Gestion du déploiement d'une solution de supervision réseau multi-sites

Guillaume Leroy

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS

Centre régional associé de Nouvelle-Aquitaine

MÉMOIRE

Présenté en vue d'obtenir

LE DIPLÔME D'INGÉNIEUR CNAM

en

INFORMATIQUE

Option Informatique, Réseaux, Systèmes et Multimédia

par

Guillaume LEROY

Gestion du déploiement d'une solution de supervision réseau multi-sites

Soutenu le 28 juin 2017

JURY

Président : M. Pierre Paradinas, Professeur, Cnam Paris

Membres : M. Richard Castanet, Professeur émérite, Bordeaux INP

M. Laurent Fallot, Maître de Conférences, Bordeaux INP

M. Mohamed Mosbah, Professeur, Bordeaux INP

M. Jérôme Mazet, Responsable Maintenance, Corenso France

Remerciements

Je tiens tout d'abord à remercier l'équipe informatique de Powerflute et particulièrement M. Patrick Kittle pour la confiance qu'il m'a témoignée en m'accordant la responsabilité de la mise en place de ce nouvel outil, ainsi que M. Gavin McKay pour son aide précieuse tout au long de ce projet.

Je remercie également Mme Stéphanie Claustres qui m'a permis de réaliser ce mémoire au sein de son entreprise et mon responsable M. Jérôme Mazet, pour ses encouragements dans ma démarche diplômante et m'avoir transmis ce sens de la rigueur durant nos 10 années de collaboration sur le site de Corenso France. Je le remercie particulièrement pour ses conseils avisés lors de la réalisation de ce projet et la rédaction de ce mémoire.

Je remercie bien entendu l'ensemble du corps enseignant et les agents du CNAM Nouvelle-Aquitaine que j'ai côtoyé pendant ces 5 dernières années et particulièrement M. Laurent Fallot et M. Mohamed Mosbah pour leur accompagnement et le temps qu'ils m'ont consacré tout au long de la réalisation de mon mémoire.

Enfin, je remercie mes parents pour leur soutien et leurs encouragements incessants et bien entendu ma compagne pour son aide précieuse et les sacrifices qu'elle a consentis lors de mon parcours au CNAM Nouvelle-Aquitaine.

Liste des abréviations

Abréviation	Description
ACL	Access Control List
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
BMC	Baseboard Management Controller
CCTA	Central Computing and Telecomms Agency
CIM	Common Information Model
CQL	CIM Query Language
DMTF	Distributed Management Task Force
DMZ	DeMilitarized Zone
DNS	Domain Name System
DSI	Direction des Services Informatiques
ERP	Enterprise Ressource Planning
GPAO	Gestion de Production Assistée par Ordinateur
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMB	Intelligent Chassis Management Bus
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IHM	Interface Homme Machine
IIS	Internet Information Services
IOS	Internetwork Operating System
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
KPI	Key Performance Indicators
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
MOA	Maîtrise d'OuvrAge
MOE	Maîtrise d'Œuvre
MPLS	MultiProtocol Label Switching
NSM	Network System Management
OID	Object IDentifier
OS	Operating System
OSI	Open System Interconnection
PDCA	Planifier Développer Contrôler Ajuster
PDU	Protocol Data Unit
PGI	Progiciel de Gestion Intégré
RDS	Remote Desktop Service
RPC	Remote Procedure Call
RPM	Red Hat Package Manager
RSYNC	Remote SYNChronization
RTSP	Real Time Streaming Protocol

SAM	Security Account Manager
SAN	Storage Area Network
SAP	Systems, Applications and Products
SCTP	Stream Control Transmission Protocol
SDK	Software Development Kit
SI	Système d'Information
SLA	Service Level Agreement
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UML	Unified Modeling Language
VPN	Virtual Private Network
WBEM	Web-Based Entreprise Management
WMI	Windows Management Instrumentation
WQL	Windows Management Instrumentation Query Language
WS-Management	Web Services for Management
XML	eXtended Markup Language

Glossaire

Agent : élément logiciel embarqué dans un élément actif du réseau permettant sa gestion par une station de supervision.

Alerte : signal qui prévient d'un incident.

API : Application Programming Interface, que l'on traduit en français par Interface de Programmation Applicative, solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services.

ASN.1 : Abstract Syntax Notation One, standard international spécifiant une notation destinée à décrire des structures de données.

Authentification : procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.

Cluster : on parle de cluster (en français : grappe de serveurs ou ferme de calcul), pour désigner des techniques consistant à regrouper plusieurs ordinateurs indépendants (appelés nœuds, node en anglais), pour permettre une gestion globale et dépasser les limitations d'un ordinateur.

Commutateur : dispositif qui achemine les données issues d'un des différents ports d'entrée vers un port de sortie spécifique.

Confidentialité : la confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

CRON : programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiées à l'avance, ou selon un cycle défini à l'avance.

CSV : un fichier CSV (Comma-Separated Values) est un fichier tableur contenant des données sur chaque ligne séparées par un caractère de séparation (généralement une virgule, un point-virgule ou une tabulation).

Datacenter : un Datacenter ou centre de données est un site physique sur lequel se trouvent regroupés des équipements constituants (qui constituent le système ?) du système d'information de l'entreprise.

Datagramme : paquet de données circulant dans un réseau TCP/IP.

Evénement : signal qui permet, par ses différents états, d'indiquer la situation ou l'évolution d'une partie d'un système.

Flux : un flux réseaux est une succession de paquets transitant d'une interface source à une interface de destination.

Hôte : ordinateur qui, dans un réseau, fournit divers services aux utilisateurs et gère les commandes d'accès au réseau.

IETF : groupe informel et autonome, engagé dans le développement des spécifications pour les nouveaux standards d'Internet, et composé de personnes qui contribuent au développement technique et à l'évolution d'Internet et de ses technologies.

Intégrité : vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

Interface : ensemble de moyens permettant la connexion et l'interrelation entre le matériel, le logiciel et l'utilisateur.

IP : protocole de télécommunications utilisé sur les réseaux qui servent de support à Internet, qui permet de découper l'information à transmettre en paquets, d'adresser les différents paquets, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée.

Modèle OSI : cadre de référence pour l'organisation des réseaux locaux, qui décompose la gestion du transfert des données en sept couches superposées réalisant une interface entre l'application locale et le matériel utilisé pour la transmission des données.

MPLS : MultiProtocol Label Switching, mécanisme de transport de données basé sur la commutation d'étiquettes ou "labels", qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie.

NAS : Network Attached Storage, serveur de fichiers autonome relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.

Nœud : dans un réseau, tout point constituant un carrefour d'où les informations sont acheminées.

Notification : émission d'un message d'information vers un utilisateur ou vers un système.

Open source : logiciel distribué avec l'intégralité de ses programmes-sources, afin que l'ensemble des utilisateurs qui l'emploient puissent l'enrichir et le redistribuer à leur tour.

Paquet : ensemble de bits et d'éléments numériques de service constituant un message ou une partie de message, organisé selon une disposition déterminée par le procédé de transmission et acheminé comme un tout.

Pare-feu : le pare-feu (ou firewall en anglais) est un système permettant de filtrer les paquets de données échangés avec le réseau.

PDU : Protocol Data Unit, paquet de données élémentaires échangé entre deux ordinateurs au moyen des protocoles appropriés, et ce, au niveau d'une seule des couches du modèle OSI.

Ping : commande issue du monde Unix qui permet de mesurer le temps de réponse d'une machine à une autre sur un réseau.

Port : dans une architecture client-serveur, connexion virtuelle permettant d'acheminer les informations directement dans le logiciel d'application approprié de l'ordinateur distant.

Protocole : ensemble des spécifications décrivant les conventions et les règles à suivre dans un échange de données.

Renifleur : un renifleur est un composant logiciel de récupération des informations circulant sur le réseau.

Requête : ensemble de commandes dont l'exécution permet d'obtenir un résultat.

RFC : publication de référence portant sur le réseau Internet et rédigée par les experts du réseau.

Routage : détermination par des routeurs du chemin que doit emprunter une information sur un réseau afin de parvenir à sa destination dans les meilleures conditions possibles.

Routeur : dispositif qui effectue le routage des paquets.

RSYNC : Remote SYNChronization ou synchronisation à distance, est un logiciel de synchronisation de fichiers. Il est fréquemment utilisé pour mettre en place des systèmes de sauvegarde distante.

Serveur : dispositif matériel ou logiciel qui fournit des services à d'autres programmes (et à leurs utilisateurs).

SOAP : protocole applicatif indépendant des modalités de transport, permettant l'appel synchrone ou asynchrone d'un service.

Supervision : surveillance de l'état d'un réseau et de ses composants.

Trame : ensemble de bits consécutifs formant un bloc à l'intérieur duquel se trouvent des zones pour la transmission des données de l'utilisateur et des informations de service.

UML : l'UML est une notation permettant de modéliser un problème de façon standard

VPN : Virtual Private Network, système permettant de créer un lien direct entre des ordinateurs distants.

Web Service : service web, programme informatique permettant la communication et l'échange de données entre applications et systèmes hétérogènes dans des environnements distribués.

XML : eXtended Markup Language, langage permettant de représenter toute structure arborescente de données, chaque nœud ayant une sémantique et une syntaxe définie par une balise.

Table des matières

Introduction

La supervision des systèmes d'informations est devenue cruciale pour piloter avec efficacité le support, la maintenance, la sécurité et les évolutions des nombreux systèmes composant les réseaux informatiques. La complexité des réseaux augmente d'année en année dans nos entreprises et la moindre défaillance peut s'avérer très coûteuse. Il devient nécessaire d'effectuer de la maintenance proactive[1] et d'utiliser pour cela des technologies de suivi précises et en temps réel, vérifiant l'état des ressources indispensables au fonctionnement correct des applications et des processus de production.

Les outils de supervision informatique existent depuis de nombreuses années maintenant, avec le temps ils se sont perfectionnés et proposent désormais un large éventail de fonctionnalités offrant à la DSI (Direction des Services Informatiques) une meilleure efficience. Grâce à ses outils, elle gagne du temps sur la résolution des incidents, la maintenance quotidienne et peut ainsi mieux se concentrer sur des tâches de recherche et développement à plus forte valeur ajoutée. Le fait de pouvoir disposer d'indicateurs de disponibilité précis lui permet de mieux planifier les évolutions d'infrastructure et de justifier ses performances auprès de ses clients.

Cependant, les nombreuses solutions et technologies existantes ne facilitent pas toujours le travail de la DSI lors du déploiement d'une plateforme de supervision réseau. En effet, outre le choix du logiciel, se pose la question de son paramétrage qui doit être cohérent avec le projet de supervision, ainsi que la façon dont chaque entreprise souhaite le mener à bien.

Dans ce mémoire, nous allons présenter le contexte dans lequel a été réalisé ce projet pour le compte de Powerflute, et les réponses que j'ai apportées, afin de mettre en service un système qui soit le plus adapté possible au besoin initial tout en conservant la flexibilité nécessaire pour répondre aux évolutions permanentes du SI (Système d'Information).

[1] Site Internet Silicon [En ligne] (Page consultée le 08 Mai 2017) http://www.silicon.fr/blog/maintenance-proactive-eviter-les-couts-astronomiques-des-pannes

Partie I - Notre projet de supervision et ses enjeux

Nous allons dans cette première partie faire une présentation du groupe Powerflute et de l'usine de Corenso France pour laquelle je travaille. Nous présenterons les enjeux de ce projet de supervision ainsi que les exigences que nous avons formulées.

Chapitre 1 : Le contexte du projet

Depuis la fusion du groupe Corenso avec le groupe Powerflute en Novembre 2014, une nouvelle équipe de support informatique s'est constituée. Afin d'optimiser le travail de celle-ci, il devenait nécessaire de se doter d'un outil de supervision réseau pour avoir une vision en temps réel de l'état opérationnel de la totalité de l'infrastructure informatique. Cet outil garantit la maintenance en condition opérationnelle du système informatique.

Je travaille depuis 10 ans sur le site de Corenso France à Saint-Seurin-sur-l'Isle (Gironde), en tant que technicien réseau, et c'est sous mon impulsion que la nouvelle DSI (Patrick Kittle et Gavin McKay), a décidé de me confier ce projet de supervision. M. Jérôme Mazet, mon responsable local, a accepté que je mène ce projet qui présente une importance particulière sur notre site. En effet, notre site fait partie des unités qui produisent sans interruption, il est donc très important que l'ensemble des applications soient fonctionnelles 24h/24 et 7j/7. Disposer d'un outil de visualisation de l'état du réseau et de ses ressources, notamment pendant les astreintes, présente de nombreux avantages.

Actuellement, aucun logiciel n'effectue la supervision du réseau Powerflute/Corenso. Seule l'usine de Corenso France, pour laquelle je travaille, s'est dotée il y a plusieurs années (2007) du logiciel open source NAGIOS afin d'effectuer la supervision de son propre réseau. Cependant, suite aux évolutions techniques effectuées en 2016, cet outil n'est plus à jour. De plus, sa configuration nécessite des connaissances avancées car elle ne s'effectue qu'à partir de fichiers de configuration texte qu'il devient compliqué de gérer. La solution retenue devra être configurable sans avoir de connaissances avancées sur le système de supervision et devra pouvoir être déployée sur l'ensemble des sites du groupe.

Il existe cependant dans le groupe quelques logiciels déjà en place qui répondent chacun partiellement à la problématique :

- La supervision des équipements actifs du réseau s'effectue actuellement grâce à la suite Cisco MERAKI, une solution « Cloud » de configuration réseau qui offre des fonctionnalités de visualisation en temps réel de l'état des matériels réseaux des différentes usines et bureaux du groupe ;

- L'interface « Cloud » de SYMANTEC grâce à laquelle nous pouvons visualiser, en temps réel, l'état de protection antivirus de chaque ordinateur du groupe et qui dispose également d'un système d'alerte par e-mail en cas de problème rencontré sur un poste ;
- Le système de gestion de Datacenter virtuel INTEROUTE VDC offre une vue globale des serveurs fonctionnant sur le Datacenter du groupe ;
- Le logiciel PANDA « Cloud » effectue le suivi des postes de travail et gère le déploiement et les mises à jour logicielles ;
- Le logiciel VEEAM Backup s'occupe d'assurer la disponibilité des machines virtuelles et des données. Il est capable de faire remonter des alertes par e-mail en cas d'erreur lors des sauvegardes ;
- Certains serveurs sont dotés d'interfaces IP d'administration de type HP ILO (Integrated Lights Out) capables de remonter des alertes par e-mail en cas de panne ou défaillance matérielle.

Les solutions citées précédemment ne sont pas complètement efficaces dans la mesure où elles sont spécifiques à leur domaine. L'objectif de ce projet est de trouver une solution centralisée, grâce à laquelle il sera possible de visualiser l'état de l'intégralité des services du réseau sur un outil unique.

Chapitre 2 : L'infrastructure informatique

L'intégralité de l'infrastructure réseau du groupe a dû être reconçue suite à la fusion. En effet Powerflute ne possédait qu'un seul site de production en Finlande (Savon Sellu) et Corenso possède plus de 10 sites répartis à travers le monde. Le groupe Corenso avait une infrastructure qui était alors la propriété de Storaenso, notre ancien groupe. Un nouveau réseau a donc été construit pour réaliser l'interconnexion entre les sites et les infrastructures internes de chaque site ont été, elles aussi, mises à jour.

Ce grand projet de migration technique devait également prendre en compte les impératifs techniques liés à l'installation de l'ERP SAP de Powerflute ainsi que du logiciel ABB-CPM (GPAO : Gestion de Production Assistée par Ordinateur) sur les sites de production de carton de Pori en Finlande et de Saint-Seurin-Sur-L'Isle en France.

Avant cette migration, le réseau était très hétérogène : il n'existait pas de réelle politique de normalisation de l'infrastructure et chaque site était en possession de matériels de marques différentes. Il fallait donc impérativement uniformiser le réseau pour le sécuriser, le fiabiliser et faciliter sa maintenance et ses évolutions futures.

Cette grande migration informatique a impacté le SI sur les points suivants :

- Changement des routeurs, commutateurs et points d'accès pour la suite CISCO Meraki ;
- Modifications des plages d'adresse IP ;
- Changement de l'annuaire et de la messagerie ;
- Modification des règles de nommage des équipements ;
- Nouveau réseau privé virtuel entre les sites ;
- Changement d'opérateur et évolution vers la technologie Fibre Optique pour les sites connectés jusqu'alors par une technologie cuivre et mise en place d'une connexion de secours avec basculement automatique ;
- Nouvelle infrastructure serveur ;
- Nouveaux Datacenter ;
- Migration vers Windows 2012 ;
- Changement des terminaux et ordinateurs ;

- Nouvelle organisation de l'équipe informatique ;
- Nouveaux outils de suivi des incidents (FreshDesk).

Autrement dit, à la fin de la migration, la majeure partie de la documentation du réseau existante (lorsqu'elle existait) devient obsolète. L'un des objectifs de ce projet est également de centraliser l'ensemble de ces nouvelles informations. Ceci afin d'offrir une visualisation de la topologie complète du réseau à l'équipe de support qui verra son travail de dépannage facilité.

Ce projet de supervision doit donc aboutir à l'installation d'un outil permettant aux équipes techniques d'être réactives lors de la survenance d'une panne, et également proactives car il sera alors possible d'anticiper les pannes possibles.

L'équipe informatique de notre groupe est un réel service indépendant et multi-site auprès duquel chaque site paye chaque année des sommes importantes. Par conséquent, ces sites attendent des résultats en retour. Il est donc important de pouvoir justifier de façon précise des temps de disponibilité des applications et de fournir des indicateurs de performance KPI (Key Performance Indicators) et SLA (Service Level Agreement). Il est également important que la DSI puisse disposer des indicateurs de performance des applications et services externes afin d'avoir des éléments concrets pour la négociation et le contrôle de leurs contrats.

Chapitre 3 : Présentation de l'entreprise

Dans ce chapitre nous verrons l'environnement industriel de ce projet et sa dimension mondiale.

3.1) Historique du site de Corenso France

Notre site de production est plus que centenaire. En 1746, on utilisait déjà la force motrice du barrage hydraulique, présent sur l'Isle (affluent de la Dordogne), pour des activités de minoterie. Cette minoterie est détruite par un incendie et à partir de 1914 ce site produit du carton gaufré ou ondulé et fabrique des boîtes et autres objets avec ces cartons. Cette usine est la propriété de la famille Soustre.

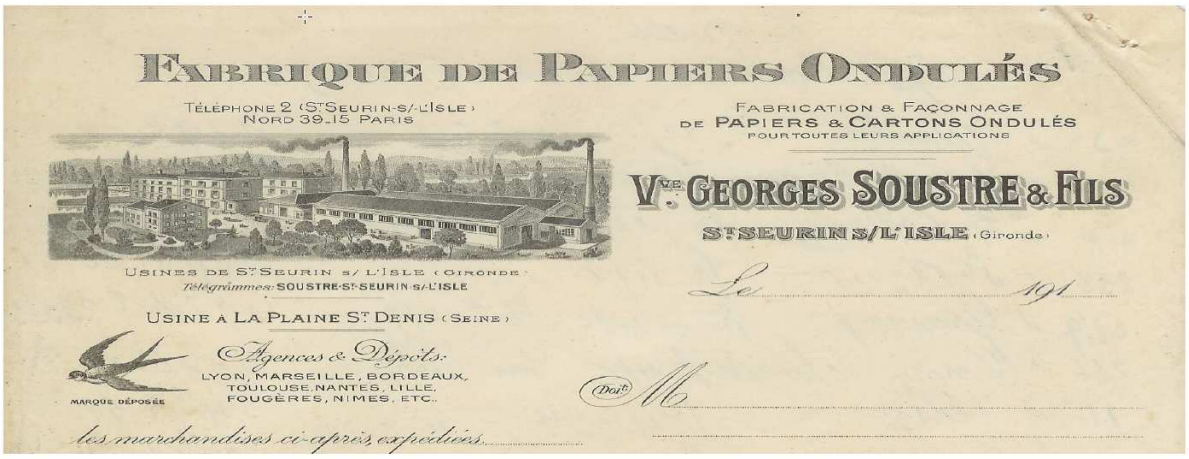


Figure 1 - Papier en-tête papeterie Soustre & Fils

Dès 1920, la société Soustre se hisse au rang des premières sociétés françaises pour la fabrication de carton ondulé.

En 1970, la société entreprend sa mutation vers les cartons pour enroulement sur le site de Moulin-Neuf.

En 1983, Papeteries R. Soustre & Fils débute les ventes à l'exportation, la taille du marché français ne suffisant plus à assurer son développement.

Le Groupe Enso Gutzeit, devenu Stora Enso en 1998, se porta acquéreur début 1990 de l'intégralité des actions formant le capital de Papeteries R. Soustre et Fils. En 1991, Enso Gutzeit et UPM constituèrent une société commune à laquelle chaque partie apporta ses

machines à cartons pour enroulement et usines de transformation : ainsi naquit Corenso United le 1er Octobre 1991.

Pour marquer de manière forte son appartenance à ce groupe, la société changea son nom en 1998 pour prendre celui de Corenso France. Sera conservée l'appellation « Usine Soustre » pour marquer son attachement à son passé et à ses traditions.

Figure 2 - Exemples de produits Corenso United

En 2014, Storaenso vend son activité de production de tubes en carton (Corenso United) à la société Powerflute.

Powerflute

CORENSO

Figure 3 - Logos actuels Corenso & Powerflute

3.2) Corenso France aujourd'hui

Corenso France est une usine de production de carton pour tube. Elle emploie 93 personnes. La capacité de production de l'usine est de 95 000 tonnes par an.

Figure 4 - Vue aérienne de l'usine Corenso France

Le carton produit par CORENSO FRANCE est constitué à 100 % de Fibres Cellulosiques de Récupération (FCR) ou vieux papiers. Les FCR proviennent de collectes sélectives issues de l'industrie ou des ménages.

Le processus de fabrication est constitué de 3 pôles :

- la préparation de pâte,
- la machine à papier (fabrication du carton),
- la transformation (découpe en galettes et emballage).

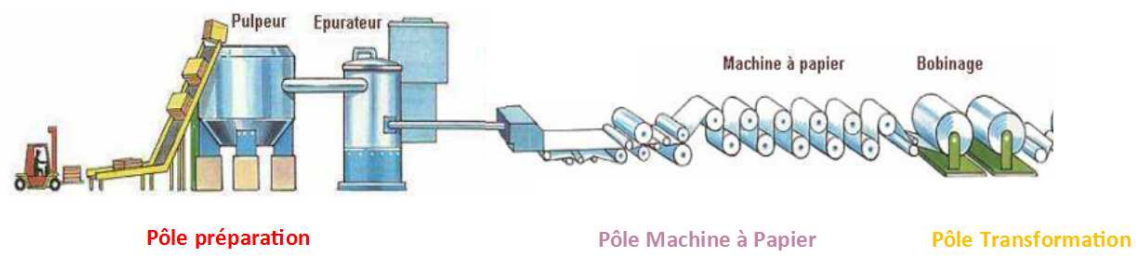


Figure 5 - Processus de production

Au pôle préparation de pâte, les balles de vieux papiers sont désintégrées en présence d'une grande quantité d'eau de façon à obtenir une suspension de fibres.

Au pôle machine à papier, la feuille humide est pressée entre des rouleaux de grand diamètre pour parfaire l'égouttage puis séchée par contact avec des cylindres sécheurs.

Au pôle transformation, le carton sec est découpé en galettes ou bobines de tailles diverses sur la bobineuse et emballé selon les spécifications des clients.

Tout le processus de fabrication du papier est à feu continu. Le personnel de fabrication travaille en 5 x 8 et la machine est arrêtée une fois par mois à l'occasion des arrêts techniques ou arrêts pour nettoyage.

Les autres unités de production de carton de notre groupe fonctionnent sensiblement de la même manière. Les tuberies utilisent notre carton sur leur ligne de production de tubes et mandrins. À l'aide de spiraleuses, les galettes de papiers sont déroulées puis encollées pour être finalement spiralées.

Figure 6 - Fabrication des tubes par une spiraleuse

Environ 70 % du carton que nous fabriquons est destiné aux tuberies Corenso (clients internes). Nous livrons également des entreprises « externes ». Ainsi nos cartons sont utilisés en grande partie pour la fabrication de tubes et mandrins qui serviront de support aux matières pouvant être enroulées (papier, fil, métal). Certains de nos clients utilisent notre carton pour la fabrication de cornières destinées à renforcer les emballages traditionnels. Notre carton est également utilisé dans la construction pour le moulage de poutres en béton

et pour la fabrication de plaques de plâtre. L'industrie métallurgique s'en sert pour concevoir des sondes de température.

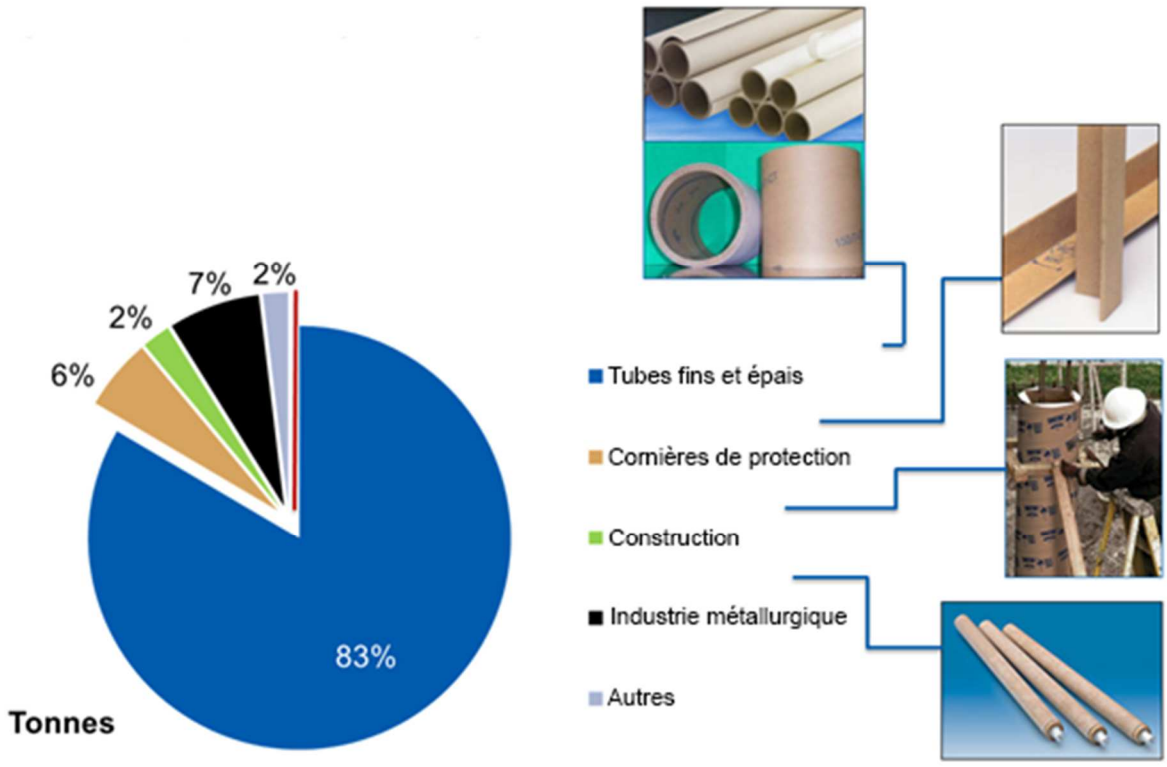


Figure 7 - Répartition de la production par utilisation

Le personnel de Corenso France est réparti dans différents services :

- Le service Fabrication ;
- Le service Commercial ;
- Le service Qualité, Environnement, Sécurité ;
- Le service Logistique ;
- Le service Maintenance (Électrique, Mécanique et Informatique) ;
- Le service Projets et Travaux neufs ;
- Le service Financier ;
- La Direction.

Voici l'organigramme de l'entreprise :

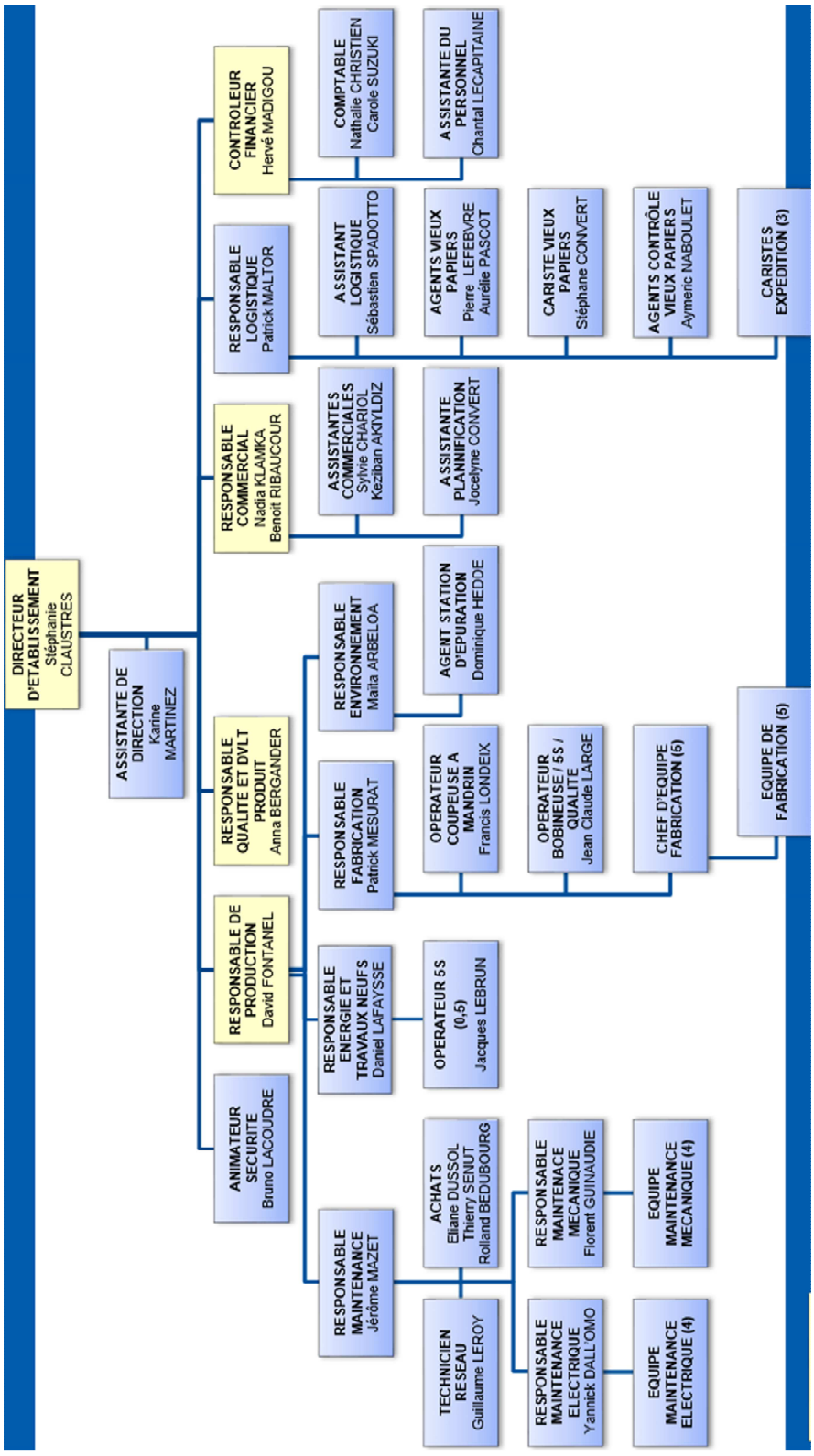


Figure 8 - Organigramme Corenso France

3.3) Le groupe Powerflute

Le groupe Powerflute emploie plus de 1000 personnes à travers le monde. Son chiffre d'affaires est d'environ 200 millions d'euros par an. Il dispose de plusieurs unités de production et de bureaux commerciaux répartis principalement en Europe, mais également en Asie et aux États-Unis. Nous distinguons les unités de production de cartons (papeteries) et les unités produisant les tubes (tuberies). La figure 9 présente la répartition géographique des différentes unités de notre groupe.

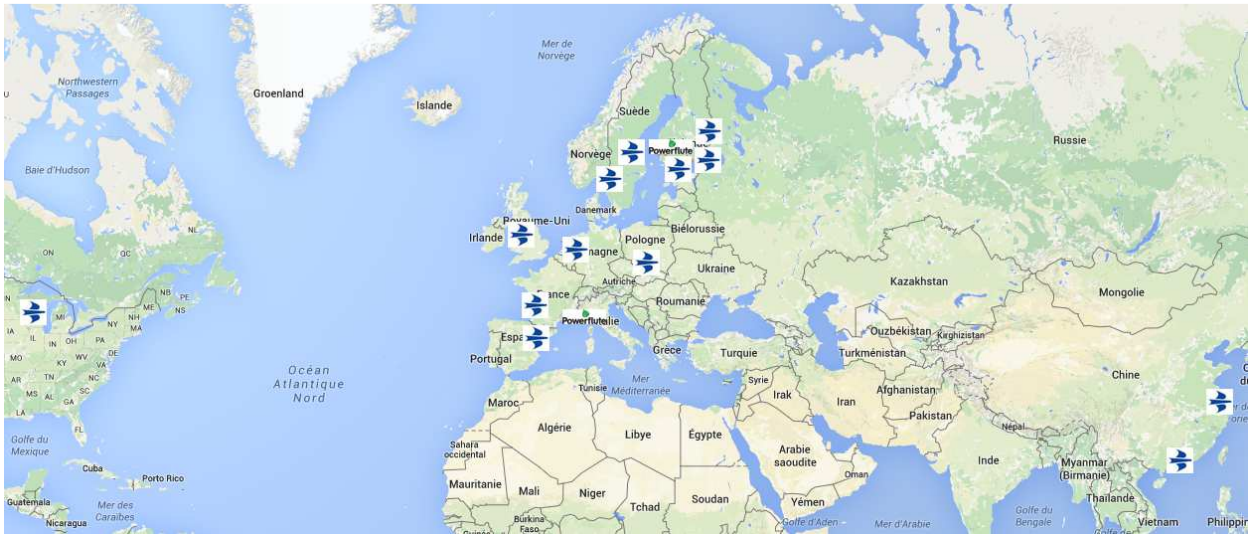


Figure 9 - Répartition géographique des unités Corenso et Powerflute

Finlande :

Corenso Loviisa (tuberie)

Corenso Imatra (tuberie)

Corenso Pori (papeterie)

Corenso Helsinki (bureaux)

Powerflute Savon Sellu (papeterie)

France :

Corenso France (papeterie)

Powerflute Monaco (bureaux)

USA :

Corenso Wisconsin Rapids (papeterie et tuberie)

Suède :

Corenso Bäckefors (tuberie)

Corenso Söderala (tuberie)

Chine :

Corenso Hangzhou (tuberie)

Corenso Foshan (tuberie)

Allemagne :

Corenso Elfes – Krefeld (tuberie)

Pays Bas :

Corenso Edam (tuberie)

Espagne :

Corenso Tolosana (tuberie)

Chapitre 4 : Le service Informatique

Nous allons présenter dans ce chapitre l'environnement humain qui compose la cellule de maintenance informatique de notre site de Corenso France et du groupe Powerflute.

4.1) Site de Saint-Seurin-sur-l'Isle

Au début des années 2000, la multiplication des postes informatiques, l'informatisation de la ligne de fabrication (Supervision papetière Metso/Valmet) et l'installation d'un nouveau logiciel de gestion de production (GPAO Orchis), incitent la direction à recruter en interne un ingénieur informaticien. M. Jérôme Mazet rejoint donc la société en tant que responsable informatique dès 2003.

Très rapidement, il apparaît essentiel de recruter un technicien réseau afin de gérer dans de bonnes conditions le maintien en condition opérationnelle du réseau et les différents projets informatiques. Je rejoins en 2007 le service Informatique en remplacement du précédent technicien afin que M. Mazet soit totalement disponible pour le projet d'installation de SAP, à l'époque initié par notre groupe Storaenso.

L'appartenance de notre usine à ce groupe nous fait bénéficier de certains avantages comme la gestion externe de la messagerie, des contrôleurs de domaines, des accès réseaux et VPN et de prix avantageux sur certains matériels. Nous restons totalement autonomes pour la gestion interne de notre réseau (matériels et applications).

En 2009, M. Mazet prend la responsabilité du service maintenance auquel je suis donc rattaché. Mes fonctions évoluent aussi puisque je m'occupe maintenant des projets d'automatisation, de la maintenance et des évolutions des automates industriels et des écrans de contrôle IHM (Interface Homme Machine). J'effectue ces tâches en collaboration avec le service Électrique.

En 2015, Corenso devient la propriété du groupe Powerflute et nous quittons le réseau Storaenso progressivement jusqu'en 2016. Powerflute construit un nouveau réseau et je deviens un membre de l'équipe de support informatique pour le compte de Powerflute.

Sur le site de Corenso France nous disposons de plusieurs serveurs hébergeant les différentes applications nécessaires au fonctionnement de notre unité. Actuellement nous assurons la maintenance sur 21 serveurs virtuels hébergés par 5 serveurs hôtes VMWARE ESX, dont 2 serveurs ESX configurés en cluster. Nous disposons également de 2 baies de stockage de type SAN (Storage Area Network) également configurées en cluster.

Les principales applications hébergées ainsi en interne sont les suivantes :

- GPAO ABB – CPM : Gestion de la production ;
- Supervision VALMET : Contrôle et régulation de notre machine à papier ;
- VIP : Planification, réception et gestion du stock de vieux papiers ;
- Sage : Logiciel de paye ;
- ETemptation : Gestion des pointages des employés ;
- RDS 2012 : Terminal Serveur pour la partie bureautique et connexion aux applications (Messagerie, SAP, ABB-CPM) ;
- 5TPCI : Serveur de fichier et d'impression ;
- Intranet : Site intranet de notre unité, héberge également des applications spécifiques comme la gestion électronique des rondes de maintenance ou la gestion des fiches AC/AP (Actions Correctives et Préventives) ;
- Altiged : Gestion de la documentation.

Les applications externes à notre site sont les suivantes :

- SAP : PGI (Progiciel de Gestion Intégré) principal du groupe ;
- Messagerie Microsoft Exchange ;
- Système de gestion des incidents (FreshDesk) ;

La plupart des postes sont des clients légers (35 en tout), qui se connectent au serveur RDS2012 ou à l'application de supervision de notre machine à papier (Windows terminal server 2003). Certains utilisateurs bénéficient de postes fixes (7) ou de portables (10) qui peuvent supporter certaines applications métier spécifiques (dessin industriel, édition des schémas électrique, application comptable, etc.). La distribution du réseau est actuellement assurée par 7 baies de brassage interconnectées en fibre optique.

Nos tâches quotidiennes au sein du service informatique consistent à apporter un support aux utilisateurs et à résoudre les problèmes techniques de façon pérenne. Bien entendu un certain temps est consacré à la maintenance des systèmes, mais une grande partie de notre temps de travail est utilisé pour la réalisation de projets (en informatiques ou en automatisme). C'est ce temps qui sera utilisé pour ce projet, et grâce auquel la réalisation sera effectuée dans les conditions de fonctionnement habituelles de notre service.

4.2) L'équipe informatique du groupe

Depuis fin 2014 et la vente de Corenso à Powerflute, une nouvelle équipe de support s'est construite. Certains membres de cette équipe étaient déjà présents avant le rachat, mais beaucoup des membres de cette équipe viennent tout juste d'être recrutés. Bien que nous soyons dispersés sur des sites distants, nous travaillons en équipe.

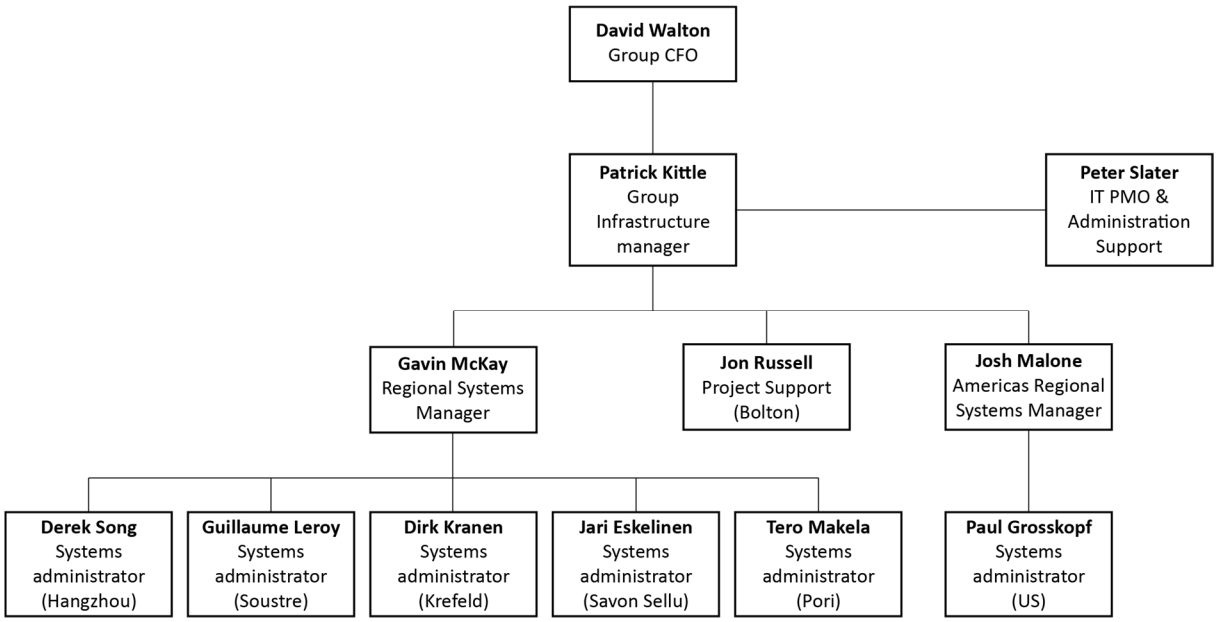


Figure 10 - Organigramme de l'équipe informatique Powerflute & Corenso

Les sites de production de carton disposent chacun de leur propre administrateur système. En effet, ces sites présentent une importance stratégique majeure, car sans eux les tuberies ne peuvent pas fonctionner. D'autre part, la densité et la complexité du réseau sont beaucoup plus importantes dans les papeteries que dans les tuberies, unités qui nécessitent moins de ressources informatiques. Les papeteries étant des unités fonctionnant en continu, les administrateurs système sont soumis à des astreintes afin d'assurer les dépannages à tout

moment. Des règles de remplacement sont définies afin d'assurer la maintenance continue sur chaque site.

Nous nous réunissons chaque semaine en web-conférence pour faire le point sur les nouveautés de l'infrastructure, les projets en cours et sur les difficultés rencontrées sur chaque site. L'expérience de chacun est désormais utile à tous.

Nous utilisons le même outil de gestion des incidents (FreshDesk[1]). Les tickets ainsi créés par les utilisateurs sont assignés à chacun de nous de façon aléatoire. Ceci implique une connaissance du réseau de chaque site, ce qui n'est pas le cas actuellement, et il en découle une perte de temps entre le moment où le ticket est créé et où il est assigné à la personne étant la plus à même de répondre à la demande.

[1] FreshDesk [En ligne] (Page consultée le 04 juin 2017) http://www.freshdesk.com

Chapitre 5 : Les enjeux de la supervision

La performance du SI est devenue cruciale dans toutes les entreprises. Par conséquent la bonne gestion de l'infrastructure aussi bien matérielle que logicielle est le socle de la santé d'une entreprise. La DSI doit, tout en se conformant aux normes, se doter d'outils lui permettant de s'assurer de la maîtrise de ses engagements.

5.1) La gestion des incidents par ITIL

ITIL, acronyme d'Information Technology Infrastructure Library, définit un cadre de référence pour la gestion au quotidien de la DSI afin d'améliorer la qualité du service informatique pour les utilisateurs. ITIL propose un ensemble de guides rassemblant les bonnes pratiques à adopter en matière de management de services informatiques.

Cette bibliothèque a été initiée en 1986 par le CCTA (Central Computing and Telecomms Agency), qui publiera ses premiers guides en 1989. À l'époque, l'informatique commence à prendre de l'importance au cœur des entreprises et il devient nécessaire de définir des méthodes pour recenser et cataloguer les meilleures pratiques en matière de gestion de production informatique. En effet, dans les années 80, les besoins commerciaux exigent le déploiement de nouveaux services informatiques et notamment de services supports nécessaires à la résolution des problèmes rencontrés par les clients avec les outils informatiques.

ITIL répond à cette problématique en définissant le service informatique comme un ensemble de processus. La démarche ITIL vise à sensibiliser l'ensemble des acteurs du service informatique sur l'impact qu'a la disponibilité et la performance des outils sur la santé de l'entreprise. La version 3 d'ITIL publiée en 2007 met l'accent sur la maîtrise des cycles de vie des services. Cette dernière version s'articule autour de 5 livres :

Stratégie des services : ce livre définit comment aligner les stratégies d'entreprises et l'outil informatique, ceci afin de définir une cohérence pour mieux diriger l'entreprise dans ses projets. L'objectif est de faire collaborer les différents départements de l'entreprise et de s'assurer de la création de valeur durant le cycle de vie des applications informatiques.

Conception des services : ce livre propose des moyens de concevoir des services performants en prenant en compte les points de vue internes à l'entreprise, mais aussi le point de vue des fournisseurs et des clients.

Transition des services : cet ouvrage décrit comment élaborer une stratégie de transition en prenant en compte les risques liés à la mise en place de nouveaux services. L'objectif est de planifier au mieux les ressources associées au changement, de diminuer leurs impacts et bien entendu de valider l'adéquation des nouveaux services avec la stratégie de l'entreprise.

Exploitation des services : ce volume explicite comment suivre la stratégie opérationnelle pour garantir la qualité de service offerte aux utilisateurs. En effet, lors de la phase d'exploitation, un certain nombre d'événements peuvent survenir et peuvent être des incidents ou des problèmes.

La figure ci-dessous représente les processus ITIL de gestion des événements.

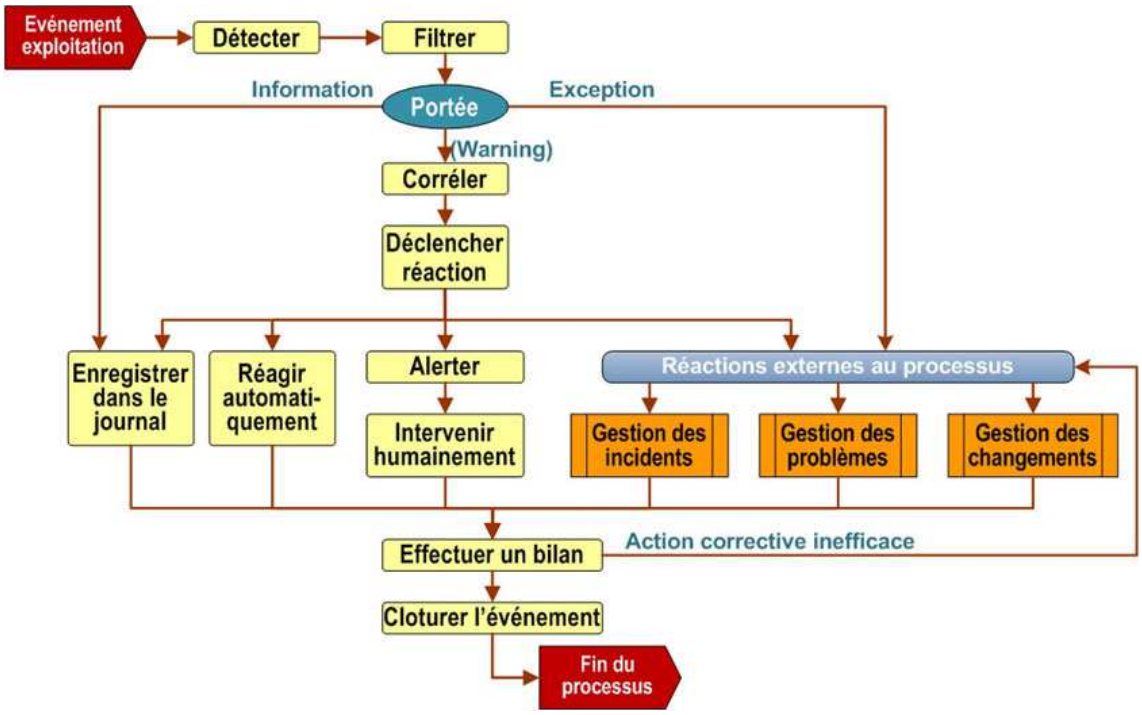


Figure 11 - Processus ITIL de gestion des événements, ITIL France [En ligne] (Page consultée le 04 Juin 2017) http://www.itilfrance.com/index.php?pc=pages/docs/itilv3-04/40-30.inc&pg=menu_itilv3.inc&pt=Processus%20et%20fonctions

Amélioration permanente des services : ce livre définit les techniques de réflexion à adopter pour améliorer les différents processus. Il développe une méthodologie cyclique en sept étapes :

- Définir ce qu'il faudrait mesurer ;
- Définir ce qu'il est possible de mesurer ;
- Collecter les données ;
- Reformater les données ;
- Analyser les données ;
- Utiliser les informations ;
- Mettre en place les actions correctives.

Les deux derniers ouvrages nous intéressent particulièrement dans le cadre de ce projet. Ils couvrent plusieurs processus, mais surtout la gestion des événements. L'objectif étant de détecter les événements pouvant survenir au sein d'un réseau informatique, de leur donner une signification et de déterminer la réaction appropriée.

ITIL définit de façon claire le vocabulaire utilisé par les équipes informatiques :

Événement : changement d'état ayant de l'importance pour la gestion d'un service informatique. Souvent employé pour désigner une alerte, il s'agit ici de gérer les événements tout au long de leur cycle de vie. Un événement peut être une notification émise par un service informatique ou un outil de supervision.

Incident : interruption non prévue d'un service informatique. Il faut ainsi dépanner les utilisateurs le plus rapidement possible afin de minimiser l'impact défavorable perçu par les utilisateurs.

Alerte : avertissement qu'un seuil a été atteint, que quelque chose a changé, ou qu'une panne s'est produite. L'alerte a pour objectif de prévenir au plus tôt l'équipe d'exploitation afin qu'elle y apporte une réponse appropriée dans les meilleurs délais.

Problème : cause d'un ou de plusieurs incidents. La cause d'un problème n'est pas forcément connue au moment de l'enregistrement de celui-ci. Il faut ici chercher à identifier les problèmes, ou erreurs connues, avant que des incidents ne se produisent. Lorsque cela n'est

pas possible, il faut s'assurer de rechercher la cause première de l'incident afin d'initier les actions correctives nécessaires et empêcher le problème d'apparaître de nouveau.

Processus : ensemble d'activités structurées conçues pour atteindre un objectif spécifique. Un processus traite une ou plusieurs entrées définies et les transforme en résultats.

ITIL donne plusieurs préconisations dans la gestion des incidents. Les outils de supervision ont leur importance car ils détectent les incidents et font remonter les alertes rapidement à la cellule de maintenance. Ils offrent également les moyens d'analyser la cause des problèmes à posteriori.

ITIL est à la base de la norme BS15000 qui est la première norme de gestion de services informatiques formelle. Cette norme est développée par le BSI (British Standard Institute). La norme ISO/CEI 20000 est issue de la norme BS15000 et elle est désormais la norme de référence en ce qui concerne la certification des services informatiques.

Cette norme s'articule en deux parties. La première définit les procédures qu'une organisation devra appliquer afin d'obtenir la certification, la seconde définit les pratiques à adopter. Cette norme s'appuie sur les principes du cycle de Deming (PDCA : Planifier Développer Contrôler Ajuster – Plan Do Check Act) et sur les processus du référentiel ITIL.

Actuellement, notre cellule de support ne dispose pas de certification ITIL, cependant c'est en mettant en place les outils et procédures dès maintenant que nous pourrons prétendre à cette certification prochainement. Étudions maintenant les logiciels existants qui permettent d'effectuer les relevés d'informations nécessaires à la détection des événements d'exploitation.

5.2) Le marché des solutions de supervision

Les technologies et protocoles de supervision apportent de bons moyens d'accéder et de contrôler les logiciels et le matériel. Chacun d'entre eux est nécessaire pour construire une supervision centralisée de l'ensemble du SI. Il est indispensable que l'ensemble de ces protocoles soient implémentés et utilisés car chacun possède sa pertinence propre. Il faut donc que l'outil de supervision supporte ces différents protocoles car il doit pouvoir s'adapter à un environnement hétérogène**.**

Il existe de nombreuses solutions logicielles de supervision pour une entreprise. La plupart s'installe sur le SI interne et s'y adapte en utilisant plusieurs technologies de supervision (SNMP, WMI, NetFlow, etc.). Le choix ne dépend donc pas uniquement des fonctionnalités attendues mais également du ressenti des administrateurs, de la politique d'entreprise et de son besoin en supervision.

Il existe sur le marché des solutions proposant des finalités d'utilisation différentes :

Les outils de type **NMS** (Network Monitoring System), sont dédiés à l'équipe technique et leur apporte une vision globale de l'état de santé des nœuds physiques du réseau et des applications. Ces outils utilisent des sondes pour collecter les informations sur l'état technique de l'infrastructure et les présenter, de façon cohérente, aux membres de l'équipe technique de la DSI (Nagios[1] par exemple).

Les outils de type **BAM** (Business Activity Monitoring), présentent en temps réel des indicateurs sur le fonctionnement du processus métier. C'est un moyen efficace pour juger du bon fonctionnement des processus de l'entreprise. L'une des particularités des systèmes de BAM est de fournir des rapports de performance en temps réel à la portée des responsables fonctionnels de l'entreprise. Ces outils s'interfacent avec le réseau et les applications de l'entreprise mais ne sont pas suffisants pour une équipe technique. L'application Centreon BAM[2] est l'un de ces outils.

Les outils de type **BSM** (Business Service Management), observent la qualité des services métier grâce aux données présentes sur le SI et ses performances. Ceux-ci ne sont pas adaptés pour les équipes de maintenance mais permettent à la DSI de mieux comprendre l'impact des performances de l'infrastructure réseau sur les performances financières de l'entreprise. Ceci dans le but de mieux utiliser les ressources informatiques et de définir les priorités dans les améliorations à apporter au SI. L'application HPE Operation Management[3] est un outil BSM.

[1] Site Internet de NAGIOS [En ligne] (Page consultée le 5 Mai 2017) https://www.nagios.org/ (Page consultée le 5 Mai 2017)
[2] Site Internet Centreon BAM [En ligne] (Page consultée le 20 mars 2017) https://www.centreon.com/fr/solution/centreon-bam-business-activity-monitoring/
[3]Site Internet HP [En ligne] (Page consultée le 05 Mai 2017) https://saas.hpe.com/fr-fr/software/oneview-operations-management-performance-monitoring

Les outils **APM** (Application Performance Management) surveillent les performances des applications. Ceci grâce à des « renifleurs » de réseau qui capturent les paquets transitant par une interface réseau et d'en déduire des métriques utiles pour diagnostiquer et anticiper les problèmes de performance. Très adaptés aux équipes techniques spécialisées dans la maintenance d'applications ils peuvent-être inadaptés aux équipes de maintenance réseau. On peut citer l'application Packetbeat[1] comme solution APM.

Il faut différencier ces outils car les utilisateurs finaux ne sont pas les mêmes, ils sont cependant bien souvent complémentaires. Dans le cadre de ce projet de supervision, nous devons apporter une vision de l'infrastructure informatique à l'équipe de support. Nous sommes donc à la recherche d'un outil de type NSM avant tout. Cependant il apparaît important de choisir un outil qui pourra être utilisé lors de l'implémentation éventuelle d'un outil de type BAM dans le futur.

Le marché des solutions de supervision NMS est saturé, on retrouve beaucoup d'acteurs et notamment les constructeurs les plus connus comme IBM, HP ou Computer Associates. Les solutions Open-Source sont elles aussi nombreuses et bien souvent basées sur la solution NAGIOS. Cela reflète bien l'enthousiasme que suscite la supervision réseau auprès des administrateurs systèmes. Cependant il est parfois compliqué de devoir effectuer un choix parmi ces solutions très proches les unes des autres.

Il convient de classer les solutions de supervision en fonction du type d'outil de supervision. Cela en élimine un certain nombre. Ensuite, il convient de les différencier en fonction :

- des ressources (techniques ou humaines) nécessaires à leur installation et leur fonctionnement ;
- de leurs interfaces, fonctionnalités et performances ;
- de leur coût de possession.

Certains de ces logiciels sont conçus pour fonctionner de façon exclusivement interne au réseau de l'entreprise et certaines solutions dites « Cloud » proposent un portail externe à l'entreprise. Certaines utilisent des agents spécifiques qui doivent être installés sur les

[1] Site Internet Packet Beat [En ligne] (Page consultée le 5 Mai 2017)
https://www.elastic.co/products/beats/packetbeat

machines à superviser, d'autres des collecteurs désignés au sein du réseau interne. Ces collecteurs sont destinés à collecter puis transmettre les données de supervision sur la plateforme « Cloud ».

Bien entendu, pour effectuer un choix parmi ces solutions, il faut savoir et comprendre comment l'on souhaite mener son projet de supervision et donc définir de façon précise la granularité souhaitée et les fonctionnalités attendues.

5.3) Fonctionnalités d'un superviseur NMS

La supervision ou l'hyperviseur a pour but de donner une vision globale du SI via une console unique et de détecter les incidents pouvant survenir sur l'architecture informatique. Le fonctionnement du SI est ainsi surveillé de façon permanente par l'hyperviseur qui déclenchera une alerte dès qu'un traitement ne s'est pas exécuté correctement. Cette alerte sera ensuite traitée par les équipes de maintenance opérationnelle.

La supervision peut être décrite comme un automate permettant de fiabiliser le travail de la DSI. En effet, couplé à des instruments de métrologie, elle met en exergue des tendances et analyse précisément le déroulement des incidents.

Les enjeux sont donc multiples :

- Diminution du temps de résolution des incidents ;
- Meilleur prévision des approvisionnements en ressources informatiques ;
- Plus de précision dans l'analyse des causes d'un incident ;
- Connaissance du niveau de fonctionnement réel du SI.

En conséquence, plusieurs fonctionnalités sont attendues d'un hyperviseur de nos jours :

- Présenter de façon lisible les événements quelle qu'en soit la source ;
- Corréler les différents événements ;
- Gérer les périodes de maintenance ;
- Faciliter la construction des vues métiers ;
- Intégrer facilement les événements provenant de plusieurs sources de supervision ;
- Proposer l'édition de rapports affichant les métriques indispensables au pilotage ;

- Assurer les remontées d'événements même lors d'incidents ou périodes de maintenance ;
- S'adapter à l'environnement et à l'infrastructure informatique qui est en perpétuelle évolution ;
- Être extensible pour répondre à d'éventuelles évolutions techniques qui pourraient ne pas être gérées de façon native par l'outil ;
- Pouvoir s'interfacer avec des outils de gestion de service Informatique (ITSM, Information Technology Service Management).

La supervision ne se limite plus maintenant à la supervision de l'infrastructure : applications, respect des SLA et processus sont désormais la cible des outils de supervision. La supervision est donc un outil important dans la bonne gestion du support et de la maintenance des systèmes informatiques, et il s'intègre parfaitement dans les recommandations effectuées par ITIL. L'installation d'un système de supervision constitue l'une des premières briques à mettre en place dans une démarche de certification ITIL.

Chapitre 6 : Formulation des exigences

Conformément aux attentes que nous avions sur ce projet de déploiement d'une supervision NMS, voici les exigences que nous avons formulées :

Surveillance :

Le système devra pouvoir contrôler la disponibilité des équipements. Cette surveillance devra pouvoir se paramétrer à intervalles réguliers et être personnalisable par équipement. Le résultat de l'évaluation de la disponibilité se fera de la façon suivante :

- Disponible ;
- Partiellement indisponible ;
- Totalement indisponible.

La disponibilité des équipements suivants devra être contrôlée :

- Serveurs Hôtes ;
- Serveurs Virtuels ;
- Commutateurs, routeurs et points d'accès ;
- SAN ;
- Autres équipements disposant d'une adresse IP fixe (caméras, automates, etc.).

Il devra pouvoir mesurer des informations spécifiques à chaque équipement concerné :

- Serveur Windows ou Linux : charge processeur (%), mémoire (%), espace disque restant (Go), débit interface réseau (Mbps) ;
- Commutateurs et routeurs : débit des interfaces d'interconnexion (Mbps) ;
- Infrastructure VSPHERE : charge processeur (%), mémoire (%), espace disque restant (Go), débit interface réseau (Mbps), état de santé global ;
- Serveurs et SAN : charge processeur (%), mémoire (%), espace disque des LUNS (Logical Unit Number) restant (Go), débit interface réseau (Mbps), température de fonctionnement (°C), état de santé global.

Dimensionnement :

Le système de supervision devra être à même de superviser 500 hôtes (adresses IP). Chaque hôte pouvant supporter plusieurs points de contrôle (5). Le système devra donc être capable de superviser 2 500 services.

Interface :

L'interface de consultation et de paramétrage devra être accessible à distance et sur site, et fonctionner grâce à un navigateur web pour être accessible au plus grand nombre sans nécessiter de logiciel spécifique.

Elle devra permettre :

- L'organisation des éléments supervisés ;
- L'édition de rapports de disponibilité ;
- L'édition de graphiques de tendance sur les mesures ;
- Une personnalisation en fonction du profil utilisateur.

Rapport et graphique :

- Il doit être possible de générer différents graphiques pour toutes les ressources réseaux et systèmes que l'on souhaite et sur une période allant des 5 dernières minutes à 18 mois auparavant ;
- On doit pouvoir exporter ces données sous un format standard (CSV, XML) ;
- L'édition de rapports de SLA pour chaque site et application doit être possible.

Cartographie (optionnel) :

- Un outil de cartographie serait apprécié pour visualiser de façon rapide l'état de la plateforme et l'interconnexion entre les éléments supervisés ;
- Cet outil devra hiérarchiser les vues.

Événements :

La solution doit pouvoir gérer les différents événements pouvant survenir :

- Anomalie ;

- Surcharge ;
- Dégradation de la qualité d'un service ;
- L'apparition d'une alarme doit engendrer des notifications :
    - sur l'interface ;
    - par e-mail ;
    - par création d'un ticket dans l'outil de gestion des incidents ;
- L'affichage d'un historique des événements devra être disponible sur l'interface.

Infrastructure :

- L'outil devra pouvoir s'intégrer au réseau actuel sans nécessiter de nouvelles ressources matérielles ;
- Son fonctionnement ne devra pas nécessiter d'opération manuelle en dehors des opérations de mise à jour. L'outil doit être capable de se relancer de façon automatique après une panne matérielle ;
- La solution devra être fiable, c'est-à-dire garantir la collecte et la sauvegarde des données.

Coût et délais :

- Le coût de la licence devra être raisonnable et adapté au regard des fonctionnalités attendues ;
- La charge du projet en interne ne doit pas impacter le fonctionnement normal du service ;
- Le projet ne devra pas consommer plus de 150 jours-hommes sur les ressources internes de l'entreprise ;
- Le délai est d'un an, la solution devra donc être pleinement opérationnelle sur l'ensemble des sites du groupe Powerflute fin 2017.

Sécurité :

- La plateforme de supervision ne doit pas créer de brèches dans la sécurité du réseau ;
- La plateforme de supervision doit pouvoir offrir des droits d'administration différents en fonction de ses utilisateurs ;
- Les mises à jour doivent être autonomes ou très rapides à effectuer.

Charge en production :

Une fois en production, le système de supervision doit fonctionner de façon totalement autonome. Seules les opérations de mise à jour doivent être assurées par les opérateurs. Ces opérations doivent être faciles à effectuer même pour quelqu'un n'étant pas un spécialiste de l'outil de supervision. Les administrateurs de la solution ne devront pas avoir à consacrer plus de 10 % de leur temps à ce système (2 jours par mois uniquement pour les opérations de maintenance, projet ou développement exclu).

Maintenant que nous connaissons nos besoins de façon précise, nous verrons dans la prochaine partie quelles sont les technologies, protocoles et outils de supervision existants qui nous ont été utiles pour mener à bien ce projet.

Partie II - Les solutions de supervision

Une étude de marché concernant le déploiement d'une supervision nécessite un investissement de la part de la DSI qui se positionne bien comme la MOA (Maîtrise d'Ouvrage), mais qui peut être en charge également de la MOE (Maître d'œuvre). Avant de choisir une solution, il est important d'appréhender le fonctionnement des technologies de supervision. C'est pourquoi je vais commencer par présenter les principaux protocoles de supervision pour ensuite détailler notre démarche de sélection pour notre future solution de supervision.

Chapitre 1 : Les protocoles de supervision

Dans cette partie nous allons présenter les principaux protocoles de supervision des systèmes d'informations qui, couplés aux outils de supervisions, permettent de visualiser de façon claire l'état global de l'infrastructure informatique.

1.1) SNMP

SNMP (Simple Network Management Protocol) est sans doute le protocole de supervision le plus répandu. Ce protocole réseau est défini par IETF (Internet Engineering Task Force) dans la RFC 1157 (Request For Comments). Il permet la création d'un système de gestion des équipements via un réseau TCP/IP. La grande majorité des équipements actifs d'un réseau TCP/IP (commutateurs, routeurs, serveurs, pare-feu, onduleurs) intègrent ce protocole.

Il existe actuellement 3 versions différentes du protocole SNMP :

- SNMP v1 (RFC 1155, 1157 et 1212).
- SNMP v2c (RFC 1901 à 1908).
- SNMP v3 (RFC 3411 à 3418).

La coexistence des trois versions est détaillée dans la RFC 3584.

L'environnement SNMP est constitué de :

- La station de supervision ou de gestion qui va exécuter les requêtes nécessaires à la collecte des informations, et maintenir à jour une base d'information représentant le résultat de cette collecte. Les agents SNMP présents sur les différents éléments actifs du réseau seront chargés de répondre aux demandes effectuées par la station de supervision.
- La MIB (Management Information Base) est une collection d'objets résidant dans une base d'information virtuelle. Ces collections d'objets sont définies dans des modules spécifiques aux équipements implémentant le protocole SNMP.
- Le protocole lui-même, qui s'appuie sur TCP/IP pour son fonctionnement.

Il convient de bien comprendre le protocole SNMP. Nous allons détailler le fonctionnement de ces trois éléments principaux ci-après.

1.1.1) Le protocole SNMP

Le protocole SNMP est constitué d'un ensemble de requêtes, de réponses et d'alertes. La station de supervision envoie des requêtes à l'agent, lequel retourne des réponses. Lorsqu'un événement anormal intervient sur l'élément réseau, l'agent est en mesure d'envoyer une alerte à la station de supervision.

La technologie SNMP s'appuie sur le modèle OSI (Open System Interconnexion). Ce modèle de communication mis en place par l'Organisation internationale de normalisation (ISO) comporte 7 couches. Le rôle du modèle OSI, décrit dans la norme ISO 7498-1, est de standardiser la communication entre les machines. SNMP est un protocole situé entre la couche 4 et la couche 7 du modèle OSI (cf. figure 12).

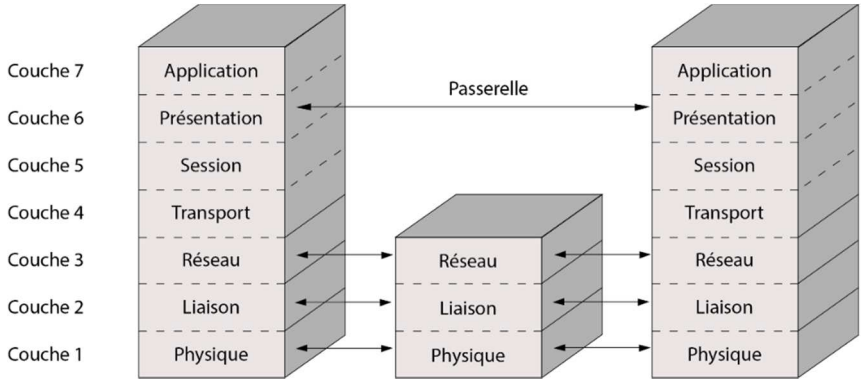


Figure 12 – Les couches du modèle OSI

Au niveau des couches OSI inférieures, le protocole SNMP utilise le protocole UDP (User Datagram Protocol) sur les ports 161 et 162. Le paquet UDP est encapsulé dans un paquet IP (Internet Protocol).

Le port 161 est utilisé par les agents présents sur les équipements afin de recevoir et répondre aux requêtes SNMP de la station de supervision. Le port 162 est utilisé par la station de supervision pour recevoir les alertes (notifications ou traps) provenant des agents.

La station de gestion peut utiliser plusieurs type de requêtes SNMP :

- La requête *GetRequest* qui recherche une variable sur un agent ;
- La requête *GetNextRequest* qui recherche la variable suivante ;
- La requête *GetBulk* qui recherche un ensemble de variables regroupées ;
- La requête *SetRequest* qui change la valeur d'une variable sur un agent.

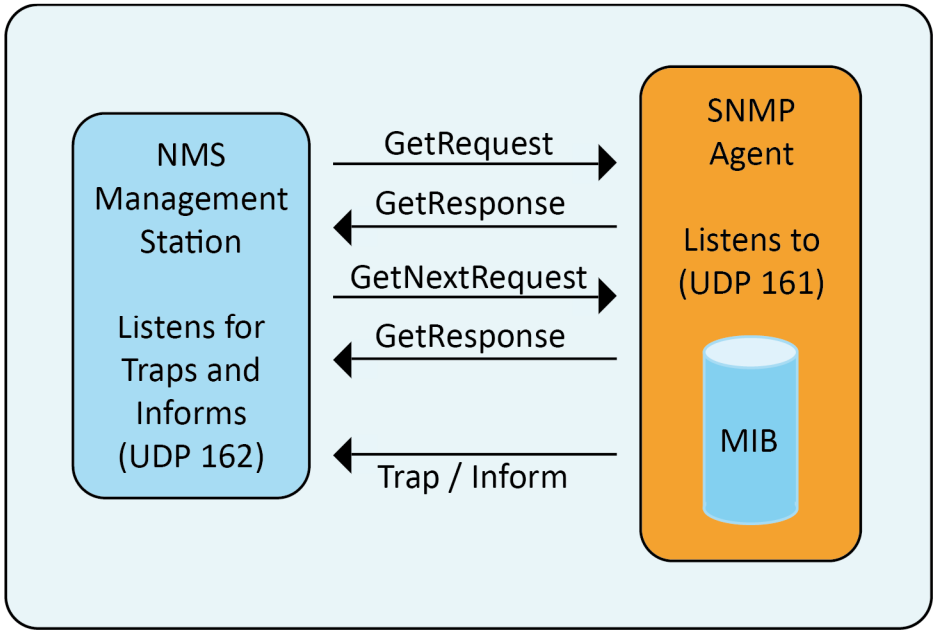


Figure 13 - Mécanismes d'échanges SNMP

À la suite d'une requête, l'agent répond toujours par un GetResponse, même si la GetRequest était incorrecte.

Les requêtes de notifications (traps) sont utilisées uniquement par les agents afin de signaler des anomalies à la station de gestion.

Le protocole SNMP s'appuie sur le protocole UDP pour interroger les différentes MIB. La trame SNMPv1 est complètement encodée en ASN.1 (Abstract Syntax Notation One) et sa longueur est variable. Les requêtes et les réponses ont le même format.

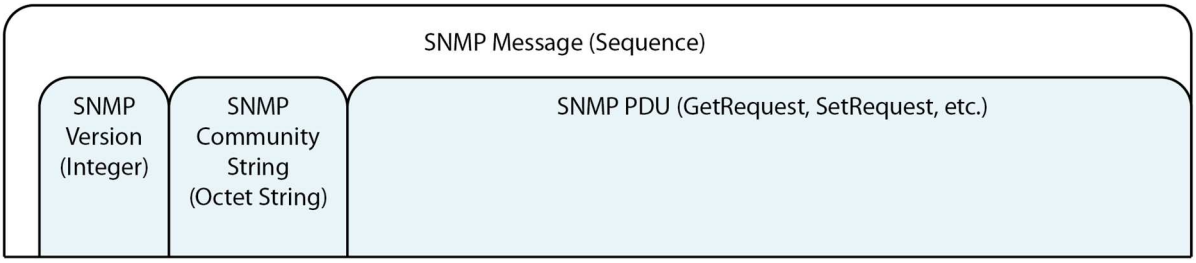


Figure 14 - Trame SNMP v1 par Douglas Bruey, R. (2005), SNMP : Simple? Network Management Protocol [En ligne] (Page consultée le 14 février 2017) http://www.rane.com/note161.html

La communauté définit des domaines d'administration bien souvent utilisés comme mot de passe, elle définit également si la station de gestion possède des droits en lecture ou en écriture. Le PDU (Protocol Data Unit) est décrit dans la figure 15.

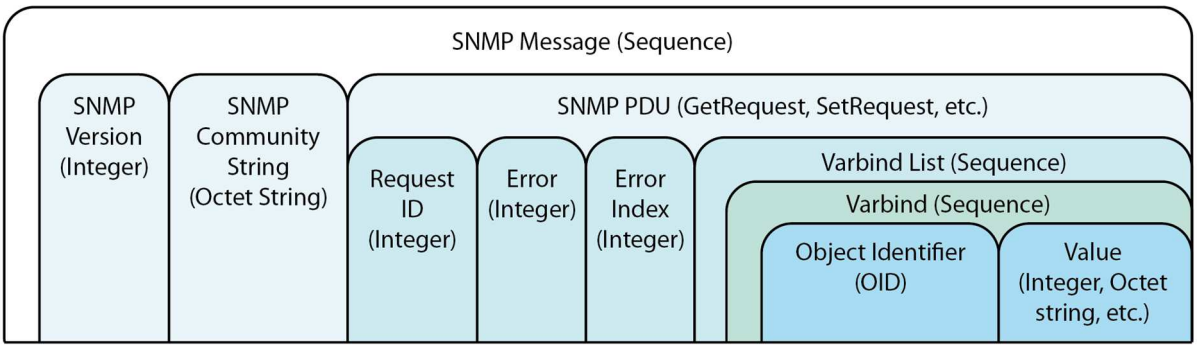


Figure 15 - Détails du PDU SNMP par Douglas Bruey, R. (2005), SNMP : Simple? Network Management Protocol [En ligne] (Page consultée le 14 février 2017) http://www.rane.com/note161.html

Le champ « Request ID » permet à la station de supervision d'associer les réponses à ses requêtes. Les champs « error » et « error index » sont ici pour prendre en compte une erreur renvoyée par l'agent en cas de mauvaise requête par exemple. L'OID (Object Identifier) se réfère plus directement à un nœud de la MIB. Le champ « Value » contient la donnée qui nous intéresse et que l'on veut écrire ou récupérer.

Il existe 3 versions du protocole. La version 2 essaie principalement de limiter le flot d'informations induit par les requêtes SNMP en introduisant une requête GETBULK qui est une requête GET améliorée. En 1996, l'IETF a formé un nouveau comité en vue d'examiner les

problèmes de sécurité dans SNMP. Le standard SNMPv3 voit le jour en 1998. Cette version reprend les améliorations de SNMPv2 en incluant de nouveaux éléments de sécurité, ces derniers constituant de fait la principale amélioration.

SNMP formalise donc les échanges possibles entre les entités SNMP (agents et managers). Mais SNMP modélise également les informations d'administration, c'est la MIB qui est utilisée pour cela et que nous allons décrire maintenant.

1.1.2) La MIB SNMP

Il était nécessaire de fournir une représentation unifiée des différents composants à administrer. La MIB définie la structure des objets administrés, pour cela elle se base sur la syntaxe SMI (Structure of Management Information). Cette dernière est issue de la norme RFC1155 définie par l'IETF en 1990[1].

La MIB est une collection d'informations organisée de façon hiérarchique. Elle comprend un ensemble d'objets qui représentent une caractéristique du nœud administré. Elle est une spécification définissant le nommage, le type, le format et les actions auprès des objets administrés. Elle est ainsi une interface d'accès à tous les objets administrés, c'est-à-dire à l'instrumentation sous-jacente du nœud.

[1] Site Internet de l'IETF, RFC1155 [En ligne] (Page consultée le 15 avril 2017) https://www.ietf.org/rfc/rfc1155.txt

Chaque objet est repéré par un identifiant, c'est L'OID, qui représente le chemin parcouru dans l'arborescence (voir figure 16). Un OID est composé d'une série d'entiers sur la base des nœuds de l'arbre, séparés par des points. Il existe également une représentation lisible par l'homme qui est une série de noms séparés également par des points, chacun représentant un nœud de l'arbre. L'arborescence d'objets est constitué du nœud au sommet de l'arbre appelé racine ou « Root-Node », des nœuds possédant des enfants appelés branches et des nœuds ne possédant pas d'enfants appelés feuilles.

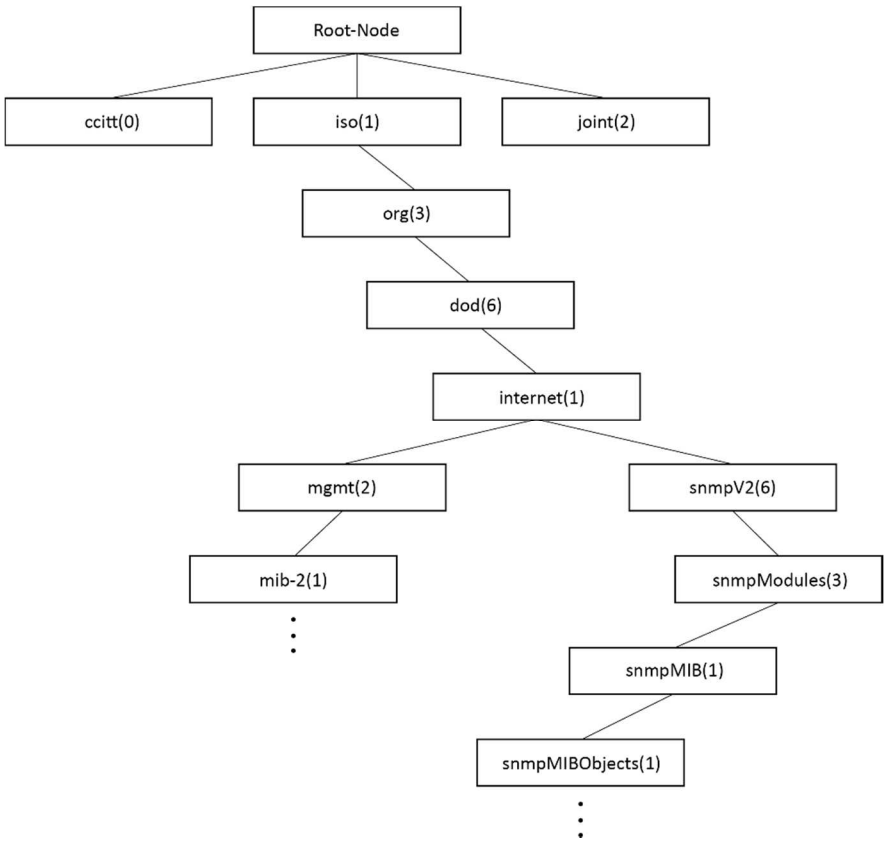


Figure 16 - Structure de l'arborescence SMIv2 pour SNMPv2

Un fichier MIB est un document écrit en langage ASN.1 qui définit pour chaque objet les éléments suivants :

- Nom ou OID, définit de manière unique un objet managé ;
- Type et Syntaxe, spécifie comment les données sont représentées et transmises entre le manager et les agents ;
- Rôle (description) ;

- Droits d'accès ;
- Statut.

La MIB-II correspond à un ensemble d'informations standards dont disposent tous les équipements qui implémentent SNMP. Les constructeurs peuvent également y adjoindre leur propre MIB pour donner accès à des objets spécifiques à leur application ou matériel.

Ces dernières, appelées MIB privées, apportent de nouvelles variables propres à chaque équipement que la MIB II ne pouvait pas apporter. La MIB privée différencie les constructeurs par un numéro unique qui est attribué par l'ISO. Ainsi, chaque constructeur possède un OID différent.

SNMP est donc un excellent moyen de collecter des informations utiles à l'administration de son réseau car il permet l'accès à un ensemble d'informations critiques sur chaque nœud du réseau. Ce standard est très largement implanté par les constructeurs sur leurs différents matériels.

1.2) WMI

Le WMI (Windows Management Instrumentation) est le système de gestion des éléments logiques et physiques des systèmes Microsoft Windows. Ce système de gestion interne au système d'exploitation est en charge de la surveillance et du contrôle de l'ensemble des ressources du système. Il offre la possibilité d'exécuter un programme, d'arrêter un service, de relancer le système, et surveille donc le fonctionnement et les performances. Cet outil est très pratique pour un administrateur réseau car c'est une API (Application Programming Interface) unique qui effectue l'ensemble des tâches d'administration.

WMI est issu du travail du groupe DMTF (Distributed Management Task Force) dont Microsoft fait partie et de l'initiative WBEM (Web-Based Enterprise Management). De cette initiative de normalisation est né le modèle CIM (Common Information Model), schéma orienté objet dont le but est de fournir une administration cohérente et unifiée de tous les éléments gérés. WMI est donc une implémentation du modèle CIM.

Le modèle CIM offre une décomposition des éléments du SI en s'appuyant sur la modélisation UML (Unified Modeling Language). CIM utilise un méta-modèle standardisé par le DMTF qui

reprend la notion de classe, propriété, de méthode et d'association. Un méta-modèle est une sorte de diagramme de classes qui définit la structure d'un ensemble de modèle

L'architecture WMI est constituée de 3 couches :

- les ressources gérées (Managed resources) ;
- l'infrastructure WMI ;
- les consommateurs (WMI Consumer).

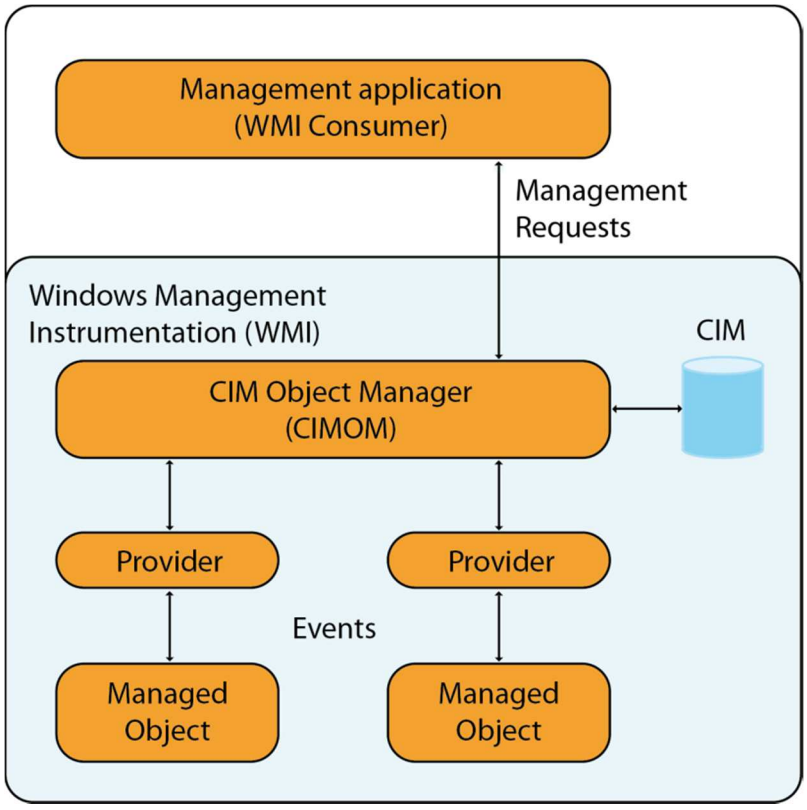


Figure 17 – Architecture WMI

Les ressources gérées sont les composants logiques ou physiques gérables par l'intermédiaire de WMI. Ceci inclut le système, les disques, les périphériques, les journaux, les fichiers, les répertoires, les composants réseaux, les processus, les paramètres de la Base de Registres, la sécurité, les services, la base SAM (Security Account Manager), l'annuaire LDAP (Lightweight Directory Access Protocol), l'installeur Windows, le WDM (Windows Driver Model) et la MIB SNMP.

Le WQL (Windows Management Instrumentation Query Language) est une implémentation Microsoft du CQL (CIM Query Language) dédiée au WMI. On peut donc, à partir de requêtes, agir sur les objets d'un système.

Exemple : *SELECT * FROM Win32_LogicalDisk WHERE FreeSpace < 2097152*

On peut ainsi interroger la base CIM qui est l'arborescence des classes représentant les éléments logiques et physiques du système. Ces classes sont groupées dans des espaces de nom (namespaces). Ce sont des groupes logiques de classes représentant un espace spécifique de gestion. Certaines parties de cette arborescence de classes sont gérées par des fournisseurs (providers) externes. Il existe un provider spécifique pour accéder aux fichiers de logs par exemple.

La sécurité d'accès et d'utilisation du WMI définit des droits différents en fonction du nom d'utilisateur et de l'espace de nom à atteindre. La sécurité utilisée pour l'authentification est celle de Windows (Kerberos[1]) et requiert donc d'utiliser des comptes préalablement configurés sur les postes clients. Par ailleurs chaque requête WMI utilise DCOM (Distributed Component Object Model) qui nécessite le mécanisme de transport RPC (Remote Procedure Call). Ce dernier crypte les paquets et offre ainsi un bon niveau de confidentialité et d'intégrité. Ce mécanisme d'authentification et d'échange est donc beaucoup plus sécurisé que le SNMP dans sa version 2.

Le protocole WMI permet d'accéder à des informations détaillées concernant le système d'exploitation, cependant il est beaucoup plus lourd que le SNMP (5 fois plus consommateur de ressources[2]).

Le protocole WMI peut dans certains cas poser des problèmes de communication à travers les pare-feu qui peuvent être traversés. SNMP est déprécié par Microsoft[3] et WMI peu à peu

[1] Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets.
[2] Site Internet Solarwinds [En ligne] (Page consultée le 17 Février 2017) https://support.solarwinds.com/Success_Center/Network_Performance_Monitor_(NPM)/What_polling_method_should_I_use%3F
[3] Site Internet technet.microsoft.com [En ligne] (Page consultée le 26 Mai 2017) https://technet.microsoft.com/en-us/library/hh831568(v=ws.11).aspx

remplacé. Microsoft préfère proposer à l'utilisation les derniers protocoles standards spécifiés par le DMTF : Le WS-Management (Web Services for Management).

1.3) WS-Management

Publié dans sa version finale (1.0) en 2008, le WS-Mangement (Web Services for Management) est une spécification du DMTF basé sur SOAP (Simple Object Access Protocol) définissant un protocole de communication pour l'administration des serveurs, périphériques, applications et services Web.

SOAP est un protocole de transmission de messages utilisant XML (eXtended Markup Language) et définissant un ensemble de règles afin de structurer les échanges de messages (voir figure 18). Il est particulièrement utile pour les dialogues requêtes-réponses.

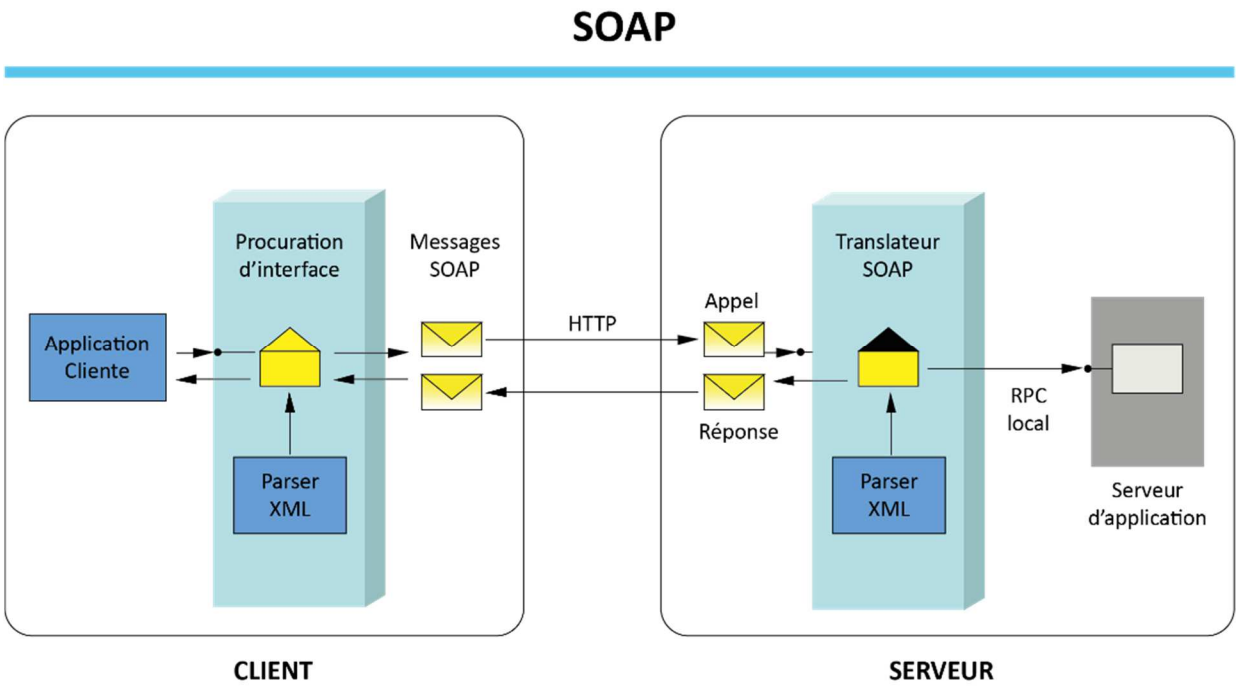


Figure 18 - Mécanismes d'échanges de messages SOAP

Un message SOAP valide est un document XML au bon format[1]. La figure 19 représente un exemple d'échange de messages SOAP. Ici la méthode appelle un service qui double la valeur d'un entier donné.

Signature de la Methode

```
int doubleAnInteger ( int numberToDouble );
```

Requête

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope
 SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/1999/XMLSchema">
      <SOAP-ENV:Body>
              <ns1:doubleAnInteger
               xmlns:ns1="urn:MySoapServices">
                      <param1 xsi:type="xsd:int">123</param1>
              </ns1:doubleAnInteger>
      </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Réponse

```
<?xml version="1.0" encoding="UTF-8" ?>
<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/1999/XMLSchema">
      <SOAP-ENV:Body>
              <ns1:doubleAnIntegerResponse
               xmlns:ns1="urn:MySoapServices"
               SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
                      <return xsi:type="xsd:int">246</return>
              </ns1:doubleAnIntegerResponse>
      </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figure 19 - Exemple d'échange SOAP par Nicholas Quaine [En ligne] (page consultée le 27 mai 2017) http://www.soapuser.com/fr/basics3.html

Ces échanges de fichiers XML s'effectuent en utilisant le protocole HTTPS qui authentifie et crypte les messages échangés, il offre par conséquent un très bon niveau de sécurité.

WS-Management fournit donc la possibilité via un échange de messages SOAP d'effectuer les tâches suivantes :

- Obtenir, mettre à jour, supprimer ou créer des paramètres et des valeurs dynamiques ;
- Enumérer le contenu de tables ou de fichier de logs ;
- Souscrire aux événements pouvant survenir sur les ressources gérées ;
- Exécuter des méthodes spécifiques de gestion sur les équipements gérés.

[1] Site Internet W3C sur XML [En ligne] (Page consultée le 20 Mars 2017) https://www.w3.org/XML/

WS-Management fournit également une couche d'abstraction permettant d'accéder aux informations CIM (WS-CIM).

WS-Management est un protocole récent et donc particulièrement adapté aux infrastructures distribuées souvent rencontrées de nos jours, notamment les architectures orientées services (SOA). Ce protocole est aussi habile pour la supervision que pour la gestion des équipements. Ainsi depuis 2008, les systèmes d'exploitation Microsoft incluent WinRM qui est l'implémentation que Microsoft a faite du WS-Management.

1.4) IPMI

IPMI (Intelligent Platform Management Interface) est une interface de supervision des composants matériels des ordinateurs et serveurs. En effet, il collecte des informations sur le matériel sans avoir besoin d'un système d'exploitation. Il est le résultat d'une initiative des constructeurs (Dell, IBM, Cisco…) qui souhaitaient offrir la possibilité de visualiser des informations sur l'état matériel (sondes de températures, vitesses de rotation des ventilateurs, etc.) à distance, même machine éteinte.

Ceci est possible grâce à une puce matérielle appelée BMC (Baseboard Management Controller).

Le BMC effectue l'interface entre l'application de gestion et le matériel. Il utilise IPMB (Intelligent Platform Management Bus) et ICMB (Intelligent Chassis Management Bus) pour communiquer avec les différents éléments matériels du châssis (voir figure 20). Il est possible d'interroger le BMC via le réseau et de collecter des informations intéressantes sans avoir à installer le moindre agent sur l'ordinateur cible. HP ILO ainsi que Dell IdRAC (Integrated Dell Remote Access Card) sont des implémentations de l'IPMI.

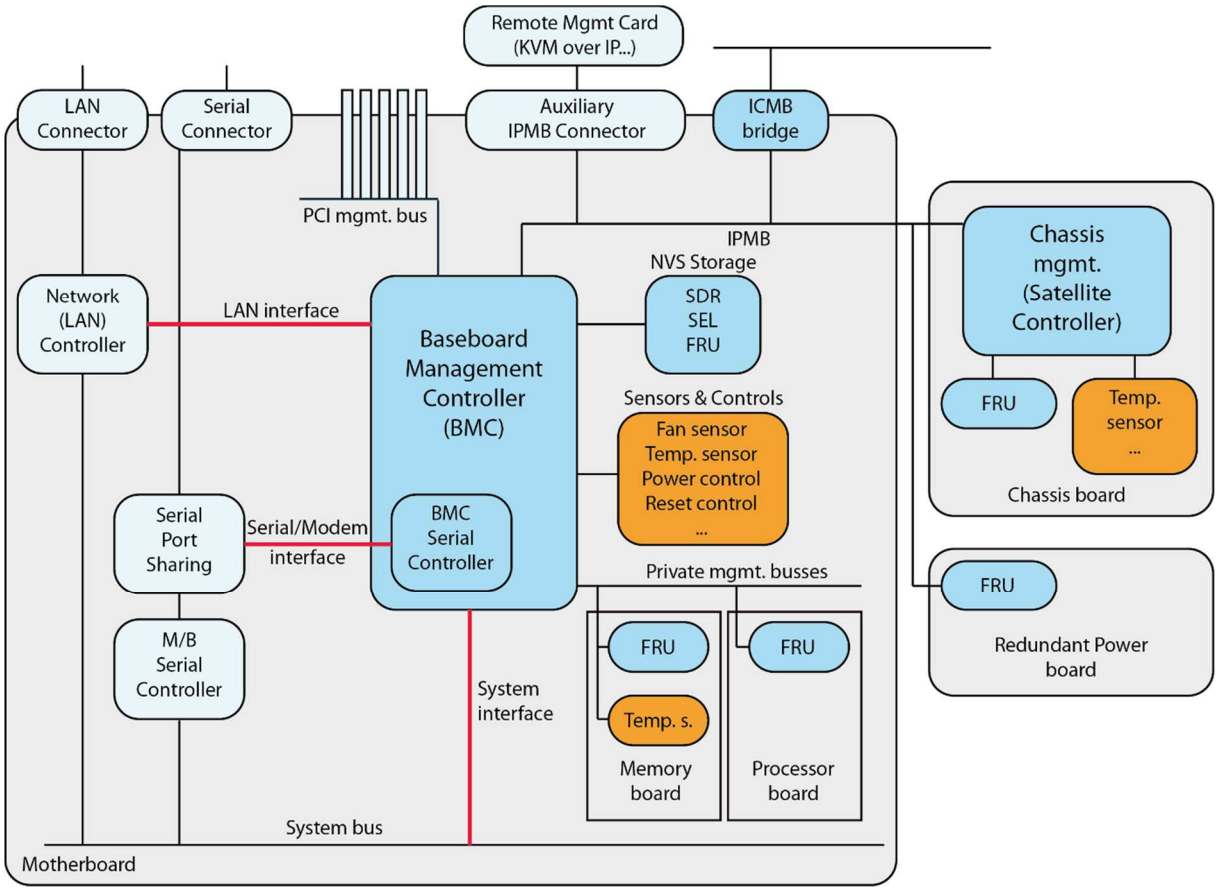


Figure 20 - Interconnexion du BMC avec les éléments physiques du système par Werner Fisher [En ligne] (Page consultée le 28 mai 2016) https://www.thomas-krenn.com/en/wiki/IPMI_Basics

La dernière version d'IPMI (2.0) apporte un niveau de sécurité suffisant. Cependant IPMI, dans son implémentation faite par les constructeurs peut représenter une faille de sécurité[1]. Il est très important de cloisonner le réseau d'administration IPMI et d'effectuer la mise à jour du BMC si l'interface IPMI est utilisée.

IPMI offre un accès aux statuts des serveurs et remonte les données en provenance des capteurs ou bien des sondes de température, il vérifie l'état des ventilateurs, et peut même contrôler jusqu'à l'alimentation. L'IPMI se porte donc plus sur la question de la supervision matérielle et apporte un moyen, sûr et rapide, d'accéder à ces informations importantes pour contrôler l'état de fonctionnement des machines et serveurs.

[1] Article en ligne « Sold Down the river » par Dan Farmer, [En ligne] http://fish2.com/ipmi/river.pdf (Page consultée le 17 avril 2017)

1.5) NetFlow/IPFix

NetFlow est une architecture de surveillance des réseaux développée par Cisco System qui collecte des informations sur les flux IP transitant par les interfaces des équipements. Netflow définit un format d'exportation des informations sur les flux réseaux et supervise, de façon fine, les ressources utilisées par l'ensemble des équipements connectés au réseau. Netflow est implémenté sur l'ensemble des équipements de type routeur de la marque Cisco.

Un flux réseau est défini par :

- Une adresse de source et de destination ;
- Un protocole (UDP, TCP…) ;
- Un type de service (Champ ToS présent dans l'entête IPv4) ;
- Un port applicatif ;
- Les interfaces d'entrées et de sortie du commutateur/routeur.

Grâce à NetFlow, les commutateurs et routeurs Cisco sont donc capables de maintenir une table (cache NetFlow) contenant les flux actifs transitant par leurs interfaces. Le protocole NetFlow est disponible depuis la version 12 des IOS[1] Cisco. À chaque nouveau paquet reçu, le routeur met à jour cette table, soit en créant une nouvelle entrée si le flux est nouveau, soit en incrémentant les compteurs d'une entrée existante. Les entrées de ces tables sont supprimées lorsque la connexion est expirée.

Les informations disponibles dans le cache peuvent donc être exportées afin d'être stockées et sauvegardées dans le but d'être analysées. Ce mécanisme de transfert utilise des trames NetFlow qui suivent le protocole définit par Cisco. Chaque trame d'export NetFlow regroupe plusieurs entrées du cache interne du routeur, elle contient une suite de Flowset. Chaque Flowset est constitué d'un « Template Flowset » qui représente l'organisation des données et d'un « Data Flowset » qui contient les données elles-mêmes (voir figure 21). Ces flux sont encapsulés dans des segments UDP afin d'optimiser les performances de traitement. Cependant le protocole NetFlow n'assure pas la confidentialité, l'authentification et l'intégrité des données échangées.

[1] IOS = Internetwork Operating System (Système d'exploitation pour la connexion des réseaux)

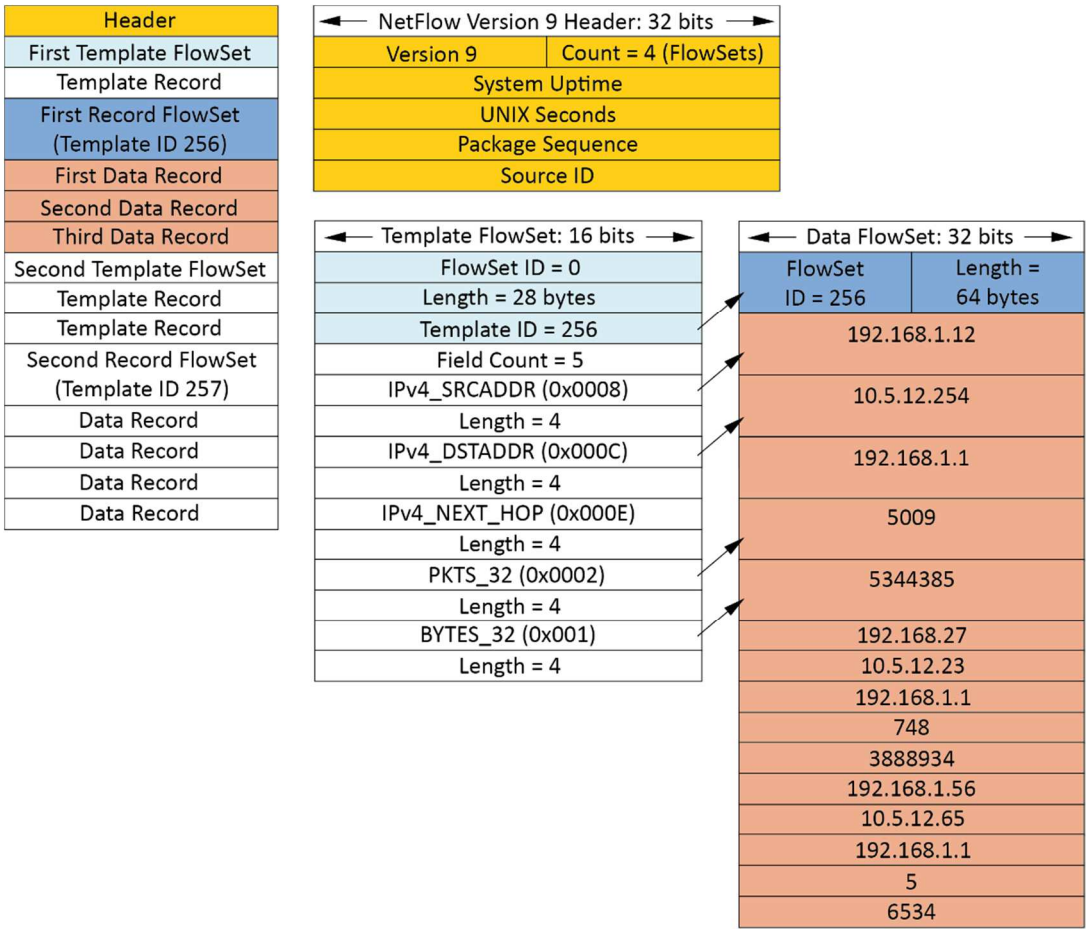


Figure 21 - Détail du paquet d'export NetFlow, Cisco.com [En ligne] (Page consultée le 22 mars 2017) http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html

Le destinataire des trames NetFlow, le NetFlowCollector est un serveur en charge du filtrage et du stockage des données de flux. Ces données pourront être ensuite présentées sous forme statistique ou graphique pour être analysées ou surveillées.

IPFix est le protocole standard développé par l'IETF en se basant sur la version 9 de NetFlow. Il apporte quelques améliorations à ce dernier et notamment propose l'utilisation du protocole SCTP (Stream Control Transmission Protocol). Ce protocole apporte une meilleure fiabilité ainsi que plus de sécurité et de performance dans l'envoi des informations. Il est par exemple possible d'utiliser le protocole TLS (Transport Layer Security) avec TCP.

L'analyse des flux réseaux offre aux administrateurs une vision claire et précise de ce qui transite sur leur réseau. Des outils d'analyse les présentent sous forme de tableaux de bord qui facilitent la lecture de la performance du réseau. Ils peuvent indiquer le type de consommation par utilisateur, par application et par type de flux.

Ces protocoles de supervision proposent donc une solution aux administrateurs soucieux de maîtriser avec précision les données transitant sur leur réseau. Les outils de supervision réseau compatibles avec NetFlow/IPFix analysent en temps-réel les flux et sont capables de générer des alertes en cas de dépassement anormal d'un seuil.

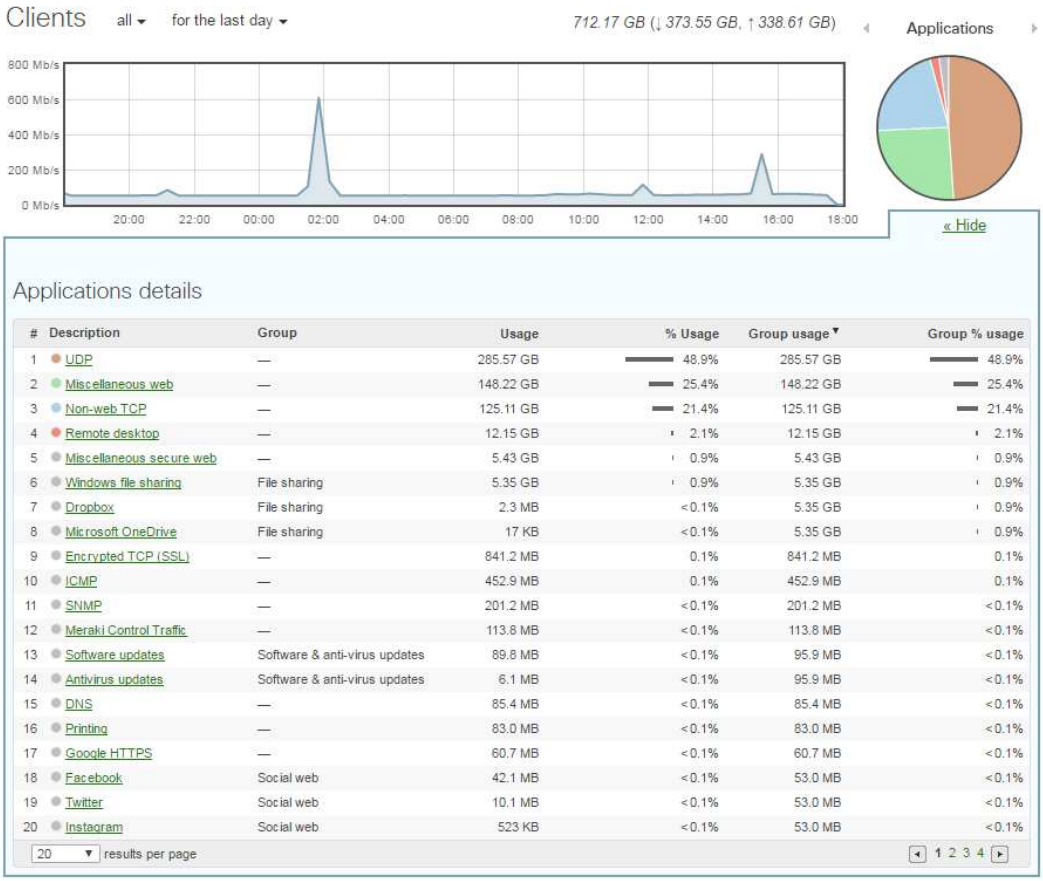


Figure 22 - Tableau de bord NetFlow Cisco Meraki

Les communautés scientifiques et informatiques, ainsi que les constructeurs, se sont donc accordés pour mettre au point plusieurs standards dans le domaine de la gestion et de la supervision. Les protocoles présentés dans ce mémoire ne représentent pas une liste exhaustive des technologies de supervision existantes, mais sont des standards bien en place dans le monde de la supervision des SI. Chacun d'entre eux possède des avantages et des inconvénients. Nous verrons que la question du choix du protocole se pose à chaque fois qu'un nouveau besoin de supervision survient. Les réseaux étant souvent des environnements informatiques extrêmement hétérogènes, ce n'est qu'en couvrant les protocoles les plus courants que l'on peut espérer obtenir une supervision suffisamment globale.

Chapitre 2 : Le choix de la solution

Même si les solutions de supervision peuvent concerner les différents services d'une entreprise, c'est la DSI qui sera en première ligne durant ce projet. C'est elle qui devra recenser les besoins et accompagner la mise en place et la maintenance de la solution. Cela impose d'avoir une certaine rigueur dans ce choix qui se doit d'être cohérent avec la politique de la DSI. Nous allons dans cette partie documenter les étapes qui nous ont conduits à choisir l'outil de supervision Centreon.

2.1) Évaluation du besoin en supervision

On vient de le voir, les solutions et protocoles de supervision sont nombreux. La DSI dispose donc d'un large choix d'outils lorsqu'elle souhaite mettre en place une supervision de son SI. Les besoins en supervision du SI du groupe Powerflute requiert l'installation et la configuration d'un outil NMS. Ce type d'outil possède un coût, que ce soit en termes de licence ou de temps. Il est donc important de choisir la solution qui répond aux besoins actuels et futurs car elle accompagnera le SI pendant de nombreuses années.

En dehors de l'investissement que cela nécessite, il faut considérer la solution dans sa globalité et s'assurer qu'elle réponde correctement à chacun des besoins formulés par Powerflute. Il faut donc se poser les bonnes questions dès le départ car c'est une étape importante pour la DSI mais également pour l'entreprise qui l'accompagne.

Dans un premier temps, il est important de savoir :

- Ce que l'on souhaite superviser. Quel est le périmètre présent et à venir ?
- Pourquoi superviser. Quels sont les problèmes déjà rencontrés ou possibles ?
- Pour qui superviser. Qui va devoir gérer et utiliser la supervision ?

Dans un second temps il faudra savoir comment nous souhaitons superviser.

Dans notre cas d'étude, la solution doit proposer la possibilité de superviser les éléments essentiels au fonctionnement du réseau qui est le support indispensable à la bonne marche des unités du groupe Powerflute. L'infrastructure réseau est récente, il y a donc peu de changements majeurs à envisager dans les quelques années à venir. Cependant la supervision

doit déjà être conçue avec assez de flexibilité pour s'adapter aux évolutions techniques futures.

Les principaux critères de choix sont donc les suivants :

- Capacité d'adaptation au SI ;
- Capacité de mise à jour ;
- Possibilité de superviser de façon centrale une implantation réseau distribuée ;
- Utilisation des protocoles standards de supervision ;
- Facilité de développement des sondes et nombre de sondes préconfigurées disponibles ;
- Facilité d'intégration progressive de la solution ;
- Possibilité d'effectuer un test de la solution ;
- Possibilité de stocker les données collectées sur une période assez longue (1 à 2 ans) ;
- Capacité à présenter ces données et à construire des rapports afin de dégager des tendances pour orienter les choix stratégiques de la DSI ;
- Capacité de configuration des alertes et des escalades ;
- Fonctionnement intuitif et ajout de nouveaux composants rapide ;
- Possibilité de configurer de façon précise les sondes de chaque équipement afin de définir des seuils d'alerte précis ;
- Possibilité d'accès depuis tout type de terminal (ordinateur, smartphone) ;
- Performance du support de la solution, fourniture de guides d'utilisation détaillés ;
- Sécurité et résilience de la solution ;
- Prix et mode de licence de la solution.

L'intégralité de ces critères ne dépend pas uniquement de la solution en elle-même mais aussi de la manière dont elle sera configurée et utilisée. Ces critères conviennent à la plupart des projets de supervision NMS, mais il est également important de définir de façon précise ce que l'on souhaite superviser et comment on souhaite le faire.

La mise en place d'un tel outil doit commencer par une analyse des chaînes de liaisons qui composent le SI sur chaque site. Ces liaisons doivent-être décrites avec une granularité

suffisante pour identifier les points de contrôle essentiels, ainsi que leurs métriques. Il faut également recenser les applications et définir leur importance dans les processus métier. Il convient ensuite de représenter les différentes interactions entre ces applications pour définir les points critiques et les données à récolter.

De cette première analyse, doivent ressortir des exigences précises que l'outil devra pouvoir accomplir. Il faut également définir les métriques réseaux utiles pour comprendre, contrôler et prédire le déroulement des applications. Afin d'être pertinentes pour les informaticiens et les utilisateurs des applications, ces métriques doivent avoir un sens du point de vue de l'application et pas seulement de l'infrastructure. Durant la phase de test on validera chacune de ces exigences pour être en mesure d'évaluer la pertinence de chaque outil.

On en déduit alors plusieurs étapes :

L'observation : consiste à regarder les applications métier dans leur ensemble et à comprendre le comportement et les exigences en termes de performance des applications, ceci afin de définir les sondes devant être utilisées.

La modélisation : il faut construire des modèles pour mieux comprendre l'utilisation du réseau faite par les applications.

Le déploiement : consiste à programmer la solution afin qu'elle réponde aux modèles préalablement définis.

La validation : c'est la phase durant laquelle l'équipe technique et les responsables métier s'accordent sur les résultats obtenus durant les tests. Ces tests doivent satisfaire les exigences émises par les techniciens et les responsables métier.

Durant le déploiement de la solution, chaque sonde doit être paramétrée avec précision afin d'être à même de retourner un défaut uniquement quand il y a une situation réellement anormale. L'observation du comportement des sondes et des premiers graphiques générés par la supervision doit conduire à un ajustement du réglage de la solution. La capacité de la station NMS à offrir aux administrateurs une interface de gestion permettant de mener ses réglages avec efficacité est un des critères de sélection ayant son importance.

Voyons maintenant quelles sont les stations NMS aptes à répondre au besoin de Powerflute et comment nous avons effectué notre choix.

2.2) Présentation des solutions étudiées

Devant la multitude d'outils de supervision proposés, il est bien évidemment impossible de tester intégralement chaque solution existante sur le marché. Nous avons choisi de nous concentrer sur 3 outils. En effet, les outils de supervisions sont souvent similaires et répondent chacun à leur façon aux principaux critères de sélection. Nous avons fait le choix de tester ces applications car chacune a ses propres spécificités techniques et fait office de référence dans le domaine de la supervision réseau.

La société Solarwinds créée en 1999 commercialise plusieurs solutions de sécurité et de supervision réseau. Les produits NPM (Network Performance Monitor) et SAM (Server & Application Monitor) qu'elle commercialise correspondent tous les deux au besoin exprimé par Powerflute. Ces produits sont adaptés à des entreprises de toutes tailles et sont évolutifs.

La société Centreon (ex Merethis), spécialisée dans la supervision réseau depuis plus de 10 ans, distribue en version gratuite la partie NMS (Centreon CES) de ses logiciels.

Panda Security existe depuis 1990. Elle commercialise des solutions de sécurité pour les particuliers et professionnels. Panda Security a fait partie des premiers à avoir commercialisé des solutions de sécurité « Cloud » et également une solution de supervision « Cloud » des systèmes et périphériques : « Panda System Management ».

Ces trois solutions utilisent des architectures de fonctionnement différentes. Nous allons étudier ces différences dans la partie suivante.

2.3) Architecture et réponse au besoin

2.3.1) SOLARWINDS

NPM de Solarwinds[1] est une application qui s'installe sur l'infrastructure réseau du client et nécessite un ou plusieurs serveurs Windows pour fonctionner. Les produits commercialisés par Solarwinds s'articulent autour du cœur de leur système appelé Orion.

Il est possible d'adapter l'architecture NPM en fonction de la taille du réseau à superviser, et ainsi d'obtenir une architecture distribuée disposant d'assez de performances pour gérer un grand nombre de nœuds réseau répartis géographiquement sur des sites distants.

La console de visualisation est un site internet accessible de façon interne, et éventuellement externe, au réseau de l'entreprise si celle-ci l'autorise. Cette console permet également d'effectuer la configuration. Un outil de découverte du réseau est disponible et alimente de façon automatique l'interface de supervision.

Les sondes disponibles sont nombreuses et adaptées à la majorité des matériels et logiciels existant. Ces sondes utilisent bien entendu le protocole SNMP mais également L'IPMI, le WMI, NetFlow, ou encore SYSLOG (supervision des événements système, *logs*).

Les solutions Solarwinds disposent d'une bonne communauté d'utilisateurs, de forums de support actif et d'une documentation complète et détaillée. Il est important de noter que les avis des clients de Solarwinds sont, dans l'ensemble, relativement bons[2].

Le prix de NPM Solarwinds se situe aux alentours de 8 000€ pour la licence NPM seule et pour un nombre de nœuds limité (500). Le coût global de cette solution est assez élevé par rapport au nombre d'éléments supervisés. La plupart des fonctionnalités intéressantes sont inclues dans des licences supplémentaires ce qui augmente considérablement le prix final de la solution.

[1] Fiche technique Solarwinds NPM [En ligne] (Page consultée le 12 mai 2017)
http://content.solarwinds.com/creative/pdf/datasheets/sw_npm_datasheet_0512.pdf
[2] Site Internet Trustradius [En ligne] (Page consultée le 22 Février 2017)
https://www.trustradius.com/products/solarwinds-network-performance-monitor/reviews

2.3.2) CENTREON

Centreon CES[1] est une solution qui s'installe sur le réseau interne de l'entreprise. En fonction de la taille de l'infrastructure à superviser, il est possible de déployer plusieurs serveurs de supervision afin d'obtenir une architecture distribuée adaptée au nombre d'éléments à superviser et de leurs emplacements géographiques.

L'interface de gestion web est accessible en interne mais peut également l'être en externe en fonction de la configuration des pare-feu. Centreon supporte la majorité des protocoles de supervision actuels.

Ce logiciel gratuit est disponible avec quelques sondes préconfigurées uniquement. Cependant il est important de noter que la plupart des sondes peuvent être configurées manuellement et qu'il existe une forte communauté développant des sondes et les proposant gratuitement. Il est donc facile de trouver des sondes pour la grande majorité des équipements et applications de son réseau. Il est également possible d'acheter des packs de sondes préconfigurées.

L'interface de gestion est simple, mais il est impératif de comprendre les concepts de supervision pour bien appréhender ce logiciel. La documentation est complète et les forums d'utilisateurs très actifs.

La version CES gratuite peut s'enrichir de fonctionnalités supplémentaires comme la cartographies (MAP) ou évoluer vers un outil de supervision BAM. L'achat de licence permet de disposer d'un support professionnel.

2.3.3) Panda System Management

Panda System Management[2] est une solution « Cloud », c'est-à-dire qu'elle ne monopolise pas, ou peu, de ressources physiques en interne.

[1] Fiche technique Centreon CES [En ligne] (Page consultée le 15 mai 2017) https://static.centreon.com/wp-content/uploads/2016/03/factsheet-Centreon-fr.pdf
[2] Fiche technique Panda System Management [En ligne] (Page consultée le 15 mai 2017) http://resources.pandasecurity.com/enterprise/solutions/pcsm/pcsm-user-datasheet-fr.pdf

La console de visualisation et de gestion est donc accessible pourvu que l'on ait accès à Internet. Panda System Management base son fonctionnement sur des agents installés en local sur les serveurs et ordinateurs du réseau. Certains de ces agents peuvent être configurés pour jouer le rôle de collecteur. Ces collecteurs sont en charge de récupérer des informations via SNMP ou autre à travers le réseau local, et de les transmettre à la plateforme « Cloud ».

Certaines sondes sont fournies avec la licence standard, mais beaucoup sont payantes. Le catalogue des sondes disponibles est moins riche que ses concurrents et la communauté des utilisateurs semble moins active.

Panda System Management est une solution avant tout pensée pour la supervision des postes utilisateurs mais propose, également, une approche intéressante pour la supervision de tous les nœuds du réseau.

Cette solution logicielle étant déjà utilisée au sein de notre groupe pour la supervision des machines Windows (serveurs ou postes de travail), il apparaissait intéressant de l'étudier car le coût de sa licence est déjà pris en compte dans le budget de la DSI. Seules les sondes spécifiques payantes auraient représenté un coût supplémentaire.

2.4) Comparatifs et choix définitif

2.4.1) Tableaux comparatifs de ces solutions

Dans les tableaux suivants (figure 23 à 25), nous avons repris les principaux critères de sélection d'un outil de supervision et avons effectué pour chaque solution retenues des essais ou recherches afin de déterminer une note sur chacun de ces critères (1 = ne satisfait pas ou peu, 2 = satisfait en partie, 3 = satisfait, 4 = satisfait complètement).

Le dernier tableau (figure 26) reprend quant à lui les exigences que nous avons formulées et la capacité que chaque outil avait à répondre à ces dernières (1 = ne satisfait pas, 2 = satisfait en partie, 3 = satisfait parfaitement).

Critères	Solarwinds	Note /4
Adaptation	La solution permet de déployer des satellites supplémentaires en cas d'augmentation du volume. Possibilité d'externaliser la base de données et de construire plusieurs serveurs de vue si besoin	4
Mise à jour	Chaque année une importante mise à jour est publiée et accessible aux clients possédant les anciennes versions, la mise à jour s'effectue via un fichier d'installation et un outil d'aide et de préparation à la mise à jour	4
Supervision centrale	Un serveur de vue unique regroupant l'intégralité des informations collectées	3
Utilisations des standards : SNMP WMI IPMI SYSLOG NETFLOW JMX SBLIM	SNMP WMI IPMI SYSLOG NETFLOW JMX . Dispose également d'un agent pouvant transmettre les informations au serveur central.	4
Sonde préconfigurée et développement	Configuration après découverte automatique du réseau simplifié, détection automatique des types de matériels via SNMP.	3
Intégration	Installation de l'architecture bien documentée.	3
Possibilité d'effectuer un test de la solution	Essai 30 jours	2
Stockage	Dépend de la capacité de stockage allouée aux bases SQL	3
Reporting	Tableaux de bord et rapports personalisés possibles.	3
Seuils d'alertes et règles de notification	Interface web qui permet un accès rapide aux sondes et un paramétrage rapide des seuils. Possibilité de notifier les utilisateurs par groupes en fonctions des alertes.	3
Fonctionnement intuitif	Interface web simplifiée, satisfaction globale des utilisateurs de la solution.	3
Accès	Via un portail accessible depuis internet, application mobile payante.	3
Support, guide, documentation	Dispose d'un forum d'utilisateur, d'une documentation complète et d'un bon support technique. Forte communauté d'utilisateurs.	3
Sécurité et résilience de la solution	Possibilité de configurer la solution en haute disponibilité. Solution sécurisée.	3
Prix et mode de licence de la solution	12800e la première année puis maintenance annuelle. La prix de la licence est fonction du nombre de points de contrôle.	2
Avis global	Bonne solution technique dotée d'une bonne communauté d'utilisateurs ayant l'air dans l'ensemble satisfaits de ce produit. Solution performante mais très coûteuse.	2
		48

Figure 23 - Évaluation de la solution Solarwinds

Critères	Centreon	Note /4
Adaptation	Permet de construire une architecture distribuée avec autant de satellites que nécessaire.	4
Mise à jour	Mise à jour des différents composants disponibles couramment et facilement installables. Mise à jour de la version du produit supporté et bien documenté.	4
Supervision centrale	Un portail d'accès interne à l'entreprise centralise les données.	2
Utilisations des standards : SNMP WMI IPMI SYSLOG NETFLOW JMX SBLIM	SNMP WMI IPMI SYSLOG NETFLOW JMX SBLIM. Possibilité d'utiliser un agent local pour la récupération d'éléments plus spécifiques.	4
Sonde préconfigurée et développement	Beaucoup de sondes gratuites sont fournies et disponibles en téléchargement. Cependant la configuration de certaines sondes peut être fastidieuse.	3
Intégration	Pas d'outils de découverte automatique des équipements du réseau. Cependant installation plateforme très rapide et grâce aux quelques sondes préconfigurées est fonctionnel en quelques minutes.	3
Possibilité d'effectuer un test de la solution	Version gratuite	4
Stockage	Dépend de la capacité de stockage allouée au serveur central	3
Reporting	Tableaux de bord simples sur la version gratuite, les versions payantes offrent plus de possibilités pour construire des rapports plus complexes.	3
Seuils d'alertes et règles de notification	Réglage entièrement personnalisable et règles de notifications précises	3
Fonctionnement intuitif	Interface minimaliste mais efficace, interface de configuration facile à prendre en main quand on a bien compris les bases du fonctionnement	3
Accès	Portail interne à l'entreprise, possibilité d'application mobile.	2
Support, guide, documentation	Très forte communauté, forum très actif, documentation complète et support assuré en version payante.	3
Sécurité et résilience de la solution	Possibilité de configurer l'infrastructure en haute disponibilité. Solution sécurisée, si l'on suit les recommandations.	3
Prix et mode de licence de la solution	Version CES gratuites. Possibilité d'obtenir des packs de sondes et des fonctionnalités avancées pour 10000e la première année puis 2000e de maintenance annuelle.	2
Avis global	Très bonne solution gratuite. Enormement de guides disponibles pour répondre aux besoins les plus courants. Pas de facturation au nombre de sondes. Un standard reconnu dans la communauté.	4
		50

Figure 24 - Évaluation de la solution Centreon

Critères	Panda	Note /4
Adaptation	Utilisation de satellites pouvant être un ordinateur du réseau.	4
Mise à jour	Mise à jour automatique	4
Supervision centrale	Portail "Cloud" d'accès à l'ensemble des données.	2
Utilisations des standards : SNMP WMI IPMI SYSLOG NETFLOW JMX SBLIM	SNMP SYSLOG WMI	4
Sonde préconfigurée et développement	Quelques sondes préconfigurées, peu de sondes disponibles comparé aux autres solutions.	1
Intégration	Solution "Cloud", outil de découverte, configuration rapide.	3
Possibilité d'effectuer un test de la solution	Version payante, essai 30 jours	2
Stockage	Illimité	3
Reporting	Outils de reporting simple à configurer	3
Seuils d'alertes et règles de notification	Configuration personalisée limitée	2
Fonctionnement intuitif	Interface rapide mais pas toujours intuitive.	2
Accès	Portail "Cloud", application mobile.	3
Support, guide, documentation	Support standard, peu d'utilisateurs pour la partie spécifique NMS	2
Sécurité et résilience de la solution	Fragilité de la collecte des données avec les agents locaux.	2
Prix et mode de licence de la solution	Version payante, mais solution déjà en place et financée.	2
Avis global	Solution intéressante pour la gestion des postes de travail mais plus limitée sur la partie supervision réseau.	4
		43

Figure 25 - Évaluation de la solution Panda System Management

Type	Description du test	SOLARWINDS	Note /3	CENTREON	Note /3	PANDA	Note /3
Supervision	Ping : vérifier la présence et les temps de latence	OK	3	ok	3		3
Supervision	Windows : Récupérer la consommation de CPU en %	OK	3	ok	3		3
Supervision	Windows : Récupérer l'état d'un service	OK	3	Possible	2	Possible	2
Supervision	Meraki : Récupérer l'état d'une interface et le débit	OK	3	Possible	2	Non satisfait	0
Supervision	Matériel serveur : Récupérer l'état des composants matériels (disques par exemple) en IPMI	OK	1	OK		Non satisfait	0
Supervision	Sauvegarde : récupérer l'état des sauvegardes VEEAM	OK	3	OK	3	OK	3
Supervision	Réseau : surveillance des ports ouverts d'un serveur	OK	1	OK	3	OK	3
Supervison	Temps de déploiement d'une nouvelle sonde	Court	3	Long	2	Long	2
Supervison	Temps d'ajout d'une sonde déjà déployée sur un autre équipement	Court	3	Court	3	Court	3
Supervision	Réaction en cas d'alerte : relancer un service automatiquement	Non satisfait	1	Faisable	2	Non satisfait	1
Reporting	Afficher l'ensemble des équipements d'un site particulier	OK	3	OK	3	OK	3
Reporting	Afficher toutes les sondes CPU	OK	3	OK	3	OK	3
Reporting	Afficher tous les débits des ports des switchs Meraki	OK	3	OK	3	Non satisfait	1
Reporting	Extraction des données	OK	3	OK	3	OK	3
Alerte	Réception d'un e-mail en cas d'alerte au reponsable site	OK	3	OK	3	OK	3
Alerte	Réception d'un e-mail à l'équipe IT si problème précédent dans un état critique et pas résolu au bout de 30 minutes	OK	3	OK	3	OK	3
			42		41		36

Figure 26 - Tableau de réponses aux exigences

2.4.2) Notes finales obtenues par les solutions

SOLUTION	NOTE 1	NOTE 2	TOTAL
SOLARWINDS	**48**	**42**	**90**
CENTREON	**50**	**41**	**91**
PANDA	**43**	**36**	**79**

Figure 27 - Tableau des notes des solutions étudiées

Les solutions Solarwinds et Centreon sont très proches du point de vue des fonctionnalités. Nous avons fait le choix de Centreon CES car il est issu d'un standard de la supervision (NAGIOS) et dispose d'une communauté d'utilisateurs plus importante auprès de laquelle sa réputation n'est plus à faire. Il était également important de trouver une solution avec un coût minimum car la mise en place de la nouvelle infrastructure réseau du groupe Powerflute/Corenso s'est avérée très coûteuse et les budgets initialement prévus étaient déjà dépassés. Ce critère d'importance n'est malheureusement pas du tout rempli par Solarwinds qui, même s'il propose des fonctionnalités très évoluées, est très coûteux.

Centreon, de par sa proche filiation avec Nagios, utilise un principe de fonctionnement similaire et une certaine compatibilité. L'outil NAGIOS et ces principes de supervision étant déjà connus par moi-même, il était plus cohérent pour garantir la réussite du projet de choisir des technologies déjà maîtrisées.

Enfin, la rapidité d'installation de l'infrastructure de Centreon CES constatée lors de la phase d'essai, comparée par exemple à celle nécessaire par la solution de Solarwinds, a été un argument supplémentaire. L'installation d'une solution de supervision à l'échelle d'un groupe implique une installation progressive sur chacun des sites. Qu'elle nécessite ou non l'ajout de composants techniques, il est important que les équipes chargées de sa configuration consacrent leurs efforts à la configuration de la supervision plutôt qu'à son installation.

Nous venons de voir les principales solutions technologiques qu'il est important de connaître lorsque l'on souhaite se lancer dans un projet de supervision de son infrastructure réseau. Les outils sont nombreux et il est important de choisir un outil NMS qui soit cohérent avec le projet de l'entreprise. Si les ressources humaines internes sont disponibles, il est possible de choisir un outil totalement gratuit mais les équipes devront consacrer du temps pour le configurer. Les DSI disposant de peu de ressources humaines peuvent s'orienter sur des solutions payantes qui proposent des modèles de configuration destinés à faciliter la mise en œuvre de la supervision. Des sociétés comme Centreon proposent également leur expertise par le biais de services d'aide au déploiement de leur solution.

Dans tous les cas, il est important que l'ensemble de l'équipe informatique se saisisse de l'importance du déploiement d'un tel outil. La définition claire des besoins dès le départ du projet et l'affinement de ces derniers tout au long de celui-ci sont très importants pour sa réussite. Il n'existe pas de solution de supervision « clés en main » qui soit totalement adaptée aux spécificités du SI. Nous allons, dans la prochaine partie, développer comment nous avons procédé pour l'organisation de ce projet et expliquer l'ensemble des choix techniques que nous avons réalisés afin que Centreon reflète au mieux l'organisation du SI de Powerflute.

Partie III - Conception et mise en production de la plateforme de supervision

Nous avons, dans les deux précédentes parties, situé le contexte de ce projet, défini notre besoin en supervision et choisi un outil de supervision. Ce choix possède la particularité de demander un effort particulier à l'équipe projet. En effet il s'agit maintenant d'installer et de conceptualiser la solution Centreon, et ceci uniquement sur les ressources internes de l'entreprise.

Chapitre 1 : Gestion du projet

La réalisation d'un projet de supervision n'est pas un projet classique car elle nécessite une implication particulière de la DSI. Nous allons voir dans cette partie comment nous avons organisé nos travaux afin de s'assurer la conception d'un outil en parfaite adéquation avec nos attentes, en prenant en compte les contraintes de ressources.

1.1) Organisation du projet

Sur ce projet, j'interviens avec une grande autonomie, à la fois en tant que chef de projet mais aussi en tant que MOA et MOE. Le projet est supervisé par M. Patrick Kittle qui fait donc partie de la MOA ainsi que M. Gavin McKay. En tant que chef de projet, je me devais d'établir un budget clair. Le fait d'avoir choisi un outil libre impliquait surtout de proposer une budgétisation du temps nécessaire à la réalisation de ce projet en interne.

Afin de se donner les moyens de respecter la planification proposée en début de projet, j'ai défini plusieurs jalons qui se devaient d'être respectés. Un suivi hebdomadaire a donc été réalisé avec un point oral effectué avec l'ensemble de l'équipe projet. Les étapes de validation ont été effectuées par e-mails et discussions instantanées avec la MOA ceci afin de respecter le principe de gestion de projet selon les cycles en V. Ainsi, depuis la définition des exigences jusqu'à la mise en production, j'avais la certitude de travailler de façon efficace en suivant le cap donné par la DSI.

J'ai également mis en place un pilotage du projet par les risques. J'ai donc identifié dès le départ du projet les risques principaux et effectué un suivi de ceux survenant durant le projet (voir annexe 1). Cette méthode a permis d'orienter certains choix techniques mais aussi de construire une planification réaliste et de l'adapter aux vues des tâches habituelles de chacun.

Le projet a été réalisé dans les délais fixés et le logiciel ainsi fourni répond correctement aux besoins que nous avions exprimés au début du projet. Plusieurs séries de tests ont été réalisés pour vérifier la conformité de la solution finale. Ces tests ont été effectués au fur et à mesure du déploiement des sondes de notre système et ont permis de détecter certains écarts. Ces derniers nous ont conduits à des ajustements de configuration avant la livraison définitive et le début de l'installation de la supervision sur les sites du groupe Powerflute.

Cette gestion de projet a notamment permis d'identifier que les techniciens des différents sites étaient peu disponibles, et qu'il fallait limiter au maximum leur temps de travail sur ce projet. Ceci a conduit à la conception d'une méthodologie pour paramétrer Centreon sur chaque site de façon rapide et ne nécessitant pas de connaissance approfondie de l'outil de la part des techniciens.

1.2) Les phases du projet

Ce projet se découpe en 3 phases principales.

Phase 1 :

Cette première phase avait pour but de trouver et préparer la solution technique, mais aussi de décrire une méthode spécifiquement adaptée à Powerflute, pour s'assurer du bon déploiement sur chaque site. En plus de déterminer de façon précise l'architecture technique de fonctionnement, il était important de s'organiser afin de canaliser les efforts des administrateurs. Ceci afin de s'assurer de la cohérence du déploiement et éviter un environnement de supervision trop hétérogène.

Cette méthode d'organisation permet le paramétrage de la solution de façon rapide afin que les administrateurs se concentrent avant tout sur la finalité plus que sur l'import lui-même.

À la fin de cette phase, la supervision est fonctionnelle sur le site de Corenso France. Ce premier déploiement a été l'occasion de tester différents paramétrages de Centreon dans le but de trouver la configuration optimale pour l'utilisation que souhaite en faire Powerflute.

Phase 2 :

La deuxième phase du projet mobilise cette fois-ci l'ensemble des ressources de l'équipe. On dispose maintenant de la méthode et des outils nécessaires au succès de cette étape. J'ai donc organisé une réunion de présentation de l'outil final avec l'ensemble de l'équipe IT, pour la sensibiliser à son utilisation et présenter notre méthode. Cette réunion a permis de déterminer un planning de mise en production sur chaque site. Chacun des membres de notre équipe s'est vu attribuer plusieurs sites, et doit être en mesure de livrer des documents qui seront utilisés pour le paramétrage de la solution de supervision dans les délais convenus.

Chaque responsable de site sera également accompagné par moi-même durant le déploiement de la supervision.

Durant cette phase, un autre technicien a été choisi pour faire partie des administrateurs de la solution, des sessions de formation à l'administration seront donc organisées par mes soins. La rédaction du support de formation devra être effectuée rapidement car la formation sera probablement organisée durant l'été, période où la charge de travail sera plus compatible (les dates ne sont pas encore déterminées avec précision).

Une fois le paramétrage définitivement validé par l'ensemble de l'équipe, je pourrais effectuer la rédaction de la documentation du système de supervision Powerflute/Corenso, c'est-à-dire des procédures liées à son administration.

Phase 3 :

La troisième phase correspond à la vie du projet. Un système d'information étant en perpétuel mouvement, il convient de s'assurer de la mise à jour et de l'ajout des sondes nécessaires au fil de l'utilisation de Centreon. Les administrateurs de la supervision seront les garants de ces mises à jour grâce à une file de support dédiée dans l'outil ITSM du groupe.

1.3) Planification

La particularité de ce projet réalisé en interne est qu'afin d'obtenir une planification détaillée, il nous fallait dans un premier temps avoir choisi l'outil et étudié son fonctionnement, ceci afin de mieux comprendre l'ensemble des taches nécessaires à l'installation et au paramétrage de la solution.

En début de phase 1, suite aux études effectuées sur Centreon, nous avons donc pu effectuer une liste de tâches prévisionnelles :

- Inventorisation et mise à jour des plans réseaux ;
- Installation d'un Centreon CES de test sur le site de Corenso France ;
- Test des différentes sondes et configuration des modèles ;
- Test du paramétrage (groupes, modèles) ;
- Installation du serveur central ;

- Installation du collecteur pour le site de Corenso France ;
- Configuration du collecteur sur le central ;
- Import des sondes validées dans le système de test ;
- Création des modèles de service définitivement validés ;
- Import et paramétrage des groupes d'hôtes, services, contacts, accès ;
- Import des hôtes ;
- Rédaction de la documentation ;
- Installation des collecteurs pour chacun des sites ;
- Déploiement sur chacun des sites ;
- Formation à l'administration.

Chacune de ces tâches s'est vue attribuer une durée estimée en nombre de jours sur la base de 5 heures par jour. En effet, ce projet ne doit pas porter atteinte au fonctionnement du réseau ni à la qualité de service rendu aux utilisateurs de Powerflute. Il est donc raisonnable de conserver 2 heures pour se consacrer aux tâches quotidiennes.

Le détail de ces tâches est disponible sur le diagramme de Gantt (Fig. 28, page suivante)

Figure 28 - Diagramme de Gantt de la phase 1 du projet

1.4) Méthodologie

La mise en place d'un outil de supervision à l'échelle d'un groupe n'est pas réalisable en une seule fois. En effet, le nombre important de sites et l'hétérogénéité des matériels présents dans chacun d'eux impliquent d'utiliser une méthode de configuration incrémentale. Il s'agit donc de trouver une méthode pour organiser et simplifier le travail de configuration de la supervision pour chaque site. Cela suppose un accompagnement de la part du chef de projet qui doit veiller à ce que les futurs utilisateurs se familiarisent avec la solution.

Le site pilote choisi est, bien entendu, celui de Corenso France pour lequel je travaille depuis maintenant 10 ans, et possède donc une très bonne connaissance des éléments constituant le réseau. Le travail sur ce site pilote a pour but d'établir à la fois la configuration initiale de l'outil mais également de dégager une méthode globale qui nous assurera la réussite de la mise en place de la supervision sur les différents sites Powerflute/Corenso.

Il a donc fallu travailler sur la manière de configurer et définir les différents concepts de supervision utilisés par Centreon CES. Cette manière de procéder se veut adaptée au besoin et à l'organisation du SI de Powerflute. Voici les étapes que nous avons suivies lors de l'implémentation de Centreon CES sur un nouveau site :

- Répertorier les services métier concernés par l'utilisation du support informatique ;
- Faire un inventaire des applications nécessaires au fonctionnement du site ;
- Définir les liens entre ces différentes applications. La description fonctionnelle du SI de Corenso France est disponible en Annexe 2 ;
- Effectuer un inventaire des ressources matérielles nécessaires à l'exécution de ces applications et de ces échanges ;
- Déterminer les services qu'il sera intéressant de superviser et ainsi définir les modèles de service et les modèles d'hôtes qui seront utilisés. Ces modèles sont détaillés dans le catalogue des indicateurs en annexe 9 ;
- Définir un niveau de criticité par hôte et service. Pour le site de Corenso France, nous avons simplement repris le travail précédemment effectué sur le PRA (Plan de Reprise d'Activité) qui définit déjà un certain niveau de criticité par application et matériel.

Concernant le classement des hôtes, il faut absolument un administrateur qui connaisse bien la relation existant entre matériels et applications métier et ayant une réelle expérience de la maintenance du site.

Concernant le classement des services, ce sont les administrateurs de la supervision qui définissent le niveau de criticité car nous avons décidé que cet indicateur était en lien avec les fréquences de vérification. En effet, il est inutile de surveiller à trop grande fréquence certains services alors que d'autres nécessitent une surveillance plus accrue. De cette façon, il est possible d'alléger le travail du moteur de supervision et de maîtriser la consommation en ressources du système de supervision.

Le suivi de ces étapes préalables à l'implémentation de la supervision sur chacun des sites est indispensable pour s'assurer de l'efficacité de la supervision dès sa mise en œuvre. Ces informations permettront de vérifier que toutes les sondes nécessaires sont disponibles. Si certaines sont manquantes, elles devront-être paramétrées.

Bien entendu, un suivi est à réaliser durant les premiers jours de fonctionnement de la supervision sur chaque site, ceci afin de s'assurer de la stabilité des collectes et de réajuster les seuils de chaque sonde de façon plus précise. Ce travail a pour objectif de limiter les notifications qui sont également appelées « fantômes » et qui portent préjudice à l'efficacité réelle de la solution de supervision.

Chapitre 2 : Installation de Centreon

Afin de concevoir le système de supervision, il est important de maîtriser ses principaux éléments de configuration. Nous allons maintenant expliquer le fonctionnement de Centreon et comment nous avons effectué son intégration au sein de notre réseau.

2.1) Fonctionnement du logiciel

L'interface de Centreon CES présente 4 principales fonctionnalités :

- L'affichage des données de la supervision ;
- La possibilité d'exporter les informations ;
- Une interface de configuration ;
- L'affichage des tendances ;

Cette interface est hébergée par un serveur Apache grâce auquel il est possible de consulter et de paramétrer les données stockées dans une base de données MySQL. Pour l'entreposage des données de performances, Centreon utilise des bases de données RRD. L'ensemble de ces bases (MySQL et RRD) sont alimentées par Centreon Broker qui est en charge de gérer les événements du système de supervision. Centreon Broker SQL est chargé d'insérer les données de supervision en base de données et de transmettre les données de performance à Centreon Broker RRD. Ce dernier est en charge d'alimenter les fichiers RRD nécessaires à l'affichage des graphiques de tendances et de performances. Les données de supervision proviennent du moteur de la supervision : Centreon Engine.

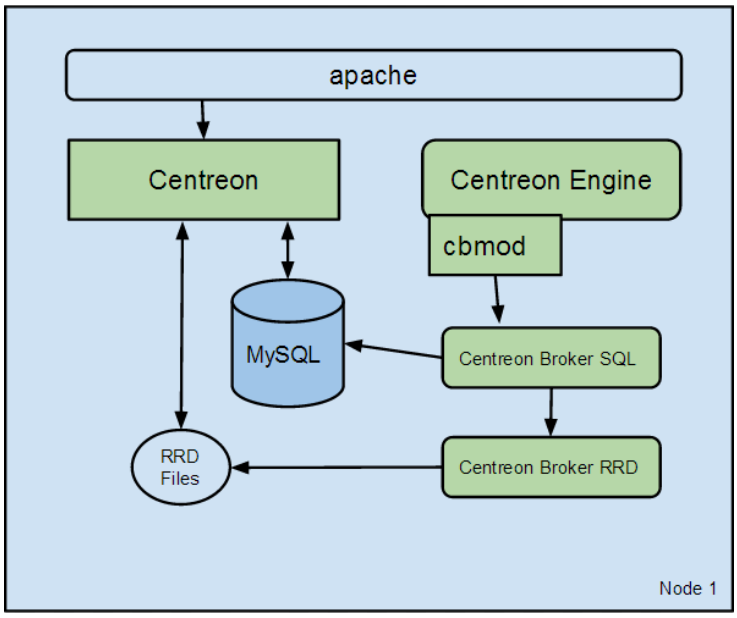


Figure 29 - Eléments de fonctionnement de Centreon, Documentation Centreon CES [En ligne] (Page consultée le 12 février 2017) https://documentation-fr.centreon.com/docs/centreon/en/2.8.x/installation/architecture/03a.html

Centreon Engine et Centreon Broker sont des évolutions du cœur de fonctionnement de NAGIOS. Ce dernier présentait des limites dans ses performances, c'est pourquoi à l'époque la société Merethis a décidé de développer son propre « fork » à NAGIOS. Ce nouveau moteur permet à Centreon CES de gérer plus d'hôtes et services en étant moins consommateur de ressources[1]. Il apporte également la possibilité d'effectuer des modifications de sa configuration à chaud et garantit ainsi une continuité dans la relève des informations, même pendant les opérations de maintenance et de configuration.

Pour effectuer la configuration, Centreon utilise le service CentCore qui est en charge de générer les fichiers de configuration puis de les exporter vers le moteur de supervision Centreon Engine. Centcore génère également les fichiers de configuration pour les serveurs satellites.

[1] Site Internet du Blog Centreon [En ligne] (Page consultée le 04 Février 2017) http://blog.centreon.com/centreon-engine-centreon-broker-benchmarks-techniques-de-performance/?lang=fr

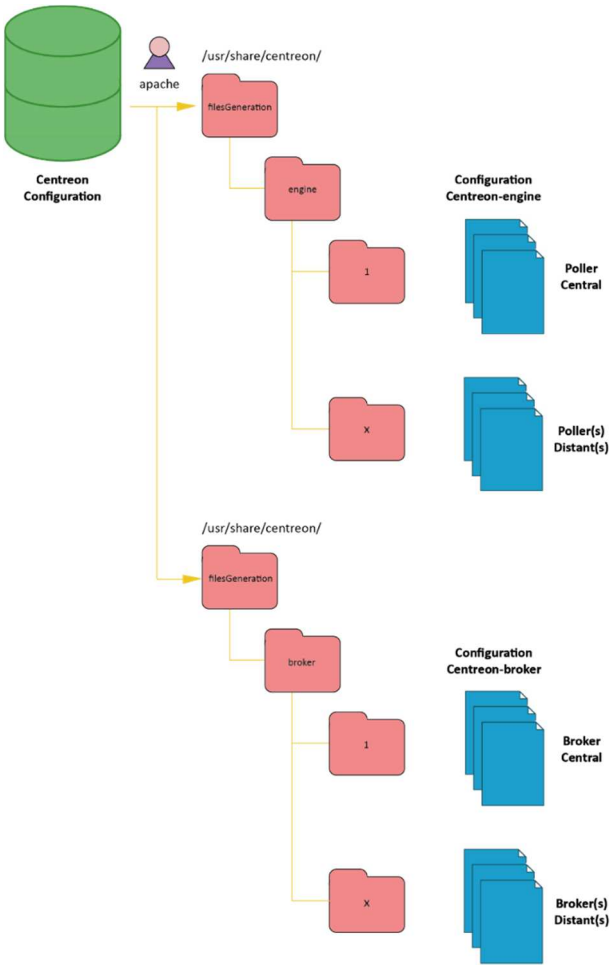


Figure 30 - Emplacement des fichiers de configurations Centreon, Atelier de Kermit [En ligne] (Page consultée le 12 février 2017) http://www.sugarbug.web4me.fr/atelier/techniques/principes/generate_conf/

Centreon Engine est chargé de l'ordonnancement, c'est-à-dire qu'il lance de façon automatisée des sondes qui lui présenteront en retour un résultat qu'il sera apte à interpréter. Ces sondes peuvent-être programmées dans n'importe quel langage de programmation supporté par le système d'exploitation, pourvu qu'elle renvoie un résultat formaté de façon convenable pour être interprété puis transmis au broker par l'intermédiaire de CBMOD. Ce sont ces sondes qui définiront la technologie de supervision utilisée pour récolter l'information sur les nœuds du réseau.

Centreon CES utilise le système d'exploitation CentOS, sur lequel il est possible d'installer les applicatifs nécessaires à l'exécution des sondes. CentOS est un OS libre basé sur la distribution RedHat. Elle est en fait la version libre et optimisée pour les applications serveurs et principalement les serveurs web. Le support de cette solution est communautaire. Elle fait partie des 3 principales distributions Linux utilisées pour l'hébergement de sites internet

(20.5 % en 2017[1]). Le principal intérêt de cet OS provient de l'outil YUM qui facilite l'exploitation et la gestion des paquets au format RPM (RedHat Package Manager). Toutes les dépendances logicielles sont automatiquement calculées par YUM (Yellowdog Updater, Modified), il n'est donc pas nécessaire de vérifier les versions de chaque paquet. Tous les éléments de CES ainsi que les applicatifs nécessaires à l'exécution des sondes peuvent être mis à jour grâce à la commande « yum update » exécutée sur la console du serveur Centreon.

2.2) Architecture choisie

De par la dispersion géographique des sites du groupe Powerflute, notre projet implique une architecture distribuée que supporte Centreon CES. Cette architecture se compose de deux types d'entités, le serveur central et le serveur satellite. La différence principale entre eux est l'absence de base de données et de console graphique sur le serveur satellite.

Le serveur central reste une entité autonome et peut conserver des tâches de collectes comme être configuré sans moteur de supervision. Le serveur satellite dispose du moteur de supervision ainsi que la possibilité de transmettre les informations au broker du serveur central par l'intermédiaire du programme CBMOD.

Sur le serveur central, le service Centcore est chargé d'exporter la configuration des moteurs de supervision vers lui-même ainsi que les serveurs satellites.

Cette architecture offre une meilleure répartition de la charge du travail de supervision entre plusieurs serveurs géographiquement distants ou non l'un de l'autre. L'autre avantage est de pouvoir placer le serveur satellite à un endroit spécifique du réseau afin d'être en mesure de collecter des informations à l'intérieur d'une DMZ (DeMilitarized Zone) par exemple.

La disponibilité de la solution est également importante. En effet toute indisponibilité ou plantage du serveur central implique une perte partielle ou totale de la supervision. Il est donc possible de configurer un serveur central secondaire.

[1] Site Internet W3techs [En ligne] (Page consultée le 15 Février 2017)
https://w3techs.com/technologies/history_details/os-linux

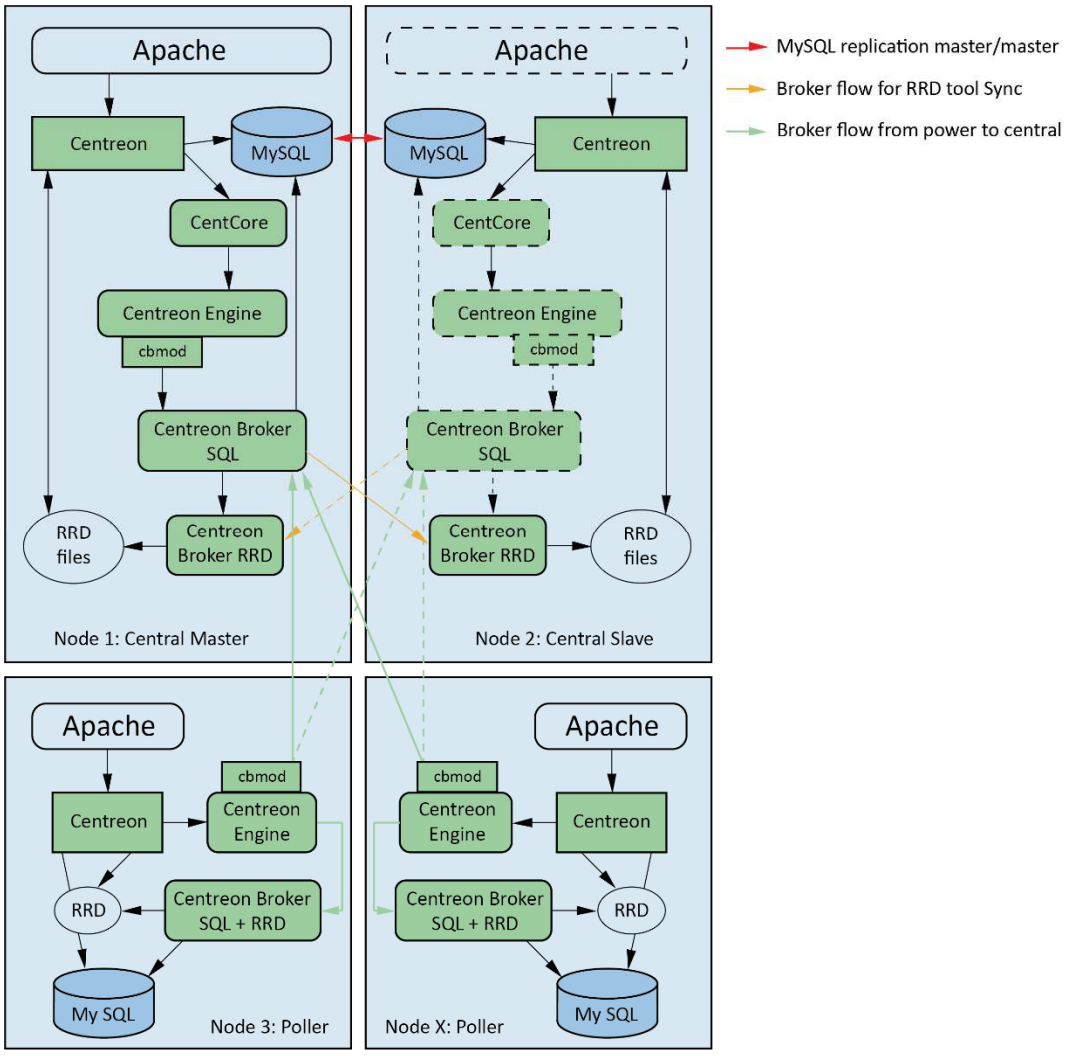


Figure 31 - Architecture Centreon distribuée redondante avec Interface graphique, Documentation Centreon CES [En ligne] (Page consultée le 12 février 2017) https://documentation-fr.centreon.com/docs/centreon/en/2.8.x/installation/architecture/03d.html

Ce serveur central de secours possède l'intégralité des données présentes dans les bases de données du central grâce à une réplication MySQL bidirectionnelle. En cas de panne du serveur central, il suffit donc de démarrer les services Apache, CentCore, Centreon Engine ainsi que Centreon Broker SQL sur le serveur de secours. Pour les serveurs satellites, ce basculement est transparent car ils sont paramétrés pour envoyer les informations de supervision via CBMOD à l'adresse IP virtuelle qui factorise les deux serveurs centraux. En fonction du serveur actif, ces informations sont envoyées à un des deux services Centreon Broker SQL.

Dans la configuration que nous avons choisie, les serveurs satellites disposent de leur propre interface graphique. Cette dernière offre la possibilité de visualiser les données de supervision

du satellite lui-même. Ainsi, même isolé suite à une perte totale de la connectivité aux serveurs centraux, il est possible de garder un accès à l'outil de supervision. Ceci présente un intérêt pour la résolution des incidents majeurs. En effet, il serait préjudiciable de perdre tout accès à cet outil dans ces moments critiques. Cette configuration nous assure également la continuité de la collecte et évite la perte d'informations.

Avec cette architecture distribuée redondante, il est important de s'assurer de la cohérence de la configuration de chaque serveur. Il faut en effet que chaque sonde puisse être exécutée par chacun des serveurs satellites. Pour les sondes ne demandant pas de ressources applicatives supplémentaires, nous avons mis en place une synchronisation (via RSYNC) du dossier les contenant entre le serveur central et les serveurs satellites. Les sondes nécessitant l'installation de composants supplémentaires sur le système doivent faire l'objet d'une installation manuelle sur chacun des serveurs (central ou satellite).

Lorsque la supervision est fonctionnelle, elle exécutera les sondes qui viendront alimenter ses bases de données et s'occupera de la gestion des évènements. Pour cela Centreon utilise les codes de retour des sondes suivants :

Codes pour les hôtes :

Statut	Code de retour	Description
UP	0	L'hôte est disponible et joignable
DOWN	1	L'hôte est indisponible
UNREACHABLE	2	L'hôte est injoignable

Codes pour les services :

Statut	Code de retour	Description
OK	0	Le service ne présente aucun problème
WARNING	1	Le service a dépassé le seuil d'alerte
CRITICAL	2	Le service a dépassé le seuil critique
UNKNOWN	3	Le statut du service ne peut être vérifié

2.3) Implantation réseau et dimensionnement

Nous allons voir dans cette partie comment nous avons intégré les différents serveurs Centreon au cœur du réseau Powerflute.

Powerflute dispose de plusieurs sites éloignés géographiquement mais tous reliés par un réseau VPN de type MPLS. Ainsi, chaque site se retrouve sur le même réseau et dispose d'un réseau privé complet. Pour différencier les sites et effectuer une séparation des différents réseaux, chacun des sites dispose de plusieurs plages d'adresses IP privées. On retrouve donc l'ensemble de ces sous-réseaux sur chaque site du groupe :

- Réseau « Management » ;
- Réseau « Primary » ;
- Réseau « Serveur » ;
- Réseau « Production » ;
- Réseau « ISCSI » ;
- Réseau « Voice » ;
- Les différents réseaux WiFi ;
- Des réseaux de production (automatisme) différents en fonction des sites.

Powerflute dispose de plusieurs Datacenter loués. Les règles de pare-feu autorisent l'ensemble des sites à communiquer sans restriction vers les Datacenters où on retrouve, entre autres, les serveurs de messagerie et les serveurs SAP. Ces mêmes règles permettent donc le positionnement du serveur central Centreon dans le Datacenter principal et le positionnement des satellites sur le réseau « serveurs » de chaque site. La communication entre le central et les satellites se faisant par le biais d'une liaison SSH, les échanges sont cryptés et sécurisés.

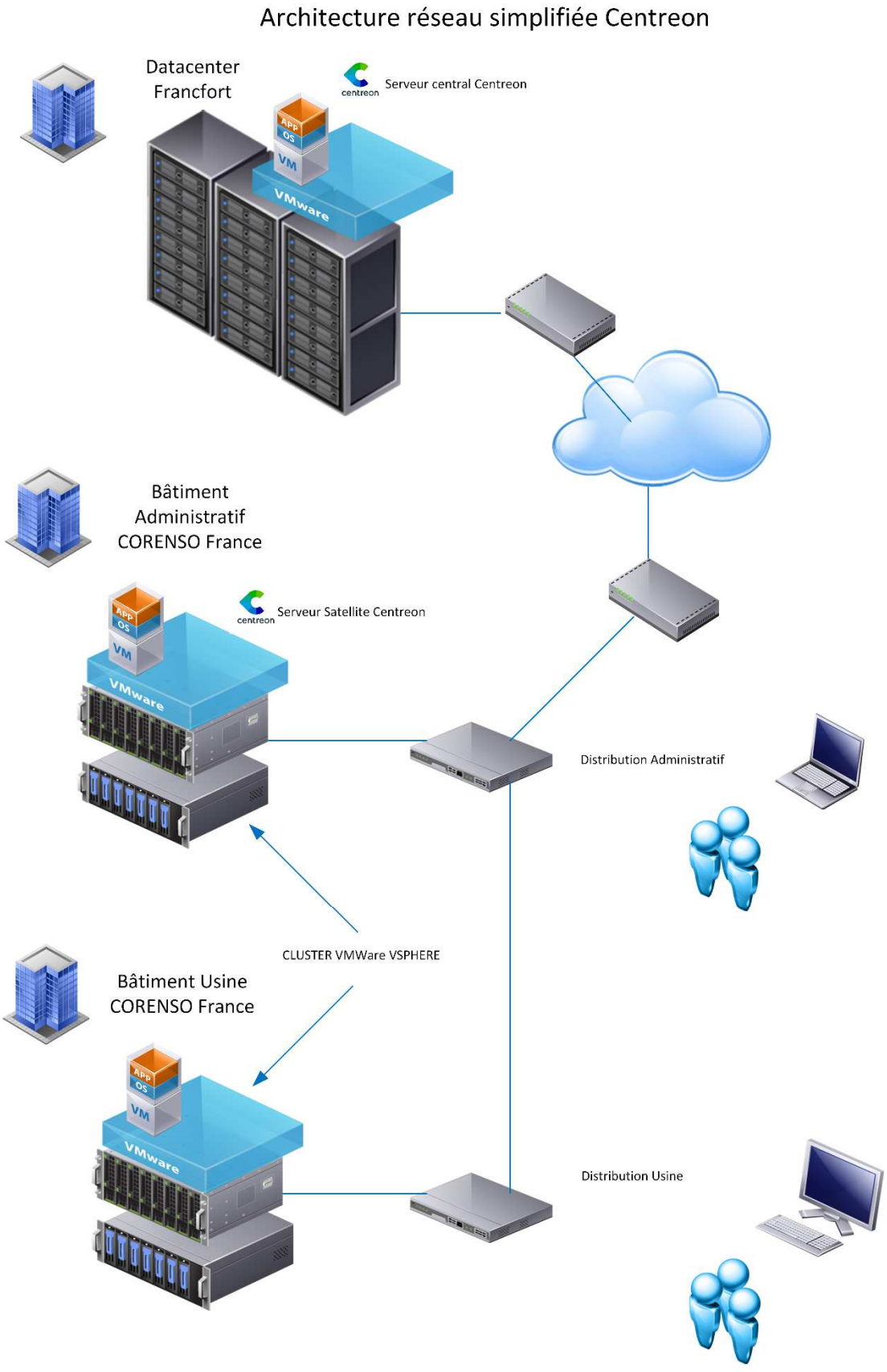


Figure 32 - Architecture réseau simplifiée de Centreon

Certains sous-réseaux peuvent-être protégés et ne peuvent donc pas être atteints depuis le réseau du Datacenter. Dans ce cas, l'utilisation d'un serveur satellite local est indispensable. La communication entre le satellite et les équipements situés sur ces réseaux spécifiques à certains sites (automatisme) peut nécessiter l'ouverture de port sur les pare feu (SSH : 22). Ces configurations sont à étudier en fonction de chaque site et du besoin, ou non, de supervision des éléments situés sur ces réseaux qui sont parfois gérés par des équipes d'exploitation différentes (sous-traitants).

Les sites comprenant un grand nombre de nœuds à superviser (France, Finlande, États-Unis) bénéficient d'un cluster VSPHERE et donc d'une architecture serveur totalement redondante assurant le fonctionnement normal de la supervision, même en cas de destruction totale de la moitié des ressources matérielles. Ces serveurs sont également accompagnés par la solution de sauvegarde Veeam Backup & Réplication qui effectue chaque jour une sauvegarde de chaque machine virtuelle de l'infrastructure et nous garantit donc de pouvoir restaurer ces machines à un état antérieur.

Maintenant que nous savons où placer les différentes entités constituant le système de supervision, voyons quelles ressources sont nécessaires au fonctionnement de celui-ci.

Les recommandations en termes de ressources matérielles sont les suivantes pour Centreon :

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

Figure 33 - Recommandation dimensionnement Centreon, Documentation Centreon CES [En ligne] (Page consultée le 12 février 2017) https://documentation-fr.centreon.com/docs/centreon/en/2.8.x/installation/prerequisites.html

Nombre de services	/var/lib/mysql	/var/lib/centreon
< 500	10 GB	2.5 GB
500 - 2000	42 GB	10 GB
2000 - 10000	210 GB	50 GB
10000 - 20000	420 GB	100 GB
20000 - 50000	1.1 TB	250 GB
50000 - 100000	2,3 TB	1 TB

Figure 34 - Recommandation espace disque Centreon, Documentation Centreon CES [En ligne] (Page consultée le 12 février 2017) https://documentation-fr.centreon.com/docs/centreon/en/2.8.x/installation/prerequisites.html

Nous avons besoin de superviser environ 700 hôtes pour 3 500 services et nous souhaitons pouvoir conserver les données de performances pendant 18 mois. Afin de prendre une marge confortable, nous avons choisi d'attribuer une mémoire vive de 8 GB avec 8 processeurs virtuels et un disque de 250 GB à notre serveur central.

Les serveurs satellites étant des entités autonomes dans l'architecture que nous avons choisie, ils sont par conséquent plus gourmands en ressources. Il faut bien entendu prendre au cas par cas le dimensionnement de chaque serveur satellite. Pour le site de Corenso France, nous avons environ 110 hôtes et 550 services. Nous avons donc dimensionné ce serveur de la façon suivante : 4 processeurs virtuels, 4 GB de mémoire et 80 GB d'espace disque. Cette configuration nous assure une bonne souplesse d'utilisation. Nous essaierons d'aligner la configuration des autres satellites sur celle-ci.

Les serveurs satellites sont positionnés sur les réseaux internes des entités de notre groupe et donc de la responsabilité directe de l'équipe de maintenance Powerflute. Leur installation doit donc, dans la mesure du possible, s'effectuer sur une architecture serveur assurant une certaine redondance. C'est le cas avec l'architecture VMWARE VSPHERE en cluster dont nous disposons sur chaque site ou nous avons positionné nos serveurs satellites.

Afin d'harmoniser au mieux le système de supervision, les administrateurs doivent s'assurer que chaque satellite dispose des mêmes fonctionnalités. Ceci notamment afin de garantir que tous les modèles de supervision paramétrés sont en mesure de fonctionner sur l'ensemble des satellites. Tout au long de la vie du système de supervision, lors de l'ajout de nouveaux

modèles, les responsables de la maintenance de la solution devront donc s'assurer du déploiement correct des nouvelles technologies de supervision sur l'ensemble des serveurs constituant la solution Centreon.

Voici donc comment nous avons installé cette nouvelle application dans notre réseau. Cette implantation, tout comme dans chaque projet de supervision, doit se faire en prenant en compte les spécificités techniques de l'infrastructure globale et des ressources disponibles sur chaque site. Les solutions de virtualisation présentent de nombreux avantages lors de ces implantations et sont des technologies à privilégier. D'autre part les ressources nécessaires à Centreon étant raisonnables au regard des capacités de chaque site, aucun investissement matériel n'est nécessaire.

Implantation des instances Centreon

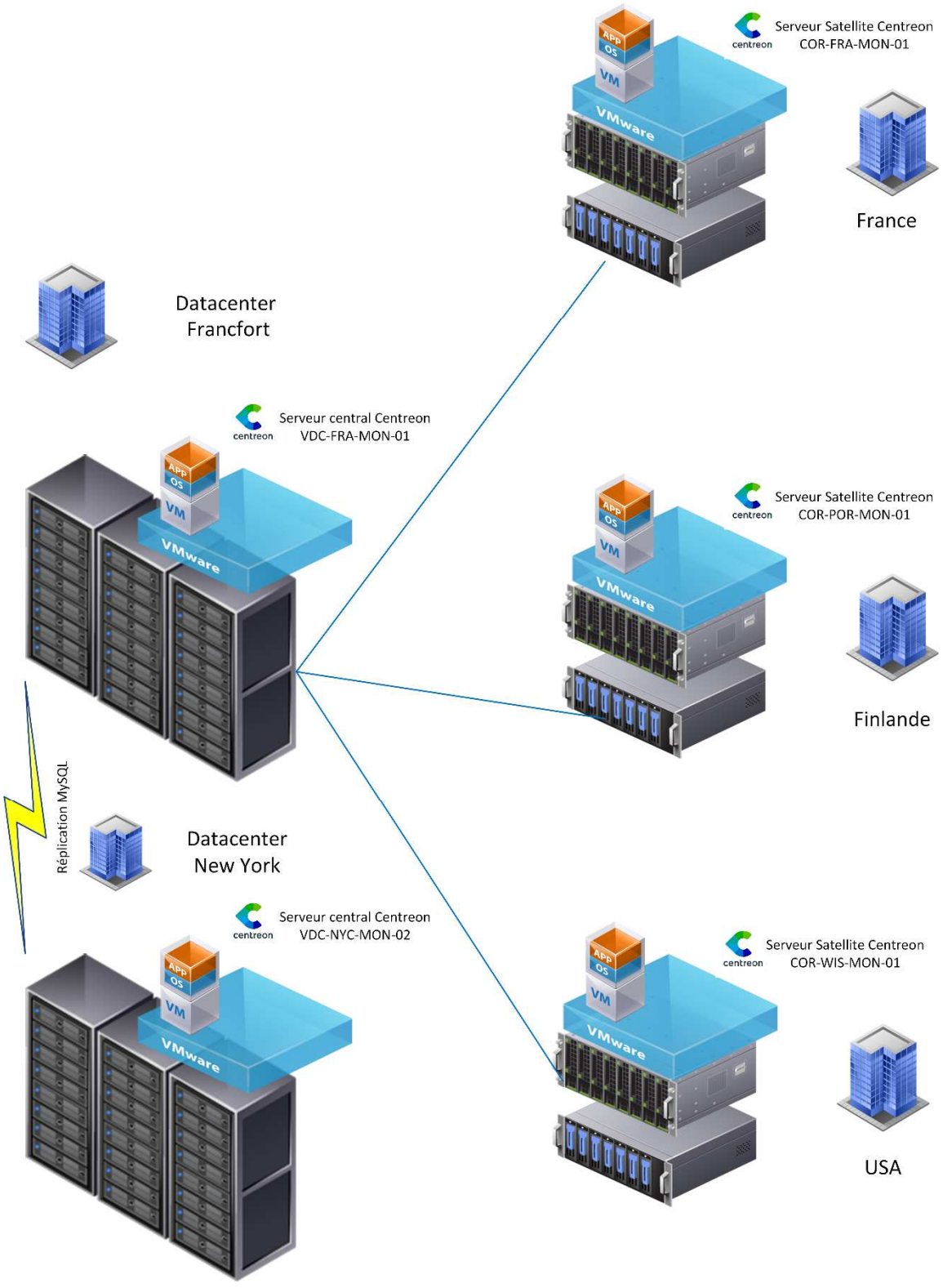


Figure 35 - Implantations des instances de Centreon

2.4) Éléments de configuration

Centreon CES, en plus d'apporter des solutions techniques qui fiabilisent l'infrastructure du système de supervision, permet grâce à son interface graphique ou encore via le module Centreon CLAPI (Centreon Command Line API[1]) de configurer la solution de façon assez souple pour l'adapter au SI de n'importe qu'elle entreprise.

Ceci est rendu possible par l'utilisation des concepts de supervision suivants :

Les hôtes :

Un hôte est une entité possédant une adresse IP et constituant l'une des ressources du système d'information. Il peut donc s'agir d'un serveur, d'un commutateur, d'un routeur, etc.

Les services :

Un service est un point de contrôle qui est rattaché à un hôte. C'est le service qui définit par exemple la vérification de l'espace disque restant sur un serveur Windows.

Les commandes :

La commande définit la ligne de commande nécessaire pour exécuter une sonde. Elle peut comporter des arguments et des variables afin de pouvoir être exécutée sur plusieurs hôtes et avec des paramètres différents.

Les périodes temporelles :

Les périodes temporelles définissent un intervalle de temps pour chaque jour de la semaine et active l'ordonnanceur sur un temps donné.

Les contacts :

Ces sont à la fois les utilisateurs de la plateforme de supervision mais également les personnes recevant les notifications.

[1] Site Internet de la documentation de Centreon [En ligne] (Page consultée le 16 février 2017) https://documentation.centreon.com/docs/centreon-clapi/en/latest/

Les groupes :

Ils regroupent les objets (hôtes, services et contacts) et permettent d'appliquer des filtres sur l'affichage de la console de supervision et de gérer les droits en fonction de groupes d'utilisateurs.

Les catégories :

Les catégories (d'hôtes ou de services), classent les hôtes ou les services différents au sein d'une même catégorie. Les catégories sont aussi le moyen de définir une criticité permettant de traiter les incidents par ordre de priorité.

Les modèles :

Un modèle d'hôtes, de services ou de contacts définit une pré-configuration de l'un de ses objets. L'objectif est ici de faciliter la création d'objets fortement similaires. Il existe une notion d'héritage entre ces modèles.

Grâce à ces principaux concepts de supervision, nous pouvons organiser les différents éléments qui définissent la structure globale du SI. Chacun de ces éléments est défini par un ensemble de paramètres. La bonne maîtrise de ses concepts est donc très importante lors de la phase d'analyse et de configuration. Une partie importante de ce projet a été de trouver une méthodologie adaptée pour rendre cette configuration plus facile tout en gardant une bonne cohérence de l'affichage de l'outil de supervision.

2.5) Les données de performance

Les données de performance sont cruciales dans un outil de supervision réseau. Ces données sont collectées grâce aux sondes et stockées par le serveur central Centreon CES. Il est tout d'abord important de stocker uniquement les données de performance ayant du sens et un réel intérêt pour l'analyse des différents indicateurs du SI.

Lors du processus de sélection de sonde et de paramétrage, il faut donc veiller à ce que la sonde choisie retourne les données de performance souhaitées et de façon cohérente avec les autres sondes pouvant cohabiter pour fournir le même type d'indication. Il faut donc que les unités soient les mêmes.

Les données de performance sont retournées au cœur de Centreon grâce à la ligne de résultat fournie par les sondes. Ces données sont situées après le « pipe » noté « | », sous le format suivant :

'label'=value[UOM];[warn];[crit];[min];[max]

Label = nom de l'indicateur

Value = valeur de l'indicateur

UOM = unité de mesure

Warn = seuil d'alerte WARNING

Crit = seuil d'alerte CRITICAL

Min = valeur minimum

Max = valeur maximum

Il est très important de vérifier les unités de mesure ainsi retournées par les sondes. Certaines sondes retournent énormément de données de performance. C'est, par exemple, le cas de la sonde SNMP Centreon qui relève la consommation CPU. La consommation en pourcentage de chaque cœur logique du serveur est renvoyée, ce qui conduit à la construction de graphiques contenant parfois plus de 16 courbes. Cela ne facilite pas la lecture et est totalement inutile. C'est pourquoi il est donc possible de paramétrer certaines sondes afin de déterminer le format exact et les valeurs qui devront être retournées par le script. Les scripts ne permettant pas d'effectuer cette personnalisation sont à éviter.

Ces données sont ainsi enregistrées dans les bases RRD (Round Robin Database). Ces bases de données, sous forme de fichiers *.rrd* sont conçues avec RRDTool pour faciliter l'affichage de graphiques.

Les sondes sont les éléments du système de supervision les plus à même d'évoluer. En effet, les évolutions matérielles et logicielles peuvent conduire à des changements de technologies, et donc de scripts, pour la collecte des données. La mise en place de nouvelles sondes implique la création de nouveau fichiers *.rrd* et donc à la perte des indicateurs précédents. Cependant, il est possible de manipuler la base de données MySQL de Centreon afin d'assigner manuellement les fichiers RRD à une sonde. Il est donc possible de récupérer les données de performance de l'ancienne sonde et de conserver son historique de relevés. C'est pourquoi il

est très important d'harmoniser les unités de mesures des indicateurs, sans quoi il n'est pas possible d'effectuer cette manipulation.

Nous venons donc de présenter comment fonctionne Centreon, comment nous l'avons configuré et intégré à notre infrastructure. Dans la prochaine partie nous verrons comment nous avons sélectionné les sondes nécessaires pour répondre au besoin de Powerflute.

Chapitre 3 : Choix des sondes

Les sondes sont les éléments centraux de la supervision. Nous allons dans cette partie présenter notre démarche de sélection et les sondes qui étaient nécessaires afin de concevoir un système répondant à notre besoin initial.

3.1) Critères de sélection des sondes

Je me suis attaché à définir et à paramétrer les principales sondes indispensables pour répondre au besoin de supervision du groupe. Je me suis concentré sur la partie infrastructure serveur (supervision de la virtualisation et des serveurs Windows) et infrastructure réseau (supervision matériels Meraki). En effet ces équipements sont présents sur chaque site et grâce à leur supervision, nous pourrons rassembler suffisamment d'informations pour répondre à notre besoin initial de supervision.

Durant la première phase du projet, plusieurs essais ont été effectués afin de trouver les sondes à utiliser. Dans la version open-source de Centreon, on dispose déjà d'un nombre suffisant de sondes pour couvrir une grande partie des attentes. On l'a vu, plusieurs technologies existent et certaines fois, plusieurs technologies sont possibles pour récolter une même information.

Les sondes ou *Plug'ins* sont des programmes qui effectuent des vérifications et retournent les informations à Centreon. Ces programmes sont soit compilés, comme c'est le cas pour beaucoup de sondes Nagios écrites en C, soit interprétés lorsqu'il s'agit de langages de script de type Python, Perl ou Shell. La performance de la solution est particulièrement liée à la qualité de ces programmes. La sonde la plus commune utilise le protocole ICMP (Internet Control Message Protocol) via la commande « PING » pour vérifier les interfaces réseau et en déduire l'état en ligne ou non des éléments supervisés et leur temps de réponse.

De ce fait, il faut privilégier des programmes (sondes) ayant des faibles latences de manière à ne pas encombrer le moteur de supervision. Les intervalles de vérification qui se paramètrent dans Centreon doivent être les plus cohérents possibles. Ils arbitrent entre la précision des données récoltées et la performance induite par l'exécution répétée du programme. Il n'est donc pas toujours facile de faire son choix et pourtant il faut choisir la sonde la plus pertinente

en termes de simplicité, performance, sécurité et résultat. Ce sont ces quatre critères de sélection que j'ai retenus pour ce projet.

Simplicité :

La sonde ne nécessite pas d'installation complémentaire sur le serveur satellite ou sur les éléments supervisés. La sonde dispose d'une bonne documentation et d'un nombre de paramètres suffisant pour répondre au besoin.

Performance :

La sonde est peu gourmande en ressource processeur et réseau, et ne renvoie pas de données de performance (ou de tendances) si ce n'est pas nécessaire.

Sécurité :

Le protocole utilisé par la sonde est sécurisé, aucune information d'identification n'est nécessaire à chaque lancement de la sonde, la sonde ne nécessite pas l'ouverture de port sur les pare-feu.

Résultat :

Le résultat obtenu correspond à celui attendu, l'indicateur est fiable, pertinent et les données de performance sont retournées selon le format attendu et lisibles.

Le début du projet a été consacré à la mise à jour de l'inventaire du réseau de Corenso France et de sa documentation. Nous disposions donc d'un plan détaillé du réseau, de la liste précise du matériel et des différentes applications qu'il supporte. Le serveur Centreon CES de test étant installé et opérationnel, nous devions nous attacher à ce que nous allions véritablement superviser et comment nous allions le faire.

Dans les parties suivantes, nous verrons quelles sondes ont été sélectionnées en fonction des besoins de supervision et des technologies disponibles. Ce travail nous a permis d'établir une première version du catalogue des indicateurs (annexe 9).

3.2) Les serveurs Windows-Linux

Les informations nous intéressant sur les systèmes d'exploitation sont les suivantes :

- Consommation processeur en % ;
- Consommation mémoire en % ;
- Espace disque restant en % ;
- Débit des interfaces réseau en Mbps ;
- Connexion RDP possible.

Il est possible de collecter ces informations grâce à SNMP ou pour Windows, WMI et WS-Management.

SNMP :

Centreon CES nous fournit une sonde prête à l'emploi qui interroge tous les éléments nous intéressant (Centreon-Plugins)[1]. Pour fonctionner, cette sonde nécessite l'installation du service SNMP sur l'hôte Windows ainsi que le paramétrage des communautés et serveurs autorisés à effectuer des requêtes SNMP.

De conception récente, ce nouveau type de script interroge à lui seul un bon nombre d'indicateurs sur la majorité des équipements.

Voici la commande que nous avons paramétrée dans Centreon pour interroger en SNMP les serveurs Windows et Linux :

- *$USER1$/centreon_plugins.pl --plugin=os::'$_SERVICEOS$'::snmp::plugin --mode='$_SERVICEMODE$' --hostname='$HOSTADDRESS$' --snmp-version='$_HOSTSNMPVERSION$' --snmp-community='$_HOSTSNMPCOMMUNITY$' --warning='$_SERVICEWARNING$' --critical='$_SERVICECRITICAL$' --filter-perfdata="$_SERVICEPERFDATAFILTER$" --snmp-timeout=15 --snmp-retries=3*

Cette commande utilise des macros et arguments. Les macros *$_SERVICE* et *$_HOST* correspondent à des variables qui seront définies au niveau du paramétrage de l'hôte et du service. Ici l'argument *$HOSTADDRESS$* correspond à l'adresse IP de l'hôte. Grâce aux arguments et macros, on peut utiliser la même ligne de commande pour superviser plusieurs hôtes avec des paramètres éventuellement différents.

[1] Site Internet du blog de Centreon [En ligne] http://blog.centreon.com/one-plugin-to-rule-them-all-or-not/?lang=fr (Page consultée le 16 mars 2017)

Il est impossible d'utiliser le SNMP dans sa version sécurisée (SNMPv3) sur les systèmes Microsoft Windows. Cependant les données transitant sur le réseau ne sont pas des données importantes et leur cryptage n'est pas nécessaire dans notre cas. Le fait de pouvoir limiter les adresses IP autorisées à effectuer les requêtes offre déjà un niveau suffisant de sécurité. L'installation du service SNMP peut s'effectuer sur plusieurs serveurs Windows simultanément via une simple ligne de commande PS (PowerShell) :

- *Invoke-Command -ComputerName COR-FRA-RDS-05,COR-FRA-RDS-06 -scriptblock {Install-WindowsFeature snmp-service }*

Cette dernière utilise donc la technologie WinRM.

Concernant l'installation et la configuration du SNMP sur les serveurs Linux, il s'agit d'éditer le fichier de configuration de SNMP (snmpd.conf) du système d'exploitation pour lui indiquer la bonne communauté de lecture. Si SNMP n'est pas installé il faut installer le paquet NET-SNMP. Le nombre de serveurs Linux étant très faible sur le réseau de Powerflute, ces manipulations pourront être effectuées au cas par cas.

La configuration du service SNMP sur les serveurs Windows est possible via la création d'une stratégie de groupe. Cette stratégie de groupe paramètre le nom de la communauté et les adresses IP des serveurs autorisés à effectuer une interrogation SNMP sur les serveurs cibles. Ainsi, il est possible de configurer l'intégralité des serveurs d'un site en liant cette stratégie à l'OU (Organizational Unit) de l'annuaire contenant les serveurs. Cette manipulation ne demande que quelques minutes à un administrateur grâce aux consoles d'administration Windows.

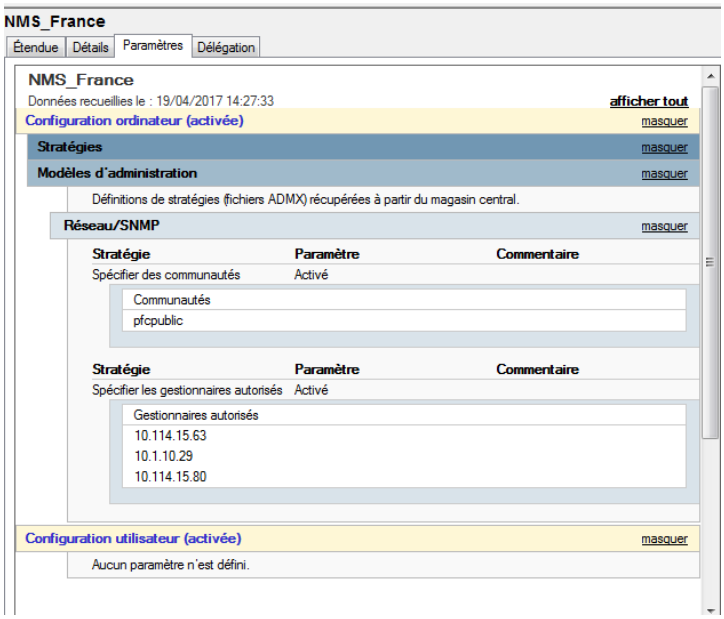


Figure 36 - Stratégie de groupe pour la configuration SNMP Windows

Nous utiliserons plusieurs stratégies de groupe, chacune définissant l'adresse du serveur satellite utilisé pour interroger le site. Nous avons également rajouté l'adresse du serveur central car, en cas de panne d'un collecteur, nous aurons la possibilité de transférer la charge de supervision sur ce dernier. Cette manipulation peut être rapidement effectuée en changeant le serveur de supervision associé à chaque hôte. Il est possible grâce à Centreon CLAPI d'effectuer un changement massif sur plusieurs hôtes à l'aide d'un script. Dans la stratégie de groupe suivante, que nous utilisons en France, nous avons également pensé à rajouter l'adresse du serveur de test.

Vous trouverez en annexe 5 l'état final de visualisation d'un hôte Windows dans Centreon.

Notes à propos du WS-Management :

Nous avons vu dans la partie 2 de ce mémoire que SNMP est déprécié par Microsoft, que le protocole WMI est voué à disparaître et que si l'on souhaite proposer une technologie de supervision actuelle et viable dans le temps, il paraît plus judicieux d'utiliser le WS-Management. WinRM étant une implémentation du WS-Management, il est également possible d'utiliser Centreon Plugin pour effectuer des requêtes WSMan grâce à l'utilisation de « Openwsman » qui est une implémentation open-source du WS-Management.

Cependant, à l'heure actuelle, la documentation de Centreon est encore très vague au sujet de l'utilisation du WSMan. J'ai rencontré plusieurs difficultés pour l'installation de ce dernier sur les serveurs Centreon et le manque de maturité de ces plugins ne permet pas à l'heure actuelle de répondre intégralement à notre besoin. C'est pourquoi nous avons décidé de conserver SNMP pour l'interrogation des systèmes d'exploitation. Lorsque cette technologie sera plus à maturité nous pourrons changer les modèles de supervision pour utiliser ce nouveau standard.

3.3) L'environnement VMWARE

La supervision d'un environnement VMWARE est un peu particulière car nous n'utiliserons pas un protocole standard de la supervision. En effet, si l'on souhaite récupérer des informations détaillées sur l'état de l'architecture VMWARE il est préférable d'utiliser L'API de VMWARE.

Centreon propose pour cela un connecteur, Centreon VMWARE, qui peut être utilisé par le plugin Centreon-Plugin. Centreon VMWARE est en fait un programme PERL chargé de récupérer des indicateurs VMWARE.

Le principe de fonctionnement est le suivant :

- Lorsque l'ordonnanceur souhaite récupérer une information VMWARE, il se connecte au serveur Centreon VMWARE et lui transmet sa demande ;
- Ce dernier peut ensuite, grâce au SDK (Software Developpement Kit) de VMWARE, effectuer un appel à l'instance VMWARE ;
- Le résultat sera retransmis ensuite au client pour être traité dans la supervision.

L'intérêt d'utiliser le serveur Centreon VMWARE est de garder une session ouverte avec le serveur ESX ou le Virtual Center VMWARE. En effet, il est également possible d'utiliser le SDK de VMWARE directement grâce à un plugin tel que Check_VMWARE_API, mais ce dernier ouvre une session à chaque demande de connexion, les logs de connexion se remplissent très rapidement et deviennent illisibles car l'utilisateur de supervision se connecte sans cesse.

Afin d'effectuer des requêtes sur l'environnement VMWARE il convient de paramétrer sur celui-ci un utilisateur ayant des droits en lecture uniquement. Il est possible de récupérer des

informations sur les machines virtuelles, les serveurs ESX ainsi que l'état de l'environnement VSPHERE et de son cluster.

Un environnement VSPHERE peut également envoyer des traps SNMP lors de l'apparition des alarmes. Les traps VSPHERE sont intéressantes car elles remontent un grand nombre d'informations sur l'état global du système.

La supervision active couplée à la supervision passive nous permet de faire remonter assez d'éléments à la supervision pour avoir une idée globale de l'état de santé de l'environnement VMWARE.

Nous avons rencontré des problèmes de stabilité avec Centreon VMWARE. Les sondes ne parvenaient pas à relever les informations souhaitées de façon stable et nous n'avons pas réussi à solutionner le problème. Devant le risque que cela pouvait présenter en termes de temps et de fiabilité de l'information, nous avons finalement décidé d'utiliser le plugin Check_VMWARE_API qui s'est avéré beaucoup plus stable. Nous reprendrons les essais sur le connecteur Centreon VMWARE plus tard.

Vous trouverez en annexe 4 l'affichage ainsi obtenu dans Centreon.

3.4) Les équipements réseaux

Concernant la supervision des éléments d'interconnexion réseau nous avions plusieurs types de matériels à superviser :

- Les commutateurs et routeurs Cisco Meraki ;
- Les commutateurs HP ;
- Les points d'accès WiFi Cisco Meraki.

Les éléments de la marque Cisco Meraki sont interrogeables en SNMP. Il est donc possible de relever les informations souhaitées via des requêtes SNMP. Cisco fournit aussi la MIB Meraki. Depuis l'interface de configuration Meraki, il est également possible de configurer les notifications (traps) SNMP. En version bêta chez Cisco, j'ai demandé l'activation de cette fonctionnalité. Cependant, les notifications sont envoyées depuis le Cloud de Meraki, et donc depuis l'extérieur du réseau. Nous n'avons pas souhaité modifier la configuration des pare-feu pour cela, cette fonctionnalité ne sera donc pas utilisée.

Les informations qui nous intéressent sont l'état de fonctionnement du commutateur ainsi que l'état des liaisons de type « UPLINK ». Sur ces dernières, il est important de récupérer, en plus de l'état, les bandes passantes.

Il n'est pas possible par SNMP de connaître directement la bande passante d'un lien. Cependant il est possible de récupérer un compteur représentant les octets ayant transités par une interface. Ainsi, en effectuant une comparaison entre deux points de mesure, il est possible d'en déduire une bande passante.

Nous avons trouvé plusieurs scripts pour effectuer cette tâche. Le plus pertinent est sans doute celui fourni par la sonde Centreon-Plugins. En effet, cette dernière répond totalement à notre besoin puisqu'elle retourne les données de performance dans un format d'affichage lisible dans Centreon. De plus, cette sonde peut être utilisée pour différents matériels et retournera toujours les données avec le même format

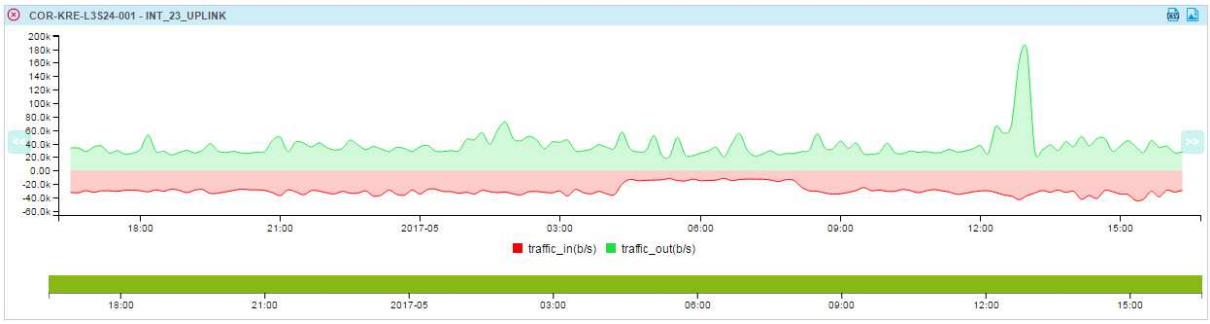


Figure 37 - Exemple de graphique de débit avec la sonde Centreon-Plugins

La visualisation d'un commutateur Meraki dans Centreon est disponible en annexe 6.

3.5) Les serveurs physiques et NAS

Nous nous sommes également posé la question de la supervision des serveurs physiques, c'est-à-dire des serveurs hôtes VMWARE ainsi que des baies de stockage NAS. Le script VMWARE collecte déjà certains éléments comme la santé globale du système et la consommation de ses ressources, ce qui est déjà un bon indicateur mais qui n'est pas suffisant pour connaître avec détail l'état des composants matériels du serveur.

Les serveurs HP disposent d'une interface de gestion appelée ILO qu'il est possible d'interroger en SNMP ou en IPMI. Il est possible d'accéder à ces données en utilisant le script

Centreon-Plugins. Ce dernier utilise l'API XML afin de communiquer avec l'interface ILO des serveurs HP. Il est ainsi possible de relever l'état de l'ensemble des capteurs gérés par le BMC.

L'activation des notifications SNMP est également effectuée afin d'obtenir un message d'erreur détaillé en cas d'apparition d'une panne. En effet, l'ajout dans Centreon des MIBS SNMP associées au serveur HP permet de traduire les notifications et d'afficher un message compréhensible.

Concernant nos serveurs HP, ces étapes de configuration ont été l'occasion de paramétrer correctement les interfaces ILO afin d'effectuer des remontées précises d'alertes par e-mail aux administrateurs locaux. Il était important aussi de configurer correctement les contrats d'assistance (HP Care Pack). En effet les interfaces ILO ont la possibilité de remonter les informations de diagnostic matériel à HP directement. Ainsi, en cas de panne matérielle, HP est directement informé et le support peut procéder à l'envoi d'un technicien sur site avec le matériel nécessaire (on parle de maintenance proactive). Ces serveurs étant d'une importance capitale, l'activation de cette fonctionnalité était indispensable.

La visualisation d'un serveur physique dans Centreon est disponible en annexe 7.

3.6) Vidéosurveillance IP

L'état du réseau de vidéosurveillance IP a son importance sur certains sites, notamment sur le site de Corenso France où la gestion de l'infrastructure de vidéosurveillance est sous la responsabilité du Service Informatique. Il est important de vérifier l'état de fonctionnement des enregistreurs et de chaque caméra.

Chaque caméra doit être disponible sur le réseau, et les enregistreurs doivent être en mesure de se connecter sur le port RTSP (Real Time Streaming Protocol) afin d'enregistrer le flux vidéo. Il est également important de mesurer la bande passante de l'interface Ethernet de chaque caméra afin d'être certain qu'un flux vidéo est bien enregistré par les serveurs d'enregistrement. Cette sonde devra avoir la particularité d'alerter si le débit est trop faible sur l'interface. Il est possible de définir des seuils négatifs lors du paramétrage des seuils « Warning » et « Critical ».

Nous utiliserons donc une sonde de débit (identique à celle utilisée pour les commutateurs) ainsi qu'une sonde vérifiant l'ouverture des ports RTSP et HTTP (HyperText Transfer Protocol).

La surveillance des enregistreurs est effectuée de la même manière que les serveurs Windows, c'est-à-dire en utilisant SNMP. Le système d'enregistrement actuel de marque D-LINK ne propose malheureusement pas de fonctionnalité de supervision permettant à Centreon de vérifier avec détail le fonctionnement de l'enregistrement de chaque caméra.

3.7) Les salles informatiques et électriques

Les salles informatiques sont toutes dotées d'une climatisation qu'il est important de vérifier. Les sondes internes des serveurs peuvent déjà nous alerter sur un dysfonctionnement éventuel du système de climatisation mais il est également possible d'installer des sondes de température autonome.

La société AKCP[1] fourni une variété de sondes interrogeables en SNMP. Nous pouvons donc effectuer un suivi de la température ou de l'humidité d'une salle. Ces sondes sont installées dans les salles informatiques et les locaux électriques. Elles contrôlent l'état de fonctionnement des climatisations présentes dans ces locaux. Dans le milieu industriel une surchauffe de certains équipements de commande, notamment des variateurs de vitesse, peut avoir des conséquences considérables sur l'activité de production. Être capable de déceler au plus vite cette surchauffe est un service supplémentaire que nous pouvons offrir aux équipes de maintenance électrique.

Figure 38 - Sonde température AKCP SensorProbe 2

[1] Site Internet AKCP [En ligne] (Page consultée le 04 mai 2017) http://www.akcp.com/

3.8) Les automates industriels

L'automatisation fait également partie des éléments importants à surveiller, particulièrement sur le site de Corenso France. Depuis plusieurs années déjà, les automates industriels sont tous équipés d'interfaces Ethernet utilisées pour leur programmation à distance, ou encore pour échanger des informations avec les automates voisins. Il faut donc superviser le fonctionnement du réseau des automates.

Il est possible de vérifier la présence d'un élément grâce à une requête ICMP. Cependant, les automates actuellement en fonctionnement dans l'usine de Corenso France ne supportent pas de technologie de supervision particulière. Impossible donc de relever les informations comme l'occupation mémoire et processeur des automates industriels.

Il est possible d'effectuer des interrogations MODBUS/TCP et ainsi de relever des informations spécifiques dans la mémoire de l'automate. Cependant la supervision des procédés industriels n'est pas le sujet de ce projet.

Chapitre 4 : Conception de Centreon CES pour Powerflute

Nous venons de voir le fonctionnement des sondes. Il est maintenant très important d'exploiter les données de ces sondes de façon correcte et adaptée à notre environnement. Nous allons dans ce chapitre détailler les modalités de représentation du SI avec Centreon.

4.1) Définitions des modèles

Afin de faciliter la configuration de la supervision, Centreon utilise le concept des modèles d'hôtes et de services.

4.1.1) Les modèles d'hôtes

Les modèles d'hôtes sont des objets de supervision qui possèdent toutes les caractéristiques définissant un hôte et pouvant être utilisés comme base pour la configuration d'un nouvel hôte. C'est donc un objet préconfiguré qui sera utilisé pour insérer de nouveaux éléments plus rapidement. Ils uniformisent le paramétrage en s'assurant que chaque hôte respecte bien le format et les paramètres définis dans le modèle.

Un hôte peut donc hériter d'un modèle d'hôte et un modèle d'hôte d'un autre modèle d'hôte. Les paramètres hérités peuvent être surchargés (modifiés) par l'hôte.

Ainsi, il convient de découper son système d'information en différentes couches pour définir les modèles et ainsi gagner du temps lors de la configuration.

La liste des modèles d'hôtes est disponible dans le catalogue des indicateurs en annexe 9**.**

Ces modèles seront amenés à évoluer au fil de l'implémentation de la supervision sur les différents sites du groupe.

4.1.2) Les modèles de services

Les modèles de services sont des objets de supervision qui possèdent toutes les caractéristiques d'un service et peuvent être utilisés comme base pour la configuration d'un autre service. Un modèle de service peut hériter d'un seul autre modèle de service. Au niveau

de la configuration du service, il est possible de surcharger les paramètres hérités afin de personnaliser certains réglages.

Nous avons décidé de mettre en place plusieurs modèles de base pour le paramétrage des informations les plus communes à l'ensemble des services tels que :

- Intervalle d'exécution de la sonde ;
- Intervalles de notification ;
- Criticité de l'élément.

Ces modèles de base nous assurent qu'un ensemble de paramètres obligatoires est bien lié à chacun des services ajoutés.

Nous avons ensuite conçu les modèles de services spécifiques aux sondes que nous avions choisies. En fonction de la sonde, nous avons lié un des modèles de base précédents.

Les modèles de services peuvent être rattachés à un ou plusieurs modèles d'hôtes. Lors de la création d'un nouvel hôte (une nouvelle machine virtuelle à superviser par exemple), il suffit ainsi de connaître le modèle d'hôte principal pour paramétrer automatiquement l'ensemble des sondes rattachées à celui-ci. Cela facilite grandement le travail d'administration de la solution.

4.2) Gestion des notifications et escalades

Centreon gère également les escalades de notifications. Ce mécanisme alerte les différents membres de l'équipe informatique en fonction du nombre de notifications envoyées. Si un problème n'est pas acquitté au bout d'un certain temps, c'est un autre technicien qui recevra la notification.

Nous paramètrerons avec précision ces règles d'escalade au fur et à mesure du déploiement de la solution mais nous avons déjà sélectionné cette règle d'escalade :

- Au bout de 2 notifications, l'alerte est envoyée à un autre technicien ;
- Au bout de 4 notifications un ticket est créé dans le système de gestion des incidents ;

Ainsi tous les membres de l'équipe sont informés du problème.

Pour paramétrer ces règles, nous utilisons les groupes de contact et les groupes d'hôtes. Dans le cadre de ce projet nous avons décidé de mettre en place des notifications par e-mail sur tous les sites du groupe. Afin de permettre au serveur Centreon d'envoyer des e-mails aux techniciens sur leur messagerie professionnelle, il faut paramétrer le serveur *Postfix*. En effet, pour l'envoi des e-mails, il faut absolument utiliser la passerelle SMTP du groupe. Une fois *Postfix* paramétré et redémarré, il est possible d'utiliser les commandes de notification par mail définies par Centreon. Ce paramétrage doit s'effectuer sur le serveur central ainsi que sur les serveurs satellites car ces derniers sont en charge de l'exécution de la commande de notification.

Sur le site de Corenso France, nous disposons déjà d'une passerelle SMS de type FOXBOX[1]. Elle était utilisée par l'ancien système de supervision NAGIOS ainsi que par d'autres applications internes. Nous avons donc choisi de l'utiliser pour réaliser l'envoi des SMS de façon locale. En France, le coût de l'abonnement est de 14€ par mois pour un envoi illimité de SMS, et l'achat de la passerelle est de 400€. Le paramétrage de cette FOXBOX est simple et rapide, une fois les adresses réseaux paramétrées et la carte SIM déverrouillée. Il suffit d'utiliser le script et l'API fournis pour que Centreon soit capable d'envoyer des SMS.

4.3) Création des groupes d'objets

Les groupes d'objets réunissent les différents objets de configuration dans l'interface de Centreon. Leur utilisation est indispensable afin d'harmoniser la configuration de l'outil, surtout lorsqu'il est destiné à être utilisé sur plusieurs lieux géographiques et par plusieurs utilisateurs. Nous allons expliquer l'utilité des groupes d'objets, et l'utilisation que nous en avons faite pour notre projet.

4.3.1) Les groupes d'hôtes et de services

Le principal intérêt des groupes d'hôtes et de services est de filtrer les affichages de Centreon. Ils offrent ainsi la possibilité d'obtenir des taux de disponibilité par groupe d'hôtes. Les

[1] Site Internet SMSFoxBox [En ligne] (Page consultée le 5 mai 2017) https://www.smsfoxbox.it/en/foxbox-mini.html/

groupes d'hôtes sont également utiles pour le paramétrage des escalades car ils appliquent l'escalade sur un ensemble d'hôtes.

Lors de la première phase du projet, l'inventorisation du réseau et des applications nous a permis de dégager plusieurs types de groupes d'hôtes :

- Les groupes définissant les sites (ex : COR-FRA-SITES) ;
- Les groupes définissant le type d'équipement (ex : FIREWALL-DEV) ;
- Les groupes définissant le réseau sur lequel l'équipement est connecté (ex : PROD-NET) ;
- Les groupes définissant les applications supportées par les hôtes (AUTOMATION-APP) ;
- Le groupe définissant les services métier concernés (PRODUCTION-DPT).

Ainsi, lors de l'ajout d'un nouvel élément, voici les questions qu'il faut se poser :

- Sur quel site est l'équipement ?
- Quel est l'équipement ?
- Sur quel(s) réseau(x) est-il connecté ?
- Quel(les) application(s) supporte-t-il ?
- Quel(s) service(s) métier utilise(nt) l'application ?

Cette méthodologie de questionnement est à utiliser pour chaque hôte lors de l'implémentation d'un nouveau site dans la supervision. Elle permet de filtrer les informations mais également de mieux comprendre l'impact qu'une indisponibilité de l'hôte peut avoir sur les utilisateurs. En effet, dans l'interface de Centreon, il suffit maintenant de regarder la liste de groupes d'hôtes pour répondre à ces questions.

Les groupes de services regroupent les services pour éditer des rapports de performance par type d'application (base de données, applications métier, etc.). Ils offrent la possibilité d'agréger des services utilisant des ressources différentes. Nous avons effectué des essais sur l'application de gestion des matières premières (VIP) au niveau du site de Corenso France. Cette application nécessite que le serveur web et la base de données soient disponibles sur le serveur Windows de VIP. Les rapports sont édités grâce à un serveur Crystal Report situé sur le serveur Intranet. Afin d'avoir une vision de l'ensemble du fonctionnement de cette

application indispensable à la logistique, nous avons créé un groupe de service nommé « VIP » auquel nous avons lié les services suivants :

- Serveur Apache serveur VIP ;
- Serveur Mysql sur Serveur VIP ;
- Service Crystal report sur serveur Intranet ;
- Serveur Apache sur serveur Intranet ;
- PING sur les deux serveurs.

On pourra donc, une fois la supervision pleinement déployée, implémenter des groupes de services en fonction du besoin de chaque site, ou au niveau des applications partagées par certains d'entre eux.

4.3.2) Groupes de contacts et d'utilisateurs

Le paramétrage des utilisateurs et des ACL (Access Control List) doit se faire de manière à refléter au mieux l'organisation de notre SI. Elles sont complexes à définir et méritent une certaine attention, notamment pour les accès aux menus et actions. Il faut donc commencer par définir les comportements et les profils des utilisateurs.

La supervision sera utilisée par l'ensemble de l'équipe Informatique. Les administrateurs étant susceptibles d'intervenir sur la majorité des sites, la visualisation de la supervision devra leur être possible sur tous les sites. L'accès à l'administration sera réservé à un petit nombre d'utilisateurs maîtrisant la configuration de Centreon.

Dans Centreon, les contacts définissent les utilisateurs de la supervision. Dans notre cas de figure, il s'agira de l'ensemble des administrateurs réseau du groupe (superviseurs et administrateurs).

Il est possible d'utiliser des modèles de contacts afin d'obtenir une trame de paramétrage commune pour l'ensemble des utilisateurs. Nous avons défini 2 modèles de contacts : « Internal_Mail » et « Internal_SMS ». Ces modèles définissent les commandes et les intervalles de notification par défaut.

Il est également possible de définir des groupes de contacts qui ont pour objectif de faciliter le paramétrage de la notification et des escalades de notification. Dans notre paramétrage, il

existe un groupe de contacts par site supervisé pour effectuer la notification ciblée des administrateurs. Grâce à cela nous pouvons assigner un administrateur à un groupe pour lui assurer de recevoir les notifications relatives à un site.

On peut donc identifier nos utilisateurs et les assigner à certains sites. Pour autoriser, à certains utilisateurs, l'accès ou non à certaines fonctionnalités de la solution de supervision, on peut définir les ACL de manière à spécifier :

- L'accès aux menus ;
- L'accès aux ressources (elles nous servent principalement pour déterminer qui a accès à quel site) ;
- L'accès aux actions (fonctionnalités de Centreon).

Ici, nous avons 2 profils : Administrateur et Superviseur. Deux listes d'accès ont donc été créées pour différencier les accès de ces profils.

La gestion des droits d'accès a une importance capitale dans la vie du logiciel de supervision. En effet, il est important que les techniciens n'aient qu'un accès limité et ne puissent pas administrer eux même la solution. La configuration intégrale de l'outil doit être réservée à l'équipe de supervision qui maîtrise les concepts, les paramètres, et qui doit, grâce à une gestion rigoureuse et méthodique, assurer le fonctionnement correct de l'outil.

Les superviseurs souhaitant effectuer des mises à jour doivent en faire la demande via le système de gestion des tickets Powerflute. L'équipe de supervision sera ainsi prévenue et effectuera la mise à jour en respectant les règles et les procédures que nous avons définies durant ce projet.

4.4) La gestion des dépendances

Lorsqu'une panne intervient sur un équipement, il est probable que cette panne ait une incidence sur le fonctionnement d'autres éléments supervisés. Cela peut entraîner la réception par les administrateurs de plusieurs notifications simultanées, ce qui aura pour effet de les désorienter dans leur analyse de panne.

Afin de limiter l'envoi des notifications et de cibler les alertes, il est possible de paramétrer des liens de dépendance entre les éléments supervisés. Centreon définit deux types de dépendances, les dépendances physiques et logiques.

Les dépendances physiques prennent en compte les liens physiques reliant les éléments de l'infrastructure réseau. Ce type de lien ne peut être défini qu'entre les hôtes. Chaque hôte possède donc des relations de parenté avec les hôtes environnants. Si les hôtes parents d'un hôte deviennent injoignables, alors l'ordonnanceur considèrera cet hôte comme injoignable.

Les dépendances logiques définissent les liens entre les hôtes ou les services dépendant les uns des autres pour l'exécution d'une application. Le paramétrage de ces dépendances désactive l'exécution de certaines sondes et/ou l'envoi des notifications.

Le paramétrage des dépendances physiques est relativement simple puisqu'il suffit d'observer les liens physiques entre les éléments. Le paramétrage des liens logiques demande un peu plus de réflexion sur le fonctionnement des applications.

Dans le cadre de notre projet, nous avons choisi de nous concentrer avant tout sur les dépendances physiques. Les dépendances logiques seront paramétrées au cas par cas et au fur et à mesure du déploiement sur chacun des sites.

4.5) Les sondes passives

Le paramétrage des sondes passives dans Centreon permet d'afficher de façon lisible dans l'interface de supervision les notifications SNMP émises par certains équipements. La réception d'une notification SNMP dans Centreon fait intervenir plusieurs mécanismes.

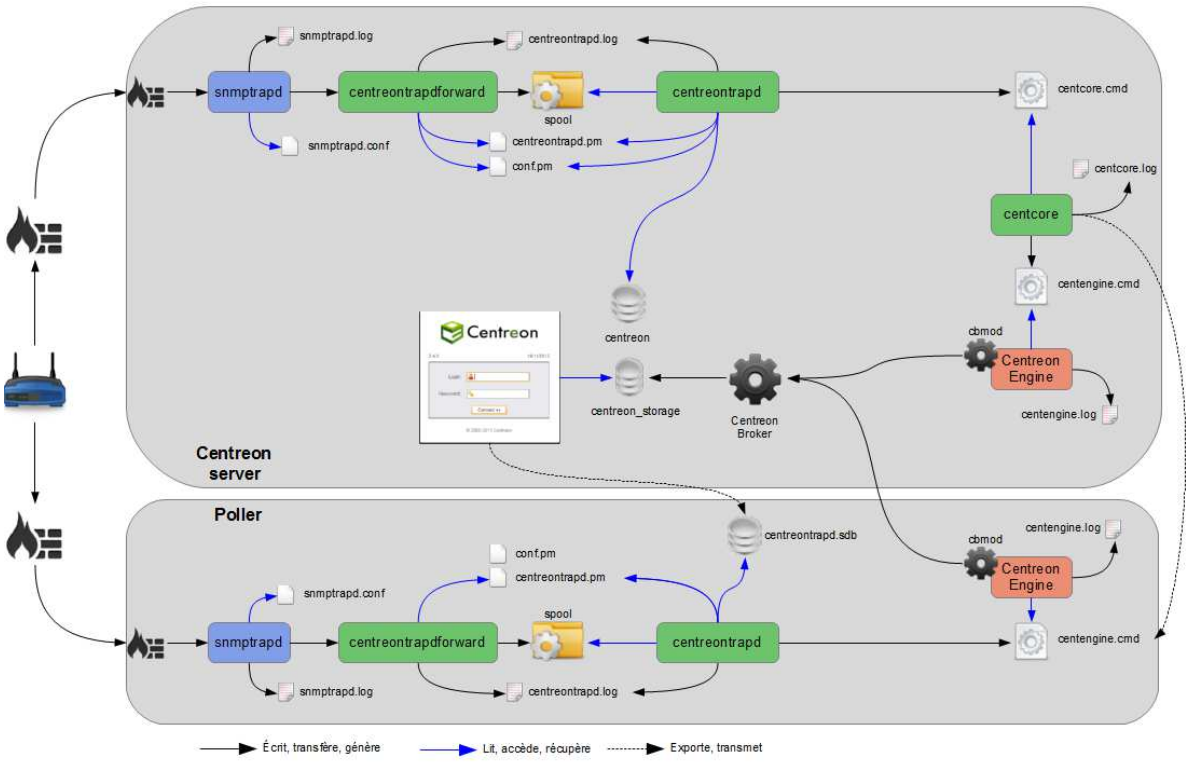


Figure 39 - Mécanismes de fonctionnement des notifications SNMP avec Centreon

Lorsqu'une trap est réceptionnée sur le port UDP 162 d'un satellite Centreon, elle est dans un premier temps lue par le processus « snmptrapd » (voir figure 39). Ce processus doit-être configuré de manière à transmettre ce message à « centreontrapdforward » qui enregistre les informations contenues dans la notification SNMP dans un fichier provisoire (/var/spool/centreontrapd/).

Le processus qui vient lire les nouveaux fichiers présents dans le répertoire « SPOOL » est « Centreontrapd ». Ce processus possède une connexion à la base de données des notifications SNMP générées par Centreon grâce à l'import des différents fichiers MIB spécifiques aux constructeurs. Après avoir vérifié que la notification provenait bien d'un équipement paramétré dans Centreon, grâce à l'adresse IP de l'émetteur de la notification, il traduit l'OID reçu à l'aide de la base de données « centreontrapd.sdb » puis l'envoie au moteur de Centreon pour actualiser le statut de l'équipement et afficher le message de façon lisible.

Après l'import des fichiers MIB, Centreon conserve les différents OID correspondant aux équipements émetteurs dans une base de données. Sur les serveurs satellites, cette base de données est générée et transmise par le serveur central lorsque l'on applique la configuration du satellite depuis l'interface principale de configuration. Sans cela, les informations ne seraient pas lisibles dans l'interface de Centreon.

Cette base contient donc la traduction de l'OID de chaque notification SNMP et le statut correspondant au message. L'import des MIB dans Centreon assigne un statut en fonction des informations contenues dans la MIB, mais cela peut réserver des surprises. Il est important de vérifier après import les statuts assignés à chaque notification depuis l'interface de Centreon. En effet, si une notification se voit assigner un statut « OK » alors qu'il devrait être « CRITICAL », la supervision ne notifiera pas les utilisateurs. Certains constructeurs fournissent des MIB contenant des centaines d'OID, il est possible d'effectuer des changements en masse en se connectant directement à la base de données MySQL de Centreon.

Dans certains cas, il peut être utile d'enrichir le message de sortie avec des informations complémentaires. Il est possible de paramétrer un contrôle actif suite à la réception d'une trap, ceci grâce aux commandes « PREEXEC ». Le résultat de ces commandes est utilisable sous forme de variables à insérer dans le message de sortie de la sonde passive.

Certains constructeurs offrent la possibilité de renvoyer, via un OID unique et un ensemble de variables, un nombre important de messages différents. Les arguments contenus dans la notification peuvent alors avoir des sens différents et concerner une simple information comme une alerte critique. Il faut donc veiller à observer les messages pouvant être reçus et utiliser les filtres de Centreon pour leur assigner un statut critique ou non. Il est possible pour cela d'utiliser les expressions régulières afin d'analyser le contenu de l'argument et d'en déduire un statut, plutôt que d'utiliser la définition de statut général de la trap en question.

Pour vérifier la fraîcheur de l'information reçue dans Centreon, on peut contrôler le temps depuis lequel aucune trap SNMP n'a été réceptionnée et exécuter une commande qui viendra mettre à jour le statut du service. Dans certains cas, on considèrera que nous sommes dans un état normal car c'est une information (cas d'une sonde contrôlant l'état d'un matériel et ne renvoyant un message qu'en cas d'erreur). Dans d'autre cas, nous pouvons nous retrouver

en situation d'alerte. Grâce à cela, on peut être alerté d'un éventuel mauvais fonctionnement par manque de trap.

Le paramétrage de la réception des traps SNMP suit ces étapes :

1. Recherche des MIBS de l'équipement et import dans Centreon ;
2. Vérification des statuts dans la base de Centreon ;
3. Paramétrage de l'hôte dans Centreon ;
4. Ajout d'un service grâce au modèle de service ;
5. Sélection des messages (OIDs) pouvant être reçus sur le service ;
6. Essais de réception des traps ;
7. Ajustement des statuts et/ou des filtres.

Grâce aux traps SNMP on peut, avec un seul service, s'assurer de contrôler un grand nombre d'éléments et ainsi d'être alerté de la moindre situation anormale. Il ne faut pas oublier qu'il s'agit d'un service passif et que si un problème technique empêche la réception des traps, l'équipe technique ne sera pas avertie. Il faut donc s'assurer de paramétrer un ou plusieurs services actifs exécutant des sondes SNMP ou autre qui donnent un résultat général sur la santé de l'équipement. Il faut parfois pour cela prendre du temps pour analyser les MIBs constructeurs.

4.6) Gestion des niveaux de risques

ITIL[1] indique que la priorité des incidents doit être déterminée par l'impact qu'ils représentent sur l'activité métier et sur l'urgence à trouver une solution. Les indicateurs de criticité de Centreon définissent cette priorité d'action au niveau des catégories d'hôtes et de services.

Concernant les services, nous avons choisi d'effectuer ce paramétrage au niveau des modèles génériques. En effet, le niveau de risque étant également lié à la fréquence de vérification, cela nous a permis de s'assurer que chaque service créé à partir d'un modèle soit lié à un

[1] Site Internet ITIL France [En ligne] (Page consultée le 16 Février 2017) http://www.itilfrance.com/pages/docs/hgelun/itilv2_incidents.pdf

niveau de service. Si le niveau de service paramétré dans le modèle ne convient pas, il est toujours possible de le surcharger dans les paramètres du service directement.

Concernant le paramétrage sur les hôtes, c'est au technicien local de définir ces priorités car il connaît bien la relation qui existe entre l'activité métier et les différents éléments du réseau.

De manière à uniformiser les règles de priorité, nous avons repris les paramètres de notre outil ITSM qui définit les paramètres de criticité comme suit :

- Haute importance : arrêt des lignes de production/les utilisateurs ne peuvent plus travailler. L'intervention doit avoir lieu dans l'heure ;
- Moyenne importance : dégradation d'un service n'empêchant pas la production mais ne permettant pas aux usagers d'effectuer toutes leurs tâches de façon normale. L'intervention doit avoir lieu dans les 6 heures ;
- Basse importance : dégradation de service n'impactant pas directement les usagers mais pouvant à long terme créer un problème plus important. L'intervention doit avoir lieu dans les 48h.

4.7) Méthode d'import avec Centreon CLAPI

Centreon CLAPI est en fait une API de paramétrage pour Centreon. Les administrateurs de la supervision peuvent l'utiliser à la place de l'interface Web habituelle pour effectuer les tâches de paramétrages suivantes :

- Ajout/Suppression/Mise à jour des objets de configuration (hôtes, services, groupes etc.) ;
- Générer les fichiers de configuration ;
- Copier la configuration sur les serveurs satellites ;
- Redémarrer un serveur satellite ;
- Importer et exporter des objets.

Cet outil est d'une grande utilité et nous a permis de gagner énormément de temps sur ce projet, en nous permettant d'automatiser la configuration de Centreon grâce aux fichiers CSV de configuration que nous avons produits. Grâce à cette méthode on s'assure également de limiter les erreurs de saisie.

J'ai donc créé un script shell qui lit un fichier sous format .csv et exécute pour chaque ligne du fichier la commande CLAPI correspondante. Ces fichiers sont et seront remplis par les administrateurs de chaque site car ils centralisent toutes les informations collectées sur le réseau. Ce fichier CSV (disponible en annexe 10) contient la liste des hôtes du réseau et, pour chacun d'entre eux, un certain nombre de paramètres :

- Le nom de l'hôte ;
- L'adresse IP de l'hôte ;
- Sa description ;
- Les modèles d'hôtes à appliquer ;
- Les groupes d'hôtes auquel il appartient ;
- Le ou les hôtes parents et enfants ;
- Le niveau de criticité de l'hôte.

Ce script exécute dans un premier temps l'import des hôtes, puis effectue ensuite la liaison de parenté et assigne un niveau de criticité.

Grâce à l'outil Centreon CLAPI et aux modèles d'hôtes et de service, on peut ainsi importer la configuration dans Centreon très rapidement à condition que l'ensemble des modèles souhaités existent dans Centreon. Les administrateurs de la supervision peuvent donc concentrer leurs efforts sur le remplissage de ce fichier Excel et non pas sur le paramétrage de Centreon lui-même.

Vous trouverez en annexe 8 une capture d'écran de l'interface principale de Centreon obtenu suite à la configuration de ce dernier.

Chapitre 5 : Vie du projet

Lors de ce projet, je me suis très rapidement aperçu que le déploiement d'un système de supervision impliquait de suivre une méthodologie et des processus précis. Ceci afin de garantir une certaine harmonisation au niveau de la configuration malgré les besoins différents de chacun des sites de notre groupe. En effet, cela nécessite une certaine rigueur dans la gestion de la configuration initiale mais également lors des différentes évolutions de configuration qui interviendront tout au long de la vie de Centreon. Aussi, nous verrons que l'organisation même du service informatique ayant en charge la prise en compte des notifications du système de supervision, a une importance sur l'efficacité future de la solution.

5.1) Organisation du déploiement

La mise en service de la solution de supervision sur les différents sites nécessite une méthodologie adaptée. Lorsque j'ai déployé la solution pour le réseau de Corenso France, j'ai essayé de définir une méthodologie qui soit facile et rapide à mettre en œuvre. En effet, il est important, sur ce projet, de mettre à contribution les administrateurs locaux afin qu'ils saisissent bien les enjeux de ce nouvel outil de supervision. Cependant, la mise en service de l'outil ne doit pas leur demander trop d'efforts ni de temps.

C'est pourquoi j'ai décidé de guider au mieux leur travail en leur demandant de remplir un seul fichier Excel, dans lequel seules quelques colonnes doivent-être remplies, pour me permettre de configurer Centreon grâce à l'utilitaire Centreon CLAPI et au script d'import présenté au chapitre précédent.

En fin de première phase du projet, j'ai donc organisé une réunion d'information avec tous les administrateurs réseaux du groupe Powerflute. Cette réunion avait pour objectif de présenter la manière dont nous avions pensé la configuration de Centreon et son fonctionnement. La fin de cette présentation a été l'occasion d'expliquer aux agents de l'équipe « Infrastructure » ce qui était attendu d'eux, et notamment la saisie des éléments de configuration dans le fichier CSV destiné à être importé dans Centreon.

Il est souvent conseillé que les projets de supervision ne soient pas menés par l'équipe interne de la DSI[1]. Nous avons malgré tout fait ce choix car, lors de l'implémentation sur chaque site, je serai la personne en charge de décrypter les documents qui me seront fournis et je pourrai y apporter un regard extérieur. De plus, mon expérience passée sur les systèmes de supervision me permet d'avoir un certain recul, même s'il n'est probablement pas le même qu'un spécialiste ayant déjà installé de nombreuses supervisions dans plusieurs sociétés.

Afin de garantir les mises à jour du système au cours de son utilisation, nous allons voir dans la prochaine partie comment nous pensons organiser l'équipe en charge de l'administration de la solution.

5.2) Organisation de l'équipe informatique

5.2.1) Responsabilités

Un système d'information est en perpétuel mouvement, le système de supervision se doit de coller au plus près de la configuration physique du réseau et cela à tout moment. Il faut définir une organisation et des règles garantissant que Centreon soit mis à jour en temps réel.

Il est également nécessaire qu'un ou plusieurs responsables de l'administration de Centreon soient désignés et mis à contribution lors des différents projets impliquant l'installation de nouveaux éléments (applications, serveurs etc..) sur le réseau du groupe Powerflute.

Voici quelles seraient les missions du (ou des) responsable(s) supervision :

- Maintenir le système à jour ;
- Garantir l'harmonisation de la configuration de chaque serveur ;
- Installer des nouvelles sondes et créer les modèles ;
- Mettre à jour la documentation interne et le catalogue des indicateurs ;
- Ajuster les réglages de la solution afin de garantir l'efficacité des sondes et des notifications ;
- Assurer le transfert des notifications en cas d'indisponibilité d'un contact ;

[1] L. Fontaine et B. Legros*, Centreon - Maitrisez la supervision de votre Système d'Information*, ENI EDITION, 2012.

- Ajouter les points de contrôle nécessaires à chaque fois qu'un incident non détecté se produit.

Certaines de ces missions pourront être déléguées à la société Centreon dans le cas de l'achat d'une licence de support.

Pour autant, cette équipe d'administration n'a pas pour vocation d'effectuer les ajouts ou suppression d'hôtes dans Centreon. En effet, la configuration a été réfléchie afin que tous les opérateurs puissent faire ces ajouts, l'utilisation des modèles permettant de configurer rapidement de nouveaux hôtes. Cependant, l'équipe de supervision pourra assister les techniciens durant ces étapes d'administration.

Une file spécifique a été créée dans notre outil ITSM afin que les techniciens effectuent leurs demandes de mise à jour ou d'ajout de sonde.

Chaque membre de notre équipe, avec ses compétences propres, pourra intervenir en tant qu'expert. Leur expérience pourra alors être mise à profit lorsque de nouveaux besoins en supervision spécifiques à un domaine ou une application se présenteront (ex : DNS, Exchange).

Ainsi, un ou plusieurs rôles sont assignés à chaque membre de l'équipe :

- Responsable supervision : garant de la cohérence et du bon fonctionnement de la plateforme (quelques heures de travail par semaine) ;
- Exploitant : garant de la prise en compte des alertes et de l'adéquation de la supervision avec le SI (quelques heures de travail par mois) ;
- Experts : administrateur de domaines spécifiques (quelques heures de travail par an).

Ainsi, le rôle et les responsabilités de chacun sont clairement définis. La constitution de cette cellule de supervision est essentielle à l'efficacité de cette solution à long terme.

5.2.2) Organisation

Nous avons décrit dans le précédent chapitre (Partie III, chapitre 4), comment nous avons utilisé les différents concepts de supervision définis dans Centreon. Ces concepts offrent la possibilité d'adapter la supervision aux contraintes organisationnelles de l'équipe informatique.

Chaque service informatique possède une organisation propre, auquel s'ajoutent les objectifs de disponibilité des applications informatiques. Grâce à la gestion des notifications, escalades, niveaux de risques et contacts, il est possible de s'assurer de l'efficacité de la supervision.

Nous avons vu que le groupe Powerflute dispose de 2 types d'unités de production : les usines de production de carton et les tuberies. La gestion des notifications est différente en fonction du site supervisé. En effet les unités de production de carton travaillent à flux continu quand les tuberies travaillent uniquement les jours ouvrables.

La gestion des notifications sur les sites des tuberies a donc été pensée de façon à envoyer les alertes à l'informaticien responsable de chaque site. En cas d'absence de ce dernier, il conviendra de transférer les notifications au responsable secondaire qui a été désigné par la DSI de Powerflute. Les alertes sont envoyées par e-mail 24h/24 et 7J/7. Sur les sites de chaque tuberie, il faut également qu'il y ait un correspondant informatique qui puisse assister les techniciens lors de leurs opérations à distance (pour les opérations de redémarrage manuel ou de branchements). En effet, ces sites ne disposent pas tous d'un technicien sur site de façon permanente. Il faudrait également désigner deux correspondants par tuberie afin de s'assurer de la disponibilité continue de l'un d'entre eux.

Cette gestion est légèrement différente sur les sites de production de carton. Les alertes sont envoyées 24h/24 et 7J/7 mais toujours à au moins deux techniciens informatiques. Sur le site de Corenso France il s'agit de moi-même et de M. Mazet.

Cette gestion sera identique sur le site de Corenso Wisconsin (États-Unis) qui possède également deux informaticiens (Josh Malone et Paul Grosskopf). Sur le site de Corenso Pori (Finlande), qui ne possède qu'un informaticien (Tero Makela), c'est Jari Eskelinen qui travaille également en Finlande sur le site de Savon Sellu, qui est en mesure d'intervenir le plus rapidement. Il conviendra d'organiser les congés de ces derniers afin de s'assurer qu'au moins l'un des deux soit toujours disponible pour intervenir.

Cette organisation permet de s'assurer que chaque notification sera reçue par un technicien. Cependant, elle a ses limites si l'on souhaite réaliser une prise en compte des notifications 24h/24, avec des interventions sur site, car elle implique des astreintes presque permanentes sur de nombreux membres de l'équipe. Malgré la possibilité de se connecter à distance via

VPN, ces astreintes sont particulièrement contraignantes et ne favorisent pas la qualité de vie au travail. Elles peuvent même être contraires à certaines législations[1] en fonction des pays concernés. Je recommanderais soit une augmentation des effectifs, soit l'externalisation de la prise en compte des notifications de Centreon, ceci afin de soulager l'équipe technique interne du groupe Powerflute et de gagner en réactivité lorsqu'un incident se produit sur le réseau. Pour cela, il faudrait évaluer le coût d'un prestataire extérieur capable de gérer des interventions sur l'ensemble des sites du groupe et le comparer aux coûts engendrés par le recrutement de nouvelles ressources en interne. Même si le recrutement en interne de nouveaux techniciens est plus coûteux, ce choix me parait-être le plus judicieux car ils pourront également être mis à parti sur les projets, la maintenance des systèmes et le support aux utilisateurs.

La gestion des périodes d'astreintes repose avant tout sur la politique de notre DSI et son souhait de proposer ou non des ressources en continu sur l'ensemble des sites. J'ai proposé un calendrier afin de s'assurer uniquement de la prise en compte, sans interruption, des notifications sur l'ensemble des sites. Ce dernier inclut uniquement les 6 administrateurs systèmes du groupe qui devront, une semaine par mois, prendre en compte les notifications émises par Centreon en dehors des heures de présence sur site des techniciens locaux. Ce calendrier est disponible en annexe 11.

Centreon ne sait pas gérer directement un calendrier d'astreinte, cependant il est possible grâce à une tâche CRON exécutant des commandes Centreon CLAPI de gérer dynamiquement le destinataire des notifications.

Centreon offre une gestion souple et adaptative des règles de notifications. Elles pourront donc évoluer et s'adapter par la suite. Le plus important est d'être réactif au niveau de la configuration de Centreon afin de s'assurer que ce soit toujours les bons contacts qui soient notifiés. Ce sont les responsables de la supervision qui auront en charge ces paramétrages.

[1] Site Internet du service public [En ligne] (Page consultée le 15 mai 2017) https://www.service-public.fr/particuliers/actualites/A11297

5.2.3) Processus d'administration

Le(s) responsable(s) de la supervision doivent pouvoir s'appuyer sur des procédures lors de l'administration au quotidien de la solution de supervision.

Nous avons déjà expliqué la manière dont nous avons organisé la création des différents modèles et groupes afin d'adapter Centreon à nos propres besoins. Ces éléments de configuration sont propres à notre organisation et doivent être documentés et intégrés aux procédures de mise à jour de Centreon. Les administrateurs de la supervision doivent disposer de guides précis garantissant que chaque service contrôlé soit paramétré en suivant les règles que nous avons préalablement définies.

J'ai donc pour cela modélisé les processus de création des nouveaux modèles dans Centreon ayant pour objectif d'enrichir le catalogue des indicateurs.

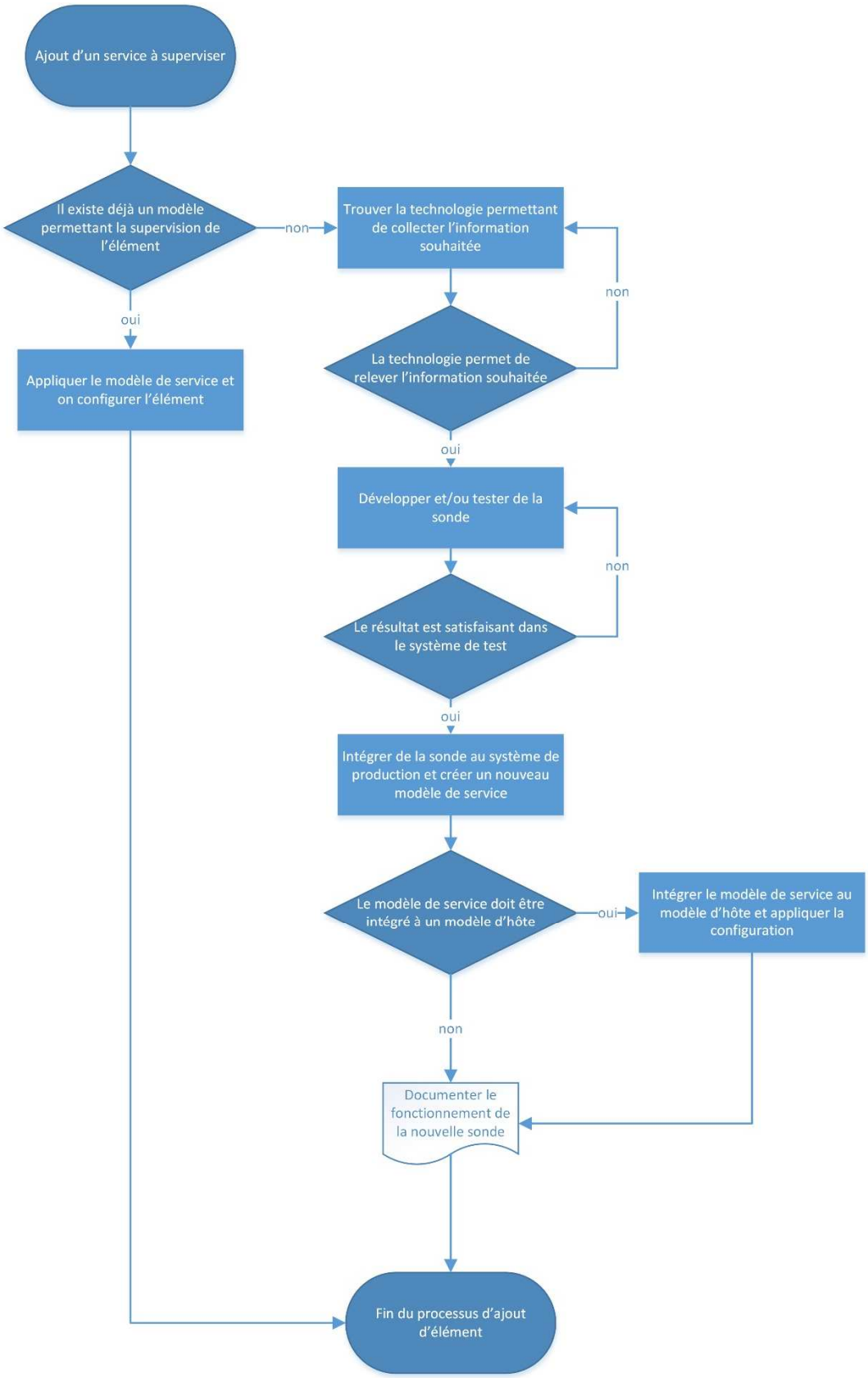


Figure 40 - Processus d'ajout d'élément à superviser

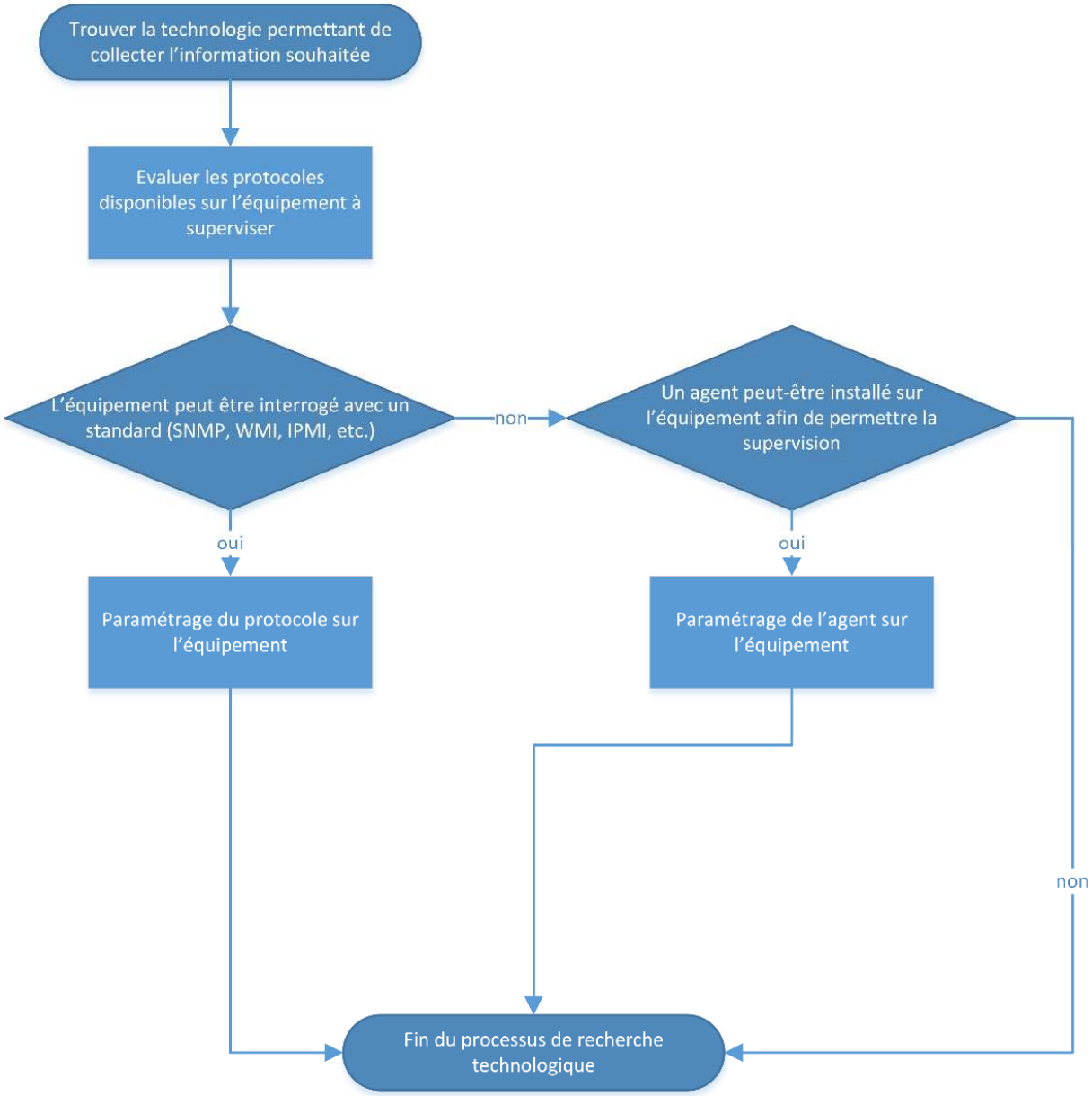


Figure 41 - Processus de recherche technologique

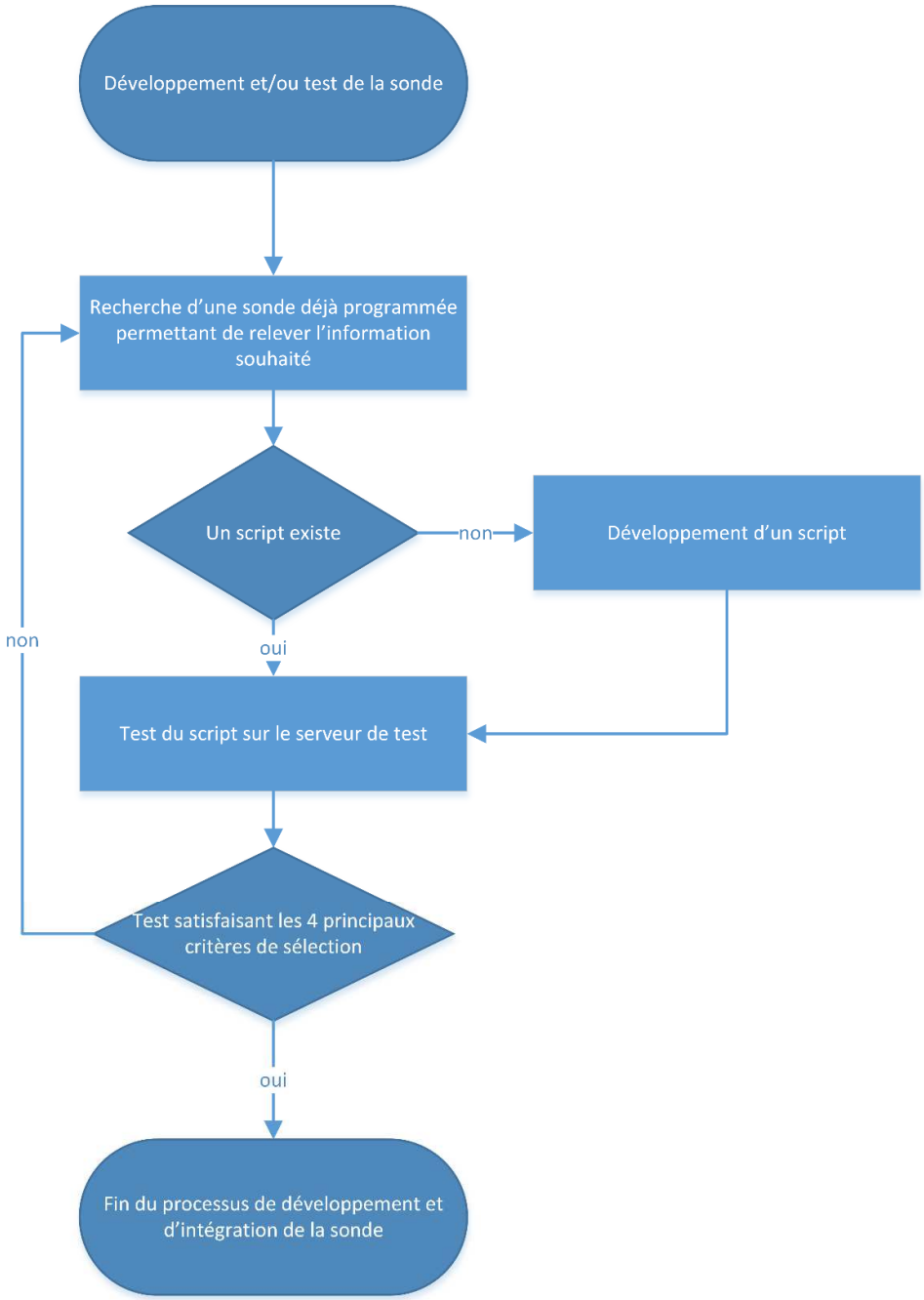


Figure 42 - Processus de développement et test des sondes

Chapitre 6 : État d'avancement du projet

Je vais, dans ce chapitre, présenter l'état d'avancement du projet, mon retour d'expérience et les pistes d'améliorations qu'il me semble intéressant d'étudier.

6.1) Aujourd'hui

À la date de rédaction de ce mémoire, la solution de supervision Centreon est entièrement fonctionnelle sur le Site de Corenso France. Sur ce site, nous avons actuellement 140 hôtes et près de 500 services. La solution est en service depuis deux mois et après quelques ajustements de paramétrage, elle fonctionne parfaitement puisque nous ne recevons les notifications qu'en cas de problème majeur ou activité anormale. Des problèmes sur le réseau électrique, et notamment quelques coupures sur le réseau ondulé de l'usine, nous ont permis de constater que nous recevions bien uniquement celles provenant des hôtes parents.

Les sites des tuberies de Krefeld, Edam, Tolosana, Bolton, Foshan et Hangzou sont également paramétrés dans la supervision depuis fin avril. Le paramétrage du site de Pori (Finlande) est planifié pour la fin du mois de mai.

Le retour d'expérience est plutôt positif, car dès la mise en place de l'outil nous avons pu détecter des problèmes sur les différents sites (espace disque ou espace mémoire trop faible). Des discussions avec notre fournisseur d'accès (Interoute) sont en cours pour que Centreon puisse effectuer la supervision de l'infrastructure serveur qu'ils nous louent sur chaque site des tuberies.

Depuis le début de ce projet, plusieurs incidents on eut lieu notamment sur l'infrastructure serveur de Pori (Finlande). Il est intéressant de constater que si l'outil avait déjà été fonctionnel sur ce site, ces incidents auraient sans doute pu être évités. Des incidents sur le serveur RDS 2012 m'ont également conduit à rajouter des sondes pour vérifier le fonctionnement des services nécessaires à son bon fonctionnement.

6.2) Pistes de réflexions

Bien entendu Centreon ne demande maintenant qu'à être enrichi, une certaine veille doit donc s'opérer de la part de chaque utilisateur, et surtout des responsables de la supervision.

Certains besoins facultatifs ont pour le moment été mis de côté, comme la visualisation et la centralisation de la documentation.

Nous espérions pouvoir installer le module libre NagVis[1] mais son paramétrage est très chronophage et présentait un risque de dépassement des délais. Il semble également plus judicieux d'utiliser la version payante Centreon MAP, qui est totalement adaptée et permet une configuration assez rapide des différentes vues.

La partie documentation du réseau, qu'il est intéressant d'intégrer à cet outil, sera étudiée prochainement, il est en effet possible d'utiliser Centreon Knowledge Base[2], qui est l'outil de type Wiki intégré à Centreon. Malheureusement, j'ai pu constater que la documentation du réseau de Powerflute était très succincte, il convient donc dans un premier temps de rassembler, compléter et mettre à jour toute cette documentation.

Ce projet a été l'occasion de balayer plusieurs technologies et notamment, on l'a vu, la technologie de supervision MODBUS TCP/IP. Puisque j'interviens également sur la partie automatisme il me paraît intéressant d'étudier la possibilité d'utiliser Centreon à des fins de collectes de données sur les automates industriels. Il serait ainsi possible de collecter, en temps réel, les données vitales des systèmes automatisés et ceci pourrait alléger considérablement la charge de travail des techniciens qui effectuent ces relevés de façon manuelle.

Enfin, maintenant que la solution est pleinement fonctionnelle, mon objectif est d'affiner sa granularité, c'est-à-dire développer et installer petit à petit de nouvelles sondes pour rendre notre outil plus efficace. Il serait en effet très intéressant de se pencher avec plus de précision sur la supervision des applications, qu'elles soient sous la responsabilité de la DSI ou de fournisseurs externes.

Maintenant que la solution Centreon CES est fonctionnelle, il serait également intéressant d'étudier la possibilité de rajouter la surcouche Centreon BAM[3] qui élargira les fonctionnalités actuelles vers une supervision de type BAM. Cette mise à jour nous ouvrira la possibilité

[1] Site Internet NagVis [En ligne] (Page consultée le 04 mai 2017) http://www.nagvis.org

[2] Documentation de Centreon [En ligne] (Page consultée le 5 mai 2017) https://documentation-fr.centreon.com/docs/centreon-knowledge-base/fr/latest/index.html

[3] Fiche technique Centreon BAM [En ligne] (Page consultée le 05 mai 2017) https://static.centreon.com/wp-content/uploads/2016/05/factsheet-BAM-fr.pdf

d'afficher des indicateurs de disponibilité des applications lisible par tous via le portail Intranet du groupe Powerflute. Ainsi nous pourrions communiquer au plus vite à tous lorsqu'un incident se produit et éviter les appels ou les tickets pouvant être créés simultanément par les utilisateurs.

6.3) Problèmes rencontrés

Ce projet n'est pour le moment pas totalement terminé, mais nous avons déjà rencontré quelques problèmes avec Centreon lors du déploiement de la solution.

Le premier problème a été le dysfonctionnement des rapports et donc l'impossibilité d'afficher les statistiques de disponibilité. Cette fonctionnalité étant très importante, j'ai passé plusieurs heures à essayer de résoudre le problème, sans succès. Après signalement sur le forum Centreon, il s'est avéré que le problème était en fait un « bug » de la dernière version du logiciel. Nous avons pu obtenir un correctif quelques semaines plus tard. Ceci démontre la bonne réactivité des équipes de développement malgré la gratuité du logiciel.

Le fonctionnement et le paramétrage des traps SNMP, notamment sur certains équipements, est parfois étrange. Nous avons actuellement un problème sur un serveur SAN qui, malgré un paramétrage identique à ses homologues, ne renvoie aucune information SNMP via les traps, même en utilisant les traps de test. L'assistance HP m'a conseillé d'effectuer une mise à jour des ILO. Ces mises à jour sont à planifier sur un arrêt de production.

Il semblerait que le serveur satellite de Corenso France ne prenne pas toujours en compte les modifications de configurations. Après un redémarrage de ce dernier, on arrive à faire fonctionner de nouveau la mise à jour de la configuration depuis le serveur central. Le problème est déjà apparu à deux reprises et je n'ai pas pu le solutionner jusqu'alors. Plusieurs vérifications ont été effectuées et tous les mécanismes semblent fonctionner correctement. Lors de la prochaine apparition de ce problème, nous devrons transmettre certains fichiers logs sur le forum d'assistance Centreon.

Conclusion

La gestion d'un réseau à l'échelle d'un groupe, implanté au niveau mondial, nécessite de la rigueur et, nécessairement, des outils assurant de piloter la gestion du SI avec efficacité. L'implantation d'un logiciel de supervision réseau est désormais une étape essentielle à mettre en œuvre pour garantir la bonne gestion du Service Informatique, en suivant les recommandations ITIL. La supervision du SI est essentielle pour anticiper et résoudre au plus vite les dysfonctionnements et planifier les besoins en ressources.

Un projet de supervision demande un investissement de la part de la DSI. L'évaluation du besoin présent et futur, le choix de l'outil et la configuration de ce dernier représente un coût à la fois financier et humain.

Que le projet soit mené de façon externe ou interne, il faut de toute manière mobiliser la DSI afin qu'elle définisse de façon précise ses attentes et fournisse les documents nécessaires à l'élaboration de la supervision.

Si le projet est réalisé intégralement en interne, comme nous l'avons décidé, il demandera un investissement particulier de la part des acteurs du projet. Par ailleurs, nous avons pu constater que le fait d'avoir une parfaite maîtrise de son outil de supervision permet d'être réactif lors des modifications et ajustements de configuration. Ceci est d'une importance majeure car un outil de supervision mal configuré ne sera pas utilisé par les administrateurs, fatigués de recevoir des notifications inutiles.

Le choix de mener ce projet de supervision en interne s'est avéré être judicieux dans notre cas, car avec un investissement financier minime (coût de l'infrastructure serveur), notre DSI s'est dotée d'un outil dont le retour sur investissement peut être très important. Dans un environnement industriel comme celui dans lequel a été réalisé ce projet, chaque heure d'arrêt machine se chiffre en milliers d'euros. Désormais, à l'ère de l'industrie 4.0[1], les applications informatiques sont au cœur du fonctionnement de nos unités de production.

Un projet de supervision doit se mener de façon continue, le SI évolue bien entendu, mais les besoins également. Il est important de mettre en place des procédures qui se déclencheront

[1] Site ZDNET [En ligne] (Page consultée le 26 mai 2017) http://www.zdnet.fr/actualites/industrie-40-une-revolution-tranquille-en-profondeur-a-l-heure-digitale-39850734.htm

après chaque incident non détecté par la supervision, afin que de nouvelles sondes soient configurées pour assurer leur détection. Prendre en compte les aspects de la supervision lors de chaque projet impactant le SI est également nécessaire.

À l'échelle d'un groupe, il faut également coordonner le travail des administrateurs souvent éloignés les uns des autres. C'est pourquoi il est nécessaire de mettre en place une « cellule supervision » qui sera en charge de coordonner les actions de supervision et de tenir à jour une documentation appropriée. Cette cellule aura la charge d'adapter la configuration des alertes aux contraintes organisationnelles et techniques de l'équipe informatique. Il faut également définir une politique de gestion des notifications précise qui, couplée à l'organisation même des ressources humaines du service de support informatique, assurera la prise en compte rapide des incidents et donc leur résolution.

Ce projet m'a permis de mieux cerner les enjeux de la supervision système et d'acquérir une connaissance plus approfondie des réseaux présents sur chaque site de notre groupe. Il a été également, pour moi, l'occasion de faire mes preuves auprès de cette jeune équipe informatique et de démontrer ma capacité à gérer de façon autonome un projet de déploiement informatique demandant des compétences réseaux et système spécifiques.

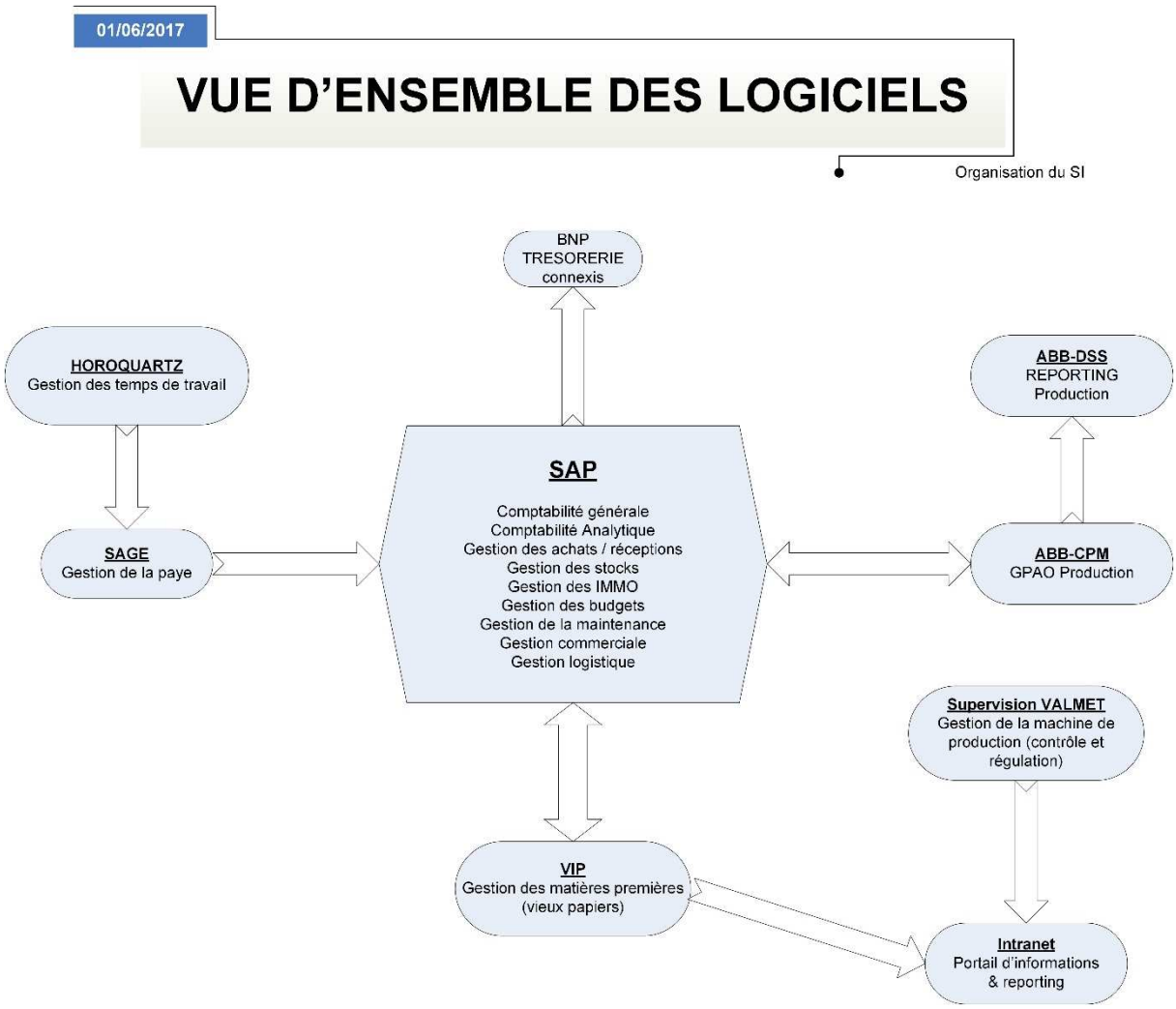
Humainement, j'ai trouvé ce projet particulièrement intéressant, il m'a permis de mieux connaître chaque membre de l'équipe informatique, de perfectionner mon anglais et mes compétences. J'ai pris un réel plaisir à travailler sur ce projet qui me tenait à cœur et qui marque l'étape finale de mon parcours au CNAM Nouvelle-Aquitaine.

Annexes

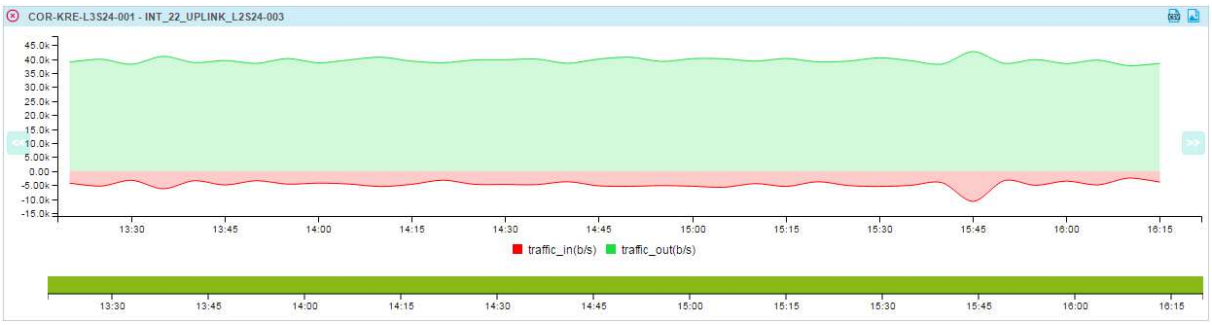
Table des annexes :

N°	Risques	Probabilité	Gravité	Coût	Impact	Nature (CQD)	Action de réduction
	RESSOURCES						
1	Une seule personne est en charge du projet	3	2	6	Risque de débordement ou de prise de décision individuelle erronnée	Qualité/Délais	Suivi du planning, validation obligatoire des prises de décisions individuelles par email.
2	Disponibilité de la DSI	1	2	2	Délais de réponses pour les étapes de validation	Délais	Utiliser la réunion hebdomadaire pour effectuer les validations et les emails
3	Estimation de la charge de travail	2	2	4	Les estimations des délais ne sont pas réalistes	Délais	Le planning devras être affiné dès que la solution est choisi afin de permettre une meilleure évaluation de la charge de travail.
4	Priorité aux taches quotidiennes	2	3	6	les tâches de maintenance habituelles et externes au projet doivent suivre leur cours	Délais	Le planning sera réajusté chaque semaine en fonction de l'état d'avancement réel des taches
5	Pas de support du logiciel choisi	2	3	6	En cas de panne majeure impossibilité de contacter le support	Coût	Etudier la possibilité d'acquérir une license permettant d'accéder au support. S'assurer de disposer des sauvegardes nécessaires à la reprise du système.
	TECHNOLOGIE						
6	Maitrise technique du sujet	1	3	3	Temps nécessaire plus important que prévu	Délais	Suivi des avancées de R&D grâce au planning. Planification des points techniques à risques en début de projet.
7	Risque de créer des failles de sécurité	1	3	3	Risque en matière de sécurité	Qualité	les procédures doivent systèmatiquement inclure une vérification de la sécurité des nouveaux échanges : EBIOS.
8	Infrastructure réseau insuffisante	1	2	2	La solution ne peut pas être déployée sans l'ajout de ressources	Coût	La validation de l'architecture technique devra intervenir assez tôt afin de permmettre la commande de matériels supplémentaires si besoin.
9	Performance et consommation de l'application	1	3	3	La solution consomme une part trop importante des ressources du réseau une fois déployée	Délais	Vérification des ressources consommées par sites et vérifications des retour utilisateurs de la solution.
10	Cohérence entre le besoin et les fonctionnalitées de l'application	2	2	4	La solution ne répond pas au besoin formulé	Qualité	Effectuer un prototypage actif afin de valider au plus tôt les exigences du logiciel (rédaction d'un cahier de test unitaire).
	UTILISATION						
11	Implication des utilisateurs	1	2	2	Les utilisateurs n'accepte pas l'application ou ne comprennent pas son intérêt	Coût	Prévoir présentation de la solution choisie
12	Formation des utilisateurs	1	2	2	Les utilisateurs n'osent pas utiliser la solution	Coût	Prévoir une formation plus approfondie avec chaque utilisateur individuellement
13	Mise à jour de la solution	1	3	3	Les utilisateurs ne peuvent pas mettre à jour eux même la solution	Qualité	Prévoir une file spécifique dans l'outil ITSM pour que les utilisateurs puissent facilement demander la mise à jour de la solution
14	Connaissance des administrateurs	2	3	6	Un seul utilisateur maitrise totalement la solution	Qualité	Prévoir une formation spécifique à 1 ou 2 utilisateurs maximum. Constituer une équipe de supervision.
15	Documentation spécifique et procédures d'exploitation	2	2	4	La documentation spécifique du logiciel paramétré pour le groupe Powerflute n'existe pas	Qualité	Une documentation en Anglais doit être livrée en fin de projet

Annexe 2 – Vue d'ensemble des logiciels



Annexe 3 – Graphique de performance d'une sonde de débit dans Centreon



Annexe 4 – Visualisation de l'état d'une infrastructure VSPHERE dans Centreon

S	Hosts	Services	Status	Duration	Last Check	Tries	Status information
	COR-FRA-VSP-01	PING	OK	3w 1d	1m 32s	1/2 (H)	OK - 10.114.15.10: rta 0.207ms, lost 0%
		RDP	OK	1M 4w	34m 34s	1/5 (H)	x224 OK. Connection setup time: 0.002766 sec.
		SNMP_CPU_W	OK	4w 2d	49s	1/2 (H)	OK: CPU(s) average usage is: 3.50%
		SNMP_DISK_W	OK	1M 3w	37m 5s	1/5 (H)	OK: Storage 'C:\ Label: Serial Number 16eb8dd7' Total: 59.66 GB Used: 35.97 GB (60.29%) Free: 23.69 GB (39.71%)
		SNMP_MEM_W	OK	1h 37m	2m 20s	1/2 (H)	OK: RAM Total: 8.00 GB Used: 7.18 GB (89.70%) Free: 844.06 MB (10.30%)
		SNMP_TRAFFIC_W	OK	4w 2d	4m 35s	1/2 (H)	OK: All interfaces are ok
		SNMP_UPTIME_W	OK	1M 3w	35m 50s	1/5 (H)	OK: System uptime is: 30d 4h 39m 28s
		TRAP_VSPHERE	OK	1M 2w	19h 51m	1/5 (H)	NO TRAP SINCE 24h
		VSP_CPU	OK	1w 3d	2m 5s	1/2 (H)	CHECK_VMWARE_API.PL OK - cpu usage=16.09 %
		VSP_DATASTORE_HA_1	OK	1w 3d	38m 21s	1/5 (H)	CHECK_VMWARE_API.PL OK - Storages : 'HA_Volume_1'(used)=830381 MB (79.21%)
		VSP_DATASTORE_HA_2	OK	1w 3d	34m 35s	1/5 (H)	CHECK_VMWARE_API.PL OK - Storages : 'HA_Volume_2'(used)=790144 MB (75.37%)
		VSP_DATASTORE_LA_1	OK	1w 3d	35m 51s	1/5 (H)	CHECK_VMWARE_API.PL OK - Storages : 'LA_Volume_1'(used)=296337 MB (57.91%)
		VSP_MEM	OK	1w 3d	2m 6s	1/2 (H)	CHECK_VMWARE_API.PL OK - mem usage=50.74 %
		VSP_NET	OK	1w 3d	3m 21s	1/2 (H)	CHECK_VMWARE_API.PL OK - net usage=2666.00 KBps
		VSP_STATUS	OK	1w 3d	34m 36s	1/5 (H)	CHECK_VMWARE_API.PL OK - 15/17 VMs up (0 templates), 2/2 Hosts up, Soustre overall status=gray, no config issues

Annexe 5 – Visualisation d'un hôte Windows dans Centreon

COR-FRA-TSE-01	PING	OK	1d 15h	3m 43s	1/2 (H)	OK - 10.114.15.20: rta 0.553ms, lost 0%
	RDP	OK	1M 4w	39m 43s	1/5 (H)	x224 OK. Connection setup time: 0.004598 sec.
	SNMP_CPU_W	OK	4d 4h	58s	1/2 (H)	OK: CPU(s) average usage is: 1.31%
	SNMP_DISK_W	OK	1M 2w	37m 13s	1/5 (H)	OK: All storages are ok.
	SNMP_MEM_W	OK	4d 4h	1m 5s	1/2 (H)	OK: RAM Total: 48.00 GB Used: 18.66 GB (38.87%) Free: 29.34 GB (61.13%)
	SNMP_SERVICE_BROKER	OK	1M 2w	38m 29s	1/5 (H)	OK: All service states are ok
	SNMP_SERVICE_GATEWAY	OK	1w 2d	37m 44s	1/5 (H)	OK: All service states are ok
	SNMP_TRAFFIC_W	OK	4d 4h	59s	1/2 (H)	OK: All interfaces are ok
	SNMP_UPTIME_W	OK	1M 2w	37m 14s	1/5 (H)	OK: System uptime is: 4d 3h 38m 1s

Annexe 6 – Visualisation d'un commutateur dans Centreon

COR-KRE-L3S24-001	INT_1_WAN	OK	6d 15h	4m 53s	1/2 (H)	OK: Interface 'Port 1' Traffic In : 180.40Kb/s (0.02%), Traffic Out : 178.62Kb/s (0.02%)
	INT_21_UPLINK_L2S24-001	OK	2d 13h	1m 46s	1/2 (H)	OK: Interface 'Port 21' Traffic In : 4.12Kb/s (0.00%), Traffic Out : 5.50Kb/s (0.00%)
	INT_22_UPLINK_L2S24-003	OK	2d 13h	3m 32s	1/2 (H)	OK: Interface 'Port 22' Traffic In : 5.02Kb/s (0.00%), Traffic Out : 39.63Kb/s (0.00%)
	INT_23_UPLINK	OK	6d 15h	4m 53s	1/2 (H)	OK: Interface 'Port 23' Traffic In : 14.77Kb/s (0.00%), Traffic Out : 19.34Kb/s (0.00%)
	INT_24_UPLINK_L3S24-002	OK	2d 13h	1m 46s	1/2 (H)	OK: Interface 'Port 24' Traffic In : 42.41Kb/s (0.00%), Traffic Out : 75.90Kb/s (0.01%)
	INT_2_UPLINK_L2S08-001	OK	2d 13h	3m 32s	1/2 (H)	OK: Interface 'Port 2' Traffic In : 2.09Kb/s (0.00%), Traffic Out : 39.22Kb/s (0.00%)
	INT_9_UPLINK_L2S24-004	OK	6d 15h	4m 53s	1/2 (H)	OK: Interface 'Port 9' Traffic In : 1.43Kb/s (0.00%), Traffic Out : 38.91Kb/s (0.00%)
	PING	OK	2d 13h	1m 46s	1/2 (H)	OK - 10.104.5.50: rta 19.036ms, lost 0%

Annexe 7 – Visualisation d'un serveur Hôte dans Centreon

COR-FRA-VMH-02I	HP_ILO_CONTROLLER	OK	1M 3w	40m 53s	1/5 (H)	OK: All 1 components are ok [1/1 ctrl].
	HP_ILO_CPU	OK	1M 3w	42m 9s	1/5 (H)	OK: All 2 components are ok [2/2 cpu].
	HP_ILO_DRIVE	OK	1M 3w	38m 23s	1/5 (H)	OK: All 2 components are ok [2/2 pdrive].
	HP_ILO_FAN	OK	1M 3w	39m 39s	1/5 (H)	OK: All 6 components are ok [6/6 fans].
	HP_ILO_HEALTH	OK	1M 3w	40m 54s	1/5 (H)	OK: All 89 components are ok [1/1 battery, 2/2 cpu, 1/1 ctrl, 2/2 driveencl, 6/6 fans, 1/1 ldrive, 24/24 memory, 4/4 nic, 2/2 pdrive, 2/2 psu, 44/44 temperatures].
	HP_ILO_MEMORY	OK	1M 3w	42m 10s	1/5 (H)	OK: All 24 components are ok [24/24 memory].
	HP_ILO_NIC	OK	1M 3w	38m 24s	1/5 (H)	OK: All 4 components are ok [4/4 nic].
	HP_ILO_PSU	OK	1M 3w	39m 40s	1/5 (H)	OK: All 2 components are ok [2/2 psu].
	HP_ILO_TEMPERATURE	OK	1M 3w	40m 55s	1/5 (H)	OK: All 44 components are ok [44/44 temperatures].
	TRAP_HP_HW	OK	1M 3w	22h 2m	1/5 (H)	NO TRAP SINCE 24h

Annexe 8 – Tableau de bord principal de Centreon

Annexe 9 – Catalogue des indicateurs

HOST TEMPLATE	Host template description	SERVICE TEMPLATES LINKED	Service template description
VEEAM	Used to collect Veeam traps to monitor backup system	TRAP_VEEAM	Passive service check waiting for traps from Veeam B&R
DELL_HW	Used to monitor Dell hardware	PING	PING
ESX_HOST	Used to monitor ESX server	ESX_CPU	Check CPU of the VM HOST SERVER
		ESX_MEM	Check Memory of the VM HOST SERVER
		ESX_DATASTORE	Check Datastore free space
		ESX_HEALTH	Check Global Health and return the detail of the problem
		ESX_STATUS	Check global status (similar to health)
HP_HW	Used to monitor HP hardware	PING	ICMP - PING
WIN_SRV	Used to monitor Windows servers	PING	PING
		SNMP_CPU_W	Check CPU %
		SNMP_DISK_W	Check Disk Space (all disks found on the system)
		SNMP_MEM_W	Check free memory
		SNMP_SWAP_W	Check SWAP memory
		SNMP_TRAFFIC_W	Check severals traffic on Interfaces
		SNMP_UPTIME_W	Check Uptime (just to display the uptime)
		RDP	Check if RDP port is open on the server
HP_ILO	Used to check ILO (physical server check)	HP_ILO_CONTROLLER	Check disk controller
		HP_ILO_CPU	Check CPU state
		HP_ILO_DRIVE	Check disks
		HP_ILO_FAN	Check FAN status
		HP_ILO_MEMORY	Check Memory Status

HOST TEMPLATE	Host template description	SERVICE TEMPLATES LINKED	Service template description
		HP_ILO_PSU	Check Power Supply Unit
		HP_ILO_TEMPERATURE	Check global Temperature
WIN_WEB	Used to check http server	HTTP	Check HTTP port 80
MYSQL_SERVER	Used to check Mysql Online & running	DATABASE_MYSQL	Check connection to database
HP_SAN	Check Hp San status	PING	
		TRAP_HP_LEFTHAND	Trap to receive alerts
HP_STO	Check HP storage system	PING	ICMP - PING
SERVER_INT	Used to check only IP Interface (ping)	PING	ICMP - PING
ISCSI		PING	ICMP - PING
HP_UPS	Check UPS	PING	ICMP - PING
		HP_UPS_BATTERY_PERCENT	Display % of battery (SNMP check)
		HP_UPS_INPUT_VOLTAGE	Display input voltage
VSPHERE	Check Vpshere environnment (VSP win server)	TRAP_VSPHERE	Trap to collect all details when an error occur
		VSP_CPU	Check CPU
		VSP_DATASTORE	Check datastore
		VSP_MEM	Check memory
		VSP_NET	Check network interface
		VSP_STATUS	Check global health status
LINUX_SRV	Used to check Linux server	PING	ICMP - PING
		SNMP_CPU_L	Check CPU %
		SNMP_DISK_L	Check Disk Space (all disks found on the system)
		SNMP_MEM_L	Check free memory
		SNMP_SWAP_L	Check SWAP memory
		SNMP_TRAFFIC_L	Check several traffic on Interfaces
		SNMP_UPTIME_L	Check Uptime (just to show the uptime)
MERAKI_SW	Used to monitor Meraki Switch	PING	ICMP - PING
		SNMP_INT	Check interface status
		SNMP_BW	Check interface bandwidth
HP_SW	Used to monitor HP Switch	PING	ICMP - PING
		SNMP_INT	Check interface status

HOST TEMPLATE	Host template description	SERVICE TEMPLATES LINKED	Service template description
		SNMP_BW	Check interface bandwidth
CAM_DLINK	Used to monitor IP camera and more specificaly DLINK IP CAM	PING	ICMP - PING
		HTTP_AUTH	Check HTTP access with authentication
		DLINK_BW	Check bandwidth on cam interface, and alert if bandwidht too low
		RTSP	Check RTSP port on the webcam
IPSCR	IP CAM screen	PING	ICMP - PING
PROD_PRINTER	Production printer	PING	ICMP - PING
PLC	PLC / automation devices	PING	ICMP - PING
ROUTER	Router	PING	ICMP - PING

Annexe 10 – Exemple de fichier CSV d'import

	A	B	C	D	E	F	G	H
1	**HOSTNAME**	**DESCRIPTION**	**IP**	**HOST TEMPLATE |**	**POLLER**	**HOSTGROUP |**	**PARENT**	**CATEGORY**
2	MANDATORY		MANDATORY	MANDATORY		MANDATORY	MANDATORY	MANDATORY
3	COR-KRE-ICC-01	ICC ESX Krefeld		SERVER_INT|COR-KRE|GENER	VDC-FRA-MON-01_CENTRAL	COR-KRE-SITE|SERVER-DEV|	SICOR-KRE-L3S24-001	High_importance
4	COR-TOL-ICC-01	ICC ESX Tolosana		SERVER_INT|COR-TOL|GENER	VDC-FRA-MON-01_CENTRAL	COR-TOL-SITE|SERVER-DEV|	SICOR-TOL-L3S24-001	High_importance
5	COR-BOL-ICC-01	ICC ESX Bolton		SERVER_INT|COR-BOL|GENER	VDC-FRA-MON-01_CENTRAL	COR-BOL-SITE|SERVER-DEV|	SICOR-BOL-L3S24-001	High_importance
6	COR-EDM-ICC-01	ICC ESX Edam		SERVER_INT|COR-EDM|GENEF	VDC-FRA-MON-01_CENTRAL	COR-EDM-SITE|SERVER-DEV|	SICOR-EDM-L3S24-001	High_importance
7	COR-LOV-ICC-01	ICC ESX Lovlisa		SERVER_INT|COR-LOV|GENER	VDC-FRA-MON-01_CENTRAL	COR-LOV-SITE|SERVER-DEV|	SERVER-NET|MANAGEMENT-NE	High_importance
8	COR-IMA-ICC-01	ICC ESX Imatra		SERVER_INT|COR-IMA|GENER	VDC-FRA-MON-01_CENTRAL	COR-IMA-SITE|SERVER-DEV|	SERVER-NET|MANAGEMENT-NE	High_importance
9	COR-HEL-ICC-01	ICC ESX Helsinki		SERVER_INT|COR-HEL|GENER	VDC-FRA-MON-01_CENTRAL	COR-HEL-SITE|SERVER-DEV|	SERVER-NET|MANAGEMENT-NE	High_importance
10	POW-MON-ICC-01	ICC ESX Monaco		SERVER_INT|POW-MON|GEN	VDC-FRA-MON-01_CENTRAL	POW-MON-SITE|SERVER-DEV|	SERVER-NET|MANAGEMENT-I	High_importance
11	COR-BAC-ICC-01	ICC ESX Backefors		SERVER_INT|COR-BAC|GENER	VDC-FRA-MON-01_CENTRAL	COR-BAC-SITE|SERVER-DEV|	SERVER-NET|MANAGEMENT-NE	High_importance
12	COR-MOH-ICC-01	ICC ESX Mohed		SERVER_INT|COR-MOH|GENE	VDC-FRA-MON-01_CENTRAL	COR-MOH-SITE|SERVER-DEV|	SERVER-NET|MANAGEMENT-N	High_importance
13	COR-HAN-ICC-01	ICC ESX Hangzhou		SERVER_INT|COR-HAN|GENEF	VDC-FRA-MON-01_CENTRAL	COR-HAN-SITE|SERVER-DEV|	SICOR-HAN-L3S24-001	High_importance
14	COR-FOS-ICC-01	ICC ESX Foshan City		SERVER_INT|COR-FOS|GENER	VDC-FRA-MON-01_CENTRAL	COR-FOS-SITE|SERVER-DEV|	SICOR-FOS-L3S24-001	High_importance
15	COR-BOL-GW-01	GatewayVIP		ROUTER|COR-BOL|GENERIC_C	VDC-FRA-MON-01_CENTRAL	COR-BOL-SITE|ROUTER-DEV|	TRANSIT-NET|NETWORK-APP|	High_importance
16	COR-BOL-HSRP-01	HSRP Primary		ROUTER|COR-BOL|GENERIC_C	VDC-FRA-MON-01_CENTRAL	COR-BOL-SITE|ROUTER-DEV|	TRANSIT-NET|NETWORK-APP|	High_importance
17	COR-BOL-HSRP-02	HSRP Backup		ROUTER|COR-BOL|GENERIC_C	VDC-FRA-MON-01_CENTRAL	COR-BOL-SITE|ROUTER-DEV|	TRANSIT-NET|NETWORK-APP|	High_importance
18	COR-BOL-VRRP-VIP	VRRP VIP		ROUTER|COR-BOL|GENERIC_C	VDC-FRA-MON-01_CENTRAL	COR-BOL-SITE|ROUTER-DEV|	TRANSIT-NET|NETWORK-APP|	High_importance
19	COR-BOL-L3S24-001	Switch Server Room		MERAKI_SW|COR-BOL|GENER	VDC-FRA-MON-01_CENTRAL	COR-BOL-SITE|SWITCH-DEV|	MANAGEMENT-NET|PRIMARY-F	High_importance
20	COR-BOL-L3S24-002	Switch Server Room		MERAKI_SW|COR-BOL|GENER	VDC-FRA-MON-01_CENTRAL	COR-BOL-SITE|SWITCH-DEV|	NCOR-BOL-L3S24-001	High_importance

Annexe 11 – Proposition de planning pour la prise en compte des notifications

MOIS 1					
Site	**Ressources**	**Semaine 1 Guillaume LEROY**	**Semaine 2 Tero Makela**	**Semaine 3 Paul GROSSKOPF**	**Semaine 4 Jari Eskelinen**
Corenso France	Responsable	**Guillaume LEROY**	**Tero Makela**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet
Corenso Pori	Responsable	**Guillaume LEROY**	**Tero Makela**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen
Powerflute Savon Sellu	Responsable	**Guillaume LEROY**	**Tero Makela**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen
Corenso Wiskonsin	Responsable	**Guillaume LEROY**	**Tero Makela**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone
Tuberies et bureaux	Responsable	**Guillaume LEROY**	**Tero Makela**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	à désigner	à désigner	à désigner	à désigner
MOIS 2					
Site	**Ressource**	**Semaine 1 Dirk Kranen**	**Semaine 2 Derek Song**	**Semaine 3 Paul GROSSKOPF**	**Semaine 4 Jari Eskelinen**
Corenso France	Responsable	**Dirk Kranen**	**Derek Song**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet
Corenso Pori	Responsable	**Dirk Kranen**	**Derek Song**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen
Powerflute Savon Sellu	Responsable	**Dirk Kranen**	**Derek Song**	**Paul GROSSKOPF**	**Jari Eskelinen**

	Correspondants	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen
Corenso Wiskonsin	Responsable	**Dirk Kranen**	**Derek Song**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone
Tuberies et bureaux	Responsable	**Dirk Kranen**	**Derek Song**	**Paul GROSSKOPF**	**Jari Eskelinen**
	Correspondants	à désigner	à désigner	à désigner	à désigner
MOIS 3					
Site	**Ressource**	**Semaine 1 Dirk Kranen**	**Semaine 2 Derek Song**	**Semaine 3 Guillaume LEROY**	**Semaine 4 Tero Makela**
Corenso France	Responsable	**Dirk Kranen**	**Derek Song**	**Guillaume LEROY**	**Tero Makela**
	Correspondants	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet	Guillaume LEROY Jérôme Mazet
Corenso Pori	Responsable	**Dirk Kranen**	**Derek Song**	**Guillaume LEROY**	**Tero Makela**
	Correspondants	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen
Powerflute Savon Sellu	Responsable	**Dirk Kranen**	**Derek Song**	**Guillaume LEROY**	**Tero Makela**
	Correspondants	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen	Tero Makela Jari Eskelinen
Corenso Wiskonsin	Responsable	**Dirk Kranen**	**Derek Song**	**Guillaume LEROY**	**Tero Makela**
	Correspondants	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone	Paul GROSSKOPF Josh Malone
Tuberies et bureaux	Responsable	**Dirk Kranen**	**Derek Song**	**Guillaume LEROY**	**Tero Makela**
	Correspondants	à désigner	à désigner	à désigner	à désigner

Bibliographie

Ouvrages imprimés :

Autissier D., Delaye V., 2008, *Mesurer la performance du système d'information*, EYROLLES, Paris, 97 p.

Dumont D., 2007, *ITIL – pour un service informatique optimal*, EYROLLES, Paris, 378 p.

Fontaine L., Legros B., 2012, *Centreon, Maitrisez la supervision de votre Système d'Information*, ENI EDITION, Paris, 461 p.

Gabès J., 2009, *Nagios 3 pour la supervision et la métrologie*, EYROLLES, Paris, 506 p.

Lecompte S., Boulanger T, 2008, *XML Par la pratique*, ENI EDITION, Paris, 378 p.

Printz J., 2012, *Architecture Logicielle*, DUNOD, Paris, 512 p.

Mauro D. R., Schmidt K. J., 2005, *Essential SNMP*, O'REILLY, 462 p.

PIGNET F., 2008, Réseaux Informatique - Supervision et administration, ENI EDITION, Paris, 274 p.

Sites Internet :

Atelier de Kermit [En ligne] (Page consultée le 15 février 2017) http://www.sugarbug.web4me.fr

Centreon, documentation [En ligne] (Page consultée le 15 février 2017) https://documentation-fr.centreon.com/docs/centreon/fr/2.7.x/

Cisco [En ligne] (Page consultée le 19 février 2017) http://www.cisco.com

DMTF sur WSMan [En ligne] (Page consultée le 15 mars 2017) https://www.dmtf.org/standards/wsman

IETF [En ligne] (Page consultée le 25 février 2017) https://www.ietf.org

ISO [En Ligne] (Page consultée le 18 avril 2017) http://www.iso.org/iso/fr/

ITIL France [En ligne] (Page consultée le 15 février 2017) http://www.itilfrance.com

Frame IP sur SNMP [En Ligne] (Page consultée le 10 février 2017) http://www.frameip.com/snmp/

Nagios Plugins, documentation [En ligne] (Page consultée le 22 janvier 2017) https://nagios-plugins.org/doc/guidelines.html

RRDTOOL [En ligne] (Page consultée le 22 janvier 2017) http://www.mrtg.org/rrdtool

Liste des figures

Gestion du déploiement d'une solution de supervision réseau multi-sites, Mémoire d'Ingénieur C.N.A.M., Bordeaux 2017.

Résumé

La supervision réseau est désormais un enjeu crucial pour les entreprises qui se doivent d'assurer une forte disponibilité du système d'information. La DSI du groupe Powerflute a donc décidé de se doter d'un tel outil après le rachat du groupe Corenso et la restructuration complète de son réseau informatique. Parmi la multitude d'outils disponibles, c'est Centreon, un logiciel libre, qui a été sélectionné et sa mise en fonction réalisée en interne. En dehors des considérations techniques qui permettent de s'assurer de l'efficience de la solution, l'organisation du service informatique a son importance. En effet, un tel outil nécessite que des règles soient définies, que ce soit pour l'administration ou la prise en compte des incidents au quotidien. Pour créer de la valeur, il est donc primordial pour une entreprise de mener une réflexion globale sur l'implantation et la gestion de son système de supervision. Ce document a pour objectif de répondre à cette problématique dans le contexte actuel et futur du groupe Powerflute.

Mots clés : supervision des réseaux, système d'information, SNMP, alertes, sondes, protocoles, pilotage, infrastructure réseau.

Summary

The monitoring of mission critical Information Systems is now a crucial issue for companies in order to ensure high availability of their IT assets. Therefore, Powerflute group ISD decided to implement such a tool after the takeover of the Corenso group of companies and the complete revamp of its IT network and key systems. Among the wide array of available tools, the free software Centreon has been selected and its implementation realized in-house. Apart from the technical considerations which ensure the efficiency of the solution, the IT service organisation is also a significant input into the design. Indeed, such a tool has requirements to define rulesets for administration, day-to-day operational activities and exceptional activities such as planned outages and service breaks. To create value, it is thus imperative for a company of which the business activities rely heavily on their Information Systems to devote a global perspective to the Monitoring Systems' proper setup, configuration and ongoing management. The purpose of this document is to answer these problems for the current and future requirements of Powerflute group.

Key words: network monitoring, information system, SNMP, alerts, probes, protocol, management, network infrastructure.