# VPS & Docker

## Risques encourus

*Ils existent de nombreux risques. Les principaux risques portent sur la confidentialité, la disponibilité et l'intégrité. Voici quelques-un des risques auxquels nous pouvons être exposé et donc par la suite, pouvoir nous en protéger.*

- *Infiltration dans nos VPS,*
- *Attaque de type dos (denial-of-service attack),*
- *Fishing,*
- *Authentification par Brutforce,*
- *Sniffing de données.*

*Nos services doivent aussi être opérationnels 24 heures sur 24. Ce qui veut dire que nos serveurs doivent être à tous prix protégés de tout type de problème physique, aussi bien une panne électrique qu'une panne du matériel.*

### Par le VPS

Nous avons commencé par changer le mot de passe d'accès à nos VPS. Nous avons ensuite sécurisé l'accès à notre VPS avec SSH. Cet accès est sécurisé car il utilise une clé unique par machine pouvant se connecter. En plus de cette clé, il faut entrer une pass-phrase pour pouvoir s'y connecter.

## Contre-mesures mises en place

Nous avons mis en place l'authentification par clé et, par conséquent, désactivé l'authentification par mot de passe. De plus, le compte `root` à eu un changement de mot de passe par un nouveau à chiffrement fort. Depuis la mise en place de la connexion par clé, le compte `root` n'est plus accessible de manière externe.

*Nous avons également mis en place `fail2ban` qui empêche toute tentative d'attaque DOS. Cette sécurité va bannir une adresse IP lorsque celle-ci réalise trop de tentatives de connexion refusées. La règle utilisée est de 10 tentatives en 2 minutes maximum, 20 minutes de bannissement de l'adresse IP. De plus, la protection contre l'attaque DDOS et la récidive est également suivie par `fail2ban`.*

# Services

## Risques encourus

### Par chacun des services déployés

### Au niveau intégrité

### Au niveau confidentialité

### Au niveau disponibilité du service

## Contre-mesures

### Proposition

### Mise en place