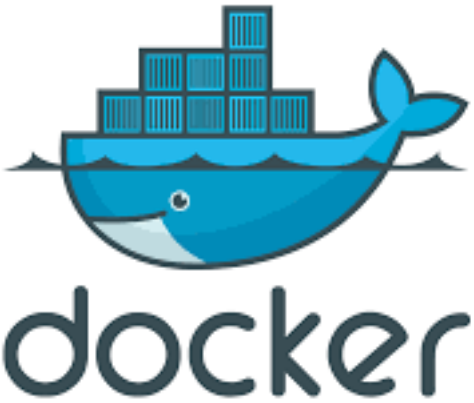
École pratique des hautes études commerciales

Rapport final

Administration système et réseaux II



Culem Adrien
Gaudin Adrien
Micciche David
2TL2
Groupe N°8

August 7, 2016

Contents

1 Introduction

Dans le cadre du cours d'administration système et réseaux, nous avons reçu la mission de créer l'entièreté d'une infrastructure réseaux répondant aux besoins d'une entreprise fictive. Le projet est divisé en plusieurs parties, nous avons donc dû rajouter des services à notre infrastructure tout au long du semestre. Cela inclut un service mail, des serveurs webs, un serveur DNS, un service de VoIP, un service de partage de fichiers,etc... Toute cette infrastructure a été réalisée, à l'aide de docker, sur plusieurs VPS hébergés par OVH.

2 Cahier des charges

Avant tout, l'entreprise devra posséder plusieurs sites internet. Un premier sera destiné aux clients potentiels, un deuxième sera uniquement dédié aux autres entreprises (B2B) tandis que le dernier sera, quant à lui, un intranet uniquement disponible pour les employés de l'entreprise (ERP). Les employés devront également avoir accès à Internet. Tous ces sites devront être accessibles via des adresses (URL) différentes.

Ensuite, l'entreprise aura besoin de fournir une boîte mail à chacun de ses employés. Tous devront donc disposer de leur adresse mail personnelle dans le domaine de la compagnie. La société devra également posséder des adresses mails génériques, telles qu'une adresse de contact, une adresse concernant le B2B, etc... permettant à des actuels ou futurs clients de joindre, directement, certaines sections de l'entreprise. Les employés devront pouvoir consulter leurs mails aussi bien au sein de l'entreprise que depuis chez eux ou même en déplacement.

Une infrastructure permettant de faire de la VoIP devra également être fournie. L'entreprise sera donc joignable depuis Internet sur un identifiant public particulier (ID SIP). Un plan de numérotation devra évidemment être écrit et respecté. Tous les employés disposeront d'un softphone à l'exception des ouvriers qui posséderont un seul poste pour eux tous. Une boîte vocale devra de même être disponible pour chaque employé. Tous les travailleurs devront également pouvoir se joindre entres eux. Toutefois, certaines contraintes s'appliqueront à chaque poste. Par exemple, tous les appels pour le directeur devront transiter par sa secrétaire.

Finalement, dans un travail quotidien, une entreprise se doit de posséder un système de partage de fichiers pour tous les regrouper et les rendre facilement accessibles par l'ensemble des employés. Chaque travailleur doit posséder son propre répertoire. Chaque section doit également posséder le sien (Les comptables, les ouvriers, ...). Les fichiers partagés doivent être accessibles facilement depuis l'explorateur de fichiers traditionnel. Ces répertoires sont disponibles aussi bien depuis l'intérieur de l'entreprise que partout ailleurs. Enfin, le système doit être aisément récupérable en cas de perte de données (Backup).

3 Traduction en langage technique

Tous les sites internet devront être joignables sur différentes adresses:

1. Le site internet à destination des clients potentiels devra être accessible sur une adresse commençant par www.
2. Le site de business to business devra être accessible sur une adresse commençant par B2B.
3. L'ERP/Intranet sera quant à lui uniquement joignable en local avec le préfixe intranet.

Un serveur DNS devra être implémenté afin que les sites soient joignables sur une URL et non pas sur l'adresse IP. Une base de données sera également nécessaire au bon fonctionnement de l'ERP et des sites internet. Un système de backup sera évidemment indispensable en cas de perte de données.

Pour créer l'infrastructure mail, un serveur central sera requis, par exemple de type Postfix/Dovecot. Chaque ordinateur au sein de l'entreprise devra posséder un client mail afin de récupérer les courriels via un service POP3 ou IMAP. Pour que le domaine mail soit joignable sur internet, via son nom, par n'importe qui, un record MX devra être ajouté dans le DNS.

Un serveur de VoIP devra être déployé et un plan de numérotation devra également être pensé. Des softphones devront être installés sur les ordinateurs des employés. Le serveur SIP sera joignable sur l'adresse wt8.ephec-ti.be

Afin de réaliser du partage de fichiers, deux propositions sont disponibles. La première consiste en un serveur permettant d'utiliser des protocoles "classiques" comme SMB. La seconde réside plutôt dans l'utilisation du Cloud comme le font très bien des services très connus tels que Google Drive, DropBox et autres...

Quant à la sécurité de l'infrastructure elle sera organisée selon le schéma ci-après. Un firewall placé à l'entrée du réseau protégera les avant-postes de notre infrastructure. Celui-ci sera soutenu par un proxy, un reverse proxy et une architecture autour d'une DMZ afin d'assurer la pleine sécurité de notre réseau contre tous types d'attaques malvenues.

4 Proposition de solutions techniques

4.1 Web et DNS

Pour les sites internet, le choix des serveurs est vaste mais ceux qui se présentent comme les meilleurs sont Apache ou nginx. Le DNS sera très probablement réalisé à l'aide de BIND qui paraît être la solution la plus répandue. Quant à la sécurité, le firewall Iptable semble être la seule solution mais celle-ci peut en outre être améliorée et facilitée par l'utilisation d'outils tels que UFW ou Shorewall.

4.2 Mail

Dans le domaine des serveurs mails Linux, les 3 solutions qui apparaissent les plus adaptées dans notre cas sont : sendmail, Postfix ou Dovecot. Toutefois, chacune comporte des inconvénients. Sendmail et Postfix ne faisant tous les deux que du SMTP, ils devront être couplés à Dovecot si on désire avoir un service POP3 et/ou IMAP. Quant au choix du client, il est relativement libre puisque tous les clients existants sur le marché font plus ou moins la même chose (Thunderbird sur Linux, Courrier sur Windows, etc...).

4.3 VOIP

Le leader Open-Source des serveurs SIP est sans doute Asterisk, mais bien d'autres existent. Certains tournent sur base d'Asterisk (FreePBX) ou même le combinent à des services mails (Elastix). Du côté des produits propriétaires, Cisco fournit un service SIP tout comme Microsoft, Oracle et d'autres grands noms de l'industrie informatique. Dans le cadre de l'intégration d'un service de VoIP dans une entreprise, un plan de numérotation doit être établi en respectant certaines règles de redirection d'appels. Celui-ci définira le comportement du serveur Asterisk selon l'exemple ci-dessous.

1. Les ouvriers ont le numéro 11, ils peuvent être appelés par tout le monde et peuvent appeler tout le monde en interne.

2. La secrétaire possède le numéro 22, elle peut recevoir ou donner des appels à tout le monde aussi bien en interne qu'en externe. Elle peut également rediriger les appels.

3. Les comptables ont un numéro de type 33xx et peuvent joindre l'extérieur ainsi que tout le monde en interne à l'exception du directeur. Un numéro 33 est également prévu afin d'appeler le premier comptable disponible.

4. Les commerciaux ont, quant à eux, un numéro de type 44xx et répondent aux mêmes règles que les comptables.

5. Le directeur est titulaire du numéro 55, il peut appeler tout le monde aussi bien en interne qu'en externe mais tous les appels qui lui sont directement adressés passent d'abord par celui de la secrétaire.

4.4 Partage de fichiers

Deux différentes directions se présentent. Une première option est Samba qui permet d'adapter le protocole SMB/CIFS à tous les systèmes basés sur le noyau UNIX outre un VPN pour assurer la connexion à distance pour l'accès aux fichiers partagés. La seconde option consiste dans l'utilisation du cloud avec un service tel que OwnCloud, solution open-source concurrente de DropBox et équivalents, basé sur l'extension du protocole HTTP, WebDav.

5 Choix de solutions

5.1 DNS

En premier lieu, nous avons installé, à l'aide de l'outil BIND, deux name server distincts chacun dans un VPS différent et dans un container individuel. Un premier possédant les ressources records (RR) des services mail, voip et web. L'autre en possédant uniquement un seul pour l'intranet. Toutes les IPs de ces RR sont associées au domaine wt8.ephec-ti.be.

Nous n'avons pas réellement rencontré de problèmes si ce n'est l'application d'une structure DMZ complète. Le problème vient de ce que le service Docker refuse l'utilisation simultanée du même port, même sur des sous-réseaux différents. Une solution potentielle serait de lier deux VPS via un VPN et utiliser l'interface Docker du deuxième VPS comme second sous réseau.

5.2 Web

Ensuite, nous avons choisi de rendre accessible les sites internet grâce à des serveurs NGINX, chacun sur un container différent, tous redirigés sur les ports 80 et 443 via un reverse proxy (lui aussi NGINX) qui servira également à intercepter les hostnames de chaque sites. Ces "virtuals hostnames" permettent aux internautes d'accéder aux sites sans devoir indiquer un port différent, même si les serveurs web sont sur la même IP.

L'utilisation d'un proxy pour la navigation web des employés reste toutefois absente mais la solution serait d'installer un serveur proxy Squid en transparence.

5.3 Mail

Pour le serveur mail, un container composé de Postfix et Dovecot a été créé. Postfix sert de relay SMTP pour l'envoi de mail tandis que Dovecot, en contingence avec un service POP3, permet la récupération des courriers dans les boites de chaque utilisateur. Ces derniers ont un identifiant et un mot de passe uniques, cryptés en MD5, pour réduire les vulnérabilités. Ceci permet aux utilisateurs du service de se connecter directement via leur client mail favori, tel que ThunderBird ou Outlook.

L'installation du serveur mail fut la plus éprouvante dès lors que les fichiers de configurations sont longs et peu commentés. Malheureusement, quelques fonctionnalités demandées ne fonctionnent pas. Par exemple, il est impossible de récupérer ses emails en POP/IMAP via un client mail parce que ces derniers ne sont pas stockés dans le bon répertoire sur le MTA. Il n'y a pas non plus de client Web.

Une solution serait de passer sur un service "all-in-one", tel que Webmin, qui fournit un service mail pré-configuré ou d'utiliser celui d'OwnCloud. Ces deux derniers exemples sont plus simple d'approche que la solution que nous avons choisie et résoudraient à la fois le problème de récupération des emails et le manque de client web.

5.4 VOIP

Quant à la VoIP, un serveur Asterisk a été utilisé pour permettre les communications sur SIP. Afin de passer nos appels nous utilisons une application mobile nommée CSipSimple disponible sur android qui est simplement un softphone.

Un des principaux problèmes rencontrés était le manque d'un softphone de bonne qualité. Par exemple, l'application Android CSipSimple refuse de raccrocher, Zoiper quant à elle transmet le son une fois sur dix... L'implémentation des boîtes vocales n'a pas été réussie ni celle de la redirection des appels par la secrétaire.

5.5 Partage de fichiers

La solution qui a finalement été choisie est l'utilisation de OwnCloud usant le système webDAV. Celle-ci est très pratique et possède une interface graphique particulièrement attractive. C'est pourquoi sans trop d'hésitation, un serveur de ce type a été réalisé.

Comme l'installation de OwnCloud est extrêmement simple, aucun problème n'a été rencontré lors de sa mise en place.