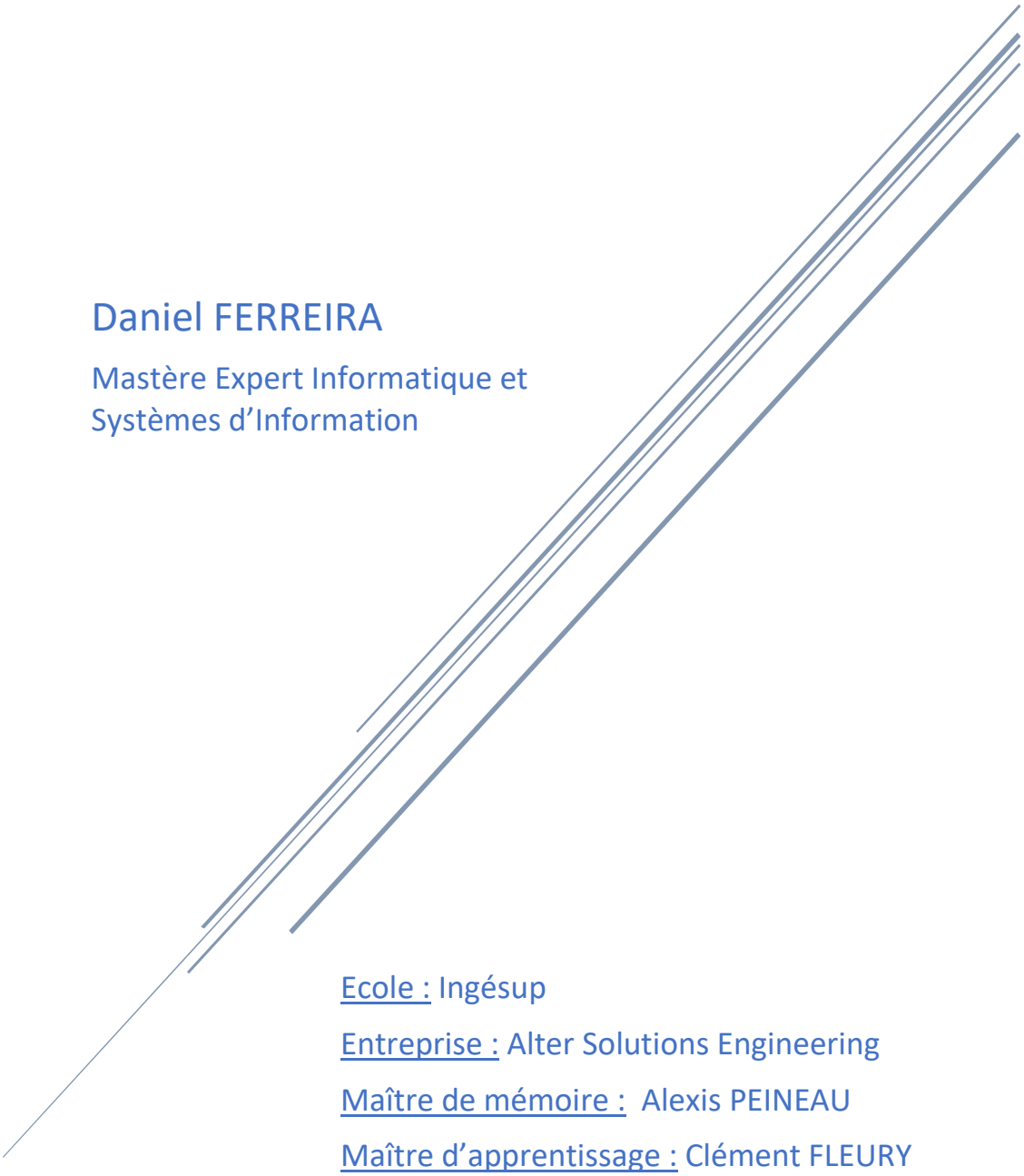
LA SUPERVION INFORMATIQUE

Intégration d'une solution de supervision au sein d'un Système d'Information

Daniel FERREIRA

Mastère Expert Informatique et Systèmes d'Information



Ecole : Ingésup

Entreprise : Alter Solutions Engineering

Maître de mémoire : Alexis PEINEAU

Maître d'apprentissage : Clément FLEURY

Année : 2016 – 2017

Remerciements

Pour commencer, je veux adresser mes remerciements aux intervenants ainsi qu'aux équipes pédagogiques d'Ingésup pour leurs partages et encadrements durant ma scolarité.

Je désire également remercier Clément FLEURY (maître d'apprentissage) pour sa précieuse directive, son soutien, sa sympathie, sa pédagogie ainsi que ses conseils avertis qui m'ont été d'un appui considérable durant cette année.

Je remercie mon tuteur de mémoire Alexis PEINEAU pour son suivi et ses conseils pour la rédaction de ce mémoire.

Mes remerciements les plus chaleureux vont à tous mes amis d'Ingésup qui m'ont apporté leur support moral et intellectuel durant ces belles années d'étude.

Je souhaite également remercier Nathalie RUFFIE pour son soutien et ses encouragements lors de la rédaction de ce mémoire.

Pour finir, je tiens à remercier mes proches et tout particulièrement mes parents pour leur soutien tout au long de mes années d'études.

Table des matières

Introduction

Auparavant l'informatique était réservée aux grandes entreprises, aujourd'hui elle est accessible par tous et est devenu un élément fondamental. Il a fallu 15 ans, de 1990 à 2005 pour voir l'étendue de ses technologies investir tous les secteurs. Elle est en évolution constante et permet d'offrir des améliorations sur les processus de travail mais aussi de favoriser l'innovation et d'obtenir un avantage concurrentiel. L'informatique est également une source de problème dans les entreprises puisqu'elle fait souvent l'objet de coûts importants et doit répondre aux besoins de l'organisation. Ce type de problème affecte toutes les entreprises, qu'elles soient petites, moyennes ou grandes. Beaucoup d'entre celles-ci détiennent une infrastructure informatique non maitrisée, fonctionnant donc d'une manière non optimale. De plus, le service informatique fait souvent l'objet d'un investissement minime avec des solutions non adaptées aux activités de l'entreprise. Les grandes entreprises ont même parfois tendance à se reposer sur leurs infrastructures actuelles, et ainsi se retrouvent rapidement avec des problèmes techniques et fonctionnels qui dureront puisqu'elles ne se concentrent pas sur la planification d'amélioration.

Ces problèmes, qui impactent toutes les organisations, peuvent être résolus par une bonne gestion des parcs informatiques. Tout au long de cette étude, nous tacherons d'appréhender la place du Système d'Informations au sein des entreprises et de déterminer son pilotage. La question qui se pose alors est la suivante : quels outils permettent de pallier à ces problèmes tout en favorisant un bon pilotage sans pour autant impacter considérablement les Systèmes d'Informations existant ? En informatique, nous utilisons le terme de « supervision » qui consiste à gérer et surveiller les infrastructures. Pour ce faire, et ce au risque de paraître peu exhaustif, nous nous intéresserons à l'intégration de ce type d'outil au sein d'un SI et nous étudierons les paramètres à prendre en compte afin que celle-ci soit la plus optimale possible. Nous tenterons, par la suite, de déterminer en quoi les outils de supervision sont-ils nécessaires au sein d'un Système d'Informations ?

I. Alter Solutions Engineering

1.1 Le groupe

Alter Solutions Engineering est une PME* et un regroupement de sociétés spécialisé dans divers domaines et secteurs d'activité. Il a été créé en 2005 par les associés Maxime LACOUR et Louis VACHETTE lors de la fusion des entités Alter Solutions et Alter Défense.

Alter Solutions est la société proposant des expertises à la pointe des nouvelles technologies dans les secteurs des transports, de l'énergie et des systèmes d'informations.

Alter Défense, quant à elle, propose d'accompagner et de répondre aux besoins de sous-traitance des industriels dans les secteurs de l'aéronautique, de l'aérospatiale et de la défense.

Ces entités, regroupées dans la structure de Alter Solutions Engineering, permettent à celle-ci de gérer l'ensemble des métiers transversaux tels que les services Comptabilité, Ressources Humaines, etc. La majorité du personnel, soit les ingénieurs et chargés d'affaires, travaille au quotidien directement au sein des sociétés clients. Cela permet aux autres collaborateurs de travailler dans les locaux du siège social.

En 2011, une nouvelle entité est créée : Alter Frame. Cette filiale est une entreprise d'édition de solutions informatiques.

Durant l'année 2015, le groupe a étendu ses filiales, jusque-là situées en France et dont le siège et le centre d'expertise se situent à Versailles, en dehors des frontières françaises en ouvrant d'autres agences en Belgique et au Portugal. D'autres filiales sont en cours de développement en Europe : Angleterre, Pays-Bas, Allemagne et Suisse.

* Merci de se référencer à la liste des abréviations en page 58 pour tous les mots contenant un astérisque.

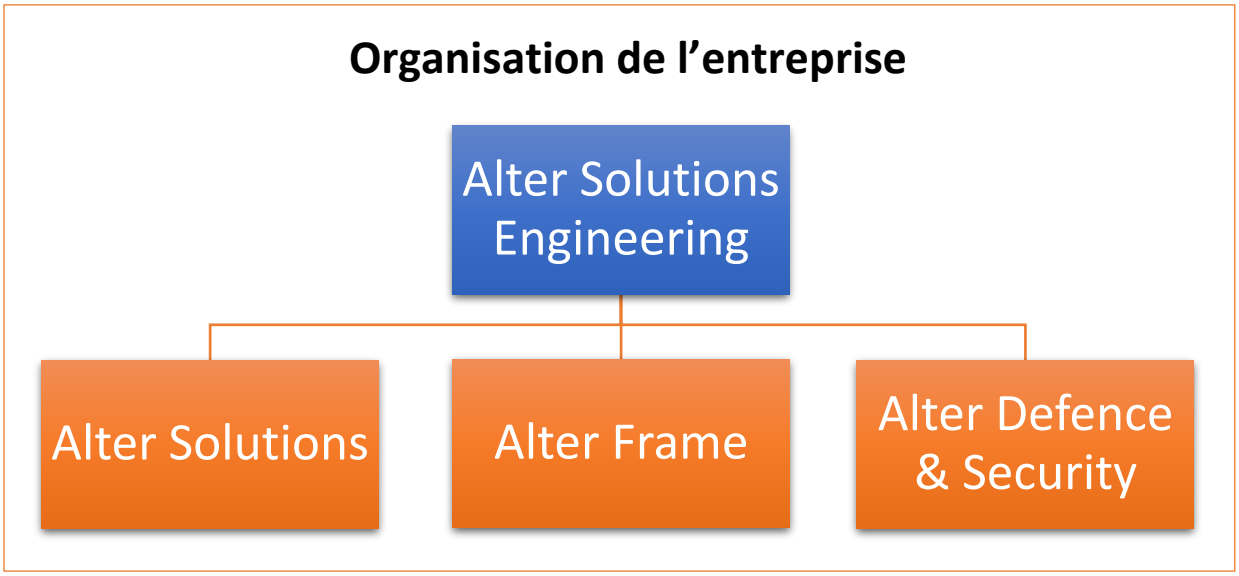


Figure 1. Tableau représentant l'organisation de la compagnie Alter Solutions Engineering, Avril 2017.

1.2 Les chiffres

En 2016, le groupe a réalisé un chiffre d'affaire de 20 M€, soit environ une croissance de 20% par an avec un total de 375 collaborateurs dont 20% de techniciens.

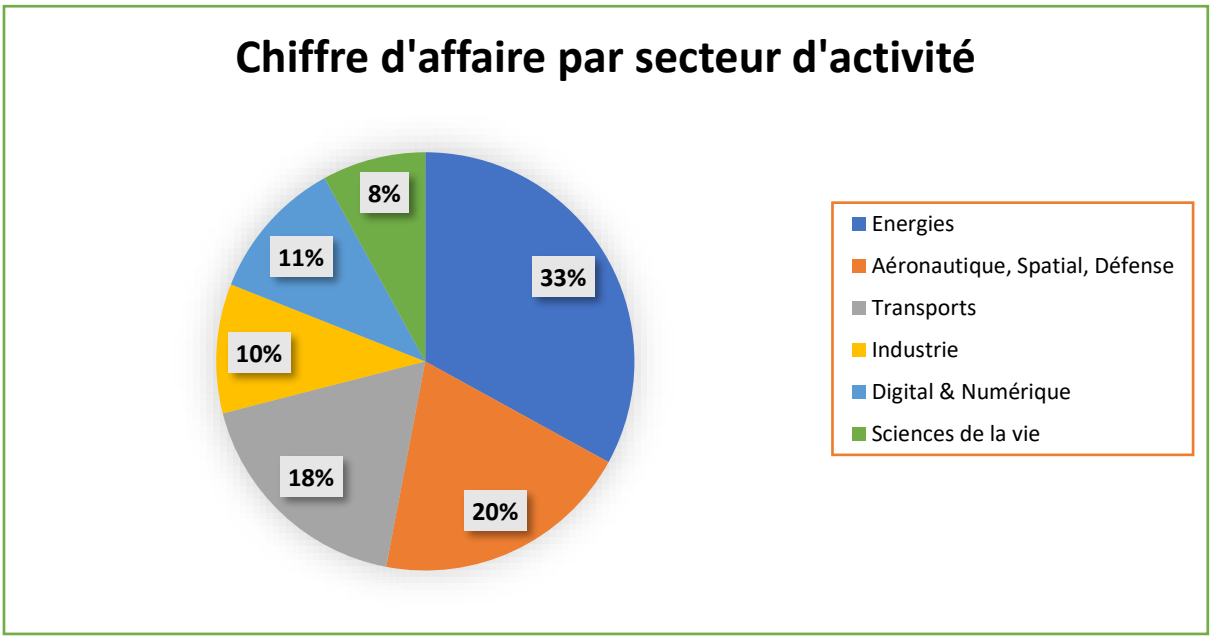


Figure 2. Diagramme circulaire représentant le chiffre d'affaire de la compagnie Alter Solutions Engineering par secteur d'activité, Avril 2017.

Nous pouvons voir sur ce graphique que les activités majeures sont l'Energie, l'Aéronautique, le Spatial et la Défense ainsi que les Transports ; le reste des activités – à savoir l'Industrie, le Digital et le Numérique ainsi que les Sciences de la vie – ne représentant qu'une part minime (29%).

1.3 Secteurs d'activités

Comme vu précédemment, Alter Solutions Engineering intervient sur plusieurs secteurs d'activités. Ils sont cités ci-dessous par ordre décroissant du pourcentage des parts de marché au sein de la compagnie :

- L'Energie : l'industrie a toujours été étroitement lié à l'énergie et à la disponibilité de dispositifs techniques permettant de la transformer en force motrice, en puissance, pour faire fonctionner les équipements de production ou développer de nouveaux moyens de transport. Alter Solutions Engineering apporte une expertise dans les domaines techniques et les matériels dédiés aux principaux acteurs de ce secteurs : pétrole et gaz, transport et distribution d'énergie électrique et nucléaire.
- L'Aéronautique, le Spatial et la Défense : ce domaine est reconnu pour son haut niveau d'exigence et son expertise historique, et est devenu une industrie de pointe. Forts de beaux succès industriels, celle-ci doit néanmoins sans cesse réinventer les solutions de demain et accroître son potentiel innovant. *Alter Defence & Security* intervient avec les industriels sur des projets d'envergures dans les différents secteurs de ce domaine : Aéronautique civil et militaire, Spatial et Défense.
- Transports : le secteur du transport connaît des volumes de trafic en pleine expansion, il est au cœur de l'innovation industrielle pour améliorer la sécurité, respecter les enjeux environnementaux et proposer à ses usagers une efficacité au quotidien. Alter Solutions Engineering travaille sur les solutions de demain en collaborant sur des projets novateurs avec les grands acteurs de ce secteur : Automobile, Ferroviaire, Transports Urbains.
- L'Industrie : les nouveaux enjeux liés au développement durable et à l'efficacité énergétique poussent le secteur à se renouveler et à évoluer. Le secteur industriel est donc en pleine mutation et doit relever de nombreux défis écologiques et technologiques. Alter Solutions Engineering accompagne les grands acteurs de ce secteur dans ces changements en apportant une expertise ciblée.
- Le Digital : l'économie contemporaine est portée par une révolution technologique, la numérisation, qui permet de très forts gains de productivité dans le stockage, le traitement

et la transmission d'informations et se traduit par le développement rapide des technologies de l'information et de la communication (TIC). Alter Solutions Engineering accompagne les acteurs de cette révolution au quotidien dans leurs projets novateurs.

- Les Sciences de la vie : le secteur des sciences de la vie est un acteur clé de l'économie novatrice qui stimule la concrétisation des idées novatrices dans le domaine médical qui permettront d'améliorer les soins de santé et la façon dont ils sont prodigués. Alter Solutions Engineering propose ses solutions aux petites et moyennes entreprises qui mettent au point des produits diagnostiques, biopharmaceutiques et pharmaceutiques et des appareils médicaux, ainsi qu'aux entreprises multinationales qui exploitent des filiales dans les domaines de la recherche et du développement (R&D).

1.4 Domaine de compétences

Ci-dessous, le récapitulatif des domaines de compétences de Alter Solutions Engineering.

Ingénierie Logiciel

Compétence		Technologie
Périmètre fonctionnel : - Assistance à maîtrise d'ouvrage - Conception fonctionnelle - Rédaction de spécification - Maquettage d'application	Validation logicielle : - Intégration / Validation - Qualification	Langage de programmation : - Web : ASP.Net, Java, J2EE, HTML5, PHP5, Javascript - Embarqué /client lourd : C#, .Net, Java, C, C++ - Mobile : Surface .NET, Objective-C, Java pour Android
Périmètre technique : - Gestion de configuration et ingénierie système - Architecture technique d'application - Développement - Interfaces (WebServices, SOAP* UI, Port Com, I2C, etc.) - Test unitaires	Accompagnement au déploiement : - Conduite du changement - Assistance au déploiement - Formation - Support/Helpdesk	Base de données : - Oracle, SQL Server, Mysql, MariaDB, Postgre-SQL, SQL Lite Serveurs applicatifs : - Nginx, Apache, IIS*, Tomcat

Cyber-Sécurité

Conseil / Audit de la gouvernance SSI* : - Stratégie de la sécurité / SMSI* / PSSI* - Accompagnement à la certification - Mise en conformité réglementaire - Analyse des risques - Management de la continuité des activités	Expertise / Architectures techniques - Sécurisation d'infrastructure SI - Gestion des identités et des accès - Sécurité des systèmes industriels et embarqués - Systèmes de détection d'intrusion intelligents - SIEM* – solutions de gestion des évènements de sécurité

Mécanique et structure

Génie Mécanique : - Conception : analyse fonctionnelles, AMDEC*, DAO*, CAO* - Calculs : cinématique, RDM*, thermique, CFD*, structure - Modélisation fonctionnelle - Ingénierie systèmes : spécifications, gestion des exigences, gestion des interfaces et intégration - Sûreté de fonctionnement	Génie Civil et Travaux : - Dimensionnement et calcul d'éléments standards - Calcul de structure : charpente métallique, béton armé, coffrage, ferraillage - Tracé de voie, VRD*, géotechnique - Conception d'ouvrages d'art et tunnels - Infrastructures portuaires et minières
Outils : - Catia V5-V6, Creo 2 (pro Engineer), Inventor, Autocadn PDMS - Ansys, Abaqus, Fluent, nCode - Orcaflex, Deepline, Diodore - Matlab Simulink, Amesim - Doors, Rhapsody	Outils : - Robot, Tekla - BRT, Covadis, Mensura

Electronique, Electrotechnique et Systèmes de Communication

- Banc de test : Conception et pilotage, modélisation et qualification de systèmes, études hardware et software, développement des IHM* - CEM* : Calculs et simulations, études des sources, analyses des différents couplages, risque foudre, essais / qualification - Electronique de puissance : Interrupteur, alimentation, transistors, différents convertisseurs (hacheurs, redresseurs, onduleurs, etc.)	- Electronique analogique : Capteurs, circuits d'instrumentations, calculateurs, circuits d'amplification électronique - Electronique numérique : Logique combinatoire, logique séquentielle et programmable, programmation VHDL et VERILOG, étude de FPGA* et d'ASIC* - Informatique industrielle : Architecture des calculateurs, systèmes à microprocesseurs, programmation, systèmes temps réel

Project Management

- Gestion de projet	- Planification
- Audit de processus et qualité	- Inspection
- Doc & Cost Control	- Gestion de contrat

Process et Production

- Génie des procédés	- Mise en service et essais
- Production	- Sûreté de fonctionnement
- Maintenance	

1.5 L'entité Alter Frame

1.5.1 L'activité

Comme dit précédemment Alter Frame est la plus jeune entité de Alter Solutions Engineering mais elle est aussi différente de par son activité. En effet, elle s'occupe de l'édition de solutions informatiques, ce qui comprend l'édition de logiciels, le développement de solutions techniques personnalisées et enfin de l'audit et de l'évolution de solutions existantes (re-engineering).

1.5.2 L'évolution

L'entreprise a suivi pendant les deux dernières années deux axes principaux. Le premier est celui du développement d'infrastructures technologiques pour le traitement d'un important nombre de données (Big Data). La seconde ligne directrice de l'entreprise est le développement de solutions connectées (Cloud) au profit de l'industrie.

Afin de rester dynamique l'entreprise a choisi d'intégrer plusieurs composantes telles que :

- Le développement de partenariat à long terme avec de grandes entreprises (Air Liquide et Airbus, et bien d'autres).
- L'intégration de programmes de recherche européens.

Actuellement l'entreprise comprend 20 collaborateurs et emploie 4 personnes par an afin de répondre aux besoins des projets innovants proposés par d'autres entreprises.

1.5.3 Les équipes

Afin de mieux répondre aux multiples demandes, Alter Frame est divisé en plusieurs équipes :

- Une équipe concentrant son activité sur des projets basés sur les technologies JAVA ou WEB (PHP).
- Une équipe basant son activité sur des projets utilisant les technologies Microsoft basées sur le Framework .NET et en C#.
- Une équipe réseaux et systèmes qui s'occupe de l'infrastructure informatique de Alter Solutions Engineering ainsi que les serveurs hébergeant les différentes applications internes et externes (celle des clients).

II. Le contexte

2.1 Le Système d'Information au sein de l'entreprise

Aujourd'hui l'informatique est présente dans la plupart des entreprises, elle est même souvent le cœur de fonctionnement et donc indispensable pour la gestion. L'activité d'une entreprise consiste à communiquer, rechercher de l'information, créer des documents et effectuer des calculs. Elle est ainsi investie dans tous les domaines d'activités. Une entreprise doit être en permanence dans une démarche d'amélioration de son cœur de métier et le Système d'Information (SI) est un secteur qui permet de la faciliter. Chaque SI sera adapté afin de réduire les tâches à valeur ajoutée pour gérer et fournir des informations exploitables. Ces informations peuvent être celles des clients via des plateformes telles que les sites web ou même des outils comme le CRM (*Customer Relationship Management*). Dans le cas d'un site web, nous traitons la suite des commandes, les informations du client. Dans le cas d'un CRM, qui est un outil pour optimiser les interactions avec les clients, nous sommes en mesure de simplifier le processus de vente et de marketing. Ce type d'outil peut dynamiser la productivité quand il est adopté par l'ensemble des services (RH*, service client, chaîne logistique, etc.). L'informatique a automatisé certaines tâches, comme la gestion de la comptabilité avec des outils tels que SAGE. Ces outils permettent également de fournir une bonne qualité de service et une réactivité accrue.

La mise en place et le maintien d'un SI demande un investissement important, il est donc important d'évaluer les besoins de l'entreprise pour dimensionner le SI. Car un SI sous-dimensionné est pénalisant, puisqu'il ne répondra pas aux besoins.

2.2 Gouvernance du Système d'Information

La gouvernance des systèmes d'information se définie comme un ensemble de moyens qui contribue à un pilotage efficace et une homogénéité de tous les composants du SI. Elle désigne une manière d'administrer et de diriger afin d'améliorer l'efficacité et la productivité des entreprises. Elle concerne la Direction des Systèmes d'Informations, mais également tous les métiers de l'entreprise. Par définition, la gouvernance détermine les objectifs, les fonctions et les tâches permettant différentes études qui proposeront de nouvelles solutions. Elle est donc directement liée à la stratégie de l'entreprise car elle permet à celle-ci d'améliorer sa capacité de créer de la valeur et ainsi d'augmenter le chiffre d'affaire, d'améliorer le taux de marge et la rentabilité. Il est prouvé que les entreprises possédant un faible niveau de gouvernance n'obtiennent que peu de bénéfices par rapport à leurs investissements. Alors que celles qui disposent d'une gouvernance forte et stable, en retirent de réels avantages. Ainsi, la gouvernance du SI va s'appuyer sur 5 points importants.

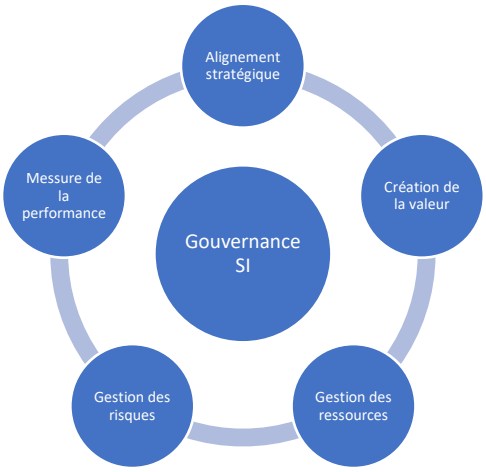


Figure 3. Tableau représentant les cinq points nécessaires à la gouvernance du Système d'Information, Avril 2017.

Le Système d'Information doit être aligné sur la stratégie générale de l'entreprise. Il doit donc ordonner en permanence ses objectifs afin qu'ils soient en accord avec la stratégie générale. Tous ces objectifs devront être justifiés afin d'obtenir le budget pour leur mise en place. Il faudra donc que ces objectifs mettent en évidence la valeur créée. S'ils ne respectent pas ce critère, alors il n'aura pas lieu d'être intégré au sein de l'organisation. Ces objectifs peuvent prendre la forme de nouveaux services proposés aux clients tels que la maintenance de leurs sites internet, ou de leurs applications, ou encore d'améliorer la qualité ou l'efficacité des produits existants. Ces objectifs concernent également la mise en place d'outils et de processus internes aux entreprises avec des outils comme le CRM, évoqué précédemment. Enfin, ces outils permettent le développement des relations entre

l'entreprise et les fournisseurs ou les clients. La communication est un point très important, la mise en place d'un outil efficace et permettant un suivi sur les produits peut améliorer la fluidité des échanges. Par exemple, la mise en place d'un outil de gestion de projet comme *Redmine*, va permettre de communiquer sur les avancés ou modifications d'un projet. Il va, à terme, permettre un gain de temps et un meilleur suivi de qualité avec le client. Cette solution est par ailleurs mise en place chez Alter Frame pour la gestion des projets.

Avant de mettre un outil en place au sein d'un Système d'Information, il faudra également prendre en compte les risques qu'il pourrait engendrer. En effet, un Système d'Information est en changement permanant. L'intégration ou la mise à jour d'un outil doit faire l'objet d'une étude de risque. Celui-ci permettra d'évaluer si la mise en place pourrait engendrer un risque majeur pour le SI. Pour cela, il faut être capable de prendre conscience de l'ensemble des menaces auxquelles est exposé le système d'exploitation afin de mettre en place les mesures adéquates pour les éliminer. Ces risques peuvent être externes, c'est-à-dire liés à l'environnement de l'entreprise, de son activité, du marché sur lequel elle intervient, de ses concurrents ou des réglementations. Ils peuvent également être internes, liés donc à l'organisation de l'entreprise, de son management et de ses processus. Or, la première difficulté provient de l'aménagement et de l'évolution du Système d'Information en lui-même. Comme dit précédemment, il évolue constamment. De nouvelles applications apparaissent, de nouvelles mises à jour sont nécessaires ou des changements sur les équipements doivent être réalisés. Ces applications de plus en plus importantes fonctionnent parfois sur des systèmes différents, sont destinés à des utilisateurs divers, en utilisent des plateformes matérielles différentes. De plus, ces applications nécessitent une multitude de bases de données qui fonctionnent via des technologies différentes. Il est donc primordial de disposer d'un inventaire complet des équipements, ainsi que tous les processus mis en place. Le système a tendance à devenir complexe, tout en répondant aux attentes de l'entreprise, il peut cependant contenir des failles et par la suite devenir corrompu. Par ailleurs, un grand nombre d'entreprises voit leur SI se complexifier, parfois de manière injustifiée. Ceci est souvent la répercussion d'un empilement d'applications diverses, accumulé sur plusieurs dizaines d'années. Le ciblage voire la connaissance d'un problème peut s'avérer délicat. À ce moment, la détection d'une panne ou d'une donnée compromise peut devenir très compliquée. Le système devient complexe par la multitude de matériels et de technologies. Un SI est obligatoirement composé de routeurs, de switchs, de pare-feu et de serveurs. La quantité est bien sûr définie en fonction du besoin et des utilisateurs. On intègre également les postes clients, qui représentent une masse matérielle, des logiciels et surtout l'utilisateur en lui-même. L'utilisateur va être un paramètre à prendre en compte pour la sécurité du

SI. Plus le nombre d'utilisateurs est important, plus la ressource en matériel réseau sera conséquente.

La gouvernance prend en compte également l'équipe en charge de faire évoluer et de maintenir le Système d'Informations. Des compétences multiples sont nécessaires, mais celles qui sont indispensables pour avoir une infrastructure sont les compétences réseau et système. Car le cœur d'une infrastructure passe tout d'abord par le matériel permettant la communication en interne mais également en externe. Nous parlons ici de la mise à disposition d'une connexion Internet, ainsi que d'une communication interne à l'entreprise. Dans la plupart des entreprises, nous pouvons distinguer deux équipes. Une équipe réseau qui se chargera de mettre à disposition une infrastructure complète et répondant aux besoins de l'entreprise ; ainsi qu'une équipe système qui prendra la responsabilité de la gestion des plateformes qui seront utilisés par les employés de l'entreprise. Ces deux équipes sont amenées à travailler en étroite collaboration pour respecter une homogénéité du SI. Ainsi, l'entreprise disposera du minimum requis pour toute activité. Les outils indispensables aujourd'hui à toutes entreprises sont une connexion Internet, un serveur de stockage avec toutes les données de l'entreprise y compris celle des employés, un serveur de comptabilité pour la gestion ainsi qu'un serveur de messagerie et une solution de téléphonie pour la communication. Il ne faudra pas oublier l'aspect sécurité dans cette infrastructure, et par la suite, l'entreprise aura sans doute besoin de compétences spécifiques pour une technologie adaptée à son secteur. Toutes ces équipes et ces compétences doivent être regroupées et évoluer de manière cohérente afin de fournir un Système d'Information fonctionnel.

Pour résumer, le SI doit être fonctionnel, comme nous venons de l'expliquer, mais il doit également être performant et répondre intégralement aux exigences de l'entreprise. Il doit donc être capable de mesurer la performance et de surveiller l'activité afin de contrôler les résultats des objectifs stratégiques de l'entreprise. Pour cela, nous allons prendre en compte quatre axes : l'axe financier, l'axe client, l'axe organisationnel ainsi que l'axe des processus internes. L'axe financier prend en compte l'analyse des bénéfices et des déficits financiers, ainsi que la perception des actionnaires. L'axe client, quant à lui, comprend l'attente des clients et leur perception envers l'entreprise. L'axe organisationnel comporte l'optimisation des capacités à changer ou à améliorer le SI et implique les Ressources Humaines ainsi que l'infrastructure. L'axe des processus internes implique une analyse de l'efficacité des processus internes à l'entreprise afin de déterminer celle qui apporte de la valeur, et sur lesquels l'entreprise devra se concentrer pour réussir.

2.3 Les besoins de Alter Solutions Engineering

Alter Solutions Engineering ambitionne d'améliorer la maîtrise et les performances de son Système d'Information. Son SI est constitué de matériels et de logiciels en interne et en externe, c'est-à-dire hébergés chez un fournisseur d'hébergement. Son infrastructure est ainsi composée de matériels réseaux et de serveurs contenant les informations utilisateurs et un serveur hébergeant les applications du service comptabilité. La compagnie dispose également d'applications utilisées en interne, totalement hébergées chez un fournisseur d'hébergement. De plus, Alter Frame prend en charge le maintien des serveurs clients où sont stockées les applications, qui sont également hébergés chez un fournisseur. Il est donc indispensable de mettre en place une solution permettant de surveiller ces différents systèmes et applications. Cette solution doit être simple à installer et compatible avec les systèmes Windows, Linux ainsi que les équipements réseaux. Elle doit également être capable de surveiller les services FTP* **, HTTP*, MySQL souvent utilisés par les applications web. Une surveillance sur les services de connexions à distance comme le SSH* serait également nécessaire puisqu'il est très utilisé comme moyen de connexion à distance sur les serveurs. Pour maintenir ses applications en état de fonctionnement, la machine sur laquelle elles seront hébergées devra également être surveillée. L'outil devra donc être capable de surveiller les éléments d'une machine comme son CPU**, sa RAM* ou l'espace disque. Cet outil permettra ainsi de mesurer les performances, la disponibilité et l'intégrité de nos différents équipements. Il donnera une visibilité améliorée sur l'infrastructure afin de faciliter les prises de décision. Si un problème est soulevé, alors les équipes en charge du projet pourront y remédier rapidement en ayant les informations nécessaires. Pour que les informations soient communiquées aux différentes équipes, l'outil devra intégrer une interface intuitive adaptée à tout type d'utilisateur. L'outil doit ainsi supporter la gestion des utilisateurs afin de créer différents groupes avec des droits appropriés.

Le besoin principal de Alter Solutions Engineering est donc de disposer d'un outil de supervision permettant de répondre à toutes ses attentes.

III. Qu'est-ce que la supervision ?

La supervision est une technique de suivi et de pilotage d'un SI. C'est un processus d'acquisition, de collecte et de centralisation de données (mesures, alarmes, état de fonctionnement). Il est à la fois une application de surveillance du bon fonctionnement d'un système ou d'une activité, et de contrôle via des commandes et de diagnostic.

** Merci de se référencer au glossaire en page 57 pour tous les mots contenant un double astérique.

Ce logiciel de supervision fonctionne généralement sur un ordinateur en communication sur un réseau local ou distant. Ce système assure un rôle de gestionnaire d'alarmes, d'évènements déclenchés par des dépassements de seuils (afin de prévoir un éventuel accident) et de temps de fonctionnement. Il permet donc de remonter des informations techniques et fonctionnelles au SI. L'informatique étant devenue un point important dans l'entreprise, le SI est au centre de l'activité des différents métiers et doit fonctionner en continuité pour garantir l'efficacité de l'entreprise. Le réseau, les terminaux des utilisateurs, les serveurs d'applications et les données constituent les points importants où la disponibilité et la qualité de service conditionnent le bon fonctionnement de l'entreprise. Il faut donc réduite les problèmes liés à l'informatique, car une indisponibilité du SI a des impacts nocifs sur l'activité ainsi que sur la notoriété de l'entreprise. Il existe deux enjeux majeurs au sein d'un SI : Le premier est de garantir la disponibilité du système en cas de panne ou de dégradation. Le second est de pouvoir anticiper les problèmes afin de garantir une remonté d'information rapide et une durée d'intervention minimale. La supervision inclut donc plusieurs activités : surveiller, visualiser, analyser, piloter, agir et alerter. Elle nous permet de surveiller de manière intuitive notre SI, de disposer ainsi d'une vue d'ensemble. En effet, ce type d'outil permet de créer une cartographie de tous les éléments supervisés et permet d'intervenir de manière plus rapide et ciblée. Il permet également d'analyser différentes mesures pour éviter d'éventuels accidents. Dans le cas potentiel d'accidents, l'outil créé des alertes contenant des informations pertinentes concernant le type de problème et la cause de l'accident ; ce système permet une meilleure réactivité.

La question qui se pose alors est la suivante : Que pouvons-nous superviser au sein d'un SI ?

Au sein d'un SI, il est possible de superviser le réseau ainsi que ses équipements. Plusieurs types de matériels constituent les équipements :

- Il y a, premièrement, des commutateurs et des routeurs, qui admettent la récupération et la supervision de différentes données telles que la disponibilité - qui permet de savoir si l'équipement est toujours en état de fonctionnement -, ou encore les alertes comme un port du routeur qui ne fonctionne pas.
- Il y a également des onduleurs, qui sont des dispositifs électroniques permettant de subvenir aux besoins des équipements en cas de panne électrique au sein du bâtiment. Ils présentent l'avantage de communiquer leur état ainsi que les charges en temps réel qu'ils supportent.
- Les imprimantes font aussi partis des équipement sur lesquels nous pouvons récupérer des informations pertinentes telles que leur disponibilité, leur état et leurs consommables.

- Il est possible de superviser également les serveurs et ainsi de récupérer les informations concernant leurs différentes ressources (CPU, RAM, etc.)
- Il y a également les applications et les services dont l'une des fonctions est de faire remonter certaines informations telles que leurs disponibilités, la cohérence des réponses aux interrogations de l'application sur le service et enfin leur performance. Si un service n'est plus disponible, alors son responsable en sera informé et pourra par la suite le relancer.

Le responsable informatique peut être averti de différente manière : par son interface de supervision (cartographie), par e-mail ou encore par SMS. Certains outils de supervision permettent même de prévoir une tâche lorsqu'un problème survient. Ainsi, à la suite d'une coupure de service par exemple, il est possible de relancer le service, par une commande. Nous parlons dans ce cas-là d'automatisation de tâches.

3.1 La métrologie

Les informations récupérées sont des mesures définies. On appelle ce processus Métrologie qui est la science des mesures. Elle permet d'acquérir, de garder et de tracer des valeurs numériques. C'est donc un ensemble de techniques et de savoir-faire permettant de donner une valeur à une observation. Lorsqu'un problème sur une application est rencontré, il est pertinent de chercher à lui appliquer des valeurs qui pourront par la suite être étudiées. Ces valeurs peuvent prendre plusieurs formes, soit la machine physique telle que le CPU* (*Central Processing Unit*) utilisé sur le serveur, soit l'application comme un site internet avec un nombre de personnes connectées identifié. Une fois les valeurs obtenues, l'objectif est alors de les interpréter de manière simple et efficace. La métrologie vient donc en complément de la supervision et permet de remonter, sous forme de graphiques, les tendances afin d'appréhender d'éventuelles futures anomalies.

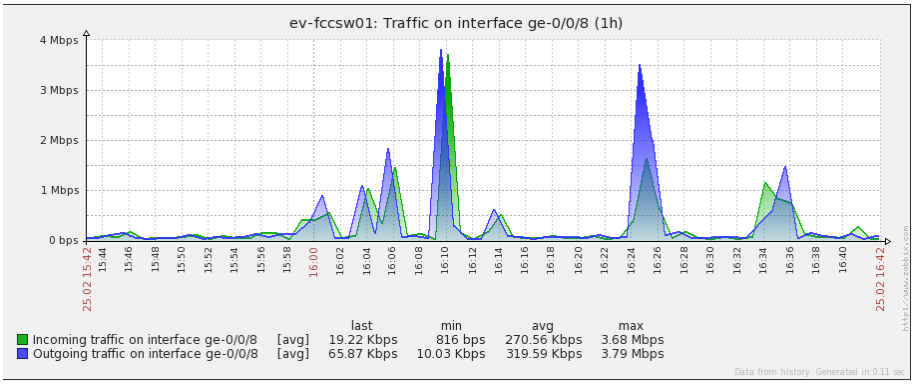


Figure 4. Graphique représentant le débit entrant et sortant d'un routeur

La figure 4 représente un graphique récapitulant le trafic entrant (en vert) et sortant (en bleu) sur un port d'un routeur. Il est facile d'interpréter ces résultats sous cette forme car il est aisé de connaître les horaires de pointe du trafic. La métrologie, sous la forme de graphique, présente les avantages de disposer de mesures facilement interprétables, sauvegardées et ainsi réutilisables suivant les études et les problématiques souhaitées par l'entreprise à des moments différents. En effet, pour déterminer et anticiper un éventuel problème ou besoin, des mesures sur une période large sont nécessaires à toute recherche ou observation. Une analyse précise nécessite donc un maximum d'informations. Avec ces données, il est intéressant de faire des observations selon la fréquence de l'utilisation, l'horaire, le temps et de voir s'il y a des anomalies. Prenons l'exemple d'une forte utilisation dans une tranche horaire anormale, telle que la nuit lors de la fermeture des bureaux d'une entreprise, l'observation qui sera faite sera alors une utilisation possiblement frauduleuse.

3.2 Les protocoles réseaux nécessaires à la supervision

Pour nous permettre de récupérer les différentes mesures (données) de nos équipements à distance, nous allons nous référencer à quelques protocoles réseaux.

3.2.1 Le protocole IPMI

Tout d'abord le IPMI (*Intelligent Platform Management Interface*) est un ensemble d'interfaces communes permettant de surveiller certains composants mais également de contrôler le matériel à distance. Il est ainsi possible de travailler en réseau. IPMI est un protocole introduit en 1998 et utilisé par certains constructeurs tels que Dell, HP ou Compaq. Il fut par la suite standardisé en 2013 avec un accès en source ouverte, ce qui a permis son déploiement dans différents domaines, hétérogènes et donc multiplateformes. Grâce à ce protocole, nous pouvons accéder aux statuts des serveurs et ainsi connaître leur état de marche (allumé ou éteint), remonter des données en provenance des capteurs, des sondes de températures, vérifier l'état des ventilateurs ou encore contrôler l'alimentation. Dans les cas d'un équipement éteint ou nécessitant un redémarrage, il est possible de le rallumer et donc d'appréhender l'état de la machine à un instant précis. En effet, les serveurs peuvent disposer d'une carte BMC (*Baseboard Management Controller*) - totalement indépendante -, composée d'un BUS** et d'un processeur dédié et connecté à une carte réseau. Ce système fonctionne de manière permanente même lorsque le serveur est hors service. Ce protocole dispose de multiples commandes, qui peuvent varier en fonction de la marque du matériel, mais la plus

importante pour la supervision est la commande SDR*. Cette commande SDR dispose de beaucoup d'options qui nous permettrons de disposer d'informations sur l'état de nos disques, tel que la situation des ventilateurs par exemple. De plus, le protocole est intégré au sein de nombreux outils de supervision, permettant ainsi de remonter des alertes.

3.2.2 Le protocole SNMP

Il existe également le protocole SNMP (*Simple Network Management Protocol*) qui permet aux administrateurs réseaux de gérer les multiples équipements dont ils disposent mais également de diagnostiquer les problèmes rapidement. Ce protocole fonctionne avec un superviseur - qui est donc un serveur de supervision -, et des agents installés sur les équipements à superviser. Les informations récoltées sont enregistrées dans une base de données nommée MID (Management Information Base). Le protocole SNMP conçu par CISCO, HP et Sun, fut normalisé par l'IETF (Internet Engineering Task Force) et le modèle OSI*. Il permet de contrôler à distance l'état des matériels réseaux. Il est fortement utilisé dans les réseaux locaux, et est basé sur l'échange de messages entre un périphérique et une station d'administration. Il existe trois versions du protocole : SNMP v1, SNMP v2 et SNMP v3.

- Le SNMP v1 est une version dite légère et est la plus répandue.
- Le SNMP v2 est une version complexe et donc peu utilisée. Elle assure un niveau de sécurité plus élevé (authentification, cryptage, etc.), avec des messages d'erreur plus précis.
- SNMP v3 dispose des avantages de la v2 sans en présenter les inconvénients. Elle dispose d'un modèle de sécurité USM (*User-based Security Model)* en s'abstenant du décryptage des messages de commande qui transitent sur le réseau et permet de gérer les droits en fonction des utilisateurs.

Ce protocole peut être installé sur chaque composant réseau qui peut être administré grâce à un agent. Cet agent est un programme qui enregistre continuellement les informations des composants et les stocke dans une base de données (MIB). Nous pourrons ainsi depuis une station d'administration, interroger chaque nœud « manageable » du réseau, prendre connaissance de son état ou consulter les informations par exemple. Le protocole SNMP utilise le modèle client-serveur, dans lequel le client est représenté par la station d'administration NMS (*Network Management Station*) qui interroge des serveurs représentés par les agents SNMP fixés sur les nœuds administrables. Ces nœuds administrables peuvent être des machine hôtes (ordinateurs, serveurs, etc.) ou des éléments réseaux (hubs, routeurs, commutateurs). Le SNMP fonctionne sur le niveau 7

du modèle OSI (voir figure 5 ci-dessous) mais s'appuie nettement sur le protocole UDP (User Datagrem Protocol). Il fonctionne donc en mode non-connecté c'est-à-dire qu'il ne contrôle pas les données transmises.

	Modèle OSI	Modèle DOD
7	Application	SNMP
6	Présentation	
5	Session	
4	Transport	UDP
3	Réseau	IP
2	Liaison	
1	Physique	

Figure 5. Tableau représentant la place du SNMP du modèle DOD par rapport au modèle OSI

En utilisant le protocole UDP, le protocole SNMP utilise obligatoirement des ports. Les deux ports normalement réservés à ce dernier sont :

- Le port 161 : sur ce port, la station d'administration va émettre des commandes (set, get, getnext) vers un agent qui répond (response).
- Le port 162 : les messages d'alerte émis par l'agent vers la station d'administration transitent par ce port.

Le Manager NMS, ou plus communément appelé station de gestion de réseau, est un point important du protocole SNMP. Il est représenté par un poste serveur ou un logiciel d'administration, qui fournit aux administrateurs une vue d'ensemble des équipements. Les logiciels d'administration utilisent les informations réunies par le NMS dans une base de données (MIB) et interroge les MIBs gérées par les agents. Le NMS va donc s'appuyer sur le protocole SNMP pour encapsuler ou décapsuler les messages échangés, générer les commandes émises par l'administrateur et traiter les alertes des agents.

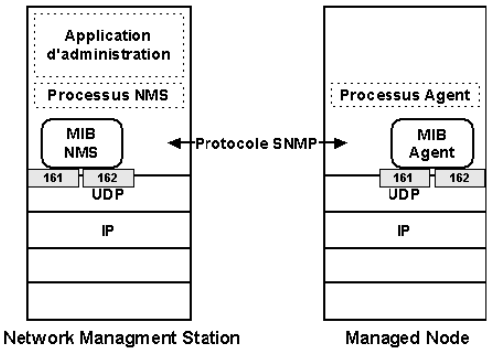


Figure 6. Communication entre le Manager et l'Agent de supervision

L'agent SNMP est un composant logiciel qui vérifie le fonctionnement du nœud administrable. Cet agent sera utilisé par le NMS grâce aux commandes et aux requêtes SNMP. Or, il peut également envoyer des alertes au manager sans être obligatoirement sollicité puisque sa MIB lui permet de réaliser des traitements qui lui appartiennent. L'agent peut être autonome ou « passif », c'est-à-dire qu'il peut être totalement dépendant du manager. Celui-ci procède à des relevés réguliers auprès des agents qui vont renvoyer les informations et les paramètres demandés. Ce processus s'appelle le *Polling*. Mais cette technique possède quelques inconvénients car il peut engendrer une surcharge du trafic réseau. Plus le réseau est grand, plus le nombre de matériel à superviser sera important. Dans ce cas, le *Polling* risque d'utiliser une grosse partie de la bande passante qui pourrait amener à une surcharge du réseau. Pour pallier à ce problème, il est possible d'intégrer des agents dits particuliers. Ces agents sont nommés Agent-Proxy et Sondes Rmon.

L'agent Proxy permet de gérer les équipements dits non standard, il agit comme passerelle entre un système propriétaire et le SNMP en traduisant les informations. Il va ainsi répartir les charges d'administrations en récupérant les informations sur le réseau et transférer les données pertinentes vers le manager.

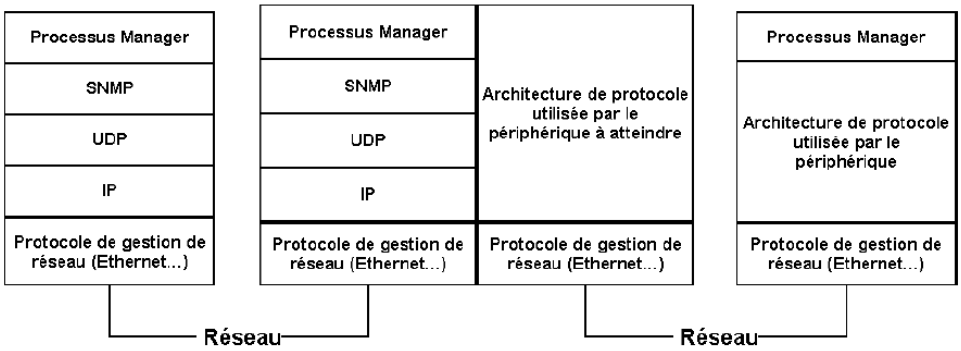


Figure 7. Schéma représentant le rôle du Proxy Agent

La sonde RMON (Remote MONitoring) est un équipement spécifique pour l'écoute d'un trafic. Il sera placé à un emplacement stratégique afin de récupérer les activités sur un réseau. L'objectif de cette collecte de données est d'optimiser les performances du réseau. Ces sondes peuvent être de deux types : RMON 1 (couche 1 et 2 du modèle OSI) et RMON 2 (couches 3 à 7 du modèle OSI) (se référer à la figure 5).

Chacun de ces agents, va donc collecter et stocker une multitude de données propre au nœud administrable qu'il surveille. Ces données seront stockées sur une MIB qui peut être décomposée en MIB standard ou MIB privée. Le MIB standard va contenir de nombreuses informations de base

comme les compteurs de paquets émis et reçus par le nœud. Mais tous les logiciels clients peuvent lire ces compteurs ; en effet, le flux ne peut être contrôlé car accessible par le plus grand nombre en source ouverte. Ainsi, les constructeurs de ces logiciels exploitent un grand nombre de possibilités et divers composants réseau. On parle à ce moment-là de MIB privée puisque les informations sont spécifiques à une technologie précise. Mais comment est gérer le traitement de ces informations ?

Les données stockées deviennent rapidement imposantes au sein des MIB, dont certaines possèdent un grand nombre de variables. OSI a donc défini une structure de classification nommée SMI (*Structure of Management Information*). Cette structure se compose d'identifiants appelés OID (*Object Identification*) qui sont établis à partir d'une classification arborescente. En 1990 une nouvelle structure (MIB-2) a été défini par la RFC** 1158 afin de pallier aux évolutions technologiques. Ainsi, chaque variable SNMP peut être retrouvée grâce à son nom ou à identification OID. Par exemple, si nous voulons avoir des informations sur la mémoire vive (RAM) d'un serveur, nous pouvons aller interroger la variable RAM ou la variable ayant son OID correspondant.

Cette fin de partie concernant le protocole SNMP va s'intéresser aux données clients qui peuvent être envoyées au serveur manager (NMS). En effet, le SNMP utilise des échanges de message de type Requête-Réponse entre le manager NMS et les agents clients. Ce protocole fonctionne en mode non connecté, ce qui implique qu'il ne contrôle pas les données transmises. Il ne garantit donc pas la bonne transmission des messages à son destinataire. Le manager NMS peut envoyer trois types de messages aux agents clients :

- GetRequest : qui va aller chercher la valeur d'une variable nommée et désignée.
- GetNextRequest : qui va lire séquentiellement la valeur d'une variable sans forcément connaître le nom.
- SetRequest : va enregistrer une valeur dans une variable particulière et désignée.

L'agent, quant à lui, va pouvoir envoyer des messages de deux types au NMS:

- GetReponse : qui est une réponse à une requête.
- Trap : qui est une alerte déclenchée par un événement.

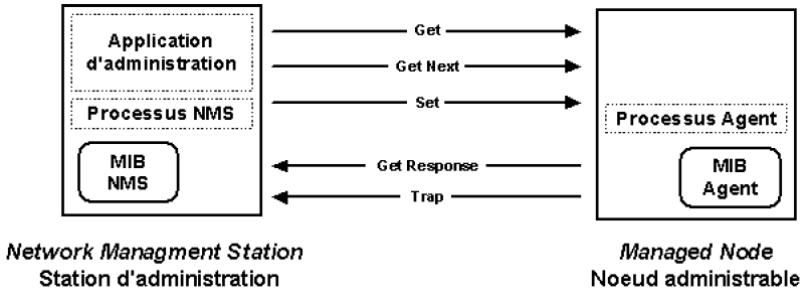


Figure 8. Echanges SNMP entre le Manager et l'Agent

Les échanges SNMP sont principalement constitués de ces cinq commandes (voir le tableau de la figure 8). Les SNMP v2 et V3 ont apporté quelques commandes et réponses supplémentaires mais ne sont pas souvent utilisés pour la supervision.

3.2.3 Le Syslog

Le protocole Syslog est principalement utilisé par des systèmes UNIX. Il vise à transporter via un réseau, les messages de journalisation – données journalières générées - gérés par une application vers un serveur hébergeant une centralisation des logs. Il permet ainsi d'avoir accès à des informations quotidiennes de nos différents systèmes sur un seul serveur. Ce protocole détermine la notion de périphérique, de relais et de collecteur. Un périphérique est une machine ou une application qui gère les messages Syslog. Un relais est une machine ou une application qui reçoit les messages et les transmet à une autre machine. Un collecteur, quant à lui, est une machine ou une application qui reçoit les messages Syslog mais ne les transfert pas. Ainsi, les périphériques et les relais sont des émetteurs lorsqu'ils envoient des messages Syslog. Les relais et collecteurs sont des récepteurs puisqu'ils reçoivent des messages Syslog.

Le protocole Syslog est défini par des notions de fonctionnalité, de sévérité et de priorité dans les messages qu'il créé. La fonctionnalité correspond au type d'application générant le message Syslog. Il existe 24 fonctionnalités définies par la RFC 3164 qui sont les suivantes :

Numéro de fonctionnalité	Usage
0	Messages du noyau
1	Message du niveau de l'utilisateur
2	Système de messagerie
3	Démons systèmes
4	Message de sécurité / autorisation
5	Messages générés en interne par le Syslogd
6	Système d'imprimante en ligne
7	Système de nouveau réseau
8	Système UUCP** (Unix to Unix Copy Protocol)
9	Démon de l'horloge
10	Message de sécurité / autorisation
11	Démon FTP
12	Système NTP **
13	Journal d'audit
14	Journal d'alert
15	Démon de l'horloge
16	Utilisateur local 0
17	Utilisateur local 1
18	Utilisateur local 2
19	Utilisateur local 3
20	Utilisateur local 4
21	Utilisateur local 5
22	Utilisateur local 6
23	Utilisateur local 7

Figure 9. Tableau représentant les 24 fonctionnalités (0 étant compris comme une fonctionnalité) en fonction de son usage, défini par la RFC 3164.

Dans ce tableau, nous pouvons remarquer que le contenu et les définitions de ces fonctionnalités ne sont pas nettement définis. Nous y retrouvons plusieurs fois les fonctionnalités correspondant à l'horloge ou à l'authentification. De plus, parmi ces fonctionnalités, certaines sont aujourd'hui obsolètes telles que l'UUCP. En résumé, les fonctionnalités correspondent au type d'application qui génère le message Syslog. Il faut également retenir que seule l'application décide de la fonctionnalité qu'elle utilisera et le choix du numéro de la fonctionnalité est de la responsabilité du projet ou du développeur de cette application.

Nous avons ensuite la sévérité d'un message Syslog qui correspond au degré d'urgence. Il existe 8 degrés de sévérité qui sont toutes définies par les RFC*. Ces niveaux sont les suivant :

Numéro de sévérité	Usage
0	Urgence : le système est inutilisable
1	Alerte : des mesures doivent être prises immédiatement
2	Critique : conditions critiques
3	Erreur : conditions d'erreur
4	Attention : conditions d'avertissement
5	Avis : conditions normales mais significatives
6	Renseignements : messages d'informations
7	Déboguer : messages de niveau débogage

Figure 10. Tableau représentant les 8 niveaux (0 étant considéré comme un niveau) de sévérité d'un message Syslog correspondant aux niveaux d'urgence, avril 2017.

Ainsi, la sévérité correspond aux degrés d'importances allant d'un simple débogage à une urgence où le système est inutilisable. Comme pour les fonctionnalités, l'application seule décide de la sévérité qu'elle utilisera mais le numéro de sévérité est déterminé par le projet ou le développeur de l'application.

Pour finir, notons que la priorité du message Syslog est définie par sa fonctionnalité et sa sévérité. Cette valeur est donc le résultat de la multiplication de la fonctionnalité par 8 auquel sera ajoutée la sévérité.

Illustrons cette dernière phrase avec un exemple : une fonctionnalité 17 qui correspond à l'utilisateur local 1 du poste avec une sévérité de 6 correspondant à un message d'information, aura une priorité de 142 ((17 x 8) + 6). La priorité maximale est de 191 car la fonctionnalité la plus élevée définie par les RFC est de 23 et la sévérité la plus grande est de 7 ((23 x 8) + 7 = 191). Le terme employé est celui de priorité. Cependant, il ne correspond pas à la réalité d'exécution puisqu'un message de priorité maximale ne sera pas traité plus rapidement qu'un message de priorité minimale. Le terme est donc mal choisi.

Le protocole Syslog est un protocole défini en texte, il utilise donc les caractères du code ASCII (*American Standard Code of Information Interchange*). L'ASCII est une norme de codage composée de caractère, apparue dans les années 1960 et aujourd'hui particulièrement utilisée.

Il utilise principalement le protocole UDP (*User Datagram Protocol*) et le port 514. Mais il existe également des implémentations de Syslog en TCP** (*Transmission Control Protocol*) ou en SSL (*Secure Sockets Layer*) en utilisant d'autre port. Une trame de protocole Syslog est composée de trois parties, la PRI (la priorité), la HEADER (le nom de l'hôte et la date du message) et le MSG (le message) :

- Le PRI est composé de trois, quatre ou cinq caractères, le premier étant < suivie d'un nombre représentant la priorité et finissant par >.
- La partie Header est composée de deux champs : le champ *Timestamp* qui représente la date sous la forme suivante : aaaa-mm-ddThh:mm:ssZ ; et le champ *Hostname* représentant l'appellation de la machine. Cette appellation peut être le nom de la machine, son adresse IP au format IPv4 ou IPv6.
- La partie MSG est composée du message texte qui sera transféré.

Le protocole Syslog est ainsi un protocole réseau qui permet à une application de générer des messages à destination d'un serveur. Mais ce protocole, plutôt simple, rencontre certains problèmes. Le premier est l'utilisation du transport UDP, qui est un protocole n'offrant aucune garantie d'acheminement. Un paquet UDP sera envoyé par un émetteur mais il n'est pas possible de vérifier la bonne réception ou le traitement du paquet par le récepteur. De plus, ces messages ne sont pas numérotés, le récepteur ne peut alors pas savoir s'il en a perdu un. Ce problème est également présent lors du séquencement à la réception des messages car un émetteur peut envoyer deux paquets dans un ordre précis. Or, le récepteur peut les recevoir dans l'ordre inverse, c'est-à-dire qu'il reçoit le message 2 avant le 1, et puisque les messages ne sont pas numérotés, alors l'analyse faite à partir de ces messages peut être totalement erronée.

Comme évoqué précédemment, les fonctionnalités sont composées de 24 valeurs, mais certaines ne sont plus utilisées ou sont redondantes comme par exemple l'authentification. Ceci n'est pas forcement problématique quand une entreprise possède peu de machines mais devient plus compliqué quand le SI devient plus important. Un grand nombre de doublons sera présent, ce qui impactera l'intégrité des données à terme. Syslog utilise le protocole UDP, qui est un protocole orienté message. Une trame Syslog est envoyée par UDP en un seul paquet IP qui sera reçu en une seule fois. Il n'est donc pas nécessaire de posséder un mécanisme de synchronisation entre l'émetteur et le récepteur. Cependant, Syslog peut utiliser parfois le protocole TCP, qui est orienté flux. Dans ce cas-là, il sera plus difficile d'extraire du flux TCP les messages Syslog. En effet, le TCP fonctionne différemment, un envoi peut correspondre à plusieurs réceptions et plusieurs envois peuvent correspondre à une seule réception. Il est donc nécessaire d'intégrer un système de synchronisation entre l'émetteur et le récepteur, réalisé par l'intégration du SYN sur les trames TCP. Le protocole Syslog s'appuie naturellement sur UDP, il hérite donc de toutes les faiblesses du protocole UDP, telles que:

- La possibilité de créer une trame Syslog en falsifiant l'adresse IP de l'émetteur.
- La possibilité de créer entièrement une trame Syslog et l'envoyer au serveur.

Ces différents protocoles seront utilisés par les outils afin de répondre aux besoins spécifiques d'une entreprise. Ils donnent accès à différentes informations comme la disponibilité d'un matériel, du temps de réponse d'une application.

La partie suivante va se concentrer sur les différents types de supervision et leurs utilités.

3.3 La supervision de disponibilité

Comme son nom l'indique, la supervision de disponibilité consiste à s'assurer de la disponibilité des composants matériels et logiciels. Le but étant de récupérer des informations sur une machine physique, et de savoir si elle est éteinte ou allumée. Cette supervision permet également de connaître la disponibilité d'un système d'exploitation, en s'appuyant sur différentes données comme son CPU, sa mémoire vive, ou l'espace des disques. Effectivement il est intéressant de disposer en temps réel des informations sur le système qui contient les informations ou les applications de la compagnie, en particulier quand les problèmes concernant un système peuvent provenir d'une multitude de paramètres. Une indisponibilité, par exemple, peut émaner d'une surcharge du processeur ou bien de la mémoire vive. Dans ce cas, une surcharge peut être provoquée par les différentes applications disponibles sur la machine.

Le processeur, quant à lui, est considéré comme le cerveau de la machine, il est comparable à un cerveau humain. Il se charge d'organiser les échanges de données entre les différents composants de la machine comme les disques dur, la mémoire vive ou la carte graphique. Il nous permet, par une multitude de calcul, d'interagir avec la machine via un écran. Si le processeur (défini par une valeur CPU) est surchargé, sa capacité de traitement des différentes informations va être ralentie. Celles-ci peuvent, même à terme, être totalement indisponibles notamment si le processeur est hors service. La mémoire vive nommée RAM (*Random Access Memory*) est une mémoire de la machine vive, c'est-à-dire qu'elle sera utilisée lors de l'utilisation d'une application ou d'un service. Elle permet de gérer les informations rapidement pour pouvoir travailler avec l'application en temps réel. En d'autres termes, lors du lancement de l'application, le fichier exécutable sera stocké sur la mémoire vive et sera régulièrement mis à jour afin de pouvoir interagir avec celle-ci. Le processeur possède les mêmes caractéristiques car si la mémoire vive est surchargée, l'application connaîtra un temps de réactivité plus long et pourra même s'éteindre.

Une fois que la disponibilité de la machine est connue, il est pertinent de s'intéresser à la disponibilité des applications que l'entreprise utilise, ou des applications qui sont nécessaires à la configuration et à l'accès à distance de la machine. Le service SSH (*Secure Shell*) sur les systèmes

UNIX par exemple nous permettent d'accéder à la machine à distance via une authentification. Le SSH est une application et un protocole de communication sécurisé entre un client et une machine distante. Il est régulièrement utilisé pour la configuration et la maintenance d'un serveur, qui est normalement stocké dans une salle dédiée (salle serveur) avec un accès restreint. Il est donc indispensable au sein d'une compagnie car si le besoin d'intervenir sur la machine se fait sentir, il est nécessaire d'accéder physiquement à celle-ci. Or, ce n'est pas toujours le cas. De plus, si le serveur est hébergé chez un Hébergeur, le seul moyen d'accéder à la machine est de passer par des protocoles sécurisés. L'hébergeur nous fournis évidement une interface afin d'accéder à ce serveur mais ne peut pas être accessible et communiqué à tous les membres du service en charge de le maintenir. Il servira, par exemple, au service développement qui se charge de développer une application ou un site web sur le serveur. Il est donc indispensable que ce service soit accessible afin de ne pas freiner la production. La disponibilité et l'accès deviennent donc des enjeux primordiaux.

Une fois que la connexion à la machine depuis l'extérieur est assurée, l'intérêt se porte sur des services plus spécifiques. Si l'entreprise héberge un site web sur le serveur, l'application gérant la base de données est un point très important. Une base de données (BDD) est un système qui enregistre des informations de manière classée et est utilisée dans toutes les applications ou sites internet. Ces plateformes ne peuvent pas être disponibles si leur base de données est inaccessible. Car toutes les données sont stockées sur cette application, tant les données propres à la plateforme comme celles des utilisateurs qui peuvent y avoir accès. La question qui se pose alors est celle de la récupération de ces informations ? La réponse est bien sûr en rapport avec l'application de supervision qui interroge la machine cliente afin de récupérer les informations souhaitées.

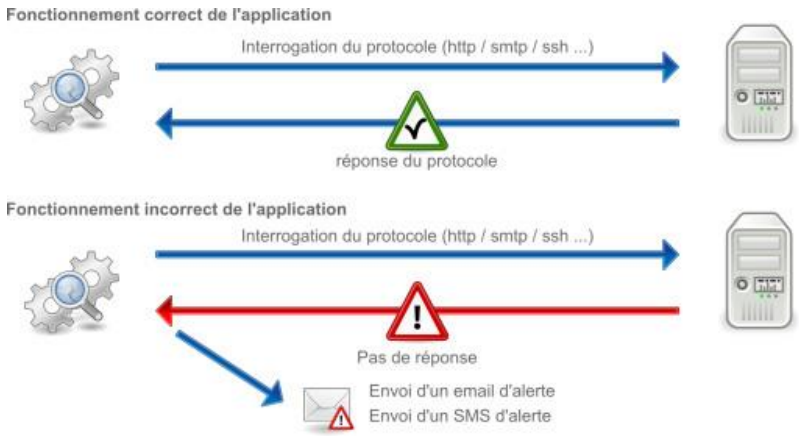


Figure 11. Schéma représentant le processus de vérification d'une machine ou d'un service.

La disponibilité s'applique également au matériel réseau d'une entreprise. On parle de Routeur, de Switch ou de Pare-feu. Un routeur assure le routage des paquets entre plusieurs réseaux indépendants, il va donc les transférer d'une interface réseau à une autre. Un switch, également

appelé commutateur réseau, est constitué de plusieurs ports Ethernet qui permettent de connecter une multitude de postes de travail ou de serveurs dans un même réseau. Il permet en plus de créer des réseaux virtuels afin de gérer le trafic interne en recevant une information et en l'envoyant vers un ou plusieurs destinataires précis. Il permet ainsi de sécuriser un réseau interne en isolant des postes de travail ou des serveurs qui ne doivent pas être accessibles par tous. Le Pare-feu va, quant à lui, protéger les machines dans un réseau interne des intrusions provenant d'un réseau externe comme Internet. Il va filtrer les données échangées sur le réseau vers l'extérieur mais également en interne.

Ces trois matériaux réseaux sont essentiels au sein de l'infrastructure d'une entreprise. Il est donc nécessaire de s'assurer de leurs bons fonctionnements et même de pouvoir surveiller une utilisation inhabituelle. En effet, tout le trafic réseau passe obligatoirement par ce matériel, il est donc indispensable de pouvoir surveiller les activités dangereuses. Pour cela, le protocole SNMP est utilisé en particulier car il est disponible sur tous les matériels réseaux administrables. Ainsi, les informations sont collectées, le statut du matériel est déterminé (allumé ou éteint), et la connaissance de la surcharge du port ou non est définie, ce qui pourrait avoir pour conséquence un disfonctionnement de celui-ci.

Figure 12. Schéma représentant le processus de vérification sur un matériel réseau via le protocole SNMP

Aujourd'hui, tous les employés d'une entreprise travaillent d'un poste de travail et ont besoin au minimum d'avoir un accès internet, que ce soit pour avoir accès à leur boite e-mail ou à un serveur de l'entreprise pour utiliser une application. L'accessibilité de tout ce trafic passe obligatoirement par ces matériaux réseaux, donc une simple indisponibilité, même minime, peut couper l'activité d'un grand nombre de collaborateurs.

L'ensemble des données collectées concernant la disponibilité sert à établir des rapports avec de précieuses données statistiques qui permettent d'optimiser l'infrastructure. Ces rapports sont exprimés selon des variables : horaire quotidienne, hebdomadaire, mensuelle ou annuelle.

Disponibilité	Indisponibilité sur une année
90 %	876 heures (environ 1 mois et 6 jours)
95 %	438 heures (environ 18 jours)
99 %	87 h 36 min (environ 3,6 jours)
99,9 %	8 h 45 min 36 s
99,99 %	52 min 33,6 s
99,999 %	5 min 15,36 s

Figure 13. Exemple de temps d'indisponibilités par an

Ces valeurs ne sont pas généralisées, chaque fournisseur de solutions dispose de ses propres taux de disponibilité. La disponibilité de service chez les hébergeurs de serveurs ou de sites internet est très importante, elle est une preuve de qualité de service et un paramètre de crédibilité et de notoriété. Il existe différents services ou médias qui réalisent régulièrement des tests sur la disponibilité des plus grands hébergeurs. Prenons l'exemple de BFM Business[1] qui réalise régulièrement des relevés ou recensement d'informations sur ces données. Les valeurs de la figure suivante ont été réalisées entre le 17/04/2017 au 16/05/2017 :

Du 17.04.2017 au 16.05.2017

rang	hébergeurs	disponibilité des sites	performance d'accès aux sites	qualité globale	tendance
1	Smile	99.99	98.10	99.52	→
2	Alter Way	99.97	98.10	99.50	↑
3	Claranet	99.98	98.00	99.49	↓
4	Ecritel	99.99	97.70	99.42	→
5	Linkbynet	99.98	97.10	99.26	↓
6	Groupe O.T.	99.98	96.00	98.98	→
7	ITS Integra	99.99	95.60	98.89	↓
8	Jouve	99.97	94.90	98.71	→
9	Prosodie/Internet Fr	99.97	94.00	98.48	↑
10	Atos Origin	99.96	93.40	98.32	↓
11	Orange Business Services	99.99	93.00	98.24	↑
12	Coreye	99.97	93.00	98.23	↑
13	Interoute / Easynet	99.95	91.70	97.89	↓
14	Colt France	99.95	90.40	97.57	↓
Moyenne		99.98	95.07	98.75	↓

Figure 14. Tableau des taux de disponibilité d'hébergeurs entre le 17/04/2017 au 16/05/2017

[1] http://bfmbusiness.bfmtv.com/services/indicateurs-ip-label/hebergement-en-haute-disponibilite/

Avant de s'orienter vers les valeurs et statistiques, les objectifs doivent être fixés surtout lorsque le choix a été fait d'héberger à l'extérieur une application ou un site internet. Ces objectifs peuvent être définis en répondant à ces différentes questions :

- Quelles sont les périodes critiques du site ?
- Combien de temps d'indisponibilité est-il acceptable en dehors des heures ouvrables ?
- Quels sont les besoins concernant l'intervalle de surveillance du service ?
- Comment savoir si le site est indisponible ?
- Qui se chargera du suivi du site ou de l'application ?

D'autres paramètres sont à prendre en compte en faisant la différence entre les périodes ouvrables et non ouvrables de l'entreprise. Les besoins peuvent être différents selon ces périodes même si le site ou l'application doivent être disponibles 24h/24 et 7j/7. Pour cela, il est important de déterminer les besoins sans se référencer à des valeurs exprimées en pourcentage, mais plutôt en caractères précis et en chiffres. Nous pouvons donc déterminer :

- Aucune indisponibilité durant les heures de travail,
- Pas plus de deux périodes non programmées d'indisponibilité par mois,
- Pas plus de cinq minutes par incidents durant les heures de travail,
- Une période programmée de maintenance par mois,
- Intervention programmée de maintenance n'excédant pas 30 minutes pendant les périodes non ouvrables par mois,
- Intervalle de surveillance de 5min,
- Surveillance des applications et non du serveur physique,
- Service de surveillance accessible partout.

Une fois que ces objectifs sont clairement déterminés, l'étape suivante est de définir les paramètres de qualité de service comme le temps de réponses des applications ou des sites internet.

3.4 La supervision des temps de réponses

Lorsque la bonne fonctionnalité du matériel réseau ainsi que des serveurs est vérifiée, l'importance va être portée sur la qualité du service qu'ils offrent. En effet, l'utilisation d'une application ou d'un site web hébergé sur un serveur transite obligatoirement par le réseau. Il existe des applications telles que les e-mails, qui sont hébergés soit en interne soit en externe, et qui doivent présenter des qualités de disponibilité mais aussi de rapidité de réponse. Le but de toute application est de

répondre rapidement à un besoin, il est donc important qu'elle ne rencontre pas de problèmes de latence. Or, ces problèmes peuvent provenir de plusieurs facteurs ; du serveur hébergeant l'application, du réseau par lequel transitent les données de l'application ou encore des deux à la fois. Quand une requête est envoyée par la machine cliente, le laps de temps compris entre l'envoi de la requête et l'accusé de réception de l'application est définis comme une latence réseau si ce temps est trop élevé. C'est pour cela que l'utilisation de l'outil Ping (*Packet INternet Groper*) est indispensable quant au traitement de cette latence qui peut être généralisée. En effet, cet outil permet l'envoi de paquets contenant de simple information de connexion tout en diagnostiquant les conditions de transmissions qu'il génère. La machine source depuis laquelle le ping est exécuté va, à intervalles réguliers, envoyer un paquet *echo request* à la machine cible. Cette machine cible va répondre et la machine source recevoir un paquet *echo reply*. Si la machine source ne reçoit pas de réponse, alors elle affichera un délai dépassé. L'outil nous permet alors de connaître le temps exact que met la requête entre l'envoi et la réception du paquet. Si le temps de réception dépasse un certain délai, alors un problème au sein du réseau est possible. Ce problème peut provenir par exemple d'un *switch* ou d'un câble usé qui ralenti la transition des paquets. Les répercussions seront donc des latences dans l'utilisation de l'application ou dans l'accès à une page web. Mais le problème peut également provenir de l'application elle-même, nous parlons dans ce cas-là d'un problème applicatif. L'application est conditionnée pour traiter toute requête qu'elle reçoit ; celle-ci peut être de différente nature, prenons l'exemple du chargement d'une nouvelle page web suite à une authentification du client. Quand l'application hébergeant le site recevra cette requête, elle aura plusieurs paramètres à traiter comme l'identité de l'utilisateur, puis le diriger vers sa page personnelle. Elle va donc commencer la vérification de l'identité de la personne sur sa base de données et la véracité de l'authentification. La base de données doit être réactive afin de ne pas retarder ce premier processus. Car tout problème rencontré sur la base de données augmente le temps d'authentification. Une fois que la vérification de l'identité de l'utilisateur est réalisée, l'application devra charger la page lui appartenant. Encore une fois, ce processus de génération de page doit être réactive afin de répondre à la requête le plus rapidement possible.

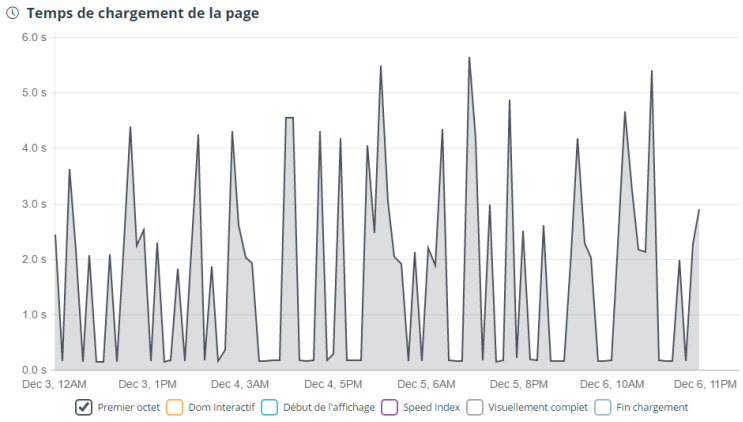


Figure 15. Schéma représentant le temps de chargement d'une page de site internet

Une latence entre deux pages web est rapidement ressentie par l'utilisateur, il est donc nécessaire de s'assurer que le temps de réponse soit optimal. D'autant plus si le site est en accès libre sur internet, destiné au grand public avec une consultation de page régulière, voire constante. Prenons l'exemple du site web de l'entreprise, qui sera accessible et regardé par un grand nombre de personne interne ou externe de l'organisation. Dans ce cas, le site représente l'image de l'entreprise et contient les informations importantes destinées aux futurs clients ou aux futurs partenaires. Ceci est particulièrement vrai quand le site internet est le seul outil de communication de l'entreprise et qu'il devient de fait la plateforme par laquelle elle échange avec ses clients. Par exemple, les sites d'achats sont les outils principaux sur lesquels les entreprises constituent leurs chiffres d'affaire.

Il est donc intéressant de vérifier les différents processus de l'application afin de s'assurer de la réactivité de celle-ci. Car si une application rencontre des problèmes de réactivité, elle peut provoquer une perte d'activité au sein d'une entreprise. Chaque latence est perçue comme une perte de temps, qui peut se multiplier par le nombre d'utilisateur de cette application. Plus le nombre d'utilisateur est important plus la perte de temps va être conséquente. Rappelons que le but premier d'une application est d'automatiser des tâches afin de faciliter le travail des employés mais également de réaliser un gain de temps. Or, si l'application ne répond pas à ces deux critères, elle n'a donc pas lieu d'être utilisée.

Ce type de supervision est très utilisé pour le contrôle des contrats de service. Ces contrats sont présents chez les hébergeurs de serveurs ou de solutions. Lorsqu'une entreprise héberge un serveur chez un prestataire, il souhaite bénéficier d'une prestation de gestion de maintenance de celui-ci ; il est question alors de mettre en place un contrat de maintenance informatique. Dans ce contrat, la partie importante consiste à définir des engagements de service appelé SLA. Le terme SLA est

l'abréviation de *Service Level Agreement* qui se traduit par accord de niveau de service, convention de service ou encore engagements de service. L'objectif est de formaliser les besoins du client de façon à les rendre clairs et ainsi fournir des critères d'évaluation de la prestation. Il permet d'établir ainsi une relation de confiance entre le client et le fournisseur et d'éliminer les attentes illusoires.

La rédaction d'un SLA varie en fonction du type de prestation. Cette prestation peut être de type réseau, applications ou hébergement (serveur) mais les critères de performance restent les mêmes. Le SLA traite les points suivant :

- La liste des services, leur description et leur étendue.
- La définition des niveaux de service et leurs critères de mesure, incluant le temps de réponse du prestataire en cas de pannes, d'incidents ou encore le taux de disponibilité du serveur.
- La sécurité et la récupération des données.
- Les dates de début et de fin de contrat.
- Les conditions de renouvellement et de résiliation.
- L'obligation d'information et de conseil par le prestataire.
- Les relations avec les tiers.
- Les litiges, les plaintes, la propriété intellectuelle et le droit applicable.
- Et enfin, le prix et les conditions de paiement.

Les entreprises qui fournissent ce type de service sont des ASP (*Application Service Provider*) qui se traduit en français par Fournisseur d'Application Hébergées. Ces entreprises fournissent via des abonnements, un accès à des applications ainsi qu'une infrastructure et une maintenance. Qu'il s'agisse d'applications, de modules spécifiques ou de solutions globales, de nombreux logiciels d'entreprise sont aujourd'hui hébergés chez un ASP. Ce type de solutions semble désormais arriver à maturité et vise une meilleure flexibilité des parcs informatiques ainsi qu'une simplification de la gestion des licences, serveurs, infrastructures. Il consiste donc à proposer une utilisation à distance de logiciels et de services informatiques. Ces fournisseurs utilisent ce type de supervision afin de garantir un suivi sur la disponibilité et de garantir une qualité au client.

3.5 La supervision des activités techniques

La supervision des activités techniques prend en compte la surveillance de tous les composants d'une application tels que les bases de données, les serveurs web, les applications de messagerie et bien d'autres. Cette surveillance est possible grâce à des sondes spécifiques qui sont installées sur les serveurs en question afin d'avoir une vision détaillée des performances de chaque service. Ce type de surveillance et les outils utilisés sont appelés APM (*Application Performance Management*) qui se traduit en français par la gestion des performances des applications. Ils permettent donc une surveillance et une gestion des performances du code et des dépendances des applications. Ils prennent également en considération la disponibilité et le temps de réponse des outils ainsi que les expériences globales des utilisateurs. Ainsi, les outils APM permettent de détecter et d'analyser les problèmes et les ralentissements empêchant la bonne exécution d'une application. Mais ce terme commence à se généraliser et être utilisé pour tout ce qui se rapporte aux performances. Certains fournisseurs de solutions l'utilisent même comme terme pour désigner tous types de supervision d'applications. Ils sont ainsi séparés en trois types d'outils de surveillance APM :

- La surveillance basée sur les applications, qui sont des outils utilisant différentes métriques de serveur et d'application. Ils peuvent déterminer le nombre de requêtes que gère une application en temps réel pour pouvoir ainsi déterminer les pages internet qui pourraient être ralenties. Cependant, ces outils ne peuvent pas déterminer si le problème provient du code de l'application.
- Les outils de performance au niveau du code de l'application qui analysent en profondeur les codes utilisés. Des outils comme *AppDynamics* ou encore *Dynatrace* répondent à ces besoins d'analyse et de suivi des transactions des applications.
- Les outils basés sur le réseau comme *Extrahop* utilisent le terme APM puisqu'ils ont la capacité de mesurer les performances des applications en fonction du trafic réseau. Mais ces outils sont plus communément nommés NPM (Network Performance Management).

Certains outils sont par contre concentrés sur les paramètres des serveurs et des applications et non sur les performances de code. Ces outils vont surveiller les performances des composants du serveur comme le CPU ou la mémoire vive mais visent à aller plus loin. En effet, pour mesurer la performance d'une application web, il est nécessaire d'analyser les journaux d'accès et de connaître la durée de demande d'une page internet. Ainsi, une comparaison de réactivité entre les pages est effectuée, les pages lentes sont mises en évidence, et une performance globale du site est dessinée. Par exemple, l'équipe de développement sera informée en temps réel si sa base de données génère des piques

d'utilisations. Ils peuvent également identifier exactement la requête de la base de données ou la requête web qui pose problème.

Les solutions APM vont aider à identifier rapidement les problèmes d'application courants et ainsi connaître l'utilisation globale des applications pour comprendre les piques de trafics ; de trouver les problèmes de lenteur ou de connexion avec les dépendances des applications comme la base de données SQL, les files d'attente ou les mises en cache ; d'identifier les requêtes SQL qui sont lentes et les pages web avec un trop gros volumes et donc des transactions conséquentes.

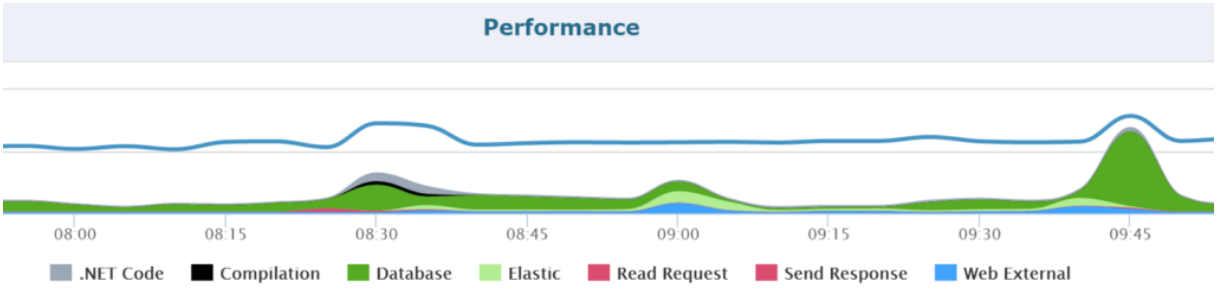


Figure 16. Schéma de performance de services

Il est intéressant, pour une équipe de développeurs, de contenir ces informations car ils pourront rapidement accéder à la cause principale du problème. Ils seront capables de mesurer les performances de chaque demande et transaction sur l'application, ce qui permet de comprendre les demandes les plus utilisées, les plus lentes et ainsi d'en déduire une amélioration. Ces problèmes peuvent venir d'une erreur ou d'un mauvais codage, il est donc important d'identifier si le problème ne s'applique qu'à une page de l'application ou s'il est général. Une surveillance réalisée tout au long de la conception de l'application peut permettre d'obtenir des informations sur le produit en question. On peut ainsi se poser des questions telles que :

- Quelles sont les méthodes clés du code utilisé ?
- Quelles méthodes impactent la rapidité de l'application ?
- Existe-t-il des problèmes de compilation ou de collecte de déchets ?
- Quelles dépendances sont appelées ?

En posant ce type question, il est plus aisé de trouver la source des problèmes rencontrés.

Prenons un exemple de problème connu au sein de nombreuses entreprises : celui d'une dépendance de l'application ou d'un problème de trafic.

Dans ce cas, la cause du problème peut être l'exécution de requête SQL trop lente. Une requête SQL est une remontée d'informations disponibles dans une base de données et exécutée dans un ordre précis. Le service de base de données peut soit contenir des incompatibilités, soit être victime d'une panne. Il est également possible que le problème provienne du service web HTTP qui échoue lors de la demande de chargement d'une page. Le dépannage des problèmes de production est difficile, mais les traces de transactions peuvent y remédier. En effet, ces traces permettent de disposer en détails des renseignements sur le code et la façon donc cela affecte l'utilisation. Elles contiennent plusieurs données telles que les informations sur la demande web comme l'adresse de la page, les informations de l'utilisateur, les dépendances utilisées (SQL, HTTP, etc.), la déclaration d'enregistrement ou encore les erreurs de l'application.

Les développeurs ont donc principalement besoin de surveiller les paramètres comme la collecte des ordures d'une application, la mise en file d'attente des demandes, les volumes de transactions, les temps de chargement des pages etc. Il peut également être essentiel de surveiller des éléments comme *Redis* qui est un magasin de structure de données en mémoire, utilisé comme base de données, cache et agent de messagerie ; ou encore des outils comme *Elasticsearch* qui permet d'effectuer et de combiner des recherches variées sur les données structurées, non-structurées, de géolocalisation ou d'indicateur.

Les paramètres standard d'un serveur ou d'une application peuvent être très utiles pour la surveillance, puisqu'ils détiennent des journaux sur les activités réalisées. Ces journaux sont très prisés par les développeurs quand une application est déployée. En effet, les journaux des applications contiennent les évènements enregistrés par celles-ci. Par exemple, une base de données va enregistrer les erreurs de fichier, ce qui est par la suite indispensable afin de cibler le problème.

D'autres problèmes sont à prendre en compte, si nous utilisons des logiciels *Middleware* qui permettent à différentes applications hébergées sur de multiples serveurs, d'échanger et de fonctionner entre elles via un réseau. Dans ce cas-là, la surveillance des applications est à combiner avec la gestion du trafic sur le réseau. Il est donc question de la supervision du temps de réponse entre elles.

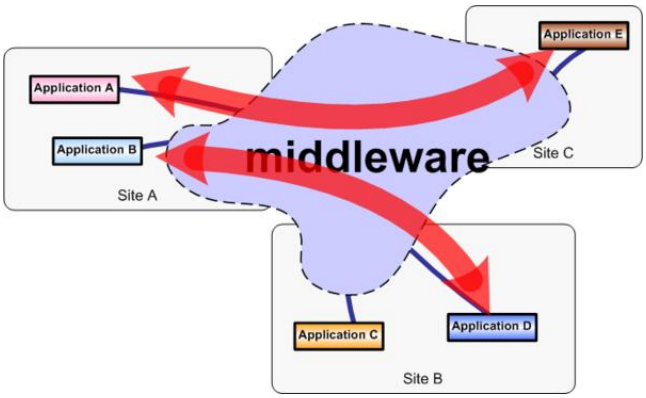


Figure 17. Schéma de communications Middleware

Le but de ces surveillances est d'éviter qu'un utilisateur contacte le SI afin de communiquer une erreur à laquelle il serait confronté et dont le SI n'aurait appréhendé. Il faut donc avoir à l'esprit l'ensemble des facteurs pouvant créer des problèmes afin de les éviter, car les erreurs sont la ligne directive de défense pour trouver un problème sur une application. Il faut donc être capable de trouver et de corriger ces erreurs avant que l'utilisateur en soit la victime. Pour cela, il faut exercer un suivi régulier des erreurs potentielles, et de disposer de rapports et d'alertes précis afin de maîtriser les différentes applications. La recommandation première est donc de disposer et de configurer les alertes importantes sur les nouvelles exceptions qui sont mises en place afin de surveiller les taux d'erreurs globaux de l'application. Avant de déployer une nouvelle application ou extension, il est important de vérifier le tableau de bord des erreurs pour avoir la certitude de l'absence de quelconques problèmes.

3.6 La supervision des activités métiers

La supervision des activités métiers ou BAM (*Business Activity Monitoring*) prend en compte l'acquisition et l'analyse en temps réel de données associées à des processus métiers de l'entreprise. La supervision est généralement divisée en deux parties : la supervision technique et la supervision métier.

La supervision technique regroupe les éléments matériels et logiciels (valeur du CPU, taux d'occupation des disques, messages des fichiers journaux, état des services d'application) et permet d'obtenir sous forme de graphique un suivi des performances (évolution en temps réel du CPU, des disques, des temps de réponse, etc.).

La supervision métier, quant à elle, permet de rassembler les indicateurs techniques en entité métier. Prenons l'exemple d'un service important pour une entreprise comme la messagerie électronique. Une messagerie d'entreprise peut rapidement devenir compliquée ; elle peut être constituée en plusieurs parties avec : deux serveurs de distributions, un serveur de nettoyage, un serveur de stockage, deux serveurs de webmail.

Avec la supervision technique, il est possible de connaître les indicateurs de chacun de ces serveurs ainsi que leurs états de fonctionnements. Or, la supervision doit être compréhensible par tout le monde en entreprise et pas uniquement les employés du SI. Les personnes décisionnelles, spécialisées dans des domaines autres que le SI, doivent connaître les évolutions et les problèmes le concernant afin de pouvoir prendre les bonnes décisions. Il faut donc pouvoir convertir les données techniques en données intelligibles et fonctionnelles. Pour illustrer ce propos, un indicateur métier représente un regroupement d'indicateurs techniques. En effet, si nous voulons avoir un indicateur métier sur l'activité du webmail de l'entreprise, nous allons regrouper les informations techniques suivantes : processus web sur les deux serveurs ainsi que l'authentification des utilisateurs sur le serveur LDAP (*Lightweight Directory Acces Protocol*) qui regroupe les identités numériques. Chaque indicateur technique impacte le métier auquel il est attaché. Par exemple :

- Si la disponibilité de l'interface du webmail est à l'état critique, alors le métier voit sa disponibilité chuter de 100%.
- Si l'état du processus HTTP sur le premier serveur est dans un état critique, alors le métier voit sa disponibilité diminuer de 1%.
- Si l'état du processus HTTP sur le deuxième serveur est dans un état critique, alors le métier voit sa disponibilité baisser de 1%.
- Si l'état du processus HTTP sur les deux serveurs est dans un état critique, alors le métier voit sa disponibilité s'écrouler de 100%.
- Si l'authentification des utilisateurs sur le serveur LDAP est dans un état critique, alors le métier voit sa disponibilité tomber de 100%.

Ainsi, nous disposons d'indicateurs métiers correspondant au service de messagerie webmail ; quand un utilisateur n'arrive pas à se connecter à l'interface web du webmail, l'activité métier est à 0% ; si seul un des deux processus HTTP fonctionne, alors la disponibilité est de 99% car nous estimons que les performances du service ne sont pas optimisées. Cet exemple est valable et adaptable à toutes les activités techniques de l'entreprise.

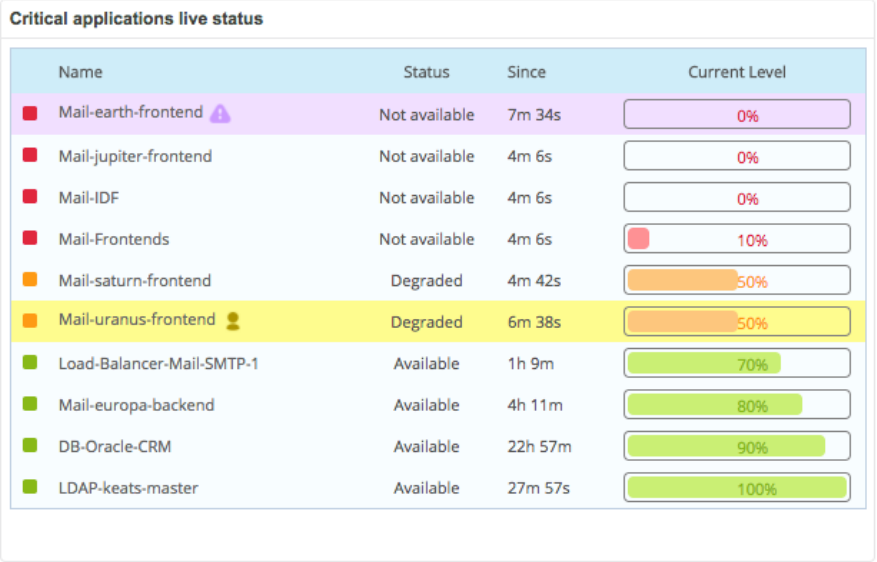


Figure 18. BAM du service de messagerie[2]

Les autres activités métiers comme l'envoi et la réception des e-mails sont également définis sur le même modèle. Il est d'ailleurs possible de créer une activité métier en regroupant plusieurs mesures d'activités techniques et ainsi créer une activité métier MAIL centralisant toutes celles liées aux e-mails.

Une solution BAM peut être utilisée dans tous les domaines d'une entreprise comme les Ressources Humaines, la Comptabilité, le CRM (Customer Relationship Management) ou une plate-forme de e-commerce. Elle fournit aux responsables fonctionnels des indicateurs de performance ou KPI (*Key Performance Indicators*) qui synthétisent l'état d'une activité métier. Sur l'exemple d'une plateforme de e-commerce, on mesure par exemple le nombre de commandes par heure ou par jour, l'état des stocks produits en temps réel, l'identification des produits les plus ou moins consultés. Les données permettant de calculer les indicateurs de performance sont récupérées grâce à des sondes logiciels spécifiques quant aux activités techniques. Les outils BAM se focalisent sur deux types de sondes : les alertes de dépassement de seuil et les alertes de performances. Certains de ces outils permettent même la création de scénarios, simulant ainsi des actions de clients consultant les sites de e-commerce. Ces scénarios sont exécutables de manière automatisée, ce qui permet de mesurer en temps réel les activités des utilisateurs et ainsi d'appréhender le fonctionnement des étapes d'achat, et de détecter les étapes à améliorer.

[2] https://blog.centreon.com/nouvelles-versions-des-produits-centreon-compatibles-centreon-3-4/?lang=fr

3.7 La supervision de l'expérience utilisateur

La supervision de l'expérience utilisateur est la dernière étape des projets de supervision. Une fois que nous avons la certitude que nos applications sont fonctionnelles, nous nous assurons, avec nos mesures de temps de réponse, que l'application est adaptée aux utilisateurs. Pour cela, nous utilisons des scénarios d'utilisation des applications en nous mettant à la place de l'utilisateur. Ces scénarios vont s'assurer du bon fonctionnement de chaque page et de chaque fonctionnalité de l'application et du temps de réponse entre chaque action possible par l'application. Les scénarios et donc les fonctionnalités sont exécutés à intervalle régulier. Les résultats sont ensuite stockés sur une base de données afin d'être retranscrits sous forme de graphique pour un suivi métier.

Le fonctionnement de cette supervision est différent suivant le type d'utilisation ; d'un côté, il y a la supervision des applications comme les sites internet ou extranet et d'un autre côté, il y a les applications internes. Pour les sites accessibles de l'extérieur, la machine de l'utilisateur n'est pas connue ni maitrisée (système d'exploitation, navigateur, logiciel de protection, etc.). Il est donc primordial de maîtriser l'application quant à sa disponibilité et sa qualité de service (temps de réponse). *« Amazon a estimé qu'un temps de chargement d'une seconde de plus lui ferait perdre près de 1,6 milliards de dollars de ventes par an »*[3]. Sachant que seuls les temps de réponses des applications en interne peuvent être évalués, une fois que les données sont sorties de l'entreprise, la qualité du temps de réponse n'est plus surveillée et donc n'est plus maitrisée. Or, pour les applications en interne, dans lesquelles le Système d'Informations doit être maîtrisé, le type de poste utilisateur et les versions des logiciels utilisées sont répertoriés. Ainsi, les données de disponibilité et de performance sont pertinentes puisqu'elles sont calculées sur et au sein d'un environnement connu.

Si un scénario échoue ou si une fonctionnalité ne répond plus, alors une alerte est levée. Si une page ou une fonctionnalité d'un site de e-commerce est inaccessible, alors le scénario va le détecter mais ne donnera pas la source du problème (serveur web, serveur d'application, base de données, etc.). Cette supervision s'appuie sur tous les autres types de supervision ; en effet, nous ne pouvons pas simplement nous appuyer sur l'expérience utilisateur car celui-ci ne nous donne en aucun cas la source du problème. Il est d'ailleurs impensable de se référencer à l'expérience d'un seul utilisateur (le développeur par exemple). Finalement, les supervisions techniques et la supervision de l'expérience utilisateur sont étroitement liées.

[3] https://www.ecommerce-nation.fr/indicateurs-webperf-ameliorer-experience-utilisateur

IV. Se confronter à l'intégration d'un outil de supervision

Le processus d'intégration d'un outil au sein d'un Système d'Information commence par la venue d'un nouveau besoin. Une fois que les besoins sont définis, il est nécessaire de prendre connaissance de l'existant du SI pour ensuite réaliser une étude de solution. A la suite de cette étude, un certain nombre de propositions se mettra en place et un choix de solution sera à réaliser en prenant compte de certains paramètres concernant le Système d'Information ; à savoir les impacts organisationnels et financiers. Une fois le choix fait, le processus d'intégration de l'outil pourra être réalisé.

4.1 Etat des lieux

Le Système d'Informations de Alter Solutions Engineering est constitué de matériels et de logiciels présents en interne mais également en externe. En ce qui concerne les matériels et logiciels en interne, l'entreprise possède :

- Un routeur/Pare-feu : matériel permettant de sécuriser le réseau interne de l'entreprise du réseau externe via des règles de sécurité.
- Trois *switchs* : équipement permettant d'élargir le nombre de matériel connecté au réseau interne de l'entreprise.
- Un serveur de stockage : contenant les données des utilisateurs ainsi que les dossiers partagés.
- Un serveur de comptabilité : contenant les applications de comptabilité sur un système Windows Server 2012 R2.
- Environ 70 postes de travail : sous des systèmes Windows, Mac et Linux.
- Environ 50 lignes téléphoniques fixes.

Les applications majeures comme les e-mails sont hébergées en externe, tout comme le site web de Alter Solutions Engineering, le CRM et les applications utilisées par les différentes équipes de développeurs de Alter Frame. Ils disposent ainsi de serveurs dédiés, qui consistent à disposer d'une machine physique totalement dédiée à l'usage de la compagnie au sein d'un hébergeur spécialisé. Ces serveurs permettent de disposer de la totalité des ressources matérielles, ainsi que la liberté de configurer totalement le serveur et d'installer les logiciels souhaités. Les serveurs dédiés sont constitués de plateforme de virtualisation, qui consiste à faire fonctionner un ou plusieurs systèmes d'exploitation ou applications comme un logiciel présent sur un serveur par exemple. Ces serveurs sont donc constitués de plusieurs machines virtuelles contenant chacune un système d'exploitation,

une application avec un espace de stockage qui lui est propre. Ils disposent également de serveurs mutualisés principalement utilisés pour l'hébergement de site web. Cette solution est aujourd'hui la plus utilisée et la moins couteuse pour héberger un site internet. Elle met à disposition un site web qui est hébergé sur un serveur partageant ses ressources avec d'autres sites web appartenant sûrement à d'autres clients de l'hébergeur. Cet hébergement est préconfiguré et pré-paramétré, il n'est donc pas possible de personnaliser le système, le serveur web, les applications ou les services.

Les serveurs dédiés sont donc constitués d'une plateforme de virtualisation contenant plusieurs machines virtuelles. Ces machines virtuelles sont principalement sous une distribution Linux et plus précisément sous un système Debian. Ce système est totalement gratuit et dispose d'un grand nombre de logiciels et de paquets disponibles. Il est ainsi l'un des systèmes Linux le plus complet et donc compatible à toutes utilisations. En 2002, il était constitué d'environ 8 500 paquets et aujourd'hui, il en dispose plus de 43 000 (voir la figure 19 ci-dessous).

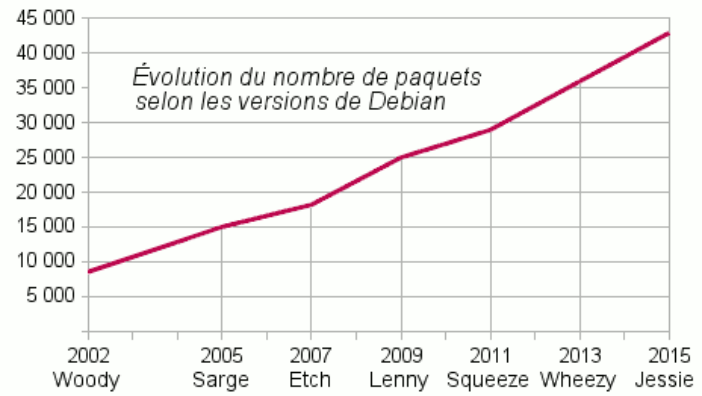


Figure 19. Schéma représentant l'évolution du nombre de paquets selon les versions de Debian, entre les années 2002 et 2015

Le système Debian est également réputé pour sa qualité, puisqu'il est régulièrement mis à jour pour des améliorations sur les applications ou pour des raisons de sécurité. De plus, avant l'intégration totale des nouvelles mises à jour, une version de test est mise en ligne appelée *testing*, cette version est déconseillée aux utilisations de production (entreprise) avant confirmation de son efficacité. Puis une version dite stable est partagée une fois que tous les correctifs sont apportés.

Le système Debian est ainsi le système d'exploitation le plus apte à répondre aux besoins de production pour tout type d'application. Il est également le système le plus maîtrisé par les développeurs et administrateurs système de Alter Solutions Engineering.

4.2 Etude des solutions

Parmi les solutions en sources ouvertes, c'est-à-dire gratuites et accessibles par tous les utilisateurs d'internet, qui sont adaptées au monde de l'entreprise, nous comptons deux principaux outils. Ces outils sont Centreon et Zabbix, deux solutions centrées sur la supervision informatique.

Premièrement, Centreon est une solution de supervision de systèmes, de réseaux et d'applications. Cette application est gratuite mais son cœur d'application dispose de modules complémentaires qui sont payants. Elle fournit une interface simple sur l'état d'un Système d'Informations et est éditée par une société française nommé Merethis. Centreon est basé sur Nagios, qui fut créé en 1996. Nagios est un ancien logiciel de supervision destiné à informer de problèmes éventuels dans le SI d'une compagnie avant que les clients, utilisateurs ou managers ne le fasse. Il surveille ainsi les machines physiques et virtuelles ainsi que les services qu'il utilise, et alerte lors d'un dysfonctionnement et même lorsque le problème est résolu. Ce logiciel est libre et sous licence GPL (Licence Publique Générale) et composé de trois parties :

- Le moteur de l'application qui ordonne les tâches de la supervision.
- L'interface web permettant une vue d'ensemble du Système d'Informations.
- Les sondes permettant de surveiller les différents services souhaités et pouvant être adaptées à nos besoins.

Nagios est certes performant mais peu ergonomique puisque son interface web est basée sur le langage CGI (*Common Gateway Interface*) qui permet seulement un affichage sur une page web. Il est ainsi impossible de modifier via l'interface web les paramètres de Nagios.

Centreon, quant à lui, utilise du langage PHP qui permet d'accéder à une page dynamique. Il est ainsi une surcouche de Nagios, et permet donc via l'interface graphique de configurer les options ; ces configurations seront par la suite réécrites dans les fichiers de Nagios. L'interface de Centreon va également remonter et exploiter les données collectées par Nagios, récupérées via l'outil NDOutils (*Nagios Remote Plugin Executor*) en stockant les évènements dans une base de données.

En 2012, Centreon intègre son propre moteur de collecte appelé *Centreon Engine* - version améliorée de Nagios -, ainsi qu'un nouveau gestionnaire d'événement appelé *Centreon Broker* et d'une interface web gérée par *Centreon Web*. Ces intégrations permettent aujourd'hui à Centreon de fournir les fonctionnalités suivantes :

- Consulter la métrologie et l'état des machines et des services,
- Tableau de bord modifiable via des *widgets*** accessibles depuis une interface web,

- Définir les hiérarchies du réseau pour déterminer les machines arrêtées et les machines non-joignables,
- Surveillance active et passive via de nombreux protocoles et agents de supervision,
- Gestion avancée des alertes,
- Gestion avancée des droits d'accès utilisateurs,
- Automatisation d'actions correctives sur une machine ou un service,
- Chiffrement des communications avec authentification des flux via un certificat.

Centreon partage les prérequis pour une installation du système en fonction du nombre d'hôtes à surveiller.

Nombre de services	Nombre d'hôtes estimé	Nombre de collecteurs	Central	Colleteur
<500	50	1 central	1 vCPU / 1 Go RAM	
500 – 2000	50 – 200	1 central	2 vCPU / 2Go RAM	
2000 – 10000	200 – 1000	1 central + 1 collecteur	4 vCPU / 4 Go RAM	1 vCPU / 2 Go RAM
10000 – 20000	1000 – 2000	1 central + 1 collecteur	4 vCPU / 8 Go RAM	2 vCPU / 2 Go RAM
20000 – 50000	2000 – 5000	1 central + 2 collecteurs	4 vCPU / 8 Go RAM	4 vCPU / 2 Go RAM
50000 – 100000	5000 – 10000	1 central + 3 collecteurs	4 vCPU / 8 Go RAM	4 vCPU / 2 Go RAM

Figure 20. Tableau des prérequis d'installation de Centreon[4]

Dans le tableau de la figure 20, nous constatons que plus le nombre d'hôtes est élevé, plus la demande de ressources est importante. En effet, pour surveiller au minimum 50 000 hôtes il est conseillé de disposer d'une machine serveur central qui centralise toutes les données traitées par trois collecteurs.

Certaines de ces fonctionnalités sont intégrées parmi les modules payants de Centreon ; les principaux sont Centreon MAP, Centreon MBI et Centreon BAM. Centreon MAP est un outil de modélisation et de visualisation de l'état du Système d'Informations en temps réel. Il est composé

[4] https://documentation-fr.centreon.com/docs/centreon/en/2.8.x/installation/prerequisites.html

d'une librairie graphique totalement et facilement manipulable et configurable. Il permet ainsi d'avoir une vue d'ensemble de l'infrastructure et de gérer différents schémas qui peuvent être consultés par différents utilisateurs. Ces schémas sont interactifs, c'est-à-dire qu'ils permettent de réaliser des tâches à partir de la représentation graphique du matériel ou du service. Centreon MBI (*Monitoring Business Intelligence*) est un outil d'aide à la décision et facilite la gestion de l'infrastructure en apportant une visibilité sur les activités de l'infrastructure. Il génère des compteurs de performances et des données de capacité sur les différents services du Système d'Informations. Centreon BAM (*Business Activity Monitoring*) est adapté pour les équipes non techniques de l'entreprise à avoir une perspective du Système d'Informations.

La deuxième solution de supervision gratuite est Zabbix, qui fut créée en 1998 mais passe seulement sous licence GPL en 2001 avec une version alpha et atteint sa version finale en 2004. Elle est développée en langage C et également constitué d'une interface web développée en PHP et en JavaScript. L'évolution de cette solution est constante puisque deux mises à jour majeures sont réalisées par an. Aujourd'hui, Zabbix est sous licence GPL par l'entreprise Zabbix SIA fondée en 2005 afin de fournir un support technique aux professionnels ainsi que des services d'intégration, de déploiement, de consulting et de formation. Elle a ainsi développé déférents partenariats avec de grandes entreprises internationales. Avec une croissance constante, Zabbix est devenue depuis quelques années, l'une des applications gratuites de supervision les plus populaires à l'international.

Zabbix est décomposé en plusieurs parties. La première étant la partie serveur, qui est la composante principale de l'application. Elle permet de surveiller à distance mais également sur une infrastructure en local, les matériels et les différents services comme les serveurs web, les serveurs de messagerie et bien d'autres. Elle gère également la notification aux administrateurs de l'infrastructure par e-mail. Pour cela, elle utilise le protocole SNMP, que nous avons détaillés précédemment, afin de superviser les hôtes, mais dispose également d'un agent à installer sur les machines à surveiller afin de récupérer les informations nécessaires en temps réel.

Zabbix est aussi composé de trois « filiales » ou interfaces :

- *Zabbix Frontend,* qui est l'interface de visualisation des événements mais surtout l'interface d'administration et de configuration. *Zabbix Frontend* est une interface web développée en PHP, elle est donc accessible sur toutes les plateformes intégrant un navigateur internet.
- *Zabbix Proxy,* qui collecte les informations de performance et de disponibilité des hôtes, pour ensuite les transmettre au serveur Zabbix. Il permet ainsi de réduire la charge du serveur puisque les informations collectées par le *Proxy* seront traitées sur l'hôte avant d'être

transmises au serveur. Cette solution est idéale quand le nombre d'hôtes est important, car le nombre d'information transitant sur le réseau sera réduit, ainsi que les ressources du serveur qui auraient dû être utilisées pour traiter ces informations. Il est également indispensable quand plusieurs machines hôtes sont distantes (hébergées sur un site différent).

- *Zabbix Agent* permet un déploiement rapide sur les machines systèmes. Cet agent est optimisé pour la surveillance des ressources locales d'un hôte ainsi que les applications qu'il détient. Mais il n'est pas utilisable sur les différents matériaux réseaux comme les routeurs, *swicths*, etc.

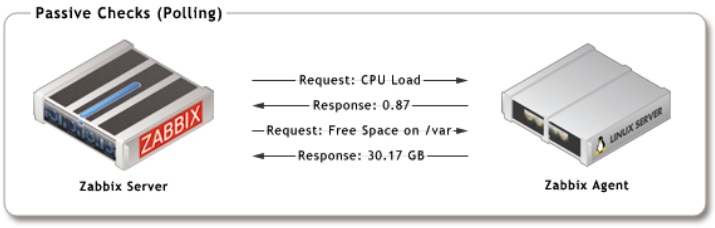


Figure 21. Schéma représentant les informations échangées entre le serveur Zabbix et l'agent installé sur un hôte

La capacité sur le serveur Zabbix dépend du nombre d'hôte que nous devons surveiller, l'organisme français d'information sur la supervision donne un référentiel sur la configuration nécessaire des serveurs. (Cf figure 23 suivante).

Type	Plateforme	Processeur	Mémoire RAM	Hôtes
Petite	Ubuntu Linux	Pentium II	256 Mo	20
Moyenne	Ubuntu Linux 64 bits	AMD Athlon 3200+	2 Go	500
Grande	Ubuntu Linux 64 bits	Intel Dual Core 6400	4 Go	>1000
Très grande	RedHat Entreprise	Intel Xeon 2xCPU	8 Go	>10000

Figure 22. Tableau des prérequis du serveur Zabbix en fonction du nombre d'hôte

4.3 Choix de la solution

Chaque outil dispose de ses avantages et de ses inconvénients, voici donc un comparatif des deux solutions.

Centreon est un outil adapté aux grandes infrastructures, car il demande de plus grosses ressources que Zabbix. Son installation est simple via des installateurs mis à disposition comprenant en particulier son l'installation complète et de tous les paquets nécessaires. Il est également simple à configurer via son interface internet et dispose pour le réseau interne, d'une découverte automatique des hôtes via un protocole NMAP. L'interface internet permet également d'afficher les résultats sur les alertes grâce à son système de *reporting*. Mais elle contient certains inconvénients comme l'outil *Centreon MAP* qui est un complément payant de l'application. Cet outil est très pratique mais également indispensable quand nous voulons superviser un Système d'Informations. L'outil MAP permet d'avoir un visuel simple et constant sur l'infrastructure, et de pouvoir réagir rapidement en cas de problème sur un hôte en ayant un indicateur sur l'emplacement de celui-ci. Il est ainsi impossible de disposer de cette option qui est pourtant importante et pratique sur la version gratuite de l'outil. De plus, il est impossible de créer et de paramétrer un écran contenant différents graphiques provenant de différents services et hôtes. Ceci permettrait d'avoir une vue en temps réel sur un ensemble de valeurs d'hôtes et de services différents. Une option qui serait encore une fois intéressante pour faciliter l'analyse des besoins du Système d'Informations.

A contrario, Zabbix est un outil adapté aux petites et moyennes infrastructures, exigeant peu de ressources comme nous avons pu le voir précédemment. Un des points forts de Zabbix est qu'il contient énormément de sondes différentes répondant ainsi à beaucoup d'exigences des administrateurs systèmes et réseaux comme par exemple la supervision d'une application web. Effectivement, il permet de récupérer des informations comme le temps de réponse ainsi que la vitesse des transferts qui sont des éléments indispensables au bon fonctionnement d'un site internet. Il permet également une configuration totale depuis l'interface web, ainsi que la possibilité de mettre à jour Zabbix en « quelques clics » sur celle-ci. Il dispose comme Centreon d'un collecteur, appelé *Zabbix Proxy,* dont nous avons détaillés les caractéristiques dans la partie précédente, qui collecte les informations des hôtes pour ensuite le redistribuer au serveur. De plus, l'agent installé sur les hôtes est léger, ce qui permet de ne pas surcharger des hôtes qui contiennent déjà énormément d'applications, et permet de ne pas avoir à prendre en compte un espace trop important pour l'intégration de cet agent sur ces machines. Depuis la version 3.0, sortie en février 2016, Zabbix chiffre les échanges entre tous les composants basés sur le protocole TLS** (*Transport*

Layer Security) ce qui n'était pas le cas avant. Ce problème était important car si des hôtes étaient surveillées à distance, alors les informations les concernant était lisibles par tous.

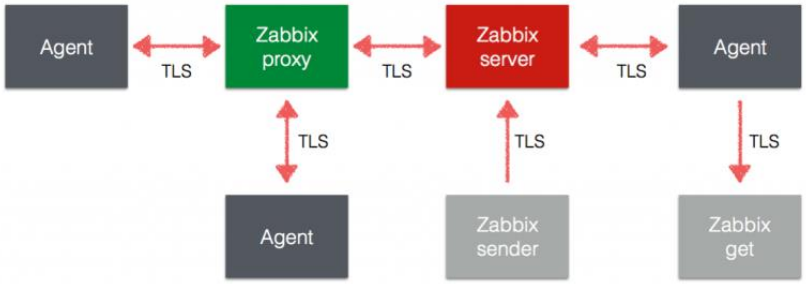


Figure 23. Chiffrement des échanges entre les composants Zabbix[6]

Une autre fonctionnalité très intéressante de la version 3.0 est celle qui permet d'avoir des prévisions sur la qualité de service des hôtes. Il est ainsi possible d'avoir une estimation sur le temps restant avant qu'un disque dur ne soit complet. Ceci facilite le pilotage du Système d'Informations en calculant les risques potentiels à venir.

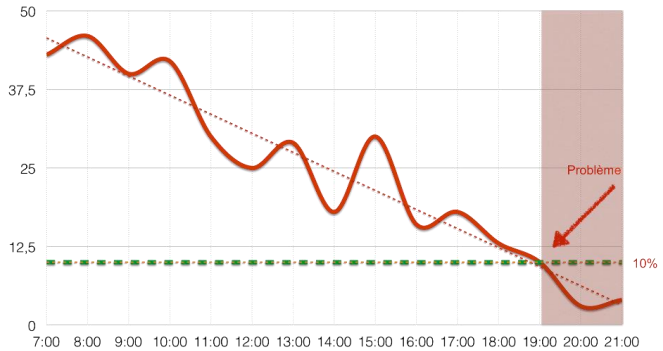


Figure 24. Prévision de criticité sur l'espace de stockage d'un disque dur

Les inconvénients de Zabbix sont la mise en place des *templates* (ensemble de configurations) nécessitant une connaissance accrue de ces configurations. De plus, c'est un outil totalement indépendant, c'est-à-dire qu'il ne fonctionne et ne communique avec aucun autre logiciel.

Alter Solutions Engineering a donc choisi d'intégrer l'outil Zabbix car il répond favorablement aux besoins définis en deuxième partie. Effectivement, il permettra de surveiller le matériel réseau via le protocole SNMP ainsi que les machines sous système Windows et Linux et les services nécessaires

[6] https://steve.destivelle.me/zabbix-3-0-est-sorti/

aux applications grâce à l'agent Zabbix. Les informations seront transmises au serveur contenant l'application Zabbix, qui ne demande que peu de ressources tant au niveau matériel qu'au niveau du trafic sur le réseau entre les hôtes et le serveur. Il serait problématique que l'application prenne une grosse partie de la bande passante du réseau interne de l'entreprise. De plus, le serveur Zabbix est compatible pour fonctionner sur un système Debian (Linux) maitrisé par nos équipes d'administrateurs système et nos développeurs.

L'interface web permet de paramétrer totalement les différentes options via une connexion sécurisée. Elle permet également de créer des groupes d'utilisateurs afin de déterminer des droits spécifiques. Ainsi, nous pouvons donner l'accès à la surveillance de certains hôtes aux personnes chargés du projet avec des droits différents : accès aux graphiques des différents composants, envoi d'alertes, etc. Nous pouvons aussi créer un profil dédié pour les clients de Alter Frame afin qu'ils aient accès en temps réel aux informations de leurs applications via l'interface web.

Via l'interface web, nous pouvons configurer l'envoi des alertes par e-mail, et déterminer quelles données (alertes) doivent être envoyées. Il est effectivement possible de configurer des alertes différentes en fonction des groupes utilisateurs, ce qui permet de différencier les informations communiquées aux développeurs et celles pouvant être communiquées aux clients.

L'outil répond ainsi à nos besoins et est facilement intégrable au sein de notre Système d'Informations. Cette intégration, a obligatoirement des impacts, autant sur le SI qu'au niveau organisationnel et financier.

4.4 Identification des impacts

4.4.1 Impacts sur le Système d'Informations

L'intégration d'un nouvel outil au sein d'un Système d'Informations a quelques impacts sur le SI et l'entreprise qu'il est intéressant d'énumérer dans cette étude. Zabbix doit disposer d'un serveur dans lequel sont centralisées toutes les données de surveillance. Ce serveur doit donc être intégré à l'infrastructure en prenant compte de certains paramètres. Le serveur doit disposer des ressources nécessaires en fonction du nombre de matériels et de services qu'il devra superviser, via un serveur physique ou un serveur virtuel. Dans le cas de Alter Solutions Engineering, nous avons décidé de le « virtualiser ». Il faut par la suite lui attribuer un adressage au sein du réseau interne de l'entreprise pour qu'il puisse communiquer avec les différents équipements. Nous devons également créer des règles de routage afin que le réseau interne puisse accéder vers l'extérieur, et ainsi être également

accessible de l'extérieur pour accéder à l'interface web de l'entreprise. Cette interface web devra également détenir un certificat afin de sécuriser les échanges vers l'extérieur et ainsi approuver la légitimité des données.

Des changements sur les équipements réseaux à superviser seront également nécessaires puisque l'outil transite via le protocole SNMP. Ainsi, les équipements devront supporter ce protocole et devront être activés. Des changements seront également apportés sur les serveurs à surveiller puisque l'agent Zabbix devra être installé pour remonter les informations au serveur Zabbix.

L'outil Zabbix étant totalement indépendant, il n'aura ainsi aucun impact sur le fonctionnement d'un matériel ou d'un logiciel existant.

4.4.2 Impacts organisationnels

L'intégration d'un nouvel outil aura un impact au niveau de l'organisation d'une entreprise, puisqu'il amènera à des changements. Cet outil aura pour objectif d'être utilisé par plusieurs équipes ; les personnes formant ces équipes ne seront pas formées à l'outil. Il faudra donc prendre en compte la mise en place de formations sur l'outil Zabbix en fonction des besoins de chaque équipe. Une fois que ces équipes sont formées, une homologation de l'intégration de cet outil devra être mise en place pour tous les nouveaux équipements et services. Ainsi, à la création d'une nouvelle machine virtuelle qui hébergera une application par exemple, l'agent Zabbix devra être installé et configuré pour envoyer les informations au serveur Zabbix. Pour que les informations soient réceptionnées, l'administrateur du serveur Zabbix devra être au courant de cette nouvelle implémentation afin de le configurer sur le serveur. L'outil devra être implémenté dès la création de cette machine virtuelle et ainsi être testé en préproduction, c'est-à-dire avant la mise en production de l'application. Ceci permettra de réaliser des tests et d'avoir la certitude que les composants importants de l'application soient supervisés.

L'outil permettra d'augmenter la réactivité des équipes chargées de faire fonctionner un équipement ou une application. Restons sur l'exemple de l'application, dans ce cas, le bon fonctionnement de l'application dépend des équipes de développement mais également des équipes systèmes. Si au cours du projet, un développeur remarque que les ressources attribuées à la machine hébergeant l'application ne sont pas nécessaires, il devra le communiquer aux équipes systèmes. Ces équipes devront faire une vérification pour déterminer si la machine en question est en réel manque de ressource. De plus, pour déterminer si ce manque n'est pas ponctuel, c'est-à-dire un manque de ressource à un moment précis pouvant venir d'une mauvaise configuration faite par un développeur,

l'équipe système aura besoin d'informations sur une durée étendue. Ce processus peut prendre un certain temps, qui peut être allégé si l'équipe système dispose déjà de toutes les informations.

La communication entre les services sera ainsi améliorée avec des informations adaptées aux types d'utilisateurs, via des données techniques (valeur exacte de l'utilisation de la RAM), des données quantifiables (pourcentage d'espace disque) et des graphiques représentatifs.

4.4.3 Impacts financiers

Zabbix étant un outil totalement gratuit, et répondant entièrement à nos besoins, l'impact financier de l'intégration de cet outil ne sera pas conséquent. Disposant déjà de matériels pris en charge par l'outil, autant réseaux que serveurs, l'achat de nouveaux matériels ne sera pas nécessaire. Cependant, l'outil central devra être installé sur un serveur qui sera totalement et uniquement dédié à cet usage. Si une entreprise n'utilise pas de virtualisation, alors l'achat d'un serveur physique est obligatoire. Les caractéristiques de ce serveur seront déterminées par le nombre total de matériel à superviser (Cf figure 22). Dans le cas de Alter Solutions Engineering, l'utilisation de machine virtuelle est favorisée, permettant ainsi de ne pas acheter un nouveau serveur, en partageant les ressources d'un seul serveur dédié à la virtualisation.

Le seul coût envisageable est celui d'un certificat afin que l'interface web de Zabbix soit sécurisée. Ce certificat est à prendre en compte seulement si cette interface doit être accessible depuis l'extérieur du réseau de l'entreprise. Il sera donc obligatoire si les équipes devant accéder aux informations de l'outil sont implémentées sur des sites distants.

Une perte financière peut-être envisageable si les équipes devant utiliser cet outil doivent être formées. Mais cette perte sera rapidement compensée, puisqu'il améliorera la rapidité d'intervention ; il permettra d'anticiper les éventuels incidents et de réduire les risques ; et il améliorera le pilotage du Système d'Informations pour une meilleure productivité.

Conclusion

La place de l'informatique est aujourd'hui importante dans toutes les entreprises, qu'elles soient petites, moyennes, ou multinationales, et nécessite une attention particulière pour améliorer la productivité et les services proposés. Pour répondre à ces différents besoins, le Système d'Informations a tendance à devenir complexe par sa multitude, voire sa multiplication, d'applications. Son maintien devient ainsi difficile et imprévisible, il est donc important de le surveiller. Les enjeux majeurs des équipes informatiques sont de garantir la disponibilité et le niveau de service en cas de panne ou de dégradation mais également d'anticiper les incidents, et/ou de garantir une remontée de service rapide avec des durées d'intervention minimes.

Aujourd'hui, il existe de nombreux outils répondant à cette problématique qui doivent s'adapter à toutes les infrastructures ; ils peuvent donc être intégrer au sein de PME mais également au sein de grandes entreprises. On appelle ce processus la supervision qui répond aux exigences techniques et aide en particulier au pilotage d'un Système d'Informations. Ces outils nous permettent, effectivement, de disposer d'informations en temps réel en ce qui concerne nos infrastructures par la surveillance. Ils permettent, grâce à une visualisation du SI, d'intervenir plus rapidement sur les incidents, mais également d'anticiper les futurs problèmes. La supervision est en effet un enjeu primordial par rapport au pilotage du SI, qui doit correspondre aux objectifs métiers et à l'opérationnalité de l'organisation. Les indicateurs fournis par ces outils faciliteront les éventuelles évolutions à mettre en œuvre permettant d'intégrer des services innovants et ainsi d'améliorer la compétitivité de l'entreprise.

Ce processus de supervision est amené à être standardisé, puisque le but principal dans tous les domaines de compétence est d'automatiser au maximum les tâches régulières. L'automatisation est considérée comme un progrès technique et technologique contenant des pratiques susceptibles de remplacer les interventions humaines. Elles visent ainsi à réduire le travail de surveillance et de contrôle humain, permettant ainsi de réaliser des tâches répétitives voire dangereuses, de manière plus efficace sans forcément mettre en danger des vies humaines. Cette automatisation vise à accroître la rapidité et la précision d'exécution, voire à réaliser des actions impossibles par un humain. Le secteur le plus impacté par l'automatisation de tâches est l'automobile ; celle-ci ayant pour objectif de créer des voitures totalement autonomes. Pour que les systèmes soient autonomes, ceux-ci doivent pouvoir être supervisés ou se superviser tout seul. Ce système d'automatisation amène à la résolution d'incidents qu'ils se soient déjà déroulés ou qui peuvent se produire.

Bibliographie

Association Métrodiff [s.d] Qu'est-ce que la métrologie. Disponible sur http://www.metrodiff.org/cmsms/index.php/metrologie-contemporaine/qu-est-ce-que-metrologie.html

Bell S. (2015) Les 5 grands principes de la gestion du risque informatique. Disponible sur http://www.journaldunet.com/solutions/expert/63147/les-5-grands-principes-de-la-gestion-du-risque-informatique.shtml

BFMBusiness [s.d] Hébergement en haute disponibilité. Disponible sur http://bfmbusiness.bfmtv.com/services/indicateurs-ip-label/hebergement-en-haute-disponibilite/

Cacheux C. (2014) La supervision métier en temps réel : nouveau levier d'optimisation pour les sites marchands. Disponible sur http://www.journaldunet.com/ebusiness/expert/57755/la-supervision-metier-en-temps-reel---nouveau-levier-d-optimisation-pour-les-sites-marchands.shtml

Centreon (2016) Nouvelles versions des produits Centreon compatibles Centreon 3.4. Disponible sur https://blog.centreon.com/nouvelles-versions-des-produits-centreon-compatibles-centreon-3-4/?lang=fr

Destivelle S. (2016) Zabbix 3.0 est sorti. Disponible sur https://steve.destivelle.me/zabbix-3-0-est-sorti/

Dorigny M. (2015) Monitoring : supervision et métrologie. Disponible sur https://www.it-connect.fr/monitoring-supervision-et-metrologie/

Dulot J. (2017) Quels indicateurs webperf pour améliorer votre expérience utilisateur ? Disponible sur https://www.ecommerce-nation.fr/indicateurs-webperf-ameliorer-experience-utilisateur/

Legros B. et Fontaine L. (2016) Centreon, Maîtrisez la supervision de votre Système d'Information 2ème édition. Edition ENI.

Majdoub A. (2016) Nagios, La clé de la supervision informatique. Edition ENI.

OVH [s.d] Haute Disponibilité. Disponible sur https://www.ovh.com/fr/solutions/ip-load-balancing/haute-disponibilite.xml

Polito J. (2016) Monitoring et supervision. Disponible sur https://www.supinfo.com/articles/single/2789-monitoring-supervision

POM Marketing (2014) Supervision informatique ou pilotage du système d'information ? Parlon-nous de la même chose ? Disponible sur http://www.pom-monitoring.com/blog/supervision-informatique-ou-pilotage-du-systeme-dinformation-parlons-nous-de-la-meme-chose/

Smile [s.d] Qu'est-ce qu'un Middleware ? Disponible sur http://middleware.smile.fr/Concepts-des-moms-et-jms/Qu-est-ce-qu-un-middleware

Stackify (2017) What is APM ? Disponible sur https://stackify.com/what-is-apm/

Top10Hebergeurs [s.d] 99,9 % de disponibilité, mythe ou réalité. Disponible sur http://www.top10hebergeurs.com/articles/realite_disponibilite.htm

Table des illustrations

Glossaire

BUS : Ensemble de liaison physique (câbles, etc.) pouvant être exploitées en commun par plusieurs éléments matériels afin de communiquer.

CPU : Représente le processeur qui est un composant présent dans de nombreux composants électroniques qui permet d'exécuter des instructions machine des programmes informatique.

FTP : Protocole de communication destiné au partage de fichiers sur un réseau.

NTP : Protocole permettant de synchroniser l'horloge locale d'un ordinateur via une référence d'heure défini.

RFC : Ensemble de documents qui font référence auprès de la Communauté Internet et qui décrivent, spécifient, aident à l'implémentation, standardisent et débattent de la majorité des normes, standards, technologies et protocole liés à Internet et aux réseaux en général.

TCP : Principal protocole de la couche de transport du modèle TCP/IP. Il permet au niveau applications, de gérer les données en provenance ou à destination de la couche inférieur IP.

TLS : Protocole de sécurisation des échanges internet.

UUCP : Ensemble de programmes qui permettent à deux machines d'échanger des fichiers et d'exécuter des commandes sur la machine distante.

Widgets : Composant d'interface graphique avec lequel un utilisateur peut interagir.

Liste des abréviations

AMDEC :	Analyse des Modes de Défaillances, de leurs Effets, et de leur Criticité
APM :	Application Performance Management
ASCII :	American Standard Code of Information Interchange
ASIC :	Application Specific Integrated Circuit
ASP :	Application Service Provider
BAM :	Business Activity Monitoring
BMC :	Baseboard Management Controller
CAO :	Conception Assistée par Ordinateur
CEM :	Compatibilité ElectroMagnétique
CFD :	Computational Fluid Dynamics
CGI :	Common Gateway Interface
CPU :	Central Processing Unit
CRM :	Customer Relationship Management
DAO :	Dessin Assisté par Ordinateur
FPGA :	Field Programmable Gate Array
FTP :	File Transfert Protocol
GPL :	Licence Publique Générale
HTTP :	HyperText Transfert Protocol
IETF :	Internet Engineering Task Force
IHM :	Interface Homme Machine
IIS :	Internet Information Services
IPMI :	Intelligent Platform Management Interface
KPI :	Key Performance Indicators
LDAP :	Lightweight Directory Acces Protocol
MBI :	Monitoring Business Intelligence
MIB :	Management Information Base
NDOuils :	Nagios Remote Plugin Executor
NMS :	Network Management Station
OID :	Object Identification

OSI :	Open Systems Interconnexion
PHP :	Hypertext Preprocessor
PING	Packet INternet Groper
PME :	Petites et Moyennes Entreprises
PSSI :	Politique de Sécurité du Système d'Information
RAM :	Random Access Memory
R&D	Recherche et Développement
RDM :	Résistance Des Matériaux
RFC :	Request For Comments
RH :	Ressources Humaines
RMON :	Remote MONitoring
SDR :	Software Defined Radio
SI :	Système d'Information
SIEM :	Security Information and Event Management
SLA :	Service Level Agreement
SMI :	Structure of Management Information
SMSI :	Système de Management de la Sécurité de l'Information
SNMP :	Simple Network Management Protocol
SOAP :	Simple Object Access Protocol
SSH :	Secure SHell
SSI :	Sécurité des Systèmes d'Information
SSL :	Secure Sockets Layer
TCP :	Transmission Control Protocol
TIC :	Technologies de l'Information et de la Communication
TLS :	Transport Layer Security
UDP :	User Datagrem Protocol
USM :	User-based Security Model
UUCP :	Unix to Unix Copy Protocol
VRD :	Voirie et Réseau Divers