



HAL
open science

Supervision de l'infrastructure des systèmes d'information métier du Service de santé des armées

Jacques Bidanel

► **To cite this version:**

Jacques Bidanel. Supervision de l'infrastructure des systèmes d'information métier du Service de santé des armées. Architectures Matérielles [cs.AR]. 2012. dumas-01066307

HAL Id: dumas-01066307

<https://dumas.ccsd.cnrs.fr/dumas-01066307>

Submitted on 19 Sep 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CONSERVATOIRE NATIONAL DES ARTS & METIERS
Centre Régional associé de Rennes

Mémoire présenté en vue
d'obtenir le diplôme d'ingénieur **C.N.A.M.**
en informatique

Jacques BIDANEL

**SUPERVISION DE L'INFRASTRUCTURE
DES SYSTEMES D'INFORMATION METIER
DU SERVICE DE SANTE DES ARMEES**

soutenu le 20 Juin 2012

JURY

PRESIDENT:

Professeur POLLET

MEMBRES:

Mr ROSTOLL
Mr CHAMPION
M DESCAT

Version 1.0 , imprimée le 15 mai 2012
en Recto/Verso pour être respectueux de l'environnement

REMERCIEMENTS

Mes vifs remerciements vont d'abord à Monsieur Champion, qui m'a proposé ce sujet de mémoire. Il m'a apporté son soutien et les moyens pour mener à bien ce projet, dans un contexte professionnel difficile. Je remercie l'équipe TME Bull et Mr Cattachio, qui malgré leur charge de travail, ont toujours trouvé le temps pour donner les renseignements utiles, sur les Systèmes d'Information hébergés au CeTIMA.

Ma reconnaissance va particulièrement à Mr Rostoll, pour son aide et ses précieux conseils, tout au long de la rédaction de ce mémoire d'ingénieur.

Une pensée particulière à l'ensemble des équipes, que j'ai encadré et à mes différents supérieurs hiérarchiques, qui m'ont encouragé, lors de mon parcours au CNAM, pendant ces 10 ans.

Je remercie aussi le Médecin Général Inspecteur Le Saint, pour son engagement à valider mon diplôme d'ingénieur CNAM, à mon arrivée à la DRSSA de Brest, le Médecin Général Inspecteur Pats pour avoir défendu cet objectif professionnel et le Médecin Général des Armées Nedelec, pour avoir donné un avis favorable à ma demande.

RESUME

Le Système d'information fait aujourd'hui partie intégrante de l'organisation des entreprises. Son importance nécessite des outils pour surveiller son bon fonctionnement et mesurer sa disponibilité. Après avoir présenté les différents Systèmes d'Information du Service de Santé des Armées et les normes utilisées, nous exposons la démarche projet, avec une analyse détaillée des architectures installées, pour rédiger un cahier des charges. Une étude des offres des logiciels du marché dégage une solution pour une plateforme logicielle de supervision. Elle apporte une vue globale du fonctionnement des services et des applications, des mesures de leur performance, avec un système d'alerte, en cas d'incident.

MOTS CLEFS : Supervision, Métrologie, Système d'Information Métier, Nagios, Centreon, Cacti

SUMMARY

Information System is now part of the business organization.

Its importance requires tools to monitor its good health and to measure its availability. After presenting the different Information Systems of the Health Service of the Armed Forces and the standards used, we outline the project approach, with a detailed analysis of installed architectures, in order to write specifications. A study of software market offers a solution for a monitoring platform. It provides an overview of the functioning of services and applications, measures of performance, with a warning system in case of incident.

KEY WORDS : Monitoring, Performance measurement, Information System, Nagios, Centreon, Cacti

1. Service de Santé des Armées et du CeTIMA.	8
1.1. Service Santé des Armées.	8
1.2. Le Centre de Traitement de l'Information Médicale des Armées (CeTIMA).	12
2. Le projet de supervision.	14
2.1. Objectifs, Enjeux.	14
2.2. Organisation du projet.	15
2.3. Concepts de la supervision	23
2.4. Outils standards.	25
3. Etude des SI Métier du SSA (Phase 1).	28
3.1. Système d'Information Métiers	28
3.1.1. Système d'Information des Services Médicaux d'Unité (SISMU).	28
3.1.2. Système d'Information des Hôpitaux (SIH).	32
3.1.3. Système d'Information du RAVitaillement (SIRAV)	35
3.2. Technologies utilisées	36
3.3. Gouvernance et Normes au SSA.	37
4. Cahier des charges fonctionnel (Phase 2).	40
5. Etude des solutions du marché et choix de la solution de supervision (Phase 3).	43
5.1. Offres des logiciels de supervision du marché.	43
5.2. Test et notation des logiciels Open Source	45
6. Etude de la plateforme de supervision et de ses composants (Phase 4)	47
6.1. Présentation de Nagios	47
6.2. Fonctionnement Nagios et ses Agents/Centreon/Cacti.	49
6.3. Architecture de la plate-forme.	55
6.4. Etude détaillée des logiciels éditeurs et agents Nagios	57
6.5. Etude de JBoss Operation Network (JON).	58
7. Maquettage (Phase 5)	59
7.1. Plateforme installée	59
7.2. Tests réalisés.	60
7.3. Bilan : compromis techniques pour une meilleure efficacité de l'outil de supervision.	61
8. Mise en œuvre sur les plateformes opérationnelles (Phase 6).	64
8.1. Installation sur le SI des DRSSA	64
8.2. Installation sur le SI SIMU du CeTIMA.	65
9. Bilan du projet (Phase 7) : Retour d'EXpérience, propositions d'évolutions et d'amélioration	67
9.1. Retour d'Expérience sur l'organisation	67
9.2. Retour d'Expérience technique	70
9.3. Proposition d'évolutions et d'amélioration	71

page vierge

INTRODUCTION

Quels sont les éléments majeurs pour le bon fonctionnement d'une entreprise ? De nombreuses études sur l'organisation des entreprises, mettent en évidence le rôle majeur de l'information et l'existence de trois sous-systèmes internes : système de décision ou de pilotage, système opérant et système d'information. Par ailleurs, on peut aussi constater qu'une information n'a de la valeur que si elle est pertinente, fiable et surtout disponible. D'après ces constats, on voit rapidement la position et le rôle essentiel, dans l'entreprise du Système d'Information (SI), qui se définit comme l'ensemble des informations échangées et des ressources (personnels, procédures, matériels...) mises en œuvre pour recueillir, stocker, exploiter, diffuser ces dernières.

En transposant ces analyses au Service Santé des Armées (SSA), on constate que le Système d'Information(SI) est le socle de base, qui coordonne les activités du système de production de soin, dans les hôpitaux, les Centres Médicaux, les Antennes Vétérinaires ou Centres de Médecine de Prévention des Armées ...

Il permet aussi de mettre à la disposition des autorités, les informations nécessaires à la prise de décision. Déclinés par métiers, ces systèmes d'information s'appuient sur des moyens informatiques, dont le périmètre ne cesse de devenir de plus en vaste, avec l'interconnexion des intranets, d'internet, des systèmes distribués et hétérogènes (téléphonie, réseau Wifi/3G, onduleurs, appareils médicaux...) et de technologies toujours plus nouvelles. Cette complexité croissante accroît les risques de panne. Mais on demande aussi une plus grande disponibilité et un temps de dépannage réduit.

En effet, le moindre incident peut avoir de lourdes conséquences aussi bien financières qu'organisationnelles. Dans le milieu médical du SSA, organisé autour du patient, cela peut encore être plus dramatique. Les problèmes doivent être anticipés, pour ne pas avoir d'impact sur le fonctionnement des services, sur la productivité du système et sur la satisfaction des utilisateurs.

Ainsi la surveillance des SI par un système de supervision, s'avère indispensable et primordial.

La supervision centralisée permet d'avoir en temps réel, une cartographie d'ensemble du système, de contrôler les ressources allouées et de réduire les coûts. Ce suivi des performances des composants assure une meilleure estimation des besoins. La maintenance est plus rapide et plus efficace, car le système est capable de diagnostiquer, et bien souvent, de réparer seul les pannes. Si ce n'est le cas, il se charge d'alerter immédiatement les personnes concernées. Une traçabilité des actions est assurée et permet d'extraire des rapports d'activité, qui serviront dans la conduite du changement, le suivi des contrats de service et l'optimisation du coût des processus métiers.

Le projet proposé est d'étudier la mise en place d'un outil de supervision, sur les Systèmes d'Information du Service Santé des Armées, au Ministère de la Défense.

Le document décrit les actions réalisées pour mener à bien cette mission.

Après une présentation du Service Santé des Armées (SSA) et du Centre de Traitement de l'Information Médicale des Armées (CeTIMA) au chapitre 1, le chapitre 2 définit plus précisément le projet avec ses objectifs, ses enjeux et l'organisation retenue (Qualité/Coût/Délai/Risques). La notion de supervision est ensuite développée, avec les outils de base disponibles (lignes de commande, protocole SNMP...).

Dans le chapitre 3, nous débuterons l'étude par étudier chacune de ses plateformes « métier » et les technologies mises en œuvre, en n'oubliant pas d'intégrer, dans notre analyse, les normes et bonnes pratiques utilisées au Ministère de la Défense.

Connaissant les éléments à superviser, un cahier des charges fonctionnel a été rédigé et expliqué au chapitre 4, avec une grille d'évaluation pour faciliter le choix du meilleur produit.

Au chapitre 5, nous avons établi un bilan des offres logicielles du marché, avec leur notation individuelle, par rapport aux critères précédemment définis.

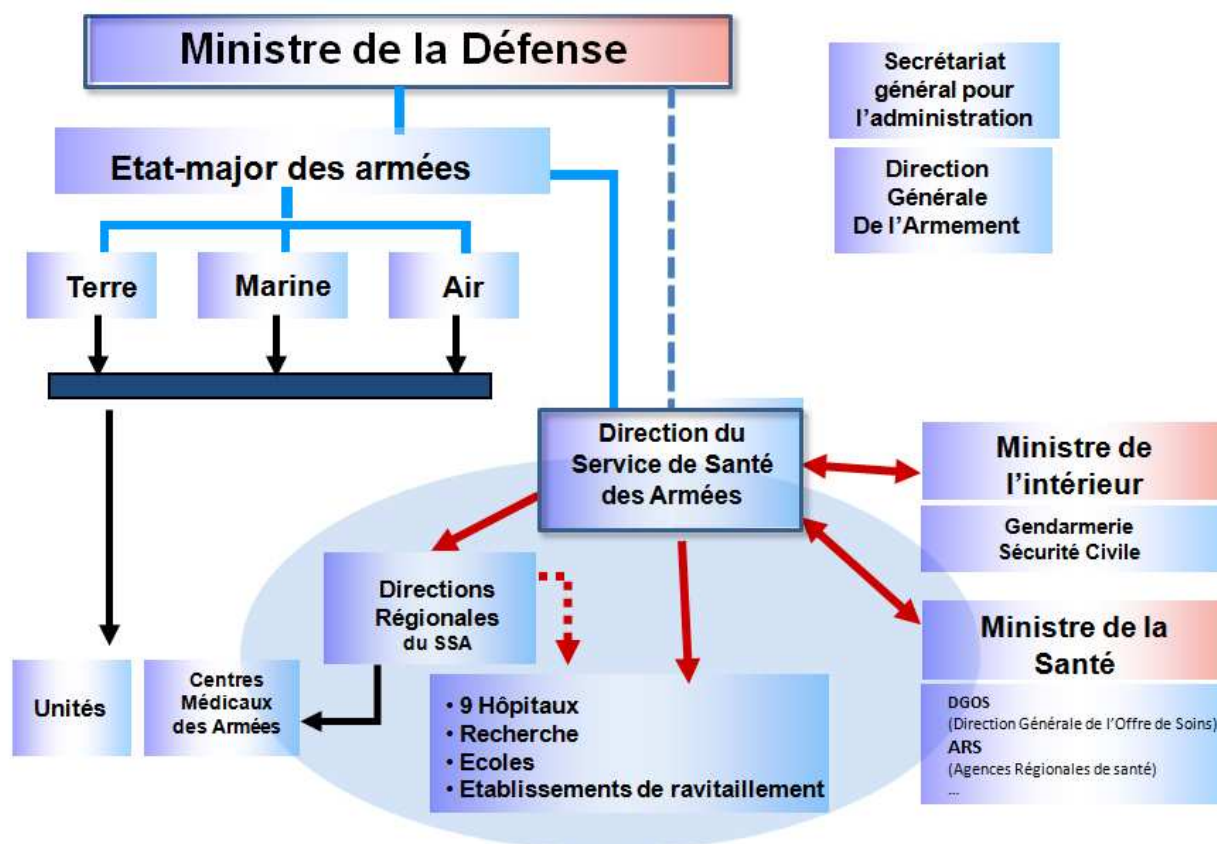
Pour le logiciel sélectionné, une étude détaille ses fonctionnalités, au chapitre 6, avec les outils complémentaires à installer, configurer ou à coder, pour réaliser les contrôles souhaités du SI.

Au chapitre 7, nous détaillons la validation de notre architecture sur une maquette. Ce travail a mis en évidence certaines impossibilités techniques et des compromis ont été négociés pour une meilleure efficacité de l'outil, avant son déploiement en production au chapitre 8. Avant de clore notre étude, nous avons analysé l'organisation mise en place et évalué les résultats techniques du projet. Pour répondre à certains problèmes techniques remontés, nous concluons dans ce dernier chapitre, par des évolutions et des compléments d'amélioration, pour une meilleure maîtrise des Systèmes d'Information du SSA.

1. Service de Santé des Armées et du CeTIMA.

1.1. Service Santé des Armées.

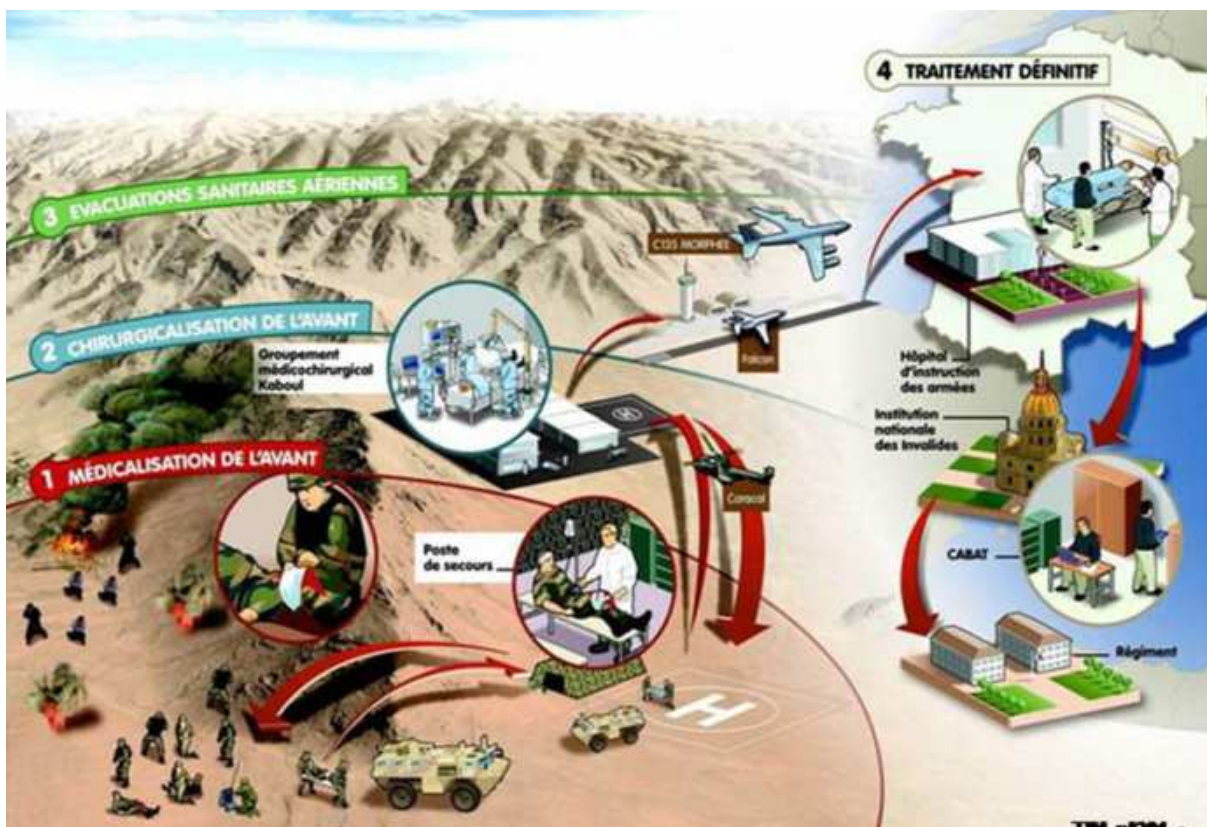
Le Service de santé des armées (SSA) est la structure médicale des forces armées françaises du Ministère de la Défense. Créé sous sa forme actuelle en 1948, le Service de Santé des Armées constitue, depuis 1970, l'un des rares organismes interarmées, qui relève directement du Chef d'Etat Major des Armées (CEMA).



Il a pour mission d'assurer aux armées une couverture complète de l'ensemble de la chaîne sanitaire, de la médecine préventive aux soins immédiats, à l'hospitalisation et au suivi des patients, pour les personnels militaires et civils du Ministère de la Défense et de la Gendarmerie (Ministère de l'Intérieur), en métropole, outre mer et en OPérations Extérieures (OPEX). Il constitue un élément essentiel du dispositif militaire, pour toute opération requérant la présence de moyens sanitaires adaptés (par exemple lors de la guerre du golfe où sur place, 10 % des effectifs totaux engagés provenaient du SSA, comme en Afghanistan avec 300 militaires sur 4000 effectifs déployés).

Le « livre blanc », fixe les objectifs en matière de défense nationale, avec la possibilité de déployer 35 000 hommes, dans le cadre d'une ou de plusieurs opérations, menées hors du territoire national. Le service de santé serait chargé d'apporter un support médical à 700 blessés éventuels par jour.

Pour remplir cette mission de soutien médical hors de France, en temps de crise ou de guerre, le SSA doit disposer de structures et d'effectifs propres sur le territoire national, afin de garder à sa disposition des moyens humains au statut adapté, en effectif suffisant et détenteurs de compétences à jour.



Exemple soutien SSA : sur-le-champ de bataille, au poste de secours mobile ou section chirurgicale modulaire, rapatriement avec l'avion médicalisé Morphée, dans les HIA avec le soutien SSA (ravitaillement sanitaire, administration...)

Le SSA assure une mission de service public, avec l'ouverture de ses 9 Hôpitaux d'Instruction des Armées (HIA) au monde de la santé publique. Ce rôle permet d'assurer un volume d'activité suffisant pour maintenir et développer les compétences des équipes médicales nécessaires au soutien des forces et de générer des ressources financières au travers des soins dispensés aux assurés sociaux.

Cette activité d'hôpitaux de proximité a une capacité totale de 3200 lits, (2% de la capacité publique d'hospitalisation, taille équivalente au CHU de Toulouse). Les 8500 personnels affectés, dont 700 médecins, assurent 560000 journées d'hospitalisation par an, avec 15% de patients d'origine militaire. Les établissements hospitaliers répondent aux certifications et normes des organismes de Santé publique. Par ailleurs, le SSA assiste la Sécurité Civile, pour toute gestion de crise potentielle (catastrophe naturelle, épidémie de grippe...)

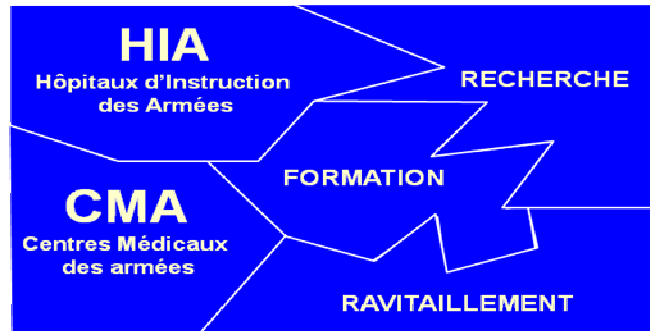
A la tête du SSA, la Direction Centrale du Service de Santé des Armées (DCSSA), dispose de divers établissements qui lui sont hiérarchiquement rattachés.

Si l'essentiel des effectifs est employé dans les organismes du service (neuf hôpitaux, deux écoles, un établissement de recherche et ses deux annexes, six directions régionales et des services de logistique médicale), la moitié des médecins militaires servent dans des unités et dépendent hiérarchiquement du commandement. Ils sont compétents en matière de soins, d'aptitude médicale et d'expertise, de prévention, d'enseignement et de recherche dans les domaines médicaux, paramédicaux, pharmaceutiques et vétérinaires.

En 2011, pour accomplir l'ensemble de ses missions, le Service de Santé des Armées emploie 16 000 personnes, dont les deux tiers sont des personnels militaires, avec 1 860 médecins et 10 610 infirmiers.

Son budget est actuellement évalué à 1.3 Milliards € par an, dont 900 Millions du Ministère de la Défense et 400 Millions pour les produits des activités hospitalières.

Le Service de santé des Armées est organisé en 5 composantes :

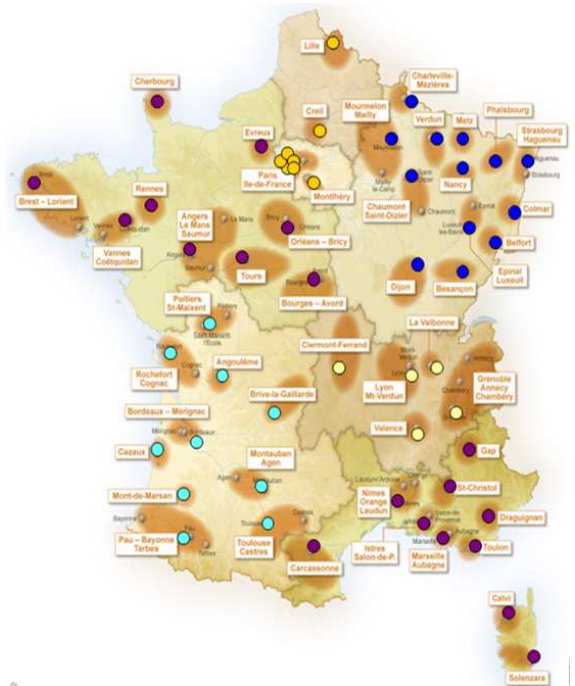


A - Médecine d'Unité pour le soutien des forces

Le Centre Médical des Armées (CMA) constitue la structure élémentaire chargée du soutien direct des formations des trois armées (Terre/Air/Mer) et de la Gendarmerie. Piloté par les Directions Régionales du Service de Santé (DRSSA), il assure le soutien médical de proximité au profil du personnel militaire et civil des Bases De Défense (BDD) : soins courants, médecine préventive, contrôle de l'aptitude à l'emploi... Les personnels des CMA sont susceptibles d'être projetés en opérations extérieures pour assurer les missions médicales de terrain.

Il existe 55 CMA en métropole, sous l'autorité de 6 Directions Régionales (DRSSA).

Nota : Le Système d'Information utilisé dans les CMA est le Système d'Information des Services Médicaux d'Unités (SISMU)



B - Activité Hospitalière

Dans le prolongement et en complément des CMA, les Hôpitaux d'Instruction des Armées (HIA) ont pour mission prioritaire le soutien des forces en leur offrant des soins médicaux spécialisés et des moyens d'expertise performants. Ils reçoivent les militaires blessés rapatriés des théâtres d'opérations extérieures. Le parc hospitalier militaire regroupe 9 HIA en France, et un Centre Hospitalier des Armées (CHA) à Djibouti.

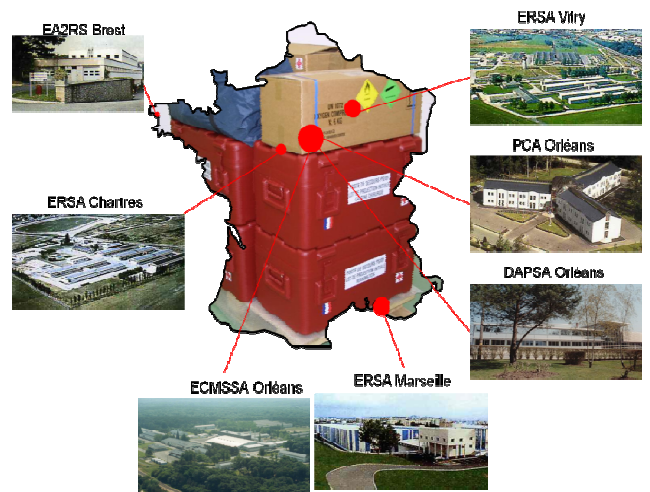
Nota : Le Système d'Information utilisé dans les HIA est le Système d'Information des Hôpitaux (SIH)



C - Le Ravitaillement

Le SSA assure le ravitaillement sanitaire en approvisionnements nécessaires au fonctionnement des CMA, des HIA et des formations médicales de soutien opérationnel. Ces approvisionnements, essentiellement constitués de médicaments, d'articles pharmaceutiques et de matériels techniques médicaux-chirurgicaux, permettent de traiter les malades et les blessés en temps de paix, comme en temps de crise ou de guerre. La pharmacie centrale d'Orléans est une unité de production pharmaceutique de type industriel et fabrique des médicaments spécifiques aux besoins des armées.

Nota : Le Système d'Information utilisé dans les établissements de ravitaillement est le SIRAV (application GMAO de Carl Master)



D- La Recherche

La recherche du SSA, qu'elle soit fondamentale, appliquée ou clinique est directement liée au soutien des forces. Elle a pour but l'amélioration de la prévention, de l'assistance et des soins apportés aux militaires. Regroupé prochainement à Brétigny sur Orge, l'Institut de Recherches Biomédicales des Armées (IRBA) étudie dans différents domaines comme les risques NRBC (Risques Nucléaires, Radiologiques, Biologiques et Chimiques), la télémédecine, les soins médico-chirurgicaux en opérations, la maîtrise de la capacité opérationnelle du combattant en milieu hostile ...



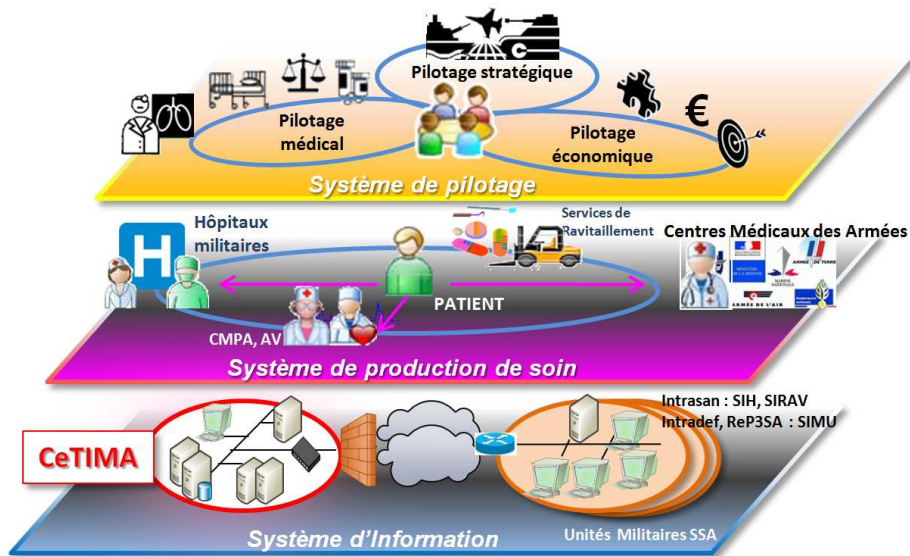
E- La Formation

Le SSA est responsable de la formation initiale et continue de son personnel. L'Ecole de Lyon assure la formation technique et militaire des élèves officiers médecins, pharmaciens, vétérinaires et chirurgien-dentistes, en complément de l'enseignement dispensé par les universités de ces deux villes. L'Ecole du Val de Grâce à Paris est chargée du suivi pédagogique du 3^{ème} cycle des études médicales, adapté à l'environnement militaire opérationnel terrestre, maritime ou aéronautique. L'Ecole du Personnel Paramédical des Armées de Toulon prépare au diplôme d'état les futurs infirmiers, destinés à servir dans les trois armées et de la Gendarmerie.

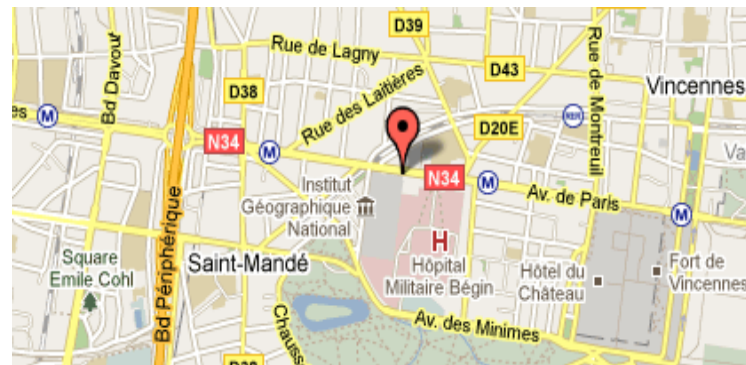


2.2. Le Centre de Traitement de l'Information Médicale des Armées (CeTIMA).

Le Centre de Traitement de l'Information Médicale des Armées (CeTIMA) est le centre informatique national, qui héberge l'ensemble des plateformes nationales des Systèmes d'Information du SSA. Situé à Paris, cet établissement regroupe également les chefs de projets fonctionnels, chargés des études concernant la mise en œuvre des applications médico-administratives, autour du dossier patient, pour les systèmes de production de soin et de pilotage du SSA.



Il est implanté dans l'enceinte de l'Hôpital d'Instruction des Armées Bégin, à Saint-Mandé, en bordure du bois de Vincennes.



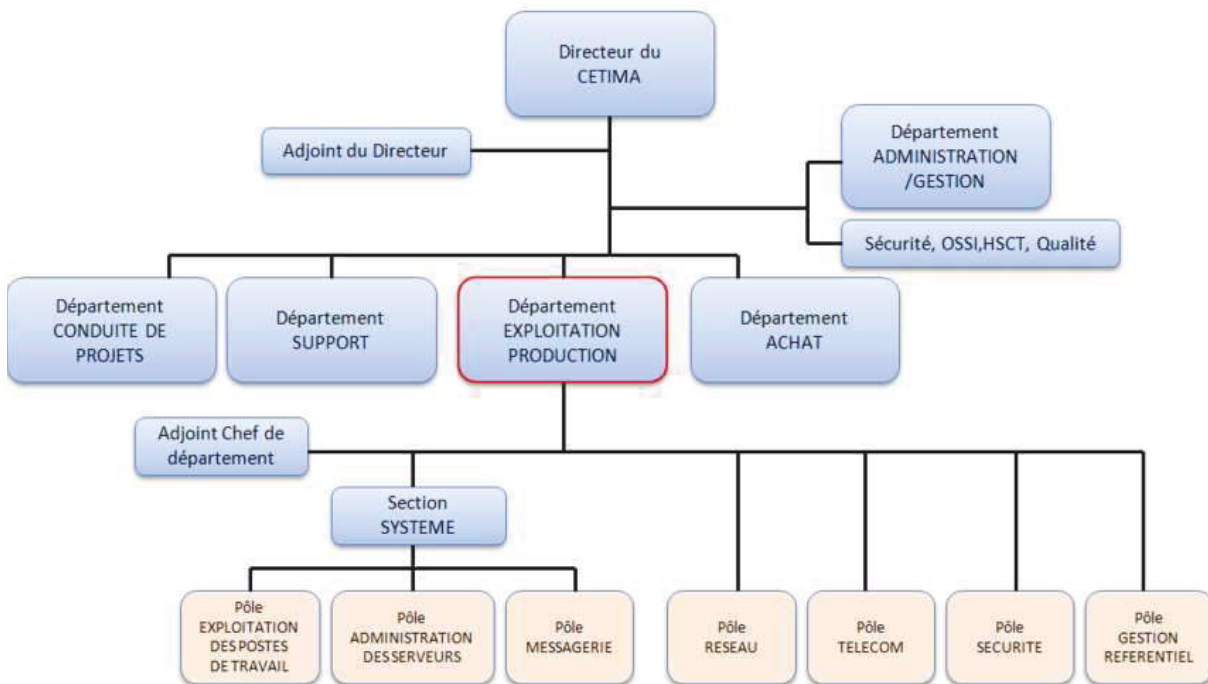
Le CeTIMA est un organisme de la logistique santé, directement subordonné à la Direction Centrale du Service de Santé des Armées (DCSSA).

Il a pour mission de :

- Conduire les projets informatiques (étude et mise en œuvre des applications médico administratives) ;
- Assister la DCSSA pour l'élaboration du schéma directeur informatique ;
- Gérer les crédits consentis par la DCSSA ;
- Soutenir les utilisateurs de l'informatique du SSA ;
- Gérer les Systèmes d'Information du SSA ;
- Gérer la réserve ministérielle informatique ;
- Réaliser la passation des marchés informatiques et le suivi des achats.

L'effectif moyen du CeTIMA se situe autour de 80 personnels militaires et civils, dont 85% de techniciens.

Il est organisé en différents départements, avec en particulier le département Production/Exploitation, dirigé par le LCL Champion, qui est le tuteur entreprise de ce mémoire CNAM.



2. Le projet de supervision.

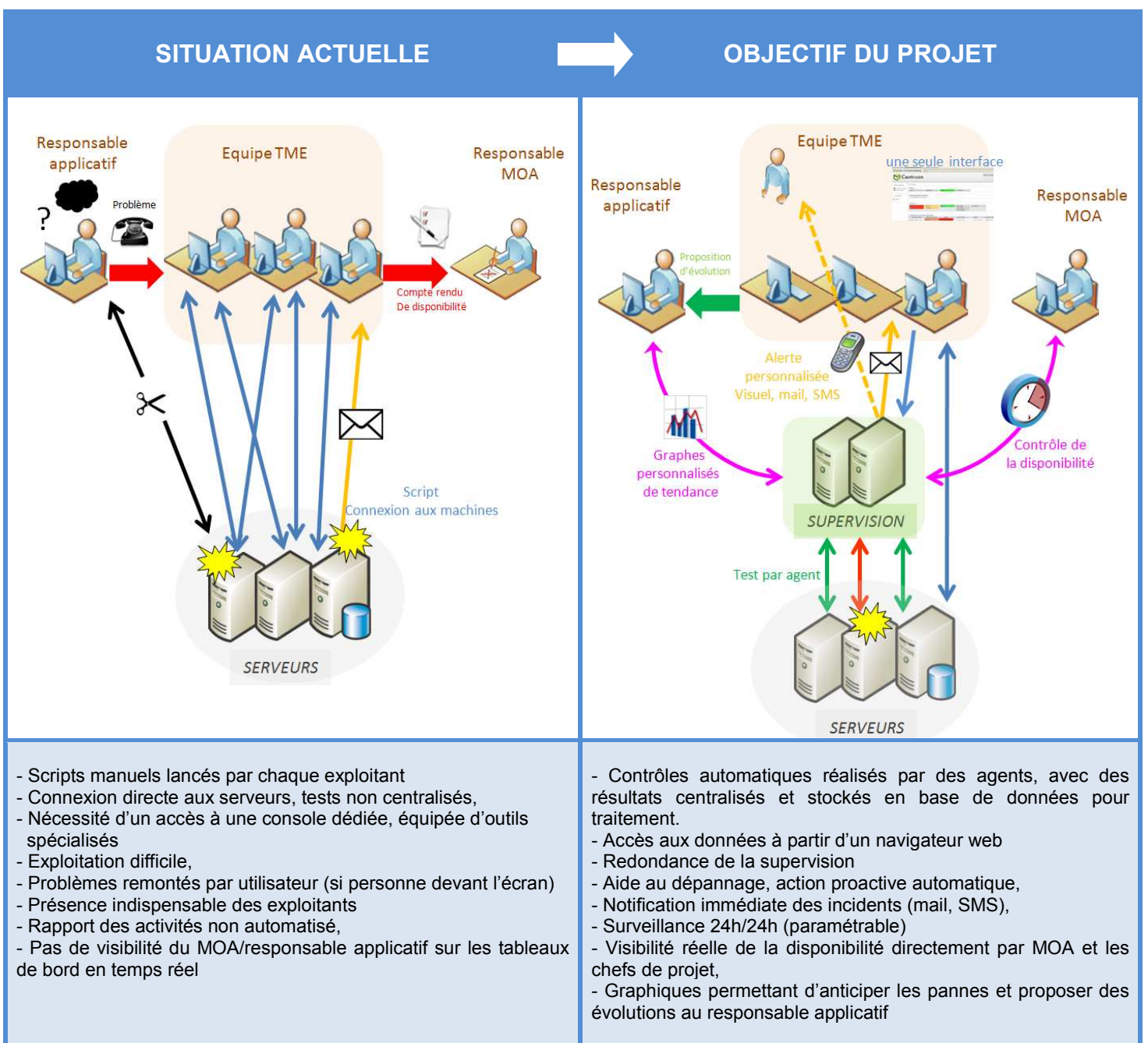
2.1. Objectifs, Enjeux

Comme indiqué précédemment, les Systèmes d'Information du SSA hébergés au CeTIMA nécessitent une disponibilité sans faille. Le chef du département « exploitation-production » du CeTIMA est le MOA (Maitre d'Ouvrage) de ces projets d'infrastructure et le responsable de leur bon fonctionnement...

Aussi fin 2010, un contrat de sous-traitance a été signé avec la société BULL pour assurer l'exploitation de ces plateformes. Trois personnes, composant l'équipe TME (Tiers Maintenance Applicative), assurent en permanence, sur le site, l'administration et les maintenances préventives/correctives des différents serveurs et équipements installés.

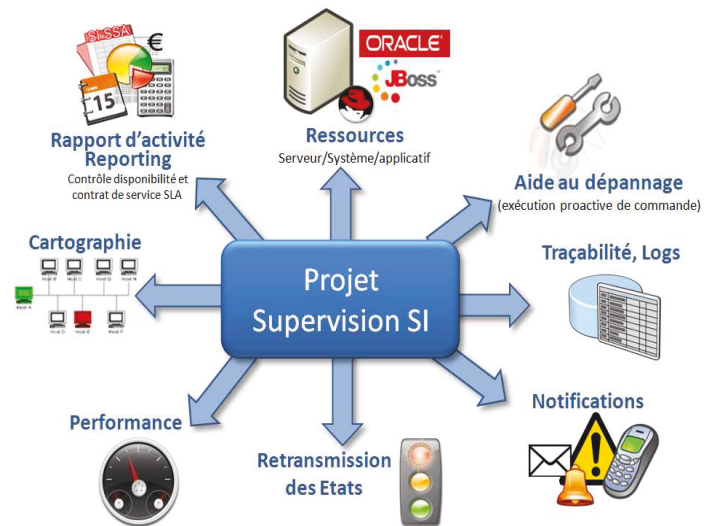
Un contrat est en cours de publication, pour la partie Tiers Maintenance Applicative (TMA).

Sous le contrôle du MOA, le projet proposé consiste à étudier et fournir à l'équipe TME, un outil de supervision centralisé, permettant d'optimiser l'organisation actuelle et de contrôler les objectifs contractuels de disponibilité.



Le projet consiste donc à :

- Etudier les Systèmes d'Information à monitorer, les matériels, les technologies et les processus mis en œuvre ;
- Identifier et proposer des indicateurs à surveiller, considérés comme sensibles, par les responsables applicatifs, sur les différentes plateformes;
- Définir un cahier des charges répondant aux nouveaux besoins organisationnels de supervision: surveillance automatique du SI, stockage des états, notification en cas d'anomalie, dépannage plus facile, courbe d'évolution, visibilité des disponibilités par le MOA et les chefs de projet ...;
- Suivant les contraintes imposées (techniques, financière, calendaire), définir une solution technique adéquate ;
- Après maquettage, mettre en œuvre cette solution sur les plateformes opérationnelles ;
- Former les personnes de la TME, à ces nouveaux outils.



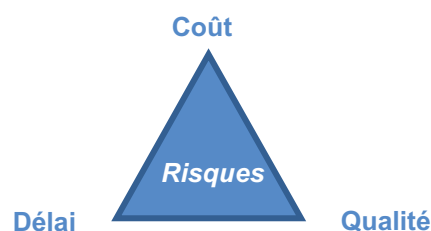
Les enjeux de ce projet sont donc doubles :

- Technique, dans un domaine informatique en pleine évolution ;
- Financier, car la mise en place de cette plateforme, permettra un gain de productivité pour l'exploitation des SI et un atout pour renégocier le contrat de service en fin d'année 2011

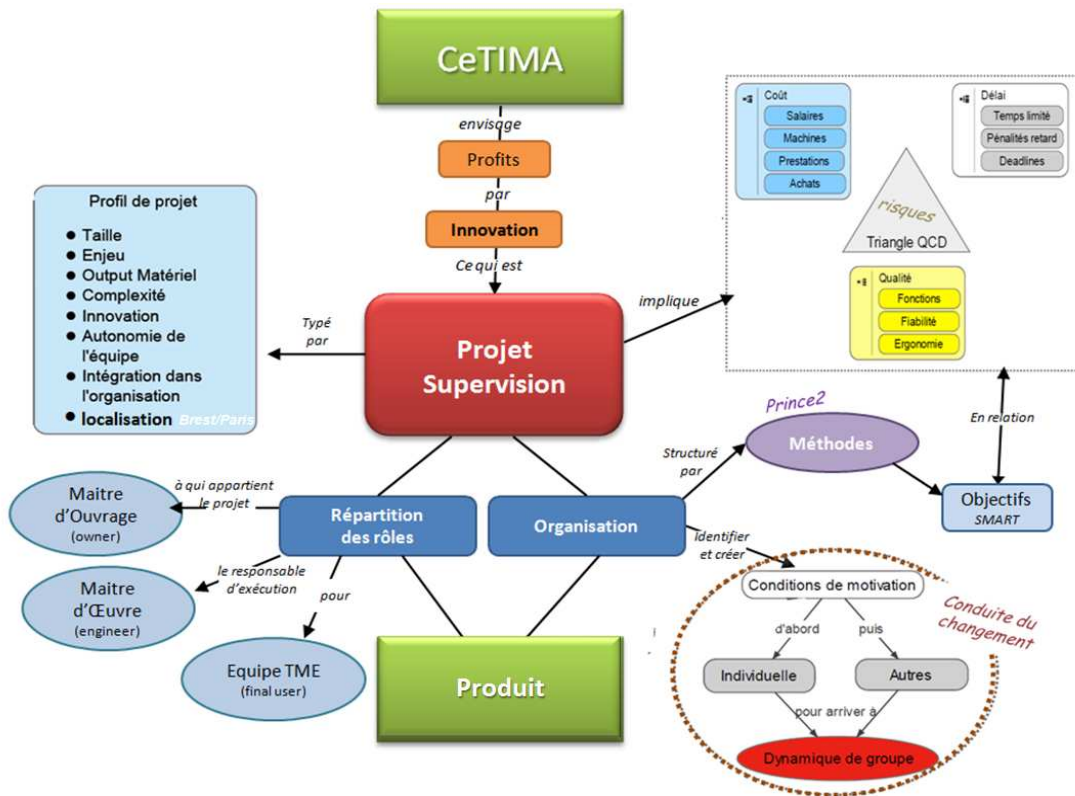
2.2. Organisation du projet.

Le projet a débuté par une réunion de lancement, le 19/04/2011 [CCR-CETIMA-SUPERV], avec une présentation générale du projet (objectifs/périmètre), des contraintes générales (coût, délai, contraintes d'organisation...) et des livrables attendus.

L'ensemble de la démarche retenue pour le projet s'appuyait sur un compromis validé par le groupe de pilotage entre les coûts, les délais et la qualité optimale, pour atteindre les objectifs, en minimisant les risques de dérive sur le projet.



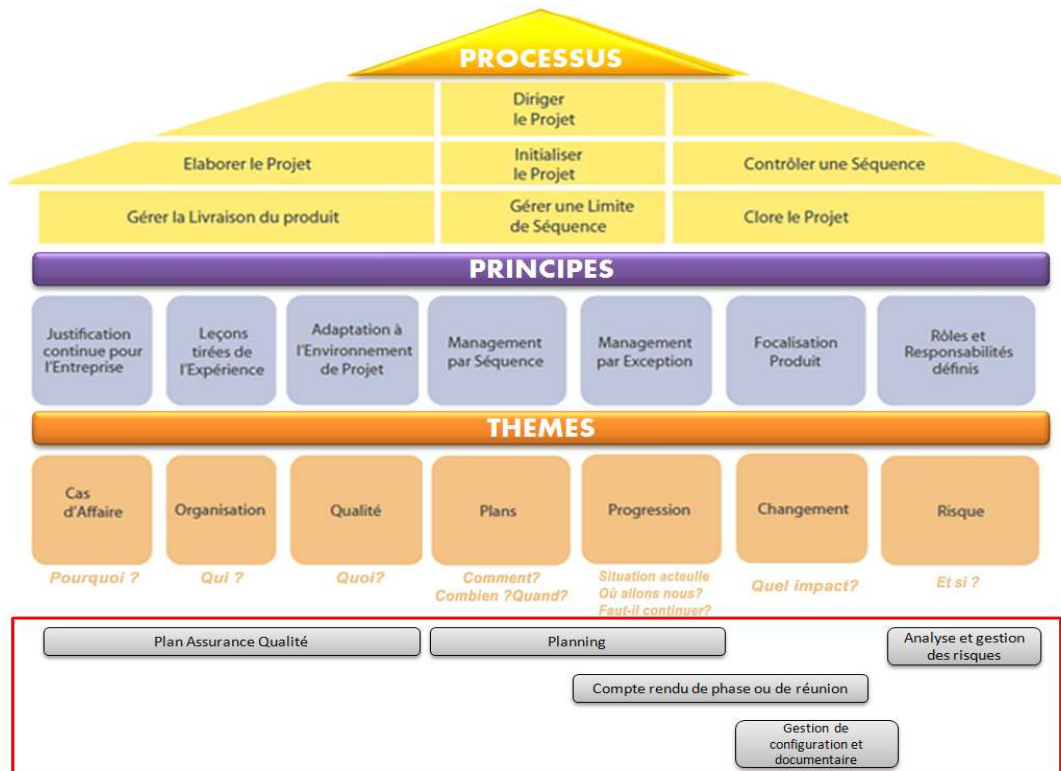
Pour la mise en place de l'organisation et la gestion du projet, aucune méthode n'était imposée. Nous avons souhaitée avoir une approche standard de gestion de projet. Parmi les nombreuses méthodes du marché (MPMM, PMBOK...), nous avons retenu Prince2 (PProjects IN Controlled Environments) pour son approche simple, générique et flexible, sa facilité à s'implémenter et sa convergence avec la gestion de services ITIL, utilisée au Ministère de la Défense (voir paragraphe 3.3.3). Intégrant déjà les bonnes pratiques éprouvées et établies du monde industriel, elle permet d'avoir un langage commun, avec des thèmes et des processus prédéfinis, couvrant l'ensemble du spectre d'une bonne gestion de projet. De plus, son choix est pertinent pour son organisation orientée client/résultat, avec un focus sur les livrables. Avec un découpage en phase, ce management « par exception » permet un gain de temps indéniable et est parfaitement adapté à notre fonctionnement distant imposé.



En partant du contexte de notre projet, schématisé ci-dessus, nous avons adapté cette méthode à notre environnement, sans modifier la philosophie générale.
 Pour faciliter la diffusion des documents, des processus et des composants ont été regroupés par livrables importants (figure suivante) :

- Plan d'Assurance Qualité [PAQ-SUPERV-NP]
- Gestion de configuration [CONF-DOC-SUPERV-NP]
- Analyse des risques [RISQ-SUPERV-NP]
- Planning du projet [PLAN-SUPERV-NP]

PRINCE2



Organisation
Projet

Rien dans la méthode n'a été supprimé, pour garantir un niveau de gouvernance, de contrôle et de planification optimal et surtout faciliter un retour d'expérience, en fin de projet.

2.2.1 La Qualité

Nous avons proposé un Plan d'Assurance Qualité [PAQ-SUPERV-NP] pour valider l'organisation retenue (responsabilité, réunion, suivi), la méthode (description des phases d'étude et de réalisation) et les outils utilisés, pour contrôler et assurer la qualité, tout au long du projet.

Définition des Rôles et missions

La première tâche a été de définir et valider les rôles et les fonctions des différents intervenants dans l'organisation du projet : MOA Maitrise d'OuvrAge (tuteur d'entreprise), MOE Maitrise d'Œuvre (moi-même et l'Equipe TME).

Un comité de suivi et de pilotage a été nommé pour :

- suivre l'avancement des travaux, dans le respect des échéances et contraintes du projet.
- décider les grandes orientations du projet
- redéfinir de nouveaux objectifs en cas de problèmes fonctionnels/techniques ou risques identifiés

Planification des réunions et suivi des changements

Les principaux acteurs du projet et les plateformes SI étant sur Paris, avec l'étude réalisée à Brest. La stratégie initiale a été de programmer des réunions régulières de suivi, tous les 15 jours par visioconférence (le lundi après midi), avec comme support de travail, un document PowerPoint diffusé peu avant la réunion. Par ailleurs, des réunions de travail ponctuelles à Paris étaient définies avec l'équipe TME, pour les transferts des compétences techniques des SI métiers. Elles étaient suivies d'un compte rendu rédigé dans les 5 jours, pour validation, avant leur exploitation dans les études et les développements. Ces jalons étaient aussi l'occasion d'assurer la conduite de changements, qui pouvaient être de trois types : changement d'une condition ou d'un produit, modification de la spécification ou questions. Les problèmes ou les incidents rencontrés, avec la mesure de leur impact sur le projet étaient signalés, ainsi que des propositions de solutions palliatives.

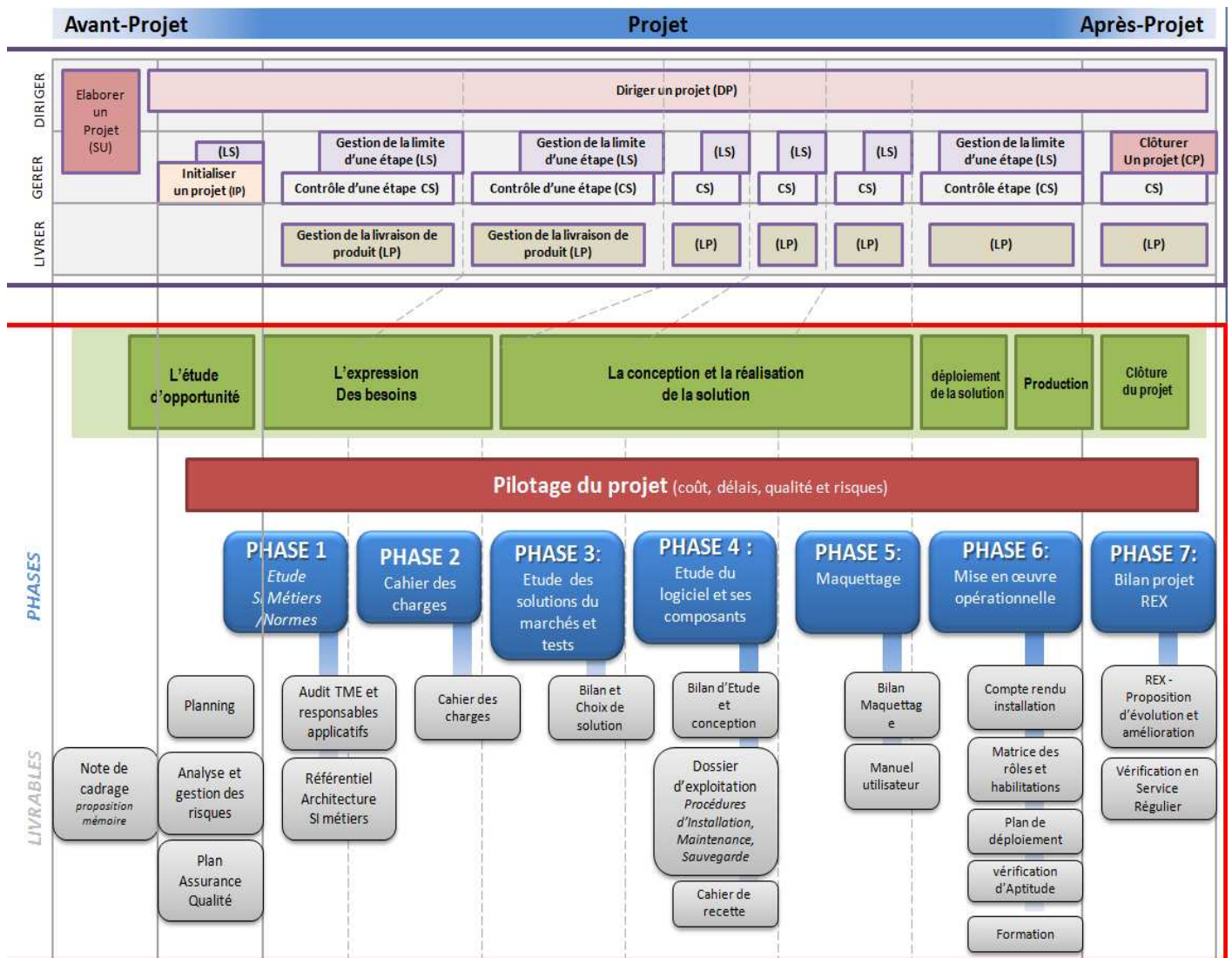
Après discussion, ces compromis étaient validés et consignés aux comptes rendus. Les changements les plus importants sont listés au paragraphe 7.3, après la phase maquettage.

Phases « Projet » retenues

Une nouvelle fois en s'inspirant de la méthode Prince2, nous sommes arrivés à l'organisation projet suivante avec 7 étapes de projet et les livrables associés. (Voir schéma de la page suivante)

Ces 7 phases sont :

- 1 – Etude des SI métiers
- 2 – Définition du cahier des charges fonctionnel
- 3 – Etude des solutions du marché et choix du logiciel de supervision
- 4 – Etude du logiciel et développement de ces composants
- 5 – Maquettage
- 6 – Mise en œuvre sur les plateformes opérationnelles
- 7 – Bilan Projet : Retour d'Expérience, Propositions d'évolution et d'amélioration



Contrainte SSI : Gestion documentaire adaptée

Une contrainte importante de sécurité a été imposée : la non divulgation à l'extérieur du SSA du plan d'adressage IP et du nommage des serveurs. En plus du suivi des livrables et de la traçabilité des modifications, la gestion de configuration (documentaire et logicielle) a donc été adaptée pour répondre à ce degré de confidentialité.

Règle de nommage de la documentation

une **fonction** (CR Compte rendu, PV Procès Verbal, BL Bordereau de Livraison, PAQ...)

le **nom du projet** : SUPERV (Supervision)

un **degré de classification** de sécurité :

DR Diffusion Restreinte, uniquement diffusable au sein du SSA

NP Non Protégé et diffusable au sein du SSA et au CNAM

MD MoDifié pour le CNAM, afin de faire disparaître les paramètres spécifiques de l'architecture SSA, qui sont des données sensibles au sein du Ministère de la Défense

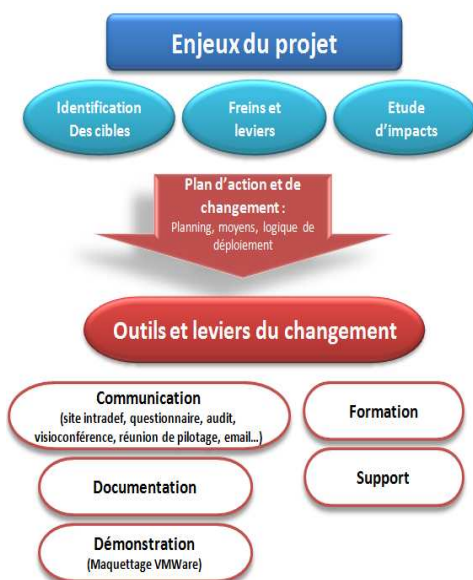
Une **version** sous la forme X.y (1.0 pour la version initiale). A partir de l'état approuvé, toute modification mineure entraîne une évolution du y; toute modification majeure entraîne une évolution du X, avec un retour à 0 pour y.

Des outils bureautique communs au projet ont été actés (Office 2003, MS Project 2003) et un outil de communication, sous la forme d'un portail web sécurisée en interne au SSA, pour diffuser et rendre disponible l'ensemble de la documentation du projet.

Conduite du changement

Dès le début de la gestion et du pilotage d'un projet, il faut aussi assurer une conduite du changement, car tout changement majeur ou mineur, qui impacte les personnes, nécessite une phase de préparation. Une conduite proactive doit être élaborée pour les accompagner.

En effet, la mise en place d'un nouvel outil peut déstabiliser les utilisateurs (perte de repère dans les actes de gestion quotidiens, manque de maîtrise des nouvelles procédures, questionnement sur leur devenir...).



Comme le montre le schéma suivant, notre stratégie de conduite du changement était de :

- **Communiquer** clairement, régulièrement (visioconférence régulière avec le MOA et l'équipe TME) et de façon transparente (mise à disposition de l'ensemble des informations sur un portail dédié au projet sous wordpress (outil déjà déployé à la DRSSA Brest, un outil type Zimbra aurait été peut être plus adapté, mais n'était pas compatible avec la configuration du serveur de messagerie lotus).
- **Documenter** l'étude avec un planning, des indicateurs d'avancement à jour.
- **Présenter le produit** avant son déploiement, en s'appuyant sur les travaux de la phase maquettage (démonstration sous VMware)
- **Réaliser des livrables** complets et exploitables, comme support de formation
- **Rester disponible** pour toute question sur le projet (téléphone avec une boîte vocale en cas d'absence, email, possibilité de laisser des commentaires sur le site web du projet)

2.2.2 Les Coûts

Partie « logicielle et matériels informatiques »

Une contrainte forte imposée par le MOA était l'utilisation de produit open source, pour ce projet de supervision. L'ensemble des outils utilisés pendant l'étude était des logiciels courants (suite Bureautique Office Microsoft) ou gratuit (VMWare Server, linux Centos/Ubuntu, version d'évaluation JON, Oracle ...), sur mon PC portable personnel.

Partie « ressources humaines »

La partie étude a été réalisée en grande partie au titre du DIF (Droit Individuel à la Formation), du Compte Epargne Temps et sur les congés. Dans les coûts indirects, il fallait éviter de solliciter de manière excessive les responsables du CeTIMA ou l'équipe TME. Aussi un effort de planification a été réalisé, pour avertir des dates des réunions de pilotage ou de visioconférence, avec un délai raisonnable. Par souci d'efficacité, les audits des acteurs des SI métiers utilisaient si possible des Questionnaires à Choix Multiples rapides et concis. Pour minimiser la partie déploiement piloté par l'équipe TME, une attention particulière a été apportée à une rédaction documentaire détaillée et minutieuse, pour minimiser la durée d'intervention sur Paris.

Partie « coût de fonctionnement »

Un budget personnel pour le transport et l'hébergement sur Paris a été dimensionné et approvisionné (2000€).

2.2.3 Les Délais / Le Planning (Calendrier projet page suivante)

La volonté du MOA était une mise en place de la solution de supervision, avant la fin de l'année 2011, en priorité sur le SI Métier « SISMU ». La contrainte initiale CNAM était la finalisation du rapport de mémoire avant fin octobre 2011, pour une soutenance en décembre 2011. Le planning projet a donc été établi pour chaque phase projet, pour répondre aux contraintes CeTIMA et CNAM, avec un pilotage complémentaire, pour le suivi de la rédaction du mémoire CNAM. (planning transmis tous les 3 semaines, au tuteur CNAM, avec comme livrable, le chapitre associé du mémoire).

Avec un démarrage en avril 2011, les différentes phases d'étude et de conception se sont succédées, sans trop de difficultés, avec des revues de phases régulières, jusqu'à l'été, où les logiciels retenus furent étudiés en détails, avec le développement des agents spécifiques. L'ensemble fut maqueté jusqu'à mi-septembre, avec un investissement important dans l'étude et l'installation des produits Oracle, JBoss et JON, dans un environnement VMWare, avec un début de mise en œuvre, sur les plateformes de production, planifié en octobre 2011.

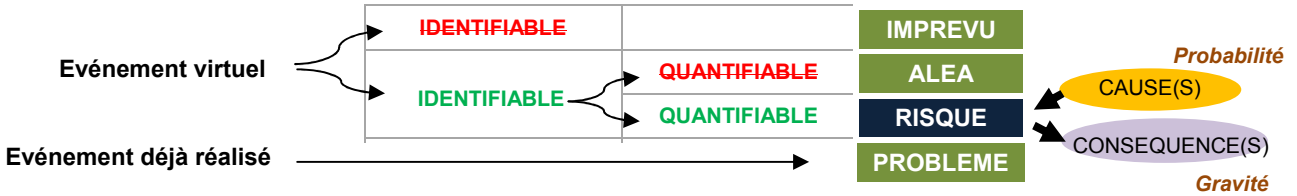
Néanmoins, un aléa non identifié, dans les risques analysés au chapitre suivant, a bouleversé l'organisation du projet et ses missions. En effet, il était imposé d'avoir l'UV d'anglais avant de pouvoir soutenir le mémoire. Dans un premier temps, j'ai décidé de continuer normalement de concert le déroulement du projet et les révisions d'anglais. Malheureusement après 3 voyages et tests au British Council de Paris, il fallut admettre l'échec (à... 2 points près sur 100) et l'impossibilité de soutenir en fin 2011. Aussi un nouveau planning a été renégocié avec le MOA et les ressources humaines du Ministère de la Défense, dans un contexte de changement d'employeur (DIRISI) en 2012.

Cet incident et l'analyse des conséquences sur le projet sont développés dans la partie retour d'expérience du chapitre 9.

2.2.4 Les Risques

Un dispositif de maîtrise des risques a été demandé par le MOA, pour identifier les principaux risques et mettre en place des actions adaptées pour le bon déroulement du projet.

Par définition, un risque est un événement potentiel indésirable, plus exactement un événement dont l'apparition n'est pas certaine, mais dont la manifestation est susceptible d'affecter les objectifs du projet. Il est normalement identifiable et quantifiable.



L'événement incriminé a une cause (avec une **Probabilité** qu'elle arrive) et des conséquences (avec une **Gravité d'impact** sur le projet)

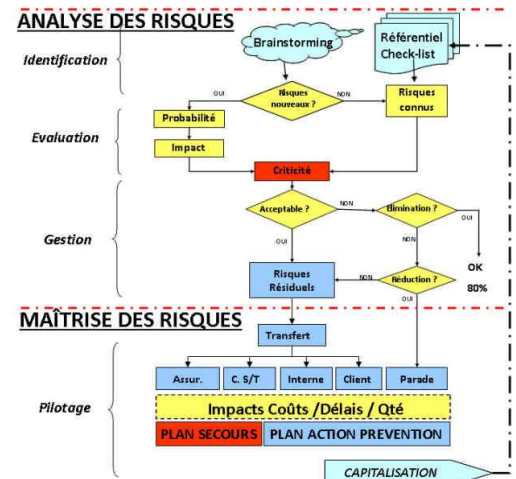
Les risques peuvent être classés en différentes catégories : stratégique (liés au fait de faire ou pas faire le projet), décisionnel, industriel, technologiques, contractuels, financiers, politiques, sociaux et réglementaires. Un management des risques permet de se préparer, de réagir rapidement, de saisir les opportunités ou de réduire l'exposition.

Méthode utilisée

De nombreuses méthodes d'analyse des risques existent: AMDEC, APR, HAZOP, EBIOS, MELISA, MEHARI ..

La méthodologie générale est souvent la même :

- **IDENTIFIER** les risques ;
- **QUANTIFIER** la criticité du risque avec le couple (probabilité ; gravité) ;
- **DETERMINER DES ACTIONS** soit **DE PREVENTION** (pour réduire la probabilité d'occurrence : audits, déléguer, supprimer la cause) soit **DE PROTECTION** (pour réduire l'impact du risque avéré : diversifier les sources, redonder, plan B) ou **DE VIGILANCE** (pour augmenter la détectabilité de mon risque) ;
- **SUIVRE** et contrôler la mise en place de ses moyens ;
- **CAPITALISER** pour faire profiter les autres projets de notre expérience : documenter les risques, les causes, les résultats obtenus...



L'objet du projet n'était pas de réaliser une étude longue et détaillée avec d'une méthode normative complexe, mais d'identifier rapidement les risques majeurs, dans un minimum temps et de mettre un plan d'actions appropriées.

Aussi nous avons utilisée la méthode fournie par le gouvernement québécois, ou plus exactement par la Direction Générale des Solutions d'Affaires en Gestion Intégrée des Ressources DGSAGIR, (organisme pilotant les projets SI du Gouvernement du Québec), Dans cet outil, chaque danger a la même probabilité (et donc criticité) et seuls les indices de gravité 4&5 demandent un plan d'action. Mais son bilan rapide donne directement une très bonne visibilité sur les risques à contrôler, avec un questionnaire de 60 questions sous format de macro Excel, à l'intention des responsables informatiques. Ce processus est facilement rejouable en cours de projet pour réévaluer les risques. Adapté à l'environnement SSA et aux différents acteurs du projet, notre document d'analyse des risques **RISQ-SUPERV-NP**, disponible en annexe 19, a permis d'identifier les risques potentiels ou les facteurs critiques de notre projet.

Bilan de l'étude des risques

Après avoir répondu en groupe au questionnaire, nous arrivons au tableau de conclusion suivant :

Graphique des risques par zone de risques				
Ensemble du projet moyenne : 2.2				
1	2	3	4	
Zone de risques : Environnement du client moyenne : 2.09				
Zone de risques : Envergure du projet moyenne : 1				
Zone de risques : Impacts sur les affaires moyenne : 2.4				
Zone de risques : Caractéristiques de l'application moyenne : 2.2				
Zone de risques : Caractéristiques du projet moyenne : 2.29				
Zone de risques : Organisation du projet moyenne : 2.13				
Zone de risques : Équipe de projet moyenne : 2.25				
Zone de risques : Environnement de développement moyenne : 2.17				
Zone de risques : Technologies utilisées moyenne : 3				
Mineur	Significative	Sévère	Critique	Catastrophique

Le traitement du fichier a fait ressortir 7 éléments sensibles, pour lesquels un plan d'action et un responsable ont été définis :

Extrait document projet : Analyse des risques [RISQ-SUPERV-NP]

Catégorie du risque	Question	Criticité (1 à 5)	Plan d'action	Responsable
Environnement client	Q3 - Degrés d'importance pour le MOA	4 (Application stratégique)	Pilotage : -Rédiger un Plan d'Assurance Qualité du projet -Réaliser des mises à jour régulières des documents projet. -Faire remonter rapidement tout problème bloquant	MOE
Environnement client	Q8 – Temps et disponibilité du MOA et des équipes du CeTIMA	4 (faible disponibilité, car les personnes d'abord assurer leur missions quotidiennes)	Pilotage : -Réaliser les audits avec des QCM pour gagner du temps. -Consultation du planning/livrable/avancement du projet consultable 24h/24h sur un site intranet. -Réaliser des documents synthétiques PowerPoint comme support de travail, avant les réunions de pilotage - Prévenir et confirmer 15 jours à l'avance la visioconférence ou la réunion de travail	MOE
Environnement client	Q11-Probabilité d'un changement d'instance politique	4 (Très forte probabilité : transfert en cours du MOE du SSA vers DIRISI)	Verrouillage administratif -Acter par écrit du processus projet et de son calendrier actuel par les instances supérieurs du SSA (CMG Brest, représentant du personnel, compte rendu AMR...) -Valider avec MOA/CNAM des impacts d'un report éventuel de la soutenance en juin au lieu de décembre -Préparer la prolongation éventuelle du Congés Individuel de Formation.	MOE
Caractéristique de l'application	Q25 - Interfaces avec d'autres systèmes	4 (plusieurs applications mise en œuvre)	Référencement : Définir clairement la liste des applicatives mises en œuvre et des contacts correspondants au CeTIMA, avant de les auditer.	MOE
Equipe de projet	Q39 - Lien de communication entre les acteurs du projet	4 Distant : MOE sur un site non proche (Brest) du MOA et Equipe TME, qui sont sur Paris	Information / pilotage: - Réaliser régulièrement des réunions de pilotage (visioconférence tous les 15 jours) et réunion de travail sur Paris - Définir un budget personnel hébergement/ transport (2000€) - Mettre en place des outils de communication complémentaire : site intranet collaboratif pour diffuser/échanger l'information, échange par messagerie internet ou téléphonie mobile en cas de coupure des communications institutionnelles, mise en place d'un répondeur téléphonique en cas d'absence - Documenter au maximum le projet, pour avoir un support pour une reprise du projet par un nouvel MOE, démarche vérifiée à chaque revue de phase	MOE MOE
Equipe de projet	Q45 – Connaissance des logiciels de supervision	4 (faible connaissance des outils de supervision)	Formation : Réaliser une étude approfondie des produits du marché (livre, internet...) et analyser en détail le fonctionnement de chacun	MOE
Technologies utilisées	Q57 – Mélanges de diverses composantes technologiques	4 (multiples technologies : oracle, JEEE, apache...)	Formation : Se documenter, étudier ces technologies Les tester sur plateforme pour parfaitement les maîtriser	MOE

2.3. Concepts de la supervision

Avant de rentrer dans le vif du sujet, il convient dans ce chapitre, de donner les définitions et des notions de la supervision, pour avoir un langage commun et lever quelques approximations parfois constatées sur certains sites internet.

Définitions

SUPERVISION :

Surveillance du bon fonctionnement d'un système ou d'une activité,
ou Surveiller, rapporter et alerter les fonctionnements normaux et anormaux.

METROLOGIE

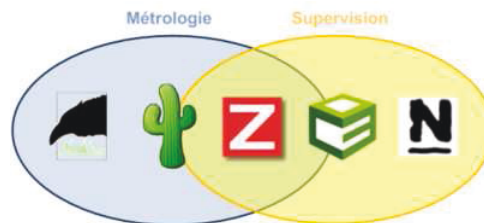
Opération qui consiste à donner une valeur numérique à une grandeur.

Bien que leur but soit différent, comme montre le tableau ci-dessous, ces deux notions sont souvent confondues et complémentaires. On utilise souvent le terme anglais **MONITORING** pour recouvrir les deux domaines.

SUPERVISION	METROLOGIE
Etat	Donnée de performance
Résultat Numérique (0,1, 2,3)	Résultat analogique (1.5/ %..)
Traitement à l'Instant T	Traitement dans la durée
Orientée service	Orientée précision
Diagnostic/dépannage	Anticipation/Evolution
Tableau de bord	Graphique
Changement d'état	Evolution dans le temps



Certains produits se sont spécialisés dans un domaine, d'autres essayent de couvrir l'ensemble du besoin.



Sans rentrer tout de suite dans les détails, les solutions de supervision et de métrologie vont souvent de paire, car dans la majorité des cas, les deux fonctionnalités doivent être associées, pour répondre aux demandes des exploitants

Exemple : -*Supervision* : pour tester le bon fonctionnement d'un service fourni par un serveur

-*Métrologie* : pour savoir le nombre d'utilisateurs qui utilisent ce service

Le processus final **REPORTING** consiste ensuite à utiliser les résultats de la supervision et de la métrologie pour générer des rapports de synthèse, qui sont une aide à la décision, pour le contrôle et la gestion du changement des SI.

Fonctionnement / Objectifs

La chaîne de supervision est constituée de 4 phases :

- **COLLECTER** les données avec un ciblage (quoi mesurer, fréquence, granularité, précision), avec l'acquisition (mesure active/passive) et le stockage (au bon format) ;
- **ANALYSER** les résultats recueillis (extraction, filtrage, synthèse) ;
- **ACTION** (automatique) : Suite à l'analyse, suivant les critères, une notification visuelle /sonore/ email/ SMS ou des actions correctives (coupe pare-feu, vidage cache...) sont réalisées.
- **PILOTAGE**, qui correspond aux actions de l'opérateur : tableaux de bord, recherche de traces dans les logs, acquittement d'une alarme, action corrective...

La supervision a différents rôles, pour répondre aux besoins toujours plus grands, exigés de performance et de qualité :

- Avoir une disponibilité et une accessibilité des outils de l'entreprise, pour garantir la productivité.
- Assurer un fonctionnement 24h/24 et 7j/ 7 (en théorie, voir schéma ci-dessous)
- Avoir une visibilité du SI et remonter des informations permettant son pilotage (performance réelle par rapport aux objectifs attendus, respect contra de service SLA...) et son évolution (coût maintenance, augmenter les ressources....)
- Anticiper les pannes par une gestion pro active
- Réduire la durée d'intervention, en permettant de localiser la panne et de la définir rapidement.
- Remonter les informations d'IDS et fournir des indicateurs SSI au DSI
- Connaître rapidement l'effet d'une action sur le SI (nouveaux clients, nouvelles machines etc. ...)

Pourcentage de disponibilité	Temps d'arrêt annuel (1 journée = 24h)	Temps d'arrêt annuel (1 journée = 8h)
90%	876 heures (36.5 jour)	291.2 heures (12.13 jour)
95%	438 heures (18.2 jour)	145.6 heures (6.07 jour)
99%	87.6 heures (3.65 jour)	29,12 heures (1,21 jour)
99.9%	8 heures 45 minutes	2.91 heures
99.99%	52,56 minutes	17,47 minutes
99,999 %	5,256 minutes	1,747 minutes
99.9999%	31.536 secondes	10,483 secondes

Périmètre

De nombreux éléments peuvent être supervisés au niveau des machines (station, serveurs, réseau) ou de l'environnemental :

- Utilisation du système (%CPU, nombre de cores utilisés...)
- Nombre de processus (contentions, zombies) ;
- Utilisation de la mémoire (cache, swap, fautes) ;
- Utilisation des ressources (remplissage des disques, temps de calculs, . . .) ;
- Utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs) ;
- Disponibilité des services (files d'attente batch, interfaces, HTTP, DHCP, DNS, SMTP/POP, LDAP, . . .) ;
- Capteur température processeurs, température du boîtier, vitesse de rotation des ventilateurs ;
- Sécurité (nombre d'authentifications, de tentatives échouées de login, de scans) ;
- Intrusions logiques (login d'utilisateur sur des systèmes restreints, . . .), réseaux (scans, Déni de service), physiques (salle système, bâtiment) ;
- Etat des onduleurs (% capacité, temps de disponibilité, état des batteries), des imprimantes (niveau encre, papier) ;

On les classe souvent en différents types de supervision :

- La **Supervision système** : elle consiste à surveiller le réseau, l'infrastructure et les machines du Système d'Information (Processeur, Mémoire, Stockage) ;
- La **Supervision Applicative** : elle consiste à surveiller les applications et logiciels (base de données, serveur web...);
- La **Supervision Métier** : elle va consister à surveiller les processus métiers de l'entreprise (qui est un agrégat des indicateurs système, applicatif) ;
- La **Supervision de la sécurité** : elle consiste à surveiller les attaques potentielles sur le Système d'Information (virus, intrusion).

Pour ce dernier point, la supervision de la sécurité ne fait pas partie du cahier des charges du projet, (car hors du contrat d'exploitation, réalisé par la TME-Bull).

Néanmoins, des propositions d'outils de sécurité sont évoquées, comme proposition d'amélioration, au paragraphe 9.3.5.

Une partie des éléments de sécurité (pare-feu, serveur authentification, proxy) sont hébergés chez Orange, qui assure la supervision de la sécurité. Les actifs « réseau » sont supervisés par une console dédiée, de même que la gestion des antivirus. Le contrôle du pare-feu Netasq à l'entrée des DMZ Métier fait néanmoins partie du périmètre de notre solution de supervision.

Cet éclatement de la supervision sera analysée au paragraphe 9.6, avec la difficulté pour les entreprises d'aujourd'hui, à corréliser toutes ces informations.

2.4. Outils standards.

2.4.1. Commandes de base.

Pour monitorer un système, Linux et Windows proposent une panoplie de commandes permettant d'analyser et de retourner un ensemble d'informations relatives à l'état du système. L'analyse de ces données permet à l'administrateur de faire un état des lieux du système et effectuer les actions, qui s'imposent.

LINUX :

Commandes : ps, free, tload, top, uptime, vmstat, du, df , who , ping, nmap ...

Fichiers : fichiers logs

Moyen de supervision : Script shell , logiciel Glances

WINDOWS :

Commandes : ping, netstat, nslookup , nbstat ...

Fichiers, base de données : journal des événements, base des registres

Moyen de supervision : requête WMI, script VBScript

En quelques lignes de scripts constitués des commandes ci-dessus ou de requêtes SQL, pour les bases de données, une supervision « bas niveau » peut être assurée rapidement.

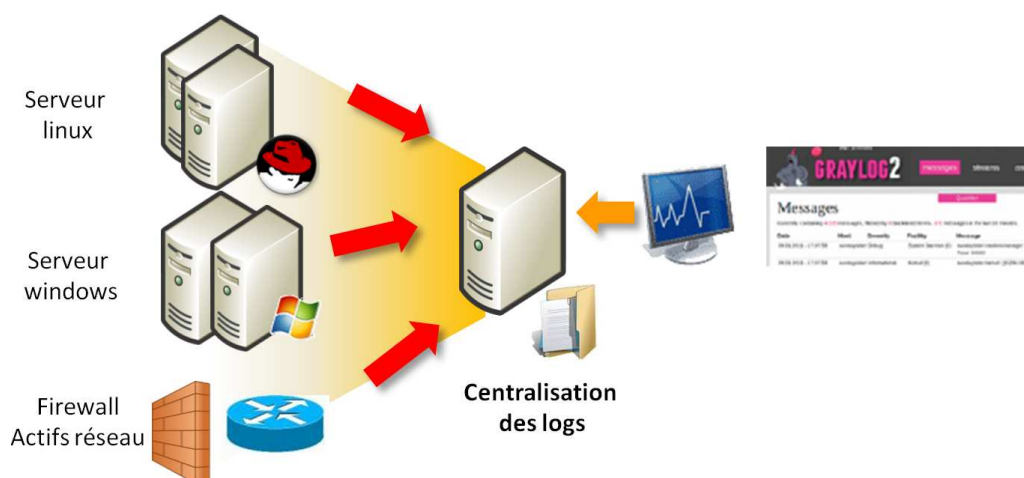
Mais, cette méthode est à éviter autant que possible, pour les difficultés de maintenir ces scripts « maison » à long terme.

2.4.2. SYSLOG.

Ce protocole de transmission, défini par les RFC 3164 et RFC 5424 permet de centraliser les événements de plusieurs équipements sur une seule machine pour analyse. Il utilise le protocole UDP à destination du port 514.

Chaque événement système est accompagné du type de service (facility), sa gravité (severity), l'horodatage (date/heure (timestamp)) et de la machine concernée (host).

Deux projets concurrents apportent des améliorations au protocole initial : syslog-ng et rsyslog. Des logiciels de filtrages et d'analyse, comme Graylog2, facilitent l'exploitation des résultats



Les journaux systèmes et applicatifs étant extrêmement nombreux, verbeux et nécessitant un volume de stockage, l'option SYSLOG sur les plates-formes SI métier n'a pas été retenue.

2.4.3. SNMP.

SNMP (Simple Network Management Protocol) est un protocole simple de gestion de réseau, proposé en 1988, par l'IETF. La connaissance de son fonctionnement est indispensable pour acquérir une partie des indicateurs du SI. Il est implanté dans la majorité des outils de supervision du marché.

SNMP permet de :

- Connaître l'état d'un équipement réseau (CPU, bande passante) ;
- Configurer certains paramètres (équilibrage de charges) ;
- Etre alerté d'un problème interne (alimentation, surchauffe).

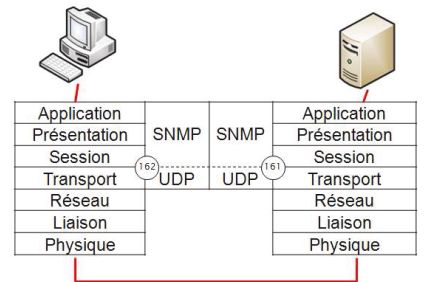
Architecture

Le modèle d'échange entre le manager NMS (Network Management Station) et l'agent contrôlé est basé sur deux types d'opération possibles :

- La requête, émise par la station vers l'agent, qui retourne une réponse ;
- Une alarme (trap) envoyée directement par l'agent vers la plate-forme, lorsqu'un événement se présente.

Protocole

Dans un souci de rapidité, le protocole SNMP ne transporte que des variables, par le biais du protocole de transport UDP, utilisé pour sa simplicité et son poids (8 octets au lieu des 20 de TCP), mais avec ses défauts (un paquet en mode non connecté et non fiable peut être perdu). L'agent reçoit les requêtes sur le port 161 et le superviseur reçoit les alarmes sur port 162. Ces ports devront être ouverts sur les pare-feu du SSA pour permettre la remontée des informations.



MIB

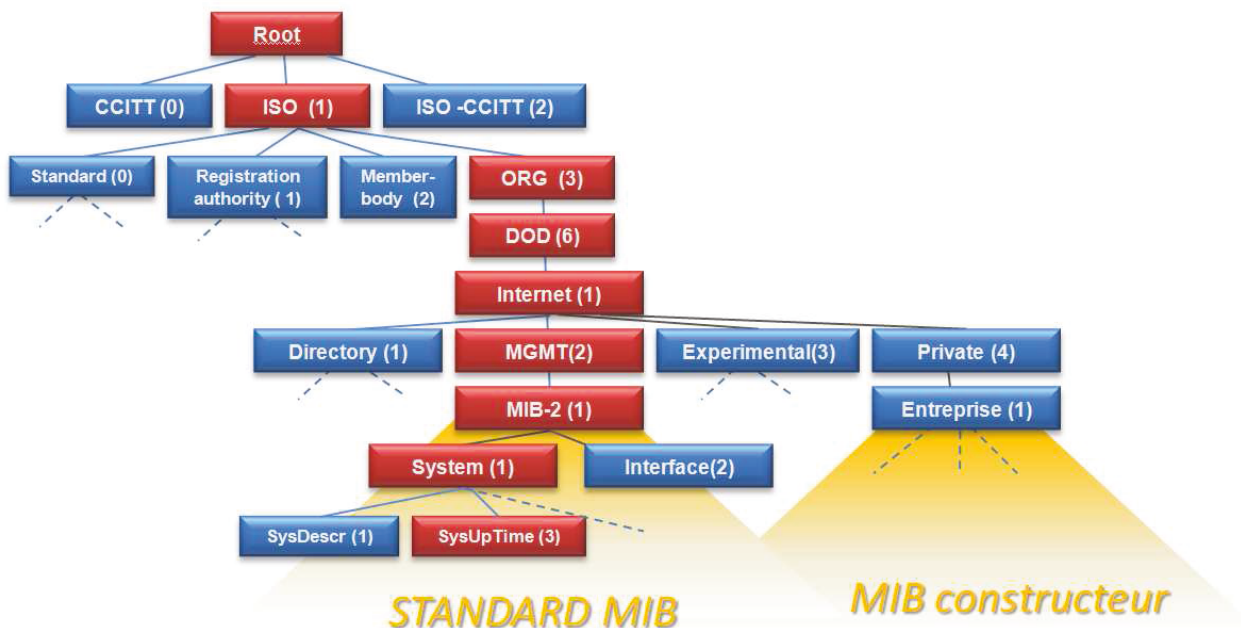
La MIB (Management Information Base) correspond à une base d'information de gestion, spécifique à chaque équipement et à chaque constructeur, qui définit les informations accessibles, les paramètres modifiables et les alertes à envoyer (traps). La MIB est une structure arborescente, où chaque feuille correspond à une information sur l'équipement.

SMI (Structure of Management Information) est le langage qui sert à définir un objet géré par la MIB.

Chaque objet correspond à :

- Un nom (Object Identifier (OID)) ;
- Une syntaxe décrite en langage ASN-1 (Abstract Syntax Notation One), qui définit son type, son codage et un droit d'accès read/write.

Utilisée au début des années 90, la version MIB1 est devenue rapidement obsolète. La MIB2 l'a remplacé avec l'ajout des groupes « Transmission » et « SNMP », dans le sous ensemble 1.3.6.1.2 –msgt).



Dans la structure arborescente de la MIB2, chaque nœud est défini par son OID .

Exemple

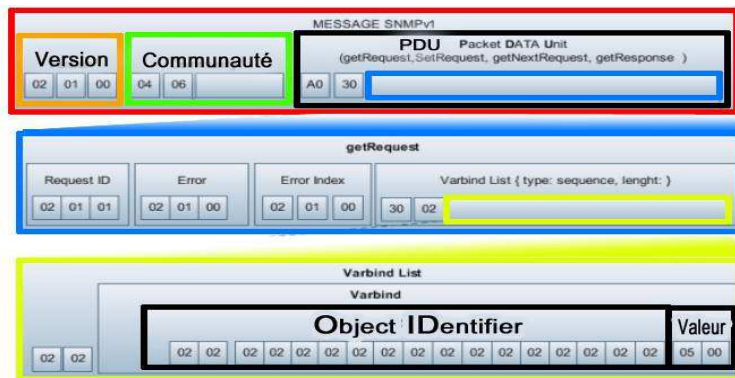
iso(1). org(3). dod(6). internet(1). mgmt(2). Mib-2(1).System(1).SysUpTime(3) => .1.3.6.1.2.1.1.3
SysUpTime = .1.3.6.1.2.1.1.3.

Il suffit d'interroger cet OID pour avoir la valeur du temps d'utilisation de l'équipement depuis sa mise sous tension.

La branche standard MIB-2 contient 11 sous-branches, dont les principales sont :

- **SYSTEM** (1), branche obligatoire, fournit des informations générales sur le système (nom, localisation, contact) et la description donnée par le constructeur/éditeur de la MIB (champ sysDescr) ;
- **INTERFACE** (2) contient le nombre d'interfaces réseau du système et des informations sur celles-ci (l'adresse physique, la vitesse, la MTU, le nombre de paquets émis ou reçus,...) ;
- **AT** (3) définit l'ensemble des informations permettant d'établir une correspondance entre une adresse physique et une adresse réseau, soit le cache ARP le plus souvent ;
- **IP** (4) contient la totalité des paramètres IP de chaque interface, définit une valeur (permettant d'identifier si le système fait du routage) et comporte des statistiques liées au volume de trafic et au nombre d'erreurs ;
- **UDP** (6) **TCP** (7) fournissent la liste des connexions établies, les adresses et les ports en écoute pour les deux protocoles de transport.

Dans la branche constructeur (1.3.6.1.4.1), Chaque éditeur/équipementier définit sa MIB dite privée, librement accessible, où sont décrites les caractéristiques propres à leur matériel.



Trame SMNP V1.0

Version

Il existe 3 versions du protocole caractérisées par des niveaux de sécurité différents :

SNMPv1 : RFC 1155 1156 1157 (1990)

La sécurité est basée sur la connaissance d'une chaîne de caractère (communauté), pour gérer les accès à la MIB. Cette donnée est présente dans toutes les requêtes faites par le manager NMS à l'agent SNMP. Malheureusement, ce « mot de passe » est transmis en clair et peut donc être intercepté par une personne malveillante, qui n'aura aucune difficulté à interroger à son tour les équipements.

SNMPv2 : RFC 1902 1903 1904 1905 1906 1907 (1996)

Déclinée sous 4 formats différents (SNMP v2p, V2c, V2u, V2*) dont une compatible la version v1 (v2c), la seconde version corrige les limitations imposées par la SMI (par exemple la taille des compteurs limitée à 32 bits) et l'ajout de deux nouvelles commandes, mais l'aspect sécurité n'a pas évolué.

SNMPv3 : RFC 3411 3412 3413 3414 3415 3416 3417 3418 (2002)

La version 3 apporte enfin un niveau de sécurité adaptée avec 3 modules de sécurité (horodatage, authentification, confidentialité gérés par les modèles USM (User Based Security Model) pour l'authentification et VACM (View Access Control Model) pour le contrôle d'accès à la MIB.

Au SSA, cette dernière version est utilisée sur les équipements réseau, boîtiers F5 et firewall.

Limite du protocole SNMP

Malgré le fait que la MIB contienne énormément d'informations techniques, le protocole SNMP ne permet de faire remonter en standard des informations capitales, pour la supervision comme l'état des services de haut niveau (HTTP, SGBD...).

3. Etude des SI Métier du SSA (Phase 1)

Objectif :

Cette phase a consisté à **étudier les trois plateformes** du SI métiers du SSA à superviser, par ordre de priorité de supervision, et comprendre les technologies et matériels mis en œuvre. Cette étude a aussi permis, avec l'aide des responsables applicatifs, de consolider les risques mis en œuvre, lors du déploiement de la solution.

Pour appréhender les indicateurs pertinents à surveiller, **chaque technologie utilisée a été analysée** dans le but d'identifier les variables clés, qui dimensionnent le système et servent de seuils d'alerte, pour prévenir un incident.

Organisme militaire ouvert vers des missions d'utilité publique, le Service Informatique du SSA se doit d'appliquer les **normes et recommandations** dans sa politique de mise en œuvre et de maintenance informatique. Nous avons donc aussi étudié et intégré ces référentiels d'organisation, décrits au chapitre 3.3, dans notre démarche.

Méthodologie réalisée :

Comme données d'entrée de notre étude, des documents techniques ont été fournis par l'équipe TME : linéaires, l'adresse IP des serveurs et la documentation d'exploitation plus ou moins complète des logiciels applicatif [BL-SUPERV-N1-DR].

J'ai demandé une réunion avec le responsable informatique de l'Hôpital d'Instruction des Armées de Brest [CCR-HIA-SUPERV-N1-NP] pour d'appréhender le Système d'Information Hospitalier, comprendre l'interconnexion des divers logiciels éditeurs et se sensibiliser aux contraintes des utilisateurs.

Les différents responsables applicatifs ont été sollicités par mail ou téléphone, pour avoir une vision globale des flux générés par leur application, ainsi que pour identifier la criticité et la sensibilité des ressources manipulées. Un questionnaire [QAPPL-SUPERV-DR] (voir annexe 16) a été transmis au préalable pour préparer l'audit et être plus efficace.

Livrables attendus :

-Référentiel Architecture SI [ARCH-SUPERV-DR]

3.1. Système d'Information Métiers

Nous allons détailler dans ce paragraphe les trois Système d'Information, hébergés au CeTIMA.

3.1.1. Système d'Information des Services Médicaux d'Unité (SISMU).

3.1.1.1. Objectifs.

Le SSA, pour répondre aux contraintes de son métier, doit pouvoir être en relation avec la communauté médicale. Avec la fin de la concession de service public du Réseau Santé Social (RSS) au 31/10/2004, le SSA se devait de réaliser sa propre communauté, avec le Système d'Information des Services Médicaux d'Unité (SISMU), au travers d'un espace sécurisé offrant des services spécifiques dédiés, à la communauté médicale interne au SSA et des échanges avec les diverses communautés médicales externes. A l'instar du ministère de la santé avec à l'étude le Dossier Médical Personnel (DMP), piloté par l'ASIP (Agence des Systèmes d'Information Partagés de Santé), le SSA a déployé un logiciel LUMM, utilisant comme support SISMU, pour la gestion des dossiers médicaux des personnels militaires.

Les objectifs de Système d'Information des Services Médicaux d'Unité (SISMU) sont donc de :

- Constituer une base de données unique des dossiers médicaux des personnels de la Défense ;
- Répondre aux obligations du Dossier Médical Partagé (DMP) tout en prenant en compte les spécificités médico-militaires ;
- Assurer une relation étroite entre le médecin d'unité et l'hôpital militaire de rattachement ainsi qu'avec les organismes de la chaîne logistique Santé ;
- Ouvrir le Service Médical d'Unité sur la médecine civile (privée et publique) et la formation continue en ligne (Internet).

SISMU correspond au système d'information utilisé par les Services Médicaux d'Unités (SMU) des unités des armées, de la Gendarmerie et du SSA, réorganisés en Centre Médicaux des Armées (CMA).

3.1.1.2. Applications mise à disposition.

Le portail propose aux utilisateurs différentes fonctionnalités :

- une messagerie santarm, hébergée chez un opérateur extérieur, sécurisée (*Sign&Mail®*) homologuée sur l'internet et l'intranet défense (Intradef) ;
- un accès sécurisé vers internet ;
- un logiciel médical et un logiciel médico-militaire forment le Logiciel Unique Médico-militaire et Médical (LUMM), qui est l'application principale de SISMU, hébergée sur les plates-formes du CeTIMA ;
- des liens, vers d'autres applications du SSA, à travers le réseau ReP3SA :
 - Un logiciel de gestion des approvisionnements pharmaceutiques PASTEL (Programmation des Approvisionnements Santé à Traitement Effectué Localement) ;
 - L'application Vidal (Référentiel des médicaments des laboratoires de pharmacie) ;
 - L'application Bedouin (Banque Epidémiologique de Données sur l'Outre-mer et la zone Intertropicale) ;
 - L'application Qualigram (référentiel documentaire des vétérinaires du SSA) ;
 - Bientôt l'application Preventiel pour la gestion médico-administrative des Centres de Médecine de Prévention des Armées (en remplacement des serveurs Chimed, installés en local).

Le LUMM, qui est donc le logiciel principal de SISMU, permet l'accès au Dossier Médical Partagé pour tous les personnels du Ministère de la Défense pris en charge par le SSA. Il doit donc être accessible de partout, (compte tenu de la mobilité des militaires), par une connexion Internet sécurisée, sur un navigateur web, avec authentification des utilisateurs par Carte de Professionnel de Santé (CPS).

L'application LUMM doit être opérationnelle 24h sur 24, 7 jours sur 7.



Le LUMM est structuré en différents menus qui permettent la planification des rendez-vous, la gestion des consultations médicales, l'administration du dossier patient, le recueil d'activité, les requêtes sur l'ensemble des données, l'aide au suivi des dossiers par des alarmes, l'impression des formulaires types...

3.1.1.3. Architecture.

L'architecture s'articule autour : (voir schémas de la page suivante)

- du **réseau local LAN et des postes clients** des Centres Médicaux des Armées, composés d'un ordinateur par médecin, pharmacien, chirurgien, dentiste et d'un ordinateur dans chaque secrétariat, dans les salles de soins, d'urgences, de biométrie, de pharmacie ;
- du **réseau REP3SA "Réseau des Professionnels de Santé du SSA"**, (*accessible via un lien xdsl ou RNIS*). Il est composé d'une zone logique de confiance, dite Réseau Professionnel de Santé (RPS), offrant des services sécurisés dédiés décrits ci-dessus.
- des **plates-formes applicatives** en DMZ au CeTIMA.

Il y a 3 plates-formes différentes :

- **Production** (pour le logiciel opérationnel utilisé par les unités) ;
- **Formation** (pour la formation des utilisateurs) ;
- **Qualification** (pour valider les mises à jour et les modifications logicielles).

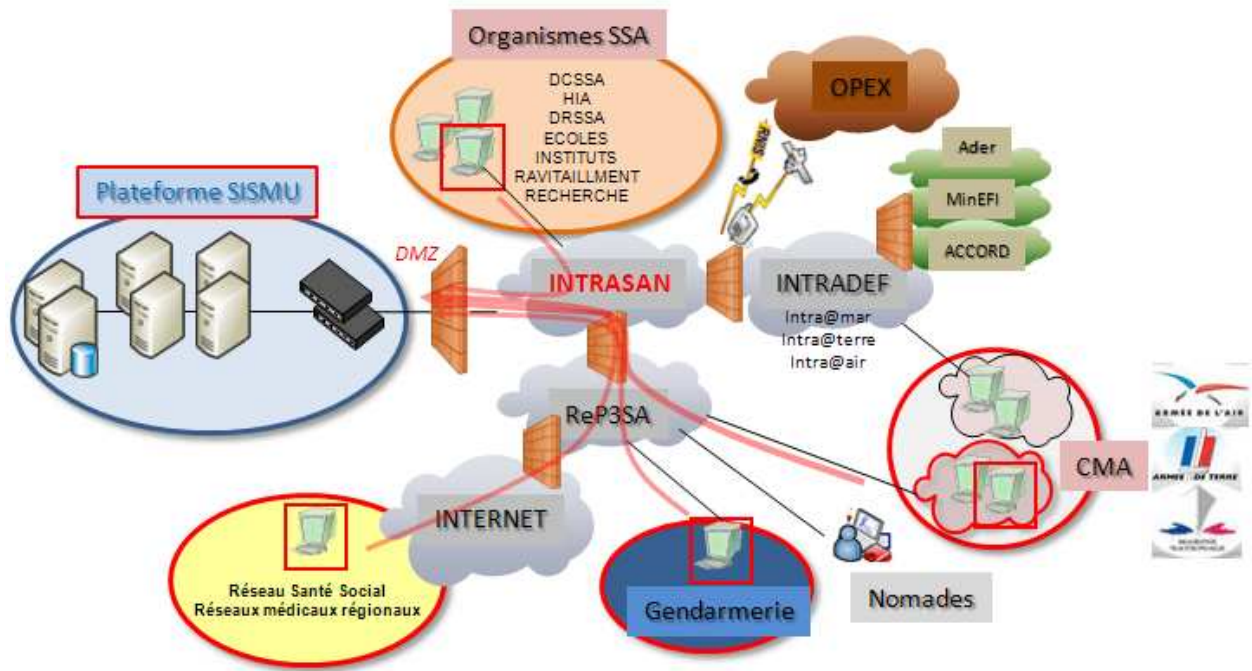
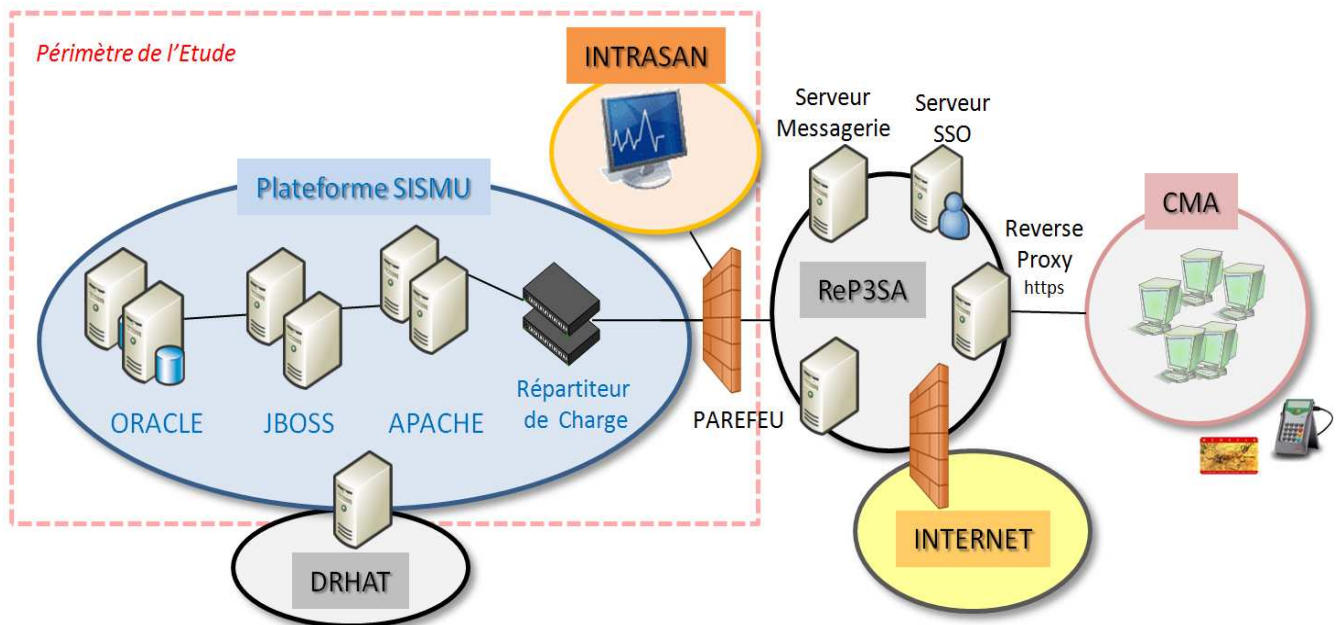


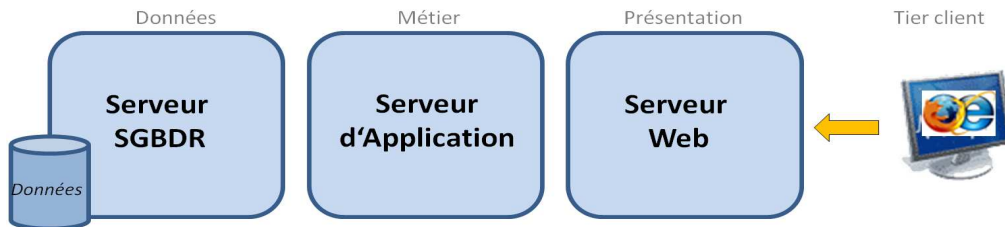
Schéma simplifié :



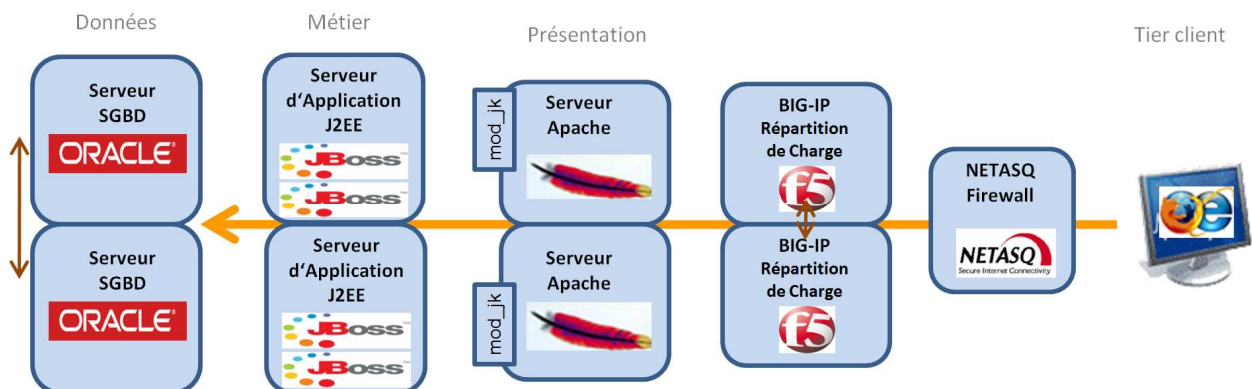
3.1.1.4. Fonctionnement.

Le logiciel est développé à partir du progiciel Health.Web® par la société ARES. Il s'appuie sur une structure générique incluant une gestion de dictionnaires et permettant des échanges de données structurées dans des formats normalisés. Le LUMM respecte le standard de structure GEHR (*Good Electronic Health Record*).

Ce progiciel Health.Web® repose sur une "architecture n-tier" avec un serveur web Apache, un serveur d'application J2EE (*JBoss*) et une base de données sous Oracle.



Un Loadbalancing (répartition de charge), de manière matérielle, est géré en tête de réseau par deux boîtiers F5, pour distribuer les requêtes reçues. Pour une haute disponibilité, l'ensemble est redondé, avec deux serveurs frontaux apaches installés avec le module mod_jk, pour assurer les redirections vers deux serveurs JBoss (deux instances logicielles chacun), qui réalisent les requêtes de données, vers deux serveurs oracle montés en cluster.



Avec une interconnexion extérieure avec la Direction des Ressources Humaines de l'Armée de Terre (DRHAT), un fichier de données permet la mise à jour de certains éléments de la base de données oracle, de manière périodique.

3.1.2. Système d'Information des Hôpitaux (SIH).

3.1.2.1. Objectifs.

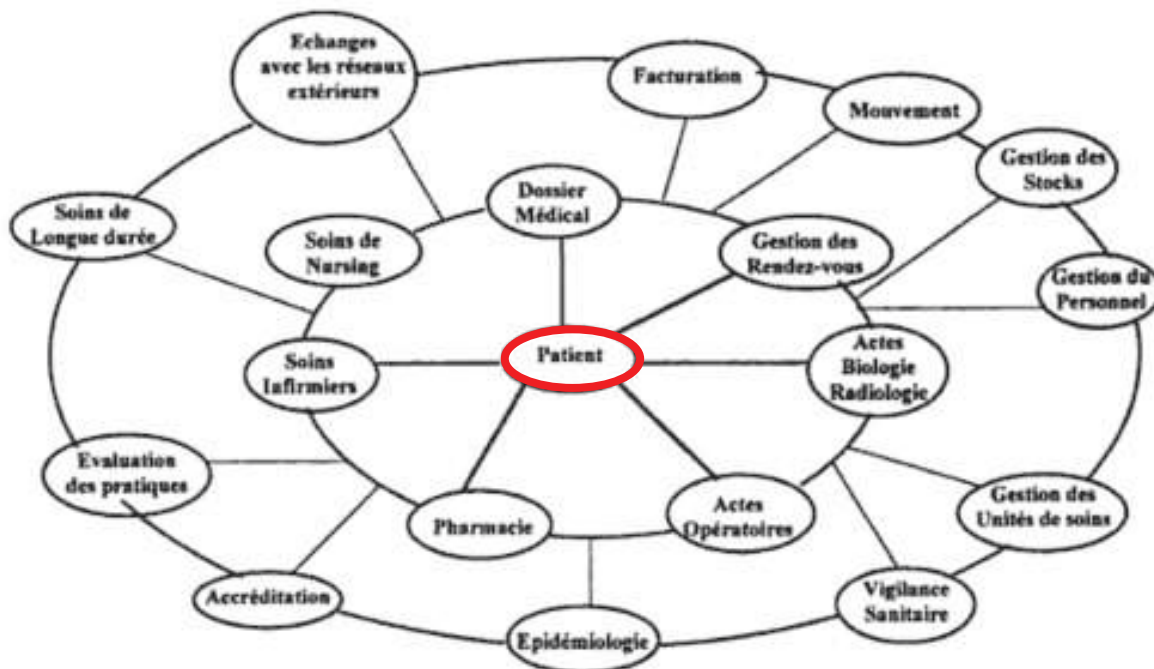
Le système d'Information des Hôpitaux (SIH) est orienté vers l'accueil et la gestion du patient pour les hôpitaux militaires. Il fournit au personnel un accès sécurisé aux informations médicale et administrative.

Le SIH a pour but :

- Améliorer la pertinence et la validité des données médicales ;
- Diminuer le temps de saisie des données et éviter une redondance de l'information ;
- Améliorer et fiabiliser les échanges d'informations ;
- Fournir différents renseignements concernant le patient et les données médico-économiques.

Périmètre :

Le SIH est composé d'un grand nombre de logiciels sectoriels couvrants les différentes fonctionnalités spécifiques très vastes des différents professionnels de santé. (voir schéma ci-dessous)



Gestion SI médical – P. Degoulet Ed.Masson

Normes:

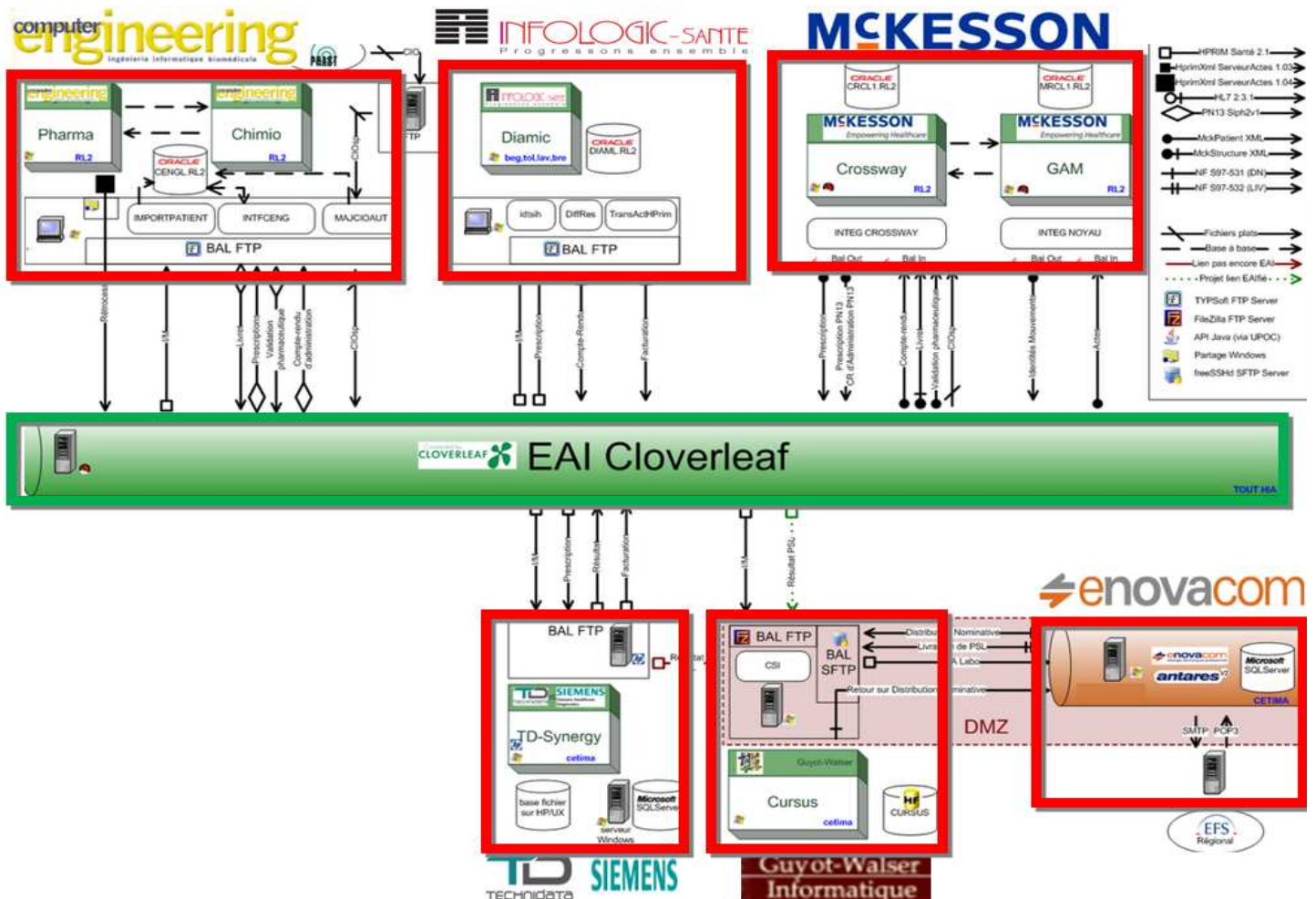
La difficulté est l'interopérabilité, pour permettre le dialogue entre ces différents logiciels très hétérogènes, s'appuyant chacun sur des normes différentes:

- **DICOM** (Digital Imaging and Communications in Medicine) : norme sur l'imagerie médicale numérique suivie par la NEMA (National Electrical Manufacturers Association) et l'ACR (American College of Radiology), auxquels se sont joints le JRIA au Japon, l'ANSI aux USA et le CENTC251 en Europe.
- **HPRIM** (s'appuyant sur l'ASTM aux USA) : norme française pour les échanges inter-laboratoires.
- **HL7** (Health Level 7) : norme de l'organisation HL7 sur l'échange d'information des couches applicatives, évoluant actuellement vers XML – norme ISO/HL7 21931/2009.

Des tentatives d'uniformiser les échanges et des formats de données sont en cours actuellement à l'ISO, à l'UIT, à l'AFNOR et au comité européen de normalisation CENTC251 (CEN Technical Committee 251)

3.1.2.2. Applications mises à disposition.

Le SIH est constitué de différents logiciels hétérogènes de différents éditeurs, dont nous allons décrire rapidement les fonctions.



Basé sur les progiciels **GAM** et **CROSSWAY**, proposé par l'éditeur Mc KESSON, **AMADEUS** constitue le logiciel le plus important, pour supporter l'ensemble des activités du processus de soins dans les hôpitaux. Il offre les fonctionnalités suivantes :

- Module Rendez-vous ;
- Module Unités de Soins : Gestion des lits, résultats laboratoires, gestion des actes avec ou sans cotation, synthèse, entrée patient, sortie, décès ;
- Module Prescription : Planification de soins, demande d'acte (médicaments, perfusion, demande examen de type laboratoire, imagerie, prescriptions infirmières, régimes, matériel) ;
- Module Dossier Médical Commun : consultation le dossier patient (antécédent, données vitales, données administratives, résultats labo, synthèse des RDV et séjours).

Le Progiciel **CHIMIO** de COMPUTER ENGINEERING permet de gérer le circuit des chimiothérapies (prescription, calcul et impression des fiches de fabrication et des étiquettes, traçabilité, doses cumulées et historiques des chimiothérapies, cotation CCAM et suivi des coûts ...)

Le Progiciel **PHARMA** du même éditeur assure le circuit du médicament et la gestion de la pharmacie (prescription, protocole médicamenteux, validation pharmaceutique, gestion des stocks et achats ...).

Le Progiciel **DIAMIC** de INFOLOGIC gère le domaine anatomie et pathologie (suivi technique, une gestion des banques d'images, cotation automatique...).

Conçu spécialement pour la transmission des résultats entre laboratoires, le logiciel **TD-SYNERGY**, distribué en France par TD Technidata, automatise plusieurs fonctions, allant des demandes d'analyses (Biochimie, Hématologie, Immunologie, Bactériologie, Virologie, Histologie, Cytologie, Génétique, Gestion de la banque du sang, Gestion des dons d'organes) en laboratoire, à la production et à la communication des résultats d'examen.

Développée par la société Guyot-Walser Informatique, **CURSUS** est une solution de traçabilité transfusionnelle et de gestion de dépôts de produits sanguins, choisie par plus de 190 établissements français, pour assurer le suivi informatique de l'hémovigilance.

Le logiciel **ANTARES** de la société ENOVACOM est un serveur d'échanges électroniques professionnels, dédié au monde médical. Il est conforme aux recommandations du GMSIH (Groupement pour la Modernisation des Systèmes d' Informations Hospitalier). L'ensemble des protocoles d'échanges standards ou spécifiques à la santé est géré : smtp/pop3, s-mime, hprim net, http/ssl, ftp, ssh, soap messaging service, tedeco sous ip, VPN / Hélios, PES V2, xmodem, pesit, ...

Afin d'assurer la mise en conformité avec la législation en vigueur, Antares permet la signature électronique et la vérification de son authenticité, le chiffrement et le déchiffrement de données de tous types, avec la gestion des certificats.

Il est utilisé pour les échanges avec l'EFS (Etablissement Français du Sang).

3.1.2.3. Architecture.

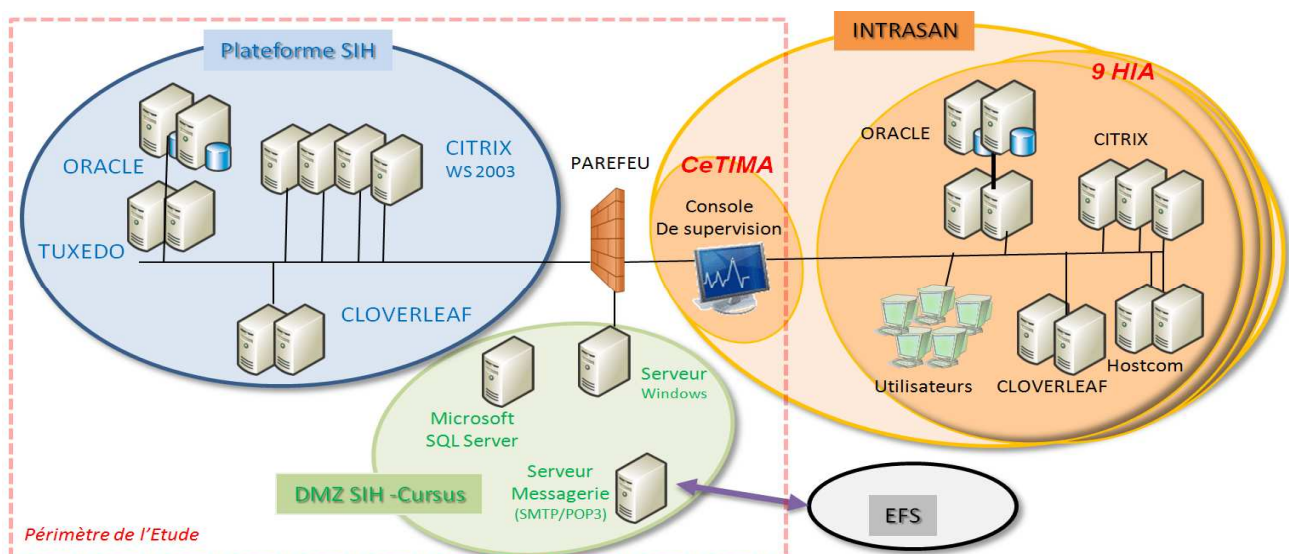
Vu le nombre de logiciels mis en œuvre, l'interopérabilité dans le SIH est un problème majeur, aussi pour permettre le dialogue entre les logiciels hétérogènes, on utilise l'EAI (Entreprise Application Integration) **CLOVERLEAF** de E.NOVATION, dédié au monde de la santé.

Ce « hub de communication » assure une gestion centralisée de tous les flux du SIH, avec :

- Une centralisation des flux (aux formats HL7, HPRIM, PN3) ;
- Un formatage de données dans un flux ;
- Une gestion des erreurs ;
- Une traçabilité des flux.

Chacun des 9 hôpitaux du Service de Santé des Armées dispose de sa propre plate-forme SIH. Les serveurs SIH du CeTIMA ne sont pas là, pour gérer l'organisation quotidienne d'un hôpital.

La plate-forme du CeTIMA a pour but de transmettre à chaque HIA le référentiel métier du Service de Santé des Armées. Elle héberge aussi le module Coursus de gestion du sang, qui s'occupe des échanges entre les HIA et l'Etablissement Français du Sang.



3.1.2.4. Fonctionnement.

Autour de l'EAI Cloverleaf, le système Amadeus (cible principale de notre étude du SIH) fonctionne sur une architecture n-tiers, composé :

- un serveur cloverleaf ;
- un serveur hébergeant le moniteur transactionnel tuxedo (*transactions for unix, extended for distributed operations*) créé par ATT, repris par BEA et aujourd'hui proposé par ORACLE;
- un serveur de base de données Oracle.

3.1.3. Système d'Information du RAVitaillement (SIRAV).

3.1.3.1. Objectifs.

Le système d'Information du Ravitaillement offre l'ensemble des outils nécessaires pour le fonctionnement de la composante Ravitaillement Sanitaire du SSA.

3.1.3.2. Applications mise à disposition / Architecture

Le Système d'Information est composés de différents logiciels :

GMAO (*Gestion de la Maintenance Assistée par Ordinateur*)

Cette application sert aux suivis préventif et correctif des équipement biomédicaux (défibrillateur, scanner ...), suivant les politiques de maintenance et de renouvellement préétablies.

RARS (*Référentiel des Articles du SSA*)

Il correspond au catalogue des articles du SSA, de leurs descriptifs et des dotations de référence.

RADARS (*Recueil et Analyse des Données de Données de Ravitaillement Sanitaire*)

Ce logiciel assure la logistique des stocks des ERS (Etablissements du Ravitaillement Sanitaire), avec la gestion des comptes en valeur et des matériels.

CDRAV (*Consolidation des Données du Ravitaillement*)

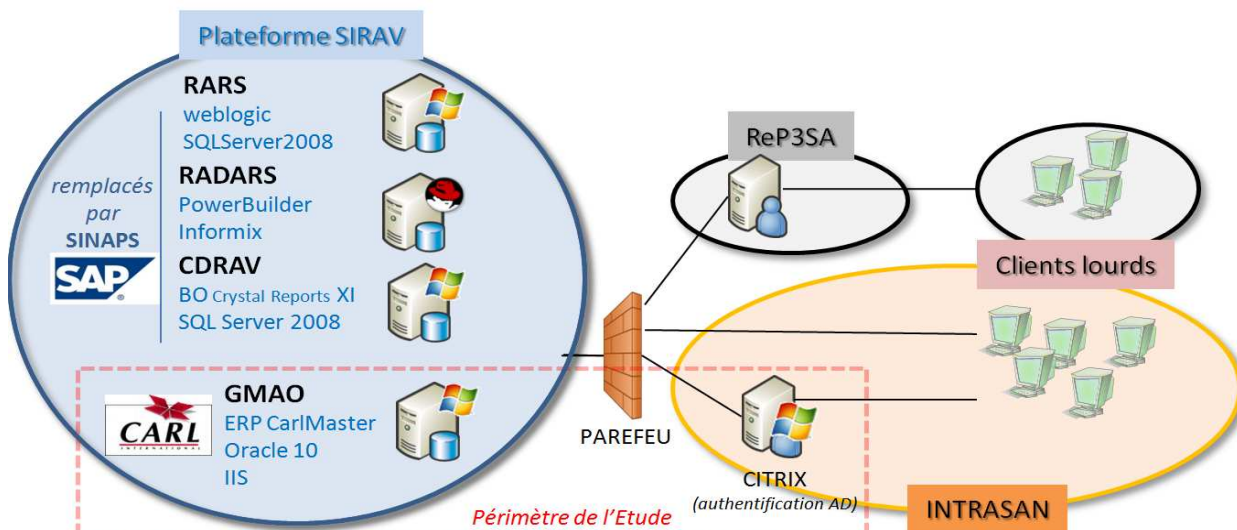
Correspondant à un infocentre Business Object, il permet la génération de rapports de suivi et des commandes vers les fournisseurs,

ORGAPHARMA est un GPAO, outil de Gestion de Production de la PCA (Pharmacie Centrale) pour la planification et la gestion des gammes de production des médicaments.

Une refonte du SIRAV est à l'étude, avec le remplacement début 2012, des derniers logiciels cités, qui utilisent des clients lourds. Le nouveau projet **SINAPS** sera « full web », basé sous l'ERP de SAP et interfacé avec le système interarmées Chorus, pour les imputations financières. Nous nous intéresserons donc uniquement à l'application multi-sites GMAO de la société Carl Software, accessible sur le réseau Intrasan ou ReP3SA. Les principaux utilisateurs sont les ateliers de maintenance du ravitaillement sanitaire et les services d'ingénierie biomédicale des HIA.

3.1.3.3. Architecture.

Les postes clients GMAO sont équipés d'un client lourd Carl Master, pour la connexion à l'ERP de Carl Software, à travers une ferme de serveurs Citrix sous Windows 2003. Le processus métier offre néanmoins aux utilisateurs distants, un client web léger, attaquant un serveur web Microsoft IIS, pour la création de tickets d'incident dans l'application. Les données sont stockées dans une base de données Oracle 10g.



3.2. Technologies utilisées

Nous avons étudié, en détail, les technologies communes aux différents SI, afin d'identifier les valeurs et composants sensibles, à référencer dans nos indicateurs à visualiser.

Un résumé de l'étude des technologies mise en œuvre est consultable à l'annexe 2

Suivant les ressources disponibles (CPU, RAM, débit, nombre de serveurs, nombre d'instances...), certains paramètres dimensionnent les limites à ne pas dépasser par les ressources et les requêtes disponibles pour les utilisateurs, afin de conserver un SI opérationnel. Il faut donc contrôler ces valeurs maximales et alerter en cas de dépassement de seuil.

Serveur apache :

Le fichier de configuration http.conf, définit les caractéristiques du serveur web.

- Max Clients** : nombre maximum de clients (*si le nombre est dépassé, les clients supplémentaires sont mis en attente*)
- MaxRequestPerChild** : nombre de requêtes géré par le processus fils de httpd
- MaxSpareServers** : nombre maximal de processus httpd inoccupés que l'on conserve

Serveur JBoss

a- Sur le serveur apache le fichier de configuration du module mod_jk définit les nœuds mise en œuvre, avec le port utilisé, le facteur de répartition de charge et la définition du Loadbalancing des serveurs JBoss

b – fichier.xml sur le serveur JBoss.

- MaxThreads** : nombre maximum de threads du pool
- Accept_count** : nombre max de requêtes dans la file d'attente
- ConnectionTimeout** : délai d'attente maximum dans la liste d'attente

c- Configuration du pool de connexion JDBC

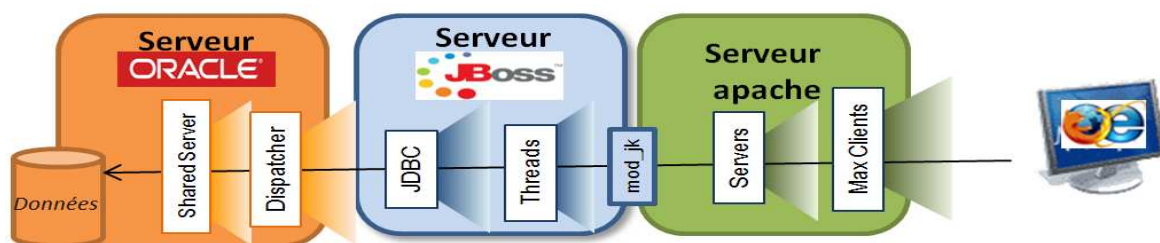
- MaxActive** : nombre maximum de connexions actives simultanément dans le pool
- MaxIdle** : nombre maximum de connexions en attente dans le pool.
- MaxWait** : temps d'attente, avant que le pool ne renvoie une erreur, quand une connexion demandée n'est pas disponible.

Une l'**API JMX** (Java Management Extensions) est fournie dans le monde Java pour superviser les modules JEE. L'étude du composant Mbeans est essentielle pour comprendre la mise en œuvre des agents de supervision assez développés, pour retourner les indicateurs souhaités du cahier des charges.

Serveur Oracle

Les valeurs importantes sont définies dans le fichier init.ora ou initSID.ora

- MTS_dispatchers** donne le nombre et les caractéristiques des dispatchers (adresse, description, protocole, CONNECTION nombre max de connexions pour chaque dispatcher, DISPATCHER le nombre initial de dispatchers lancés).
- MTS_Max_dispatchers** nombre de process dispatcher simultanés maximum
- MTS_Max_Servers** nombre de process simultanés maximum



Valeurs limites pour chaque composant

3.3. Gouvernance et Normes au SSA.

Depuis des années, le Service de Santé des Armées s'est engagé dans de nombreuses démarches qualité, adaptées à la diversité de ses missions. L'informatique du Service Santé n'est pas exclue de ce processus et essaye d'appliquer au mieux les normes actuelles.

Au Ministère de la Défense, une démarche ITIL a été initialisée à la DIRISI, pour adapter les méthodes d'organisation des centres Informatiques à ces bonnes pratiques.

Après avoir défini le concept de supervision au chapitre 2.3, nous allons voir la manière, dont elle a été normalisée par l'ISO et l'ITIL.

3.3.1. Normes ISO 2700X.

ISO/ CEI 27001 Exigences SMSI

ISO/CEI 27002 Mesures et sécurités

ISO/CEI 27003 Implémentation SMSI

ISO/CEI 27004 Indicateurs

ISO/CEI 27005 Appréciation des risques

ISO/CEI 27006 Certification des organismes

ISO/CEI 27007 Audit SMSI

ISO/CEI 27008 Audit mesures de sécurité

ISO/CEI 27010 Gestion de la communication inter secteur

ISO/CEI 27031 Continuité d'activité

ISO/CEI 27032 Cyber sécurité

ISO/CEI 27033 Sécurité réseau

ISO/CEI 27034 Sécurité des applications

ISO/CEI 27035 Gestion des incidents

ISO/CEI 27036 Audit des mesures de sécurité du SMSI

ISO/CEI 27037 Gestion des preuves numériques

ISO/CEI 27011 Spécifique secteur des communications

ISO/CEI 27799 Spécifique domaine médical en 2008 (*)

(*) Dans le domaine de l'informatique de santé, la norme ISO 27799:2008 fournit des lignes directrices permettant d'interpréter et de mettre en œuvre l'ISO/CEI 27002, en garantissant la Confidentialité, la disponibilité et l'intégrité des informations médicales personnelles.

Pour assurer le critère « disponibilité » du système, l'ISO/CEI 27001 (extrait point 10.3.1 ci-dessous) impose une supervision et une maintenance des ressources du Système d'Information. Mais elle n'indique pas comment les réaliser et avec quels moyens.

A.10.3 System planning and acceptance		
<i>Objective:</i> To minimize the risk of systems failures.		
A.10.3.1	Capacity management	<i>Control</i> The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

La norme souligne, par exemple, que l'utilisation des principales ressources (CPU, disque dur, fichiers de configuration) doit être maîtrisée. La supervision entre donc dans ce périmètre en informant sur l'état des ressources pour permettre d'intervenir de manière proactive en anticipant les évolutions nécessaires au système (exemple warning sur un espace disque).

3.3.2. ISO/CEI 7498-4, supervision des réseaux.

L'ISO propose la norme 7498-4, pour définir une architecture d'un protocole d'administration.

Ce concept est défini sur 5 axes :

- **The performance management** : la gestion des performances correspond à l'aspect communication entre les machines et surveiller la disponibilité des services à travers le contrôle des flux, le débit... ;
- **The fault management** : la gestion des anomalies détecte les problèmes et essaye de localiser efficacement et rapidement la panne matérielle ou logicielle ;
- **The configuration management** : la gestion de la configuration des équipements et versions utilisées par le système comme le matériel, les logiciels, les données ;
- **The Security management** : la gestion de la sécurité contrôle l'accès aux ressources en garantissant l'intégrité, l'authentification et la confidentialité des données ;
- **The accounting management** : la gestion comptable permet une gestion la consommation des ressources par un utilisateur en vue de réguler l'accès et établir une facture.

Le premier axe, « the performance management » correspond à une solution de métrologie et permet d'évaluer la performance du Système d'information. Il faut donc collecter des informations, stocker ces résultats dans une base de données, puis les analyser sous une forme facilement exploitable (un graphique par exemple).

Le second « fault management » définit une solution de supervision, avec une détection de problème, pour l'isoler le plus précisément, afin de le résoudre le plus efficacement possible.

3.3.3. ITIL (Information Technology Infrastructure Library.)

Le Ministère de la Défense applique aujourd'hui la démarche ITIL (Information Technology Infrastructure Library), avec la mise en place de centre d'appel, de gestions des incidents et des problèmes, avec la centralisation des sites hébergeurs de ressources serveurs et la mise en place d'outils communs de gestion de parc (gestion des configurations).

Il y a aussi une volonté de contractualiser les prestations informatiques, proposées aux unités et chefs de projet, en mettant en place des contrats de service (SLA , Service Level Agreement), de disponibilité et de continuité des services, avec une gestion financière des moyens informatiques réellement utilisés.

Crée en 1989, en Angleterre, par la CCTA (Central Computer Telecom Agency), sa dernière version v3 date de 2007. ITIL propose une bibliothèque de livres, qui recueille les meilleures pratiques pour une direction informatique.

L'objectif de cette approche est que toute l'entreprise utilise le même vocabulaire et les mêmes processus quel que soit le service informatique. Le but est de créer une cohérence et une synergie autour des processus du centre de Production Informatique.

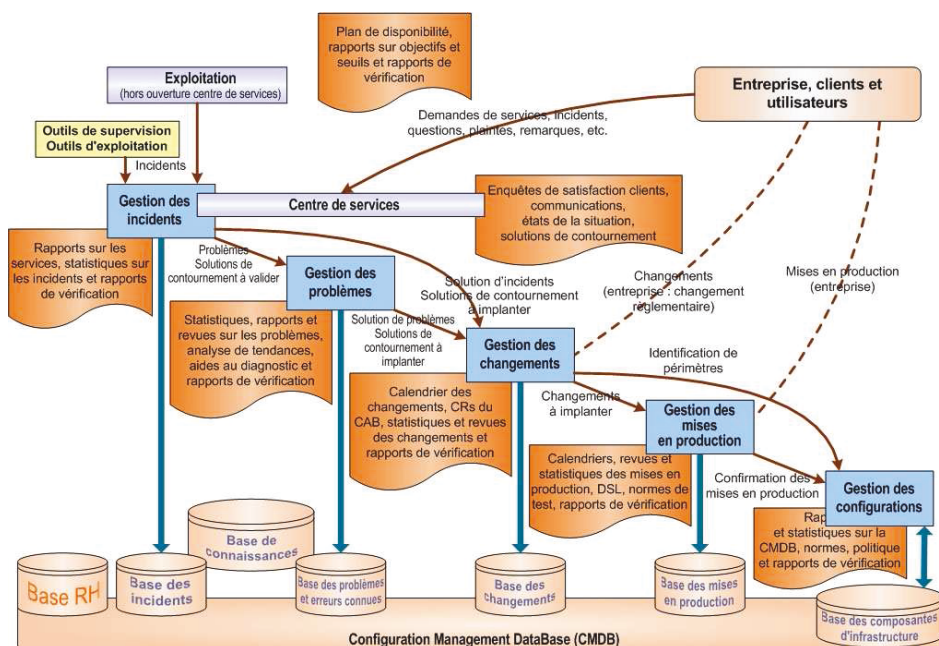
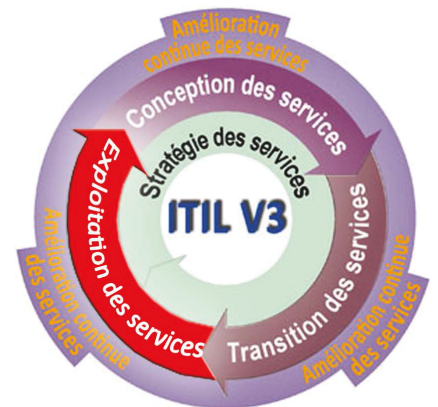
ITIL aborde notamment les sujets suivants :

- Comment organiser un système d'information ;
- Comment améliorer l'efficacité du système d'information ;
- Comment réduire les risques ;
- Comment augmenter la qualité des services informatiques.

L'approche orientée client est mise en avant, avec en particulier l'état de la disponibilité en temps réel du système d'information.

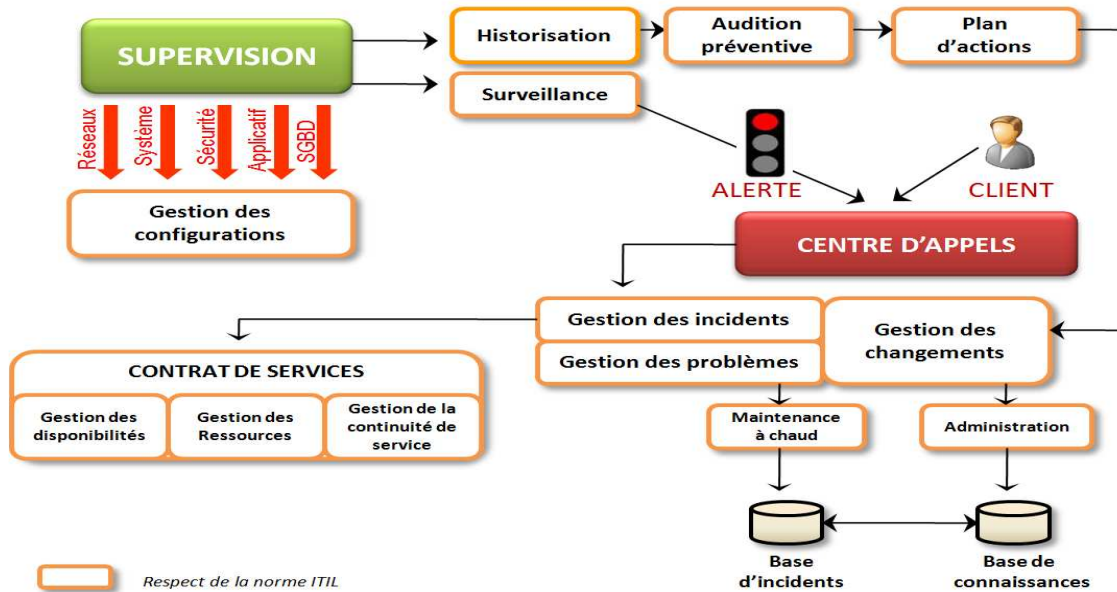
Les 6 livres du noyau sont les suivants :

- Introduction officielle à ITIL - Le cycle de vie des services ;
- Stratégie des services (*Service Strategy*) ;
- Conception des services (*Service Design*) ;
- Transition des services (*Service Transition*) ;
- Exploitation des services (*Service Operation*) ;
- Amélioration continue des services (*Continual Service Improvement*).



Extrait www.itilfrance.com

Dans le cas de la supervision du système d'information, la supervision rentre dans le cadre de « l'exploitation des services », avec le processus de gestion des événements, qui déclenche une série d'action (gestion des incidents, gestion des problèmes, gestion des Changements...). Dans la logique de progrès continu, on fait une distinction entre les incidents et les problèmes, qui sont les causes de ces incidents.



L'outil de supervision peut ainsi répondre aux métriques de disponibilité proposée par l'ITIL :

- **Fréquence des pannes** : par jour, par mois, par an ;
- **Performance de la restauration** : temps de restauration et de redémarrage du service après interruption ;
- **MTBF** (Mean Time Between Failures) : temps moyen entre le redémarrage complet d'un service et son interruption suivante;
- **MTBSI** (Mean Time Between System Incidents) : temps moyen entre deux pannes ;
- **MTTR** (Mean Time To Repair) : temps moyen entre l'apparition d'un incident et sa résolution.

4. Cahier des charges fonctionnel (Phase 2)

Objectif :

Cette phase correspondait à formaliser, dans un Cahier Des Charges Fonctionnel (CDCF), les besoins recueillis (technique, formation, documentation) et les contraintes (calendrier, budget, sécurité) exprimés par le Maître d'Ouvrage (MOA), pour assurer la supervision des SI métier.

Méthodologie réalisée :

Afin de gagner un temps précieux, un questionnaire général sous forme de Questions à Choix Multiples [QUES-SUPERV-NP], (disponible en annexe 17), couvrant un large périmètre de la supervision SI, a été fourni aux différents acteurs du projet, pour cerner le périmètre et les besoins du projet (contexte, technologie de supervision, Serveur, OS, réseau, plates-formes, alerte, rapports/ graphes/ tableaux de bord, Gestion utilisateur, architecture..). Le dépouillement des réponses a permis de faire remonter le périmètre et les besoins attendus.

Un audit de l'équipe TME a aussi été réalisé pour comprendre leurs méthodes actuelles de travail dans l'exploitation des plates-formes métiers, hébergés au CeTIMA (SISMU, SIH, SIRAV).

Des échanges téléphoniques et par courriel avec les différents experts techniques du CeTIMA ont abouti par la définition des exigences opérationnelles en termes de sauvegarde [BL-SUPERV-N2-NP] ou de règles de sécurité, décrites par le responsable du pôle sécurité du CeTIMA [CCR-CETIMA-SUPERV-N2-DR]. (Sécurité pare-feu, MIB autorisée, protocoles autorisés...).

Les standards de supervision, utilisés dans le futur, au Ministère de la Défense ont été indiqués par la DIRISI Brest et Rennes (Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la Défense) [CCR-DIRISI-SUPERV-DR].

Un premier cahier des charges a été proposé au groupe de pilotage du projet [CDCF-SUPERV-NP] avec les fonctionnalités désirées, les contraintes budgétaires et calendaires, ainsi que 19 critères de choix, listés par importance. Il a été discuté, consolidé, amendé, avant d'être définitivement accepté.

Livrables attendus :

- CdCF Cahier des Charges Fonctionnel (Fonctionnalité, Budget, Planning, Critères de choix) ;

Les fonctionnalités demandées

1. Licence, langue, système d'exploitation

Critère 1 : Les solutions libres de supervision seront privilégiées, pour les avantages suivants : coût nul de licence, facilité de personnalisation, mise à jour gratuit et respect des standards pour une meilleure interopérabilité,

Critère 2 : La langue utilisée sera de préférence française

Critère 3 : La solution devra fonctionner sur un système d'exploitation linux

2 Installation et Configuration

Critère 4 : L'installation et la configuration de la solution ne doivent pas demander de compétence particulière et être intuitives.

Critère 5 : Un système d'auto découverte fiable serait un point positif, pour faciliter l'ajout d'équipement, mais dans tous les cas la solution doit offrir la possibilité de gérer la cartographie du réseau manuellement pour faire la différence entre la topologie logique (comprise par un système d'auto découverte) et la topologie physique.

3 Interface utilisateur

Critère 6 : L'interface utilisateur doit être conviviale et la prise en main rapide.

Critère 7 : La majorité de la configuration (définition des utilisateurs, des équipements à surveiller...) doit pouvoir se faire à distance via une interface web ou une application cliente.

Critère 8 : Nous souhaitons pouvoir générer différents graphiques, pour toutes les ressources systèmes et réseaux, sur différentes échelles de temps.

Critère 9 : La génération d'un rapport au format standard (html, pdf, excel) avec des tableaux de bord (hebdomadaires, mensuels et annuels) pourra être réalisée à la demande ou de manière automatique avec une distribution par email.

4 Gestion des profils utilisateurs

Critère 10 : La solution doit permettre de créer des groupes d'utilisateurs avec différents droits possibles :

- Droit de modification des paramètres (ajout d'un équipement, modification des seuils d'alerte...)
- Droit d'affichage du statut des équipements
- Droit d'ajouter, modifier et supprimer des utilisateurs et des groupes ...

Le nombre approximatif des personnes utilisatrices du système de supervision est fixé à 3 personnes pour la TME et une dizaine en consultation, pour vérifier la disponibilité par rapport aux contrats de service.

L'accès à l'interface distante utilisera un système d'authentification par nom d'utilisateur et mot de passe ou en l'annuaire actif directory (protocole LDAP).

5 Supervision des plates-formes

5.1 Cibles et protocoles utilisés

La solution doit au moins être en mesure de surveiller, jusqu'à une centaine de serveurs physiques, qui sont des serveurs http (apache, IIS), Firewall, SGBD, applicatif JAVA (JBoss,tuxedo..), ferme Citrix, messagerie.

Tous les indicateurs à contrôler seront identifiés par un nom, l'adresse IP du serveur, sa communauté SNMP et l'élément contrôlé : interface, service, ressource (Mémoire, CPU, espace disque, nombre de transactions, présence d'un fichier)...

Ce contrôle sera réalisé par une interrogation SNMP ou par des agents à définir, à intervalle régulier, qui doit être personnalisable par équipement.

Critère 11 : Le protocole de supervision utilisera le protocole SNMP de la version 3.

Critère 12 : Des agents devront être disponibles, pour remonter les résultats non réalisés SNMP, sur Windows serveur 2003 et linux Redhat Entreprise. L'installation doit être simple et les agents ne doivent pas rendre instable le système d'exploitation et les applications installées.

Aucun système de centralisation de log (syslog) n'est actuellement utilisé au CeTIMA

5.2 Gestion des événements

Critère 13 : Un événement est un changement d'état ou d'une valeur d'un indicateur identifié. La solution doit savoir analyser ces données et détecter une anomalie, une surcharge, une dégradation de la qualité d'un service...cela avant que ce soit un utilisateur qui prévienne les administrateurs du problème. Sur l'interface, on doit pouvoir visualiser la liste de tous les événements qui ont eu lieu. Un système de filtre, permettant de ne visualiser que les événements concernant un seul équipement par exemple, et un système de comptage des événements sont souhaitables. Les événements doivent être conservés au moins 1 an dans la limite de 20 événements par jour pour permettre à l'équipe TME d'analyser une panne ou un ralentissement répétitif d'un équipement par exemple

5.3 Gestion des alertes

Critère 14 : Une alerte intervient, lorsqu'un événement a lieu. Cette notification a pour but d'informer le plus rapidement possible les personnes souhaitées. Bien sûr tous les événements ne doivent pas provoquer une notification, il doit être possible de définir les événements à notifier, le seuil de notification et les utilisateurs et/ou les groupes à notifier, lorsque ce seuil est atteint.

On doit pouvoir modifier la fréquence de ces notifications et les personnes à avertir.

Les moyens utilisés par défaut seront l'alerte visuelle (console, pop up, icône warning) avec un message électronique. Les solutions d'envoi de SMS et de messages vocaux seront étudiés, mais ne seront mis en œuvre qu'après l'accord de l'Officier de Sécurité informatique (compatibilité avec la Politique de Sécurité Informatique du Ministère de la Défense avec l'ouverture vers le réseau téléphonique)

6 Haute disponibilité

Critère 15 : Une solution de redondance sera étudiée pour éviter de perdre les moyens de supervision et de dépannage, en cas de perte du serveur de supervision

7 Compatibilité avec les standards du Ministère de la Défense

Critère 16 : Les plates-formes Métier du Cetima seront peut être amenées à être gérées par la DIRISI, en 2014 .Des contacts avec la DIRISI seront pris, pour connaître leur standard et vérifier la compatibilité du logiciel, avec leur système de supervision

8 Gestion distribuée

Critère 17 : Par rapport au point précédent de reprise de la supervision par la DIRISI, l'architecture mise en place doit être compatible avec une gestion distribuée, répartie par plate-forme ou par lieu géographique (avec la mise en place de notion de soutien par base de défense). Par exemple, une console de supervision pourrait réaliser l'acquisition sur une plate-forme technique. La consolidation des données et la visualisation serait réalisée sur un site distant.

Par ailleurs, l'étude de la supervision des plates-formes du Cetima pourra servir de socle, pour l'implémentation d'une supervision des plates-formes SIH dans chaque hôpital, avec une remontée de synthèse globale au Cetima.

9 Support et Evolutions

Critère 18 : La solution doit être bien documentée, avec un support si possible gratuit. Une forte communauté avec nombreux forums est un gage d'un produit innovant, avec des évolutions régulières.

Critère 19 : Le système proposé doit être modulaire, ouvert à des évolutions futures et facilement interfaçable avec d'autres logiciels. Des améliorations et des évolutions seront proposées, en complément de la fonction supervision, pour optimiser les opérations de maintenance.

L'importance de ces critères

Numéro critère	Critère par importance	Importance *	Réponse/Notes **
1	Logiciel libre	10	Oui /Non
16	compatibilité avec les outils DIRISI	10	Oui /Non
17	Architecture distribuée multi site	9	Oui /Non
11	Supervision compatible SNMP	8	Oui /Non
12	Supervision par agents paramétrables	8	Oui /Non
13	Gestion des événements	8	Oui /Non
10	Gestion des utilisateurs	8	Oui /Non
14	Gestion des alarmes	8	Oui /Non
3	Logiciel sous linux	7	Oui /Non
15	Haute disponibilité	7	Oui /Non
18	Documentation et support	7	Note sur 5
19	Evolutivité, interfaçage avec outil de métrologie, graphe, reporting	6	Note sur 5
9	Génération de rapports	6	Oui /Non
4	Installation et configuration facile	5	Note sur 5
7	Interface web distante	5	Oui /Non
8	Graphe	5	Note sur 5
6	Interface conviviale	5	Note sur 5
2	Interface en français	5	Oui /Non
5	Découverte du réseau	4	Oui /Non

Importance : 10 Important, 1 souhaitable

Note : 5 = répond totalement au critère énoncé; 4 = répond en grande partie; 2 = répond partiellement; 1 = ne répond pas ; NA : Non Applicable

Ressources humaines

Le projet ne comprendra que moi-même de façon permanente. Néanmoins, il fera appel aux responsables d'exploitation (TME) et responsable applicatif de manière ponctuelle, pour expliquer le fonctionnement des plateformes métier SI et éclaircir certains points techniques, mis en œuvre au CeTIMA, non listés initialement dans le cahier des charges.

Budget : Coût nul (solution libre privilégiée)

Organisation : (extrait PAQ) Une réunion de lancement sera réalisée à Paris avec le comité de suivi pour le début du projet. Le projet sera réalisé à DRSSA Brest, avec un accès distant sur les SI métiers du CeTIMA, avec des visioconférences régulières (tous les 15 jours) et un ou deux séjours à Paris pour valider les revues de phases, avec le comité de suivi / MOA et réaliser le déploiement, sur les plateformes opérationnelles.

5. Etude des solutions du marché et choix de la solution de supervision (Phase 3)

Objectif :

Après avoir établi un bilan des logiciels de supervision du marché, il fallait choisir le logiciel de supervision, répondant au mieux aux critères du cahier des charges.

Méthodologie réalisée :

Une étude de l'état de l'art et des solutions de supervision du marché a été entreprise, en auditant certaines entreprises connues (DCNS, Thalès, Alcatel), pour connaître leur architecture de supervision. Lors de la visite du salon Linux Open Source à Paris [CRR-SALON-NP], les grands éditeurs du monde open source de la supervision ont été rencontrés et questionnés sur leurs produits et références sur le marché. Après les conférences (Centreon, Shinken), nous avons dialogué avec certains utilisateurs de sociétés françaises (SNCF, Air France, La Poste), sur leur retour d'expérience dans le domaine. Après une veille technologique sur les forums et les sites internet, une liste exhaustive de logiciels susceptibles de répondre à notre besoin a été rédigée. Après cette première présélection, une plate-forme de test a été installée sous un environnement VMware Server, pour un gain de temps et de facilité de mise en œuvre, afin de noter ces produits, suivant les critères du CdCF.

Livrables attendus :

-Document de synthèse « Choix de solution » (Bilan des solutions du marché, notation, choix du logiciel) [CHOIX-SUPERV-NP]

5.1. Offres des logiciels de supervision du marché

De nombreuses plates-formes de supervision existent aujourd'hui. Certaines se contentent de connaître l'état des nœuds du réseau, d'autres permettent de connaître l'état des services et des applications. Il y a même la possibilité de ressortir de nombreuses statistiques permettant plus qu'une supervision mais du reporting, avec une analyse fine et des tableaux de bord métier.

5.1.1. Offres propriétaires.

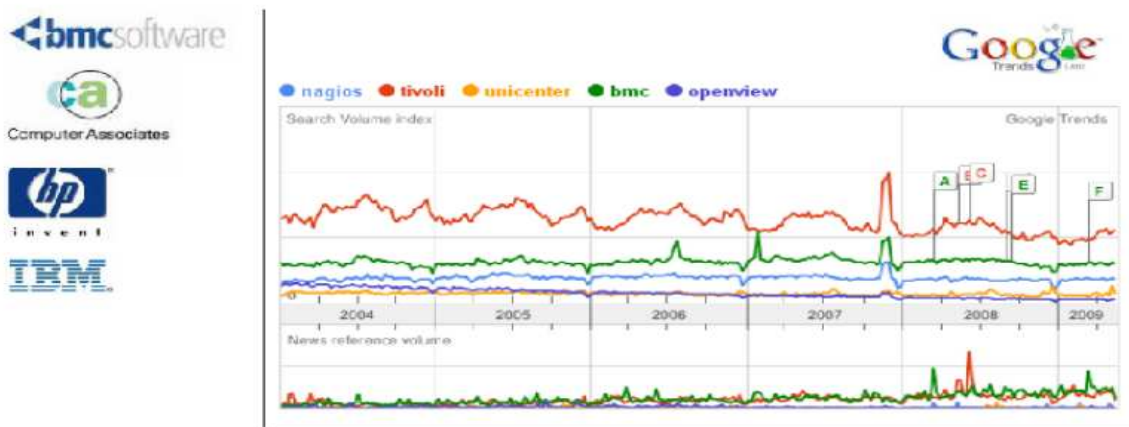
Le nombre d'éditeurs offrant des solutions intégrées de supervision est assez limité:

BMC (Patrol ou Mainview), Computer Associate (Unicenter), HP (gamme Openview) et IBM (Tivoli).

D'autres sociétés se spécialisent dans la supervision de domaine spécifique : Panorama (Altaworks) gère uniquement l'aspect sécurité, PathWAI (Candle) se spécialise principalement sur la supervision des applications.

Le point commun de ces solutions est un prix élevé d'acquisition, de formation et de support.

La solution d'un produit libre, pour notre outil de supervision, étant imposée dans le cahier des charges, nous n'entrerons pas, dans le détail de ces solutions propriétaires et redirigerons vers les liens internet des éditeurs fournis en fin de document.



Part de Marché des solutions de supervision - source RMLL Nantes 2010 – Olivier Jan

5.1.2. Offres des logiciels libres.

Le critère numéro un du cahier des charges était l'utilisation d'un logiciel libre.

Comme le montre l'étude réalisée par la CIGREF sur la « Maturité et gouvernance de l'Open Source, La vision des grandes entreprises » (voir tableau ci-dessous), aujourd'hui la supervision libre a un haut niveau de maturité dans le monde de l'entreprise. Depuis 2 à 3 ans, les projets de Supervision Open Source ne sont plus vus comme des « sous solutions », mais bien comme une véritable alternative fiable à des solutions propriétaires onéreux.

Catégories de solutions	Maturité		
	Technologique	d'usages	de moyens
Administration	2,92	2,70	2,59
Supervision	3,80	3,33	3,07
Gestion d'incidents	2,88	3,00	2,86
Asset Management	2,80	2,80	2,83
Gestion de configuration	3,00	2,80	2,67
Détection d'incidents / sondes	3,42	3,00	2,92
Ordonnancement	1,60	1,25	1,20

Note maximale : 4

Extrait : http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/Maturite_et_Gouvernance_de_l_Open_Source_CIGREF_2011.pdf

Les avantages de l'utilisation d'un produit libre (comme Nagios) sont multiples :

- Le code source disponible ;
- L'interopérabilité ;
- La possibilité de superviser des applications internes sans connecteur « propriétaire » ;
- Un développement collaboratif et ouvert ;
- Moins d'administration (car on n'administre que ce qu'on installe) ;
- Des coûts non liés au périmètre

Dans notre recherche de **produits open source de supervision**, nous avons listés les produits suivants (dont les caractéristiques sont détaillées en annexe 5)

- Nagios
- Shinken
- Zabbix
- Icinga
- OpenNMS

Pour information, certains produits ont été écartés de nos études pour les raisons suivantes :

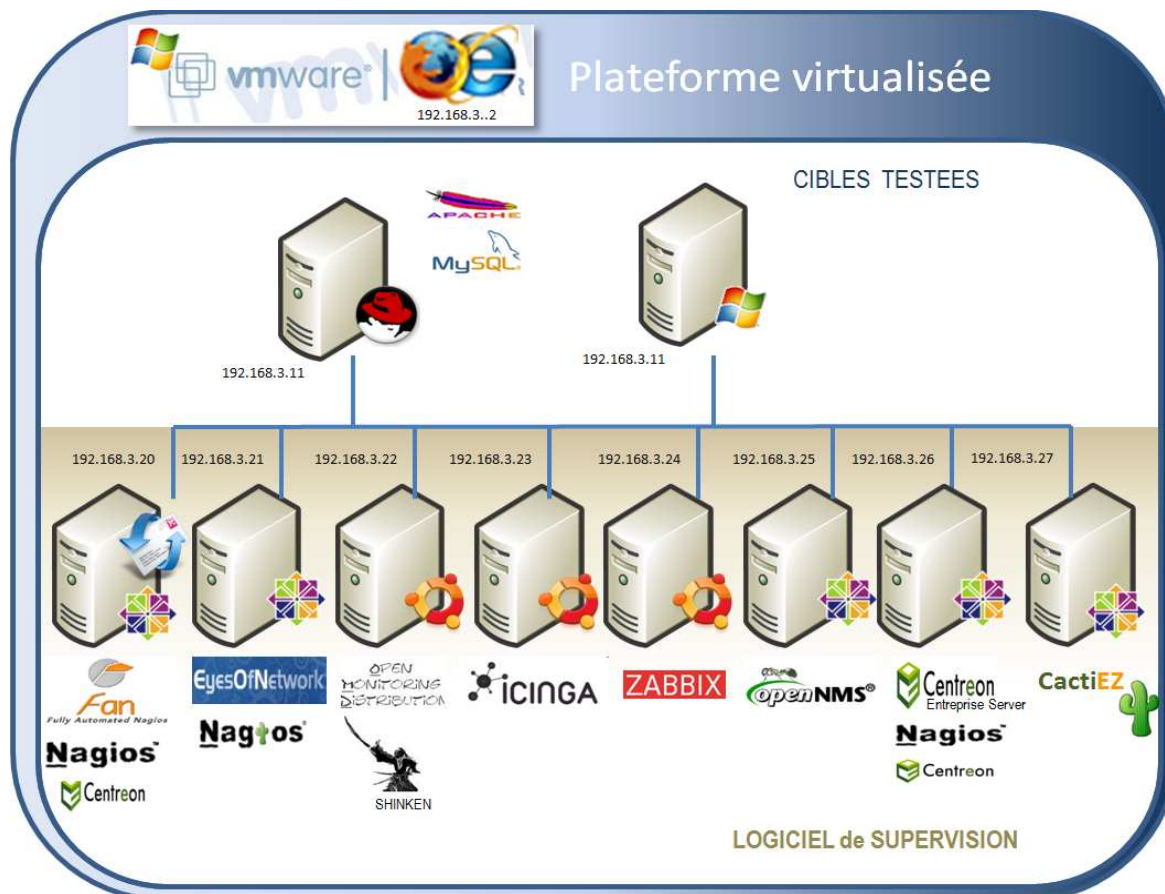
- OP5 et Hyperic (racheté par VMware) : pour leur manque de pérennité avec la priorité affichée par l'auteur pour la version Entreprise.
- Ganglia est très orienté cluster de calcul (HPC) et ne répond pas à tous nos besoins.

Pour répondre aux **besoins de métrologie** non couverts par les outils de supervision, nous avons recensés les produits suivants : MRTG, CACTI et MUNIN

5.2. Test et notation des logiciels Open Source

Pour économiser un temps considérable (d'installation, de configuration, de débogage..), nous avons utilisé des packages ou distributions préinstallées de solution de supervision, détaillés en annexe 6. Cette méthodologie a permis d'avoir rapidement des systèmes de supervision complets et stables, directement exploitables, avec des logiciels complémentaires. Non demandés dans le cahier des charges, ils pourront être proposés, comme axes de progrès et d'amélioration en phase 7 de notre projet.

Faute de solution « préformatée », les sources logicielles ont été installées sur un serveur linux standard sous Ubuntu 11.04.



Plateforme de test (adresse IP définies à titre indicatif)

Afin de contrôler les spécifications affichées et valider les critères du cahier des charges, les tests suivants ont été effectués : test host actif (check_ping), test service web (check_http), test SNMP (utilisation RAM serveur) sur deux machines avec des environnements différents (linux et Windows serveur 2003).

En complément, l'analyse de la documentation et du site éditeur du logiciel a confirmé si le produit pouvait répondre aux autres spécifications imposées par le cahier des charges (support, communauté active).

Un compte rendu a été rédigé [CH-SUPERV-DR], avec le tableau final de synthèse (voir page suivante)

Après le dépouillement des résultats, le logiciel Nagios, couplé avec l'interface d'administration Centreon a été retenu, pour la partie supervision. Pour les graphes de tendances, Centreon ne répondait pas à tous les besoins demandés. Aussi, même s'il ne fait pas partie des standards actuels de la DIRISI, nous avons retenu Cacti comme complément en métrologie. C'est le seul produit libre, émergent du marché, dans le domaine de la génération de graphiques d'évolution et de performance. Il est plus évolué que le logiciel de MRTG (Multi-Router Traffic Grapher) et plus complet que Munin.

Choix du logiciel de supervision

Extrait document [CH-SUPERV-NP] du 17/07/2011

LOGICIEL	Plateforme de test	Base de données possible	Logiciel libre	Compatibilité DIRISI	Architecture distribuée Multisite	SNMP	Agent paramétrable	Gestion événements	Gestion des utilisateurs	Gestion des alarmes	sous linux	Haute dispo.	Doc. Support	Evolution Métrologie Reporting	Génération de rapport	Installation et configuration facile	Interface web	Graphes	Interface conviviale	Interface français	Découvert réseau
CRITERE			10	10	10	8	8	8	8	8	7	7	7	6	6	5	5		5	5	4
NAGIOS + CENTREON	FAN +EON	Nagios (fichiers, MySQL) Centreon (MySQL, RRDTool)	OUI	OUI	Nagios en standard (NON) mais Addon (DNK, Martin), CENTREON (OUI)	OUI	OUI	OUI	OUI	OUI	OUI	OUI avec Addon	5/5	4/5	Addon	Nagios 2/5, Centreon 4/5	OUI	4/5	4/5	Nagios(NON), Centreon(OUI)	NON
CES	CES	MySQL, RRDTool	OUI**	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	5/5	4/5	Payante ou Addon	5/5	OUI	4/5	4/5	OUI	Payante
SHINKEN	Ubuntu avec script d'installation	fichier, MySQL, Oracle, SQLite	OUI	partiel*	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	3/5	3/5	Addon	3/5	OUI	3/5	3/5	NON	OUI
ZABBIX	Ubuntu + source du site	MySQL, Oracle, SQLite, Postgresql	OUI	NON	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	4/5	4/5	Addon	4/5	OUI	4/5	4/5	OUI	OUI
ICINGA	Ubuntu + source du site	MySQL, Postesql, Oracle	OUI	partiel*	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	4.5/5	4/5	Intégré + Addon	4/5	OUI	4.5/5	4.5/5	OUI	OUI
OPENNMS	OSE	Postgresql	OUI	NON	Add on	OUI	OUI	OUI	OUI	OUI	OUI, windows, mac OS	OUI	3.5/5	3/5	Addon	3/5	OUI	3.5/5	4/5	NON	OUI

Pour la fonction supervision à la DIRISI, Le produit retenu est Nagios couplé à Centreon. De plus, des compétences Nagios existent déjà en interne au CeTIMA, pour exploiter le produit.

Deux produits répondent aux critères : Nagios/Centreon (à installer de manière indépendante) et CES de Merethis, qui propose un produit packagé sous CentOS.

Actuellement aucun référentiel d'OS libre n'est défini au Ministère de la Défense, CES fonctionne sur CentOS (version libre Redhat), l'option de l'installation « manuelle » permet d'utiliser les produits sur CentOS, Redhat, Debian et Ubuntu. Dans le cadre du projet de mémoire CNAM, nous étudierons en détails Nagios et Centreon installés de manière manuelle. Cette démarche permettra de mieux comprendre leur fonctionnement propre et appréhender les problèmes de maintenance des deux logiciels.

La solution CES de Merethis offre différents avantages :

- 1- La société Merethis, qui développe le logiciel Centreon, ne peut offrir qu'un produit intégré stable et efficace, et propose des opportunités d'évolution technologique libre par rapport à Nagios
- 2- La solution intégrée est directement exploitation, sans gros paramétrage (CD ISO), par rapport à une solution Nagios/Centreon avec des installation longues et fastidieuses (serveur MySQL, apache, NdoUtils, plugin nrpe, ncsa..)
- 3- Des sondes sont fournis en standard pour les besoins du projet (base de données oracle, serveurs d'application (JBOSS, Tomcat 5), serveurs Web Apache)
- 4- Des outils de reporting (Centreon BI création automatique de rapports) répondent aux besoins du projet

Mais les deux derniers points sont des services payants de Merethis et il y a peu de retour d'expérience de ce produit encore jeune (3 mois),

6. Etude de la plateforme et de ses composants (Phase 4)

Objectif :

Le but de cette étape était de définir l'architecture de supervision et coder les composants nécessaires à son fonctionnement.

Méthodologie réalisée :

Une étude détaillée de Nagios/Centreon/Cacti a permis d'identifier les nombreux composants nécessaires à leur fonctionnement : des serveurs de base de données MySQL, un serveur web apache, agents, une configuration du protocole SNMP, un serveur messagerie postfix, associés à des packages linux...

Les flux entre les différents composants ont été dessinés et une architecture type retenue.

Un document a dû être établi pour chaque processus du contrôle et par éléments complémentaires à superviser. Les agents fournis en standard ne répondant pas à tous nos besoins, nous avons développé en python ou modifié des agents pour certains composants (oracle, JMX). Avec des fiches d'installation par composant, un dossier complet d'exploitation [EXP-SUPERV-DR] a été rédigé, décrivant aussi les opérations de maintenance et de sauvegarde.

Le SSA envisageait d'acheter le produit JBoss Operations Network (JON), une étude a vérifié les caractéristiques du produit et la possibilité d'interconnexion avec notre solution.

Livrables attendus :

- Etude détaillée de la plateforme de supervision [ETUDE-SUPERV-DR]
- Jeux de test [JX-SUPERV-DR]
- Dossier d'exploitation (installation, maintenance, sauvegarde) [EX-SUPERV-DR]

6.1 Présentation de Nagios

6.1.1 Généralités

Nagios est un logiciel libre sous licence GPL, retenu pour notre projet.

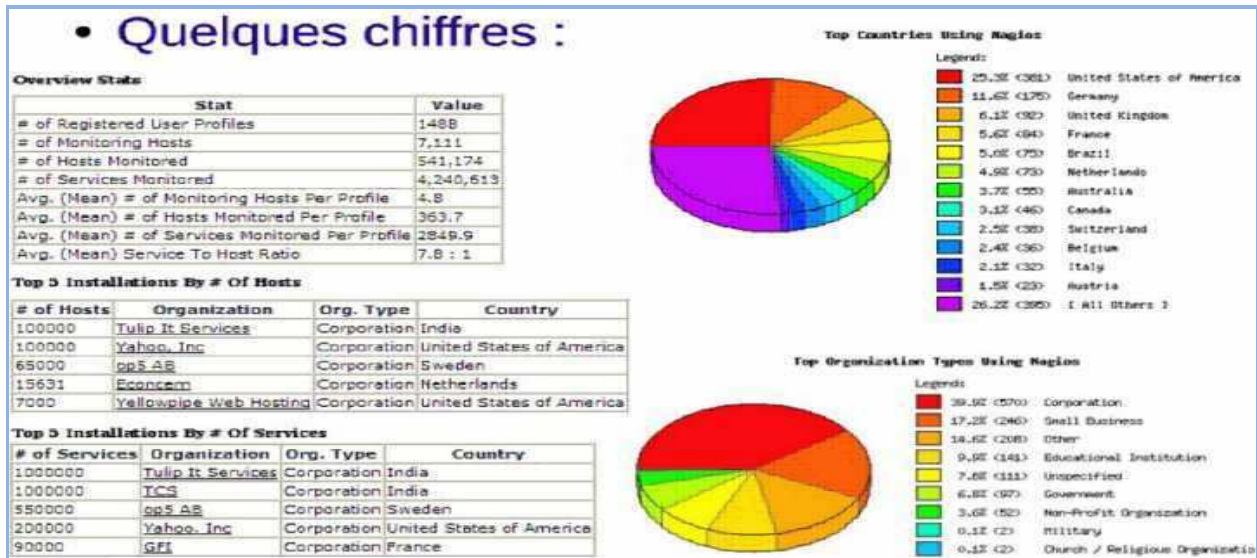
C'est aussi comme le montre le diagramme ci-dessus, le logiciel le plus connu et la référence dans le marché des solutions open source de supervision.



Part de Marché des solutions de supervision - source RMLL Nantes 2010 – Olivier Jan

Soutenu par une large communauté, le logiciel est reconnu et utilisé par de nombreuses sociétés à travers le monde, (comme le montre les tableaux ci-dessous), auxquelles on peut ajouter les noms de sociétés françaises comme : Air France, Thalès, Stade de France, RATP, CNRS(150hôtes), Arkea-Crédit Mutuel (330hôtes/1400services), CNRS (150hôtes), Inter Mutuelle Assistance (66 hôtes/189services) lastminute (105 hôtes/604services), Institut Pasteur (140hôtes/143services), Hôpitaux de Paris AP-HP...

L'Américain Ethan Galstad est à l'origine de la première version, développée en C, sous le nom de NetSaint en 1999. Il a depuis monté sa société et commercialise une version commerciale Nagios XI, tout en « continuant » à assurer le développement du Nagios Core. S'appuyant sur le Moteur Nagios Core, cette version inclut une nouvelle interface de gestion plus simple à mettre en place. La configuration des sondes peut être faite depuis l'interface web, au lieu du paramétrage des fichiers en ligne de commande. Ces fonctionnalités ont néanmoins un prix (fonction des hôtes) : 1-50 hôtes, 1295\$; 51-100 hôtes, 1995\$ et en illimité 2495 \$.



Source Nagios.org : utilisation de Nagios dans le monde

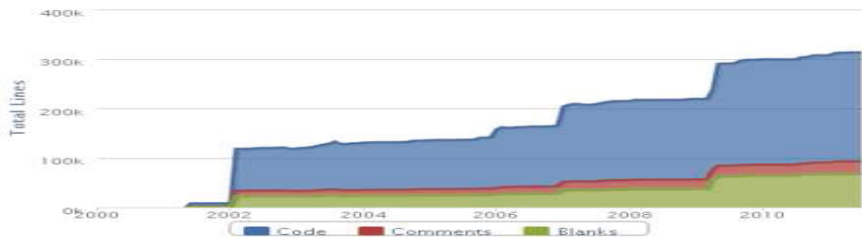
6.1.2. Fonctionnalités.

Voici les principales possibilités offertes par Nagios :

- Superviser des ressources machines (processeur, disques durs, mémoire, les fichiers de log, . . .) ;
- Superviser des services : SMTP, POP, HTTP, ICMP, LDAP, SNMP... ;
- Superviser des données comme la température, la luminosité, l'humidité par des sondes ;
- Possibilité de définir des gestionnaires d'événement, qui s'exécutent pour une résolution pro-active des problèmes ;
- Envoi d'alertes sous plusieurs formes (affichage, email, SMS...) vers des groupes de contact, avec une possibilité d'escalade ;
- Historisation des événements et données, qui peuvent servir pour l'élaboration de rapport ;
- Interface web pour suivre l'état du réseau, son évolution, ses problèmes ;
- Définition de plages horaires de surveillance ;
- Niveau de hiérarchie des équipements permettant de distinguer un serveur en panne et un serveur injoignable ;
- Conception simple de plugins extérieurs écrits dans différents langages de programmation : scripts shell (bash,ksh..),C++,perl,python, ruby,PHP... ;
- Support pour l'implémentation de serveurs de supervision redondants et distribués.

Nagios est compatible l'IP V6. En cas d'utilisation d'agent SNMP, il convient juste de vérifier que les MIB des équipements supervisés mesurent du trafic en IP V6.

6.1.3. Pérennité de nagios (Core/Entreprise).



Evolution du code de Nagios Core - Source : www.ohloh.net/p/nagios.
En 2009, avec le conflit ouvert avec Netway et le fork Icinga et , Ethan Galstad accepte des évolutions proposées par la communauté Nagios. Depuis plus évolution ...

Il convient de revenir sur la notion open core avec le modèle Community/Entreprise :

Un logiciel nommé *Community ou Core*, est proposé gratuitement, par un auteur ou une société. Une communauté lui propose des évolutions ou des patches. Une version commerciale payante *Enterprise*, avec des fonctionnalités avancées, est supportée par la même société éditrice du logiciel, qui reverse à la communauté, au bout d'un moment, les améliorations de la version Enterprise. Mais souvent, on constate peu d'évolution de la version libre, dû fait du produit payant, avec les prestations associées. C'est un peu la dérive ressentie pour les projets Hyperic et Zenoss, que nous avons écartés de notre évaluation. Certains experts du monde libre s'alarment aujourd'hui de cette dérive, qu'on pourrait comparer au shareware, où pour utiliser une version optimale, il faut investir dans la solution payante non bridée.

Avec la création de Nagios Entreprise en 2008 par Ethan Galstad et la commercialisation de Nagios XI, Nagios prendra-t-il le même chemin ? Depuis 2007, Ethan Galstad s'est éloigné de plus en plus de sa communauté, en laissant peu de temps à son équipe (Toon Voon et Andreas Ericson) pour faire évoluer le cœur de Nagios. Ce cercle officiel de développeurs reste fermé et silencieux aux demandes d'évolutions de la communauté mondiale (proposition pour Nagios 4 du produit Shinken développé en python (plus rapide que le codage en C), évolution de Nagios en mode distribué, abandon de NDO en natif...). Le manque de roadmap, de communication de son créateur a fait naître certaines tensions, qui ont entraîné en 2009 la naissance de « forks ».

Depuis 2 ans, Nagios Core n'a pas eu d'évolution majeure. Mais l'immense avantage de Nagios est sa fiabilité, et le nombre de ses utilisateurs, après plus de 10 ans d'utilisation, Il réalise parfaitement son travail d'ordonnancement, pour lequel il a été conçu, suivant le principe KISS (keep is Short an Simple - Simple et efficace). Son interface SGBDD n'est pas intégrée dans le Core et laisse l'opportunité à des optimisations de traitement (remplacement NDO obsolète par Merlin ou Centreon Broker, l'ajout de la haute disponibilité, Centreon Engine...)

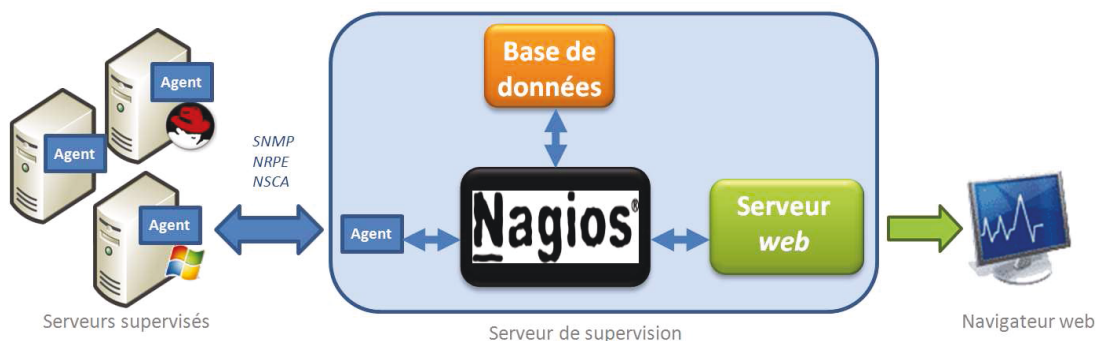
Sans forcément remettre en cause la pérennité du produit, on peut s'interroger sur l'évolutivité du produit à long terme, et on se doit de surveiller avec attention des produits ambitieux avec de nouvelles fonctionnalités (Shinken, Icinga), qui restent pour l'instant compatibles avec Nagios.

6.2. Fonctionnement Nagios et ses Agents/Centreon/Cacti

6.2.1. Fonctionnement de Nagios.

Nagios se décompose en 3 parties :

- un **ordonnanceur** gère l'ordonnancement et les dépendances des vérifications. Il détermine ensuite suivant les réponses, les actions à réaliser : mise à jour de l'affichage dans l'interface, génération d'un événement, notification ;
- une **Interface de contrôle** (sous forme d'application CGI), nécessitant un serveur web pour visualiser une vue d'ensemble du système d'information et d'éventuelles disfonctionnements ;
- des **sondes, agents ou plugins extérieurs** qui réalisent le test et revoit le résultat.



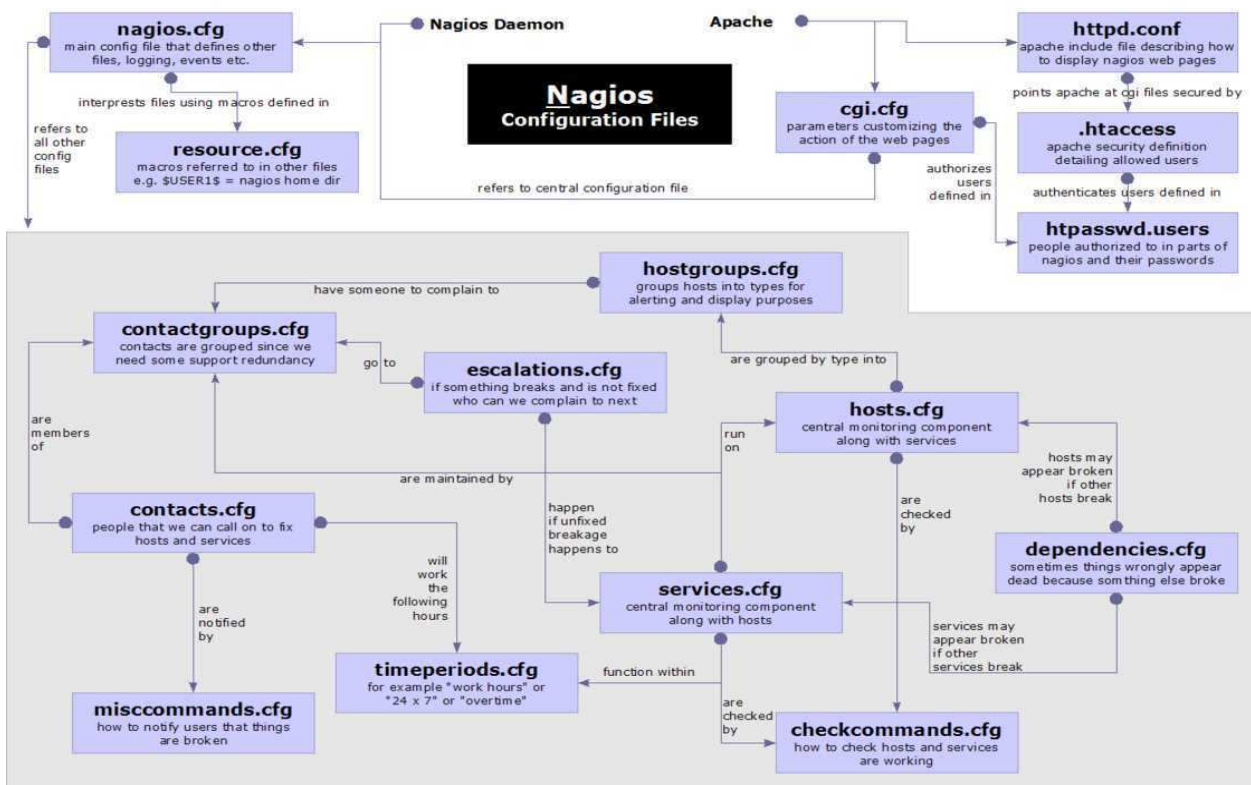
La principale force de Nagios est sa modularité, en laissant la supervision à des agents extérieurs, qu'il lance et dont il gère les résultats retournés.

Par ailleurs, Nagios n'est qu'un outil de supervision. Pour la métrologie, il faut lui associer un autre outil (Centreon, Cacti) pour la gestion des données de performance.

Pour éviter de solliciter deux fois l'équipement, certains agents retournent en un seul résultat, les valeurs d'états (analysées par la supervision), mais aussi des données de performance (stockées dans une base de données RDD) et mises à disposition des outils de métrologie.

La configuration de Nagios sans outil spécifique revient à éditer des fichiers texte, dont nous n'allons pas expliquer toutes les options possibles, et qui traitent chacun un thème bien précis. Nous ne listerons seulement que les principaux, qu'il est intéressant néanmoins de connaître pour comprendre le fonctionnement interne de Nagios, même si l'interface d'administration Centreon permet d'ignorer leur présence.

- **Hôte** (*hosts.cfg*) équipement supervisé défini par une adresse ip, un nom, un plugin d'état, éventuellement un parent.
- **Groupe d'hôtes** (*hostgroups.cfg*) Groupements de « hosts » fait pour faciliter l'administration (fonction, application) : serveur linux, serveur windows, boîtier de répartition de charte, firewall
- **Services** (*services.cfg*) On associe à chaque hôte les services à contrôler (ping, tcp, http, sgbd, ...).
- **Groupe de services** (*servicegroups.cfg*) Groupement de plusieurs services pour simplifier la configuration et optimiser l'affichage
- **Contacts** (*contacts.cfg*) personnes qui doivent être contactées (sms, mail, ...) en cas de défaillance d'un ou de plusieurs services.
- **Groupe de contacts** (*contactgroups.cfg*) rassemblement des contacts pour les alertes.
- **Tranches horaires** (*timeperiods.cfg*) définition des tranches horaires applicables (heures ouvrées, 24h24h, 7j7j). Elles sont utilisées pour la vérification des services et l'envoi des notifications.
- **Dépendances** (*dependencies.cfg*) dépendances entre les hôtes et les services.
- **Escalades** (*escalations.cfg*) définit l'escalade de notification pour un hôte ou un service donné.
- **Commandes** (*commands.cfg*) déclaration des commandes de vérification, de notification et de gestion des événements.



Le schéma précédent montre l'interconnexion entre chacun des fichiers texte de configuration. Leur paramétrage et leur exploitation au quotidien peut devenir rapidement complexe, laborieux et inadapté aux grands environnements. Une interface conviviale devient un atout indispensable, la plus évoluée est Centreon, que nous avons retenue et que nous décrivons au paragraphe 6.2.3.

6.2.2. Agent, Plugin de Nagios

6.2.2.1. Agent.

Comme nous l'avons dit, Nagios ne dispose pas de mécanismes internes, pour récupérer l'état d'un service ou d'un hôte distant. C'est le rôle des agents, plugins, modules ou greffons, qui effectuent les vérifications sur la ressource distante. Nagios utilise le résultat qu'ils retournent, pour déterminer l'état de l'hôte ou du service.

Distribués indépendamment du moteur Nagios, il est possible de créer ses propres plugins pour les adapter à des services spécifiques à l'entreprise. Ils peuvent être développés dans n'importe quel langage de programmation (Perl, C, shell, wmi ...), il suffit de respecter la norme Nagios avec des codes retour suivants :

- **0 = tout va bien (OK)**
- **1 = avertissement (WARNING)** – seuil alerte dépassé
- **2 = alerte (CRITICAL)** – le service ne fonctionne pas
- **3 = inconnu (UNKNOWN) ou UNREACHABLE**, il est impossible de déterminer l'état du service

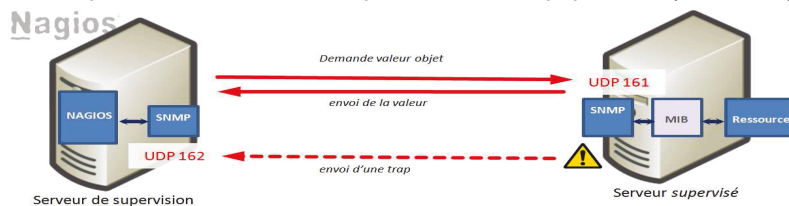
Il y a la possibilité de renvoyer une ligne de texte décrivant l'état courant, pour aider au diagnostic.

Le serveur Nagios est déjà fourni avec un package de plugin standards, pour les utilisations les plus courantes. Des sites dédiés (exemple Nagios Exchange) mettent à la disposition de la communauté tout un lot de plugins, pour les cas les plus complexes. Il néanmoins parfois difficile de faire le bon choix, étant donné le grand nombre et la qualité aléatoire parfois proposée.

6.2.2.2. Différentes Méthodes.

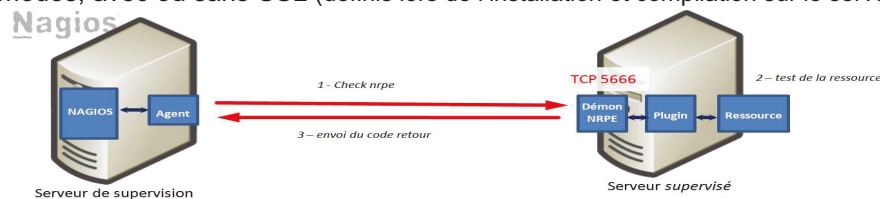
Les plugins peuvent fonctionner selon 3 méthodes :

- [Avec le protocole SNMP](#), décrit au paragraphe précédent, en interrogeant la MIB distante (UDP161), ou réceptionnant une alerte trap venant de l'équipement (UDP 161).



- [Surveillance passive via le plugin Nagios NRPE](#) (Nagios Remote Plugin Executor).

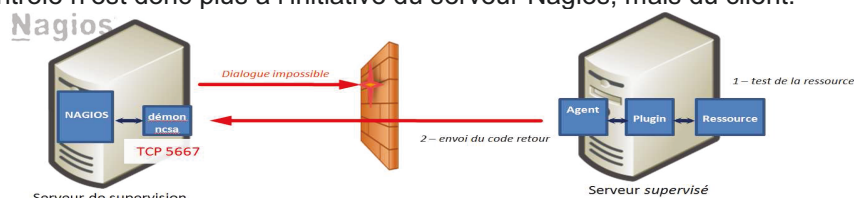
Le module NRPE Nagios s'installe sur l'équipement à superviser. Il est appelé depuis le serveur Nagios via la commande `check_nrpe`. Le démon NRPE reçoit la demande de vérification sur le port TCP 5666, exécute la commande associée (définie dans le fichier de paramétrage), retourne le résultat. NRPE peut fonctionner sous 2 modes, avec ou sans SSL (définis lors de l'installation et compilation sur le serveur distant).



Fichier nagios.cfg (sur le serveur de supervision):	Fichier nrpe.cfg commun à tous les serveurs (ou <code>nrpe_local.cfg</code> spécifique à un serveur supervisé):
<pre>define command{ command_name check_nrpe_load command_line \$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c check_load }</pre>	<pre>command[check_load]=usr/lib/nagios/plugins/ check_load -w 15,10,5 -c 30,25,20</pre>

- [Surveillance passive via le plugin Nagios NSCA](#) (Nagios Service Check Acceptor).

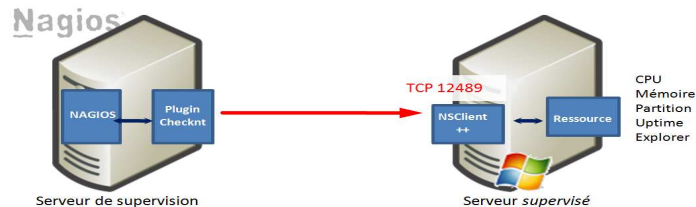
L'utilisation de NRPE nécessite d'avoir accès à la machine supervisée. Si on ne peut pas y accéder (exemple firewall entre client et serveur Nagios), on utilise le client NSCA. Installé directement sur la machine supervisée, il exécute régulièrement des vérifications selon la planification, qui a été décidée en local. Il envoie ensuite les résultats au serveur Nagios, qui les reçoit via son démon NSCA pour traitement. Ce contrôle n'est donc plus à l'initiative du serveur Nagios, mais du client.



Cas de NSClient++ pour windows

NSClient++ est un plugin pour environnement Windows ; permettant de récupérer d'importantes informations sur une machine distante Windows. Il permet l'utilisation des agents nagios standards.

- **check_nt** (TCP12489) pour le contrôle de la version de Windows (CLIENTVERSION), la moyenne de la charge CPU sur les x dernières minutes (CPULOAD), le temps d'activité sans interruption du serveur (UPTIME), la taille/pourcentage d'occupation des disques Windows (USEDISKSPACE), l'utilisation de la mémoire (MEMUSE) et l'état d'un ou plusieurs services (SERVICESTATE ou PROCSTATE)



- **check_nrpe** (TCP5566) propose plus de fonctionnalités en pouvant commander l'exécution d'un script distant pour procéder au test d'une ressource avec différents modules (CHECKDISK, CHECKSYSTEM, CHECKCPU, CHECKUPTIME, CHECKSERVICESTATE, CHECKPROCSTATE, CHECKMEM, CHECKHELPERS) et les NRPE Handler.

Cas de test par ligne de commande via SSH

Souvent, les responsables applicatifs ne sont pas enclins à installer des agents sur leurs serveurs, il y a donc la possibilité de lancer directement des commandes à distance par SSH

exemple : `ssh serv1@nagios '/usr/local/nagios/libexec/check'`

Cette méthode pose le problème de l'authentification, avec la saisie du mot de passe par Nagios. Il est donc nécessaire d'utiliser l'authentification asymétrique (génération de clé par ssh-keygen (attention passphrase vide (risque SSI, même si l'agent nagios a un compte sans privilège), déploiement ssh-copy-id).

L'avantage de SSH est qu'il est présent en standard sur la majorité des serveurs linux et évite le déploiement d'un agent, sur le serveur distant.

Le gros inconvénient de SSH est qu'il nécessite trois fois plus de ressources (demandée par la phase d'authentification) que l'agent nrpe. L'utilisateur Nagios doit aussi avoir un accès en Shell, sur le serveur distant.



Liste de tests fournis en standards par nagios

check_apt	check_breeze	check_by_ssh	check_clamd
check_cluster	check_dbcp	check_dig	check_disk
check_disk_amb	check_dns	check_dummy	check_file_age
check_flexlm	check_ftp	check_http	check_icmp
check_ide_smart	check_ifoperstatus	check_ifstatus	check_imap
check_ircd	check_load	check_log	check_mailq
check_mrtg	check_mrtgtraf	check_nagios	check_ntp
check_nt	check_ntp	check_ntp_peer	check_ntp_time
check_nwstat	check_oracle	check_overcr	check_ping
check_pop	check_procs	check_real	check_rpc
check_sensors	check_smtp	check_ssh	check_swap
check_tcp	check_time	check_udp	check_ups
check_users	check_wave		

6.2.3. Fonctionnement de Centreon.

Créée en 2003, sous le nom d'Oreon, par Cédric Temple, Centreon est une couche applicative qui se positionne au-dessus de Nagios. Elle intègre une interface multi-utilisateurs complète et intuitive, avec une gestion de la configuration Nagios et une console de supervision apportant des fonctionnalités avancées. C'est un projet français, avec une large communauté d'utilisateurs. En tant qu'éditeur, Merethis propose aujourd'hui un support et des extensions payantes, mais laisse le cœur de Centreon sous licence GPL et donc en libre accès.

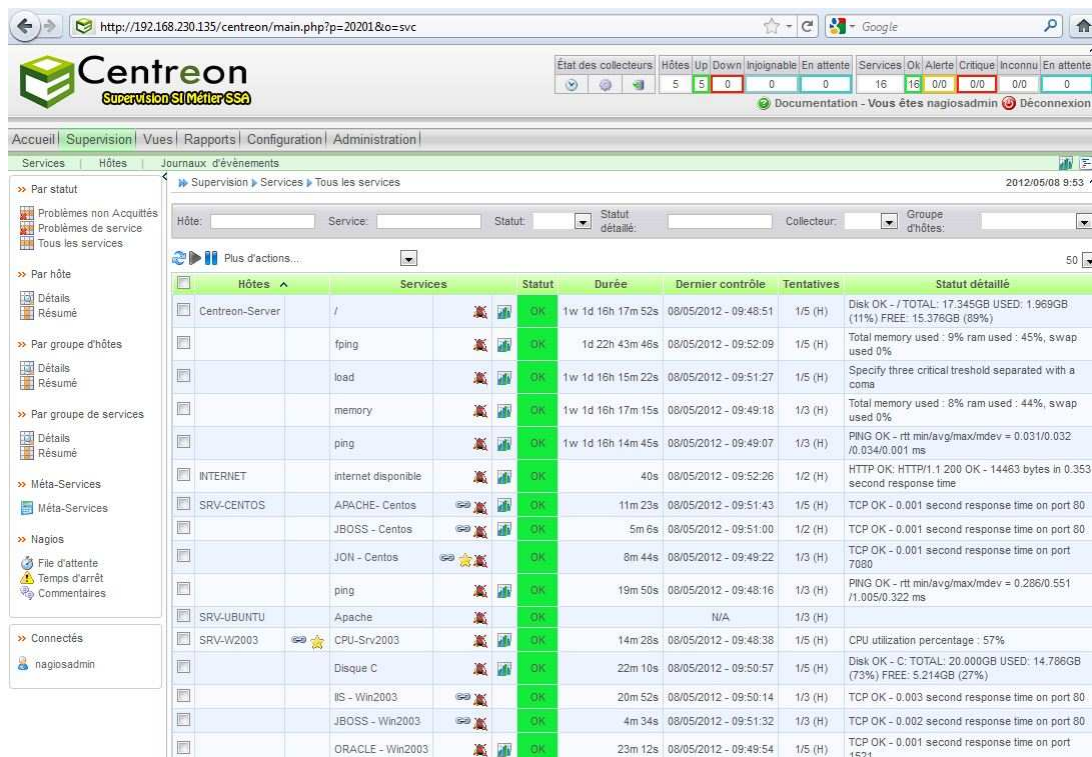
Centreon est divisé en plusieurs composants :

- **CentreonWeb** (appelé aussi par Centreon) avec une interface web présentant des tableaux de bords (monitoring) et quelques graphiques de performance.
- **CentreonCore** est le cœur de la solution et permet aux différents composants d'interagir.
- **CentreonStorage** est l'outil de métrologie de Centreon. Il récupère les données envoyées par Nagios, stocke les informations, dans deux bases : RRDTools (pour conserver les données sur de grandes périodes) et MySQL Centreon Storage 2 (pour régénérer les fichiers RRDTools en cas de problème).

Centreon assure une gestion graphique des fichiers texte de configuration Nagios (*.cfg) et des plugins. Ces informations de configuration sont stockées dans une autre base de données. Ces fichiers sont générés à la demande et peuvent être testés, avant la mise en production.

Il offre une gestion simplifiée des traps SNMP, avec un chargement suivi d'une compilation automatique des MIB et une remontée d'alertes de SNMPTT vers Nagios. Chaque OID a son entrée et peut être associé à un service (opération réalisée par le script traphandler fourni par Centreon).

Le logiciel permet d'intégrer des modules supplémentaires : CentreonSyslog, CentreonWeatherMap, CentreonNTOP, CentreonMap, CentreonDisco.



The screenshot shows the Centreon web interface. At the top, there's a navigation bar with 'Accueil', 'Supervision', 'Vues', 'Rapports', 'Configuration', and 'Administration'. Below that, there's a 'Services' section with a table of monitoring data. The table has columns for Hosts, Services, Status, Duration, Last Control, Attempts, and Detailed Status. The 'Status' column is highlighted in green for 'OK' entries. The 'Detailed Status' column provides specific metrics for each service, such as disk usage, memory usage, and response times.

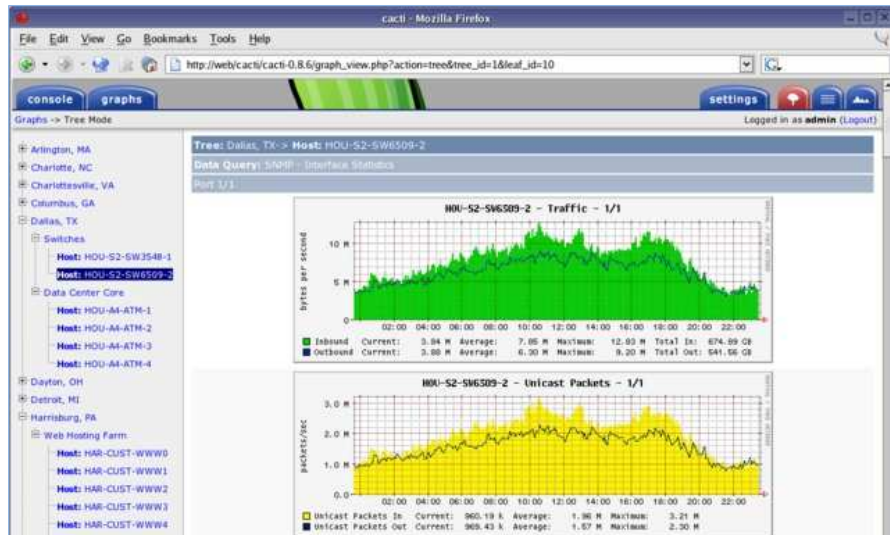
Hôtes	Services	Statut	Durée	Dernier contrôle	Tentatives	Statut détaillé
Centreon-Server	/	OK	1w 1d 16h 17m 52s	08/05/2012 - 09:48:51	1/5 (H)	Disk OK - /TOTAL: 17.345GB USED: 1.969GB (11%) FREE: 15.376GB (89%)
	fping	OK	1d 22h 43m 46s	08/05/2012 - 09:52:09	1/5 (H)	Total memory used : 9% ram used : 45%, swap used 0%
	load	OK	1w 1d 16h 15m 22s	08/05/2012 - 09:51:27	1/5 (H)	Specify three critical threshold separated with a coma
	memory	OK	1w 1d 16h 17m 15s	08/05/2012 - 09:49:18	1/3 (H)	Total memory used : 8% ram used : 44%, swap used 0%
	ping	OK	1w 1d 16h 14m 45s	08/05/2012 - 09:49:07	1/3 (H)	PING OK - rtt min/avg/max/mdev = 0.031/0.032 /0.034/0.001 ms
INTERNET	internet disponible	OK	40s	08/05/2012 - 09:52:26	1/2 (H)	HTTP OK: HTTP/1.1 200 OK - 14463 bytes in 0.353 second response time
SRV-CENTOS	APACHE - Centos	OK	11m 23s	08/05/2012 - 09:51:43	1/5 (H)	TCP OK - 0.001 second response time on port 80
	JBOSS - Centos	OK	5m 6s	08/05/2012 - 09:51:00	1/2 (H)	TCP OK - 0.001 second response time on port 80
	JON - Centos	OK	8m 44s	08/05/2012 - 09:49:22	1/3 (H)	TCP OK - 0.001 second response time on port 7090
	ping	OK	19m 50s	08/05/2012 - 09:48:16	1/3 (H)	PING OK - rtt min/avg/max/mdev = 0.286/0.551 /1.005/0.322 ms
SRV-UBUNTU	Apache	OK		N/A	1/3 (H)	
SRV-W2003	CPU-Srv2003	OK	14m 28s	08/05/2012 - 09:48:38	1/5 (H)	CPU utilization percentage : 57%
	Disque C	OK	22m 10s	08/05/2012 - 09:50:57	1/5 (H)	Disk OK - C: TOTAL: 20.000GB USED: 14.768GB (73%) FREE: 5.214GB (27%)
	IS - Win2003	OK	20m 52s	08/05/2012 - 09:50:14	1/3 (H)	TCP OK - 0.003 second response time on port 80
	JBOSS - Win2003	OK	4m 34s	08/05/2012 - 09:51:32	1/3 (H)	TCP OK - 0.002 second response time on port 80
	ORACLE - Win2003	OK	23m 12s	08/05/2012 - 09:49:54	1/5 (H)	TCP OK - 0.001 second response time on port 1521

L'interface graphique se compose de six vues :

- Une page d'accueil « home » reprenant le « tactical overview » de Nagios qui offre une vue globale des événements, des incidents et de certaines statistiques de performance.
- Une page « monitoring » avec plusieurs vues disponibles ;
- Une page « views » pour tous les graphiques et une cartographie du réseau ;
- Une page « reporting » sous forme de tableau de bord ;
- Une page « configuration » et « administration » pour la gestion des accès utilisateurs.

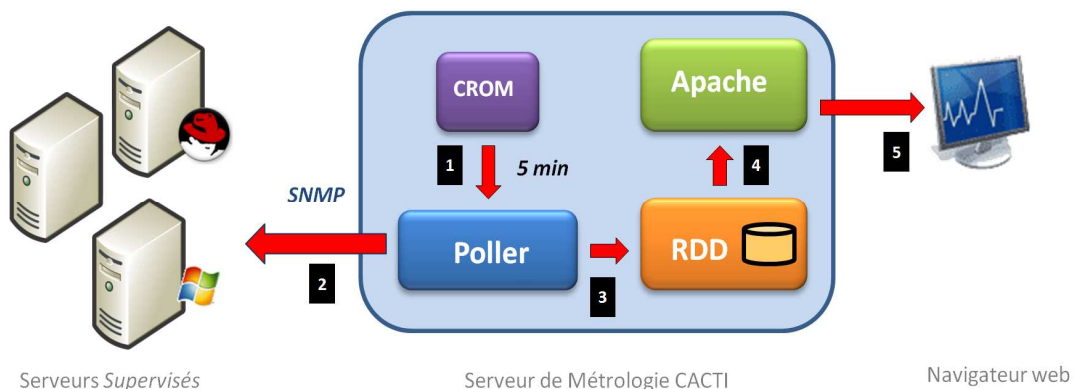
6.2.4. Fonctionnement de Cacti

Pour l'instant limités à certains templates, les graphes de Centreon se contentent de tracer certaines données de performance remontées par Nagios, sans offrir la possibilité de les traiter pour obtenir des graphes « logiciel/métier », comme pour un serveur web ou une base données. Il est donc nécessaire d'utiliser un logiciel de métrologie dédié, qui mesure ces indicateurs.



Nous rappellerons que Cacti n'interprète pas les résultats obtenus et n'est donc pas destiné à alerter quiconque en temps réel à propos de problèmes éventuels (Même si le plugin thold pourrait assurer cette fonction). Cacti n'est pas un outil de supervision, mais simplement comme MRTG, un générateur évolué de graphes. Il n'y a malheureusement pas de lien direct avec Nagios (à part un plugin d'intégration à l'état bêta de lien d'URL : NPC)

Son fonctionnement consiste, à intervalles réguliers (fréquence paramétrée à 5 minutes dans le fichier cron), à réaliser des requêtes SNMP par un poller, qui ordonnance les scripts et enregistre les résultats dans une base RRD. Cette dernière peut être interrogée avec RRDTool à la demande de manière dynamique pour générer des graphes, de manière personnalisée et aisée à l'aide de modèles (templates) en xml, avec un affichage rapide sous forme d'arborescence.



Des plugins peuvent être intégrés à Cacti (comme Weathermap (cartographie), thold (alerte)...) pour augmenter ses fonctionnalités.

6.3. Architecture de la plate-forme.

L'association de Nagios et de Centreon permet la constitution d'une solution de monitoring à la fois puissante et efficace, couplée à des agents de contrôle adaptables à chaque test.

Pour intégrer ces éléments, nous allons maintenant définir le plan d'architecture de notre plate-forme de supervision, (voir schéma paragraphe 6.3.3), les pré-requis pour leurs installations et les interactions entre les différentes couches logicielles.

6.3.1. Les logiciels pré requis (voir synoptique page suivante)

Apache

Un serveur web est indispensable pour l'accès à l'interface web en php de Centreon et cacti.

RDDtools et la base de données RRD (Round Robin Database)

Développé par Tobias Oetiker (créateur de MRTG), le fonctionnement de ce SGBD est assez simple par rapport à MySQL. La base de données est de taille fixe, avec un remplissage cyclique et adaptée pour la sauvegarde de données de performance chronologiques et le tracé de graphes.

Le mécanisme de remplissage des RRD, dans notre architecture est donc le suivant : les résultats des sondes sont remontés depuis les hôtes vers Nagios. Nagios inscrit les données reçues dans un fichier intitulé perfddata. Les données de ce fichier sont récupérées par Centstorage, qui les inscrit dans une base de données MySQL de secours (Centreon Storage2), et les ajoute à la fin de la base RRD.

Lors qu'un utilisateur demande la consultation d'un graphique, la page Centreon concernée appelle le binaire rrdtool, qui se charge de générer les graphiques.

Bases de données MySQL

- **Base NDO**

En standard, Nagios stocke les résultats des vérifications dans des fichiers binaires, peu optimisés et non réutilisables par des programmes tiers. Nous utilisons NDOUtils (Nagios Data Output Utils) pour stocker ses résultats dans une base de données NDO, mis à disposition de Centreon, qui les utilise pour réaliser le tableau de bord des états.

NDO est composé du module NDOMOD, lancé sur le serveur Nagios, Ce module récupère les informations remontées par Nagios et les transmet au daemon NDO2DB, qui écoute sur un port TCP 5668 et écrit les données reçues, dans la base de donnée MySQL NDO.

- **Centreon 2 et Centreon2 Storage**

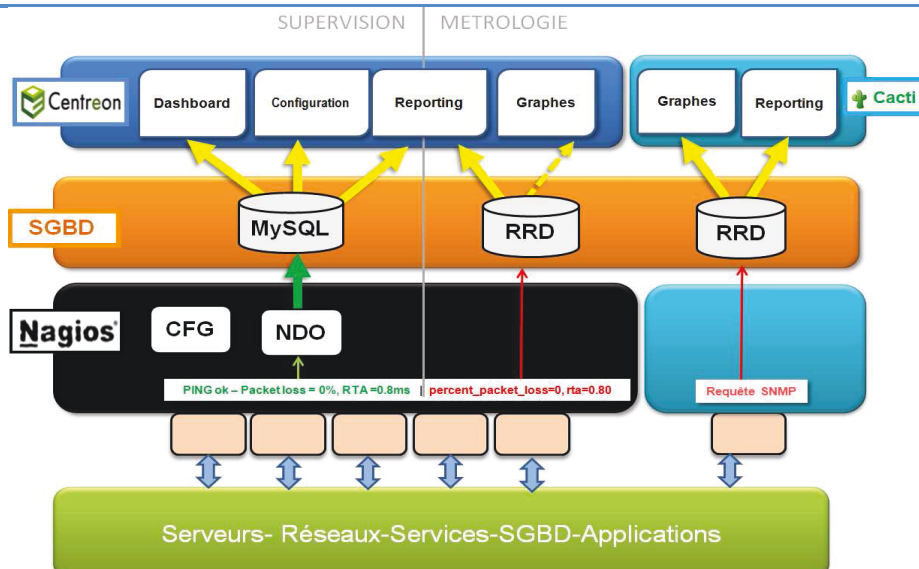
Elles sont respectivement la base de données de configuration de Centreon et la base de stockage des données de performances en secours de la base de données RRD.

- **DBCacti** est la base de données de configuration de Cacti

Postfix

Couplé à l'outil mailx, Postfix est utilisé en serveur relais de messagerie pour l'envoi des alertes vers le serveur de messagerie du CeTIMA et les boîtes aux lettres des groupes de contacts.

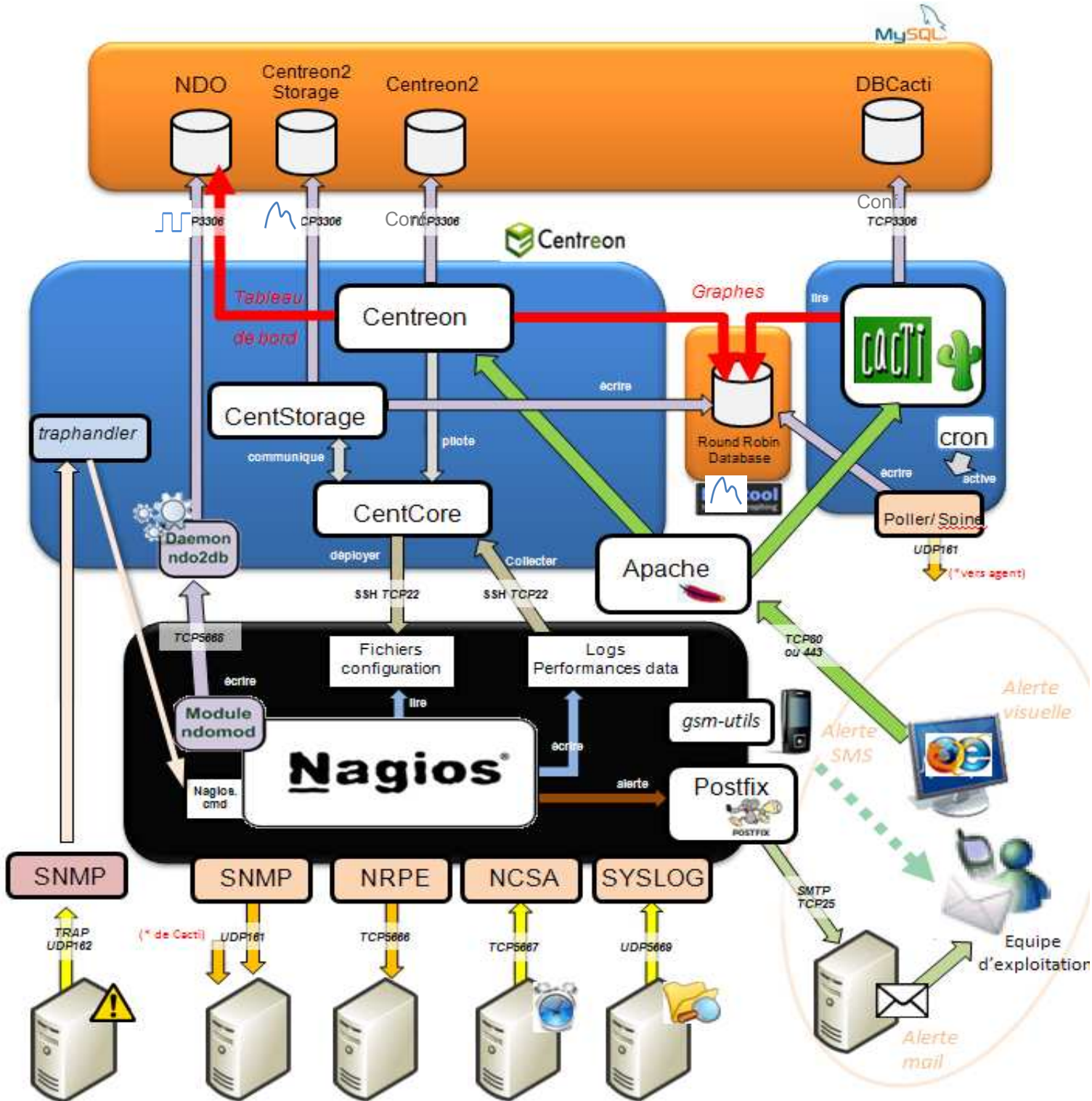
6.3.2. Flux de remontée des informations



Les agents pilotés par Nagios retournent les résultats des tests réalisés sur les serveurs et services supervisés. Comme le montre le schéma, **les états de supervision** sont stockés dans la base MySQL NDO, qui sert à générer le tableau de bord du système.

Nagios ne sait pas gérer **les données de métrologie**, mais les récupère et les stocke dans une base de données RRD. Centreon peut ensuite avec les outils RRDtools, gérer des graphes simples à la demande des utilisateurs. Pour les graphes plus complexes, la convivialité des templates de Cacti est mise à profit, pour générer les autres graphes de performance.

6.3.3. Synoptique de l'architecture



6.3.4. Sécurité.

La sécurité sous Linux passe notamment par la gestion des accès aux fichiers. Pour cette raison et se prémunir des dysfonctionnements des logiciels, il est préférable, de passer par un utilisateur aux accès limités, autre que le root pour démarrer ces logiciels. Cette logique générale s'applique à Nagios, Centreon et Cacti, comme aux outils associés.

De même une attention particulière sera réalisée, lors de la création des bases de données MySQL et RDD, pour définir un mot de passe complexe, pour assurer une sécurité optimale, suivant les règles SSI.

6.3.5. Mise en œuvre

Une étude complète du fonctionnement de Nagios a été réalisée (synthèse disponible en annexe 3), avec en particulier le détail des autres fonctionnalités :

- Gestion des contacts ;
- Ordonnancement des vérifications (type d'état, valeur des états, séquençage, dépendance d'hôtes et services)
- Réparation pro-active (Gestionnaire d'événement) ;
- Fonctionnement des remontées d'alertes/Escalade (alerte visuelle, sonore, email, SMS, RSS...).

6.4. Etude détaillée des logiciels éditeurs et agents Nagios

Chaque indicateur identifié a été intégré à un dossier d'étude par matériel ou technologie : ressources serveurs (disque, CPU, RAM), boîtier de répartition de charge F5, serveurs web apache, bases Oracle, serveurs JBoss, serveurs Citrix, serveur SMTP, serveur Rapport Mensuel...

Etude des logiciels de contrôle fournis avec le logiciel ou le matériel

Les interfaces d'administration des applicatifs ou des matériels (voir captures ci-dessous) ont été examinées, pour savoir si elles étaient interfaçables avec Nagios, en particulier JBoss Operation Network (JON) de Redhat, qu'envisageait d'acquérir le CeTIMA. Son fonctionnement est expliqué au paragraphe suivant.



Oracle Enterprise Management 11g

Console JBoss / Outil VisualVM

Console administration boîtier F5

Etude des Sondes Nagios par technologie à superviser

Certains « checks » étaient fournis en standard avec Nagios/Centreon (Tests disk, CPU, RAM, test port SMTP...). D'autres ont nécessité des recherches poussées sur internet. Des agents Nagios ont été adaptés à notre environnement : check_oracle, check_oracle_health, check_jmx... ou des templates de graphes Cacti .

Les scripts shell déjà utilisés ont été « décortiqués », en plusieurs fonctions élémentaires et intégrés dans un processus agent NRPE/commande Nagios, expliqué précédemment.

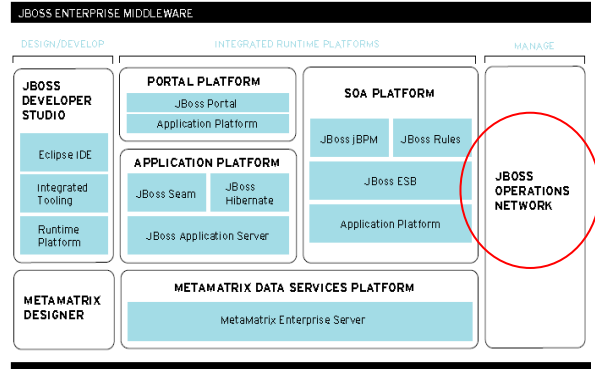
Il faut signaler que certains agents sont complexes à mettre en œuvre et nécessitent une compétence pointue en Java (leur maintenabilité sera discuté avec le MOA, en fin de phase 5 du projet)

La phase suivante du projet consistera à contrôler la mise en œuvre de ces outils et contrôler qu'ils sont efficaces, mais aussi maintenables, évolutifs et modifiables sans trop d'investissement par l'équipe TME, qui assurera leur maintenance préventive et corrective.

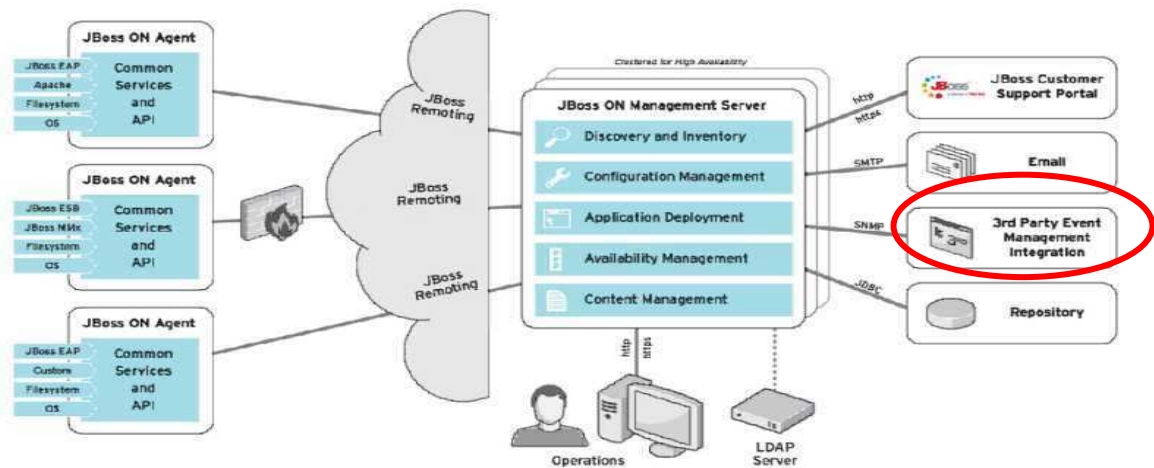
6.5. Etude de JBoss Operation Network (JON)

JON (JBoss Operation Network) est la version commerciale de l'outil open source JOPR (fusionné avec le projet RHQ). Il s'intègre dans l'offre complète Redhat, comme le montre le schéma.

RHQ est en fait le produit de la collaboration depuis 2004, entre la société Hyperic (connue pour ses produits de supervision) et Redhat.



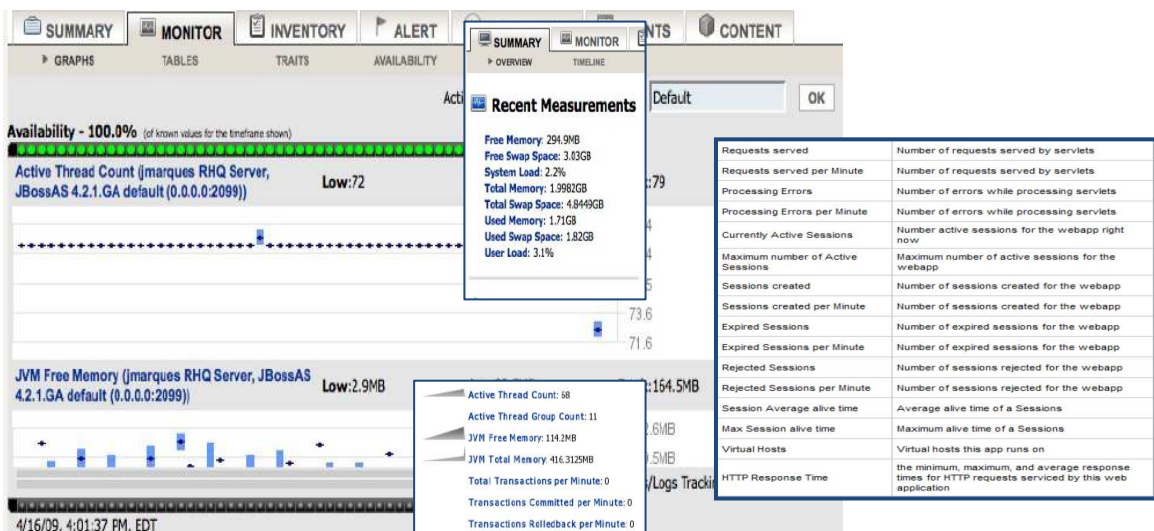
Cet outil peut donc être considéré comme un concurrent de Nagios, puisqu'il permet de surveiller plusieurs types de ressources: système, réseau, java... Le déploiement de JON passe aussi par l'installation d'agent sur les systèmes distants, qui permettent l'accès à la configuration. Ces agents ont la capacité de découvrir automatiquement les ressources dont ils ont la responsabilité. Le serveur JON prend ensuite en charge la synthèse des informations collectées et la présentation. L'outil peut être installé tant sur des serveurs Linux que Windows.



Traps SNMP possibles avec Centreon /Nagios

En conclusion, c'est un outil puissant, qui permet de faire remonter facilement des informations sensibles, comme le montre les vues ci-dessous (nombre de requêtes/min, nombre de threads utilisés, sessions rejetées...).

JON propose des agents ou connecteurs pour superviser les serveurs Tomcat, Jboss, Apache, Oracle... Des alertes visuelles ou mail peuvent être programmées suivant des seuils d'alertes, ainsi que des traps SNMP vers des outils extérieurs.



7. Maquettage (Phase 5)

Objectif :

Une maquette de l'outil a été réalisée sur une plate-forme VMWare, pour valider les choix techniques des phases précédentes.

Méthodologie réalisée :

La plateforme de maquettage était composée des serveurs, des systèmes d'exploitation représentant les différents composants des plateformes SI Métier du CeTIMA.

Les logiciels de supervision ont été installés, suivant les procédures d'installation rédigées, lors de la phase précédente.

Les tests réels ont validé :

- Le fonctionnement interne de l'architecture retenue ;
- La remontée par les agents développés des indicateurs définis dans le cahier des charges ;
- Les visualisations des tableaux de bords et graphes sur la console de supervision ;
- Les alertes par email et SMS ;
- Les risques d'utilisation de certains composants jugés trop complexes ou pas assez aboutis.

Livrables attendus :

- Résultats des tests [[MAQ-SUPERV-DR](#)]
- Manuel Utilisateur [[UTIL-SUPERV-DR](#)]

7.1 Plateforme installée

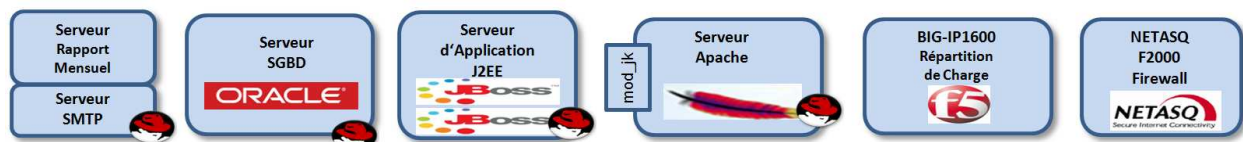
N'ayant pas pléthore de matériels, une machine Biprocesseur avec 8Go de RAM a été utilisée pour monter un environnement VMWare, hébergeant trois serveurs cibles, installés avec trois systèmes d'exploitation différents (Centos/Redhat, Ubuntu/Debian, Windows 2003R2) et deux stations de supervision. L'installation et le paramétrage des différents serveurs (en particulier JBoss et Oracle) ont nécessité beaucoup de patience, et une recherche longue et attentive sur internet, pour se former et avoir une documentation fiable, avant d'interfacer correctement les produits.

Configuration :

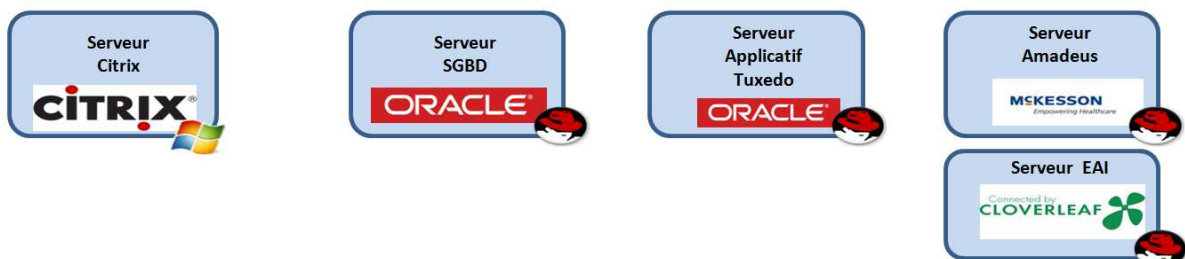
Machine1	Machine2	Machine3	Superv1	Superv2
CentOS/Redhat	Ubuntu/Debian	Windows 2003	SUPERV1	SUPERV2
Apache JBoss6 Oracle 10g JON 2.4, agent RHQ Postgresql Agent SNMP, nrpe	Apache JBoss6 Oracle Xe 10g (faute de puissance) Agent RHQ Agent SNMP, nrpe Répertoire fichier test	JBoss6 Oracle 10g JON 2.4, Agent RHQ SMTP, IIS Agent NSClient++	Nagios Centreon Cacti Postfix <i>gsm-utils</i> DBD ::Oracle <i>Oracle client</i>	Nagios Centreon Cacti

Pour information les architectures réelles :

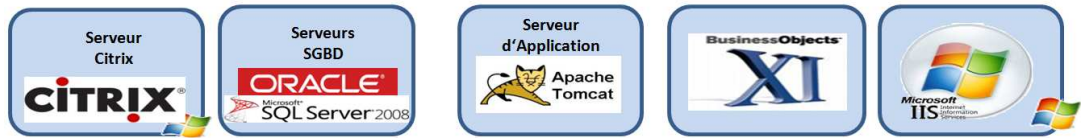
SISMU



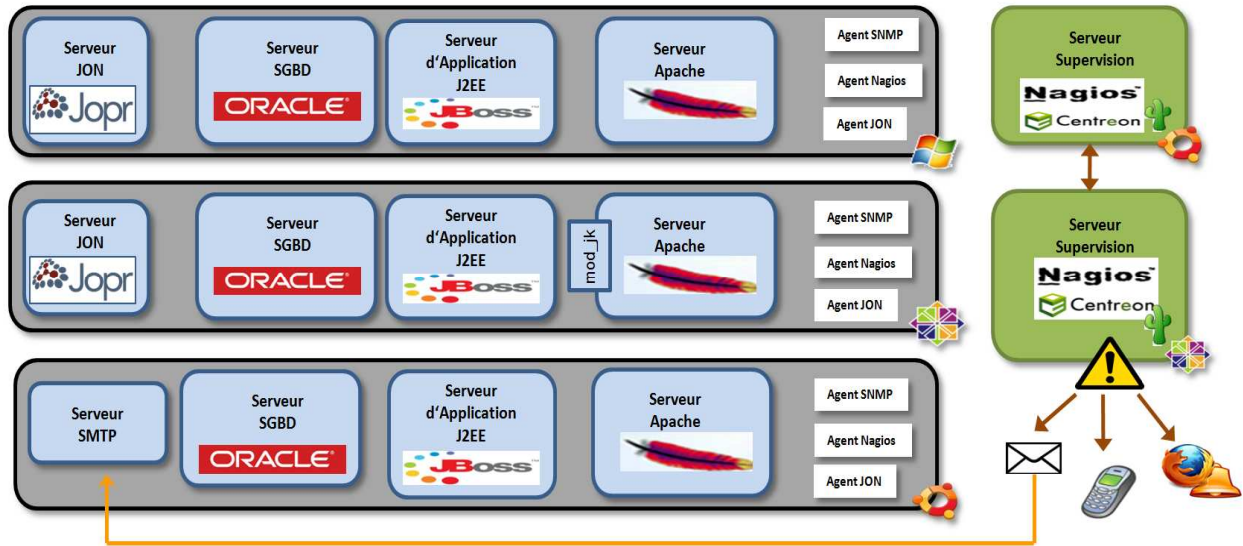
SIH



SIRAV (en cours de refonte)



MAQUETTE



7.2. Tests réalisés

Analyse de JON

Ce test de JON a été réalisé, avec l'installation du serveur sur la machine1 et des agents sur les machines 2 et 3. Il apparaît que JON est un produit puissant, avec des connecteurs disponibles pour apache, oracle, JBoss, F5. Comme l'indique la présentation précédente, son interfaçage avec Nagios ne peut être réalisé que par trap SNMP.

Fonctionnement Nagios/Centreon : configuration d'hôtes et de services, remontée des notifications visuel dans Centreon, par messagerie (serveur SMTP) et SMS (bibliothèques gsmllib ou gammu utilisées avec un portable Sony Ericsson K550i)

Agents Nagios standards pour la supervision Système : CPU, RAM, espace disque

Agents spécifiques pour les applications: JBoss (check_jmx), Oracle (check_oracle, check_oracle_health)..

Agents npre développés en scripts sh, avec des commandes de base dans le fichier npre.conf des serveurs supervisés.

Templates Cacti : tests SNMP Oracle (non concluants pour Oracle 10g V10.1), templates pour apache2, chargement Template F5

Point de vue méthodologie, les tests ont d'abord été réalisés en ligne de commande, avant de définir l'agent de vérification au sein de Nagios.

Un tableau de test a été établi, avec les résultats attendus et les résultats constatés.

Certains problèmes sur plateforme ont permis de mettre en évidence la non-remontée d'informations. Ce blocage a nécessité de revenir à la phase d'étude précédente, pour résoudre ces incidents (en partie dû à des problèmes de droits d'accès).

7.3. Bilan : compromis techniques

pour une meilleure efficacité de l'outil de supervision

Tout d'abord, l'étude et la mise en œuvre sur maquette ont montré qu'on ne pouvait pas répondre à toutes les contraintes du cahier des charges, sans une dérive des coûts ou des délais. En effet, des études et des recherches complémentaires étaient nécessaires pour répondre au besoin de reporting, mais pénalisait le planning général.

De plus, dans certains cas, il n'y avait tout simplement pas de solutions simples et gratuites, pour répondre aux besoins du projet.

En page suivante, le schéma résume les options techniques proposées au MOA, pour rester conforme au planning initial. Ces choix avaient pour principal but de simplifier l'architecture de supervision (suppression de Cacti), assurer une meilleure prise en main du produit par les utilisateurs et une maintenabilité optimale du système, en reportant sur le logiciel de Redhat JON ou la console web de F5, une partie de la métrologie.

7.3.1 Redondance Cacti/Nagios et JON

Comme l'a dévoilée l'étude précédente de JBoss Operation Network (voir paragraphe 6.6) et sa mise en œuvre aisée, cet outil de Redhat est aussi un logiciel de supervision, qui recouvre certaines fonctionnalités de Nagios et en particulier de Cacti, avec une meilleure ergonomie. Afin d'éviter d'avoir plusieurs outils à maintenir avec des résultats identiques et redondants, il a été acté en réunion de pilotage, avec le MOA, de privilégier **l'utilisation de l'outil JON** (mis en œuvre début septembre par l'équipe TME). Comme il existait des agents JON disponibles pour les serveurs web Apache, Cacti n'assurait plus que la création des courbes de **charge des boîtiers F5, visibles aussi sur l'interface web des matériels**. Aussi, il a été décidé de retirer le logiciel Cacti, du champ de la solution finale. Des agents et traps SNMP sont implantés sous JON et les boîtiers F5, pour le dialogue avec Nagios.

7.3.2 Limite de Nagios : vue globale du SI Métier non satisfaisante

Une finalité du projet était d'avoir un tableau de bord synthétique de l'état de santé, par des SI métier. Les travaux réalisés ont démontré que Nagios était avant tout un logiciel de surveillance de services au niveau du protocole IP. Comme nous détaillerons en fin de rapport, les produits open source sont très orientés techniques et délaissent la présentation simple et synthétique, demandée par les dirigeants, qui ne sont pas des spécialistes informatiques. Nagios et Centreon ne dérogent malheureusement pas à cette règle et ne répondent pas correctement à ce besoin, s'ils ne sont pas couplés à d'autres produits de cartographie (paragraphe 9.2) ou de reporting (paragraphe 9.3). Mais cette fonctionnalité nécessite des développements spécifiques ou l'achat d'extensions Centreon payantes. Afin de respecter le calendrier initial, avec l'accord du MOA, nous avons listé en annexe 12, les produits gratuits et payants, dont l'utilité sera examinée dans un projet ultérieur.

7.3.3 Utilisation des agents Nagios JBoss/JMX

L'étude théorique des agents Nagios démontre la possibilité de développer des agents pour rechercher certains indicateurs JBoss au moyen de JMX. La mise en place de ces sondes (notamment leur paramétrage) demande une connaissance approfondie de l'application Java déployée et des agents MBean disponibles. Aussi j'ai déconseillé au MOA, de mettre en œuvre ses agents, qui réclament trop d'investissements pour les configurer et ensuite les maintenir. La meilleure solution est de **privilégier JON pour superviser les architectures JBoss**, avec une remontée d'alerte par SNMP.

7.3.4 Choix de la distribution Nagios

Après une présentation des différentes installations de Nagios/Centreon et des discussions en comité de pilotage, la **solution CES** de la société Centreon (annexe 6.1) a été retenue, comme cœur de notre plateforme de supervision. Avec le système d'exploitation linux Centos, elle s'intègre complètement dans les mises à jour Redhat disponibles sur les plateformes Métier. L'installation ultra-rapide (15 minutes au lieu de 4 h avec des packages individuels) et le paramétrage automatiques des différents composants (Nagios, Centreon, bases de données MySQL, RDD et des agents standards) apportent un gain non négligeable aux équipes de maintenance, avec un unique produit à gérer en gestion de configuration.

7.3.5 Limiter le degré d' « intrusivité » des agents nagios

Pour la supervision de certains indicateurs, il est nécessaire d'installer du code logiciel sur les serveurs. Dans un souci de minimiser les risques d'incompatibilité, le comité de pilotage a privilégié les agents passifs (exemple SNMP) et demander de limiter le nombre de scripts à installer, sur les matériels opérationnels. Ainsi même si cela n'est pas élégant pour les puristes Nagios, nous avons choisi de **lancer directement les commandes de contrôle via SSH** (voir p49), plutôt que d'utiliser le fonctionnement nrpe.

Nécessitant plus de rigueur de développement, cette méthode est beaucoup lente, moins académique, mais elle est maîtrisée par l'équipe TME. L'autre avantage non négligeable est que le protocole SSH et les clés qu'authentification sont déjà déployés sur l'ensemble des serveurs au CeTIMA.

7.3.6 Conflit Nagios/Centreon : complexité pour la redondance

Centreon facilite grandement l'administration de Nagios et la gestion des SNMP, grâce à l'utilisation de bases de données MySQL. Mais cela aussi un gros défaut, car cette architecture complique la mise en place d'une solution de redondance. Des projets spécifiques existent pourtant pour Nagios (DMX, Merlin) et sont explicités au paragraphe 9.3.4.

Mais l'environnement devient plus que complexe avec Centreon : synchronisation des différentes bases de données MySQL interdépendantes (mesures, SNMP, configuration), duplication des modules d'ordonnancement, couplés à une unique interface apache. A ce stade de l'étude, avec l'accord du MOA, **l'analyse de la redondance Centreon a été suspendue** et proposée comme une évolution future, pour ne pas pénaliser l'avancement du projet.

7.3.7 Sauvegarde de la plateforme

Une proposition de sauvegarde par backup manager a été proposée au MOA. L'outil standard de sauvegarde automatique au Service de Santé des Armées est le **logiciel TINA** (compatible linux). Ce dernier sera déployé sur la station de supervision, par l'équipe d'exploitation du CeTIMA.

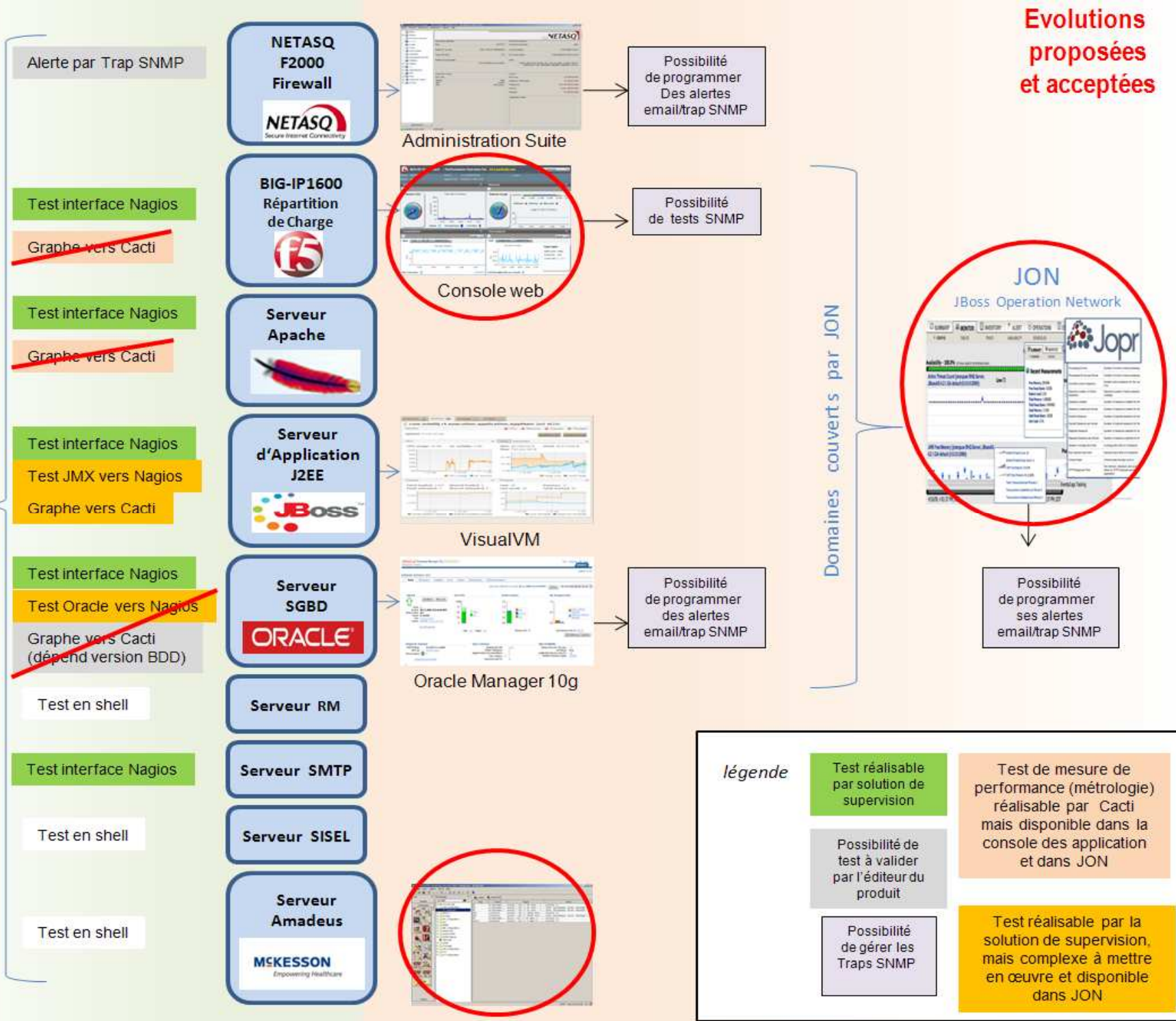
Solution étudiée de supervision

Nagios
Centreon

- Etats des contrôles
- Graphes (CPU, Mémoire, disk, trafic)

~~**Cacti**~~

Graphes non couverts par Centreon



Evolutions proposées et acceptées

8. Mise en œuvre sur les plateformes opérationnelles (Phase 6)

Objectif :

Le but de cette phase était d'installer et paramétrer la solution de supervision, dans les environnements de production.

Méthodologie réalisée :

La politique retenue était de déployer et tester les agents par couches successives (ping host, ressources matérielles, service, snmp, commande ssh, fonction nrpe spécifique, application ...) et non par équipement.

Ce déploiement pouvait impliquer l'apparition de risques. Lors de l'audit de la phase 1, les principaux risques avait déjà été identifiés avec l'aide des techniciens du CeTIMA : dysfonctionnement provoqué par l'installation de dépendance, de mise à jour de bibliothèque ou l'activation du protocole SNMP, le changement de configuration de l'équipement, l'installation des agents sur l'équipement supervisé... Avant le lancement du processus de déploiement, pour une capacité de réversibilité, cet impact de changement de configuration a été assuré par une sauvegarde des configurations - déjà réalisée de manière automatique et régulière, conformément au Plan de Continuité d'Activité (PCA), mis en œuvre dans l'établissement.

Chaque test de check a été réalisé suivant une grille prédéfinie, avec une comparaison résultat mesuré /résultat attendu. Si un écart inexplicable était constaté, il était décidé un retour aux configurations précédentes et une analyse approfondie sur la maquette, avant de rejouer les tests.

Livrables attendus :

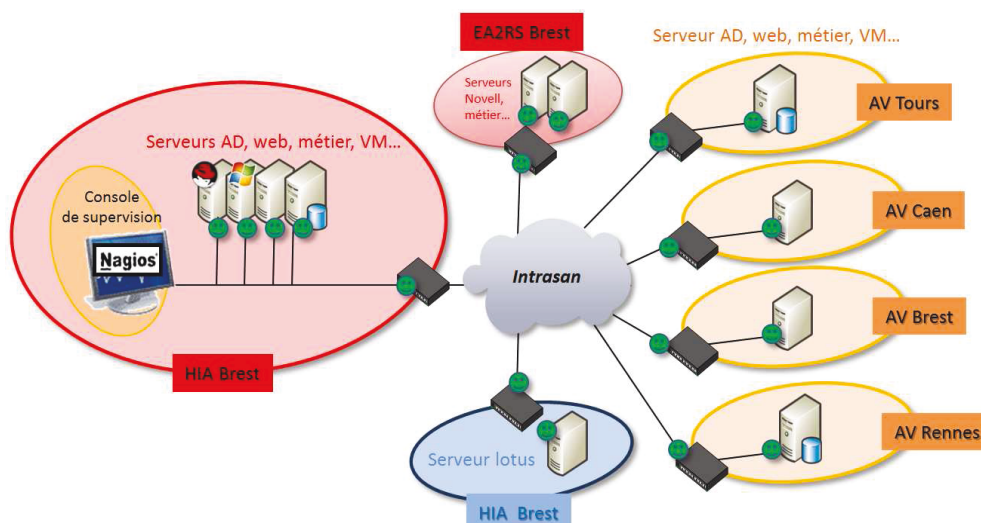
- Jeux des tests - [TESTS-SUPERV-DR]
- Plan de formation et conduite du changement – [FORM-SUPERV-NP]
- Procès-verbal de Vérification d'Aptitude – [PV_VA-SUPERV-NP]
-

8.1. Installation sur le SI des DRSSA

Le Système d'Information des DRSSA (Directions Régionales du Service de Santé des Armées) ne faisait pas partie du périmètre de l'étude. Mais fin 2011, son responsable SIC (moi-même) a décidé de déployer la solution de supervision à la DRSSA Brest, en attendant les accords de mise en œuvre par l'équipe TME et la disponibilité des serveurs des plateformes nationales.

Ce déploiement avait les atouts suivants :

- Le système et les technologies supervisées étaient moins complexes et complètement maîtrisés;
- Les tests de validation pouvaient être (re)joués dans un contexte plus souple et moins stressant (cible limitée en cas de défaillance, responsabilité directe, facilité de jouer les tests en soirée...);
- La solution correspondait à un besoin réel et urgent : soulager les travaux d'exploitation et permettre au CorSIC (Correspondant local SIC), d'avoir une vue sur le dysfonctionnement informatique potentiel de son unité, en cas d'absence des informaticiens;
- La mise en œuvre permettait de valider la documentation du projet.

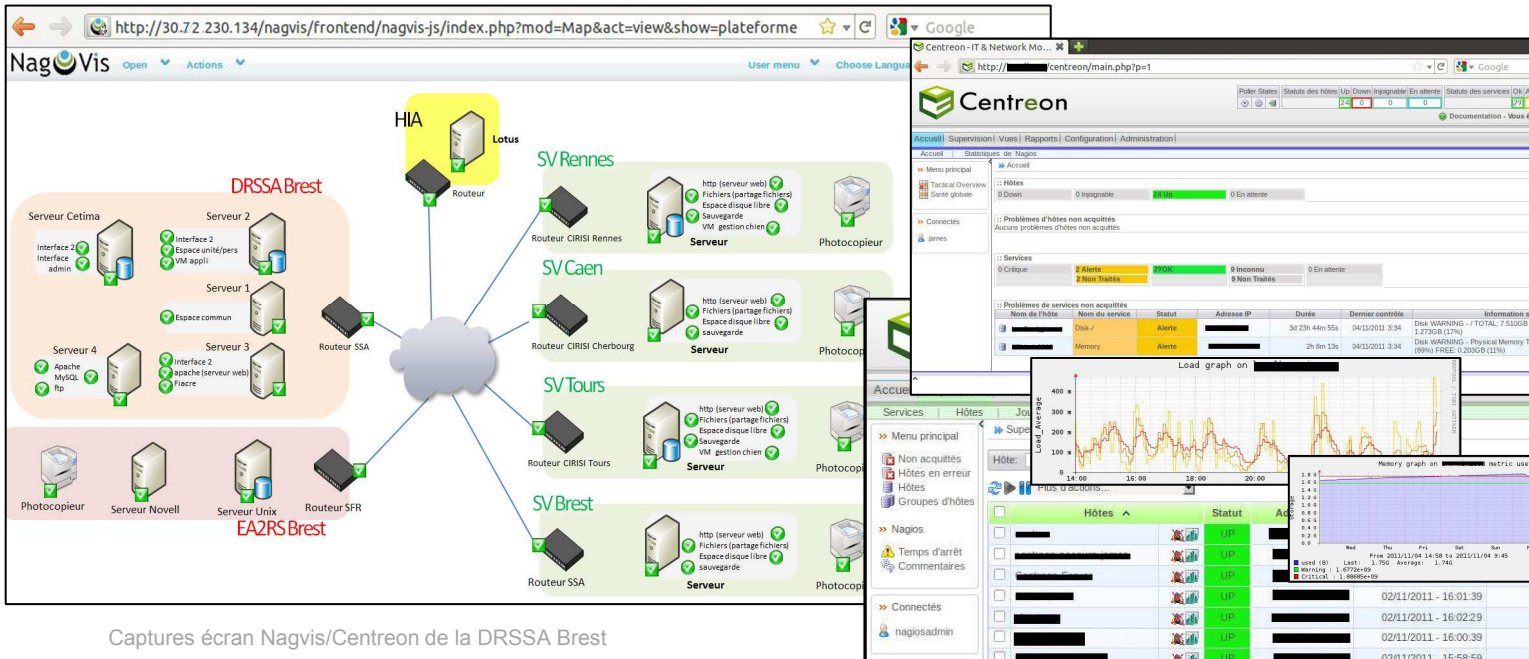


Cette supervision correspond aujourd'hui à une supervision opérationnelle, qui réalise les tests suivants :

- test « ping » sur les serveurs, les « VMwares » et le routeur de sortie intradef
- services supervisés : http (80), fiacre (3050), MySQL (3306), lotus (1352), courrier (8088), windows(139)
- contrôle de l'espace disque, de la mémoire disponible et des sauvegardes journalières ou des répliquions hebdomadaires.

Son installation a été aisée, rapide et transparente pour les utilisateurs.

Néanmoins, il apparaît parfois des erreurs aléatoires, dans les contrôles des équipements des sites distants. Ces anomalies nécessiteront une étude approfondie, après le retour d'expérience, pour revoir les seuils de notification ou l'installation d'une architecture distribuée.



Captures écran Nagvis/Centreon de la DRSSA Brest

8.2. Installation sur le SI SISMU du CeTIMA

Après accord du MOA, j'ai installé et paramétré le serveur Nagios/Centreon, suivant les procédures étudiées.

Pour le **serveur Nagios/Centreon de supervision**, aucune difficulté majeure n'a été rencontrée pour l'installer ou le configurer, par rapport aux documents d'installation rédigés :

- Installation CES - P_CES_SUPERV-NP-1.0*
- Installation Nagios - P_NAGIOS-SUPERV-NP-1.3*
- Installation Centreon - P_CENTREON-SUPERV-NP-1.0*
- Installation Postfix - P_POSTFIX-SUPERV-NP-1.0*
- Installation Nagvis - P_NAGVIS-SUPERV-NP-1.1*

Dans un souci contractuel et de sécurité SSI, l'intégration de la machine sur le réseau opérationnel du SSA a été réalisée par l'équipe Système/Pôle Administration des serveurs.

Pour garantir l'intégrité des produits logiciels, sur les serveurs opérationnels, le **déploiement des agents locaux Nagios** a aussi été réalisé par l'équipe TME, suivant les procédures rédigées dans la phase précédente. Comme signalé au paragraphe 7.3.5, pour limiter l'intrusivité des agents Nagios, sur certaines architectures sensibles, les agents NSClient et NRPE n'ont pas tous été déployés :

- Installation agent NSCLIENT Client Windows - P_NSCLIENT-C-SUPERV-NP-1.0*
- Installation NRPE Client linux - P_NRPE-C-SUPERV-NP-1.2*

Suivant la priorité initiale, la supervision n'a été réalisée que sur le Système d'Information SISMU. La phase de déploiement de la supervision a été complexe, notamment au niveau organisationnel, avec des difficultés dans la maîtrise du planning. Nous détaillerons ces problèmes dans le chapitre suivant.

Néanmoins, les principaux contrôles sont aujourd'hui en place (test ping, test des ressources, commande ssh déjà actives, snmp, listener oracle ...) et sont de bon augure pour le Nagios définitif, sur les autres SI métiers.

Acheté pendant l'été par le CeTIMA, le logiciel JON (JBoss Operation Network), étudié au paragraphe 6.6, a aussi été installé, pour couvrir la supervision de JBoss, apache, oracle.

Son utilisation donne déjà satisfaction, avec la remontée des ressources JBoss et la bande passante utilisée par les utilisateurs. La maîtrise complète de cet outil nécessitera sans doute un temps d'adaptation, mais répond déjà à un périmètre de la supervision, qui n'était pas couvert par les scripts manuels précédemment utilisés.

Les paramétrages et l'activation en SNMP V3, des boitiers F5, suivant la procédure extraite du document projet : AGENT POUR F5 - [F5-AGENT-SUPERV-DR-1.0](#)), est en cours de réalisation, par l'équipe réseau du CeTIMA.

Un paramétrage des accès sur la console Nagios/Centreon permet un accès web aux utilisateurs et l'envoi d'alertes par messagerie. L'utilisation d'alerte SMS demande une étude complémentaire des risques SSI, mais est documentée.

Les documents pour la formation de l'équipe TME pour prendre en compte complètement les outils, les mettre en œuvre sera un support précieux, pour une maintenance optimale des produits.

<input type="checkbox"/>	Centreon	Disk/		OK	30/03/12 17:23:03	3d 23h 59m 13s	1	Disk OK - /TOTAL: 9.475GB USED: 0.696GB (7%) FREE: 8.779GB (93%)
<input type="checkbox"/>		Linux_ntp_service		OK	30/03/12 17:25:42	4d 1m 21s	1	1 process matching ntpd (> 0)
<input type="checkbox"/>		Load		OK	30/03/12 17:24:39	3d 15h 7m 7s	1	Load average: 0.15, 0.21, 0.17.
<input type="checkbox"/>		Memory		OK	30/03/12 17:24:45	3d 23h 57m 28s	1	Total memory used : 41% ram used : 66%, swap used 0%
<input type="checkbox"/>		Ping		OK	30/03/12 17:23:42	4d 22h 34m 36s	1	OK - 127.0.0.1: rta 0,034ms, lost 0%
<input type="checkbox"/>		Snmp		OK	30/03/12 17:23:03	3d 23h 58m 35s	1	1 process matching snmpd (> 0)
<input type="checkbox"/>		Disk/		OK	30/03/12 17:20:59	3d 5h 45m 32s	1	Disk OK - /TOTAL: 9.627GB USED: 5.942GB (61%) FREE: 3.685GB (39%)
<input type="checkbox"/>		Linux_FileSystem_tmp		OK	30/03/12 17:22:13	3d 5h 44m 32s	1	Disk OK - /tmp TOTAL: 0.984GB USED: 0.033GB (3%) FREE: 0.952GB (97%)
<input type="checkbox"/>		Linux_FileSystem_var		OK	30/03/12 17:23:03	3d 5h 44m 1s	1	Disk OK - /var TOTAL: 1.938GB USED: 1.018GB (52%) FREE: 0.920GB (48%)
<input type="checkbox"/>		Linux_ntp_service		OK	30/03/12 17:25:51	3d 5h 46m 3s	1	1 process matching ntpd (> 0)
<input type="checkbox"/>		Load		OK	30/03/12 17:25:07	6h 25m 57s	1	Load average: 0.20, 0.18, 0.22.
<input type="checkbox"/>		Memory		OK	30/03/12 17:25:39	3d 5h 46m 3s	1	Disk OK - Swap Space TOTAL: 15.625GB USED: 0.000GB (0%) FREE: 15.625GB (100%)
<input type="checkbox"/>		Oracle_FileSystem_home		OK	30/03/12 17:23:03	3d 5h 43m 57s	1	Disk OK - /home TOTAL: 4.829GB USED: 1.971GB (40%) FREE: 2.858GB (60%)
<input type="checkbox"/>		Oracle_FileSystem_u01		OK	30/03/12 17:20:59	3d 5h 45m 34s	1	Disk OK - /u01 TOTAL: 6.798GB USED: 4.258GB (62%) FREE: 2.540GB (38%)
<input type="checkbox"/>		Oracle_Process_LISTENER		OK	30/03/12 17:25:15	3d 5h 16m 32s	1	1 process matching /u01/oracle/product/ora102/bin/tnslnsr (> 0)
<input type="checkbox"/>		Oracle_Process_pmon		OK	30/03/12 17:22:19	22h 18m 47s	1	4 process matching pmon (> 2)
<input type="checkbox"/>		Ping		OK	30/03/12 17:22:13	3d 5h 44m 32s	1	OK - 223.30.18.114: rta 1,290ms, lost 0%
<input type="checkbox"/>		Snmp		OK	30/03/12 17:22:46	3d 5h 44m 4s	1	1 process matching snmpd (> 0)
<input type="checkbox"/>		Disk/		OK	30/03/12 17:23:04	3d 5h 54m 1s	1	Disk OK - /TOTAL: 9.627GB USED: 3.751GB (38%) FREE: 5.876GB (62%)
<input type="checkbox"/>		Linux_FileSystem_tmp		OK	30/03/12 17:25:13	3d 5h 51m 32s	1	Disk OK - /tmp TOTAL: 0.984GB USED: 0.036GB (3%) FREE: 0.949GB (97%)
<input type="checkbox"/>		Linux_FileSystem_var		OK	30/03/12 17:23:03	3d 5h 53m 32s	1	Disk OK - /var TOTAL: 1.938GB USED: 0.428GB (22%) FREE: 1.510GB (78%)
<input type="checkbox"/>		Linux_ntp_service		OK	30/03/12 17:20:59	3d 5h 50m 32s	1	1 process matching ntpd (> 0)
<input type="checkbox"/>		Load		OK	30/03/12 17:22:13	3h 3m 51s	1	Load average: 0.42, 0.20, 0.19.
<input type="checkbox"/>		Memory		OK	30/03/12 17:25:41	3d 5h 51m 17s	1	Disk OK - Swap Space TOTAL: 15.625GB USED: 0.000GB (0%) FREE: 15.625GB (100%)
<input type="checkbox"/>		Oracle_FileSystem_home		OK	30/03/12 17:22:58	3d 5h 54m 1s	1	Disk OK - /home TOTAL: 4.829GB USED: 1.541GB (31%) FREE: 3.288GB (69%)
<input type="checkbox"/>		Oracle_FileSystem_rmandata		OK	30/03/12 17:24:14	3d 5h 52m 32s	1	Disk OK - /rmandata TOTAL: 24.608GB USED: 11.577GB (47%) FREE: 13.031GB (53%)
<input type="checkbox"/>		Oracle_FileSystem_u01		OK	30/03/12 17:23:42	3d 5h 53m	1	Disk OK - /u01 TOTAL: 6.798GB USED: 3.925GB (57%) FREE: 2.873GB (43%)
<input type="checkbox"/>		Oracle_Process_LISTENER		OK	30/03/12 17:25:14	3d 5h 16m 34s	1	1 process matching /u01/oracle/product/ora102/bin/tnslnsr (> 0)
<input type="checkbox"/>		Oracle_Process_pmon		OK	30/03/12 17:24:50	2h 46m 21s	1	4 process matching pmon (> 2)
<input type="checkbox"/>		Ping		OK	30/03/12 17:22:13	3d 5h 54m 48s	1	OK - 223.30.18.112: rta 0,789ms, lost 0%
<input type="checkbox"/>		Snmp		OK	30/03/12 17:23:43	3d 4h 52m 56s	1	1 process matching snmpd (> 0)
<input type="checkbox"/>		Disk/		OK	30/03/12 17:24:14	22h 22m 52s	1	Disk OK - /TOTAL: 9.461GB USED: 3.710GB (39%) FREE: 5.751GB (61%)
<input type="checkbox"/>		Jboss_FileSystem_soft1		OK	30/03/12 17:25:15	22h 21m 37s	1	Disk OK - /soft1 TOTAL: 14.188GB USED: 6.757GB (47%) FREE: 7.431GB (53%)
<input type="checkbox"/>		Jboss_FileSystem_soft2		OK	30/03/12 17:24:44	22h 22m 10s	1	Disk OK - /soft2 TOTAL: 13.542GB USED: 4.317GB (31%) FREE: 9.225GB (69%)
<input type="checkbox"/>		Jboss_java_process		OK	30/03/12 17:24:16	4h 57m 33s	1	2 process matching /jdk1.5.0_15/bin/java (> 1)
<input type="checkbox"/>		Jon_java_process		OK	30/03/12 17:22:22	22h 24m 32s	1	1 process matching /usr/java/jdk1.6.0_26/jre/bin/java (> 0)
<input type="checkbox"/>		Linux_FileSystem_tmp		OK	30/03/12 17:24:14	22h 22m 40s	1	Disk OK - /tmp TOTAL: 2.835GB USED: 0.083GB (2%) FREE: 2.752GB (98%)
<input type="checkbox"/>		Linux_FileSystem_usr		OK	30/03/12 17:23:42	22h 23m 16s	1	Disk OK - /usr TOTAL: 5.677GB USED: 4.068GB (71%) FREE: 1.608GB (29%)
<input type="checkbox"/>		Linux_FileSystem_var		OK	30/03/12 17:24:39	22h 22m 24s	1	Disk OK - /var TOTAL: 4.727GB USED: 0.257GB (5%) FREE: 4.469GB (95%)
<input type="checkbox"/>		Linux_http_service		OK	30/03/12 17:24:14	22h 22m 52s	1	11 process matching httpd (> 3)
<input type="checkbox"/>		Linux_ntp_service		OK	30/03/12 17:23:19	22h 23m 34s	1	1 process matching ntpd (> 0)
<input type="checkbox"/>		Load		OK	30/03/12 17:22:18	22h 24m 32s	1	Load average: 0.08, 0.09, 0.06.
<input type="checkbox"/>		Memory		OK	30/03/12 17:24:43	22h 22m 6s	1	Disk OK - Swap Space TOTAL: 16.003GB USED: 0.000GB (0%) FREE: 16.003GB (100%)
<input type="checkbox"/>		Ping		OK	30/03/12 17:24:39	22h 22m 26s	1	OK - 223.30.18.18: rta 0,964ms, lost 0%
<input type="checkbox"/>		Snmp		OK	30/03/12 17:24:41	22h 22m 24s	1	1 process matching snmpd (> 0)
<input type="checkbox"/>		Disk/		OK	30/03/12 17:24:16	4h 57m 33s	1	Disk OK - /TOTAL: 9.461GB USED: 1.557GB (16%) FREE: 7.904GB (84%)
<input type="checkbox"/>		Jboss_FileSystem_soft1		OK	30/03/12 17:25:41	5h 1m 10s	1	Disk OK - /soft1 TOTAL: 14.188GB USED: 6.595GB (46%) FREE: 7.593GB (54%)
<input type="checkbox"/>		Jboss_FileSystem_soft4		OK	30/03/12 17:24:41	4h 57m 9s	1	Disk OK - /soft4 TOTAL: 13.639GB USED: 4.101GB (30%) FREE: 9.538GB (70%)
<input type="checkbox"/>		Jboss_java_process		OK	30/03/12 17:26:34	4h 55m 15s	1	2 process matching /jdk1.5.0_15/bin/java (> 1)
<input type="checkbox"/>		Jon_java_process		OK	30/03/12 17:23:18	4h 58m 31s	1	1 process matching /usr/java/jdk1.6.0_26/jre/bin/java (> 0)
<input type="checkbox"/>		Linux_FileSystem_tmp		OK	30/03/12 17:24:50	4h 56m 59s	1	Disk OK - /tmp TOTAL: 2.835GB USED: 0.070GB (2%) FREE: 2.764GB (98%)
<input type="checkbox"/>		Linux_FileSystem_usr		OK	30/03/12 17:25:13	5h 1m 36s	1	Disk OK - /usr TOTAL: 5.677GB USED: 3.448GB (60%) FREE: 2.229GB (40%)
<input type="checkbox"/>		Linux_FileSystem_var		OK	30/03/12 17:24:15	4h 57m 34s	1	Disk OK - /var TOTAL: 4.727GB USED: 0.275GB (5%) FREE: 4.451GB (95%)
<input type="checkbox"/>		Linux_http_service		OK	30/03/12 17:23:17	4h 58m 33s	1	11 process matching httpd (> 3)
<input type="checkbox"/>		Linux_ntp_service		OK	30/03/12 17:22:46	4h 59m 4s	1	1 process matching ntpd (> 0)
<input type="checkbox"/>		Load		OK	30/03/12 17:26:43	5h 6s	1	Load average: 0.12, 0.09, 0.08.
<input type="checkbox"/>		Memory		OK	30/03/12 17:23:19	4h 58m 30s	1	Disk OK - Swap Space TOTAL: 16.003GB USED: 0.000GB (0%) FREE: 16.003GB (100%)
<input type="checkbox"/>		Ping		OK	30/03/12 17:22:57	4h 58m 53s	1	OK - 223.30.18.19: rta 0,710ms, lost 0%
<input type="checkbox"/>		Snmp		OK	30/03/12 17:23:19	4h 58m 30s	1	1 process matching snmpd (> 0)
<input type="checkbox"/>		Disk/		OK	30/03/12 17:23:03	3d 3h 22m 27s	1	Disk OK - /TOTAL: 60.482GB USED: 15.338GB (25%) FREE: 45.144GB (75%)
<input type="checkbox"/>		Linux_http_service		OK	30/03/12 17:21:47	2d 22h 9m 27s	1	13 process matching httpd (> 3)
<input type="checkbox"/>		Linux_ntp_service		OK	30/03/12 17:24:45	2d 21h 49m 1s	1	1 process matching ntpd (> 0)
<input type="checkbox"/>		Load		OK	30/03/12 17:23:03	3d 3h 22m 27s	1	Load average: 0.04, 0.02, 0.00.
<input type="checkbox"/>		Memory		OK	30/03/12 17:23:42	3d 3h 21m 22s	1	Disk OK - Swap Space TOTAL: 5.156GB USED: 0.000GB (0%) FREE: 5.156GB (100%)
<input type="checkbox"/>		Ping		OK	30/03/12 17:25:57	1d 22h 22m 44s	1	OK - 223.30.18.22: rta 0,701ms, lost 0%
<input type="checkbox"/>		Snmp		OK	30/03/12 17:21:45	2d 21h 46m 45s	1	1 process matching snmpd (> 0)

Extrait Procès-verbal d'attitude partiel [PV-SUPERV-NP]

9. Bilan du projet (Phase 7) : Retour d'EXpérience, propositions d'évolutions et d'amélioration

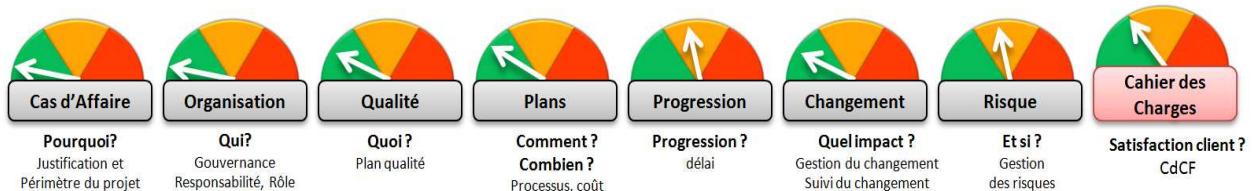
Objectif :

Après une phase d'utilisation, un bilan final était indispensable, pour clore le projet, sous la forme d'un Retour d'Expérience (REX). Cette étape permettait de tirer les enseignements positifs et négatifs du projet, pour alimenter une base de connaissance, pour les projets futurs. Ce processus de collecte d'informations visait une évaluation des résultats obtenus en termes de délai/coût/qualité et une analyse des écarts constatés. Il concernait aussi bien les résultats et les moyens utilisés, pour atteindre ces objectifs, que les méthodes d'organisation appliquées.

Méthodologie réalisée :

Une réunion avec l'équipe TME et le MOA a eu lieu pour discuter honnêtement et ouvertement des résultats de l'étude et de l'organisation, que j'avais managé.

La méthode traditionnelle est de reprendre les documents issus du projet (planning, compte-rendu, échanges de mail...) et de détecter ce qui a bien fonctionné et comment ont été gérées les difficultés, durant le planning. Un des 7 principes de la méthode de gestion de projet Prince2 (voir schéma complet page 14) est aussi de permettre de tirer les leçons de l'expérience. En rebalayant les 7 thèmes de la méthode, nous avons rapidement une tendance des points forts et des faiblesses de l'organisation de notre projet.



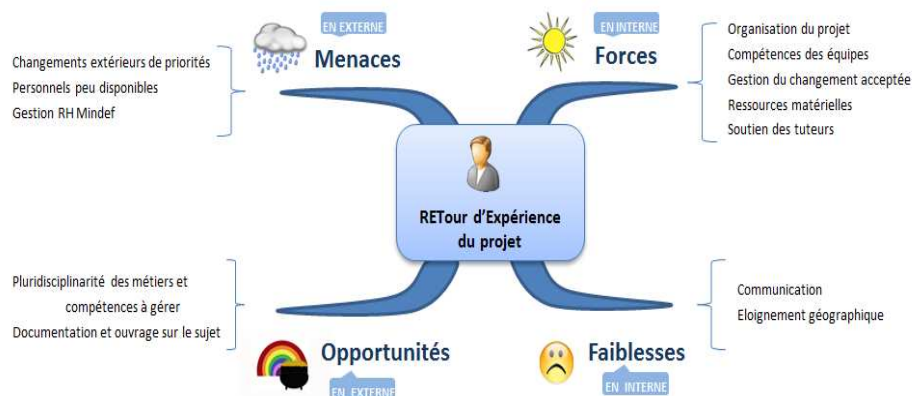
Mais ce n'était pas assez complet, car s'il est facile de faire un bilan technique en reprenant le cahier des charges et en comparant à la réalité, il est plus difficile de parler objectivement et d'analyser nos faiblesses et mettre des mots sur son ressenti. Il existe pour cela des méthodes de capitalisation des connaissances de retour d'expérience plus ou moins complexes à utiliser: MKSM, KADS, REX CYGMA, KOD Nous avons retenu la grille REX, proposée sur internet, par le CEDIP (service à compétence nationale du Ministère de l'Écologie, du Développement Durable, des Transports et du Logement), pour les SS2I, que nous avons adapté à notre environnement. Un extrait est fourni en annexe 19.

Livrables attendus :

- Retour d'Expérience [REX-SUPERV-DR]
- Bilan des changements [CHGT-SUPERV-DR]
- Propositions d'amélioration et d'évolution [EVOL-SUPERV-NP]
- Procès-verbal de Vérification en Service Régulier [VSR-SUPERV-NP]

9.1. Retour d'Expérience sur l'organisation

En analysant en détail, le résultat de notre grille d'évaluation du CEDIP, nous avons dessiné la carte simplifiée ci-dessous, sous forme d'analyse SWOT (Strengths, Weakness, Opportunities, Threats), qui illustre le retour d'expérience personnel du projet.



9.1.1 Points faibles

Nous allons étudier en détail quelques faiblesses, qui sont ressorties de notre bilan. Ces risques ont peut-être été sous-estimés ou mal maîtrisés (figure 67.1 ci-dessous), dans notre analyse de gestion des risques, avec des conséquences dans le report de certains jalons.

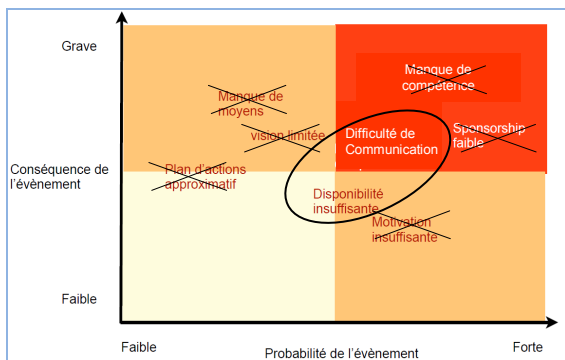


Fig. 67.1. Risques sous-estimés dans un projet informatique (extrait *Management des systèmes d'information*, Edition Pearson)



Fig. 67.2. Stratégie d'accompagnement

Manque de disponibilité

Comme expliqué au paragraphe 2.2.1, l'acquisition de l'UV d'anglais avait initialement été comprise comme pouvant donner lieu à une dérogation, avant la soutenance CNAM. Cette nouvelle contrainte a été identifiée trop tardivement, comme un risque impactant le projet. La préparation de l'examen a pesé sur ma disponibilité pleine et entière, pendant la phase 6 du projet, qui a duré plus longtemps que prévue. Les plateformes opérationnelles et l'équipe TME n'étaient pas non plus toujours disponibles aux dates souhaitées. Mais cette situation s'expliquait logiquement, par le déploiement programmé aux mêmes dates de la version LUMM V2, sur le système d'information SISMU et était observée de près par la direction centrale. Cette logique stratégie d'entreprise privilégiant le bon fonctionnement des logiciels utilisateurs, plutôt que l'évolution de notre outil de maintenance, a donc été acceptée et intégrée, mais a eu des conséquences, sur le planning initial.

Difficulté de communication

L'éloignement a eu aussi des conséquences sur la communication dans le projet. N'étant pas de manière permanente, dans les locaux du CeTIMA, pour avoir une réponse directe et immédiate aux questions posées. Il a fallu adapter la stratégie d'accompagnement et la conduite du changement, développées au chapitre 2.2.3. Nous avons eu une attention particulière sur la qualité des supports diffusés et un effort de synthèse dans les documents PowerPoint présentés en visioconférence, avec un suivi rigoureux des informations reçues. Cet accent mis sur la démarche qualité est aussi un des atouts forts du projet.

9.1.2 Points forts

Méthode et organisation

La phase maquettage a été une phase difficile et complexe à gérer, avec des problèmes de paramétrage et de réglages (comme l'installation d'Oracle ou JON sur différents systèmes d'exploitation). Seul un suivi méthodique des nombreuses installations, dans une démarche qualité maîtrisée, avec des tests répétés, dans l'environnement VMware (avec l'utilité des snapshots) auront permis de venir à bout d'une documentation et d'un soutien, qui faisaient parfois véritablement défaut, pour les outils open source. La rigueur et la méthodologie utilisées, basées sur des processus et des rôles clairement définis, auront été une des forces du succès de ce projet.

Connaissances technique et organisationnelles acquises

Par ailleurs, point faible initial, les lacunes dans les compétences demandées pour ce projet ont rapidement été comblées, avec le soutien de l'équipe TME et des responsables applicatifs. Les recherches internet, les différentes lectures réalisées (listées en fin de mémoire) et les rencontres importantes (Jean Gabès à Paris [CCR-SALON-SUPERV-NP], Olivier Jan à Nantes [CRR-CANOPSIS-SUPERV-NP]) ont complété la motivation d'être techniquement à niveau et je ne peux que me réjouir des différentes compétences acquises, lors de cette étude.

Acteurs et environnement compétents / conduite du changement aisée

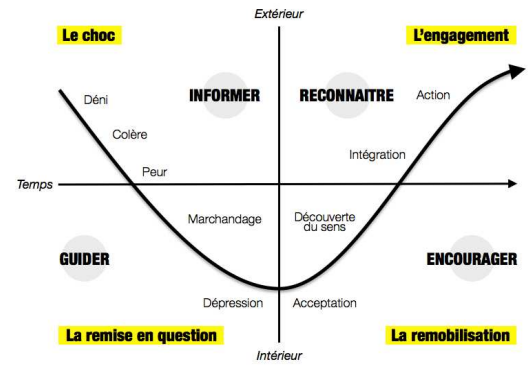
Enfin, la conduite du changement, développée en page 16 a été facilitée par la qualité des différents acteurs du projet. Le Ministère de la Défense est une administration habituée au changement (mutation régulière des militaires, restructuration des établissements de la Défense, fluctuation des budgets ...). Fortes de la discipline militaire, ses personnels savent s'adapter à l'environnement et n'ont pas peur d'évoluer ou de se remettre en cause, quand ces changements sont cohérents, expliqués et accompagnés. Il n'a donc pas été nécessaire de se référer au schéma habituel des Ressources Humaines (vallée du changement), pour répondre au choc du changement.

En plus de cet environnement d'entreprise favorable, le projet s'intégrait dans un besoin demandé et donc naturellement accepté par les différents acteurs du projet (MOA, équipe TME, responsables applicatif..). Il n'y avait pas de changement d'organisation ou de modification de la culture d'entreprise, mais un changement d'outil et de méthodes de travail. L'objectif était une optimisation du fonctionnement, l'amélioration des résultats et des performances, la satisfaction des clients, un meilleur pilotage des SI. L'outil supervision permettait par ailleurs une reconnaissance et une mise en valeur du travail de l'équipe TME, avec l'accès direct aux informations par l'interface web du produit, pour constater la disponibilité des serveurs d'exploitation.

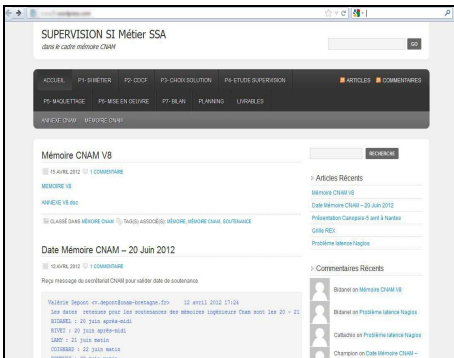
Même si je n'avais pas d'autorité directe sur ces personnels, le professionnalisme et la compétence des équipes rencontrées auront été une force, pour faire aboutir le projet, avec le soutien sans faille du MOA. Lors des impossibilités techniques (paragraphe 7.3) ou des imprévus (paragraphe 2.2.1), ce dialogue et cette confiance auront facilité l'arrivée vers des solutions de contournement.

Cette adhésion peut aussi s'expliquer par la bonne stratégie retenue pour cette conduite du changement, axée sur la communication :

- un portail web (blog sous wordpress), avec la documentation complète de l'étude ;
- des tableaux de bords avec des indicateurs à jour, avec une explication des difficultés rencontrées ;
- des présentations régulières sous forme de powerpoint de l'avancement du projet.



La vallée du changement : du choc à l'engagement
 Courbe du docteur Elisabeth Kübler-Ross adaptée à la conduite du changement



Portail intranet du projet

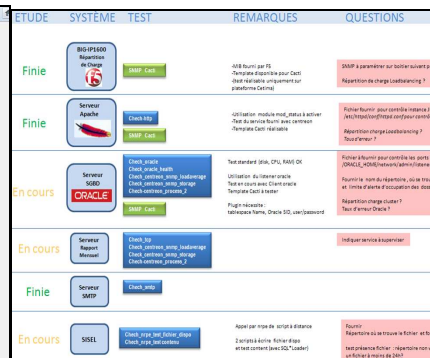


tableau de bord avec indicateurs



présentation powerpoint synthétique

9.2. Retour d'Expérience technique

Pour le bilan technique, il nous a suffi de reprendre le CdCF et de vérifier les fonctionnalités disponibles. Une réunion avec l'équipe TME a conclu de formaliser les difficultés d'utilisation du logiciel et des attentes d'évolution :

BILAN DU RETOUR D'EXPERIENCE TECHNIQUE

AVANTAGE	PROBLEME / MANQUE	PROPOSITION DE SOLUTION
-Installation simple et rapide (CES)	1-Complexité de certains agents à paramétrer et soutenir	-Choix d'interface d'administration propriétaire disponible (JON,console web F5..)
-Configuration rapide des checks élémentaires	2-Nécessité de se connecter à l'interface web ou à sa messagerie pour consulter les alertes	-Proposition d'amélioration des fonctionnalités nagios au chapitre 9.3.1
-Solution stable et fiable	3-Manque de graphe métier pour les décideurs	-Proposition de cartographie (<i>chapitre 10.3.2</i>) et remarque sur hypervision (<i>chapitre 9.3.4</i>)
-L'interface Centreon est très utile pour le paramétrage des fichiers de configuration (mais interface Nagios plus simple pour la maintenance)	4-Temps important de latence de résultats des tests (sur serveur CeTIMA installé)	-Changement du broker par défaut par un plus compétitif (<i>annexe 7</i>)
	5-Document Excel des indicateurs difficiles à décrypter pour une personne extérieure au projet	-Utilisation MediaWiki (<i>chapitre 9.3.1</i>)
	6-Problème de remonter d'alerte sur les sites distants.(DRSSA)	-Etude d'architecture distribuée (<i>chapitre 9.3.3</i>)

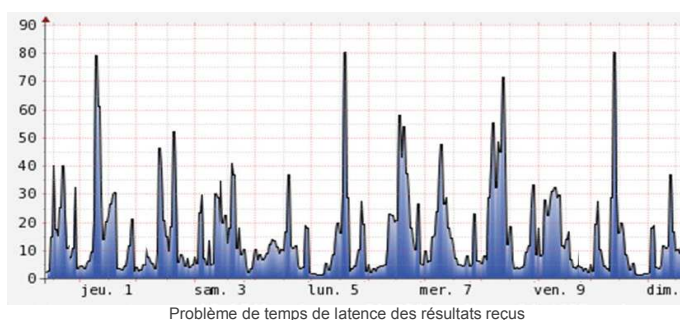
Synthétisés dans le tableau ci-dessus, nous allons développer quelques défauts signalés, avant de proposer des réponses ou évolutions, dans le paragraphe suivant.

9.2.1 Objectifs / résultats atteints

Comme le montre ce mémoire, la solution Nagios est un choix technique judicieux, pour les besoins du service. Certes ils existent de nombreux agents Nagios (plus ou moins complexes et maintenables dans le temps), mais Nagios n'est pas véritablement fait pour les hautes couches applicatives complexes, comme on l'a rappelé au paragraphe 7.3. Aussi nous avons choisi d'abord l'efficacité et la simplicité, cette stratégie explique pourquoi 78 % du périmètre est actuellement couvert par Nagios, les outils propriétaires couvrant l'autre domaine.

9.2.2 Problèmes rencontrés

Comme indiqué dans le tableau (problème 4), lors de la mise en œuvre au CeTIMA, nous avons constaté des problèmes de temps de réponse des sondes installées, comme le montre le graphe ci-dessous. Loin d'être pénalisant pour les performances du moteur Nagios, une optimisation pourrait être étudiée, par le remplacement du broker NEB (Nagios Event Broker) par défaut.



Par ailleurs, point de vue documentation, dans notre étude, toutes les informations (nom du serveur, commande de test, seuil d'alerte, paramétrage, dépendance, contact ...) sont contenues dans un grand fichier excel. Le document est difficilement exploitable par des personnes extérieures au projet. Dans le futur, la présentation des informations devrait pouvoir se faire de manière étendue et aisée, avec l'ajout de fonction de suivi, de gestion de versions et de retour d'expérience.

9.2.3 Eléments réutilisables

Les enseignements tirés de l'étude démontrent que Nagios peut être utilisé et déployé rapidement. Ainsi certains responsables informatiques de HIA m'ont contacté pour avoir des informations et mon ressenti sur le produit. Les procédures d'installation et de déploiement leur ont été fournies, pour une utilisation dans leur établissement. De même des échanges réguliers ont lieu, avec le responsable Nagios de la DIRISI Brest, pour discuter des méthodes utilisées et partager les problèmes techniques rencontrés.

9.3. Proposition d'évolutions et d'amélioration

Suite aux problèmes techniques signalés au paragraphe précédent, j'ai étudié des solutions et des améliorations. Dans ce chapitre, des pistes d'évolution, sortant du cahier des charges initial, sont aussi présentées, dans des domaines complémentaires, pour assurer un meilleur suivi des ou tout simplement pour réfléchir sur l'avenir de l'outil. Cette démarche s'inscrit dans la gestion du changement et la perspective générale d'ouverture du soutien informatique, à des organismes extérieurs au Ministère de la Défense et le besoin de contrôle des contrats de service, signés avec ces sociétés.

9.3.1. Améliorations de certaines fonctionnalités.

9.3.1.1 Optimisation Nagios Shinken (voir annexe 5.1)

Piloté par le français Jean Gabès, Shinken est un projet prometteur de réécriture du noyau de Nagios en python, avec des fonctionnalités complémentaires (corrélations, système distribué...).

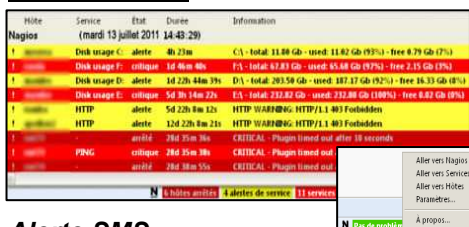
Dans son architecture, plusieurs processus font chacun une tâche spécifique, ce qui permet de multiplier par 5 le gain de performance de la supervision. Son fonctionnement est détaillé en annexe 5.

9.3.1.2 Optimisation des temps de latence (voir annexe 7)

Pour les problèmes de latence des checks Nagios, des brokers (qui assurent l'ordonnancement des tests) développés par Centreon ou le projet gearman peuvent remplacer plus efficacement le modèle NEB (Nagios Event Broker) fourni en standard par Nagios.

9.3.1.3 Alertes visuelles (Plugin Firefox), SMS , ou iphone/Android

Alerte visuelle



Host	Service	Etat	Down	Information
Nagios (mardi 13 juillet 2011 14:48:29)				
1	Disk usage C:	alerte	4h 23m	C:\ - total: 11.88 Gb - used: 11.82 Gb (99%) - free 8.79 Gb (7%)
1	Disk usage F:	critique	1d 06m 46s	F:\ - total: 67.83 Gb - used: 65.68 Gb (97%) - free 2.15 Gb (3%)
1	Disk usage D:	alerte	1d 22h 44m 39s	D:\ - total: 203.59 Gb - used: 187.87 Gb (92%) - free 15.73 Gb (8%)
1	Disk usage E:	critique	5d 3h 14m 22s	E:\ - total: 232.82 Gb - used: 232.80 Gb (100%) - free 0.02 Gb (0%)
1	HTTP	alerte	5d 22h 8m 12s	HTTP WARNING: HTTP/1.1 403 Forbidden
1	HTTP	alerte	12d 22h 8m 21s	HTTP WARNING: HTTP/1.1 403 Forbidden
1	SMTP	alerte	2h02 51m 36s	CRITICAL: Plugin timed out after 10 seconds
1	PING	critique	2h02 51m 36s	CRITICAL: Plugin timed out
1	SMTP	alerte	3h02 58m 55s	CRITICAL: Plugin timed out

N 6 hôtes actifs 4 alertes de service 11 services

Pas de problème

Allez vers Nagios
Allez vers Services
Allez vers Hôtes
Paramètres...
À propos...

Pour faciliter le contrôle des alertes de Nagios, un plugin Nagios Checker pour Firefox ou chrome permet de se connecter à travers l'interface CGI de Nagios et afficher en temps réel les alertes dans la barre d'état du navigateur. Plus besoin d'avoir une fenêtre constamment ouverte sur la page de supervision des statuts, dès qu'un problème est détecté, la barre d'état change de couleur.

Alerte SMS

En branchant un téléphone portable sur la station Nagios, il est possible d'envoyer des messages SMS correspondant aux alertes remontées. La procédure d'installation et de paramétrage est définie dans la procédure [P_SMS-SUPERV-NP]

Administration par smartphone et iphone/ipad

Des applications pour android (nagbag,janai,anag...) ou iphone (teeny nagios, nagios mobile...) sont aussi disponibles pour visualiser et administrer à distance Nagios.

Elles nécessitent néanmoins un accès wifi ou 3G et une dérogation par rapport à la PSI (Politique de Sécurité Informatique) actuelle du ministère.



9.3.1.4 Reporting (génération de rapport) (voir annexe 12)

Centreon offre la possibilité de visualiser à l'écran, dans la partie vue, des rapports de synthèse des contrôles réalisés, sous forme de tableau ou de graphes. Mais il ne permet pas de les exporter ou envoyer par messagerie automatiquement sous forme de pdf ou doc.

Des add-ons pour centreon sont proposés (Centreon Business Intelligence, Centreon Business Activity Monitoring, Centreon Map), mais malheureusement payants, comme le module cereusreporting, pour génération de rapports pdf sous Cacti. Seul le module gratuit nectar, pour Cacti, propose de transmettre de manière périodique un graphe à une adresse de messagerie, mais son utilisation est limitée.

Il manque donc un système complet de reporting, qui pourrait être développé avec les outils open source BIRT ou JaspertReport décrits en annexe 12.

9.3.1.5 Base de connaissances (MediaWiki)

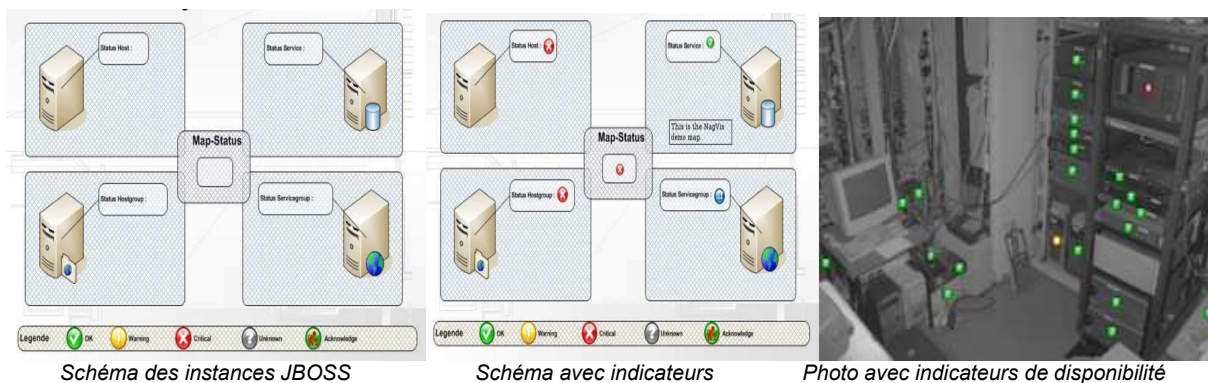
Afin de permettre une meilleure utilisation de l'outil de supervision, la documentation est indispensable. Des manuels d'installation et d'utilisation ont été rédigés, pendant le projet (voir liste en annexe 1). Mais il faut qu'ils puissent évoluer et rester à jour des nouveaux tests implantés dans Nagios et Centreon. La solution la plus efficace est l'utilisation de Mediawiki [P_WIKI_SUPERV_NP], une base de connaissances Wikipedia, accessible par tous les exploitants des SI métiers. Elle pourra contenir le descriptif des tests effectués et les explications pour résoudre les problèmes récurrents. Quand l'administrateur reçoit une alerte, il n'a plus qu'à cliquer sur le lien présent dans l'e-mail et à appliquer les instructions qui lui sont données.

9.3.2 Outils de cartographie

Nagvis



Nagvis est un outil de cartographie, qui récupère les données de Nagios, pour les visualiser sur un fond d'écran personnalisable. Le principe est de choisir une image du SI et de placer sur celle-ci des marqueurs correspondants aux hôtes ou services, qui changent d'état suivant les résultats remontés. Plusieurs cartes avec un degré de détail différent peut être défini par catégorie (SI, plateforme, localisation...), suivant le public visé (administrateurs, responsables applicatifs, décideurs ...), avec la possibilité de les afficher par rotation automatique (15s par exemple), sur un écran de contrôle. Nagvis récupère les états affichés, suivants deux méthodes : Ndomy (lecture d'une base MySQL/NDO2DB) ou Ndo2fs (lecture fichier à plat). Dans notre projet, nous disposons de la base NDO de Nagios.



Point de vue maintenance, ces cartes permettent de voir rapidement, où est localisée la mesure remontée en anomalie.

Weathermap

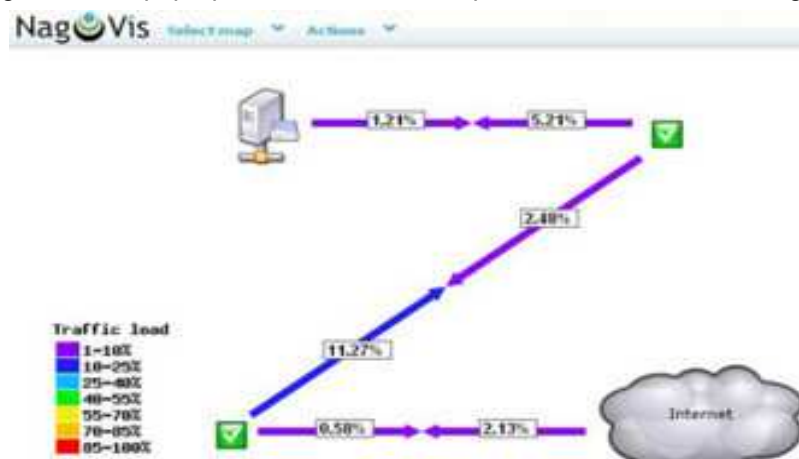


S'appuyant sur la base RDD, Weathermap est un outil libre, pour générer des cartes graphiques avec des mesures de bandes passantes. Il ne permet pas de retrouver l'historique des états, mais d'afficher une vue synthétique de l'état du réseau à l'instant T.

Il peut être utilisé soit tout seul ou intégré comme plugin Nagvis.

Les fonctions de Network Weathermap sont :

- Affichage sous une forme graphique intuitive de la charge des principaux liens réseau.
- Matérialisation des flux par deux flèches, dont la couleur varie en fonction des volumes de données échangées.
- Définition d'une image de fond pour matérialiser la topologie de votre réseau.
- Possibilité de gérer des « pop-ups » en fonction de la position de la souris sur le graphique.



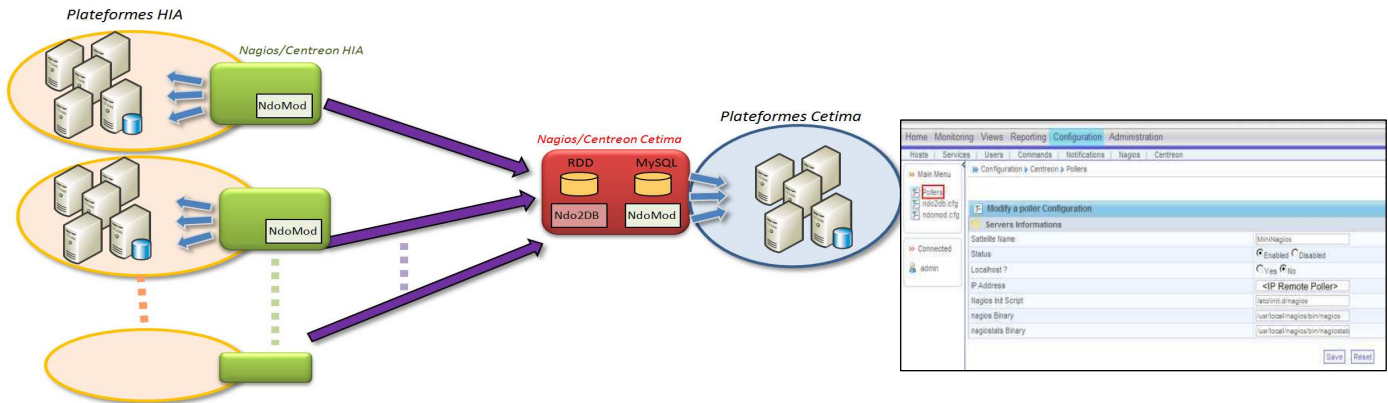
Cette carte permet localiser rapidement les goulots d'étranglement et donc les évolutions nécessaires.

9.3.3. Architecture distribuée.

L'étude pour la supervision du SIH de la plateforme du CeTIMA peut servir de base pour l'implémentation d'une solution Nagios sur chaque plate-forme des HIA. Une consolidation des états de l'ensemble du SIH national peut ainsi être réalisée, en faisant remonter les résultats pertinents, sur une console centrale au CeTIMA. Les serveurs Nagios des HIA réalisent l'acquisition des états, par les agents locaux, seules les données sont dupliquées au niveau central.

Le système de relais « Event Broker » est un plugin interne à Nagios, qui permet de mettre en place ce mode de fonctionnement avec NDOMOD. Pour simplifier encore la tâche, un menu pour « architecture distribuée » est disponible dans Centreon, où on définit le Nagios Maître et les Nagios Distants (notion de poller ou satellite)

Des architectures plus complexes (DNX, Merlin) peuvent être mises en œuvre, et sont décrites en annexe 10.



Définition de satellite sous Centreon

9.3.4. Redondance.

La machine de supervision n'est pas exempte de panne. Dans notre environnement critique, il est conseillé d'installer une station de supervision de secours, qui prend le relais en cas de défaillance de la station Maître. Il existe différentes méthodes, pour assurer la redondance et le basculement entre les deux stations.

Redondance pure

La méthode la plus simple, qui vient à l'esprit, est de dupliquer les contrôles sur les deux machines, mais activer les notifications par défaut que sur la station maître. On active un agent sur la station de secours pour tester l'état du maître et basculer la notification en cas d'incident. (Fig. A)

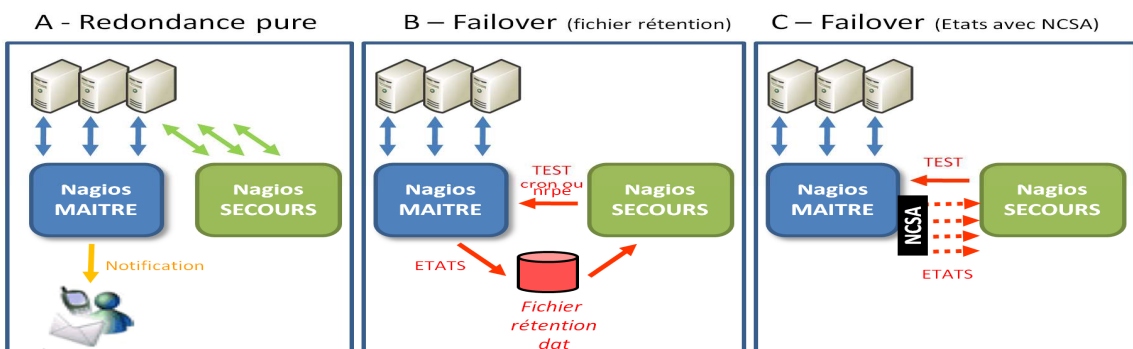
Avantage : simplicité de mise en œuvre (recopie), deux interfaces web de contrôle avec un suivi de l'état des hôtes d'un superviseur à l'autre.

Inconvénient majeur : duplication des tests sur le réseau, augmentation du trafic et des sollicitations supplémentaires des équipements supervisés.

Mode failover

On active le superviseur de secours en cas de panne sur le premier. On active la surveillance de l'état du superviseur maître par un ordonnanceur standard cron ou l'utilisation d'un agent nrpe.

L'avantage de cette méthode est d'éviter une duplication des tests. L'inconvénient est que le superviseur de secours ne connaît pas, à priori l'état précédent des hôtes et services, lorsqu'il prend la main. (Temps de latence jusqu'à l'ordonnancement du prochain test).



Deux solutions sont possibles :

-Un fichier de rétention des états (retention.dat) commun, partagé en NFS, stocke l'ensemble des états, mais sa mise en place est complexe. (fig. B) ;

-La station maître transmet au Nagios semi-dormant, les états grâce à NCSA et aux commandes OCSF et OCHP, avec un impacte non négligeable sur les performances de la station maître à chaque envoi. (fig. C)

Par ailleurs, comme l'a indiqué le retour d'expérience, après quelques mois d'utilisation, les techniciens délaissent rapidement l'interface Centreon (utile pour la génération des fichiers de configuration initiaux), pour l'interface dépouillée de nagios, pour les opérations de dépannage, comme l'avait signalé un responsable DIRISI, lors d'une interview. Il n'est donc pas nécessaire de redonder la plateforme Centreon, qui pourra être réinstallé en cas de défaillance, avec les sauvegardes des bases de données. Cette option facilite la mise en œuvre d'une solution de redondance uniquement Nagios, qui a été étudié (voir document [P_REDONDANCE_NAGIOS-SUPERV-NR]), avec le choix de la figure C.

9.3.5. Mise en place d'une supervision de la sécurité.

Comme constaté en début de rapport (page 20), la supervision de la sécurité ne faisait pas partie du périmètre demandé par le SSA. Néanmoins, nous avons proposer dans ce chapitre des outils, qui peuvent répondre à un besoin futur. En complément des firewalls actuellement déployés, des systèmes de détection d'intrusion peuvent être installés sur les plates-formes SI Métier, pour optimiser la sécurité des Systèmes d'Information du SSA.

Ci-dessous les Outils Open Source les plus connus :



SNORT est un NIDS (Network Intrusion Détection System) écrit par Martin Roesch. Placé en Sniffer (carte réseau en mode "promiscuous"), il analyse en temps réel le trafic réseau. Les paquets sont décortiqués puis analysés par rapport à des signatures et des règles, au niveau réseau (IP, ICMP), transport (TCP,UDP), application (http, telnet). En cas d'anomalie, il peut interagir avec le firewall, pour bloquer les intrusions (IPS).



OSSEC est un HIDS (Host Intrusion Detection System), une application de détection d'intrusion. Il permet de surveiller l'intégrité des fichiers systèmes, aussi bien sur des postes Linux que Windows. OSSEC détecte également des attaques de pirates comme les rootkits, les scans de ports, et analyse les logs du système, des applications et des services.



Prelude Hybrid IDS centralise les informations en provenance de plusieurs emplacements (senseurs) sur le réseau. Le but de ce type d'IDS est d'avoir une vision globale sur les composants constituant un système d'information en permettant une supervision centralisée en matières d'alertes d'intrusions remontées par les NIDS (Snort, Bro) et les HIDS (Ossec, Samhain) présents sur l'architecture du réseau supervisé, avec un analyseur de logs et une solution de corrélation, suivant la norme IDMEF (Intrusion Détection Message Exchange Format). Il peut interagir avec des éléments extérieurs (exemple : pare-feu en cas d'attaque). Pour l'avenir, il faut espérer que ce projet prometteur open source ne soit pas remis en cause par son rachat, en février 2012, par la société CS, qui édite déjà le logiciel de supervision Vigilo, basé sur Nagios, mais avec des modules payants.

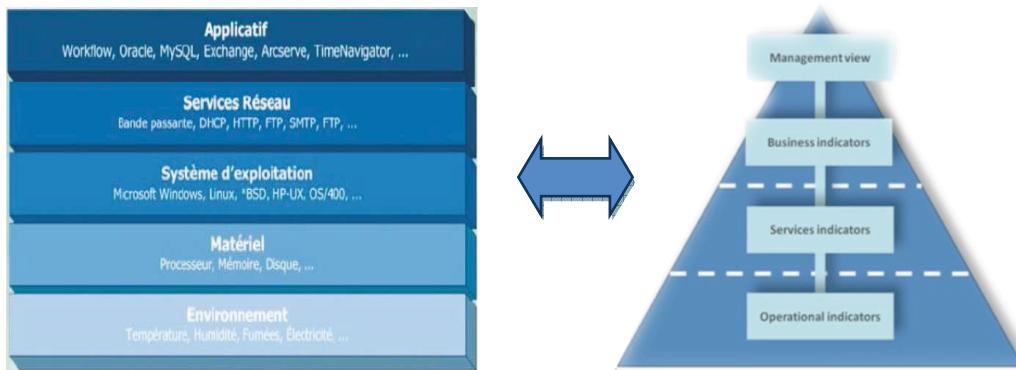
9.3.6 Hypervision.

Enfin, la présentation des SI Métier du SSA a montré la segmentation actuelle de la globalité de la supervision, au long de la chaîne métier :

- Les réseaux locaux des utilisateurs gérés par les CIRISI locales ;
- Le réseau ReP3SA et certaines fonctionnalités (messagerie, AAA, Internet) soutenus par Orange ;
- Les actifs réseaux supervisés par une solution dédiée ;
- La supervision des plates-formes assurée par notre Nagios et des outils complémentaires comme JON.

Ce constat montre la limite et les incohérences entre la supervision fournie aujourd'hui aux entreprises et l'évolution des SI, depuis les 10 dernières années. Aucun outil de supervision ne peut contrôler parfaitement l'intégralité du SI. Certaines parties ne peuvent être surveillées que par des produits fournis par l'éditeur. Il est donc nécessaire pour avoir une vision globale du système, d'avoir des outils de corrélation, synthétisant l'ensemble des informations remontées, qui seront comparées aux besoins exprimés.

Effectivement, comme le signalent les responsables métiers, les outils techniques actuels ne collent plus aujourd'hui exactement aux besoins des décideurs, avec le passage d'une gouvernance technique à une gouvernance orientée business et l'émergence de normes standards « best practices » (ITIL, CoBit, VallT).



La représentation traditionnelle du SI change avec des évolutions technologiques comme :

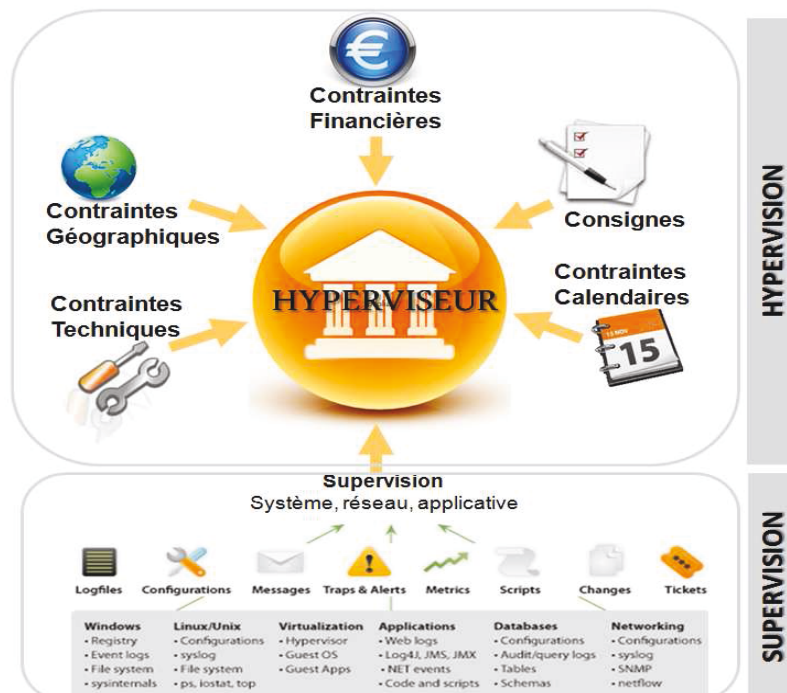
- de nouveaux environnements plus complexes : intranet des employés, extranet des fournisseurs/client et l'internet ;
- la virtualisation massive (VMware, Xen...) amenant une distinction difficile entre serveur physique/virtuel, hébergé/hébergeant ;
- la redondance et la haute disponibilité qui rendent la représentation traditionnelle plus lourde à modéliser ;
- le Cloud Computing (Saas, Paas, IaaS) qui fait exploser la notion même de matériel (à l'instant t, vous ne savez plus quel composant de votre infrastructure est sollicitée).

Ces évolutions ont pour conséquence, la difficulté à localiser les moyens techniques mis en œuvre, l'impossibilité d'utiliser des agents de supervision et une vision non complète de la chaîne des ressources mises en œuvre.

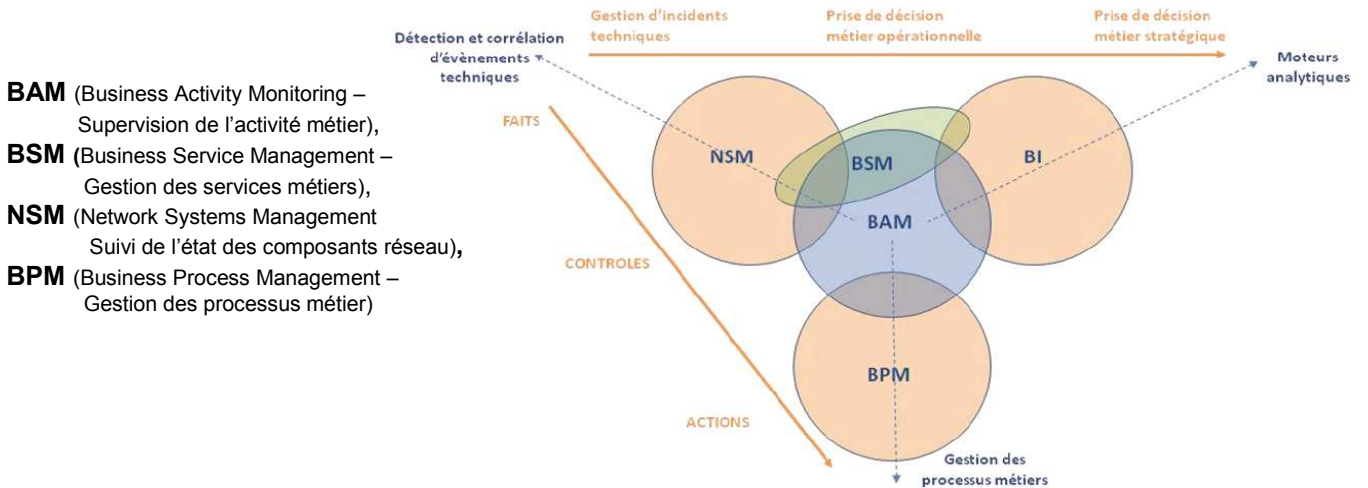
Les besoins des entreprises nécessitent aujourd'hui des contrôles et des mesures à tous les niveaux :

- Technique : utilisation des ressources, gestion des événements, alerte de sécurité ;
- Utilisateur : scénarios, réponse des applications (performance), contrôle fonctionnel ;
- Métiers : contrôles financiers, calcul des coûts d'incidents et impacts métiers.

Ce concept est aujourd'hui connu sous le nom d'hypervision, (ou supervision V2) qui a pour ambition de modéliser la supervision d'un SI, en consolidant l'existant, en alignant la technique sur les objectifs métiers de l'entreprise, avec une approche Globale/Détail (Top Down).



Chez les éditeurs commerciaux, de nouveaux produits commencent à apparaître (Actional de Progress Software ou les offres de Syster) dans des acronymes publicitaires plus ou moins complexes :



Mais comme le montre le schéma ci-dessus, des solutions actuelles proposées ne couvrent pas encore tout le spectre du besoin de l'hypervision, avec une supervision centralisée du SI de l'entreprise.

Le monde open source est encore absent de ce milieu, bien que des propositions commencent à prendre forme avec :

- La gestion des performances applicatives avec le projet Sikuli du MIT ou des propositions d'éditeur open Source : Webinject de Groudwork, Selenium d'Opsview, le projet Wat
- Les add-ons Nagios orienté « métier » (Nagios Business Process, Nagvis, futur Nareto); (voir Annexe 12)
- Le projet Cucumber de Holmwood, le projet allemand IT-COCKPIT
- Des projets orientés ITIL (EON, iTop, OTRS) (voir Annexe 13)
- Des outils de gestion de logs permettant une analyse fine métier (Graylog2, Log.io) ;
- Des logiciels de corrélations comme OSSIM d'alienvault.

Néanmoins un projet open source, (français comme shinken), commence à faire parler de lui: **CANOPSIS**, de la société Capensis. Entre autres, le groupe industriel EIFFAGE l'a retenu pour la surveillance de son nouvel ERP et finance le développement du module « reporting », sous licence AGPLV3 (donc pas surprise par rapport à une version entreprise). Recettée pendant l'été 2012, une version stable opérationnelle est prévue à la rentrée. Capensis a fait une présentation son produit, à Nantes, le 5 avril 2012 [CRR-CANOPSIS-SUPERV-NP]. Son fonctionnement est décrit en annexe 14.

Comme l'a fait remarquer Olivier Jan, chef de ce projet, fondateur du site monitoring.fr (voir annexe15) et figure emblématique mondiale de la supervision open source, lors de son exposé, l'hypervision répond à des réels besoins des DSI et des décideurs financiers des entreprises, aussi c'est une des pistes que doit obligatoirement prendre la supervision de demain.

Couplé au produit Shinken, Canopsis est sans nul doute le projet à surveiller, dans les années à venir.

CONCLUSION

La supervision est devenue un secteur à part entière, dans les entreprises soucieuses de la disponibilité de leurs Systèmes d'Information. Ce projet a permis au Service de Santé des Armées de s'équiper d'un outil modulaire, basé sur le produit open source Nagios, simple et efficace.

L'étude de ces logiciels de supervision a montré le dynamisme des produits open source, avec des sorties régulières de nouvelles versions et l'apparition de concepts ambitieux : Shinken, Canopsis. Lors du déroulement de l'étude, des choix ont dû être réalisés, pour répondre aux contraintes calendaires et aux impossibilités technologiques. Comme souligné dans le dernier chapitre, les outils open source ne répondent pas obligatoirement aux nouveaux besoins des entreprises, en particulier pour la surveillance des applications et l'intégration dans une solution complète validée ITIL. Néanmoins la plateforme Nagios installée, en complément du logiciel JBoss Operation Network, propose déjà un outil pertinent et efficace, qu'il conviendra de faire évoluer, avec les améliorations et les nouveautés techniques à venir.

Finir mon parcours au CNAM aura été pour moi, un objectif professionnel, car c'est une école de volonté, reconnue pour la qualité des connaissances enseignées. Le bilan de cette fin de parcours, avec ce projet en vue d'obtenir le diplôme d'ingénieur CNAM, aura été double.

Tout d'abord, techniquement, l'étude du projet couvrait l'ensemble des spécialités de l'informatique : réseau, système (Linux, script shell, VMware, Loadbalancing, redondance...), applicatifs (JBoss, Tomcat, Tuxedo, SQL, Oracle...)... Il aura fallu, avec une certaine nostalgie, ré-ouvrir les anciens cours du CNAM, les supports de formation LPI Linux et étudier de nombreux livres techniques, pour redécouvrir ou acquérir tous ces concepts. Le maquetage et l'installation opérationnelle de la plateforme aura nécessité de faire dialoguer ces différentes technologies, avec plus ou moins de patience et de difficultés.

Certes l'éloignement n'a pas facilité les échanges, mais a obligé à plus de rigueur dans la documentation présentée, le suivi des plannings et la gestion de la communication. Ce mémoire aura été une expérience technique et organisationnelle plus qu'enrichissante.

Enfin, cette étude aura été aussi une aventure humaine, avec ses sacrifices, ses déceptions, ses joies... Les nuits auront été courtes, mais la satisfaction est aujourd'hui grande, d'avoir participé à ce projet ambitieux du SSA. La démarche et les connaissances acquises seront, sans nul doute, des atouts pour la recherche d'un nouveau poste, en cette période délicate de restructuration, au Ministère de la Défense.

page vierge

GLOSSAIRE

AFNOR : *Association Française de Normalisation*

API (*Application Programming Interface*) Interface fournie par un programme informatique pour l'interaction avec d'autres programmes.

ASN.1 (*Abstract Syntax Notation One*) Standard de ISO/CEI spécifiant une notation destinée à décrire des structures de données.

ASN.1 (*Abstract Syntax Notation number One*) Notation formelle qui permet de spécifier facilement les informations dans une base de données.

AV (*Antenne vétérinaire*) Service du SSA assurant le soutien médical des animaux (chiens, chevaux) du Ministère de la Défense, le contrôle de l'eau et de l'alimentation distribuées sur les bases militaires.

BDM (*Business Data Model*) Structure de données métier utilisée pour échanger des informations entre des applications au travers d'un intergiciel.

CEDIP service à compétence nationale du Ministère de l'Écologie, du Développement durable, des Transports et du Logement

CGI (*Common Gateway Interface*) ou (*Interface passerelle commune*) : Interface normalisée utilisée par les serveurs http. CGI est le standard qui indique comment transmettre la requête du serveur Web au programme et comment récupérer la réponse générée.

CLOUD : Ressources informatiques distribuées sur intranet ou internet, proposés en tant que « services » pour de multiples utilisateurs. (voir SaaS, Paas, IaaS)

Cluster Ensemble de serveurs, au minimum deux, garantissant une redondance entre eux pour assurer une continuité de service et/ou répartir la charge de calcul et/ou la charge réseau

CMA : (*Centre Médical des Armées*) Centre médical dans les bases Marine/Terre/Air ou Gendarmerie.

CMDB (*Configuration Management DataBase*) : Base de données des composants (matériel, processus...) d'un système d'information défini dans ITIL.

CMPA : (*Centre de médecine de Prévention des Armées*) Service du SSA assurant le contrôle médical périodique et obligatoire des personnels civils du Ministère de la Défense.

CNAM (Conservatoire National des Arts et Métiers)

CoBIT (*Objectifs de contrôle de l'Information et des Technologies Associées*) Référentiel permettant d'instaurer un langage commun dans la Gouvernance des Systèmes d'Information tout en tentant d'intégrer d'autres référentiels tels que ISO 9000, ITIL ou ISO/CEI 27001.

DGSAGIR (*Direction Générale des Solutions d'Affaires en Gestion Intégrée des Ressources*), organisme, dépendant du Centre de Service partagés du Gouvernement du Québec, pilotant l'ensemble des projets informatiques de l'administration québécoise.

DHCP (*Dynamic Host Configuration Protocol*) Configuration automatique des paramètres

DIRISI (*Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la défense*) Organisme regroupant l'ensemble des informaticiens de l'Armée de l'Air, de la Marine et de l'Armée de Terre. En 2014, elle intégrera les autres organismes restants (SSA, DGA, SGA, SEA...) et permettra d'avoir une seule entité pour la gestion de la globalité du Système d'Information du Ministère de la Défense.

DNS (*Domain Name Server*) Protocole de gestion des noms de domaine réseau, avec une résolution traduisant un nom de serveur par son adresse IP.

DRDB (*Distributed Replicated Block Device*), système permettant de synchroniser deux éléments.

DRHAT (*Direction des Ressources Humaine de l'Armée de Terre*)

DRSSA : (*Direction Régionale du Service de Santé des Armées*) Au nombre de six au niveau national, organisme régional chargé d'administrer et piloter les activités des CMA et organismes SSA associés relevant de son autorité, dans le domaine soutien des forces.

EAARS (*Echelon Avancé Réduit de Ravitaillement Sanitaire*)

EAI (*Enterprise Application Integration*). Famille d'intergiciels d'échanges rapides et de manière asynchrone de messages électroniques de faible taille.

EFS (*Etablissement Français du Sang*)

GNU/GPL (*General Public License/ Licence Publique Générale*) Licence qui fixe les conditions légales de distribution des logiciels libres du projet GNU. Chaque personne a la permission de modifier le travail, de l'étudier et de redistribuer le travail ou un travail dérivé.

Heartbeat Signal échangé pour tester la disponibilité des éléments du cluster, et gérer la haute disponibilité.

HTTP (*Hyper Text Transfert Protocol*) Protocole de communication du Web.

IaaS : (*Infrastructure as a service*) Cloud proposant des Infrastructures (serveur, réseau, stockage) comme service

IETF (*Internet Engineering Task Force*) Groupe de travail qui développe les nouveaux standards pour l'informatique.

IP (*Internet Protocole*) Protocole de la couche « Réseau » de l'ISO.

ISO (*International Organisation for Standardization*) Organisation internationale de standardisation regroupant les organismes similaires de 89 nations se chargeant des standards informatiques actuels.

ITIL (*Information Technology Infrastructure Library*) Ensemble d'ouvrages définissant les bonnes pratiques pour la gestion de services informatiques.

J2EE (*Java Enterprise Edition*.) Spécification de Sun pour définir une approche structurelle multi niveaux pour les applications Java.

JON (*JBoss Operation Network*) version commerciale de l'outil open source JOPR/RHQ, proposée pour la supervision de l'offre Redhat (linux Redhat, JBoss, Tomcat..) et les interfaces extérieures (Apache, Oracle..)

MIB (*Management Information Base*), Base d'informations structurée d'un équipement utilisé par SNMP

MOA (*Maîtrise d'OuvrAge*). Définissant le besoin du projet, son calendrier et le budget consacré, il est *client* du MOE à qui il passe commande de la réalisation d'un produit (ouvrage), nécessaire à son activité.

MOE (*Maîtrise d'œuvre*) : C'est l'entité retenue par le maître d'ouvrage MOA pour réaliser l'ouvrage, dans les conditions de délais, de qualité et de coût fixés par ce dernier conformément à un contrat. Il est responsable des choix techniques inhérents à la réalisation de l'ouvrage suivant les exigences du cahier des charges. Le MOE fournit le produit demandé par la MOA.

MRTG (*Multi Router Traffic Grapher*) Logiciel gratuit basé sur SNMP permettant la traduction graphique de données

MySQL Système de gestion de bases de données open source.

NagiosQL : Interface Web d'administration de Nagios

NConf : Interface web de configuration de Nagios (développé par Sunrise)

NRPE : *Nagios Remote Plugin Executor*

NSCA : *Nagios Service check Acceptor*

NSClient : *Nagios Service Client*

OID (*Object Identifier*) nom définissant un objet dans le MIB de SNMP.

Open Source Logiciel dont le code source est disponible.

OSI (*Open Systems Interconnection*) Architecture à 7 couches, qui normalisent les niveaux de service et interactions entre les ordinateurs qui échangent des données à travers un réseau.

PaaS : (*Platform as a service*) Cloud proposant des Plates-formes (.Net, J2EE, SGBD ...) comme service

PERL : Langage de programmation interprété reprenant des fonctionnalités du langage C et des langages de scripts.

PHP (*Hypertext PreProcessor*) Langage de script utilisé pour la création de page Web dynamique.

PNG (*Portable Network Graphics*) Format ouvert d'images numériques, qui a été créé pour remplacer le format GIF.

QoS (*Quality of service*) Qualité d'un service informatique pour un utilisateur. Elle se mesure à partir de nombreux facteurs différents comme la disponibilité du service, le temps d'attente pour obtenir le service, l'intégrité des données.

RAID (*Redundant Array of Independent Disks*) Architecture spécifique de disques durs, afin d'augmenter la disponibilité des données.

RDDTool : *Round-Robin Database Tool*

RFC (*Request For Comment*) Série de documents techniques émanant de la communauté de recherche et du développement, pouvant devenir des normes.

SaaS : (*Software as a service*) Cloud proposant des Logiciels (standards ou métiers) comme service

SI (*Système d'Information*) Ensemble des moyens (organisationnels et humains, logiciels, matériels) qui permettent de gérer l'information (acquérir, stocker, rechercher, restituer, transformer, enrichir, échanger, archiver).

SIH (*Système d'Information des Hôpitaux*) Système d'Information composé de divers logiciels éditeurs (Amadeus de Mc Kesson, Chimio/Pharma de Engineering, Cursus de Guyot Walsler, TD-Siemens de Siemens, Antares de Enovacom) fédéré par un EIA de Cloverleaf, pour offrir des outils pour l'organisation et la gestion quotidienne d'un hôpital.

SIRAV (*Système de RAVitaillement*) Système d'Information, utilisé par la composante Ravitaillement Sanitaire du SSA pour la gestion et la maintenance du parc d'équipements biomédicaux

SISMU (*Système d'Information Santé Médical d'Unité*) Système d'Information (composé en particulier du logiciel LUMM) utilisé dans les unités et les Centres Médicaux des Armées, pour le suivi médical des soldats.

SLA (*Service Level Agreement*) Accord entre un fournisseur de services et un client permettant la définition d'un niveau de service attendu (notion ITIL)

SMS (*Short Message Service*) Message court (160 caractères max) utilisé en téléphonie mobile

SMTP (*Simple Mail Transfer Protocol*) Protocole de communication pour l'envoi de courriels vers les serveurs de messagerie électronique.

SNMP (*Single Network Management Protocol*) Protocole de communication qui permet la gestion, l'interrogation et la surveillance de composants réseau.

SOAP (*Simple Object Access Protocol*) Protocole de communication d'objets entre systèmes distants.

SSA (*Service de Santé des Armées*)

TCP (*Transmission Control Protocol*) Protocole de la couche Transport de l'ISO en mode connecté

TCP/IP d'une station (adresse IP, Masque réseau, passerelle, DNS...)

UDP (*User Datagram Protocol*) Protocole de la couche Transport de l'ISO en mode non connecté

UIT (*Union International des Télécommunication*) Le secteur de la normalisation des télécommunications, l'UIT-T, intervient également dans le domaine de l'e-Santé, notamment avec son Groupe d'étude 16. Le groupe de coordination de la normalisation de l'e-Santé (eHSCG5), créé en 2003, associe les organisations et comités OMS, ISO/TC 215, CEN/TC 251, IEEE/1073, IEC/TC 62, DICOM, OASIS et HL7. Il maintient une liste de normes dans les secteurs de l'e-santé.

Val-IT Référentiel de gouvernance des systèmes d'Information complétant CoBit, dans le domaine des Investissements à forte composante IT pour des projets "métier", du management d'un "Portefeuille" de projets et de programmes et du suivi des "business cases"

Webinject : Solution de test applicatif à l'aide de requête HTTP/HTTPS. (Extension pour Nagios)

BIBLIOGRAPHIE et WEBOGRAPHIE

- Jean GABES, **NAGIOS 3 pour la supervision et la métrologie**, Editions EYROLLES 2009
- Olivier JAN, **NAGIOS au cœur de la supervision Open Source**, Editions ENI, 2008
- Wolfgang BARTH, **NAGIOS, 2Ed System and Network Monitoring**, Edition Open Source GmbH 2009
- David Josephsen , **Building a monitoring Infrastructure with Nagios** , Edition Prentice Hall, 02/2007
- Wojciech Kocjan, **Learning Nagios 3.0** , Packt Publishing , Octobre 2008
- M. Schubert,D Bennette,J Gines, A Hay,**Nagios 3 Entreprise Network Monitoring**, Edition Syngress 2008
- François Pignet, **Réseaux Informatiques - Supervision et Administration**. Ed. ENI 2007.
- H.P. MADERS & J.L MASSELIN – **Piloter les risques d’un projet** , Ed Eyrolles , 2009
- Christian DUMONT, **ITIL pour un service informatique optimal** 2ed, Edition EYROLLES 2007
- **ITIL V3 – Formation** du Chef de Bataillon Laurent Barbey, Chef de la section Ingénierie du CIRISI Mindef – 01/2010.
- Tony Bourke, **Server Load Balancing**, Edition O’Reilly Media , août 2001
- David AUTISSIER, **Mesurer la performance du Système d’Information**, édition EYROLLES 2008
- E. Fimbel, S. Costa , **Management des systèmes d’information**, 11^{ème} éd, Edition Pearson ; 2010
- P. Degoulet & M Fieschi, **Informatique Médicale**, 3ed., Edition Masson , 2000
- Thomas Urban , **Cacti 0.8 Beginner’s Guide**, Packt Publishing , Mars 2011
- S. Alapati,D. Kuhn & Bill Padfield, **Oracle Database 11g Performance Tuning Recipes**, Ed Apress,29/08/11
- M. J. Kamir , **Apache Server 2 Bible** , edition Hungry Minds , 2004
- V. Chopra, S. Li & J. Genender, **Apache Tomcat 6**, Edition Wiley Publishing Inc, 2007
- Francesco Marchioni – **JBoss AS5 Performance Tuning** , Packt Publishing , Décembre 2010

- **BIRT** : www.eclipse.org/birt/phoenix/ , consulté 08/2011
- **Blog et forum sur monitoring** : www.monitoring-fr.org, consulté 08/2011
- **CANOPSIS** : www.canopsis.fr , consulté 03/2012
- **CACTI** <http://cacti.net>, consulté 06/2011
- **CENTREON** : www.centreon.com, consulté 08/2011
- **CIGREF** : www.cigref.fr , consulté 07/2011
- **Communauté Francophone de Supervision Libre**: www.cfsl-asso.org et www.monitoring.fr.org (voir annexe 14)
- **DNX** Distributed Nagios eXecutor : <http://dnx.sourceforge.net>, consulté 08/2011
- **EON** (Eyes Of Network) : www.eyesofnetwork.com, consulté 08/2011
- **FAN** (Fully Automated Nagios) : <http://fannagioscd.sourceforge.net>, consulté 07/2011
- **Formation Supervision et Métrologie 3 & 4** Juin 2010 – CNRS : http://cesar.com.univ-mrs.fr/IMG/pdf/supervision_v2010_avec_commentaires.pdf, consulté 08/2011
- **GANGLIA**: <http://ganglia.sourceforge.net>, consulté 06/2011
- **GRAPHITE** : graphite.wikidot.com/start consulté 08/2011
- **ICINGA** : www.icinga.org, consulté 06/2011
- **Installation JBoss Clustering** : www.scribd.com/doc/54422322/JBoss-clustering-et-tuning-lab-2-3 08/2011
- **ISO** Information security management systems. www.iso.org, consulté 05/2011
- **ITCockpit** : <http://www.open-itcockpit.com> consulté 11/2011
- **ITIL** : www.itilfrance.com, consulté 07/2011
- **ITOP** : www.combodo.com, consulté 08/2011
- **JasperREPORTS** : <http://jasperforge.org/projects/jasperreports>, consulté 08/2011
- **JBOS**S : www.jboss.org consulté 08/2011
- **JMX** : <http://www.oracle.com/technetwork/java/javase/tech/javamanagement-140525.html> consulté 08/2011
- **JON** (présentation) : www.scribd.com/doc/47627502/1-26-7P-njakusz-jboss-management consulté 08/2011
- **MediaWiki** : www.mediawiki.org consulté 09/2011
- **MERLIN** : www.op5.org/community/plugin-inventory/op5-projects/merlin, consulté 08/2011
- **MK CHECK** : http://mathias-kettner.de/check_mk.html, consulté 08/2011
- **MK_LIVESTATUS** : http://mathias-kettner.de/checkmk_livestatus.html, consulté 08/2011
- **MOD_GEARMAN** : gearman.org consulté 07/2011
- **MRTG** Tobi Oetiker : www.mrtg.org, consulté 07/2011
- **MUNIN** : www.munin-monitoring.org, consulté 08/2011
- **NBPA Nagios Business Process Add-on** : <http://bp-addon.monitoringexchange.org>, consulté 08/2011

- **Nagios plugin**. Developer-guidelines. <http://nagiosplugins.org>, *consulté 07/2011*
- **NAGIOS** The Official Nagios: www.nagios.org, *consulté 08/2011*
- **Nagios World Conference** : <http://www.nagios.com/events/nagiosworldconference> , *consulté 08/2011*
- **NAGVIS**: www.nagvis.org, *consulté 08/2011*
- **NINGA** : www.op5.org/community/plugin-inventory/op5-projects/ninja, *consulté 08/2011*
- **OMD** (Open Monitoring Distribution) : <http://omdistro.org/>, *consulté 08/2011*
- **OP5** : www.op5.com *consulté 06/2011*
- **OPENNMS** : www.opennms.org, *consulté 06/2011*
- **OpenSource Monitoring Conference** : www.netways.de/en/osmc , *consulté 08/2011*
- **ORACLE** : www.oracle.com/fr/index.html *consulté 08/2011*
- **OSSEC HIDS** : www.ossec.net, *consulté 08/2011*
- **OTRS:ITSM** : www.otrs.com , *consulté 08/2011*
- **Plugin Cacti** : <http://docs.cacti.net/plugins>, *consulté 08/2011*
- **Plugin Nagios**, Nagios Exchange : www.nagiosexchange.org, *consulté 08/2011*
- **PNP4NAGIOS** : www.pnp4nagios.org, *consulté 08/2011*
- **PRELUDE** : www.prelude-technologies.com, *consulté 08/2011*
- **RRDTool** : (Round Robin Database Tool) : www.mrtg.org/rrdtool, *consulté 08/2011*
- **SHINKEN** : www.shinken-monitoring.org, *consulté 08/2011*
- **SNMP** : Research International Inc. SNMP RFCs. www.snmp.org, *consulté 07/2011*
- **SNORT NIDS** : www.snort.org, *consulté 08/2011*
- **TRUK** : www.thruk.org, *consulté 07/2011*
- **VISUALVM** : <http://visualvm.java.net> *consulté 08/2011*
- **WEATHERMAP** : www.network-weathermap.com, *consulté 08/2011*
- **ZABBIX**, www.zabbix.org, *consulté 06/2011*

- **Forums de discussion :**

- <http://forums.monitoring-fr.org/>,
- <http://exchange.nagios.org/>,
- <http://forum.centreon.com/>,
- <http://www.linkedin.com/> (groupes Nagios users, Cacti users)

CONSERVATOIRE NATIONAL DES ARTS & METIERS
Centre Régional associé de Rennes

ANNEXE

Mémoire présenté en vue
d'obtenir le diplôme d'ingénieur **C.N.A.M.**
en informatique

Jacques BIDANEL

**SUPERVISION DE L'INFRASTRUCTURE
DES SYSTEMES D'INFORMATION METIER
DU SERVICE DE SANTE DES ARMEES**

soutenu le 20 juin 2012

JURY

PRESIDENT:

Professeur POLLET

MEMBRES:

Mr ROSTOLL
Mr CHAMPION
Mr DESCAT

Version 1.0, imprimée le 15 mai 2012
en Recto/Verso pour être respectueux de l'environnement

1. Documentation du projet.....	89
2. Technologies utilisées dans les SI.....	91
2.1 Serveur web apache.....	91
2.2 Serveur JBoss.....	91
2.3 Serveur Oracle.....	94
3. Mise en œuvre de Nagios.....	95
4. Fichiers de configuration Nagios.....	98
5. Logiciels de supervision Open source.....	99
5.1. SHINKEN.....	99
5.2. ICINGA.....	101
5.3. ZABBIX.....	101
5.4. OPENNMS.....	101
6. Distribution linux de supervision.....	102
6.1. CES (Centreon Enterprise Server).....	102
6.2. FAN (Fully Automated Nagios).....	102
6.3. EON (Eyes Of Network).....	102
6.4. OMD (Open Monitoring Distribution).....	103
6.5. CatiEZ.....	103
7. Broker.....	104
8. Autres outils à suivre.....	105
9. Gestion Syslog dédiée Centreon.....	105
10. Architecture distribuée.....	106
11. Interface graphique.....	106
12. Reporting (génération de rapports).....	107
13. Logiciels NOC Open Source, conformes ITIL.....	109
14. Hypervision : projet Canopsis.....	110
15. Communauté France : Monitoring.fr.org.....	111
16. Questionnaire SI Métier.....	112
17. Questionnaire pour rédaction CdCF.....	115
18. Analyse des risques.....	119
19. Grille REX.....	127

page vierge

1. Documentation du projet

1.1 Avant projet

- Proposition de mémoire CNAM- [SUJ-CNAM-SUPERV-NP-2.1](#)
- Nomination de Mr Champion comme tuteur SSA

1.2 Documents fournis pour l'étude

(Envoi document spécification CETIMA - [BL-SPECIF-SUPERV-N1-DR-1.0](#))

SISMU

Schéma de plateforme SISMU
Document ARES-LUMM V2
TME dossier exploitation V1.1 Application LUMM 2

SIH

Cartographie cible RL 2
Formation Cloverleaf 5.5
L54 - Exploitation Amadeus 2 SR V1.1

SIRAV

Schéma SIRAV
Fourniture mot de passe serveur - [PWD-SUPERV-N1-DR-1.0](#)
Liste des serveurs (gérés par TINA) - [BL-TINA-SUPERV-N3-DR-1.0](#)
Indicateurs supervision SISMU - [BL-IND-SUPER-N2-NP-1.0](#)

1.3 Compte-rendu de réunion ou visioconférence

- Réunion de lancement 19/04/2011 - [CCR-CETIMA-SUPERV-N1-DR-1.0](#)
- Réunion DIRISI Brest 12/05/2011 - [CCR-DIRISI-SUPERV-DR-1.0](#)
- Réunion HIA Brest 12/05/2011 - [CCR-HIA-SUPERV-N1-NP-1.0](#)
- Salon Linux Open Source 11/05/2011 - [CCR-SALON-SUPERV-NP-1.0](#)
- Bilan des travaux 2 mai 2011 - [VISIO-SUPERV-N1-DR-1.3](#)
- Bilan des travaux 16 mai 2011 - [VISIO-SUPERV-N2-NP-1.0](#)
- Bilan des travaux 29 Juin 2011 avec CNAM- [VISIO-SUPERV-N3-NP-1.0](#)
- Bilan des travaux au 30 Juillet 2011 - [VISIO-SUPERV-N4-NP-1.0](#)
- Bilan des travaux au 16 Aout 2011 - [VISIO-SUPERV-N5-DR-1.0](#)
- Bilan des travaux au 6 Septembre 2011 - [VISIO-SUPERV-N6-NP V1.0](#)
- Bilan du mémoire CNAM/CeTIMA au 26 Septembre 2011 - [CCR-CNAM-SUPERV-N1-1.0](#)
- Bilan des travaux au 10 décembre 2011 - [VISIO-SUPERV-N7-NP V1.0](#)
- Bilan des travaux au 27 Mars 2012 - [VISIO-SUPERV-N8-NP-1.0](#)
- Bilan contact DIRISI Air (directives exploitation de solution de supervision DIRISI) - [BL-INFO-SUPERV-DR-1.0](#)
- Réunion Capensis – Hypervision Canopsis 05/04/2012 – [CCR-CANOPSIS-SUPERV-NP-1.0](#)

1.4 Livrables

- Plan Assurance Qualité [PAQ-SUPERV-NP-1.4](#)
- Gestion documentaire - [DOC-SUPERV-NP-2.0](#)
- Analyse des risques – [RISQ-SUPERV-NP-1.1](#) Voir annexe 18
- Planning - [PLANNING-SUPERV-NP 3.3](#)
- Tableau de bord – [TB-SUPERV-DR-3.2](#)

PHASE 1 : Etude des SI

Questionnaire pour les responsables applicatif- [AQUEI-SUPERV-DR-2.0](#) Voir annexe 16
Bilan d'architecture SI [ARCH-SUPERV-DR-1.0](#)

PHASE 2: CDCF

Questionnaire pour analyser le besoin - [QUES-SUPERV-NP-2.0](#) Voir annexe 17
Cahier des charges fonctionnel - [CDCF-SUPERV-NP-1.1](#)
Liste des indicateurs à superviser – [IND-SUPERV-DR-1.1](#)

PHASE 3 : Etude des solutions du marché et choix de la solution de supervision

Synthèse – choix d'une solution de supervision - [CH-SUPERV-NP-1.2](#)

PHASE 4 : Etude de la plateforme et ses composants

- Etude détaillée de la plateforme de supervision - [ETUDE-SUPERV-DR-1.0](#)
- Jeux de test [JX-SUPERV-DR-1.0](#)
- Dossier d'exploitation (installation, maintenance, sauvegarde) - [EXP-SUPERV-DR-1.1](#)

- AGENT POUR F5 - [F5-AGENT-SUPERV-NP-1.1](#)
- AGENT POUR NETASQ - [NETASQ-AGENT-SUPERV-DR-0.2](#)
- AGENT POUR JBOSS - [JBOSS-AGENT-SUPERV-DR-1.1](#)
- AGENT POUR APACHE - [APACHE-AGENT-SUPERV-NP-1.0](#)
- AGENT POUR ORACLE - [ORACLE-AGENT-SUPERV-DR-1.1](#)
- AGENT DELL OPENMANAGE – [DELL-OPENMANAGE-SUPERV-NP-0.1](#)
- AGENT POUR SISEL - [SISEL-AGENT-SUPERV-NP-0.1](#)
- AGENT POUR AGENT SISMU SPECIFIQUE - [SISMU-AGENT-SUPERV-DR-0.1](#)
- AGENT POUR MC KESSON - [MC_KESSON-AGENT-SUPERV-DR-0.2](#)
- AGENT POUR SQL SERVER - [SQL_SERVERL-AGENT-SUPERV-NP-0.1](#)

Procédures d'installation

- Installation Nagios - [P_NAGIOS-SUPERV-NP-1.3](#)
- Installation CENTREON - [P_CENTREON-SUPERV-NP-1.0](#)
- Installation NAGVIS et intégration Nagios, Centreon- [P_NAGVIS-SUPERV-NP-1.1](#)
- Installation CACTI - [P_CACTI-SUPERV-NP-1.1](#)
- Installation CES – [P_CES_SUPERV-NP-1.0](#)
- Installation JBOSS – [P_JBOSS-SUPERV-NP-1.1](#)
- Installation JON-RHQ-JOPR - [P_JON-SUPERV-NP-1.0](#)
- Installation ORACLE 10G- [P_ORACLE-SUPERV-NP-1.0](#)
- Installation CLIENT ORACLE - [P_CLIENT_ORACLE-SUPERV-NP-1.1](#)
- Installation SNMP - [P_SNMP-SUPERV-NP-1.0](#)
- Installation Script POSTFIX-NDO-NAGIOS-CENTREON - [P_SCRIPT-SUPERV-NP-1.0](#)
- Installation NRPE Client linux - [P_NRPE-C-SUPERV-NP-1.2](#)
- Installation agent NSCLIENT Client Windows - [P_NSCLIENT-C-SUPERV-NP-1.0](#)
- Installation MK_LIVESTATUS [P_MK_LIVESTATUS-SUPERV-NP-0.1](#)
- Installation POSTFIX - [P_POSTFIX-SUPERV-NP-1.0](#)
- Installation plugin Firefox pour nagios - [P_PLUGIN_FIREFOX-SUPERV-NP-1.0](#)
- Installation SSH - [P_SSH-SUPERV-NP-1.0](#)
- Installation Alerte SMS - [P_SMS-SUPERV-NP1.0](#)
- Installation Alerte RSS- [P_RSS-SUPERV-NP1.0](#)
- Installation Sauvegarde Supervision - [SUPERV-SUPERV-NP-1.0](#)
- Installation MediaWiki Base de connaissances - [WIKI-SUPERV-NP-1.0](#)
- Installation VisualVM – [P_VISUALVM-SUPERV-NP-1.0](#)
- Installation Redondance Nagios – [P_REDONDANCE-NAGIOS-NP-0.1](#)
- Installation Canopsis – [P_CANOPSIS_SUPERV_NP-0.1](#)

PHASE 5 : Maquettage

- Résultats des tests de maquettage - [MAQ-SUPERV-DR-1.1](#)
- Manuel Utilisateur - [UTIL-SUPERV-DR1.0](#)

Manuels d'utilisation

- Manuel CENTREON [U_CENTREON-SUPERV-NP-1.0](#)
- Manuel NAGVIS - [U_NAGVIS-SUPERV-NP-1.1](#)
- Manuel CACTI - [U_CACTI-SUPERV-NP-1.0](#)
- Utilisation des plugins - [U_CHECK-SUPERV-NP-1.0](#)
- Création d'un plugin Nagios – [U_CREA_CHECK-SUPERV-NP-1.0](#)
- Utilisation des traps SNMP avec Centreon – [U_TRAP_SUPERV_NP -1.0](#)

PHASE 6 : Mise en production

- BL station de supervision - [MAT-SUPERV-DR-1.0](#)
- Compte rendu d'installation – [DRSSA_BST-SUPERV-DR 2.1](#)
- Mise en production – [FORM-SUPERV-DR-1.0](#)
- Jeux des tests - [TESTS-SUPERV-DR 3.3](#)
- Formation – [FORM-SUPERV-DR1.2](#)
- Procès-verbal (partiel) de Vérification d'Aptitude SISMU – [PV_PARTIEL-SUPERV-NP-1.0](#)

PHASE 7 : Clôture projet : Rex, propositions d'amélioration

- Retour d'expérience - [REX-SUPERV-DR-1.0](#) Voir extrait annexe19
- Propositions d'amélioration et d'évolution - [EVOL-SUPERV-NP-1.1](#)
- Procès-verbal de Vérification en Service Régulier – [PV_VSR-SUPERV-NP-0.1](#)

2. Technologies utilisées sur les SI

2.1 Serveur web apache

La configuration générale du serveur est contenue dans le fichier **httpd.conf** (avec éventuellement les fichiers **access.conf** (contrôle d'accès) et **srm.conf** (pages web et script CGI), s'il est signalé dans le fichier les variables **AccessConfig** et **RessourceConfig**).

Certaines directives permettent de définir les performances du serveur :

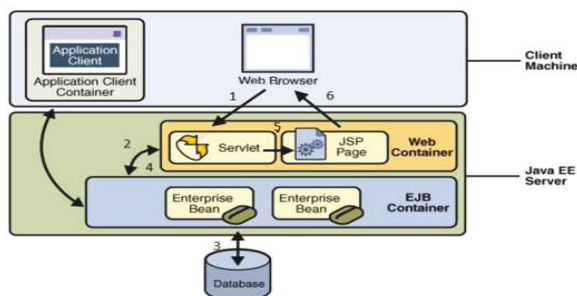
- Max Clients** : nombre maximum de clients (si le nombre est dépassé, les clients supplémentaires sont mis en attente)
- StartServers** ; nombre de processus httpd au démarrage
- MaxRequestPerChild** : nombre de requêtes géré par le processus fils de httpd
- MaxSpareServers** : nombre maximal de processus httpd inoccupés que l'on conserve (défaut 10)
- MinSpareServers** : nombre minimal de processus httpd (défaut 1)

```
Exemple <IfModule worker.c>
StartServers2
MaxClients150
MinSpareThreads25
MaxSpareThreads75
ThreadsPerChild25
MaxRequestsPerChild0
</IfModule>
```

2.2 Serveur JBoss

JBoss est un serveur d'application JEE (Java Entreprise Edition), Open Source sous licence LGPL, proposé par Redhat, utilisant différents services, au travers de différentes API.

2.2.1 Fonctionnement



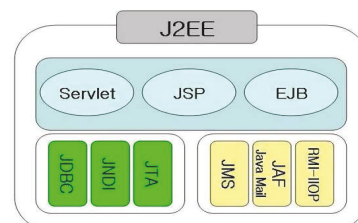
1. Le client émet une requête HTTP à destination de l'application, c'est en général une servlet qui reçoit la requête et qui en extrait les informations.
2. Les informations sont utilisées pour appeler les traitements métier.
3. Les composants du modèle manipulent les données du système d'information (lecture, enregistrement, mise à jour, ...).
4. Les traitements métier retournent les données résultats à la servlet, qui stocke ces données pour les rendre accessibles aux Java Server Pages (JSP).
5. La servlet appelle la JSP adéquate.
6. La JSP s'exécute, inclut les données transmises par la servlet, et génère la réponse au client.

2.2.1.2 Principaux Composants JEE

- **Servlet** est un composant Java, côté serveur orienté requêtes/réponse, Il permet de recevoir les requêtes HTTP , de les traiter et de fournir au client une réponse .
- **JSP (Java Server Pages)** : structurellement proche des pages PHP ou ASP, cette technologie Java permet le développement de page dynamique.
- **EJB (Entreprise JavaBeans)** : EJB est un composant métier distribué, gérant les transactions, la sécurité...
Il existe 3 types d'EJB :
 - **Session** : ils encapsulent l'ensemble des fonctionnalités métier nécessaires à l'application, ils peuvent, selon leurs configurations, maintenir ou non des informations sur les clients et les traitements qu'ils réalisent (**Stateless/Stateful**). Les EJB Session Stateful reflète la discussion avec un client particulier. Le serveur d'application a autant d'instances que de clients connectés au serveur. Ces EJB représentent un utilisateur connecté.
 - **Entity** : composant persistant représente les données qui alimentent les SGBD **MessageDrivenBean (MDB)** la file d'attente des messages postés par le serveur
- **JPA (Java Persistence API)** : Ces entités Java sont des objets persistants : leur état est sauvegardé dans une base de données relationnelle. L'API JPA assure le mapping entre les bases de données relationnelles et les objets du monde Java.
- **web services** : Assurent l'interopérabilité se basant sur http, ils ont constitués d'une collection de endpoints , décrit dans le WSDL (Web Service Description Language) au format XML , précisant les méthodes invoquées, l'URL ...

2.2.1.3 Principaux Services JEE

- **Services d'infrastructure** :
 - **JDBC** (Java DataBase Connectivity) permet aux programmes Java d'accéder aux bases de données ;
 - **JNDI** (Java Naming & Directory Interface) implémente un service de nommage et permet l'accès aux services d'annuaire d'entreprise (LDAP, DNS, NIS...);
 - **JTA** (Java Transaction API) / **Hibernate** définit les interfaces de gestion des transactions ;
 - **JCA** (JEE Connector Architecture) : permet d'utiliser une ressource du système d'information qui ne possède pas d'interface native Java/JEE (SAP ...).



• **Services de communication:**

- o **JMS** (Java Message Service) gère l'envoi de message applicatif entre les composants par un mécanisme asynchrone ;
- o **JAAS** (Java Authentication and Authorization Service) assure la gestion de l'authentification et des droits d'accès ;
- o **JavaMail** : permet la création et l'envoi de message électronique via Java ;
- o **RMI/IIOP** (Remote Method Invocation/Internet InterORB Protocol) API Java qui permet l'appel de fonctionnalité à distance, en utilisant une communication réseau.

NOTA : Citons pour information d'autres plateformes JEE

- **Commerciale** : Websphere d'IBM, GlassFish de Sun, Weblogic de BEA, Oracle 9i Application Server, Sun One.

- **Open Source** : JBoss, JOnAS, Apache Geronimo.

2.2.2. Architecture utilisée pour SISMU

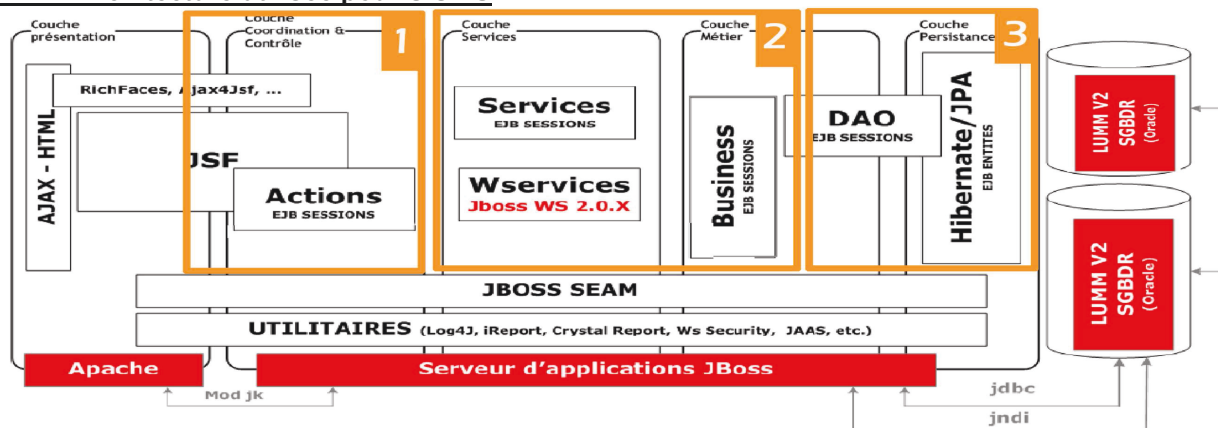


Figure 3 – Modèle d'architecture générale de développement par couches
(Information et schéma extrait de document ARES-LUMM-V2-DOSARTECH-V2.2)

1 - La Couche coordination contrôle est responsable de la fourniture des pages HTML et du traitement des requêtes. Elle est implémentée avec JSF et EJB3.0 de type Session Stateful

2 - Couches Service et Métier est responsable de la fourniture des services métiers

Implémentée par EJB3 Session et composants JBoss Web Service 2.0.X

3 - La Couches Persistance implémenté par Hibernate/JPA (Java Persistence API) et les classes DAO (Data Access Object),

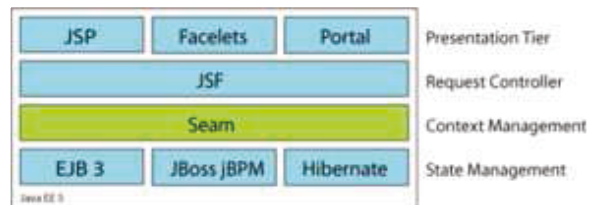
En résumé, nous arrivons à l'architecture simplifiée suivante :

1 - un client de type navigateur : HTML/Javascript/AJAX

2 - un serveur apache, gérant le traitement des requêtes en provenance du navigateur, couplé au mod_jk pour gérer le loadbalancing et la tolérance de panne des différentes instances JBoss

- 3 - un moteur JEE (JBoss EAP) avec différentes instances, gérant
- Un ordonnanceur pour la gestion de la navigation pour le site web (page JSF)
 - Un gestionnaire de transactions (Conteneur EJB)
 - Un mappeur objet/relationnel pour la couche de persistance (Hibernate/JAP)

4 -pour relier les différentes couches, JBoss Seam, un Framework JEE (dédié JSF/EJB3), offrant une grande rapidité de développement pour les applications web 2.0 dites « riches » (technologies Ajax)



Pour information :

La Gestion des logs est assurée par Log4J, qui pourra nous servir pour la recherche des pannes.

La Gestion de la sécurité est réalisée par JAAS (Java Authentication & Autorisation Service).

Le reporting se base sur iReport/Jaspers et Crystal Reports.

2.2.3 Fichiers importants de JBoss

- **A - Sur le serveur apache, le fichier de configuration du module mod_jk**

La répartition de charge JBoss peut être assurée de deux façons :

- Répartition verticale : plusieurs instances sur le même serveur physique
- Répartition horizontale : plusieurs instances réparties sur plusieurs serveurs.

La plateforme SISMU assure les 2 cas.

L'intégration du serveur JBoss avec un serveur web frontal se fait à travers un connecteur configuré dans JBoss (connecteur JK) et d'une extension mod_jk ajoutée au serveur web Apache (module mod_jk.so dans apache2/modules) dialoguant avec le protocole AJP13 (Apache Jserv Protocol)

La configuration d'un serveur JEE, avec un serveur web, utilise la notion de travailleur (worker), qui identifie une instance. Chaque travailleur est caractérisé par l'association d'un nom d'hôte (ou adresse IP) et d'un numéro de port). Le module mod_jk d'Apache agit comme un routeur de requêtes vers un ou plusieurs processus de serveur JEE.

Selon la configuration et les besoins, les types de worker suivants sont utilisés ajp13 (gestion instance serveur JEE), lb (configuration répartition de charge) ou status (obtenir des statistiques de répartition de charge).

Le module mod_jk assure cette répartition de charge en utilisant l'algorithme de répartition de charge Round-Robin (requêtes envoyées alternativement sur chacune des instances, toujours dans le même ordre). La gestion de l'affinité de session est néanmoins gérée, pour conserver sur le même serveur la session d'un même utilisateur.

Il gère aussi la tolérance aux pannes, avec un basculement des requêtes vers un autre serveur en cas d'anomalie du serveur initial.

Fichier workers.properties	Fichier httpd.conf
<pre># liste workers worker.list=loadbalancer,status <i>declaration loadbalancing</i> # definition noeud 1 (ajp13) <i>définition de connexion server 1</i> worker.worker1.type=ajp13 <i>connexions sont de type AJP13</i> worker.worker1.host=localhost <i>adresse IP serveur JEE</i> worker.worker1.port=8009 <i>port utilisé</i> worker.worker1.lbfactor=1 <i>facteur de repartition de charge</i> worker.worker1.connection_pool_size=10 # en cas de crash, reprise vers le nœud 2 worker.worker1.redirect=worker2 # definition noeud 2 (ajp13) worker.worker2.type=ajp13 <i>définition de connexion server 2</i> worker.worker2.host=localhost <i>possibilité de le mettre en actif/passif</i> worker.worker2.port=8109 <i>avec worker.worker2.activation=disabled</i> worker.worker2.lbfactor=1 worker.worker2.connection_pool_size=10 #fonctionnement de l'équilibrage de charge worker.loadbalancer.type=lb <i>définition loadbalancing</i> worker.loadbalancer.balance_workers=worker1,worker2 worker.loadbalancer.sticky_session=True <i>avec affinité de session</i> worker.status.type=status</pre>	<pre>... LoadModule jk_module modules/mod_jk.so <i>ajout mod_jk à la liste des modules chargés</i> ... # parametrage de mod_jk # JkWorkersFile conf/workers.properties <i>fichier de configuration à prendre en compte</i> JkShmFile logs/mod_jk.shm JkLogFile logs/mod_jk.log JkLogLevel info JkLogStampFormat "[%a %b %d %H:%M:%S %Y]" JkMount /* loadbalancer <i>quelles URL nous redirigeons et vers qui</i></pre>

- **B – Dans le fichier *server.xml* du nœud 1 sur serveur JBoss**

Pour traiter les requêtes entrantes, les connecteurs JEE utilise des threads dédiés au traitement de la requête et à l'envoi de la réponse. Pour éviter la création et suppression inutiles de threads, on utilise un pool de threads disponibles pour traitement, au lieu de détruire et recréer à chaque demande.

Dans les parties (*Executor/connector/Valve/Listener*), sont définies les valeurs de configuration du serveur :

maxThreads (défaut 40) : nombre maximum de threads du pool
minSpareThreads (défaut 25) : valeur initiale
accept_count (défaut 10) : nombre max de requêtes dans la file d'attente
connectionTimeout : délai d'attente maximum dans la liste d'attente
Valeur du listener pour JMX

- **C - Configuration des ressources sur JBoss (en particulier le pool de connexion JDBC)**

On indique le nom de la classe Java du pilote JDBC (driverClassName), l'URL de connexion du SGBD, et le nom d'utilisateur/password pour se connecter à la base.

Les informations de dimensionnement et de fonctionnement interne du pool de connexions sont disponibles :

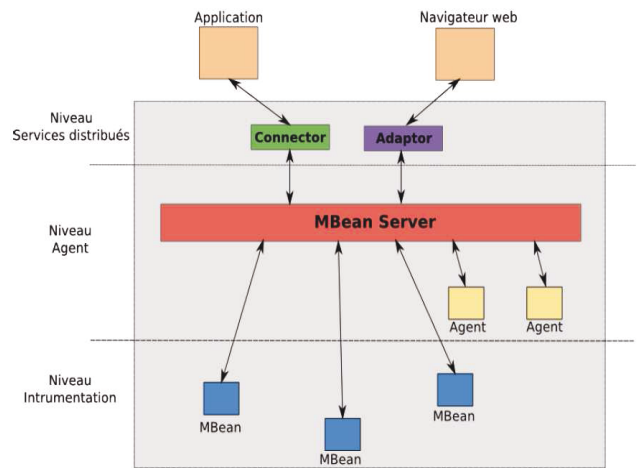
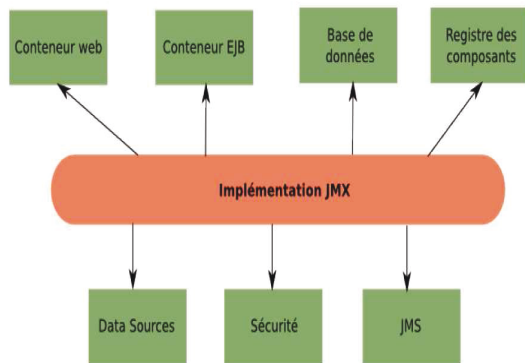
initiaSize (défaut 0) : nombre de connexion présente dans le pool au démarrage.
maxActive (défaut 8) : nombre maximum de connexions actives simultanément dans le pool
maxIdle (défaut 8) : nombre maximum de connexions en attente dans le pool.
minIdle (défaut 0) : nombre minimum de connexions en attente dans le pool.
maxWait (défaut temps d'attente indéfini) : temps d'attente, en millisecondes, avant que le pool ne renvoie une erreur, quand une connexion demandée n'est pas disponible.

2.2.4 API JMX

Conçue pour la supervision des applications Java, l'API Java JMX (Java Management Extensions) implémente un service de supervision, dans l'application JEE. Il est possible de développer ses propres outils, pour collecter les données, auprès de ce service de supervision Java.

Dans le serveur JEE, on associe à chaque objet Java un composant appelé MBeans, qui permet d'obtenir des informations et d'exécuter des traitements sur cet objet. Les MBeans de la JVM sont tous répertoriés et rendus accessibles via un élément central : le serveur de MBeans (MBean Server).

Des connecteurs (HTTP, SNMP, SOAP, RMI) sont disponibles pour s'interconnecter avec le MBean server et avoir une vue d'ensemble des MBeans et des composants du serveur JEE.



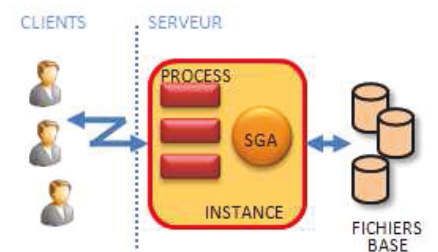
2.3. Serveur Oracle

Une base de données est constituée d'un certain nombre de fichiers : des fichiers de données, des fichiers journaux, des fichiers de contrôle, un fichier d'initialisation ou de paramétrage, un fichier de mot de passe et des fichiers d'archivage des journaux

Une instance active, ce sont des services ou processus (qui assurent la maintenance du serveur de données et les entrées / sorties vers les fichiers), des process server et une zone de mémoire SGA.

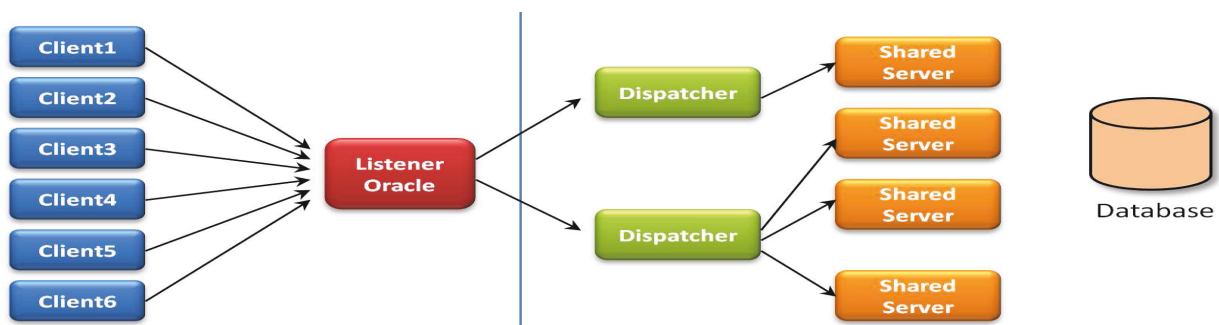
Une instance est caractérisée par son identificateur SID (System Identifier), une variable positionnée dans l'environnement.

Les fichiers de données contiennent les données proprement dites (essentiellement les tables et leurs lignes), mais aussi les autres objets Oracle connexes aux tables : index, vues, synonymes, database links, procédures stockées, etc...



Fonctionnement :

- Le client contacte le serveur de base de données après avoir résolu le nom de service.
- Le listener (LISTENER) valide le nom de service Oracle stocké par le client et redirige la connexion cliente vers un dispatcher moins chargé.
- Le listener envoie les informations au client qui peut se connecter sur le dispatcher approprié, qui place la requête dans une file d'attente (request queue) où le premier SHARED_SERVERS disponible se servira.
- Le dispatcher manage les requêtes serveur du client vers les SHARED_SERVERS ou Processus Serveur (ora_S00n), qui traite la requête, accède au SGBD et met le résultat dans la file d'attente de réponse (response queue) du dispatcher demandeur.



Valeurs importantes : Fichier init.ora ou initSID.ora

- **MTS_DISPATCHERS** donne le nombre et les caractéristiques des dispatchers (adresse, description, protocole, CONNECTION nombre max de connexions pour chaque dispatcher, DISPATCHER le nombre initial de dispatchers lancés (default = 1))
- **MTS_MAX_DISPATCHERS** nombre de process dispatcher simultanés maximum
- **MTS_SERVERS** le nombre de process serveur créés au démarrage
- **MTS_MAX_SERVERS** nombre de process simultanés maximum

3. Mise en œuvre de Nagios

3.1. Contacts

A chaque host et à chaque service, on associe un contact ou groupe de contacts, dans une période définie, afin de prévenir les responsables techniques uniquement pour les incidents, qui les concernent.

3.2. Ordonnancement des vérifications

Nagios est un ordonnanceur de vérifications (exemple paragraphe 4.4). Voyons tout d'abord comment, il détermine l'état d'un service ou d'un hôte supervisé.

Types d'état

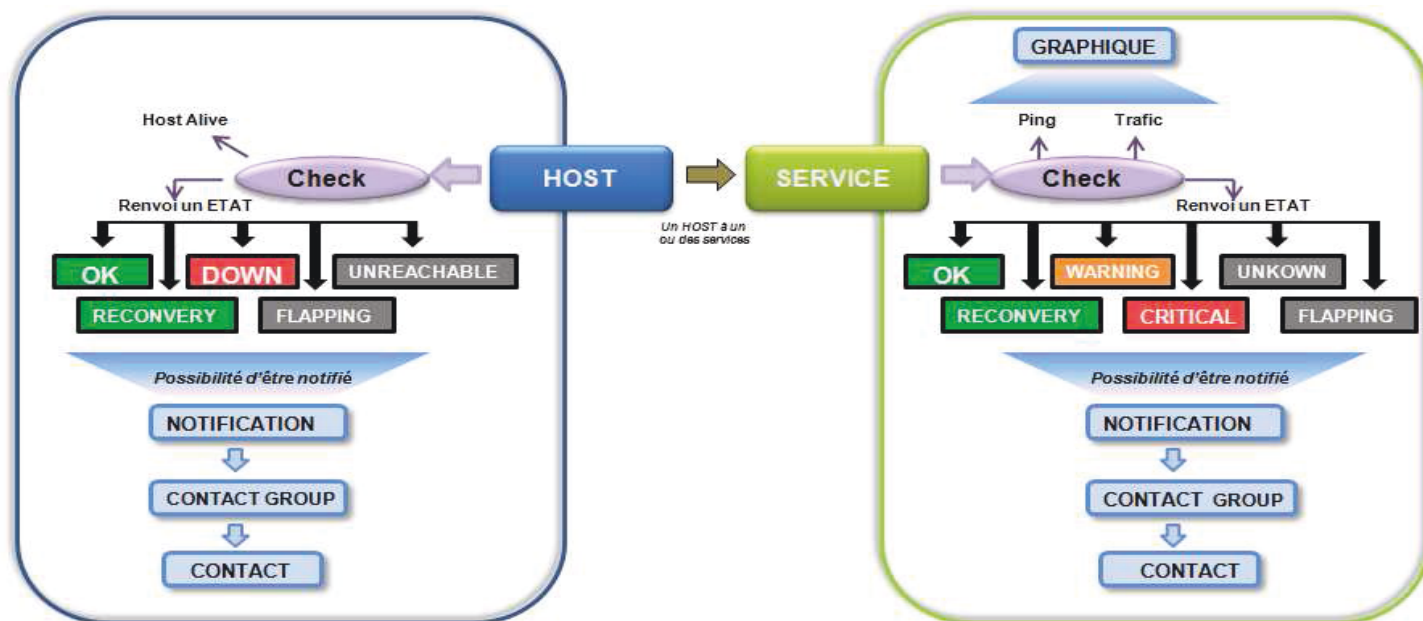
SOFT

- le problème a été détecté, l'état courant est en cours de caractérisation ;
- aucune notification n'a encore été émise ;
- possibilité d'agir pour éviter les alertes, par une action corrective (Gestionnaire événement).

HARD

- le problème est établi (stable), l'état identifié ;
- les notifications sont en cours ;
- possibilité d'agir pour éviter les alertes (Gestionnaire événement).

Valeurs des états



Pour le contrôle des **HOST**, on lui affecte une commande de vérification (check), réalisée par l'agent ou sonde, qui retourne une valeur, correspond à l'état du serveur. Cette valeur peut être :

- OK** : Host joignable sans problème
- RECOVERY** : il sort d'une période d'indisponibilité
- DOWN** : il n'est pas disponible
- UNREACHABLE** : il n'est pas joignable ou ne l'a jamais été
- FLAPPING** : il est plus ou moins joignable (voir explication ci-dessous)

Pour les **services**, le test est identique, avec les retours possibles suivants :

- OK** : Service opérationnel
- RECOVERY** : sort d'une période d'indisponibilité
- WARNING** : Avertissement sur le service (seuil sensible atteint)
- CRITICAL** : Erreur critique sur le service
- UNKNOW** impossibilité de déterminer l'état du service
- FLAPPING** : période de ballotage (voir ci-dessous).

Détection du Flapping

Flapping correspond à un changement d'état trop fréquent

Si la détection est activée, lorsque le host/service "bagotte", un envoi interne d'une notification "flapping start" est réalisé et bloque les notifications pour ce host/service. Lorsque le comportement se stabilise, la notification "flapping stop", débloque des notifications pour ce host/service et les tests courants continuent. Cette option permet d'éviter des alertes inutiles, pour des micro-dysfonctionnements, qui sont néanmoins historisés.

Séquençage des types d'état

➤ **Détection d'un problème**

(OK,hard) → (CRITIQUE,soft) → (CRITIQUE,soft) → (CRITIQUE,hard)

Nagios est configuré pour tester à plusieurs reprises un élément (max check attempts – ici 2 tests max) avant de réagir à l'anomalie et de passer en état hard.

➤ **Retour à la normale (RECOVERY)**

(CRITIQUE,hard) → (OK,hard)

(CRITIQUE,soft) → (OK,soft) (OK,hard)

Dépendance d'hôtes et services

L'objectif est d'augmenter la pertinence des notifications, en supprimant les alertes sans intérêt.

Ce paramétrage permet aussi optimiser la charge du serveur Nagios (et des machines supervisées) en supprimant les contrôles inutiles, et limiter le nombre des alertes.

Cette dépendance consiste à définir les relations de parents/fils entre les hosts/services.

Par défaut, dans Nagios si un hôte est en état DOWN, les services sont toujours surveillés, mais les alertes associées ne sont pas envoyés.

Par exemple : On évite de lancer des tests/ou remonter des notifications inutiles pour un service fils (service apache), alors que le serveur parent (serveur intranet) est indisponible (une erreur JBoss pour un serveur oracle HS ...)

3.3. Réparation pro active (Gestionnaire d'événement)

C'est programme externe déclenché par Nagios, destiné à résoudre un problème avant d'alerter.

Il ne renvoie rien à Nagios (qui continue son ordonnancement pour tester un éventuel retour à la normal).

Les commandes sont exécutées par le gestionnaire d'événement (event-handler), lorsqu'un hôte ou un service est dans un état d'erreur SOFT, rentre dans l'état d'erreur HARD ou revient d'un état SOFT ou HARD. On peut lier un event-handler à une ressource ou à un modèle, auquel cas toutes les ressources concernées peuvent bénéficier du traitement.

Les variables décrivant le résultat d'un test de ressource permettent aux gestionnaires d'évènements de réagir en conséquence. Voici les valeurs que peuvent prendre ces variables :

- \$HOSTSTATE\$ = « UP » ou « DOWN »
- \$HOSTSTATETYPE\$ = « SOFT » ou « HARD » (déterminé par max_check_attempts)
- \$HOSTATTEMPT\$ = un nombre entier positif (nombre d'essais)
- \$SERVICESTATE\$ = « WARNING », « CRITICAL », « UNKNOWN » ou « DEPENDENT »
- \$SERVICESTATETYPE\$ = « SOFT » ou « HARD » (déterminé par max_check_attempts)
- \$SERVICEATTEMPT\$ = un nombre entier positif (nombre d'essais)

Si l'il s'agit de réagir sur un hôte à distance, l'adresse de l'hôte est disponible dans \$HOSTADDRESS\$.

Exemple dans notre projet : relance du service http

Le service apache du serveur web est en défaut, on lance une commande de relance du service, avant de passer l'état du service en anomalie. Il devra être redémarré, si un agent renvoie 3 fois de suite une erreur CRITICAL de type SOFT (juste avant de passer en HARD et de déclencher une notification).

L'utilisation d'un gestionnaire d'évènement se fait par l'option event_handler :

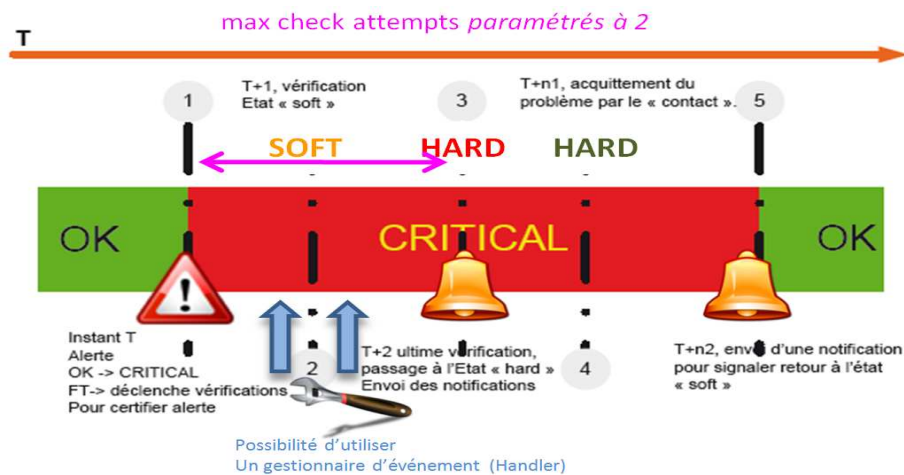
```
define service {
  service_description HTTP
  host_name WWW          [...]
  event_handler_enabled 1
  event_handler handle-httpd-error      [...]
}
```

Appel du gestionnaire d'évènement :

```
define command {
  command_name handle-httpd-error
  command-line $USER1$/reload_httpd.sh $HOSTADDRESS$ $SERVICESTATE$ $SERVICESTATETYPE$ $SERVICEATTEMPTS$
}
```

Le script reload_httpd.sh va n'agir que si les arguments transmis après le \$HOSTADDRESS\$ sont "CRITICAL" "SOFT" "3", se connecter, par ssh sur l'hôte de manière transparente, avec les droits nécessaire pour relancer le service httpd et relancer le service, avant de se déconnecter.

3.4. Exemple de problème.



1. A l'instant T, « hosts » et « services » supervisés changent d'état, ils passent de « ok » à « critical ». Cette étape déclenche un cycle de vérification des incidents.
2. T+1, première vérification. On peut réaliser une commande par gestionnaire d'événement (Handler) pour tenter de corriger le problème
3. T+2, fin du cycle de vérification, on confirme l'incident et bascule « hosts » et « services » à l'état « hard ». Le cycle de notifications peut commencer.
4. T+n1, les notifications sont stoppées après avoir été acquittées par l'administrateur.
5. T+n2 Retour à l'état ok, notification pour retour à la normale.

3.5. Fonctionnement des remontées d'alertes / Escalade

Lorsqu'un problème apparaît sur un serveur ou un service supervisé, Nagios cherche dans ses fichiers de configuration les contacts et les modes d'alerte paramétrés, avant de notifier l'alerte, par le meilleur canal (email en journée/SMS la nuit) et à la bonne personne. Ainsi un expert du service défaillant sera alerté, ciblant les compétences nécessaires et réduisant proportionnellement les délais de remise en service.

En cas de disfonctionnement prolongée, on peut programmer une stratégie d'escalade de l'incident en notifiant l'incident, après une certaine durée d'indisponibilité, à un niveau supérieur ou à une personne plus qualifiée, jusqu'à retour à la normale. (Exemple : alerter le Centre d'Appels, en cas d'indisponibilité prolongée d'un service, pour anticiper la réaction des utilisateurs, qui pourront aussi être alertés par un flux RSS sur l'intranet local).

Exemple :

- au bout de 3 tests défectueux consécutifs sur le service portail internet prévenir l'administrateur, pour dépannage
- au bout de 6 tests défectueux consécutifs sur le service portail internet prévenir le chef de service, pour expertise
- au bout de 8 tests défectueux consécutifs sur le service portail internet prévenir le centre d'appel pour l'accueil des utilisateurs mécontents



Alerte visuelles ou sonore

Lorsqu'un incident survient, une alerte est déclenchée. Elle est visible sur l'interface graphique, avec un code couleur suivant l'importance (Vert : Bon fonctionnement, Orange : Warning, Rouge : Panne). Cette alerte visuelle peut être couplée avec un signal sonore.



Alerte mail

Centreon signale le défaut, avec des informations aussi précises que possibles, par courrier électronique grâce au module mail postfix, à une ou plusieurs adresses de messagerie prédéfinies.



Alerte SMS

Les deux méthodes obligent l'administrateur à rester devant son écran ou à proximité pour réagir au plus vite. Une autre est d'envoyer un message sur le téléphone portable de la personne à prévenir. Un SMS (*Short Message Service*) permet de transmettre un court message textuel de 160 caractères maximum. La solution la moins coûteuse est de connecter un GSM directement sur le serveur avec un câble data USB. Le GSM doit posséder un modem intégré qui répond aux commandes AT. La bibliothèque gsmliib ou gammu permet de piloter un GSM et d'envoyer un SMS aux contacts associés aux services ou hôtes en panne. Il ne faudra pas oublier de surveiller la disponibilité du service d'alerte SMS et l'état des batteries du portable par Nagios (présence /dev/ttyACM0).

Par ailleurs, il existe aussi des applications pour recevoir les alertes ou surtout superviser son système à partir de son téléphone portable Androide (Anetmon, Ngamondroid, Nagdroid) ou iPhone (Nagios4 iPhone, iNag). Ces options ne seront pas développées dans le projet, car elles ne sont pas compatibles avec la politique SSI du Ministère de la Défense.



Alerte RSS

Les flux RSS sont très utilisés pour suivre les flux d'actualité. Constitué d'un simple fichier XML, ce vecteur d'information est facile à mettre en œuvre avec le plugin `rss_multiuser` et la commande de notification d'alerte `notify-by-rss`, offerte par Centreon. Ce flux RSS de supervision peut par exemple être installé sur un portail intranet, pour informer le centre d'appels ou directement les utilisateurs, de la non-disponibilité d'une ressource.

4. Fichiers de configuration Nagios

HOSTS

```
define host{
  host_name      my-host
  alias          my-host.domain.ac.uk
  address        168.192.0.1
  check_command  check-host-alive
  max_check_attempts 10
  check_period   24x7
  notification_interval 120
  notification_period 24x7
  notification_options d,r
  contact_groups unix-admins
  register      1
}
```

SERVICE

```
define service{
  name                ping-service
  service_description PING
  is_volatile         0
  check_period        24x7
  max_check_attempts 4
  normal_check_interval 5
  retry_check_interval 1
  contact_groups      unix-admins
  notification_options w,u,c,r
  notification_interval 960
  notification_period 24x7
  check_command        check_ping!100.0,20%!500.0,60%
  hosts                my-host
  register             1
}
```

COMMANDE POUR UNE VERIFICATION

```
define command{
  command_name check-host-alive
  command_line $USER1$/check_ping -H $HOSTADDRESS$ -w 99,99% -c 100,100% -p 1
}
```

COMMANDE POUR UNE ALERTE

```
define command{
  command_name notify-by-email
  command_line /usr/bin/printf "%b" "***** Nagios *****\nNotification Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional Info:\n\n$SERVICEOUTPUT$" | /bin/mail -s "" $NOTIFICATIONTYPE$ alert - $HOSTALIAS/$SERVICEDESC$ is $SERVICESTATE$ "" $CONTACTEMAIL$
}
```

CONTACT

```
define contact{
  contact_name      chris
  alias             Chris Brew
  service_notification_period 24x7
  host_notification_period 24x7
  service_notification_options w,u,c,r
  host_notification_options d,r
  service_notification_commands notify-by-email
  host_notification_commands host-notify-by-email
  email             someone@somewhere
}
```

GROUPE DE CONTACT

```
define contactgroup{
  contactgroup_name unix-admins
  alias             Unix Administrators
  members           chris
}
```

PERIODE TESTS

```
define timeperiod{
  timeperiod_name 24x7
  alias           24 Hours A Day, 7 Days A Week
  sunday          00:00-24:00
  monday          00:00-24:00
  tuesday         00:00-24:00
  wednesday       00:00-24:00
  thursday        00:00-24:00
  friday          00:00-24:00
  saturday        00:00-24:00
}
```

5. Logiciels de supervision Open source

5.1. SHINKEN

www.shinken-monitoring.org/

Version actuelle : 1.0 (heroic hedgehog) 28/02/2012

Version web démo : <http://demo-shinken.web4all.fr>

Le nom vient des sabres Shinken japonais, les armes les plus coupantes des samouraïs.

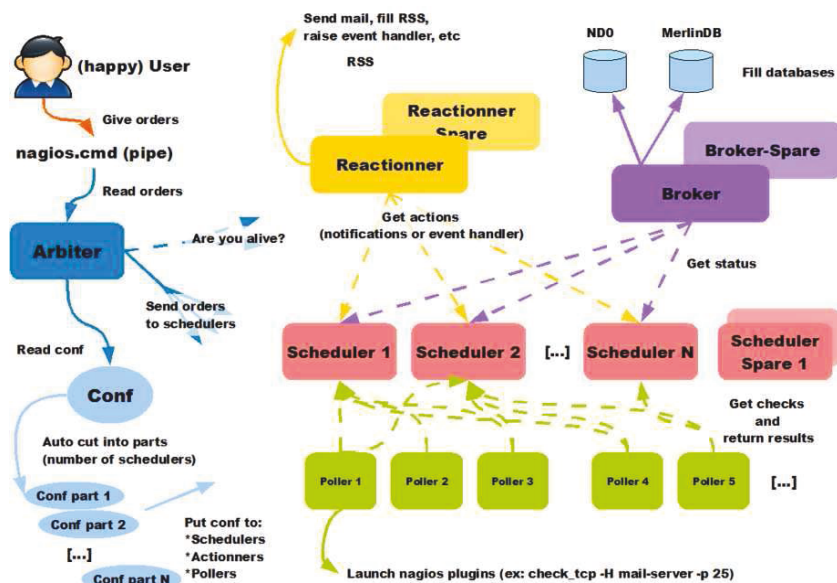
Le projet Shinken consiste en une refonte complète du cœur de Nagios en python, apportant une nouvelle architecture plus souple et plus facile à maintenir que le daemon monolithique actuel. Il est développé par le français Jean Gabes, qui l'a proposé pour l'évolution de Nagios v4, à Ethan Galstad.

Ainsi en se basant sur la configuration actuelle de Nagios, et les plugins disponibles, Shinken est capable de le remplacer, en restant compatible avec les fichiers de configuration. Avec une interface « vision source/impact/criticité », il apporte des fonctionnalités supplémentaires :

Mais il est également possible d'obtenir bien plus qu'un Nagios standard :

- Mise en avant du trio corrélation+règles business+gestion criticité/ Business Rules
- supervision distribuée hautement disponible très facile de manière intégrée
- Escalade de notification plus simple à gérer (pas nombre d'escalade mais en durée)
- Détection et Changement à chaud des relations de dépendances (outil de découverte très modulaire intégré réseau & Vmware)
- Gestion des périodes de maintenance
- 5 fois plus rapide que le Nagios classique
- Fonctionne sous windows et android, compatible avec la base mongoDB

Architecture



Un démon par fonctions :

1. l'administrateur rentre sa configuration sur l'ARBITER, qui va alors découper automatiquement la configuration et la pousser sur chacun des schedulers.
2. Les SCHEDULERS vont planifier les vérifications, analyser les résultats et le suivi des actions associés..
3. Les POLLERS vont lancer les sondes demandées par les ordonnanceurs
4. Le REACTIONNER va déclencher une action (alerte SMS, RSS, script pro-actif, ...) en fonction des résultats des contrôles.
5. Le BROKER va stocker les données collectées selon les modules (NDO, LiveStatus, Merlin, CouchDB, ...) qui ont été choisis.

L'avantage d'une telle configuration est que tous les éléments peuvent avoir un ou plusieurs "spare" (type raid5)

Aujourd'hui l'interface d'utilisation habituelle est Truk, couplé au projet ambitieux « graphite » (avec un daemon « carbon », sa base de données whisper (similaire à RDD) et son interface graphite webapp), pour l'aspect génération de courbes d'évolutions.

Mais avec une nouvelle équipe renforcée, il est annoncé une nouvelle interface webui, avec menu drop-down et de nouveaux dashboards avec widget, dont on voit des captures d'écran, ci-dessous. Ce sera

sans nul, un tournant pour le choix de Shinken, comme outil principal de supervision en lieu et place du vieux Nagios, qui a cessé d'évoluer.

Shinken Hello admin! | Parameters | Log out

Dashboard | Impacts | IT problems | All | System

Overview
Problems: Unhandled 3 | All 240

DOWN: esx2

Alias: esx2
Address: unexistent
Parents: No parents
Members of: linux

Notes: (none)
Importance: Top for business

This element has got an important impact on your business, please fix it or acknowledge it.

Host Status: **DOWN** (since 27m 53s)

Status Information: check_ping: Invalid hostname/address - unexistent

Performance Data
Current Attempt: 1/1 (HARD state)

Last Check Time: was 34s ago
Next Scheduled Active Check: in 4m 27s
Last State Change: Tue Apr 10 09:35:27 2012

Active/passive Checks: **ON**
Notifications: **ON**
Event Handler: **ON**
Flap Detection: **ON**

Try to fix it! | Acknowledge it | Recheck now
Show impact map | Submit Check Result
Send Custom Notification | Schedule Downtime

Impacts

- Apps/Erp is CRITICAL since 2w 4d
- db-server-2/MySQL is CRITICAL since 2w 4d
- db-server-1/MySQL is CRITICAL since 2w 4d
- db-server-2 is UNREACHABLE since 27m 55s
- db-server-1 is UNREACHABLE since 27m 55s
- db-server-2/os_linux_default_check_cron is OK since 2w 4d
- esx2/os_linux_default_check_shell is OK since 2w 4d

Impact sur le SI en 3D

Graphs | Comments | Downtimes

Add Comments | Delete Comments

Author	Comment	Creation	Expiration
webui	Acknowledge from WebUI.	Fri Mar 23 10:35:12 2012	N/A
webui	Acknowledged by WebUI gesture.	Fri Mar 23 10:59:51 2012	N/A

Possibilité d'ajouter des commentaires

Shinken CRITICAL: Apps/Erp since 2w 4d

Impact map of Apps/Erp

2 of 5

Menu drop-down

Shinken Dashboard | Impacts | IT problems | All | System

Erp is CRITICAL since 2w 3d

Corrélation Règles+criticité

WWW is CRITICAL since 2w 3d

Google.com is OK since 1w 6d

Free.fr is OK since 1w 13h

CRITICAL: Apps/Erp

Root problems unacknowledged:

- esx2 is DOWN since 3m 11s

Show dependency tree

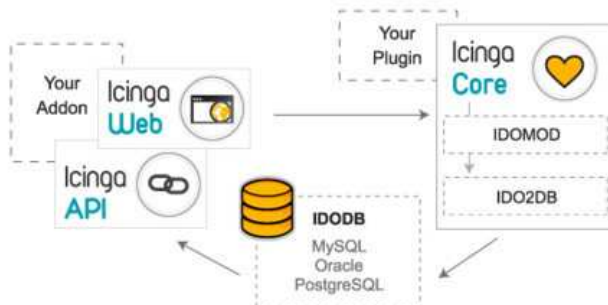
- lvs-server-1/Lvs is OK since 2w 3d 23h 54m 27s
- file-server-2/Nfs is OK since 2w 3d 23h 54m 27s
- file-server-1/Nfs is OK since 2w 3d 23h 54m 27s
- db-server-1/MySQL is CRITICAL since 2w 3d 23h 54m 9s
 - db-server-1 is UNREACHABLE since 3m 13s
 - esx2 is DOWN since 3m 11s

5.2. ICINGA



www.icinga.org
Version actuelle : 1.6.1 / nov 2011

Avec une Communauté allemande active, soutenue par la société Netways (en conflit avec Ethan Galstad, opposé à la création de fork Nagios), le produit Icinga apporte un joli lot de fonctionnalités et pas seulement que sur le Core Nagios. Il propose une compatibilité avec l'IPv6 et un élargissement de l'éventail de compatibilité du Broker avec des bases de données comme MySQL, PostgreSQL et Oracle. Le produit propose 4 modules : Icinga Core (gestion des tâches et contrôle des résultats, sauvegarde dans la base de données par IDODB), Icinga-Web (interface web d'administration), Icinga-Mobile (interface administration pour iPhone, Android, BlackBerry), Icinga-Reporting (système de génération de rapports en se basant sur Jasper Serveur (Tomcat)).
A noter la sortie cet été de la version 1.5, avec la présentation des données Nagios au format JSON, qui permet une sortie vers un logiciel de reporting comme Jasper Reports (Annexe 12.4)



Les sources sont disponibles sous forme de fichier tar, package Redhat, Centos, Suse, Debian, Ubuntu, Gentoo, FreeBSD, OpenSolaris
Une démo est présente sur le web (classic.demo.icinga.org), avec une image VMware ESX téléchargeable.

5.3. ZABBIX



www.zabbix.com
Version actuelle : 1.8.5

Zabbix a été créé par le letton Alexei Vladishev. Soutenu par ZABBIX SIA et développé en C, cette plateforme libre de supervision est très orientée système et s'occupe de métrologie en interne. L'interface web est quant à elle, développée en PHP et en JavaScript.
Disposant d'un outil de découverte des équipements, il se place en concurrent direct de Nagios, avec comme avantage l'intégration en natif de RRDTool pour les graphiques dynamiques, une conception plus moderne et des fonctionnalités avancées. Le « serveur ZABBIX » peut être décomposé en 3 parties séparées : Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Avec une interface agréable, avec de nombreux graphes, Zabbix n'offre néanmoins pas comme Nagios une gestion souple des dépendances, importante dans les grands environnements.

Les sources sont disponibles pour Redhat, CentOS, Suse, Debian, Ubuntu, Gentoo
Il y a possibilité de tester le produit avec un CD BOOT, une image VMware ou XEN

5.4. OPENNMS



www.opennms.org
Version actuelle : 1.8.18 du 16-05-2011

OpenNMS est la première plate-forme applicative de gestion de réseau de niveau entreprise développée par Tarus Balog en 1999, dans le cadre d'un modèle open source.
OpenNMS couvre aussi bien la supervision (réception des alarmes et contrôle actif des équipements) que la gestion des performances (suivi des indicateurs de performance dans le temps, positionnement de seuils et envoi d'alerte en cas de dépassement). Néanmoins sa configuration est lourde à gérer et n'offre pas la gestion des dépendances entre hôtes et services.

Les sources sont disponibles pour Windows, solaris, Mac OS, linux (rpm, deb)
Le produit peut être testé avec une démo sur internet (<http://demo.opennms.org>)

6. Distribution linux de supervision

6.1. CES (Centreon Enterprise Server)



Une distribution linux, proposée par Merethis (développeur de Centreon) permet rapidement et facilement d'installer Centreon et ses dépendances. CES permet de gérer au choix un serveur de supervision complet, un système distribué avec serveur central et satellites. Au lancement de la machine, il suffit de saisir central ou poller pour installer un serveur central ou un serveur satellite. Livrés avec plusieurs versions, la version libre (version standard) propose : Centreon, Nagios, Nagios Plugin, NdoUtils, NRPE, NSCA, Une sélection de plugins additionnels. Les autres versions " Essentials "," Advanced " " Advanced Plus offrent des sondes supplémentaires et outils métiers (Centreon MAP pour la cartographie, Centreon BI pour création de rapport, Centreon BAM (Gestion par activité métier).

Des extensions Core (gratuites) peuvent être installées comme Centreon Broker (remplace NDO), Centreon CLAPI (piloter Centreon en ligne de commande), Centreon E2S (contrôle journaux événements Windows), Centreon Syslog (visualisation des logs dans Centreon), Centreon NTOP

Méthode installation	CD ISO v2.0 09-02-2011
Site	www.centreon.com
Développeur	MERETHIS
OS	CenTOS 5.5

6.2. FAN (Fully Automated Nagios)



C'est une distribution sous CentOS (version libre de Redhat Entreprise), permettant une installation rapide de Nagios, Centreon, Nagvis et Nareto. Son auteur était Cédric Temple (créateur de Centreon), qui a laissé la main, après son intégration dans l'équipe de la société Merethis, tout en restant dans ce projet.

Méthode installation	CD installation FAN (Fully Automated Nagios) v2.1 – 14-04-2011
Site	fannagioscd.sourceforge.net
Développeurs	Communauté française : Olivier LI-KIANG-CHEONG (président monoring.fr) et Cédric TEMPLE (core développeur Centreon)
OS	CenTOS 5.5
Produits Complémentaires	CENTREON 2.0.2 : une surcouche administration Nagios NAGVIS 1.4.1 un module de graphe NDOutils 1.4 : outils et base de données NDO pour stockage des données de performance NARETO1.1.6 : outils de reporting développé par Cédric Temple , qui a arrêté son évolution RSYSLOG : gestion des logs
Informations complémentaires	Possibilité de tester le produit Démo sur le web http://fan-demo.gezen.fr/

6.3. EON (Eyes Of Network)



Cette distribution propose des outils complets supplémentaires correspondant aux processus ITIL avec la gestion des évènements, de la disponibilité, des problèmes, de la capacité et la gestion de parc. Ces logiciels pourront être proposés comme une évolution de la plateforme installée, pour permettre des fonctionnalités dans le domaine du monitoring et du reporting. L'interface LILAC n'apporte pas un plus à l'interface native de Nagios, mais cette distribution permet de tester les outils intégrables à Nagios comme Cacti, NagiosBP, Weathermap, Nagvis et des améliorations comme MK Livestatus.

Méthode installation	CD installation EON (Eyes Of Network) V2.2 – Novembre 2010
Site	www.eyesofnetwork.com
Développeur	Société APX
OS	CenTOS 5.5

Produits Complémentaires	NAGVIS 1.5.5: cartographie personnalisée de la disponibilité, CACTI 0.87g: gestion des performances, Cacti Syslog 1.05 : gestion des logs NAGIOSBP 0.9.6 : gestion de la criticité des applications, NTOPI 4.0.3: métrologie réseau WEATHERMAP 0.97 : cartographie de la bande passante, BACKUP MANAGER 2.0: Outil de sauvegarde de la solution, EONWEB 2.2: Interface Web unifiée de la solution, MK LIVESTATUS 1.1.8 : remplace NDOutils en plus efficace LILAC 2.0 : interface web d'administration GLPI 0.78: Gestion de parc. GED (Generic Event Dispatcher) : gestion multi sites et sécurisée des évènements,
--------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6.4. OMD (Open Monitoring Distribution)



Soutenue par une forte communauté allemande, cette distribution offre des produits nouveaux comme Shinken, Check_Mk avec MK-livestatus.

Méthode installation	Packet de OMD (Open Monitoring Distribution) V0.48– 22/05/2011
Site	http://omdistro.org/
Développeur	Communauté: Mathias Kettner (Créateur du check_MK et MK_LiveStatus), oerg Linge (Créateur de PNP4Nagios), Sven Nierlein (Créateur de Thruk), Matthias Flacke et Michael Friedrich (Equipe Icinga)
OS	Debian, Redhat ou Suse
Produits Complémentaires	NAGVIS 1.5.9 : cartographie personnalisée de la disponibilité, PNP4NAGIOS 0.6.13: graphe RRDTOOL 1.4.5: gestion base de données résultat (remplace MRTG) CHECK MK 1.1.10p3: agent optimisé remplace agent nrpe, et récupère toutes les informations de l'hôte avant d'extraire les données souhaitée MK LIVESTATUS 1.1.10 : remplace NDOutils en plus efficace THRUK : Interface administration Agent : check_nrpe , ncsa, check_logfiles , check_oracle_health WEBINJECT1.6.7 : test poussé serveur http Multisite 1.1.10p3

6.5. CatiEZ



C'est une Distribution assez particulière, car axée sur Cacti et les outils de métrologie.

Méthode installation	CD BOOT ISO V0.7– 17/05/2011
Site	http://cactiez.cactiusers.org/
Développeur	Jimmy Conner du cacti group
OS	CentOS 5
Produits Complémentaires	Cacti v0.8.7c : outils de métrologie SNMP Plugin Architecture Spine poller (poller de requête amélioré ex cactid) Netflow Collection : mesure flux réseau Syslog Collection : lire les messages syslog sur cacti Ntop : plugin pour les statistiques réseaux Thresholding (thold) : gestion des alertes Weathermaps : outils de cartographie des flux Auo-Discovery WMI Queries Router Config backup Nagios

7. Broker (Ordonnanceur des données dans les SGBD)

7.1. NDOutils

NDOutils est un plugin standard de Nagios (aussi utilisé dans Nagios XI Entreprise) qui permet d'enregistrer les informations collectées, dans une base de données.

Cela a 2 incidences :

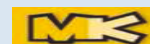
- La possibilité de mettre en place un mode dit « distribué », qui permet d'utiliser plusieurs serveurs de collecte et un de centralisation. Ainsi cela permet de « répartir » les charges de ressources nécessaires sur différents serveurs. Il suffit ensuite au serveur central de les regrouper et les traiter, il n'a plus qu'à les collecter. (voir les architectures distribuées présentées au paragraphe 10.3.3 du mémoire)
- Amélioration notable des performances. En effet, il est plus rapide de rechercher des informations dans une base de données qui est structurée, plutôt que dans un fichier à plat, par défaut dans Nagios) qu'il faut parcourir entièrement à chaque utilisation.

NDO est composé de deux modules NDOMOD et NDO2DB :

- NDOMOD doit être lancé sur le serveur Nagios. Il permet de récupérer les informations collectées par Nagios et de les transmettre via un socket TCP à NDO2DB. Ce module est chargé automatiquement par Nagios.
- NDO2DB est un démon, qui écrit les données reçues dans une base de données. Il nécessite un script d'init, pour démarrer.

Version 1.4b9 - 27octobre2009

7.2. MK_LIVESTATUS



http://mathias-kettner.de/checkmk_livestatus.html

MK_Livestatus est un module de courrage d'événements, pour Nagios, qui permet d'accéder aux données nagios, sans middleware de type ndo ou merlin. L'accès aux données est immédiat et sans IO disque. Il est assez facile à mettre à disposition via un socket TCP à la place d'un socket Unix. Il utilise un langage de requête LQL (proche de SQL)

Version 1.1.0

Possibilité de tester une démo avec FAN et truk sur internet <http://fan-demo.gezen.fr/>

7.3. Centreon Broker



www.centreon.com/fr/Centreon-Extensions/presentation-de-centreon-broker.html

Avec Centreon Engine (alternative au moteur Nagios en lui restant compatible) et Centreon Broker (concurrent de NDO), les développeurs de Merethis veulent démontrer à la communauté Nagios que Nagios peut être amélioré grâce à la réécriture partielle du code et à l'intégration de correctifs correspondants aux nouveaux besoins des utilisateurs. Ainsi, ce nouveau broker a pour but d'offrir un nouveau moyen d'injecter les événements de Nagios en base de données, à la place de NDO (qui n'a pas évolué comme Nagios). En se voulant plus performant, le couple Centreon/Centreon Broker de Merethis est comparé au produit concurrent d'OP5 Ninja/Merlin. Les deux sociétés se sont mises néanmoins d'accord pour utiliser un modèle de base commun.

Version 2.02 – 7 mars 2012

7.4. Mod_gearman



gearman.org

Ce projet prometteur propose une autre alternative à NDO, avec son module NEB (Nagios Event Broker) déléguant le contrôle des checks à un worker.

Version 1.2.6 15 mars 2012

8. Autres outils à suivre

8.1. Agent MK Check

http://mathias-kettner.de/check_mk.html

Disponible sous Windows et Linux, MK Check remplace les agents standards (nscs ou nrpe). C'est un système de check hybrid actif/passif, qui permet de récupérer plusieurs tests en une seule requête et donc un gain de performance. Basé sur livestatus, il propose aussi une nouvelle console de supervision, complètement paramétrable, avec des filtres complexes.

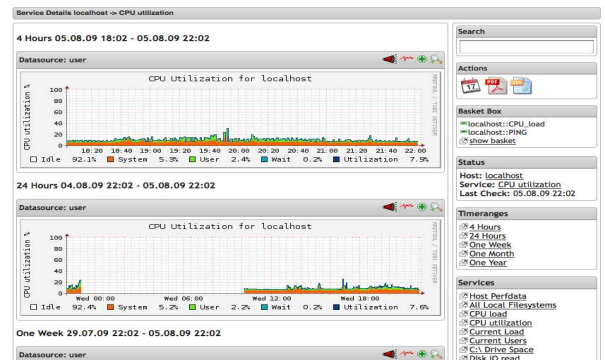


Source : www.monitoring-fr.org

8.2 Outils de métrologie PNP4NAGIOS

www.pnp4nagios.org

PNP est l'acronyme de 'PNP is NOT Perfparse'. Cet add-on permet de récupérer le champ performance des résultats de Nagios et enregistrer les résultats dans une base rrdtool, pour réaliser des graphes. Concurrent de Cacti (sans offrir pour l'instant le vaste choix des templates de la communauté, il offre néanmoins l'avantage d'utiliser les résultats de Nagios et d'éviter de faire des doubles requêtes (Nagios et Cacti). Il est l'outil conseillé à interfacier à Shinken, pour la métrologie et Nagvis pour la cartographie)



9. Gestion Syslog dédiée Centreon

<http://www.centreon.com/fr/Centreon-Extensions/core-extensions.html>

Centreon E2S

Centreon E2S, Windows EventLog vers Syslog

Centreon E2S parcourt à intervalle régulier les journaux d'évènements Microsoft Windows et contrôle ces derniers au travers de règles définies par l'utilisateur.

[Plus d'informations >>](#)

Compatibilité : Centreon 2.x -- Type : CGNU GPL 2 -- Catégorie : Extension Centreon -- Auteur : MERETHIS

Centreon Syslog

Centreon Syslog, surveillance d'évènements syslog

Centreon Syslog permet de visualiser dans Centreon les évènements remontés dans une base de données.

[Plus d'informations >>](#)

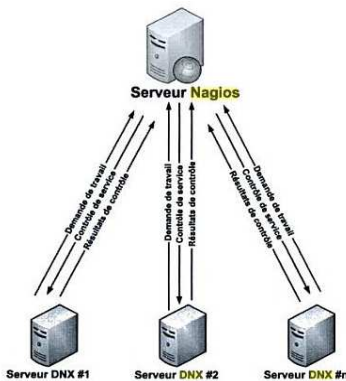
Compatibilité : Centreon 2.x -- Type : CGNU GPL 2 -- Catégorie : Extension Centreon -- Auteur : MERETHIS

10. Architecture distribuée

10.1. DNX

Distributed Nagios eXecutor
Enterprise Scalability for Nagios

<http://dnx.sourceforge.net>



DNX est un Addon pour Nagios, qui implémente la supervision distribuée, avec une configuration maître/esclave. Le serveur distribue dynamiquement et automatiquement les contrôles à effectuer à un groupe d'esclaves. La seule grande modification à faire sur le serveur Nagios est d'ajouter la directive de configuration et ajouter le module DNX dans le fichier nagios.cfg.

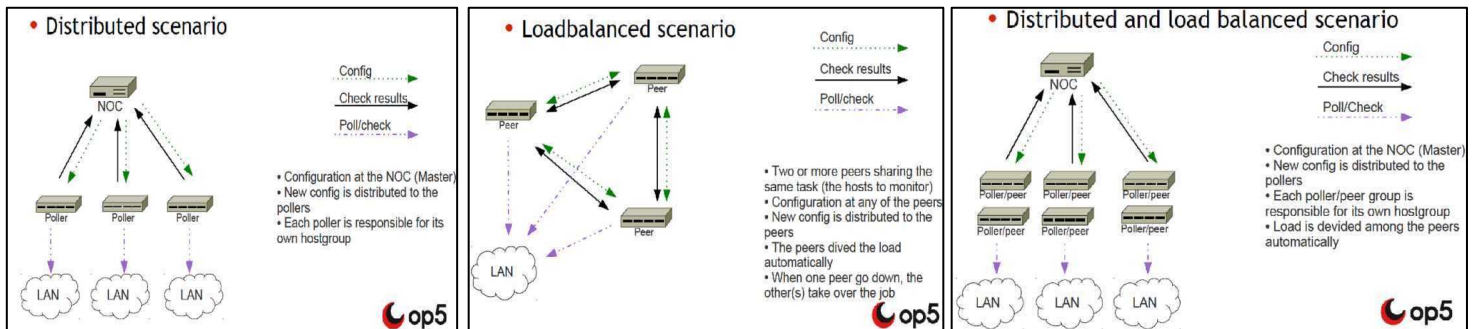
DNX ouvre des ports de communication supplémentaires : Dispatcher UDP 12480 (sur le client pour récupérer la commande à lancer) et Collector UDP 12481 (sur Nagios pour recevoir les résultats de la commande).

10.2. MERLIN



www.op5.org/community/plugin-inventory/op5-projects/merlin

Couplé à Ninja comme interface web, Merlin est un module Nagios (partie broker) spécialement développé spécialement pour les environnements distribués et loadbalancing.



Source : présentation de Peter Andersson (OP5) Munich 2010

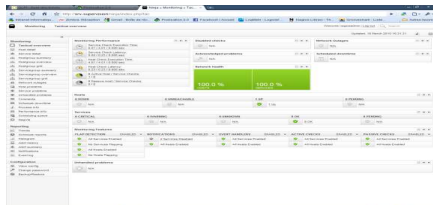
11. Interface graphique

11.1. NINGA



www.op5.org/community/plugin-inventory/op5-projects/ninja

version actuelle 1.1.0



Piloté par OP5, le projet Ninja est une interface graphique flexible pour Nagios. Il est surtout utilisé avec le projet Merlin de la même société, pour offrir une solution complète d'administration.

11.2. TRUK

www.thruk.org Version actuelle 1.0.9



Truk est une interface ultra rapide pour Nagios en perl, utilisant livestatus, pour l'accès aux données Nagios. Elle apporte des fonctionnalités supplémentaires : navigation par page, thème, recherche multicritère. La Map réseau disparaît, mais l'addon Nagvis (compatible livestatus) peut parfaitement réaliser ce travail. Il est intégré en standard dans shinken

12. Reporting (génération de rapports)

12.1. Centreon

www.centreon.com



En plus de proposer la solution libre Centreon, Cette entreprise propose aujourd'hui des services autour de ce produit, de la supervision.

Des extensions payantes de la suite logicielle Centreon sont proposées :

Centreon Business Intelligence (BI) : Moteur de reporting qui donne la possibilité de générer des rapports personnalisés automatiques sur les disponibilités et les performances de votre Système d'Information (SI).
Version 1.3.6 du 7 juin 2011 - Coût : 3990€/an - maintenance 1an : 990€

Centreon Business Activity Monitoring (BAM) : Destiné aux responsables de production, qui souhaitent une visualisation synthétique des activités métiers (Business Activity)

Version 2.3.7 du 7 juin 2011 - Coût : 3190€/an - maintenance 1an : 650€

Centreon Map (module de cartographie avec une navigation arborescence).

Version 3.1.3 du 7 juin 2011- Coût : 2000€/an - maintenance 1an : 1000€

Cette société a aussi lancé Centreon Engine, un fork de Nagios, se basant sur le moteur central de Nagios V3.2.X. Le but de la démarche est de continuer à améliorer les performances de Nagios Core (en conservant une compatibilité avec Nagios, Icinga et Shinken) et remotiver la communauté Nagios, qui voit ses demandes d'évolution, rejetées par Nagios Entreprise.

12.2. Nagios Business Process Add-on

<http://bp-addon.monitoringexchange.org/>



NBPA apporte à Nagios une dimension orientée application/métier.... Il permet d'agréger des résultats de contrôles techniques à l'aide d'opérateurs logiques (et, ou ...) afin de les présenter en vues Métier.

Version 0.9.6 03.6.2011

Demo internet: <http://fan-demo.gezen.fr/nagiosbp/cgi-bin/nagios-bp.cgi>

12.3. Plugins Cacti

Nectar : <http://docs.cacti.net/plugin:nectar> Version actuelle : V0.3 30-10-2010

Ce plugin propose d'envoyer un graphe (au format jpeg, png) de manière périodique à une adresse de messagerie. Cette méthode permet par exemple d'avoir tous les matins un état du système, pour contrôler sa disponibilité ou le respect du contrat de service de l'équipe d'exploitation.

Report Title**	Id	Interval	Count	Offset	Next Run	Last Run	From	To	Type	Enabled
New Report	1	Day(s)	1	0	2009/12/15 20:35:00	never	report@team-scheck.de	Reinhard.Scheck@team-scheck.de	Inline PNG Image	Disabled

image extraite de <http://docs.cacti.net/plugin:nectar>

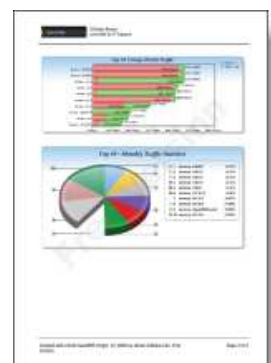
Aggregate <http://docs.cacti.net/plugin:aggregate> Version actuelle : V1.0 bêta (malheureusement encore à l'état bêta)

Ce plugin permet de rassembler sur un même graphe, plusieurs graphes existants et faciliter ainsi une analyse des mesures réalisées

CereusReporting : <http://www.network-outsourcing.de> Version actuelle : v 1.76.31

Pour information, car en version non open source, CereusReporting offre la possibilité de générer un rapport en pdf d'une page d'arborescence de graphe.

Ce plugin montre l'intérêt que portent les sociétés commerciales, à Cacti et plus généralement au monde de la supervision open source, en proposant des add-ons, dans des domaines comme le reporting, où il y a un manque malgré le besoin réel des utilisateurs.



12.4. JasperREPORTS



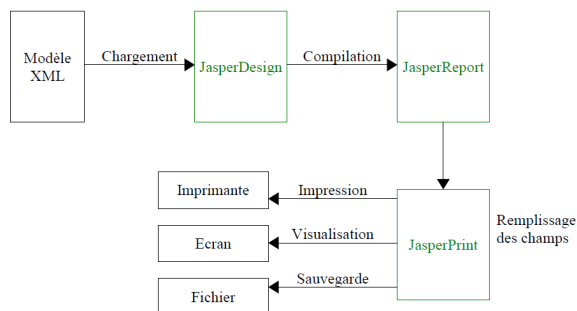
<http://jasperforge.org/projects/jasperreports> Version actuelle : 1.1.0

La librairie JasperReports a été conçue en 2001 par Teodor Danciu, qui a également participé à de nombreux autres projets Open Source (Hibernate, framework Avalon ...). Elle permet de créer des rapports à partir de fichiers XML. Le résultat peut être affiché à l'écran, imprimé ou stocké dans des fichiers au format PDF, HTML, XLS, CSV ou XML. C'est aussi le processus retenu pour la gestion des rapports dans SISMU.

La création de rapports avec JasperReports se déroule généralement en 4 étapes :

- l'obtention d'un fichier modèle XML (à l'aide d'éditeurs graphiques comme iReport ou OpenReports Designer)
- la construction du rapport à partir du modèle
- le remplissage des différents champs du rapport avec les données en provenance de diverses sources (bases de données, classes Java ...).
- l'exportation du résultat dans plusieurs formats possibles (PDF, HTML ...).

Le fonctionnement de JasperReports est relativement simple. En effet, tous les concepts tournent autour du langage Java. Une fois le modèle XML (JasperDesign) compilé, il est chargé dans un objet Java (JasperReport) qui peut lui-même être sérialisé et stocké dans un fichier (avec l'extension .jasper). Cet objet sérialisé est alors utilisé lorsque l'application désire compléter le rapport avec des données. En fait, la définition du rapport nécessite la compilation de toutes les expressions Java déclarées dans le modèle XML. Le résultat obtenu après le processus de remplissage des champs est un nouvel objet Java (JasperPrint) qui représente le document final. Celui-ci peut être stocké sur disque pour un usage ultérieur (sous forme sérialisée et avec l'extension .jrprint), directement imprimé ou encore transformé dans un format lisible (PDF, HTML, ...).



12.5. BIRT



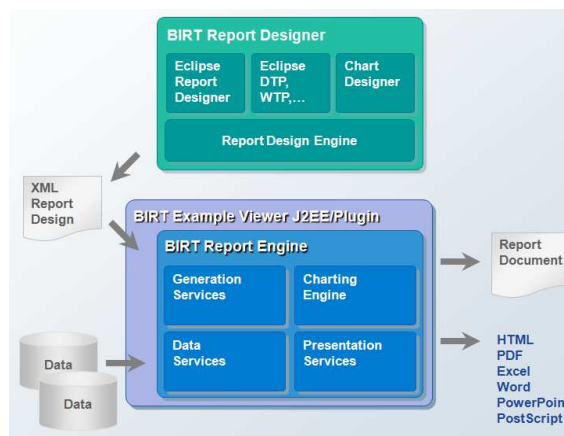
www.eclipse.org/birt/phenix/

Version actuelle : 3.7

BIRT (Business Intelligence and Reporting Tools), logiciel open source édité par Actuate, est un projet de la communauté Eclipse comprenant un générateur de graphiques, un générateur d'états et un environnement de conception.

Comme tout outil de restitution classique (le plus connu étant probablement BO), BIRT permet de générer des états dans de nombreux formats : HTML, PDF, XLS, DOC ou PPT. Cet outil s'intègre sous forme de plug-in dans l'outil de développement Eclipse mais peut être également utilisé comme une application autonome.

Il a été retenu par Merethis pour le développement de son produit commercial Centreon BI.



12.6. NaReTo

www.nareto.org



NaReTo (*Nagios Reporting Tool*) était un produit développé par Cédric Temple, proposant une interface de haut niveau nagios, composée de trois modules : suivi Temps-Réel, suivi des Alarmes, et reporting. Aujourd'hui, il n'est plus soutenu par son auteur. Mais il est cité dans notre étude, car sa reprise serait annoncée par une nouvelle équipe de développeurs et il répond actuellement à un véritable besoin de « Reporting Métier » pour les outils de supervision open source émergents (Shinken, Icinga...).

14. Hypervision : projet Canopsis



<http://www.canopsis.org> Version actuelle : release 20.12.03

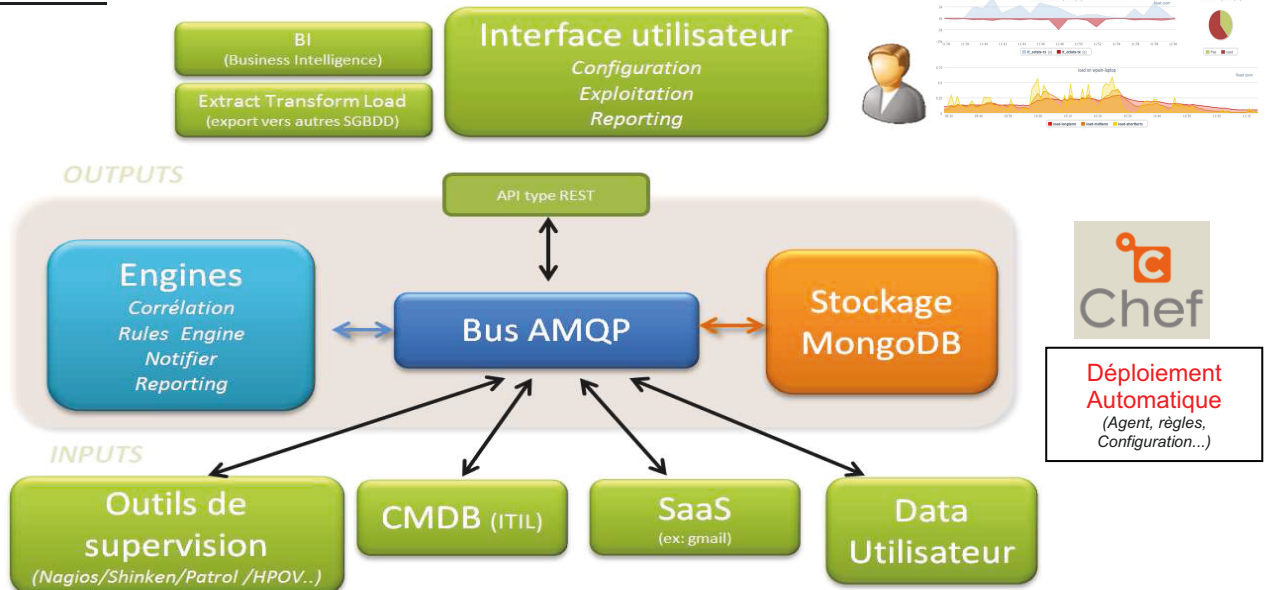
CANOPSIS est une solution d'hypervision open source, livrée sous licence AGPL 3, proposée par la SSL Capensis. Canopsis est un produit encore jeune en phase de développement et intéresse déjà de nombreux industriels (Auchan, Norauto, la poste, SNCF...). Ainsi le groupe EIFFAGE a financé la partie reporting du projet pour la gestion de son nouveau ERP. Sa mise en œuvre donnera lieu avant la rentrée 2012 à un package stable de Canopsis.

Le chef de projet de ce logiciel est Olivier Jan, une des célébrités de la supervision open source en France. Il est partie du constat du manque des outils de supervision actuels uniquement orientés techniques, avec une gestion hôtes/services obsolète. Avec les évolutions technologiques (virtualisation, Cloud, clustering...), le contrôle des états et la vision à plat ne reflètent plus la réalité. Les vues ne permettent pas de remonter rapidement à la source d'un dysfonctionnement et de calculer ses impacts sur la globalité de la production informatique. Par ailleurs les DSI et les managers des entreprises demandent aujourd'hui une gestion SI orientée business, centrée sur les objectifs de services (ITIL, Cobit...) et du ressenti des utilisateurs.

Objectifs

- Fédérer, agréer, compléter, consolider les solutions de supervision
- Réconcilier la vision technique et vision métier des SI
- Approche globale vers les détails (Top/Down)
- Ouvrir la supervision à des nouveaux publics.

Fonctionnement



L'architecture de canopsis est basée sur une architecture multi-tiers, dont l'élément central est un bus de messages AMQP (Advanced Message Queuing Protocol). En back end, la base de données utilisée est de type Nosql et permet de stocker directement les données, au format JSON. De nombreux connecteurs existent pour Nagios/Icinga/Shinken, Syslog, SNMP traps, CMDB (inventory), ...

Dans cette architecture, Nagios revient à sa place initiale : contrôle de protocole, contrôle de seuil et les notifications. On se base sur collectd pour la métrologie. Il y a certes moins de plugin, mais ils sont mieux écrits et plus efficaces, avec des intervalles de contrôle plus restreints (<10s) grâce au protocole UDP.

Pour le suivi des logs, point faible de Nagios, Canopsis a choisi les logiciels logstash et Graylog2. Nagvis est intégré comme solution de cartographie.

Le point fort du produit est son interface graphique (95% du développement global du projet) avec des Dashboards personnalisables, sous forme de widget. Le reporting (en temps différé) consiste à définir des limites bornées à la surveillance et à planifier à la demande, des rapports aux formats pdf, html, cvs, odt. L'automatisation des configurations (inventaire, déploiement des agents, configuration Nagios, Graylog2, collecte ...) est assurée par le produit libre Chef, qui permet de s'adapter rapidement aux évolutions rapides du SI.

15. Communauté France : Monitoring.fr.org

15.1. Historique

- 2007 : Olivier JAN publie ses notes de recherche autour de Nagios et la supervision open source
- 2007 : premier contact avec Ethan Galstad et création du blog
- 2008 : deuxième contact avec Ethan et première idée de structuration d'une communauté.
- 2009 : Romuald Fronteau rejoint Olivier pour la mise en place des forums de support Nagios
- 2010 : Nagios-fr devient Monitoring-fr
- 2010 : Jean GABES rejoint l'équipe Monitoring-fr
- 2010 : Olivier LI KIANG CHEONG rejoint l'équipe Monitoring-fr
- 2010 : Création de l'association Communauté Francophone de la Supervision Libre (CFSL) www.cfsl-asso.org

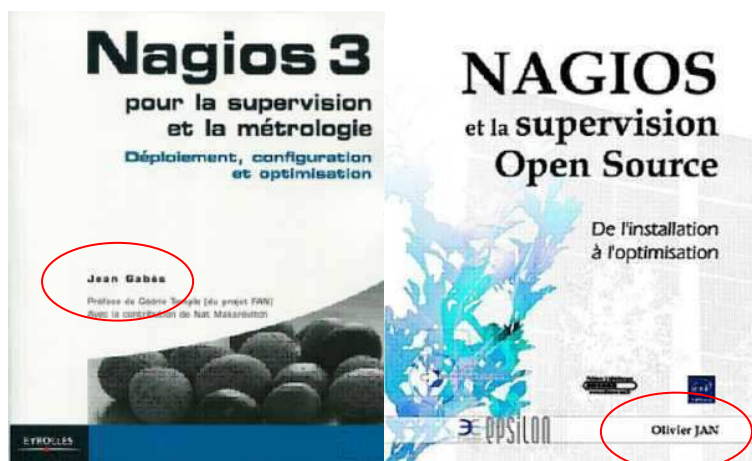
15.2. Membres actifs



15.3. Manifestation Nagios : Conférences, salons, rencontres



15.4. Livres de référence en français



Remarques

Soutien		Remarques
Documentations disponibles		
Hot line utilisateur/technique		
Soutien	<input type="checkbox"/> Equipe TME <input type="checkbox"/> CeTIMA <input type="checkbox"/> Autre :	

Gestion de configuration		Remarques
Version logicielle		

Supervision (contrôles souhaités)		
Mesure	Seuil alerte	Alerte
<i>Partition C</i>	<i><80%</i>	<i>Affichage console</i>
<i>Service http</i>	<i>Non présent</i>	<i>Email TME et responsable applicatif</i>

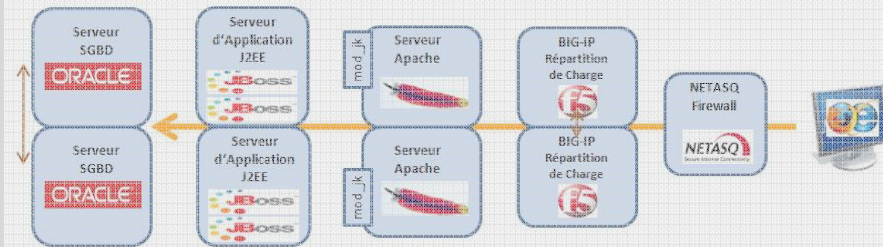
Projet(s) connexe(s)	Remarques

Risque(s) particulier(s) à savoir, avant le début de l'étude ou pour la mise en œuvre sur les plateformes opérationnelles	Remarques

Planning		Remarques
Date souhaitée de mise en place de la supervision (sept/octobre) ou date à éviter		(date à valider par MOA)

Architecture / Flux applicatif
Schéma d'architecture et explication

Exemple : architecture n-tier apache /JBoss/Oracle avec redondance et loadbalancing



17. Questionnaire pour rédaction CdCF

document projet [QUES-SUPERV-NP]

0. Contexte et projet

- ▶ Dans quel contexte le projet est-il envisagé ?
 - Premier équipement d'une solution de supervision
 - Extension de la supervision à un périmètre plus large
 - Remplacement de la solution de supervision existante, à périmètre équivalent
 - ▶ Le projet concerne-t-il la supervision pour le compte d'une entreprise cliente (contexte d'infogérance) ?
 - Non
 - Oui
 - ▶ Quelles sont les grandes familles d'équipements informatiques à superviser (plusieurs réponses possibles) ?
 - Serveurs physiques
 - Serveurs virtualisés
 - Applications (y compris les middlewares tels que SGBD ou serveur HTTP, applications métier).
 - Applications virtualisées. Détailler :
 - Réseaux (bande passante, QOS, routeurs, firewalls...).
 - Appliances particulières (boîtiers réseau, d'encryptage, de firewall, applicatifs...).
 - Périphériques. Détailler les types et nombre :
 - Autre(s), précisez :
 - ▶ Décrivez la répartition géographique des éléments à superviser, au moyen d'une cartographie faisant apparaître chaque site concerné avec le nombre de ses serveurs (par système d'exploitation), les types de liaisons réseau (LAN, WAN, VPN...) et, le cas échéant, les principales applications à superviser :
 - Dans quelle proportion les serveurs à superviser sont-ils virtualisés ?
 - ▶ Qu'ils soient virtualisés ou non, quels sont les rôles des serveurs à superviser (plusieurs réponses possibles) ?
 - Serveurs hébergeant des machines virtuelles
 - Contrôleur de domaine
 - Serveur DNS
 - Serveur DHCP
 - Serveur HTTP interne à l'entreprise
 - Serveur HTTP hébergeant des sites Internet
 - Serveur SMTP ou Serveurs Exchange
 - Serveur FTP
 - Annuaire LDAP ou ActiveDirectory
 - Messagerie
 - Stockage
 - Impression
 - Proxy et/ou firewall
 - SGBD
 - Sauvegarde
 - Serveur applicatif Java et middleware Java
 - Serveur applicatif .Net
 - Fermes de serveurs Citrix
 - Autre(s), précisez :
 - ▶ Qu'il s'agisse d'un besoin interne ou d'un contrat d'infogérance, listez les contraintes les plus sévères en matière d'engagement de service et de temps de rétablissement (par exemple, « Remise en route des serveurs contrôleurs de domaine en deux heures maximum ») :
- Rédaction réservée**
- ▶ Quel est le nombre approximatif des personnes utilisatrices des éléments à superviser ? **3 personnes TME pour la supervision, une dizaine pour le SLA**
 - ▶ Combien d'administrateurs système sont concernés par la solution ? **3 personnes TME**

1. Profil général de la technologie de supervision

- ▶ Dans quel cadre s'inscrit la technologie proposée :
 - Logiciel spécifique exclusivement dédié à la supervision de :
 - Serveurs physiques
 - Serveurs virtualisés / hyperviseurs
 - Machines virtuelles
 - Serveurs de messagerie
 - Serveurs SGBD
 - Serveurs d'application et technologies web
 - Applications métier
 - Réseaux
 - Périphériques
 - Autre(s) :
 - Module dédié à la supervision avec couverture plus large.
- ▶ Quelle est la capacité de supervision de la solution ?
 - Moins de 30 serveurs
 - 30 à 300 serveurs
 - 300 serveurs à 1000 serveurs
 - Plus de 1000 serveurs

- ▶ Quel est le modèle d'édition de la solution (plusieurs réponses possibles) ?
 - Proiciel "commercial"
 - Open source commercialisé et maintenu par l'éditeur
 - Open source distribué librement et maintenu par la communauté
 - Application SaaS ou ASP
 - Autre(s), précisez :
- ▶ La solution est-elle certifiée par d'autres fabricants de matériels ou de logiciels informatiques ?
 - Non
 - Oui
- Si Oui, lesquels ?
- ▶ Décrivez l'architecture logique de la solution (éléments à déployer, composants/plugin-ins, agents actifs ou passifs ...) : **Voir cahier des charges**
- ▶ La solution permet-elle d'importer et d'exploiter via le protocole SNMP les bases de données MIB (Management Information Base) qui décrivent les équipements présents sur le réseau ?
 - Non
 - Oui (**partiellement, sondage port SNMP ouvert sur les différents serveurs à réaliser**)
- ▶ Comment la solution de supervision peut-elle être configurée (plusieurs réponses possibles) ?
 - Au moyen de scripts
 - Construction graphique et écrans spécifiques de configuration
 - Par réutilisation de modèles de configuration d'hôtes
 - Autre(s), précisez :
- ▶ Quels sont les pré requis en matière de droits système pour une pleine exploitation de la solution ?
 - Avoir les droits sur les serveurs supervisés pour installation des agents éventuels**
- ▶ La configuration permet-elle de déclarer les plages horaires d'arrêts programmés ?
 - Non
 - Oui
- ▶ La solution permet-elle de définir des SLA (Service Level Agreement), c'est-à-dire des ensembles de métriques contractuelles, et de les superviser ?
 - Non
 - Oui, à quel niveau(x) est-il possible de définir ces SLA ?
 - Serveur
 - Réseau
 - SGBD
 - Web
 - Serveur d'applications
 - Applications
 - SLA métier
 - Ressenti utilisateurs (navigation...)
 - Autre(s) :

2. Supervision de serveurs physiques et virtuels

2.1. Serveurs physiques et Systèmes d'exploitation

- ▶ Quels sont les systèmes d'exploitation supervisés par la solution (plusieurs réponses possibles).
Précisez les versions compatibles dans chaque cas ?
 - Windows
 - Unix (précisez les distributions) : Redhat Entreprise
 - Linux (précisez les distributions) :
 - IBM AIX
 - IBM i Operating System (AS/400)
 - HP UX
 - Sun Solaris
 - OpenVMS
 - Autre(s), précisez :
- ▶ Quelles métriques la solution permet-elle de surveiller sur un serveur (plusieurs réponses possibles) ?
 - Activité des processeurs
 - Consommation instantanée de mémoire vive
 - Pics de consommation de mémoire vive
 - Occupation de l'espace de stockage
 - Présence d'agents, de services ou de processus définis
 - Présence du serveur sur le réseau (ping ethernet)
 - Flux entrants et sortants liés aux cartes réseau
 - Durée d'arrêt
 - Taux de disponibilité
 - Température
 - Autre(s), précisez :

2.2 Spécificités à la supervision de serveurs lames ("Blade")

- ▶ La solution identifie-t-elle les serveurs lames en tant que tels ?
 - Non
 - Oui

2.3 Supervision "native" de serveurs virtualisés et machines virtuelles

- ▶ La solution permet-elle de superviser des serveurs virtualisés ?
 - Non
 - Oui
- ▶ La solution permet-elle de superviser au niveau hyperviseur de virtualisation ?
 - Non
 - Oui
- ▶ Quels sont les prérequis à observer pour pouvoir superviser les serveurs virtualisés ? **Rédaction réservée**
- ▶ La solution permet-elle de découvrir et superviser nativement l'arborescence Machine Physique / Hyperviseur / Machines Virtuelles / Système d'exploitation / Processus (SGBD, Serveur d'application, Process réseau...) ?
 - Non
 - Oui

3. Supervision de périphériques

- ▶ Quels périphériques informatiques la solution permet-elle de superviser (plusieurs réponses possibles) ?
 - Baie de disques ou SAN
 - NAS
 - Lecteur/enregistreur de bandes magnétiques
 - Imprimante
 - Scanner
 - Onduleur
 - Périphérique SNMP
 - Autre(s), précisez :

4. Supervision des réseaux

- ▶ Quels éléments du réseau la solution permet-elle de superviser (plusieurs réponses possibles) ?
 - Routeurs et switches
 - Appliances de firewall et/ou de proxy
 - Bornes Wifi
 - Bande passante
 - Ports TCP
 - Flux VoIP
 - Trafic UDP
 - Autre(s), précisez :
- ▶ Dans quelle mesure la solution est-elle capable de détecter automatiquement et de restituer graphiquement les flux du réseau ? **Graphe flux réseau**
- ▶ La solution est-elle capable de renifler des paquets réseau (« Packet sniffing ») ?
 - Non
 - Oui
- ▶ La solution permet-elle de superviser les classes de qualité de service du réseau (QoS) ?
 - Non
 - Oui

5. Supervision de plateformes

5.1 Supervision des serveurs web

- ▶ La solution offre-t-elle des fonctions adaptées à la supervision des serveurs web ?
 - Non
 - Oui : quels serveurs web la solution prend-elle en charge (plusieurs réponses possibles).
Précisez les versions prises en charge :
 - Apache
 - IIS
 - Sun Java System (Netscape / iPlanet)
 - Autre(s), précisez :
- ▶ Quels sont les éléments supervisables sur un serveur Web (plusieurs réponses possibles) ?
 - Nombre de visites d'un site
 - Nombre de visites d'une page (« hits »)
 - Nombre de visites d'un site ou d'une page par visiteur distinct
 - Temps de chargement d'une page Web
 - Surveillance d'une URL prédéfinie, via HTTP ou HTTPS
 - Surveillance d'une séquence d'URL prédéfinie au sein de la navigation d'un utilisateur
 - Surveillance des codes d'erreur renvoyés aux utilisateurs (par exemple l'erreur 404 « Page non trouvée »)
 - Autre(s), précisez : **A définir dans l'étude**

5.2 Supervision de serveurs de messagerie

- ▶ La solution offre-t-elle des fonctions adaptées à la supervision des serveurs de messagerie ?
 - Non
 - Oui : quels serveurs de messagerie la solution prend-elle en charge (plusieurs réponses possibles).
Précisez les versions prises en charge :
 - Microsoft Exchange
 - Postfix
 - Sendmail
 - Autre(s), précisez : Lotus
- ▶ Quels sont les éléments supervisables sur un serveur de messagerie (plusieurs réponses possibles) ?
 - Nombre de messages émis par SMTP
 - Nombre de message reçus par POP3
 - Trafic lié au protocole IMAP
 - Test « round trip » (suivi de l'émission d'un message test jusqu'à sa réception sur le même serveur, en « boucle »)
 - Autre(s), précisez : **Test présence serveur messagerie**

5.3 Supervision des serveurs d'applications

- ▶ La solution offre-t-elle des fonctions adaptées à la supervision des serveurs d'application et middleware ?
 - Non
 - Oui : quels serveurs d'application la solution prend-elle en charge (plusieurs réponses possibles).
Précisez les versions prises en charge :
 - Tomcat
 - JBoss
 - WebLogic
 - WebSphere
 - Autre(s), précisez : **Tuxedo**
- ▶ Quels sont les éléments supervisables sur un serveur Web (plusieurs réponses possibles) ?
 - Mémoire JVM
 - Charge CPU du processus serveur d'application
 - File de thread
 - Hit et métriques sur les composants « Servlet »
 - Hit et métriques sur les composants « Web Services »
 - Hit et métriques sur les composants « EJB »
 - Hit et métriques sur les composants « Spring »
 - Utilisateurs concurrents sur le serveur et par application
 - Surveillance des pools de connexions aux bases de données
 - Surveillance des Transactions JTA
 - Surveillance des files JMS
 - Autre(s), précisez :
- ▶ La solution permet-elle de suivre des chaînes d'appels multi-tiers et de corréler la performance entre les tiers (type servlet/web-service/ejb hébergés sur des serveurs d'application distincts) ? **A étudier**
- ▶ La solution permet-elle de superviser des serveurs d'application en cluster, de gérer des groupes et d'observer les métriques par membre d'un groupe cluster ? **A étudier**

5.4 Supervision de SGBD

- ▶ La solution offre-t-elle des fonctions adaptées à la supervision de SGBD ?
 - Non
 - Oui : quels SGBD la solution prend-elle en charge (plusieurs réponses possibles) ?
Précisez les versions prises en charge :
 - IBM DB2
 - Informix
 - Ingres
 - Microsoft SQLServer
 - MySQL
 - Oracle Database
 - Sybase
 - Autre(s), précisez :
- ▶ Quelles sont les métriques disponibles pour la supervision de SGBD ?
 - Nombre de bases de données en ligne,
 - Occupation de l'espace de stockage alloué à base
 - Consommation de la RAM serveur allouée au SGBD
 - Consommation de la mémoire cache interne au SGBD
 - Nombre de connexions utilisateur
 - Temps moyen et maximal de traitement d'une transaction
 - Nombre de transactions soumises par seconde
 - Nombre de transactions traitées par seconde
 - Nombre d'opérations d'entrée/sortie (I/O)
 - Occurrences de certaines erreurs qualifiées du SGBD
 - Temps de montage/démarrage des bases
 - Temps de sauvegarde
 - Autre(s), précisez :

5.5 Supervision des applications métiers

- ▶ La solution offre-t-elle des fonctions adaptées à la supervision des applications métiers développées et hébergées dans les serveurs ?
 - Non
 - Oui quels types d'application la solution prend-elle en charge (plusieurs réponses possibles) ?
 - Précisez les versions prises en charge :
 - Java / JEE
 - .Net / C#
 - PHP
 - Autre(s), précisez :
- ▶ L'application doit-elle être modifiée pour être prise en charge par la supervision et être mesurée ?
 - Non
 - Oui à quel(s) niveau(x) l'application doit-elle être modifiée ?
 - Par le développeur
 - Modification à la volée lors du déploiement
 - Autre(s) technologie(s) de mise en oeuvre :

- ▶ La solution permet-elle de suivre des chaînes d'appel multi-tiers et de corréliser la performance entre les tiers (type frontal web/ serveurs d'application / application / SGBD) ?
 - Non
 - Oui, détaillé : **Suivant les possibilités du logiciel retenu**

5.6 Supervision du "ressenti" utilisateurs

- ▶ Le ressenti peut-il être capturé à travers un robot de test simulant un navigateur ?
 - Non
 - Oui
 - Si Oui, ce robot de test est-il :
 - Un produit tiers
 - Une technologie intégrée à l'application
 - ▶ Le ressenti peut-il être capturé par divers temps de réponse mesurés au niveau de différentes couches ?
 - Non
 - Oui lesquelles ? **Suivant les possibilités du logiciel retenu**
 - Réseau
 - Frontal web
 - SGBD
 - Composants métier de l'application
 - Autre(s) :

5.7 Supervision des logs et fichiers

- ▶ La solution est-elle capable de détecter des événements spécifiques dans des fichiers de journalisation (logs) ?
 - Non
 - Oui quels sont les types de logs pris en charge par la solution (plusieurs réponses possibles) ?
 - Logs du système d'exploitation
 - Logs du middleware (SGBD, serveur Web...)
 - Logs applicatifs propriétaires
 - N'importe quel fichier texte structuré
 - ▶ La solution permet-elle de suivre les changements dans les fichiers de configurations ?
 - Non
 - Oui
 - Si Oui, précisez :
 - Les types de fichiers : **texte**
 - La configuration des plateformes supportées :
 - ▶ La solution permet-elle de comparer des configurations au sein d'un groupe homogène pour rendre compte des erreurs de configuration ?
 Suivant les possibilités du logiciel retenu
 - ▶ La solution de supervision permet-elle de superviser ses propres composants ?
 - Non
 - Oui (**haute dispo à prévoir actif/actif ou actif/passif**)

6. Gestion des alertes

- ▶ La solution est-elle livrée avec des jeux d'alertes prédéfinis ?
 - Non
 - Oui
 - ▶ La solution permet-elle de définir des dépendances entre alertes, de façon à réduire leur prolifération en cas de problèmes en cascade (exemple : si un serveur tombe en panne, une alerte est émise pour signaler la panne du serveur, mais pas pour les applications qu'il héberge) ?
 - Non
 - Oui

6.1. Alertes serveur

- ▶ Quelles sont les alertes spécifiques aux serveurs prises en charge (plusieurs réponses possibles) ?
 - Dépassement instantané d'un seuil de charge des processeurs

- Dépassement prolongé d'un seuil de charge des processeurs
- Dépassement instantané d'un seuil de mémoire vive
- Dépassement prolongé d'un seuil de mémoire vive
- Dépassement d'un seuil d'occupation sur un volume logique
- Arrêt non planifié d'un service ou d'un agent
- Survenance d'un événement prédéfini dans un fichier log
- Création d'un fichier prédéfini
- Augmentation soudaine de la taille d'un fichier prédéfini
- Modification d'un fichier prédéfini
- Détection d'un virus
- Autre(s), précisez :

6.2. Alertes réseau

- ▶ Quelles sont les alertes spécifiques au réseau prises en charge par la solution (plusieurs réponses possibles) ?
 - Non présence/non réponse d'un équipement réseau
 - Panne d'un port sur un équipement réseau
 - Consommation de bande passante supérieure à un seuil
 - Taux d'erreur TCP/IP supérieur à un seuil
 - Autre(s), précisez :

6.3. Remontée des alertes

- ▶ Les alertes sont-elles journalisées par la solution, de façon à pouvoir être consultées ?
 - Non
 - Oui
 - ▶ Par quels canaux la solution est-elle capable de faire remonter les alertes (plusieurs réponses possibles) ?
 - Console propriétaire
 - Console tierce
 - Fenêtres « pop-up »
 - Messagerie instantanée
 - E-mail
 - Appel téléphonique piloté par un serveur vocal
 - SMS/Pager
 - Autre(s), précisez :

- ▶ La solution permet-elle de définir des priorités ou des sévérités d'alertes ?
 - Non
 - Oui la remontée des alertes peut-elle être configurée en fonction des horaires et de leur priorité ?
 - Non
 - Oui

- ▶ La solution permet-elle de définir des groupes de destinataires des alertes ?
 - Non
 - Oui de quelle façon peuvent être utilisés les groupes de destinataires (plusieurs réponses possibles) ?
 - Envoi des alertes à des destinataires d'un groupe
 - Association des alertes aux groupes de destinataires en fonction des catégories d'équipements concernés
 - Association des alertes aux groupes de destinataires en fonction des horaires
 - Escalade des alertes d'un groupe à l'autre
 - Autre(s), précisez :

- ▶ Les alertes peuvent-elles être répétées selon une fréquence définie, jusqu'à leur acquittement ?
 - Non
 - Oui

- ▶ La solution permet-elle d'escalader les alertes sur différents canaux (par exemple : la première notification a lieu par fenêtre pop-up, puis par SMS 5 minutes plus tard si elle n'est toujours pas acquittée) ?
 - Non
 - Oui

6.4. Acquittement des alertes et actions correctrices

- ▶ La solution permet-elle d'acquitter les alertes ?
 - Non
 - Oui
 - ▶ L'administrateur peut-il préciser l'acquittement des alertes en distinguant la simple prise en charge du problème de la fin de sa résolution ?
 - Non
 - Oui
 - ▶ Depuis quels canaux l'acquittement des alertes est-il possible (plusieurs réponses possibles) ?
 - Console propriétaire
 - Console tierce
 - Fenêtres « pop-up »
 - E-mail
 - Appel téléphonique piloté par un serveur vocal
 - SMS
 - Autre(s), précisez : (**possibilités limitées par la politique de sécurité informatique**)
 - ▶ Lors de l'acquittement d'une alerte, la solution propose-t-elle de ne plus la signaler jusqu'à nouvel ordre ?
 - Non
 - Oui

- ▶ La solution permet-elle de déclencher l'exécution d'actions correctrices en fonction des alertes ?
 - Non
 - Oui quels types d'actions correctrices sont proposés par la solution (plusieurs réponses possibles) ?
 - Redémarrage de process ou de services
 - Arrêt de process ou de services (stratégie de mise en sécurité pour éviter la propagation de certains problèmes)
 - Arrêt d'un serveur ou d'un équipement
 - Redémarrage d'un serveur ou d'un équipement
 - Autre(s), précisez :

7. Console de supervision

- ▶ La console fonctionne-t-elle dans un navigateur Web ?
 - Non
 - Oui Si Oui, quels sont les navigateurs Web (plusieurs réponses possibles – précisez les versions supportées) ?
 - Apple Safari
 - Google Chrome
 - Microsoft Internet Explorer
 - Mozilla Firefox
 - Opera
 - Autre(s), précisez :
- ▶ La console indique-t-elle en temps réel les équipements qui sont en ligne et ceux qui ne le sont pas ?
 - Non
 - Oui
- ▶ La console inclut-elle une fonction de recherche multicritères pour trouver des équipements dans le périmètre de supervision ?
 - Non
 - Oui
- ▶ La console est-elle accessible depuis n'importe quel terminal du réseau ?
 - Non
 - Oui Si Non, quels sont les pré requis pour pouvoir accéder à la console ? La console est-elle disponible en environnement PDA ?
 - Non
 - Oui, sans restriction fonctionnelle
 - Oui, avec des restrictions fonctionnelles (précisez lesquelles) :
 - ➔ **possibilités limitées par la politique de sécurité informatique**
 - Si Oui, avec quels PDA la console est-elle compatible (plusieurs réponses possibles) ?
 - Android
 - Blackberry
 - iPhone
 - Windows CE
 - Autre(s), précisez :
- ▶ La console peut-elle être personnalisée aux couleurs de l'entreprise (logo, couleurs...) ?
 - Non
 - Oui

8. Rapports, graphiques et tableaux de bord

- ▶ La solution inclut-elle sa propre technologie de tableaux de bord graphiques ?
 - Non
 - Oui
- Si Non, quelles sont les applications tierces de tableaux de bord graphiques compatibles avec la solution ?
- ▶ Les graphiques sont-ils intégrés à la console de supervision ?
 - Non
 - Oui
- ▶ Quels sont les formats possibles de restitution ou d'extraction des rapports (plusieurs réponses possibles) ?
 - HTML
 - PDF
 - XML
 - CSV
 - Microsoft Excel
 - Autre(s), précisez :
- ▶ La solution permet-elle de programmer la distribution des rapports par e-mail ?
 - Non Jbid1234
 - Oui

La solution est-elle livrée avec des jeux de rapports ou de requêtes prédéfinis ?

- Non
- Oui Si Oui, lesquels ? **SLA**
- ▶ Les graphiques, rapports et cartes sont-ils cliquables de façon à amener l'utilisateur sur des données plus détaillées de l'élément cliqué ?
 - Non
 - Oui

9. Gestion des utilisateurs

- ▶ La solution définit-elle des profils différents associés aux utilisateurs ?
 - Non
 - Oui
- ▶ La solution permet-elle de distinguer les droits de visualisation (supervision) des droits d'intervention (déclencher des actions) ?
 - Non
 - Oui
- ▶ Quels sont les critères sur lesquels la solution permet de définir les droits de supervision ou d'intervention (plusieurs réponses possibles) ?
 - Type d'équipement (serveur, imprimante...)
 - Sous-ensemble du réseau
 - Tranches horaires
 - Autre(s), précisez :

10. Architecture technique

- ▶ La solution permet-elle l'ajout de composants (plug-ins) ?
 - Non
 - Oui .Quels sont les prérequis pour ces composants ?
 - Composant stable et maintenable**
- La solution permet-elle l'ajout de composants développés par le client ?
 - Non
 - Oui .Dans quels langage de programmation les composants spécifiques doivent-ils être développés (plusieurs réponses possibles) ?
 - C/C++
 - Perl
 - Linux shell
 - Python
 - Ruby
 - Autre(s), précisez :
- ▶ Quels sont les composants middleware nécessaires à l'installation de la solution (plusieurs réponses possibles) ?
 - Serveur Web
 - SGBD
 - Framework Microsoft .NET
 - Librairie graphique
 - Autre(s), précisez :
- ▶ Quels sont les serveurs Web compatibles en tant que middleware (plusieurs réponses possibles) ?
 - Apache
 - Microsoft IIS
 - Sun Java System Web Server
 - Autre(s), précisez :
- ▶ Sur quel SGBD la solution repose-t-elle pour stocker ses propres données (plusieurs réponses possibles) ?
 - IBM DB2
 - Informix
 - Ingres
 - Microsoft SQLServer
 - MySQL
 - Oracle Database
 - Sybase
 - Autres, précisez : **A définir suivant la solution retenue (Oracle ou mysql si possible)**
- ▶ Les données de supervision sont-elles interrogeables avec une application tierce ?
 - Non
 - Oui Si Oui, quelles sont les possibilités d'interrogation des données de supervision (Plusieurs réponses possibles) ?
 - Accès direct aux fichiers ou aux SGBD de la solution
 - Accès via une API
 - Export des données en fichier structuré type CSV
 - Autre(s), précisez :
- ▶ Les échanges entre la console de supervision et le serveur sont-ils cryptés ?
 - Non
 - Oui
- ▶ La solution peut-elle être répartie sur plusieurs serveurs pour en optimiser la charge et la disponibilité ?
 - Non
 - Oui

18. Analyse des risques

L'outil Excel proposé DGSAGIR (Direction Générale des Solutions d'Affaires en Gestion Intégrée des Ressources du Gouvernement du Québec) a été adapté à l'environnement SSA. Il a permis d'identifier les risques potentiels ou les facteurs critiques de notre projet et à produire un plan d'action approprié.. (www.cspq.gouv.qc.ca).

Extrait document projet [RISQ-SUPERV-NP]

Facteurs de risque		Choix
Environnement du client	1- Processus de gestion et d'appropriation du MOA (Maîtrise d'Ouvrage)	
	1 Processus de gestion intégrant tous les différents éléments : gestion de projet / livrables / gestion du changement	X
	2 Processus de gestion intégrant les principaux éléments de gestion de projet	
	3 Processus de gestion intégrant peu d'éléments de gestion de projet, mais qui sera ajusté en conséquence	
	4 Peu d'expérience en gestion de projet – accompagnement requis sur certains aspects	
	5 Accompagnement soutenu requis pour supporter la gestion du projet	
	2- Position des relations avec le MOA	
	1 Bonne complicité dans la gestion du projet	
	2 Bonne communication – sommes confiants de trouver ensemble les solutions	X
	3 Problèmes ad hoc dans les relations – situation globale sous contrôle	
	4 Relations tendues avec un plan de résolution des problèmes	
	5 Relations tendues nécessitant l'intervention d'un tiers	
	3- Degré d'importance de l'application pour le MOA	
	1 Application non stratégique et d'intérêt pour un seul groupe	
	2 Application non stratégique et d'intérêt pour plusieurs groupes	
	3 Application critique au succès du projet	
	4 Application stratégique pour le SSA	X
	5 Application critique à la mission du SSA	
	4- Justification du projet	
	1 Justification complète, supportée par le CeTIMA, projet stratégique	X
	2 Justification complète, supportée par le CeTIMA, projet peut être annulé	
	3 Justification incomplète mais le projet est supporté par le CeTIMA	
	4 Justification incomplète	
	5 Aucune justification pour le projet	
	5- Processus décisionnel du MOA/MOE	
	1 Processus bien défini et appliqué	X
	2 Processus bien défini mais pas appliqué de façon uniforme et continue	
	3 Processus défini mais non implanté	
	4 Processus non défini	
	5 Aucun processus spécifique	
	6- Adhésion des dirigeants au projet	
	1 Adhésion totale confirmée des dirigeants	
	2 Adhésion implicite des dirigeants	X
	3 Adhésion à confirmer auprès des dirigeants	
4 Adhésion litigieuse nécessitant des actions précises		
5 Aucune adhésion manifestée par les dirigeants		
7- Priorisation du projet par rapport aux autres travaux		
1 Projet prioritaire par rapport aux autres travaux		
2 Bon niveau de priorité accordé au projet (équipe TME doit assurer son contrat SLA d'exploitation des plateformes SI)	X	
3 Priorité à confirmer par rapport aux autres travaux		
4 Priorité mitigée par rapport aux autres travaux		
5 D'autres travaux sont jugés prioritaires par rapport au projet		

Envergure du projet	8- Disponibilité des utilisateurs TME ou MOA	
	1 Pleinement disponibles	
	2 Disponibles que partiellement	
	3 Moyennement disponibles	
	4 Faible disponibilité	X
	5 Aucune disponibilité	
	9- Variété des profils utilisateurs de la solution de supervision	
	1 Tous les utilisateurs concernés ont le même profil	
	2 Quelques profils similaires d'utilisateurs (<i>administrateur, consultation</i>)	X
	3 Bonne variété de profils différents d'utilisateurs	
	4 Plusieurs variétés de profils utilisateurs concernés	
	5 Profils utilisateurs encore inconnus	
	10- Connaissances des utilisateurs en informatique	
	1 Très bonnes connaissances en informatique	X
	2 Bonnes connaissances générales en informatique	
	3 Connaissances minimales en informatique	
	4 Connaissances en informatique à compléter, nécessitant de la formation	
	5 Aucune connaissance en informatique	
	11- Probabilité d'un changement d'instance politique	
	1 Aucune probabilité de changement d'instance politique	
	2 Faible probabilité de changement d'instance politique	
	3 Changement possible d'instance politique	
	4 Très forte probabilité d'un changement d'instance politique (<i>transfert du MOE d'employeur en cours</i>)	X
	5 Changement d'instance politique en cours	
	12- Coûts globaux de réalisation du projet	
	1 Moins de 100 000 €	X
	2 Entre 100 001 € et 300 000 €	
	3 Entre 300 001 € et 500 000 €	
	4 Entre 500 001 € et 1 000 000 €	
	5 Plus de 1 000 001€	
	13- Efforts informatiques	
	1 Moins de 100 jours-personnes	X
	2 Entre 101 et 300 jours-personnes	
	3 Entre 301 et 800 jours-personnes	
	4 Entre 801 et 1 500 jours-personnes	
	5 Plus de 1 501 jours-personnes	
	14- Efforts des utilisateurs	
	1 Moins de 50 jours-personnes	
	2 Entre 51 et 150 jours-personnes (<i>correspond aux 5-6 mois du projet CNAM</i>)	X
	3 Entre 151 et 400 jours-personnes	
	4 Entre 401 et 750 jours-personnes	
	5 Plus de 751 jours-personnes	
	15- Nombre de ressources dans l'équipe de projet	
	1 Moins de 5 personnes (<i>1 personne</i>)	X
	2 Entre 5 et 10 personnes	
	3 Entre 11 et 20 personnes	
	4 Entre 21 et 40 personnes	
5 Plus de 41 personnes		

Impacts sur les affaires	16- Impacts stratégiques et critiques sur le fonctionnement de l'entreprise (risques sociaux inclus)	
	1 Très faibles impacts	
	2 Impacts moyens	X
	3 Impacts significatifs	
	4 Impacts très importants	
	5 Impacts stratégiques et critiques	
	17- Impacts budgétaires et financiers	
	1 Négligeables	
	2 Impacts moyens	X
	3 Impacts significatifs	
	4 Impacts très importants	
	5 Impacts stratégiques et critiques	
	18- Niveau des bénéfices potentiels attendus	
	1 Moins de 100 000 €	
	2 Entre 100 001 € et 300 000 €	X
	3 Entre 300 001 € et 500 000 €	
	4 Entre 500 001€ et 1 000 000€	
	5 Plus de 1 000 001 €	
	19- Impacts de l'application sur les utilisateurs	
	1 Négligeables	
2 Impacts moyens (<i>solution de secours : script, interface produits</i>)	X	
3 Impacts significatifs		
4 Impacts très importants		
5 Impacts stratégiques et critiques		
20- Nombre d'utilisateurs touchés		
1 Moins de 100 personnes	X	
2 Entre 101 et 300 personnes		
3 Entre 301 et 800 personnes		
4 Entre 801 et 1 500 personnes		
5 Plus de 1 501 personnes		
Caractéristiques de l'application	21- Énoncé clair et compréhension des besoins	
	1 Besoins clairement définis et approuvés par MOA	X
	2 Besoins clairement définis mais non approuvés par le client	
	3 Besoins incomplets ou mal documentés	
	4 Besoins ambigus nécessitant de l'interprétation	
	5 Besoins non connus ou contradictoires	
	22- Domaine d'application du système	
	1 Équipe de projet expérimentée avec l'application	
	2 Type d'application bien comprise, expérience limitée de l'équipe	X
	3 Type d'application bien comprise, peu d'expérience de l'équipe	
	4 Type d'application non maîtrisée par l'équipe de projet	
	5 Application expérimentale	
	23- Type et complexité des données	
	1 Données simples et connues de l'équipe	X
	2 Données simples mais pas connues de l'équipe	
	3 Données nominatives et confidentielles	
4 Données stratégiques de nature monétaire et budgétaire		
5 Données stratégiques ayant des impacts vitaux sur les affaires		
24- Réponse d'un progiciel aux besoins fonctionnels		
1 Répond à 100 % des besoins (aucun développement additionnel)		

Caractéristiques du projet	2 Répond à 80 % des besoins (20 % de nouveau développement)	X	
	3 Répond à 60 % des besoins (40 % de nouveau développement)		
	4 Répond à 40 % des besoins (60 % de nouveau développement)		
	5 Répond à 20 % des besoins (80 % de nouveau développement)		
	25- Interfaces avec d'autres systèmes (existants ou à venir)		
	1 Aucune		
	2 Peu de liens et sous le contrôle de l'équipe		
	3 Peu de liens mais sous le contrôle d'une autre équipe	X	
	4 Plusieurs liens sous le contrôle de l'équipe		
	5 Plusieurs liens et hors du contrôle de l'équipe		
	26- Qualité et appréciation des phases et livrables précédents		
	1 Complétés par la même équipe et acceptés par MOA	X	
	2 Complétés par une autre équipe et bonne qualité du travail		
	3 Résultats précédents nécessitent des ajustements		
	4 Résultats précédents produits par la même équipe et nécessitant des corrections importantes		
	5 Résultats précédents produits par une autre équipe et nécessitant des corrections importantes		
	27- Durée et échéancier fixés		
	1 Durée et échéancier flexibles et sous le contrôle de l'équipe de projet	X	
	2 Durée et échéancier fixes mais facilement atteignables		
	3 Durée et échéancier réalistes mais demandant une gestion serrée		
	4 Durée et échéancier optimistes mais atteignables		
	5 Durée et échéancier irréalistes		
	28- Type de financement du projet		
	1 Temps et matériel sans maximum		
	2 Temps et matériel avec un maximum renégociable	X	
3 Temps et matériel avec un maximum fixe			
4 Prix fixe avec changements possibles au budget			
5 Prix fixe sans changement possible au budget			
29- Degré d'implication de ministères et organismes			
1 Mécanismes en place pour assurer le succès du projet			
2 Mécanismes en place mais nécessitent une période de rodage (<i>découverte du fonctionnement CeTIMA à réaliser</i>)	X		
3 Mécanismes en place mais nécessitent une période de rodage et d'approbation			
4 Certains mécanismes sont absents			
5 Certains mécanismes présentent des lacunes			
30- Degré d'implication de fournisseurs externes (TME)			
1 Mécanismes en place pour assurer le succès du projet	X		
2 Mécanismes en place mais nécessitent une période de rodage			
3 Mécanismes en place mais nécessitent une période de rodage et d'approbation			
4 Certains mécanismes sont absents			
5 Certains mécanismes présentent des lacunes			
31- Dépendance entre les livrables			
1 Aucune dépendance significative			
2 Dépendance entre les livrables entièrement sous notre contrôle			
3 Dépendance entre quelques livrables accessoires sous la responsabilité d'un autre secteur ou d'un sous-contractant	X		
4 Dépendance entre des livrables importants sous la responsabilité d'un autre secteur ou d'un sous-contractant			
5 Dépendance avec une majorité de livrables sous la responsabilité d'un autre secteur ou d'un sous-contractant			
32- Dépendance avec d'autres projets (en cours ou à venir)			
1 Aucune dépendance significative			
2 Dépendance entre des projets entièrement sous notre contrôle	X		
3 Dépendance entre quelques projets accessoires sous la responsabilité d'un autre secteur ou d'un sous-contractant			
4 Dépendance entre des projets, avec des projets importants sous la responsabilité d'un autre secteur			

Organisation du projet	33- Définition claire du projet et de ses limites	
	1 Projet clairement défini	
	2 Multiples projets, clairement définis	X
	3 Projet sujet à révision en cours de route	
	4 Pas de définition claire des livrables et des attentes	
	5 Projets multiples avec critères d'acceptation ambigus ou mal définis	
	34- Définition claire des responsabilités de tous les intervenants	
	1 Responsabilités clairement définies et diffusées	
	2 Responsabilités multiples, clairement définies	X
	3 Responsabilités sujet à révision en cours de route	
	4 Responsabilités mitigées, mal définies, non diffusées	
	5 Pas de définition claire des responsabilités des intervenants	
	35- Compréhension et engagement des intervenants au projet	
	1 Très bonne compréhension et engagement manifesté	
	2 Bonne compréhension et engagement implicite	X
	3 Compréhension et engagement à confirmer	
	4 Compréhension et engagement nécessitant des actions précises	
	5 Compréhension ambiguë et aucun engagement signifié	
	36- Planification détaillée du projet et des livrables	
	1 Planification exhaustive complétée	
	2 Planification complétée mais à valider	X
	3 Planification en cours d'élaboration	
	4 Planification nécessitant des changements importants, risques de dérives importants	
	5 Aucune planification du projet	
	37- Outils et processus de suivi et de reporting	
	1 Outils et processus en place et fonctionnels	
	2 Outils et processus en place mais pas fonctionnels (<i>pas de lien fonctionnel/hiérarchique entre l'équipe TME et MOE</i>)	X
	3 Outils et processus choisis mais controversés	
	4 Outils et processus en voie d'être définis	
	5 Aucun outil ou processus de suivi désigné	
	38- Gestion des changements	
	1 Processus en place et fonctionnel	
	2 Processus en place mais pas fonctionnel (<i>pas de lien fonctionnel/hiérarchique entre l'équipe TME et MOE</i>)	X
	3 Processus choisi mais controversé	
	4 Processus en voie d'être défini	
	5 Aucun processus désigné	
	39- Lien de communication entre les acteurs du projet	
	1 Direct : MOE intégré à l'équipe utilisateur TME	
	2 Proche : MOE sur le site du CeTIMA	
	3 Local : MOE sur Paris (contact direct aisé avec MOA ou TME en cas de difficulté)	
	4 Distant : MOE sur un site non proche (Brest) du MOA/Equipe TME (communication indirect par mail ou téléphone)	X
	5 Aucun contact direct avec les utilisateurs ou MOE (sous traitance par le MOE)	
	40- Gestion de la qualité	
	1 Processus en place et fonctionnel	
	2 Processus en place mais pas fonctionnel (<i>pas de lien fonctionnel/hiérarchique entre l'équipe TME et MOE</i>)	X
	3 Processus choisi mais controversé	
	4 Processus en voie d'être défini	
5 Aucun processus désigné		

Équipe de projet	41- Expérience pertinente du mandataire du projet		
	1	Expérience très pertinente en gestion de projets similaires	
	2	Expérience pertinente en gestion de projets d'autres natures (<i>projets DCNS : SAD, PA CdG, SNLE, SSI PAU..</i>)	X
	3	Quelques expériences en gestion de projets	
	4	Faible expérience en gestion de projets	
	5	Aucune expérience pertinente	
	42- Expérience pertinente du chargé de projet		
	1	Expérience très pertinente en gestion de projets similaires	
	2	Expérience pertinente en gestion de projets d'autres natures (<i>projets DCNS : SAD, PA CdG, SNLE, SSI PAU..</i>)	X
	3	Quelques expériences en gestion de projets	
	4	Faible expérience en gestion de projets	
	5	Aucune expérience pertinente	
	43- Expérience pertinente du pilote / de l'équipe de pilotage		
	1	Expérience très pertinente dans des projets similaires	
	2	Expérience pertinente dans des projets d'autres natures (<i>projets DCNS : SAD, PA CdG, SNLE, SSI PAU..</i>)	X
	3	Quelques expériences dans ce type de projet	
	4	Faible expérience dans ce type de projet	
	5	Aucune expérience pertinente	
	44- Expérience de l'équipe dans des projets similaires		
	1	Expérience très pertinente dans des projets similaires	
	2	Expérience pertinente dans des projets d'autres natures (<i>projets DCNS : SAD, PA CdG, SNLE, SSI PAU..</i>)	X
	3	Quelques expériences dans ce type de projet	
	4	Faible expérience dans ce type de projet	
	5	Aucune expérience pertinente	
	45- Connaissance des applications ou des progiciels de supervision		
	1	Excellente connaissance des produits de supervision	
	2	Connaissance générale d'applications de même nature	
	3	Connaissance théorique des produits de supervision	
	4	Faible connaissance des produits de supervision	X
	5	Aucune connaissance des produits de supervision	
	46- Dépendance de ressources clés		
	1	Aucune dépendance, ressources facilement remplaçables	
	2	Faible dépendance, ressources remplaçables	X
	3	Dépendance de certaines ressources clés mais remplaçables	
	4	Dépendance de plusieurs ressources clés mais remplaçables	
	5	Forte dépendance de ressources clés, ressources irremplaçables	
	47- Disponibilité des ressources techniques requises		
	1	Pleinement disponibles	
	2	Disponibles que partiellement	X
	3	Moyennement disponibles	
	4	Faible disponibilité	
	5	Aucune disponibilité	
	48- Disponibilité des ressources de pilotage requises		
	1	Pleinement disponibles	X
	2	Disponibles que partiellement	
3	Moyennement disponibles		
4	Faible disponibilité		
5	Aucune disponibilité		

Environnement de développement	49- Connaissance et expérience avec la méthodologie	
	1 Méthodologie de l'équipe de projet	
	2 Méthodologie maîtrisée par l'équipe de projet	X
	3 Méthodologie connue par l'équipe de projet	
	4 Connaissance théorique de la méthodologie	
	5 Aucune expérience avec la méthodologie	
	50- Connaissance et expérience avec les standards, normes, etc.	
	1 Normes et standards de l'équipe de projet	
	2 Normes et standards maîtrisés par l'équipe de projet	
	3 Normes et standards connus par l'équipe de projet	X
	4 Connaissance théorique des normes et standards	
	5 Aucune expérience avec les normes et standards	
	51- Connaissance et expérience avec les outils	
	1 Outils spécifiques à l'équipe de projet	
	2 Outils standard maîtrisés par l'équipe de projet	
	3 Outils connus par l'équipe de projet	X
	4 Connaissance théorique des outils	
	5 Aucune expérience avec les outils	
	52- Accès aux compétences et expertises primordiales requises	
	1 Expertise présente au sein de l'équipe de projet	
2 Expertise présente au SSA	X	
3 Aucune expertise au SSA		
4 Expertise assez rare dans le marché		
5 Aucune expertise disponible		
53- Disponibilité de l'environnement de développement et d'essais		
1 Environnement disponible en tout temps		
2 Environnement disponible à l'intérieur de plage prédéfinie	X	
3 Environnement offrant peu de disponibilité		
4 Environnement contingenté et engorgé		
5 Très faible disponibilité de l'environnement de développement		
54- Disponibilité de la documentation		
1 Documentation largement diffusée		
2 Documentation disponible au SSA	X	
3 Documentation partielle disponible au SSA		
4 Peu de documentation disponible		
5 Aucune documentation disponible		
Technologies utilisées	55- Degré de maturité des technologies en cause	
	1 Technologies connues et démontrées	
	2 Technologies connues, démontrées, quelques nouvelles composantes	
	3 Technologies nouvelles pour l'équipe mais démontrées sur le marché	X
	4 Technologies de pointe	
	5 Technologies non éprouvées / en développement	
	56- Degré de complexité de l'architecture technologique	
	1 Architecture simple et traditionnelle	
	2 Architecture d'une complexité moyenne	X
	3 Architecture d'une complexité moyenne, expérience limitée de l'équipe	
4 Architecture complexe et centralisée		
5 Architecture complexe et distribuée		

57- Mélange de diverses composantes technologiques		
1	Petit nombre de composantes connues, équipe expérimentée	
2	Petit nombre de composantes connues, équipe peu expérimentée	
3	Plusieurs composantes, expertise démontrée de l'équipe de projet	
4	Multiplés composantes à intégrer, : <i>SNMP, supervision, métrologie, Oracle, JBoss, Apache ..</i>	X
5	Multiplés composantes à intégrer, intégration non démontrée	
58- Degré d'importance de la performance du système		
1	Performance du système sans importance	
2	Performance du système peu importante	
3	Performance du système importante	X
4	Performance du système astreignante	
5	Performance du système critique	
59- Degré d'importance de la sécurité du système		
1	Aucun besoin spécial de sécurité des données	
2	Besoins limités en sécurité	
3	Environnement habituel de sécurité	X
4	Besoins spéciaux en sécurité, inhabituels	
5	Multiplés niveaux de sécurité, contraintes importantes	
60- Expertise disponible à l'équipe de projet (support, formation)		
1	Expertise disponible au SSA	X
2	Expertise disponible par des fournisseurs externes	
3	Fournisseurs avec expertise unique mais pas sur le chemin critique	
4	Expertise rare sur le marché	
5	Dépendance sur la disponibilité de fournisseurs, expertise pointue	

19. Grille REX

Le retour d'expérience (REX) est un processus de réflexion mis en œuvre pour tirer les enseignements positifs et négatifs du projet. Dans ce processus d'évaluation, inspiré d'une grille proposée par le CEDIP, on porte un regard sur la démarche développée, les méthodes employées, les livrables réalisés, le rôle et le niveau d'implication des acteurs concernés, ainsi que sur les moyens utilisés.

Extrait document projet [REX-SUPERV-NP]

Identifiant : on entend par « qualité de l'identifiant » le statut que détenait, dans le cadre du projet concerné, la personne qui complète la grille : chef de projet, membre de l'équipe projet, chargé d'études, directeur, etc.

Critères : ils sont au nombre de 8 (pertinence, cohérence, synergie, efficacité, efficience, durabilité, impact, flexibilité).

Indicateurs : ils ne sont pas exhaustifs. Ils permettent de relever les points forts ou faibles dans le cadre du projet concerné et s'appliquent à l'action de tous les acteurs (commanditaire et ses représentants, conseils internes et externes, etc.).

Observations, analyse des causes : dans cette partie, peuvent s'exprimer un avis global sur le critère et les indicateurs concernés, une identification des différentes causes possibles expliquant les réponses positives ou négatives par indicateur, toutes sortes de commentaires.

Éléments à capitaliser : il s'agit ici de faire des propositions de capitalisation à partir des points forts et faibles précédemment identifiés et analysés, en prenant en compte, le cas échéant, d'autres expériences : *Quels sont les enseignements à tirer de cette expérience ?*

IDENTIFICATION DU PROJET :

Intitulé : SUPERVISION SI METIER DU SSA

Commanditaire : CeTIMA

Résultat (s) attendu(s) : Mise en place d'une architecture de supervision opensource à base du logiciel Nagios sur les plateformes métier du SSA.

Critères	Indicateurs	O	U	N	Observations, analyse des causes	Eléments à capitaliser
		I	I	N		
Pertinence <i>Dans la commande, les besoins, les objectifs ou les finalités ont-ils été clairement identifiés ? Les objectifs initialement arrêtés répondent-ils aux besoins de façon satisfaisante ? Le projet était-il compatible avec les contraintes imposées par le contexte et avec les exigences du commanditaire ?</i>	Commande suffisamment claire du commanditaire au regard de la problématique de départ.	X			Le besoin dépasse le CeTIMA car des demandes de la DRSSA et certains HIA pour information d'installation de nagios Les différents acteurs (MOE,MOA,TMA) avaient des projets transversaux cruciaux pour le Mindef, mais tous ont fait de leur mieux pour répondre présent malgré les contraintes	
	Identification des besoins des bénéficiaires de l'action, des contraintes et des exigences.	X				
	Réponse à un réel besoin.	X				
	Acteurs clairement identifiés et rôle de chacun bien défini.	X				
	Bonne prise en compte du contexte.	X				
	Conformité des objectifs avec les besoins.	X				
	Démarche suffisamment cadrée.	X				
	Compatibilité de la production demandée avec le contexte et les contraintes imposées.	X				
Cohérence <i>Les moyens (humains, matériels, etc.), mis à la disposition du chef de projet, permettaient-ils d'atteindre les objectifs et finalités visés(dimensionnement, complémentarité, etc.), dans les délais impartis ?</i>	Moyens suffisants et adaptés pour l'atteinte des objectifs.	X	X		Difficultés financières parfois pour se rendre à Paris (contraintes non négociables imposées par les RH Mindef au début du projet)	Compétences de l'équipe TME
	Compatibilité et complémentarité des moyens.	X				
	Compétences des personnes impliquées dans le projet.	X				
	Démarche co-construite et partagée (cadres, personnels, etc.).	X				

Critères	Indicateurs	O	N	Observations, analyse des causes	Éléments à capitaliser
		U	O		
		I	N		
Synergie <i>La coordination des actions entre acteurs a-t-elle été optimale ? Des dysfonctionnements dans les relations ont-ils eu un impact sur les résultats effectivement obtenus ?</i>	Implication suffisante du commanditaire et/ ou de ses représentants dans le processus. Régularité des échanges avec ceux-ci. Tensions entre acteurs du projet. Suivi efficace des actions.	X		Coupe dans le planning du projet pour passer l'UV Bulats anglais (imposé avant la soutenance) et gérer changement d'employeur (SSA/DIRISI)	Anticiper les problèmes extérieurs au projet
Efficacité <i>Les résultats obtenus ont-ils été conformes aux objectifs visés ? L'ensemble des objectifs a-t-il été atteint ? Quel est le niveau d'atteinte des objectifs ?</i>	Atteinte des objectifs fixés Satisfaction des besoins des bénéficiaires. Difficulté pour réaliser les productions attendues. Évolution de la commande ayant joué sur les résultats. Réactivité suffisante Planning respecté Budget respecté	X	X	Partiel : certaines impossibilités techniques des outils opensource Phase maquettage : mesure temps de réponse BDD oracle et supervision parefeu (éditeur réticent à donner des informations d'interfaçage nagios)	Des compromis ont toujours été obtenus pour éviter les conflits et permettre de continuer la dynamique du projet Communication pour expliquer les retards
Efficience <i>Par rapport aux résultats obtenus, les moyens mobilisés étaient-ils surdimensionnés ou inadaptés ?</i>	Solutions alternatives possibles (moyens, méthodes, etc.). Organisation des actions suffisamment structurée. Respect des délais. Bonne adéquation mission / moyens / résultats	X			
Durabilité <i>Y a-t-il maintien, dans le temps, des résultats obtenus par rapport aux objectifs visés ?</i>	Volonté de faire évoluer l'organisation et le fonctionnement du service de la part du commanditaire, voire de ses représentants. Diffusion en interne des résultats obtenus. Diffusion en externe des résultats obtenus. Suivi assuré des résultats et du plan d'actions. Des compétences ont développé	X			Dynamique du MOA de toujours évoluer et progresser Démarche qualité Pluridisciplinarité du projet : réseau, qualité, BDD, web, Java, VMware, linux, analyse des risques, communication...
Impact <i>Le projet (sa conduite, ses résultats, la production réalisée) a-t-il eu des effets prévus ou non sur le système (contexte, organisation, acteurs) dans lequel il s'est déroulé ?</i>	Motivation renforcée des acteurs pour l'application des résultats et du plan d'actions éventuel. Effets prévisibles des travaux menés à moyen et à long terme. Contacts et dialogue améliorés entre les services et entre les agents de la structure.	X			
Flexibilité <i>Tout au long du projet, y a-t-il eu adaptation du service et des acteurs ? Des modifications sont-elles intervenues dans le processus, le rôle des acteurs, les moyens mis en oeuvre, etc. ?</i>	L'organisation et les modes de fonctionnement du service ont été modifiés pendant le projet. Évolution du périmètre du projet, des méthodes, des moyens, etc. au cours du projet pour s'adapter aux évolutions du contexte. Redéfinition du rôle des acteurs.	X	X	Suite au temps demandé pour passer l'UV d'anglais et report de la soutenance de décembre 2011	moyens dimensionnés /méthodes sélectionnées correctement et en début de projet (uniquement problème de planning /disponibilité)