IPSSI Ex Calibra

Une image contenant capture d’écran, Rectangle, Bleu électrique, bleu

Description générée automatiquement Une image contenant texte, Police, logo, Graphique

Description générée automatiquement

Stage Technicien Systèmes réseaux

Du 09 Mai au 05 Juillet

Tuteur de stage : Eugenie Firsova

Superviseur académique : Marie-Christine

Etablissement : BTS préparé à l’IPSSI

Entreprise d’accueil : Ex Calibra (14 Rue des Messageries)

**REMERCIEMENTS**

Je tiens tout d’abord à remercier l’**IPSSI**, et particulièrement **Maxime DEVAINON** pour m’avoir fait confiance. L’écoute et l’accompagnement dont j’ai bénéficié m’ont permis de trouver rapidement un stage, dans le but d’affiner mes compétences acquises en classes.

Je pense également à Monsieur **Antoine Balavoine** fondateur de l’entreprise de l’entreprise, qui a cru en mon potentiel et m’a accueilli au sein de son entreprise.

A ce titre, je souhaiterai remercier tout particulièrement Madame **Eugenie Firsova** administratrice Systèmes Réseaux, qui m’a épaulée et conseillée et qui m’a surtout transmis son expertise dans le domaine des **Systèmes** et **Réseaux**.

Ce stage m’a permis d’affiner certaines pistes pour mon orientation professionnelle et constitue l’aboutissement de ma première année de BTS SIO Option SISR.

**SOMMAIRE**

INTRODUCTION

**I-) Présentation de la société**

1.Présentation

2.Domaines d’activités

3.Les clients

**II-) Consolidation des compétences**

1.Les missions

2.Les outils mis à ma disposition

3.Compétences personnelles et professionnelles acquises

**III-) Projet de stage**

Conclusion

INTRODUCTION

Etant étudiant en première année BTS SIO Option SISR à l’IPSSI, j’ai effectué un stage au sein de l’entreprise Ex Calibra du 09 Mai au 05 Juillet. Durant ce stage j’ai acquis des compétences dans le domaine Systèmes Réseaux sous la supervision de **Eugenie Firsova** l’administratrice Systèmes Réseaux de l’entreprise. Je vais vous présenter dans ce mémoire mon parcours durant ce stage.

**I-) Présentation de la société**

1.Présentation

Ex Calibra signifie littéralement "en dehors du calibre", cela exprime que la société est en gros différente des autres, cela met en valeur leur capacité à être à l'écoute de leurs clients et de leurs besoins, de s'y adapter au plus juste.

Créer le 1er septembre 2001 par Mr. **Antoine Balavoine**, Ex Calibra est une Société à responsabilité limitée situé au 14 Rue des Messageries offrant des services et conseils informatique.

2.Domaines d’activités

* Ventes de matériel informatique : serveurs, routeurs, ordinateurs, imprimantes etc.
* Développement web : site web pour des entreprises, applications mobiles, bases de données, maintenance de fonctionnalités etc.
* Gestion de Systèmes et Réseaux : migration de boîtes mails, gestion et mise en place de serveurs Windows, sauvegardes de données clients, installations et configuration d’antivirus et antimalwares, mise en place de stratégies de groupes pour des clients, mise en place et gestion des réseaux d’entreprises etc.

3.Les clients

La clientèle de Ex Calibra est très vaste. Elle est constituée en somme de : cabinet dentaire, cabinet d’avocats, particuliers etc.

**II-) Consolidation des compétences**

1.Les missions

* **Dépannage d’une imprimante (15 mai 2023) :**

Le client de Ex Calibra nous a contacté pour nous faire part d’un problème avec une de leurs imprimantes qui ne fonctionnait pas. Ma responsable de stage et moi nous rendions sur place pour analyser le problème.

1. **Etape 1 :** Constat

L’imprimante s’allumait mais indiquait des voyant d’erreurs.

D’après la documentation technique de l’imprimante les erreurs correspondaient à un souci sur le firmware.

1. **Etape 2 :** Installation du firmware

Ma responsable de stage me chargea d’essayer de résoudre le problème.

Elle m’a fait part d’un **Firmware** qu’il fallait installer sur mon pc pour réinitialiser l’imprimante.

L’imprimante était de la marque HP il fallait donc installer le firmware correspondant au modèle de l’imprimante. Dans les étapes à suivre lors de l’installation du logiciel firmware il y’en avait une où il fallait entrer l’adresse IP de l’imprimante en question. Mais au début je ne disposais pas de moyen de connaître l’adresse IP de l’imprimante car il n’y a pas d’interface visuelle pour savoir.

1. **Etape 3 :** Adressage IP de l’imprimante

Ma responsable de stage me parla alors d’un logiciel nommé **Advanced IP Scanner,** qui permet de faire un scan réseaux et de voir le nom et l’adresse IP de tous les appareils connectés sur le réseau. J’ai donc branché un câble Ethernet sur mon pc et également sur l’imprimante pour pouvoir lancer le scan.

Il fallait également entrer la plage de sous-réseau dans laquelle se situe le réseau de l’entreprise. Le scan effectué tous les appareils connectés au réseau apparût sauf l’imprimante.

Après réflexion on m’a expliqué que la carte réseau de l’imprimante devait être configuré en IP fixe. Nous avons donc dû récupérer la configuration du réseau local du client

J’ai donc connecté mon pc à l’imprimante grâce à un câble adapté. Et essayé de détecter l’imprimante en câblé, mais cela ne fonctionnait pas car mon pc était en DHCP, ma responsable de stage me proposa de le mettre en IP fixe, sauf qu’en IP fixe on n’a pas accès à la connexion internet pour détecter l’imprimante sur le firmware. J’ai donc mis mon pc en IP fixe et en même temps branché le câble Ethernet pour avoir accès à internet. Donc mon pc était en IP fixe comme l’imprimante et il avait accès à internet en Ethernet comme l’imprimante. Ce qui me permit de détecter l’imprimante sur le firmware et de connaître la plage d’adresse IP dans laquelle se situait son adresse IP et de faire un autre scan réseau pour ensuite savoir l’adresse IP de l’imprimante et de l’entrée sur le firmware pour le configurer et changer l’adresse IP de l’imprimante et la mettre en DHCP pour qu’elle puisse avoir une adresse IP aléatoire et correct sur le réseau de l’entreprise.

1. **Etape 4 :** Remise en état de l’imprimante chez le client

Après ça on pouvait maintenant détecter l’imprimante et imprimer une page test pour voir si on pouvait imprimer et tout était bon. Nous avions donc renvoyé l’imprimante chez le client et la configurer sur le réseau de leur cabinet et imprimé des pages test. L’imprimante fonctionnais à merveille.

* **Création d’une GPO via Windows Serveur 2019 (du 16 Mai 2023 au 29 Mai 2023):**

Un des clients d’Ex Calibra (une bibliothèque) avait besoin d’utiliser des postes publics. Anciennement ils possédaient un logiciel qui gérer ces postes publics mais à la suite d’un changement serveur vers une version de Windows Serveur plus récente le logiciel est devenu incompatible et l’upgrade du logiciel à un coup trop élevée pour le client.

Nous avons donc proposé une solution via les GPO afin de mettre en place les restrictions utilisateurs / logiciels.

1. **Etape 1 :** Migration d’un contrôleur de domaine de Windows Serveur 2012-16 vers Windows Serveur2019

On m’a demandé d’essayer de faire une migration d’un contrôleur de domaine du Serveur test de l’entreprise. Dans le cas où il faudra migrer celui de la bibliothèque. Pour ce faire j’ai procédé comme suit :

* Installation de Windows Serveur 2019 en virtuel avec Hyper V
* Installation du nouveau contrôleur de domaine sur Windows Serveur 2019
* Migration des rôles FSMO (Flexible Single Master Operation, ce sont des rôles qui permettent de donner les droits prioritaires). Dans le cadre de la migration vers Windows serveur 2019, le 2012 est le serveur principal qui possède les droits prioritaires donc la migration des rôles FSMO sur la machine virtuelle Windows serveur 2019 va donner la priorité au serveur 2019 et il deviendra alors le serveur principal pour le contrôleur de domaine. Pour la migration on peut la faire via l’interface des stratégies de groupes ou en ligne de commande PowerShell. Il y’a 5 rôles en tout :

1. Contrôleur de schéma
2. Maître d’opération des noms de domaine
3. Maître RID
4. Emulateur PDC
5. Maître d’infrastructure

Il faut faire la commande **netdom query fsmo** pour voir sur quel domaine se situe tel rôle (chaque rôle est suivi du domaine dans lequel ils sont intégré).

Pour les migrer on suit les commandes dans l’ordre sur le powershell :

- on fait d’abord Windows+R et on écrit **ntdsutil.exe** et **ok**

- **rôle**

- **connections**

- **connect to server** « nom du serveur »

- **transfer** « nom du rôle »

Et enfin on refait **netdom query fsmo** pour vérifier si tout est bon.

1. **Etape 2 :** Création de la GPO

La seconde étape va consister à la création de la GPO.

Nous pouvons ouvrir soit l’application **Gestionnaire de stratégie de groupe** depuis le menu démarrer,ou depuis le **Gestionnaire de serveur** on suit le chemin suivant : Outils 🡺 Gestion des stratégies de groupe.

On fait clic droit sur le nom de domaine et on clique sur « **Créer un objet GPO dans ce domaine, et le lier ici »** et on donne un nom à notre GPO. Ensuite on fait un clic droit sur notre GPO créée et on fait **Appliquer** et **Modifier**.

Pendant la modification on active et désactive les paramètres en fonctions des restrictions que nous voulons ajouter sur les sessions publiques des PC de la bibliothèque.

1. **Etape 3 :** Sauvegarde et ajout de la GPO sur les sessions publiques

Après configuration complète de la GPO, nous avons fait une sauvegarde des paramètres de la GPO dans un dossier enregistré sur le Windows serveur 2019, sommes connecté au serveur de la bibliothèque en connexion à distance et avons transféré le fichier de sauvegarde des paramètres de la GPO sur le serveur du client, dans une GPO vide avec le même nom que celle donné pendant la création sur notre serveur test. Après quoi nous avons pu lier la GPO à leur domaine.

* **Migration de mail vers Office 365 et ajout de DKIM sur des hébergeurs de domaine (Amen, OVH, Gandi, Viaduc etc) (durant toute la période du stage)**

Certains de nos clients ont leurs boites mail et leur domaine héberger sur des hébergeurs particuliers. Cependant ces hébergeurs particuliers ne sont pas à 100% sécurisé et n’ont pas assez d’espaces de stockage pour les mails sauf pour les domaines. Les clients ont donc opté pour une migration de leur serveurs mail vers Office 365 pour plus de sécurité. Office 365 est beaucoup utilisé pour l’hébergement mail et les signatures DKIM de nos jours.

1. **Etape 1 :** Office 365

Premièrement, il faut se connecter au compte Microsoft Office 365 du client avec l’identifiant admin (qui nous permet d’avoir accès au paramètre supplémentaire de sécurité).

Dans **Panneau de configuration** on clique sur mail pour effectuer la configuration de la boite mail actuelle du client, à ce niveau-là, nous avons deux types de configuration qui se présente :

- Configuration dite « automatique » c’est quand la boite est déjà hébergée chez Microsoft, nous avons besoins de renseigner seulement les identifiants de connexion de la boite mail

- Configuration dite « manuelle » c’est quand la boite est hébergée autre part que chez Microsoft (ovh, hébergement privé, amen …etc). La configuration ce fait alors de façon manuelle dans la quel nous avons besoins de renseigner le serveur IMAP ou POP et SMTP ainsi que les ports respectifs de ces serveurs en plus de l’identifiant de connexion de la boite mail (adresse mail / mot de passe).

\*La configuration automatique/manuelle de ces boîtes mails est nécessaire pour pouvoir récupérer toute l’historique avant le lancement de la procédure de migration.

Par la suite nous allons sur Office 365 dans l’onglet **Admin** dans la section à gauche. Dans **Utilisateur** on fait **+Ajouter un utilisateur** et on ajoute l’adresse mail du client avec le domaine par défaut (en @*nomdudomaine*.onmicrosoft.com).

- On va dans **Paramètre** dans l’onglet à gauche puis dans **Domaines** et on clique sur **+Ajouter un domaine** et on ajoute le domaine du client. Microsoft va ensuite faire une vérification d’appartenance du domaine en nous indiquant les différents enregistrement DNS à renseigner chez l’hébergeur du domaine.

Après avoir eu la confirmation que le domaine est sain auprès de Microsoft 365 on doit se rendre de nouveau dans les comptes utilisateurs et modifier le domaine de/des boite(s) mail(s).

Après avoir finalisée les étapes coté Office 365, on peut se connecter avec la nouvelle adresse mail du client sur le même logiciel de messagerie et on importe son historique des mails précédemment synchronisée sur un poste (Qui était hébergé sur les serveurs tiers à Microsoft).

1. **Etape 2 :** Le DKIM

Le DKIM (DomainKeys Identified Mail), est un protocole qui permet de générer des signatures électroniques à l’envoie de nos mails qui sont vérifiables par Microsoft ou n’importe quel fournisseur de boîtes mail par une méthode d’authentification cryptographique. C’est en quelque sorte un moyen fiable et sécurisé de contrôler les mails.

Pour tous nos clients ayant leur boîtes mails maintenant hébergé par Microsoft, nous avons gardé les domaines hébergés chez les hébergeurs particulier car c’est plus pratique. Mais Microsoft doit pouvoir faire une vérification de l’authenticité de ces hébergeurs. Pour ce faire il faut configurer le DKIM de Microsoft sur ces hébergeurs. La méthode varie selon l’interface en ligne de chaque hébergeur.

* + - Sur Office 365 on va dans l’onglet **Admin** à gauche
    - Sur la nouvelle page qui s’affiche on va dans l’onglet à gauche dans la partie **Centre d’administration** et on clique sur **Sécurité**
    - Une nouvelle page s’ouvre et toujours à gauche on va dans l’onglet **Stratégies et règles 🡺 Stratégies de menace 🡺 Règles (Paramètre d’authentification des e-mails) 🡺 Onglet DKIM**
    - On clique sur le domaine que nous ajouter dans les étapes de synchronisation de la boîte mail du client avec le bon alias
    - On active l’interrupteur **Signer les courriers pour ce domaine en utilisant des signatures DKIM (**qui ne s’active pas parce que les enregistrement DNS ne sont pas effectué**)**
    - Puis dans la fenêtre qui s’ouvre on entre les informations données par Office 365 sur la partie du site de l’hébergeur de domaine qui concerne les enregistrement DNS (qui est aléatoire pour chaque hébergeur, il faut donc s’adapter à chaque interface, impossible de prévoir)
    - Une que les enregistrements fournis par Office 365 sont ajoutés sur le site de l’hébergeur de domaine on attend 5 à 10 min pour réactiver l’interrupteur **Signer les courriers pour ce domaine en utilisant des signatures DKIM**. Une fois qu’il s’active tout est bon

**NB :** Parfois l’attente pour l’activation de la signature DKIM du domaine peut aller au-delà de 10 min voire quelques jours. Tout dépend des serveurs.

2.Les outils mis à ma disposition

Durant ce stage j’ai appris à utiliser plusieurs outils. Certains que je connaissais déjà et d’autre que non.

* **Environnement MAC OS**

Ayant toujours exercé sur du Windows, je me suis beaucoup familiarisé avec l’environnement MAC OS durant mon stage. La majorité des clients de Ex Calibra travaillent avec des MAC. En effet l’environnement Mac est certes limité mais est plus sécurisé. Mais si on veut faire des trucs spécifiques on peut toujours installer des machines virtuelles Windows sur Mac. Certains des clients ayant des logiciels métiers compatibles qu’avec Windows on pouvait installer des VM sur les postes Mac.

* **Outil de contrôle à distance (TeamViewer)**

Nous connaissons tous l’interface de Bureau à distance fournie sur Windows. Mais elle a des limites car la personne qui veut prendre en main un appareil avec Bureau à distance doit être sur le même réseau que l’ordinateur cible et avoir les droits d’administrateur sur le réseau. Pourtant tous les clients sont dans des sociétés différentes par conséquences sur des réseaux différents. Et parfois il faut intervenir sur les postes à distances de plusieurs clients en simultané donc impossible de se déplacer.

L’outils **TeamViewer** est un outil qui permet de prendre en main un poste ou un appareil à distance en ayant l’ID et le mot de passe de l’appareil cible. Et on a la possibilité de créer un réseau de prises en main en enregistrant les nom des postes sans avoir à mettre l’ID et le mot de passe et aussi de les classer par entreprises (par clients).

* **Advanced IP scanner**

Cet outil permet de scanner le réseau sur lequel on se situe, de voir l’adresse IP/MAC de tous les appareils connectés sur ce réseau et même d’interagir avec ces appareils.

On peut explorer les fichiers de l’appareils

On peut lancer des requêtes ping, telnet, ssh etc.

On peut transférer des fichiers

On peut prendre en main

On peut envoyer des messages etc.

* **Synology NAS**

Synology NAS est un logiciel qui permet de partager et de synchroniser des fichiers et des données tout en ayant un contrôle total sur tous les partages et les synchronisations. Les NAS de Synology peuvent stocker de gros volumes de données et la capacité de stockage dépend évidemment des disques qu’on y installe.

On peut configurer des RAID sur Synology ce qui permet de prévenir des éventuelles pannes de NAS.

Par exemple si sur un serveur de type NAS qui contient 5 disques on en a 2 qui tombent en panne, un RAID2 va permettre de synchroniser et de répartir les données et le stockage de ces 2 disques sur les trois autres qui fonctionnent.

Il existe des RAID (0,1,2,5,20 etc) suivant la même logique en fonction du nombre de disques.

3.Compétences personnelles et professionnelles acquises

* **Les recherches**

Dans le domaine des systèmes et réseaux, il est souvent nécessaire de faire beaucoup de recherches. Par exemples dans le cadre des ajouts des enregistrements DNS pour la signature DKIM de Microsoft sur les hébergeurs. Il a fallu chercher sur google comment faire ses ajouts parce que les interfaces sont différentes. Dans toutes les missions que j’ai effectué durant mon stage j’ai fait beaucoup de recherche. Ce qui m’a permis de développer et d’améliorer ma capacité à m’adapter en effectuant des recherches.

* **La patience**

La patience n’est pas une qualité à avoir seulement dans notre quotidien. Elle peut être très utile en entreprise ; surtout dans le domaine des Systèmes et Réseaux.

Par exemple la confirmation de l’ajout DKIM par un hébergeur peut prendre 2 à 4 jour si l’hébergeur n’est pas toujours actif.

Ou durant une intervention sur place chez un client, le client peut avoir plusieurs questions et plusieurs situations à présenter. Et il faut être à l’écoute et patient avec eux. Ne pas donner l’impression d’être dérangé ou d’être en situation compliqué par rapport aux demande supplémentaires du client.

* **Troisième compétence**

CONCLUSION