

Utilisation de Trivy

⚠ Pré-requis. Ce sujet nécessite les sujets :

- Docker
- Docker 2
- Docker compose

1 Introduction

i Trivy. Avec les conteneurs nous pouvons facilement de nombreux outils qui, chacun, est susceptible d'avoir des failles de sécurité. Afin de faciliter l'audit et la vérification de ces composants, nous allons utiliser Trivy.

2 Installation

- Installez Trivy en suivant cette documentation.
- Utilisez Trivy pour vérifier l'image d'Alma Linux (il devrait y avoir des alertes) :

```
trivy image almalinux
```

- Construisez une image `alma-updated` qui est une `almalinux` mise à jour (il faut, un répertoire, un `dockerfile` et un `docker build`).
- Vérifiez que dans cette dernière version, les failles sont corrigées.

3 Catastrophe !

- Utilisez Trivy pour vérifier l'image `my-app`.

i Note : Vous devriez trouver des failles de sécurité qui touchent, Alma Linux, Tomcat, Sprint-Boot ainsi que les drivers JDBC utilisés. Bref, nous avons du travail.