Projet Admin

Rapports

2TL1-10

Rapport client

Cahier des charges

L'entreprise souhaite remplacer ses serveurs vieillissants, et fait appel à nous pour la phase de conception et de validation d'une nouvelle infrastructure d'hébergement des services informatiques. L'entreprise a besoin de deux sites externes www.wt2TL1-10.ephec-ti.be et b2b.woodytoys.be joignable par les clients. D'un site interne pour tous les membres de l'entreprise. De plus, chaque membre de l'entreprise doit avoir sa propre adresse email. Le réseau téléphonique doit être géré par téléphonie IP.

Traduction des besoins

En clair, il faut que nous mettions en place ceci :

- Des serveurs web
- Une base de données
- Des serveurs dns
- Un serveur mail
- Un serveur de téléphonie IP

Propositions

Pour répondre aux attentes du client, nous proposons de mettre en place ceci :

- Un serveur apache joignable de l'extérieur, contenant le contenu html du site.
- Un serveur dns joignable de l'extérieur gérant le nom de domaine wt2TL1-10.ephec-ti.be et connaissant l'adresse ip de serveur apache externe.
- Un serveur apache joignable que par les machines internes à l'entreprise contenant le contenu html du site interne.
- Un serveur dns joignable que par les machines internes à l'entreprise gérant le nom de domaine b2b.woodytoys.be .
- Un résolveur DNS unbound
- Mail
- voip

Justification

En ce qui concerne les serveurs web, nous avons choisi Apache. Apache est le serveur web le plus utilisé et aussi le plus facile à mettre en place. Nous justifions les trois serveurs webs par le fait que deux d'entre eux doit être joignable de l'extérieur et un de l'intérieur, de ce fait nous préférons les trois pour des raisons de sécurité.

Pour ce qui est des services dns, nous avons choisi bind car comme apache il s'agit du plus utilisé et du plus facile à mettre en place. Nous avons choisi de diviser les serveurs dns en trois différents, un interne qui n'a besoin que d'être joignable depuis l'intérieur, un externe qui lui doit pouvoir être joignable depuis l'extérieur, et un résolveur joignable depuis les machines internes. Nous avons choisi ce système là pour des raisons de sécurité, ne pas laisser des serveurs internes être joignable de l'extérieur.

Besoins en maintenances

Serveurs déployés

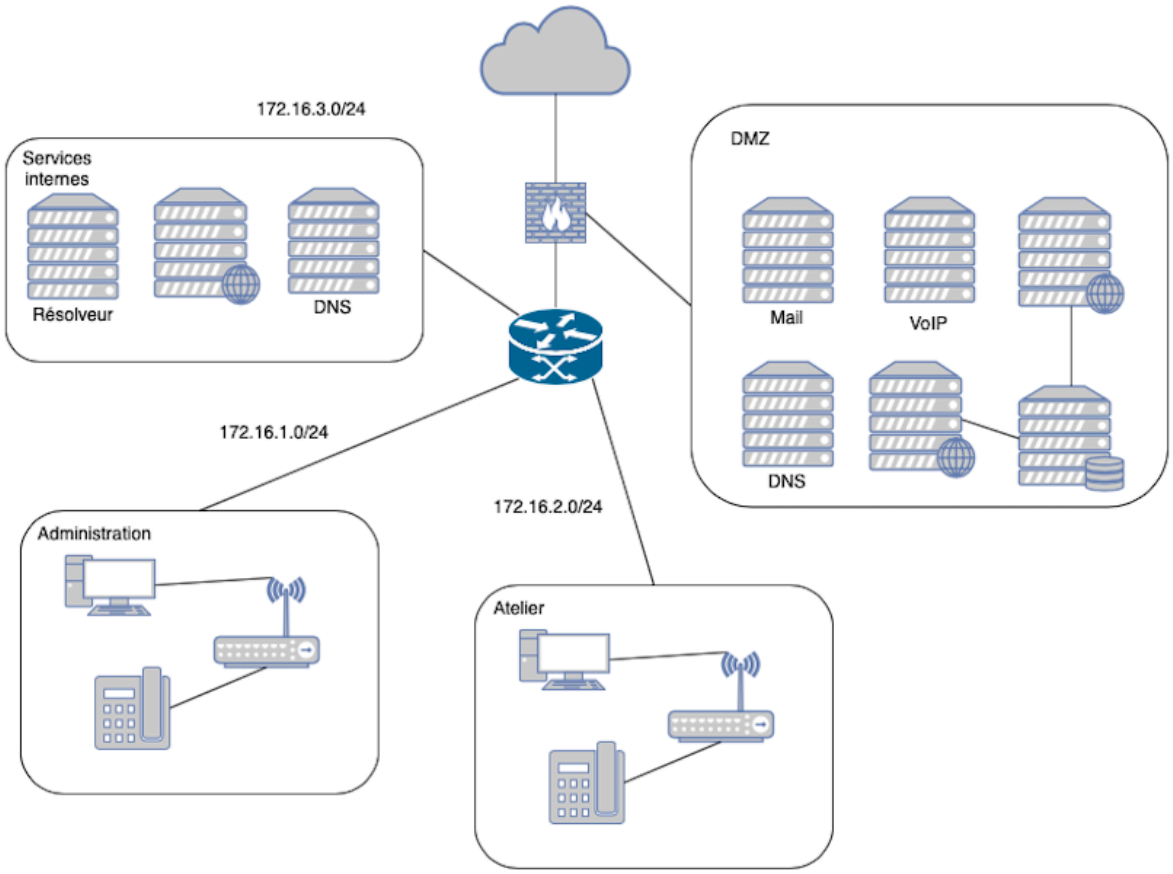
A ce stade, nous n'avons déployé que les trois serveurs web, le serveur web interne et le serveur web externe. Les serveurs dns et mail sont toujours en cours de testing.

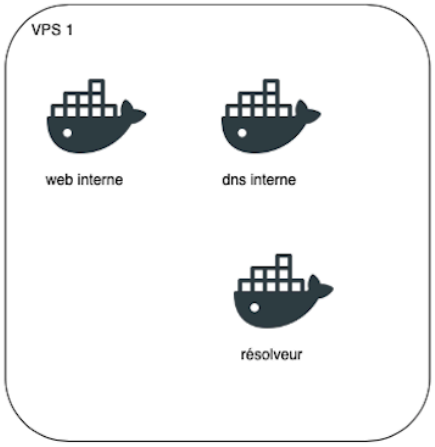
Temps estimé

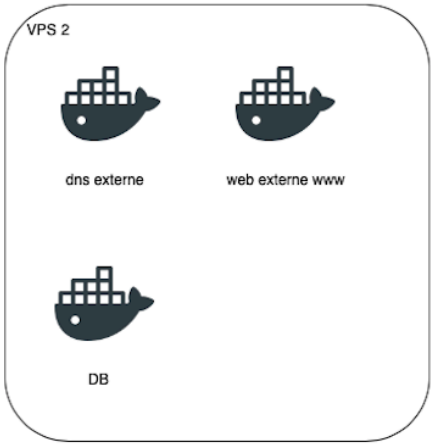
Les serveurs dns devraient être déployé d'ici une semaine, le mail et voIp quant à eux prendront un peu plus de temps.

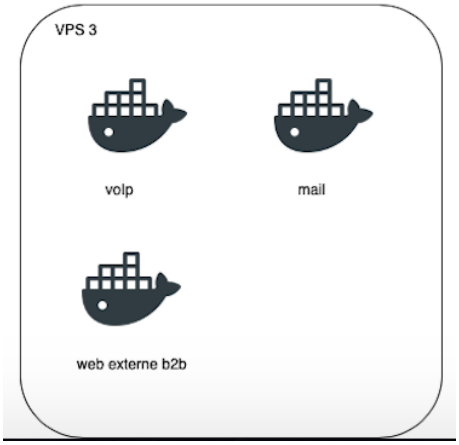
2TL1-10

Schémas









2TL1-10

Analyse de sécurité

Vps et docker

Tous d'abord les risques encourus quand nous nous connectons par mot de passe à nos vps sont simples, si quelqu'un arrive à intercepter la communication, il pourra lire notre mot de passe et donc prendre possession de notre vps. De plus, il est important de ne pas mettre des containers docker accessibles depuis l'extérieur sur le même vps que des containeurs qui gérent l'interne. En effet, les serveurs en liens avec l'extérieur sont plus susceptibles de se faire pirater et donc pourrait donner des informations internes à l'entreprise.

Solutions

Pour la connexion au vps nous allons nous connecter qu'une seule fois par mot de passe et ensuite utiliser la connexion par clé partagée. En effet, nous allons créer 4 utilisateurs sur chaque vps, et partager une clé pour chaque utilisateur. Grâce à cela seul les utilisateurs ayant la clé pourront se connecter au vps et le trafic sera chiffré.

Pour la répartition des containeurs, nous avons séparé les serveurs externes et les serveurs internes.

Risques

Web interne

D'autres utilisateurs externes puissent avoir accès.

Dns interne :

D'autres utilisateurs externes puissent faire des requêtes dessus.

Solutions

Web interne

Lui donner grâce à la commande « Require » la liste des adresses ip qui sont autorisées.

Dns interne

Modifier le fichier named.conf.options et ajouter allow-query{#ip} pour n'autoriser que les requêtes venant de ces adresses ip.

2TL1-10

Rapport technique

Groupe

Groupe 2TL1-10. Membre : DELESTIENNE Damien, SALPIETRO Florence, SERVAIS Léon

Damien : Pour cette partie, j'ai mis en place les deux serveurs web, interne et externe. De plus, j'ai travaillé sur les deux serveurs dns qui sont presques opérationnels mais il faut encore les déployer sur le vps pour pouvoir les tester.

Léon : Début de la configuration du serveur mail.

Méthodologie

Pour travailler sur ce projet, nous travaillons de la sorte :

Tout d'abord prise de connaissance de la tâche à réaliser, des adresses ip, des pages web, etc.. Après cela, nous essayons de mettre en place notre serveur sur une vm ubuntu et de rendre ce serveur opérationnel et respectant les conditions. Une fois cette étape franchie, nous réalisons le docker file et construisons l'image docker qui va avec pour après faire tourner le container docker sur base de cette image.

Avancement

A l'état actuel des choses, seul les serveur web fonctionnent comme il faut. Les trois serveurs dns ont été configurer mais nous devons encore les tester avec le vps et avec des requêtes dig. La configuration du serveur mail est en cours.

Justification schémas

Tout d'abord pour le schéma logique, nous avons préféré le séparer en trois parties :

Une partie DMZ qui reprend tous les serveurs qui seront joignables depuis l'extérieur. Cela comprend : les webs externes, la db, le dns externe, le mail, le voip. Nous avons préféré isoler les services joignables depuis l'extérieur pour éviter que quelqu'un de l'extérieur puisse accéder à un service interne à l'entreprise.

Une partie service interne qui reprend tous les serveurs joignables par les machines interne à l'entreprise et donc : le web interne, le dns interne, le résolveur. En mettant les services internes entre eux nous nous assurons qu'ils ne seront pas joignables de l'extérieur mais que par les machines internes.

Une partie terminaux, qui elle, comprend toutes les machines internes à l'entreprise.

Pour ce qui est du schéma physique, nous avons décidé de séparer les services de manière équivalente pour s'assurer une vitesse de travail correcte de la part de nos serveurs. Le seul choix logique a été de séparer les 3 serveurs dns pour que chaque vps puisse être joignable sur le port 53(udp). Pareil pour les serveurs web qui eux sont pour l'instant sur le port 80.

Adressage

Nous avons choisi de diviser l'entreprise et ses terminaux en trois parties : les serveurs internes, l'atelier et l'administration. Pour ces trois parties, nous leur avons attribués un sous réseaux d'adresses privées de classe b : 172.16.1.0/24 172.16.2.0/24 172.16.3.0/24

Problèmes rencontrés

- Gérer l'accès au web interne
- Tester les serveurs dns

Changements apportés

- Ajuster le schéma logique : rajouter des liens, rajouter un deuxième web externe, mettre la dmz en lien direct avec le firewall, rajouter l'adresse ip des serveurs internes.
- Ajuster le schéma physique : rajouter deux containers docker, un pour le deuxième web externe et un pour la db.
- Ajuster l'orthographe et la ponctuation.
- Rajouter les parties concernant notre avancement.