

MEMOIRE

DE

FIN D’ETUDES 3iL

**DEGBOGBAHOUN TOYIN**

**2016-2017**

**Tuteur Enseignant : Mr Abdelhadi MIFDAL**

**Tuteur de stage : Mr Stéphane SANCHEZ**

*Remerciements*

Je souhaite tout d’abord adresser, ici, tous mes remerciements aux personnes qui m'ont apporté leur aide pendant ce stage de fin d’études, ainsi qu’à ceux qui ont contribué à l'élaboration de ce rapport.

En premier lieu Monsieur Pedro LUCAS, Directeur géneral de Netplus, pour m’avoir donné l’opportunité d’effectuer mon stage au sein de son organisation.

Je remercie tout particulièrement mon tuteur de stage, Monsieur Stéphane SANCHEZ, Directeur des opérations de Netplus, pour son aide, ses conseils et le temps qu’il a su me consacrer. Son suivi m’a permis de monter en compétences aussi bien que dans le domaine technique que dans la gestion de projet.

Je remercie également toute l’équipe technique et commerciale de Netplus pour son accueil et son investissement durant ma période de stage, en particulier Monsieur Kevin RIVRAIN, Ingénieur Systèmes et Réseaux, pour son accompagnement lors de la réalisation de mon projet.

Je n’oublie pas de remercier aussi Monsieur MIFDAL, mon maître de stage, ainsi que tout le corps enseignant de 3iL pour leurs interventions durant mon cycle de formation.

Sommaire

[1 INTRODUCTION - 3 -](#_Toc490674830)

[1.1 Préambule - 3 -](#_Toc490674831)

[1.2 Confidentialité - 3 -](#_Toc490674832)

[1.3 Environnement - 3 -](#_Toc490674833)

[1.3.1 La société - 3 -](#_Toc490674834)

[1.3.2 Netplus : acteur spécialisé dans l’hébergement de données de santé - 4 -](#_Toc490674835)

[1.3.3 Présentation de la solution d’hébergement - 5 -](#_Toc490674836)

[1.3.4 Le contexte HDS - 5 -](#_Toc490674837)

[1.3.5 Organigramme de l’équipe Netplus - 9 -](#_Toc490674838)

[1.3.6 Stratégie de l’entreprise - 10 -](#_Toc490674839)

[2 RAPPORT DE STAGE - 11 -](#_Toc490674840)

[2.1 L’environnement technique - 11 -](#_Toc490674841)

[2.2 Le projet client : Sodexo - 13 -](#_Toc490674842)

[2.2.1 Présentation - 13 -](#_Toc490674843)

[2.2.2 Suivi projet - 14 -](#_Toc490674844)

[2.3 Le projet interne : Supervision - 18 -](#_Toc490674845)

[2.3.1 Qu’est-ce que c’est la supervision ? - 18 -](#_Toc490674846)

[2.3.2 Problématique - 19 -](#_Toc490674847)

[2.3.3 Suivi projet - 21 -](#_Toc490674848)

[2.3.4 Conclusion - 29 -](#_Toc490674851)

[3 L’INDUSTRIALISATION DU SI - 30 -](#_Toc490674852)

[3.1 Présentation - 30 -](#_Toc490674853)

[3.1.1 Problématique - 31 -](#_Toc490674854)

[3.1.2 L’automatisation - 31 -](#_Toc490674855)

[3.1.3 L’orchestration - 32 -](#_Toc490674856)

[3.2 L’industrialisation appliqué à la supervision - 33 -](#_Toc490674857)

[3.2.1 Présentation de l’outil Ansible - 33 -](#_Toc490674858)

[3.2.2 Supervision proactive - 35 -](#_Toc490674859)

[4 Conclusion Générale - 37 -](#_Toc490674860)

# INTRODUCTION

## Préambule

Depuis quelques années, nous constatons une forte croissance de la numérisation dans plusieurs corps de métiers comme celui de la banque, de l’assurance et maintenant de la santé.

Les innovations technologiques comme les objets connectés, la télésanté, l’intelligence artificielle ou encore le social engineering envahissent le monde de la santé.

Dans le cadre de la santé numérique ou de l’E-Santé, la digitalisation ne se limite plus à des fonctions administratives, mais touche désormais le cœur du métier.

Ainsi la gestion des données de santé et leur interopérabilité constituent un enjeu important dans l’ère du numérique.

## Confidentialité

Au regard du projet de supervision qui recouvre et parcourt tout le système d’informations de la société Netplus, certains documents qui seront fournis ou présentés dans le cadre de mon mémoire sont soumis à une totale confidentialité.

## Environnement

### La société

Créer en 1996, Netplus est aujourd’hui un acteur reconnu de l’hébergement, du -SaaS-Service as a Structure et du -Cloud Computing-. En 2013, l’entreprise fait le choix de se positionner sur le secteur de la santé et est agréée hébergeur de données de santé à caractère personnel –HADS-. Compte tenu de cet agrément, d’une durée de 3 ans renouvelable, l’entreprise se doit d’effectuer une revue annuelle pour évaluer sa conformité. D’ici 2018, l’entreprise devra évoluer dans un environnement ISO 27001 pour conserver son agrément.

En tant qu’hébergeur HADS, Netplus est le partenaire technique de la stratégie cloud et d’hébergement critique des entreprises et des administrations de la santé. Elle propose une prestation d’infogérance adaptée à chacun. Celle-ci a mis en place des méthodes et une architecture visant à atteindre la plus grande qualité de service : plan de continuité d’activité -PCA-, architecture multi site actif-actif, traçabilité, sécurité, confidentialité.

La société propose ses services à la fois aux éditeurs de logiciels -SaaS- mais aussi à des acteurs du secteur de la santé tels que : les laboratoires, les groupes pharmaceutiques, les assurances et mutuelles et aussi des particuliers. Pour ce faire, elle a bâti plusieurs partenariats avec des entreprises comme OpenStack, VmWare, Oracle spécialisées dans les services du cloud.

### Netplus : acteur spécialisé dans l’hébergement de données de santé

Figure 1 : L’évolution de Netplus

### Présentation de la solution d’hébergement

Netplus propose un service conforme aux dispositions de l’agrément pour l’hébergement de données de santé à caractère personnel. Le cœur de l’infrastructure d’hébergement est réparti sur deux sites et s’appuie sur un plan de continuité d’activité garantissant une haute disponibilité du service.

Le service d’hébergement de données de santé proposé par la société est destiné aux éditeurs de logiciels traitant des données de santé à caractère personnel et souhaitant délivrer à leur client une application en mode SaaS.

Les typologies d’utilisateurs finaux des applications hébergées sont :

* Personnels de santé manipulant des données produites ou recueillies à l’occasion des activités de soins, de préventions, de diagnostics.
* Eventuellement, Patients accédant exclusivement à ses données de santé.

Le service d’hébergement de données de santé à caractère personnel comprend :

* L’hébergement -PCA-, Plan de Continuité d’Activité, multi-site est entièrement redondé dans nos deux centres serveur,
  + Centres de serveur de niveau Tier 3+, certifiés ISO 27001
    - Netplus - Equinix PA2, 114 rue Ambroise Croizat, 93200 Saint Denis
    - Netplus - Equinix PA3, 114 rue Ambroise Croizat, 93200 Saint Denis
* L’infogérance Système et réseaux de la plateforme d’hébergement
* Un dispositif de sauvegarde et d’archivage des données conforme aux dispositions légales en vigueur
* Un -SLA-, Service Level Agreement, de 99,9% hors période de maintenance contractuelle.

### Le contexte HDS

Les contraintes pour l’obtention de l’agrément HDS se traduisent par toutes les mesures à entreprendre par l’hébergeur pour répondre aux exigences de l’-ASIP- Agence française de la santé numérique.

Avant tout, il s’agit d’avoir le consentement du patient. Netplus reporte donc cette obligation contractuellement sur le responsable de traitement et l’éditeur de logiciel qui doit au préalable demander l’accord du patient pour l’usage de ses données de santé.

Concernant la politique du contrôle d’accès, la gestion des habilitations des professionnels de santé est du ressort du client. Celui-ci est tenu d’utiliser un dispositif d’authentification forte au niveau de l’accès à l’applicatif. Netplus assure quant à elle la mise en place d’un système d’authentification à double facteurs pour l’accès aux serveurs de la plateforme.

Afin d’établir un périmètre de sécurité Netplus doit s’acquitter de certaines exigences qu’on peut résumer en quatre termes : disponibilité, intégrité, confidentialité, traçabilité.

|  |  |
| --- | --- |
| **Disponibilité** | Selon le contrat de services, Netplus garantit l’accès aux plateformes. La disponibilité doit être supérieure ou égale à 99,9%. |
| **Intégrité** | Elle garantit que les données échangées sont exactes et complètes. |
| **Confidentialité** | La confidentialité des données doit être totale : seules les personnes autorisées peuvent accéder aux données et aux ressources. |
| **Auditabilité** | L’audibilité doit permettre de conserver toute trace d’accès, des tentatives d’accès et des actions sur les plateformes. |

Ainsi, la bonne conformité des éléments ci-dessous,est une obligation pour répondre aux exigences HDS en termes de sécurité notamment lors du déploiement d’une plateforme client et fait mention tout particulièrement des mesures à prendre par chaque partie.

* Sous la responsabilité du client
* Les comptes permettant un accès privatif ou administratif à l’application sont nominatifs et individuels.
* Les mots de passe utilisés pour se connecter aux serveurs respectent un certain niveau de complexité.
* La mise en place d’une double authentification ou d’une authentification forte.
* Le changement des mots de passe d’accès à l’application à une fréquence régulière définie avec une politique de gestion d’historique.
* La présence d’une note d’information pour les utilisateurs finaux : les patients doivent être informés de leurs droits d’accès à leurs données personnelles de santé.
* Sous la responsabilité de Netplus
* Les accès au système se font via des protocoles sécurisés.
* Seuls les ingénieurs système et réseau de Netplus - Cloud Santé ont accès aux serveurs de la plateforme.
* Les accès aux serveurs de la plateforme se font exclusivement à partir de comptes nominatifs et individuels.
* Les mots de passe utilisés pour se connecter aux serveurs respectent un certain niveau de complexité.
* Le changement des mots de passe d’accès à l’application à une fréquence régulière définie avec une politique de gestion d’historique.
* Toutes les commandes exécutées sur le système lors d’une session sur les serveurs de la plateforme sont enregistrées et conservées sur un serveur de log distant.
* Limitation du nombre de packages installés lors du déploiement des plateformes : Il s’agit de vérifier que seuls les packages nécessaires au fonctionnement de l’application ou à l’exploitation de la plateforme ont été déployés.
* Limitation des services actifs sur les systèmes : Il s’agit de vérifier que seuls les services nécessaires au fonctionnement de l’application ou à l’exploitation de la plateforme sont actifs.
* L’absence d’outil de compilation sur les serveurs.
* Une sauvegarde quotidienne, hebdomadaire et mensuelle des données et des applicatifs de la plateforme est mise en place.
* Un mécanisme de haute-disponibilité est en place sur tous les éléments de la plateforme (pour les frontaux comme les backends).
* Sous la responsabilité du médecin traitant (obligation HDS)
* Accès aux données la donnée de santé en cas d’incident et de demande d’un patient

### Organigramme de l’équipe Netplus

Figure 2 : L’organigramme de Netplus

### Stratégie de l’entreprise

Dans le cadre de la procédure d’agrément des hébergeurs de données de santé à caractère personnel précisée par le décret du 4 janvier 2006, 96 décisions d’agrément ont à ce jour été rendues, par le ministre en charge de la santé.

Ainsi, le premier élément de la stratégie Netplus, est de consolider son positionnement dans la niche de l’hébergement de données de santé en mettant en avant ses services d’hébergement et de consulting dans le déploiement des plateformes-clients.

Mais aussi, en proposant une gamme étendue de services adaptés aux besoins de la santé connectée comme la –télésanté-, le stockage d’examens, le coffre-fort numérique santé, le stockage objet, l’archivage.

Netplus ambitionne aussi d’offrir de nouveaux services innovants à forte valeur ajoutée par le biais des projets d’entreprise comme le Big Data pour les données de santé ou encore des logiciels de santé connecté,-PRM-.

D’autre part l’intégrité et la sécurité sont au cœur de la stratégie d’entreprise car cela permet non seulement de fidéliser ses clients actuels, mais permet aussi d’évoluer dans un environnement serein au vu de la multiplication des cyber-attaque dernièrement.

# RAPPORT DE STAGE

J’ai eu au cours de mon stage l’opportunité de participer à plusieurs missions. Notamment le suivi d’un projet client pour une mise en conformité HDS, la gestion des incidents au niveau du support et bien sur ma mission de stage : la refonte de l’outil de supervision.

Dans cette partie, je présenterai les différentes tâches que j’ai eu à effectuer au sein de chaque mission tant sur le plan technique que sur la gestion de projet, mes apports et aussi les difficultés rencontrées.

Auparavant, il est important de présenter l’environnement dans lequel ces missions se sont effectuées.

## L’environnement technique

Le système est accessible à nos différents clients depuis Internet au travers de plusieurs opérateurs de transit et de divers équipements.

* Routeurs
* Pare-feu
* SLB –Server Load Balancing-
* Baies de stockage

**Le routeur** permet de rediriger les flux entrant et sortant vers le cluster de pare-feu. On dispose de 3 connexions internet permanentes fournis par 3 opérateurs différents pour assurer la continuité du service. Il permet de rediriger les flux concernant un client sur son propre -Vlan-.

**Le cluster de pare-feu** gère toutes les règles de sécurité du réseau en définissant les protocoles et types de communication. Il est composé de deux -V-sys- complètement hétérogènes. Le premier se charge des règles de communication entre l’extérieur et la –DMZ-, pour tous les équipements situés en front et middle-end, ces règles concernent principalement les flux web et mail. Le deuxième système se charge des règles entre la DMZ et la zone HDS, pour tous les équipements en back-end : bases de données, les serveurs de sauvegardes et de logs.

**Les SLB** hébergent les adresses IP publiques liées aux applications, ainsi que les certificats délivrés par les autorités de certification pour les flux HTTPS.

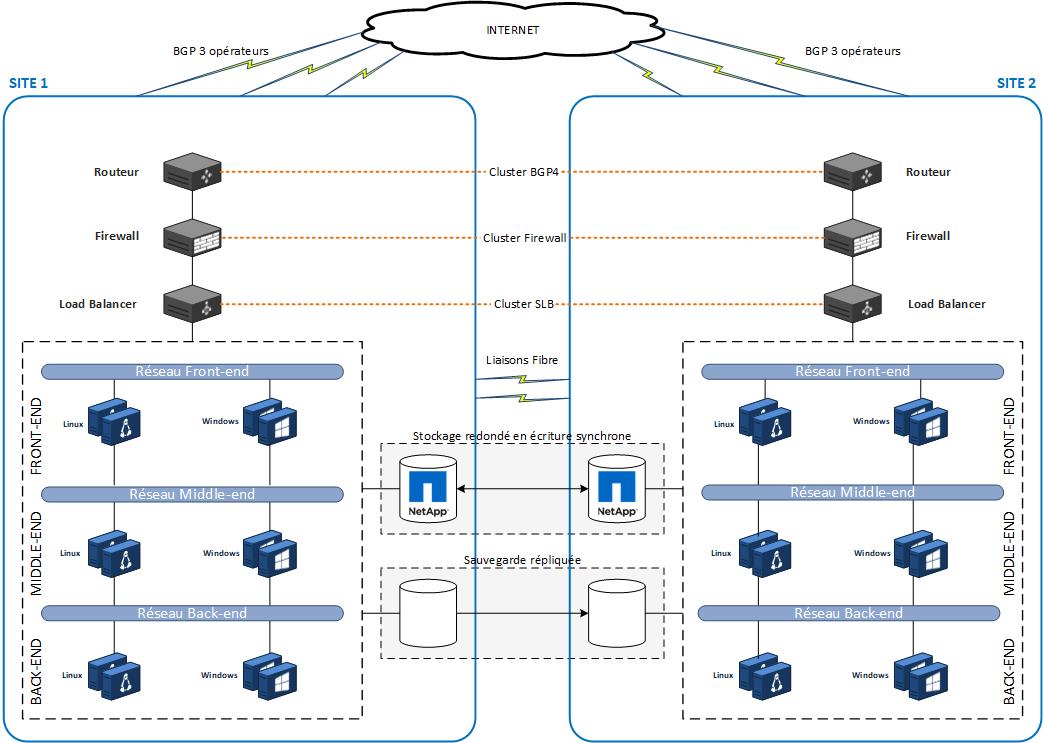
**Les baies de stockage** quant à elles conservent toutes les données applicatives et de bases de données. Les données sont stockées sur un volume -SAN-. Ce type de volume permet une bonne qualité de service puisque couplée à des liaisons fibres, elle garantit un débit entre 8 et 10 Gbit pour la transmission des données. Elle assure la redondance et peut fonctionner sur des environnements différents : Windows, linux et Unix. Elle permet ainsi d’assurer une synchronisation transparente et immédiate entre les serveurs web (applicatifs) et de BDD. Chaque client a une instance qui tourne sur un nœud du cluster de base de données. Il est donc relativement aisé de monter à l’échelle en ajoutant des nœuds au système de cluster et de répartir les bases de données clients sur les différents nœuds de ce cluster.

Figure 3 : Architecture de Netplus

En parallèle de ces mécanismes fonctionnels directement reliés au service, un système de statistiques, de sauvegarde et d’analyse est implémenté, à la fois au niveau des frontaux et des bases de données, et ce sur des serveurs dédiés.

Les plateformes de production et de pré-production sont redondés. C’est sur cette pré-production que les mises à jour système et applicative sont testées et validées avant d’être appliqués sur la production.

L’ensemble de ces services système, réseau, applicatif sont supervisés par un outil interne de supervision et un autre externe afin d’avoir une disponibilité de la surveillance en cas de défaillance de l’outil initial. Le but étant d’alerter l’équipe d’infogérance au moindre comportement anormal sur l’ensemble des serveurs et des équipements.

Une –métrologie- est aussi appliquée afin d’avoir des graphiques sur le débit, la latence des flux. La métrologie sert aussi à la facturation en fonction du contrat auquel aurait souscrit le client.

Les applicatifs déployés par Netplus, sont fournis par les clients. Ceux-ci précisent aux équipes de Netplus les modalités de déploiement et de test des nouvelles versions applicatives.

Les clients et Netplus communiquent via un outil de ticket, afin de tracer et de suivre toutes les demandes effectuées.

## Le projet client : Sodexo

### Présentation

La société Sodexo avait comme projet la mise en place d’une application dédiée à l’individualisation et la distribution de repas aux résidents des établissements de santé. L’applicatif permet, après une phase d’observation des habitudes alimentaires de chaque patient, de proposer des menus adaptés aux besoins de chacun.

Le projet était triparti. D’une part, Sodexo l’initiateur du projet, Télécom Santé entreprise spécialisée dans l’accompagnement numérique des établissements de santé et Netplus pour l’hébergement de l’applicatif et des données.

Le projet était intéressant, avec une difficulté abordable pour un premier projet puisqu’il s’agissait du déploiement de deux serveurs : applicatif et BDD avec une architecture assez simple.

J’ai pu assister aux différentes phases du projet de la signature du contrat HDS au passage en exploitation.

### Suivi projet

Le projet s’est déroulé sur une période d’un mois.

1. Workshop Technique

Durant cette phase, il a fallu convenir des spécificités techniques des deux serveurs et de la faisabilité du déploiement. L’application est composée de deux containers sous Docker et une base de données SQL Server sur Windows. Même si j’ai déjà entendu parler de Docker j’ai approfondi mes recherches personnelles pour comprendre au mieux cette technologie. L’architecture suivante a été proposée et validé par le client pour le déploiement.

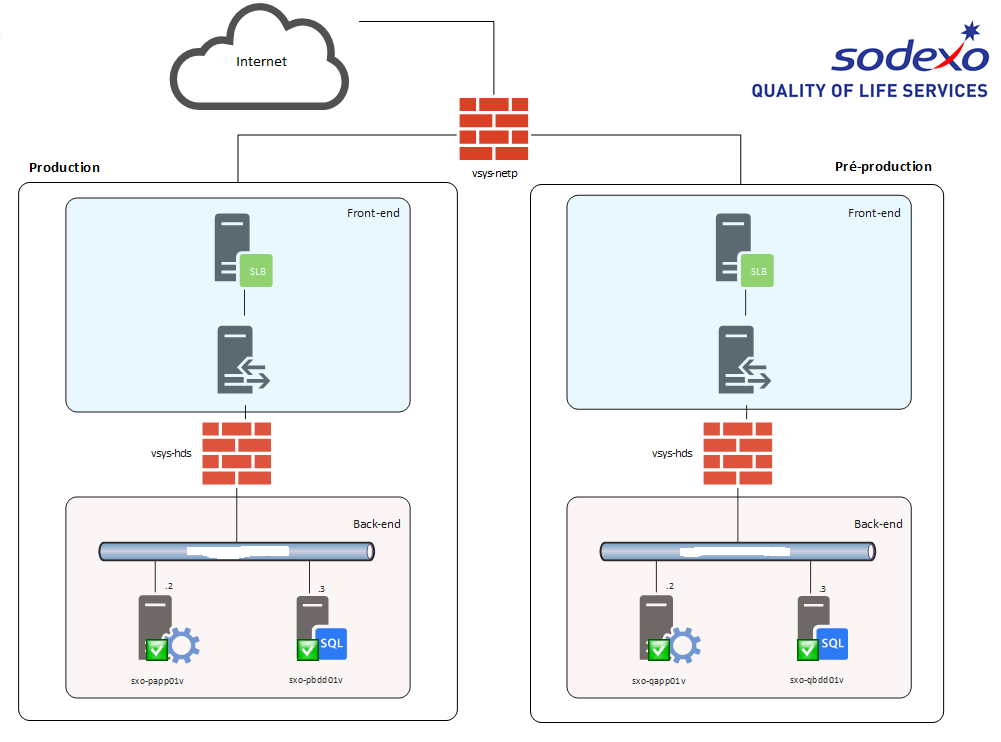


Figure 4 : Architecture client Sodexo

1. Plateforme de Pré-production

Une fois le périmètre établi, j’ai commencé à installer les machines de pré-production à partir des templates sur le VMware. Une machine linux pour l’application et une Windows pour la base de données.

Suite à la livraison des conteneurs, j’ai pu tester que tous les services nécessaires étaient fonctionnels et que les conteneurs fonctionnaient correctement sur les machines. Et tester que l’application discutait bien avec la base de données. Après cette phase j’ai pu passer à la production.

1. Plateforme de Production

Etant donné que les services fonctionnaient correctement sur la pré-production. Je suis passé à la mise en conformité HDS des deux machines en respectant les règles métier.

* Installation

Une fois les machines installées avec toutes leurs composantes, je les ai mis dans des vlans cloisonnés. Je suis intervenu sur chaque équipement réseau pour rendre accessible l’application depuis l’extérieur. A commencer par la mise en place d’un certificat SSL pour le serveur web NGINX. J’ai dû générer le -CSR- en fonction des informations fournies par le client et commander le certificat. Une fois le certificat reçu il fallait le mettre en place sur le SLB et configurer le serveur web pour n’accepter que des flux en HTTPS ou rediriger les flux HTTP en HTTPS de manière transparente. Le serveur web faisait office aussi de reverse proxy pour simplifier l’architecture. Une fois la matrice des flux construite, j’ai configuré le pare-feu pour établir les règles nécessaires de communication.

* Sauvegarde

Selon les règles métier, nous devons mettre en place une sauvegarde des serveurs, toutefois, l’application étant sous forme de conteneurs, je n’ai pas mis en place la sauvegarde du serveur applicatif étant donné que c’est la société Télécom Santé qui gère les images des containers.

Par contre pour le serveur de BDD, une sauvegarde des bases a été mise en place avec le logiciel Bareos. Bareos est un logiciel de sauvegarde et de restauration de fichiers en mode client-serveur dans un réseau, distribué en Open Source.

* Log centralisé

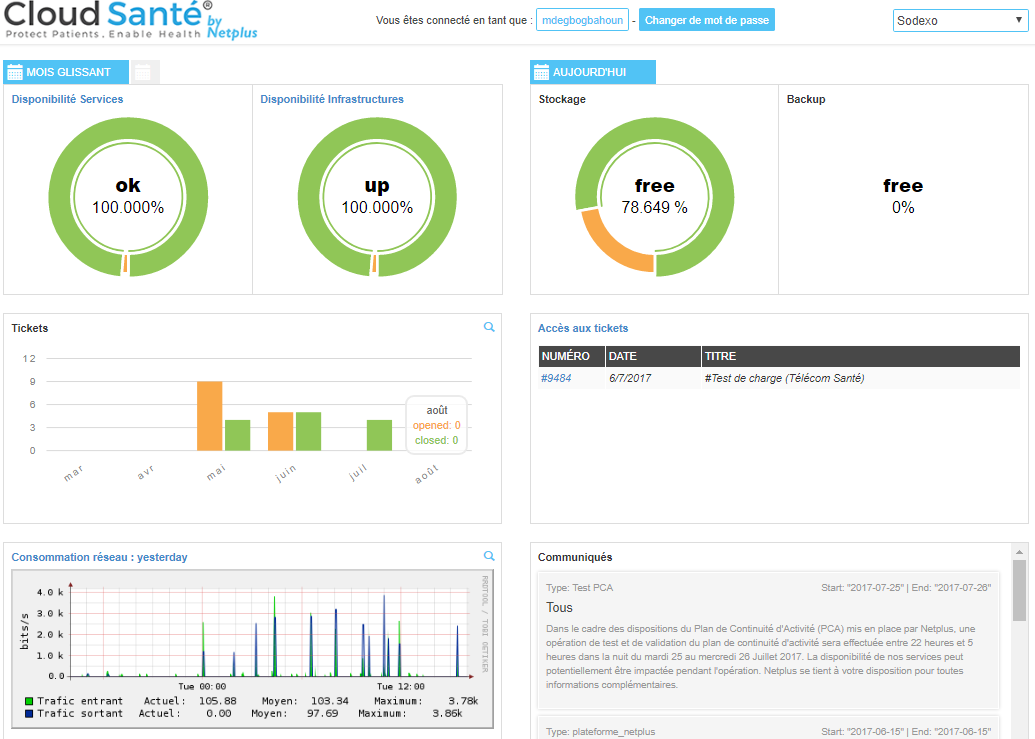
A chaque déploiement, en plus des logs locaux on se doit de conserver les logs sur un autre emplacement afin d’avoir une trace et pouvoir les exploiter en cas de problèmes sur la machine. Ainsi les logs concernant l’application, du proxy, et de la machine ont été exportés.

* Supervision

La supervision des machines ont été faits sur Nagios. En plus des check habituels de la machine (RAM, CPU, DISK) et des processus (-NTP,Auditd,SSL-), j’ai mis en place des check spécifiques à Docker pour surveiller l’état des processus. En effet il existe un plugin sur le site de Nagios Exchange (Plateforme d’échanges de sondes) permettant de surveiller un container, le défaut de cette sonde est qu’elle retournait l’état global du conteneur. En effet s’il existe plusieurs processus dans le conteneur, l’arrêt d’un des processus générait comme alerte, l’arrêt du conteneur. Ainsi j’ai adapté le plugin pour qu’il ne retourne que l’état du processus comme l’avait spécifié le client.

* Recette

Une fois tous ces éléments en place, ainsi que la documentation pour le reste de l’équipe, j’ai créé les accès pour le portail de support et le portail client dont voici un aperçu.

Figure 5 : Portail client Sodexo

Le projet a été bien accueilli par le client, on a eu des retours positifs en phase de running et lors des échanges pour le support. Le projet en soi ne présentait pas une énorme difficulté mais il m’a fallu un peu de temps d’un point de vue technique pour comprendre les fonctionnalités de chaque équipement en détail. Mais à la fin j’ai pu constater que même si mes tâches étaient différentes, elles formaient un tout, parfois pas forcement visible par l’utilisateur final.

## Le projet interne : Supervision

### Qu’est-ce que c’est la supervision ?

Depuis plusieurs années, la supervision est un outil incontournable pour tous les systèmes d’informations. Un système d’informations peut parfois mal fonctionner et causer de sérieux dégâts tant sur le plan technique que sur le plan commercial à l’entreprise. Ainsi avec un outil de supervision efficace, l’entreprise peut anticiper les pannes récurrentes et être proactifs sur divers évènements. La supervision permet donc d’avoir une vision globale sur le SI, mais aussi offre la possibilité d’auditer les systèmes, surveiller leur disponibilité, alerter et reporter les responsables du SI.

Concernant le principe de fonctionnement, l’outil de supervision dispose de sondes appelées généralement des checks pour évaluer l’état d’un équipement ou d’une application. Ces sondes, pour la plupart des scripts, sont exécutés sur les équipements supervisés via plusieurs protocoles, notamment le protocole –SSH- ou bien souvent le protocole natif –SNMP-.

Toutefois le choix du protocole utilisé dépendra du check qu’on voudrait réaliser. Par exemple, dans le cas de la vérification d’une page internet, une requête via le protocole –HTTP- suffit pour déterminer si une page internet est bel et bien active avec un temps de réponse qui peut être retourné. Ou encore pour vérifier si un hôte est actif ou non, un check via le protocole –ICMP- nous permet de connaitre son état.

Dans le cas du SNMP, le snmp est un protocole présent sur une très grande majorité des équipements, une fois le service activé sur l’équipement ,le protocole interroge les –OID- présents dans la –MIB- de chaque équipement et permet de recueillir et remonter des informations sur le matériel, la performance et aussi les statiques de chaque composant ou application.

L’avantage du SNMP réside dans le fait qu’il n’ait plus besoin d’installer des agents supplémentaires propriétaires sur l’hôte à surveiller telle que les démons -NRPE- avec Nagios ou encore – Zabbix Agent-. Le protocole permet d’établir une certaine sécurité à condition d’utiliser les versions 2 ou 3 et en mettant un nom de communauté, ainsi on restreint la portée des personnes pouvant interroger les hôtes via le SNMP.

Figure 6 : Le protocole SNMP en polling

### Problématique

Dans le cadre de l’infogérance, nos différents clients doivent être informés de l’état de “santé“ de leurs équipements, à travers le portail qui est mis à leur disposition mais aussi en recevant des alertes mails. Il s’agit aussi d’un outil essentiel pour l’équipe technique, celui-ci nous permet d’intervenir assez rapidement en cas de problèmes afin de tenir nos engagements envers les clients et assurer la disponibilité, comme prévu dans le –SLA-.

La société Netplus a lancé comme projet la refonte globale du système de supervision jugée obsolète. En effet celle-ci date de plus de 9 ans et ne répond plus aux exigences métier et cela pour différentes raisons, notamment en cause :

* **La notification** : Une non-notification, comme une sur-notification, est néfaste à une supervision efficace.

Dans le premier cas, elle est causée par le fait que certains seuils d’avertissement sont mal définis sur les équipements voire absents. Par ailleurs certains seuils n’ont pas été testés avant d’être implémenté. Ainsi nous ne disposons pas d’éléments viables pour statuer sur le véritable d’un équipement.

Dans le deuxième cas, cela est dû à une mauvaise gestion des états oscillants (Flapping), en l’espace de 3 mois j’ai pu comptabiliser 12000 mails ne concernant que la supervision dans ma boîte mail. Au fil du temps et face à un très grand nombre de mails, il devient très compliquer de distinguer les vrais problèmes de ceux qui sont moins inquiétants.

* **Les sondes** : On a constaté une absence de sondes sur les équipements et parfois une défaillance de ceux déjà installés puisqu’ils ne remontent pas assez de détails dans le cas d’un état critique.
* **Fail-Over** : L’architecture actuelle n’est pas redondée, la supervision est sur une machine physique qui est présente que sur un seul site du Datacenter. Une coupure de ce site entrainera la perte de la supervision.
* **La gestion** : La gestion actuelle de la supervision est fastidieuse. Elle se fait sur un fichier de configuration en **XML** de plus de **7000 lignes**. Par ailleurs pour chaque arrivée d’une nouvelle plateforme ou dans le cas d’une modification, il faut modifier à la fois les hôtes, les services, les contacts et faire de même pour les contacts au niveau de la cartographie dans les fichiers de configuration de Nagvis.

Face à toutes ces problématiques, il a fallu revoir toute la configuration et les processus d’intégrations à la fois pour les plateformes, des contacts et bien évidemment au niveau de la notification.

Le projet s’est déroulé en plusieurs étapes qui structureront la prochaine partie, de la phase d’audit à la migration. Le projet s’est déroulé une période totale de 4 mois avec la méthode agile. Je faisais un point à chaque fin de semaine ou début de semaine avec le directeur des opérations et l’ingénieur qui m’accompagnait lors de cette mission.Il était alors question de discuter des objectifs de la semaine, de l’avancement et de la validation ou non des tests.

### Suivi projet

**Phase 1 : L’audit**

Durant cette phase, il a fallu recenser tous les équipements, leurs sondes, et faire un état de lieu global de l’architecture actuelle. L’entreprise utilise actuellement le logiciel open-source Nagios, pour la supervision en France et en Chine et aussi une supervision externe chez l’éditeur OVH.

|  |  |  |
| --- | --- | --- |
| Site | Version | Description |
| France | Nagios Core 3.2.0 | Surveillance des équipements clients à Equinix et Boulogne |
| Chine | Nagios Core 3.4.1 | Surveillance des équipements en Chine |
| OVH | Nagios Core 3.2.1 | Surveillance de quelques clients et de des sites de Boulogne. |

Tableau des installations.

Sur chaque site nous avons répertorié l’ensemble des Check que réalise notre Nagios au niveau applicatif et matériel ainsi que la liste des commandes.

On n’a pu constater que la supervision externe n’était pas complète et ne surveillait que les urls de certains clients et quelques équipements réseaux. De ce constat on se rend compte que les installations ne sont pas harmonisées, et ont été conçus au fur et à mesure pour répondre à des besoins immédiats. D’où l’importance d’une définition en amont des règles métier permettant d’établir des procédures communes de gestion.

**Phase 2 : Etude des besoins**

L’étude des besoins exige une compréhension globale de la situation actuelle puisqu’ à l’origine d’un projet il y’a bien souvent une situation insatisfaisante qu’il faut résoudre et aussi améliorer dans le même temps. Il a fallu recenser tous les besoins et les pistes d’amélioration à la fois en prenant en compte l’avis du chef de projets, des commerciaux et de l’ensemble de l’équipe technique. Une fois ces besoins établis, on a pu définir le cahier des charges de la solution. Ci-dessous un tableau récapitulatif des exigences fonctionnelles, qui décrivent les caractéristiques et les processus que le système doit respecter.

|  |  |
| --- | --- |
| Numéro | Description de la fonctionnalité |
| F1 | Gestion des alertes optimisée (Alerter les bonnes personnes au bon moment) |
| F2 | Accès restreint et étanchéité des vues entre clients. |
| F3 | Envoi de traps SNMP (Pour la baie de stockage) |
| F4 | Historisation des évènements et reporting. |
| F5 | Génération de graphs |
| F6 | Cartographie |
| F7 | Proactivité |
| F8 | Intégration au portail. |
| F9 | Page web en responsive design. |
| F10 | Mise en place d’escalades pour les alertes. |
| F11 | Optimisation des seuils d’avertissements. |
| F12 | Implémentation des plateformes plus efficaces. |
| F13 | Facilité de déploiement |
| F14 | Bases de connaissances étendues. |
| F15 | Automatisable |
| F16 | Liaison à un wiki. |
| F17 | Génération de tickets |

Tableau des exigences fonctionnelles.

|  |  |
| --- | --- |
| Numéro | Description de la fonctionnalité |
| F1 | Haute disponibilité en Fail-Over |
| F2 | Authentification forte et centralisé (AD/LDAP) |
| F3 | Traçabilité complète des accès et actions |
| F4 | Mise en place de la sauvegarde |

Par ailleurs les machines doivent respecter des exigences techniques obligatoires pour assurer la disponibilité, l’intégrité, la confidentialité et l’audibilité du système.

Tableau des exigences techniques.

En dehors des exigences, certaines contraintes ont été émises pour assurer la performance de la solution et simplifier sa gestion, quelques-unes ont été définies avant le lancement du projet et d’autres pendant la phase du -POC-. Ces exigences ont contribué, d’une part, à la mise en place d’un périmètre et d’autre part, à restreindre les critères de choix de la future solution.

|  |  |
| --- | --- |
| Numéro | Description de la fonctionnalité |
| F1 | Solution Open-Source |
| F2 | Sondes principalement en SNMP |
| F3 | Pas d’installation d’agents supplémentaires |
| F4 | Supervision sur écran |

Tableau des contraintes.

### **Phase 3 : Choix de la solution et réalisation du POC**

Les critères de choix de la solution se basent ainsi sur les spécificités décrites dans la phase précédente. Une étude comparative des solutions a été menée en s’appuyant notamment sur la documentation officielle, les différents forums et blog de chaque solution. On a retenu cinq critères principaux. Ces critères ont été pondérés pour répondre aux besoins de manière plus précise.

Figure 7 : Diagramme radar des solutions

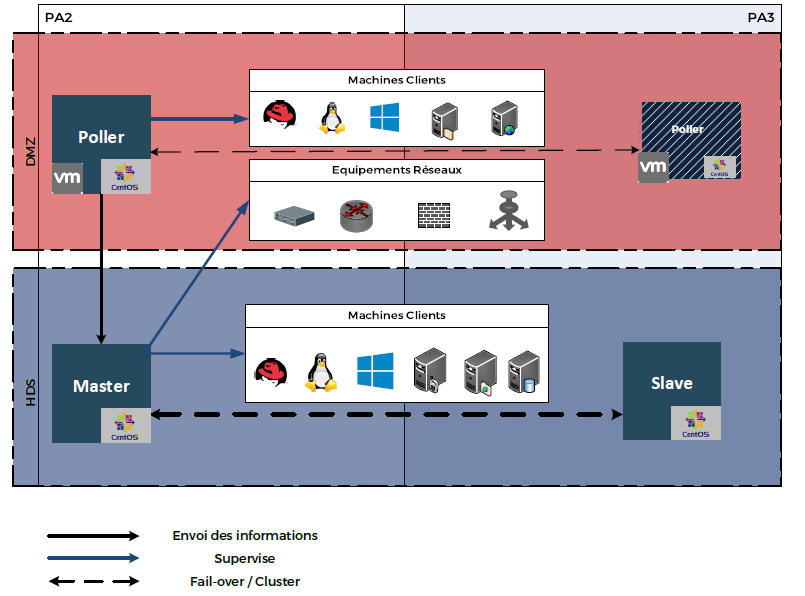
Le diagramme radar permet un comparatif plus visuel qu’un tableau. Les deux solutions Zabbix et Centreon étant très proches. J’ai réalisé une maquette de ces deux solutions pour avoir une idée plus précise. Suite à l’installation et des tests de checks, le choix a été fait de partir sur la solution **Centreon** qui correspondait au mieux à nos attentes.

Figure 8 : Architecture physique en France

Centreon est installé sur deux machines physiques présentes sur deux sites distincts du Datacenter. Le rôle du –Poller- est de superviser les machines situées en front-end et en middle, des serveurs web pour la plupart. Le Master quant à lui supervise les équipements réseaux et les serveurs en back-end, des serveurs de bases de données pour la plupart.

Concernant la chine on implémentera un poller qui disposera de sa propre interface web mais sera connecté au central de France afin d’avoir une solution unifiée et centralisée.

Pour la supervision externe, une plateforme complète sera déployé chez OVH avec comme objectif la supervision des services critiques et des autres Centreon (France et Chine).

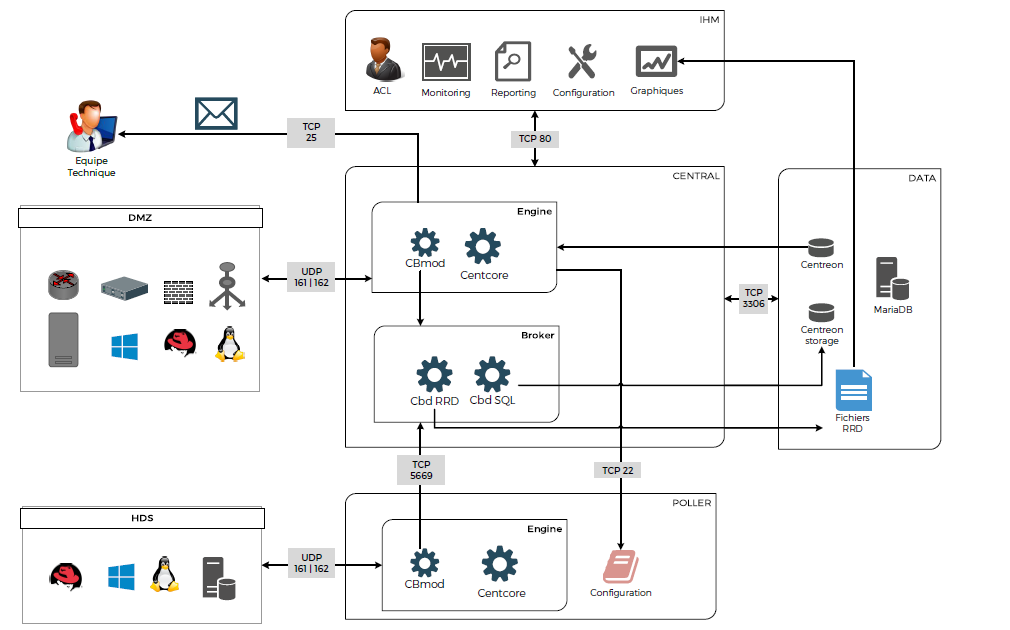
* Architecture logique du POC

Figure 9 : Architecture logique de Centreon

L’architecture ci-dessus décrit le fonctionnement de Centreon.

Le satellite central (Central) est composé de deux instances :

- l’engine, moteur de la supervision, se charge d’effectuer les checks sur les machines et de récolter les données résultantes. Le démon cbmod envoie ensuite les informations au broker. Il se charge aussi de l’envoi des notifications.

- le broker, module de traitement, se charge de générer les fichiers –RRD- pour les graphiques grâce à son démon Cbd (Centreon broker deamon) RRD, le démon Cbd SQL de stocker les données de performances dans la base de données.

Le poller est une extension du central, il dispose simplement d’une instance engine qui a les mêmes fonctionnalités tout comme celui du satellite central.

Suite à l’installation du premier central et du poller, nous avons pu tester les différentes fonctionnalités et vérifier qu’elle correspondait bien aux exigences.

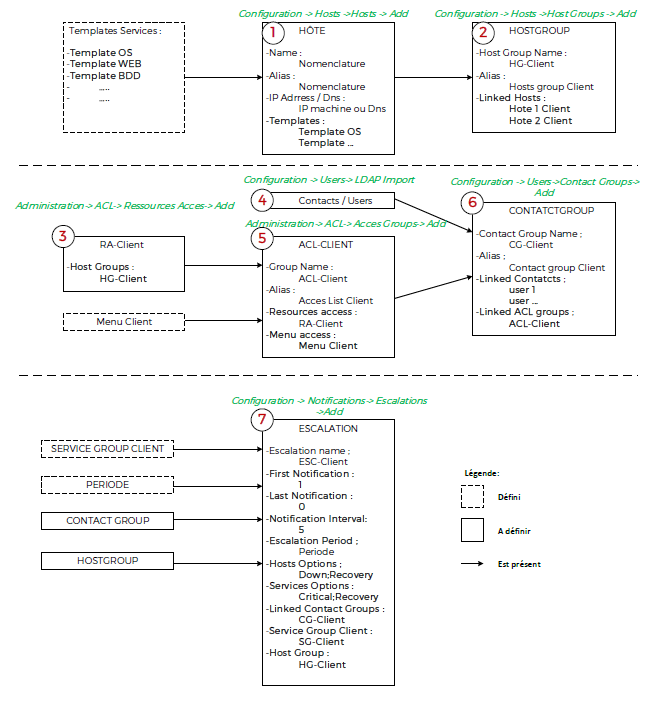
Mes principales réflexions lors de la réalisation ont porté sur la gestion des notifications,des templates et du Fail-Over.

* Templates et notifications

Le but des templates est d’optimiser et uniformiser le déploiement des machines. Ainsi lors de l’arrivée d’une nouvelle machine, il suffit de choisir les bons templates en fonction des services que regroupe celle-ci. Par exemple, pour un serveur debian, web en front-end. On lui appliquera un template Debian selon la version (Debian 7 ou 8) et un template web (apache ou ngninx). J’ai défini les services qu’on doit surveiller pour tout type de machine ainsi, s’il y’avait une différence au niveau des checks de l’OS on les séparait (ce qui est le cas des distributions Debian), et dans le cas contraire, on pouvait les regrouper.

Concernant les notifications la difficulté était d’alerter correctement l’équipe technique. En heures ouvrés on a fait le choix de ne plus recevoir de mails mais de mettre en place des écrans de supervision ou on verrait toutes les alertes. En heures non ouvrés, j’ai mis en place la notification par sms directement via des boitiers GSM, en évitant les –API-, pour assurer la continuité du service et une indépendance d’internet. Cependant les alertes par sms ne concernent que les services jugées d’une criticité sévère. Toutefois un rapport détaillant les évènements passés des dernières 24h est généré et envoyé à l’équipe technique ainsi qu’aux collaborateurs.

Ci-dessous, le schéma récapitulant le processus de l’arrivée d’une plateforme avec les règles métier.

Figure 10 : Processus d’arrivée d’un client

La définition de ces processus a permis d’accélérer la mise en place de la supervision. J’ai pu mettre en place une plateforme en moins de 5 min alors qu’auparavant cela m’aurait demandé 15 à 20 min.

### **Phase 4 : Migration**

Le POC ayant été concluant, en vérifiant les principaux aspects fonctionnels la suite du projet était la migration. Nous avons débuté par les équipements réseaux (Firewall, les SLB, les Switchs et Routeurs), la baie de stockage et les équipements électriques. Par la suite, les serveurs internes, serveurs mails, proxy,ldap,ftp. Enfin, les serveurs des clients. Avec la mise en place d’un planning on a migré les plateformes de pré-production et de production de chaque projet.

Cela fut aussi l’occasion de vérifier que le transfert des compétences a été bien réalisé auprès des ingénieurs en charge des différents projets et aussi d’affiner les sondes, templates, et certains seuils d’avertissement.

### Conclusion

Le projet de supervision fut pour moi une expérience très enrichissante, particulièrement sur le plan technique. Il m’a permis de parcourir l’ensemble du système d’informations et de manipuler divers équipements réseaux. Bien évidemment avant de superviser des éléments il se doit de comprendre les tenants et les aboutissants de chaque fonctionnalité et service que regroupe un équipement réseau ou un serveur. Cela fut pour moi l’occasion d’apprendre énormément.

Malgré un retard de livraison de deux semaines, ma solution a été bien accueillie par l’ensemble de l’équipe et des collaborateurs. Je regrette de n’avoir pu tester quelques fonctionnalités additionnelles, comme la mise en place de -grafana- ou encore la génération automatique des tickets mais le résultat est tout de même très positif et répond aux besoins priorisés par le DSI.

# L’INDUSTRIALISATION DU SI

De nos jours, les infrastructures IT sont de plus en plus complexes et dynamiques avec des rythmes d’évolution qui s’accélèrent. La virtualisation a marqué le pas d’une nouvelle méthode de gestion du SI et constitue une première réponse à cette évolution. Toutefois l’industrialisation est un nouveau moyen, encore sous exploité, qui permettra aux –SI- d’être plus efficace, plus rapide et moins coûteux au vu de l’évolution prononcée vers la numérisation.

J’ai choisi ce sujet car j’ai pu observer lors de mon stage un grand nombre de tâches récurrentes pour le support mais aussi lors des déploiements de projet. Par exemple au niveau du support, des demandes de logs de la part des clients, la création des comptes d’accès, les mises à jour applicatives. Il est vrai que certaines tâches sont déjà automatisées via des scripts entre autre mais l’industrialisation pour ma part va plus loin que cela. Elle permet de standardiser et uniformiser les règles de gestion que ce soit au niveau matériel, des processus et des configurations.

Le but de cette partie est d’expliquer : En quoi l’industrialisation permet-elle d’améliorer le SI ? Pour ce faire dans un premier temps, je présenterai un état de l’art du système actuel puis dans un second temps, un cas plus concret avec l’industrialisation de la supervision.

## Présentation

La demande pour une mise en exploitattion plus rapide des services est de plus en plus croissante dans les infrastructures. L’automatisation actuelle des tâches permet d’apporter un premier élément de réponse à la demande.

Ce fait est encore plus vrai au sein de la société Netplus, étant nouveau dans le domaine de l’hébergement des données de santé. Elle possède des capacités réduites en termes d’investissement et de personnel comparée à des grands groupes. L’entreprise se doit donc d’optimiser au maximum ses ressources afin de faire face à l’arrivée de grands groupes dans ce domaine.

### Problématique

Il est vrai que même si les projets sont différents, on constate lors du déploiement des plateformes une répétition des tâches qu’on peut catégoriser en plusieurs étapes.

* Construction des machines virtuelles
* Configuration réseau
* Mise en place des utilisateurs et des groupes
* Déploiement des applications
* Arrêt de la supervision
* Déploiement des applications
* Redémarrage des services
* Mise en marche de la supervision
* Maintenance des serveurs
* Connexion aux serveurs
* Mise à jour applicative via des scripts

### L’automatisation

L’automatisation actuelle des tâches permet de réduire le temps de besoins par le biais des scripts et de certaines fonctionnalités .On peut citer en exemple :

-Lors de la création des comptes, la présence de plusieurs scripts ont été développés pour l’envoi des credentials soit pour le compte support ou pour le portail.

-Lors de l’installation des machines virtuelles, l’outil Kickseed est utilisé pour mettre en place différentes configurations de bases telles que : le mot de base de l’utilisateur root, la connexion au -LDAP- …..

Toutefois le problème qui se pose notamment pour les scripts est que chaque ingénieur peut l’implémenter d’une manière différente. Se pose aussi la question de l’efficacité du script.

L’automatisation des tâches présente ainsi plusieurs avantages :

* Réduction des coûts d’exploitation
* Meilleure rentabilisation
* Meilleure cohérence des services
* Diminution des erreurs

### L’orchestration

L’orchestration est un ensemble de processus automatiques de coordination et de gestion des systèmes informatiques.

Elle fait partie intégrante ainsi de l’industrialisation et permet d’alléger et homogénéiser la gestion des infrastructures et des bases de données. Elle se distingue toutefois de l’automatisation car son but est de gérer l’enchainement des tâches. Elle agit sur leur déclenchement et leur planification selon les règles définis par l’utilisateur.

Le but de l’orchestration est donc de mettre en œuvre les workflows dans le but de répondre à une requête de l’administrateur ou de l’utilisateur final. On peut prendre en exemple la création d’une nouvelle vm, l’orchestre pourra défini comme étapes :

* Une demande des informations de la machine (nom,cpu,disque,ram,ip,vlan)
* La frabication de la machine sur le vcenter
* L’intervention sur les équipements réseaux (routeur,switch,baies de stockage) pour la configuration réseau
* Une mise à jour de la -CMDB- et du DNS.

L’orchestration présente ainsi plusieurs avantages pour les sociétés délivrant des services de cloud computing :

* Coordonner les work flow
* Diminution des délais de traitement
* Homogénéiser les processus
* Superviser les ressources
* Services prêt à l’emploi pour l’utilisateur

En résumé, l’industrialisation présente de nombreux avantages qui ont pu être chiffré suite à des observations en entreprise :

* Réduction de plusieurs semaines à 3 heures la livraison d’un environnement
* Réduction des erreurs humaines de plus de 50%
* Réduction du temps d’exécution des tâches et processus de plus de 50%

Malgré ces nombreux avantages, l’industrialisation est parfois difficile à accepter, car il parait légitime de se demander si elle ne remplacerait pas les activités d’un ingénieur .Pour ma part non, au contraire, en déléguant ces tâches de bas niveau, l’industrialisation permettrait de se dégager du temps afin de travailler sur des projets avec une plus forte valeur ajoutée.

D’autre part la mise en place des outils d’industrialisation a un coût matériel et de ressources, il est important de se poser aussi des questions sur son utilité pour une petite entreprise telle que Netplus ? Je pense que oui, en effet, les projets sont pour le moment de petite envergure mais multiples, ainsi pour répondre à ces besoins, l’entreprise ne pourrait pas augmenter les ressources physiques en fonction du nombre de projet mais devrait améliorer les processus.

## L’industrialisation appliqué à la supervision

Quelques temps après le début de mon stage l’entreprise a lancé en parallèle le projet d’automatisation avec l’arrivée d’un autre stagiaire. Ainsi j’ai pu collaborer avec lui pour la partie supervision .Cela m’a permis de découvrir l’outil d’automatisation et d’orchestration Ansible.

### Présentation de l’outil Ansible

Ansible est une plate-forme logicielle open-source pour la configuration et la gestion des serveurs. Elle permet le déploiement des logiciels, d’exécuter les tâches sur le serveur et la gestion de leur configuration. L’avantage de cet outil est qu’il est sans agent, et utilise le protocole SSH pour les différentes actions .Ces actions sont écrites en -YAML-, il s’agit d’un format de représentation de données comme le XML.

Il fonctionne sous forme de modules, par exemple le module shell permet d’exécuter des commandes sur la machine distante. Les modules constituent les fonctions de l’outil, on peut par ailleurs définir et implémenter ses propres modules en langage python.

Dans le dossier de configuration de Ansible, /etc/ansible, on retrouve plusieurs éléments qui permettent de mieux comprendre son fonctionnement :

* Le fichier hosts.yml constitue l’annuaire des serveurs distants ou peuvent s’effectuer l’industrialisation.Un compte root est nécessaire pour accéder à ces machines.
* Le dossier deploy qui regroupe les dossiers roles et playbook :
* Playbook

Le dossier playbook est un dossier qui regroupe un ensemble de fichiers en yml .Chaque fichier définit un playbook qu’on peut définir comme un orchestre. Le playbook est chargé d’exécuter les rôles (tâches automatisables) et de les ordonnancer.

Exemple :

|  |  |
| --- | --- |
| Playbook | Description |
| p\_app\_lamp\_install | Installe la stack LAMP |
| p\_app\_apache\_install | Installe apache |
| p\_app\_php\_install | Installe php |
| p\_app\_mysql\_install | Installe Mysql |

* Rôles

Le dossier rôle contient toutes les tâches qui seront exécutés à partir du playbook .Elles sont séparées de façon unitaire.

Exemple :

|  |
| --- |
| **Role** |
| r\_app\_apache\_install |
| r\_app\_mariadb\_install |
| r\_app\_mysql\_install |
| r\_app\_nginx\_install |
| r\_app\_php\_install |
| r\_app\_postgresql\_install |
| r\_app\_sqlite\_install |

### Supervision et Industrialisation

Le module CLAPI (Command Line API) est un module de Centreon permettant sa gestion en lignes de commandes. Ainsi en le couplant à Ansible via le module shell on peut mettre en place une industrialisation de la supervision.

Le module permet une configuration sur tout type d’éléments de Centreon :

* Hôtes
* Utilisateurs
* Services

Il m’a notamment permis via un script la mise en place des interfaces des équipements réseaux.

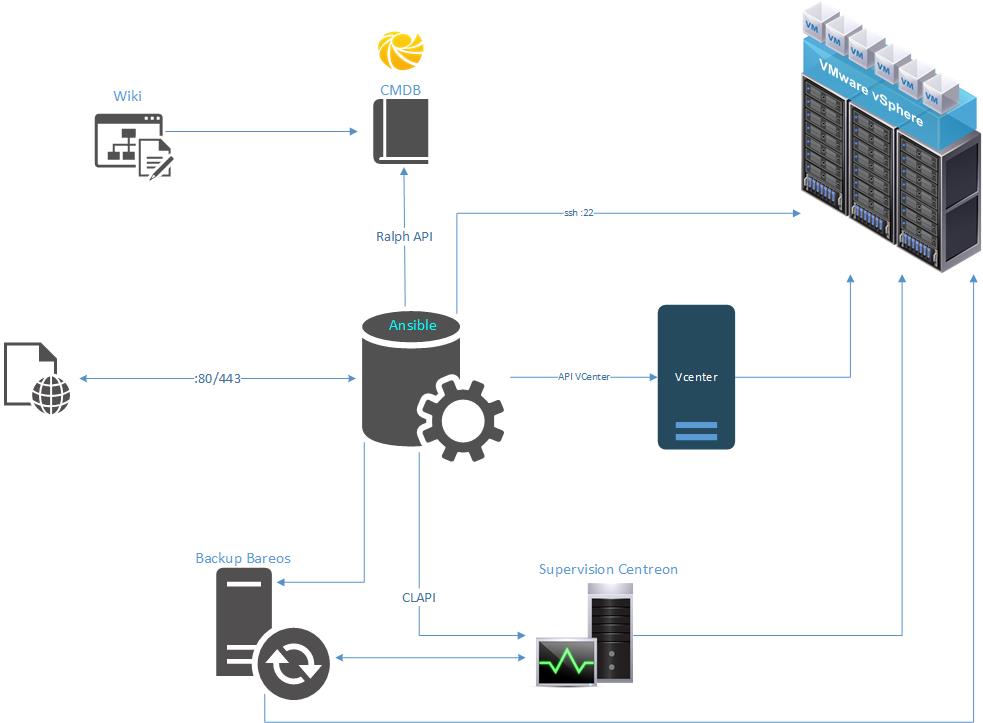
Partant de ce constat on peut réfléchir à une manière d’implémenter la supervision dès la création d’une nouvelle machine.En effet une fois que le playbook pour la création de la machine virtuelle a été joué, on peut mettre en place un playbook de supervision qui se chargera de :

1. Détecter l’os et installer le Template adéquat Ex : Template CentOS 7
2. Détecter l’ensemble des services et leur installer les templates Ex : Template MySQL

Ainsi on pourrait dès la création d’une nouvelle plateforme, retirer la supervision du flux de travail et se focaliser sur d’autres tâches.

La présence des event-handler au sein de Centreon ouvre des possibilités vers des actions d’une industrialisation plus intelligente. Celle-ci détecterait par exemple l’arrêt d’un service et aurait des actions à accomplir via Ansible avant d’alerter l’utilisateur.

Le but étant d’obtenir un SI standardisé avec des règles de gestion commune et harmonisé.

Figure 5 : Schéma d’Ansible

# Conclusion Générale

Le stage de fin d’études au sein de Netplus a été pour moi une expérience des plus enrichissantes à bien des égards. En effet j’ai beaucoup appris sur le plan technique en parcourant tout le système d’information par le biais de mes missions. J’ai pu prendre du recul sur les différentes notions acquises durant mon cursus d’ingénieur.

Le stage a été aussi l’occasion de vivre une belle expérience humaine qui m’a permis de m’améliorer sur le plan personnel et de la communication en matière d’interactions et d’échanges avec les interlocuteurs internes et externes et la prise de parole en public.

J’ai été ravi que le directeur des opérations m’ai laisse pas mal de choix et de liberté dans les projets cela m’a permis de m’affirmer et aider à prendre un peu plus d’initiatives.

* Bibliographie, Webographie
  + Livres, documents :
* Centreon Maîtrisez la supervision de votre Système d’informations, Editions Eni
  + Pages Internet :
* [**http://esante.gouv.fr/asip-sante**](http://esante.gouv.fr/asip-sante)
* **https://documentation-fr.centreon.com/**
* **http://www.droit-technologie.org**
* **http://sugarbug.web4me.fr**
* **http://irp.nain-t.net/doku.php/215snmp:40\_les\_mibs**
* [**http://searchdatacenter.techtarget.com**](http://searchdatacenter.techtarget.com/definition/data-center-as-a-service-DCaaS)
* [**www.wikipedia.com**](http://www.wikipedia.com)
* [**http://www.latribune.fr/**](http://www.latribune.fr/)
* [**www.zdnet.fr**](http://www.zdnet.fr)
* **https://fr.talend.com**
* **http://blogduyax.madyanne.fr/haute-disponibilite-avec-corosync-et-pacemaker.html**
* Glossaire

-Saas- : Software as a Service

-HADS- : Hébergeur Agrée des Données de Santé

-HDS- : Hébergement des données de santé

-SLA- : Service level Agreement.

Le Service Level Agreement, ou SLA est un contrat ou la partie d'un contrat par lequel un prestataire informatique s'engage à fournir un ensemble de services à un ou plusieurs clients.

-CSR- : Certificate Signing Request

Le CSR servira à donner des informations lors de la génération du certificat numérique

-SSH- : Secure Shell

Protocol de communication sécurisé, la sécurité se fait au niveau de l’échange de clé.

-SNMP- : Simple Network Management Protocol

Protocol de gestion de réseau. Permet en autre de gérer et diagnostiquer les équipements réseau.

-OID- : Object Identifier

Les OID sont des identifiants universels, elles désignent dans le cadre du SNMP une donné

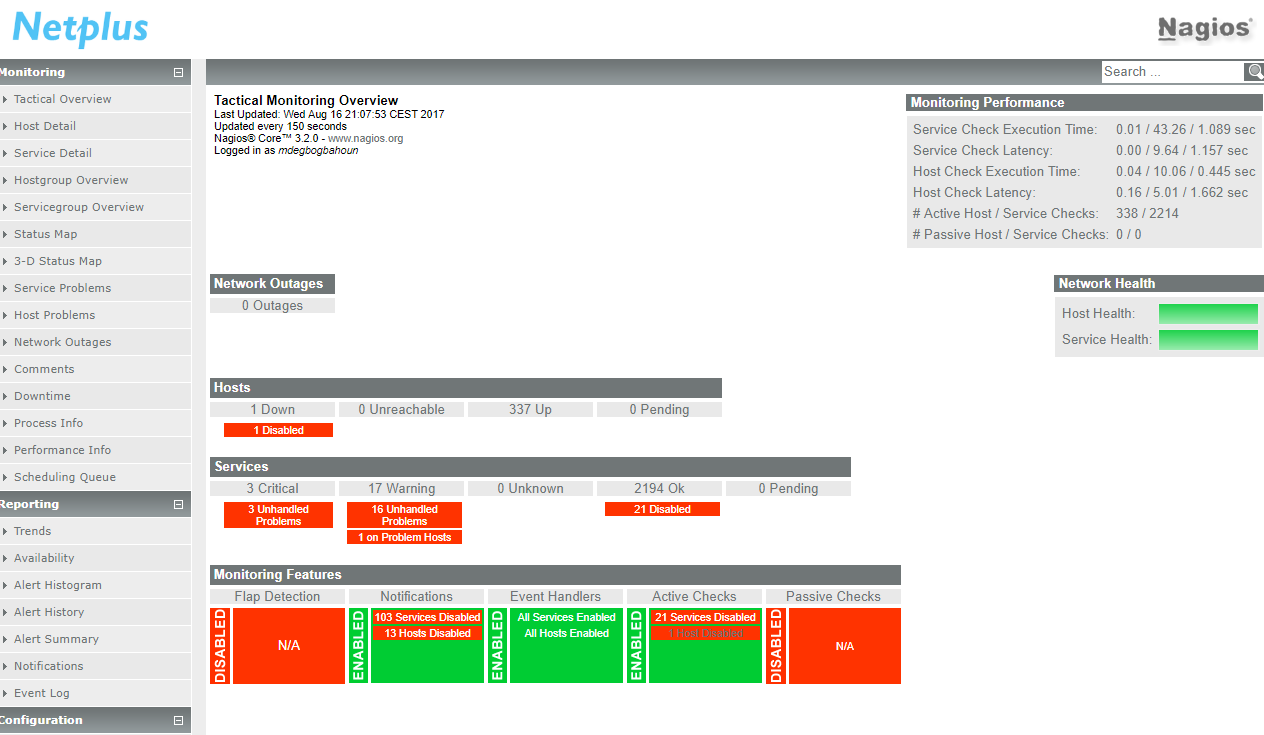
-MIB- : Management Information Base

Permet la gestion des OID

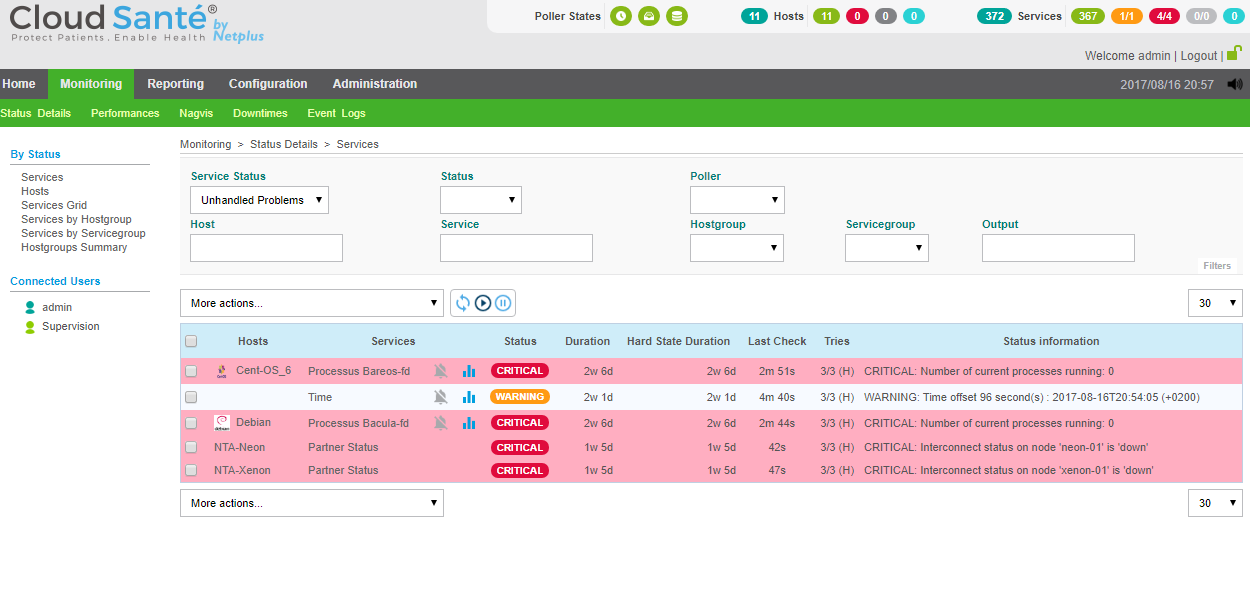
-Poller- : Dans le cas de Centreon un poller un un serveur à part entère effectuant des check snmp mais qui se distingue du central car on déllégue au poller des check spécifique ou des équipements particulier.

–RRD- Round Robin Databases

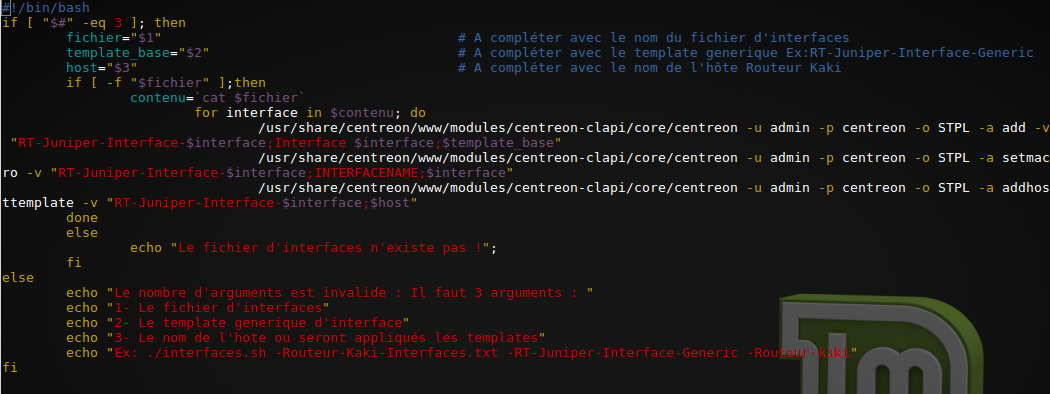
Permet la génération de graphiques

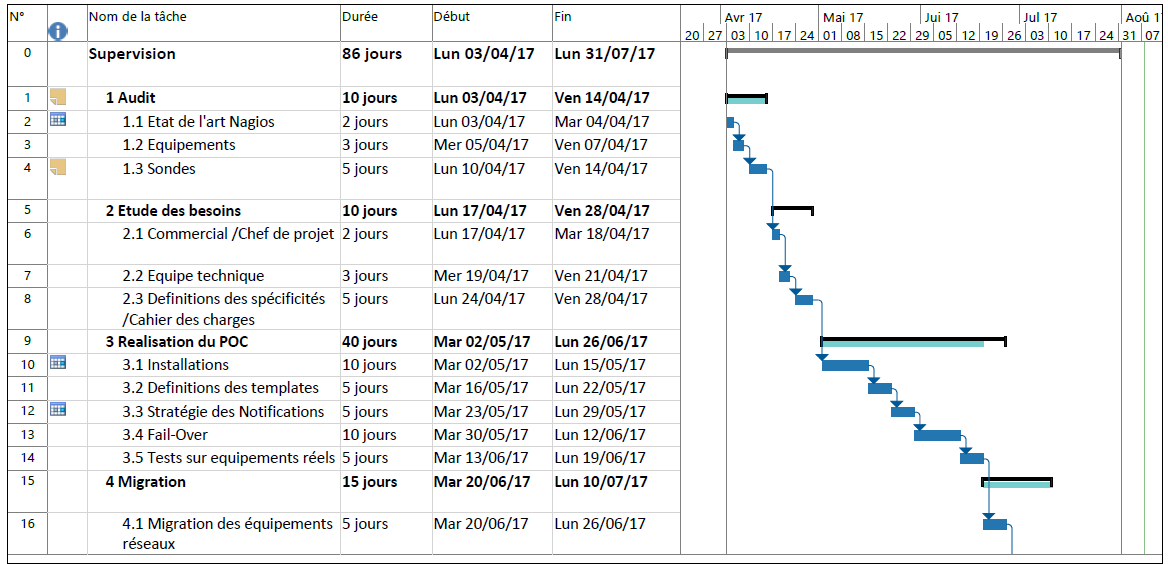
* Annexes

Aperçu de l’existant



Aperçu de la solution finale.

**

Apercu du script pour la mise en place des interfaces

Apercu du planning projet