Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Stage technicien, Administration système et réseaux

David TISSERAUD

Gexell

Responsable entreprise : Sylvain HEMMERLIN

Responsable académique : Rabah IGUERNAISSI

2021

Table des matières

1 Introduction

Dans le cadre de mon DUT réseaux et télécommunication, j'ai recherché un stage pour finaliser ces deux années d'études. Lors de ce stage, j'espère pouvoir découvrir le monde professionnel pour compléter les connaissances que j'ai pu acquérir dans un contexte scolaire. Ces deux approches, intéressantes individuellement et complémentaires me permettront de mieux être préparé à ma future activité professionnelle.

A Gexell, j'aurai l'occasion de faire des missions variées, et d'apprendre sur plusieurs sujets différents pour développer de nouvelles compétences. L'objectif de ce stage est de mettre en place des outils, tout en réglant les problèmes internes ou des problèmes clients, en participant à des interventions chez des clients. Ce stage est donc une mise en conditions du métier d'administrateur système et réseaux pour me préparer à la réalité du monde du travail.

2 Entreprise

2.1 Présentation de l'entreprise

Gexell est une entreprise qui propose ses services à des entreprises, pour l'installation de leurs serveurs ou des leurs matériels informatiques. Elle propose aussi un service de maintenance de ses appareils informatiques. Etant revendeur « SAGE », elle propose l'installation de ces logiciels ainsi qu'un support et une formation pour leur utilisation. « SAGE » est un ensemble de logiciel de gestions de comptabilité, de paie qui permet aux utilisateurs de gagner du temps sur leurs tâches quotidiennes. Gexell est aussi revendeur des antivirus « ESET », des systèmes de sauvegarde « BEEMO » ainsi que du service de sécurisation de mail « Mailinblack », et donc propose la mise en place de ces produits à ses clients.

2.2 Organigramme

Durant ce stage j'ai intégré le service « Assistance, Système & Réseaux».

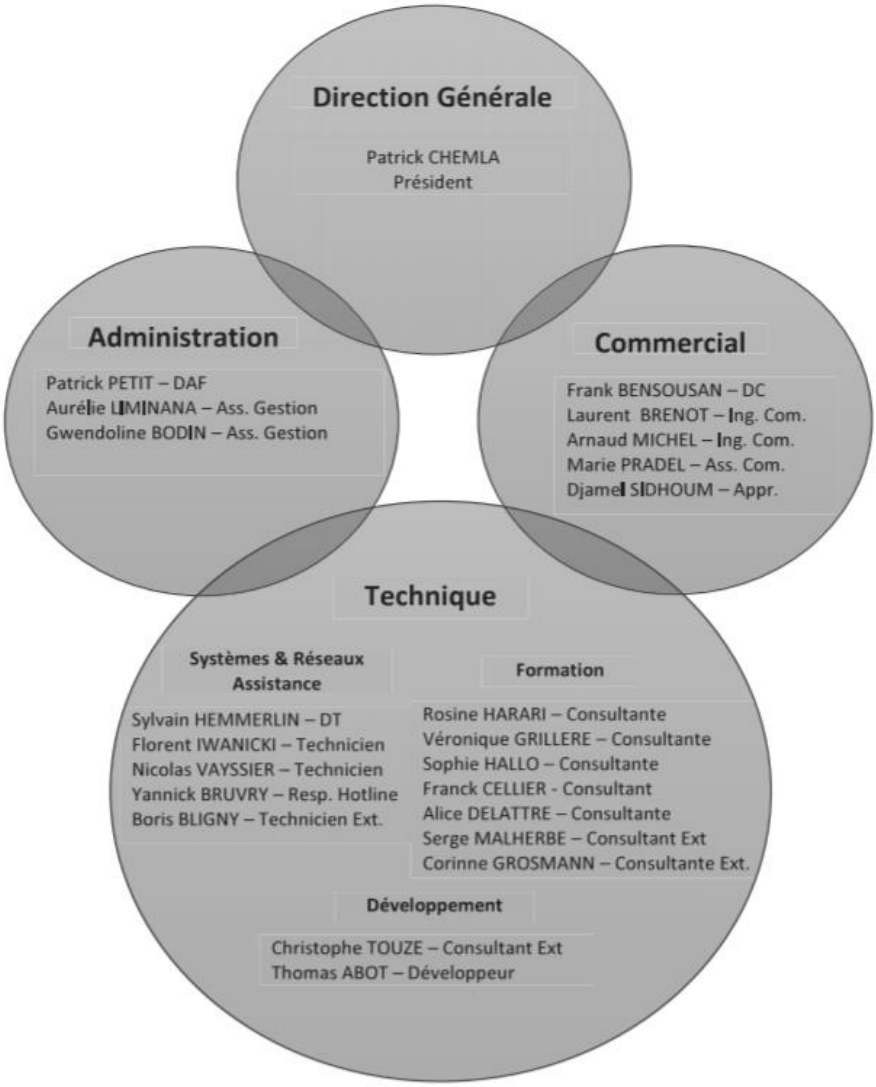

Figure 1. Organigramme Gexell

2.3 Présentation du groupe «Assistance, Système & Réseaux » du pôle technique

Le groupe « Assistance, Système & Réseaux » du pôle technique est chargé de répondre aux demandes des clients concernant leur problèmes informatiques, ainsi que de surveiller quotidiennement le bon fonctionnement des machines des clients ayant un contrat de maintenance. Il s'occupe notamment aussi de l'installation et de la maintenance chez les clients des services dont Gexell est revendeur.

3 Environnement de test

3.1 Contexte

Il est très important d'avoir un environnement de test lors que l'on essai d'installer des outils ou de les modifier, cela permet de pouvoir essayer plusieurs choses sans craindre de nuire au fonctionnement des machines de production.

3.2 Hyper-V

Pour crée cet environnement de test, je vais utiliser Hyper-V, l'hyperviseur de Microsoft. On peut donc créer des machines virtuelles, et les configurer en fonction des besoins, par exemple augmenter la mémoire RAM qui peut d'ailleurs être dynamique, ainsi que le nombres de processeur ou la taille du stockage de données sans l'interruption de la machine virtuelle. Il est aussi possible de créer des switches virtuels pour permettre aux VM d'être dans le même réseau que la machine hôte de l'hyperviseur.

3.3 Création des machines virtuelles

Pour mon environnement de test, je vais créer deux VM dites clients qui seront des Windows 10 Pro, ainsi qu'un serveur Windows 2019 qui hébergera le rôle Active Directory, et y relier les deux VM clientes. Toutes ces VM seront configurées avec une mémoire RAM dynamique, 4 processeurs et relié sur un switch virtuel. Plus tard, un Serveur Windows 2019 servira de serveur de test pour ESET Protect, ainsi qu'un Debian 10 qui servira de serveur de test pour Zabbix

4 ESET Protect

4.1. Présentation d'ESET Protect

ESET Protect est la version 8 de ESET Remote Administrator (ERA), il s'agit d'un service de supervision et de management des Antivirus ESET. Il permet différentes tâches sur les ordinateurs supervisés, telle que le lancement de mises à jour d'un système d'exploitation. Avec cet outil, on peut voir les ordinateurs ou les serveurs qui ont des antivirus non à jour et les mettre à jours à distance. Il est également possible de les installer à distance, ainsi que d'activer les licences et de paramétrer les antivirus. ESET Protect est donc très utile car il permet de faire à distance tout ce que l'on aurait pu faire en étant physiquement devant l'ordinateur et automatiser plusieurs tâches de gestion des antivirus pour gagner du temps.

4.2. Installation d'ESET Protect sur Windows Server 2019

Pour installer ESET Protect sur un Windows Server 2019, il faut commencer par installer une version de Java Development Kit (JDK). Une fois l'installation terminée, on peut alors chercher le .zip d'installation sur le site d'ESET. Bien qu'il soit nommé ESET Remote Administrator, son nom en version 8 est ESET Protect, je l'appellerai donc ainsi dans le cadre de ce rapport. On peut alors procéder à l'extraction du .zip puis lancer le setup d'installation. Une première fenêtre nous propose

de choisir la langue, puis on peut réellement commencer l'installation. On a alors une liste de composants à installer, il faut donc se document sur la nature de chacun d'entre eux. Dans notre cas, après avoir vérifié leur utilité on choisit de laisser le choix par défaut. Ensuite, l'installeur nous demande de choisir la version de JDK que l'on souhaite utiliser. On peut alors sélectionner celui installé plus tôt. Par la suite, l'installation se lance.

Le processus d'installation nous demande quelques informations essentielles :

- Personnaliser le mot de passe
- Une licence ESET
- Des informations pour la création du certificat

4.3 Utilisation d'ESET Protect

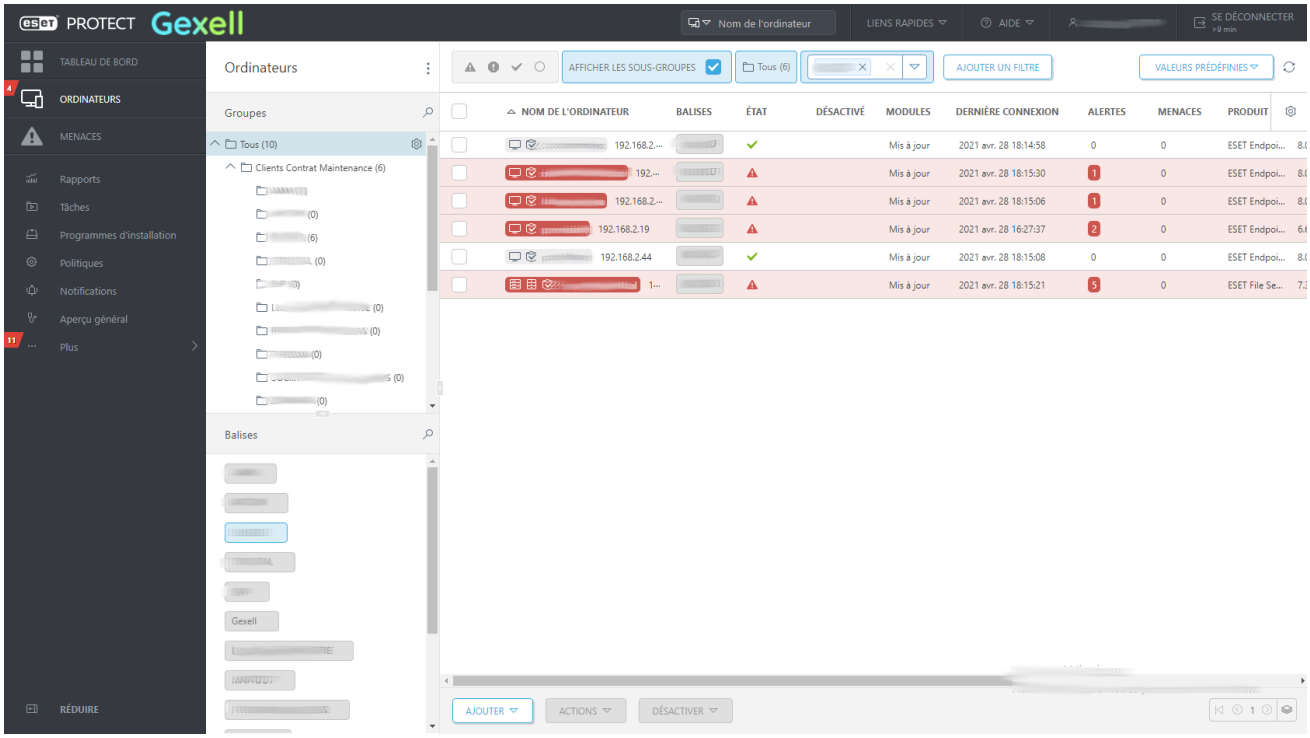

Figure 2. Interface web d'ESET Protect

Une fois l'installation terminée, on a alors accès à l'interface WEB d'ESET Protect. Elle se constitue de plusieurs onglets disposés sur la gauche de la page :

- Le premier onglet, nommé « tableau de bord », permet de visualiser l'état des ordinateurs enregistrés ainsi qu'une multitude d'autres informations à leur propos. On peut aussi créer nos propres fenêtres sur ce tableau de bord.
- Ensuite, l'onglet « ordinateurs » est l'espace où on retrouve tous les ordinateurs détectés par ESET Protect. On peut les organiser dans une arborescence de groupes (statiques ou dynamiques). Les groupes dynamiques listent des ordinateurs qui remplissent les conditions du groupe.

- L’onglet « menace », liste toutes les menaces détectées sur l’ensemble des machines.
- L’onglet « rapports », est un ensemble de modèles de rapports, qui peuvent servir à visualiser différentes informations. C’est l’approche brut de ce que fait l’onglet tableau de bord. Cet onglet permet aussi de programmer des envois de rapports par mail, ou juste de les enregistrer sous forme de fichier PDF. On peut également créer soit même ses modèles de rapports.
- L’onglet « tâches », est le second onglet de le plus important après l’onglet « ordinateurs », il permet de créer des tâches que l’on peut ensuite exécuter à l’aide de déclencheurs sur des ordinateurs ou sur des groupes d’ordinateurs. Les déclencheurs de tâches sont notamment programmables, ce qui permet toute sorte d’actions. Les tâches peuvent aussi cibler des groupes dynamiques permettant des automatisations, comme la création d’un groupe dynamique des ordinateurs ayant des mises à jour Windows à faire et cibler une tâche de mise à jour Windows sur ce groupe et rendre la tâche quotidienne.
- L’onglet « programmes d’installation », donne des méthodes de déploiement d’agent.
- L’onglet « politiques », est important. Il permet de configurer l’antivirus et l’agent des ordinateurs grâce à des politiques, on peut appliquer les politiques sur des ordinateurs ou sur des groupes, l’ordre de priorité étant de l’ordinateur aux groupes « tous » mais cette priorité peut être ignorée grâce à un paramètre de la politique.
- L’onglet « notifications », permet de paramétrer des alertes par mails pour différents problèmes, tel que la détection d’un virus sur un ordinateur par exemple.
- L’onglet « gestions des licences » permet d’enregistrer toutes les licences que l’on utilise et d’avoir quelques informations sur celle-ci, comme par exemple, leurs composants matériels ou les logiciels installés.
- L’onglets « utilisateurs » permet de créer des utilisateurs de la console web, cela peut être utile si un client souhaite avoir accès à la console, on peut alors lui créer un compte et limiter ses accès au groupe qui correspond à son entreprise.
- L’onglets « paramètres du serveur », permet d’ajouter des fonctionnalités au serveur ESET Protect, ou de personnaliser l’interface web, j’y ai activé la possibilité d’envoyer des mails.

4.4 Objectif 1 : Méthode de déploiement des Agents

La première problématique est donc de décider de quelle manière nous allons déployer l’agent. Un premier problème se dessine : ESET Protect n’est pas pensé pour fonctionner facilement avec des systèmes autonomes différents mais plutôt avec la présence d’une active directory locale.

On décide alors de se pencher vers la solution de déploiement par Group Policy Object (GPO) et pour les clients qui n’ont pas d’active directory, je ferai l’installation manuellement. Pour ces deux méthodes, l’onglet « programmes d’installation » d’ESET Protect fournit un .exe qui contient les

informations du serveur ESET Protect, et pour la GPO, il fournit un fichier de configuration (.ini) qui contient les informations du serveur ESET Protect. Toutefois, ce .ini est a utiliser avec le .msi de l'agent qui est à récupérer sur le site de ESET.

Une fois que les installeurs sont prêts, il faut alors concevoir le GPO pour le déploiement par GPO. Pour cela, il faut créer un GPO qui sera utilisé par le groupe des ordinateurs du domaine et qu'on lie au domaine cible. Puis, je paramètre la GPO sur installation de package dans « configuration d'ordinateur>stratégie>paramètre du logiciel » et j'indique le .msi. Si le .msi se trouve dans le même dossier que le .ini, alors, lors de son exécution le .msi prendra en compte la configuration présente dans le .ini qui est celle qui permet de contacter le serveur ESET Protect.

Je me mets alors à tester cette solution GPO dans mon environnement de test. Beaucoup de problèmes vont être soulevés. Le premier étant que la GPO ne fonctionne tout simplement pas. Heureusement, dans l'observateur d'évènement Windows je pouvais y voir l'erreur en question ; elle est due au fait que la GPO se lance sans connexion internet. Cela est réglable dans les paramètres de la GPO où il faut activer une option qui demande à la GPO d'attendre que le réseau soit prêt avant de se lancer. Toutefois, même après cette manipulation, nous avons de nouveau la même erreur. Alors, je cherche quelle pourrait être la cause et je trouve finalement une solution : rajouter du délai d'attente à la GPO. Les GPO ont une option assez récente qui permet de demander à la GPO d'attendre un temps défini pour que tous les paramètre requis soit activés avant de se lancer. J'active donc cette option et cette fois, l'environnement de test fonctionne bien avec cette GPO. Mais, lorsque déployé sur les serveurs active directory des clients, je me rends compte que les machines mettent beaucoup de temps à installer l'agent, voir ne l'installe jamais. Ce phénomène vient d'un défaut des GPO, il faut que l'ordinateur redémarre pour qu'une GPO de configuration d'ordinateur prenne effet, or la plupart des utilisateurs en entreprise ne redémarrent rarement, voire jamais, leurs appareils, nous sommes donc obligés d'attendre qu'ils le fassent ou que Windows Update redémarre l'ordinateur pour faire une mise à jour.

Lors du déploiement, un problème s'est montré. Pour parler de ce problème, il faut comprendre comment l'agent communique avec le serveur ESET Protect. L'agent ESET, échange avec le serveur via le port TCP 2222, évidemment ce port est automatiquement autorisé au niveau du clients lors de l'installation de l'agent pour le serveur qui se trouve derrière un routeur PfSense et qui possède un pare-feu. Ce pare-feu n'a donc pas cette règle, il faut donc créer une règle qui redirige le port 2222 vers le port 2222 en whitelistant certaines IP. A priori, ce n'est pas un problème, il suffit d'autoriser les IP de tous les clients. Toutefois, certains clients ont des IP publiques qui changent tous les jours. En effet, ils utilisent des box d'opérateur et leur abonnement ne stipule pas que leur IP publique est fixe et donc il change régulièrement. Pour contourner ce problème je vais utiliser un service Web nommé FreeMyIp, il s'agit d'un Dynamique DNS, il permet de créer un sous domaine sur leur nom de domaine pour qu'il nous donne une URL contenant un token. Lorsque l'on fait une requête http

sur cette URL cela lie l'IP public qui a fait cette requête au nom de domaine crée plus tôt, mais on ne peut pas demander aux clients de tous les jours de passer cette requête http. Il faut donc un moyen de l'automatiser. Pour résoudre ce problème, j'ai eu l'idée d'utiliser une tâche planifiée sur leur serveur qui utilisera la commande « curl » toutes les minutes. Ainsi, leur IP sera constamment à jours par rapport au nom de domaine, ainsi on peut whitelister le nom de domaine et non l'IP.

4.5 Objectif 2 : Supervision des Ordinateurs trouvés

Une fois les GPO mises en place et les agents installés manuellement là où ils devaient l'être, commence alors un travail quotidien de supervision des ordinateurs trouvés et de paramétrage de la console WEB ESET Protect.

Tout d'abord, pour la supervision, il va s'agir de contrôler que tous les ordinateurs trouvés soit bien à jours au niveau du système d'exploitation, que l'antivirus soit bien à jour ou installé. Sinon, il faut faire les mises à jour et installer l'antivirus. Pour faire tout cela, il s'agit de tâche créable avec l'onglet de tâches ou avec des raccourcis dans l'onglet « ordinateurs ». Cela va aussi consister à lancer des analyses avec nettoyage sur des ordinateurs relevant des menaces d'infections. Et tout simplement les classifier de manière organisée, pour cela j'ai créé une arborescence de groupes et des balises au nom de chaque client, les balises sont une sorte de tag que l'on applique sur des taches, ordinateurs, politiques pour pouvoir faciliter leur recherche en sélectionnant cette balise qui agira comme filtre.

En outre, j'ai configuré l'interface web, j'ai notamment activé l'accès au serveur SMTP de manière à pouvoir être alerté par mail de n'importe quel problème ou à pouvoir recevoir des rapports par mail, j'ai donc crée des modèles de rapport. Un premier modèle permet de résumer des problèmes actifs sur les ordinateurs. Un autre modèle permet de résumer l'historique des détections de pare-feu des sept derniers jours de tous les ordinateurs. Un dernier modèle permet d'afficher un rapport des menace détectées dans les sept derniers jours. J'ai ensuite configuré leur envoi par mail hebdomadaire tous les lundi à neuf heure. Ensuite, j'ai recherché la méthode pour crée d'autre compte d'accès à l'interface dans l'éventualité qu'un client demande un accès privé. Il faut donc pouvoir restreindre leur accès à leurs ordinateurs uniquement. J'ai donc crée un jeu de droit qui leur permet de voir leurs ordinateurs et de créer leurs propres tâches ainsi que leur propre politique. Ainsi, on les isole complètement du reste de la console et on les empêche d'interférer avec les machines des autres clients. J'ai décidé de créer des groupes dynamiques, l'un de ces groupes liste les ordinateurs qui ont besoin d'une mise à jour du système d'exploitation ; une autre liste ceux ayant des modules obsolètes et une dernière liste tous les PC relevant des problèmes. Enfin, j'ai créé des politiques, une d'entre elles permet de whitelister un certificat dans le filtrage SSL. En effet, certains clients avaient des problèmes avec celui-ci lorsqu'ils voulaientt accéder au site de leur banque. Aussi, j'ai créé une politique pour supprimer la Pop-Up de démarrage des antivirus ESET de tous les ordinateurs clients

et pour mettre un mot de passe d'accès à la configuration des antivirus pour éviter les fausses manipulations de la part du client. On sécurise ainsi leur antivirus.

Après avoir pu tester ces manipulations sur mon environnement de test, nous avons déployé, le serveur ESET Protect en production et j'ai continué de gérer ce serveur ainsi que la supervision des antivirus jusqu'à la fin du stage.

5 Zabbix

5.1 Présentation de Zabbix

Zabbix est un logiciel de supervision, il permet donc de surveiller l'état de différents éléments sur les ordinateurs sur lesquels on a installé l'agent. L'outil est simple à prendre en main pour une utilisation basique, mais peut aussi être paramétré avec plus de précisions.

5.2 Installation de Zabbix sur Debian

Dans notre cas, nous installons Zabbix 5.4 sur Debian 10 et avec une base de données MySQL. Tout d'abord, il faut ajouter au dépôt aptitude le paquet Zabbix dans la version que l'on souhaite, on peut obtenir la version à jour ou antérieur sur le site de Zabbix. On peut alors dépaqueter le .deb téléchargée puis mettre à jour le dépôt aptitude avec apt update. On installe alors tous les paquets nécessaires au fonctionnement d'un serveur Zabbix. Il faut ensuite créer la base de données ainsi que l'utilisateur de base de données Zabbix. Cet utilisateur doit avoir tous les droits nécessaires. Il faut enfin configurer la base de données. Après le redémarrage des services Zabbix, ainsi que l'activation au démarrage de ces services, on peut accéder à l'interface web.

5.3 Utilisation de Zabbix

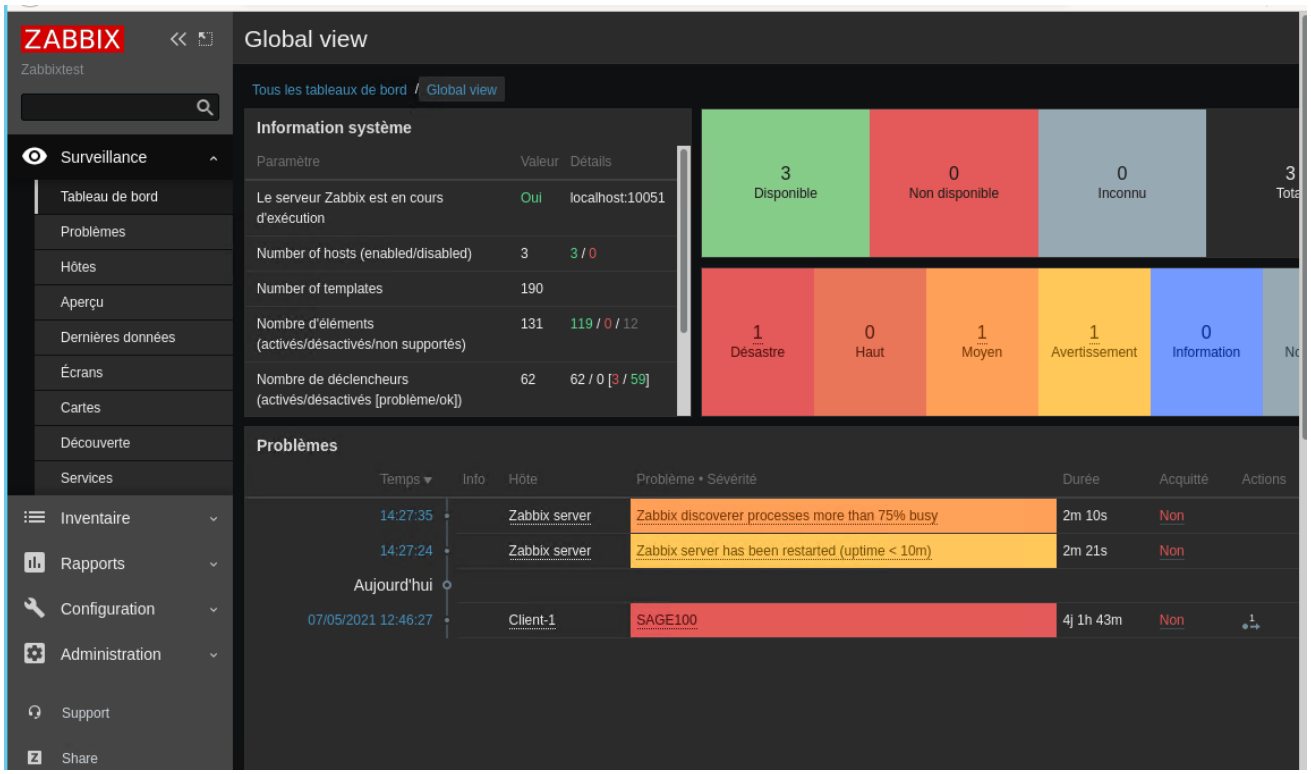

Figure 2. Interface web de Zabbix

Zabbix se présente sous la forme d'une interface web avec différents menus :

Les deux onglets principaux vont être « Surveillance » et « Configuration » :

- Dans l'onglet « Surveillance », on va principalement utiliser le sous-onglet « Tableau de bord » il permet notamment d'observer les problèmes détectés sur les ordinateurs par Zabbix.
- Dans l'onglet « Configuration », il y a plusieurs sous-onglets importants, le premiers « Groupes d'Hôtes » est le sous onglet où l'on peut voir et créer des groupes d'ordinateurs.

A présent, nous allons voir plus en détails les sous-onglets de l'onglet « Configuration » :

- Le sous-onglet, « modèles », est un onglet où on peut créer des « groupes » de règles de supervision. Néanmoins, il faut d'abord savoir comment sont organisées les règles de supervisions sur Zabbix. Il y a également les éléments qui sont des règles de surveillance. Ce sont ces objets qui vont définir ce que l'on surveille. Ces éléments sont reliés à une application. Une application est un groupe d'éléments. On peut par exemple créer une application « Service Windows » et dedans y ranger tous les éléments qui surveillent chaque service Windows. Puis, il y a les modèles qui sont des groupes d'applications, par exemple le

modèle Windows dans lequel on peut mettre l'application « Service Windows ». Et enfin, il y a les déclencheurs, ce sont les règles de déclenchement d'alerte, ces règles sont assez permissives en termes de complexité, permettant de créer des déclencheurs très précis.

- Il y a ensuite le sous-onglet « Hôtes ». C'est ici que l'on peut voir et ajouter les ordinateurs supervisés. Toutefois, pour que le contact avec le serveur se fasse, il faut qu'ils aient l'agent installé et configuré. On peut aussi y créer des règles de supervision pour les attacher uniquement à quelques ordinateurs et non à un modèle.
- Et enfin, le sous onglet « Action » permet de donner des instructions au serveur lorsqu'une alerte est déclenchée. On peut par exemple demander d'envoyer un mail lorsqu'une alerte grave est déclenchée. Pour faire fonctionner correctement ce sous-onglet, il faut avoir configuré des utilisateurs de la console Zabbix. Par défaut, il y a le compte Admin mais on peut en crées d'autres. Chacun de ces comptes peut être limité dans ses accès et avoir des types de média relié, tel qu'une adresse mail, les types de médias sont les informations d'accès au moyen de le joindre cela peut être son adresse mail par exemple. Il faut alors aller dans l'onglets type de média pour configurer le serveur SMTP pour les mails par exemple.

5.4 Objectif 1 : Supervision Service Windows SAGE/SAGE100

Le but de cette première mission sur Zabbix est de pouvoir superviser des services Windows, plus précisément dans notre cas les service Windows SQL de SAGE pour vérifier qu'ils sont bien démarrés.

Il y a une contrainte à respecter car il y a deux services SQL SAGE différents. Cela est du au fait qu'il y a SQL Express et SQL Standards. En fonction du type d'SQL que le client achète, le nom de l'instance SAGE change et donc le nom du service aussi, mais un client ne peut pas avoir les deux, donc il ne faut pas qu'une erreur remonte si l'un des deux services est absent, cela étant normal.

J'ai donc commencé par créer un groupe SAGE, puis un modèle et une application du même nom. Puis, il faut créer deux éléments différents ; un pour SAGE et un autre pour SAGE100. Il faut rentrer la clé d'action que l'agent Zabbix va utiliser pour chacun d'entre eux pour récolter l'informations sur le service Windows. Dans notre cas cette clé est « service.info[NOMSERVICE, state] ». Toutefois, le nom du service qu'il faut indiquer dans la clé n'est pas celui d'affichage que l'on voit dans le menu des Services Windows il s'agit de celui côté système, pour l'obtenir il suffit d'aller dans les propriétés du service en question et il est indiqué. Il faut ensuite dans la création de l'élément indiquer que la valeur afficher est « Windows service state » puis sélectionner l'application crée plus tôt.

Cet élément va renvoyer une valeur de 0 à 255, mais on sait que 0 est la valeur qui indique que le service est en fonctionnement et 255 la valeur qui indique que le service n'a pas été trouvé.

Il est donc plutôt décidé que le déclencheur d'alerte Zabbix s'activera uniquement si la valeur retourner est entre 1 et 254.

Pour le déclencheur SAGE je vais donc indiquer, « si le dernier résultat de l'élément SAGE est supérieur à 0 et inférieur à 255 alors déclencher une alerte ». Cela se présente sous cette forme, « {SAGE :service.info[SAGE,state].last()>0 and {SAGE :service.info[SAGE,state].last()<255 », nous créons alors un déclencheur similaire pour SAGE100 et ainsi nos deux éléments sont prêts pour fonctionner

On a donc plus qu'à ajouter le modèle sur les ordinateurs, puis à tester si tout fonctionne. Pour les tester je peux changer les services à surveiller et mettre des services qui peuvent être arrêter sans conséquence et voir si cela déclenche une erreur.

5.5 Objectif 2 : Supervision disque virtuel RAID Dell sur serveur physique

Pour cette seconde mission, le but est de superviser l'état des volumes RAID. Un volume RAID est un disque de stockage virtuel qui utilise plusieurs disques physiques pour son stockage. Ce type de disque permet notamment d'assurer l'intégrité des données si un certain nombre de disques physiques sont défectueux. Le nombre dépend du type de RAID utilisé ; il donc très important de vérifier l'état des disques physiques et du RAID en lui-même. Dans notre cas, nous nous intéressons au volume RAID produit par la marque DELL, ce détail est important car chaque constructeur donne un logiciel qui ajoute par exemple des commandes DOS qui donnent des informations sur le volume. Pour DELL, ce logiciel est Open Manage Server Administrator (OMSA). Tout comme la première mission, j'ai créé un modèle et l'application. Cette fois, pour l'élément et la clé d'action, il n'y a pas une clé toute faite, il faut donc la construire soi-même.

Dans ce but, je commence par regarder comment obtenir le statut du volume RAID. Pour se faire, OMSA donne cette commande « omreport storage vdisk ». Elle donne plusieurs informations sur le volume RAID mais la ligne qui nous intéresse est la ligne « Status ». Je dois vérifier que cette ligne a pour valeur « OK ». Donc, dans un premier temps je vais filtrer le résultat de cette commande pour pouvoir n'avoir que cette ligne. Néanmoins, je ne peux pas filtrer simplement avec le pattern « Status » comme une autre ligne possède ce mot.

J'essaie alors de filtrer avec la commande « find » qui est l'équivalent Windows de « grep » pour linux. Cette manipulation permet d'afficher que les lignes contenant le pattern indiquer ou d'exclure la ligne avec le pattern indiquer si on rajouter l'option /v, ce qui donne le résultat suivant : « omreport storage vdisk | find /v 'Protection' | find 'Status', cette commande donne pour résultat : « Status : OK ».

Je n'ai donc plus qu'à faire en sorte que l'agent Zabbix exécute cette commande et récupère cette ligne. Justement, une clé d'action sur Zabbix est l'exécution de commande, mais il faut que l'agent

soit configuré avec l'autorisation d'utilisation de commande à distance. Par chance, c'est déjà le cas sur les agents installés. Toutefois, lorsque j'écris la clé d'action, il y a un problème, il faut entourer la commande que doit exécuter l'agent de guillemet, or les guillemets sont déjà utilisés par la commande « find » et on ne peut pas utiliser les guillemets simples. Il faut donc trouver un autre moyen que « find » pour filtrer et qui n'utilise pas les guillemets. Je trouve alors la commande « findstr », il s'agit d'une commande qui a les mêmes propriétés que « find » hormis qu'il n'est pas nécessaire de mettre des guillemets. En la remplaçant, j'ai pu faire ma clé d'action qui ressemble à ceci « system.run[« omreport storage vdisk | findstr /v Protection | findstr Status »,] ». Je finis alors de paramétrer l'élément en indiquant que l'information sera de type texte et en sélectionnant l'application créé pour cet élément. Ainsi, il ne me reste plus qu'à configurer le déclencheur d'alerte, il doit donc se déclencher si le retour de la commande diffère de « Status : OK », donc j'indique que si le résultat de la commande ne contient pas « OK » alors on déclenche l'alerte.
On peut alors ajouter le modèle aux serveurs à superviser. Pour tester, je peux simplement inverser la règle de déclenchement. De plus, Zabbix permet de voir le retour de la commande utilisé par l'agent je peux donc voir s'il s'agit bien de la ligne attendue.

6 Installation Serveur/poste de travail

6.1 Contextes générales des installations

Une installation de poste de travail ou de serveur peut avoir plusieurs contextes. Dans un premier cas il peut s'agir d'un client qui accueille un nouvel employé et qui a donc besoin d'un poste de travail. Je pars alors d'une installation de zéro sur un nouvel ordinateur. C'est aussi le cas lorsque c'est l'employeur qui change d'ordinateur. Il faut récupérer ses données pour les mettre sur le nouvel ordinateur après l'installation. Pour ce qui est des serveurs, il y a trois catégories : la première est la simple installation d'un nouveau serveur, il faut alors installer tous les services qui vont être nécessaires aux clients. Dans le deuxième cas, pour un remplacement de serveur, comme pour un poste de travail il faut alors penser à récupérer les données et à adapter la configuration du serveur pour coller avec celle de l'ancien. Enfin, l'installation d'un serveur cloud (dans notre cas il s'agit de VM logé sur un serveur physique) où il faut créer la VM puis procéder à l'installation du serveur.

6.2 Installation poste de travail

A plusieurs reprises, j'ai pu m'occuper de l'installation de nouveaux postes de travail pour des employés de l'entreprise.
Il faut noter que le procédé diffère en fonction de la demande du futur utilisateur. Il peut y avoir des modifications à apporter à la machine avant son installation. Par exemple j'ai dû, pour une machine,

rajouter 8 Go de mémoire vive et y placer le SSD de l'ancien ordinateur. Il a donc fallu que j'ouvre le boîtier de l'ordinateur qui était une petite unité centrale de Lenovo.
Une fois les premières modifications apportées, je peux démarrer l'ordinateur, il faut alors commencer par installer Windows 10 Pro. Lors de l'installation, il faut indiquer l'ordinateur sera utilisé dans un cadre professionnel. Pour le nom de la session, j'indique le prénom ou le nom du futur utilisateur et je réponds à toutes les questions de confidentialité en permettant le moins de choses, pour des raisons de confidentialité.
Une fois l'installation terminée et la session ouverte, je commence par changer le nom de l'ordinateur pour mettre PC-le_prénom_utilisateur, ensuite je peux commencer l'installation des logiciels, pour les logiciels de base tel que Google Chrome et 7zip nous utilisons le site ninite qui permet de créer un .exe qui installe plusieurs logiciels d'un coup. Puis, je mets Google Chrome en navigateur par défaut. Après, il faut installer les logiciels Sage. En amont, j'installe SQL 2019 et l'outil de management SQL. Une fois ces deux éléments installés, je peux commencer à installer les logiciels Sage, j'installe l'antivirus ESET ainsi que l'agent, puis j'installe de logiciel demandé par l'utilisateur tel que One Drive ou autres utilitaires. Enfin, on fait les mises à jour Windows.

6.3 Installation serveur physique/cloud(VM)

Lors du stage, j'ai pu installer des serveurs physiques pour remplacer d'anciens serveurs et des serveurs cloud. Les procédés d'installation diffèrent dans les deux cas.

Dans le cas du serveur physique, il peut y avoir du matériel à rajouter tel que des disques durs ou de la mémoire RAM. Au démarrage, il faut créer le volume de stockage virtuel RAID. Après cela, j'installe Windows Server.
Après avoir mis à jour les pilotes et firmware du matériel, je commence par installer les logiciels Sage (uniquement ceux nécessaire et ceux dont le client possède une licence). Dans le cas où SQL est une version d'SQL express, il faut aussi installer SQL Backup Master. Il s'agit d'un logiciel qui permet de sauvegarder des bases de données. Je vais aussi installer Cobian Backup qui est un logiciel de sauvegarde de fichiers.

On procède alors à quelques réglages. Tout d'abord, je crée un groupe d'utilisateur « sage » et j'autorise ce groupe dans SQL avec le profil « sysadmin ». Ensuite, je configure le port d'écoute de SQL sur le port TCP 1433 et j'autorise dans le pare feu de Windows le port 1433 en entrée.

Enfin, lors du remplacement, je fais la migration des fichiers de l'ancien vers le nouveau serveur. Je restaure et je mets à jour les bases de données si nécessaire et je configure l'outil de sauvegarde du serveur et l'outil des bases de données. Il faut alors passer sur les postes de travails pour changer des potentiels lecteurs réseau pour les rediriger vers le nouveau serveur.

Dans le cas d'un serveur cloud, il y a bien plus d'étapes car il ne s'agit pas d'un remplacement de serveur. En effet, Gexell propose à ses clients d'héberger les applications Sage sur un serveur qu'il

gère lui-même. Ces serveurs sont hébergés dans un datacenter. Finalement, on parle de ces serveurs comme étant hébergés « dans le cloud ». La migration d'un client sur l'offre cloud de Gexell diffère d'une migration « on premise ». Tout d'abord, je dois m'intéresser au contexte de ces serveurs cloud. Il s'agit de VM sur un serveur physique hébergé, le réseau des VM est géré par un pfsense. Chaque VM est située dans un VLAN différent de manière à les isoler les unes des autres. Il faut donc commencer par configurer le pfsense pour accueillir cette nouvelle VM. Je commence par créer un nouveau VLAN portant le numéro « 1x », x étant le numéro de la VM, VLAN 10 étant le VLAN de la première VM. Ce VLAN doit être crée sur l'interface LAN_INTERNE_VM qui correspond à l'interface physique hn2. J'appelle alors ce VLAN, VLAN_NOMCLIENT. Je configure ensuite l'interface VLAN avec le nom VLAN_NOMCLIENT et avec l'adresse IP 172.16.x.1/24, x étant le numéro du VLAN.

Ces serveurs étant destinés à une utilisation à distance, il y a donc de fortes chances qu'il soit utilisés par des utilisateurs dit « nomade », il faut donc prévoir un serveur VPN. Le but est de permettre aux clients de se connecter au réseau depuis leur entreprise mais aussi depuis chez eux en cas de télétravail. Dans ce cas l'accès se fait à l'aide du VPN, étant donné que seul l'IP de l'entreprise sera autorisé à se connecter au serveur cloud grâce au bureau à distance. Pour cela, je vais me servir d'OpenVPN qui est déjà implémenté dans Pfsense, je commence par regarder les port UDP disponible, et je prend le suivant du dernier utilisé, si le dernier est 1196 alors j'utiliserai le 1197. Une fois cela noté je peux commencer à installer le serveur OpenVPN, la description du serveur VPN doit être le nom du client et la valeur Tunnel network est 172.16.1x.0/24, x étant le numéro du VLAN, indiquer la même IP pour la valeur localnetwork.

Enfin, je dois configurer le pare-feu du pfsense. D'abord, je crée des alias pour les IP et Ports autorisé, un alias d'IP pour l'accès en RDP, un alias de Ports pour l'accès à Internet et au serveur ESET Protect. Une fois terminé, je peux créer les règles dans le pare-feu. Il faut créer une règle pour l'accès internet en utilisant l'alias de port crée précédemment, puis une règle pour accéder à la sauvegarde FTP. La logique étant de tout bloquer, sauf les flux identifiés. Par exemple, pour certains produits Sage, il est nécessaire de laisser passer les connexions vers le serveur de mises à jour de l'éditeur. Puis, je crée une règle NAT pour les connexions RDP en utilisant l'alias d'IP crée précédemment comme étant une source fiable.

Une fois la partie réseau correctement configurée. peut alors commencer la création de la VM à l'aide d'Hyper-V. Je vais donc créer un nouvel ordinateur virtuel. La particularité va être de penser à bien lier la machine au VLAN qui convient. Le déploiement d'un nouveau client passe par l'utilisation d'un serveur « master » qui contient l'installation par défaut des serveur cloud faisant ainsi gagner énormément de temps. Lorsque la session s'ouvre, un script powershell se lance et il faut alors le suivre pour faire la configuration de base de serveur. D'abord, j'indique le nom du serveur SRV-NOMCLIENT, puis il configure la carte réseau en lui indiquant le numéro du VLAN. Ensuite,

il installe le rôle AD DS et crée un domaine active directory avec « gexell.com » comme nom de domaine. Windows ne permettant pas l'installation automatisé du rôle services bureau à distance en local, il faut le faire manuellement. Cela se fait dans le gestionnaire de serveur, dans ajout de fonctionnalités et de rôles. Je peux alors y installer le services bureau à distance en démarrage rapide et session. J'indique ensuite au script que l'on a installé le service et il continue alors son travail en créant un nouveau compte administrateur, et un groupe « Gexell_Admins ». Il y met le compte crée précédemment puis il active la corbeille active directory. Enfin, il crée trois délégation DNS, ces délégations sont importantes car le nom de domaine étant Gexell.com, le DNS essaiera de résoudre tous les sous domaines avec gexell.com même ceux qui sont dans d'autre réseaux, ces délégations permettent donc de faire la résolution des sous-domaines en utilisant un autre résolveur DNS externe, ici le routeur Pfsense. Après cela, le script prend fin, je peux le supprimer et supprimer la tâche planifiée qui le lance.

Après cela, il reste encore plusieurs choses à faire. Dans un premier temps, il faut changer de compte pour se connecter sur le nouveau compte administrateur et ainsi désactiver l'ancien. Ceci est une mesure de sécurité car le nom « Administrateur » étant celui par défaut la plupart des attaques visent ce nom de compte. Ensuite il faut initialiser un second disque nommé DATA sur lequel je donne le contrôle total au groupe Gexell_Admins, puis il faut créer un dossier Sage et un dossier BackupSQL. Sur le dossier Sage, il faut donner l'accès à un groupe d'utilisateur Sage qui contient tous les utilisateurs du client. Par sécurité, nous interdisons les utilisateurs d'accéder au dossier contenant les sauvegardes. Toutefois, il faut désactiver l'héritage des droits en faisant attention étant donné que lorsqu'on le désactive il faut changer le type de droit du nouvel administrateur sur le dossier pour indiquer qu'il a le droit sur le dossier les sous dossiers et tous les fichiers. Puis, il faut activer les clichés instantanés sur les deux disques durs. Cette option permet à Windows de garder en mémoire l'état précédent des disques ce qui permet en cas de problème de revenir sur une version précédente. Après cela, il faut créer un groupe d'utilisateurs au nom du client pour y mettre tous les utilisateurs du client.

Il faut ensuite configurer le rôle RDS. Il faut permettre au groupe crée précédemment de se connecter en bureau à distance et définir la fermeture de session automatique pour les sessions déconnectées. Aussi, il faut démarrer le gestionnaire de licences RDS pour y faire l'activation du serveur de licences et y ajouter les licences d'accès.

Une fois terminé, il faut activer la licence de l'antivirus et installer l'agent d'ESET Protect. Je peux alors commencer à installer les applications Sage nécessaires et celle dont le client à une licence. Si le client à une instance SQL Express, il faut installer SQL Backup Master pour configurer une sauvegarde. En mesure de sécurité supplémentaire, j'installe RDP Defender, qui détecte les échecs de connexion au service RDS et bloque l'IP source. J'ajoute dans une liste blanche l'IP publique du client et l'IP du bureau de Gexell. Ensuite, il faut configurer la sauvegarde FTP Duplicati. Duplicati

permet de sauvegarder des dossiers sur un équipement de stockage distant (ici, un NAS) et d'envoyer des mails d'alertes. Il faut donc commencer par configurer l'objet des mails par le nom du client, puis créer une sauvegarde. Je nomme la sauvegarde « Sauvegarde BDD » puis je définis un mot de passe. Il faut alors indiquer qu'il s'agit d'une sauvegarde par FTP en SSL et indiquer la destination qui est le NAS. Aussi, il faut indiquer le chemin de destination « /home/NOMCLIENT ». Lorsque l'on valide le répertoire, il va être crée s'il n'existe pas. Cette sauvegarde contient le dossier Sage, BackupSQL et les bureaux et documents des utilisateurs. Je mets comme heure d'exécution 22h et j'active l'option « rétention de sauvegarde intelligente ». Cette option permet d'avoir une rétention cohérente des sauvegardes.

Il faut alors paramétrer l'agent Zabbix, il est déjà installé grâce à master mais, il faut y éditer le fichier de configuration et il faut changer dans ce fichier les valeurs SERVER. Je dois également renseigner le nom du serveur Zabbix, la valeur HOSTNAME et y renseigner le nom du client. Puis, sur le serveur Zabbix, il faut mettre le serveur détecté dans le bon groupe de supervision et lui assigner des modèles.

Pour finir, si le client a des utilisateurs nomades, il faut installer sur les poste de travail le client VPN : « OpenVPN connect » pour les Windows et « Tunnelblick » pour les mac. Je dois y ajouter les fichiers de configuration spécifiques à chaque utilisateur, que je récupère sur le serveur VPN.

6.4 Mise à jour du master

Après cela, je suis désormais bien au courant du procédé d'installation d'un serveur cloud. J'ai eu pour mission de chercher des moyens d'optimiser le master, qui est le modèle qu'on utilise pour installer les serveur cloud et ainsi gagner plus de temps.

Par sécurité, j'ai d'abord travaillé sur une copie du master, car l'intégrité d'un master est très importante. Je crée alors une VM, comme s'il s'agissait d'un serveur cloud, à partir du disque copié du master. J'utilise également la fonction d'Hyper-V « cliché instantané » qui permet de remettre la VM dans un état antérieur.

Une fois connecté sur la VM du master, je peux alors visualiser les éléments à changer. En premier lieu, j'ai commencé par mettre à jour l'antivirus ESET file security. Puis, j'ai remarqué que Notepad++ demandait des mises à jour. Sur demande de mon tuteur j'ai désactivé les notifications de mise à jour de l'application car elles sont trop fréquentes et ne sont pas nécessaire.

Puis alors, j'ai pu me pencher sur le script d'installation. Ce script s'occupe de changer le nom du serveur, de paramétrer la carte réseau, d'installation l'active directory et autres tâches communes à tous les serveurs. Néanmoins, il y a différentes choses qu'on l'on peut rajouter ou optimiser, par exemple le script lancer un redémarrage entre le renommage du serveur et le paramétrage de la carte réseau et redémarrage encore après, ce redémarrage au milieu était donc inutile. Puis, lors de l'installation je devais mettre manuellement Google Chrome en navigateur par

défaut. J'ai donc cherché à ce que le script crée une GPO qui met Google Chrome en navigateur par défaut à tous les utilisateurs, mais cela s'est avéré extrêmement compliqué. Normalement, le navigateur par défaut est changeable grâce aux clés de registre, chose qu'il est très simple de modifier, grâce à une GPO mais, depuis Windows 10 il y a deux clés de registre et l'une d'elle est chiffrée. Il s'agit d'une sécurité et malheureusement celle-ci ne pourra pas être changée si facilement. J'ai alors cherché une méthode pour contourner cette clé et j'ai finalement trouvé un outils nommé « SetDefaultBrowser.exe » qui via une commande dans le cmd permet de modifier le navigateur par défaut. Ainsi, il ne reste plus qu'à créer un GPO qui crée une tâche planifiée qui exécute cette commande à la première connexion de la session. Mais cela est très dur à faire en Powershell. J'ai donc décidé de d'abord la créer manuellement puis de l'exporter. Ainsi, je n'aurai plus qu'à mettre une commande d'import en Powershell dans le script. J'ajoute aussi une autosuppression de la tache planifiée liée au lancement du script, pour ne plus avoir à le faire manuellement et aussi une suppression automatique du dossier d'installation, où se situe le script. Toutefois, comme le script peut avoir échoué je mets cette suppression après la dernière confirmation du script.

Enfin, j'ajoute l'installeur manuel de l'agent ESET pour ne plus avoir à le chercher sur Google Chrome, ainsi que l'outil Wiztree, qui permet de voir quels sont les dossiers qui occupent le plus d'espace disques. Je mets Wiztree et SetDefaultBrowser dans un répertoire dans le C : pour qu'il soit accessible de toutes les sessions.

Après plusieurs vérifications, la mise à jour du master que j'ai faite a été acceptée et utilisée en production.

7 Missions mineures

7.1 Bitwarden

7.1.1 Présentation de Bitwarden

Bitwarden est un gestionnaire de mot de passe, c'est-à-dire qu'il s'agit d'un coffre-fort virtuel dans lequel on peut stocker différent mot de passe et les lier à des sites. Bien que cela puisse sembler être une augmentation du risque de fuite de mot de passe il est en fait recommandé d'utiliser de ce type d'outil, car dans un premier temps n'ayant plus besoin de retenir les mots de passe, on peut alors leur donner une longueur improbable, Bitwarden dispose justement d'un outil pouvant générer des mots de passe de 129 caractères remplissant les conditions de sécurités, ce mot de passe est donc plus sécurisé que n'importe lequel que l'on aurait pu imaginer. L'utilisateur a sa part de responsabilité est sur le choix du mot de passe maître, qui permet d'ouvrir le coffre-fort, il faut un mot de passe mémorisable mais assez fort. On peut alors utiliser les mots de passe retenu dans le coffre-fort en les copiant puis en les collant là où on en a besoin.

7.1.2 Ecriture d'une documentation sur l'installation et l'utilisation de bitwarden

J'ai eu pour missions de rédiger une documentation d'installation et de paramétrage de Bitwarden pour être lue par les salariés de Gexell. Cela doit leur permettre de s'approprier plus simplement cet outil. J'ai donc commencé à utiliser Bitwarden de manière personnelle pour pouvoir découvrir son fonctionnement et ainsi juger personnellement de l'intérêt des différents paramètres que propose cet outil. Ainsi, après plusieurs semaines d'utilisation j'ai rédigé cette documentation en ayant pour but d'être clair. Dans ce but, j'ai décidé de diviser en deux parties la documentation : la première partie serait uniquement destiné à l'installation sur les différents appareils, ainsi qu'à la connexion au serveur Bitwarden interne de Gexell. Puis, la seconde partie est destinée au paramétrage de Bitwarden pour ceux qui voudrait augmenter la sécurité de l'application ou juste personnaliser l'interfaces.

7.2 PfSense Netgate

7.2.1 Présensation pfsense

PfSense est un routeur et pare-feu open source qui fonctionne sur l'OS FreeBSD. Il est simple à prendre en main notamment grâce à son interface web, il est aussi configurable en ligne de commande. PfSense est développer par Netgate et est tout aussi bien installable sur VM que physiquement avec les routeurs PfSense Netgate.

7.2.2 Configuration et mise en place dans le réseau d'un pfsense

Pour la configuration du pfsense, j'ai pu tout au long du stage me familiarisé avec l'interface web de pfsense, ainsi j'ai pu configurer le pfsense en gardant les mêmes propriétés que l'ancien. Pour le configurer, il a fallu le brancher en réseau directement à mon ordinateur et sortir mon ordinateur du réseau de Gexell pour éviter que le DHCP de l'ancien et du nouveau ne rendre en conflit. Une fois configuré, On a procédé à l'échange des routeur, l'ancien étant une VM sur un ordinateur, elle a été arrêtée et nous avons alors brancher le nouveau sur la box. Aucune anomalie ne semblait survenir dans les jours qui ont suivies, on peut donc ne conclure que c'est un succès.

8 Conclusion

Lors de ce stage, chaque mission m'a permis de voir des aspects très importants du métier d'administrateur système et réseaux. ESET Protect et Zabbix m'ont permis de voir l'installation et le déploiement de serveurs de supervision et de leurs agents. Aussi, j'ai pu me familiariser avec le fonctionnement de ces outils. Par exemple, ESET Protect m'a permis d'en apprendre plus sur le fonctionnement des antivirus. D'autre part, l'installation des serveurs m'a permis d'utiliser les fonctions du gestionnaire de serveur Windows ainsi que plusieurs autres paramétrages nécessaires à un serveur. J'ai également dû écrire des documentations techniques, comme il est important de savoir comment chaque outil en production a été mis en place. Avec Bitwarden, j'ai dû écrire une documentation d'utilisation qui demande des méthodes d'écriture différentes que pour une documentation technique habituelle. Enfin, j'ai pu tout au long du stage appliquer mes connaissance réseaux au travers des Pfsense et de leurs configurations.

Pour conclure, stage m'a donc permis d'assembler les connaissances que j'ai pu obtenir personnellement ou grâce aux études et d'en faire de réelles compétences. Ainsi, j'ai pu prendre confiance en mes compétences et être plus sûr de moi. Aussi, j'ai pu confirmer que le domaine de l'administration système et réseaux était ce qui me plaisait et que je souhaitais m'orienter dans cette voie pour mon projet professionnel. Pour la suite, je compte poursuivre mes études et continuer dans l'administration système et réseaux durant l'alternance qui se déroulera l'année prochaine en Licence professionnelle Métiers de l'informatique : administration et sécurité des systèmes et des réseaux (LP ASUR).

9 Remerciements

Je tiens à remercier mon tuteur de stage, Mr Hemmerlin, directeur technique, pour son accueil, le temps passé ensemble et le partage de son expertise au quotidien. Avec son accompagnement, j'ai pu accomplir avec succès mes missions et découvrir le quotidien d'un administrateur système et réseaux.

Je remercie également toute l'équipe de Gexell pour leur accueil au sein de l'entreprise. J'ai pu facilement m'intégrer et travailler avec eux.

Enfin, je remercie toutes les personnes qui prêteront attention à ce rapport de stage et qui prendront le temps de le lire.

10 Sitographie

Documentation de Microsoft : https://docs.microsoft.com/

Documentation de Zabbix : https://www.zabbix.com/documentation/4.0/

Documentation d'Installation de Zabbix :

https://www.zabbix.com/download?zabbix=5.2&os_distribution=debian&os_version=10_buster&db=mysql&ws=apache

Documentation de ESET Protect : https://help.eset.com/protect_admin/80/fr-FR/fs.html

11 Glossaire

DUT, Diplôme Universitaire de Technologie

VM, Machine Virtuelle

JDK, Java Development Kit

FTP, File Transfer Protocol

GPO, Group Policy Object

OS, Operational System, Système d'exploitation

DNS, Domain Name System

NAT, Network Address translation

SMTP, Simple Mail Transfer Protocol

SQL, Structured Query Language

ERA, ESET Remote Administrator

RAID, Redundant Array of Independent Disks

RAM, Random Access Memory, Mémoire vive

NAS, Network Attached Storage