Institut Universitaire de Technologie,

Aix-Marseille Université

Rapport de Stage

Diplôme Universitaire de Technologie

Spécialité Réseaux et Télécommunications

Technicien support informatique de niveau 1

Guillaume CHANTROUX

SUDERIANE

Responsable entreprise : Majdouline GHARIB

Responsable académique : Sébastien SANCHEZ

2021

Table des matières

1. Introduction

La sollicitation des services fournis par un prestataire informatique n'est pas négligeable pour une entreprise. L'atout considérable de ce dernier étant la possibilité de pouvoir maintenir le parc informatique* de l'entreprise, qu'il s'agisse du matériel, des logiciels ou du réseau. Les missions du prestataire dépendent principalement des besoins de la clientèle.

Dans le cadre de mon DUT*, Diplôme Universitaire de Technologie, Réseaux et Télécommunications à l'Université d'Aix-Marseille, j'ai réalisé mon stage de fin d'étude au sein du prestataire informatique SUDERIANE.

Pendant cette période de 10 semaines, j'ai eu la possibilité de me familiariser avec un environnement technique et convivial ce qui m'a permis d'approfondir mes connaissances acquises tout au long de ma formation dans un milieu professionnel. Ainsi différentes missions variées m'ont été confié, et grâce à ce stage, j'ai eu l'opportunité de travaillé sur des projets qui m'ont permis de visualiser en quoi consiste la profession de technicien au support informatique.

Dans un premier temps, je décrirai l'entreprise Suderiane, son secteur d'activité ainsi que son organigramme. Puis, j'aborderai plus précisément le métier de technicien support informatique que j'ai pu observer à Manosque. Enfin, je parlerai les diverses missions réalisées au cours de ce stage. Et pour conclure, j'établirai un bilan de ces dix semaines passées à leur côté.

2. Présentation de l'entreprise

Prestataire informatique depuis 1998, Suderiane a pour objectif d'apporter des solutions informatiques ,qui correspondent au degré de maturité digitale, qui seront au service du cœur de métier des entreprises clientes. Ces solutions sont adaptées aux besoins des PME, des associations et des collectivités afin de permettre aux organisations de gagner en productivité et en confort.

L'assistance technique pour le dépannage informatique se fait via un contrat de fonctionnement adaptable et comportant de la supervision de serveur, du support illimité pour les incidents, de la maintenance préventive et garantie un rappel sous quatre heures ouvrées. Près de 250 clients sont sous contrat sur un total d'environ 300 clients.

Forts d'une équipe d'une trentaine de personnes, Suderiane est à même d'apporter une expertise dans plusieurs domaines tels que la maintenance informatique, l'externalisation de données, la sécurité informatique ou encore la mise en place de liens internet et de téléphonie sur IP. L'équipe est composée de techniciens et d'ingénieurs expérimentés qui interviennent à distance ou sur site pour résoudre tous problèmes informatiques sur des serveurs, le réseau, des postes de travail ou autres.

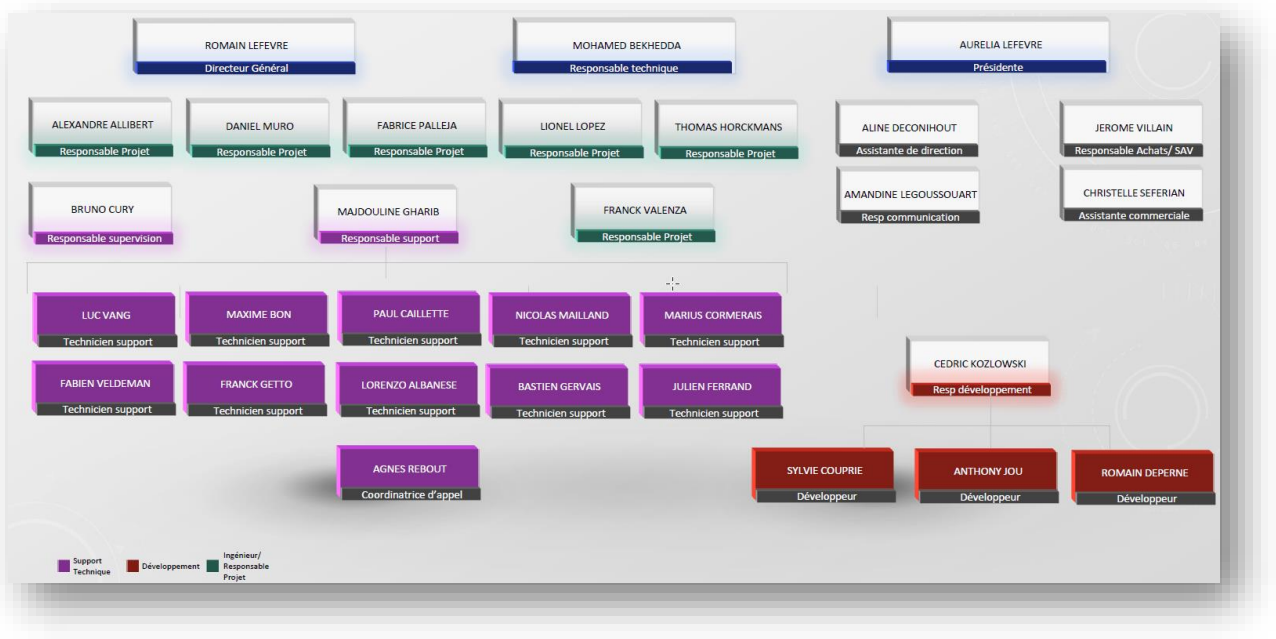


Figure 1 : Organigramme de Suderiane.

Suderiane intervient sur toute la Provence-Alpes-Côte d'Azur grâce à ces deux implantations à Manosque et La Seyne-sur-Mer qui garantissent une intervention rapide des équipes techniques en cas de problèmes informatiques.

Figure 2 : Carte des deux implantations dans la région PACA.

3. Le métier de technicien support informatique chez Suderiane

Mon stage s'est déroulé sur le site de Manosque au côté des techniciens du support. Il faut savoir que le support technique est divisé en groupes de trois à quatre personnes pour optimiser le traitement des tickets*. En effet, la répartition de clients par groupe permet notamment de se concentrer principalement sur des clients dont le parc informatique est connu afin d'améliorer l'efficacité de chaque intervention. L'un des autres avantages est que cela construit un lien avec les clients qui amène à une sympathie naturelle avec le support, car ce seront les mêmes techniciens qui seront en relation avec eux.

Je n'appartenais pas à un groupe particulier à part entière, mais j'alternais plutôt entre les groupes pour d'une part, travailler avec un maximum de personnes différentes que ce soit à distance ou tout simplement via une intervention sur le site du client. Avoir fait ainsi est à mon sens une bonne chose puisque chaque personne a une méthode et une vision des choses différentes. D'autre part, cela a été fait ainsi étant donné que certains groupes étaient débordés et un soutien supplémentaire leur était nécessaire.

Au début de ce stage, j'étais plutôt dans le groupe C car parmi ce groupe, il y avait toujours au moins une à deux personnes présentes. En effet, du fait de cette période de crise, certains ont préféré travailler à distance et cela a pu être réalisé plus souvent vu que je pouvais les aider dans les tickets nécessitants l'utilisation de l'atelier. C'est pourquoi, au fur et à mesure, j'ai commencé à alterner entre chaque groupe pour épauler dans la masse de ticket.

3.1 Qu'est-ce que le support informatique ?

Habituellement, un technicien support informatique a pour mission de résoudre des problèmes informatiques à distance, à l'aide d'outils logiciels ou en communicant par téléphone et messagerie. Il doit remédier au problème tout en guidant l'utilisateur vocalement ou en prenant le contrôle de son ordinateur. À la suite de son intervention, le technicien peut profiter de cette occasion pour former l'utilisateur en lui expliquant les manipulations et le but de l'opération. Cette formation possède deux objectifs. Le premier étant que du côté utilisateur, cette explication est généralement très appréciée car elle lui permettre de comprendre et de pouvoir résoudre seul (dans les cas possibles) le problème qui pourrait réapparaître. Deuxièmement, du côté support, cela permet d'alléger le nombre de futurs appels, car l'utilisateur n'appellera plus et pourra même former ses collègues à son tour.

Or, à Suderiane, le technicien support ne se limite pas aux interventions à distance. Il peut être amené à travailler en atelier pour préparer des équipements qui seront par suite livrés au client, mais il peut également effectuer des interventions sur site.

Pour ce qui est des moyens de communication avec le client, Suderiane utilise le logiciel 3CX pour téléphoner, mais également TeamViewer ou encore AnyDesk pour la prise en main à distance des postes de travail et Outlook pour l'envoi des mails.

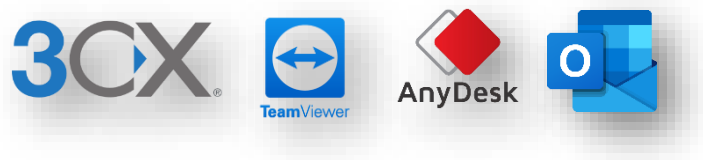


Figure 3 : ***Logiciels de communication utilisés.***

3.2 L'arrivée des incidents/SR

Les incidents et les SR correspondent aux demandes de chaque utilisateur. La définition de ces deux demandes sera décrite dans les parties 4.1 pour les incidents et 4.2 pour les SR.

Les demandes des utilisateurs sont faites de deux manières : soit ils appellent le standard téléphonique, soit ils envoient un mail au support. Chaque demande correspond à un ticket qui va être créé et qualifié dans le logiciel Octopus. Cela se présente ainsi :

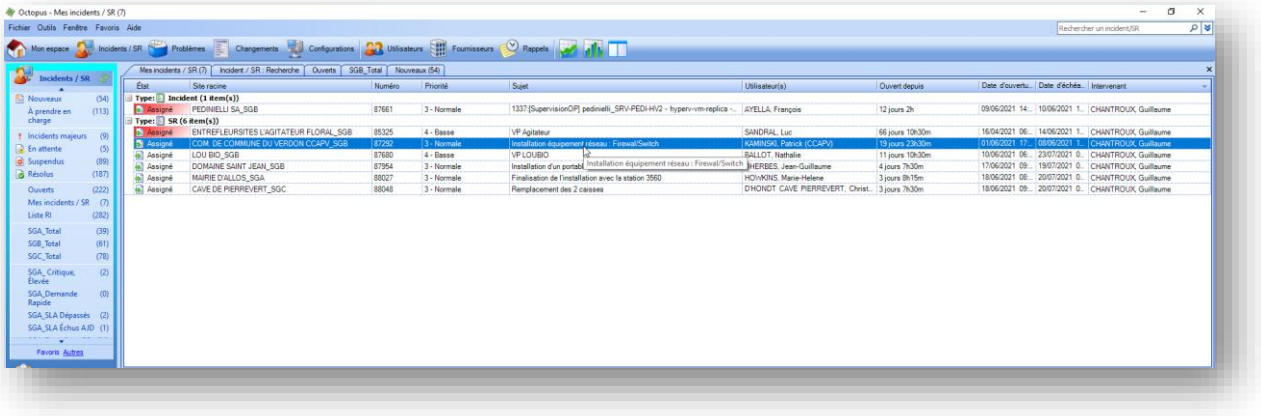


Figure 4 : Tickets qui me sont attribués dans Octopus.

La prise en main de ce logiciel a été pour moi une épreuve. Il est composé d'énormément d'informations et de catégories à maîtriser. Sur la figure 4, on y retrouve les tickets qui m'ont été attribués. L'une des choses les plus importantes à faire lors de la résolution d'un ticket est de noter son temps ainsi que l'activité effectuée. Certains tickets sont facturés au temps passé, c'est pourquoi il faut impérativement inscrire ce temps. Écrire l'activité et d'autant plus important, car une autre personne du support peut prendre le relais et voir ce qui a déjà été fait pour clôturer le ticket en cas d'absence de la personne qui l'avait pris en charge.

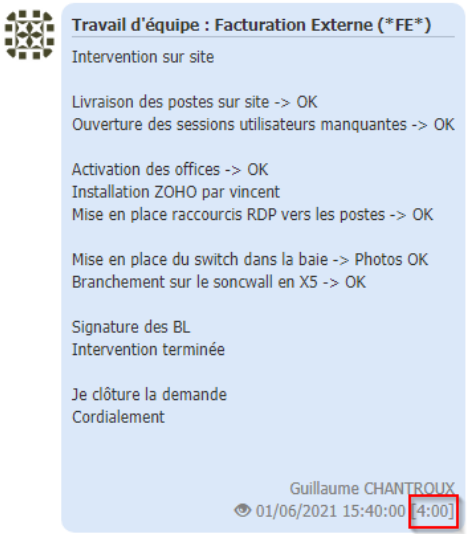


Figure 5 :
Activité et effort total
dans la résolution d'un ticket.

4. Les missions qui m'ont été attribuées

Comme on peut s'en douter, je n'ai pas une qu'une seule mission à prendre en charge. Des tickets s'ouvrent quotidiennement et ils doivent être clôturés le plus rapidement possible pour une satisfaction cliente optimale. C'est pourquoi je n'ai pas un projet défini et que je vais présenter les plus grandes parties que j'ai pu effectuer. À mon sens, cela m'a permis de découvrir un maximum de choses différentes en un temps assez court, mais également d'obtenir une vision plus globale de ce qu'est le quotidien d'un technicien support informatique.

4.1 Incidents

Les incidents correspondent aux problèmes que les utilisateurs rencontrent. Ce sont les soucis qui sont censés pouvoir être traités rapidement. Il y a un facteur à prendre en compte pour chaque ticket : le SLA* (Service Level Agreement). Il doit être respecté un maximum et peut ainsi mesurer l'efficacité et la rapidité de prise en charge et de traitement du ticket. Le SLA d'un incident est bas, ce qui veut dire qu'il faut le traiter de préférence rapidement pour ne pas influer sur la statistique globale.

Les incidents sont de tout type. Ils sont dans la majorité des cas traités à distance en prenant la main sur le poste de travail du client. Cela peut aller de l'oublie d'un mot de passe de session, un problème sur une boîte mail, la configuration d'une imprimante, un logiciel qui est dysfonctionnel ou encore l'ajout d'une connexion VPN*. Parmi les incidents, on retrouve également les tickets créés automatiquement par les logiciels de supervision*.

Les incidents sont intéressants du fait de leur diversité, mais aussi grâce à l'aspect de communication avec un utilisateur qui est enrichissant. Personnellement, je n'étais absolument pas à l'aise lors des conversations téléphoniques, mais avec les conseils des personnes du support, j'ai pu remédier à ce défaut.

Je n'ai pas trouvé pertinent de parler d'un incident en particulier toutefois, il faut savoir que ce genre de ticket est quotidien.

4.2 SR

Les SR, contrairement aux incidents ont un SLA plus élevé, car ils peuvent être mis en pause à tout moment dans le cas où une urgence se présenterait. Ces tickets correspondent aux demandes d'utilisateurs ou bien du responsable informatique. On y retrouve la préparation d'équipements, les visites préventives (abordées au 4.2.2) ou encore les mises à jour de logiciel ou de l'antivirus.

4.2.1 Préparation de matériel en atelier

La préparation de matériel est une tâche récurrente. Cela peut concerner des ordinateurs, des serveurs, des switch* ou encore des firewalls*. Dans ces deux sous-parties, j'aborderai dans un premier temps, seulement les postes de travail puis dans un second temps, un routeur firewall.

4.2.1.1 Postes de travail

La préparation d'un poste de travail est liée à une demande du responsable informatique du client. Dans la plupart des cas, il s'agit d'un nouvel ordinateur qui est commandé puis amené en atelier pour s'en occuper. Mais cela peut très bien être aussi de l'amélioration d'ordinateur.

L'amélioration est nécessaire quand la machine devient lente ou bien que la version Windows du système est trop ancienne. L'avantage d'améliorer l'équipement est la somme d'argent totale qui sera dépensée. Je m'explique, on vérifie et examine dans un premier temps si l'ordinateur a la possibilité de passer sous Windows 10 dans les meilleures conditions. De ce fait, on peut se faire un ordre d'idée sur ce qui est à ajouter pour calculer le prix total potentiel. Si la solution d'amélioration n'est pas rentable en comparaison à un achat d'une nouvelle machine, on privilégiera la commande.

Au cours des différents ordinateurs que j'ai été amené à prendre en charge, j'ai pu rencontrer ces deux cas. Il faut bien se rappeler qu'une installation de poste est facturée au temps passé donc il faut impérativement le renseigner sur Octopus.

Dans le cas d'une amélioration, j'ai eu à ajouter de la mémoire RAM* et à changer des disques HDD* en SSD*. Qui dit changement de disque dit transfert de données. Étant donné que le client garde son ordinateur, il va de soi qu'il veut également conserver ses données (c'est aussi le cas mors d'un remplacement complet). Cela se faisait via le logiciel AutoBackup qui stockait les données dans un disque dur externe puis les retransférait une fois le système prêt. Cette étape est faite en atelier lorsqu'il s'agit d'une amélioration, mais faite sur site quand on remplace l'ordinateur du client.

Parlons maintenant de la préparation du système. La première étape était de déployer l'image Windows à partir du serveur de déploiement de Suderiane. Cela se fait via le « Boot Menu* ».

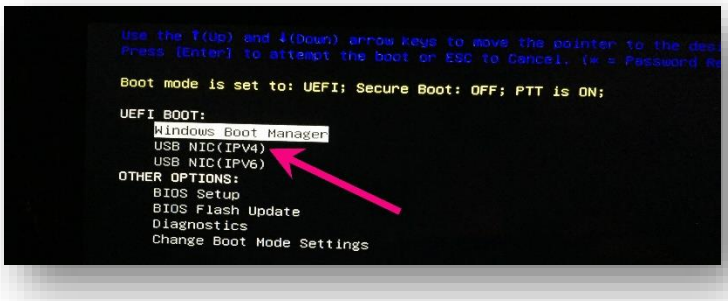


***Figure 6 :** Accès au serveur de déploiement depuis le BIOS*.*

L'image accessible depuis le serveur est souvent mise à jour pour gagner du temps. En effet, il n'est pas sans savoir que de nombreuses mises à jour Windows sont disponibles régulièrement et garder une ancienne image équivaut à télécharger et installer ces mises à jour manquantes à chaque nouveau poste de travail devant être traité. Pour ce qui est des mises à jour, il vient s'ajouter celles des drivers et du BIOS qui causent beaucoup de problèmes de compatibilités si elles ne sont pas effectuées.

Une fois l'image en place, il reste tout un tas d'élément à faire. Pour ce qui est des logiciels standards style navigateur, et même TeamViewer pour la prose en main à distance ultérieur, Suderiane possède un script qui les installe tous en une seule fois ce qui ajoute encore une fois un côté pratique et optimisé. Il y a également Eset (antivirus) fourni par Suderiane dont les licences se trouvent dans le dossier du client. Ce dossier contient tout un tas d'informations, dont le parc du client ou encore des procédures, des configurations ou encore les photos de la baie serveur*.

Une chose importante à faire est de renommer le poste en fonction de la politique de nommage du contrôleur de domaine (DC)*. En d'autres termes, les noms ont une suite logique avec un nombre ou bien sont écrits avec le nom de famille de l'utilisateur qui possédera le poste. Le renommage doit être fait avant d'intégrer l'ordinateur au domaine*.

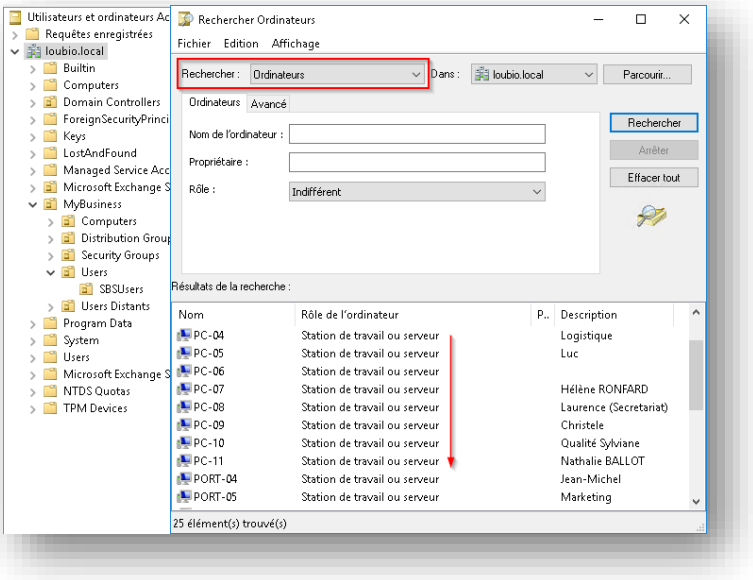


Figure 7 : Filtrage le l'Active Directory* par ordinateur et politique de nommage.

Pour l'intégrer, il faut que le poste puisse communiquer avec le serveur AD (Active Directory). C'est pourquoi, il faut que la machine se trouve dans le même réseau que ce dernier. À cet effet, on utilise un VPN , Virtual Private Network, qui est normalement configuré sur le pare-feu du parc client. Toutes les informations concernant la clé partagée du VPN ou encore l'adresse IP à laquelle se connecter est renseigné dans le logiciel KeePass qui permet de stocker des mots de passe en tout genre (comme l'administrateur ou encore les identifiants de certains utilisateurs). J'ai eu beaucoup de difficulté avec cette partie-là, car toutes les informations n'étaient pas forcément renseignées et chaque client à un logiciel VPN différent (qui n'est pas indiqué non plus).

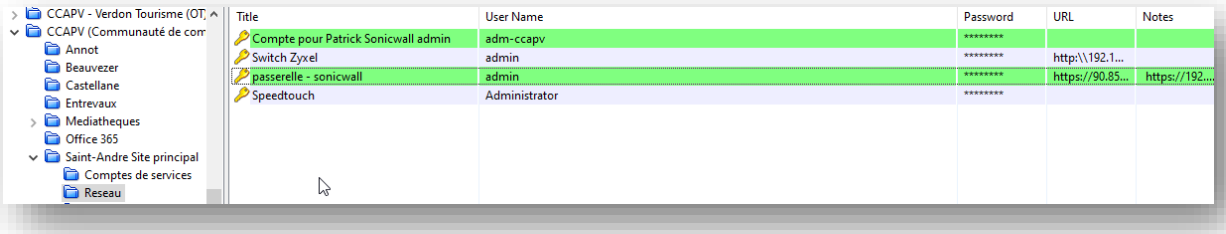


Figure 8 : Récupération d'identifiants et de mots de passe via KeePass.

Une fois connecté au VPN, on peut ajouter la machine au domaine. De plus, grâce à cette intégration, il est maintenant possible de se connecter aux sessions des utilisateurs si toutefois le mot de passe est connu (présent dans KeePass). Si ce n'est pas le cas, il faut appeler cet utilisateur pour obtenir cette information.

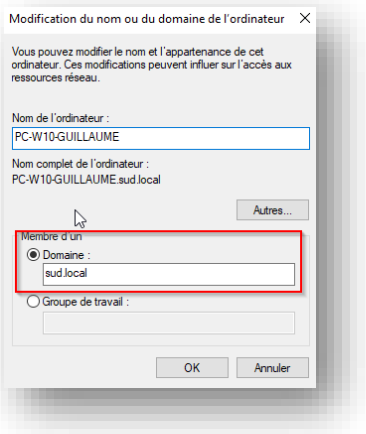


Figure 9 :
Adhésion d'un poste à un domaine.

Pouvoir se connecter à sa session est un gain de temps. En effet, depuis le début, on se trouve sur une session d'administrateur local. Or, on ne peut pas configurer la boîte mail par exemple sur ce compte. Il y a aussi les raccourcis sur le bureau (qui sont à la demande du client comme celui redirigeant vers le TSE*, Terminal Server Edition).

4.2.1.2 Routeur Firewall

Le firewall à configurer était pour client dénommé CCAPV. C'était un SonicWall avec le modèle TZ 270W.

***Figure 10 :* SonicWall TZ 270W avec les deux antennes.**

Un nouveau site était sur le point d'être mise en place donc un nouveau parc devait être également conçu de toute pièce. Pour cela, à partir du parc informatique des autres sites, j'ai choisi une plage d'adresse IP qui était disponible pour ne pas créer de conflit. Ce réseau était le 192.168.114.0/24.

Avant tout début de configuration, il faut enregistrer le routeur via un compte MySonicWall géré par Suderiane. Celui-ci contient tous les firewalls de chaque client catégorisé. Cette manipulation est premièrement utile pour activer la licence, mais également pour de la sauvegarde de la configuration via un cloud. Il s'avère que la sauvegarde m'a été utile, car avec une erreur de configuration, je n'avais plus accès au TZ et il m'a donc fallu le réinitialiser. Grâce à celle-ci, je n'ai donc pas eu à refaire toute ma configuration déjà effectuée. La première étape était donc de définir l'interface LAN* (Local Area Network) avec une IP faisant partie de la plage précédemment définie.

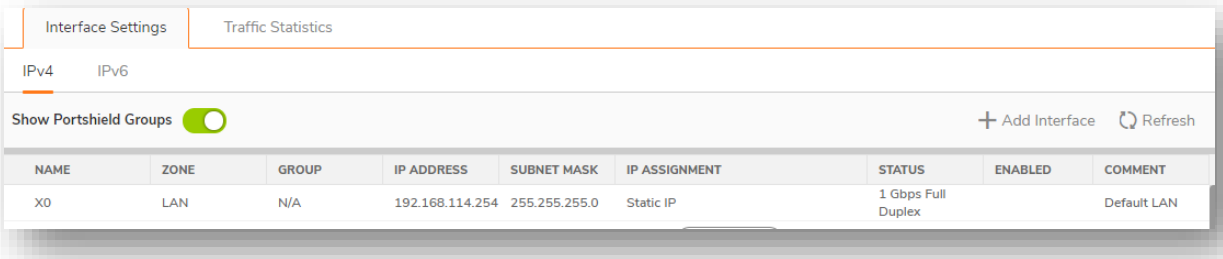


***Figure 11 :* Interface LAN configurée.**

Cette interface fera également office de DHCP* (Dynamic Host Configuration Protocol) pour les postes de travail.

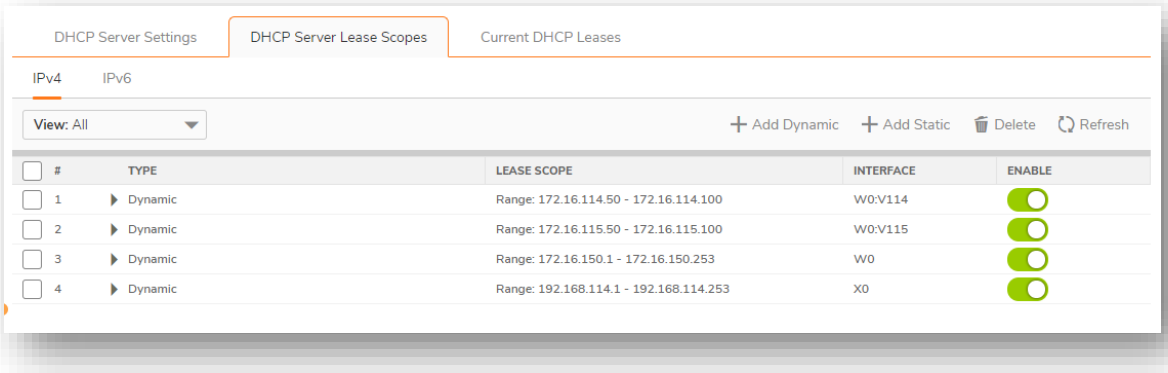


Figure 12 : Plages d'adresse DHCP pour la zone LAN, le Wifi public ainsi que le Wifi privé.

Le pool d'adresse concernant la zone LAN correspond à la dernière ligne de la figure 12. On peut y voir également d'autres plages DHCP qui correspondent aux deux Wifi (privé et public) que j'ai dû paramétrer. Pour cela, il a fallu créer des zones de type « Wireless » (sans-fils en français) :

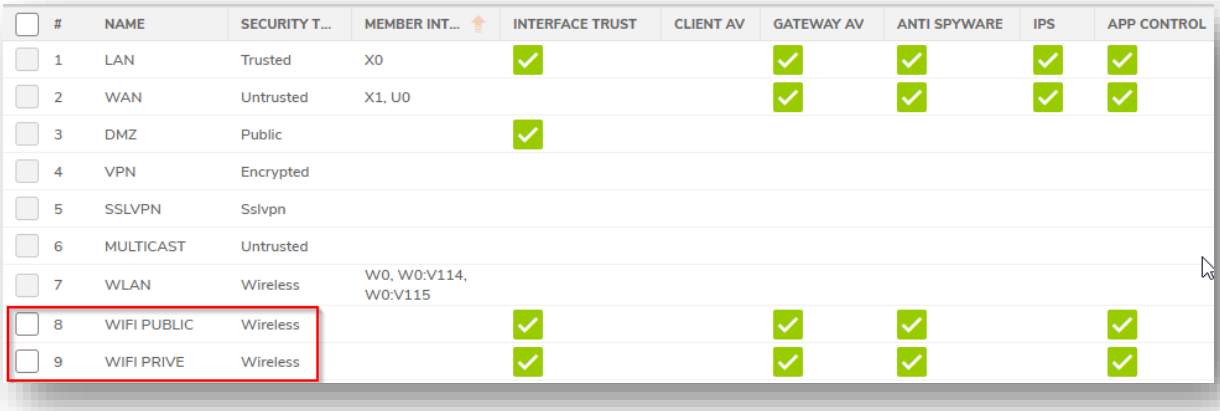


Figure 13 : Création des zones de Wifi public et privé.

À la suite de cela, on crée deux interfaces distinctes qui seront attribuées chacune à leurs zones respectives.

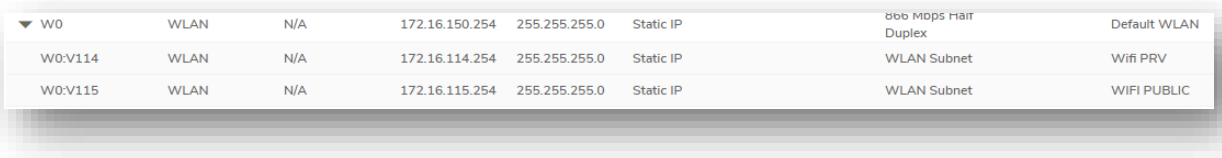
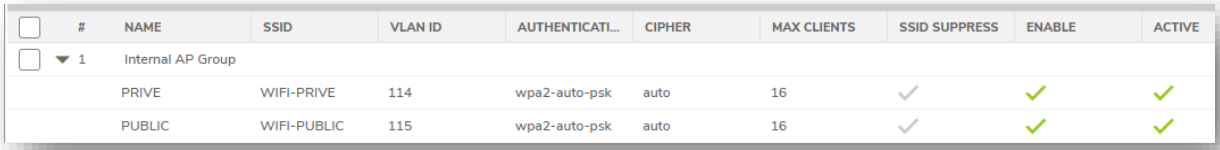


Figure 14 : Configuration des interfaces sans fils.

Enfin, il faut définir les points d'accès. En effet, si on regarde la figure 14, on remarque deux antennes Wifi sur le firewall. Habituellement, Suderiane relie le firewall à un point d'accès extérieur au routeur, c'est pourquoi je n'ai pas pu me baser sur des exemples sur d'autres sites ou même d'autres clients.

Après plusieurs recherches, nous sommes arrivés à activer les deux points d'accès avec une clé différente pour chacun qu'il a fallu conserver dans KeePass pour à l'avenir les retrouver au besoin.



#	NAME	SSID	VLAN ID	AUTHENTICATI...	CIPHER	MAX CLIENTS	SSID SUPPRESS	ENABLE	ACTIVE
1	Internal AP Group								
	PRIVE	WIFI-PRIVE	114	wpa2-auto-psk	auto	16	✓	✓	✓
	PUBLIC	WIFI-PUBLIC	115	wpa2-auto-psk	auto	16	✓	✓	✓

Figure 15 : Activation des points d'accès.

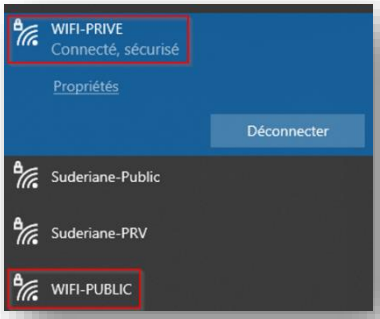


Figure 16 : Apparition des points d'accès depuis le sélecteur de réseau de l'ordinateur.

À ce stade, ce sont seulement des Wifi qui permettent un accès internet. Or, la différence entre un wifi public et privé est que le privé peut communiquer avec les équipements de l'interface LAN, mais également pourra se servir du VPN que nous configurerons juste après. Par intuition, j'ai don ajouté des règles d'accès permettant ce trafic. Malheureusement, cela n'a pas fonctionné directement. Après plusieurs tentatives et recherches sur Internet, nous avons dû appeler directement SonicWall afin qu'il puisse investiguer sur le problème. La solution était une petite case à coché permettant le ping vers la passerelle de l'interface LAN depuis la zone Wifi privé.

L'étape suivante était la configuration du VPN dit « agressif ». La particularité de ce dernier est que l'on configure de part et d'autre des sites le VPN avec des plages d'adresses sources et de destinations autorisées à utiliser le VPN (la configuration se fait en inversée selon l'endroit où on se situe).
Les choses à inverser seront marquées de flèches rouges sur les figures qui vont suivre.

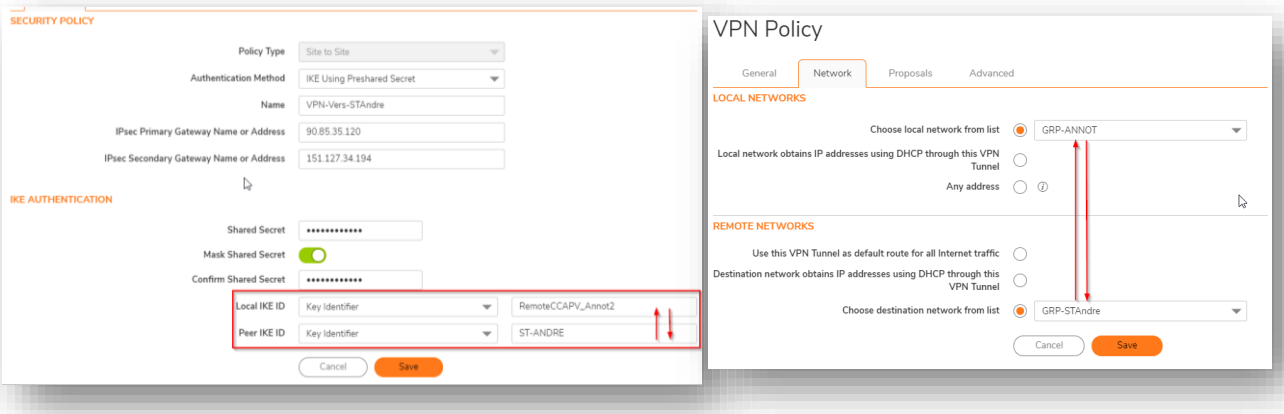
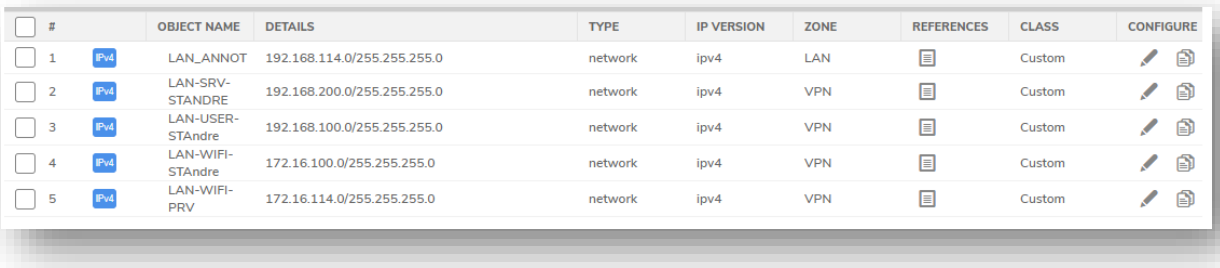


Figure 17 : Paramètres appliqués lors de la configuration du VPN.

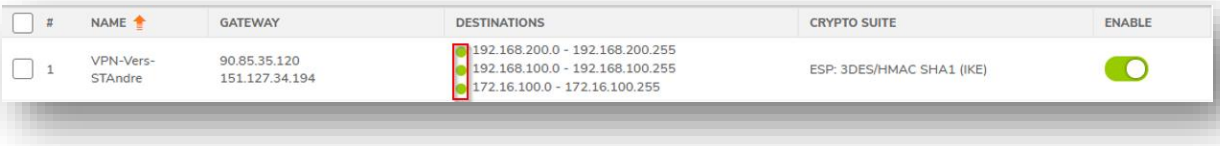
Sur la figure 17, on peut voir des objets avec « GRP-**** » comme nom. Ces objets ont précédemment été créés pour contenir les différentes plages IP qui seront autorisées à transiter via le VPN.



#		OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	REFERENCES	CLASS	CONFIGURE
1	IPv4	LAN_ANNOT	192.168.114.0/255.255.255.0	network	ipv4	LAN		Custom	
2	IPv4	LAN-SRV-STANDRE	192.168.200.0/255.255.255.0	network	ipv4	VPN		Custom	
3	IPv4	LAN-USER-STAndre	192.168.100.0/255.255.255.0	network	ipv4	VPN		Custom	
4	IPv4	LAN-WIFI-STAndre	172.16.100.0/255.255.255.0	network	ipv4	VPN		Custom	
5	IPv4	LAN-WIFI-PRV	172.16.114.0/255.255.255.0	network	ipv4	VPN		Custom	

Figure 18 : Objets correspondants à des plages IP précises qui seront organisés dans différents groupes.

Si tout fonctionne correctement, des points vers de part et d'autre des plages IP apparaissent pour signaler la bonne configuration du VPN.



#	NAME	GATEWAY	DESTINATIONS	CRYPTO SUITE	ENABLE
1	VPN-Vers-STAndre	90.85.35.120 151.127.34.194	192.168.200.0 - 192.168.200.255 192.168.100.0 - 192.168.100.255 172.16.100.0 - 172.16.100.255	ESP: 3DES/HMAC SHA1 (IKE)	

Figure 19 : VPN opérationnel.

À ce stade, le ticket n'était pas terminé, mais j'ai dû m'arrêter ici car la fin de mon stage était le jour de cette dernière configuration. De plus, pour clôturer celui-ci, une intervention sur site était requise pour conclure la configuration du firewall. En effet, une des choses manquantes était de paramétrer l'accès distant pour manager le SonicWall. L'accès devant être limité uniquement par les plages IP de Suderiane, j'ai seulement créé les objets relatifs à ces plages.

Enfin, il aurait fallu brancher une des interfaces du firewall (préalablement mis en DHCP) à une LiveBox qui récupérerait une adresse IP qui aurait permis la connexion à distance.

4.2.2 Visites préventives

La visite préventive ou « VP » est une procédure de supervision consistant à vérifier la bonne santé des serveurs et des pare-feux de clients. Cette dernière permet d'éviter en amont des problèmes qui auraient pu être rencontrés dans le futur. C'est une tâche devant être effectuée une fois par an mais depuis la situation de crise due à la crise sanitaire, il était préférable de convenir à une VP à distance. Malgré tout, une année sur deux, une intervention sur site est essentielle pour souffler les serveurs (cela consiste à les nettoyer et à retirer la poussière accumulée à l'intérieur).

En premier lieu, avant d'effectuer la VP, il faut contacter le responsable informatique (RI) du client en question afin d'informer de notre intervention à distance. C'est une étape importante parce qu'elle permet au client de prendre connaissance que l'on s'occupe d'eux, mais également d'expliquer en quoi consiste la VP. Il est également important de notifier que ce passage n'aura aucun impact avec leur travail afin de les rassurer. En d'autres termes, aucune coupure ne sera rencontrée ainsi qu'aucune sollicitation de leur part n'est attendue.

Par suite, un formulaire correspondant à la procédure à suivre pour effectuer la VP est à compléter.
À chaque étape, trois choix sont possibles :

- La validation : celui-ci souligne qu'après-vérification, aucun problème a été rencontré.
- La mise en erreur : il faut cocher cette option lorsqu'une anomalie est repérée. Un champ de texte est prévu pour renseigner les informations sur cette anomalie. Un ticket sera alors ouvert à la fin de la VP pour que le problème soit traité ultérieurement.
- Le non-applicable : certains critères peuvent ne pas être vérifiés, car le matériel ou la conception du parc du client ne sont pas adéquats.

Certains soucis sont simples à résoudre, il n'est donc pas nécessaire de les noter en erreurs. Or, il est préférable de ne pas les traiter durant la VP, car on ne sait pas à l'avance si ces problématiques prennent du temps.

Ce formulaire est découpé en trois grandes parties : les serveurs, les outils internes à Suderiane et les Firewalls.

4.2.2.1 Les serveurs

En ce qui concerne les serveurs, il s'agit de vérifier plusieurs spécificités dont je vais citer et détailler.

Une chose basique à faire est de vérifier les mises à jour systèmes des serveurs (qu'ils soient physiques ou virtuels). Normalement, les mises à jour sont configurées de telles sortes à ce qu'elles s'installent toutes seules via des stratégies de groupe. Or, tant qu'à faire autant les faire directement à la main. Il faut bien faire attention étant donné que certaines mises à jour demandent un redémarrage pour qu'elles soient bien effectuées. Il faut donc planifier un redémarrage dans les plages d'horaires inoccupés des employés de l'entreprise. Généralement, on planifie cela aux environ de deux ou trois heures du matin pour être certain que personne n'est impacté. Il faut aussi faire attention à cela vu que les serveurs virtuels étant hébergés sur le serveur physique, il faut planifier les mises à jour à une heure où le serveur aura déjà redémarré sinon elles ne seront pas effectuées. On place donc une marge d'une heure environ.

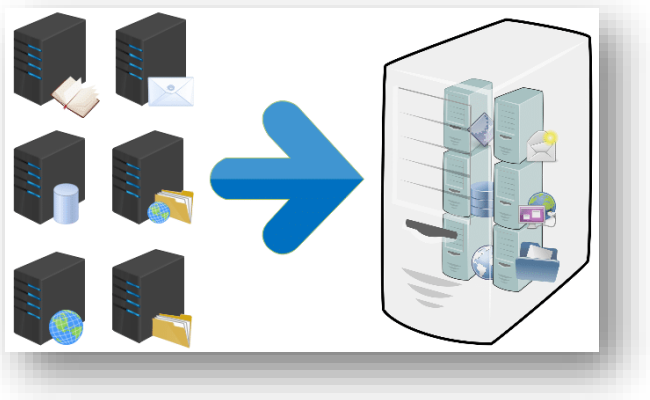


Figure 20 : Serveurs virtuels hébergés sur un serveur physique.

En ce qui concerne les mises à jour, il y a également l'antivirus Eset (celui que Suderiane fourni). Elle se fait depuis une console soit accessible depuis le serveur du client soit depuis la console dédiée à Suderiane. Enfin, il faut regarder si TeamViewer Host est bien présent sur chaque serveur pour pouvoir prendre la main dessus, car certains logiciels que les entreprises utilisent sont des logiciels dits « métiers » et ce sont des fournisseurs qui n'ont pas un accès total au serveur.

En parlant d'accès, il faut aussi examiner si la DRAC est utilisable pour contrôler le serveur. Une carte DRAC est une carte d'administration à distance des serveurs qui permet, à travers une connexion Web de prendre la main sur la console du serveur, de redémarrer, éteindre ou bien allumer le serveur.

Passons maintenant à toute la partie sauvegarde du serveur. La sauvegarde de donnée est une chose primordiale et indispensable. Les informations sur la manière dont sont organisée les données est le plus souvent renseigné sur le parc informatique du client. Il faut donc regarder si tout est bien configuré. La plus basique est la sauvegarde en local avec Wbadmin qui est un outil intégré aux serveurs Windows permettant de sauvegarder et de restaurer le système d'exploitation, les volumes, les fichiers, les dossiers et les applications.

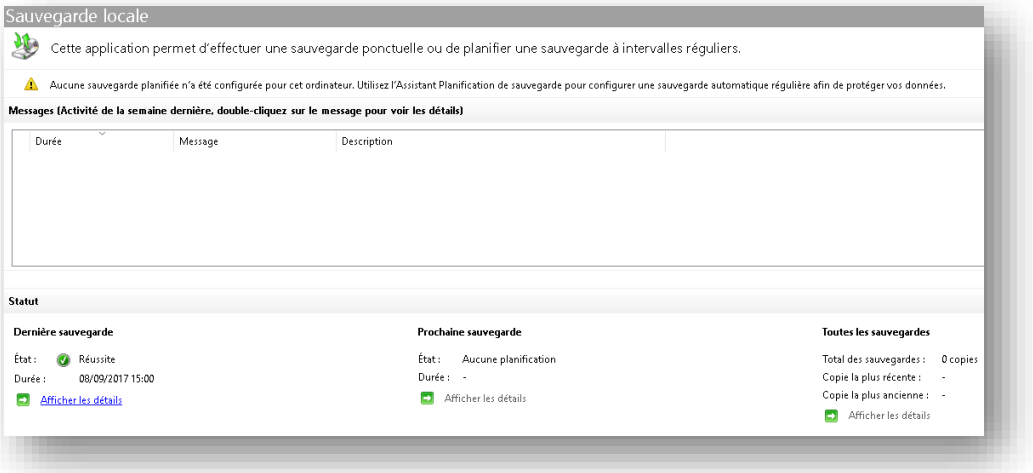


Figure 21 : Exemple de sauvegarde locale non paramétré.

Cela peut être aussi un logiciel nommé Veeam qui permet de faire des backups et des réplications des serveurs virtuels. Certaines données sont aussi sauvegardées dans ce qu'on appelle un NAS qui est un serveur de stockage en réseau autonome.
Certaines données sont externalisées. En d'autres mots, elles sont sauvegardées dans un endroit extérieur à l'entreprise. L'externalisation permet, en cas d'incendie ou autre, de conserver les données.

Mais la partie sauvegarde ne s'arrête pas ici. Parfois, certains fichiers auparavant présents ne sont plus disponibles dans un dossier partagé, car ils ont été soit corrompus soit supprimés par inadvertance. On fait alors appel aux clichés. Les clichés permettent de revenir à une version antérieure du dossier. Il est donc important qu'ils soient actifs.

Toujours dans les données, penchons-nous maintenant sur le côté un peu plus « matériel » : les disques. Sur chaque serveur, connaître l'espace restant est important, car ce n'est pas infini. Les tailles des disques sur les serveurs virtuels peuvent être agrandies depuis l'hyperviseur (plate-forme de virtualisation qui permet à plusieurs machines virtuelles avec différents systèmes d'exploitation de travailler sur une même machine physique en même temps). Mais pour ce qui est des disques physiques, ils seront à commander (avec l'accord du client bien évidemment) et à rajouter.

Une dernière chose à vérifier pour les disques physiques est le RAID. Le RAID est un ensemble de techniques de virtualisation de stockage qui permet de répartir es données sur plusieurs disques afin d'améliorer la sécurité et les performances du stockage des données. Il existe différents types de RAID, mais les plus utilisés sont les RAID 0, 1 ou 5. Le type de RAID a été défini par le chef de projet et il faut vérifier qu'il soit bien actif sur chaque disque physique. Précédemment, je parlais d'ajouter un disque en cas de manque de stockage. Il faudra évidemment configurer le RAID sur ce disque. Cette partie se fait depuis OpenManage. Cette application est un produit Dell et à la même interface que la DRAC et a les mêmes particularités, mais contrairement à la DRAC où l'accès se fait depuis le réseau, OpenManage se lance localement.

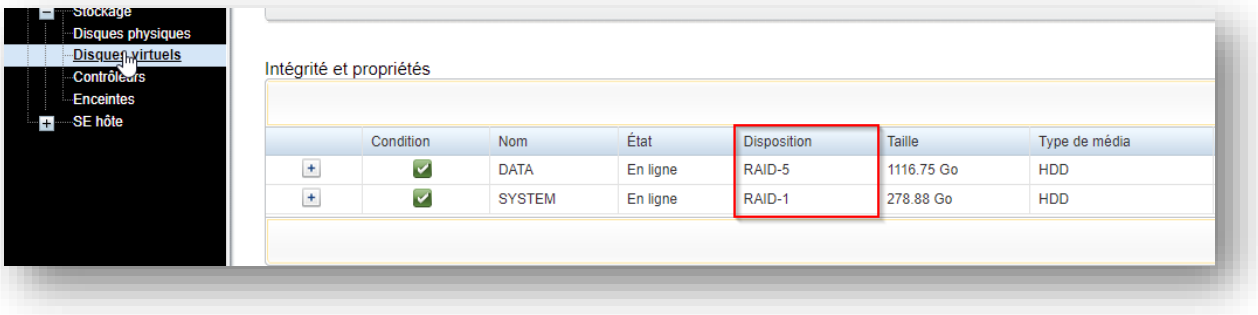


***Figure 22 :** Visualisation des disques configurés en RAID-5 et RAID-1 via la DRAC.*

Une fois que toute la partie sauvegarde a été abordée, on peut désormais passer au journal d'événements du contrôleur de domaine. Un contrôleur de domaine est un serveur qui répond aux demandes d'authentification et contrôle les utilisateurs du réseau. Le domaine est un bon moyen de hiérarchique d'organiser les ordinateurs et les utilisateurs travaillant sur le réseau. La seule chose à faire est de répertorier les erreurs de certaines catégories du journal d'événements dans un fichier Word qui sera envoyé au responsable de projet. Pour cela, sur chaque catégorie, on utilise un filtre pour ne faire apparaître que les erreurs à remonter. Ici, on est dans le cas où on ne traiterait pas les erreurs directement, c'est pourquoi un ticket sera créé où il faut donc répertorier toutes les anomalies apparues.

Enfin, une dernière chose est à vérifier pour la partie serveur. Eaton Intelligent Power Protector est un logiciel normalement présent sur les serveurs physiques et actifs sur les serveurs. Si ce n'est pas le cas, il faut impérativement en informer le responsable de projet. En réalité, ce logiciel est relié à un onduleur. L'onduleur est un dispositif permettant de protéger les équipements d'une éventuelle coupure de courant. Si on prend l'exemple d'un serveur branché sur l'onduleur qui est lui-même branché sur secteur, lorsqu'une coupure intervient, l'onduleur se met sur batterie et continue de fournir une source d'énergie électrique au serveur ce qui est primordiale dans des cas d'orage. Plusieurs fois (hors visite préventive), j'ai été amené à changer des onduleurs défectueux de certains clients. C'est un incident classé « Critique », car il impacte le matériel.

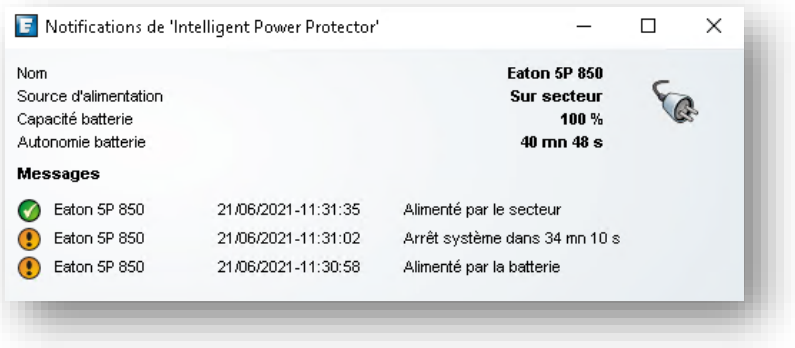


Figure 23 : Notification de l'onduleur signalant des évènements.

4.2.2.2 Les outils internes à Suderiane

Cette partie est surtout orientée supervision par Suderiane. Elle concerne tous les outils que Suderiane utilise pour gérer les clients comme le logiciel Centreon.

Centreon est un logiciel de supervision permettant d'avoir une vue synthétique des états des machines répertoriés. Différentes fonctionnalités sont offertes par ce logiciel dont une qui est souvent utilisée qui a permet d'avoir un rapport de disponibilités des ressources supervisées (hôtes, services et groupes de ressources). Ce qui est à faire est dans un premier temps de vérifier si les serveurs sont répertoriés dans Centreon puis de vérifier si aucune erreur n'est présente. On peut par exemple regarder si les clichés sur les partages sont bien activés depuis Centreon. Il faut savoir que grâce au logiciel, des tickets sont créés automatiquement avec un lien accédant à la page de l'erreur en question.

Parmi les outils qu'utilise Suderiane, on retrouve également OCS Inventory qui est une application permettant de réaliser un inventaire sur la configuration matérielle, les logiciels installés des machines du réseau de l'entreprise depuis une interface Web. Il donc vérifier depuis OCS si tous les serveurs ont bien été répertoriés. Si c'est le cas, il faut malgré tout vérifier si elle a été correctement déployée et que la GPO ne comporte pas ce genre d'erreur :

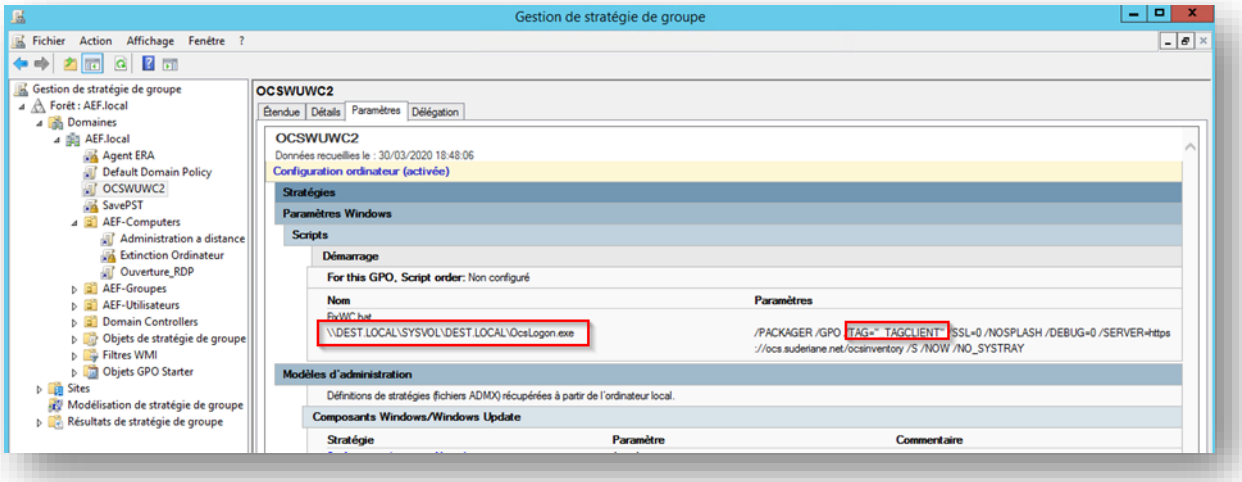


Figure 24 : Erreur à éviter lors du déploiement d'OCS.

Si c'est le cas, il faut remplacer DEST.LOCAL et _TAGCLIENT par les bonnes informations qui vont correspondre aux chemins de l'exécutable du logiciel ainsi qu'au serveur OCS. Comme cité précédemment, OCS est déployé par GPO*, autrement dit par stratégie de groupe. Cela se configure

depuis le contrôleur de domaine qui va ensuite propager la stratégie aux machines qui sont incluses dans le filtre de déploiement. Ce filtre correspondant souvent aux machines se trouvant dans le domaine.

Si ce n'est pas le cas, il faut déployer OCS à la main. Parmi toutes les VP que j'ai eues à faire, je n'ai pas rencontré ce problème mais cela a été le cas pour un autre outil de supervision : l'agent RMM (Remote Monitoring Management). L'agent RMM est un autre outil de supervision cette fois-ci plutôt orienté poste de travail. Il se déploie également par GPO. On y accède via une interface Web où chaque client est répertorié. On peut y voir notamment la dernière fois qu'un ordinateur a été allumé.

Ayant eu à déployer cet agent, je vais donc expliquer la démarche à suivre. La première étape consiste à contacter Bruno Cury qui est le responsable de supervision. Il est en charge de créer les agents qui vont être déployés. Ensuite, on commence par créer le filtre adéquat. Comme dit précédemment, c'est un agent orienté poste de travail. Après quelques recherches, la requête correspondante est la suivante : **SELECT * from Win32_OperatingSystem WHERE ProductType="1"**.

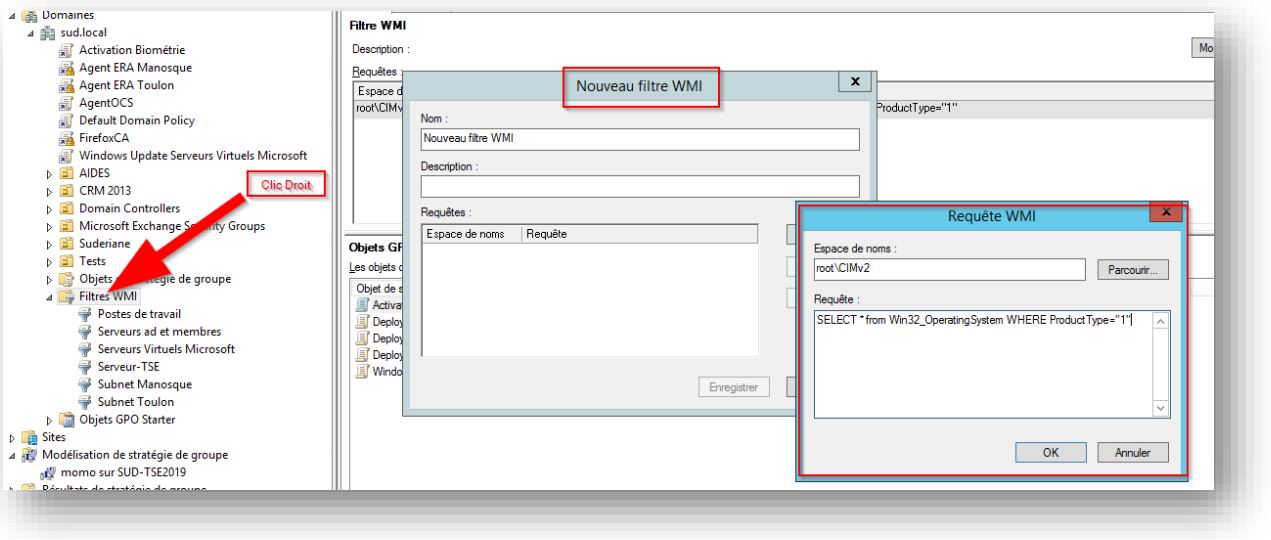


Figure 25 : Création du filtre de sélection des postes de travail.

Une fois fait, il faut maintenant créer le partage qui va contenir l'exécutable d'installation de l'agent. En effet, chaque poste de travail va récupérer automatiquement l'agent via le réseau. La GPO évite de devoir déployer à la main sur chaque poste l'agent ce qui peut s'avérer très long si c'est un gros client. De plus, cela évite de réitérer l'action si de nouveaux postes de travails sont ajouté au domaine. Afin d'ajouter une touche de sécurité, on modifie également les droits du dossier partagé. Il y a deux types d'autorisations :

- Les autorisations de partage gèrent l'accès aux dossiers partagés sur un réseau mais ne s'appliquent pas aux utilisateurs qui se connectent localement mais plutôt à tous les fichiers du partage.
- Les autorisations NTFS* sont utilisées pour gérer l'accès aux données enregistrées. Elles affectent à la fois les utilisateurs locaux et les utilisateurs du réseau et sont basées sur les autorisations accordées à un utilisateur individuel lors d'une connexion, et ce, quel que soit l'endroit depuis lequel il se connecte.

Dans notre cas, au niveau des droits sur le partage, tout le monde y aura accès en lecture. Pour ce qui est des droits NTFS, les utilisateurs authentifiés ainsi que les ordinateurs du domaine, les droits de lecture et d'exécution seront attribués.

Il ne reste plus qu'à créer la GPO qui va permettre d'installer l'agent sur les postes. Il ne faut pas oublier d'appliquer le filtre précédemment créé à cette nouvelle GPO pour bien qu'elle ne s'applique qu'aux postes de travail.

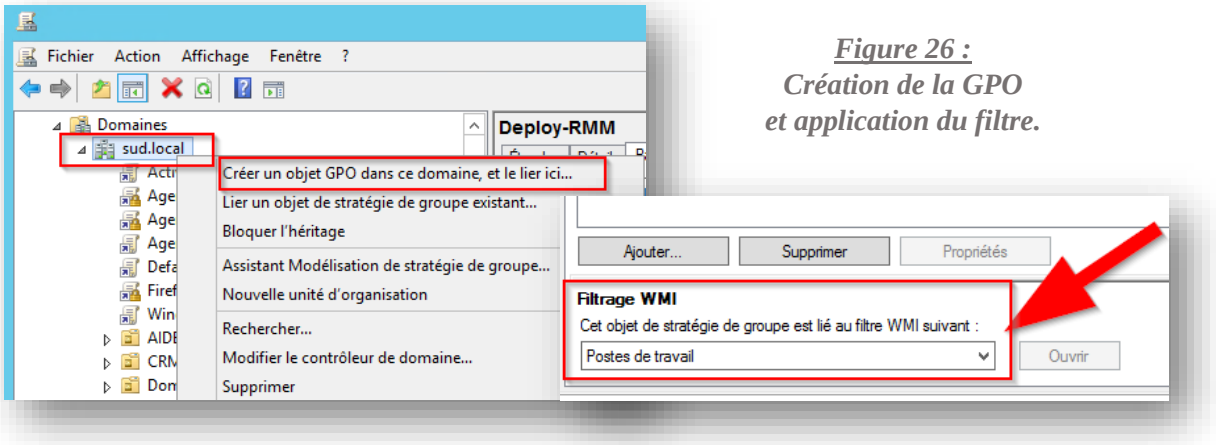


Figure 26 :
Création de la GPO et application du filtre.

Actuellement, la GPO n'effectue rien vu qu'on ne l'a pas encore liée avec l'agent. Il faut donc éditer la GPO de telle sorte à ce que le chemin pointant l'agent soit celui du dossier partagé. Au départ, j'ai malencontreusement renseigné le chemin local de l'agent ce qui a eu pour effet de ne s'être rien passé.

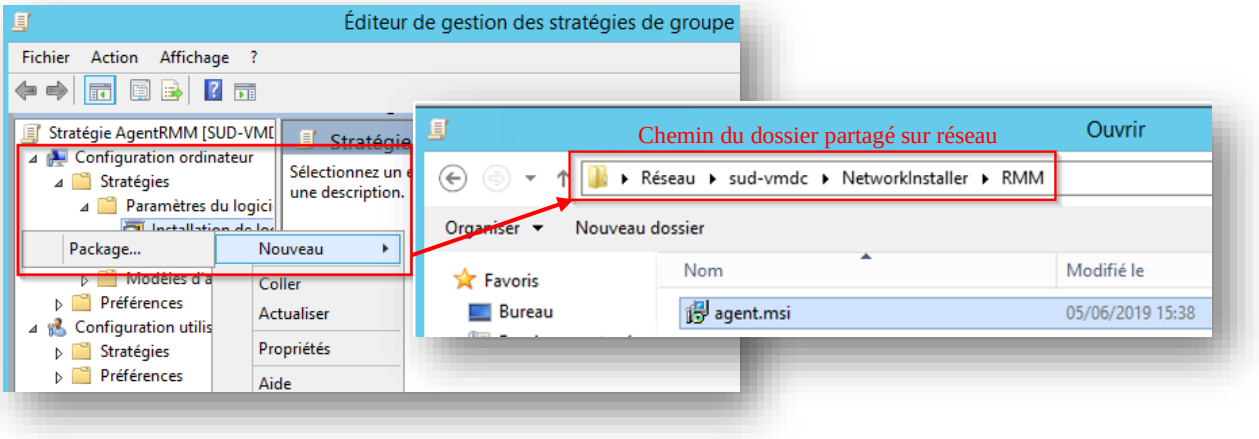


Figure 27 : Spécification du chemin du dossier partagé pour associer l'agent à la GPO.

L'agent RMM est maintenant opérationnel. Cependant, pour pouvoir vérifier depuis la console si c'est effectivement le cas, il faut attendre un démarrage d'un ordinateur, car c'est à ce moment que l'ordinateur va recevoir l'information du partage.

Une dernière chose importante concernant les outils internes de Suderiane concerne les garanties du matériel. Cette information est renseignée dans le logiciel Octopus. On se sert du numéro de série de l'équipement pour le retrouver dans le logiciel. S'il n'est pas présent, il faudra l'ajouter. Dans l'autre cas, il faut savoir si la garantie a expiré ou non. Dans le cas où elle serait expirée, il faut contacter le responsable de projet pour savoir si des démarches ont déjà été effectués pour renouveler cette garantie. Souvent, des devis sont déjà en cours, mais il faudra malgré tout spécifié dans le rapport qui sera fait au client qu'un devis est préconisé.

4.2.2.3 Les firewalls

Tous les firewalls en possession des clients sont des SonicWall. De la même manière que pour les serveurs, vérifier les mises à jour du firewall est requis. Pour ce qui est de la sauvegarde de la configuration, il y a deux procédés :

- Télécharger le fichier de configuration et le déplacer dans le dossier du client qu'utilise Suderiane pour conserver tout un tas d'informations.
- Créer une backup via le cloud qui sera par la suite accessible depuis le site de MySonicWall via les identifiants utilisés pour enregistrer le firewall.

Conserver la configuration est primordial car en cas de mauvaise manipulations ou de changement d'équipement, la configuration sera simplement à importer plutôt qu'à refaire depuis le début.

Un point très important doit impérativement être vérifié concernant les firewalls. La sécurité en accès extérieur. En d'autres termes, il faut que le SonicWall ne soit accessible qu'uniquement depuis les IP de Suderiane. L'accès d'un réseau WAN* vers un autre réseau WAN doit apparaître comme ci-dessous. Si ce n'est pas le cas, il faudra créer un objet contenant les IP de Suderiane et définir les règles d'accès de cette manière.

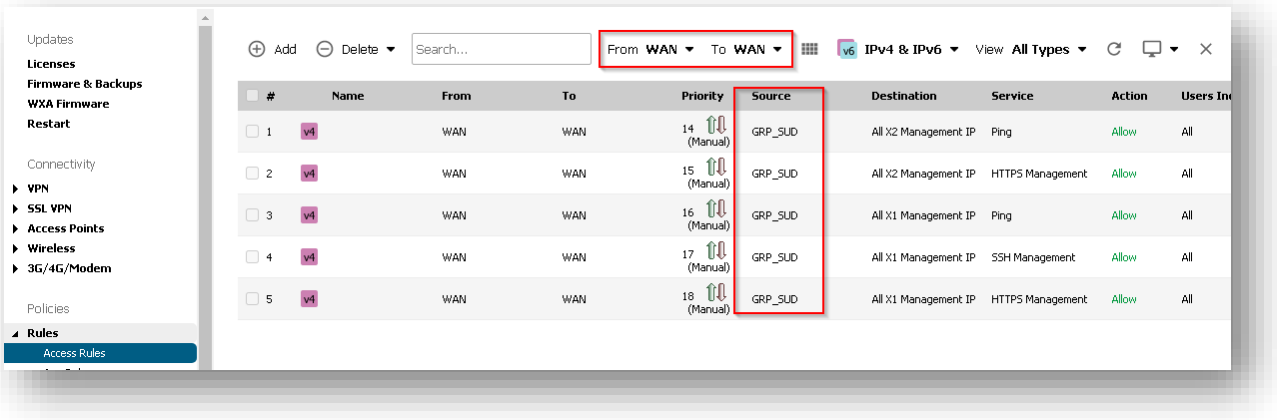


Figure 28 : Sécurité d'accès WAN vers WAN.

De plus, pour l'accès d'un réseau WAN vers un réseau LAN, il ne faut pas que des règles soit présentes avec une source définie sur « Any » sauf en cas de règle HTTPS* vers le serveur exchange.

Enfin, il faut vérifier la bonne activation des services de gestion unifiée des menaces (UTM). Ce sont des services liés aux SonicWall permettant des fonctionnalités supplémentaires qui ne sont pas disponibles dans les pare-feux traditionnels. Parmi ceux qui doivent être activés, on retrouve le Content Filter, le Gateway Antivirus, l'Intrusion Prevention, l'Anti-Spyware, le RBL Filter ou encore le Stealth Mode. Ces services ne sont plus disponibles une fois la garantie du pare-feu expirée. Toute une procédure est à respecter concernant tous ces services. Si une anomalie est détectée, il ne faut pas la modifier directement. Parfois, ils ne sont pas activés pour une raison précise. Pour ce faire, on précise dans un fichier Word toutes les modifications potentielles à faire. Ce fichier sera transmis lors de la création du ticket prévu à cet effet.

N'ayant pas été prévenu, j'ai coché quelque chose qui était présente sur la procédure et cela a eu pour effet de stopper les sauvegardes externalisées d'un client. Cette case avait pour but d'activer l'inspection sur les CIFS* (Common Internet Files System). On ne m'en a pas tenu rigueur, mais cela aurait pu éviter à d'autres de passer du temps à chercher une résolution à cette erreur.

5. Conclusion

Ce stage de dix semaines en entreprise, réalisé au sein de Suderiane, m'aura été bénéfique tant sur la partie technique que sur le plan humain.

Au côté de leur équipe, j'ai pu pleinement découvrir l'activité au sein d'un support technique qui m'a donné l'opportunité de réaliser énormément de missions variées. De ce fait, j'ai eu l'occasion d'approfondir mes connaissances techniques tout en consolidant celles développées tout au long de ma formation de DUT Réseau et Télécommunication. Le métier de technicien support est enrichissant, car chaque jour, des nouvelles problématiques se posent et permettent d'accumuler de multiples acquis, mais également de progresser dans le processus de réflexion d'une difficulté.

Ce stage m'aura aussi permis d'accroître ma capacité à communiquer, aussi bien avec les clients qu'avec les équipes techniques. J'ai notamment pu constater l'importance du travail d'équipe dans un domaine comme celui-ci. Quant au monde l'entreprise, j'ai pu l'aborder pour la première fois dans des conditions agréables et chaleureuses grâce à la bonne humeur et l'entraide quotidienne de chacun.

6. Remerciements

Je tiens tout d'abord à remercier Mme. Majdouline GHARIB, responsable du support technique et tutrice, de m'avoir accepté en tant que stagiaire, mais également de m'avoir assisté dans la réalisation de certaines tâches. Je tiens aussi à la remercier pour tous ces conseils, que ce soit technique ou humain, qu'elle m'a apporté tout au long de cette expérience lors de nos discussions quotidiennes.

Je remercie aussi particulièrement l'équipe C dont font partie M. Luc VANG , M. Bastien Perez, M. Maxime BON ainsi que M. Paul CAILLETTE, de m'avoir fortement assisté notamment au début du stage et qui ont su me mettre en confiance dès les premières semaines. De ce fait, j'ai pu pleinement apprécier le stage dans tous ses aspects. Je n'en oublie pas non plus les autres équipes qui m'ont accompagné pendant le stage et qui m'ont assisté dans toutes mes missions. Poser des questions à chacun d'entre eux m'a permis d'avoir les différents avis et méthodes de travail de chacun ce qui m'a facilité la communication au sein du support technique.

Mais je tiens avant tout à souligner l'ambiance générale, que ce soit au sein du support technique ou des autres services. Tous, sans exception , ont une bonne humeur qui les animent et c'est grâce à eux que cette expérience a été très enrichissante et valorisante pour moi.

7. Glossaire

Parc informatique, désigne l'ensemble des ressources matérielles qui composent une. Il comprend les informations relatives aux serveurs, imprimantes bornes Wifi et autres équipements informatiques.

DUT, Diplôme Universitaire de Technologie

Tickets, sont les enregistrements d'une tâche effectuée (ou qui doit être effectuée) par le support informatique afin de résoudre les problèmes et les demandes des clients.

SLA, Service Level Agreement pouvant être traduit en français par « accord de niveau de service ». Il concerne la partie du contrat qui précise le niveau de service que le prestataire s'engage à délivrer au client.

VPN, Virtual Private Network ou Réseau Privé Virtuel en français est un système permettant de créer un lien entre des ordinateurs distants avec une autre entité. Les échanges entre les deux machines sont isolés du trafic qui se trouve sur des réseaux publics.

Supervision, est un procédé de suivi et de pilotage informatique. Elle peut être une application de surveillance, de contrôle ou de diagnostic visant à surveiller le bon fonctionnement d'un système ou d'une activité.

Switch, commutateur en français, est un équipement qui relie plusieurs équipements dans un réseau. Il peut également créer des liens virtuels.

Firewall, pare-feu en français, est un matériel permettant d'instaurer une politique de sécurité sur le réseau en définissant les types de communications autorisés.

RAM, Random Access Memory est la mémoire vive, présente dans tous les ordinateurs qui permet de stocker provisoirement des données.

HDD, Hard Disk Drive est un support magnétique de stockage de données numériques.

SSD, Solid State Drive est un support de stockage ayant la particularité de puces de mémoire flash. Il remplit la même fonction qu'un disque dur HDD, mais il est dépourvu de toute partie mécanique.

Boot Menu, Menu de Démarrage en français, est un menu qui permet de sélectionner l'application ou le périphérique à partir duquel on souhaite démarrer la machine.

BIOS, Basic Input Output System, désigne un composant essentiel d'un ordinateur qui effectue des opérations de base lors de la mise sous tension.

Baie serveur, est une armoire destinée à recevoir les boîtiers d'appareils électronique, réseau ou informatiques.

Contrôleur de domaine, DC, est un serveur important pour l'AD.

Active Directory, AD, est un type de domaine.

Domaine, est un ensemble de machines partageant des informations d'annuaire.

TSE, Terminal Server Edition est un composant de Windows qui permet à un utilisateur d'accéder à des applications ou à des données stockées sur un ordinateur distant.

LAN, Local Area Network, ou réseau local en français, est un réseau informatique où les machines qui y participent s'envoient des trames au niveau de la couche liaison sans utiliser d'accès Internet.

DHCP, Dynamic Host Configuration Protocol, est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'un ordinateur.

GPO, Group Policy Object ou stratégie de groupe en français, représente des fonctions de gestion centralisée de Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un AD.

NTFS, New Technology File System, est un système de fichier très répandu permettant l'organisation des données sur les disques durs et des supports de données.

WAN, Wide Area Network ou réseau étendu en français, désigne un réseau couvrant une grande zone géographique. Le plus grand réseau WAN étant le réseau Internet.

HTTPS, HyperText Transfer Protocol Secure, est la combinaison du http avec une couche de chiffrement comme SSL ou TLS.

CIFS, Common Internet File System, est un protocole permettant aux programmes d'effectuer des demandes de fichiers et de services sur des postes de travail distants via Internet.