

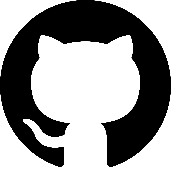
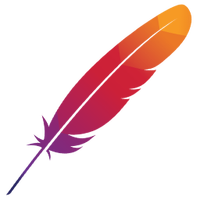
Rapport **technique**

***Module 1*** : Mise en place d’une infrastructure DNS et Web

Par :

PERSYN Loïc – ROSAR Nicolas – VANKEERBERGHEN Jordan

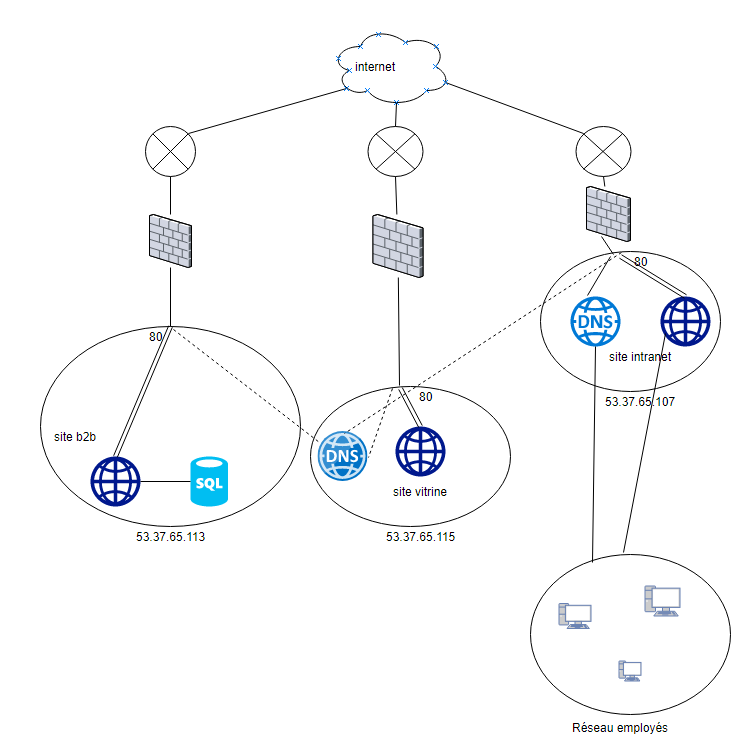




Date de remise : 27-04-2018

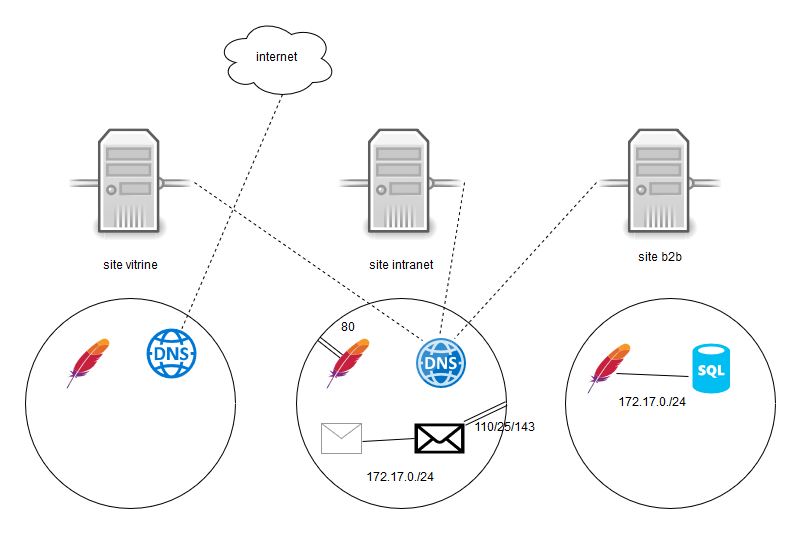
1. Schémas réseau

# Schéma logique



Notre implémentation est composée de 3 sites web placé chacun sur un VPS différent qui possèdent donc une adresse IP différente. La base de données mySQL qui ne communique qu’avec le site b2b est située dans le VPS avec ce site. Le serveur DNS renvoie vers les différents VPS correspondant à la demande. Il possède le NS avec le glue record et toute demande faite à wt3.ephec-ti.be renverra sur ce serveur DNS qui, lui renverra vers le bon VPS.  
Le dernier VPS possède le site intranet et le résolveur qui sont accessible de l’intérieur par les employés.

# Schéma physique



Dans notre premier VPS nous avons le site vitrine accessible via le DNS se trouvant dans le second VPS. Dans le deuxième VPS nous avons le site intranet accessible seulement par les employés (restriction gérée au niveau du DNS). Nous avons les services mail **Dovecot** et **Postfix** (pas encore implémentés a 100%) qui communiqueront via les port 143, 110 et 25. Dans ce VPS nous avons aussi le DNS qui redirige les requêtes en fonction de l’adresse demandée. Dans le dernier VPS nous avons le site b2b avec la base de données qui communique via le réseau privé de Docker.

1. Problèmes rencontrés

# Symptômes

1. Problèmes de compréhension pour la mise en place du DNS.
2. Impossibilité de créer de nouveaux volumes. La commande de création fonctionne mais l’emplacement (trouvé avec volume *inspect*) dans lequel celui-ci est supposé se trouvé est vide.
3. Fail2ban (voir point V) dans « 3.1 VPS ».

# Causes

2.2.1 x

2.2.2 Probablement une mauvaise manipulation.

2.2.3 Inconnues

1. Sécurité et mise en place

# VPS

Afin de garantir un maximum la sécurité de notre VPS, voici la procédure que nous avons suivi :

1. Nous avons créé un user personnel pour notre utilisation ainsi qu’un user *vvandens* pour le professeur ;
2. Utilisation de la cryptographie asymétrique pour l’authentification. Dépôt de chaque clé publique dans les VPS correspondants. Concrètement la clé publique *vvandens.pub* a été ajoutée au fichier *authorized\_keys* dans le VPS attribué à l’user *vvandens*. La même manipulation a été réalisée pour ajouter notre clé publique dans note compte VPS personnel. Cela dans le but d’authentifier le compte qui veut se connecter au VPS par une comparaison entre la clé privée de l’user et la clé publique présente sur le VPS
3. Suppression de l’accès SSH au compte root car il est le premier ciblé par les attaques du fait qu’il possède tous les droits d’administration sur le serveur en question ;
4. Installation de Fail2Ban afin de prévenir des intrusions dans notre VPS. *Fail2ban* lit les logs de divers services tels que SSH, Apache, FTP… à la recherche d’erreurs d'authentification répétées et ajoute une règle [bien](https://doc.ubuntu-fr.org/iptables) spécifique pour bannir l'adresse IP de la source.
5. Fail2ban :

Problème rencontré lors de l’installation sur le VPS de Loïc. Celui-ci a été banni automatiquement.

# Services

## 3.2.1 Web

## 3.2.2 MySQL

## 3.3.3 DNS (non terminé)

1. Validation du déploiement

Nous allons utiliser la stratégie dite du « pilote ». Cela signifie que nous le mettrons en place seulement sur une zone géographique, pour notre unique. Grâce à cette méthode nous allons pouvoir valider et approuver l’ensemble des processus à mettre en place. Une fois que tout est validé, on peut lancer le déploiement pour plusieurs entités.

1. Monitoring

On pourrait mettre en place un MRTG (Multi Router Traffic Grapher) qui va nous permettre de récupérer des informations sur le trafic dans le réseau. Il utilise un protocole bien précis qu’est le SNMP pour interroger des équipements comme des routeurs, switchs ou serveurs.

Une autre solution serait d’utiliser les services de monitoring proposés par OVH. Ils vont vérifier l’état du serveur ainsi que le bon fonctionnement des applications de notre serveur.