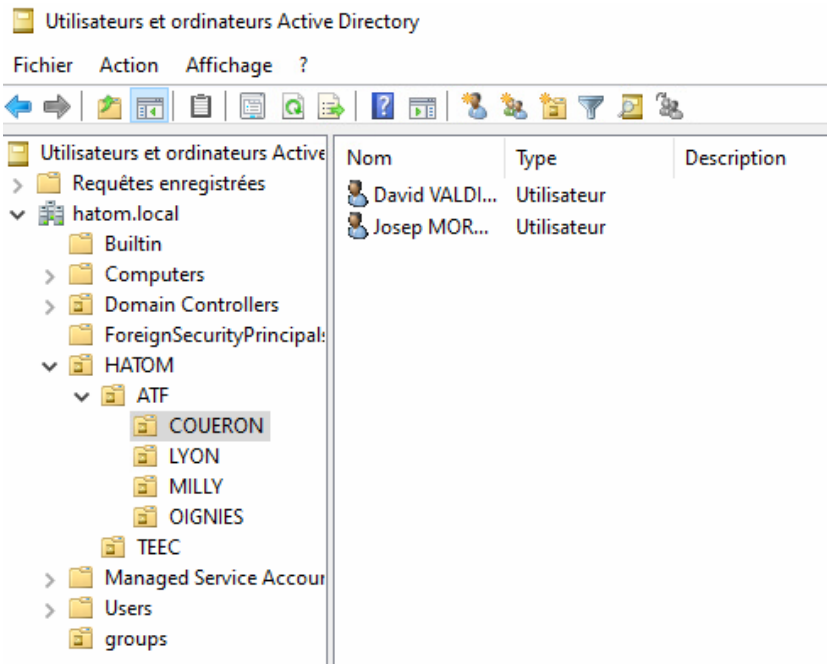
Maxime
LE BRAS
SIO1 - SISR

Le 20/05/2024

Note de synthèse 1ère année BTS SIO



Stage réalisé à l'entreprise Aide Informatique à Montlhéry (91310) du 20 mai 2024 jusqu'au 21 juin 2024

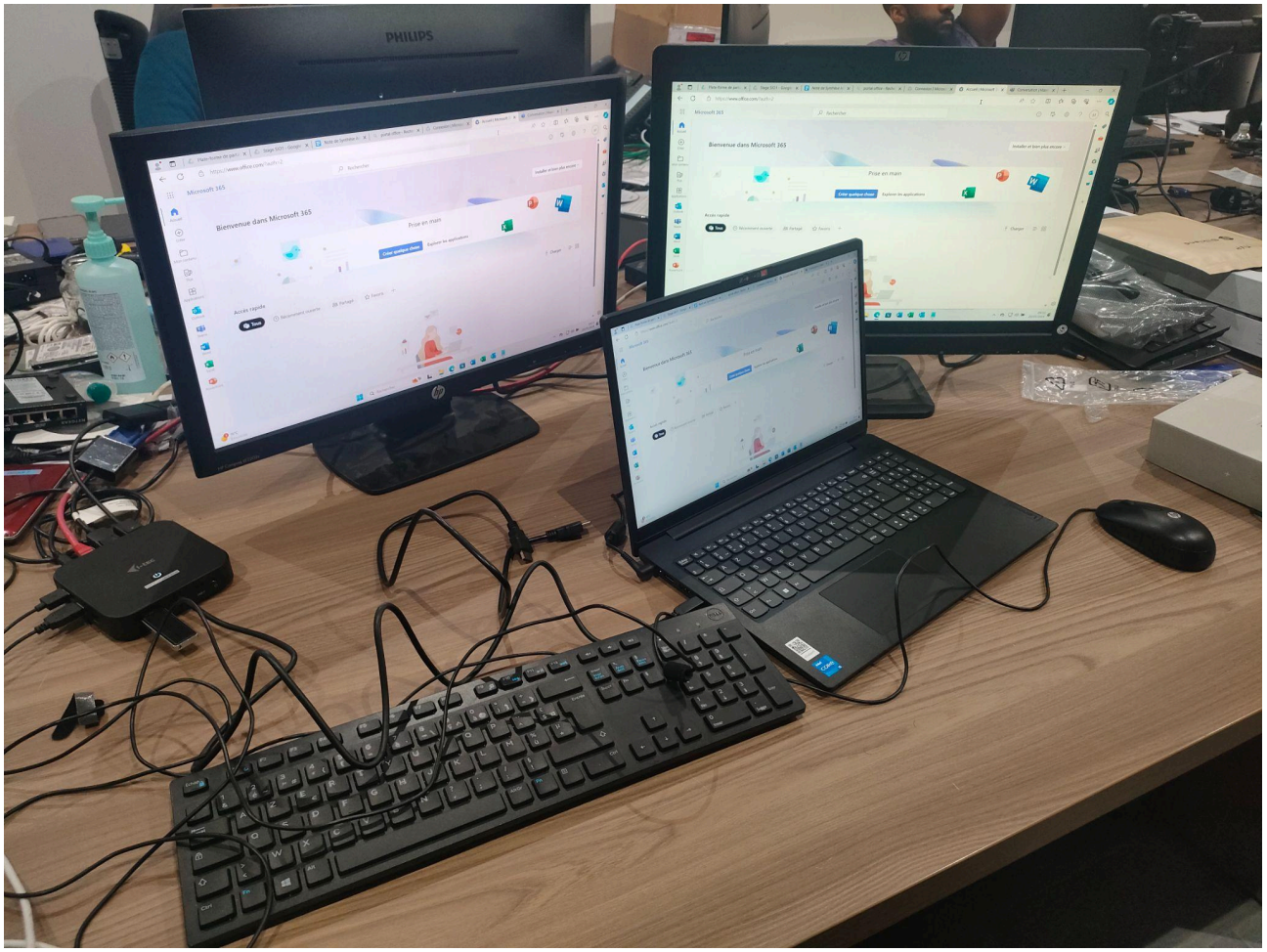
Tuteur de stage : Steven VONIN, Administrateur Réseau

Sommaire

I - Présentation de l'entreprise

Effectuant mon stage au sein de Aide Informatique créée en 1999 par Franck VALETTE, c'est une entreprise qui fait de la vente de logiciels en lien avec la gestion, la comptabilité, les relations clients et les payes.
Ceci est géré par un progiciel de gestion intégré (Il permet de gérer les ressources humaines, la comptabilité, l'aspect financier, l'aide à la décision, la vente, la distribution, l'approvisionnement et le commerce électronique pour une entreprise) appelé WareSoft (éditions standard, professionnelle ou entreprise) qui contient 10 modules : gestion commerciale, comptabilité, gestion de la relation client, le décisionnel, les points de vente, la production, les immobilisations (ce sont les biens que l'entreprise détient et utilise durablement), les états financiers (informations comptables en lien avec la situation de l'entreprise), les liaisons bancaires et l'automate de transfert (automatisation des tâches au niveau des échanges de données).
Elle fait aussi de la maintenance, de l'assistance informatique avec le logiciel TeamViewer, de la vente de matériels informatiques ainsi que du e-commerce (Oxatis).
De plus, elle propose des formations informatiques (WaveSoft, Ciel by Sage, EBP, Sage, Microsoft).
Cette entreprise fait de l'audit informatique et de la sécurité réseau au niveau des réseaux informatiques des particuliers et des entreprises liées à Aide Informatique (ce qui correspond à un état des lieux) afin de permettre un suivi régulier sur le réseau informatique des clients.

II - Poste de travail



Je vous présente mon environnement de travail qui m'a permis de réaliser toutes mes tâches et projets pendant 5 semaines.
Il est composé d'un ordinateur portable qui est l'axe central de mon poste de travail, il est relié à une station d'accueil qui fait la liaison entre ce PC et les deux écrans.
La souris, le clavier, le câble Ethernet, la clé USB et les deux écrans (avec des câbles VGA, USB et USB-C) sont branchés à la station d'accueil.
Cela permet le bon fonctionnement de mon poste de travail !

III - Organigramme de l'entreprise

Franck SABIEN — **CO-GERANTS** — Franck VALETTE

Steven VONIN	**TECHNICIEN**	**TECHNICIEN**	Guy RIDARD
Sandrine GRUNWALD	**SUPPORT**	**COMPTABILITE**	Patricia LEVASTRE

IV - Projets réalisés

Projet 1 : HATOM

Tâches à réaliser, objectifs du projet, raisons du choix du projet et difficultés rencontrées

J'ai dû exécuter les tâches suivantes :

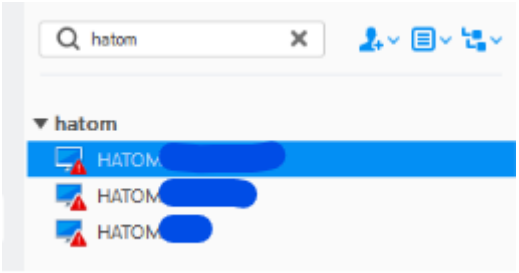
- Création d'utilisateurs dans le serveur Active Directory
- Mise en place de mots de passe sécurisés et complexes pour les utilisateurs
- Création de contacts dans ITGlue
- Création de groupes de sécurité (confidentialité, etc…)
- Mise en place des GPOs
- Audit sur le matériel informatique de l'entreprise

Les objectifs du projet sont de comprendre l'utilité et les enjeux d'un serveur Active Directory à l'échelle d'une entreprise ainsi que ses différentes fonctionnalités.

Ce projet m'a été donné dans le but de créer des sessions Windows avec un identifiant et un mot de passe robuste en excluant les caractères similaires (I et 1 ou O et 0, etc…) afin de ne pas perturber les utilisateurs lors de la saisie du mot de passe.
Le fait de rendre les mots de passe utilisateurs complexes, permet de sécuriser l'accès aux sessions et de garantir la confidentialité au niveau des utilisateurs.

J'ai eu une petite difficulté qui était la mise en place d'une GPO.
Cependant, je n'ai pas eu de difficultés particulières puisque j'ai des connaissances sur le fonctionnement d'un serveur Active Directory grâce à mes cours de cybersécurité.

Accès au serveur Active Directory de l'entreprise HATOM

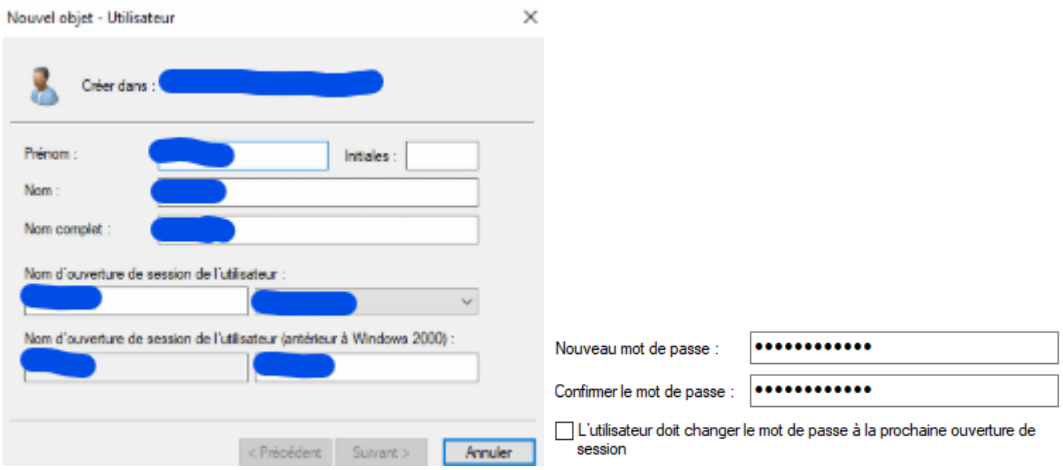


Ici, j'accède à distance aux différents serveurs de l'entreprise via TeamViewer. TeamViewer est une solution d'accès et d'assistance à distance qui permet de contrôler et de gérer des appareils à distance.

Création de contacts avec ITGlue

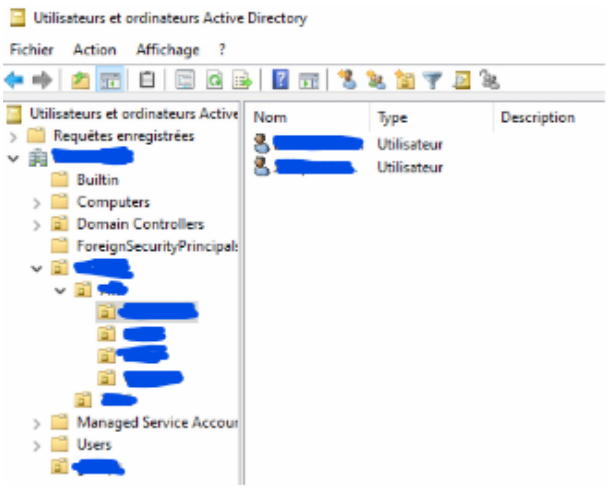
La création d'un contact permet à l'administrateur réseau d'avoir les mots de passe de l'utilisateur en cas de problèmes informatiques (support informatique).
ITGlue permet de centraliser les informations sur l'infrastructure informatique, les processus, les clients et les salariés d'une entreprise.

Création et configuration des sessions utilisateurs



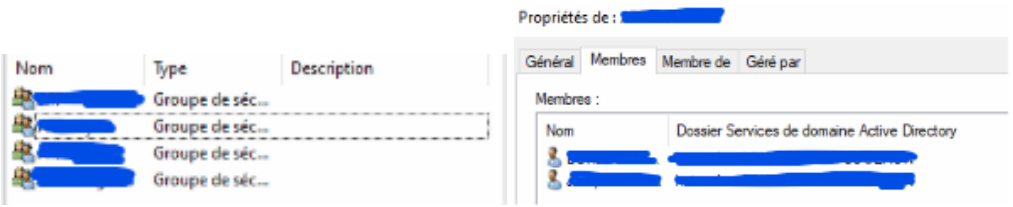
Ici, l'utilisateur n'aura pas besoin de changer le mot de passe dès la première connexion, car il respecte les normes de sécurité.

Active Directory de HATOM



L'Active Directory (AD) est une base de données et un ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour mener à bien leurs missions.

Mise en place des groupes de sécurité

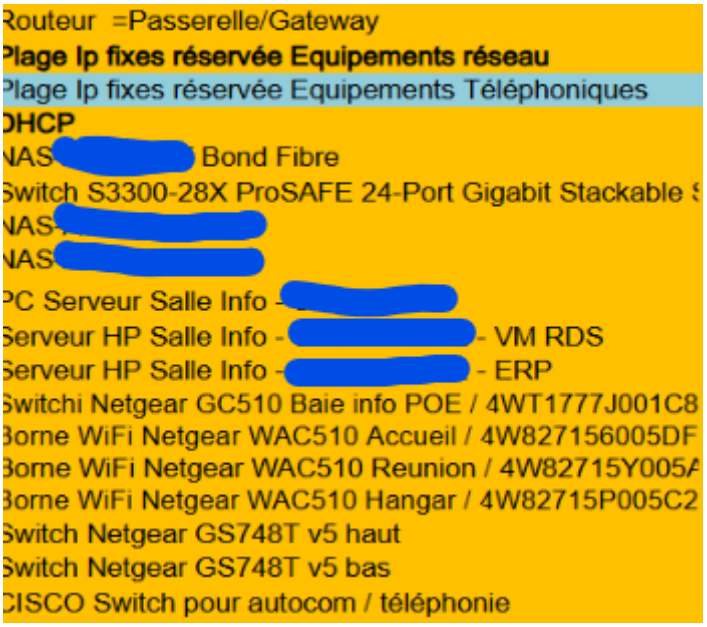


Les groupes de sécurité permettent de mettre en place des permissions et restrictions au niveau des accès ce qui permettra de sécuriser les accès à des fichiers ou documents confidentiels (confidentialité).

Mise en place des GPOs

J'ai mis en production les GPOs concernant le fond d'écran des sessions utilisateurs des salariés de HATOM ainsi que la mise en place du Pack Office (voir Projet 3 et Tâche de maintenance 1)

Audit sur le matériel informatique de l'entreprise



J'ai réalisé une vérification au niveau de l'accessibilité et de l'authentification au matériel informatique de HATOM.
J'ai constaté qu'il y a beaucoup de matériels qui ne fonctionnent pas par rapport à un problème d'accès dû à l'adresse IP ou à un refus de connexion et à un problème d'authentification (ex : bornes wifi, serveurs, etc…).
Pour conclure, il faudra remettre en place le paramétrage IP, l'authentification et l'accessibilité de certains matériels afin d'assurer la sécurité notamment.

Conclusion

Pour conclure, ce projet m'a permis d'appliquer ce que j'ai appris en cours par rapport au fonctionnement d'un serveur Active Directory.
Puis, j'ai découvert le logiciel de documentation ITGlue qui permet de créer des contacts pour les clients.
De plus, cela m'a permis d'apprendre de nouvelles notions comme la mise en place de GPOs (ex : Fond d'écran, Pack Office, etc…) ainsi que la création de groupes de sécurité.

Projet 2 : Firewall WatchGuard

Tâches à réaliser, objectifs du projet, raisons du choix du projet et difficultés rencontrées

J'ai dû exécuter les tâches suivantes :

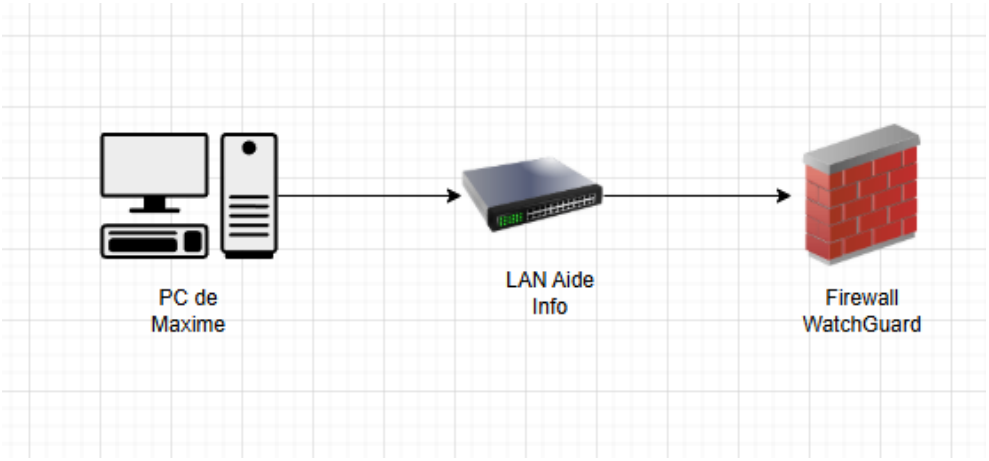
- Installation et configuration du pare-feu
- Tests de fonctionnement
- Mise en place des règles de pare-feu
- Mise en place du proxy web (blacklist, whitelist)
- Activation du certificat SSL
- Mise en place du VPN

Les objectifs du projet sont de comprendre le fonctionnement d'un pare-feu WatchGuard et de savoir l'utilité du protocole SSL et d'un VPN.

Ce projet m'a été donné dans le but de faire l'installation complète d'un Firewall WatchGuard et de le rendre fonctionnel pour le client.
Cela m'a permis de mettre en place mes connaissances en lien avec les cours de réseaux et d'apprendre de nouvelles notions (certificat SSL, VPN et proxy web (mise en pratique), etc…).

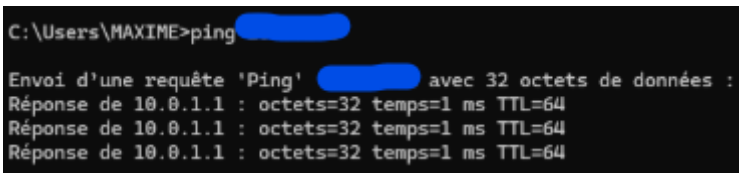
J'ai rencontré certaines difficultés au niveau de la configuration des interfaces (comment les configurer ? En DHCP ? En statique ? Pourquoi il faut mettre cette adresse IP ?), de l'environnement de travail Windows (comme en SISR ou en AP, je me suis habitué à travailler sur le système d'exploitation Linux) et de faire mes tests en lien avec le proxy web.

Schéma réseau (configuration du pare-feu physique)



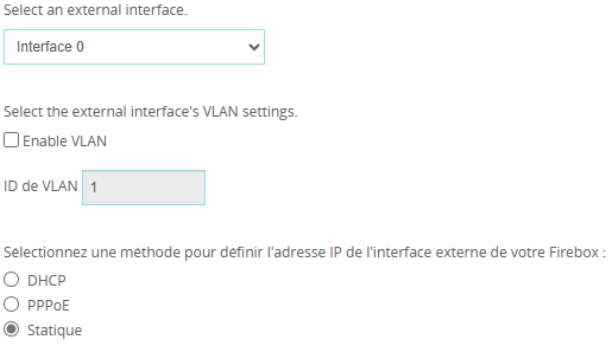
Ce schéma représente la mise en place réseau et système afin de configurer le pare-feu WatchGuard.

Accès à l'interface web du Firewall WatchGuard



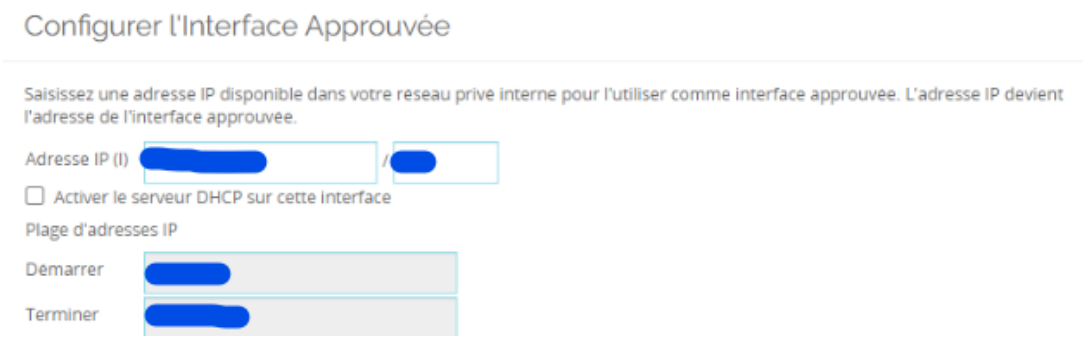
Le test de connexion entre le Firewall et le PC est fonctionnel et on accède à l'interface web du pare-feu WatchGuard.

Configuration de l'interface réseau WAN



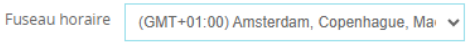
Je l'ai configuré en adresse IP statique comme le Firewall va aller au client.

Configuration de l'interface réseau LAN



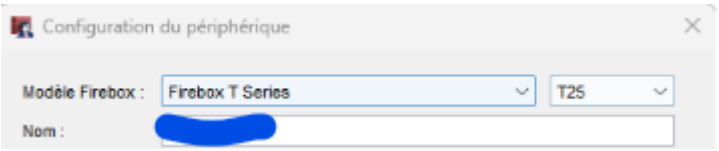
J'ai dû me connecter à une machine à distance avec TeamViewer pour avoir les informations sur le serveur de la société du client (passerelle par défaut (internet), adresse IP).

Horodatage du Firewall



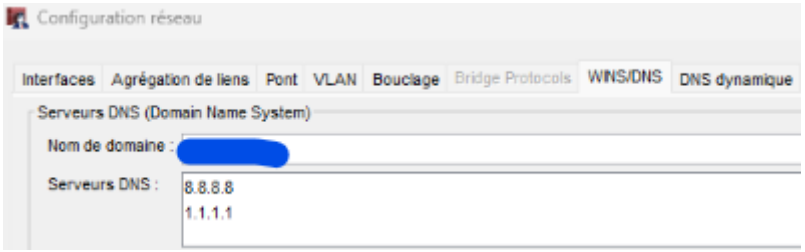
J'ai fait cette configuration afin de ne pas créer un décalage horaire entre le Firewall et la session.

Modification du nom du Firewall



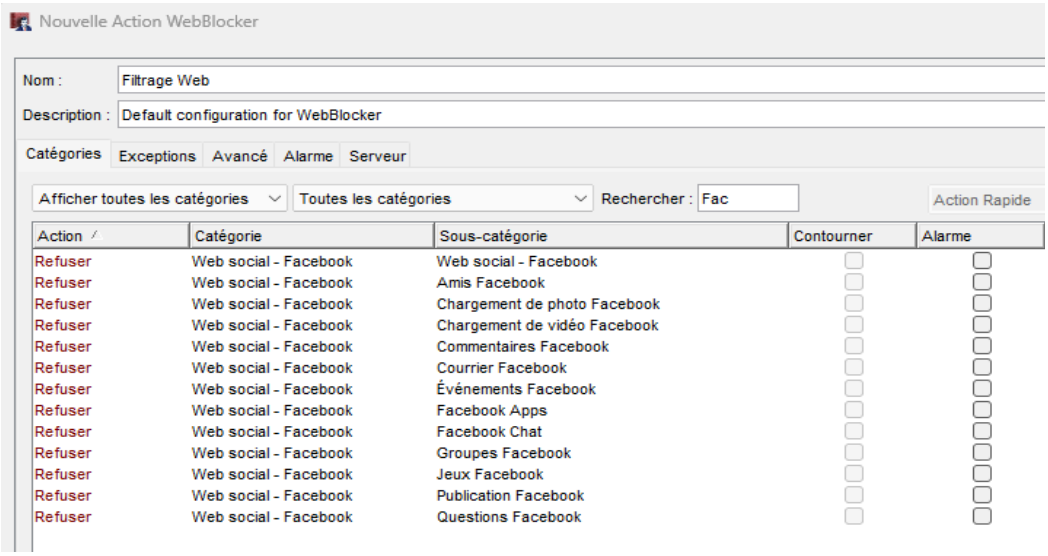
Cela permet de modifier le nom pour qu'il soit en accord avec l'entreprise.

Mise en place du serveur DNS sur le Firewall



Cette mise en place permet de se connecter à Google et de faire nos tests pour le proxy web (blacklist, whitelist).

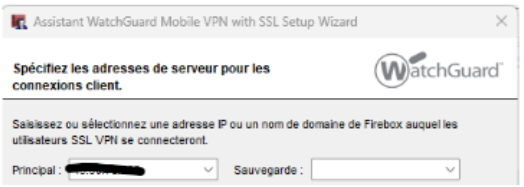
Mise en place de l'interdiction d'accès à Facebook



Ici, j'ai refusé toutes les catégories en lien avec Facebook afin de ne pas pouvoir accéder à Facebook via Google en cliquant sur le lien.

Test d'accès au site web de Facebook

Mise en place du VPN et du certificat SSL



La mise en place du VPN et du certificat SSL permet d'avoir une sécurité renforcée au niveau des communications et d'éviter les attaques malveillantes.
Plus précisément, le protocole SSL (Secure Sockets Layer) permet de chiffrer les communications en garantissant la confidentialité, l'intégrité des données et l'authentification.
De plus, le VPN (Virtual Private Network) permet de créer un tunnel privé et sécurisé entre la machine du client et le réseau Internet ce qui permet de sécuriser les communications.

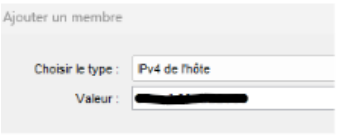
Modification de l'interface WAN du Firewall

Règles de pare-feu avec l'interdiction d'accéder à l'extérieur (Internet - WAN)

1	✓	FTP	FTP	Any-Trusted, Any-...	Any-External	tcp:21	Aucun(e)
2	✓	WatchGua...	WG-Fireware-X...	Any-Trusted, Any-...	Firebox	tcp:8080	Aucun(e)
3	✓	Ping	Ping	Any-Trusted, Any-...	Any	icmp (type: 8, ...	Aucun(e)
4	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-...	Firebox	tcp:4105 tcp:4...	Aucun(e)
5	⊘	Outgoing	TCP-UDP	Any-Trusted, Any-...	Any-External	tcp:0 (Any) u...	Aucun(e)

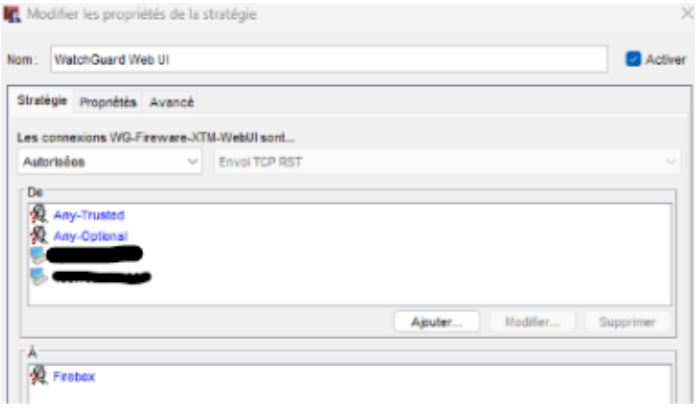
Cette règle de pare-feu (Règle 5) permet d'interdire l'accès à Internet, c'est-à-dire qui sont connectés en réseau local et qui sont liés au Firewall, ils ne peuvent pas accéder à l'extérieur (dans ce cas-là, à Internet).

Accès au Firewall



Pour que l'entreprise règle des problèmes au niveau du firewall (réseau notamment), il faut qu'elle accède au Firewall par le biais de l'IP publique de l'entreprise.

Modification des règles 6 et 9 (gestion du Firewall)



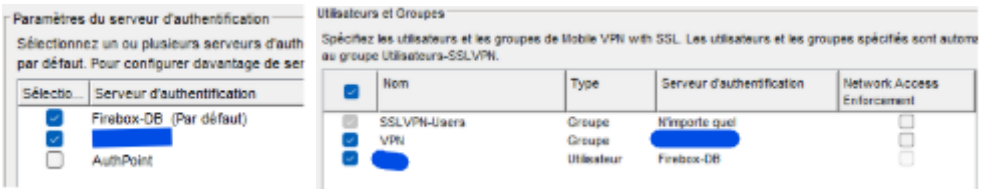
Cela va permettre à l'entreprise Aide Informatique d'accéder au Firewall en cas de problèmes chez le client.

Règles de pare-feu

1		FTP	FTP	Any-Trusted, Any-...	Any-External	tcp:21	Aucun(e)
2		HTTP-proxy	HTTP-proxy	Any-Trusted	Any-External	tcp:80	Aucun(e)
3		HTTPS-pro...	HTTPS-proxy	Any-Trusted	Any-External	tcp:443	Aucun(e)
4		WatchGua...	WG-Cert-Portal	Any-Trusted, Any-...	Firebox	tcp:4126	Aucun(e)
5		WatchGua...	SSL-VPN	Any-External, Any-...	Firebox	tcp:4970	Aucun(e)
6		WatchGua...	WG-Fireware-X...	Any-Trusted, Any-...	Firebox	tcp:8080	Aucun(e)
7		DNS-proxy	DNS-proxy	Any-Trusted	Any-External	tcp:53 udp:53	Aucun(e)
8		Ping	Ping	Any-Trusted, Any-...	Any	icmp (type: 8, ...	Aucun(e)
9		WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-...	Firebox	tcp:4105 tcp:4...	Aucun(e)
10		Allow SSL...	Any	SSLVPN-Users (A...	Any	any	Aucun(e)

Ces règles de pare-feu permettent de mettre en place le proxy web (HTTP (non sécurisé) et HTTPS (sécurisé)), le proxy DNS (résolution de nom de domaine en adresse IP), de gérer le firewall via le client lourd (WatchGuard Manager System) ou l'interface web en se connectant avec l'adresse IP, de configurer l'accès avec un VPN avec le protocole SSL (sous le port 4970) et de permettre la réalisation de pings entre le firewall et la session.

Mise en place du serveur d'authentification et du VPN



Cette mise en place permet aux employés de Cantrel de se connecter aux différents services de l'entreprise via un VPN.

Test d'accès au Firewall via le port SSL

On a réussi à accéder au Firewall via le port SSL 4970 puisqu'on a mis en place une règle de pare-feu de type SSL-VPN permettant d'accéder à l'interface web via ce port (voir Règles de pare-feu).

Conclusion

Pour conclure, ce projet m'a permis de comprendre le fonctionnement d'un Firewall, de savoir le configurer en mettant en place des règles de pare-feu en fonction de la demande du client (proxy web, proxy DNS, SSL-VPN, etc…), à accéder à l'interface web d'un Firewall via le protocole SSL, à mettre en place le serveur d'authentification et le VPN afin que les salariés puissent travailler à distance.

Projet 3 : Configuration de serveurs Windows

Tâches à réaliser, objectifs du projet, raisons du choix du projet et difficultés rencontrées

J'ai dû exécuter les tâches suivantes :

- Mise en place d'un serveur Active Directory
- Mise en place d'un serveur de bureau à distance
- Mise en place d'un serveur de licences
- Se connecter aux deux serveurs (AD/Licences) via le bureau à distance Windows
- Création et mise en place d'une GPO (fond d'écran)

Les objectifs du projet sont de comprendre les manœuvres à réaliser pour configurer complètement des serveurs Windows (Active Directory, Licences et Bureau à distance, etc…) et de mettre en place une GPO.

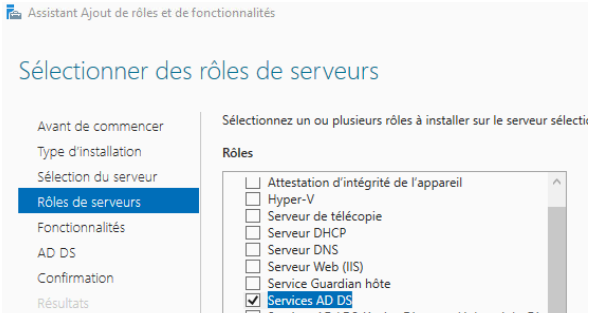
Ce projet m'a été donné pour comprendre le fonctionnement des serveurs que je mettais en place (AD, Licences, Bureau à distance, etc…) et pour aider mon tuteur de stage à réaliser les tâches qu'il devait faire pour résoudre les problèmes des clients.

J'ai rencontré certaines difficultés comme la mise en place de la GPO pour mettre le fond d'écran sur les différentes sessions Windows et à mettre en place l'autorisation d'accès à distance pour les utilisateurs de l'Active Directory.

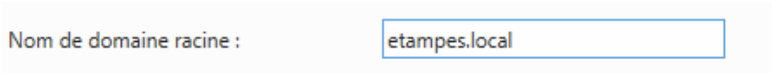
Configuration IP du serveur

```
Adresse IPv4. . . . . . . . . . . . . .: 192.168.30.20
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
Passerelle par défaut. . . . . . . . . : 192.168.30.254
```

Configuration des services du serveur

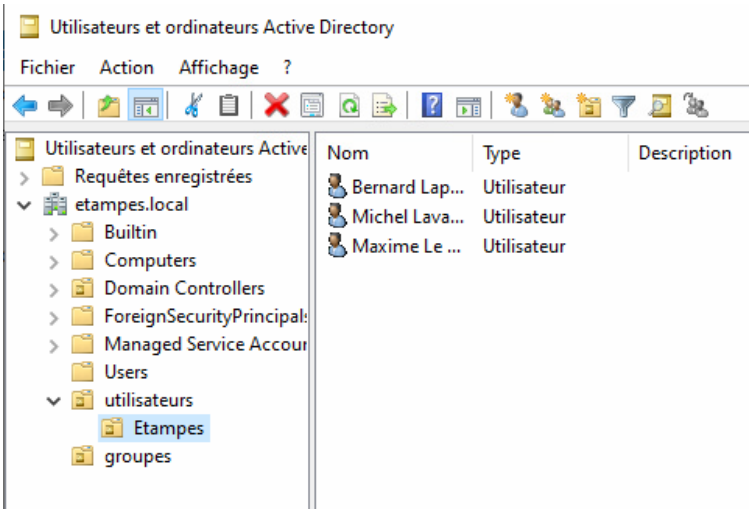


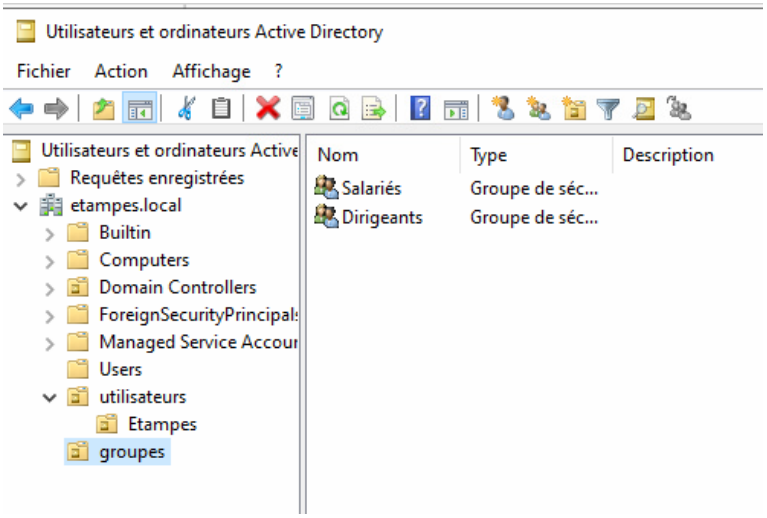
On saisit bien les services AD DS pour dire que ce serveur est bien un Active Directory.



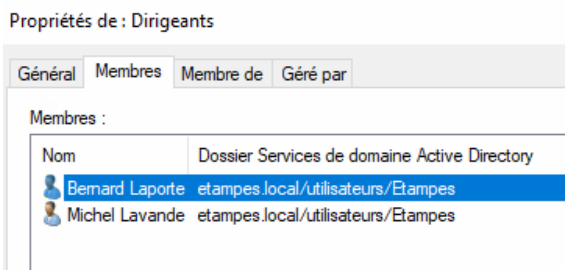
Le contrôleur de domaine est sous Windows Server 2016.

Création des utilisateurs et des groupes de sécurité de l'Active Directory



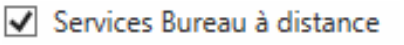


Attribution des utilisateurs dans les groupes de sécurité

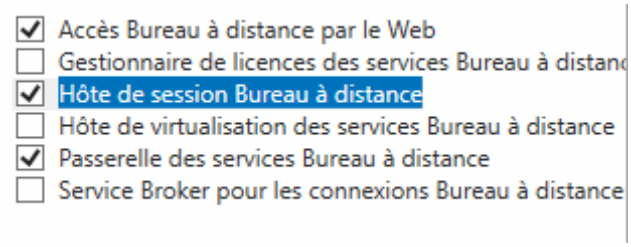


Adresse IP du deuxième serveur

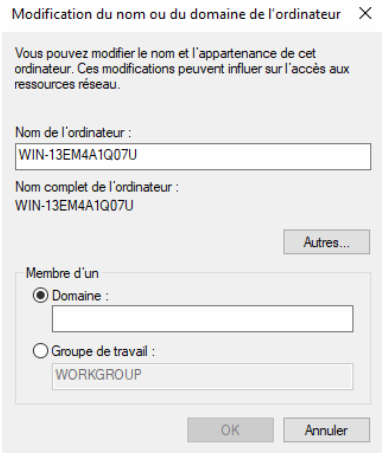
Rôle de ce serveur



Services pour mettre en place un serveur de bureau à distance

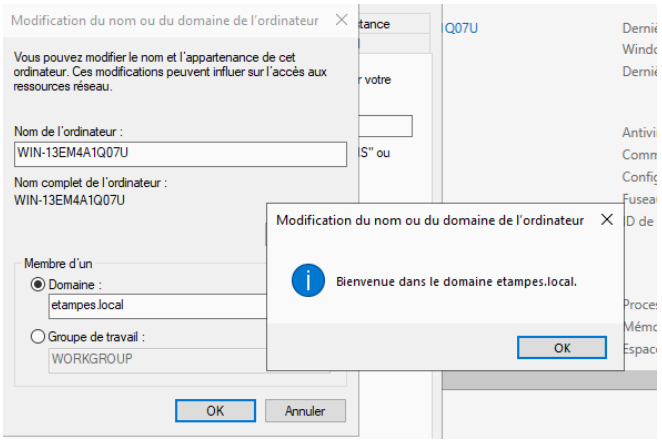


Intégration du serveur de bureau à distance dans le domaine de l'Active Directory



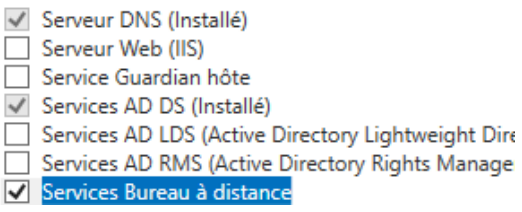
Avant de tester d'intégrer le serveur de bureau à distance, il faut vérifier si le serveur DNS est lié à l'Active Directory.

Test d'accès au domaine de l'Active Directory

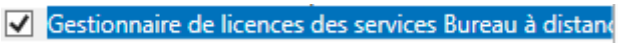


On a réussi à intégrer l'ordinateur au domaine !

Ajout d'un second rôle sur le serveur Active Directory

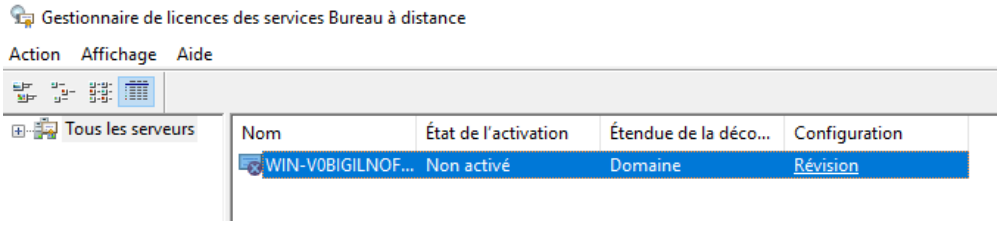


Voici le service de rôle adéquat pour installer le serveur de licences de bureau à distance :



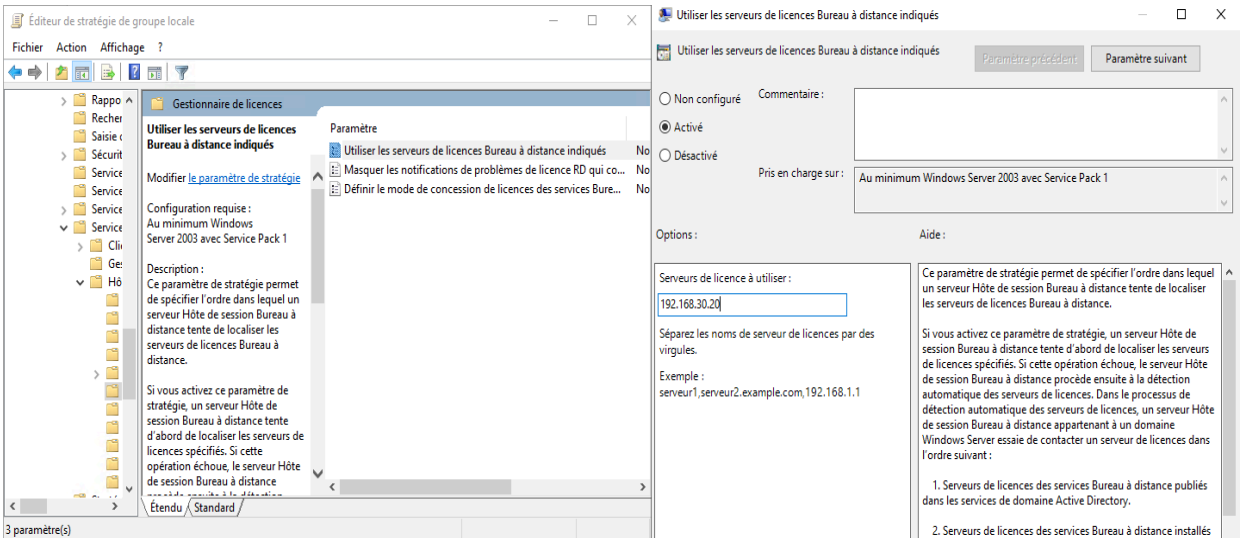
On va mettre un deuxième rôle au serveur Active Directory qui est “serveur de licence”. Le but est d’attribuer des licences utilisateurs (on peut utiliser les licences périphériques, l’inconvénient de ces licences est qu’elles sont affectées à un périphérique et s’il tombe en panne alors la licence est rompue) pour ceux qui souhaitent faire une connexion à distance sur leurs sessions. Si on a pas ces licences à temps, alors personne ne pourra se connecter.

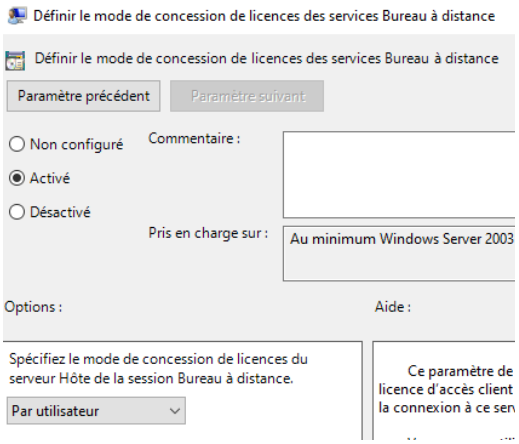
Activation du serveur de bureau à Distance



Pour faire la liaison entre le serveur AD et le serveur Bureau à distance, je vais aller dans l’éditeur de stratégie locale (gpedit.msc), ensuite, il faut trouver le moyen d’activer les licences du serveur de licences en se connectant avec l’adresse IP (192.168.30.20) et de mettre les licences par utilisateurs.

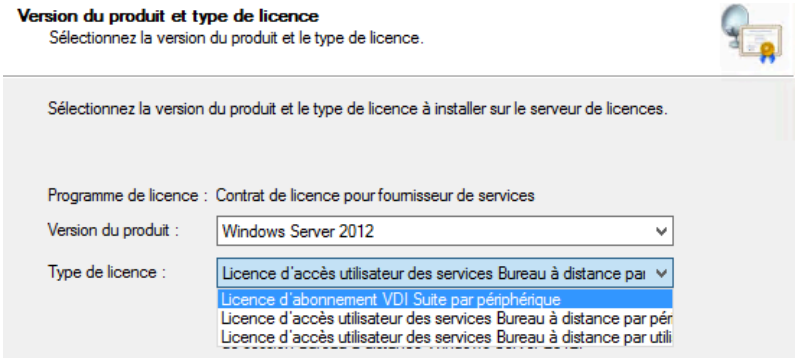
Mise en place des licences de bureau à distance





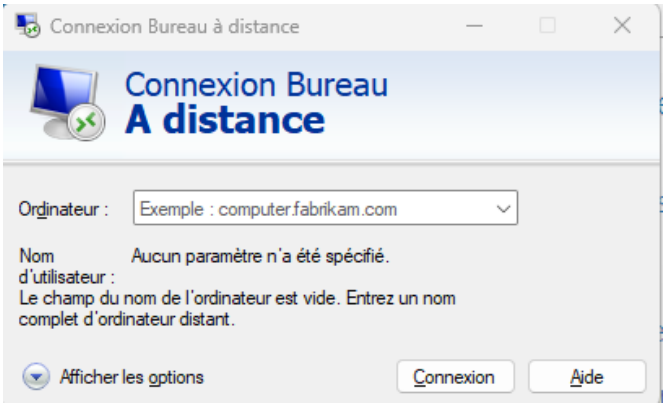
J'ai mis en place la liaison entre le serveur de bureau à distance et le serveur de licence (serveur AD de base) en allant dans l'éditeur de stratégie de groupe local de la machine serveur bureau à distance (192.168.30.22 /24).

Version de produit et type de licence pour le serveur de licences



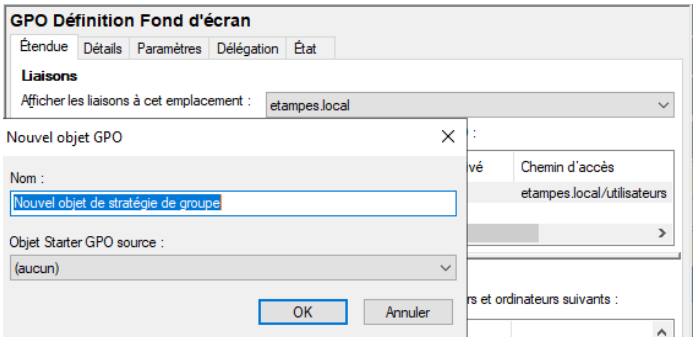
Il existe deux types de licences (par périphérique et par utilisateur) et on va utiliser celle par utilisateur par rapport à la demande de mon tuteur de stage.

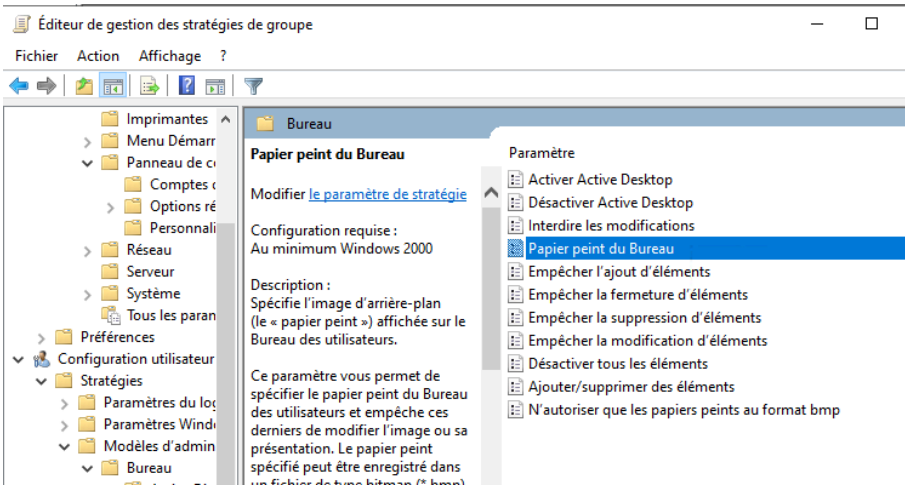
Connexion aux deux serveurs (AD/Licences - Bureau à distance)

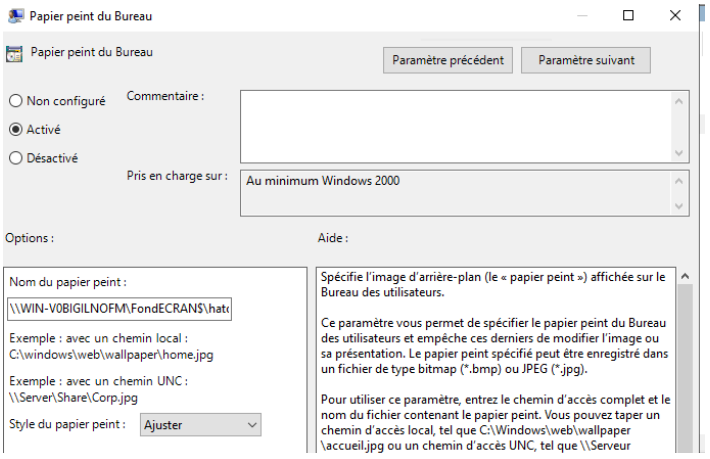


Maintenant, on pourra se connecter aux deux serveurs via leurs adresses IP respectives.
Surtout, avec la mise en place des licences sur le serveur de bureau, on peut se connecter avec plusieurs sessions.

Mise en place de la GPO

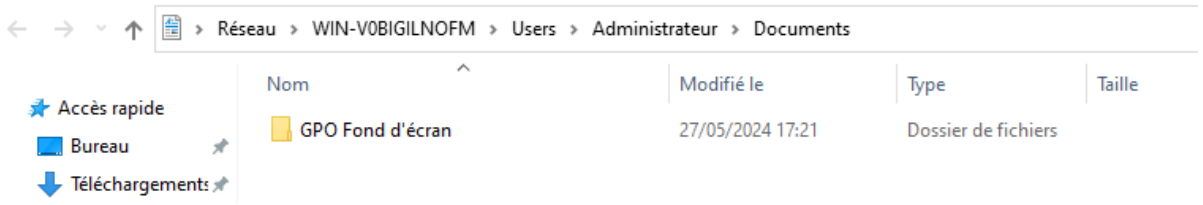






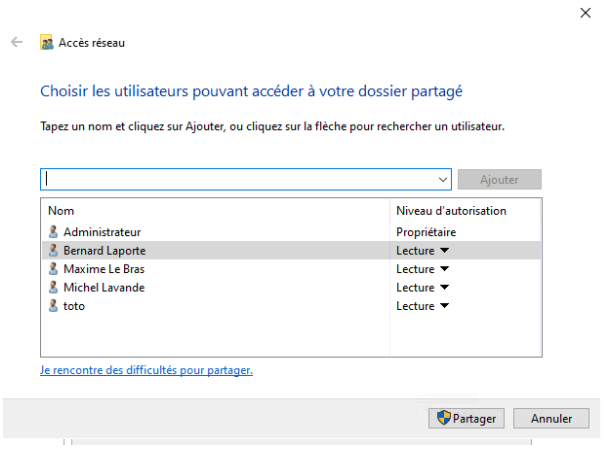
Ici, j'ai été dans le paramètre "Papier peint du bureau" du GPO pour insérer l'image de fond pour les sessions utilisateurs.

Création du dossier partagé

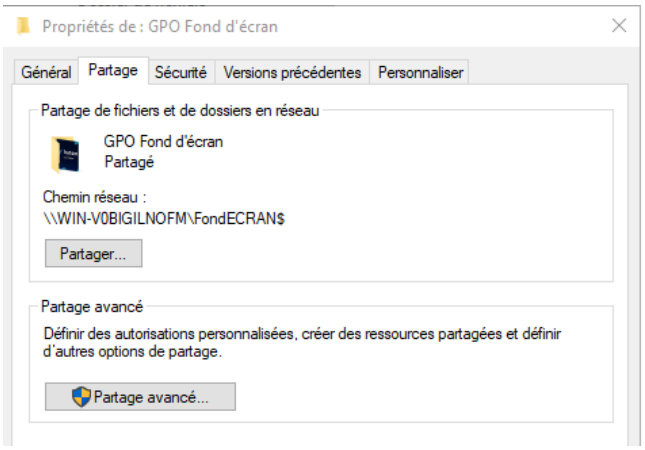


Ce dossier contiendra l'image de fond des sessions utilisateurs et il est partagé aux utilisateurs concernés.

Attribution des utilisateurs sur le dossier partagé

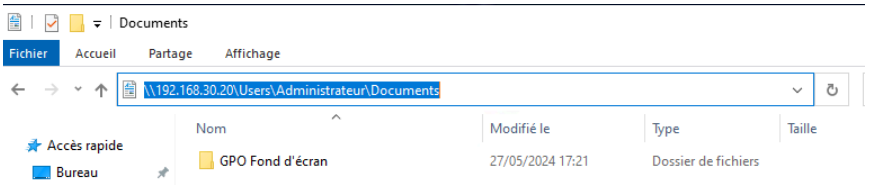


Ici, on a mis en place le partage en saisissant les utilisateurs de l'Active Directory et puis on le partage à ces personnes.



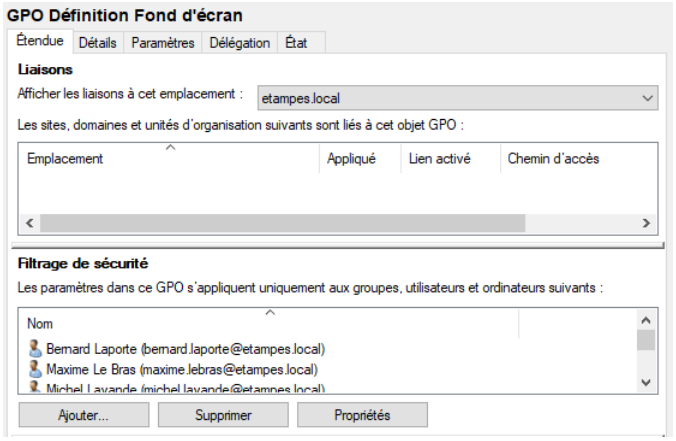
Il faut penser à aller dans "Partage avancé…" afin de masquer le partage et de bien l'activer.

Test d’accès au dossier partagé sur l’un des utilisateurs de l’Active Directory



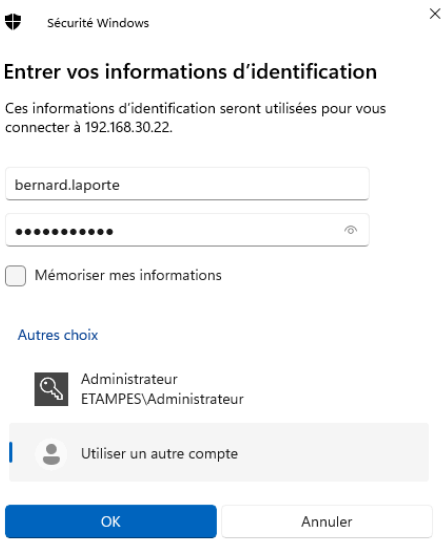
On accède bien au dossier partagé via l’adresse IP du serveur AD/Licences sur l’une des sessions Windows.

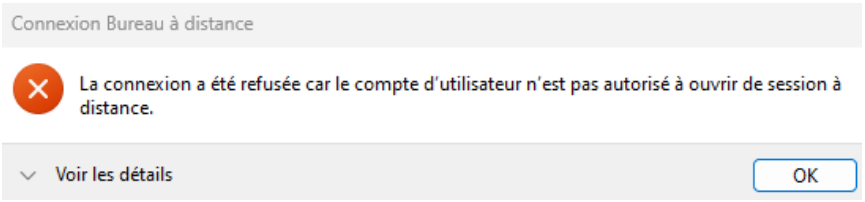
Vérification de la GPO avec les liaisons et le filtrage de sécurité



Cette GPO s’étend bien sur tout le domaine de l’Active Directory que j’ai créé (etampes.local) et elle s’applique à tous les utilisateurs authentifiés, donc cela devrait marcher.

Test de connexion à la session de Bernard Laporte

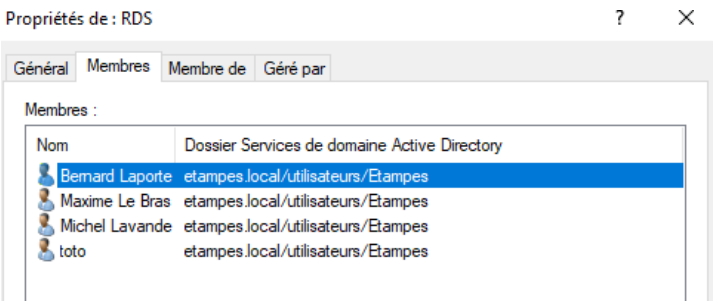


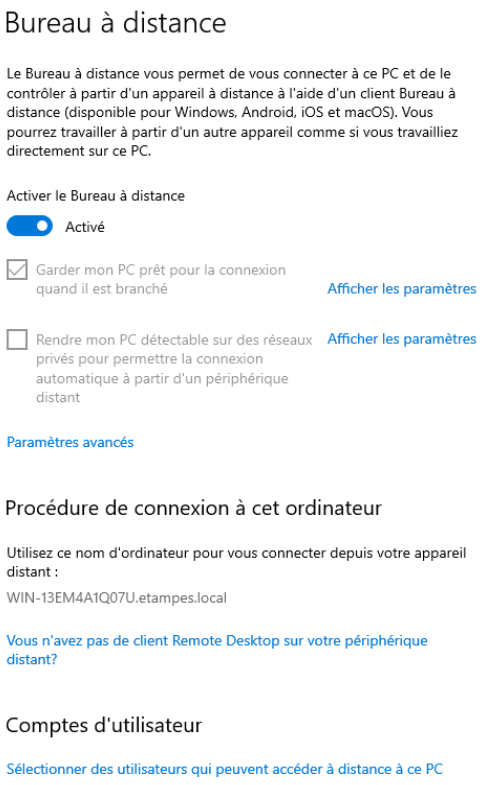


Le test de connexion sur le bureau à distance n'a pas fonctionné puisque les utilisateurs de l'Active Directory n'ont pas les droits d'aller se connecter en bureau à distance.

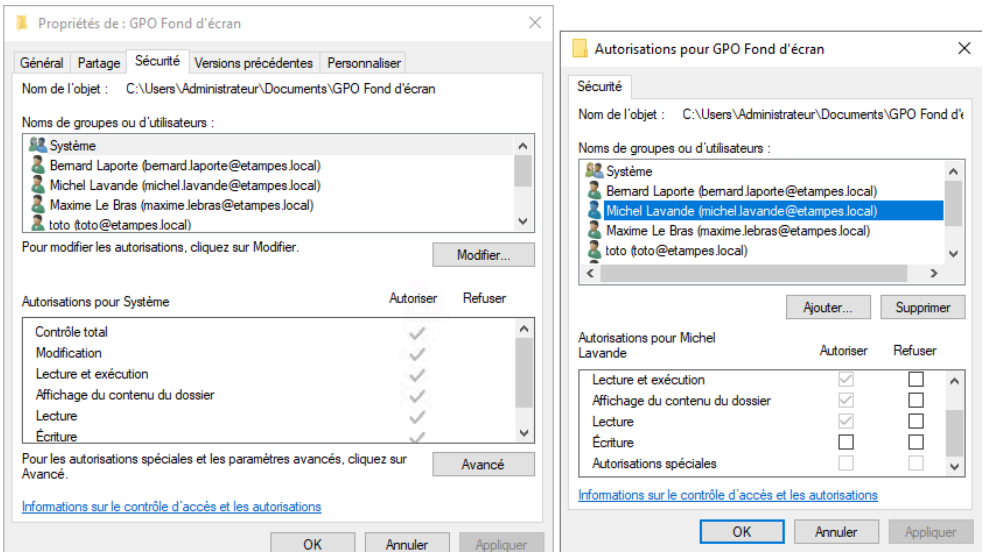
Modification pour pouvoir autoriser l'accès à distance aux utilisateurs

Il faut créer un groupe de sécurité dans l'Active Directory en mettant tous les utilisateurs un par un :

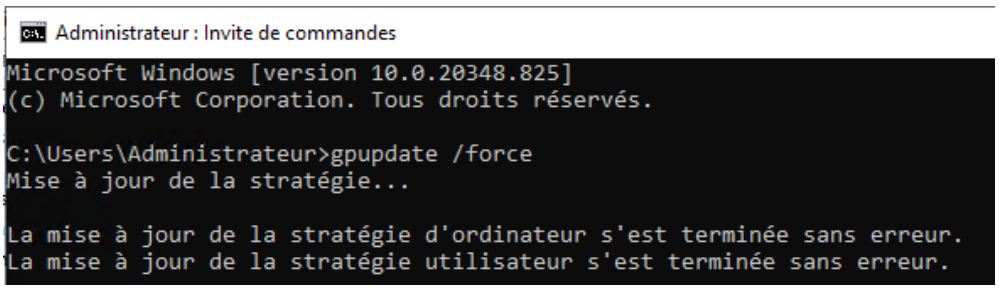




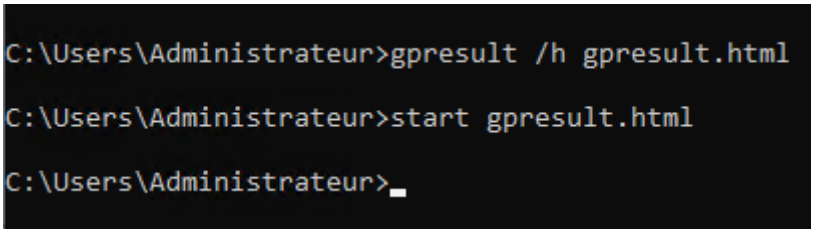
Puis, il faut aller dans le serveur Bureau à distance, il faut aller dans les paramètres Windows, sur Bureau à Distance, il faut sélectionner les utilisateurs qui ont le droit d'accéder au bureau à distance.
Si on respecte ses étapes, les utilisateurs pourront se connecter au bureau à distance.



On voit bien que l'onglet sécurité du dossier "GPO Fond d'écran", donc les droits ont été mis correctement !

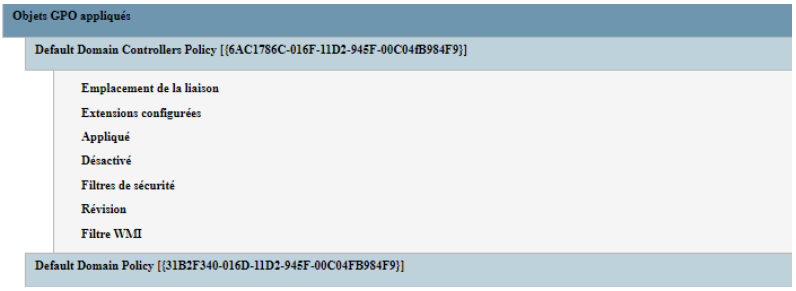


Cette commande Windows permet de mettre à jour des stratégies ordinateurs et utilisateurs des GPO mises en place dans le serveur Active Directory de manière impérative et brute.



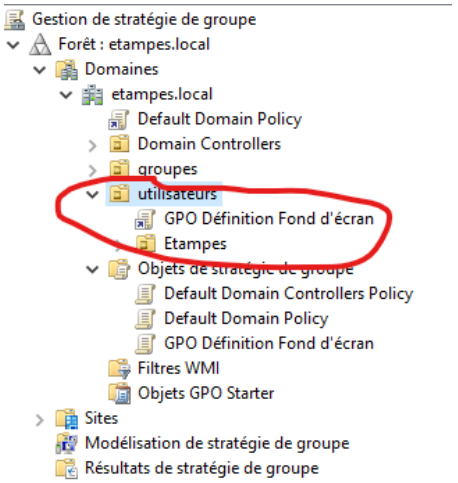
Ces commandes permettent de générer un rapport en HTML afin de voir les GPO appliquées.

Accès au rapport des GPO



On voit ici que la GPO que j'ai configurée, n'est pas appliquée.

Insertion de la GPO dans le dossier "Utilisateurs"



Il faut mettre la GPO dans le dossier où il y a tous les utilisateurs de l'Active Directory.

Conclusion

Pour conclure, ce projet m'a permis d'apprendre à installer et à configurer des serveurs Windows contenant différents services (Active Directory, etc…).

V - Maintenance Divers

Tâche de maintenance 1 : Mise en place d'une GPO pour installer et configurer Office

Tâches à réaliser, objectif de la tâche, raisons du choix de la tâche et difficultés rencontrées

J'ai dû exécuter les tâches suivantes :

- Installation et configuration du Pack Office
- Création du fichier partagé
- Création du fichier Batch
- Mise en place du fichier Batch dans la GPO

L'objectif de cette tâche de maintenance est de mettre en place une GPO qui permet d'automatiser l'installation et la configuration du Pack Office sur les sessions utilisateurs que j'ai créé.

Cette tâche de maintenance conséquente m'a été donnée, car je devais mettre en place cette GPO pour un établissement public (ESAT Paul Besson - Etampes) et j'ai dû faire des tests avec mes machines de test avant qu'on la mette en production.

J'ai rencontré certaines difficultés avec la mise en place de la GPO puisque cela n'a pas marché tout de suite et j'ai fait des recherches avec mon tuteur de stage sur Internet, donc cela nous a pris un certain temps.
Cela m'a permis de comprendre, d'apprendre certaines notions et de découvrir d'autres paramètres pour définir une GPO.

Installation et configuration du Pack Office

```
C:\>C:\Users\Administrateur\Desktop\test.bat

C:\>\\192.168.30.20\GPOOffice\setup.exe /download \\192.168.30.20\GPOOffice\config-office.xml

C:\>cd Users

C:\Users>cd Administrateur

C:\Users\Administrateur>cd Desktop

C:\Users\Administrateur\Desktop>cd..

C:\Users\Administrateur>cd Desktop

C:\Users\Administrateur\Desktop>cd..

C:\Users\Administrateur>cd Documents

C:\Users\Administrateur\Documents>cd "GPO Office"

C:\Users\Administrateur\Documents\GPO Office>setup.exe /download Configuration.xml
```

```
C:\>\\192.168.30.20\GPOOffice\setup.exe /configure \\192.168.30.20\GPOOffice\Configuration.xml
```

Contenu du fichier partagé

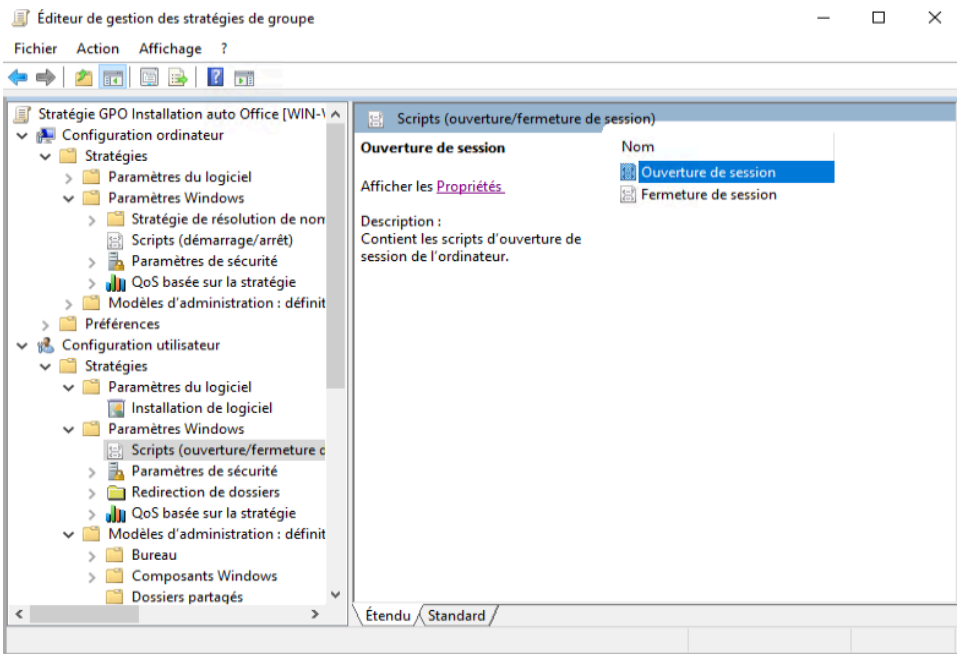
Nom	Modifié le	Type	Taille
Office	29/05/2024 11:16	Dossier de fichiers	
Configuration.xml	29/05/2024 10:41	Document XML	1 Ko
configuration-Office365-x64.xml	11/04/2024 00:10	Document XML	1 Ko
configuration-Office365-x86.xml	11/04/2024 00:10	Document XML	1 Ko
configuration-Office2019Enterprise.xml	11/04/2024 00:10	Document XML	2 Ko
configuration-Office2021Enterprise.xml	11/04/2024 00:10	Document XML	2 Ko
office.bat	29/05/2024 12:00	Fichier de commande Windows	1 Ko
setup.exe	11/04/2024 00:10	Application	7 550 Ko

Création du fichier Batch

```
@echo off
cls
echo Installation de Microsoft Office en cours...

rem Spécifiez le chemin d'accès au fichier d'installation d'Office sur le partage réseau
set INSTALLER_PATH=\\192.168.30.20\GPO_Office\setup.exe

rem Spécifiez les options de configuration pour l'installation d'Office
set INSTALL_OPTIONS=/configure Configuration.xml

rem Exécutez l'installation de Microsoft Office en mode silencieux
%INSTALLER_PATH% %INSTALL_OPTIONS%

rem Vérifiez si l'installation s'est terminée avec succès
if %errorlevel% equ 0 (
    echo Installation de Microsoft Office terminée avec succès.
) else (
    echo Erreur lors de l'installation de Microsoft Office. Code d'erreur : %errorlevel%
)

pause
```

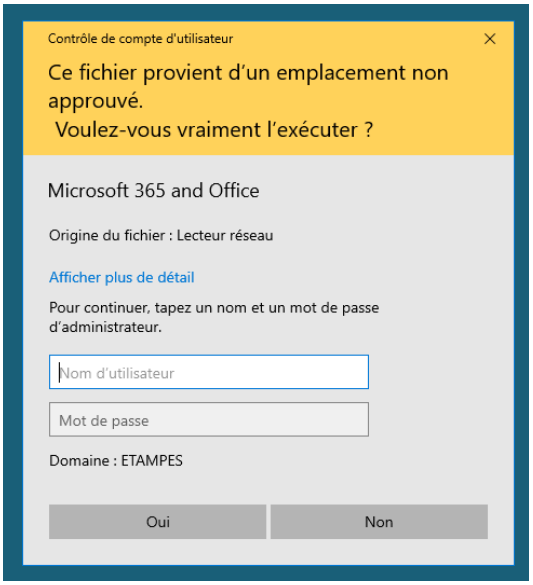
Ce fichier Batch permet de faire l'installation et la configuration d'Office lors du démarrage de la session utilisateur.

Mise en place du fichier Batch dans le GPO



On met le chemin réseau du fichier partagé "GPO_Office" où il y a le script Batch que j'ai créé.

Conclusion



Pour conclure, cette tâche de maintenance m'a permis d'apprendre à faire une GPO en fonction d'un script Batch.

Tâche de maintenance 2 : Installation de logiciels via Chocolatey Server

Tâches à réaliser, objectif de la tâche, raisons du choix de la tâche et difficultés rencontrées

J'ai dû exécuter les tâches suivantes :

- Installation d'un service web
- Configuration de Chocolatey Server
- Installation de Brave via Chocolatey Server

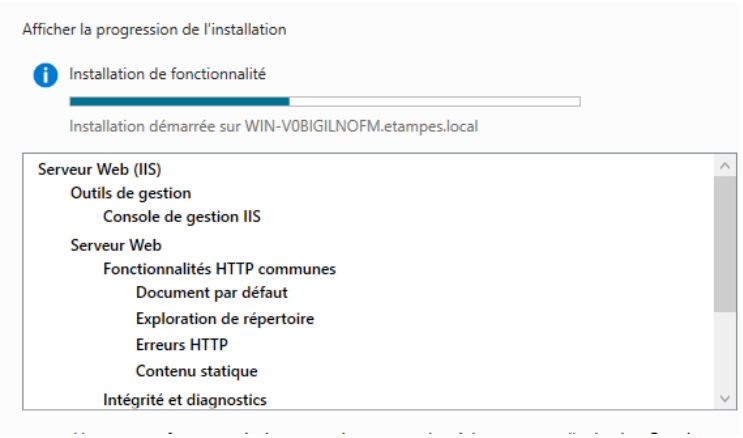
Les objectifs principaux de cette tâche de maintenance sont de m'apprendre à installer et à configurer Chocolatey Server et de le faire fonctionner en faisant des tests sur un ordinateur de test.

Cette tâche de maintenance m'a été donnée, car mon tuteur de stage voulait me montrer qu'il y a plusieurs méthodes pour installer des logiciels à distance (Chocolatey Server, lignes de commandes Chocolatey, etc…).

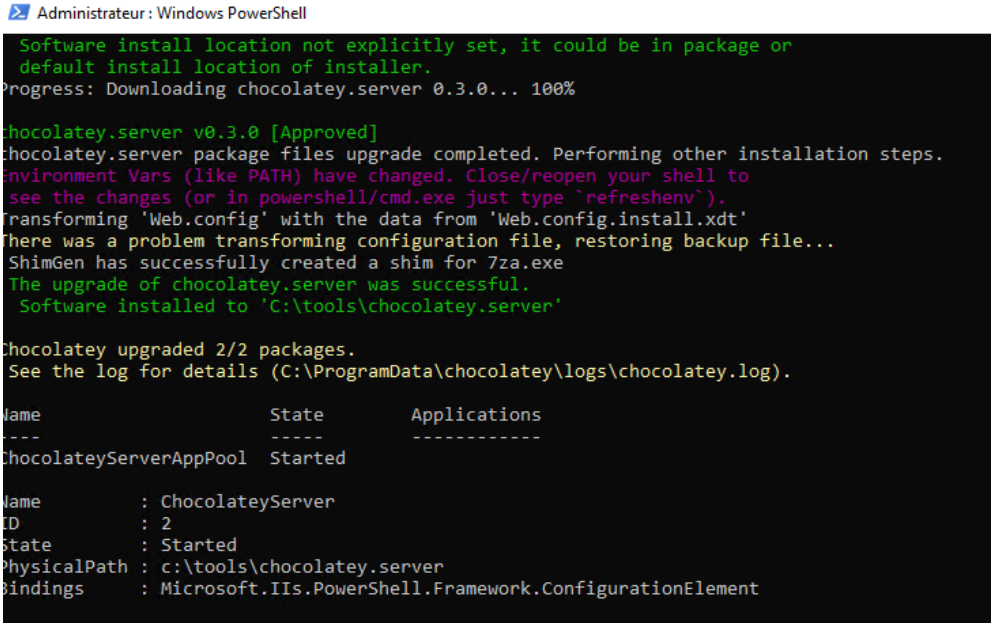
J'ai rencontré certaines difficultés, car il fallait que je comprenne à quoi servait le rôle IIS (serveur web) sur un serveur Windows et à prendre en main Chocolatey Server ainsi que ses fonctionnalités.

J’ai suivi les étapes de cette aide via ce site (Chocolatey : comment créer un dépôt local pour les paquets ? | IT-Connect).

Tout d’abord, il faut installer le service web (IIS) sur le serveur Active Directory.

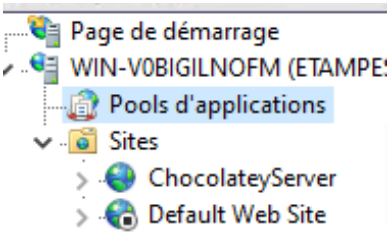


Ensuite, j’ai été prendre le script d’installation de Chocolatey Server et je l’ai téléchargé en ligne de commande Powershell en mode administrateur sur la machine serveur.



Le script d'installation Chocolatey Server permet de faire ceci :

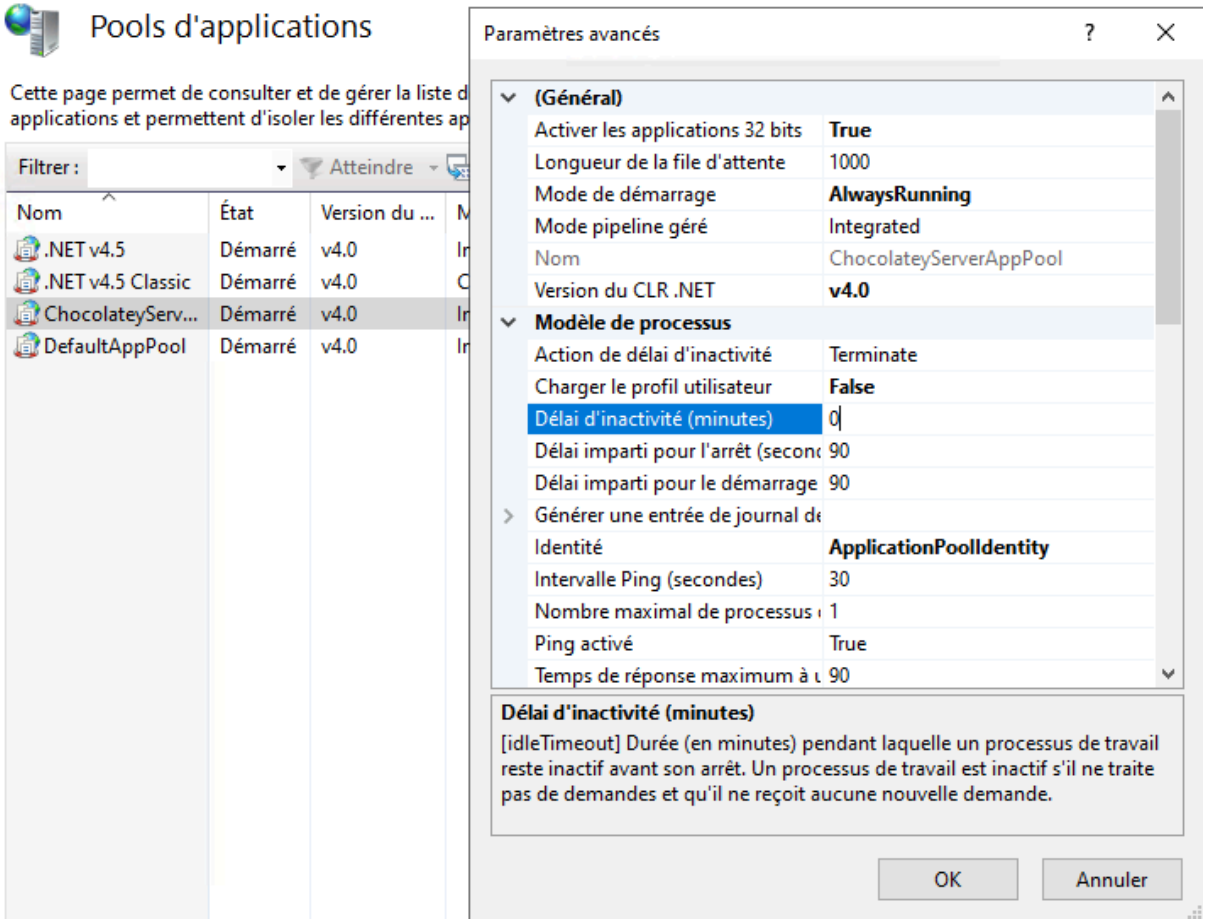
- D'installer le rôle IIS (et ASP .NET),
- D'installer Chocolatey Server dans le dossier suivant : **C:\tools\chocolatey.server**
- Créer le site "**ChocolateyServer**" dans IIS
- Créer le pool d'applications "**ChocolateyServerAppPool**" dans IIS
- Désactiver le site par défaut de IIS
- Gérer les ACL sur le dossier du site Chocolatey

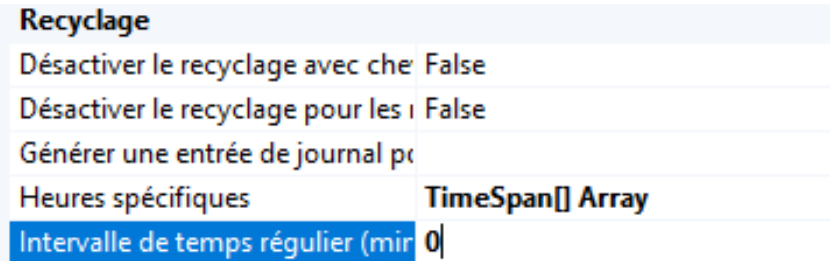


On peut voir que Chocolatey Server apparaît bien dans l'IIS du serveur Active Directory.

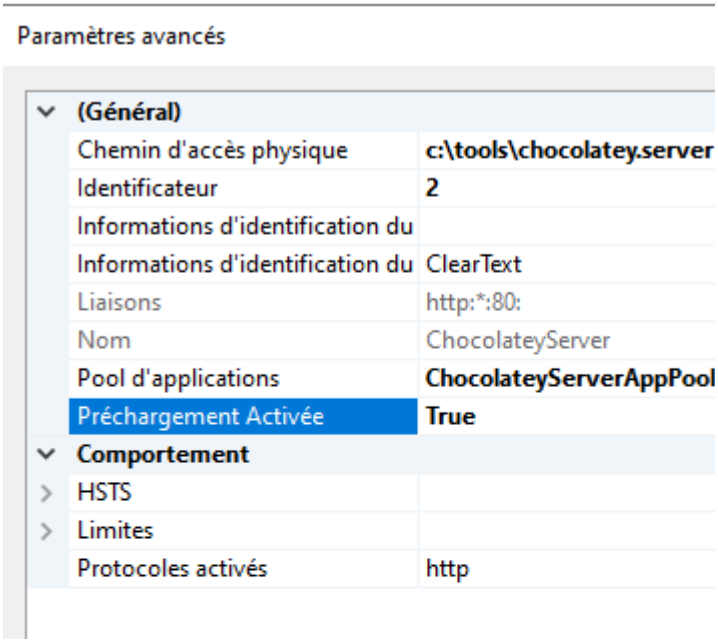
```
PS C:\Users\Administrateur> choco install IIS-ApplicationInit --source windowsfeatures
Chocolatey v2.2.2
Installing the following packages:
IIS-ApplicationInit
By installing, you accept licenses for the packages.
 [Windows Features] Deployment Image Servicing and Management tool
 [Windows Features] Version: 10.0.20348.681
 [Windows Features] Image Version: 10.0.20348.825
 [Windows Features] Enabling feature(s)
 [Windows Features] [                          0.1%                          ]
 [Windows Features] [                          1.1%                          ]
 [Windows Features] [=                         2.1%                          ]
 [Windows Features] [-                         3.1%                          ]
```

Cette commande permet d'activer le module Initialisation d'application pour l'IIS.

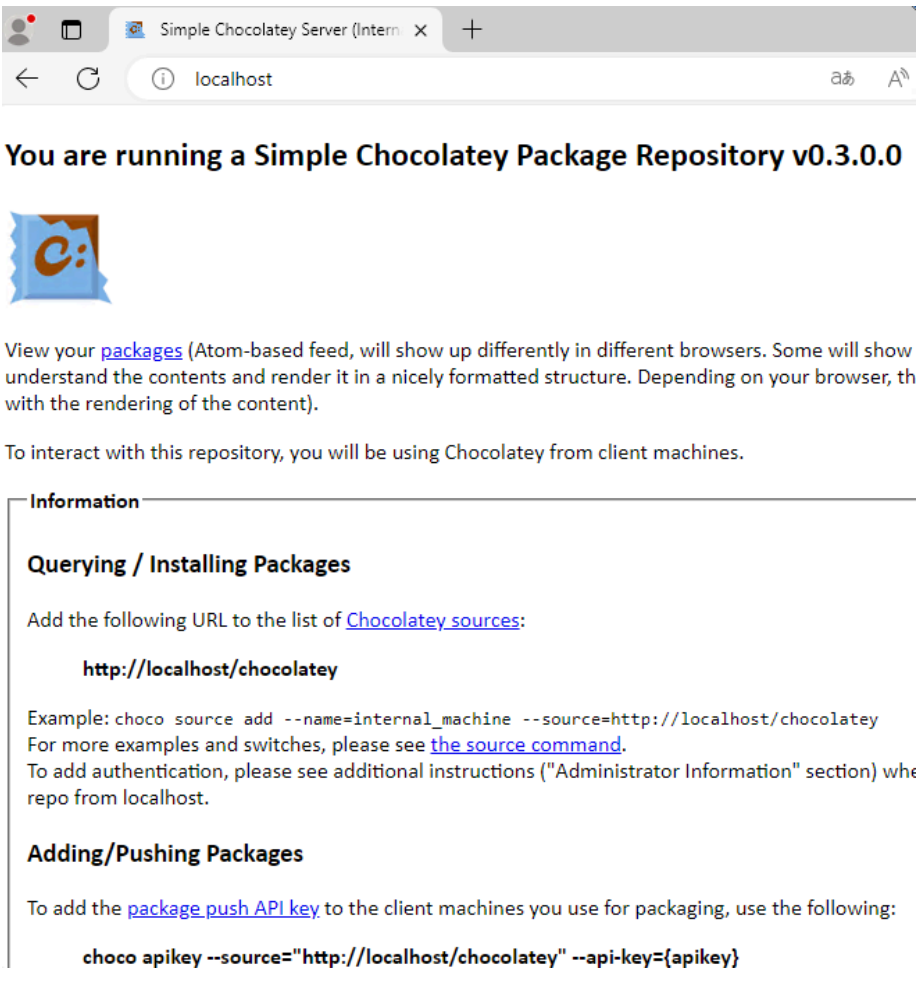




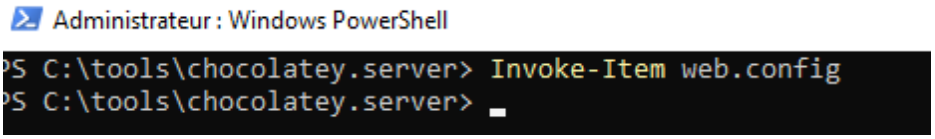
Ici, j'ai effectué la modification du mode de démarrage, du délai d'inactivité et de l'intervalle de temps régulier.

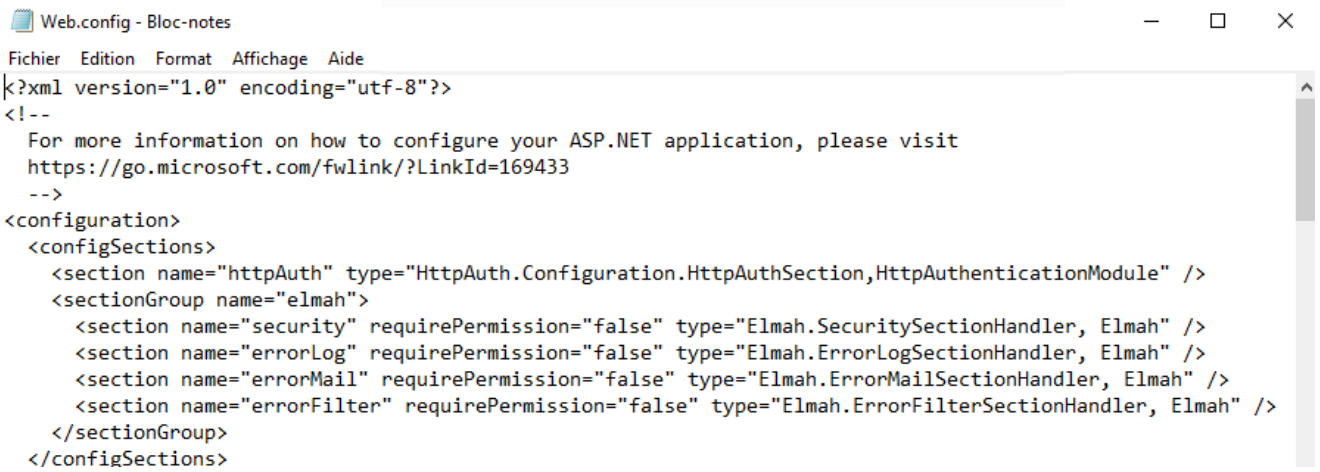


Ici, j'ai activé le préchargement du site pour prendre en compte la nouvelle configuration de celle-ci. Lorsqu'on active ce paramètre, cela améliore les performances et la réactivité du site web.



Grâce à une bonne configuration de Chocolatey Server, on peut accéder au site web de Chocolatey Server en local sur la machine serveur.





Lorsque le site web Chocolatey Server a été créé dans son répertoire, il y aura forcément un fichier de configuration web (web.config) en xml.
La commande permet d'avoir accès au fichier web.config sur la machine serveur pour pouvoir modifier la clé API (ce qui sert de mot de passe pour publier un paquet Chocolatey).
J'ai fait une recherche en trouvant l'option apiKey et en modifiant le mot de passe dans le fichier.

Afin de voir si Chocolatey Server fonctionne correctement, j'ai réalisé un test avec Brave en téléchargeant le fichier d'installation de celui-ci en extension .nupkg sur la machine serveur.

```
PS C:\> choco push .\brave.1.23.72.nupkg --source=http://192.168.30.20/chocolatey --api-key='itconnect' --force
Chocolatey v2.2.2
Attempting to push brave.1.23.72.nupkg to http://192.168.30.20/chocolatey
[NuGet] You are running the 'push' operation with an 'HTTP' source, 'http://192.168.30.20/chocolatey/'. Non-HTTPS
brave.1.23.72.nupkg was pushed successfully to http://192.168.30.20/chocolatey
PS C:\>
```

Sur la machine cliente, j'ai réalisé un test d'ajout d'un paquet sur le dépôt local Chocolatey Server avec Brave, c'est-à-dire une publication du paquet Brave sur le serveur Chocolatey Server.

```
PS C:\> choco source remove --name="'chocolatey'"
Chocolatey v2.2.2
Removed chocolatey
```

Cette commande Chocolatey permet de supprimer le dépôt communautaire de la liste des dépôts de notre machine. Cette suppression permet de réduire le risque d'installer des logiciels de sources non vérifiées ou malveillantes ce qui rend la sécurité plus renforcée.

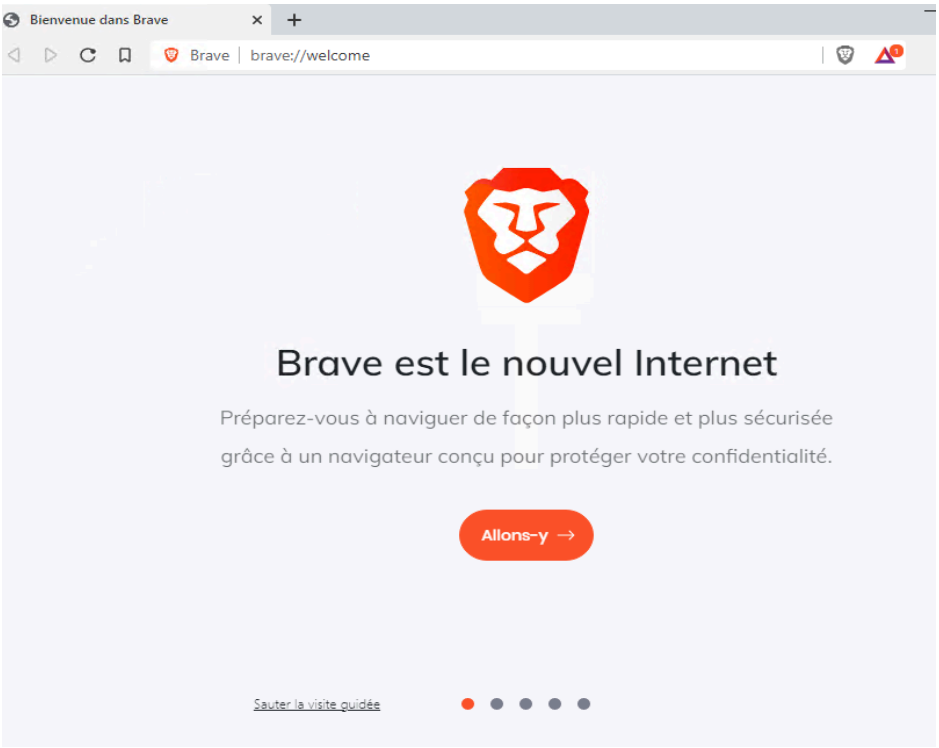
```
PS C:\> choco source add --name="'choco-itconnect'" --source="'http://192.168.30.20/chocolatey'" --priority="'1'"
Chocolatey v2.2.2
Added choco-itconnect - http://192.168.30.20/chocolatey (Priority 1)
```

Ici, j'ai fait l'ajout du dépôt local dans la machine cliente et on lui accorde la priorité la plus forte comme le serveur principal Chocolatey Server.

```
PS C:\> choco install brave
Chocolatey v2.2.2
Installing the following packages:
brave
By installing, you accept licenses for the packages.
Progress: Downloading brave 1.23.72... 100%

brave v1.23.72
brave package files install completed. Performing other installation steps.
Checking already installed version...
WARNING: No registry key found based on  'Brave*'
Installing 64-bit brave...
brave has been installed.
  brave may be able to be automatically uninstalled.
 The install of brave was successful.
  Software installed to 'C:\Users\Administrateur\AppData\Local\BraveSoftware\Brave-Browser\Application'

Chocolatey installed 1/1 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
```

Ici, avec cette commande, on fait l'installation de Brave pour voir si les actions réalisées ont bien été faites précédemment.

Ci-dessous, on voit que l'installation du navigateur Brave a bien été réalisée.




```
PS C:\> choco sources list
Chocolatey v2.2.2
choco-itconnect - http://192.168.30.20/chocolatey | Priority 1|Bypass Proxy - False|Self-Service - False|Admin Only - False.
```

Cette commande permet d'afficher les caractéristiques de Chocolatey Server qu'on a configuré.

Conclusion

Pour conclure, cette tâche de maintenance m'a permis de comprendre à quoi servait Chocolatey en général et de voir ses aspects positifs dans le cadre professionnel.

VI - Remerciements

Tout d'abord, je veux remercier les gérants Franck VALETTE et Franck SABIEN de m'avoir permis de réaliser mon stage de cinq semaines dans l'entreprise Aide Informatique puisque cela m'a permis de valider ma première année de BTS Services Informatiques aux Organisations.
Ensuite, je veux remercier mon tuteur de stage Steven VONIN de m'avoir permis de faire tous ces projets et tâches de maintenance qui m'ont permis de progresser dans le domaine de l'informatique en améliorant mes compétences que j'ai pu acquérir lors de mes cours et d'apprendre de nouvelles notions.
Pour finir, je veux remercier aussi les autres employés de m'avoir accueilli avec bienveillance.

VII - Conclusion globale

Pour conclure, ce stage m'a permis d'approfondir mes compétences, d'apprendre de nouvelles notions dans le domaine de l'informatique, de découvrir le fonctionnement d'une entreprise informatique, de m'adapter aux attentes de celle-ci et surtout de découvrir le monde professionnel.
Grâce à ce stage de cinq semaines, j'ai appris à configurer un Firewall WatchGuard, à faire l'installation complète d'un Active Directory, à mettre en place un serveur de base de données SQL et à mettre en œuvre une architecture réseau plutôt simple.
Lors de mes projets, j'ai pu appliquer ce que j'ai appris lors de mon stage (tâches de maintenances, etc…) et les connaissances que j'ai acquises durant ma première année de BTS SIO.