latest

resources:

limits:

memory: "512Mi"

cpu: "500m"

ports:

- containerPort: 3306

env:

- name: MYSQL\_ROOT\_PASSWORD

value: "1234"

- name: MYSQL\_DATABASE

value: "LED\_WG"

- name: MYSQL\_ALLOW\_EMPTY\_PASSWORD

value: "no"

- name: MYSQL\_ROOT\_HOST

value: "%"

- name: MARIADB\_MYSQL\_LOCALHOST\_USER

value: "1"

- name: MARIADB\_MYSQL\_LOCALHOST\_GRANTS

value: "ALL"

volumeMounts:

- name: mariadb-storage

mountPath: /var/lib/mysql

- name: mariadb-backup

mountPath: /backup

volumes:

- name: mariadb-storage

persistentVolumeClaim:

claimName: mariadb-pvc

- name: mariadb-backup

persistentVolumeClaim:

claimName: mariadb-backup-pvc

3) db-init-configmap.yaml 생성

db-init-configmap.yaml 파일은 웹 데이터베이스 worker node의 초기화 설정 파일이다.

k8s-yaml 폴더에 db-init-configmap.yaml 파일 생성 후, 아래 코드 작성

apiVersion: v1

kind: ConfigMap

metadata:

name: mariadb-init

data:

init.sql: |

USE LED\_WG;

CREATE TABLE IF NOT EXISTS users (

u\_id INT NOT NULL AUTO\_INCREMENT,

nickname VARCHAR(50) NOT NULL,

username VARCHAR(50) NOT NULL,

password VARCHAR(50) NOT NULL,

email VARCHAR(50) NOT NULL,

user\_role VARCHAR(50) NOT NULL,

PRIMARY KEY (u\_id)

);

CREATE TABLE IF NOT EXISTS challenges\_data (

c\_id INT NOT NULL AUTO\_INCREMENT,

c\_title VARCHAR(50) NOT NULL,

c\_ssh VARCHAR(50),

c\_web TINYINT(1) NOT NULL,

c\_link VARCHAR(50),

c\_hint TEXT,

c\_point int,

c\_difficulty VARCHAR(50),

c\_key VARCHAR(50),

c\_text TEXT,

c\_solves int,

PRIMARY KEY (c\_id)

);

CREATE TABLE IF NOT EXISTS user\_data (

d\_id INT NOT NULL AUTO\_INCREMENT,

d\_uid INT,

d\_cid INT,

d\_time datetime,

PRIMARY KEY (d\_id),

FOREIGN KEY (d\_uid) REFERENCES users(u\_id) ON DELETE CASCADE ON UPDATE CASCADE,

FOREIGN KEY (d\_cid) REFERENCES challenges\_data(c\_id) ON DELETE CASCADE ON UPDATE CASCADE);

4) service.yaml 생성

service.yaml 파일은 웹과 데이터베이스의 연동을 위한 설정 파일이다.

k8s-yaml 폴더에 service.yaml 파일 생성 후, 아래 코드 작성

apiVersion: v1

kind: Service

metadata:

name: wargame-web-service

spec:

type: NodePort

ports:

- port: 80

targetPort: 80

nodePort: 30080

selector:

app: wargame-web

---

apiVersion: v1

kind: Service

metadata:

name: wargame-db-service

spec:

type: ClusterIP

ports:

- port: 3306

targetPort: 3306

protocol: TCP

selector:

app: wargame-db

### 9.3 Web worker node 실행

1) 클러스터 삭제 및 kind 클러스터 생성

Window PowerShell 관리자 권한 실행

# DevSecOps폴더로 이동

1. cd C:\Users\Administrator\Desktop\DevSecOps

# 클러스터 삭제 명령어

2. kind delete cluster --name devsecops-cluster

3. kind delete clusters -–all

# kind 클러스터 생성

4. kind create cluster --name devsecops-cluster --config k8s-yaml/kind-config.yaml

# 노드 상태 확인

5. kubectl get nodes --show-labels

Web 이미지 빌드 및 kind 클러스터로 로드

# 웹 애플리케이션 이미지 빌드

1. docker build -t wargame-web:latest .

# 빌드된 이미지를 kind 클러스터로 로드

2. kind load docker-image wargame-web:latest --name devsecops-cluster

디플로이먼트와 서비스 배포

# deployment, service yaml 파일 배포

1. kubectl apply -f k8s-yaml/db-deployment.yaml

2. kubectl apply -f k8s-yaml/web-deployment.yaml

3. kubectl apply -f k8s-yaml/services.yaml

# 배포 상태 확인

4. kubectl get pods -o wide

5. kubectl get services

2) 웹 페이지 접속

browser 주소창: localhost:30080 or <http://Windows> Host IP:30080