Étude et mise en œuvre d'une solution opensource de supervision systèmes et réseaux

Pierre-Yves Dubreucq

le cnam

Alter Way

CONSERVATOIRE NATIONAL DES ARTS ET METIERS
CENTRE REGIONAL ASSOCIE DE LILLE

MEMOIRE
présenté en vue d'obtenir
le DIPLOME D'INGENIEUR CNAM

SPECIALITE : Informatique
OPTION : Réseaux, Systèmes et Multimédia (IRSM)

par

Pierre-Yves DUBREUCQ

ETUDE ET MISE EN ŒUVRE D'UNE SOLUTION OPENSOURCE DE SUPERVISION SYSTÈMES ET RÉSEAUX

Nagios®

Soutenu le 16 mars 2012

JURY

Présidente :	Élisabeth Métais
Membres CNAM :	Frédéric Vast
	Jean Raudrant
	Thomas Dinnyes
	Robert Vandaele
Membres Alter Way :	Vincent Vignolle
	Stéphane Vincent

Conservatoire national des arts et métiers

Résumé

Alter Way Solutions, fort de sa croissance, a eu besoin d'avoir une meilleure maîtrise des différents systèmes d'information de ses clients. Les contrats d'infogérance intègrent des niveaux de service qu'il est nécessaire de justifier et d'améliorer. La mise en place d'une solution de supervision est donc apparue comme une évidence et une nécessité.

Celle-ci aura pour rôle d'accroître la qualité de service, de fournir un regard sur la santé des systèmes d'information client, mais aussi de fournir des indicateurs qui permettront de justifier du respect des niveaux de services conclus avec le client.

Le monde de la supervision open source est très mature de nos jours, Alter Way étant spécialisé en logiciels libres, il est apparu évident de s'orienter vers une solution libre afin de couvrir l'entièreté de nos besoins et pouvant s'adapter facilement à nos contraintes.

De ce fait, j'ai étudié toutes les solutions de supervision libres du marché, puis j'ai mis en exergue les deux solutions de supervision matures et très répandues.

Le couple Nagios / Centreon est la solution qui a le mieux répondu à nos besoins et contraintes.

L'architecture de la solution de supervision se doit d'être robuste, performante et évolutive.

Mots Clefs : supervision, métrologie, gestion d'incidents, gestion de performances, disponibilité, continuité de service, niveau de service, infogérance, architecture distribuée

Summary

Alter Way Solutions needs to have more control of the various Information Systems of their customers. The outsourcing contracts include service levels and it's need to justify and improve it. The implementation of monitoring appears as obvious and essential.

This solution will allow to increase the quality of service, to provide a look at the information systems health customer, but also to provide indicators to demonstrate compliance with service level agreements to the clients.

The world of open source monitoring is very mature nowadays .Alter Way is specialized in open source software, it seemed evident to turn to an open source solution to obtain the whole of our needs and being able to adapt itself easily to our constraints.

Therefore, I studied all the opensource solutions, and then I highlighted two monitoring solutions mature and widespread.

The couple Nagios / Centreon is the solution which the best answered our needs and constraints.

The architecture of the monitoring solution must be robust, efficient and scalable.

Keywords : monitoring, weathermap, Incident Management, Performance Management, availability, continuity of service, service level agreements, outsourcing, distributed architecture

Table des matières

1. Introduction

Les méthodes de gestion de services informatiques ont considérablement évolué depuis ces dernières années. Les bonnes pratiques ITIL font désormais partie intégrante des services informatiques, notamment le respect des niveaux de services (SLA[1])

Dans le cadre d'un contrat d'infogérance, il est d'usage de spécifier ces niveaux de services exigés.

Afin de pouvoir garantir ceux-ci et de les justifier, il est devenu essentiel de mettre en place une solution de supervision.

Le groupe Alter Way est spécialisé en technologies libres et open source, c'est pourquoi les solutions étudiées ici sont toutes libres ou open source. De plus, l'offre open source de supervision est très mature. De nombreuses solutions de supervision libres sont utilisées couramment au sein de nombreuses D.S.I.[2] à travers le monde.

La supervision est un élément essentiel aux métiers de l'administration systèmes et réseaux. Elle peut s'orienter vers une supervision de parcs composés principalement de postes de travail, ou encore de serveurs, ou encore réseaux, ou tout à la fois.

C'est cette dernière possibilité qui intéresse Alter Way Solutions, et plus particulièrement le service infogérance dont je fais partie.

Il est primordial de mettre en place une solution de supervision qui fournit les indicateurs permettant de justifier les niveaux de services liés aux contrats d'infogérance. Mais la solution en elle-même ouvre la voie vers des offres commerciales supplémentaires, comme proposer des options supplémentaires aux contrats d'infogérance, ou encore des prestations d'audit pour des missions d'expertises, ou de la supervision pure...

Guide de lecture

Cette signalisation sera utilisée pour les remarques qui relèvent un point positif ou une action bénéfique au projet

Cette signalisation sera utilisée pour les points qui auraient été traités différemment si cela était à refaire

Cette signalisation sera utilisée pour les remarques qui relèvent un point négatif ou qui ont causé des problèmes

Cette signalisation sera utilisée pour les remarques qui relèvent d'une exception ou d'un point à mettre en avant

1 Service Level Agreement - Document qui définit la qualité de service requise entre un prestataire et un client
2 D.S.I. - Direction des Systèmes d'Information – il s'agit de la direction des services informatiques la plupart du temps.

2. Remerciements

Je tiens, dans un premier temps, à remercier grandement Mr Frédéric Vast, Directeur de la filière informatique et enseignant au CNAM de Lille, pour m'avoir accompagné durant tout mon cursus CNAM. Il s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire.

Je remercie Mme Véronique Torner et Mr Philippe Montarges, co-fondateurs et co-présidents du groupe Alter Way, ainsi que Mr Stéphane Vincent, Directeur Général des activités Consulting, Creative et Solutions.

Je tiens également à remercier vivement Mr Vincent Vignolle, Responsable de l'offre Continuity qui intègre le service infogérance dans lequel j'ai pu réaliser mon projet. Il a su croire en ce projet et m'a fait confiance pour le mener à bien.

Je remercie aussi tous les membres de ce jury, dont Madame Élisabeth Métais qui me fait l'honneur de le présider.

Merci à tous mes collègues d'Alter Way Solutions, et plus particulièrement à ceux du service infogérance qui ont mis toute leur bonne volonté pour participer à ce projet et ont assuré le bon fonctionnement de la solution de supervision au quotidien, sans oublier bien sûr mes autres collègues du pôle Continuity pour leur bonne humeur.

Je remercie la communauté Monitoring-FR, association dédiée au monde de la supervision libre et open source, qui est une source d'informations intarissable.

Et enfin, merci à mon épouse, pour son soutien et sa patience tout au long de mon cursus CNAM, mais aussi pour avoir relus ce mémoire.

3. Présentation d'Alter Way Solutions

3.1. Le groupe *Alter Way*

Le groupe Alter Way se définit comme un opérateur de service opensource et peut être considéré comme un des leaders en France.

Créé en 2006 par ses coprésidents actuels, Véronique Torner et Philippe Montarges, le groupe a connu un développement permanent de son activité, grâce à de la croissance organique combinée à de la croissance externe.

Alter Way a fédéré des acteurs historiques de l'Open Source et du Logiciel Libre Français complémentaires autour d'une vision à long terme de l'évolution de l'écosystème libre.

7 sociétés de service en logiciels libres (SSLL) complémentaires ont permis de proposer un accompagnement global d'un projet informatique avec des solutions libres et opensource.

Voici les entités qui ont intégrées le groupe Alter Way :

ANASKA : société spécialisée dans la formation de technologies libres.

ECLIP'S SOFTWARE : solutions ouvertes d'administration et de configuration des services DNS et DHCP

INGENIWEB : solutions Web d'entreprise spécialisée dans le langage Python.

KANOPEE : développement php[3]

NEXEN SERVICES : hébergement web à valeur ajoutée

O4DB : décisionnel et base de données

SOLINUX : développements spécifiques, infogérance système et intégration d'outils middleware

Illustration 1 : Historique du groupe Alter Way – Source Alter Way

Afin de renforcer son offre globale et de soutenir sa stratégie de développement sur le web, Alter Way a également intégré l'agence de communication Reciprok, spécialisée en conseil en communication, studio graphique et web-marketing.

3 PHP : Hypertext Preprocessor est un langage de scripts libre principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP

Via ces diverses acquisitions, Alter Way a mis en place une offre industrialisée à 360° qui repose sur 5 activités complémentaires permettant d'accompagner les clients d'amont en aval.

Voici comment se sont réparties, regroupées et organisées les structures initiales :

Les sociétés Eclip's Software, Ingeniweb, Kanpopee, O4db et Solinux ont fusionné pour créer l'entité Alter Way Solutions.

Anaska est devenue Alter Way Formation

Nexen Services est devenue Alter Way Hosting

Reciprok est devenue Alter Way Creative

Et l'entité Alter Way Consulting est composée d'experts issus ou non de chaque entité.

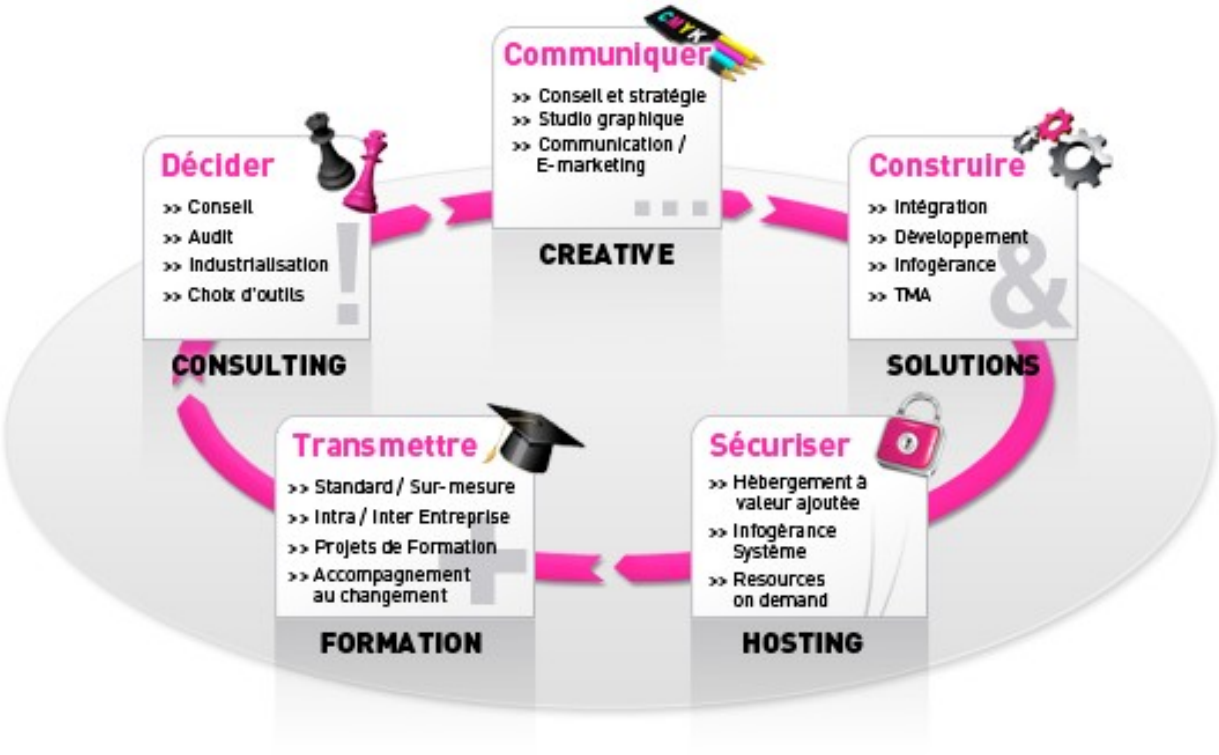


Illustration 2 : L'offre à 360° d'Alter Way – Source Alter Way

Le groupe Alter Way est bâti sur 3 piliers fondateurs :

L'expertise : Une équipe de consultants reconnus pour leur expertise et leur implication au sein des communautés libres. Certaines sociétés acquises sont fortes de plus de 10 ans d'expérience dans le domaine des logiciels libres, soit au tout début de l'apparition d'entreprises spécialisées dans le secteur du logiciel libre.

L'innovation : Un investissement fort et continu dans les dernières avancées technologiques. Une veille constante est fournie par les équipes qui sont des passionnés de logiciels libres. Et de nombreuses contributions sont reversées aux applications libres auxquelles les membres d'Alter Way participent.

L'industrialisation : Une réponse industrielle globale fournit par un seul et même interlocuteur grâce à l'offre à 360°. L'expertise du groupe Alter Way permet de proposer à ses clients des projets cadrés grâce à des méthodes et processus éprouvés.

Le Groupe Alter Way ne se veut pas être un simple intégrateur de solutions libres et opensource.

Le groupe s'inscrit dans une démarche fortement participative envers la communauté libre et opensource en investissant massivement dans l'écosystème libre.

Alter Way est par exemple le partenaire Français de la société Canonical, éditrice de la célèbre distribution GNU/Linux Ubuntu et en assure le support auprès des entreprises Françaises.

Le groupe Alter Way **contribue** fortement aux communautés libres.

Il fait parti de pôles de compétitivité basés sur l'**innovation**, et fait la **promotion** des logiciels libres à travers des conférences, des associations...

Toutes ces activités l'ont amené à créer des **partenariats** forts avec les acteurs stratégiques du monde libre et opensource.

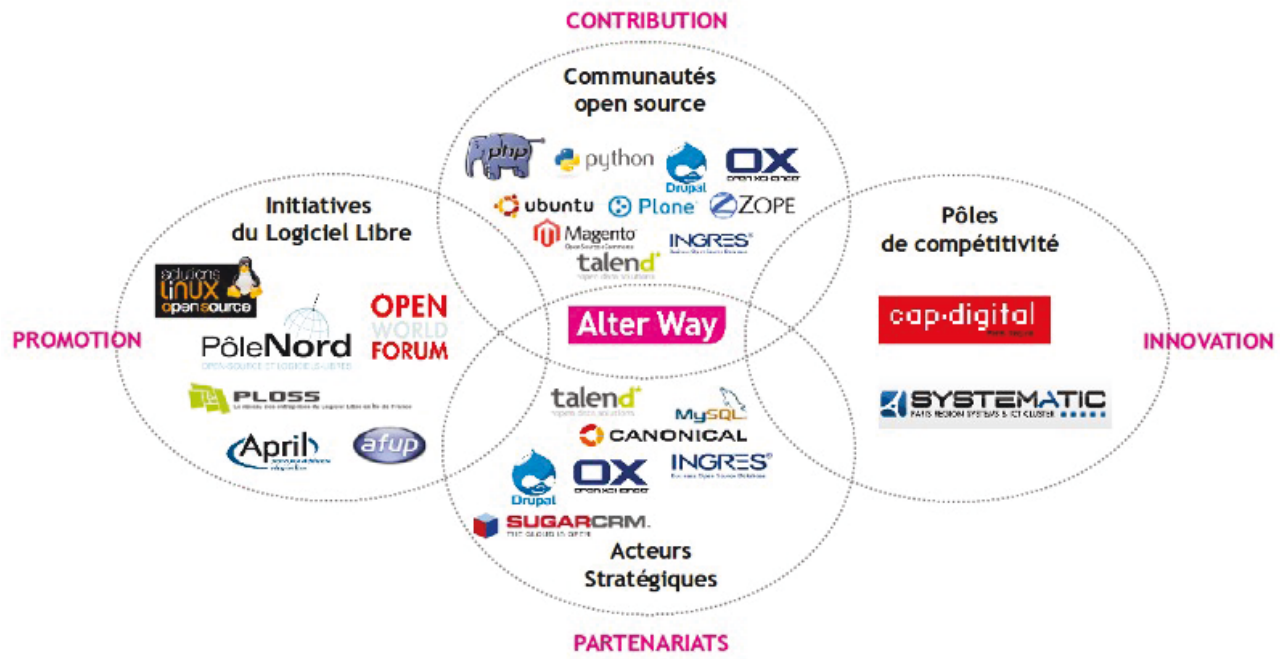


Illustration 3 : Alter Way - Acteur des logiciels libres – Source Alter Way

De nombreux salariés d'Alter Way sont engagés dans différentes communautés Libres et Open Source (PHP, Python, Ingres, OpenXchange, Zope, Plone, Talend…)

Par exemple, le président de l'AFUP (Association Francophone des Utilisateurs de PHP) est Jean-Marc Fontaine, membre d'Alter Way Consulting.

Le responsable de la communauté francophone de Ingres est Hervé Leclercq, notre

directeur technique.

Certains membres de l'entreprise font des conférences pour partager leur expertise dans des domaines précis.

L'implication des membres d'Alter Way est tout aussi diverse qu'active.

Ces participations se matérialisent par l'organisation de conférence, la mise à disposition de programme sous licence libre, la rédaction de livres et articles de presse...

Illustration 4 : Alter Way - Matérialisation des contributions – Source Alter Way

Des chiffres :

11 M€ de Chiffre d'Affaires

10 % de croissances

125 collaborateurs

Des agences à Paris, Saint-Cloud, Lille et Peronne

Illustration 5 : Alter Way - des chiffres – Source Alter Way

Des références :

Alter Way propose ces services dans tous les secteurs d'activité, et avec tous types d'entité, petites entreprises comme grands comptes, mais aussi l'administration Française.

Voici une liste non-exhaustive des différents clients d'Alter Way :

Illustration 6 : Alter Way - Nos références – Source Alter Way

Le groupe Alter Way est sollicité pour des projets d'envergure nationale et internationale.

Pour donner un exemple lié à une actualité récente, c'est Alter Way Hosting qui a hébergé le site internet des primaires du Parti Socialiste. Le site a connu 2 à 3 millions de visites le dimanche 09 octobre 2011, lors de la journée du premier tour.

Il y avait donc de fortes contraintes événementielles de disponibilité et de performances.

Voici une présentation plus détaillée de chaque activité.

3.2. Alter Way *Consulting*

Les fonctions principales d'Alter Way Consulting sont le conseil, l'audit, l'industrialisation ou encore le choix d'outils.

Notre Ambition	Apporter une contribution décisive aux **projets de changement et d'innovation** Éclairer les **choix technologiques** **Lever les freins** rencontrés dans l'utilisation de solutions open source
Nos Consultants	**Experts** dans leur domaine Reconnus par leur **communauté** Praticiens des 4 pôles d'Alter Way, **tous référents dans leur spécialité**
Nos Missions	**Tous les aspects d'un projet IT** : de la conception d'architecture à l'audit de performances Pour un **nombre étendu de technologies** **Industrialisation**
Nos principes d'intervention	**Collaboration souple et non intrusive** : vous restez maître de vos outils, nous vous apportons les informations utiles pour décider et agir **Démarche méthodologique éprouvée :** garante de l'application pertinente de notre expertise technologique

3.3. Alter Way *Créative*

Alter Way Créative est une agence de communication orientée web et divise son activité sur 3 grands axes.

Illustration 7 : La palette Alter Way Créative – Source Alter Way

3.4. Alter Way *Hosting*

Alter Way Hosting est expert en hébergement web via des outils opensource depuis plus de 10 ans et propose :

- L'hébergement et l'infogérance d'architectures complexes
- Des solutions de virtualisation pour consolider les plate-formes
- La possibilité de déploiement événementiel
- Une plate-forme E-Commerce à haute-disponibilité

Les 2 grands axes d'Alter Way Hosting sont :

Hébergement à forte valeur ajoutée	Infogérance
• Infrastructure multi-datacenters multi-utilisateurs • Virtualisation d'infrastructures • SaaS • Hébergement dédié • Stockage • Ressources à la demande / Private Cloud • PCA[4]/PRA[5]	• Conseil • Migration et déploiement • Supervision applicative complète • Administration • Assistance 24/7 • Disponibilité 99,8 % • Engagement de services (GTI[6] / GTR[7])

3.5. Alter Way *Formation*

Alter Way Formation est spécialisée dans les formations en logiciels libres, mais aussi en méthodologie de travail.

120 formations standards sont proposées dans leur catalogue.

Les formations proposées se distinguent en 3 branches différentes :

Métiers : Formations à la gestion de projets, à la conception de cahier des charges, à l'accompagnement au changement...

Méthodologie : Programmation orientée objets - les concepts, Modélisation UML pour la maîtrise d'ouvrage, ITIL – Fondation v3...

Technologie : Linux, Samba, PHP, Python, Drupal, EZ-Publish...

4 PCA Plan de Continuité d'Activité : document stratégique, formalisé et régulièrement mis à jour, de planification de la réaction à une catastrophe ou à un sinistre grave (http://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9)
5 PRA Plan de Reprise d'Activité : permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation. (http://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activit%C3%A9_%28informatique%29)
6 GTI – Garantie de Temps d'Intervention
7 GTR – Garantie de Temps de Rétablissement

Alter Way Formation propose des formations inter-entreprise, intra-entreprise ou encore sur mesure en France et à l'étranger.

Certaines formations proposées sont certifiantes comme pour le langage de développement PHP, ou encore les systèmes de Gestion de base de données Ingres[8], Mysql[9]...

3.6. Alter Way Solutions

Il s'agit du pôle d'intégration du groupe Alter Way, regroupant les activités Consulting, Creative et Solutions et concentrant plus de la moitié des effectifs du groupe (70 collaborateurs à ce jour).

Alter Way Solutions fournit à la fois des prestations d'intégration de solutions applicatives et de solutions d'infrastructure.

Voici un schéma représentatif des méthodes et compétences d'Alter Way Solutions :

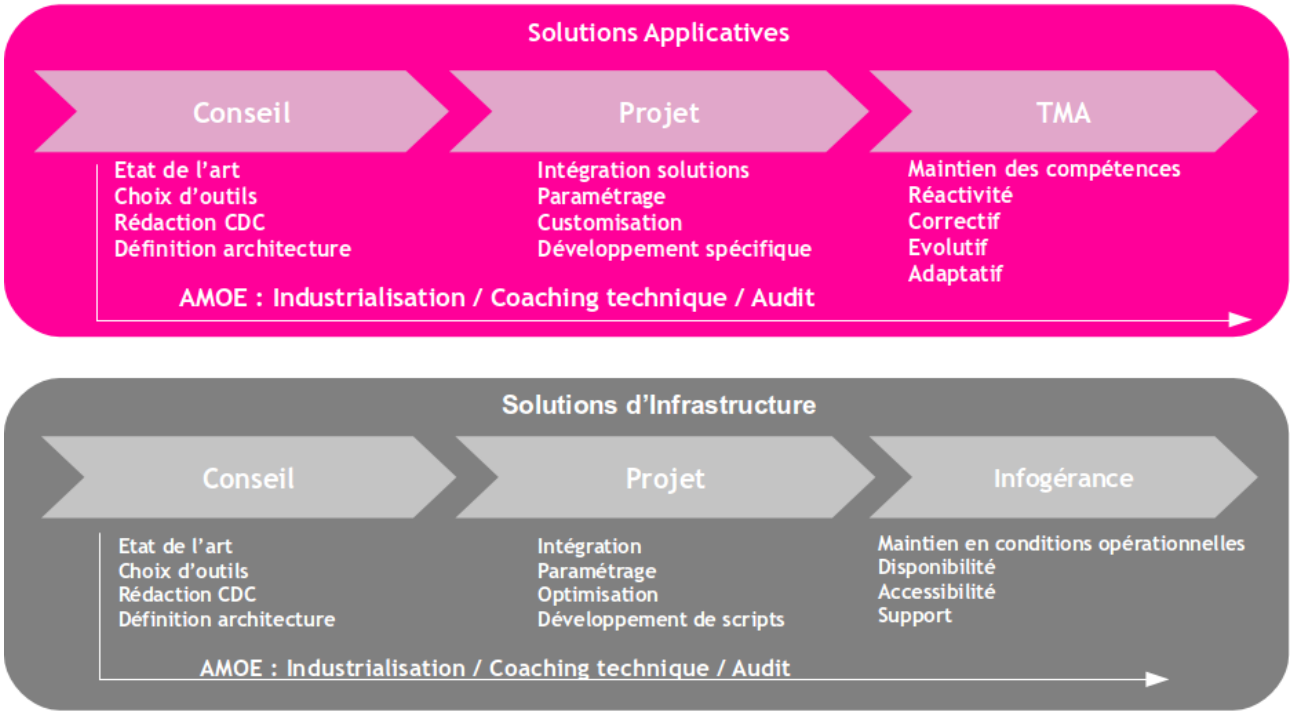


Illustration 8 : Méthodes et compétences Alter Way Solutions – Source Alter Way

Les solutions applicatives peuvent bien sûr fonctionner sur des solutions d'infrastructures mise en place par nos soins.

Dans tous les cas, on retrouve toujours la même démarche globale et industrialisée.

8 Ingres – Système de Gestion de Base de Données Relationnel, il est désormais sous licence libre
9 Mysql – Système de Gestion de Base de Données Relationnel sous licence libre

Ci-dessous un panel représentatif mais nullement exhaustif des composants open source sur lesquels Alter Way Solutions a su développer au fil des ans une expertise reconnue.

Technologies Applicatives :

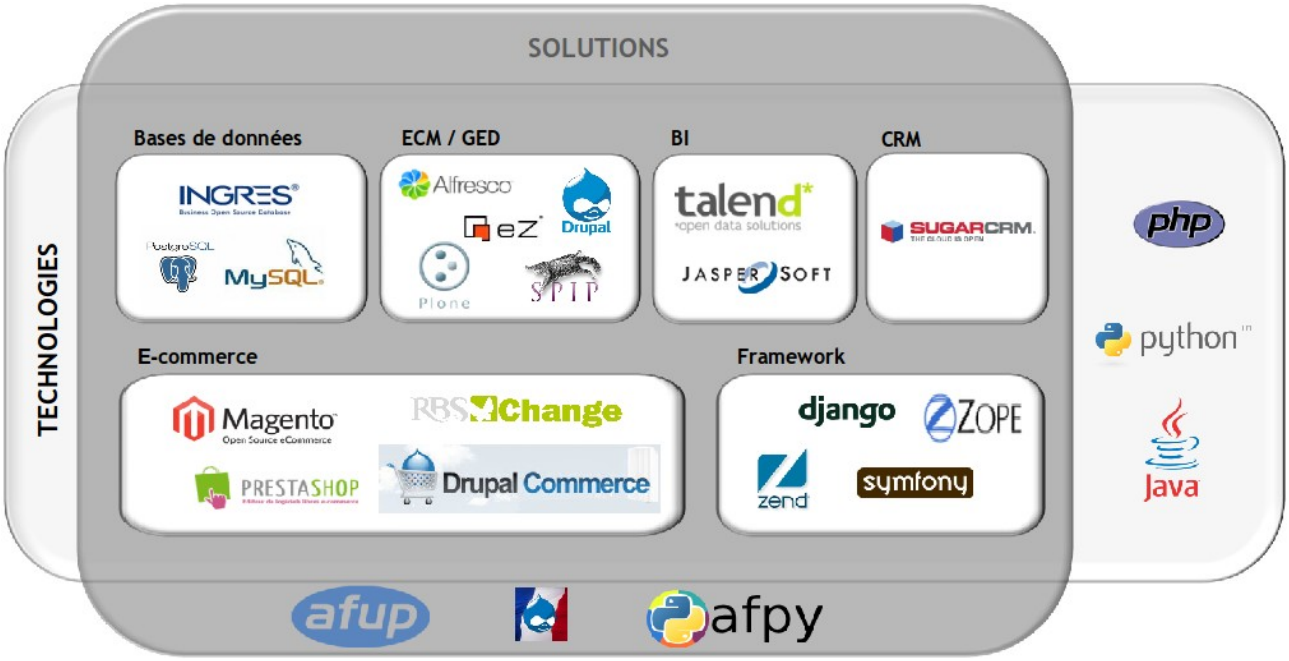


Illustration 9 : Alter Way Solutions - Nos technologies applicatives – Source Alter Way

Technologies Infrastructure :

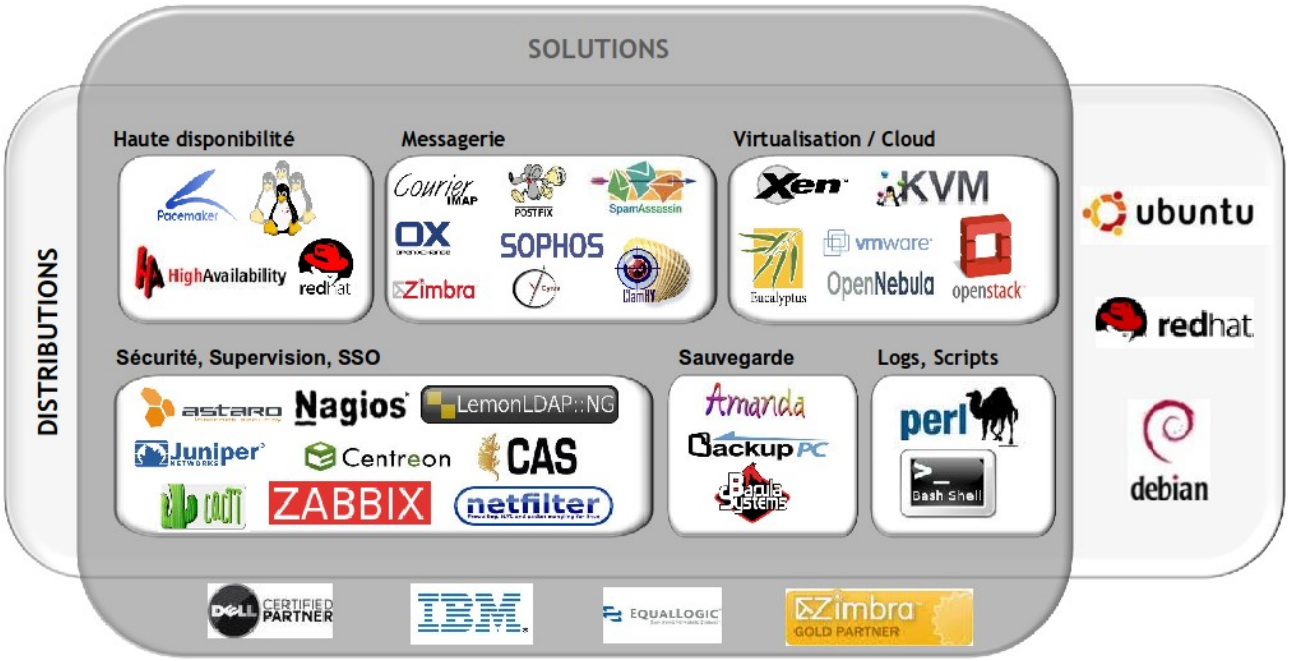


Illustration 10 : Alter Way Solutions - Nos technologies infrastructure – Source Alter Way

3.7. Alter Way Continuity

Le pôle Continuity est un pôle intégré à Solutions qui contient toutes les activités récurrentes d'Alter Way Solutions et qui va accompagner les projets durant leur cycle de vie.

On y retrouve :

- La TMA (Tierce Maintenance Applicative) en ce qui concerne le développement, comme la correction d'anomalies, la mise en place d'améliorations mineures…
- L'infogérance pour tout ce qui touche à l'infrastructure, du poste clients aux serveurs…

3.8. Ma mission au sein d'Alter Way Solutions

J'exerce mon activité actuelle au sein du pôle infogérance.

Je suis Administrateur Systèmes et Réseaux et assure des fonctions de niveaux 2 et 3 où j'apporte toute mon expertise en solutions libres.

Mon métier consiste en l'administration de serveurs, de réseaux, de firewall, d'architecture haute-disponibilité, de messagerie, d'hébergement web...

Ma mission consiste également à industrialiser les processus métiers afin d'améliorer la qualité du service rendu et la productivité.

Le fait d'être dans un service d'infogérance fournit par définition des environnements divers et variés.

Les architectures sont souvent multi-sites avec des règles de gestion du S.I. spécifiques à chaque entreprise.

On retrouve également des systèmes hétérogènes aux âges différents.

Les clients d'infogérance vont de la TPE et leur réseau de type LAN, aux grands groupes internationaux et leurs réseaux WAN alliant des contraintes de sécurité fortes.

En rapport avec ce projet, il m'a été demandé :

- D'étudier les solutions libres de supervision systèmes et réseaux et d'en réaliser un référentiel
- De mettre en place une solution de supervision couvrant tous nos besoins et qui soit évolutive
- De suivre le projet, et de réaliser la documentation associée.

4. Concepts de l'open source et des logiciels libres

Il est nécessaire pour une bonne compréhension de ce mémoire d'avoir une bonne perception de l'open source et des logiciels libres.

4.1. Les logiciels libres

4.1.1. Les prémices

Jusque dans les années 1970, les logiciels étaient plus ou moins libres d'être étudiés, utilisés, modifiés, du moins à l'intérieur du cadre universitaire, suivant ainsi la logique des sciences en général. Ce n'était pas forcément lié aux lois en vigueur, mais aucun intérêt commercial ne s'y opposait puisque seules de grosses compagnies pouvaient acheter des ordinateurs et les logiciels associés. Elles avaient tout intérêt à permettre la création de communautés de développeurs pour favoriser l'amélioration du logiciel (qui était donc leur propriété).

Autrement dit, le peu de personnes compétentes et la structure du marché pour lequel était utilisé le logiciel le rendait plus ou moins libre dans les faits.

C'est dans ce contexte, dans les années 80, qu'un programmeur de système d'exploitation au Massachusetts Institute of Technology (MIT), un certain Richard Stallman, commence à constater des restrictions des possibilités d'utilisation. Il se trouve face au problème éthique de devoir développer des logiciels dont l'utilisation sera restreinte, qui ne pourront pas être partagés en raison des droits du propriétaire du logiciel (souvent distinct du créateur). Stallman commença à constater ces restrictions en présence de programmes sur lesquels il ne pouvait intervenir, un pilote d'imprimante notamment. Robert Sproull aurait refusé de lui fournir le code source en raison d'un contrat de non divulgation que Xerox avait passé avec lui, pratique encore peu courante a l'époque.

Bien qu'anecdotique, cette petite histoire est souvent prise comme étant le point de départ de l'informatique libre, puisque c'est à partir de là, semble-t-il, que ce Richard Stallman consacrera son énergie à résoudre ce problème de conscience, ce qui fera de lui le premier et le plus emblématique des ambassadeurs du logiciel libre.

Un mouvement social s'est petit à petit constitué pour faire évoluer les droits que les utilisateurs ont sur le logiciel afin d'accéder à la libre circulation des informations dans ce domaine.

4.1.2. La naissance du logiciel libre

Voici le déroulement d'événements clefs qui expliquent la création du concept du logiciel libre et du mouvement associé.

En 1984, Richard Stallman lance le projet GNU (acronyme récursif de GNU's Not UNIX)

Le projet GNU a pour objectif de fournir un système d'exploitation libre qui reprend les concepts de fonctionnement du système de type UNIX.

En 1985, Richard Stallman crée la FSF (Free Software Fondation) qui permet de fournir une structure légale et financière au projet GNU.

La première définition de logiciel libre est née en 1986 par la FSF, encore une fois initiée par Richard Stallman.

En 1989, la première licence libre est née, il s'agit de la licence GNU GPL (General Public Licence)

La licence GPL v2 est apparue en 1991. Elle a été créée car la première version était trop restrictive, notamment pour l'utilisation de certaines bibliothèques.

La même année, la licence GNU LGPL a été conçue par la FSF. LGPL signifiait initialement GNU Library General Public License et signifie aujourd'hui GNU Lesser General Public License (Licence Publique Générale GNU Limitée) Ceci afin de limiter la confusion qui était de croire en la nécessité de déposer les librairies sous licence LGPL.

Le finlandais Linus Torvald a créé le noyau Linux également en 1991. Ce noyau était l'élément manquant à la création du système d'exploitation GNU, c'est à ce moment là qu'est né le système GNU/Linux.

C'est en 1994 que la première version de GNU/Linux a été officialisée.

En 1996, l'APRIL (Association pour la Promotion et la Recherche en Informatique Libre) a été créée. L'APRIL est une association Française qui a pour objectif de promouvoir et de défendre le logiciel libre. Elle agit aussi bien auprès du grand public, des entreprises, mais aussi des administrations. Elle dénombre à ce jour environ 5500 membres. (Personnes morales ou physiques)

Il y a eu également la création du système d'exploitation GNU/Hurd. Ce système d'exploitation utilise le noyau Hurd qui a été créé par la FSF.

En 1998, est créé la licence BSD (Berkeley software distribution). Elle permet de réutiliser tout ou partie du logiciel sans restriction. Cela veut dire que ce qui a été placé sous licence BSD peut être intégré dans un logiciel libre ou un logiciel propriétaire.

La version originale de la licence BSD incluait une clause de publicité particulièrement contraignante qui obligeait la mention du copyright dans toute publicité ou document fourni avec le logiciel. En 1999 cette clause a été retirée.

L'AFUL, Association Française des Utilisateurs de Logiciels Libres a été créée également en 1998.

En 2000 a été créée la GFDL v1.1 - GNU Free Documentation License, qui est une licence libre pour les documentations (À savoir qu'elle n'est pas compatible GPL)

Il y a également eu la création de la Licence Art Libre (LAL). Il s'agit d'un contrat juridique qui applique le principe des licences libres à la création artistique et au-delà, pour toutes productions de l'esprit régies par le droit d'auteur.

En 2001, Wikipedia a vu le jour. Il est inspiré de la logique des logiciels libres. (Collaborative et intelligence collective)

En 2002, la GFDL a été mise à jour pour devenir la version 1.2

En décembre 2002 sont apparues les licences Creative Commons, il s'agit d'un ensemble de licences qui régissent les conditions de réutilisation et/ou distribution d'œuvres

En janvier 2004, l'UNESCO élève le logiciel libre au rang de patrimoine mondial de l'humanité et confère à GNU la valeur symbolique de « Trésor du monde ».

Afin de combler un vide juridique en France en 2004, la licence CeCILL (CEA CNRS INRIA Logiciel Libre) a été créée. Elle peut être considérée comme une transposition de la GNU GPL compatible avec le droit Français.

En 2005, une nouvelle version de la CeCILL a vu le jour. Cette fois les évolutions ont été discutées avec la FSF, l'April et l'AFUL.

La même année, la société RedHat est apparue au NASDAQ avec un revenu de plus de 650 Millions de dollars et 2800 employés.

En 2007 est sortie la dernière licence GPL qui est la v3.

Une mise à jour de la licence Art Libre a été réalisée pour assurer une meilleure protection juridique aux auteurs.

Actuellement, il existe 43 licences libres compatibles GNU GPL.

Même les logiciels libres sont connus depuis peu du grand public et dès fois depuis peu par le monde de l'entreprise, le mouvement du logiciel libre est fort d'environ 30 ans d'existence.

On peut justement déterminer 3 périodes de 10 ans chacune :

- Les 10 premières années (1980-90) étaient connues principalement des universitaires
- Les 10 années suivantes (1990-2000), des offres commerciales ont fait leur apparition et la communauté libre a grandit de manière exponentielle
- Les 10 dernières années (2000 à nos jours) le logiciel libre est arrivé à un stade de maturité pour de nombreuses solutions.

Voici une représentation graphique et chronologique de l'histoire du logiciel libre et de ses faits marquants :

Illustration 11 : Historique du logiciel libre

4.1.3. Les fondements du logiciel libre

Pour qu'un logiciel soit libre, il doit fournir 4 libertés, numérotées de 0 à 3 :

- Liberté 0 : la liberté d'utiliser le logiciel
- Liberté 1 : la liberté de l'étudier et de l'adapter
- Liberté 2 : la liberté de redistribuer le logiciel de manière gratuite ou payante)
- Liberté 3 : la liberté d'améliorer et d'en faire profiter au public.

Ces 4 libertés ont permis de créer une dynamique forte autour des logiciels libres et ont ouvert la voie à l'intelligence collective.

De nombreux développeurs vont donner de leur temps de manière bénévole pour créer des logiciels, ce qui va permettre de fournir une puissance de développement exponentielle...

Des communautés vont se créer autour de logiciels libres et vont petit à petit s'organiser pour structurer leurs travaux, les évolutions... Comme on pourrait le voir dans le monde de l'entreprise.

Les entreprises justement participent également aux communautés, certaines entreprises ont d'ailleurs été créées suite au succès rencontré par leur logiciel libre.

Nagios, dont je vais parler ici, en est un très bon exemple. Une société a été créée autour de cette solution de supervision.

Les communautés de logiciels libres et leurs membres vont tester les solutions et souvent en remonter d'éventuels rapports d'anomalie. Il arrive souvent aussi que les utilisateurs soumettent des propositions d'améliorations, on retrouve souvent des forges d'idées[10].

Les membres vont aussi souvent créer de la documentation autour des solutions.

Qu'elles soient conceptuelles ou opérationnelles, on en retrouve sur tout type de support web comme les sites officiels des solutions, des wikis, des blogs...

Mais on retrouve aussi des écrits plus conventionnels avec des livres qui sortent en librairie pour les solutions les plus populaires.

On va retrouver des communautés autour d'une solution libre et son écosystème, comme le système de gestion de contenu Drupal. Mais aussi par rapport à des domaines d'activité où cette fois plusieurs solutions « concurrentes » seront mises en avant par la communauté.

La communauté monitoring-fr en est un très bon exemple. Il s'agit d'une communauté dédiée à la supervision libre. Elle n'est donc pas simplement limitée à une solution, mais a une approche plus globale du domaine en question.

Tout n'est bien sûr pas parfait. Il arrive également que des projets s'arrêtent et que la communauté disparaisse.

Les projets étant souvent menés de manière bénévole en dehors du travail, la vie peut changer les priorités de chacun et il arrive que des projets disparaissent par manque de repreneur.

10 Les forges d'idées permettent de soumettre des propositions, celles-ci sont visibles de tous avec un système de vote permettant de choisir de manière démocratique les améliorations à prioriser.

Les raisons sont diverses et variées, mais il arrive aussi que des projets soient repris par d'autres personnes, encore une fois la physionomie du logiciel libre permet ce genre de choses.

4.1.4. Valeurs, éthique et formats ouverts

La philosophie du logiciel libre est porté par des valeurs nobles :

- Partage
- Bénévolat
- Passion
- Échange
- Transparence
- Liberté
- …

Le Logiciel libre est basé sur le partage : le partage du logiciel, mais aussi le partage de la connaissance. En effet, permettre à autrui de lire du code source lui permet d'acquérir des connaissances sur le logiciel mais aussi sur la façon de coder.

Les développeurs de logiciels libres sont souvent des passionnés, il faut être volontaire, et c'est très souvent fait de manière bénévole.

Un autre avantage de la fourniture des codes sources est la transparence. Les utilisateurs peuvent analyser le code source et vérifié qu'il n'y a pas de comportement caché.

Les logiciels libres mettent un point d'honneur à respecter les standards et les formats ouverts, ce qui favorise grandement l'interopérabilité.

Le fait d'utiliser les standards et formats ouverts est conforme à la philosophie libre dans le sens où cela permet de faciliter l'accès et la compréhension à tous.

Par exemple, le navigateur internet Firefox met un point d'honneur à respecter les standards du W3C[11]

Le respect des standards et des formats ouverts permet également de garantir l'accès aux données sur le long terme, soit plusieurs dizaines d'années, ce qui n'est pas le cas d'une solution exclusivement propriétaire.

> *Étude du CIGREF - Maturité et gouvernance de l'Open Source - page 18 :*
>
> *Les logiciels libres s'appuient sur des normes et des standards connus qui offrent la promesse d'un accès aux données sur de longues périodes, c'est pour cela que les entreprises s'y intéressent.*

11 W3C – World Wide Web Consortium – Entité qui définit les standards de l'internet.

4.1.5. Réalisation de logiciel libre

Voici une infographie expliquant comment sont réalisés les logiciels libres.

Cette illustration fait partie d'un document de sensibilisation aux logiciels libres créé et utilisé par l'APRIL pour sensibiliser et informer les non initiés.

Illustration 12: Réalisation d'un logiciel libre - Source APRIL

Cette illustration permet de montrer les interactions entre les programmeurs et les utilisateurs du logiciel libre. Cela démontre qu'un utilisateur peut contribuer à un logiciel libre sans compétence technique. Il suffit simplement de faire un retour au développeur pour qu'il corrige des bugs ou fournisse des améliorations.

Les contributions peuvent être de la documentation, de la traduction, de la promotion, la proposition de nouvelles fonctionnalités...

Il est intéressant de noter qu'il existe un cycle d'amélioration continu et c'est une des plus grandes richesse du logiciel libre.

4.1.6. Types de licences libres

4.1.6.1. Licences avec obligation de réciprocité dite copyleft

Tout logiciel utilisant du code obtenu sous une licence copyleft[12], devra, s'il est diffusé, l'être sous une licence équivalente.

Les licences GNU GPL ou encore son homologue Français CeCILL sont des licences dites copyleft.

4.1.6.2. Licences permissives dites non-copyleft

Ces licences n'imposent que des contraintes très faibles, et s'approchent grandement du domaine publique.

Il est, par exemple, possible de réaliser un logiciel propriétaire à partir de code publié sous une licence de ce type.

Les licences de type BSD, MIT et leur pendant Français CeCILL-B, en sont des exemples.

4.1.6.3. Licences pour composants logiciels

Il existe une troisième catégorie de licences, se situant entre les deux précédentes. Il s'agit de licences copyleft, mais qui autorisent à lier un programme tiers, quelle que soit sa licence, aux programmes qu'elles couvrent.

Ce type de licence est le plus souvent utilisé pour les bibliothèques, mais peut très bien s'appliquer à d'autres types de programmes.

La LGPL en est l'exemple le plus connu.

La licence CeCILL-C est l'homologue Français de la LGPL

4.2. L'open source

Open Source, en français Source Ouverte, définit une licence qui permet d'accéder aux sources d'un programme informatique.

La désignation open source s'applique aux logiciels dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire la possibilité de libre

12 Copyleft - Possibilité donnée par l'auteur d'un travail soumis au droit d'auteur (œuvre d'art, texte, programme informatique, etc.) de copier, d'utiliser, d'étudier, de modifier et/ou de distribuer son œuvre dans la mesure où ces possibilités restent préservées. http://fr.wikipedia.org/wiki/Copyleft

redistribution, d'accès au code source et aux travaux dérivés.

Souvent, un logiciel libre est qualifié d'« open source », car les licences compatibles open source englobent les licences libres selon la définition de la FSF.

Le terme open source est en concurrence avec le terme « free software » recommandé par la FSF.

4.2.1. Histoire

L'utilisation de la désignation Open Source a été suggérée par Christine Peterson du Foresight Institute afin de lever l'ambiguïté du mot anglais Free Software qui signifie libre au sens de « liberté » mais surtout « gratuit », et rappeler ainsi aux utilisateurs qu'un logiciel a un coût. Il s'agissait également de choisir un vocabulaire correspondant mieux au monde des affaires, le terme Free (gratuit) de Free Software risquant généralement d'inquiéter les entreprises.

L'introduction de la désignation Open Source n'a fait qu'ajouter une nouvelle ambiguïté, car cette désignation fut détournée du sens prévu, et appliquée à des logiciels ne respectant que le second critère, la disponibilité du code source. Eric Steven Raymond avait d'abord essayé de déposer Open Source. Sa tentative ayant échoué, il créa avec Bruce Perens l'Open Source Initiative, qui délivre le label « OSI approved » aux licences qui satisfont aux critères définis dans l'Open Source Definition, une adaptation des Free Software Guidelines du projet Debian.

L'OSI (Open Source Initiative) a été créé en 1998 suite à une division avec la communauté du logiciel libre. Les créateurs jugent les contraintes apportées par les licences libres inadaptées aux réalités économiques et techniques.

Le mouvement Open Source défend la liberté d'accéder aux sources des programmes qu'ils utilisent, afin d'aboutir à une économie du logiciel dépendant de la seule vente de prestations et non plus de celle de licences d'utilisation.

4.2.2. Les fondements de l'Open Source

Ci-dessous une traduction des conditions pour le logiciel afin d'être considérés par l'OSI :

- la redistribution libre

La licence ne doit pas empêcher quiconque de vendre ou de donner le logiciel en tant que composant d'une distribution de logiciels constitués de programmes provenant de différentes sources. La licence ne doit pas exiger de droits d'auteur ou d'autres commissions sur une telle vente.

- le code-source

Le programme doit inclure le code source, et autoriser sa distribution sous forme compilée aussi bien que sous forme de code source. Lorsqu'un produit n'est pas distribué avec son code source, il doit exister un moyen bien indiqué pour l'obtenir et sans autres frais qu'un coût raisonnable de reproduction, avec une préférence pour le téléchargement gratuit depuis l'Internet. Le code source doit être la forme privilégiée pour qu'un programmeur puisse modifier le programme. Il est interdit de proposer un code source rendu volontairement difficile à comprendre. Il est également interdit de soumettre des formes intermédiaires, comme le résultat d'un préprocesseur ou d'un traducteur automatique.

- les œuvres dérivées

La licence doit autoriser les modifications et les applications dérivées, et elle doit permettre leur distribution sous les mêmes termes que ceux de la licence du logiciel original.

- l'intégrité du code source de l'auteur

La licence ne peut restreindre la redistribution d'un code source sous forme modifiée seulement si elle permet la distribution de fichiers de correction (patch) avec le code source, dans le but de modifier le programme au moment du développement. La licence doit explicitement permettre la distribution de logiciels développés à partir de codes sources modifiés. La licence peut exiger que les applications dérivées portent un nom différent ou un numéro de version distinct de ceux du logiciel original.

- la non-discrimination contre des personnes ou groupes

La licence ne doit pas discriminer des personnes ou des groupes de personnes.

- la non-discrimination contre des champs d'application

La licence ne doit pas limiter l'utilisation du logiciel à un champ d'application particulier. Par exemple, elle ne doit pas interdire l'utilisation du logiciel dans le cadre d'une entreprise ou pour la recherche génétique.

- la distribution de licence

Les droits attachés au programme doivent s'appliquer à tous ceux à qui il est redistribué, sans obligation pour ces parties d'obtenir une licence supplémentaire.

- la licence ne doit pas être spécifique à un produit

Les droits attachés au programme ne doivent pas dépendre du fait qu'il fasse partie d'une quelconque distribution de logiciels. Si le programme est extrait de cette distribution et est utilisé ou distribué sous les termes de sa propre licence, toutes les parties auxquelles il est redistribué doivent bénéficier des mêmes droits que ceux accordés par la distribution originelle de logiciels.

- la licence ne doit pas restreindre d'autre logiciels

La licence ne doit pas imposer de restrictions sur d'autres logiciels distribués avec le logiciel licencié. Par exemple, la licence ne doit pas exiger que tous les programmes distribués sur le même support soient des logiciels open source

- la licence doit être neutre sur le plan technologique

Aucune disposition de la licence ne peut aller à l'encontre d'une quelconque technologie ou style d'interface.

4.3. Open Source et Logiciels Libres

Des Logiciels Libres sous licence copyleft sont Open Source, tandis que des logiciels Open Source peuvent ne pas être libres.

En pratique, la plupart des licences de l'Open Source satisfont aux critères de liberté de la Free Software Foundation, les différentes subtilités qui les distinguent étant principalement d'ordre philosophique et commercial.

La principale critique issue du mouvement parent du Logiciel Libre est le fait que l'Open Source ne communique presque exclusivement que sur une des caractéristiques techniques des logiciels (la liberté d'accès au fonctionnement du logiciel) en occultant les motivations premières dont elles sont issues, au risque de les perdre. Ils accusent l'Open Source d'être mû par la dynamique et les ressources financières et d'expertise de multinationales, l'opposant au Logiciel Libre mû par des idéaux d'ordre philosophique et politique.

Voici un graphique de répartition des licences libres et Open Source utilisées dans les projets hébergés sur SourceForge.net[13] :

Illustration 13 : Répartition des licences libres sur SourceForge en 2011

Cette recherche m'a été inspirée suite à celle effectuée par François Planque en 2004.

Il est intéressant de voir que 7 ans après la répartition est relativement similaire (en intégrant la GPLv3 aux résultats)

13 Sourceforge.net est un site hébergeant des projets libres et opensource qui fournit des services nécessaires à ces projets. Sourceforge.net représente aujourd'hui 315644 projets Open Source avec en moyenne plus de 2 millions de téléchargements par jour.

Illustration 14 : Répartition des licences libres sur SourceForge en 2004

4.4. Carte conceptuelle du logiciel libre

Voici une carte conceptuelle réalisée par René Mérou sous licence GFDL, vous la trouverez en annexe en plus grande version :

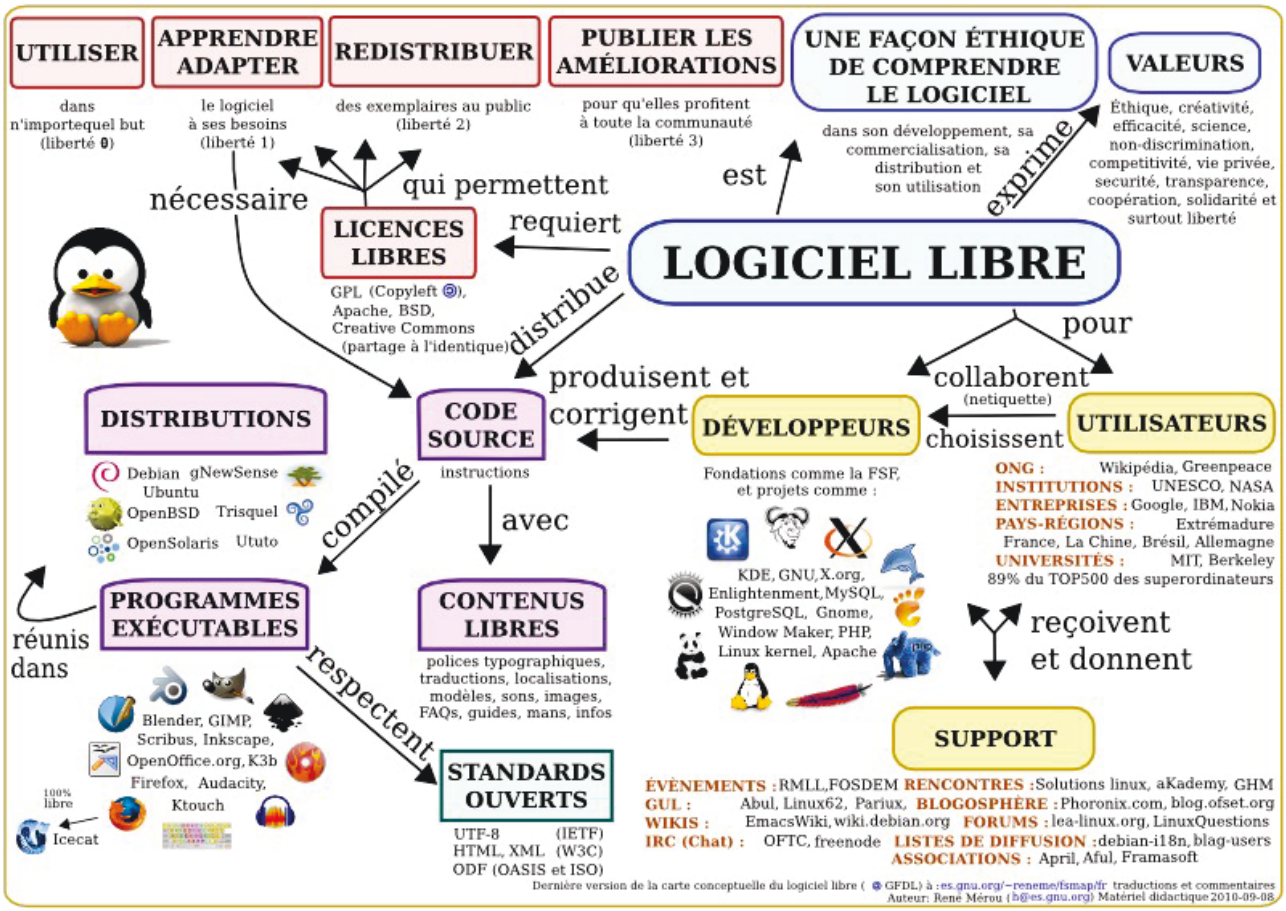


Illustration 15 : Carte conceptuelle du logiciel libre – Source René Mérou

4.5. Maturité des solutions opensource et libres

Une étude de Markess International 12 publiée en 2009 sur l'Open Source en France montre que 92 % des entreprises déclaraient y avoir fait appel.

Cette implantation va se matérialiser par l'utilisation de solution à moindre risque comme un navigateur internet, mais aussi par l'utilisation de solutions à haut risque, comme un ERP[14] qui est un élément central du Système d'Information et critique pour l'entreprise.

Dans son étude « Maturité et Gouvernance de l'Open Source » le Cigref propose 3 types de maturité :

La maturité technologique, qui est le ressenti qu'ont les entreprises au niveau technologique. (Performance, fiabilité, sécurité...)

La maturité d'usage, qui correspond à la perception d'utilisabilité des solutions open source et libres en fonction des besoins de l'entreprise.

La maturité de moyens, qui correspond à la capacité des entreprises à investir dans ces solutions libres.

Ces trois grands types de maturité sont basés sur la confiance des entreprises envers ces solutions et répondent respectivement aux questions suivantes :

Est-ce assez fiable et performant pour être intégré au S.I. ?

Est-ce que les fonctionnalités proposées répondent aux besoins ?

L'entreprise est-elle prête à investir pour mettre en œuvre ces solutions ?

L'enquête effectuée par le Cigref a porté sur 19 entreprises de différents secteurs d'activité et 270 solutions libres et opensource réparties en treize familles :

- Suites Bureautique
- Outils métiers
- Système d'exploitation
- Réseaux informatiques
- Gestion de données
- Administration
- Collaboratif
- Mobilité
- Développement
- Éducatif
- Sécurité
- Internet
- Middleware

Voici un extrait de cette étude et des graphes associés :

14 Enterprise Resource Planning – est un progiciel de gestion Intégré qui va fournir les principaux composants fonctionnels d'une entreprise, comme la gestion de production, commerciale, logistique, compatibilité...

LA MATURITÉ TECHNOLOGIQUE

La « maturité technologique » d'une solution Open Source correspond au niveau de confiance technologique pour une intégration dans un système d'information. Ce niveau de confiance technologique dépend de la qualité du développement, de la performance et de l'efficacité de la solution, du respect des normes et des standards, de l'existence d'interfaces programmatiques ou applicatives, de sa facilité d'intégration dans une architecture, etc...

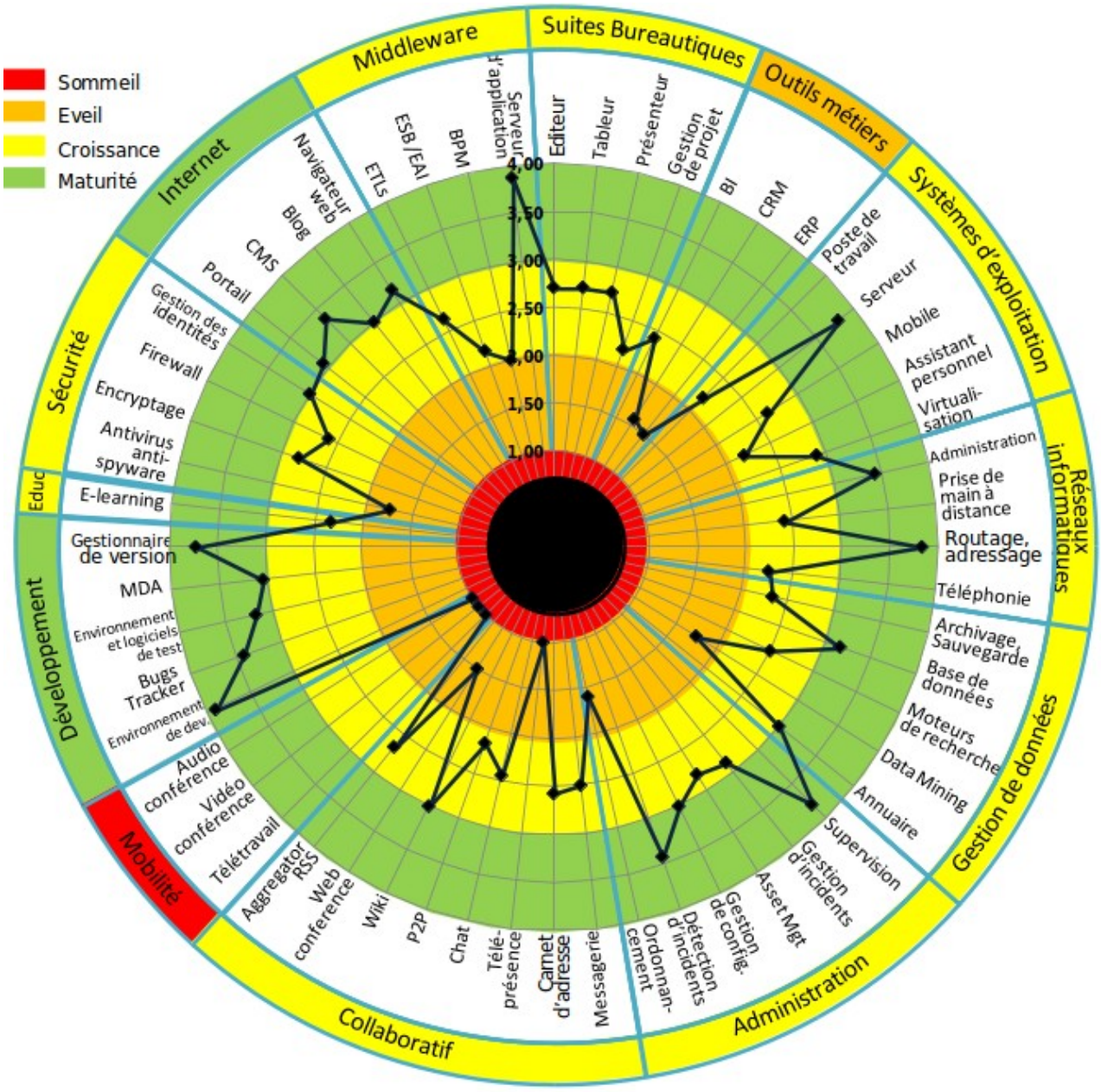


Illustration 16 : Résultats de l'évaluation de la maturité technologique - Source CIGREF

Des trois types de maturité que le CIGREF a mesuré, la maturité technologique est celle qui atteint les plus haut scores sur l'ensemble des familles.

LA MATURITÉ D'USAGE

La « maturité d'usage » correspond à la capacité qu'ont les outils Open Source à répondre aux usages des entreprises utilisatrices. Elle dépend de leur couverture fonctionnelle des besoins mais aussi de la facilité d'usage et de mise en œuvre par un utilisateur, de la qualité de la documentation associée, de la facilité de mise en œuvre d'un support adapté, et d'intégration (ergonomique, applicative...) parmi les autres outils de l'utilisateur, etc...

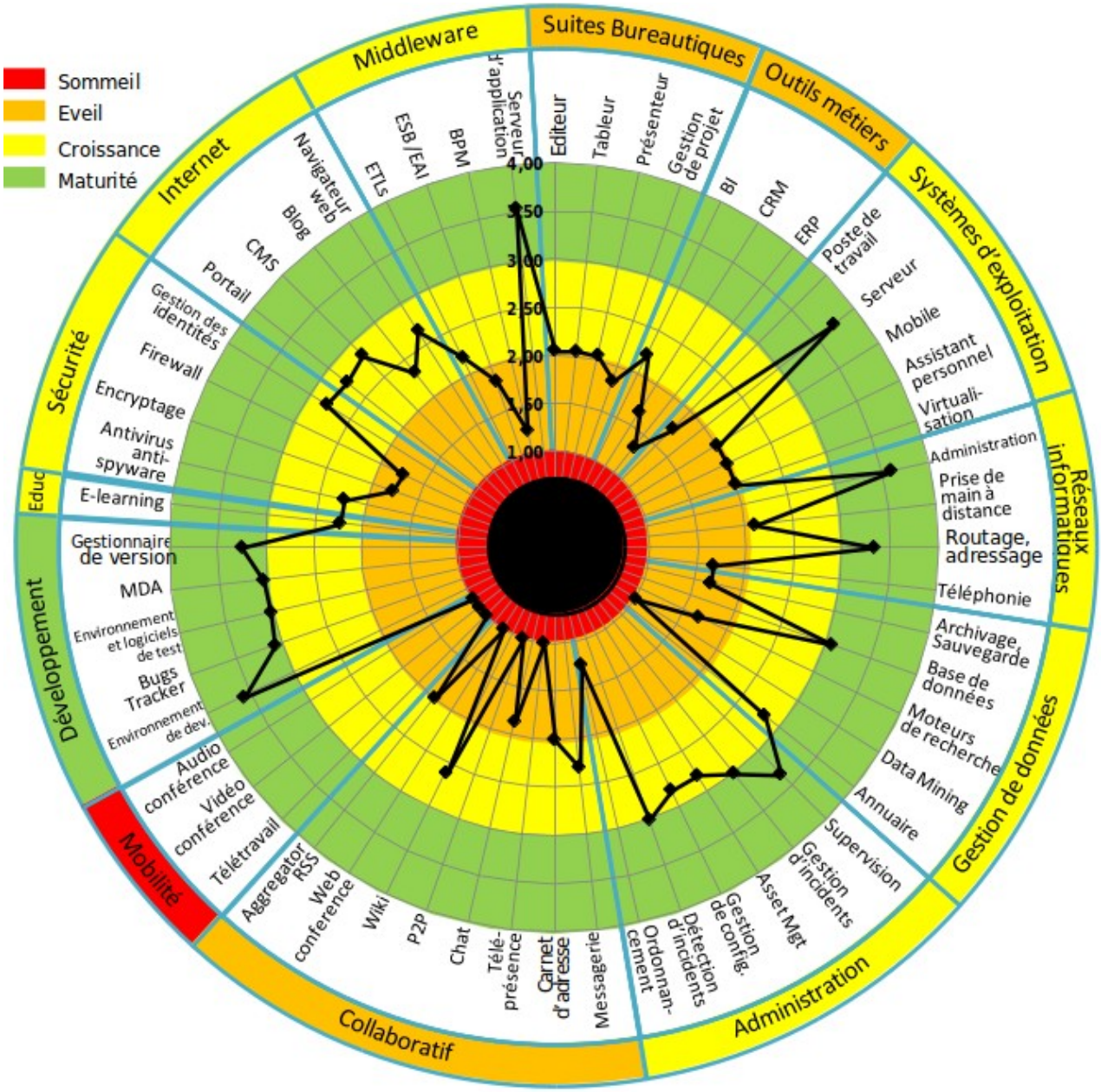


Illustration 17 : Résultats de l'évaluation de la maturité d'usage - Source CIGREF

La maturité d'usage est naturellement plus faible que la maturité technologique. Plus précisément, la maturité d'usage ne peut se développer que lorsqu'une certaine maturité technologique est atteinte, qui convainc les entreprises de tester l'usage du produit ou de l'outil.

LA MATURITÉ DE MOYENS

La « maturité de moyens » correspond au niveau de confiance que l'entreprise a dans une solution Open Source, pour y investir l'ensemble de ressources (financières, matérielles, compétences, etc.) nécessaires pour sa mise en œuvre au sein de son système d'information.

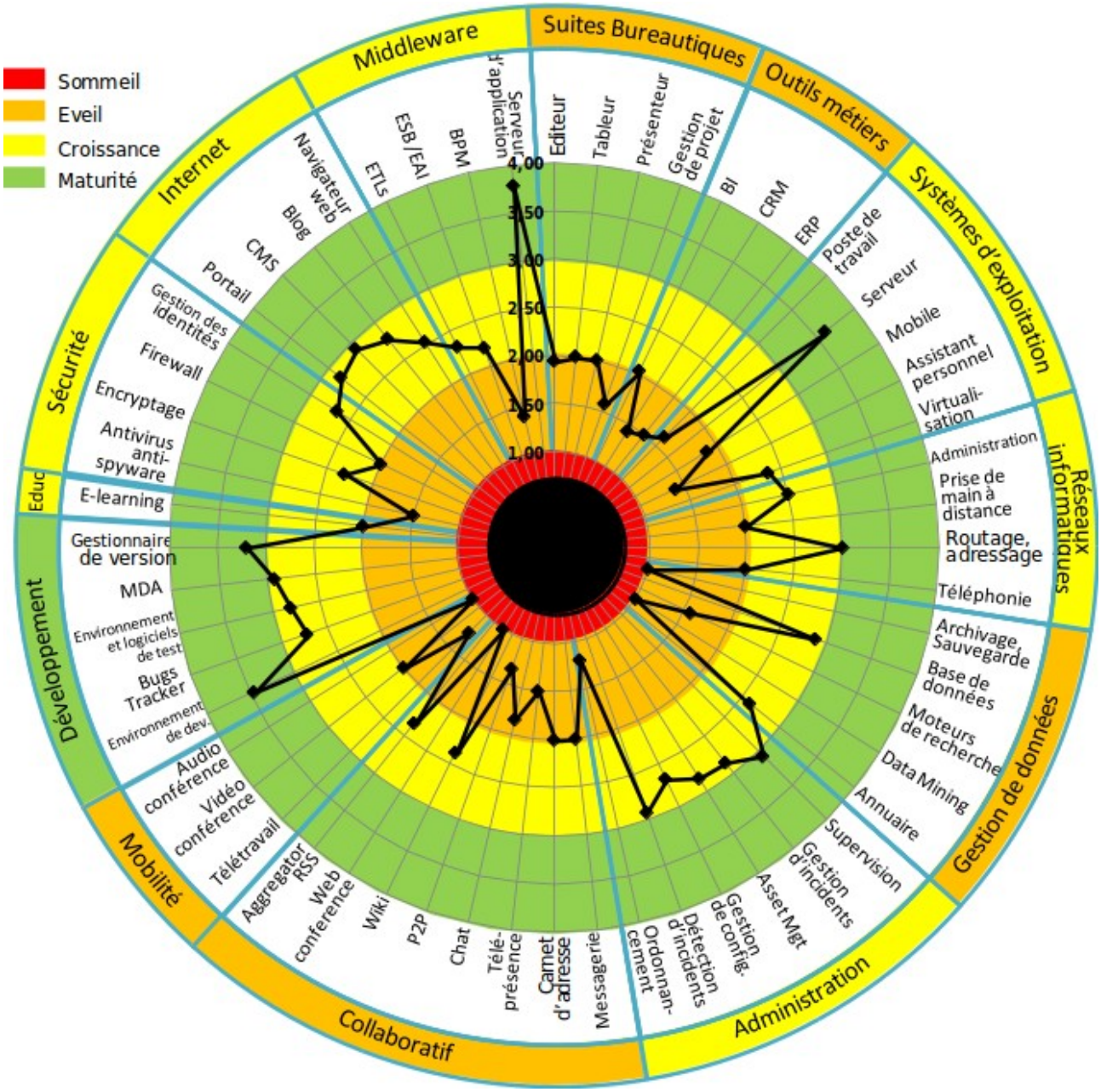


Illustration 18 : Résultats de l'évaluation de la maturité de moyens - Source CIGREF

La maturité de moyens des solutions Open Source est très proche de la maturité d'usage. Mais elle n'est pas forcément gage de qualité d'une solution.

Par exemple, l'investissement sera moindre, si le personnel est déjà formé à une solution, ou encore si celle-ci fonctionne si bien que le contrat de support n'exige pas un grand

nombre d'interventions...

L'étude du Cigref démontre que la confiance apportée aux solutions libres et opensource est bien ancrée en ce qui concerne la qualité technologique, mais la perception en terme d'usage et surtout de moyen a une certaine marge de progression.

Il est intéressant de voir quelles sont les familles les plus proches de la maturité technologique, d'usage et de moyens.

Il s'agit principalement de familles issues des services informatiques, développement, administration, réseau.

Alors que les familles portées sur les utilisateurs du S.I. comme la mobilité, le collaboratif, les outils métiers n'en sont pas encore au stade de la maturation.

La sous famille des systèmes d'exploitation est à souligner également, car considérée comme mature.

Enfin, on peut remarquer, que le sujet qui est traité dans ce projet, la supervision, est toujours classé comme mature.

L'étude CIGREF m'a permis de prendre du recul sur la vision dans les grandes entreprises des logiciels libres, en terme d'intégration, de maturité...

5. La supervision de système d'information

5.1. Définition et Concept

La supervision (monitoring en anglais) a pour rôle d'apporter de la **visibilité** sur l'état de son système d'information.

Elle permet la mise en place d'**action corrective** en cas d'incidents afin de rétablir le niveau de service souhaité dans les plus brefs délais, mais peut aussi permettre d'avoir une vision à moyen terme de l'état de ses ressources, facilitant la mise en place d'**action préventive** et de mesurer les performances de son système d'information en vue d'augmenter la satisfaction utilisateur.

Surveiller son système d'information fournit des indicateurs, remontant les **données qualitatives** ou **quantitatives** relatives à la **santé** de son système d'information.

La supervision au début était essentiellement vouée à la gestion technique de parc informatique, l'état du réseau, les taux d'occupations des ressources serveurs...

Puis elle a évolué au fur et à mesure en surveillant des services, des applications, en mesurant la disponibilité, les temps de réponses, pour arriver jusqu'à la surveillance de processus métiers. (BPM[15])

La supervision n'est donc plus seulement au service de la direction informatique en vue du maintien et de l'évolution du parc informatique, mais elle est désormais au service de tous les clients du système d'information.

15 Business Process Management

5.2. Types de supervision

5.2.1. Gestion d'incidents

La gestion d'incidents permet d'être alerté en temps réel d'un événement se produisant sur le système d'information en vue de sa remise en état afin de minimiser l'impact sur les clients du SI[16].

Avec l'analyse et le croisement des incidents remontés par la supervision, il est possible d'identifier plus facilement les problèmes (incidents récurrents selon les méthodes ITIL) de son système d'information.

5.2.2. Gestion des ressources

La gestion des ressources est l'analyse des données remontées par la solution de supervision. Elle a pour but de faciliter la gestion du parc et d'anticiper son évolution d'un point de vue matériel.

Par exemple, surveiller l'espace disque d'une machine va permettre d'anticiper une indisponibilité liée à une saturation de celui-ci. Ou encore, surveiller la consommation mémoire ou CPU va permettre d'anticiper le déplacement d'une application, ou de faire évoluer physiquement un serveur, détecter une consommation anormale comme pourrait l'être une attaque.

5.2.3. Gestion des performances

La gestion de performances est une surveillance sur la durée du système d'information.

Il s'agit de conserver un historique des données de performance afin de fournir des tableaux de bord avec des graphiques permettant une vision facile et évolutive de l'état de son système d'information.

La gestion des performances facilite la prise de décision.

Elle peut également être utilisée pour tester son système d'information.

Il est tout à fait envisageable de réaliser des tests de montée en charge et de connaître la capacité de son système d'information pour anticiper des pics.

Prenons l'exemple du site web d'une école d'Ingénieur, le site aura une consommation bien plus importante en période de résultat d'examen que le reste de l'année, les élèves cherchant à connaître leurs résultats vont réactualiser la page jusqu'à obtenir ces résultats.

Il est plus facile si l'on surveille les performances d'identifier ces pics et pourquoi pas proposer de la ressource en plus pour absorber la charge spontanée mais régulière.

16 Système d'informations

5.2.4. Gestion de la sécurité

La gestion de la sécurité permet de surveiller de manière centralisée la sécurité de son système d'information.

Le but étant de savoir facilement si on est victime de piratage ou simple tentative tout en identifiant les points faibles de son système d'information en vue d'une correction de ceux-ci.

Il est par exemple possible de surveiller via une seule interface les logs[17] des éléments de son parc informatique, tous les IDS[18] qui vont surveiller des types d'attaques...

On peut remarquer que pour tous les types de supervision, on retrouve toujours une notion d'amélioration continue comme on pourrait le retrouver dans les normes ISO ou encore les bonnes pratiques ITIL.

5.3. Les différents composants (niveaux) du système d'information

5.3.1. Matériel

La supervision matérielle consiste à récolter les informations relatives à son matériel.

On va par exemple récupérer l'état physique d'une machine, sa température, l'état de ses disques, si tous les ventilateurs sont fonctionnels...

Le but étant de remplacer le plus rapidement possible le matériel défectueux ou encore d'anticiper une future panne éventuelle, de faciliter la gestion des stocks de pièce de rechange.

5.3.2. Réseau

La supervision réseau est la surveillance et l'analyse de l'utilisation de son réseau ce qui revient entre autre à connaître le taux d'occupation de son réseau, le nombre de connexion simultanée...

Elle va permettre aussi de connaître précisément ce qui circule sur le réseau, les protocoles, leur répartition, les éléments qui consomment le plus de ressources, mais aussi la disponibilité des services rendus pas la DSI[19].

17 Logs – Les logs peuvent être considérés comme des journaux d'activité
18 Intrusion Detection System – Système de détection d'intrusion
19 Direction des Systèmes d'Informations

5.3.3. Système

La supervision système permet de surveiller le bon fonctionnement de ses systèmes d'exploitation.

Elle est orientée serveur et va fournir des informations sur l'utilisation des ressources comme l'espace disque, la présence de processus...

5.3.4. Applications et services

Les applications du système d'information sont de plus en plus supervisées. Il est notion ici d'accessibilité et d'utilisabilité, le but étant d'assurer au maximum une continuité de service et de mesurer les performances en vue d'accroître la satisfaction utilisateur.

5.3.5. Métier

Il s'agit ici de fournir une vue sur la mise à disposition de différents éléments interdépendants permettant, de manière globale, la réalisation de processus métiers propres à l'entreprise.

Ces vues ne sont à destination que des décideurs, managers...

Les éléments étant normalement supervisés, ces vues métier ne servent qu'à identifier les processus métiers affectés par telle ou telle panne à destination d'un non technicien.

Prenons l'exemple d'un magasin qui perds sa connexion internet car un élément réseau est saturé, les paiements par carte bancaire ne pourraient plus se faire.

Le décideur n'a pas d'intérêt à connaître la cause dans l'immédiat, mais il a besoin d'avoir une vue sur les processus métiers gênés par cette panne.

5.3.6. Clients

Quelle que soit le type de supervision, la finalité de la solution de supervision est liée aux clients du SI.

Ils doivent savoir que leurs services sont disponibles, en être satisfait, notamment en termes de temps de réponse, et la solution de supervision doit prendre en compte l'évolution du besoin des clients du SI et donc du SI lui-même.

Voici l'illustration des types de supervision intégrés avec les clients du SI, la lecture se fait de bas en haut :

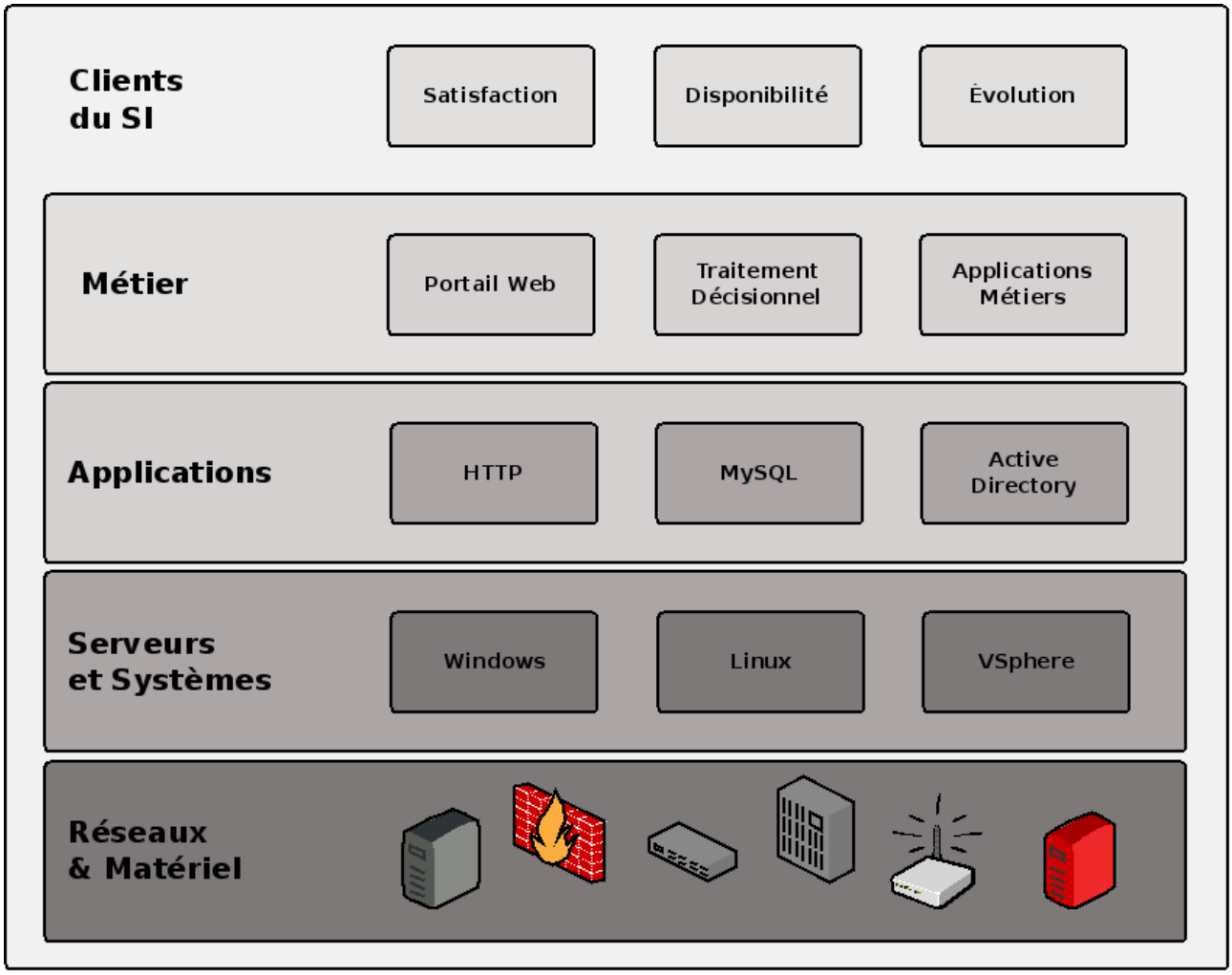


Illustration 19 : Les différents types de supervision

5.4. Les méthodes et standards de la supervision

Le monde de la supervision dispose de normes et standards facilitant l'interopérabilité des superviseurs et supervisés.

Ces normes et standards sont souvent gérés par la DMTF (Distributed Management Task Force) qui est une organisation regroupant plus de 160 entreprises et organisations dans 43 pays différents. Plus d'informations sur leur site web http://dmtf.org/about

Voici une présentation non-exhaustive des différentes méthodes d'interrogation d'élément.

5.4.1. Méthode de vérification

Il existe 2 méthodes de vérification pour une solution de supervision.

On va dire qu'elle est soit :

- Active : Lorsque la vérification est à l'initiative de la solution de supervision.

- Passive : Lorsque la vérification est à l'initiative de l'agent de supervision ou en réaction à un événement. Cette dernière peut être plus facilement tolérée par les responsables de la sécurité du système d'information étant donné qu'il s'agit de flux sortant uniquement.

5.4.2. SNMP – Simple Network Management Protocol

SNMP (Simple Network Management Protocol), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseaux de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

Le protocole SNMP est hautement déployé et permet, dans le cas de la supervision, d'interroger un équipement sur son état en temps réel.

Switchs, hubs, routeurs et serveurs sont des exemples d'équipements contenant des objets gérables via SNMP.

Via SNMP, il est possible de récupérer des informations matérielles, des paramètres, des données de performance par exemple le trafic d'une carte réseau.

Ces objets sont classés dans une sorte de base de données arborescente appelée MIB (« Management Information Base »).

Chaque équipement SNMP possède sa propre MIB basée sur un modèle commun.

Il est possible d'interroger un équipement disposant du SNMP, on retrouve ici le mode de fonctionnement actif.

Mais il est possible également de générer des Traps SNMP en cas d'événements qui se produisent sur l'équipement réseau. On retrouve ici le mode de fonctionnement passif.

5.4.3. Agents propres à la solution de supervision

De nombreuses solutions de supervision mettent à disposition des agents à installer sur les équipements à superviser, et ce sont ces agents qui vont remonter l'information auprès de la solution de supervision.

Ces agents peuvent aussi bien fonctionner de manière active ou passive.

5.4.4. Scripts

Il s'agit ici de scripts exécutés depuis la solution de supervision, adaptés à celle-ci pour tester des composants distants, comme faire un script pour déterminer la disponibilité d'une page web.

5.4.5. IPMI – Intelligent Platform Management Interface

L'interface de gestion intelligente de matériel, (ou IPMI, Intelligent Platform Management Interface) est un ensemble de spécifications d'interfaces communes avec du matériel informatique (principalement des serveurs) permettant de surveiller certains composants (ventilateur, sonde de température, …).

5.4.6. JMX – Java Management Interface

JMX (Java Management Extensions) est une API pour Java permettant de gérer le fonctionnement d'une application Java en cours d'exécution. JMX a été intégré dans J2SE à partir de la version 5.0. On peut voir JMX comme une espèce de SNMP pour Java.

5.4.7. CIM – Common Information Model

CIM est un standard de description des données administratives développé par le DMTF (Desktop Management Task Force).

5.4.8. WBEM – Web Based Enterprise Management

WBEM (Web-Based Enterprise Management) est un ensemble de technologies et de standards Internet de gestion développés pour unifier la gestion des environnements d'informatique distribuée.

WBEM fournit la capacité aux industriels de délivrer un ensemble de standards de bases bien intégrés aux outils de supervision, facilitant l'échange de données à travers d'autres différentes technologies et plate-formes. L'instance de normalisation DMTF (Distributed Management Task Force) accueille les impressions de leurs standards mais elle requiert que les individus soumettant des commentaires soient agréés pour la politique d'impression du DMTF.

5.4.9. SBLIM – Standard Based Linux Instrumentation for Manageability

SBLIM – prononcez « sublime » – pour Standards Based Linux Instrumentation for Manageability. Il consiste à permettre aux machines Linux d'accéder à l'ensemble des technologies d'administration WBEM (Web Based Enterprise Management). IBM assure le développement et la promotion de ce standard.

5.4.10. WS-MANAGEMENT – Web Services for Management

WS-Management (Web Services for Management) est une spécification définissant un protocole de communication pour l'administration des serveurs, équipements, et applications basée sur SOAP[20]. Cette spécification est devenue un standard ouvert et sa version finale 1.0.0 a été publiée par le DMTF en avril 2008. Une mise à jour de la spécification en version 1.1.0 a été publiée le 3 mars 2010

5.4.11. WMI – Windows Management Instrumentation

La technologie WMI (Windows Management Instrumentation) est une mise en œuvre de l'initiative WBEM (Web-Based Enterprise Management WBEM) de DMTF (Distributed Management Task Force) pour les plates-formes Windows. Cette initiative étend le modèle CIM (Common Information Model) pour représenter les objets de gestion dans les environnements Windows.

Tout cela signifie que WMI améliore considérablement les capacités de gestion de Windows 2000 grâce à une interface unique, cohérente, extensible et orientée objet, qui utilise les normes de l'industrie. Par ailleurs, les applications et les scripts peuvent accéder aux données WMI sur un poste local ou distant de façon totalement transparente.

WMI est pré-installé sur Windows Server 2003, Windows Server 2008, Windows XP, Windows Me, Windows 2000, Windows Vista et Windows 7

5.5. Aide à la prise de décision

La mission d'une solution de supervision est aussi d'aider à la prise de décision.

Elle va faciliter la prise de décision sur l'évolution technique, mais peut aussi permettre de connaître et donc d'anticiper des pics de consommation des ressources.

Prenons l'exemple du service informatique d'une entreprise qui gère son SI via une solution de supervision.

Le responsable du service va pouvoir choisir de recruter ou non une nouvelle personne en fonction, entre autres, du nombre d'incidents à traiter.

Mais pour cela, la supervision doit fournir des indicateurs, dans cet exemple, le nombre de ticket peut être un indicateur révélateur d'une charge de travail.

Afin d'aider à la décision, il faut avoir une vision à moyen terme de son système d'information.

Il est, par exemple, important de connaître l'occupation des ressources d'un serveur en vue de son remplacement. Des graphiques illustrant l'évolution de l'occupation de ses ressources va permettre non seulement d'envisager le changement, mais aussi de calibrer au plus près les ressources à fournir pour le nouveau serveur.

20 SOAP - Simple Object Access Protocol - protocole de RPC (Remote Procedure Call) orienté objet bâti sur XML (Extensible Markup Language, « langage de balisage extensible »).

Dans le cadre de l'infogérance d'un parc informatique il est nécessaire de présenter au client des indices de disponibilité, d'utilisation et de performance de ses services afin que celui-ci puisse apprécier le travail réalisé et anticiper de futurs besoins.

5.5.1. Indicateurs

La supervision fournit des indicateurs sur la santé de son système d'information.

Les indicateurs étant par nature mesurable, il sera facile de fixer des objectifs quantifiables en rapport avec ceux-ci.

Voici quelques exemples d'indicateurs :

- La disponibilité de ces services
- Volume d'incidents
- Temps de prise en compte d'un incident
- Temps de résolution d'un incident
- Utilisation des ressources
- …

5.5.2. Métrologie

La métrologie est la « science des mesurages et ses applications »

Il convient de connaître ce qu'il s'est passé, ce qu'il se passe et ce qu'il pourrait se passer.

Le but de la métrologie est de fournir des données liées aux performances et à la santé de son SI.

6. Projet de supervision

6.1. Besoins

6.1.1. Périmètre

Le projet de supervision a été réalisé dans un service d'infogérance structuré en niveau de compétences en rapport avec l'expérience et les technologies.

Ceci implique une architecture multi-clients, multi-sites avec des environnements

techniques hétérogènes, des contraintes de sécurité propres aux politiques de chacun.

Il faut donc se tourner vers une solution relativement standard afin que celle-ci soit connue de tous.

La solution doit obligatoirement être opensource de part le cœur de métier du groupe Alter Way, opérateur de services opensource.

6.1.2. Objectifs

Voici la liste des objectifs initiaux du projet de supervision :

- Avoir un meilleur contrôle du système d'information de nos clients.
- Améliorer la réactivité du service infogérance
- Anticiper l'évolution du système d'informations de nos clients
- Mettre à disposition des indices de disponibilité et de performance des services supervisés
- Offrir une interface de configuration accessible pour faciliter et industrialiser le déploiement des nouvelles entités supervisées.
- Superviser des serveurs (espace disque, utilisation mémoire vive...)
- Superviser des services (web, mail, dns...)
- Mettre à disposition de rapports et tableaux de bord avec graphes de tendances en adéquation avec les SLA définis (Service Level Agreement) sur les contrats d'infogérance des clients.
- Fournir de nouveaux services intégrés par défaut afin d'étoffer notre offre de service d'infogérance.
- Fournir de nouveaux services payants de supervision à la demande.

La réflexion sur la mise en place de nouveaux services payant aurait due se faire de concert avec les équipes commeciales, actuellement ces options ne se vendent pas

6.1.3. Gestion d'incidents

Le projet de supervision doit permettre de gérer de manière pro-active les incidents présents sur les systèmes d'information des clients de manière collaborative.

Le but étant d'assurer le meilleur taux de disponibilité et d'accessibilité des systèmes d'information afin de respecter à minima les SLA (Service Level Agreement) définis dans le contrat d'infogérance du client.

6.1.4. Gestion des problèmes – Escalade (Gestion d'incidents, de problèmes...)

Il doit être possible d'escalader un incident à une personne du niveau supérieur, si la personne de niveau inférieur ne peut le prendre en charge.

De même, il est nécessaire d'identifier les incidents récurrents afin que ceux-ci soient classifiés en tant que problèmes à résoudre par les niveaux supérieurs.

La notion de problème est celle que l'on retrouve dans les bonnes pratiques ITIL[21]

Définition de problème selon ITIL de Wikipédia :

Un problème est la cause inconnue d'un incident significatif ou de plusieurs incidents présentant les mêmes symptômes impactant le bon fonctionnement du système d'information ou du « métier » de l'entreprise.

6.1.5. Gestion de performances

La solution retenue va devoir fournir une vision globale par le biais de graphiques sur l'utilisation, la disponibilité et l'intégrité des ressources nécessaires au bon fonctionnement du Système d'information.

6.1.6. Possibilités de spécificités clients

Le système doit avoir une certaine souplesse et évolutivité afin de prendre en compte les spécificités clients.

Il faut que la solution reste le plus modulable possible en offrant un maximum de possibilité d'interrogation et une multitude d'environnements et d'éléments

Il doit par exemple être possible de superviser une ferme de serveurs virtualisés VMware Sphere 4

6.1.7. Multi-sites

La solution de supervision va devoir être multi-sites, ce qui va impliquer des contraintes de sécurité réseau, d'accessibilité à certains éléments.

Cela va aussi apporter des contraintes de performance réseau et de connectivité.

21 ITIL Information Technology Infrastructure Library pour « Bibliothèque pour l'infrastructure des technologies de l'information » - ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») pour le management du système d'information, édictées par l'Office public britannique du Commerce (OGC).

6.1.8. Notifications (types, fréquences...)

Un des grands risques de non-acceptation des services techniques à une solution de supervision est la gestion des notifications.

Celle-ci doit être hautement paramétrable afin de faciliter l'acceptation d'un projet de supervision par les services techniques

Par exemple, envoyer une notification toutes les 5 minutes pour un problème d'espace disque n'est pas nécessaire la plupart du temps. Une notification envoyée toutes les 30 minutes serait plus acceptable, car un utilisateur n'a pas besoin d'être informé avec si peu d'intervalle d'un problème qui n'est sûrement pas urgent.

Les destinataires des supervisions vont rapidement mettre des filtres sur leurs clients de messagerie par défaut afin de ne plus être « pollué » sur leur boîte principale.

6.2. Les principales solutions libres et opensource

L'écosystème de la supervision libre est assez riche en solutions d'un point de vue quantitatif, mais aussi qualitatif.

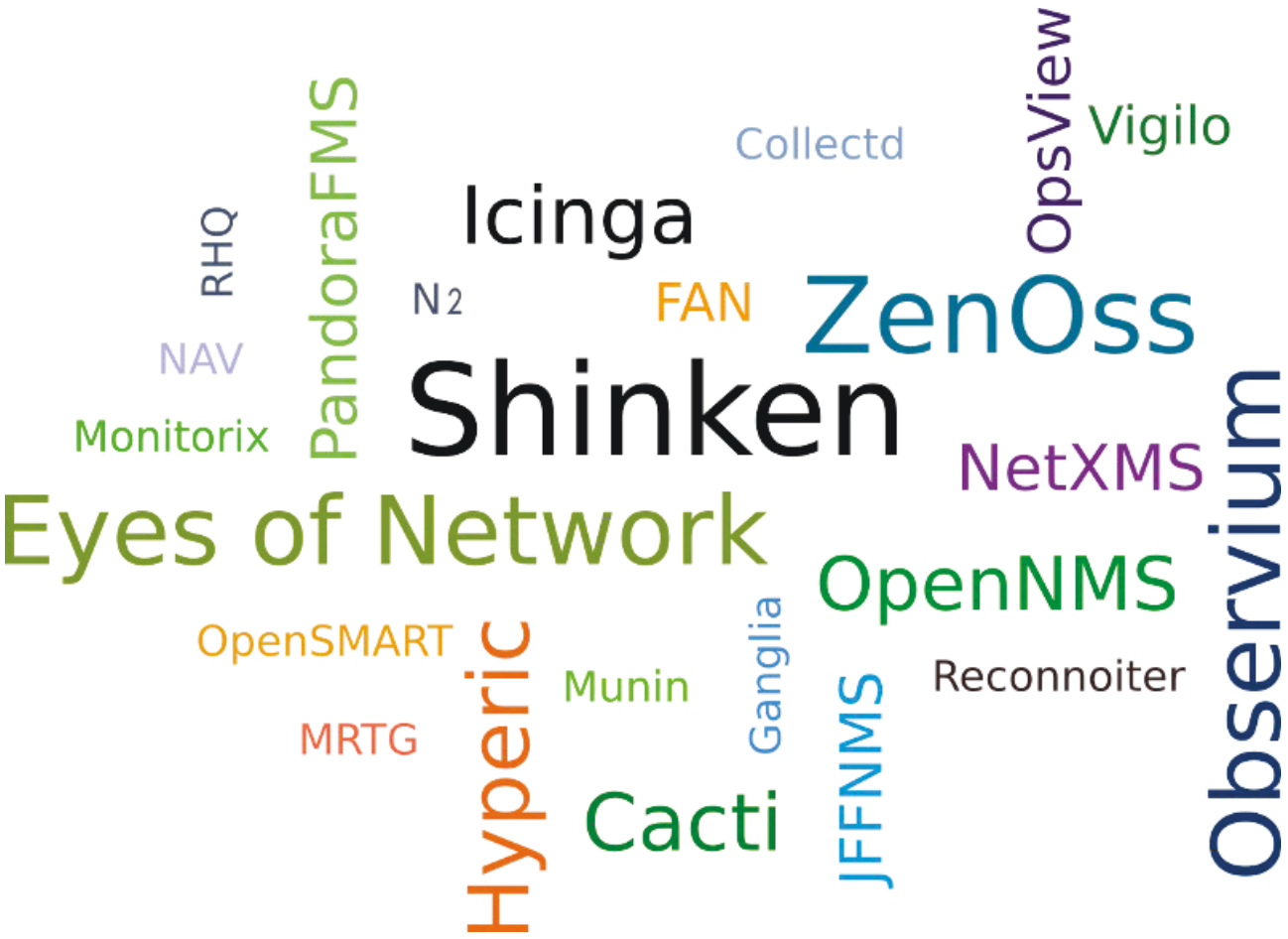
Tous les niveaux de supervision sont couverts par des solutions libres. Certaines d'entre-elles se concentrent sur une ou plusieurs fonctions, alors que d'autres compilent ces différentes solutions pour en proposer une globale.

Toutes les solutions qui vont être présentées ici permettent toutes nativement, ou via l'utilisation d'outils complémentaires, de notifier un événement quelconque comme une panne, une faute charge réseau...

Seules les applications ayant une date de publication de leur dernière version inférieur à 2 ans ont été étudiées.

Certaines solutions présentées ici proposent des versions « Entreprise » payantes, mais celles-ci ne seront pas présentées.

Voici une liste de solutions de supervision libre et/ou opensource regroupées par rôle et fonction.



6.2.1. Gestion de performances et métrologie :

Nom : MRTG (Multi Router Traffic Grapher)

Description :

MRTG est une solution qui fournit des graphes de performances en supervisant des éléments compatibles SNMP

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Collecte de valeurs via SNMP
- Génération de Graphes via RRDTool
- Rapport via interface Web
- Possibilité de notification via un plugin

Page Web : http://oss.oetiker.ch/mrtg/

Environnement serveur : Linux, Unix, Windows, Netware

Environnement client : Linux, Unix, Windows, Netware, Équipement compatible SNMP

Méthode d'interrogation : Scripts, SNMP

Licence : GPL

Dernière version et date de mise à disposition : 2.17.2 sorti le 20/02/2011

Nom : Cacti

Description :

Cacti est une solution de supervision qui a pour but de collecter des données de performance afin de fournir des graphes.

Il existe une grande communauté autour de Cacti et de nombreux plugins existent, permettant de superviser beaucoup d'éléments différents.

Cacti est souvent considéré comme le successeur de MRTG présenté ci-dessus.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Collecte de valeurs via SNMP, Script...
- Génération de Graphes via RRDTool
- Rapport via interface Web
- Notion de modèle de graphique, de modèle de source de données
- Personnalisation des graphes
- Gestion de Plugins
- Portabilité des modèles (Import et Export)
- Cacti peut être intégré à Nagios pour la notification.

Page Web : http://cacti.net

Environnement serveur : Linux, Unix, Windows

Environnement client : Linux, Unix, Windows, Netware, Équipement compatible SNMP

Méthode d'interrogation : Scripts, SNMP

Licence : GPL

Dernière version et date de mise à disposition : 0.8.7g sorti le 09/07/2010

Nom : Munin

Description :

Munin est une solution de supervision qui a pour but de collecter des données de performance afin de fournir des graphes basés sur RRDTool

L'architecture du système Munin est constituée d'un serveur principal appelé Munin-master, récupérant les informations à intervalle régulier et de plusieurs nœuds appelés Munin-node. Le nœud doit être installé sur le(s) serveur(s) à surveiller.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Notification par mail ou via Nagios
- Notion de plugins
- Génération de Graphes via RRDTool
- Intégration avec Nagios

Page Web : http://munin-monitoring.org/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL

Dernière version et date de mise à disposition : 1.4.6 sorti le 07/07/2011

Nom : Collectd

Description :

Collectd est une solution de supervision orientée gestion de performances permettant de collecter des données à intervalle adaptable.

Le mode de fonctionnement est passif, c'est le client qui pousse les données vers le serveur.

Fonctionnalités :

- Supervision de systèmes, de réseaux
- Gestion de plugins
- Notification possible via Nagios
- Support du SNMP
- Gestion de graphes
- La notification est intégrée depuis la version 4.3 mais aussi via Nagios

Page Web : http://collectd.org/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Scripts + SNMP

Licence : GPL

Dernière version et date de mise à disposition : 5.0.0 sorti le 28/03/2011

Nom : Observium

Description :

Observium est un système de découverte automatique et supervision de réseaux basé sur PHP / MySQL et orienté pour les réseaux Cisco, Linux, FreeBSD, Juniper...

Observium supporte une large gamme de distribution et de matériel.

Observium est issu d'un manque de facilité d'utilisation des solutions de supervision réseaux. Il est destiné à fournir une interface facilement navigable pour superviser la santé et les performances de votre réseau.

Fonctionnalités :

- Découverte automatique des équipements réseaux.
- Support de nombreux matériels réseaux et systèmes d'exploitation
- Gestion de graphes
- Notification par mail
- Personnalisation des graphes
- Gestion de syslog (Système de Fichiers historiques)
- Support de systèmes virtualisés
- Surveillance d'éléments physiques (Température, voltage...)
- Intégration d'outils externes (Rancid, Collectd, NfSen)
- Gestion de syslog (Système de Fichiers historiques)
- Inventaire

Page Web : http://observium.org/

Environnement serveur : Linux, Unix

Environnement client : Cisco, Linux, FreeBSD, Juniper, Foundry, HP, Entités SNMP

Méthode d'interrogation : SNMP, ICMP, IPMI

Licence : GPL

Dernière version et date de mise à disposition : 0.11.5.2261 sorti le 05/05/2011

6.2.2. Gestion d'incidents et gestion de performances réunies :

On peut parler ici de supervision globale, intégrant la supervision orientée gestion d'incidents, mais aussi gestion de performances permettant de gérer les pannes et d'avoir une idée sur certaines.

Nom : Ganglia

Description :

Solution de supervision pour Cluster[22] ou grappe de serveur à haute performance

Fonctionnalités :

- Supervision orientée Cluster
- Collecte de valeurs via des agents
- Agrégation de données
- Support SFlow

Page Web : http://ganglia.info/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur

Licence : BSD

Dernière version et date de mise à disposition : 3.2.0 sorti le 07/07/11

Nom : Monitorix

Description :

Solution de supervision légère orientée supervision de systèmes, services et éléments réseaux.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Supervision physique du matériel (Température...)
- Gestion de graphes
- Notification

Page Web : http://www.monitorix.org/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : BSD

Dernière version et date de mise à disposition : 2.3.0 sorti le 05/09/11

22 Cluster – Est une grappe de serveurs ou « ferme de calcul »

Nom : N2

Description :

Solution de supervision Client / Serveur en temps réel remontant des alertes en cas d'incidents et fournissant des données de performances sur les éléments supervisés.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Reporting
- Gestion de syslog (Système de Fichiers historiques)
- Gestion de graphes
- Notification par mail

Page Web : http://opensource.xlshosting.com/n2/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix

Méthode d'interrogation : Client / Serveur

Licence : GPL

Dernière version et date de mise à disposition : 1.0.4 sortie le 27/10/10

Nom : Hyperic Open Source Edition

Description :

Solution de supervision, couvrant de nombreux domaines tel que la gestion d'incidents, de performances, la découverte automatique.

La société éditrice de cette solution, Springsource, a récemment été rachetée par la société VMWare

Fonctionnalités :

- Gestion d'incidents
- Gestion de performances
- Découverte automatique
- Notification
- Escalade
- Surveillance des configurations

Page Web : http://www.hyperic.com/

Environnement serveur : Linux, Unix, Windows

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL

Dernière version et date de mise à disposition : 4.5.2 sortie le 19/07/11

Nom : JFFNMS

Description :

Solution complète de supervision alliant gestion d'incidents et gestion de performances avec des notions d'industrialisation natives tel que la distribution d'agent et la gestion de configuration centralisée

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Notification par mail et SNMP
- Découverte automatique des équipements et services réseaux.
- Gestion de syslog (Système de Fichiers historiques)
- Gestion de plugins / modules
- Gestion de graphes
- Sauvegarde de configuration Cisco IOS & CatOS
- Découverte automatique des services sur un équipement
- Possibilité de mettre en œuvre une architecture distribuée

Page Web : http://www.jffnms.org/

Environnement serveur : Linux, FreeBSD, Windows

Environnement client : Tout équipement compatible SNMP

Méthode d'interrogation : SNMP + Scripts

Licence : GPL

Dernière version et date de mise à disposition : 0.9.1 sortie le 05/06/11

Nom : Reconnoiter

Description :

Solution complète de supervision Client / Serveur qui remonte facilement d'éventuels incidents et des données de performances.

Fonctionnalités :

- Gestion d'incidents
- Gestion de performances
- Détection de panne
- Gestion de configuration centralisée
- Exploitation décentralisée

- Collection de données journalisées (permet de rejouer en cas de perte de connectivité par exemple)
- Notification
- Escalade

Page Web : https://labs.omniti.com/labs/reconnoiter

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur

Licence : GPL

Dernière version et date de mise à disposition : Pas de notion de version, constamment mis à jour, sortie le 21/09/11

Nom : OpenSMART

Description :

Solution complète de supervision alliant gestion d'incidents et gestion de performances avec des notions d'industrialisation natives tel que la distribution d'agent et la gestion de configuration centralisée

Fonctionnalités :

- Gestion d'incidents
- Cartographie[23]
- Reporting
- Distribution d'agent (ex : mise à jour automatisée)
- Gestion des SLA
- Inventaire
- Configuration via Interface web
- Gestion de configuration centralisée

Page Web : http://opensmart.sourceforge.net/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Windows

Méthode d'interrogation : Client / Serveur

Licence : GPL

Dernière version et date de mise à disposition : 2.0 sortie le 13/09/11

23 Cartographie – Outil de visualisation graphique de l'état de sa supervision, souvent utiliser pour représenter des entités sur une carte géographique.

Nom : RHQ

Description :

RHQ est une solution de supervision initiée par RedHat qui se veut extensible et industrialisée, notamment au niveau du déploiement.

Il est initialement prévu pour gérer les applications Jboss, mais peut superviser l'ensemble d'un environnement informatique.

Fonctionnalités :

- Notification
- Graphes de performances
- Reportage
- Inventaire
- Exécution distante
- Gestion de configuration distante
- Découverte automatique

Page Web : http://rhq-project.org/display/RHQ/Home

Environnement serveur : Linux, FreeBSD, Windows, Mac OS X

Environnement client : Linux, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL/LGPL

Dernière version et date de mise à disposition : 4.1 sortie le 02/09/11

Nom : OpenNMS

Description :

OpenNMS fait parti des solutions de supervision libre les plus connus, mais c'est aussi, une des plus anciennes. Elle a été initiée en 1999 et a déjà reçu de nombreux prix.

OpenNMS ne possède pas, comme certains concurrents, de version « Entreprise ». En effet les créateurs de cette solution tiennent absolument à conserver cela.

Fonctionnalités :

- Découverte automatique des équipements réseaux.
- Découverte automatique des services sur un équipement et mesure de disponibilité
- Reporting
- Identification et liste des coupures réseaux (outages, path outages)
- Supervision de systèmes, de réseaux et d'applications
- Notification

- Corrélation entre les alarmes afin de présenter un affichage clair des problèmes en cours
- Corrélation, notification et escalade des événements sous forme d'alarmes
- Gestion de graphes
- Cartographie
- Fourniture d'un outil de base pour traduire les MIBs et les intégrer dans l'outil

Page Web : http://www.opennms.org/

Environnement serveur : Linux, Unix, Windows, Mac OS X

Environnement client : Linux, Unix, Windows, Mac OS X, Équipement compatible SNMP

Méthode d'interrogation : SNMP

Licence : GPL

Dernière version et date de mise à disposition : 1.8.13 sortie le 10/08/11

Nom : NetXMS

Description :

NetXMS est une solution de supervision très complète de gestion d'incidents, de performances couvrant des équipements réseaux jusqu'aux applications métiers

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Découverte automatique des équipements réseaux.
- Découverte automatique des services sur un équipement et mesure de disponibilité
- Reporting
- Gestionnaire d'événements
- Vues métiers
- Notification
- Actions automatisées en cas d'événements (relance d'un service...)
- Corrélation d'incidents
- Modèles de collection de données
- Modèles d'actions automatiques
- Notion de dépendances (hôtes, services...) permettant de superviser avec une vision métier
- Cartographie
- Géolocalisation
- Tableaux de bord personnalisables

- Compatible Nagios et Plugins
- Gestion des accès très fine basée sur une Liste de Contrôle d'Accès (LCA)
- Gestion de configurations centralisées des agents avec mises à jour automatiques

Page Web : http://www.netxms.org/

Environnement serveur : Linux, Unix, Windows

Environnement client : Linux, Unix, Windows, Netware, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL

Dernière version et date de mise à disposition : 1.1.4 sortie le 11/09/11

Nom : PandoraFMS

Description :

PandoraFMS est une solution de supervision complète également. La toute dernière version fraîchement sortie est désormais orientée bonnes pratiques ITIL v3.

Fonctionnalités :

- Supervision systèmes et réseaux
- Gestion d'événements et de fautes
- Découverte automatique des équipements réseaux.
- Géolocalisation
- Gestion en ligne de commande (CLI - Command Line Interface)
- Console de visualisation personnalisable en fonction de niveaux de service
- Architecture distribuée
- Actions automatiques des agents prédéfinies
- Intégration native avec la solution de gestion d'incidents opensource Integria IMS
- Console légère pour mobiles
- Métrique orientée ITIL v3
- Interface Android

Page Web : http://pandorafms.org/

Environnement serveur : Linux, Unix, Windows

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP + WMI +Script + ICMP + SSH

Licence : GPL

Dernière version et date de mise à disposition : 4.0 sortie le 26/09/11

Nom : ZenOSS

Description :

Créé en 2005, ZenOSS a pour but de fournir le nécessaire à la supervision de parcs informatiques en un seul outil, plutôt qu'en plusieurs comme à l'époque de sa création où il fallait un logiciel par fonction. (Gestion d'incidents, gestion de performances...)

ZenOSS se veut sans agent pour faciliter la gestion et le déploiement

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Notification et résolution automatique
- Supervision de logs et de gestionnaire d'événements
- Inventaire et découverte automatique avec suivi du changement.
- Collection de données vis SNMP, SSH, WMI, JMX et Syslog
- Notion de plugins/extensions (+ de 200)
- Supervision d'environnements virtuels et de Cloud
- Reporting
- Notification par mail et SNMP
- Intégration avec des outils de gestion de configuration centralisée
- Supervision de VMWare ESX

Page Web : http://community.zenoss.org/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : SNMP, SSH, Telnet et WMI

Licence : GPL

Dernière version et date de mise à disposition : 3.2.0 sortie le 02/09/11

Nom : Opsview

Description :

Solution complète de supervision (gestion d'incident, de performance, cmdb, découverte automatique, reporting...) basée sur la solution de supervision Nagios

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Vues techniques & Vues métiers
- Reporting
- Gestionnaire d'événements
- Notification par mail et SNMP

- Actions automatisées en cas d'événements (relance d'un service...)
- Tableaux de bord personnalisables
- Compatible Nagios et Plugins
- Gestion des accès très fine basée sur une Liste de Contrôle d'Accès (LCA)
- Suivi SLA (accords de niveau de service)
- Graphique de performances
- Gestion de syslog (Système de Fichiers historiques)
- Authentification LDAP
- Architecture distribuée

Page Web : http://intervieweuse/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Windows, Mac OS X, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL

Dernière version et date de mise à disposition : 3.13 sortie le 27/07/11

Nom : Vigilo

Description :

Vigilo est une solution complète de supervision basée sur Nagios, capable de gérer des systèmes d'envergure (réseaux et serveurs) grâce à une architecture répartie et modulaire.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Notification et résolution automatique
- Supervision de logs et de gestionnaire d'événements
- Inventaire et découverte automatique avec suivi du changement.
- Collection de données vis SNMP, SSH, WMI, JMX et Syslog
- Notion de plugins/extensions (+ de 200)
- Supervision d'environnements virtuels et de Cloud
- Reporting
- Notification par mail et SNMP
- Intégration avec des outils de gestion de configuration centralisée
- Supervision de VMWare ESX

Page Web : http://www.projet-vigilo.org/site/

Environnement serveur : Linux, Unix

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL v2

Dernière version et date de mise à disposition : 2.0.0 sortie le 22/06/11

Nom : Icinga

Description :

Icinga est un fork[24] de la solution de supervision libre Nagios. Depuis la création de ce fork, la solution a considérablement évoluée et est devenue une solution à part entière.

Ce fork a été initié par la société Allemande NetWays, contributeur historique à la solution Nagios, qui avait trop de divergences avec la société éditrice de Nagios.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Reporting
- Possibilité de mettre en œuvre une architecture distribuée du système de supervision
- Notification
- Notions de plugins
- Compatible Nagios et Plugins
- Gestion des arrêts programmés
- Cartographie
- Console légère pour mobiles

Page Web : https://www.icinga.org/

Environnement serveur : Linux, Unix, MAC OS X

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL

Dernière version et date de mise à disposition : 1.5.2 sortie le 16/09/11

24 Fork - Un fork, ou embranchement, est un nouveau logiciel créé à partir du code source d'un logiciel existant – Définition Wikipedia http://fr.wikipedia.org/wiki/Fork_%28d%C3%A9veloppement_logiciel%29

Nom : Shinken

Description :

Shinken est né d'un POC (Proof Of Concept) qui visait à reproduire la solution de supervision Nagios, mais écrit en python et qui n'avait pas pour objectif d'être publié.

Au fur et à mesure des tests, Jean Gabes, le créateur, s'est aperçu que les performances étaient bien meilleures.

Le développement a continué et de nombreuses contraintes ont été améliorées, notamment au niveau de l'architecture distribuée, mais aussi de nombreux bugs ont été corrigés avec cette version.

Cette version en python a été proposée aux créateurs de Nagios pour en faire la prochaine version majeure, mais aucune réponse officielle n'a été reçue.

C'est à partir de là que l'idée de créer un fork est apparue, et la naissance de Shinken également.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Notification
- Découverte automatique des équipements et services réseaux.
- Notion de dépendances (hôtes, services...) permettant de superviser avec une vision métier
- Support de VMWare et VMotion avec découverte automatique des systèmes invités et création automatique des dépendances
- Possibilité de supervision type métier
- Compatible Nagios et Plugins
- Support de nombreuses interfaces graphiques
- Fourniture de données de performances
- Import automatique depuis GLPI (Gestion Libre de Parc Informatique)
- Escalade de notifications
- Architecture Haute-Disponibilité et distribuée

Page Web : http://www.shinken-monitoring.org/

Environnement serveur : Linux, Unix, Windows

Environnement client : Windows, GNU/Linux, HPUX, AIX, Cisco, Nortel, Entités SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : AGPL

Dernière version et date de mise à disposition : 0.6 sortie le 06/05/11

6.2.3. Solutions clefs en main – Distribution GNU/Linux orientée supervision :

Nom : FAN

Description :

FAN – Fully Automated Nagios – est une distribution GNU/Linux basée sur CentOS, qui intègre la solution de supervision Nagios et des outils satellites.

FAN intègre Nagios et ses plugins, Centreon, Nagvis, NDOUtils, NRPE et Nareto.

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Reporting
- Notification
- Actions automatisées en cas d'événements (relance d'un service...)
- Tableaux de bord personnalisables
- Gestion des accès très fine basée sur une Liste de Contrôle d'Accès (LCA)
- Graphique de performances
- Architecture distribuée
- Cartographie

Page Web : http://fannagioscd.sourceforge.net/wordpress/

Environnement serveur : Distribution GNU/Linux CentOS

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP

Licence : GPL

Dernière version et date de mise à disposition : 2.2 sortie le 01/08/11

Nom : Eyes Of Network

Description :

Solution complète de supervision (gestion d'incident, de performance, cmdb, découverte automatique, reporting...) basée sur diverses briques libres orientées ITIL

Fonctionnalités :

- Supervision de systèmes, de réseaux et d'applications
- Vues techniques & Vues métier
- Reporting

- Gestionnaire d'événements
- Notification par mail et SNMP
- Actions automatisées en cas d'événements (relance d'un service...)
- Tableaux de bord personnalisables
- Gestion des accès très fine basée sur une Liste de Contrôle d'Accès (LCA)
- Suivi SLA (accords de niveau de service)
- Graphique de performances
- Gestion de syslog (Système de Fichiers historiques)
- Authentification LDAP
- Sauvegarde automatisée de la solution
- Architecture distribuée
- Cartographie
- Gestion de parc via GLPI
- Supervision de processus métiers
- Gestion de traps SNMP

Page Web : http://www.eyesofnetwork.com/

Environnement serveur : Distribution GNU/Linux CentOS

Environnement client : Linux, Unix, Windows, Équipement compatible SNMP

Méthode d'interrogation : Client / Serveur + SNMP + IPMI

Licence : GPL

Dernière version et date de mise à disposition : 2.2 sortie le 27/11/10

À savoir qu'il existe la distribution OpenNMS Sans Effort, qui est une distribution GNU/Linux basée sur CentOS, et qui installe et configure automatiquement OpenNMS.

6.2.4. Tableau récapitulatif :

Voici un tableau récapitulatif qui regroupe les principales fonctionnalités des solutions de supervision présentées ci-dessus.

Le but étant de pouvoir comparer facilement les avantages et manquements d'une solution à une autre.

J'ai séparé les solutions par « famille », métrologie, solutions complètes, et distributions GNU/Linux prêtes à l'emploi.

Solutions	Supervision systèmes	Supervision Réseaux	Supervision Applicative	Génération de graphes	Notification	Compatible SNMP	Découverte automatique	Rapports	Cartographie	Architecture distribuée	Agent	Sans Agent	Action automatique	Extensions	Logs et gestion d'événements	Corrélation	Escalade	Gestion ACL	Gestion des SLA	Vues techniques et métiers	Interface mobile	Temps d'arrêt	Configurations centralisées	Inventaire	Outil de déploiement
MRTG	✓	✓	✓	✓		✓		✓				✓													
Cacti	✓	✓	✓	✓		✓		✓				✓		✓				✓								
Munin	✓	✓	✓	✓	✓	✓		✓				✓		✓												
Collectd	✓	✓	✓	✓		✓		✓				✓														
Observium	✓	✓	✓	✓	✓	✓	✓	✓				✓		✓	✓										✓	
Ganglia	✓	✓		✓							✓			✓		✓										
Monitorix	✓	✓	✓	✓	✓			✓			✓															
N2	✓	✓	✓	✓	✓			✓			✓				✓											
Hyperic	✓	✓	✓	✓	✓		✓	✓			✓	✓		✓										✓		
JFFNMS	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓											
NAV	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓								✓			
Reconnoiter	✓	✓	✓	✓	✓	✓	✓	✓			✓						✓							✓		
OpenSMART	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓				✓	✓				✓			✓
RHQ	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓		✓		✓	✓	✓			✓	✓	✓	✓
OpenNMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓				✓		✓	
NetXMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓				✓		
PandoraFMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
ZenOSS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓		✓	
Opsview	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			✓			
Vigilo	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓				✓		✓
Icinga	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓							✓	✓				
Shinken	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓			✓		✓				
FAN	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓			✓	✓					✓			
Eyes Of Network	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓	

Gestion de performances
Solution Complète
Distribution

Comme expliqué plus haut, toutes les solutions présentées ici permettent la notification.

Dans ce tableau, je n'ai identifié que celles qui pouvaient le faire nativement

Voici une explication des différentes fonctionnalités :

- Rapports : Possibilité de générer des rapports personnalisés.
- Action automatique : Exécution d'action déclenchée automatiquement lors de l'apparition d'événements comme une remontée d'incident.
- Logs et Gestion d'événements : Analyse des fichiers historiques (logs) et du gestionnaire d'événements Windows
- Corrélation : Il s'agit ici de corrélation d'événements, c'est à dire d'agrégation automatisée d'événements afin d'identifier plus facilement des événements. Ceci va permettre de les mettre en avant pour optimiser leur traitement.
- Escalade : Possibilité de transmettre un incident aux membres d'un niveau supérieur de manière automatique ou non.
- Gestion d'ACL : Gestion fine des droits d'accès.
- Temps d'arrêt : Permet de stopper la surveillance d'un élément pour une durée donnée si par exemple une intervention est planifiée. Ceci va permettre de

conserver un niveau de service réel.

- Configuration Centralisée : Il s'agit ici de gérer de manière centralisée des configurations, cela va des agents de supervision jusqu'au système lui-même.
- Outil de déploiement : Outil de déploiement d'agent, ou de mise à jour d'agent.

J'ai volontairement retiré de l'analyse ci-dessus les 2 solutions que j'ai choisi d'étudier de manière plus approfondie, qui sont Zabbix ainsi que Nagios et ses projets satellites.

Le fait d'avoir inventorié les solutions libres m'a permis de découvrir qu'il y en avait vraiment beaucoup et démontre un intérêt et donc un marché. Ça m'a permis aussi de découvrir beaucoup de fonctionnalités

Si c'était à refaire, je n'aurais pas étudier toutes ces solutions, car cela a pris un temps considérable. J'aurais limité mes recherches qu'aux plus répandues

6.3. Mise en exergue de 2 solutions libres majeures

Il a été décidé de tester plus en profondeur 2 solutions libres et opensource majeures, de par leur notoriété, mais aussi le périmètre fonctionnel couvert par ses deux solutions et leur écosystème.

Nagios étant bien sur la plus connue des solutions libres et open source, mais aussi sûrement la plus déployée.

Zabbix est une solution montante qui se veut globale et complète.

6.3.1. Zabbix

Zabbix, est une solution de supervision libre sous licence GPL créée par Alexei Vladishev. Zabbix permet de surveiller le statut de divers services réseaux, serveurs et autres matériels réseaux. Il permet également la création de scénario pour l'analyse des performances de son environnement sur le long terme.

Zabbix est pleinement libre et opensource. Il n'existe pas de notion de double licence comme certaines autres solutions qui fournissent une version opensource minimisée et une version contenant des blocs propriétaires (souvent à forte valeur ajoutée)

Zabbix fonctionne nativement avec les bases de données MySQL, PostgreSQL ou Oracle. Son interface web est écrite en PHP, HTML/CSS, Javascript alors que son moteur est écrit en C.

Zabbix permet la vérification simple de la disponibilité ainsi que le temps de réponse de services standards comme SMTP ou HTTP sans installer aucun logiciel sur l'hôte supervisé.

Ou alors un agent Zabbix peut également être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, l'espace disque…

Zabbix peut également réaliser le monitoring via SNMP.

Zabbix est une solution de supervision complète, qui couvre la gestion d'incidents, la gestion de performances, la gestion des SLA...

6.3.1.1. Architecture de la solution

Zabbix fonctionne donc en mode Client/Serveur ou encore sans agent.

Il stocke les remontées d'incidents, de performances et autres en base de données, et se veut capable de superviser un très grand nombre d'éléments.

6.3.1.1.1. Les composants

Le Serveur Zabbix :

Il s'agit du cœur de la solution de supervision Zabbix. Il permet de surveiller localement et à distance des éléments systèmes et réseaux. C'est lui qui va stocker les données de configuration et les données liées à la supervision (incidents, données de performance...)

Il va permettre la notification également en cas d'événement.

L'interface web Zabbix :

Il s'agit de l'interface de configuration, de gestion, de visualisation des événements.

Il s'agit d'une interface web développée en php, ce qui permet de rendre l'interface de configuration accessible depuis tout type de système d'exploitation.

Le Proxy Zabbix :

Le proxy Zabbix est très intéressant, il va permettre de collecter et de transmettre les informations au serveur Zabbix de manière autonome.

Il est intéressant, car il va permettre de superviser des environnements distants très facilement et en n'autorisant qu'un seul type de flux, ce qui facilite le passage de firewall.

Sa configuration est très simple, sur le même principe que les agents.

L'agent Zabbix :

Multiplate-forme, l'agent zabbix va se charger de la collecte de données et il va les transmettre soit au serveur, soit à un proxy Zabbix.

L'agent Zabbix renvoie beaucoup de données au serveur et fonctionne principalement de manière active.

6.3.1.1.2. Schéma d'architecture global

Voici un schéma présentant l'architecture fonctionnelle de Zabbix

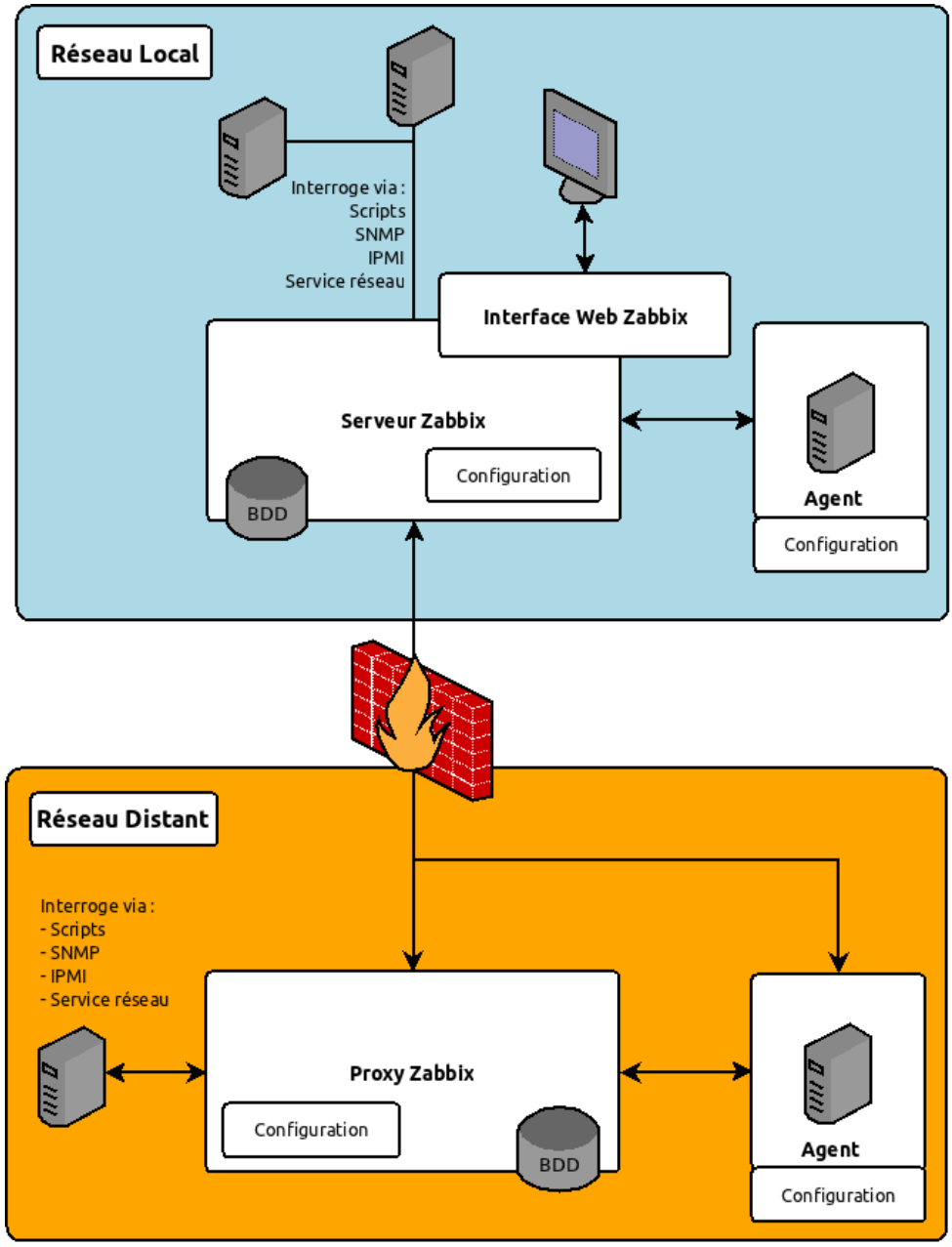


Illustration 20 : Architecture fonctionnelle de Zabbix

L'utilisation du proxy Zabbix n'est pas obligatoire, mais vivement conseillée. Il va agir comme un serveur intermédiaire entre les agents et le serveur Zabbix.

En effet, il n'y a pas ou peu d'intérêt à ouvrir des flux vers plusieurs entités plutôt qu'une seule.

De plus, cela permet d'avoir une continuité de service en cas de perte de lien réseau entre le ou les serveurs Zabbix et l'environnement distant supervisé.

Zabbix peut fonctionner de manière totalement autonome avec le Serveur et l'interface web, sans agent ni proxy.

La supervision peut aussi bien se faire de manière passive qu'active.

6.3.1.2. Type d'utilisation de Zabbix :

Zabbix a été conçu pour répondre à tout type d'architecture, de la plus simple en mono-serveur à la plus complexe en mutli-serveurs, multi-sites géographiques...

6.3.1.2.1. Mono-Serveur :

Le serveur Zabbix peut fonctionner de manière totalement autonome avec une architecture dite mono-serveur :

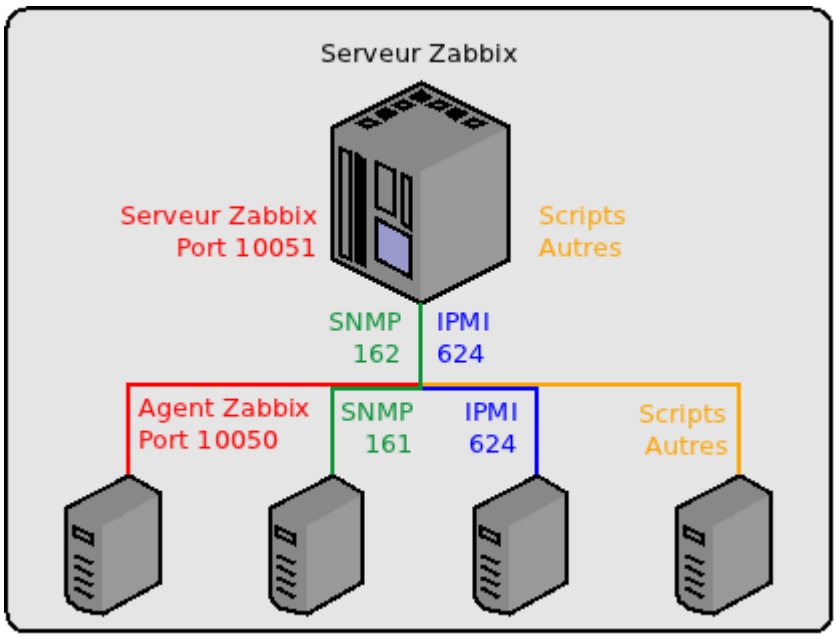


Illustration 21 : Zabbix - Architecture Mono-serveur

On va retrouver ce mode de fonctionnement dans les petites et moyennes entreprises avec un site géographique.

Le serveur Zabbix va interroger directement via des requêtes aux agents, des événements générés par les agents, des interrogations SNMP, IPMI ou encore des scripts, des interrogations réseaux …

6.3.1.2.2. Distribuée - multi-serveurs :

Il est possible avec un serveur Zabbix de contrôler plusieurs serveurs « enfants » Zabbix.

À la différence du proxy Zabbix, le serveur enfant dispose d'une interface Zabbix Frontend permettant sa configuration. Il n'est pas un simple collecteur comme le proxy Zabbix.

Ce type d'architecture peut être utile en cas de site distant. Cela permet de combiner l'administration décentralisée et centralisée.

Les serveurs Zabbix discutent entre eux sur le port 10051 comme avec les agents.

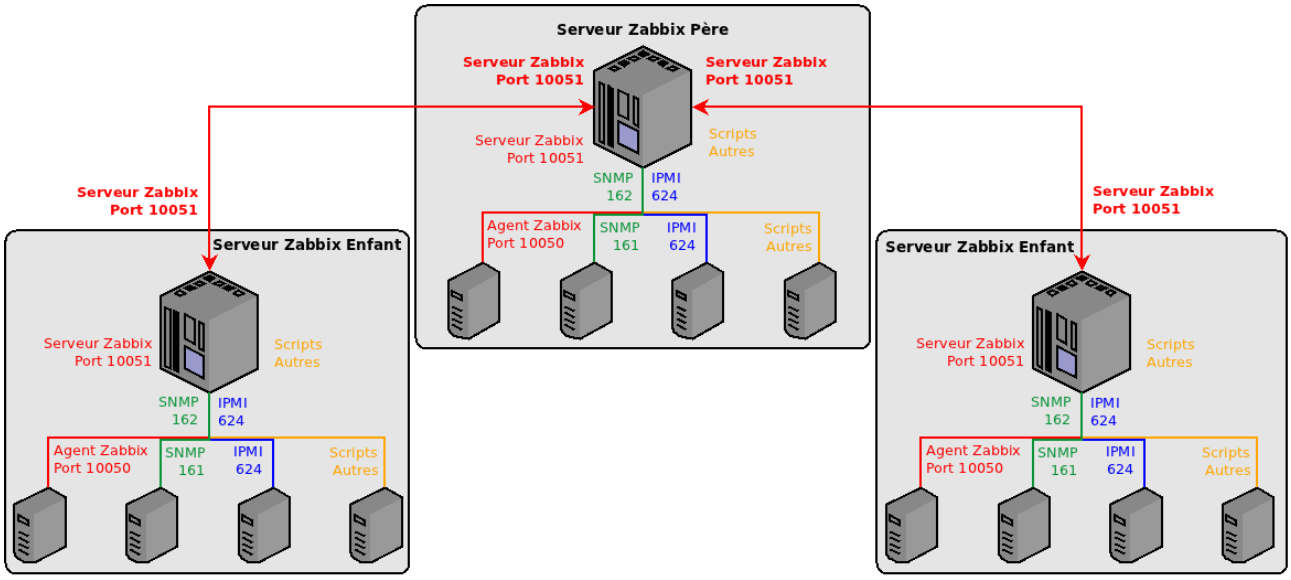


Illustration 22 : Zabbix - Architecture multi-serveurs

6.3.1.2.3. Distribuée – multi-proxy :

Avec une architecture multi-proxy, l'administration est centralisée sur un seul serveur Zabbix et utilise plusieurs proxy, à savoir des collecteurs, afin de remonter les données de différents sites.

Les proxy Zabbix ont un rôle de collecteur et ne permettent pas la configuration.

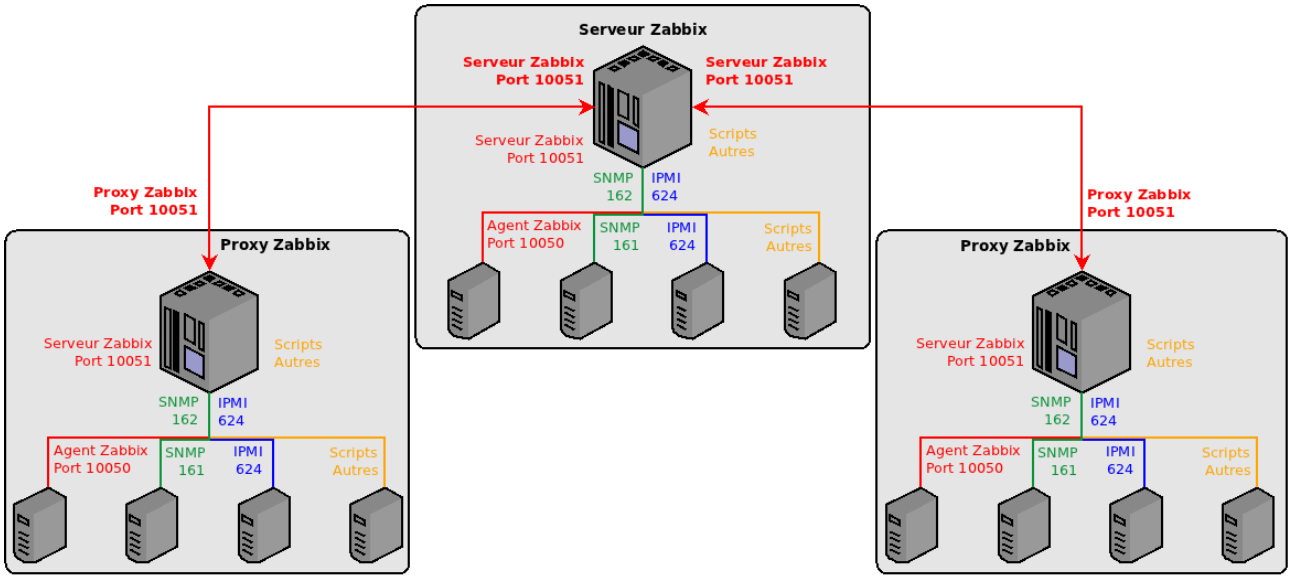


Illustration 23 : Zabbix - Architectures multi-proxy

6.3.1.2.4. Distribuée – multi-serveurs / multi-proxy :

Les serveurs Zabbix peuvent superviser leurs propres agents, tout en supervisant via les proxy Zabbix, mais aussi via d'autres serveurs Zabbix.

L'avantage est de fournir la possibilité d'administrer la supervision de manière centralisée et décentralisée selon les besoins de l'architecture.

On retrouvera ce type d'architecture sur les grands environnements.

De cette manière, il est possible de couvrir un maximum de besoins de supervision.

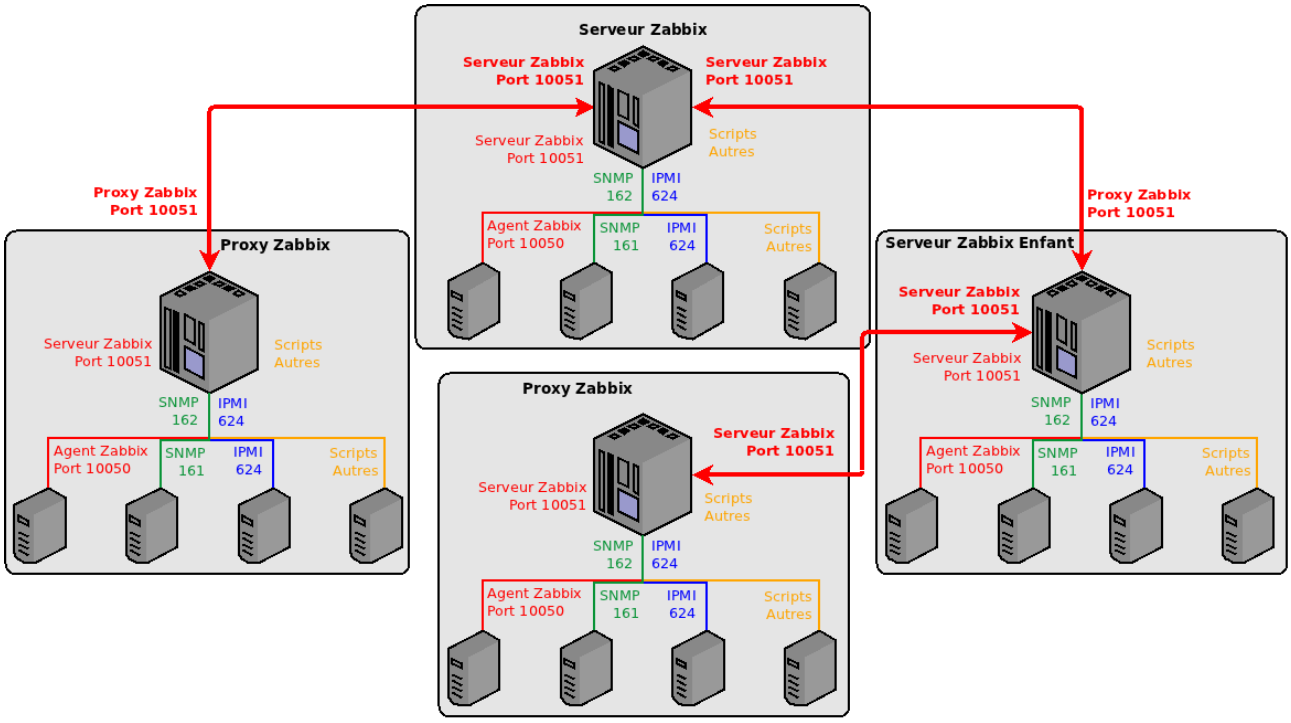


Illustration 24 : Zabbix - Architecture distribuée : multi-serveurs et multi-proxy

6.3.1.3. Fonctionnalités

Supervision distribuée :

- Possibilité de configuration centralisée
- Accès centralisé à toutes les données
- Fonctionnel jusqu'à 1000 nœuds Zabbix interconnectés.
- Nombre illimité de proxy Zabbix pour la collecte de données.

Capacité de montée en charge :

- Testé sur 100000 entités réseaux et serveurs
- Testé sur 1 000 000 contrôles de performance et disponibilité
- Traitement des milliers de contrôles de disponibilité et de performance par seconde

Supervision en temps réel :

- Gestion de performances
- Gestion de disponibilité
- Supervision de l'intégrité
- Condition de notifications flexible
- Gestion d'alerte utilisateur (mail, sms, Jabber)
- Historique

Visualisation :

- Possibilité de prédéfinir des vues utilisateur et des diaporamas
- Cartographie
- Gestion de graphes (y compris les diagrammes circulaires)
- Zoom

Résolution rapide d'incident :

- Envoi d'alerte par mail, sms, téléphone, ou encore une alerte audio.
- Il est possible d'exécuter des commandes à distance

Orienté SLA (Service Level Agreement) :

- Notion de service informatique hiérarchisé
- Rapport en temps réel du respect des SLA

Rapport et tendance :

- Intégration facile avec des outils tierces
- Statistiques quotidiennes, mensuelles, et annuelles
- Rapport sur les SLA

Import / Export de données via XML[25] :

- Partage facile de modèles

Découverte automatique d'entités réseaux :

- Découverte automatique par plage d'adresse IP, par services réseaux ou encore via SNMP
- Supervision automatique des entités découvertes

Supervision d'application web :

- Supervision de disponibilité et de performances d'application web
- Possibilité de création de scénarios flexibles visant à reproduire une utilisation humaine de l'application web
- Support des méthodes POST et GET

Flexibilité :

- Support des protocoles IPv4 et IPv6
- Agents nativement et facilement extensibles
- Beaucoup de méthodes de notifications
- Fonctionne sur un grand nombre de plates-formes

Supervision pro-active :

- Exécution automatique de commandes distante en rapport avec des événements survenus au sein du Système d'Information.
- Commandes IPMI automatiques

Agrégation :

- Supervision d'un groupe d'hôtes comme un seul

Supervision possible sans agent :

- Supervision de services distants (FTP, SSH, HTTP,...)
- Support du protocole SNMP v1,2,3
- Support du protocole IPMI
- Gestion de traps (événements) SNMP

Supervision avec les agents :

- Native avec de nombreuses plate-formes (UNIX-GNU/Linux, Windows, Novell)
- N'est pas impactée par les pertes de connexion réseau.

De nombreux contrôles possibles et pré-définis via les agents :

- Supervision de l'utilisation mémoire
- Supervision de l'utilisation réseau
- Supervision des entrées / Sorties disque

25 XML (Extensible Markup Language, « langage de balisage extensible ») langage informatique de balisage qui a pour objectif de faciliter l'échange de données entre systèmes hétérogènes

- Supervision de l'espace disque
- Contrôle des check-lists23 de fichier
- Supervision de fichiers de logs
- ...

Sécurisé :

- Gestion des droits utilisateurs flexible
- Authentification par adresse IP
- Protection contre les attaques de type brute force[26]
- Toutes les données sont stockées en base de données (Oracle, MySQL, PostgreSQL, Stylite)

Escalade et notification :

- Notifications répétées
- Escalades illimitées
- Message de retour à la normale
- Être averti de tout problème résolu.

Fonctions de gestion et de premier diagnostique :

- Possibilité de réaliser des tests de Ping, de traceroute vers un hôte
- Nombreuses autres fonctions

Tableau de bord :

- Tableau de bord personnalisables
- Notion de favori
- Plusieurs niveaux de vue

6.3.1.4. Plate-formes supportées

Le serveur de Zabbix est multi-plateformes et peut-être installé sur les systèmes GNU/Linux ou encore Unix.

La société Zabbix, valide l'installation sur les systèmes ci-dessous :

- Ubuntu Linux, AMD64, kernel 2.6.11, MySQL 5.x
- Ubuntu Linux, Intel, kernel 2.6.15, MySQL 5.0.22, PostgreSQL 8.3
- RedHat EL 5.3, Intel, kernel 2.6.18, Oracle 11gR2
- Slackware Linux, x86, kernel 2.6.29.6, MySQL 5.1.x

Concernant la récupération d'information, la supervision peut se faire de manière passive ou active.

26 Attaque de type brute force – Il s'agit de tester une à une toutes les combinaisons possibles, comme employer tous les mots des dictionnaires en plusieurs langues afin de trouver un mot de passe.

Zabbix permet de récolter des informations sur tous les équipements compatibles SNMP.

Mais il est également possible d'installer l'agent Zabbix sur les plate-formes ci-dessous :

- AIX 5.x
- FreeBSD 4.x, 5.x, 6.x
- HP-UX 10.x, 11.x
- Linux 2.4.x, 2.6.x
- Linux CentOS
- NetBSD 2.0
- OS/X 10.2
- Solaris 8, 9, 10
- Tru64 5.1B
- Windows XP, 2000, 2003, 2008, Vesta

Il en existe également des versions pré-packagées, comme des images virtuelles VMWare, ou encore Virtualbox permettant facilement d'installer Zabbix.

Et enfin, il existe des clients pour mobiles permettant de surveiller son S.I. via son mobile

6.3.1.5. Conclusion

Zabbix est une solution tout à fait viable pour superviser un système d'information, du plus simple au plus complexe.

L'architecture de Zabbix a été pensé de manière globale avec un recul suffisant pour une adaptation facilitée et en rapport avec les contraintes de Systèmes d'Information hétérogènes.

Son panel de fonctionnalités est très fourni et ouvert.

Sa communauté est grandissante, et il est déployé de plus en plus à travers le monde pour tout type de projet.

6.3.2. Nagios et Centreon

Nagios a été créé par Ethan Galstad en 1999 sous le nom de NetSaint. C'est aujourd'hui la solution de supervision opensource la plus connue et la plus répandue.

Nagios permet de superviser l'état d'hôtes ou de services à l'aide de plugins externes exécutés localement ou à distance. Il s'agit d'une solution orientée gestion d'incidents, mais elle permet également de remonter des données de performances.

En cas d'événement pré-défini, Nagios envoie une notification de changement d'état.

Il est utilisé dans les petites structures comme dans les plus grandes.

Il permet une supervision active et passive de serveurs, équipements réseaux, et surtout de services divers et variés.

Nagios est composé principalement de :

- Un ordonnanceur, qui est le cœur de la solution, prévu pour planifier les contrôles et récolter les données remontées.
- Une interface web, qui n'a pour rôle que la représentation graphique de l'état de ce qui est supervisé.
- Les sondes, qui sont des scripts permettant de réaliser ces contrôles
- Des Agents permettant d'exécuter les plugins sur des hôtes distants et d'en remonter les données de supervision.

Nagios fournit par défaut un certain nombre de sondes permettant de réaliser de nombreux contrôles. Néanmoins, grâce à la simplicité des retours attendus, de nombreuses sondes ont été réalisées par la communauté, ce qui fait la très grande force de Nagios.

6.3.2.1. Architecture de la solution

6.3.2.1.1. Architecture autonome

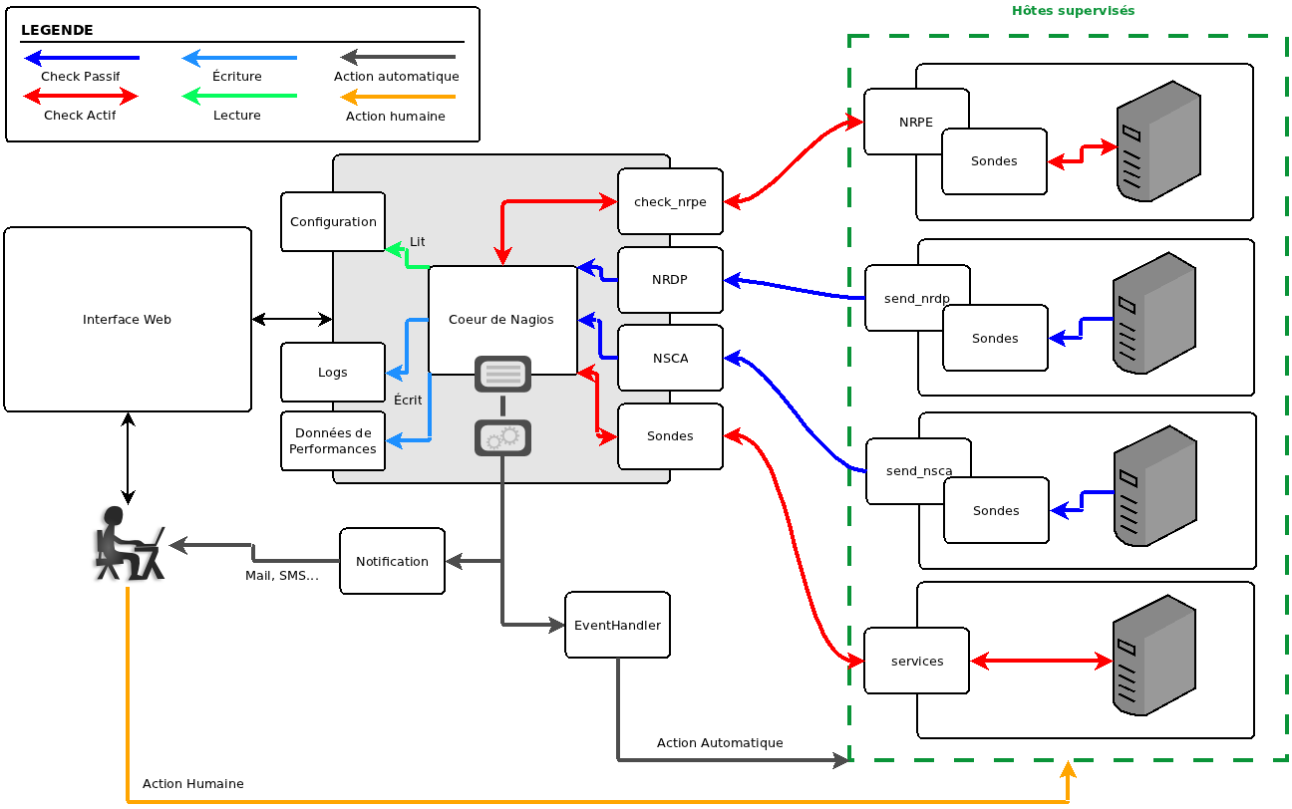


Illustration 25 : Nagios - Architecture autonome

Le cœur de Nagios est bien sûr, son ordonnanceur de contrôle.

Nagios va permettre de réaliser des contrôles dit actifs et passifs d'hôtes.

La configuration

La configuration du serveur Nagios et des éléments supervisés se fait via des fichiers plats.

Les contrôles

Les interrogations peuvent se faire aussi bien sur des serveurs via des agents ou sans, mais il peut aussi interroger des éléments réseaux sans agent, par exemple via SNMP

Il existe 3 agents Nagios pour les plate-formes Unix / Linux :

- NRPE (Nagios Remote Plugin Executor) qui fonctionne en mode actif.

  Le serveur Nagios va interroger les hôtes distants grâce à la commande check_nrpe. L'agent NRPE, installé sur l'hôte distant, va exécuter un script qui va retourner un état et si possible des données de performances.

  L'agent va lancer à la demande du serveur Nagios l'exécution en local de plugin, qui vont, par exemple, contrôler l'espace disque et indiquer l'occupation en fonction de seuils prédéfinis.

Voici un schéma officiel de fonctionnement de NRPE :

Illustration 26 : Nagios - Fonctionnement NRPE – Source : documentation officielle Nagios

Les communications entre le serveur Nagios et le client NRPE sont par défaut cryptées via SSL[27]

check_disk, check_load... sont des plugins qui vont vérifier des éléments locaux

check_http, check_ftp sont des plugins qui vont permettre de vérifier des éléments distants.

- NSCA (Nagios Service Check Acceptor) fonctionne en mode passif

  L'ordonnancement des vérifications est assuré, de façon locale, à chaque machine.

  Cela permet de n'avoir qu'un sens de connexion (sortant), ce qui est intéressant en termes de sécurité.

  NSCA est également utilisé pour les architectures distribuées.

Illustration 27 : Nagios - Fonctionnement NSCA - Source : documentation officielle Nagios

- NRDP (Nagios Remote Data Processor) le dernier né, qui peut être considéré comme une évolution de NSCA, fonctionne également en mode passif.

  Il ajoute, entre autres, une couche d'authentification, mais il permet également la remontée de plusieurs informations sur plusieurs lignes. Il envoie également son retour directement au cœur de Nagios, ce qui permet d'éviter un intermédiaire

27 SSL – Secure Sockets Layer – Protocole de sécurisation de communication internet

potentiellement consommateur de ressources.

Il peut être utilisé comme remplaçant de NSCA.

L'échange de données (crypté ou non) se fait via les protocoles web, ce qui permet de passer plus facilement les firewall

Illustration 28 : Nagios - Fonctionnement NRDP – Source : Site officiel de Nagios

Depuis l'initiation de ce projet, NRDP a fait son apparition, il est envisagé de migrer de NSCA vers NRDP qui est d'ailleurs la recommandation officielle de Nagios

Il existe d'autres agents également, mais ceux-ci ne sont pas officiellement supportés par Nagios comme :

- NSClient ++, qui peut être considéré comme un clone de l'agent NRPE pour les systèmes Windows.
- NRD (Nagios Result Distributor), qui peut être considéré comme une évolution de NSCA, surtout orienté architecture distribuée
- check_mk, qui lui englobe les fonctionnements de NRPE, NSClient, check_snmp et d'autres plugins, est bien plus puissant que les agents de base fournis avec Nagios.

  Voici le schéma de fonctionnement officiel :

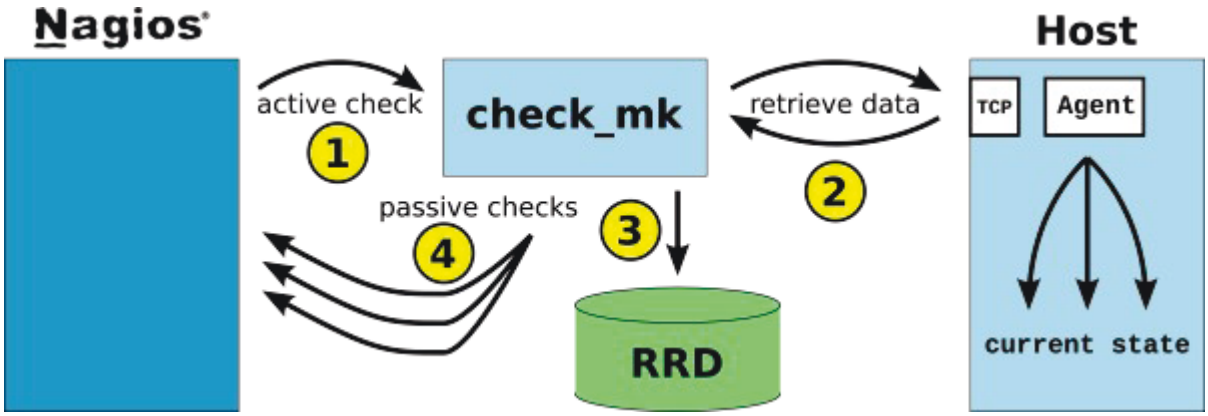


Illustration 29 : Nagios - Fonctionnement check_mk – Source : Site officiel de check_mk (Mathias Kettner)

1 : Nagios effectue une vérification active

2 : check_ml se connecte via TCP, puis check_mk_agent récupère toutes les données nécessaires et renvoie tout cela en tant que texte ASCII

3 : check_mk extrait les données de performances pour les stocker en base de données RRD

4 : check_mk récupère les données qu'il compare avec les seuils prédéfinis et soumet tous ses résultats au serveur Nagios via son service de vérification passif.

Il en existe d'autres encore, mais je ne les citerais pas, car ils sont beaucoup moins utilisés.

Et enfin, il est possible de réaliser des vérifications sans agent, directement à partir du serveur de supervision via des scripts, des interrogations de services réseaux.

États et Données récupérées :

Peu importe la méthode employée, le serveur Nagios doit recevoir un code retour exprimé toujours de la même manière :

- 0 = OK
- 1 = WARNING
- 2 = CRITICAL
- 3 = UNKNOWN

Ce sont donc ces états qui seront ensuite remontés au moteur qui prendra les décisions et lancera les actions programmées.

Il est possible également que le serveur Nagios récupère des données dites de performances.

Par exemple, le taux d'occupation d'un disque est une donnée de performance. Ces données seront réutilisées par des outils annexes et pourront, par exemple, servir à générer des graphes.

Types d'États :

Nagios distingue deux types d'états dans Nagios : les états SOFT et les états HARD.

Les états SOFT surviennent lorsqu'un contrôle revient avec un statut différent de OK ou UP, et que le service n'a pas été contrôlé autant de fois que spécifié dans la valeur « max_check_attempts »

Les états HARD surviennent lorsqu'un contrôle revient avec un statut différent de OK ou UP et que le service a été contrôlé autant de fois que spécifié dans la valeur « max_check_attempts »

Lorsqu'un le résultat d'un contrôle passif d'un hôte est reçu, les contrôles sont traités comme HARD sauf si l'option passive_host_checks_are_soft est activée.

Les notifications :

Lorsque le service renvoie toujours le même type d'erreur, l'alerte passe alors en état HARD et Nagios envoie ses notifications (courriel, SMS, etc.).

À la suite d'une notification, il est d'usage qu'un exploitant de la solution de supervision intervienne pour le solutionner ou alors pour l'acquitter.

Le Gestionnaire d'événements (EventHandler) :

Les gestionnaires d’événements sont des commandes externes qui seront exécutées automatiquement à chaque fois qu'un changement d'état d'hôte ou de service se produit.

On peut les utiliser pour résoudre les problèmes de manière préventive, mais aussi par exemple pour :

- Redémarrer un service
- Créer un nouveau ticket dans un système de helpdesk
- Enregistrer des événements dans une base de données
- Redémarrer un hôte

Interface Web :

L'interface web a principalement un rôle de visualisation.

Il est possible de réaliser des actions qui vont de l'acquiescement d'une alarme au redémarrage d'un serveur si l'eventhandler est défini.

Illustration 30 : Nagios - Interface Web

Actions d'écriture :

Le serveur Nagios va conserver les données de performances récupérées depuis les divers contrôles, mais aussi enregistrer les retours dans les fichiers de logs.

6.3.2.1.2. Architecture distribuée

Précédemment, il a été présenté l'architecture globale de Nagios, ce qui a permis de présenter le fonctionnement standard et autonome.

Plus l'infrastructure à superviser va se complexifier, plus les besoins en termes de ressource vont augmenter.

Pour palier à cela, il est possible de répartir la charge via une architecture distribuée.

L'architecture distribuée est constituée d'un serveur Nagios et d'un client NSCA (send_nsca).

Il n'y a pas de limite, hors capacité matérielle, en nombre de Nagios « fils ».

Chaque Nagios « fils » va remonter les données de supervision via le client NSCA au démon NSCA.

Celui-ci va ensuite écrire ses données dans le fichier de commande externe (nagios.cmd)

Le serveur Nagios central, dit « père », va interroger régulièrement la queue de commande externe, la traiter, puis inscrire les statuts dans le fichier de statuts.

Ces statuts seront consultables via l'interface web.

La majorité des contrôles se font en mode passif. Mais pour assurer une pertinence des données de supervision, il est prévu des mécanismes de validation des données remontées, ceci afin de générer des contrôles actifs et de prévenir une éventuelle indisponibilité d'un serveur distribué.

Le serveur Nagios, dit « père », est celui qui va s'occuper d'envoyer les notifications, d'exécuter des scripts du gestionnaire d'événements, de déterminer l'état des hôtes...

Les serveurs Nagios distribués, dit « fils », sont des installations « simplifiées ».

En effet, ils n'ont pas besoin d'interface web, ne s'occupe pas de notifications...

Le serveur distribué va transmettre au serveur Nagios central ses résultats grâce à une commande OCSP (Obsessive Compulsive Service Processor) ou OCHP (Obsessive Compulsive Host Processor)

Il s'agit de commande de remontée de contrôle de service ou hôte.

Ces commandes utilisent send_nsca pour remonter l'information à NSCA.

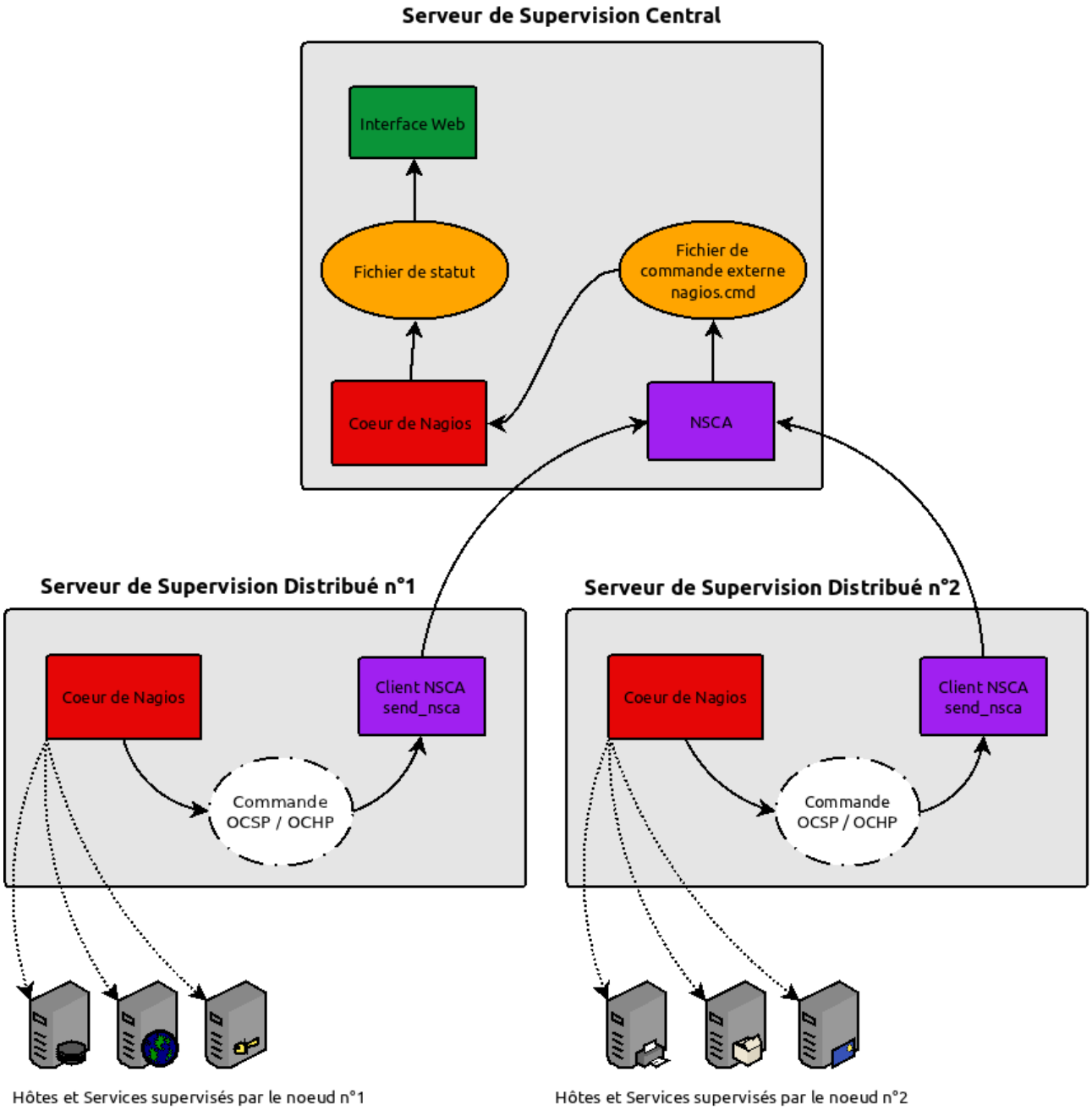


Illustration 31 : Nagios - Architecture distribuée

6.3.2.1.3. Architecture Haute-Disponibilité

Avec une architecture distribuée, il est donc possible de répartir la charge.

Cette architecture présente une faiblesse, car si le serveur central devient indisponible, c'est toute la supervision qui devient indisponible, un comble...

Pour palier à ce manquement, il est possible de réaliser une architecture Haute-Disponibilité simplement avec Nagios.

Il va y avoir un serveur dit « maître » qui va se comporter comme un serveur autonome, et un serveur dit « esclave » qui va superviser le serveur maître et reprendre les contrôles à

son compte en cas d'indisponibilité du « maître ».

Cela nécessite la mise en place d'un système de copie des configurations.

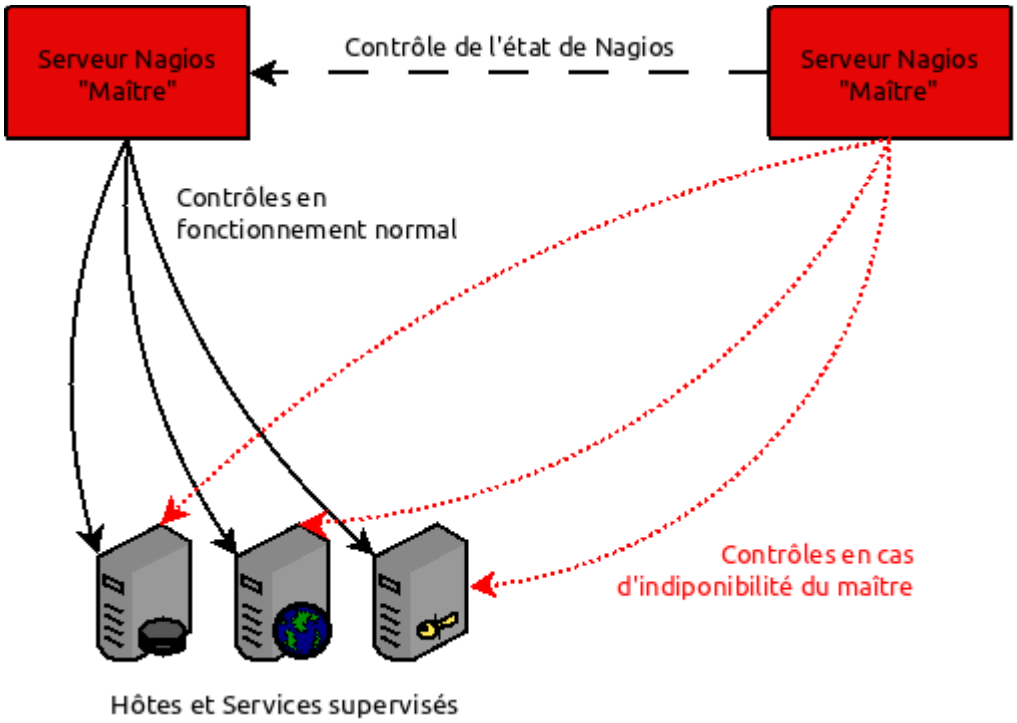


Illustration 32 : Nagios - Architecture Haute Disponibilité

6.3.2.1.4. Architecture Haute-Disponibilité avec répartition de charge

Les deux précédentes architectures répondent à deux problématiques majeures, les performances et la disponibilité de la solution de supervision.

Il est possible de conjuguer ces deux architectures pour en faire une complète, performante et hautement disponible.

Malheureusement, tout n'est pas prévu nativement dans Nagios pour mettre en place ce type d'Architecture.

Les contraintes se situeront notamment au niveau de la disponibilité des données entre le serveur « maître » et « esclave »

Il faudra prendre en compte également l'envoi des données via send_nsca.

En effet, celui-ci ne va pas gérer nativement une indisponibilité du serveur maître.

Les solutions de Haute-Disponibilité sont tout à fait possible, en s'appuyant sur d'autres technologies qui sont dédiées à des architectures complexes.

Voici le schéma logique de ce type d'architecture :

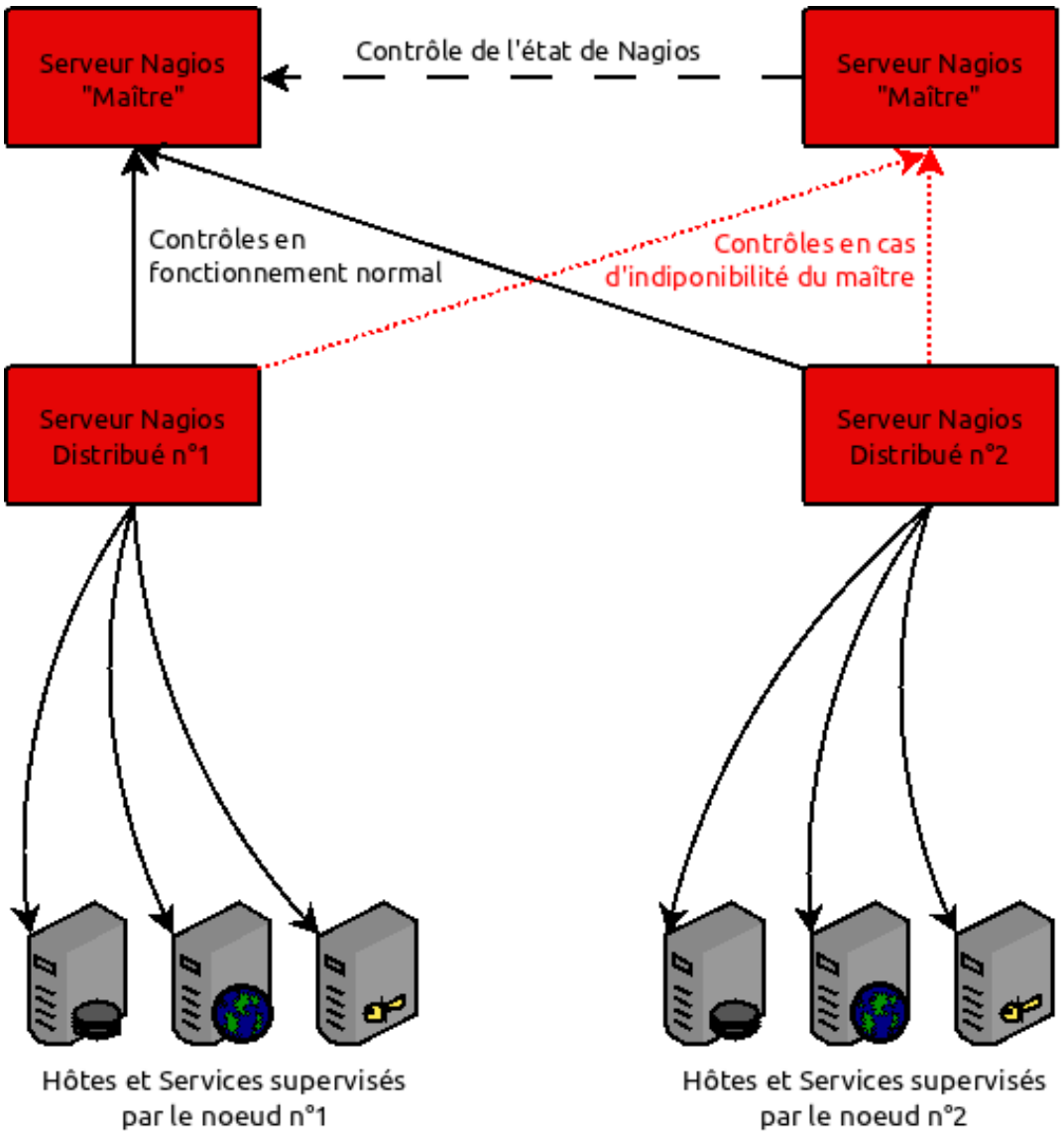


Illustration 33 : Nagios - Architecture Haute-Disponibilité avec répartition de charge

6.3.2.1.5. Nagios et le stockage en base de données

Comme expliqué précédemment, Nagios stocke ses données de supervision via des fichiers plats.

Pour palier à cela, il existe un plugin permettant de stocker ces informations en base de données (MySQL).

NDOUtils (Nagios Data Output Utils) va permettre de stocker les configurations, les états et les événements de nagios dans une base de données MySQL permettant l'utilisation de ces données par des tiers, comme Centreon que nous allons voir par la suite.

NDOUtils est composé de 4 éléments :

- ndomod : module chargé par Nagios de transférer les données vers un fichier plat, un socket UNIX ou un socket TCP. Il est appelé un Broker.
- file2sock : outil chargé d'écrire dans un socket UNIX ou TCP les données récupérées depuis un fichier plat,
- log2ndo : outil chargé d'écrire dans un socket TCP ou UNIX les données récupérées depuis les fichiers journaux de Nagios,
- ndo2db : démon qui ouvre un socket UNIX ou TCP et insère les éléments reçus dans une base de données.

Ce qui est le plus couramment utilisé est ndomod qui transmet les données à ndo2db pour le stockage en base.

File2sock et log2ndo sont utilisés dans des cas particuliers.

Il est tout à fait possible de faire fonctionner NDO en mode mono-serveur, comme en mode multi-serveurs.

Fonctionnement mono-serveur :

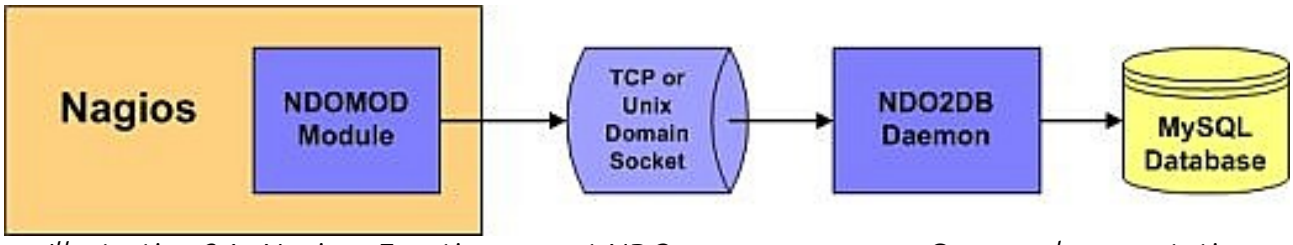


Illustration 34 : Nagios - Fonctionnement NDO en mono-serveur - Source : documentation officielle Nagios

Le broker NDOMOD transfert les données soit via TCP, soit via un socket Unix dans un format lisible par NDO2BD qui va se charger de stocker en base de données MySQL.

Fonctionnement multi-serveurs :

Illustration 35 : Nagios - Fonctionnement NDO en multi-serveurs - Source : Site officielle Nagios

Dans ce cas de figure, il y a un broker Ndomod par instance Nagios qui va transmettre ses données de la même manière au ndo2db.

Si la solution de supervision est dans une architecture distribuée, ndo2db sera sur le serveur central.

6.3.2.2. Fonctionnalités

Supervision en temps réel :

- Gestion de disponibilité de services réseaux et d'hôtes.
- Gestion des ressources (données interprétables pour de la gestion de performances)
- Gestion d'alerte utilisateur (mail, sonore...)
- Historique
- Gestion des temps d'arrêt
- Hiérarchisation des hôtes/services

Résolution rapide d'incidents :

- Envoi d'alerte par mail, sms, téléphone, ou encore une alerte audio.
- Il est possible d'exécuter des commandes à distance automatisées (EventHandler)

Rapport et tendance :

- Intégration facile avec des outils tierces
- Statistiques quotidiennes, mensuelles, et annuelles

Supervision avec les agents :

- Contrôle Actif, via NRPE
- Contrôle Passif, via NSCA ou NRDP

Supervision possible sans agent :

- Supervision de services distants (FTP, SSH, HTTP,...)
- Support du protocole SNMP v1,2,3
- Support du protocole IPMI
- Gestion de traps (événements) SNMP

Escalade et notification :

- Notifications répétées
- Escalades illimitées
- Message de retour à la normale
- Être averti de tout problème résolu.
- Plage de notification (jour, horaire)

Tableau de bord :

- Reporting (disponibilité, tendances...)
- Représentations graphiques, circulaires, par dépendance...

Sécurisé :

- Authentification par adresse IP
- Échanges NRPE cryptés via SSL

Extensible :

- Une multitude de plugins

- Création de module facile
- Facilement interfaçable

Visualisation :

- Possibilité de prédéfinir des groupes d'hôtes ou de services
- Cartographie

Architectures :

- Mono-serveur
- Distribuée
- Haute-Disponibilité
- Hautement disponible avec répartition de charge.

Ce qui n'est pas couvert nativement par Nagios l'est souvent par ses plugins ou des solutions tierces.

6.3.2.3. Écosystème

Ces solutions sont l'écosystème de Nagios et c'est l'une de ses plus grandes forces.

En effet, Nagios dispose d'une très grande communauté, sûrement l'une des plus grandes pour un projet opensource.

Il existe tellement d'extensions possibles qu'un site est dédié à leur recensement.

2862 projets autour de Nagios sont recensés dans 418 catégories sur Nagios Exchange - http://exchange.nagios.org/

L'écosystème Nagios est divisé en plusieurs types ou familles :

- Les plugins – sondes de contrôle
- Les interfaces graphiques, alternative à l'interface par défaut assez pauvre en termes de fonctionnalités et ergonomie.
- L'ajout de fonctionnalités, comme la gestion de graphique de performances, la cartographie, le déploiement de masse...
- Le remplacement de briques Nagios pour répondre à des limitations ou besoins spécifiques.
- L'interfaçage avec d'autres solutions (outils de ticket, d'inventaire, de cmdb...)
- Le reporting

Toutes les sondes qui seront créées par Alter Way Solutions seront publiées sous licence libre GPLv3 et seront mises à disposition sur Nagios Exchange

Les plugins sont des scripts écris souvent en perl, shell, python ou autre.

Si vous avez besoin de superviser un service en particulier, il est probable que quelqu'un avant vous ait eu le même besoin et qu'il ait déjà créé le plugin souhaité.

Vous trouverez alors facilement une sonde qui va vous permettre de superviser les éléments hétérogènes de votre système d'information.

Voici une liste non-exhaustive des catégories de plugins :

- Sauvegarde et Restauration
- Base de données
- Messagerie et Groupware[28]
- Matériel
- Systèmes d'exploitation
- Réseau
- Téléphonie
- …

La liste des domaines couverts est très complète.

Il faut néanmoins se méfier de ces plugins, car leur richesse est aussi une faiblesse.

Il peut être difficile de choisir un plugin si plusieurs sont sensés jouer le même rôle. Comment déterminer ce qui correspond le plus au besoin, lequel est le plus pérenne ?

Ou encore, ils peuvent simplement ne pas être compatibles avec votre environnement.

Ces sondes peuvent représenter un risque, car mal pensées, et contenir des failles de sécurité ou poser des problèmes de performances....

Pour palier à ces richesses/faiblesses, le site fournit un système de notation, ce qui permet, grâce à l'intelligence collective de faire rapidement un premier tri.

Bien sûr, tous les projets autour de Nagios ne sont pas forcément répertoriés sur ce site.

Centreon, est une extension de Nagios, qui en fait une solution de supervision à part entière et complète.

28 Groupware – outil de travail collaboratif

6.3.2.4. Présentation de Centreon

6.3.2.4.1. Le Projet Initial

Né en 2003, sous le nom d'Oreon, Centreon était destiné à fournir une interface de configuration à Nagios.

Depuis 2005, Centreon est développé désormais par une société Française, nommée Merethis.

Au fur et à mesure, ses fonctionnalités se sont considérablement étendues.

Centreon est désormais une solution complète de supervision (gestion d'incident, de performance, cmdb, découverte automatique, reporting...)

En septembre 2011, le cabinet de recherche et de conseil Gartner, a publié une étude menée à l'international sur les différentes solutions de supervision Open Source.

Gartner cite Centreon comme l'une des solutions de supervision Open Source complète et crédible.

Centreon propose, depuis peu, son propre moteur de supervision qui est un Nagios amélioré.

Il fonctionne également avec Shinken et Icinga

6.3.2.4.2. Fonctionnalités

Monitoring temps réel :

- Détection des pannes
- Détection de la disponibilité
- Définition avancée de seuils pour les alertes
- Interrogation active (pull)
- Réception passive et résultats (push)
- Réception de traps SNMP
- Diagnostic opérationnel
- Regroupement des informations par groupes d'hôtes
- Regroupement des informations par groupes de services
- Vues agrégées
- Agrégat de mesure de service (Meta service)

- Planification de temps d'arrêt programmés
- Prise en compte des problèmes par les utilisateurs
- Ajouts de commentaires
- Possibilité de parcourir les logs avec filtres de recherche
- Période et fréquence de collecte paramétrables

Répartition de charge/Haute disponibilité :

- Possibilité d'éclatement de la charge de manière :
  - stratégique (sécurité);
  - géographique (WAN);
  - topologique
- Mise en place de satellite « fail-over »
- Mise en place de satellite « pré-production »
- Possibilité de mise en place de haute disponibilité :
  - Base MySQL répliquée
  - Interface Web
  - Moteur de supervision
  - Graphiques / Rapports

Traitement des performances :

- Historisation des données de performance, elles sont non-volatiles.
- Affichage des données sous forme de graphiques RRDTool
- Comparaison des métriques / graphiques
- Affichage de graphiques de statuts (« Trends »)
- Suivi de l'évolution des données dans le temps
- Export CSV/XML
- Corrélation entre les données de performance et les états
- Modèles d'affichage des graphiques paramétrables
- Période de visualisation paramétrable

Contrôle des accès utilisateurs :

- Définition de groupes d'accès
- Limitation d'accès aux pages de l'interface
- Limitation de visualisation des groupes d'hôtes
- Limitation de visualisation des groupes de service
- Authentification LDAP
- Suivi des actions utilisateurs

Configuration flexible :

- Compatibilité Nagios 3
- Gestion de modèles de configuration
- Liaison entre les modèles d'hôtes et de services
- Gestion de bibliothèque de modèles applicatifs
- Héritages des modèles à n niveaux
- Collecte et gestion automatique des traps SNMP
- Définition de macro « sur mesure »
- Gestion de la topologie réseau
- Configuration atomique des indicateurs

Notification hiérarchisée :

- Dépendances « métiers »
- Dépendances du réseau
- Pont vers des outils de ticketing (Request Tracker, etc)
- Notification Mail, SMS ou autres
- Escalades hiérarchisées

Tableaux de bord :

- Statistiques journalières basées sur la durée des états
- Statistiques journalières basées sur le nombre d'alertes
- Affichage des rapports par hôte

- Affichage des rapports par groupe d'hôtes
- Affichage des rapports par groupe de services
- Période de visualisation paramétrable
- Export des rapports au format CSV
- Timeline interactive pour suivre l'évolution des rapports

Modularité :

Possibilité d'intégrer et de développer des modules complémentaires :

- Centreon Syslog – Licence libre GNU GPL
- Centreon NTOP – Licence libre GNU GPL v2
- Centreon Map – Licence Propriétaire Merethis
- Centreon Business Activity Monitoring - Licence Propriétaire Merethis
- Centreon Business Intelligence - Licence Propriétaire Merethis
- Centreon CLAPI – Licence libre GNU GPL v2
- Centreon Auto Deployment Tool - Licence Propriétaire Merethis
- Centreon Disco - Licence Propriétaire Merethis

Pilotage :

- Possibilité de piloter Centreon en ligne de commande (CLAPI)
  - ajout d'hôtes
  - redémarrage de Nagios
  - génération des configurations
- Chargement des configurations au format CSV ou NAGIOS

6.3.2.4.3. Architecture

Voici un schéma expliquant l'interfaçage entre Nagios et Centreon.

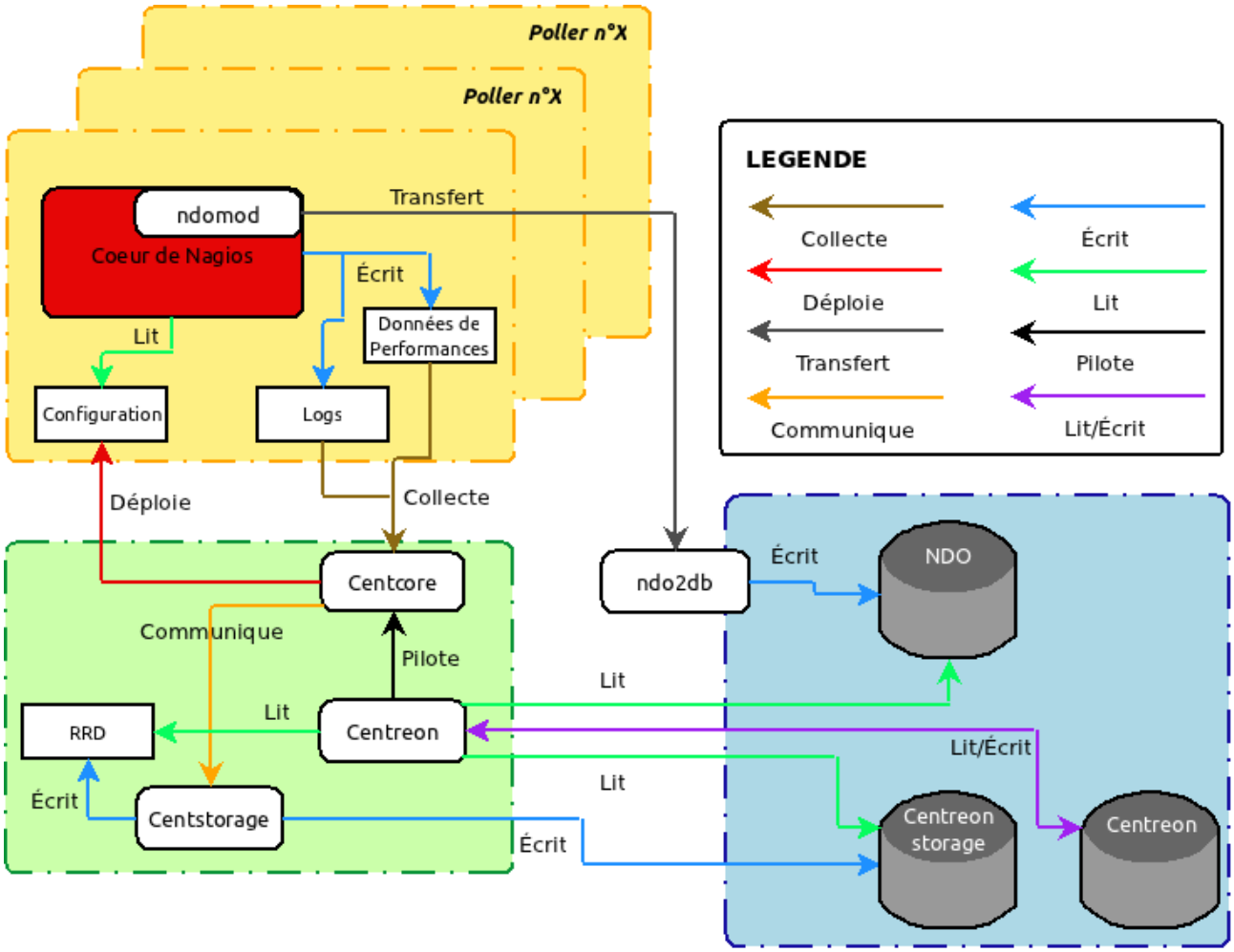


Illustration 36 : Nagios et Centreon

Un ou plusieurs Nagios vont transférer les données de supervision via ndomod à ndo2db qui, lui, va les écrire dans la base de données NDO.
Ces données seront consultées par Centreon
Centreon va stocker toutes ses données, comme sa configuration, dans la base de données Centreon.
Centcore est le démon qui va permettre de bien communiquer en cas d'architecture distribuée.
Il va se charger de déployer la configuration réalisée via l'interface web à tous les collecteurs Nagios.
Centcore collecte les logs et les données de performances et les transmet à Centstorage.
Centstorage est le démon qui va permettre d'injecter les données de performance à la base de données « Centreon Storage » et rrd pour la partie métrologique de centreon.

6.3.2.4.4. Évolutions de Centreon

Merethis développe actuellement des modules et évolutions de Centreon qui méritent de s'attarder quelque peu, et qui pourront justifier d'une intégration future.

6.3.2.4.4.1. Centreon Broker

Centreon Broker est une alternative au broker proposé par Nagios, NDOUtils.

Il a pour objectif d'apporter de nouveaux services, mais aussi d'améliorer la sécurité, les performances et la stabilité.

6.3.2.4.4.2. Centreon Engine

Ce projet vise à apporter de nouvelles façons de penser et de nouvelles fonctionnalités, tout en conservant une compatibilité totale avec Nagios, Icinga et Shinken. Les développeurs de Centreon et Merethis concentrent leurs travaux sur les points suivants :

- l'augmentation des performances
- la modernisation de l'architecture (services web, modules, utilisation de framework,...)
- l'équilibrage de charge
- la haute disponibilité
- la simplicité d'utilisation.

L'interface CGI Nagios n'a pas été incluse dans ce projet, car les utilisateurs de Centreon Engine doivent toujours être en mesure d'utiliser l'interface Web Centreon.

6.3.2.4.4.3. Centreon CLAPI

Centreon CLAPI, Command Line API, permet de piloter un serveur Centreon en ligne de commandes. Il vous donne la possibilité d'ajouter, de modifier mais aussi de supprimer tous les objets de configuration de Centreon (hôtes, services, contacts, groupes, …).

L'apparition d'une interface CLI offre des possibilités d'industrialisation et d'interfaçage intéressants avec d'autres outils.

6.3.2.4.4.4. Extensions de Centreon

Voici un graphique présentant les différentes extensions de Centreon.

Ce graphique différencie les licences des différentes extensions proposées.

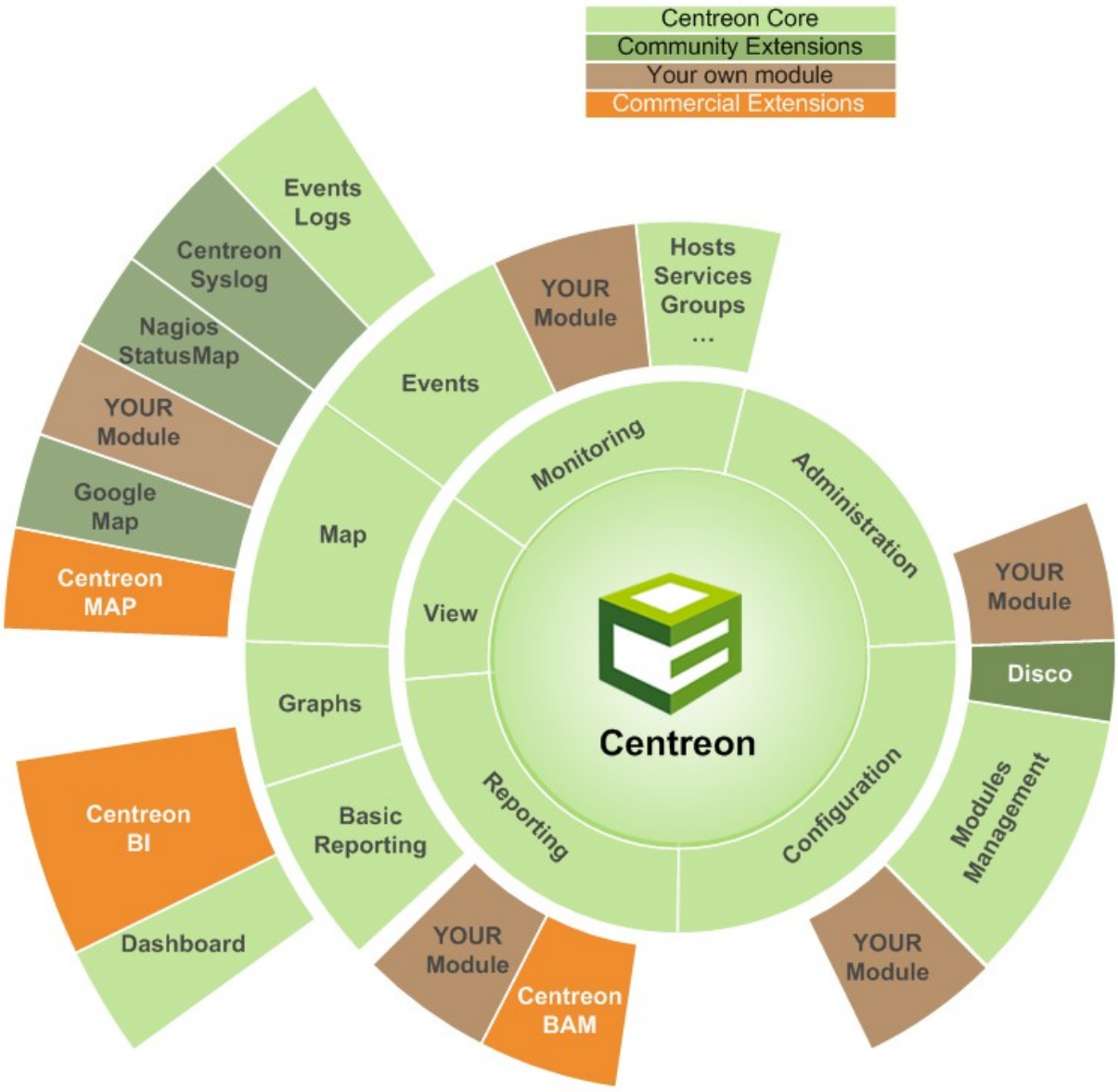


Illustration 37 : Centreon – Extensions – Source : Site Officiel de Centreon

Centreon est un noyau souple et très performant sur lequel il est possible d'intégrer un nombre illimité de modules.

6.3.3. Le choix définitif de la solution

Pour rappel, la solution de supervision aura pour but de surveiller les parcs informatiques de nos différents clients infogérés.

Elle va donc devoir satisfaire différents éléments :

- Facilité de déploiement
- Facilité de prise en main

    - mise en œuvre
    - exploitation par le niveau 1
- Surveillance d'éléments hétérogènes
    - Systèmes d'exploitation
    - Services
- Multi-sites
- Modulable et évolutive
- Investissement limité

Afin de répondre à toutes ses exigences, le choix s'est porté sur la solution de supervision Nagios / Centreon.

Voici le tableau synthétisant les fonctionnalités de Zabbix, Nagios sans et avec Centreon (et quelques extensions tierces) :

Solutions	Supervision systèmes	Supervision Réseaux	Supervision Applicative	Génération de graphe	Notification	Compatible SNMP	Découverte automatique	Rapports	Cartographie	Architecture distribuée	Agent	Sans Agent	Action automatique	Extensions	Logs et de gest. d'événements	Corrélation	Escalade	Gestion ACL	Gestion des SLA	Vues techniques et métiers	Interface mobile	Temps d'arrêts	Configurations centralisées	Inventaire	Outils de déploiement
Zabbix	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		
Nagios	✓	✓	✓		✓	✓		✓		✓	✓	✓	✓	✓	✓		✓					✓			
Nagios/Centreon	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		

On peut remarquer que la solution la plus complète est Zabbix.

Centreon, permet de combler les manquements de Nagios, du moins ceux qui sont nécessaires à ce projet.

D'autres extensions Nagios vont pouvoir couvrir ce qui n'est pas couvert nativement par Centreon.

Nagios est une solution connue et reconnue. Cette notoriété va faciliter les démarches auprès des services informatiques de nos clients.

En effet, afin d'installer les clients nécessaires à la supervision des machines, ou de Nagios distribués, il faudra l'autorisation des responsables de la sécurité du système d'information.

L'ouverture de port au niveau du firewall pourrait être facilitée.

J'utilise Nagios et Centreon depuis plusieurs années, j'ai participé au déploiement de

Nagios / Centreon dans un grand groupe français qui représentait un parc de plus de 1300 serveurs. J'en ai donc une certaine connaissance qui va me faciliter la prise en main.

Ceci offre une productivité rapide en adéquation avec la charge de travail qu'il est possible d'octroyer à ce projet.

Les environnements multi-sites sont gérés sans problème via Nagios / Centreon

Les environnements hétérogènes des clients et la diversité des services à superviser ont également été de poids dans le choix final de la solution.

Les deux solutions de supervision sont à un niveau de maturation technologique tout à fait satisfaisant.
J'estime par contre que la maturité d'usage de Nagios / Centreon est plus aboutie, surtout au niveau de la facilité d'usage et de mise en œuvre par un utilisateur, de la quantité de documentation autour de ce projet et de sa facilité d'intégration avec des outils tierces.

La richesse des plugins Nagios offrant une réponse facile et rapide à beaucoup de besoins de sondes et autres.

Zabbix ne permettra pas si facilement de s'adapter aux environnement hétérogènes des clients. La mise en place de sondes spécifiques sera plus difficile, ce qui pourrait être bloquant.

Les ressources à attribuer sur le développement de sonde sont limitées. La facilité de créer ses propres plugins Nagios est donc une force.

Zabbix couvre largement le périmètre fonctionnel recherché. Néanmoins l'investissement nécessaire à sa mise en place en rapport à sa valeur ajoutée n'était pas suffisant pour en faire notre choix définitif.

L'étude approfondie de ces solutions m'a permis d'acquérir de solides connaissances fonctionnelles sur deux des plus importantes solutions de supervision libre du marché

7. Mise en place du projet de supervision

Par définition, un service d'infogérance est l'externalisation de tout ou partie de la gestion informatique du S.I. d'un client par une société informatique.

Un service d'infogérance en société informatique gère donc plusieurs systèmes d'information complet ou non.

Alter Way Solutions a donc décider de mettre en place une solution de supervision pour ses clients.

Cette solution se doit donc d'être compatible avec un grand nombre d'environnements et d'offrir la possibilité d'avoir une architecture distribuée.

À savoir que le service d'infogérance n'est pas un service 24h/24 et 7j/7, il n'y a donc pas de périodes d'astreintes.

7.1. Architecture de la solution de supervision

Un serveur basé sur la distribution Ubuntu Serveur 10.04 LTS a été installé.

Nagios et Centreon sont installés via les sources et mis à jour régulièrement via des scripts permettant d'automatiser ces mises à jour.

Pour faciliter la gestion, il est préconisé d'installer les agents NRPE ou NSCA via les paquets propres à chaque distribution. Une gestion de version des sources sur chaque serveur n'est pas envisageable sur le long terme.

La solution de supervision est de type distribuée et fonctionne actuellement, soit avec l'interrogation d'agent NRPE, soit avec la remontée de vérifications effectuée par NSCA ou via des vérifications par script ou encore par SNMP.

Mais il arrive également, selon les besoins, qu'un collecteur distant soit mis en place et que seul ce collecteur remonte les informations auprès du serveur Nagios / Centreon centralisé.

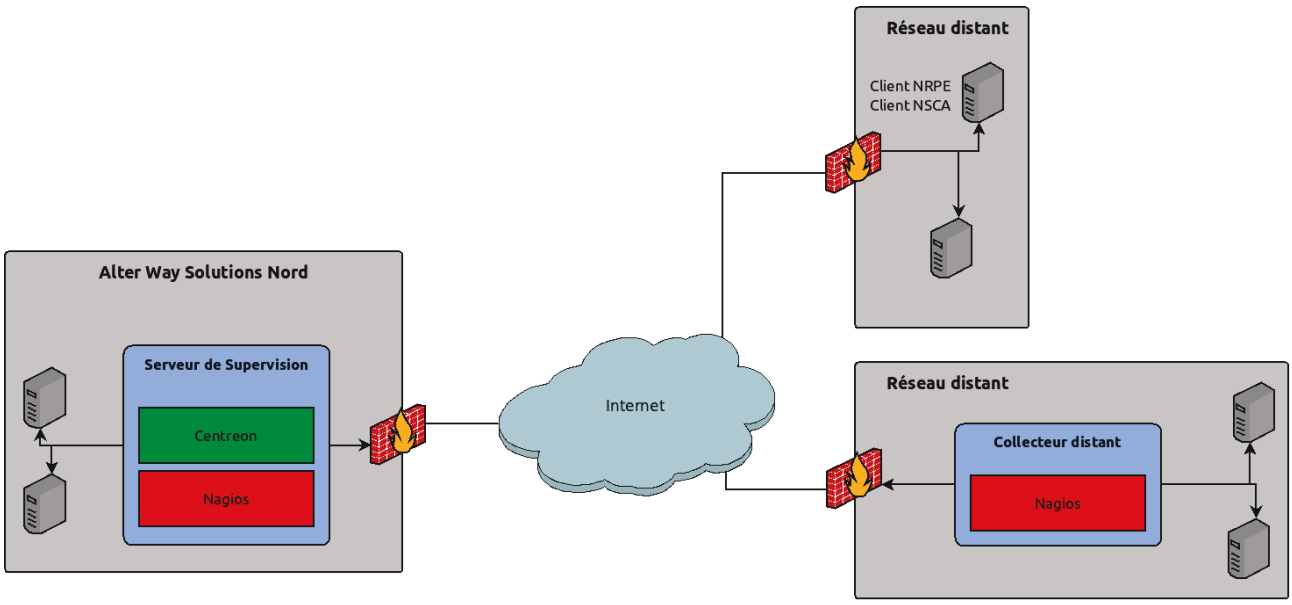


Illustration 38 : Architecture de la solution de supervision

La flexibilité qu'offre Nagios / Centreon permet de superviser tous les clients qui le souhaitent.

7.2. Méthodes de vérification

Nous sommes reliés par des connexions VPN avec la globalité de nos clients.

Il a été décidé de privilégier les contrôles dits Actif, pour cela le client NRPE a été installé sur les serveurs distants.

Il est également possible de réaliser des contrôles directs via des scripts ou des interrogations SNMP.

Une communauté snmp dédiée a été créé pour les entités n'en disposant pas encore, et pour celle qui utilisait déjà SNMP, les sondes ont été adaptées en fonction.

Sur les plus grosses infrastructures, il est possible et conseillé de mettre en place un collecteur Nagios qui va renvoyer ses données via NSCA ou NRDP.

Les échanges SNMP n'ont pas tous pu être mis en version 3 (plus sécurisée) à cause de certaines versions d'implémentations sur les distributions GNU/Linux agées.

7.3. Les types de supervision en rapport avec le contrat d'infogérance

Pour rappel, voici les différents niveaux des éléments à superviser :

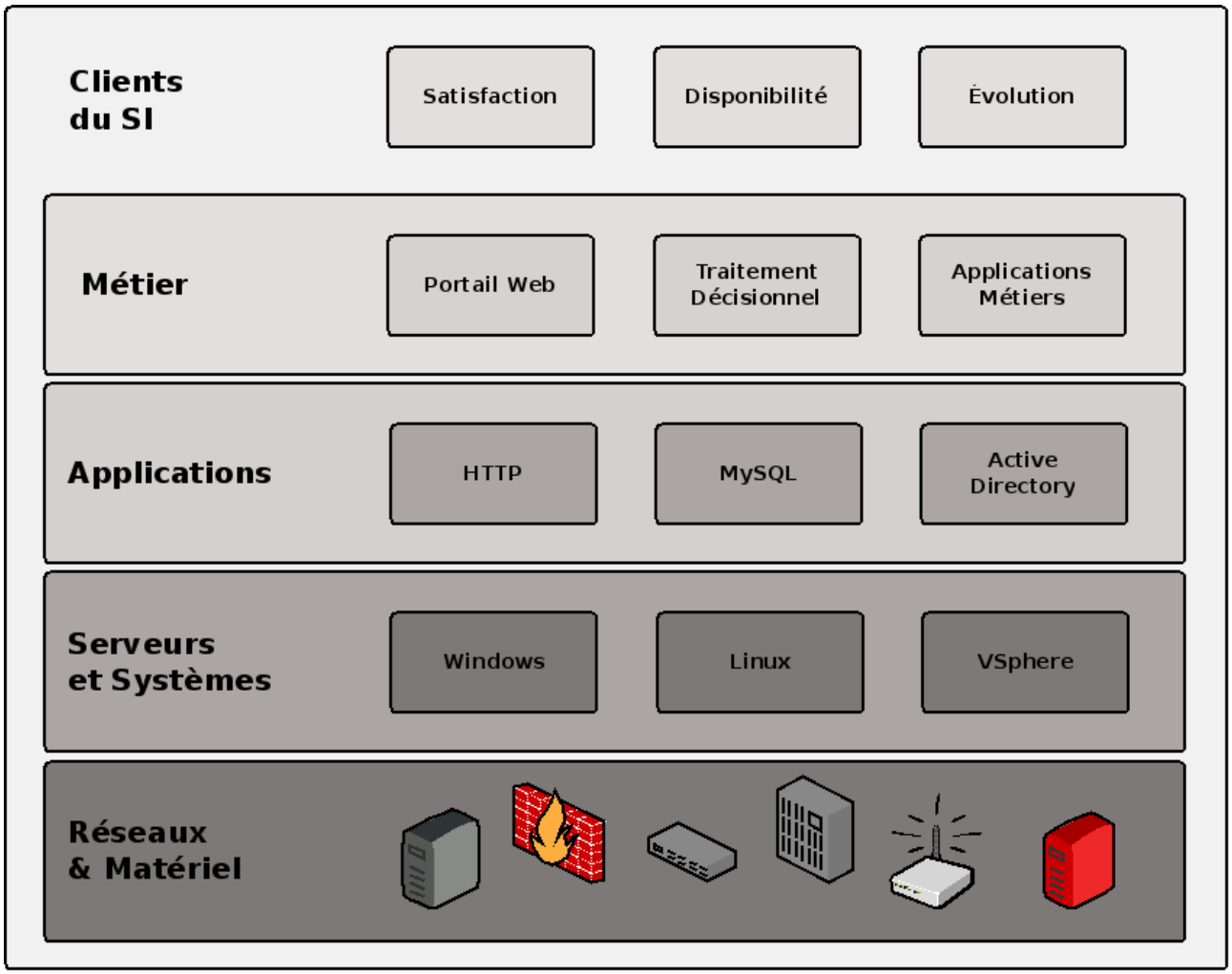


Illustration 39 : Les différents types de supervision

Il a été décidé de segmenter les différentes sondes de supervision à partir de ces niveaux de supervision et en rapport avec leur complexité de mise en place.

7.3.1. Les sondes de base officielles Nagios / Centreon :

Il s'agit à chaque fois des plugins officiels fournis par Nagios ou Centreon.

Dans tout type d'infrastructure, ces contrôles seront sûrement à utiliser.

Ces sondes couvrent des contrôles classiques et se mettent en place rapidement :

- La disponibilité (ping...)

- La surveillance des ressources serveurs (espace disque...)

Elles sont désormais inclues dans les nouveaux contrats d'infogérance.

Nous avons donc intégré certains clients historiques d'infogérance à la solution de supervision et continuons d'intégrer les anciens clients au fur et à mesure.

7.3.2. Les sondes spécifiques officielles Nagios / Centreon et Nagios :

Il s'agit à chaque fois de plugins officiels fournit par Nagios ou Centreon, ceci afin de garantir une fiabilité, une pérennité et des coûts de déploiement maîtrisés.

Ces services sont plus complexes à mettre en place et sont dits spécifiques, car ils dépendent du système d'information du client.

On va donc surveiller :

- Des applications (serveur web, de base de données...)
- Des flux réseaux
- Des services réseaux

Par exemple, nous allons superviser des applications web pour certains clients, alors que pour d'autres, ce sera de la messagerie...

La mise en place de ces sondes est, à ce jour, gratuit, mais il pourrait être envisagé de mettre en place une offre commerciale qui serait vue par le client comme une ou des options à rajouter à son contrat d'infogérance.

7.3.3. Les sondes spécifiques Communautaires :

Les sondes dites communautaires sont les sondes que l'on peut trouver sur le site Nagios Exchange présenté ci-dessus, ou sur d'autres sites internet.

Il s'agit également des sondes que l'on pourrait être amené à développer pour des besoins spécifiques. Ces sondes seraient d'ailleurs redistribuées à la communauté via Nagios Exchange.

Il est arrivé de corriger des bugs de fonctionnement sur certaines sondes, ces corrections ont de suite été soumises à leur auteur.

Les sondes communautaires n'étant pas forcément maintenues, il est possible qu'il faille les modifier, ou encore s'en servir de socle pour répondre au besoin du client.

C'est pourquoi la mise en place de ces sondes et beaucoup plus complexes et nécessite une prestation spécifique.

La mise en place de ces sondes (spécifiques et communautaires) est à ce jour proposée gratuitement, mais il est envisagé de mettre en place une offre commerciale sous forme d'option au contrat d'infogérance.

8. Mise en situation - Intégration d'un client type

Pour illustrer au mieux la méthodologie employée, je vais prendre pour exemple l'un de nos clients multi-sites qui a été intégré à la solution de supervision, aux fortes contraintes de sécurité et aux spécificités variables.

Ce client est une filiale d'un groupe mondial de l'industrie de l'énergie.

8.1. Définition du système d'information cible

La société cible a souhaité garder l'anonymat, les informations permettant de l'identifier auront donc volontairement été faussées.

L'infrastructure est répartie sur 3 sites distants et disposant d'utilisateurs nomades.

De plus, des serveurs sont hébergés dans deux DataCenter[29] distincts Alter Way Hosting

Sur chaque site distant, il y a un serveur qui fournit un certain nombre de services.

8.1.1. Architecture

Les schémas ci-dessous présentent grossièrement l'architecture cible.

L'architecture est divisée en deux parties :

- À gauche, la partie « sécurisée » qui se trouve derrière le cluster de firewall situé dans l'un des Datacenter de Alter Way Hosting et qui donne sur deux MPLS[30] pour ensuite accéder aux sites du client cible.
- À droite, il s'agit de la partie « ouverte » sur internet. On va retrouver les connexions de nomades ou de travailleurs à domicile, et les différents réseaux de prestataires de services comme ceux d'Alter Way Solutions.

Une version plus grande du schéma pourra être retrouvée en annexe.

29 DataCenter – Centre de traitement des données, qui se présente comme un lieu où se trouvent différents équipements électroniques, surtout des ordinateurs et des équipements de télécommunications.

30 MultiProtocol Label Switching – qui peut être considéré comme un VPN opérateur, il s'agit d'un réseau privé de type WAN.

Illustration 40 : Architecture WAN du client cible

Voici une explication plus détaillée de l'architecture cible.

Illustration 41 : Archicture détaillée Alter Way Hosting - Site principal

Le réseau situé au Datacenter d'Alter Way Hosting à Saint Denis est composé de :

- Cluster de firewall Astaro, fournissant des services de sécurisation de flux, de proxy filtrant, de gestion de VPN...
- L'architecture de messagerie qui est composée de :
  - Un serveur d'envoi de mail et un serveur de noms de domaine
  - Un serveur de messagerie
  - Un serveur Open-Xchange
- Un serveur de fichiers dédié aux utilisateurs Nomades
- Deux routeurs BGP[31] avec répartition de charge visant à fournir la connexion internet. Ces routeurs ne sont pas gérés par nos soins.
- Deux routeurs HSRP29 avec répartition de charge qui sont fournis par l'opérateur du MPLS. Ces routeurs ne sont pas gérés par nos soins.

Voici un schéma du site de secours dans un second DataCenter Alter Way Hosting

Illustration 42 : Archicture détaillée Alter Way Hosting - Site secondaire

Sur le second Datacenter, il y a un serveur qui a plusieurs rôles :

- serveur d'envoi de mail secondaire
- serveur de nom de domaine secondaire
- serveur de messagerie

Les services d'envoi de mail et de noms de domaine secondaire sont utilisés de manière

31 Border Gateway Protocol (BGP) est un protocole d'échange de route utilisé notamment sur le réseau Internet

constante.

Il y a une bascule automatique des services en cas d'indisponibilité du site principal pour la messagerie.

Voici un schéma de l'interconnexion des sites distants et d'Alter Way Hosting

Illustration 43 : Archicture détaillée Client cible - MPLS

On retrouve sur ce schéma les deux routeurs HSRP gérés par l'opérateur.

Ils sont connectés à un premier réseau MPLS dédié aux partenaires.

Ce réseau MPLS est lui interconnecté à un site situé à la Défense où se trouve les firewall donnant ensuite accès à un deuxième MPLS qui lui, est dédié aux différentes filiales du groupe.

Et enfin sur chaque site distant, il y a un serveur GNU/Linux qui a pour rôle :

- Firewall
- Routage
- Gestionnaire de fichiers
- Gestionnaire d'annuaires

- Sauvegarde
- Envoi de mail
- Proxy Cache

Le site situé à Paris, au siège de la filiale, fournit des services en plus, comme un outil d'inventaire et de télé-déploiement nommé OCS Inventory.

8.1.2. Inventaire

Afin de préparer l'intégration de ce client à la solution de supervision, il a été nécessaire d'inventorier les éléments à superviser et ceux qui ne le seront pas.

En effet, il ne nous est pas possible de superviser l'ensemble des éléments, car certains sont hors de notre périmètre.

Sur les sites distants, il y a donc 3 serveurs centraux et chez Alter Way Hosting, il y a un serveur dédié aux nomades.

Ces 4 serveurs fournissent globalement le même service, qui est la gestion d'annuaire et de fichiers partagés.

Il y a également l'architecture de messagerie composée de 3 serveurs sur le Datacenter principal et un serveur de secours sur le serveur secondaire.

Les firewalls sont également supervisés de manière basique dans un premier temps.

8.1.3. Contraintes

L'ouverture des flux au niveau des firewall du groupe, sur le site de la Défense est très contrôlée et difficile à obtenir.

Certains protocoles sont jugés non sûr ou à risque. Dans ce cas, l'ouverture de port est refusée.

C'est le cas du protocole SNMP qui est très utilisé en supervision.

Même si la dernière version de SNMP permet le cryptage et l'authentification, les versions précédentes (1 et 2c) de SNMP ne sont pas sécurisées.

Comme elles utilisent le même port, le SNMP n'est tout simplement pas autorisé.

De plus, les informations qu'il est possible de récupérer avec SNMP sont tellement importantes qu'il est tout à fait compréhensible de refuser une ouverture de port.

Le SNMP est nécessaire aux besoins de supervision du client.

La bande passante de celui-ci est relativement faible, et il faut donc avoir un regard sur l'évolution de sa consommation.

Le protocole NRPE a été autorisé au niveau des Firewall du siège du groupe.

Il est par défaut crypté, et les informations circulant dans le tunnel crypté n'ont pas un impact fort en termes de sécurité.

L'agent NRPE qui sera installé va exécuter des scripts en local sur les serveurs supervisés.

Pour palier au problème d'utilisation du SNMP, NRPE va exécuter ses sondes avec pour méthode d'interrogation le SNMP, en local depuis le serveur.

L'agent NRPE retournera au serveur Nagios un état et des données de performance.

Avec cette méthode, nous avons donc pu contourner techniquement les contraintes liées à la sécurité sans en abaisser le niveau.

Les serveurs étant anciens et fonctionnant avec des distributions GNU/Linux non reconnues par le constructeur, il n'est pas possible d'installer les outils de surveillance du matériel.

Il n'y aura donc pas de remontée en cas de défaillance matérielle.

Sur Nagios, chaque entité doit être vérifiée en termes de disponibilité.

Par défaut, la commande de vérification utilisée est « check_host_alive » qui est une requête ICMP qui va permettre de valider la disponibilité de l'hôte.

Le problème est que le protocole ICMP n'est pas autorisé à circuler par le siège du groupe.

Afin de contourner ce problème, la commande de vérification est devenue « check_tcp » qui va permettre de vérifier qu'un port tcp est ouvert et respecte les seuils de temps de réponse prédéfinis.

Autre point, nous n'avons pas sous notre responsabilité de tous les éléments réseaux, ceux-ci ne seront donc pas supervisés.

Le fait de ne pas avoir la main sur tous les éléments des systèmes d'information, limite la possibilité de mettre en place de la cartographie

8.1.4. Définition des sondes, services

Il est à savoir que tous les serveurs qui seront supervisés sont des serveurs GNU/Linux (Debian 4 et 5)

Les sondes mises en place sont des sondes basiques, puis spécifiques et certaines sont communautaires.

Voici la liste des sondes qu'il a été décidé de mettre en place :

- Sondes de base :
  - Ping (requête icmp pour valider la disponibilité)
  - Load-Average (vérification de la charge serveur)
  - Swap (vérification de l'utilisation du swap)
  - Espace disque (vérification de l'espace disque de toutes les partitions)

- Sondes spécifiques :
  - Connexion au serveur mail sans authentification
  - Interrogation sur l'annuaire openldap
  - Test de résolution DNS
  - Test d'attribution d'adresse via dhcp
  - Vérification des trafics réseaux
  - Vérification de l'accessibilité d'application web
  - Vérification de la possibilité de se connecter à un serveur de messagerie via le protocole POP3
  - Vérification de la connexion en ssh
  - Vérification de l'accessibilité de bases de données (Mysql et PostgreSQL)
- Sondes communautaires :
  - Vérification du bon déroulement de la sauvegarde Amanda
  - Vérification de la queue de messagerie
  - Vérification de l'état des firewall shorewall sur les sites distants.
  - Vérification de la présence de processus spécifiques
  - Test de l'accessibilité de partage Samba

Certaines de ces sondes remontent des données de performance. Celles-ci vont pouvoir être interprétées par Centreon qui générera des graphes.

Cela va permettre d'avoir un regard sur l'évolution des ressources du Système d'Information et d'anticiper certains événements.

8.1.4.1. Modèles et Politique de nommage

Afin de faciliter la gestion et le déploiement, certaines mesures liées à la configuration ont été prises. Une politique de nommage a été définie. Il est préconisé d'utiliser des modèles afin d'uniformiser la configuration et gagner en productivité.

8.1.4.1.1. Politiques de nommage :

Il est nécessaire de normaliser les noms des sondes, des modèles de services, des services et les noms d'hôte.

Par exemple les noms d'hôtes devront tous commencer par le nom du client suivi d'un underscore.

Exemple : alterway_ns1, alterway_mx1...

8.1.4.2. Création de modèles :

Il est possible de créer des modèles de services. Ceux-ci vont contenir des paramètres standards qu'il ne sera pas nécessaire de personnaliser dans la plupart des cas. (Comme, les intervalles de contrôles, les destinataires des notifications...)

Il est possible de prendre le dessus sur ces configurations par défaut, lors de la création de la sonde pour un hôte donné. Ça ne fige en rien la personnalisation future.

L'utilisation de modèles va permettre de déployer plus facilement des sondes, car il n'y aura qu'à indiquer les seuils liés aux contrôles sans avoir à compléter des informations identiques à chaque fois.

Il est également possible de créer des modèles d'hôte. Ceux-ci vont contenir des réglages par défaut également, mais aussi la liste des services par défaut à déployer.

Nous avons donc créer des modèles spécifiques pour ce client, car il présente certaines particularités.

8.1.4.2.1. Modèles de service :

Configuration du modèle	Informations générales	Alias
		Nom du modèle de service
		Modèle à utiliser pour le modèle de service
	État du service	Volatile
		Période de contrôle
		Commande de vérification
		Arguments
		Nombre maximum de contrôle
		Intervalle normal de contrôle
		Intervalle non-régulier de contrôle
		Contrôles actifs activés
		Contrôles passifs activés
	Macros	Macros personnalisées (Les Macros fournissent des « variables » à Nagios et aident à l'auto-configuration des hôtes et des services.)
	Notification	Notification activée

		Contacts liés
		Groupe(s) de contacts liés
		Intervalle de notification
		Période de notification (il est possible de créer des périodes de notification, par exemple une période hors heures de travail)
		Options de notifications (Alerte - Inconnu - Critique - Recovery - Oscillant - Temps d'arrêt programmés)
		Délai de première notification
Relations	Groupe d'hôte	Il est possible de choisir de relier des modèles de service à des modèles d'hôte. De cette manière, lors de la création d'un hôte à l'aide d'un modèle, les services associés seront créés automatiquement.
	Traps SNMP	Il est également possible d'associer des modèles de service à des Traps[32] SNMP
Traitement de données	Traitement des données	Contrôle de suivi précis du service
	Options de contrôle de la fraîcheur du résultat	Contrôle de la fraîcheur du résultat (on en a besoin dans les architectures de type distribuée comme vue précédemment)
	Options d'oscillations	Détection des oscillations
		Seuil bas de détection d'oscillation
		Seuil haut de détection d'oscillation
	Options des données de performance	Traitement des données de performance
	Options de l'historique	Conserver les informations d'état
		Rétention des informations ne concernant pas le statut
		Options à enregistrer
	Gestionnaire	Gestionnaire d’événements activé

32 Le protocole SNMP définit aussi un concept de trap. Une fois défini, si un certain événement se produit, comme le dépassement d'un seuil, l'agent envoie un paquet UDP à un serveur

	d’événements	
		Gestionnaire d’événements
		Arguments
Informations supplémentaires du service	Centreon	Modèle de graphique
		Catégories
	Nagios	URL
		Notes
		URL d'action
		Icône
		Icône alternative
	Informations supplémentaires	Statut
		Commentaires

8.1.4.2.2. Modèles d'hôte :

Configuration de l'hôte	Informations générales	Nom du modèle d'hôte
		Alias
		Adresse IP / DNS
		Communauté SNMP & Version
		Modèles d'hôte parallèles. Un hôte peut avoir plusieurs modèles d'hôte en même temps.
	Propriétés du contrôle de l'hôte	Période de contrôle
		Commande de vérification
		Arguments
		Nombre maximum de contrôle
		Intervalle normal de contrôle
		Intervalle non-régulier de contrôle

		Contrôles actifs activés
		Contrôles passifs activés
	Macros	Macros personnalisées
	Notification	Notification activée
		Contacts liés
		Groupe(s) de contacts liés
		Intervalle de notification
		Période de notification
		Options de notifications (Down – Injoignable - Recovery – Oscillant - Temps d'arrêt programmés)
		Délai de première notification
	Relation	Il est possible de choisir de relier des modèles d'hôte à des modèles de service. De cette manière, lors de la création d'un hôte à l'aide d'un modèle, les services associés seront créés automatiquement.
Traitement des données	Traitement des données	Contrôle de vérification de l'hôte
	Options de contrôle de la fraîcheur du résultat	Contrôler la fraîcheur du résultat
		Seuil de fraîcheur du résultat
	Options d'oscillations	Détection des oscillations
		Seuil d'oscillations bas
		Seuil haut de détection d'oscillation
	Options des données de performance	Traitement des données de performance
	Options de l'historique	Rétention des informations de statut
		Rétention des informations ne concernant pas le statut
		Options à enregistrer
	Gestionnaire d’événements	Gestionnaire d’événements activé
		Gestionnaire d’événements

		Arguments
Informations détaillées de l'hôte	Nagios	URL
		Notes
		URL d'action
		Icône
		Icône alternative
		Image VRML
		Image de la carte des états de Nagios
		Coordonnées 2D Nagios
		Coordonnées 3D Nagios
	Informations supplémentaires	Statut
		Commentaires

L'utilisation de modèles est un vrai plus en terme d'industrialisation, car seules les valeurs comme une adresse ip ou les attributs de sondes seront personnalisés. Cela facilite grandement le déploiement.

8.1.4.3. Définition des seuils

Afin de définir les seuils de supervision, une matrice de sondes a été créée.

Les seuils de supervision à placer par sonde ont été définis lors de réunion avec le client et ont évolué au fur et à mesure de la vie du projet.

Voici les informations présentes dans cette matrice :

Groupe d'hôtes	Client_cible	Client_cible	Client_cible
Hôte	mx1	mx1	mx1
Adresse IP	192.168.2.2	192.168.2.2	192.168.2.2
Sonde	Ping	Load-Average	NRPE-DISK-/
Modèle de services	Ping-LAN	NRPE-LINUX-Load-Average	NRPE-DISK
Commande	check_centreon_ping	check_load	check_disk
Description	Vérifie le temps de réponse au ping	Vérifie le load average du serveur	Vérifie l'espace disque restant d'une partition donnée – taille : 4,6G
Dépendances	Aucune	Ping	Ping
Période de contrôle	24x7	24x7	24x7
Seuil Warning	3 Paquets ICMP – 200,20%	2.00,2.01,2.05	80,00%
Seuil Critical	3 Paquets ICMP – 400,50%	3.00,3.01,3.05	90,00%
Intervalle normal de contrôle	5 min	5 min	30 min
Intervalle non-régulier de contrôle (État SOFT)	1 min	5 min	5 min
Intervalle de Notification	5 min	5 min	30 min
Type de Check	ICMP	NRPE	NRPE
Notification	Inforgérance AWS	Inforgérance AWS	Inforgérance AWS
Type de Notification	Alerte / Inconnu / Critique / Recovery	Inconnu / Critique / Recovery	Alerte / Inconnu / Critique / Recovery
Délai de première notification	3 min	5 min	5 min
Période de notification	24 x 7	24 x 7	24 x 7
En fonction	OK	OK	OK

Cette matrice permet donc de dresser un inventaire des sondes à mettre en place.

Elle va aussi permettre de déterminer avec quels paramètres les mettre en place.

On va définir les intervalles de contrôle régulier ou non, mais aussi les intervalles de notification, les types de notifications, les périodes de notification…

Je recommande fortement l'utilisation de matrice car cela force la réflexion et permet d'éviter les oublis. Ça permet également de définir clairement les niveaux de services (SLA) avec le client.

8.2. Mise en place de la solution sur système cible

8.2.1. Déploiement

Le déploiement a été organisé par dépendance, par site et par type de sondes.

Il a été décidé de commencer le déploiement par les sites distants de Paris, Lyon et Lille.

Voici les différentes étapes du déploiement : (Phase 1)

- Ouverture de ports (Siège et Firewall Alter Way Hosting)
- Installation Agent NRPE et déploiement de la configuration (un fichier nrpe.cfg a été standardisé pour contenir les sondes de base)
- Tests de liaison entre le serveur de supervision et la machine cible
- Création des modèles de services
- Création du modèle d'hôte et attribution des modèles de services par défaut, qui seront les sondes de base que l'on retrouvera sur chaque hôte de ce client.
- Création de l'hôte à partir du modèle d'hôte précédemment créé
- Personnalisation des seuils de chacun des services par hôte créé.
- Validation des bons résultats

Il a été décidé d'observer le bon fonctionnement de la solution de supervision durant 2 semaines avant de passer à la suite du projet.

Une fois que tout a été validé, il était prévu d'installer les sondes spécifiques officielles. (Phase 2)

- Création des modèles de services
- Configuration de l'agent pour répondre aux nouvelles sondes
- Validation du fonctionnement en ligne de commande
- Création du service à partir du modèle de service avec attribution des seuils pré-définis.

Après la mise en place de ces sondes, une période de deux semaines d'observation a été également mise en place, ceci afin de valider le bon fonctionnement et de réaliser quelques réglages de seuils.

Durant cette période, le déploiement a été initié avec la même méthode pour les serveurs présents chez Alter Way Hosting, site principal et secondaire (Phase 3)

Les sondes spécifiques ont été mises en place également sur les hôtes hébergés chez Alter Way Hosting. (Phase 4)

Les serveurs sont désormais supervisés avec les sondes de base et spécifiques à l'activité du client cible.

Il faut donc mettre en place les sondes communautaires (Phase 5)

La première étape était de trouver les sondes correspondantes à notre besoin sur le portail Nagios Exchange.

Voici les sondes nécessaires au client cible :

Services	Besoin	Nom de la sonde
Cron	Permet de vérifier si le processus cron est présent – à développer par nos soins	check_cron
Samba	Permet de tester l'accessibilité à la liste des partages en anonyme	check_smb
Puremessage	Vérifie l'accès à un port TCP	check_centreon_Tcpconn
Shorewall	Vérifie l'état du shorewall	check_shorewall
Dovecot	Vérifie l'état du serveur Dovecot en rapport avec le nombre de connexion	check_dovecot

Les besoins de supervision étant aussi divers que nombreux, il a fallu rechercher ou (re)développer des sondes.

Cron – tous les processus de nuit sont exécutés via la crontab. Il est donc nécessaire de vérifier le bon fonctionnement de ce processus.

Samba – Le partage de fichiers est actuellement offert par Samba, tester la présence d'un processus ne serait pas suffisant. Il fallait donc trouver un moyen d'interroger le serveur samba sur les fichiers et dossiers disponibles. Il existe plusieurs plugins communautaires qui seront à tester pour valider le bon fonctionnement.

PureMessage – Il s'agit d'une solution antivirus / antispam éditée par Sophos pour les serveurs de messagerie. Si PureMessage fonctionne, il utilise un port TCP. Pour valider donc le fonctionnement, il suffit de valider l'ouverture de ce port. Une utilisation détournée de check_tcp sera effectuée.

Shorewall est un antivirus opensource basé sur iptables[33] Il n'est pas très répandu, mais il existe néanmoins un plugin communautaire. Il va utiliser une commande propre à shorewall pour récupérer le statut et le transmettre à Nagios.

Dovecot est un serveur de messagerie IMAP et POP3 (MDA – Mail Delivery Agent)

Une fois toutes les sondes communautaires fonctionnelles, les serveurs sont passés en phase d'ajustement des seuils (Phase 6)

Il arrive d'avoir besoin de réajuster certains seuils afin de rendre les alertes plus cohérentes et nécessaires.

Et enfin, vit le temps de l'exploitation de la supervision des serveurs.

33 outil d'administration pour le filtrage de paquets IPv4 et le NAT

8.2.2. Exploitation

Avant de pouvoir superviser efficacement les services du client cible, il a fallu informer l'équipe d'infogérance de ce qui était supervisé, comment ils étaient supervisés, et pourquoi tel ou tel service l'était à contrario d'autres.

L'équipe d'infogérance n'étant pas un grand service avec plusieurs dizaines d'exploitants, il a été décidé de ne pas mettre en place de gestion de droits d'accès.

Il y a un compte administrateur, et un compte opérateur connu de tous.

Il aurait également été possible de fournir un accès au client cible, mais il a été décidé de ne pas le faire.

Lorsqu'il y a un incident, un mail est envoyé à l'équipe infogérance afin que celui-ci soit traité le plus rapidement possible.

Il est également obligatoire pour chaque exploitant d'installer au navigateur internet Mozilla Firefox, une extension qui va consulter le statut de Nagios et remonter une alerte visuelle et sonore.

Illustration 44 : Nagios Checker

Il est également possible pour les possesseurs de téléphone de nouvelle génération de type Android ou encore IPhone d'avoir une application qui interroge le serveur Nagios. Il y a donc une remontée, en direct et peu importe l'endroit où l'on se situe, d'incidents Nagios.

Cette extension n'est pas obligatoire, elle est à la liberté de l'exploitant, il n'y a aucune obligation, notamment car il n'y a pas de service d'astreinte obligeant une continuité de service 24heures/24 et 7jours/7.

Concernant les temps de prise en charge et de résolution, ils sont bien sûr identiques aux SLA définis avec le client. Il y a également un jugement personnel réalisé par l'exploitant qui permet de déterminer si l'intervention doit se faire de manière urgente ou non.

Par exemple, un disque qui obtient un seuil d'utilisation de 90 % ne nécessitera sûrement pas la même précipitation qu'un service inaccessible.

L'intégration de ce nouvel outil de travail au sein de l'équipe d'infogérance n'a pas été facile. J'aurais dû plus impliquer les membres de l'équipe afin qu'ils assimilent mieux l'utilisation de l'outil

8.2.3. Reporting

Un comité technique est tenu tous les mois avec le client afin de faire un point sur l'état du service d'infogérance rendu.

Lors de ce comité technique, il est présenté des indicateurs sur la santé du système d'information du client cible.

Ces indicateurs sont fournis par la solution de supervision.

Il va donc être indiqué la volumétrie utilisée sur les différents serveurs, l'utilisation de la bande passante, s'il y en a des indisponibilités de service et leur cause.

L'outil de supervision est donc devenu un élément primordial au reporting client

8.2.4. Documentation

Afin de rendre autonome les membres de l'équipe, il a été créé des documentations d'exploitation.

Il s'agit par exemple de procédures de création d'hôte, de procédures de création de service.

Ces procédures ont été effectuées de manière très didactique afin d'acquérir les bonnes pratiques définies pour cette solution de supervision, comme la nomenclature des hôtes ou des services.

9. Bilan et perspectives

9.1. Bilan

9.1.1. Retours sur l'intégration d'un client type

En conclusion, l'intégration de ce client cible a permis de mettre en exergue les contraintes que nous pouvons rencontrer en rapport avec notre activité d'infogérance.

Mais elle a permis également de démontrer qu'il est possible de trouver une solution de contournement.

Grâce à la forte communauté Nagios, il a été facile de répondre à tous les besoins de supervision de ce client.

Le PRA[34] est totalement couvert par la solution de supervision.

Les indicateurs fournis par la solution de supervision sont étudiés tous les mois par le client ce qui démontre sa bonne intégration.

34 Plan de Reprise d'Activité – permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.

Désormais pour tous nouveaux serveurs seront directement intégrés à la solution de supervision. Les outils de gestion matériels sont installés par défaut afin de les interfacer avec Nagios / Centreon et donc de gérer les pannes matérielles.

9.1.2. Évaluation de la solution de supervision

Le projet de supervision est désormais utilisé pour certains de nos clients. Tous les clients n'ont pas encore été intégrés, mais ils le seront au fur et à mesure.

Il est devenu vital au quotidien pour l'exploitation des systèmes d'information que nous avons en charge.

Le temps de réaction a considérablement baissé et il arrive souvent de prévenir le client d'une résolution alors que celui-ci ne s'est même pas aperçu de la dégradation du niveau de service.

9.1.3. Indicateurs

Cette solution de supervision, nous permet désormais de fournir des indicateurs sur la santé de leur parc serveur, que ce soit à nos clients, ou simplement à notre direction, et donc par la même occasion, de justifier d'une certaine qualité de service.

Pour reprendre l'exemple du client cible utilisé pour ce rapport, voici l'évolution de la disponibilité de son infrastructure depuis la mise en place de la supervision en mai 2010.

On va pouvoir remarquer une amélioration en termes de nombre d'alertes et donc de disponibilité.

Illustration 45 : Client cible - Reporting 2010

On peut voir qu'il y a eu 182 alertes, soit une disponibilité de 99,38 % sur la période de supervision.

Illustration 46 : Client cible - Reporting 2011

Durant l'année 2011, il y a eu 112 alertes et une disponibilité de 99,6 %.

On peut donc être amené à penser que la supervision nous a permis d'avoir plus de stabilité et d'anticiper certains problèmes rendant le système d'information plus fiable.

Les indicateurs ont permis de voir une amélioration de la qualité de service rendu

9.1.4. Coût

Le coût de mise en place est difficilement estimable hormis l'achat du matériel.

Il y a le temps passé à étudier les diverses solutions libres, le temps de mise en place de la solution, qui sont des temps imputables à tous les clients.

Ensuite, il y a le temps d'intégration des clients qui va lui être imputable au temps à consacrer aux clients selon les termes de leur contrat d'infogérance.

Certains contrats n'ont aucune limite de temps à passer durant l'année, pour ceux-là l'intégration est à notre charge.

Pour les contrats d'infogérance, qui eux contiennent un temps d'intervention annuel, l'impact financier côté Alter Way est limité, car une partie est prise en charge par le contrat d'infogérance.

9.2. Perspectives

9.2.1. Évolutivité technique de la solution de supervision

Certains de nos clients ont des architectures serveurs conséquentes.

Il est donc prévu de mettre en place autant de serveurs Nagios distribués qui viendront remonter les informations au serveur Nagios central que nous avons mis en place.

De plus en plus de services seront pris en compte dans le cadre de la supervision, soit par

l'ajout de plugins communautaires, soit par le développement de nos propres plugins qui seront publiés sous licence libre.

Il est convenu d'intégrer des modules propres à Centreon, comme l'interface en ligne de commande permettant de gérer Centreon, ceci afin d'automatiser l'administration et de gagner en productivité.

Il est envisagé de fournir des indicateurs plus précis concernant les incidents eux-mêmes ou leurs prises en compte par le service infogérance.

Plusieurs pistes sont étudiées, comme la mise en place de Centreon Business Intelligence, qui est un module propriétaire de Centreon permettant d'exploiter plus en profondeur les données recueillies par la solution de supervision.

Il pourrait également être utilisé un outil d'extraction de données comme BIRT, qui est un système de création de rapports.

Il sera étudié également la mise en place de solution de cartographie afin d'avoir des vues plus réelles des parcs serveurs de nos clients. Voir l'exemple ci-dessous :

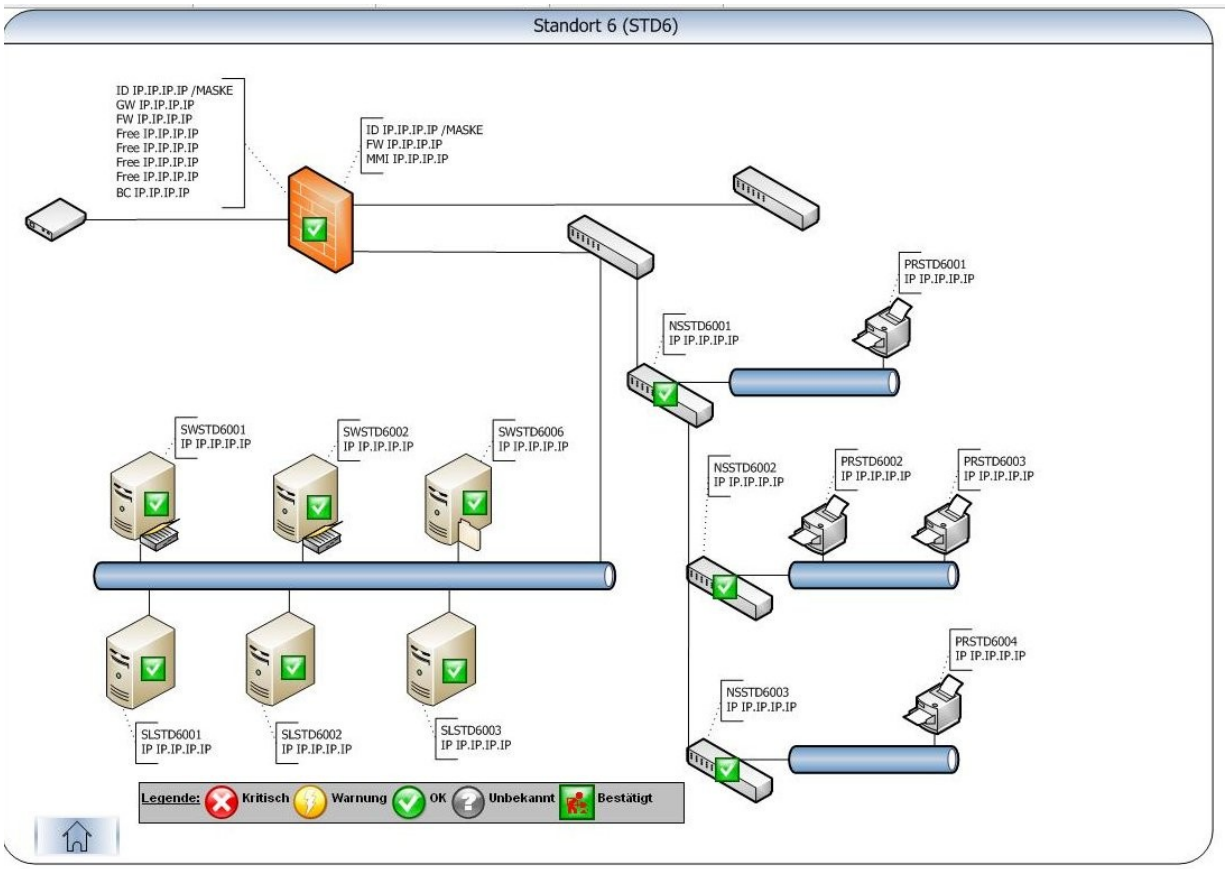


Illustration 47: Exemple de Cartographie - Source Site officiel de Nagvis

9.2.2. Évolutivité commerciale de la solution de supervision

Depuis la mise en place du projet de supervision, la surveillance des sondes de base a été intégrée au contrat d'infogérance.

Il est envisagé également de proposer à nos clients la supervision de certains éléments spécifiques moyennant un coût de mise en place et un abonnement d'exploitation.

Il arrive également que la solution de supervision soit utilisée par l'équipe Infrastructure dans le cadre de mission d'audit, comme surveiller la charge d'un serveur.

Hors l'aspect technique qui n'a pas vraiment de limite, l'aspect commercial a de fortes possibilités d'évolution.

10. Conclusion

Après avoir intégré le service infogérance, j'ai constaté le besoin de mettre en place une plate-forme de supervision. J'ai donc demandé et soumis l'idée à ma hiérarchie d'utiliser ce projet comme support de mon mémoire d'Ingénieur CNAM. Ce projet est une vraie réussite pour l'entreprise et moi-même.

10.1. L'apport du projet pour l'entreprise

Alter Way Solutions dispose désormais, pour le service infogérance, d'une solution de supervision souple, robuste et évolutive. La solution de supervision est devenue primordiale pour le bon fonctionnement du service infogérance. Elle permet d'accroître la qualité de service des systèmes d'information. Les besoins sont souvent anticipés, la durée d'indisponibilité de service a été réduite et le nombre d'incidents également.

Les indicateurs fournis par la solution mise en place permettent de constater l'évolution positive de la qualité de service rendue par le service infogérance. Ils font parti intégrante des échanges avec les clients.

Les clients disposant d'un contrat d'infogérance sont donc intégrés par défaut à la solution de supervision. Leur intégration est d'ailleurs facilitée grâce à l'expérience acquise au cours de ce projet.

La mise en place de ce projet a aussi permis d'améliorer les conditions de travail des exploitants. Les interventions ne sont plus principalement curatives, mais souvent préventives. L'état du système d'information est sous contrôle permanent facilitant grandement la gestion au quotidien. L'exploitation quotidienne se fait moins dans l'urgence, ce qui accroît le bien-être et la productivité.

Grâce à l'étude réalisée, Alter Way Solutions possède aujourd'hui une bonne connaissance de toutes les solutions de supervision libres du marché. Il est donc plus facile d'orienter un client vers telle ou telle solution de supervision libre en fonction de son besoin et de son architecture.

Des bonnes pratiques pour un projet de supervision ont pu être identifiées comme la mise en place de matrice des sondes à définir avec le client.

Les apports du projet de supervision ne s'arrêtent pas aux côtés techniques et opérationnels mais offre une approche commerciale supplémentaire. Il est désormais possible de répondre à des appels d'offre d'infogérance avec pour pré-requis une plate-forme de supervision. Les apports commerciaux ne s'arrêtent pas là, car il pourrait être envisagé de mettre en place une offre commerciale visant à proposer de la supervision externalisée.

10.2. L'apport du projet pour l'auditeur

La mise en place de ce projet m'a permis d'acquérir les connaissances techniques et fonctionnelles liées aux métiers de la supervision informatique. L'étude de toutes les solutions de supervision open source m'a permis de connaître au mieux les diverses solutions de supervision libres ce qui me permet d'avoir un regard critique envers celles-ci.

La mise en place de ce projet m'a permis de maîtriser les problématiques liées à un projet de supervision. Les approches organisationnelles et fonctionnelles sont d'ailleurs bien plus conséquentes que la mise en place technique.

Ce projet m'a d'ailleurs permis d'approfondir considérablement mes connaissances dans le domaine de la supervision libre, et plus particulièrement de Nagios / Centreon.

J'ai été amené à jouer un rôle moteur afin de proposer la solution aux clients, mais aussi afin de faire comprendre l'importance de ce nouvel outil auprès de mes collègues, ce qui a facilité son intégration.

Via ce projet, j'ai pu découvrir les différences d'appréciation et de perception des éléments d'un projet de supervision par les responsables de systèmes d'informations, comme l'expression du besoin, la criticité d'événements…

Cela m'a forcé à m'adapter en fonction du client et de son système d'information, ce qui a été très enrichissant.

Afin de mener à bien l'étude sur les différentes solutions de supervision libres, j'ai dû définir une méthode d'analyse de chaque projet et réussir à en faire une synthèse.

Ce projet m'a permis d'acquérir une méthodologie propre aux projets de supervision et d'en définir les étapes clefs. J'ai d'ailleurs été consulté récemment afin de fournir un document listant les éléments à connaître pour réaliser le chiffrage d'un projet de supervision.

Globalement, le projet de supervision est une réussite et a été très bénéfique pour Alter Way Solutions et pour moi-même.

11. Références

11.1. Bibliographie

- Nagios 3 pour la supervision et la métrologie - Déploiement, configuration et optimisation - Aux éditions Eyrolles - Auteur Jean Gabes
- Maturité et gouvernance de l'Open Source – La vision des grandes entreprises - Écrit par le Cigref en 2011.
- La maturité des solutions opensource et libres (Chapitre 5.5) : une partie provient directement de l'étude du Cigref.

11.2. Webographie

- Les prémices du logiciel libre (Chapitre 4.1.1) proviennent de Wikipedia :
  http://fr.wikipedia.org/wiki/Histoire_du_logiciel_libre
- L'histoire de l'Open Source provient de Wikipedia : (Chapitre 4.2.1)
  http://fr.wikipedia.org/wiki/Open_source
- La traduction des conditions de licence de l'OSI : (Chapitre 4.2.2)
  http://fr.wikipedia.org/wiki/Open_Source_Definition
- Version Originale des conditions de licence de l'OSI :
  http://www.opensource.org/docs/osd
- La différence entre l'Open Source et les Logiciels Libres (Chapitre 4.3) provient de cette page :
  http://fr.wikipedia.org/wiki/Open_Source_Initiative
- Une bonne partie des standards de la supervision provient de l'article ci-dessous :
  http://www.monitoring-fr.org/supervision/standards/
- Liste des licences compatibles et non compatibles GNU GPL :
  http://www.gnu.org/licenses/license-list.fr.html#GPLCompatibleLicenses
- Le schéma permettant d'illustrer le fonctionnement de Nagios avec Centreon (chapitre 6.3.2.4.3) est grandement inspiré du schéma présent sur la page de présentation de Centreon de monitoring-fr.org
  http://wiki.monitoring-fr.org/centreon/start
- Documentation officielle de Nagios
  http://library.nagios.com/library/products/nagioscore/manuals/
- Traduction de la documentation officielle de Nagios

http://doc.monitoring-fr.org/

- Documentation officielle de Zabbix
  http://www.zabbix.com/documentation/

12. Table des illustrations

13. Annexes

Tableau des différentes licences Créative Commons :

Désignation complète du contrat	Terme abrégé désignant la licence	Symboles désignant la licence				Type de licence
Paternité	CC-by					Licence libre non-copyleft
Paternité Partage des conditions initiales à l'identique	CC-by-sa					Licence libre copyleft
Paternité Pas de modification	CC-by-nd					Licence de libre diffusion
Paternité Pas d'utilisation commerciale	CC-by-nc					Licence de libre diffusion
Paternité Pas d'utilisation commerciale Partage des conditions initiales à l'identique	CC-by-nc-sa					Licence de libre diffusion
Paternité Pas d'utilisation commerciale Pas de modification	CC-by-nc-nd					Licence de libre diffusion

Voici ce qu'il est possible de faire en fonction de chaque licence :

CC-BY :

Signifie que l'on est libre de :

- Partager : reproduire, distribuer et communiquer l'œuvre.
- Remixer : adapter l'œuvre
- Utiliser l'œuvre à des fins commerciales

Condition :

- Attribution : Vous devez attribuer l’œuvre de la manière indiquée par l'auteur ou le titulaire des droits (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l’œuvre).

CC-BY-SA :

Signifie que l'on est libre de :

- Partager : reproduire, distribuer et communiquer l’œuvre.
- Remixer : adapter l’œuvre
- Utiliser l’œuvre à des fins commerciales

Conditions :

- Attribution : Vous devez attribuer l’œuvre de la manière indiquée par l'auteur ou le titulaire des droits (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l’œuvre).
- Partage à l'Identique : Si vous modifiez, transformez ou adaptez cette œuvre, vous n'avez le droit de distribuer votre création que sous une licence identique ou similaire à celle-ci.

CC-BY-ND :

Signifie que l'on est libre de :

- Partager : reproduire, distribuer et communiquer l’œuvre.
- Utiliser l’œuvre à des fins commerciales

Conditions :

- Attribution : Vous devez attribuer l’œuvre de la manière indiquée par l'auteur ou le titulaire des droits (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l’œuvre).
- Pas de travaux dérivés : Vous n’avez pas le droit de modifier, de transformer ou d’adapter cette œuvre.

CC-BY-NC :

Signifie que l'on est libre de :

- Partager : reproduire, distribuer et communiquer l’œuvre.
- Remixer : adapter l’œuvre

Conditions :

- Attribution : Vous devez attribuer l’œuvre de la manière indiquée par l'auteur ou le titulaire des droits (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l’œuvre).
- Pas d’Utilisation Commerciale : Vous n'avez pas le droit d'utiliser cette œuvre à des fins commerciales.

CC-BY-NC-SA :

Signifie que l'on est libre de :

- Partager : reproduire, distribuer et communiquer l’œuvre.
- Remixer : adapter l’œuvre

Conditions :

- Attribution : Vous devez attribuer l’œuvre de la manière indiquée par l'auteur ou le titulaire des droits (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l’œuvre).
- Pas d’Utilisation Commerciale : Vous n'avez pas le droit d'utiliser cette œuvre à des fins commerciales.
- Partage à l'Identique : Si vous modifiez, transformez ou adaptez cette œuvre, vous n'avez le droit de distribuer votre création que sous une licence identique ou similaire à celle-ci.

CC-BY-NC-ND :

Signifie que l'on est libre de :

- Partager : reproduire, distribuer et communiquer l’œuvre.

Conditions :

- Attribution : Vous devez attribuer l’œuvre de la manière indiquée par l'auteur ou le titulaire des droits (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l’œuvre).
- Pas d’Utilisation Commerciale : Vous n'avez pas le droit d'utiliser cette œuvre à des fins commerciales.
- Pas de travaux dérivés :Vous n’avez pas le droit de modifier, de transformer ou d’adapter cette œuvre.

Carte conceptuelle du logiciel libre par René Mérou :

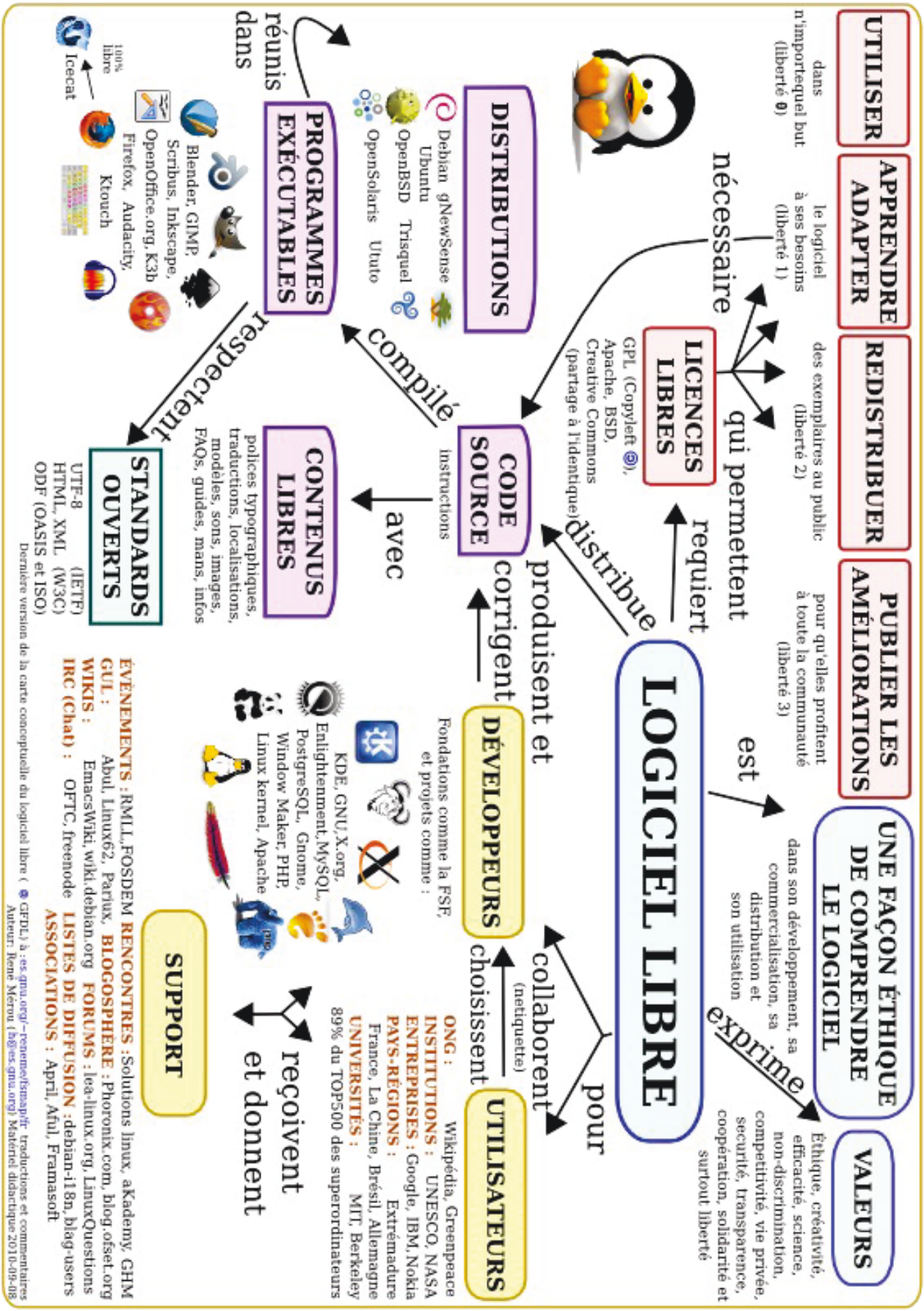


Schéma de l'infrastructure cible :

14. Glossaire

Système d'Informations	Communément appelé S.I., c'est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné, ici il s'agit de l'environnement informatique. (Définition Wikipedia - http://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27information)
D.S.I.	Direction du Système d'Informations
Infogérance	L'infogérance est un service défini comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou une partie du système d'information (S.I.) d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définie (définition de l'AFNOR). En d'autres termes, c'est l'externalisation de tout ou d'une partie de la gestion et de l'exploitation du SI à un prestataire informatique tiers http://fr.wikipedia.org/wiki/Infog%C3%A9rance
ITIL – Information Technology Infrastructure Library	Ensemble de bonnes pratiques pour la gestion d'un système d'informations. Elles ont été rédigées par des experts de l'Office public britannique du Commerce et composées de 8 livres dans sa version 2 et de 5 livres dans sa version 3. Le but d'ITIL étant d'aider à améliorer les processus propres à la gestion d'un système d'informations et d'accroître la satisfaction utilisateur, grâce notamment à une boucle d'amélioration continue comme l'on pourrait retrouver dans des normes de qualité type ISO 9001...
CMDB	Configuration Management DataBase est une notion que l'on retrouve dans ITIL. Il s'agit d'une base de données regroupant et unifiant tous les éléments du système d'Informations.
SNMP	Simple Network Management Protocol - en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance. (Définition Wikipedia - http://fr.wikipedia.org/wiki/Simple_network_management_protocol)
RRDTool	RRDtool est un outil de gestion de base de données RRD (Round-Robin Database) créé par Tobi Oetiker. Il est utilisé par de nombreux outils pour la sauvegarde de données cycliques et le tracé de graphiques, de données chronologiques. (Définition Wikipédia - http://fr.wikipedia.org/wiki/RRDTool)
log	Le terme log est notamment employé en informatique pour désigner un historique d'événements et par extension le fichier contenant cet historique (Définition Wikipédia http://fr.wikipedia.org/wiki/Log)