Déploiement d'une solution de supervision et de métrologie automatisée à large échelle

Sébastien Boggia
Université de Strasbourg — Direction informatique

Benjamin Collet
Université de Strasbourg — Direction informatique

Guillaume Schreiner
CNRS - ICube (UMR 7357)

Résumé

La nécessité de rationaliser l'exploitation a conduit à déployer une solution de supervision et de métrologie à large échelle, performante, automatisée et adaptée à toutes les communautés d'utilisateurs travaillant au sein de la Direction informatique de l'Université de Strasbourg.

Cet article présente l'architecture et les outils de supervision choisis dont Centreon *et* Nagios *ainsi que leur intégration au sein du système d'information, en particulier autour du référentiel d'équipements et de services. Les méthodes utilisées pour automatiser les interactions entre les outils de supervision et la base d'inventaire* GLPI *y sont détaillées. L'article relate également l'adaptation des nouveaux outils aux besoins des différentes communautés d'utilisateurs avec la création de tableaux de bord et d'indicateurs personnalisés.*

Mots clefs

Supervision, métrologie, Centreon*,* Nagios*,* GLPI*, inventaire,* Netmagis*, tableaux de bord.*

1 Introduction

En 2009, les trois universités strasbourgeoises ont fusionné pour créer l'Université de Strasbourg. De cette fusion est née la Direction informatique (DI), service central, regroupant l'ensemble des équipes des sept services informatiques des anciens établissements, soit 110 personnes. Dès lors, en parallèle d'une réorganisation des équipes, un important travail de fusion technique, de restructuration des services offerts aux utilisateurs a été entrepris à tous les niveaux.

La nécessité d'une solution de supervision et de métrologie cohérente et mutualisée est ainsi rapidement devenue une évidence. Dans le cadre de la mise en place d'un schéma directeur numérique, un projet d'envergure a été lancé en 2010. Celui-ci a eu pour objectif de mettre en œuvre cette solution pour l'ensemble de l'infrastructure et des services numériques de l'Université de Strasbourg.

2 Les objectifs du projet

La Direction informatique est divisée en quatre départements travaillant sur des périmètres différents :

- **le département infrastructures**, qui a en charge la gestion des infrastructures réseau, des serveurs physiques et virtuels, des bases de données et du stockage de données,
- **le département services métiers**, qui a en charge le développement et le maintien des applications métiers ainsi que des services de messagerie et des outils collaboratifs,
- **le département relation utilisateurs**, qui prend en charge la gestion des postes de travail et de téléphonie ainsi que le support aux utilisateurs,

- **le département organisation**, qui gère les processus organisationnels, la sécurité et l'architecture du sytème d'information.

Département	Volumétrie	Besoins en supervision et métrologie
Infrastructures	▪ 750 routeurs et commutateurs ▪ 930 points d'accès Wi-Fi ▪ 10 baies de stockage ▪ 850 bases de données ▪ 720 serveurs physiques et VM	▪ Disponibilité des équipements ▪ Disponibilité des services d'infrastructure
Services métiers	▪ 168 services et applications	▪ Disponibilité des services métiers
Relation utilisateurs	▪ 4 500 postes de travail ▪ 8 000 téléphones mobiles et fixes	▪ Disponibilité des serveurs et outils de gestion de parc ▪ Disponibilité de l'ensemble des services offerts aux utilisateurs de la DI
Organisation		▪ Données de reporting de la DI

Tableau 1 - Besoins en supervision de la Direction informatique

L'un des principaux objectifs a été de trouver une solution suffisamment souple pour s'adapter à des besoins de supervision hétérogènes (tableau 1). L'intérêt d'une telle solution est la possibilité de **remonter et gérer efficacement les alertes et les données de métrologie** en les adaptant au mieux au public visé.

Au lancement du projet, une quinzaine d'outils de supervision - libres ou propriétaires, pour certains spécialisés pour une seule application - a été recensée. Le plus souvent, ces outils n'étaient connus que par le gestionnaire de l'application supervisée. Certains, par exemple, étaient fortement verbeux émettant des centaines de courriels par jour. Aucun outil ne se démarquant des autres, l'idée de repartir d'une architecture entièrement nouvelle a été adoptée.

Un autre objectif de taille a été de limiter au maximum les tâches d'exploitation. La supervision, dans un contexte de charge de travail importante, est souvent considérée à tort comme non prioritaire. Un effort particulier devait être porté sur **l'automatisation de l'intégration des équipements et services dans la supervision**. Pour rendre cet objectif possible, nous devions appuyer le mécanisme sur un **référentiel unique d'équipements et de services**.

3 Architecture et outils

3.1 Choix des outils

Au lancement du projet en 2010, l'ensemble des besoins exprimés nous a conduit à retenir le logiciel *Centreon*[1]. Son architecture distribuée, basée sur des satellites *Nagios*[2] couplés au module *NDO* (*ndomod*)[3], autorise une montée en charge progressive. L'interface web de *Centreon* est riche, permettant la configuration graphique fine de tous les paramètres ainsi qu'une visualisation en temps réels de tous les services supervisés. Cette application respecte les contraintes multi-utilisateurs avec des niveaux différents d'accréditation et de délégation. *Centreon* intègre des sondes basées sur des protocoles standardisés comme *SNMP*[4]. Enfin, *Centreon* et *Nagios* sont des logiciels libres avec une communauté active développant de nombreuses extensions.

3.2 Architecture réseau

Dans le cas d'une panne majeure des infrastructures, la supervision est l'outil qui permet de rapidement diagnostiquer l'origine des problèmes. La supervision est donc un service critique qui se doit d'être le plus fiable et le plus robuste possible. Ainsi, sa mise en oeuvre nécessite de prendre des précautions au niveau réseau et système.

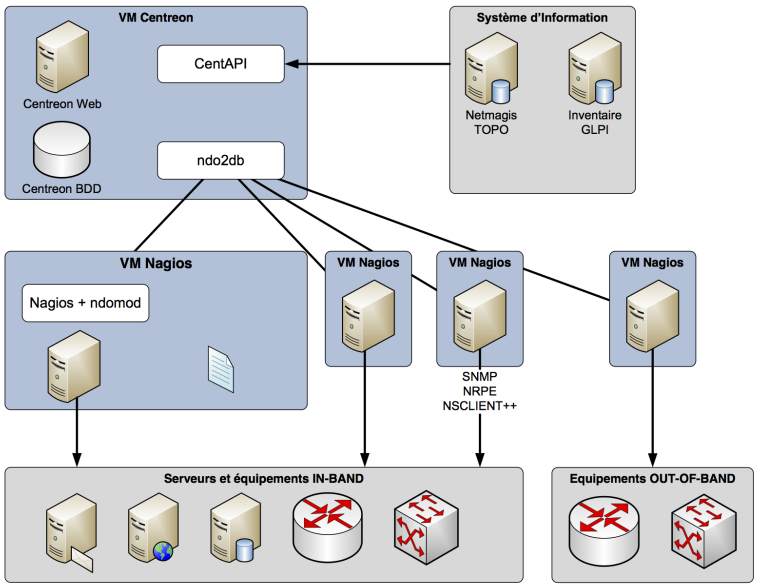

Figure 1 - Architecture distribuée de Centreon

La majorité des outils de supervision fonctionnent avec un agent installé sur l'hôte à superviser. Cet agent communique via des protocoles standardisés (*SNMP*) ou des protocoles spécifiques (*NRPE* [5], *Munin* [6]). L'interrogation de l'agent depuis la plate-forme de supervision permet de collecter les états des hôtes afin de les présenter à l'administrateur. À l'Université de Strasbourg, la Direction informatique supervise l'ensemble des services depuis un collecteur central avec des satellites distribués (figure 1).

Dans la pratique, les hôtes à superviser sont protégés soit par des pare-feux locaux, soit par des pare-feux en entrée de réseaux, ou les deux. Une bonne pratique consiste donc à créer **un réseau de supervision dédié** et autorisé à atteindre l'ensemble des hôtes supervisés. Une attention particulière au niveau de la sécurité est à porter au réseau de supervision, qui est une porte d'entrée vers l'ensemble du parc. La majorité des équipements est supervisée depuis le réseau d'administration *in-band* [1]. Pour plus de fiabilité, nous avons utilisé un réseau d'administration *out-of-band* [2] pour les équipements de cœur.

3.3 Architecture système

Notre architecture distingue deux types de systèmes, le collecteur central *Centreon* et les satellites *Nagios*. Le collecteur central *Centreon* héberge l'interface web *Centreon*, le collecteur *NDO* (*ndo2db*) qui reçoit les données des satellites *Nagios* et la base *MySQL* qui stocke les données. Une optimisation du fonctionnement de la base a été faite avec un patch sur le collecteur et module *NDO* qui permet de réduire de 90% les enregistrements pour ne conserver que les plus pertinents. Les satellites *Nagios* font tourner une instance de *Nagios* et transmettent leurs données avec le module *NDO*. L'ensemble des scripts utilisés par les sondes *Centreon* est déployé sur chaque satellite *Nagios*.

Chacun des systèmes se base sur une distribution *GNU/Linux Ubuntu LTS*. Le choix de virtualiser les systèmes, notamment les satellites *Nagios*, permet de facilement cloner et déployer un nouveau satellite en cas de montée en charge. On peut également facilement ajouter des ressources mémoire et processeur pour augmenter la puissance de la machine en cas de besoin.

Actuellement, sept satellites *Nagios* sont déployés pour l'Université de Strasbourg.

1. Réseau en bande de base, c'est-à-dire en utilisant les mêmes liens physiques que pour les données utilisateurs.
2. Réseau hors-bande, c'est-à-dire en utilisant des liens physiques dédiés.

4 Intégration autour du système d'information

Dès lors que la taille d'un parc informatique atteint une certaine dimension, la configuration de sa supervision ne peut se faire que de manière automatisée. Cela implique une centralisation des informations utiles à l'exploitation et à la supervision au sein d'une brique centrale, facilement accessible et interrogeable ; un référentiel de l'infrastructure des systèmes et équipements en production.

4.1 Référentiel

Le référentiel d'infrastructure utilisé à la Direction informatique repose sur deux éléments.

Tout d'abord un inventaire, basé sur la solution libre *GLPI*[7] dans lequel sont automatiquement enregistrées toutes les caractéristiques des systèmes déployés. Cet enregistrement est fait au moyen d'un logiciel agent, *FusionInventory*[8], installé sur le système concerné qui, à intervalles réguliers, met à jour la base centrale d'inventaire avec les changements éventuellement survenus dans sa configuration matérielle ou logicielle.

Le deuxième élément est *Netmagis*[9], lui-même alimenté par l'inventaire. Ce logiciel permet, grâce à son module *topo*, d'obtenir une cartographie complète des connexions entre les équipements réseaux. Le lien entre les équipements réseaux est découvert grâce au protocole *LLDP*[10].

4.2 Synchronisations

Bien qu'il existe déjà des extensions permettant l'import d'une liste d'hôtes depuis *GLPI* vers *Centreon*, tel que le module *Centreon-GLPI*[11], ces dernières ne nous permettaient pas d'obtenir le niveau d'automatisation et d'intégration désiré, en particulier en ce qui concerne l'application automatique de modèles de supervision aux hôtes importés, ainsi que la définition des parentés entre équipements. Ce dernier point est particulièrement important car il permet ainsi de déterminer immédiatement la source d'une interruption de service sur le réseau ; les équipements « fils » d'un équipement en panne ayant ainsi un statut particulier (*injoignable*).

Nous avons donc décidé de développer notre propre librairie de synchronisation, que nous avons nommée *CentAPI*, basée sur le module *Centreon CLAPI*[12] qui fourni une interface en ligne de commande pour contrôler *Centreon*.

Premièrement, *CentAPI* se connecte à la base de données de *GLPI* et en extrait pour chaque machine : le nom d'hôte, l'adresse IP, le système d'exploitation, le fabricant, le modèle et dans le cas d'une machine virtuelle le serveur de virtualisation sur lequel elle est hébergée. Par ailleurs, un *tag* configuré sur le client *FusionInventory* permet de définir sur chaque machine le ou les modèles de supervision applicables (figure 2).

Chaque modèle mutualise un ensemble de sondes de supervision communes à des machines ou équipements partageant un service ou des caractéristiques communes (serveur de messagerie, serveur de marque *HP*, etc.).

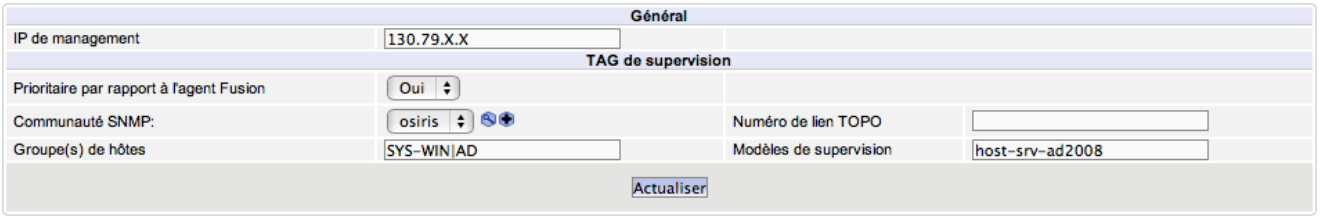

Figure 2 - Paramètres de supervision dans GLPI

Deuxièmement, *CentAPI* extrait de la deuxième brique de notre référentiel, *Netmagis*, les éléments propres aux équipements réseaux, tels que le nom d'hôte, l'adresse IP d'administration, la communauté *SNMP*, et l'*OID SNMP* du matériel. Ces éléments nous permettent de déterminer le modèle exact de l'équipement. Sont également extraits tous les liens entre les équipements réseaux, nous permettant de générer un graphe non orienté de la topologie du réseau.

À partir de ce graphe, nous pouvons déterminer le chemin entre l'hôte et un équipement de référence situé le plus près possible au cœur du réseau (un commutateur de cœur). Pour ce faire nous utilisons l'algorithme de Dijkstra. Cependant ce calcul étant coûteux, il convient de le faire pour le moins d'itérations possible. Nous allons donc, pour chaque hôte

tout d'abord vérifier qu'un de ses voisins directs n'a pas déjà un chemin connu vers l'équipement de référence. Il est par exemple inutile de déterminer le chemin complet d'un point d'accès si on a déjà le chemin du commutateur sur lequel il est connecté. Les chemins ainsi obtenus nous permettent de définir le parent de chaque équipement.

Centreon repose sur le logiciel *Nagios* installé sur les différents satellites de supervision pour effectuer les tests. Cependant afin que les parentés soient prises en compte, il est nécessaire que tous les équipements liés soient supervisés par le même satellite. Afin de palier à cette contrainte, nous avons regroupé les systèmes supervisés par secteur géographique, délimités par le commutateur de cœur associé.

Satellite	**Cible**
Central	Satellites
`sia`	Métrologie des liens réseaux et traps SNMP
`metro-be1`	Campus Esplanade
`metro-be2`	Réseau hors-bande
`metro-be3`	Campus Historique et Médecine
`metro-be4`	Satellite par défaut
`metro-be5`	Campus Illkirch

4.3 Tableaux de bord et vues

Centreon a une interface web très riche. Elle est intéressante pour l'administrateur de la plate-forme mais peut très vite dérouter l'utilisateur non averti. De plus, au sein de la Direction informatique, les équipes ne s'interressent pas toutes aux mêmes informations. Si l'on se réfère aux différents départements de la DI, le département infrastructures se focalisera plutôt sur la disponibilité des équipements, le département services métiers sur les applications et services offert aux utilisateurs alors que l'équipe support souhaitera avoir une vision plus proche du catalogue des services. Partant de ce constat, nous avons décidé de créer des tableaux de bord et des « vues » adaptées à chaque équipe.

Centreon possède une fonctionalité très intérressante de gestion des droits (*ACL*). Les *ACL* permettent de donner à un utilisateur ou un groupe d'utilisateurs une vue et des droits sur toutes sortes de ressources : un équipement, un groupe d'équipements, un service ou un groupe de services. Le système d'*ACL* permet aussi de personnaliser l'interface de *Centreon* pour n'afficher que les données ou les menus nécessaires à un groupe d'utilisateurs. Par exemple, l'utilisateur par défaut n'aura pas accès aux menus de configuration de *Centreon*. Par contre, il pourra acquitter une alarme concernant son périmètre.

Pour faciliter l'adoption de l'outil de supervision par les équipes, nous avons créé des tableaux de bord très épurés apportant une lisibilité optimale. Ces tableaux de bord s'appuient sur le système de groupes d'hôtes ou de services et sur le système d'*ACL*. Les informations affichées sont simplement récupérées dans les bases de données de *Centreon* à l'aide de requêtes *SQL*.

Les tableaux de bord ne sont pas que purement informatifs. Ils fonctionnent en interaction avec *Centreon*. Une alarme peut être acquittée directement par l'intermédiaire d'un tableau de bord. Pour chacune d'entre elles un lien symbolique pointe sur la fonctionnalité d'acquittement de *Centreon* facilitant la tâche à l'utilisateur. Les périodes de maintenance programmées — pendant lesquelles un équipement ou un service n'est pas supervisé — sont automatiquement affichées sur les tableaux de bord afin d'informer les équipes, améliorant ainsi la communication opérationnelle.

Ainsi nous avons créé plusieurs tableaux de bord :

- un tableau de bord pour le département infrastructures, qui remonte toutes les alarmes liées aux équipements ou services d'infrastructures,
- un tableau de bord pour le département services métiers, qui remonte uniquement les informations concernant les applications et services aux utilisateurs. Il ne contient aucune information sur des équipements,
- un tableau de bord pour la direction et le département organisation concernant la disponibilité des services,
- un tableau de bord pour l'équipe support qui affiche tous les avis de maintenance ou les équipements dont une maintenance programmées a été planifiée dans *Centreon*. Les avis de maintenance sont renseignés par les équipes infrastructures et services métiers. Il affiche également la disponibilité instantanée des services offerts aux utilisateurs que nous allons maintenant décrire.

4.3.1 Disponibilité des services aux utilisateurs

Un service comme l'entend un utilisateur peut être complexe. Souvent, il ne s'agit pas d'une simple application que l'on peut superviser à l'aide d'un simple test. Il est le résultat de l'interaction entre de nombreux équipements et applications apportant chacun leur brique à l'édifice.

Prenons pour exemple le service de portail captif du réseau sans fil *Osiris*. Il s'agit de deux pare-feux redondants offrant une authentification de type web. Sur chacun tourne un serveur *DHCP*, un serveur *HTTPS* et le démon de connexion des utilisateurs. Les deux portails captifs dépendent du serveur d'authentification *LDAP*.

Pour estimer la disponibilité du service nous utilisons le programme *Nagios Business Process*[13]. Il combine par différentes expressions logiques les états des hôtes et services supervisés dans *Centreon* pour déterminer la disponibilité d'un service (figure 3).

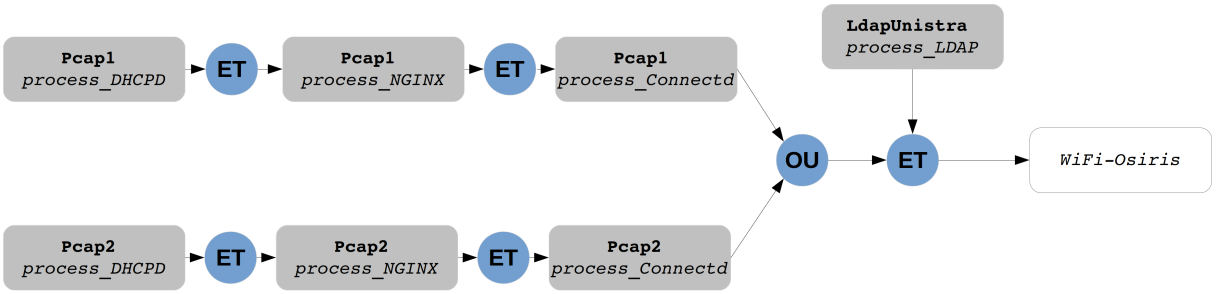

Figure 3 - Exemple de Business Process *pour le Wi-Fi*

4.3.2 Données de reporting

La Direction informatique s'est investie dans un projet[14] de mise en place de bonnes pratiques s'inspirant du modèle ITIL [3]. Le processus *ITIL* « gestion de la disponibilité » s'appuie pleinement sur la plate-forme *Centreon* et l'utilitaire *Nagios Business Process*.

Le but du processus est :

- de calculer la disponibilité des services les plus critiques par rapport aux *SLA* [4] du catalogue des services,
- de remonter les données nécessaires à l'analyse des causes d'un incident majeur,
- de mettre en place les actions et outils nécessaires pour améliorer la disponibilté d'un service.

Ainsi jour après jour des tableaux de disponibilité sont générés à partir de la base d'événements *Centreon* (tableau 2). Pour chaque service, les informations suivantes y sont remontées soit en 24 heures sur 24 ou selon les *SLA* définis (8-18 heures) :

- le taux de disponibilité de l'application sur une période donnée,
- les taux d'indisponibilité ou de service dégradé,
- le nombre d'occurences d'alerte sur la période.

Service	Disponibilté	Dégradé — Occurences	Critique — Occurences	*MTBSI* [5] (en jours)
Agenda partagé	**99,58 %**	**0,00 % — 0**	**0,42 % — 3**	**2**

Tableau 2 - Exemple de reporting pour l'agenda partagé

Avec la version *Centreon* que nous utilisons, il existe deux méthodes pour calculer la disponibilité.

En 24 heures sur 24, les données sont pré-calculées par *Centreon*. Il suffit de les collecter à l'aide d'une simple requête *SQL*.

3. *Information Technology Infrastructure Librairy* : http://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
4. *Service Level Agreement* : http://fr.wikipedia.org/wiki/Service_level_agreement
5. Le *MTBSI* (*Mean Time Between Service Incidents*) est le temps moyen entre deux pannes d'un système

Pour calculer une disponibilté selon des *SLA*, cela est un peu plus complexe. Même, s'il est tout a fait possible de configurer sur *Centreon* des plages de supervision pour un service, si celui-ci passe en alarme juste avant la fin de la plage de surveillance, il restera en alarme jusqu'à la reprise de la surveillance. La disponibilité est donc calculée à partir des logs d'événements.

4.4 Bonnes pratiques

L'exploitation d'une solution de supervision sur un large périmètre, même la plus automatisée possible, passe par la mise en place de bonnes pratiques. Celles-ci sont indispensables pour conserver une vision réaliste de l'état du système d'information.

Ainsi nous avons créé des procédures d'exploitation dédiées à la supervision. Ces procédures détaillent :

- la préparation des équipements à superviser (configurations *SNMP*, *NRPE*, adresses d'administration, *tag FusionInventory*, etc.), permettant aux administrateurs des serveurs d'inclure tous les paquets et configurations nécessaires dans les recettes *Chef* [15],
- la gestion des alertes remontées par la plate-forme de supervision c'est-à-dire la prise en compte de l'alerte : ouverture d'un ticket d'incident, acquittement de l'alarme en fonction de la criticité, etc.

Ces bonnes pratiques ne se limitent pas seulement au périmètre de l'exploitation de la supervision. Dans le département infrastructures, elles ont été intégrées dans une série de procédures que nous appelons « cycle de vie des équipements ».

Le cycle de vie d'un équipement détaille les actions à mettre en oeuvre pour exploiter un équipement, de sa mise en production jusqu'à son démantèlement, en passant par son remplacement en cas de panne. Il prend la forme d'une « check list » incluant :

- le nommage,
- l'adressage IP dont l'adresse d'administration,
- les déclarations DNS,
- la configuration des serveurs d'authentification pour les équipements,
- la génération des configurations dont celles dédiées à la supervision,
- et surtout, dans l'inventaire GLPI, le passage de l'équipement « en production », étape déclenchant son intégration dans la plate-forme de supervision.

Beaucoup de ces opérations sont basées sur l'exécution de scripts, donc partiellement automatisées. Cependant quelque soit le niveau d'automatisation, l'intervention humaine est toujours nécessaire.

5 Adaptation de la solution à une plate-forme de recherche

L'architecture proposée dans cet article peut facilement être réutilisée dans un autre contexte. En 2012, ce projet a été adapté aux besoins de la plate-forme expérimentale de recherche *IoT-LAB* (*Internet of Things*) [16] membre de l'*Equipex FIT* (équipement d'excellence *Future Internet of Things*) [17]. *IoT-LAB* est distribuée sur plusieurs sites dont le laboratoire ICube de Strasbourg qui a adapté la solution de supervision de la Direction informatique.

En terme d'exploitation, la plate-forme *IoT-LAB* est gérée de manière collégiale par les administrateurs de chaque site. D'une part, il existe des tâches locales à chaque site pour maintenir les noeuds et les services locaux. D'autre part, l'architecture centralisée de la plate-forme concentre les services critiques indispensables au fonctionnement des sites distants. Grâce à sa gestion multi-utilisateurs et le support de multiple instances de moteur de supervision, *Centreon* facilite la supervision autant au niveau local qu'au niveau global.

Dans un soucis de robustesse, une instance *Nagios* a été déployée sur chaque site pour vérifier l'état des noeuds et des services locaux en cas de panne réseau. Cette stratégie permet également de répartir la charge des instances *Nagios* car la plate-forme compte actuellement quatre sites et en accueillera trois supplémentaires.

L'architecture système et réseau reste sensiblement identique à celle de la Direction informatique (figure 4). Un serveur de supervision central héberge le serveur web *Centreon*, le collecteur *NDO* et la base *MySQL*. Les satellites *Nagios* sont instanciés dans des machines virtuelles tournant sur un serveur local *KVM* présent sur chaque site de la plate-forme. Spécifiquement pour *IoT-LAB*, les déploiements du serveur *Centreon* et des satellites *Nagios* ont été entièrement automatisés

grâce à l'outil *Fabric*[18], une librairie de déploiement de systèmes et d'applications écrite en Python. Un fichier de configuration propre à chaque site est à renseigner au préalable avant de déployer. L'ajout d'hôte et de services s'opère par la librairie *Fabric* qui appelle la commande en ligne *CLAPI* tout en consultant le référentiel de ressources renseignées dans un fichier *CSV*. Contrairement à la Direction informatique, l'exploitation de la plate-forme *IoT-LAB* ne nécessite pas un référentiel dédié comme *GLPI* et une solution basée sur des fichiers plats est suffisante. Actuellement, nous comptons 1 043 hôtes avec 1 221 services répartis sur six instances *Nagios*.

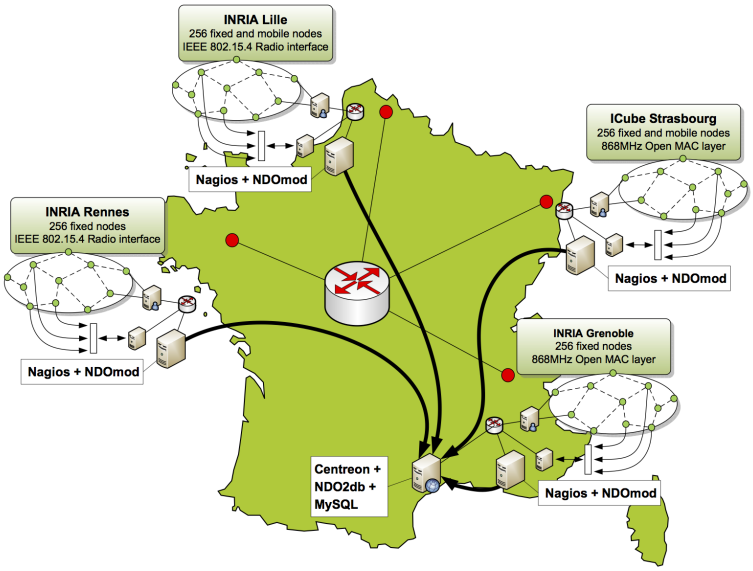

Figure 4 - Architecture Centreon distribuée IoT-LAB

Différentes populations utilisent l'interface web de *Centreon* : les administrateurs pour la supervision des services, les membres du comité de pilotage pour le reporting. À terme, les utilisateurs de *IoT-LAB* pourront consulter l'état global de la plate-forme directement via leur portail web.

6 Retour d'expérience et perspectives

La solution de supervision mise en place a largement répondu aux besoins des différentes équipes de la Direction informatique en terme de fonctionnalités. Les délais de détection de pannes et de compréhension des causes ont été sensiblement raccourcis renforçant l'impression de visibilité et de maitrise du système d'information.

En ce qui concerne l'exploitation, la fiabilité du couple *Centreon-Nagios* et la synchronisation automatique avec la base d'inventaire rendent les actions de maintenance par les experts de la plate-forme très occasionnelles. Les équipes d'exploitation ont facilement intégré les concepts de l'exploitation quotidienne des alertes au travers des interfaces mises à leur disposition.

En revanche l'automatisation a ses limites. Elle fonctionne très bien pour les équipements réseau, les systèmes ou la supervision d'applications déployées en nombre. Elle est cependant moins aisée pour les services complexes. L'absence d'un outil « magique » façon *CMDB* [6], permettant de référencer et de modéliser les services, nécessite une certaine rigueur pour maintenir leur supervision à jour. La configuration de l'outil *Nagios Business Process* reste manuelle. Il en est de même pour les serveurs et services « atypiques ». Les responsables d'applications doivent alors être impliqués dans la supervision. Heureusement, la supervision d'un service n'évolue que rarement.

Les tableaux de bord ont permis aux utilisateurs d'adopter la solution. C'est en grande partie grâce aux écrans de supervision de plus de 52" mis en place dans plusieurs équipes de la DI, dans les endroits les plus passants ou les plus visibles. Si au départ l'accueil des écrans a été plutôt mitigé, les collègues se sont rapidement intéressés aux tableaux de bords qui y étaient affichés et les ont alors naturellement adoptés.

6. *Configuration Management Database* : http://fr.wikipedia.org/wiki/Configuration_Management_DataBase

Le succès de la plate-forme engendre quelques problèmes plus techniques. L'intégration continue de nouveaux équipements et services (à ce jour plus de 15 000 tests par période de une à cinq minutes) induit une certaine latence sur les satellites. Ainsi la question se pose sur l'évolution des satellites *Nagios* vers des satellites sous *Shinken*[19] ou *Centreon Engine*[20]. *Shinken* est une implementation performante de *Nagios* écrite en *Python* qui intègre nativement de nombreuses fonctionnalités comme une architecture distribuée ainsi que les vues métiers comme *Nagios Business Process*. *Centreon Engine* est un fork de *Nagios* intégrant des patchs augmentant les performances de polling. Une évolution vers ces nouveaux satellites se fera éventuellement dans un second temps.

Enfin, l'intervention de plusieurs personnes dans les opérations de création de templates de supervision apporte un risque de perte d'homogénéité et de cohérence dans les configurations de *Centreon*. Il nous appartient de rester vigilant et d'échanger régulièrement au sein du groupe de supervision créé au sein de la DI.

7 Conclusion

La mise en place d'une solution de supervision à l'échelle de la Direction informatique de l'Université de Strasbourg est un enjeu de taille et complexe. La phase d'intégration est longue avec un investissement conséquent en matière de développement et de configuration. L'adaptation de notre architecture de supervision à une plate-forme de recherche prouve le caractère reproductible de cette solution à un autre contexte. Suite à la prise en main de ce nouvel outil, des améliorations sensibles concernant la réactivité de l'exploitation ont été mesurées, augmentant ainsi la disponibilité globale des services, et offrant une meilleure communication opérationnelle entre les équipes.

Bibliographie

[1] Centreon, as in 2013. http://www.centreon.com/.

[2] Nagios, as in 2013. http://www.nagios.org/.

[3] NDOUtils, as in 2013. http://exchange.nagios.org/directory/Addons/Database-Backends/NDOUtils/details.

[4] J. Case, M. Fedor, M. Schoffstall, et J. Davin. A Simple Network Management Protocol (SNMP), Internet Engineering Task Force Request for Comments (RFC) 1157, May 1990.

[5] NRPE - Nagios Remote Plugin Executor, as in 2013. http://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details.

[6] Munin, as in 2013. http://munin-monitoring.org/.

[7] GLPI, as in 2013. http://www.glpi-project.org/.

[8] FusionInventory, as in 2013. http://www.fusioninventory.org/.

[9] Pierre David, Jean Benoit, et Sébastien Boggia. Gérer son système d'information réseau avec Netmagis. Dans *Actes du congrès JRES2011*, Toulouse, Novembre 2011. https://2011.jres.org/archives/35/paper35_article.pdf.

[10] IEEE 802.1AB. IEEE Standards for local and metropolitan area networks - Station and Media Access Control Connectivity Discovery, 2005.

[11] Centreon GLPI, as in 2013. https://forge.centreon.com/projects/centreon-glpi.

[12] Centreon CLAPI, as in 2013. https://forge.centreon.com/projects/centreon-clapi.

[13] Nagios Business Process AddOns, as in 2013. http://bp-addon.monitoringexchange.org/.

[14] Christophe Saillard et Julien Dupré. Bilan de 4 ans d'ITIL à l'Université de Strasbourg. Dans *Actes du congrès JRES2013*, Montpellier, Décembre 2013.

[15] Christophe Palanche et Alain Heinrich. Automatisation de l'administration de 700 serveurs avec Chef. Dans *Actes du congrès JRES2013*, Montpellier, Décembre 2013.

[16] IoT-LAB, as in 2013. http://www.iot-lab.fr/.

[17] FIT Equipex, as in 2013. http://www.fit-equipex.fr/.

[18] Fabric, as in 2013. http://fabric.org/.

[19] Shinken, as in 2013. http://www.shinken-monitoring.org/.

[20] Centreon Engine, as in 2013. https://forge.centreon.com/projects/centreon-engine.