Administration système et réseaux II
Enoncé du projet

Virginie Van den Schrieck

19 février 2019

1 Approche pédagogique

Dans le cadre de ce cours, il vous est demandé de mettre en place une infrastructure réseaux répondant aux besoins d'une entreprise fictive. Ces besoins vous seront présentés ci-dessous, regroupés par type de service, chaque service constituant une mission spécifique de manière à ce que vous construisiez le réseau élément par élément. L'objectif est d'intégrer l'ensemble des services d'ici la fin de semestre à votre réseau, que vous défendrez ensuite lors de l'examen final.

Vous serez donc amenés à concevoir et configurer différents systèmes de manière autonome, et rencontrerez probablement divers obstacles ou difficultés. Cela nécessite de développer une méthodologie de recherche efficace d'information (installation, configuration, validation, debugging,...).

Vous utiliserez les VPS qui ont été mis à votre disposition pour construire le réseau de démonstration. Chaque service sera isolé dans un container Docker, et les procédures d'installation/configuration seront reprises dans une documentation qui s'enrichira au fur et à mesure du semestre.

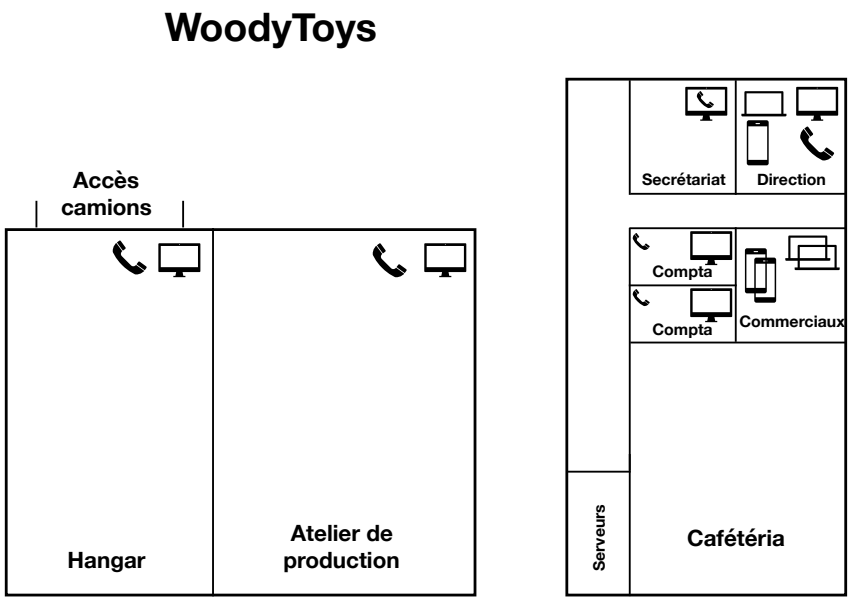
Vous serez évalués d'une part sur l'évolution de votre travail au cours du semestre (démos et rapports intermédiaires), et d'autre part sur la version finale (examen et version finale des rapports). Cette évaluation sera à la fois collective (ampleur de la réalisation finale) et individuelle (implication + supervision d'une mission spécifique).

2 Description de l'entreprise

L'entreprise qui vous contacte est l'entreprise WoodyToys (WT), qui fabrique de manière artisanale des jouets en bois. L'entreprise souhaite remplacer ses serveurs vieillissants, et fait appel à vous pour la phase de conception et de validation d'une nouvelle infrastructure d'hébergement des services informatiques.

2.1 Structure de l'entreprise

L'usine comporte un atelier où sont fabriqués les jouets, un hangar de stockage d'où partent les produits vers les revendeurs, le bureau du directeur et les bureau où travaillent les employés. Parmi ceux-ci, il y a des comptables, des commerciaux et une secrétaire L'usine dispose d'une connexion à Internet. L'atelier, le hangar et le bureau comportent un certain nombre de postes de travail et de téléphones connectés via une infrastructure IP. Un réseau Wifi permet aux employés d'utiliser des appareils portables (laptops et smartphones). Le plan ci-dessous représente schématiquement l'organisation des bureaux de l'entreprise.



2.2 Services informatiques

2.2.1 Services internes

Au niveau de la gestion des employés, il faut vous assurer que ces derniers puissent bénéficier d'un accès Internet sur leurs postes de travail, que ce soient des postes fixes ou mobile. Ils doivent également avoir accès aux services internes (ERP notamment). Il vous est demandé de ne pas vous reposer sur les services de résolution de noms ni du fournisseur d'accès, ni d'autres fournisseurs extérieurs. Un contrôle du traffic Web généré par les employés est souhaitable. Il peut en outre être intéressant de réfléchir à la gestion des identités des employés pour l'utilisation des services internes.

2.2.2 Web

La vente des produits s'effectue uniquement en B2B (revendeurs). La gestion des contacts clients, des commandes, des stocks et l'organisation de la production est gérée par un outil ERP Web uniquement accessible sur le réseau interne. L'entreprise dispose également d'un portail Web public présentant ses produits (www.woodytoys.be), et d'un site de vente en ligne réservé aux revendeurs (b2b.woodytoys.be). Le code source de ces trois sites est pré-existant, il s'agit d'un site statique en HTML/CSS pour le site vitrine, et de sites dynamiques en PHP/MySQL pour l'ERP et le site de vente en ligne.

2.2.3 Mail

L'entreprise fournit une adresse mail à chacun de ses employés, au format nom.prenom@woodytoys.be. Elle dispose également d'adresse mail génériques, dont actuellement :

— contact@woodytoys.be, redirigée chez la secrétaire
— b2b@woodytoys.be, redirigée sur les commerciaux

Les employés doivent pouvoir consulter leur courrier électronique et en envoyer **à l'aide d'un client mail classique** (i.e. pas webmail en interne) depuis l'entreprise. Ils doivent également être en mesure d'utiliser leur mail en déplacement ou à domicile.

2.2.4 Téléphonie IP

Au niveau du service téléphonique, il vous faudra concevoir un nouveau plan d'adressage en téléphonie IP reprenant les besoins suivant :

1. L'entreprise doit être accessible en VoIP depuis Internet, afin que des clients puissent la contacter. L'adresse de contact est `contact@woodytoys.be`. Les appels doivent aboutir sur le poste de la secrétaire.
2. Les employés de l'entreprise doivent pouvoir communiquer entre eux, à l'intérieur de l'entreprise, mais également depuis l'extérieur dans le cas des commerciaux qui sont souvent en déplacement. Les communications identifiées sont les suivantes :
   — Les ouvriers : Ils disposent d'un poste de téléphonie IP dans leur atelier et dans le hangar pour joindre les autres départements internes.
   — La secrétaire : Elle dispose d'un PC sur lequel se trouve un softphone, lui permettant de contacter n'importe qui.
   — Le service comptable : Réparti dans deux bureaux, il dispose d'un numéro unique permettant de joindre le premier comptable disponible, ainsi que d'un numéro spécifique par bureau. Les comptables peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur.

— Les commerciaux : Réunis dans un même bureau, ils peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur. Ils disposent de smartphones avec lesquels ils peuvent téléphoner en déplacement.
— La direction : Un numéro qui peut joindre tous les autres postes internes ainsi que l'extérieur. Ce numéro ne peut pas être joint directement, les appels devant transiter préalablement par la secrétaire.

3. Les employés doivent pouvoir disposer d'une boîte vocale.

L'entreprise est en outre engagée dans le rachat d'une entreprise concurrente. Il vous est donc demandé d'étudier dès maintenant la fusion des deux réseaux téléphoniques.

Cela signifie que :

1. Les deux plans d'adressage doivent être fusionnés en minimisant les changements nécessaires
2. Les deux serveurs de téléphonie doivent être configurés pour que les deux sites puissent se contacter en utilisant le nouveau plan d'adressage interne.

Enfin, de manière secondaire, il vous est demandé d'explorer des fonctionnalités supplémentaires, comme par exemple la visio-conférence ou l'utilisation de téléphones ou de passerelles SIP vers la téléphonie classique.

2.2.5 Fichiers de l'entreprise

Dans le cadre de son travail quotidien, l'entreprise a besoin d'un système de fichiers partagés afin de pouvoir centraliser l'ensemble des documents utilisés par les employés. Les fonctionnalités précises sont les suivantes :

— Chaque employé doit pouvoir disposer de son répertoire personnel, de même que le directeur et la secrétaire
— Chaque groupe d'employés doit disposer d'un répertoire commun
— Les employés doivent pouvoir accéder aux fichiers partagés via l'explorateur natif du système
— Le système doit pouvoir être backupé facilement
— Les employés doivent avoir la possibilité d'accéder à leurs fichiers en déplacement (PC portable ou smartphone).

3 Prototype à produire

Il vous est demandé de proposer une architecture permettant la mise en place des services. Vous ferez un prototype de démonstration de cette architecture dans votre réseau de VPS, en utilisant comme nom de domaine de base `wtX.ephec-ti.be`, avec X le numéro de votre groupe, en lieu et place du nom de domaine officiel de WoodyToys.

Votre prototype devra reproduire le réseau réel de l'entreprise pour valider l'ensemble des besoins. Réfléchissez donc bien, avant d'implémenter un service donné, à la manière dont vous allez valider qu'il répond à chacun des besoins exprimés. Vous devrez prouver, lors de la démonstration, que c'est bien le cas.

N'oubliez donc pas de tenir compte de la présence des employés dans le réseau : leurs postes doivent pouvoir communiquer entre eux, avec les services internes et avec l'extérieur (accès Internet) de manière sécurisée et en fonction de la demande ci-dessus. Réfléchissez à ce que cela implique en terme de configuration des services ! Basez votre réflexion sur un schéma réseau complet reprenant l'ensemble des informations de cet énoncé.

3.1 DNS et accès web interne

Réfléchissez aux spécificités des services accessibles en interne. En quoi diffèrent-ils des services accessibles en externe ? Comment montrer que les configurations sont fonctionnelles, sur base des choix de simulation des postes employés ?

3.2 DNS externe

Vous avez donc à concevoir et mettre en place le sous-domaine de wtX du domaine ephec-ti.be, géré par votre professeur. Il est de votre responsabilité d'envoyer les informations ad-hoc au gestionnaire du Name Serveur du domaine parent, afin que les requêtes puissent aboutir sur votre infrastructure.

3.3 Web

Votre travail n'est pas de programmer les sites web de l'entreprise, mais de déployer et configurer les services nécessaires pour les héberger. Utilisez donc des pages Web Mock-Up statiques pour la démo, ou des pages PHP/Javascript très simples. Vous ne serez bien entendu pas évalués sur le contenu ou le design de ces pages. Vous devrez par contre réfléchir à la manière dont vous allez prouver que l'infrastructure fonctionne (ex : lien entre serveur Web et BDD, accès interne/externe, ...).

3.4 Mail

Lors de la mise en place du service mail, procédez de manière incrémentale : D'abord, validez l'envoi d'un mail entre deux employés depuis le serveur, puis depuis deux postes du réseau interne, puis l'envoi de mail vers l'extérieur, et, enfin, la réception d'un mail envoyé de l'extérieur vers une adresse WoodyToys.

3.5 VoIP

Pour concevoir le prototype répondant à ce cahier des charges, vous devrez vous associer à un autre groupe afin de fusionner vos deux solutions de téléphonie. Si vous souhaitez explorer du matériel SIP, discutez-en avec le professeur.

4 Contraintes d'implémentation du prototype

Chaque groupe dispose de 3 VPS sur lesquels il peut mettre en place le prototype représentant le réseau WoodyToys proposé. Les services devront être implémentés sous forme de Dockerfiles, qui seront hébergés sur le repository Github du groupe. Ce repository Github devra être lié à un compte Dockerhub spécifique au groupe, de telle sorte que chaque service soit (idéalement) déployable en une ligne de commande sur un VPS vierge.

Ex : `docker run -d ephecAdminGr3/mail`

5 Calendrier des missions

L'énoncé du projet est vaste, et destiné à vous donner une certaine liberté quant aux éléments implémentés. Néanmoins, il y a des passages obligés et des échéances intermédiaires à respecter. Trois deadlines vous sont proposées, correspondant grosso-modo aux trois éléments principaux du cours : Web et DNS, Mail et VoIP.

1. Web et DNS : Démo et remise des délivrables lors des TPs des 13/14 mars (rentrée de Carnaval)
2. Mail : Démo et remise des délivrables lors des TPs des 27/28 mars
3. VoIP : Démo et remise des délivrables lors des TPs des 8 et 9 mai

Libre à vous aussi de proposer d'autres moments de démo au professeur, pour valider par exemple des éléments qui ne l'auraient pas été lors des échéances proposées, ou pour montrer des fonctionnalités bonus.

De fait, comme vous le constatez, tous les éléments du cahier des charges ne sont pas repris dans les démos intermédiaires. Ces éléments peuvent constituer des bonus. Vous pouvez aussi proposer des services supplémentaires à l'entreprise, pour autant que cela réponde à un besoin métier (discutez-en avec le professeur avant toute chose).

Les dernières semaines du projet seront consacrées à finaliser les fonctionnalités des modules principaux (Web, DNS, Mail et VoIP), ou, pour les groupes les plus avancés, à la mise en place de ces services supplémentaires (enrichissement de la simulation du réseau interne, fonctionnalités VoIP avancées, système de fichiers partagés, ...)

6 Délivrables attendus

A l'exception du rapport technique, les délivrables demandés seront construits au fur et à mesure des missions. D'une part, ils seront enrichis par les nouveaux éléments de service mis en place, d'autre part, ils seront retravaillés et améliorés sur base du feedback reçu du professeur.

Les premiers rapports seront probablement ceux qui vous demanderont le plus de temps, puisque vous pourrez, lors des missions suivantes, reprendre la structure de base en l'améliorant suivant les commentaires reçus et en l'adaptant aux services déployés à chaque étape. Il vous est demandé de clairement identifier les différentes versions des documents, en indiquant à chaque fois le numéro de la version et la date de révision. **Les nouveaux éléments ou les éléments modifiés seront indiqués en italique afin de permettre au correcteur de cibler sa lecture.**

De cette manière, les documents finaux vous demanderont normalement peu de travail, puisqu'ils auront été construits incrémentalement.

Pour rappel, à chaque échéance, un étudiant du groupe est responsable de la qualité des délivrables soumis, et sera évalué pour cela. Cet étudiant devra être clairement identifié en tant que responsable au début de chaque document.

6.1 Le rapport client

Dans le rapport à destination du client (4-5 pages maximum pour la version finale) devront figurer les éléments ci-dessous.

- Le cahier des charges : Reformulation de la demande du client
- La traduction des besoins du client en langage informatique
- Les propositions de solutions techniques avec comparatif des alternatives possibles
- Choix et justification de la solution
- Les besoins en maintenance de la solution proposées, afin que le client puisse prévoir le nécessaire
- Rapport sur ce qui a été déployé (solution à moitié/totalement déployée, planning pour la finalisation, ...)

Ce rapport est à destination du client, donc attention à utiliser les termes techniques à bon escient, et à ne pas vous perdre dans des détails superflus.

L'objectif pédagogique de ce rapport est de pouvoir présenter de manière simple à des non-techniciens votre démarche et le résultat de votre travail, en montrant que celui-ci répond bien aux besoins formulés.

6.2 Un rapport technique

Ce rapport étant un état d'avancement, il ne doit pas spécialement être incrémental/se baser sur une version précédente, mais peut être complète-

ment différent d'une remise à l'autre.

Ce second rapport de 2-3 pages max. s'adresse au professeur, et est destiné à mettre en avant la qualité technique de votre réalisation.Les éléments suivants devront y figurer :

- Le numéro du groupe, les noms des membres, et le nom de l'étudiant responsable de la mission. Ce dernier présente également en quelques lignes le bilan du travail de groupe durant cette mission spécifique.
- La méthodologie utilisée pour la mise en place du réseau prototype (utilisation des outils Docker, modélisation des utilisateurs, ...)
- Un état d'avancement concret sur l'infrastructure mise en place et les fonctionnalités des services réellement implémentés
- Un commentaire explicatif des schémas réseaux et les justifications des choix architecturaux effectués
- Les plans d'adressages sont présentés et justifiés en lien avec les schémas
- Une présentation des difficultés rencontrés et des problèmes éventuellement non résolus : Liste des symptômes la plus précise possible + hypothèses sur la cause de chaque problème
- Une présentation de la procédure de validation du déploiement de la solution que vous avez utilisée
- Une réflexion sur le monitoring des services déployés

6.3 Une analyse de la sécurité

Un troisième rapport (3-4 pages en version finale) doit lister les risques de sécurité auxquels sont soumis, d'une part, l'infrastructure du client, et d'autre part, votre prototype. Il doit aussi reprendre les contre-mesures que vous proposez ou avez mis en place.

Plus spécifiquement :

- La liste des risques encourus par votre VPS et votre infrastructure Docker
- Les contre-mesures mises en place (authentification par clé, Fail2Ban, firewall, ...) et les configurations associées (règles Fail2Ban, règles de firewall)
- La liste des risques encourus par chacun des services déployés au niveau de l'intégrité, la confidentialité et la disponibilité du service
- Les contre-mesures proposées voire mises en places pour chacun des services

6.4 Des schémas réseaux

Afin de documenter votre infrastructure, deux schémas réseaux sont demandés :

6.4.1 Le schéma réseau Woodytoys

Un premier schéma représentera le réseau que vous proposez à l'entreprise, tel que vous pourriez le mettre en place sur des serveurs physiques en interne. Ce réseau fera donc abstraction de la couche Docker et des VPS, et représentera les différents services organisés en VLANs/subnets IP (couche 3). Ce schéma sera accompagné d'un texte (cfr rapport technique) l'expliquant et justifiant les choix effectués.

6.4.2 Le schéma du prototype

Ce second schéma représentera l'implémentation du réseau que vous proposez sur l'infrastructure pédagogique disponible dans le cadre du cours, à savoir les VPS OVH et les conteneurs Docker. L'objectif est de montrer comment votre réseau prototype est agencé. Dans ce schéma apparaiteront cette fois les VPS et les différents conteneurs, les réseaux Docker et les mécanismes d'exposition de ports utilisés. Ce schéma sera accompagné d'un texte (cfr rapport technique) l'expliquant et justifiant les choix effectués.

6.5 Le Wiki du groupe

En plus de ces rapports, il vous est demandé de construire un Wiki sur votre repository Github de groupe. Ce Wiki reprendra une section par service, et détaillera à chaque fois :

- Comment installer le service
- Comment configurer le service (quels fichiers, quels options, ...)
- Comment maintenir le service (mises à jour du serveur, ajout/retrait d'utilisateur, modification du contenu, ...)
- Comment s'assurer qu'il fonctionne (procédure de validation voire infrastucture de monitoring)
- Comment troubleshooter le service en cas de défaillance (fichiers de logs, outils de debugging,...)

7 Evaluation du projet

La note finale de la partie TP du cours d'Administration Systèmes et Réseaux II sera entièrement constituée par l'évaluation du projet, selon deux composantes : Une partie de cotation permanente (25%) et un examen final (75%).

Pour ce qui est de l'évaluation technique de la réalisation proprement dite, une grille d'évaluation en ligne sera mise à disposition de chaque groupe d'étudiant, afin que celui-ci puisse suivre sa progression par rapport aux attentes. Cette même grille servira également pour l'évaluation finale

7.1 Cotation permanente

Les éléments suivants interviendront dans la cotation permanente :
— Individuellement : Implication dans le travail, présence aux TPs
— Individuellement : Qualité des délivrables remis lors de la supervision de la mission spécifique de l'étudiant
— Evaluation de groupe : Remises régulières des délivrables demandés, démos intermédiaires, et progression tout au long du semestre

7.2 Evaluation finale

L'évaluation finale consiste en une défense orale du projet, où chaque groupe fait une démonstration de la réalisation terminée. Cette dernière sera évaluée selon la même grille que celle utilisée pour les démos intermédiaires.

Une partie questions/réponses aura pour but de vérifier la maîtrise du projet par chaque étudiant, et servira à éventuellement ajuster la note finale en fonction des implications de chaque membre du groupe.

8 First steps

8.1 Mise en place des outils

Avant de vous lancer dans l'analyse du problème, il est important que vous preniez le temps de mettre en place les outils que vous allez utiliser dans le cadre de ce cours. Réfléchissez avec votre groupe à la manière dont vous devrez travailler.

Vous devrez entre autres :
— Créer un repository Github spécifique à votre groupe pour héberger vos fichiers de configuration
— Créer un compte DockerHub pour héberger vos images et le lier à votre repository Github pour que vos images se construisent automatiquement à chaque commit
— Créer votre wiki et sa structure
— Réfléchir à la manière dont vous allez communiquer et échanger vos coordonnées : email, gsm, chat, ...
— Etablir une « charte »de collaboration : Implication, présence aux rendez-vous, respect des échéances, efficacité des réunions, ...
— Décider collectivement comment vous allez rédiger vos rapports (LaTeX, Office 365, Google Doc, ...).
— Nommer un étudiant responsable pour chacune des trois premières missions. Cet étudiant devra s'assurer de la qualité des délivrables (rapports, code, documentation, schémas). Cela ne veut pas dire que le responsable doive produire complètement les éléments en question, mais plutôt qu'il doit s'assurer que chacun ait réalisé ce qu'il s'était

engagé à produire, que la mise en page et l'orthographe des documents soient correctes, et que les délivrables soient soumis dans les temps et le respect des consignes.

8.2 Prise en main et sécurisation des VPS

La première étape du projet consiste à sécuriser vos VPS. Vous avez vu comment configurer et sécuriser un accès SSH distant par clé, c'est le moment de l'appliquer chacun à votre VPS. Il vous est également demandé de configurer un accès pour le professeur, à savoir un compte `vvandens` avec la clé publique disponible sur le site Moodle. Veuillez à ajouter cet utilisateur aux `sudoers`, et à le configurer avec le mot de passe `adminEphec2019`.

8.3 Phase d'analyse

Prenez le temps de bien lire l'énoncé, essayez de reformuler le cahier des charges pour la première mission avec vos propres mots, et dessinez un premier schéma réseau de l'entreprise. Une fois que vous vous êtes mis d'accord sur cette infrastructure, réfléchissez à comment l'implémenter à l'aide des VPS dont vous disposez. Cette phase vous permettra de produire votre première version des deux schémas réseaux demandés : il s'agit de documents de travail essentiels que vous devrez garder à jour et avoir avec vous à chaque séance !