Administration Système Groupe 2TL2-9

Rapport Technique

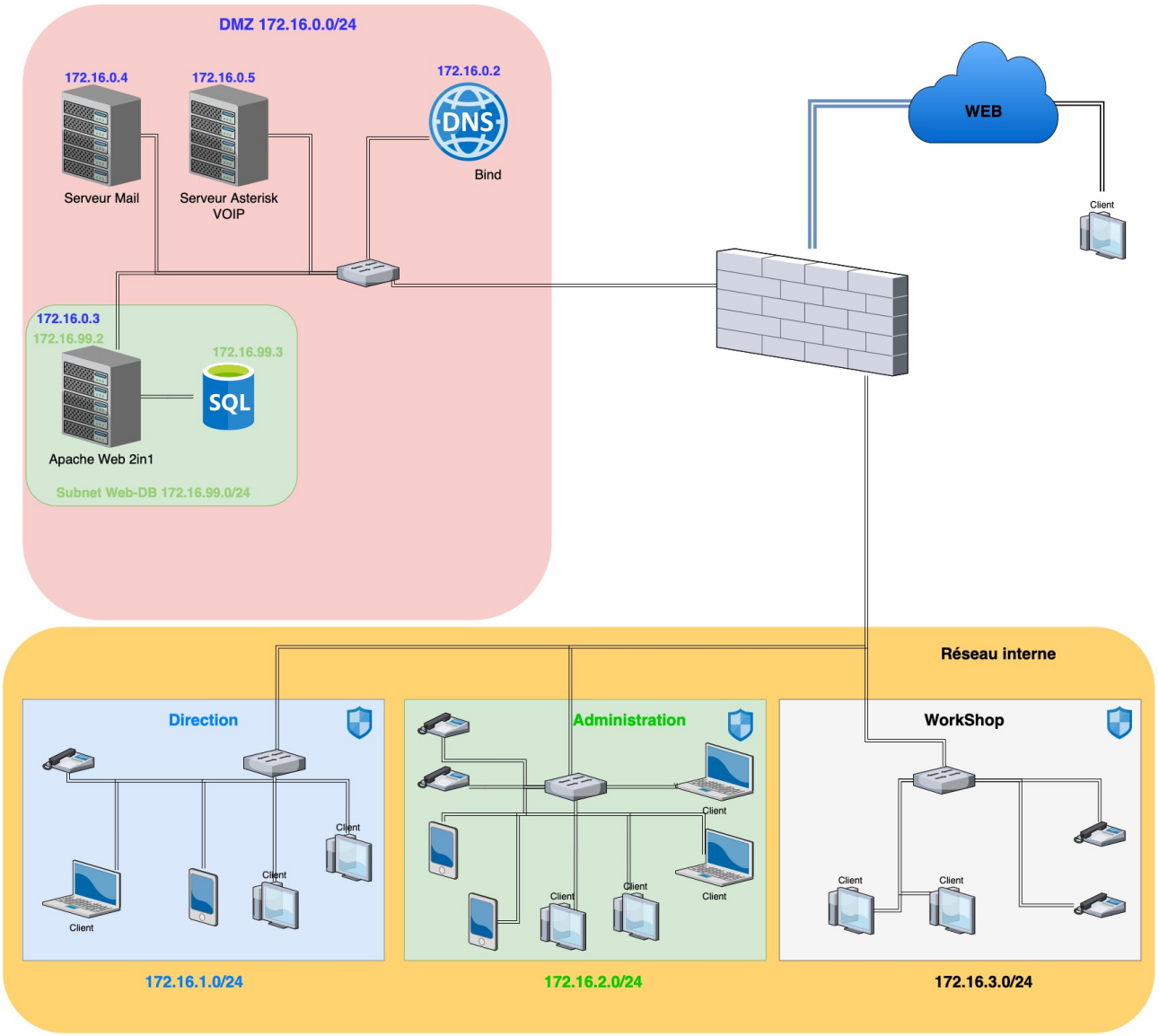
G.Lemer A.Nilens F.Janssens

4 juin 2020

Table des matières

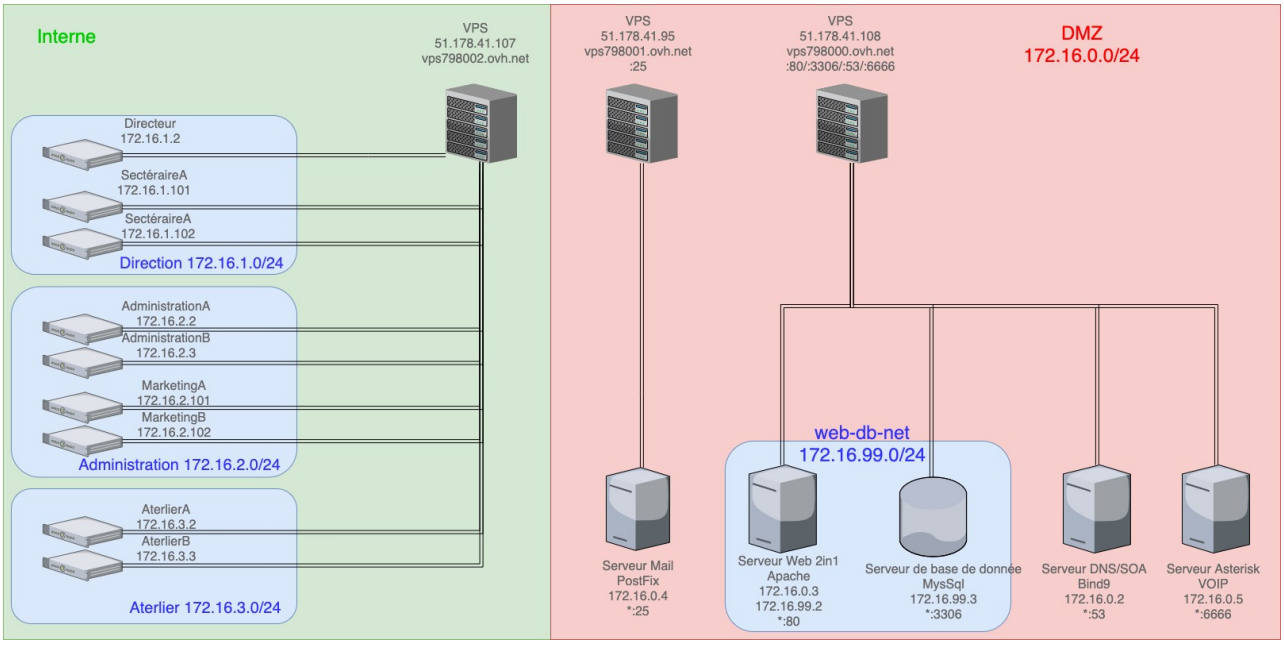
1 Schéma de déploiement

1.1 Schéma logique - WoodyToys - Schéma réel



1.2 Schéma physique - Schéma Prototype

Nous avons décidé de dédier 1 vps au réseau interne, car celui-ci représente un réseau distinct qui serait également complètement séparé en réalité. Les 2 autres vps représentent la DMZ.



2 Architecture

Nous avons décidé de découper le réseau grâce à nos vps, nous avons 2 vps représentant la zone DMZ et les services de cette zone. Pour le réseau interne, celui-ci sera géré par notre 3e vps.

Les serveurs Web, SOA, Asterisk, mail et Base de données sont placés en DMZ permettant de mieux gérer les connexions depuis l'extérieur et d'éviter que les ordinateurs internes aux réseaux soient compris en cas d'attaques. Effectivement ces serveurs sont les "passerelles" vers l'extérieur et sont donc les plus susceptibles aux attaques.

Les machines Ubuntu internes à l'entreprise sont situées sur un réseau interne sans connexion directe vers l'extérieur.

3 Difficultés

3.1 Serveur Web

Nous avons donc choisi de partir sur la mise en place d'un serveur apache. L'écriture du dockerfile et la configuration de ce dernier ne nous ont pas été particulièrement compliquées.

3.2 Serveur B2B

Nous avons décidé de mettre en place un serveur apache/PHP. La mise en place et la configuration de celui-ci n'ont pas été laborieuses. Le site communique avec la base de données grâce à mysqli. Nous avons rencontré quelques problèmes lors de la mise en place de la communication entre le site et la base de données ainsi que pour les requêtes mysqli.

3.3 Serveur base de données

L'installation de mysql ne nous a posé aucun souci en soit, mais sont interaction avec le docker fut un peut plus laborieuse.
De plus, le port vers le serveur apache a demandé de nombreuses reconfigurations, mais cela est maintenant fonctionnel.

3.4 Serveur DNS

Le serveur DNS fut plus compliqué que prévu à mettre en place. Par souci de simplicité, nous avons mis les 2 zones sur un seul et même DNS, en réalité cela se ferra avec un proxy afin de maintenir l'intégrité de la zone interne. La mise en place du docker compose ainsi que des fichiers de zones furent complexes, ça ils ont été les premiers pour moi à mettre en place.

3.5 Serveur MAIL

La mise en place du serveur mail à posé pas mal de petits problèmes consécutifs au début . Malgré une configuration assez réduite pour avoir dans un premier temps une communication entre 2 clients, nous avons été confrontés à de nombreuses erreurs de configurations en lien avec certaines versions des logiciels que nous utilisions qui n'étaient pas à jour. En ce qui concerne le serveur imap/pop, au début nous avions installé et configuré "Courier mail server". Mais un problème de communication entre le driver mysql et tourier nous a fait changé d'avis et finalement, nous avons suivi les conseils en installant et configurant Dovecot. À ce jour, tout fonctionne bien que ce soit au niveau de l'envoi d'un mail ou de la réception de celui-ci.

3.6 Serveur VOIP

La mise en place des fichiers de configurations fut assez facile, Asterisk est bien documenté donc cela n'a nécessité que du temps. En ce qui concerne le déploiement, une erreur dans la configuration d'un fichier non existant pose quelques problèmes.
Après avoir changer de Version Ubuntu pour une plus récente et quelques modifications qui on du être faite dans la configuration du serveur, celui-ci semble maintenant fonctionnel. Les Tests par SoftPhone on permis de déceler quelques anomalies dans le plan d'adressages qui sont maintenant fixer et fonctionnel.
Pour l'ajout de la nouvelle entreprise (l'extension), il suffit de rajouter l'adresse IP du serveur VOIP de la nouvelle

entreprise dans le fichier iax.conf a la ligne 'host'. À partir de la l'adressage ce fait sous forme '9XXX' (9 + numéro interne de l'extension).
Enfin, nus avons un problème concertant la mise en place de fail2ban et/ou UFW sur le serveur VOIP, celui-ci est configuré et semble être fonctionnel sur les autres services, mais ne fait pas sont travail sur le service voip. Effectivement, les 'spams' de connexion extérieurs sont incessants. Une solution pour maintenir le réseau voip interne fonctionnel est présente, mais la connexion extérieure a du être coupée pour permettre la connexion interne. Afin de limiter au maximum les problèmes liés aux attaques SIP, nous avons changé le port par défaut vers le port 6666, ce qui a presque totalement éliminé ces attaques automatiques.

4 Monitoring

4.1 Vérification des Services Web

si tout est mis en places comme expliquées dans les procédures d'installation, les pages web respectives sont disponibles aux adresses suivantes :

- *vitrine*
- *b2b*
- *(depuis un ordinateur interne) interne*

4.2 Vérification des informations de la base de donnée

afin de vérifier directement le contenu de la base de données lancée :

1. *'docker exec -it <NomDeLImage> bash -l' pour entrer en bash dans le docker*
2. *'mysql -u user -p'loggin dans mysql (password : user1234)*
3. *'use db ;' séléctionner la db*
4. *'show tables ;' montrer les tables*

4.3 Vérification de la configuration VOIP

se connecter directement dans le docker et la console Asterisk :

- *docker exec -it voip bash -l*
- *asterisk -rvvv*

affichage du Plan d'appel

- *diaplan show*
- *diaplan show <context>*

affichage des utilisateurs

- *sip show users*

affichage des queues (administration)

- *queue show*

4.4 Rassemblement des services

Le serveur rassemblant les Services web, base de données, DNS et VOIP est maintenant mis en place sous forme d'un seul docker-compose exécutable pour plus de facilitée de déploiement. Une série de 4 commandes permettent de mettre l'ensemble de ces services en place, sans aucune autre base nécessaire. L'ensemble de ces services étant préconfiguré cela permet d'avoir ces services opérationnels en quelques minutes.

5 Bibliographie

— https ://www.howtoforge.com/tutorial/how-to-create-docker-images-with-dockerfile/
— https ://www.zytrax.com/books/dns/ch4/
— https ://web.archive.org/web/20160328154322/
— https ://brocas.org/blog/post/2006/06/22/14-de-la-securite-d-une-architecture-dns-d-entreprise
— https ://tvi.al/simple-mail-server-with-docker/
— https ://www.youtube.com/watch ?v=jMQfSsO1da4list=PLnzEbgyK52Gu9fdVDHburrsG3KBIntXFK