WoodyToys - Rapport technique

EPHEC - Groupe 13

Melvin Campos Casares, Guillaume Vanden Herrewegen,
Hubert Van De Walle

6 juin 2019

Rapport technique

1. Informations sur le groupe

Numéro de groupe : **13**

Noms des membres :

- Melvin Campos Casares
- Guillaume Vanden Herrewegen
- Hubert Van De Walle

1.1. Etudiant responsable par mission

- **Partie DNS & Web :** Melvin Campos Casares
- **Partie Mail :** Guillaume Vanden Herrewegen
- **Partie VoIP :** Hubert Van De Walle

1.1.1. Bilan pour la mission DNS & Web (Melvin Campos Casares)

Le bilan pour la mission DNS & Web est relativement simple. En l'état actuel, rien n'a encore été concrètement mis en place avec Docker. Néansmoins, les premiers tests ont permis de rendre accessible de manière publique un site internet par simple appel de l'adresse IP dans un navigateur web.

Guillaume à pris en charge la construction de la partie DNS tandis que Hubert et moi-même prenions en mains la partie web.

Chacun à suivi une méthodologie identique et mis en commun concernant la sécurisation de nos VPS :

- connexion par clés SSH,
- mise à jour des VPS,
- mise en place de `fail2ban` ainsi que sa configuration,
- ajout de certaines fonctionnalités. Exemple : `fish`, un shell dont Hubert et Melvin sont fort habitué (système de prédictions, alias supportant des fonctions, etc.) et `tldr`, un man simplifié.

1.1.2. Bilan pour la mission Mail (Guillaume Vanden Herrewegen)

Nous avons continué à mettre en place le DNS et la partie web sans pour autant arriver à un résultat final. De plus, une première réflexion à été faite concernant la partie mail mais qui n'a pas encore abouti étant donné la priorité sur les DNS et web.

1.1.3. Bilan pour la mission VoIP (Hubert Van De Walle)

Nous avons fini la mise en place du DNS et avançons de bon train sur la partie web ainsi que la partie mail. Melvin à pris en charge le développement de la partie VoIP afin que nous puissions rattraper notre retard. Globalement parlant, les parties principales sont faites et beaucoup de choses sont presques finies; il ne reste que certains détails à finir afin d'achever DNS, Web et Mail.

1.1.4. Bilan final (groupe entier)

Nous avons su avancer de bon train et avons réussi à mettre intégralement en place les services DNS, Web, Base de données et Mail. Concernant le service VoIP, une partie est fonctionnelle mais au vu des soucis rencontrés, un développement supplémentaire est requi afin de le finaliser.

De plus, l'intégration du certificat SSL pour le protocole HTTPS à été mis en place. Nous utilisons Let's Encrypt et plus précisément le certificat SAN afin de déployer un certificat sur plusieurs sites internet d'un même domaine principal. Malheureusement, suite à de multiples essais pendant la création, nous avons atteint la limite des certificats disponible pendant une période d'une semaine et nous devons attendre encore quelques jours avant de pouvoir en obtenir un à nouveau. Dans le rapport d'analyse de sécurité, une image à été incluse afin de montrer le bon fonctionnement du protocole HTTPS avant les problèmes rencontrés et cité ci-dessus.

2. Méthodologie

Nous avons commencé par lire la documentation des outils Docker et commencer quelques tests afin de pouvoir mieux comprendre son fonctionnement.

La modélisation du schéma réseau à été réalisée par Guillaume Vanden Herrewegen, tout comme le début du Wiki du repository GitHub.

Nous avons choisi d'utiliser l'application **Signal** disponible gratuitement sur tout OS confondu afin de pouvoir discuter entre membres du groupe de façon plus aisée et plus rapide tout en ayant une sécurité accrue en comparaison d'autres systèmes de discussion en ligne.

Concernant la répartition des tâches, une communication entre les différents membres du groupe ainsi que l'utilisation d'un Trello privé et accessible par les différents membres à été mis en place. Des échéances ont été mis en place et nous tentons des les respecter. De plus, lorsque nous rencontrons un problème, nous les transmettons aux autres membres afin qu'une réflexion générale puisse être faite et possiblement trouver une solution de manière plus rapide.

3. Etat d'avancement

La modélisation du schéma réseau à été réalisée par Guillaume Vanden Herrewegen, tout comme le début du Wiki du repository GitHub.

Hubert et Melvin sont en charge de la partie web qui est achevé. Guillaume est en charge de la partie DNS qui, techniquement parlant, devrait être fonctionnel mais qui ne l'est pas totalement en pratique (intranet). Guillaume est également en charge de la partie Mail qui est achevé. Melvin est en charge de la partie VoIP qui concrètement parlant, ne fonctionne que partiellement. Melvin supervisait également les modifications à faire sur les différents rapports.

4. Schéma réseau et justification des choix

Schéma logique du réseau :

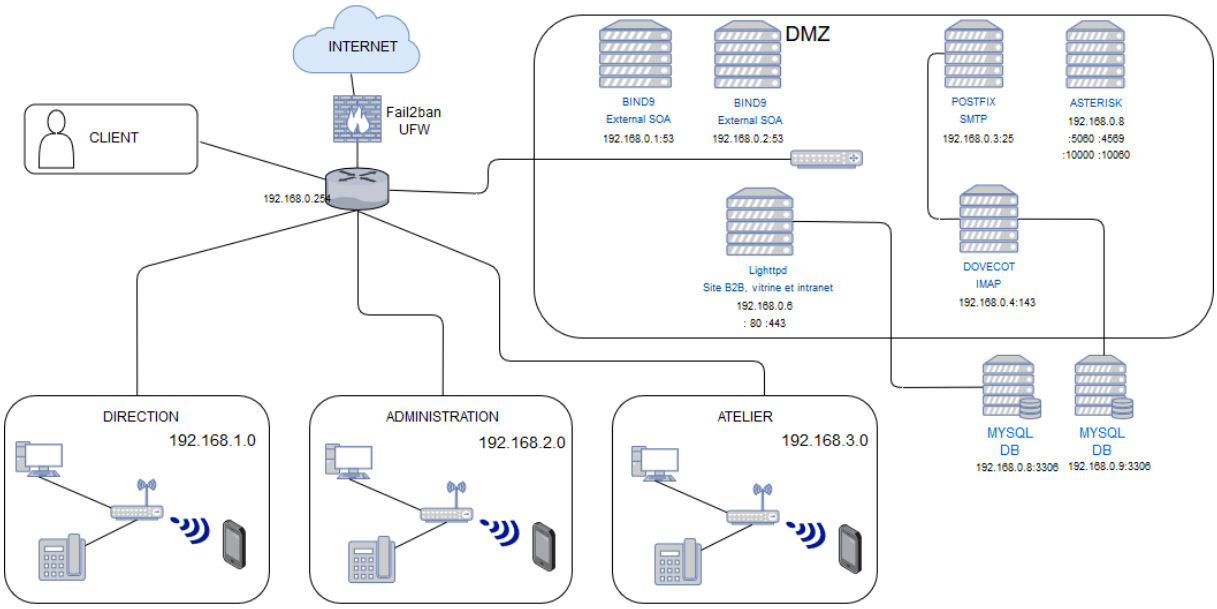

Figure 1: Schéma logique du réseau

Schéma physique du réseau :

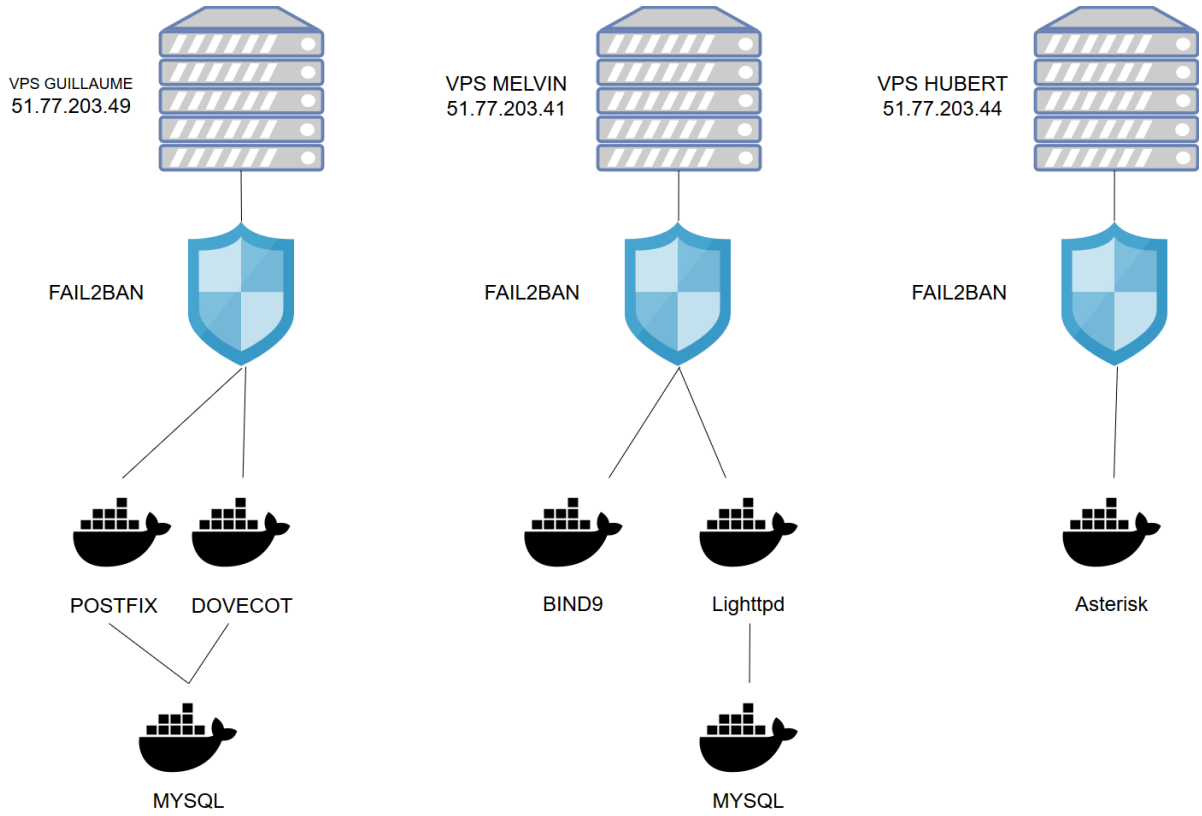

Figure 2: Schéma physique du réseau

4.1. Plans d'adressages

4.1.1. Plan d'adressage de Postfix (Mail)

Voici le plan d'adressage pour la partie mail :

Nom	Service	Adresse e-mail
Guillaume	Compte test	guillaume@wt13.ephec-ti.be
Contact WoodyToys	Contact	contact@wt13.ephec-ti.be
Direction WoodyToys	Direction	direction@wt13.ephec-ti.be
Secrétariat WoodyToys	Direction	secretariat@wt13.ephec-ti.be
Atelier WoodyToys	Ouvrier	atelier@wt13.ephec-ti.be
Hangar WoodyToys	Ouvrier	hangar@wt13.ephec-ti.be
Michel Roux	Comptabilité	m.roux@wt13.ephec-ti.be

Nom	Service	Adresse e-mail
Christine Garcia	Comptabilité	c.garcia@wt13.ephec-ti.be
Service commercial	Vente	service-commercial@wt13.ephec-ti.be
Hubert Van De Walle	Vente	h.vandewalle@wt13.ephec-ti.be
Guillaume Vanden Herrewegen	Vente	g.vandenherrewegen@wt13.ephec-ti.be
Melvin Campos Casares	Vente	m.camposcasares@wt13.ephec-ti.be
John Doe	Vente	j.doe@wt13.ephec-ti.be
Albert Dupont	Vente	a.dupont@wt13.ephec-ti.be

4.1.2. Plan d'adressage et de numérotation d'Asterisk (VoIP)

Voici le plan d'adressage pour la partie Voice-Over IP :

- L'adresse IP externe est celle du VPS sur lequel le Docker est lancé,
- L'adresse IP interne est `0.0.0.0` (afin de pointer sa propre adresse interne) et son masque de sous-réseau est `255.255.0.0`.

Voici le plan de numérotation :

- **1230 :** VoiceMail WoodyToys
- **301 :** Direction
- **302 :** Secrétariat
- **Ouvriers :**
  - **311 :** Atelier
  - **312 :** Hangar
- **Service comptabilité :**
  - **321 :** Michel Roux
  - **322 :** Christin Garcia
- **Commerciaux :**
  - **331 :** Service Commercial
  - **332 :** Hubert Van De Walle
  - **333 :** Guillaume Vanden Herrewegen
  - **334 :** Melvin Campos Casares

- **335 :** John Doe
- **336 :** Albert Dupont

Il est bien entendu possible de créer de nouveaux utilisateurs dans le service comptabilité ainsi que pour les commerciaux. Dans la configuration du DialPlan, il a été pensé de créer des numéros de 300 à 399 inclus.

De plus, lorsque le service commercial, le service comptabilité et les ouvriers tentent de joindre qui que ce soit dans la zone 300 à 309, ils sont automatiquement redirigé vers le secrétariat.

5. Difficultées

5.1. Problèmes rencontrés

5.1.1. Protection du VPS (résolu)

La mise en place de clés SSH en cryptage élevé pour chacun des membres à été implémenté.

Le compte `root` à été désactivé suite au retrait de connexion par mot de passe même si nous l'avions déjà au préalable modifié afin de mettre en place un mot de passe à chiffrement fort.

La clé SSH du compte `vvandens` à été implémentée avec succès.

Les VPS dont Melvin et Hubert sont responsables sont accessible par tous. Le VPS de Guillaume est accessible uniquement que par lui et le compte `vvandens` à l'heure actuelle et nous attendons qu'il ajoute nos clés SSH.

Fail2Ban à été installé et configuré sur les 3 VPS. Le détail de sa configuration est expliqué dans le rapport de sécurité.

5.1.2. Apprentissage de Docker (résolu)

Nous avions rencontré des soucis de compréhension lié à l'utilisation de Docker.

Suites à de nombreux essais et de la lecture de la documentation Docker, nous avons compris les fondements de Docker et des Dockerfile.

5.1.3. Mise en place d'un DNS interne et externe (achevé)

Nous avons rencontré d'innombrables problèmes lors de la création et la mise en place de la partie DNS du projet. Après de multiples tests, du débogage et la vérification des logs, nous sommes arrivés à obtenir un DNS fonctionnel.

Concrètement, seule la partie intranet de la partie web du projet ne sait être sécurisée comme il se doit, le rendant inaccessible.

5.1.4. Soucis du respect du planning interne (résolu)

Nous avons accumulé du retard suite à une mauvaise gestion du temps des différents membres du groupe.

Avec les autres cours, les autres projets et les obligations personnels de chacun d'entre nous, nous n'avons pu mener à bien cette première partie du projet mais comptons bien avancer et mener à bien ce projet et ce, dans son intégralité.

L'utilisation et le respect plus concrèt de notre Trello est de mise depuis la première échéance courant mars et rattrapons doucement mais sûrement notre retard.

A l'heure actuelle, nous pouvons confirmer que nous avons rattrapé notre retard par rapport aux autres groupes et avons mené à bien ce projet.

5.1.5. Web non disponible publiquement (résolu)

Hubert à commencé la programmation de la partie web sous `lighttpd` mais suite à de nombreux problèmes rencontrés (entre autres, lié au DNS géré par Guillaume), toute l'avancée à été retirée.

Le code source des 3 sites internet (le site vitrine ainsi que l'intranet et le b2b) ainsi que le Dockerfile sont disponible en ligne sur le repository GitHub et accessible à l'endroit suivant : docker-web/

Melvin a repris en mains le Dockerfile de la partie web afin de le créer sous `nginx` et le finaliser. Il a été possible d'afficher le site web vitrine comme site principal et le b2b ainsi que l'intranet, tous 3 en subdomain. La partie dynamique de l'intranet et b2b n'étaient pas fonctionnel.

Hubert a finalement repris en main la partie web, est reparti sous `lighttpd` au lieu de `nginx` et à mené à bien la mise en place des 3 sites internet et du support de PHP7. La partie intranet ne sait pas être testée pour le moment, suite à un problème au niveau du DNS.

5.1.6. Mail accessible uniquement que par commande (résolu)

Guillaume a pris en main la partie mail du projet. Il a très rapidement fait face à de nombreux problèmes lors de la création du Docker avec `postfix` mais heureusement, une solution a été trouvée.

La partie mail n'a été accessible que par ligne de commande au départ, le temps que nous cherchions quel outil finalement utiliser pour créer les adresses mail virtuelles.

Depuis, il est maintenant possible d'utiliser un client mail tel que Thunderbird par exemple. Concernant les adresses mail virtuelles, le service `postfix` est utilisé.

5.1.7. L'audio de l'appelant est transmis lors d'un appel en Voice over IP mais pas celui de l'appelé (en cours de résolution)

Melvin a pris en main la création et la mise en place de la partie VoIP du projet. Il a su mettre en place un serveur Asterisk avec deux comptes test afin de vérifier le fonctionnement et ajouter au fur et à mesure les éléments nécessaires pour son bon fonctionnement.

Divers problèmes ont été rencontrés en provenance de Docker (compilation du Dockerfile impossible suite à des éléments manquants, "driver failed programming external connectivity on endpoint PBX", etc.) et d'Asterisk (lancement du serveur impossible, configuration intégrale d'Asterisk hors interface graphique, etc.) et une solution a été trouvée.

Malheureusement, à l'heure actuelle, il fait face à un problème de taille puisque l'audio de l'appelant est transmis, mais pas celui de l'appelé. De plus, lorsque quelqu'un raccroche, l'appel continue pour l'autre personne.

La vérification des paquets transmis, du firewall ainsi que des logs à permis de trouver des erreurs.

Les erreurs des analyse de paquets consistent en des 404 *(not found)*, 403 *(Forbidden)* et 401 *(unauthorized)*.

Les erreurs des logs sont les suivants :

- 1 : unable to find a valid server address or name
- 1 : no configured users for ARI
- 1 : ignoring duplicated mailbox xx in contect default
  - Les xx correspondent aux deux derniers chiffres des utilisateurs et concerne tous les utilisateurs.
- 83 : unable to create channel of type "SIP" (cause 20 - subscriber absent) :
  - Alors que l'utilisateur est bel et bien connecté.
- 83 : no audio available
  - Alors que l'utilisateur dispose bien d'un micro et que le son est retransmis lors d'un test d'enregistrement audio en local.
- 51 : retransmission timeout reached on transmission
- 51 : Hanging up call - no reply to our critical packet
- 51 : re-invite to non-existing call leg on other UA

5.1.8. Mise en place du protocole HTTPS (résolu)

Le protocole HTTPS à suscité quelques questionnement au niveau de son implémentation. Melvin a commencé le support du protocole HTTPS mais n'arrivait pas à fixer une connexion refusée pour l'ACME challenge de Certbot dont les seuls pistes étaient DNS A/AAAA record(s) contenant les bonnes adresses IP ou le mur pare-feu bloquant la communication entre serveur et client.

Le problème n'ayant pas été découvert et fixé, Hubert à repris de zéro la configuration de HTTPS et l'a mené à bien tout en récupérant une partie de la configuration précédente réalisée par Melvin.

5.1.9. Limite du nombre de certificats générés par nom de domaine (en cours de résolution automatisée)

Suite à quelques tests et modifications des sites internet, nous avons compilé à plusieurs reprises notre Docker concernant la partie web. Etant donné que nous avons intégré la génération d'une clé Let's Encrypt au sein même de la compilation du Docker, il s'avère que la clé est renouvelée à chaque compilation. Cela à donc, par conséquent, entraîné le fait que nous ayons atteint le nombre limite de certificats pouvant être générés auprès de Let's Encrypt.

D'après la documentation de Let's Encrypt, il s'avère qu'un délai de une semaine environ est prévu avant de pouvoir à nouveau en générer. Le système de "fenêtre coulissante" est utilisé par Let's Encrypt. Par exemple, si nous émettons 25 certificats lundi et 25 autres vendredi, nous pouvons de nouveau en émettre à partir de lundi.

Ce problème sera donc résolu d'ici les prochains jours.

6. Procédure de validation du déploiement de la solution

Nous n'avons pas mis en place une procédure de vérification automatique. Malgré cela, nous nous sommes assuré que nos services fonctionnent correctement et avons suivi une procédure de vérification manuelle.

6.1. DNS

Pour valider le service DNS, nous avons utilisé les commandes `dig` sur nos sites web et `nslookup` sur notre nom de domaine afin de vérifier les ports. Nous avons également essayé les accès sur les sites externes. Concernant le site interne, nous avons essayé avec `curl` mais due à une erreur inconnue encore à ce jour, il nous a été impossible de voir le site.

Nous avons également vérifié l'utilisation des ports avec la commande `ss`.

6.2. Web

Pour la validation de la configuration Lighttpd, le simple fait de le lancer nous confirme sa validation ou non. En effet, en le démarrant, il nous affiche directement s'il y a un problème.

Nous avons également vérifié l'utilisation des ports avec la commande `ss`.

6.3. Mail

Pour cette partie, nous avons envoyé différents mails jusque quand le mail est arrivé à destination.

6.4. VoIP

La procédure de validation et de déploiement de VoIP est le test d'appels entre différents numéros inscrits dans le dialplan.

De plus, nous avons vérifié l'utilisation des ports avec la commande `ss`.

7. Réflexion sur le monitoring des services déployés

Le troubleshooting de nos configurations Docker a déjà été réalisé en parcourant la structure interne des images Docker déployée ainsi que des recherches dans les différents logs générés par ces derniers.

Fail2ban est déjà une forme de monitoring pour la sécurité. Il nous est possible de recevoir des mails lors des tentatives de connexions échouées.

De plus, par le biais d'Asterisk, il nous est également possible d'être prévenu par mail lorsqu'une tentative de connexion multiple échoue.