Présentation projet SAE 24

Intégration d'un réseau local professionnel pour un cabinet de médecine

AUTEUR:

ALBINET Gabriel
PIQUER Joachim
JOBARD Yanis
LAURET Alexis
TOURRET Clément

Contexte :

Notre entreprise a été contactée par un client pour mettre en place un réseau informatique. L'entreprise en question est un cabinet de médecine. Ce dernier, s'étant installé récemment, voit sa clientèle grandir de jour en jour. Le cabinet se retrouve donc avec une quantité de données, de documents et de demandes bien trop élevée pour son maigre réseau informatique. De plus, l'effectif s'étant agrandi avec l'arrivée d'un nouveau comptable, le réseau informatique actuel du cabinet n'est non seulement plus adapté à l'offre médical proposée, mais elle ne l'est plus aussi pour l'effectif.

Tout cela mène à des besoins divers dans l'aménagement d'un nouveau réseau informatique, et la solution que nous avons préparée a été élaborée par rapport à ces nécessités croissantes.

I. Besoins de la clientèle

Parmi les besoins de la clientèle, il y a tout d'abord la gestion des documents administratifs qui se pose afin de gérer les fichiers concernant les divers patients, par exemple.
Il y a également des besoins au niveau de la communication. En effet le secrétaire, le médecin et le comptable nécessitent d'avoir la capacité de communiquer par mail, par téléphone et par visioconférence pour des réunions en distanciel.

Concernant l'ergonomie, l'absence de publicités et de virus sur les ordinateurs du cabinet sera aussi de mise. D'autres points divers sur ce sujet, comme l'accès (limité) au point d'accès en salle d'attente ou l'existence d'un site web pour le cabinet seront aussi à prévoir.

Besoins	Solutions
Gestions des documents administratifs	Mise en place d'un serveur ftp et d'un réseau sécurisé.
La salle d'attente doit avoir un accès wifi pour les patients	Mise en place d'une AP Wifi en accès libre et le sécuriser pour que les patients ne puissent pas avoir accès aux autre PC
La secrétaire, le médecin et le comptable doivent pouvoir communiquer par mail	mise en place d'un service de messagerie sous linux (**Postfix**)
Site Web	Mise en place d'un site Web pour le cabinet (**Apache 2**)
La secrétaire, le médecin et le comptable doivent pouvoir communiquer par téléphones	Mise en place de téléphone IP ou softphone. Les ajouter dans le call server sous linux. (**Asterisk**)
Conférences et réunions à distance	installation de myspace et activation de la licence sur le Call server

Ne veut pas de publicité sur les postes de travail.	Mise en place d'un logiciel bloqueur de PUB.(**pihole**)
Pas de virus sur les PC	Installation d'un antivirus sur chaque poste. (**Avast**)

Pour répondre à ces besoins, nous avons élaboré plusieurs solutions, parfois regroupées sous un seul et même service :

Gestion centralisée des utilisateurs, des ressources et de la sécurité avec Active Directory

Mise en place d'un Active Directory (AD) pour centraliser la gestion des utilisateurs, des groupes, des ordinateurs et des ressources réseau du cabinet. (IAM, etc)

Gestion des sessions utilisateurs avec Active Directory : Authentification et autorisation des utilisateurs pour l'accès aux ressources réseau en fonction de leurs profils et de leurs rôles.

Service DHCP avec Active Directory : Attribution automatique d'adresses IP aux appareils du réseau pour une configuration simplifiée et une meilleure gestion des adresses IP.

Mise à jour automatique des logiciels et des postes avec Active Directory : Déploiement centralisé des mises à jour logicielles et des correctifs de sécurité pour protéger les ordinateurs contre les vulnérabilités et les cybermenaces.

Protection des fichiers avec Active Directory : Mise en place de stratégies pour protéger les données stockées sur les PCs du réseau.

Accès sécurisé à distance avec SSH

Activation du service SSH sur les PC pour permettre au serveur administrateur de configurer et d'accéder à distance aux différents ordinateurs du cabinet en toute sécurité.

Connexion chiffrée : Utilisation d'un protocole de communication sécurisé pour protéger les données transmises entre le serveur administrateur et les ordinateurs du cabinet.

Authentification par clé : Authentification forte basée sur des clés cryptographiques pour garantir que seul le serveur administrateur autorisé peut accéder aux ordinateurs du cabinet.

Contrôle d'accès : Définition de permissions précises pour contrôler les actions que le serveur administrateur peut effectuer sur chaque ordinateur du cabinet.

Améliorer la communication et la collaboration au sein du cabinet

Système de téléphonie VoIP avec Asterisk garantissant la disponibilité des appels et des fonctionnalités avancées pour une communication fluide avec les patients et les partenaires.

Solution de messagerie instantanée avec Postfix facilitant les échanges rapides et efficaces entre les membres du personnel pour une meilleure coordination des tâches.

Outil MySpace Conférence permettant d'organiser des réunions et des visioconférences en ligne de manière simple et intuitive pour une collaboration à distance optimale.

Renforcer la sécurité des données et du système informatique

Antivirus et anti-malware performants tels que Avast pour protéger les ordinateurs contre les virus, les malwares et autres cybermenaces, garantissant la sécurité des données sensibles des patients.

Pare-feu robuste bloquant les intrusions et les accès non autorisés au réseau du cabinet pour prévenir les attaques informatiques.

Outil de détection d'intrusion (IDS) tel que Snort, Suricata ou Zeek identifiant et bloquant les tentatives d'intrusion en temps réel pour une protection proactive contre les cyberattaques.

Un anti-spam efficace tel que MailCleaner filtrant les emails indésirables et protégeant les boîtes de réception contre le spam et les attaques par hameçonnage pour un environnement de travail numérique sain.

Assurer un stockage et une accessibilité des données sécurisés

Serveur NAS tel que Unraid centralisant le stockage des données du cabinet de manière sécurisée et accessible à tous les membres du personnel autorisés pour une gestion centralisée des informations.

Système de sauvegarde automatique avec Rsync garantissant la protection des données critiques en cas de panne ou de sinistre pour une continuité d'activité infaillible.

Synchronisation d'horloge précise tel que LinuxPPS pour les PCs Linux et Microsoft Windows Time Service (W32Time) pour les PCs Windows entre tous les appareils du réseau pour une meilleure coordination des activités et une gestion du temps optimisée.

Contrôler l'accès aux informations et aux ressources

Système RDS/accès à distance avec TeamViewer permettant aux médecins et au personnel autorisé d'accéder aux dossiers patients et aux applications du cabinet à distance en toute sécurité pour une flexibilité accrue dans le travail.

Réseau privé virtuel (VPN) avec TunnelBear sécurisant les connexions à distance et protégeant les données sensibles lors des déplacements pour un accès confidentiel aux informations du cabinet.

Contrôle d'accès restreignant l'accès aux sites web illégaux ou non professionnels au sein du réseau du cabinet pour un environnement de travail numérique sécurisé et approprié.

Optimiser la gestion du cabinet grâce à des outils et applications métiers

Serveur FTP avec FileZilla Server facilitant le transfert de fichiers volumineux entre les membres du personnel et les partenaires externes pour une collaboration fluide dans le partage d'informations.

Site web professionnel avec Apache 2 présentant le cabinet, ses services et ses coordonnées aux patients potentiels pour une meilleure visibilité et une communication efficace avec la patientèle.

Base de données sécurisée permettant de gérer efficacement les données des patients, les inventaires de médicaments et les profils des employés pour une organisation optimale des informations du cabinet.

Bloqueur de PUB avec pihole améliorant la productivité en bloquant les publicités et les sites web non pertinents pour un environnement de travail concentré et performant.

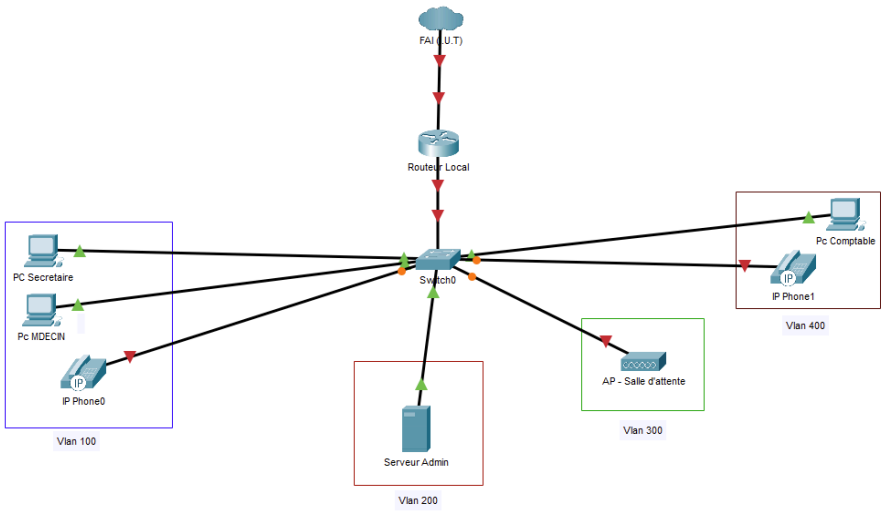
AP WiFi offrant une connexion WiFi sécurisée et performante aux patients et aux visiteurs dans l'enceinte du cabinet pour un accès internet facile et fluide.

Surveiller et maintenir le système informatique pour une performance optimale

Système de surveillance du fonctionnement avec SolarWinds suivant les performances du réseau, des serveurs et des applications pour une identification rapide des problèmes potentiels et une résolution proactive des incidents.

II. Présentation de la topologie globale (physique)

Pour répondre à ces besoins, il faudra mettre en place cette topologie :



Cette topologie comprend plusieurs éléments, dont des ordinateurs, des téléphones VoIP, un serveur, un routeur, un commutateur et un point d'accès Wi-Fi. Le réseau est divisé en quatre VLAN (réseaux virtuels locaux) pour séparer le trafic et améliorer la sécurité.

Éléments du réseau

- **Ordinateurs:** Il y a trois ordinateurs qui seront utilisés par les membres du cabinet.
- **Téléphones VoIP:** Il y a trois téléphones VoIP qui permettront aux membres du cabinet de communiquer entre eux.
- **Serveur Admin:** Le serveur Admin centralise les services du cabinet, tels que le stockage des fichiers et les applications.
- **Point d'accès Wi-Fi:** Le point d'accès Wi-Fi permettra aux patients et aux visiteurs d'accéder à Internet dans la salle d'attente.

- **Routeur:** Le routeur connecte le réseau au fournisseur d'accès Internet (FAI) et permet aux appareils du réseau d'accéder à Internet.
- **Pare-feu :** Il va permettre de gérer le traffic entrant dans votre réseau et d'y implémenter des éléments de sécurité.
- **Switch :** Le commutateur connecte les ordinateurs, les téléphones VoIP et le serveur Admin au routeur.

VLAN

Des VLAN seront utilisés pour diviser le réseau en plusieurs réseaux virtuels. Cela permet de séparer le trafic et d'améliorer la sécurité. Dans ce schéma, il y a quatre VLAN :

- **VLAN 100:** Ce VLAN est utilisé pour les ordinateurs.
- **VLAN 200:** Ce VLAN est utilisé pour les téléphones VoIP.
- **VLAN 300:** Ce VLAN est utilisé pour le serveur Admin.
- **VLAN 400:** Ce VLAN est utilisé pour le point d'accès Wi-Fi.

Fonctionnement du réseau

Chacun de ces réseaux sera réparti en Vlan, des réseaux virtuels. Bien que le FAI nous à fournis des adresses ip publiques, notre configuration ip sera la suivante :

- Vlan 100 : Vlan destinée à l'administration du réseau
- Vlan 200 : Vlan Wi-Fi
- Vlan 300 : Vlan destiné au comptable
- Vlan 400 : Vlan pour le médecin et la secrétaire

III. Déroulé de la mise en place des services et des éléments du réseau

1) Installation des systèmes d'exploitation

- Installation des O.S Windows 11 pro sur les clients
- Installation de Windows Server sur le serveur

2) Infrastructure réseau (physique)

- Branchement au switch des terminaux (Téléphones et Postes de travail.)
- Branchement au switch du routeur
- Branchement au switch de l'A.P wifi.

3) Configuration réseau

- Sur le switch configurer les différents Vlan (100, 200, 300, 400)
- Sur le routeur, configurer le routage inter-Vlan
- Mise en place d'un DHCP
- Sur le routeur, configurer un PAT pour permettre l'accès internet au réseau

4) Sécurité et accès

- Installation et configuration de l'Active directory
- Définir les utilisateurs et la gestion des politiques de sécurité sur l'A.D
- Activer SSH sur les terminaux et les commutateurs

5) Services de communication

- Installer et configurer astérisk (serveur d'appel)
- Ajout de softphone sur les postes
- Installation et configuration de Postfix (serveur mail)
- Configuration des comptes de messagerie pour les médecins
- Installation et configuration de Myspace Conférences

6) Protection et sécurité

- Installer Avast sur les postes de travail
- Configurer les MAJ automatiques et les scans réguliers
- Mettre en place Pi-hole (anti-pub)
- Configurer et intégrer le pare-feu au réseau

7) Stockage et accessibilité

- Installer et configurer un NAS avec OpenMediaVault
- Mise en place de Rsync
- Configuration de Team Viewer
- Mise en place VPN avec TunnelBear
- Mise en place d'un serveur ftp

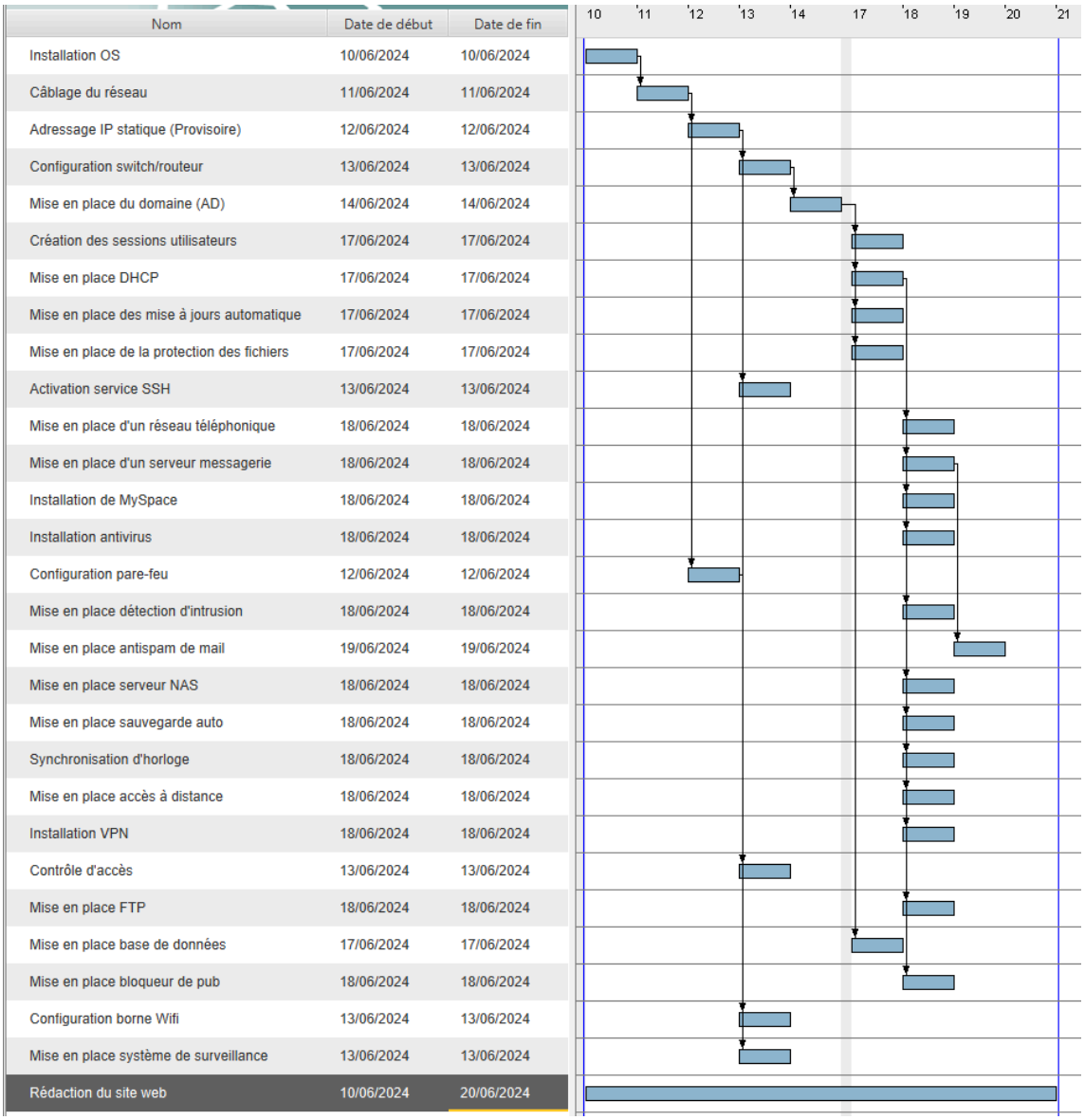
8) Surveillance et maintenance

- Installation SolarWinds (performances réseaux)
- Configurer les alertes pour identifier les problèmes

9) Finalisation et Test

- Faire les tests de tous les services pour vérifier le bon fonctionnement de tous les services et la sécurité du réseau

IV. Répartition des tâches



Nom	Date de début	Date de fin
Installation OS	10/06/2024	10/06/2024
Câblage du réseau	11/06/2024	11/06/2024
Adressage IP statique (Provisoire)	12/06/2024	12/06/2024
Configuration switch/routeur	13/06/2024	13/06/2024
Mise en place du domaine (AD)	14/06/2024	14/06/2024
Création des sessions utilisateurs	17/06/2024	17/06/2024
Mise en place DHCP	17/06/2024	17/06/2024
Mise en place des mise à jours automatique	17/06/2024	17/06/2024
Mise en place de la protection des fichiers	17/06/2024	17/06/2024
Activation service SSH	13/06/2024	13/06/2024
Mise en place d'un réseau téléphonique	18/06/2024	18/06/2024
Mise en place d'un serveur messagerie	18/06/2024	18/06/2024
Installation de MySpace	18/06/2024	18/06/2024
Installation antivirus	18/06/2024	18/06/2024
Configuration pare-feu	12/06/2024	12/06/2024
Mise en place détection d'intrusion	18/06/2024	18/06/2024
Mise en place antispam de mail	19/06/2024	19/06/2024
Mise en place serveur NAS	18/06/2024	18/06/2024
Mise en place sauvegarde auto	18/06/2024	18/06/2024
Synchronisation d'horloge	18/06/2024	18/06/2024
Mise en place accès à distance	18/06/2024	18/06/2024
Installation VPN	18/06/2024	18/06/2024
Contrôle d'accès	13/06/2024	13/06/2024
Mise en place FTP	18/06/2024	18/06/2024
Mise en place base de données	17/06/2024	17/06/2024
Mise en place bloqueur de pub	18/06/2024	18/06/2024
Configuration borne Wifi	13/06/2024	13/06/2024
Mise en place système de surveillance	13/06/2024	13/06/2024
Rédaction du site web	10/06/2024	20/06/2024

Afin de réaliser ces solutions dans les délais requis, nous allons devoir nous répartir les tâches à effectuer.

Tâche effectué ensemble	- Installation des OS - Câblage du réseau

Gabriel	- Adressage IP statique (Provisoire) - Activation SSH - Mise en place du domaine (AD) - Mise en place d'un réseau téléphonique - Mise en place serveur NAS
Joachim	- Configuration du pare-feu - Mise en place système de surveillance - Mise en place de la protection des fichiers - Mise en place d'un serveur de messagerie - Mise en place sauvegarde auto
Yanis	- Configuration switch / routeur - Création des utilisateurs - Mise en place de la base de données - Installation de MySpace - Synchronisation des horloges
Alexis	- Control d'accès - Mise en place du DHCP - Installation antivirus - Mise en place antispam de mail - Mise en place accès à distance - Mise en place FTP
Clément	- Configuration borne wifi - Mise en place des mises à jour automatique - Mise en place détection

	d'intrusion - Installation VPN - Mise en place bloqueur de PUB

Création du site Web :

Le site web comporte le compte rendu de la mise en place de l'infrastructure réseau établie durant les 2 semaines. Voici la page d'accueil du cabinet.

Dans la catégorie "Renouveau informatique du cabinet" nous avons renseigné l'ensemble des outils configurés lors du projet.

Nous avons donc configuré un serveur Windows Active Directory avec les services suivants : serveur web, DHCP, et système de sauvegarde. Par la suite, nous avons configuré un serveur Linux hébergeant un serveur téléphonique et un serveur de messagerie. Pour finir, nous avons configuré un switch et un routeur.

Configuration du switch

Sur le switch, on commence par configurer les VLANs.

```
Switch (config)#vlan 100
Switch (config-vlan)#name admin
```

Ensuite, on attribue des ports à chaque VLAN.

```
Switch (config)#int range fastEthernet 0/1 fastEthernet 0/3
Switch (config-if-range)#

Switch(config-if-range)#switchport mode access
Switch (config-if-range) #switchport access vlan 100
```

On configure ensuite le mode trunk sur le port connecté au routeur.

```
Switch (config)#int fastEthernet 0/23
Switch (config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 100,200,300,400
```

Enfin, on attribue des adresses IP aux VLANs pour l'accès à distance.

```
Switch (config-if)#int vlan 100
Switch (config-if)#

Switch (config-if)#ip address 192.168.1.100 255.255.255.0
```

Configuration du routeur :

Sur le routeur, on va créer des sous-interfaces, préciser leur VLAN d'appartenance et leurs adresses IP.

Chaque sous-interface sera la passerelle du sous-réseau virtuel que l'on aura précisé (exemple VLAN 100):

Router (config)#int gigabitEthernet 0/1.1
Router (config-subif)#encapsulation dot1q 100

Router (config-subif)#ip add
Router (config-subif)#ip address 192.168.1.200 255.255.255.0

Ici, on crée la sous-interface 1 qui sera encapsulée sur VLAN 100 et qui aura l'IP 192.168.1.200.

On fera la même chose pour les autres VLAN en remplaçant '100' par le VLAN voulu.

Maintenant que notre réseau LAN est configuré, on va tenter de le rendre accessible sur internet.

D'abord, on configure l'interface qui sera connectée au réseau de l'IUT:

Router (config)#int gigabitEthernet 0/2
Router (config-if)#ip address 172.25.0.150 255.255.0.0

Dans un premier temps, on configure une route par défaut qui envoie vers la passerelle de l'IUT:

Router (config)#ip route 0.0.0.0 0.0.0.0 172.25.255.254

Ensuite, on va préciser les interfaces qui seront dans un réseau privé (NAT inside) ici seront les sous-interfaces que l'on aura faites précédemment :

Router (config)#int gigabitEthernet 0/1.1
Router (config-subif)#ip nat inside

On fait de même pour les 3 autres sous-interfaces. On précise ensuite l'interface côté réseau public (celle reliée à l'IUT):

Router (config)#int gigabitEthernet 0/2
Router (config-if)#ip nat outside

On va créer une ACL pour dire que l'on autorise le trafic provenant d'une IP voulue :

Router (config)#access-list 1 permit 192.168.1.0 0.0.0.255
On va faire la même access-list pour chaque sous-réseau. On changera ici l'IP qu'on autorise et le numéro de l'access-list (ici 1). Chaque sous-réseau aura une access-list avec un numéro différent.

Enfin, on va créer une règle de NAT avec surcharge pour chaque access list que l'on vient de créer (ici donc 1, 2, 3, 4). On précisera l'interface connectée au réseau de l'IUT.

Router (config)#ip nat inside source list 1-4 interface gigabit Ethernet 0/2

Windows serveur

Active directory :

Activation de l'Active Directory et du DNS

Contexte

Pour configurer le DNS ainsi que le DHCP nous allons avoir besoin de l’Active Directory pour avoir une base de données centralisée.

Déroulé

Pour faire la création d’un domaine Active Directory on va avoir besoin d’un serveur DNS. C’est pour cela que nous installons le rôle DNS en même temps que le rôle AD DS.

Une fois que ces rôles sont installés, il faut redémarrer le serveur. Après le redémarrage, il faut promouvoir le serveur en tant que contrôleur de domaine.

Pour cela, il faut cliquer sur le drapeau présent sur le gestionnaire de serveur, puis cliquer sur « promouvoir ce serveur en contrôleur de domaine ».

Ensuite on clique sur « ajouter une nouvelle forêt » et à présent nous pouvons créer le domaine « cabinet.local ».

Pour finir la configuration, on suit les étapes indiquées, puis on redémarre le serveur pour que la promotion du domaine Active Directory soit prise en compte.

Nous devons créer ensuite deux unités organisationnelles. Pour faire cela on doit se connecter au contrôleur de domaine, puis ouvre la partie « Utilisateurs et ordinateurs Active Directory »

Finalement, on ajoute les deux unités organisationnelles que l'on nommera « Finance » « Secrétariat ». Puis dans chaque unité on créera 1 utilisateur.

A présent, on souhaite ajouter les PC clients au domaine. Pour ce faire, on fait un clique droit sur l'onglet « Ce PC », puis il faut cliquer sur « Propriétés », ensuite on clique sur « Renommer ce PC » et enfin on clique sur « Modifier ».

Ensuite on entre le nom de domaine du serveur Windows, et il ne reste plus qu'à rediriger le DNS de notre réseau vers celui de l'IUT pour permettre la navigation sur Internet.

Pour faire la redirection du DNS on va dans le gestionnaire de serveur, puis on va dans la configuration DNS. Ensuite on clique sur « Redirecteurs » et on ajoute l'adresse du serveur DNS de l'IUT.

Conclusion

Lors de cette partie, nous avons installé le DNS ainsi que le AD, puis on a créé des unités organisationnelles ainsi que des utilisateurs.

L'AD nous à permit de promouvoir le serveur en contrôleur de domaine. La création des utilisateurs à permis d'avoir plusieurs sessions sur les PC avec des autorisations d'accès différentes.

Configuration du partage de dossier

Contexte

Nous souhaitions créer un dossier sur le Windows serveur pour pouvoir le partager sur un autre PC et ainsi accéder au contenu de ce dossier.

Déroulé

Dans un premier temps, à la racine (C:) Sur le windows serveur on a dû créer un répertoire « Partage » ainsi que des sous-répertoires avec les nom des utilisateurs.

Ensuite on se rend sur les propriété du répertoire pour régler les propriété de partage en « accès Lecture/Écriture » pour tous les utilisateurs, puis on règle les sous-répertoires avec les noms des utilisateurs avec les autorisations que l'on souhaite.

Ensuite, sur Active Directory on se rend dans l'onglet « Services de fichiers et de stockage », puis dans l'onglet « Partages ». A présent, on crée une nouvelle tâche tout en suivant les étapes, on choisit l'emplacement du fichier que l'on souhaite partager.

Par la suite, nous mettons en place les autorisations sur le répertoire aux utilisateurs que l'on veut. Pour finir, on confirme et on crée la tâche.

Pour pouvoir accéder aux dossiers partagés via un PC client, on doit se rendre dans la partie réseau de l'explorateur de fichiers.

Ensuite on rentre dans la barre de recherche le chemin d'accès du serveur et du répertoire partagé : \\WIN-JRHHHKGMD1S\Partage (\\Nom_de_la_machine_server\Nom_du_répertoire_partagé).

Pour finir, nous avons seulement besoin d'épingler le dossier aux raccourcis rapides pour éviter une perte de temps inutile à retaper le chemin d'accès à chaque fois.

Conclusion

Dans cette partie on a créé dans un premier temps un répertoire avec des sous répertoires sur le Windows Serveur .

Ensuite on à mis en partage le répertoire à partir de l'active directory ou l'on a aussi intégrer des autorisations.

Enfin pour pouvoir avoir accès au répertoire sur le clients on rentre le chemin d'accès dans la barre de recherche présent sur l'explorateur de fichier. Par souci de rapidité, on place le dossier dans les raccourcis.

Configuration du DHCP :

Contexte

On a décidé de configurer un DHCP pour avoir l'attribution automatique des adresses IP sur certains PC.

Déroulé

La création du DHCP s'est déroulée en quelques étapes. Dans un premier temps on a dû installer le rôle DHCP sur le windows serveur (Active Directory).

Ensuite nous devons aller dans l'onglet de configuration du DHCP. Enfin on crée 4 étandue pour les 4 Vlans présents sur notre réseau.

Étendues

Voici les 4 étendue pour les Vlans

Étendue 1: 192.168.1.120/24 => 192.168.1.130/24 | Passerelle : 192.168.1.200 | DNS : cabinet.local 192.168.1.101

Étendue 2: 192.168.2.120/24 => 192.168.2.130/24 | Passerelle : 192.168.2.200 | DNS : cabinet.local 192.168.1.101

Étendue 3: 192.168.3.120/24 => 192.168.3.130/24 | Passerelle : 192.168.3.200 | DNS : cabinet.local 192.168.1.101

Étendue 4: 192.168.4.120/24 => 192.168.4.130/24 | Passerelle : 192.168.4.200 | DNS : cabinet.local 192.168.1.101

Serveur Linux

Téléphonie :

Contexte

Nous souhaitons mettre en place un serveur téléphonique avec des softphones pour que les clients et l'administrateur puissent communiquer.

Déroulé

Dans un premier temps, il faut installer FreePBX. Pour l'installation du serveur, nous avons besoin de VirtualBox. Nous hébergeons donc FreePBX sur la machine virtuelle et nous paramétrons la machine.

Nous accédons au fichier de configuration suivant :

/etc/sysconfig/network-scripts/ifcfg-eth0
à l'aide de la commande nano.

Nous modifions et ajoutons les lignes suivantes pour configurer la machine virtuelle :

BOOTPROTO="static"
IPADDR=192.168.1.105
GATEWAY=192.168.1.100
NETMASK=255.255.255.0
Ensuite, nous devons modifier le DNS dans le fichier resolv.conf car celui-ci n'est pas correct. Nous devons mettre le DNS de notre réseau, soit 192.168.1.101, sinon cela va créer des délais pour l'établissement des appels.

Une fois la configuration de la machine virtuelle terminée, nous devons la redémarrer en mode bridge. Ensuite, nous devons nous connecter au serveur web de notre VM via son adresse IP.

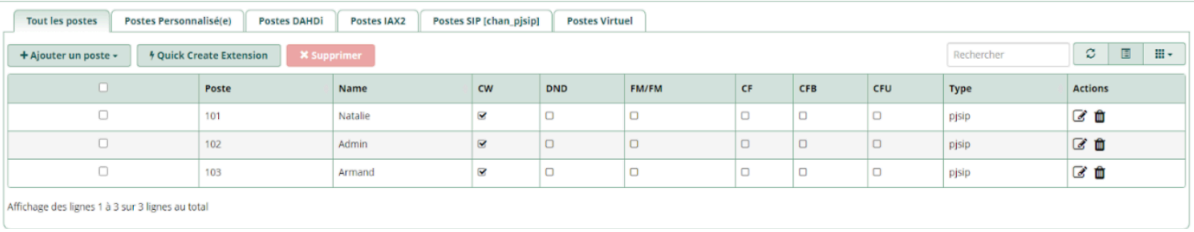
Une fois sur le site, nous allons configurer nos softphones dans l'onglet Settings puis Asterisk SIP Settings. Nous saisissons les sous-réseaux de notre installation comme suit :

Par la suite, nous cliquons sur Submit puis Apply Config pour sauvegarder la configuration.

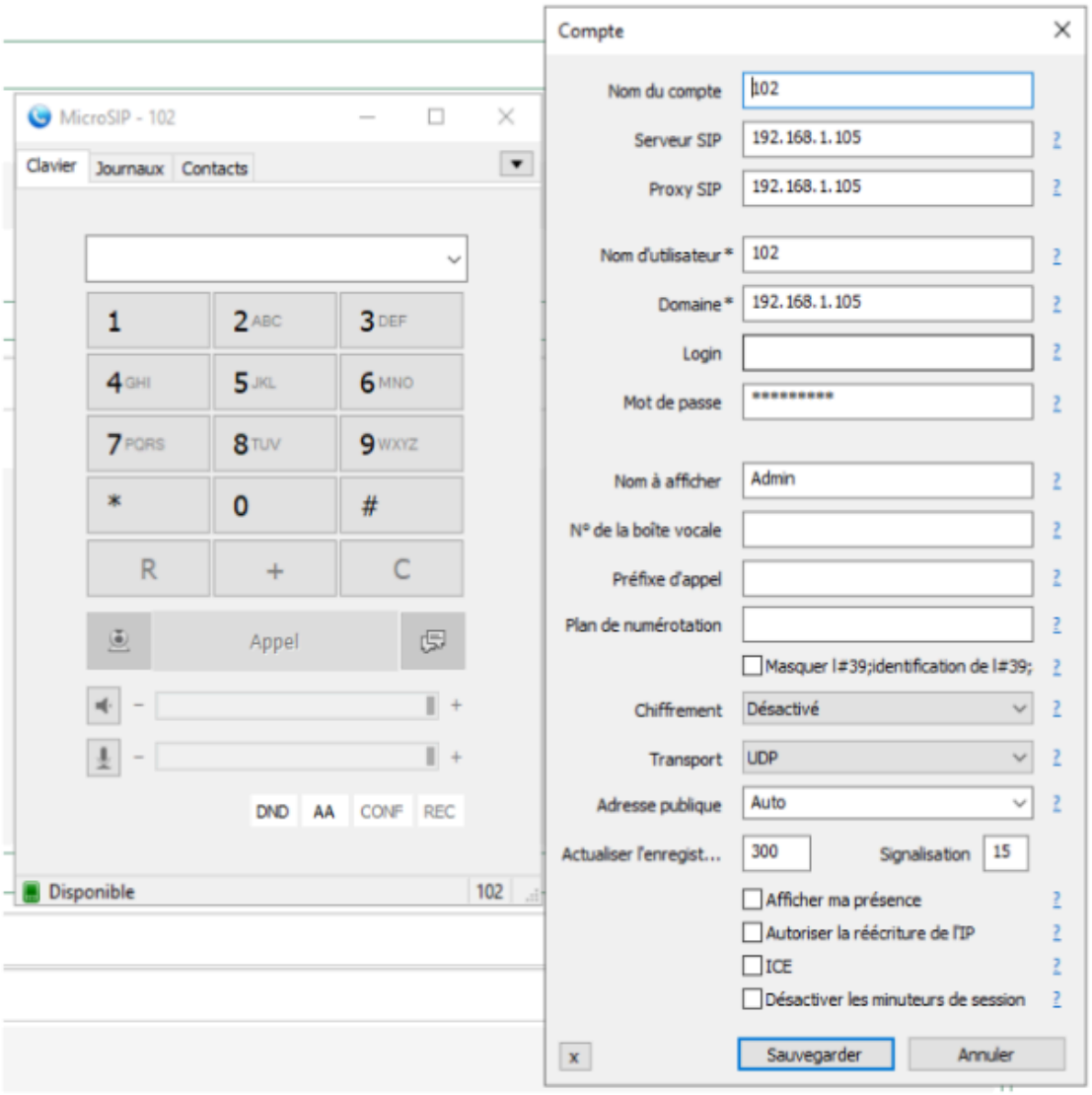
Ensuite, nous allons créer les postes téléphoniques dans le menu Application puis Extensions. Il faut ajouter un utilisateur SIP et renseigner le numéro du téléphone, qui sera le 102 pour l'admin.

Dans l'onglet General, nous mettons le Display Name qui sera le nom de l'utilisateur, ici pour un premier téléphone nous choisissons Admin. Il faut aussi choisir un Outbound CID qui portera également le nom Admin.

Ensuite, nous décidons d'activer la messagerie vocale sur les téléphones. Nous devons répéter cette opération pour les deux autres clients. Une fois les extensions créées, nous obtenons les utilisateurs suivants :



Ensuite, nous utilisons les softphones MicroSIP sur nos PC. Nous devons les configurer pour qu'ils puissent s'authentifier auprès du serveur de messagerie, nous les configurons comme suit :



Conclusion

Une fois que les softphones sont correctement configurés, nous pouvons établir des appels, des conférences et même enregistrer les appels.