

Mélanie Bulkan
BTS SIO, SN1-1

EPSI MONTPELLIER
437 Av. des Apothicaires,
34090 Montpellier



l'école d'ingénierie
informatique

RAPPORT DE STAGE

Mise en place d'une solution de supervision
du réseau (Zabbix)



OC SANTE
194 Av. Nina Simone
34960 Montpellier

Stage effectué de mi-mai à juillet 2023



REMERCIEMENTS

Tout d'abord, j'adresse mes remerciements à mon tuteur, M. MATTEONI Sylvain, pour m'avoir accepté au sein de l'entreprise OC-SANTE mais aussi pour sa bienveillance et ses conseils précieux. Sa vaste expérience et sa passion pour l'infrastructure réseau ont été une source d'inspiration pour moi. Grâce à ses remarques, j'ai pu mener à bien mes tâches et acquérir de nouvelles compétences.

Un grand merci à toute l'équipe du pôle informatique pour leur accueil chaleureux rendant le travail dans l'open space plus agréable, dynamique et motivant.

Je tiens aussi à remercier mes collègues de travail, les administrateurs réseau M. RAYNAUD Martin et M. MICHEL Stéphane, pour leur partage de connaissances et la confiance qu'ils ont portés à mon égard. Leur collaboration a contribué à rendre mon expérience de stage plus enrichissante.

Mes remerciements vont également à tous ceux qui ont accepté de partager leur temps et leurs connaissances avec moi lors des entretiens et des réunions.

Enfin, je tiens à exprimer ma profonde gratitude envers toutes les personnes qui m'ont soutenue et aidée tout au long de mon stage. Leur soutien et leur contribution ont été inestimables pour mon développement professionnel et personnel.

TABLE DES MATIERES

INTRODUCTION	1
I- PRESENTATION DES MISSIONS	5
A - Contexte professionnel de la mission	5
B - Problèmes à résoudre, contraintes, limites	8
II- DEMARCHE SUIVIE	12
A - Processus suivi – méthode	12
B - Organisation des missions.....	14
III- REALISATION DE LA MISSION	16
A- Sécurisation de la solution	16
B- Collecte des données	18
C- Dashboard et widgets	20
D- Administration	24
IV- EVALUATION DES REALISATIONS ET COMPETENCES MOBILISEES.....	26
A - Adéquation du travail	26
B – Compétences mises en œuvre	28
CONCLUSION	31
GLOSSAIRE.....	33
ANNEXES	37

INTRODUCTION

Le présent rapport décrit en différentes parties le déroulement de mon stage à OC SANTE en tant que Technicienne Informatique dans le service infrastructure et réseau.

Dans le cadre de mon BTS SIO (Service Informatique aux Organisations), j'ai eu l'opportunité de réaliser un stage d'une durée de 6 à 8 semaines. Le principal objectif de ce stage étant de renforcer mes compétences acquises en classe tout en découvrant le monde professionnel lié à mon domaine d'étude, l'informatique.

En sachant que j'ai déjà eu une expérience professionnelle en développement et que j'ai toujours été une bonne élève (du côté développement), j'ai décidé de chercher un stage côté réseau pour me faire découvrir cette branche de l'informatique que j'avais personnellement négligé et voir si cette voie pouvait me convenir ou pas. De plus, il est toujours intéressant d'avoir des compétences en réseau si on veut faire un métier lié à l'informatique car je ne suis pas encore certaine de mon futur métier.

En cherchant mon stage, un secteur d'activité m'intéresse particulièrement : la santé. J'essaie donc de postuler en utilisant des services en ligne tels que LinkedIn, Indeed, Welcome to the Jungle, etc.. en vain. J'ai même réussi à obtenir les coordonnées du RH de l'hôpital Lapeyronie lors d'une allée aux urgences mais sans suite. C'est en discutant avec ma propriétaire d'appartement Mme DE SAXCE que j'obtiens les coordonnées de mon futur tuteur de stage M. Matteoni, le responsable infrastructure et production d'OC-SANTE. J'intègre donc le service « Systèmes d'information ».



La société OC SANTE est considérée comme le premier groupe de santé indépendant de la région Occitanie. Elle regroupe plus de 3 000 employés et 19 établissements à l'échelle nationale mais se situant principalement dans l'Hérault. Au sein de ces cliniques, différents services y sont proposés tels que la chirurgie, maternité, médecine, soins de suite et de réadaptation, psychiatrie, hospitalisation à domicile, EHPAD et résidence senior.



Dans le cadre de ma mission liée au domaine de l'informatique, j'ai effectué mon stage dans les bureaux du centre médical Odysseum situé au 194 avenue Nina Simone à Montpellier. Ce centre médical est le siège social de la société. De plus, il a l'avantage d'être situé à deux pas des cliniques Plein Soleil et Millénaire qui appartiennent aussi au groupe Oc-Santé.

Ce bâtiment s'organise en 3 sections. Tout d'abord la clinique, activité principale du groupe, les bureaux situés au 3^e étage et la direction située au 4^e étage. J'ai ainsi travaillé dans un open space composé de plusieurs bureaux au 3^e étage. Cet open space regroupe différentes parties : la partie administrateur réseau (2 personnes), la partie métier (6 personnes) et la partie techniciens (5 personnes). Tout en ayant des visites régulières du DSI (directeur service informatique) M. PIRAS et du responsable infrastructure réseau et production M. Matteoni qui est aussi mon tuteur de stage.

Ces 3 corps de métier communiquent activement entre eux, notamment les techniciens et les administrateurs réseau puisqu'ils travaillent en collaboration. Des réunions sont organisées régulièrement (tous les lundis) avec le responsable infrastructure et production M. Matteoni pour faire le point sur l'avancée des projets, l'organisation de l'équipe, les astreintes*, la gestion du temps et de l'emploi du temps. Ces réunions sont aussi l'occasion pour chacun de faire part de ses éventuelles remarques personnelles.

* voir le glossaire

Ainsi, ayant commencé mon stage un lundi, j'ai eu l'occasion de me présenter et de rencontrer l'ensemble de l'équipe informatique y compris le DSI lors d'une réunion hebdomadaire. Au cours des 7 semaines passées au sein de cette entreprise, j'ai participé à diverses autres réunions pour avoir un aperçu des projets en cours (migration cluster firewall* Fortinet , mise en place de nouveaux équipements réseau, déménagement de locaux, audit de l'emplacement des bornes wifi, tâches quotidiennes, etc...)

Entouré de mon tuteur et de son équipe, j'ai pu apprendre dans d'excellentes conditions. Ce stage a été l'occasion pour moi d'en savoir plus sur l'environnement de travail des employés dans une entreprise, les problèmes hiérarchiques et comment différents métiers et personnes peuvent collaborer ensemble pour aboutir à un objectif commun qui est de faire avancer l'entreprise.

Grâce à cette expérience, j'ai aussi élargi et approfondi mes connaissances. En effet, j'ai pu observer l'infrastructure d'un grand groupe de santé sur le terrain. J'ai pu visiter différentes cliniques, leurs nouveaux locaux, leurs salles serveurs, baies de stockage et réseau, et même avoir un aperçu de leurs équipements au datacenter Netiwan (Neticenter*) à Bouillargues, près de Nîmes. Ce sont différentes et nombreuses observations sur l'environnement numérique qui ont complété ma mission principale.

De plus, tout au long de mon stage, j'étais au plus près des équipes informatiques du groupe. J'ai pu observer et suivre différents projets qui leur était attribués comme par exemple la mise en production d'une baie réseau informatique comprenant le paramétrage et la configuration des switches *, le brassage et tests avec Fluke, raccordement fibre.... L'un de leur projet le plus critique étant la migration du firewall (Fortinet) qui est passé à une version plus récente (v7.4) puisqu'il nécessitait une intervention physique qui allait engendrer une coupure générale du réseau pour tous les équipements des cliniques OC-SANTE.

Pour la réalisation de mes missions, j'ai eu accès au même environnement de travail que les équipes informatiques. Je disposais donc d'un PC portable Dell classique avec clavier, souris, et l'environnement nécessaire (logiciels, fichiers) pour travailler ainsi qu'un bureau avec deux écrans, prêtés par l'entreprise. A savoir que les administrateurs réseau avaient un matériel plus sophistiqué avec un Dell Latitude 9360 comprenant 16Go de mémoire RAM et un processeur intel core i5 de dernière génération.

De mi-mai jusqu'au mois de juillet, ma mission principale consistait à mettre en place une solution de supervision du réseau fonctionnelle pour la majorité des équipements du groupe. Tout en sachant qu'OC-SANTE dispose déjà d'un logiciel de

ce type (Eyes Of Network) mais que ce dernier n'est plus à jour et obsolète. L'entreprise a choisi la solution Zabbix pour surveiller l'ensemble des composants de leurs infrastructures. En sachant que ce groupe a besoin de superviser environ 180 VM *, 110 switches ainsi que des multiples sites web et le tout, réparti au sein de 19 établissements.

Pour présenter mon expérience de stage au sein de la société OC-SANTE, il paraît pertinent de présenter les missions qui m'étaient attribuées, puis d'envisager la démarche suivie pour aboutir à la réussite de ma mission principale. Enfin, j'aborderai les différentes tâches que j'ai pu effectuer au sein du service infrastructure pour terminer sur l'évaluation des réalisations, les compétences mobilisées et ainsi les expériences et connaissances que ce stage m'a apportées.

I- PRESENTATION DES MISSIONS

A - Contexte professionnel de la mission

Lorsque je suis arrivée dans l'entreprise, la seule personne que je connaissais était celui qui m'avait fait mon entretien d'embauche, M. Matteoni, qui est aussi mon tuteur de stage. Par chance, l'équipe infrastructure réseau dispose d'une réunion hebdomadaire tous les lundis. J'ai pu donc faire connaissance avec toute l'équipe y compris le DSI, me présenter à eux, et avoir un aperçu de l'emploi du temps, de leurs projets ainsi que de l'organisation de l'entreprise OC-SANTE.

Le siège social du groupe situé au 194 Av. Nina Simone à Montpellier est divisé en trois parties : la clinique (1^{er} et 2^{ème} étages), les bureaux (3^e étage) et la direction (dernier étage). Mon stage s'est principalement déroulé dans l'open space au 3^e étage, espace de travail partagé avec toutes les personnes du groupe OC-SANTE travaillant dans le secteur « systèmes d'information ». L'avantage d'une telle organisation est dans la proximité. Les employés peuvent travailler plus facilement en collaboration. De plus, l'open space favorise la discussion, le partage de connaissance et aussi la bonne entente du personnel ce qui améliore notre motivation et notre efficacité.

D'un point de vue organisationnel, cet open space est composé de trois zones.

▷ La partie métier s'assure d'aider le personnel et de les accompagner dans leur métier d'un point de vue solution technique. Ces personnes s'assurent de la bonne compréhension de l'utilisation de l'environnement numérique (fichiers communs, formations en ligne, accès aux serveurs de stockage ou backups numériques, logiciels spécifiques...) par les personnes du métier de la santé du groupe OC-SANTE. Elles peuvent aussi régler les problèmes liés à ces solutions numériques ou alors les transférer aux techniciens.

▷ La partie technicien, composée de 5 personnes, est chargée de régler les problèmes techniques de toutes les cliniques situées en Occitanie. De ce fait, ils sont souvent en déplacement. A savoir qu'il faut au moins un technicien au siège social (dans l'open space) pour assurer la hotline. En général, chaque technicien est spécialisé pour une ou plusieurs cliniques. Mais s'il le faut, chacun est capable d'assurer son métier quel que soit l'établissement.

► La partie administrateur infrastructure et réseau est composée de seulement deux personnes pour l'ensemble des cliniques d'Occitanie du groupe. Contrairement à la partie métier qui est souvent en télétravail, la présence d'au moins un administrateur en présentiel est toujours requise. Et contrairement aux techniciens qui s'occupent de problèmes liés aux postes (PC du personnel) ou aux imprimantes et autre matériels mineurs, les administrateurs disposent de presque tous les droits et s'occupent principalement des serveurs en faisant des manipulations qui nécessitent une rigueur supplémentaire car elles sont plus risquées d'un point de vue informatique. Ce sont aussi eux qui vont suivre et effectuer des projets majeurs comme la migration du firewall, la modification des droits GPO*, la configuration des switches, la gestion des backups des VM, etc...

Comme évoqué précédemment, ce sont les techniciens qui sont chargés de la hotline, c'est-à-dire qu'ils vont répondre à la majorité des mails et appels téléphoniques concernant un problème technique (par exemple, imprimante qui marche plus), une demande technique (par exemple, le nombre de prise RJ45 dans une salle) ou un service technique (par exemple, réinitialiser un mot de passe). Cependant, chaque technicien et administrateur vont tour à tour être chargé de l'astreinte à intervalle d'une semaine par personne.

Contrairement au monde du développement, dans le métier de technicien et administrateur système, l'astreinte est essentielle. Elle permet de garantir un service technique à tout moment. La personne en charge de l'astreinte se doit d'être prêt à répondre au téléphone et intervenir dans un délai d'une heure maximum. Malheureusement, par soucis de budget, le groupe OC-SANTE ne dispose pas d'une assistance téléphonique 24h/24. Cependant, et ce pour chaque clinique, une astreinte téléphonique est assurée les weekend et jours fériés de 8h à 20h pendant toute l'année.

Pour faciliter les échanges téléphoniques, le groupe dispose d'une solution de communication professionnelle : Mitel. Elle permet d'augmenter la productivité et l'efficacité des salariés lorsqu'ils veulent joindre une personne ou composer un numéro. En effet, en se connectant sur Mitel, chaque personne du groupe dispose de tous les contacts importants (dont le numéro d'astreinte) dans leur répertoire. Chaque membre du service informatique dispose également d'un téléphone portable professionnel rudimentaire mais robuste. Cependant, n'étant pas chargé de la hotline ni de l'astreinte (ce qui est normal pour une stagiaire), je n'ai pas pu expérimenter cette fonctionnalité, seulement l'observer.

Concernant le matériel mis à disposition, les techniciens et administrateurs disposent d'une panoplie de matériel informatique (switches, cables, pc, tablettes, outillage, etc...) mis à leur disposition. Quant à moi, on m'a prêté un pc portable (dell), avec clavier, souris et deux écrans pour une meilleure productivité mais aussi pour avoir d'emblée accès à toutes les ressources dont j'avais besoin. Ainsi, dans un dossier partagé nommé « stagiaire », j'ai retrouvé le travail qui avait été précédemment fait par les administrateurs concernant la supervision du réseau. Il y avait aussi des dossiers contenant des fichiers utiles mais confidentiels comme les adresses IP de tous les équipements qui ont besoin d'être supervisés, des scripts de déploiement GPO (pour que j'aie des exemples), etc...

A savoir qu'il y a eu quelques soucis liés aux droits de mon utilisateur. Par exemple, n'étant pas dans le bon groupe dans l'AD* , au début je n'avais pas accès à youtube (pour regarder des tutoriels). Il m'était aussi impossible d'être admin de mon poste pour faire des tests sur des scripts en les exécutant en tant qu'administrateur (chose qu'on m'avait demandé de faire), et d'autres problèmes mineurs qui ont été réglés.

Globalement, on pouvait ressentir la bonne entente du personnel et leur bienveillance à mon égard. Des événements (footing, apéros...) sont régulièrement organisés. Presque tous les matins, une personne choisie amène des viennoiseries et pâtisseries pour déjeuner. Et chaque semaine, le personnel mange ensemble dans un fast food de leur choix. L'établissement dispose aussi d'une cantine / cafeteria pensée pour le personnel et les patients. Au début de mon stage, je me suis vu attribuée un badge pour pouvoir disposer d'un tarif préférentiel à la cafétéria mais aussi pour avoir accès aux bureaux. Une chose intéressante à savoir est que les salles les plus sensibles (baie de stockage, salles serveurs...) ne peuvent pas être ouvertes avec mon badge. Seuls les badges des administrateurs peuvent ouvrir ces salles (et bien sûr les clés physiques).

D'un point de vue hiérarchique, nous retrouvons dans l'ordre, en bas de l'échelle (sans compter les stagiaires) la partie métier et la partie technicien. Ensuite, les administrateurs qui peuvent donner des ordres aux techniciens. Puis le responsable service infrastructure et réseau M. Matteoni, le DSI (Directeur Service Informatique) M. PIRAS qui est en relation directe avec le PDG du groupe M. Guillaume Ponceillé que je n'ai malheureusement pas eu l'occasion de voir. La partie métier est un peu spéciale puisqu'elle peut se référer au DSI mais aussi au DRH (Directeur Ressources Humaines) puisqu'elle constitue un secteur transversal qui n'est pas seulement lié à l'informatique.

B - Problèmes à résoudre, contraintes, limites

Tout au long de mon stage, j'ai dû faire face à divers soucis avec mes collègues pour qui les problèmes semblent faire partie intégrante leur métier. Mais le problème pour lequel j'ai obtenu un stage à OC-SANTE est le fait que leur solution de supervision anciennement utilisée n'est plus à jour et de ce fait, est obsolète.

En effet, voici quelques images pour témoigner de la vétusté de leur ancien logiciel de supervision Eyes Of Network.



(Capture d'écran de l'interface (page d'accueil) d'Eyes Of Network)

Sur l'image ci-dessus, on peut remarquer le minimalisme de l'interface et le style ni attrayant (avec les couleurs fluos), ni moderne (vieux logiciel, page web avec peu de css comme on peut le voir avec le lien bleu souligné en bas de la page). C'est d'autant plus problématique en sachant que l'open space où techniciens et administrateurs travaillent dispose d'un grand écran où est projetée cette page. Ainsi, si une alerte se déclenche, le personnel peut le voir au changement de couleur du cercle (diagramme circulaire) qui devient jaune s'il y a un avertissement, rouge s'il y a un désastre et vert si tout est fonctionnel.

Cependant, aucun moyen de savoir de quel type de problème il s'agit en regardant l'écran. Il faut se connecter sur EON (Eyes Of Network), naviguer pour trouver le bon menu, et cliquer sur une alerte pour avoir la description d'un problème ce qui peut être une perte de temps si le problème est un faux positif (parfois des alertes avec

« hôte à redémarré » remontent mais sont normales car il y a une intervention sur cet hôte en particulier qui a nécessité son redémarrage).

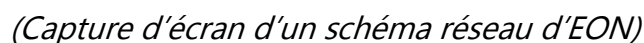
ALL	EQUIPMENT	SERVICE	STATE	OWNER	DESCRIPTION	ORIGINAL-TIME	LAST-TIME	OCCURENCES
<input type="checkbox"/>	OCSEA01	VM DISQUE Vérification de la volumétrie disque sur VM	(!)		DISKUSAGE WARNING - E: usage%=95	Jun 30, 2023 9:29:25 AM	Jun 30, 2023 9:49:25 AM	3

(Capture d'écran de la page des alertes d'EON)

L'image ci-dessus nous montre que cette interface, en plus d'être non responsive, c'est-à-dire non adapté à toutes les tailles d'écran, (les marges de la page web ont été rognées sur cette image pour qu'elle soit lisible), n'est pas du tout intuitive. Cette page nous montre les alertes actuelles sur les équipements du groupe. Nous remarquons, dans ce cas, qu'il y a une alerte jaune (avertissement) concernant le pourcentage d'utilisation du disque (espace de stockage) d'une VM.

Nous pourrions aller plus loin en disant qu'une alerte sur le pourcentage d'utilisation d'un espace de stockage n'est pas représentative du besoin d'une entreprise. En effet, si une VM possède 20To * de stockage cela voudrait dire que si l'espace de stockage atteint 95%, elle lui reste encore 1To. Ce qui est énorme ! A titre de comparaison, la VM sur laquelle j'ai implémenté Zabbix disposait de 50Go soit environ 0.06To.

Ainsi, non seulement l'interface web n'était pas esthétique sur EON mais les alertes n'étaient pas configurées correctement. Les administrateurs m'ont avoué ne pas avoir passé trop de temps à essayer de configurer ce logiciel. Notamment avec le changement constant des appareils du groupe ont causé des déménagements, des extensions ou autre. Certaines VM n'avaient pas lieu d'être sur EON tandis que d'autres n'y étaient pas tout simplement. Sans parler du fait que les mises à jour n'existent plus pour ce logiciel de supervision du réseau et que de ce fait, il devenait obsolète.



* voir le glossaire

L'objectif est donc de remplacer complètement et au plus vite ce logiciel obsolète par un nouveau : Zabbix. Dans un premier temps, il faudra veiller à ce que toutes les alertes et données recueillies soient bonnes et qu'il n'en manque pas une seule par rapport à EON (sauf si ce sont des données inutiles). Ensuite, il faudra migrer tous les appareils de EON vers Zabbix (en sachant qu'un appareil peut être supervisé à la fois sur EON et à la fois sur Zabbix). Le tout, en faisant des optimisations d'interfaces pour que ce soit agréable à regarder et pratique à utiliser. Enfin, il faudra adapter le logiciel aux besoins de l'entreprise, créer les groupes d'utilisateurs sur Zabbix, faire les cartes réseau importantes, les différents widgets et dashboards, etc...

L'implémentation de cette nouvelle solution de supervision au sein du groupe va enfin leur permettre de pouvoir monitorer leurs appareils et leurs services correctement. Nous verrons plus tard la différence et la plus-value qu'apporte Zabbix par rapport à EON.

II- DEMARCHE SUIVIE

A - Processus suivi – méthode

Tout d'abord, j'ai fait des recherches sur la manière d'installer Zabbix ainsi que sur les prérequis au niveau de la VM. Un administrateur était chargé de me créer une VM pour que je puisse installer Zabbix dessus mais je devais lui donner des spécifications tels que le nombre de processeurs requis, la quantité de mémoire RAM, de stockage, etc... En sachant que je n'ai eu accès à Eyes Of Network que vers la fin de mon stage. Je ne pouvais donc pas prendre exemple sur la précédente solution de supervision du réseau (c'était une contrainte voulue par mon tuteur).

En fonction de mes connaissances sur la taille de l'entreprise et le nombre d'équipement à superviser j'ai donc décidé d'implémenter la version « moyenne » de Zabbix avec une VM CentOS, version : 9 Stream (imposé) pouvant avoir une capacité de 10 000 données monitorées. Pour ce faire, il nous faut une configuration de 16Go de RAM, 4 CPU et 50Go en sachant que le stockage dépend du nombre de machines (hosts) et de quels vont être les paramètres supervisés. J'ai aussi choisi, de manière logique, d'installer la dernière version de Zabbix (v6.4)

A partir de là j'ai été laissée en autonomie. Travaillant dans le même espace que les administrateurs, je pouvais bien sûr leur poser des questions mais vu que j'accomplissais mes tâches assez rapidement, je les ai rarement dérangés pour poser des questions sur ma mission principale. La grande majorité des questions que je leur posais étaient par curiosité sur ce qu'ils faisaient pour essayer de voir si je pouvais les aider (mais le niveau de leurs tâches est souvent bien trop avancé pour moi).

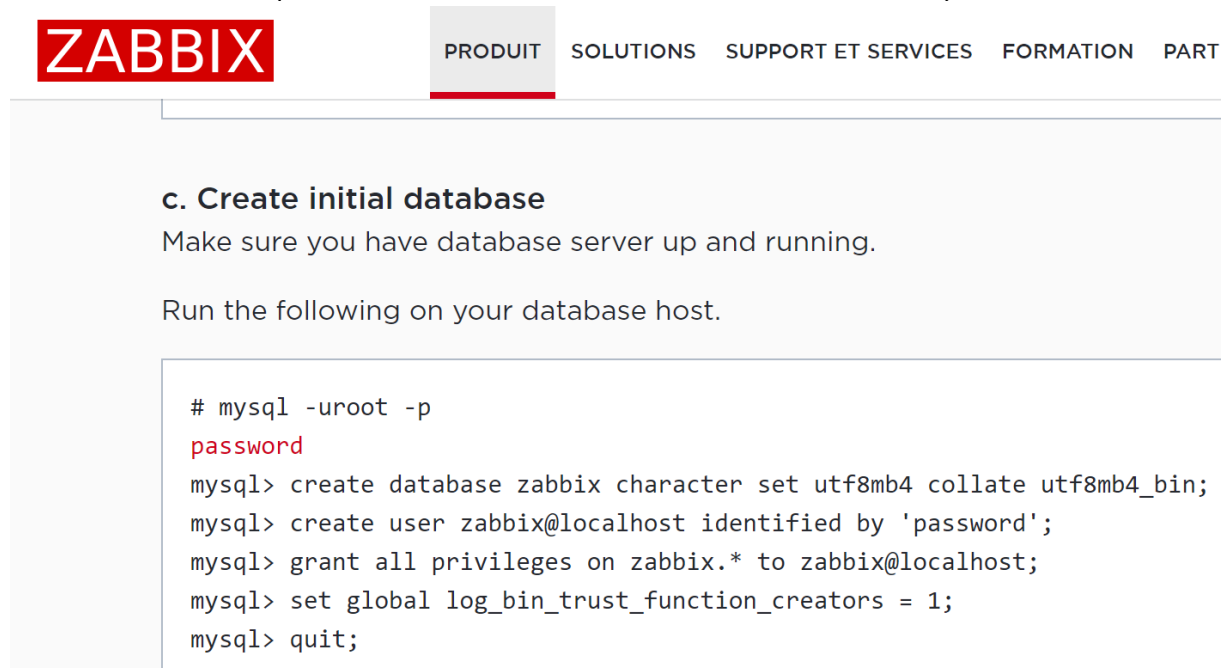
La documentation officielle de Zabbix est disponible à cette URL :

https://www.zabbix.com/documentation/6.4/downloads/Zabbix_Documentation_6.4.en.pdf

Cependant, cette documentation n'était pas complète et comporte des erreurs. Parfois la version de Zabbix décrite dans la documentation n'était pas représentative de la dernière version (même s'il y a un document par version), parfois même des erreurs d'orthographe se glissaient dans les lignes de commandes. C'était très problématique surtout pour quelqu'un qui découvre l'installation de Zabbix et qui n'est pas expert en linux ni en lignes de commandes.

Comme on peut le voir sur cette image, voici un exemple de faute dans la documentation officielle. Cette partie correspond à l'installation de la base de données que va utiliser le serveur Zabbix. Ici, la bonne ligne de commande est « `mysql -u root -p` » et non « `mysql -uroot -p` », un simple espace peut tout changer.

(Extrait de la documentation officielle de Zabbix)



The screenshot shows the Zabbix website navigation bar with the ZABBIX logo and links for PRODUIT, SOLUTIONS, SUPPORT ET SERVICES, FORMATION, and PART. Below the navigation bar, the section 'c. Create initial database' is highlighted. The text reads: 'Make sure you have database server up and running. Run the following on your database host.' Below this, a code block contains the following commands:

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

Ainsi, j'ai décidé de me fier à au moins deux sources identiques avant de faire n'importe quelle manipulation sur ma VM. Les sources que j'ai utilisées pour mon apprentissage et pour mener à bien ma mission sont principalement des sites internet. Le meilleur est (selon moi) bestmonitoringtools.com. J'ai également regardé des tutos de divers youtubeurs. Mais, étant dans un espace de travail collaboratif et professionnel, il était déplacé de ma part de mettre mes écouteurs ou casque pour regarder des tutoriels. J'ai donc préféré utiliser les sites web.

J'ai quand même globalement suivi le plan de la documentation pour implémenter Zabbix. Et comme certaines tâches nécessitaient des droits d'administrateurs ou des manipulations délicates (que je ne pouvais pas effectuer pour des raisons de sécurité), les administrateurs étaient régulièrement au courant de mon avancée et j'avais confiance en eux pour qu'ils me disent si je faisais quelque chose de mal.

B - Organisation des missions

Un planning précis ne m'a pas été fourni pour ma mission. J'ai même demandé à mon tuteur s'il avait besoin de faire le point avec moi tous les jours mais il m'a indiqué que cela n'était pas nécessaire. Je me devais juste de respecter la date limite, c'est-à-dire : avoir installé, implémenté et configuré Zabbix à la fin de mon stage de telle sorte à ce qu'il puisse être mis en production. Les seules fois où j'avais un planning précis étaient lorsque je devais faire des interventions avec des techniciens car eux devaient accomplir des tâches parfois chronométrées à la minute près.

Globalement j'avancais très vite. Par exemple, j'avais fini l'installation et la configuration du premier appareil sur Zabbix en moins d'une semaine. De ce fait, j'ai passé une grande partie de mon temps à me former auprès du personnel. J'ai donc beaucoup appris. Ils étaient ravis de répondre à toutes mes questions et me laisser observer leur travail. Et dès que les administrateurs devaient partir en intervention, j'avais le droit de les suivre pour les aider et observer leur travail. Bien sûr à chaque fois, ils me formaient pour que je puisse effectuer certaines tâches qui sortent du cadre de ma mission principale comme installer un switch, brasser des câbles, vérifier des installations (repérage des lieux, audit, etc...).

Malgré le fait que je n'étais pas dans une petite entreprise, j'étais assez libre. Si je voulais partir en intervention toute une journée avec un technicien, j'y avais le droit. A condition d'obtenir l'accord du technicien en question. Cette liberté se ressentait aussi parmi les employés. A condition de fournir son travail en temps et en heure, on pouvait faire presque ce que l'on voulait.

Mon emploi du temps était exclusivement en présentiel. Je devais travailler du lundi au vendredi de 9h à 17h avec une pause midi d'une heure. Cependant, je croisais souvent des employés qui, n'ayant rien à faire, ne faisaient rien. Pour ma part, je préférais passer mon temps libre à observer et aller en intervention. Je me rendais compte qu'une journée entière pouvait passer juste pour raccorder une fibre et vérifier qu'il n'y a aucun problème dans une installation. Il faut avouer que regarder des employés s'arracher les cheveux à cause de nombreux problèmes est assez comique.

Concernant le compte rendu que je devais rendre, il s'agit d'une documentation complète de plus d'une vingtaine de pages, sur tout ce que j'avais fait concernant ma mission principale. Cette documentation a pour but de renseigner les administrateurs sur comment j'ai installé Zabbix et surtout comment l'utiliser. En effet, n'ayant que rarement manipulé le logiciel, l'équipe informatique se devait d'apprendre à utiliser correctement Zabbix en cas de problème.

Table des matières

I – CONFIGURATION REQUISE	3
II – INSTALLATION	3
III – SECURISATION	4
Sécuriser l'accès utilisateur Zabbix	4
Certificat SSL (autosigné)	4
Certificat SSL	5
Redirection port 80 vers 443	5
Activer HSTS sur le serveur web (il faut un vrai https avant)	5
Désactivation de l'exposition des informations du serveur Web	5
Supprimer la page web par défaut apache	5
Mod_security	6
Pages d'erreur apache	6
Antivirus SentinelAgent linux	6
IV – SUPERVISION DU PREMIER APPAREIL (SWITCH)	6
Du côté du switch	6
Du côté de la VM Zabbix server	6
Du côté de l'interface web Zabbix	7
Ajouter des groupes d'hotes	7
Ajouter des hotes	7
V – NOS TEMPLATES	7
Templates créées	7
Template Cisco Switch	7
Template Cisco Switch Catalyst 9300	11
Template OCS Windows Zabbix Agent	13
Template Routeur	14
Template Sites Web	15

VI – CREER UNE CARTE	15
Sur les anciennes versions Zabbix - Weathermap API JSON	15
Les cartes sur Zabbix 6.4	16
Les cartes réseau	16
Les cartes géographiques	17
VII – DECOUVERTES ET ACTIONS DE DECOUVERTE	17
Les découvertes	17
Actions de découverte	18
Informations importantes	18
Découverte automatique d'agent zabbix	18
Configuration Zabbix (interface web)	19
Configuration de l'hôte (avec l'agent)	19
VIII – ADMINISTRATION	20
Créer un utilisateur	20
Types de média	21
IX – DASHBOARDS ET WIDGETS	21
Vue globale principale	21
Autres dashboards	22
Widgets	22
Modifier le widget « Problems by severity »	23
X – DEPLOIEMENT DES AGENTS (GPO)	24
Script d'installation des agents sur les VM	24
Déploiement GPO	24

(Aperçu de la table des matières de la documentation que j'ai fournie)

De plus, comme je l'ai évoqué précédemment, des réunions hebdomadaires ont lieu pour toute l'équipe informatique afin de partager l'avancée de chacun. C'est lors de ces réunions que je discutais de l'avancée de mon projet et que, la dernière semaine de mon stage, j'ai fait une démo de Zabbix pour toute l'équipe via Zoom (vu que certains étaient en télétravail). C'est lors de ces réunions que j'avais aussi l'occasion de répondre aux questions éventuelles des techniciens sur comment fonctionne et comment utiliser Zabbix. Je répondais aussi à leurs demandes (par exemple, la création d'une carte réseau pour l'infrastructure de la clinique d'Odysseum).

III- REALISATION DE LA MISSION

A- Sécurisation de la solution

Il ne suffit pas d'avoir une solution de supervision fonctionnelle si elle n'est pas sécurisée.

Ainsi, je me devais de configurer Zabbix correctement, en suivant toutes les bonnes pratiques. La première chose à faire est de modifier l'utilisateur par défaut (admin) et son mot de passe par défaut (Zabbix) pour éviter qu'un hacker puisse facilement y avoir accès. J'ai donc créé un nouvel utilisateur disposant de tous les droits (super admin user) mais ayant un nom d'utilisateur et un mot de passe plus sécurisé.

Contrairement à la précédente application de l'entreprise EON, j'ai décidé d'installer un certificat SSL pour que la page web de Zabbix soit en HTTPS et non en HTTP. Cela permet d'avoir une connexion plus sécurisée par le biais d'un chiffrement SLL/TLS. En plus de chiffrer les données, le protocole SLL/TLS permet d'authentifier le serveur auquel l'utilisateur se connecte et dispose d'une protection contre l'altération des données transmises.

Pour ce faire, j'ai procédé en deux étapes. Dans un premier temps, ne disposant pas du certificat d'OC-SANTE, j'ai mis en place un certificat SSL autosigné.

```
sudo yum install mod_ssl
sudo mkdir -p /etc/httpd/ssl/private
chmod 700 /etc/httpd/ssl/private
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/httpd/ssl/private/apache-selfsigned.key -out /etc/httpd/ssl/apache-selfsigned.crt
sudo vi /etc/httpd/conf.d/ssl.conf
SSLCertificateFile /etc/httpd/ssl/apache-selfsigned.crt
SSLCertificateKeyFile /etc/httpd/ssl/private/apache-selfsigned.key
systemctl restart httpd.service
```

Le problème est qu'un certificat autosigné ne suffit pas pour que le navigateur nous indique que le site est sécurisé. Il a donc fallu que je demande le certificat SSL privé du groupe OC-SANTE. Via un transfert en utilisant WinSCP (pour transférer les fichiers du pc à la VM), j'ai placé les fichiers au bon endroit sur la VM et remplacé des lignes dans le fichier de configuration d'Apache. Il faut faire attention à ce que le nom de domaine de l'interface web de Zabbix soit sous la forme xxx.oc-sante.fr pour que le certificat fonctionne. A la suite de cela, on voyait bien le cadenas sans

problème à côté du nom de domaine du site.



De nombreux autres correctifs de sécurité ont été instaurés comme la redirection du port 80 (http) vers le port 443 (https) pour s'assurer que l'utilisateur utilise bien le protocole https pour se connecter sur le site.

```
sudo vi /etc/httpd/conf/httpd.conf
<VirtualHost *:*>
ServerName [servername]
Redirect permanent / [servername]:443
</VirtualHost>
```

La désactivation de l'exposition des informations du serveur web et de la page web par défaut d'Apache (fichier /etc/httpd/conf.d/welcome.conf). On doit aussi modifier les pages d'erreurs par défaut d'Apache si on veut être sûr que le potentiel hacker ait le moins d'informations possibles sur notre système pour qu'il ait le moins de chance de trouver une faille de sécurité.

```
sudo vi /etc/httpd/conf/httpd.conf
ServerSignature Off
ServerTokens Prod
sudo vi /etc/php.ini
expose_php = Off
```

Parmi toutes ces sécurités que j'ai pu mettre en place, l'une des plus importantes est d'installer sur la VM l'antivirus SentinelAgent utilisé par OC-SANTE. (Je ne peux malheureusement pas divulguer la procédure). Cet antivirus permet de faire remonter ma VM dans la base de données SentinelAgent utilisée par l'entreprise, la visualiser et superviser les menaces (s'il y en a eu) qui ont pesé sur la machine. Et si besoin, un bouton permet d'isoler complètement la VM du réseau. Tous les appareils d'OC-SANTE (y compris le pc qui m'a été prêté) ont cet antivirus installé. De plus, grâce aux pages d'adresses IP attribuées automatiquement lorsque quelqu'un se connecte au réseau de l'entreprise, il est possible de déterminer dans quelle clinique se trouve un appareil grâce à l'adresse IP qu'elle possède actuellement. Cela permet, si l'entreprise est menacée, d'isoler seulement les appareils se situant dans une certaine zone géographique pour que les autres qui n'ont pas été impactés par la menace continuent de fonctionner normalement.

B- Collecte des données

Pour ce qui est de la collecte des données, Zabbix dispose de templates (modèles) préconçus en fonction du type d'appareil que l'on veut superviser et par quel moyen cette supervision se fait (agent Zabbix, SMTP). Cependant, les templates de Zabbix sont très gourmandes en termes d'espace et de ressources. Certaines peuvent collecter des milliers d'éléments par hôtes alors qu'une centaine suffit. On m'a donc conseillé de faire mes propres templates en partant de rien pour éviter de collecter des données inutiles et avoir un meilleur contrôle sur la supervision de nos appareils.

Ainsi, j'ai créé 6 modèles différents correspondant aux 6 types d'appareils et aux besoins de l'entreprise vis-à-vis d'eux :

Modèles

<input type="checkbox"/> Nom ▲	Hôtes	Éléments	Déclencheurs	Graphiques	Tableaux de bord	Découverte	Web
<input type="checkbox"/> 1- Cisco switch	Hôtes 112	Éléments 20	Déclencheurs 12	Graphiques 4	Tableaux de bord 1	Découverte 7	Web
<input type="checkbox"/> 1- Cisco switch Catalyst 9300	Hôtes	Éléments 33	Déclencheurs 19	Graphiques	Tableaux de bord	Découverte 1	Web
<input type="checkbox"/> 1-OCS Windows Zabbix agent	Hôtes	Éléments 31	Déclencheurs 15	Graphiques 5	Tableaux de bord 1	Découverte 4	Web
<input type="checkbox"/> 1-OCS Workstation	Hôtes 1	Éléments 14	Déclencheurs 9	Graphiques 2	Tableaux de bord 1	Découverte 3	Web
<input type="checkbox"/> 1- Routeur	Hôtes 30	Éléments 3	Déclencheurs 5	Graphiques 3	Tableaux de bord 1	Découverte	Web
<input type="checkbox"/> 1- Sites web	Hôtes 11	Éléments	Déclencheurs 1	Graphiques 4	Tableaux de bord	Découverte	Web 1

Chaque template se voit attribuer des hôtes, des éléments (les données récoltées), des déclencheurs (les alertes), des graphiques, des tableaux de bord et des découvertes (le nombre de certains éléments peut varier d'une machine à l'autre donc on a besoin de « découvrir » où sont ces éléments et combien il y en a). Les éléments découverts s'ajoutent automatiquement aux éléments de l'hôte et peuvent créer avec eux, un ou plusieurs déclencheur(s) et/ou graphique(s). La partie « web » quant à elle permet de superviser un site web à partir de son URL.

Pour les switches, la collecte des données se fait via SNMP (protocole permettant à une application de gestion de demander des informations provenant d'une unité gérée). Cela requiert d'avoir préalablement effectué une commande du type : [zabbix-server] community [MyCommunity] RO, sur tous les switches qu'on veut superviser. Cette commande permet au serveur Zabbix d'avoir accès aux données du switch en question. Le déploiement de cette commande a été effectué par un administrateur via un script powershell (confidentiel). Dans un terminal, pour recueillir des données en SNMP, on effectue un snmpwalk comme ci-dessous :

```
[infogem@OCSZAB02 ~]$ snmpwalk -v2c -c 1.3.6.1.4.1.9.9.13.1.3.1.2
SNMPv2-SMI::enterprises.9.9.13.1.3.1.2.1004 = STRING: "SW#1, Sensor#1, GREEN "
```

En précisant la communauté SNMP et l'IP du switch (confidentiel), on obtient une information en fonction de l'OID spécifié. Par exemple, ci-dessus, l'OID 1.3.6.1.4.1.9.9.13.1.3.1.2 correspond à la description des capteurs de température (ici il n'y en a qu'un) du switch. Tous les OIDs des switches sont référencés dans des MIB (Management Information Base) propres pour chaque modèle de switches. A savoir que tous les switches d'OC-SANTE (y compris les bornes wifi) sont exclusivement de la marque CISCO.

Vous trouverez en annexe quelques exemples plus détaillés de templates que j'ai créé sur Zabbix.

La collecte de données la plus complexe était pour les VM et les serveurs. L'entreprise a choisi d'installer un agent Zabbix sur chaque machine pour s'assurer de la fiabilité des données remontées sur Zabbix. J'ai donc dû faire un script d'installation de l'agent en .bash que j'ai testé par le biais de TeamViewer sur un serveur distant. Voici une capture d'écran du script en question.

```
if exist "%ProgramFiles%\Zabbix Agent 2" goto End

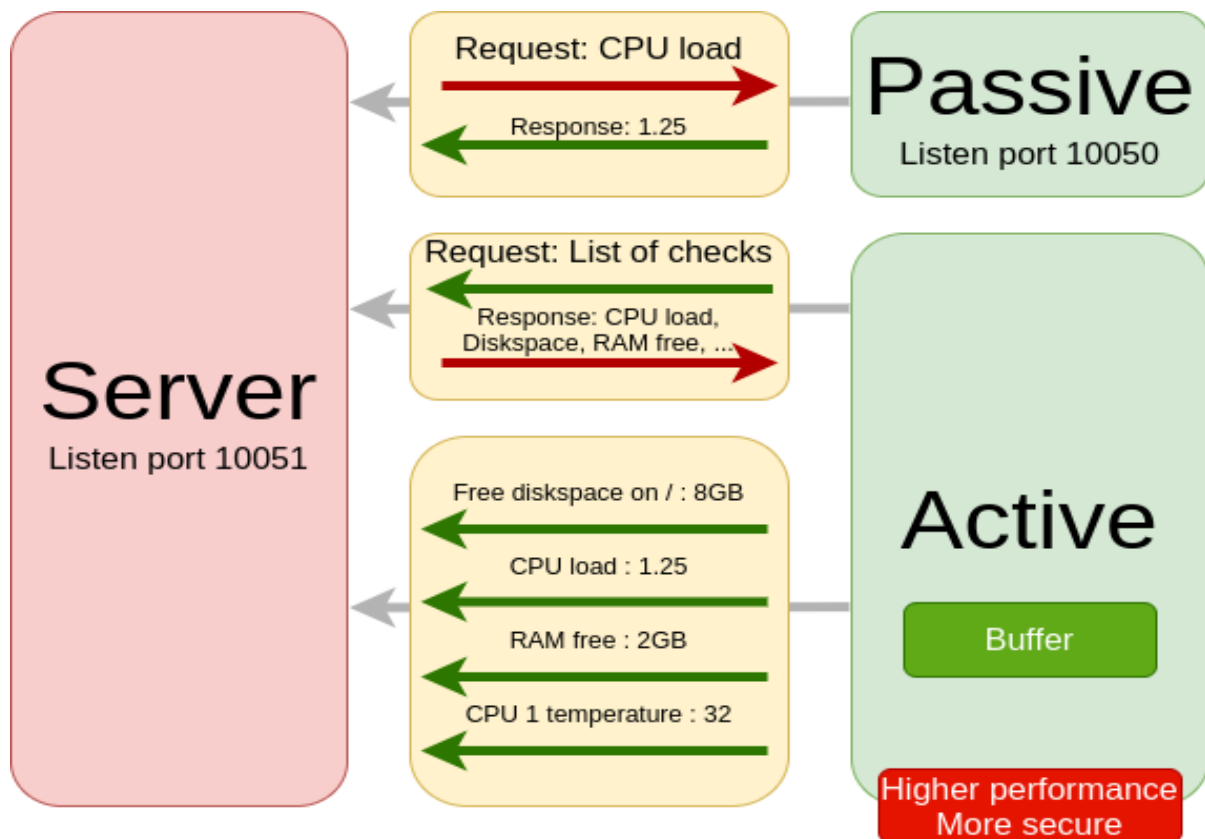
msiexec /i "%~dp0zabbix_agent2-6.4.2-windows-amd64-openssl.msi" /qn ^
    ENABLEREMOTECOMMANDS=1^
    SERVER=10.
    SERVERACTIVE=10.
    HOSTNAME=%computerName%
    HOSTMETADATA=Windows^
    TLSCONNECT=psk^
    TLSACCEPT=psk^
    TLSPSKIDENTITY=
    TLSPSKVALUE=0c58d59b02b86

net start "Zabbix Agent 2"
```

Une fois les tests effectués et validés, un déploiement GPO (effectué par les administrateurs) a permis progressivement (au redémarrage de chaque machine) d'installer l'agent Zabbix ou de ne rien faire si l'agent est déjà installé. A noter que ce script assure aussi un démarrage automatique de l'Agent Zabbix (la dernière ligne).

Du côté de l'interface web de Zabbix, un nouveau groupe d'hôte « Auto discovery » a été créé pour voir les nouvelles machines découvertes sur Zabbix par le biais de l'agent. Cette remontée d'hôte se fait via une action d'enregistrement automatique et par le biais d'une vérification active comme on peut le voir sur le schéma ci-après. Il faut aussi veiller à autoriser le port 10051 sur le firewall du serveur

Zabbix puisque la découverte automatique d'agents utilise ce port contrairement à la collecte classique de données qui utilise le port 10050 par défaut.

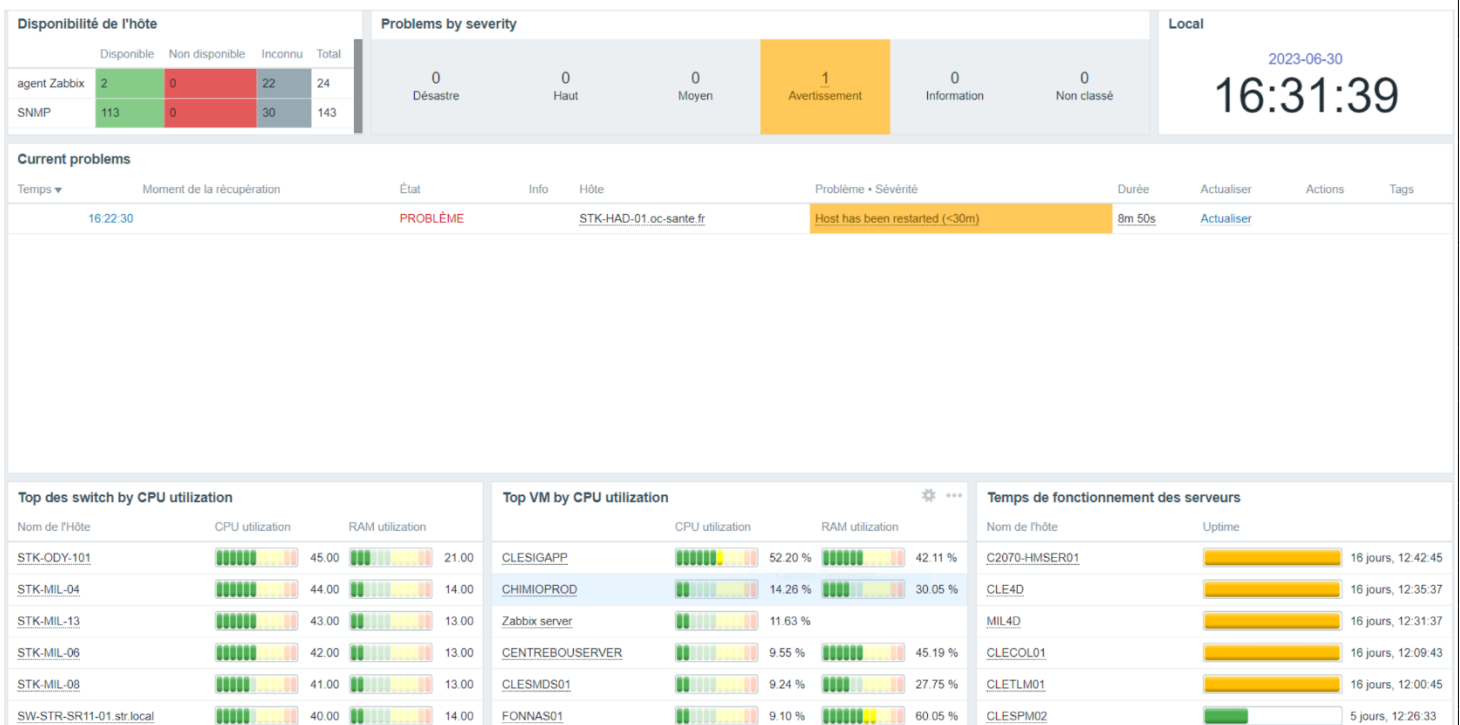


(Schéma expliquant les vérifications actives et passives sur Zabbix)

C- Dashboard et widgets

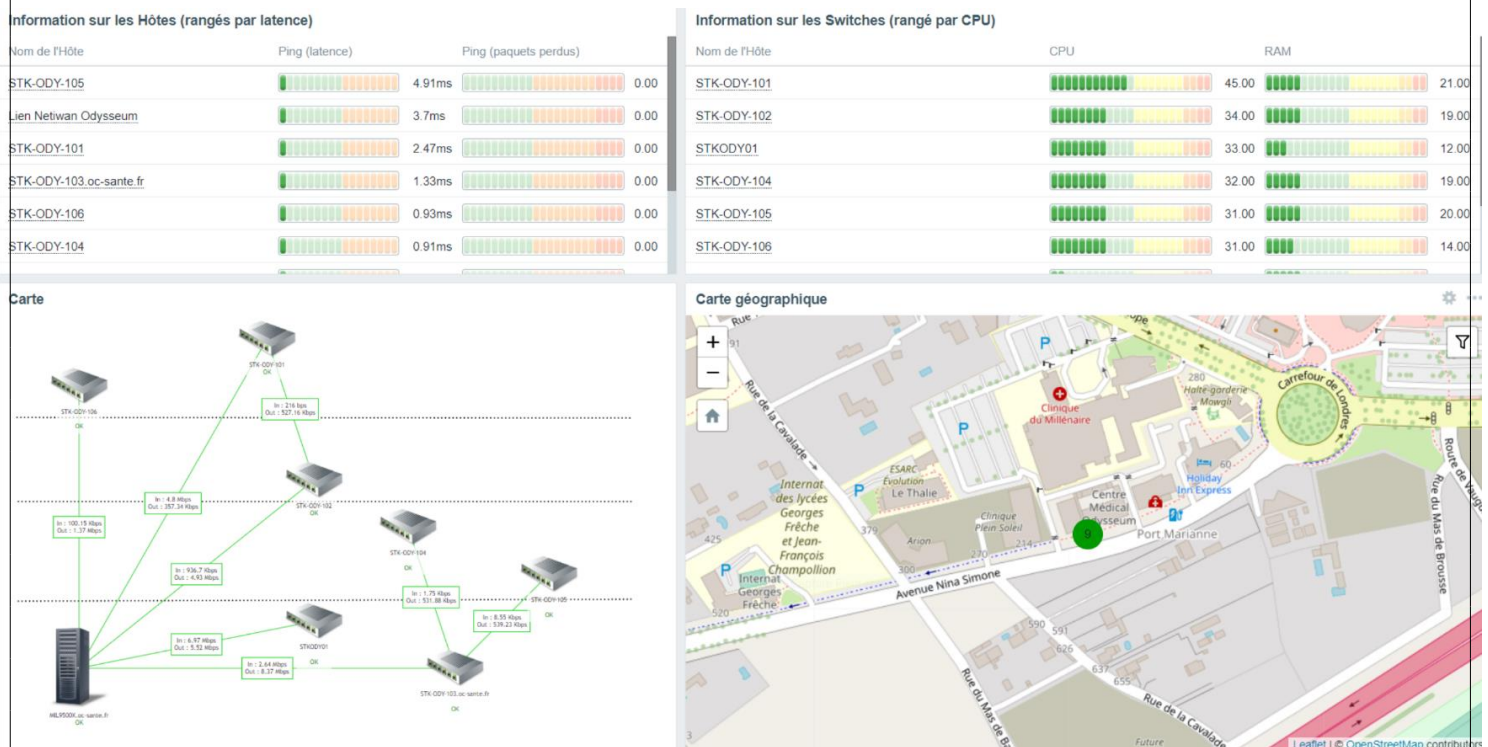
Contrairement à l'ancien logiciel de supervision d'OC-SANTE, avec Zabbix nous allons pouvoir créer des interfaces personnalisées, à la fois pratiques et agréables. Par défaut actualisé toutes les 30 secondes, le dashboard principal sur la page d'accueil est nommé « Global view » et récapitule l'ensemble des informations clés dont on a besoin ainsi qu'une vue globale des équipements problématiques.

Voici un aperçu de la vue globale en question :



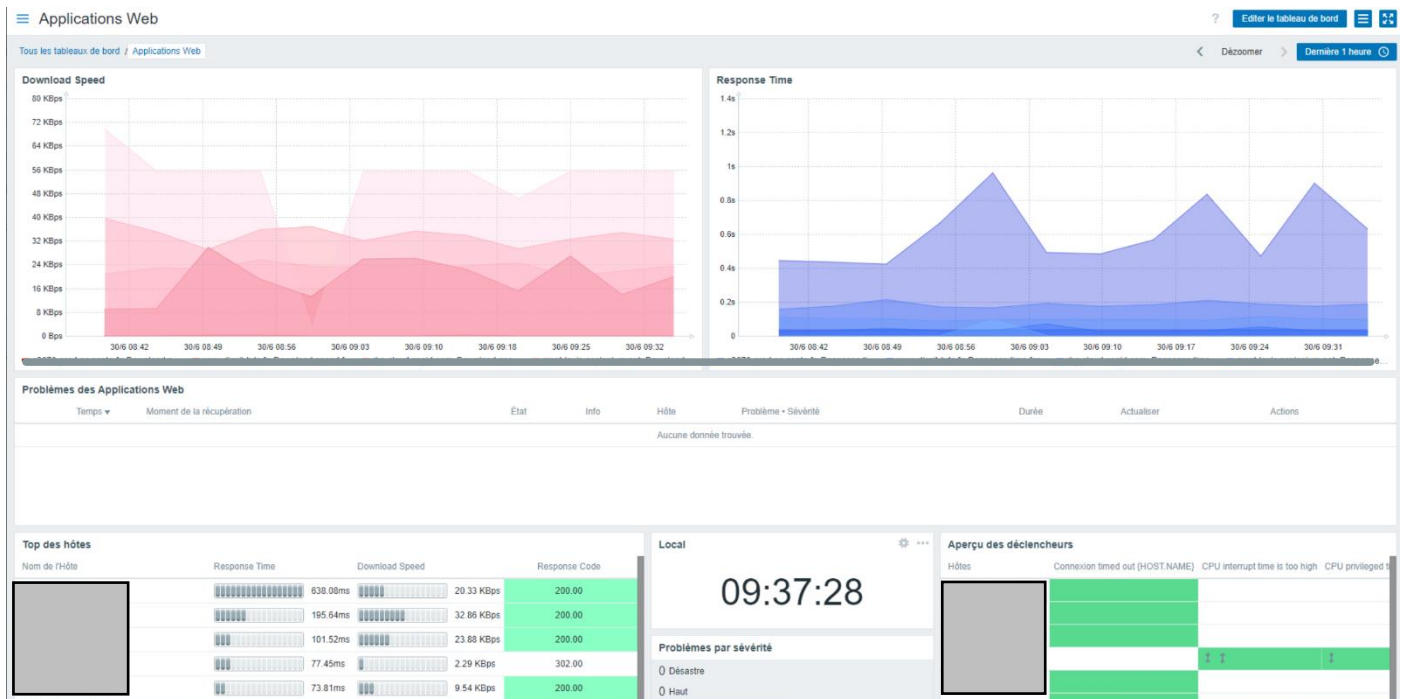
(Dashboard « Global View » de Zabbix)

En sachant qu'en plus de la vue principale, un dashboard par clinique permet de récapituler les informations de tous les hôtes appartenant au groupe de cette clinique. En voici un exemple :



(Dashboard de la clinique Odysseum)

De plus, il y a un dashboard Application Web qui affiche une vue globale (graphiques, problèmes, historique des incidents, tableau récapitulatif des informations en temps réel sur les sites web, etc...) de l'ensemble des quelques sites web supervisés.

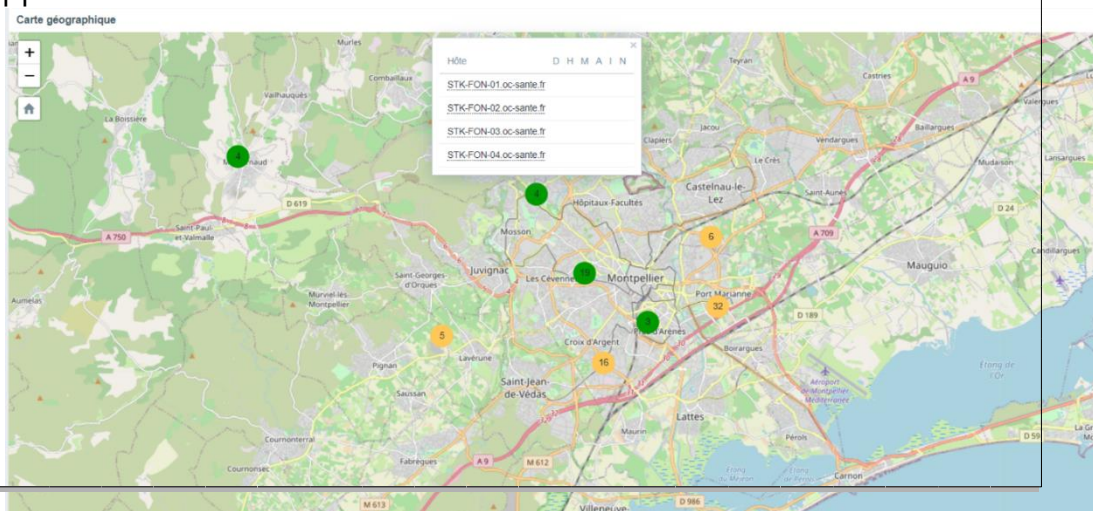


dans l'entreprise

(Dashboard dédié aux sites web les plus importants du groupe OC-SANTE)

Jugé primordial, on retrouve aussi un dashboard UPTIME qui récapitule toutes les informations (problèmes, hôtes, etc...) relatives à cet élément uptime. On peut donc savoir quelle VM n'a pas redémarré depuis longtemps, si des switches ont redémarré (provoquant ainsi une panne réseau sur les appareils branchés dessus) et d'autres informations.

Enfin, le dashboard Carte Géographique nous affiche une immense carte avec les hôtes placés dessus. Ces hôtes sont représentés par des points de couleur verte lorsqu'il n'y a pas de problème sinon rouge, orange ou bleu s'ils ont des problèmes. Ce dashboard permet d'avoir une vue d'ensemble sur l'état des équipements des différents sites par rapport à leur localisation.



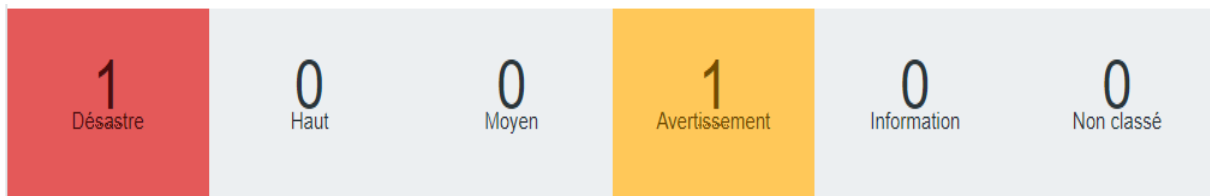
* voir le glossaire

Ces dashboards, même s'ils ont demandé beaucoup de travail, sont très pratiques. Cette partie a aussi été l'occasion pour moi de mobiliser mes compétences en développement puisque j'ai dû manipuler des fichiers utilisés pour le côté web (frontend) de Zabbix en php et css.

Par exemple, le dashboard d'affichage des alertes par défaut de Zabbix ressemble à ça :



Ce qui n'est pas pratique pour visualiser en un coup d'œil le nombre de problèmes et quels types de problèmes nous avons. Il convient donc de le modifier pour que ça ressemble à ça :



❖ Modifier la couleur

Le Widget de base ne permet pas de visualiser en un coup d'œil quels problèmes nous avons et s'ils sont grave. Pour y remédier, on peut faire en sorte que les cases se colorent uniquement s'il y a un/des problème(s) en cours (en fonction de leur sévérité).

Le fichier `/usr/share/zabbix/` comprend l'ensemble des éléments et fichiers relatifs à l'affichage du site web de Zabbix.

Dans le fichier `/usr/share/zabbix/include/blocks.inc.php`, il faut modifier la fonction « `getSeverityTableCell` ».

Il rajouter le code :

```
if ($stat['count']== 0 ) {  
    $severity = 0;  
}
```

❖ Modifier la taille des numéros (nombre de problèmes)

Dans la version par défaut, la police d'écriture des numéros de ce widget est trop petite, surtout si elle doit être projetée sur un grand écran. Pour y remédier on se rend dans le répertoire `/usr/share/zabbix/`.

Modifier le fichier css **`/assets/styles/blue-theme.css`** :

Attribut : « `.totals-lists` »

Font-size : 36px ; (au lieu de 16px)

En sachant qu'il y a aussi d'autres modifications qui ont été effectuées pour modifier l'apparence d'autres widgets, ce que nous avons vu ci-dessus était juste un exemple.

D- Administration

Du côté administratif, il m'a fallu créer différents types d'utilisateurs ayant différents rôles et différents droits en fonction des besoins de l'entreprise. Ainsi, j'ai créé un compte en lecture seule ayant uniquement accès à certains dashboards pour la projection de l'interface web sur un écran, deux comptes disposant des droits de super administrateurs pour les admins et des comptes « internal » ayant accès en lecture seule à tous les menus et les informations de Zabbix. La gestion des droits se fait via l'interface web de Zabbix.

Pour informer les techniciens d'un éventuel problème sur un équipement, j'ai aussi dû configurer l'envoi de mail automatique en fonction de la gravité de l'alerte et de l'importance de l'hôte.

Pour créer un courriel et le lier à Zabbix :

TYPE DE MEDIA

Nom : [nom du média, « email » conseillé]

Type : courriel

Fournisseur de messagerie : [pour notre cas Generic SMTP]

Port du serveur SNMTP : [Pour notre cas 465]

Courriel : [le courriel]

SMTP helo : [Pour notre cas ocszab02.oc-sante.fr]

Sécurité de la connexion : [Pour notre cas SSL/TLS]

Verifier le pair SSL : non

Verifier l'hote SSL : non

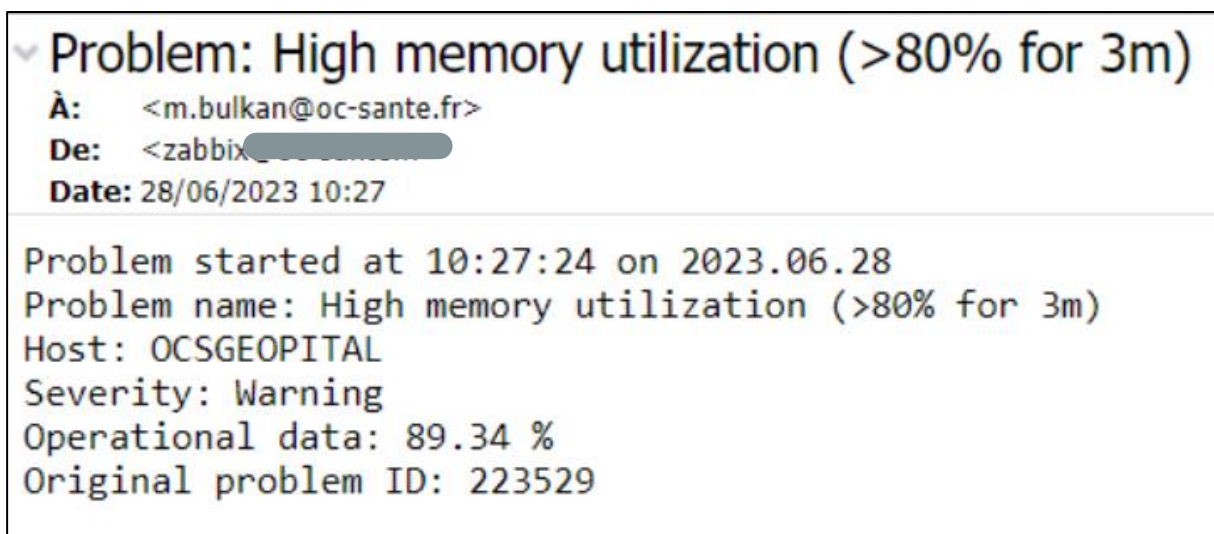
Authentification : Nom d'utilisateur et mot de passe à renseigner

Format du message [HTML]

Activé : check

Pour l'envoi d'email, 5 modèles de messages sont présents (problème, récupération de problème, mise à jour du problème, découverte, enregistrement automatique). Mais on peut en créer d'autres. Différentes variables sont supportées telles que EVENT.TIME, EVENT.NAME, HOST .HOST, etc... On peut aussi choisir l'objet et le contenu du mail ainsi que son style par le biais de balises html.

Voici un exemple d'email qu'un technicien peut recevoir :



Le style peut paraître rudimentaire l'avantage d'un mail comme cela est qu'il prend peu d'espace sur les serveurs de messagerie. L'important est de privilégier le côté pratique, que toutes les informations soient visibles et claires. A partir de là, la personne pourra utiliser l'ID du problème sur Zabbix pour retrouver les données relatives à l'hôte et essayer d'identifier la cause ainsi que la solution du problème.

IV- EVALUATION DES REALISATIONS ET COMPETENCES MOBILISEES

A - Adéquation du travail

Ma mission principale m'a été donnée en fonction de la durée de mon stage et de mon niveau d'étude (première année). Voulant être honnête, j'avais bien spécifié à mon entretien que j'étais beaucoup plus douée en développement qu'en réseau mais que je voulais quand même être intégrée au pôle infrastructure de l'entreprise. Au début il était question que je sois entourée des administrateurs pour qu'ils puissent m'accompagner et m'aider à réaliser mon travail, cependant j'ai rarement eu besoin d'aide.

Etant motivée et voulant élargir au maximum mon champ de connaissances, j'essayais de finir ma mission principale le plus vite possible tout en fournissant un travail de qualité. Ainsi mes collègues l'auront remarqué, ma plus grande qualité est d'être autonome et très rapide. Efficace. Mes capacités n'ont pas manqué de se faire remarquer auprès du responsable M. Matteoni qui m'a autorisé à faire ce que je voulais pendant mon stage (observation, interventions avec les techniciens, visite des cliniques, participation aux tâches quotidiennes, participation aux réunions, ...).

D'un point de vue général, j'essayais d'aider au mieux l'équipe informatique tout en apprenant leur métier. Et on peut dire que mon stage leur a été bénéfique pour eux. En effet, en ce qui concerne ma mission principale, il s'agit d'une solution qui va révolutionner la manière dont les équipements étaient supervisés au sein de l'entière du groupe OC-SANTE.

Grâce à Zabbix, les techniciens tout comme les administrateurs auront un meilleur aperçu et une meilleure surveillance de leur réseau. L'interface intuitive de l'application possède également de nombreux avantages. Elle permet un gain de temps considérable notamment au niveau de la visualisation des alertes qui sont affichées en détail sur l'écran de l'open space. Plus besoin de se connecter à EON (leur ancien logiciel de supervision), puis de naviguer dans les menus pour trouver quels sont les problèmes courant au sein du réseau. Désormais, un seul coup d'œil suffit pour cerner la globalité des problèmes.

Bien sûr, si un technicien souhaite obtenir plus d'informations liées à une machine ou une alerte, il aura toujours besoin de se connecter sur l'interface web de Zabbix. Cette dernière étant plus épurée, pratique et agréable que celle de EON.

L'évaluation de mon travail s'est faite tout au long de mon stage par les administrateurs qui étaient dans le même bureau que moi. Une démonstration finale a été planifiée et réalisée par mes soins lors de la réunion qui a eu lieu la dernière semaine de mon stage. Cette réunion a été l'occasion de valider ce que j'avais fait durant les 7 semaines de mon stage et de répondre aux éventuelles questions de toute l'équipe. De plus, un RDV a eu lieu avec mon tuteur, le responsable du pôle infrastructure et réseau pour un aperçu plus détaillé de toutes les fonctionnalités que j'avais mises en œuvre pour l'entreprise. Ce moment a aussi été l'occasion de remettre ma documentation personnelle et détaillée de Zabbix comprenant plus d'une vingtaine de pages.

Ainsi, le travail réalisé pendant la durée de mon stage ainsi que ma documentation ont été validés sans soucis.

Ayant eu très peu de cours sur l'infrastructure d'une entreprise (et peu de connaissances personnelles), il est clair que j'ai appris la plupart de mes compétences en réseau pendant la durée de mon stage. Le manque de connaissances était l'un des plus gros points à améliorer pour moi.

De plus, même si j'ai fourni un travail plus que suffisant de mi-mai à juillet, et que ma solution est fonctionnelle pour être mise en production immédiatement après mon départ, il y a toujours des améliorations à faire. Par exemple, le plus difficile a été pour moi de déterminer le nombre de ports disponibles pour les switches à partir de leur OID. Ce qui est normalement impossible. J'ai donc pensé à une solution alternative qui indique le nombre de ports qui n'ont pas été actifs (statut = down) pendant 60 jours. Cette simple information nécessite 4 éléments en plus pour une interface :

- La valeur qui indique si l'interface est active ou pas (up or down)
- La dernière valeur du uptime* depuis le changement de statut de l'interface
- Une autre valeur qui calcule depuis combien de temps ce changement a eu lieu en fonction du uptime actuel
- Et enfin un booléen* indiquant si l'interface est down depuis 60 jours ou pas.

En sachant qu'un seul hôte de type switch peut avoir 48*5 ports (un switch ayant au maximum 48 ports et étant stacké* avec 5 autres switches (le maximum pour OC-SANTE)), et que ces 4 valeurs supplémentaires s'appliquent pour tous les ports, cela

nous fait 960 éléments en plus pour un hôte juste pour obtenir le nombre de ports disponibles sur ce dernier. Cela crée une surcharge au niveau de Zabbix.

Donc les améliorations à fournir au niveau de la solution que j'ai rendue sont principalement des optimisations.

B – Compétences mises en œuvre

Tout au long de la durée de ce stage, j'ai dû mobiliser de nombreuses compétences. Etant dans le domaine infrastructure et réseau, il est évident que la majorité des compétences que j'ai mise en œuvre soient aussi de ce domaine. Cependant j'ai aussi pu appliquer mes connaissances en développement web et développement d'application. De plus, ma logique s'est avérée utile dans plus d'une situation.

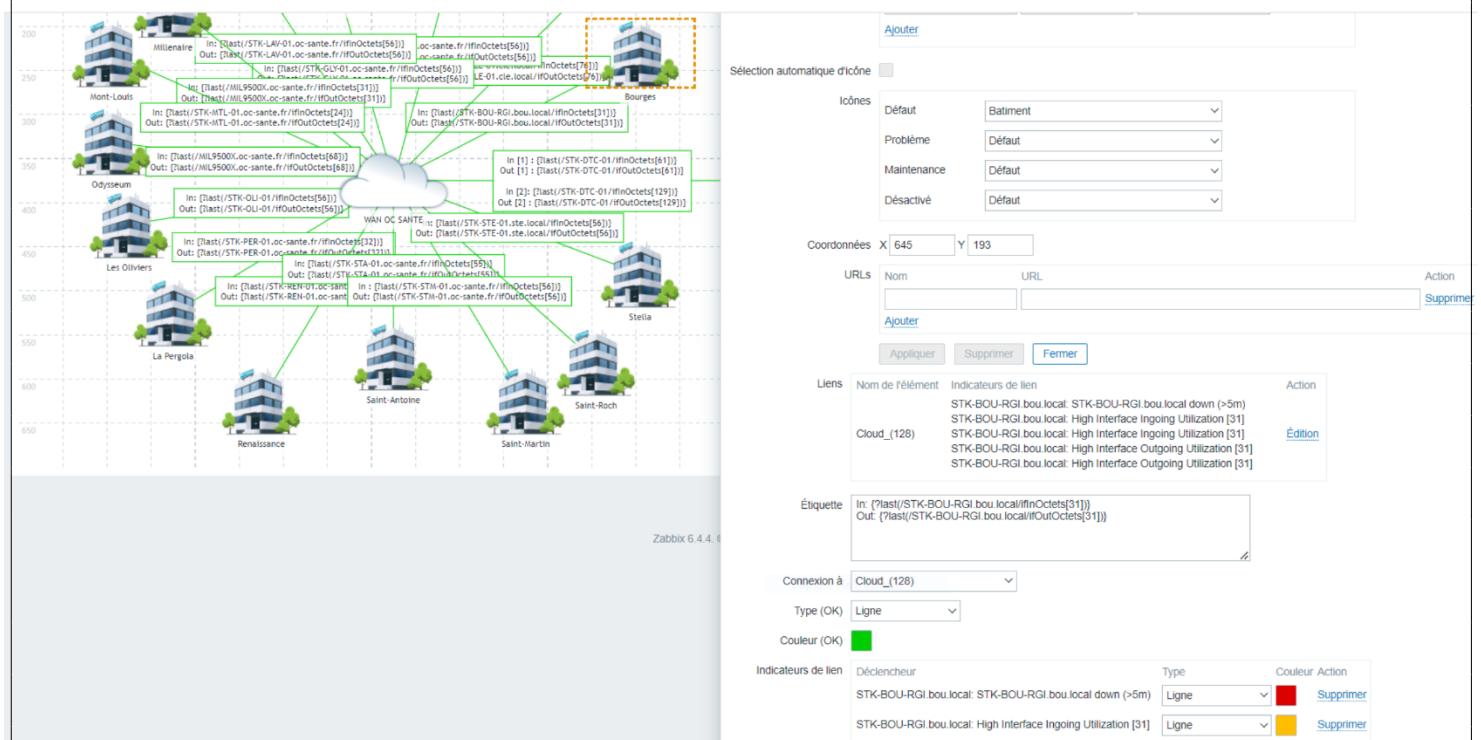
J'ai principalement exploité mes connaissances en Linux, langage shell, et infrastructure réseau d'une entreprise. Passant par la compréhension d'une adresse IP (masque de sous réseau, IPv4, IPv6, VLAN, etc...), du firewall (SNAT*, DNAT*, politiques du firewall, zones et groupes, etc...). Du côté de mes compétences en développement, j'ai pu manipuler du php et du css (Zabbix frontend).

A savoir que mes compétences en réseau lors de mon arrivée dans l'entreprise étaient difficilement suffisantes pour mener à bien les missions qui m'ont été confiées. J'ai donc dû apprendre beaucoup que ce soit en autonomie, en posant des questions ou en observant le travail de mes collègues. Chaque occasion durant ce stage était une opportunité pour moi d'en apprendre davantage sur le monde de l'informatique. Et j'ai énormément appris.

Par exemple, au début de mon stage, je n'y connaissais presque rien au protocole SNMP, ni aux OIDs, ni comment un logiciel de supervision faisait pour collecter des données relatives à d'autres appareils. Par le biais d'internet et des connaissances que m'ont transmises les administrateurs j'ai enfin compris cette notion. Ainsi j'ai appris que Zabbix interrogeait les appareils (switches) en SNMP sur le port 161 et que ces derniers fournissaient les bonnes valeurs (traps SNMP) en retour à Zabbix en fonction de l'OID spécifiée. Chaque OID fait partie d'une MIB (base de données) et que chaque modèle de switch possède sa MIB. Ainsi, pour une même valeur (par exemple la température), les OIDs peuvent différer d'un modèle de switch

à un autre. C'est ainsi que Zabbix va recueillir les données qui nous intéressent pour tous les switches.

A savoir que malheureusement, même si je disposais de compétences suffisantes pour installer et configurer correctement Zabbix, certaines fonctionnalités de ce logiciel m'ont demandé beaucoup d'effort qui auraient pu être évités si je disposais d'assez de connaissance. Certaines fonctionnalités ont même dû être abandonnées. Nous allons voir un exemple. J'ai réussi à afficher des cartes réseau avec le flux des données pour chaque switch et routeur.



(Exemple de configuration d'une carte réseau sur Zabbix)

L'image ci-dessus montre la configuration des flux (In/Entrant et Out/Sortant) de toutes les cliniques (plus précisément les routeurs) du groupe OC-SANTE. Les images de bâtiments (personnalisés avec le logo OC-SANTE dessus) représentent ces routeurs. D'emblée nous pouvons remarquer la complexité de la configuration d'une carte sur Zabbix. Malheureusement, l'apparence de ces cartes réseau ne me convenait pas. J'ai donc cherché comment la transformer pour avoir un style WeatherMap (avec des flèches entrantes et sortantes pour chaque lien) sans résultat. C'était impossible sur Zabbix, il fallait utiliser un plugin externe qu'il fallait entièrement configurer. Cela m'aurait pris trop de temps à faire par manque de connaissances. Heureusement que



les administrateurs m'ont dit que l'apparence des cartes que j'avais faites sur Zabbix étaient plus que satisfaisante et répondais à leur besoin. J'ai donc abandonné le projet.

Je suis encore loin d'atteindre le niveau que j'ai vu auprès des administrateurs réseau. Et ce, malgré le fait que je suis capable d'accomplir certaines de leurs tâches que même eux ne réussissent pas toutes leurs missions et doivent s'entraider et partager leurs connaissances. La majorité de leurs compétences sont appliquées auprès des solutions, des logiciels, des équipements et à l'infrastructure propres au groupe OC-SANTE. Les connaissances scolaires leur donnent juste de bonnes bases théoriques mais une grande partie de leur formation se fait au sein du groupe. J'ai pu le remarquer avec un nouvel administrateur qui a intégré l'entreprise au début de cette année et qui devait se faire épauler par un autre administrateur pour comprendre ses missions.

CONCLUSION

Pour conclure, mon stage en tant que technicienne réseau informatique au sein du groupe OC-SANTE a été une expérience extrêmement positive et enrichissante. J'ai eu l'opportunité de travailler en collaboration au sein de l'équipe informatique dans une entreprise à échelle nationale comprenant plus de 3000 salariés. Ainsi, j'ai pu mettre en pratique mes compétences tout en apprenant des nouvelles compétences dont le fait de travailler en entreprise, dans un secteur en lien avec mes études.

Au cours de mon stage, outre ma mission principale, j'ai été impliquée et j'ai observé plusieurs projets et tâches quotidiennes. Nous pouvons citer en exemple, la mise en production et la configuration de switches ou encore la gestion des VLANs de l'entreprise. J'ai également participé à la surveillance et à la résolution des problèmes liés aux équipements du réseau. Grâce à ces tâches, j'ai renforcé mes connaissances dans ce domaine ainsi que ma capacité à être logique, autodidacte et prendre l'initiative pour résoudre des problèmes plus ou moins complexes.

J'ai également eu l'opportunité de travailler en étroite collaboration avec les techniciens et les administrateurs du groupe, ce qui m'a permis de bénéficier de leurs conseils, de leur expertise et aussi observer leur métier et le travail qui leur est donné. Ma participation aux réunions d'équipe et aux interventions est un plus dont je suis satisfaite puisqu'ils m'ont permis de me procurer une immersion totale.

En réfléchissant à mon expérience de stage, je suis fière des réalisations que j'ai accomplies et des compétences que j'ai acquises. Ces derniers ont été bénéfiques pour moi et aussi pour OC-SANTE puisque ma mission principale leur a permis d'améliorer leur outil de supervision du réseau.

Ce stage a permis de consolider ma passion pour l'informatique et a confirmé mon choix de carrière dans ce domaine.

Pour l'avenir, je souhaite continuer mon BTS SIO, obtenir mon bachelor et viser un grade master (bac +5). Je n'ai pour l'instant pas d'idées précises concernant mon futur métier. J'espère que toutes mes interrogations concernant mon futur s'éclairciront au fur et à mesure de mon parcours scolaire et professionnel (stages).

Ainsi, je prévois de faire un stage orienté développement l'année prochaine pour le comparer avec le stage que j'ai effectué cette année et me décider sur l'orientation (développement ou réseau) de mes études. Et pourquoi pas réaliser ce stage dans une petite entreprise pour changer d'un grand groupe de santé tel que OC-SANTE. Mon objectif étant de découvrir un large éventail de possibilités avant de faire un choix décisif pour mon futur.

GLOSSAIRE

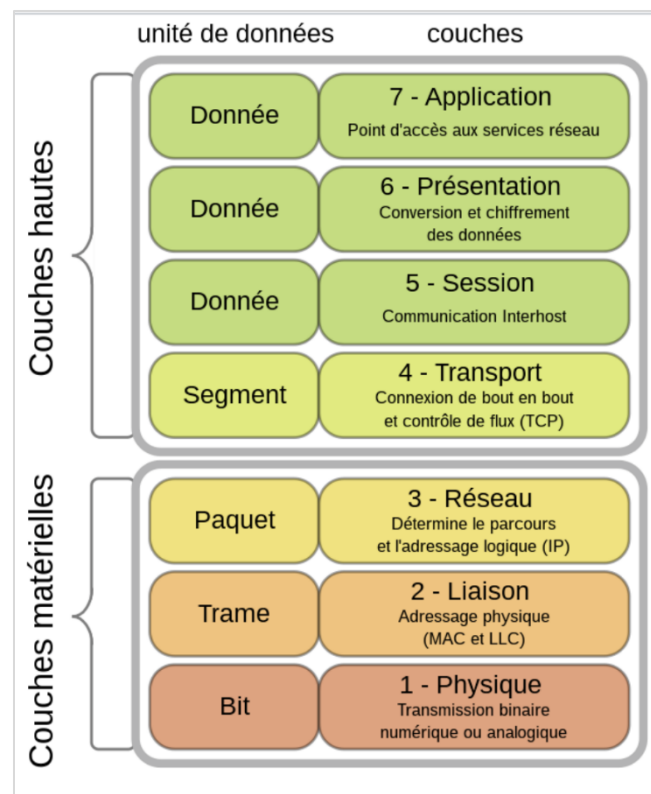
Astreinte : Une astreinte est une obligation de disponibilité (être joignable dans un délai d'une heure maximum pour l'astreinte informatique d'OC-SANTE) pendant laquelle un professionnel est prêt à intervenir en dehors des heures normales de travail en cas d'urgence ou de besoin de maintenance.

Switches : Également appelé commutateur. Il est utilisé pour relier plusieurs appareils informatiques au sein d'un réseau local (LAN). Il permet de transférer les données entre les différents périphériques connectés en analysant les adresses MAC et en créant des chemins directs pour une communication efficace.

La plupart des switches utilisés par OC-SANTE sont de niveau 2 (voir le modèle OSI ci-contre). En sachant que la plupart des cliniques de cette entreprise utilisent une topologie* en étoile.

Les switches ayant la fonction de cœur de réseau sont des switches de niveau 3 (pour le groupe OC-SANTE). C'est-à-dire qu'ils vont pouvoir gérer toutes les couches matérielles (Physique, Liaison, Réseau). Ces switches vont donc pouvoir faire du routage (adresses IP) contrairement à des switches de niveau 2 qui fonctionnent uniquement avec les adresses MAC.

Ce qui veut dire que seul une minorité des switches de l'entreprise vont pouvoir traire la couche 3 du modèle OSI. Principalement pour une question de budget.



VM : Virtual Machine (machine virtuelle en français). Il s'agit d'un environnement logiciel autonome qui émule les fonctionnalités d'un ordinateur physique. Une machine virtuelle est créée à l'aide d'un logiciel appelé hyperviseur (VMWARE vSphere pour OC-SANTE) qui divise les ressources matérielles de l'ordinateur physique en plusieurs environnements virtuels distincts. Chaque machine virtuelle dispose de ses propres ressources assignées (CPU, mémoire RAM, stockage, interfaces réseau).

Firewall : Pare-feu en français. C'est un dispositif de sécurité réseau qui contrôle et filtre le trafic entrant et sortant en fonction de règles (polices) prédéfinies applicables à tout le monde ou à certains groupes/certaines zones, protégeant ainsi le réseau contre les menaces potentielles et les accès non autorisés. La solution de pare-feu d'OC-SANTE s'appelle Fortinet.

Neticenter : Datacenter Netiwan. Netiwan est un opérateur de services et d'infrastructures proposant divers services comme : une connectivité Internet, optimisation VPN, Hébergement en Datacenter, etc...

Un datacenter quant à lui est un « centre de données ». C'est-à-dire une installation physique (un bâtiment) qui abrite des équipements informatiques et des infrastructures de stockage de données. Il fournit un environnement sécurisé et contrôlé pour héberger des serveurs, des systèmes de stockage, des équipements réseau et d'autres composants importants. Les datacenters sont conçus pour assurer une disponibilité élevée, une redondance des systèmes et une gestion efficace de la climatisation et de l'alimentation électrique.

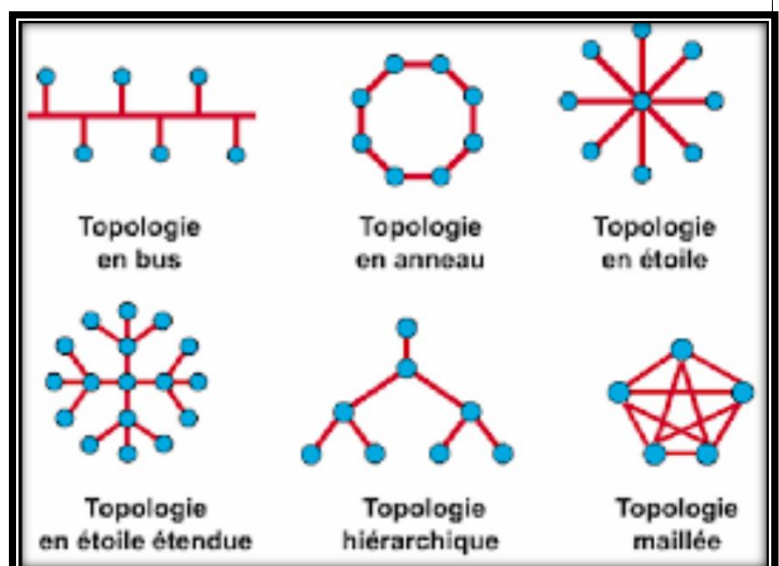
Le datacenter utilisé par OC-SANTE est partagé. Il fournit des services à plusieurs clients. Cependant, le groupe OC-SANTE dispose d'un espace qui lui est dédié au sein du Neticenter. On y retrouve leur cluster Fortinet, des switches (dont celui assurant la liaison du groupe avec le WAN (internet)) et d'autres équipements sensibles.

Topologies réseau : Une topologie réseau est la structure physique ou logique qui décrit la manière dont les appareils et les liaisons sont connectés dans un réseau informatique. Elle définit la disposition des nœuds, tels que les ordinateurs, les routeurs et les commutateurs, ainsi que les chemins de communication entre eux.

Voici un schéma montrant les topologies que l'on peut rencontrer, en sachant que les plus courantes sont les topologies en étoile, en anneau et en maillage.

On remarque que la topologie la plus efficace est la topologie maillée. Cependant, par soucis de budget, la topologie la plus répandue au sein du groupe OC-SANTE est la topologie en étoile.

Nous pouvons aussi retrouver des topologies hybrides. En effet, sur certains équipements sensibles ayant besoin de redondance, le groupe a intégré une topologie maillée venant s'intégrer sur une partie de leur topologie en étoile.



AD : L'AD ou Active Directory, est une solution centralisée de gestion des identités et des accès développée par Microsoft. Elle regroupe un ensemble de services et une base de données.

Concernant la base de données, l'AD stocke les informations d'authentification, les profils d'utilisateurs, les autorisations et les politiques de sécurité. Pour ce qui est des services, l'AD permet de gérer de manière efficace les comptes d'utilisateurs, les groupes, les ordinateurs et les ressources du réseau.

Ces services garantissent que chaque personne fournit son identité véritable (authentification), généralement en vérifiant l'ID utilisateur et le mot de passe saisi, et permettent aux utilisateurs d'accéder aux données pour lesquelles ils disposent d'autorisations.

GPO : Les GPO ou Group Policy Objects, sont des objets de stratégie de groupe utilisés dans les environnements Windows pour gérer et configurer les paramètres et les fonctionnalités des ordinateurs et des utilisateurs. Les GPO permettent aux administrateurs de définir des règles et des restrictions pour les utilisateurs et les ordinateurs au sein d'un domaine Active Directory.

Ils peuvent être utilisés pour gérer les politiques de sécurité, les paramètres du système, les applications, les droits d'accès, les scripts de connexion et de nombreuses autres configurations au niveau du réseau. Les GPO offrent un moyen puissant de contrôler et de maintenir une cohérence des configurations à grande échelle dans un environnement Windows.

To / Go : Unité de mesure de mémoire d'un ordinateur ou disque de stockage. A savoir qu'un To (téraoctet) est égal à 1024 Go (gigaoctets).

Uptime : L'uptime d'une machine désigne la durée pendant laquelle cette machine est restée en fonctionnement sans interruption ou panne. C'est la mesure du temps écoulé depuis le dernier redémarrage ou la dernière période d'indisponibilité.

A savoir que les VM du groupes OC-SANTE doivent être redémarrées tous les 30 jours maximums pour s'assurer qu'ils fonctionnent bien et qu'ils sont à jour (surtout au niveau des GPO appliquées au démarrage). Il est aussi vrai que les redémarrages réguliers peuvent aider à libérer les ressources système, à évacuer les fichiers temporaires et à maintenir les performances optimales des VM. Tandis que certains switches du groupe n'ont pas redémarré depuis des années.

Stacké : (en informatique). Du matériel stacké fait référence à un ensemble de matériels interconnectés de manière à fonctionner comme une seule entité logique. L'empilement (ou stacking) de matériel permet de combiner plusieurs appareils physiques tels que des switches en une seule unité gérée et configurée de manière centralisée. Lorsqu'ils sont empilés, les

machines partagent les ressources, les protocoles de gestion et les capacités de commutation. Cela simplifie la gestion du réseau et améliore les performances tout en assurant une redondance en cas de panne (ou dysfonctionnement) d'un ou plusieurs appareils.

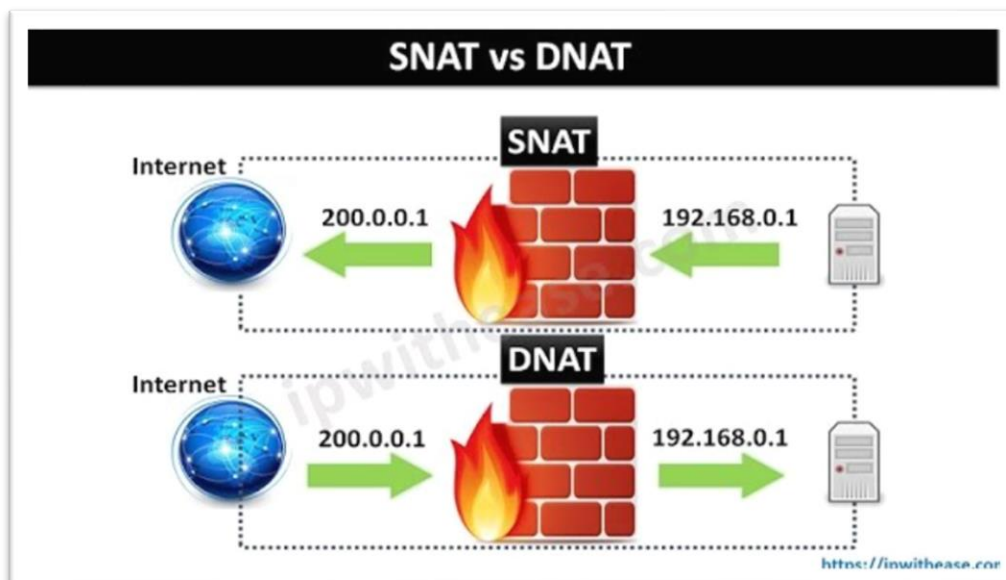
NAT (SNAT / DNAT) : Le NAT, ou Network Address Translation (traduction d'adresses réseau) est une technique utilisée pour convertir les adresses IP dans un réseau. Ces techniques de NAT sont largement utilisées pour gérer les adresses IP et faciliter la connectivité entre les réseaux privés et Internet.

Le SNAT (Source NAT) est une forme de NAT où l'adresse source d'un paquet IP est modifiée lorsqu'il traverse un pare-feu ou un routeur. Cela permet de masquer les adresses IP internes et de les remplacer par une seule adresse IP publique, permettant ainsi à plusieurs hôtes d'accéder à Internet à partir d'une seule adresse IP publique.

Par exemple, si on a un réseau local avec plusieurs ordinateurs, tous partageant une seule adresse IP publique, le routeur ou le pare-feu utilisera le SNAT pour remplacer l'adresse IP source des paquets sortants par l'adresse IP publique avant de les envoyer sur Internet. De cette manière, les réponses du serveur reviendront au routeur ou au pare-feu, qui utilisera ensuite le SNAT pour rediriger les paquets vers l'adresse IP locale appropriée.

Le DNAT (Destination NAT) est quant à lui une autre forme de NAT où l'adresse de destination d'un paquet IP est modifiée lorsqu'il traverse un pare-feu ou un routeur. Il est couramment utilisé pour rediriger le trafic entrant d'une adresse IP publique vers une adresse IP privée spécifique, permettant ainsi de rendre des services internes accessibles depuis Internet.

Voici un schéma illustrant ces termes :



ANNEXES

- **Détail de quelques-uns des modèles/templates d'hôtes que j'ai dû créer sur Zabbix**

Template Cisco Switch

Compatible avec la plupart des modèles de switch du réseau de l'entreprise

❖ **Éléments (16) : valeur (OID ou formule) :**

1. Uptime : sysUpTimeInstance
2. RAM(libre) : 1.3.6.1.4.1.9.9.48.1.1.1.6.1
3. RAM(utilisée) : 1.3.6.1.4.1.9.9.48.1.1.1.5.1
4. RAM :
$$\text{last}(\text{//cisco.switch.memory.used}) / (\text{last}(\text{//cisco.switch.memory.free}) + \text{last}(\text{//cisco.switch.memory.used})) * 100$$
5. Ping (paquets perdus) : icmpingloss[{HOST.IP},4,100,,2000]
6. Ping (latence) : icmpingsec[{HOST.IP},4,100,,2000]
7. Ping : icmping[{HOST.IP},4,100,,2000]
8. Nom : sysName.0
9. Nb Switch : sum(last_foreach{//cisco.switch.running[*]})
10. Nb Interfaces : count(max_foreach{//ifOperStatus[*],1d})
11. Nb Interfaces Up : sum(last_foreach{//ifOperStatus[*]})
12. Interfaces Disponibles (%) :
$$\text{last}(\text{//cisco.switch.interfaces.up}) / \text{last}(\text{//cisco.switch.nb.interfaces}) * 100$$
13. Nb Interface dispo : sum(last_foreach{//Disponible[*]})
14. CPU max : max(last_foreach{//cisco.switch.cpu.util[*]})
15. Temperature inlet max : max(last_foreach{//temp.inlet.[*]})
16. Temperature hotspot / outlet max : max(last_foreach{//temp.hotspot.outlet.[*]})

❖ **Déclencheurs / Alertes (13) :**

1. High CPU utilization (warning) : cpu > 80% pendant 5m (prototype de déclencheur)
2. High CPU utilization (high) : cpu > 90% pendant 5m (prototype de déclencheur)
3. High memory utilization (warning) : RAM > 80% pendant 5min
4. High memory utilization (high) : RAM > 90% pendant 5min
5. Host has been restarted (warning) : uptime < 600 (= 600s = 10min)
6. System name has changed (information) : change(nom) et len(last(nom)) > 0 pour éviter un déclenchement au moment de la création de l'hôte où la dernière valeur de nom est vide (len = 0)

7. Température is too high (warning) : max température inlet > 46°C
8. Température is too high (high) : max température inlet > 56°C
9. HOST.NAME down (désastre) : ping = 0 pendant 5min
10. Hotspot / Outlet Température is too high (warning) : > 105°C
11. Hotspot / Outlet Température is too high (high) : > 125°C
12. Peu d'interfaces disponibles (<10%) (warning) : interfaces down depuis 60j < 10 (%)
13. Peu d'interfaces disponibles (<5%) (moyen) : interfaces down depuis 60j < 5 (%)

❖ Découverte (5) :

➤ Network Interfaces

- Prototypes d'éléments (10) : OID :
 - Status Change (in systime) : 1.3.6.1.2.1.2.2.1.9.{#SNMPINDEX}.
Prétraitement multiplier par 0.01 (pour avoir la valeur en secondes)
 - Last change (of status in sec) : last(/cisco.switch.uptime) -
last(/StatusChange[{#SNMPINDEX}])
 - Interface Bits Out {#IFDESCR} : 1.3.6.1.2.1.31.1.1.1.6.{#SNMPINDEX}.
Prétraitement Changement par Sec + multiplier par 8 (octets -> bits)
 - Interface Bits In {#IFDESCR} : 1.3.6.1.2.1.31.1.1.1.10.{#SNMPINDEX}.
Prétraitement Changement par Sec + multiplier par 8 (octets -> bits)
 - Operational status of interface {#IFDESCR} : IF-
MIB::ifOperStatus.{#SNMPINDEX}. Prétraitement down(2) = 0, up(1) = 1 .
 - Description of interface : ifDescr[{#SNMPINDEX}]
 - Disponible : (last(/ifOperStatus[{#SNMPINDEX}]) -
1)*last(/LastChange[{#SNMPINDEX}]). Prétraitement : si disponible < -8640000
(60j) alors output = 0 sinon output = 1
 - Link speed : 1.3.6.1.2.1.31.1.1.1.15.{#SNMPINDEX} (vitesse max de
l'interface en bps). Prétraitement : *10000000
 - Ingoing utilization : last(/ifInOctets[{#SNMPINDEX}])/last(/LinkSpeed[{#SNMPINDEX}]) * 100 (bande passante en %)
 - Outgoing utilization : last(/ifOutOctets[{#SNMPINDEX}])/last(/LinkSpeed[{#SNMPINDEX}]) * 100 (bande passante en %)
- Prototypes de déclencheurs (4) :
 - High Interface Ingoing Utilization [{#SNMPINDEX}] (moyen) : min(/1- Cisco
switch/ifInUtilization[{#SNMPINDEX}],#2)>80
 - High Interface Ingoing Utilization [{#SNMPINDEX}] (high) : min(/1- Cisco
switch/ifInUtilization[{#SNMPINDEX}],#3)>90
 - High Interface Outgoing Utilization [{#SNMPINDEX}] (moyen) : min(/1- Cisco
switch/ifOutUtilization[{#SNMPINDEX}],#2)>80
 - High Interface Outgoing Utilization [{#SNMPINDEX}] (high) : min(/1- Cisco
switch/ifOutUtilization[{#SNMPINDEX}],#3)>90

➤ Switches Number (pour voir s'il y a des switches stackés et combien fonctionnent)

- Prototypes d'éléments (1) : OID :
 - Running : 1.3.6.1.4.1.9.9.500.1.2.1.1.6.{#SNMPINDEX}. Prétraitement si running = 4 alors output = 1, sinon output = 0
 - CPU discovery (car l'OID CPU pose problème pour certains switches)
 - Prototypes d'éléments (1) : OID :
 - CPU : 1.3.6.1.4.1.9.9.109.1.1.1.1.8.{#SNMPINDEX}
 - Prototypes de déclencheurs (2) : OID :
 - High CPU utilization (warning) : cpu > 80% pendant 5m
 - High CPU utilization (high) : cpu > 90% pendant 5m
 - Température outlet/hotspot discovery (relève les valeurs de temperature outlet/hotspot du/des switch(es))
 - Prototypes d'éléments (1) : OID :
 - Running : 1.3.6.1.4.1.9.9.13.1.3.1.3.{#SNMPINDEX}
- Avec 2 filtres sur {#TEMPDESCR} (1.3.6.1.4.1.9.9.13.1.3.1.2) = [H][o][t][s][p][o][t]
{#TEMPDESCR} (1.3.6.1.4.1.9.9.13.1.3.1.2) = [O][u][t][l][e][t]
- Température inlet discovery (relève les valeurs de temperature inlet du/des switch(es))
 - Prototypes d'éléments (1) : OID :
 - Running : 1.3.6.1.4.1.9.9.13.1.3.1.3.{#SNMPINDEX}
- Avec un filtre sur {#TEMPDESCR} (1.3.6.1.4.1.9.9.13.1.3.1.2) = [I][n][l][e][t]

❖ **Graphiques (4) :**

- CPU
- RAM
- Température
- Ping (0 ou 1)

❖ **Tableau de bord (1) :**

- Récapitule l'ensemble des graphiques ci-dessus dans un dashboard

Template OCS Windows Zabbix Agent

Utilisé pour monitorer les VM Windows par le biais d'un agent Zabbix installé.

❖ **Eléments (31), agent Zabbix donc pas d'OID mais des formules internes à Zabbix :**

- Cache bytes
- Context switches per second
- CPU DPC time
- CPU interrupt time
- CPU privileged time
- CPU queue length
- CPU user time
- CPU utilization
- Free system page table entries
- Get filesystems
- Host name of Zabbix agent running
- Memory page faults per second
- Memory pages per second
- Memory pool non-paged
- Memory utilization
- Network interfaces WMI get
- Number of cores
- Number of processes
- Number of threads
- Operating system
- Operating system architecture
- System description
- System local time
- System name
- Total memory
- Total swap space
- Uptime
- Used memory
- Version of Zabbix agent running
- Zabbix agent availability
- Zabbix agent ping

❖ **Déclencheurs (14) :**

- CPU interrupt time is too high : warning (5m)
- CPU privileged time is too high : warning (5m)
- CPU queue length is too high : warning (5m)
- High CPU utilization : warning (5m)
- High CPU utilization : high (5min)

- High memory utilization : warning (3m)
- High memory utilization : high (5m)
- Host has been restarted : warning
- Number of free system page table entries is too low : warning (5m)
- Operating system description has changed : information
- System name has changed : information
- System time is out of sync : warning (last value)
- The Memory Pages/sec is too high : warning (5m)
- Zabbix agent is not available : medium (last value)

❖ **Découverte (3), elles sont identiques aux modèles d'origine de Zabbix concernant les VM :**

- Network Interfaces discovery
- Physical disks discovery
- Windows services discovery (disabled) car trop de « fausses alertes » (déclencheurs)