



HAL
open science

iSup - Développement d'une plate-forme de supervision complète et homogène pour les réseaux Lorrains

Sébastien Morosi, Vincent Delove

► To cite this version:

Sébastien Morosi, Vincent Delove. iSup - Développement d'une plate-forme de supervision complète et homogène pour les réseaux Lorrains. JRES (Journées réseaux de l'enseignement et de la recherche) 2007, Renater, Nov 2007, Strasbourg, France. hal-04802881v2

HAL Id: hal-04802881

<https://hal.science/hal-04802881v2>

Submitted on 29 Nov 2024

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

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



Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

iSup – Développement d’une plate-forme de supervision complète et homogène pour les réseaux Lorrains

Sébastien Morosi

CIRIL - Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du Doyen Roubault
54500 VANDOEUVRE-LÈS-NANCY - FRANCE
Sebastien.Morosi@ciril.fr

Vincent Delove

CIRIL - Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du Doyen Roubault
54500 VANDOEUVRE-LÈS-NANCY - FRANCE
Vincent.Delove@ciril.fr

Résumé

Fort d’une grande expérience dans l’administration et la supervision des réseaux, le CIRIL a entrepris en 2006 le développement d’une nouvelle plate-forme afin de superviser d’une façon plus homogène les réseaux qu’il administre ainsi que les services associés.

De la conception du système d’information jusqu’à la présentation des statistiques collectées, nous nous sommes efforcés de mettre en œuvre une solution de supervision s’inscrivant dans une démarche d’unification, d’automatisation et de délégation des tâches d’exploitation dans laquelle s’est engagé le CIRIL. Par ailleurs, la diversité des technologies et des équipements à surveiller nous a poussé à apporter une attention particulière aux aspects de flexibilité et d’extensibilité de cette solution.

L’application iSup, née de ce travail, permet de remplacer la quasi-totalité des outils précédemment utilisés afin de remplir les diverses fonctions de supervision des réseaux StanNet, Lothaire et eLorraine.

Mots clefs

Supervision, statistiques, métriques, alertes, cricket, RRD

1 Introduction

La demande toujours plus importante en matière de fiabilité, de disponibilité et de sécurité a placé depuis maintenant plusieurs années la métrologie et la supervision au cœur du métier d’ingénieur réseau. La connaissance et la surveillance du comportement de systèmes de plus en plus complexes passent aujourd’hui par l’utilisation d’outils parfaitement adaptés. Une bonne solution de supervision doit à ce titre permettre aux ingénieurs de veiller au bon fonctionnement des services au quotidien (rapports d’activité, alertes sur détection de problèmes) et aux décideurs de faire les bons choix en terme de pilotage (dimensionnement, évolutions).

Au CIRIL (Centre Interuniversitaire de Ressources Informatiques de Lorraine), la multiplicité des outils couplée à la volonté de disposer d’un niveau de fonctionnalités homogène sur l’ensemble des réseaux opérés, nous ont amenés en 2006 à repenser entièrement le système de supervision en place. L’expérience acquise dans ce domaine à travers divers projets nous a permis de considérer le développement d’une nouvelle plate-forme comme une alternative envisageable, face à la mise en œuvre d’une solution commerciale ou libre. L’intégration aux différentes bases de données existantes impose dans tous les cas des développements importants.

Les éléments que nous présentons dans cet article sont pour la plupart opérationnels depuis quelques mois ce qui nous permet d’avoir un recul suffisant pour évaluer les bénéfices du travail accompli ainsi que les possibilités restant à explorer.

Après avoir exposé brièvement le contexte, nous présenterons les choix réalisés afin de répondre au mieux aux contraintes précédemment citées. En premier lieu, nous présenterons les bases de la plate-forme mise en œuvre. Par la suite nous détaillerons successivement les fonctionnalités avancées que nous avons pu construire sur ce noyau solide.

2 Contexte et besoins

La mission principale de la cellule réseau du CIRIL est d’assurer l’exploitation et l’administration des réseaux StanNet¹, Lothaire² et eLorraine³.

Ces trois réseaux forment un ensemble regroupant un nombre important d’équipements (de l’ordre du millier), de

¹ Réseau métropolitain nancéen de l’Enseignement Supérieur et de la Recherche

² Réseau Lorrain de Télécommunication à Haut débit pour les Applications Informatiques de la Recherche et de l’Enseignement Supérieur

³ Réseau haut-débit des lycées de Lorraine

technologies, de services mais aussi d'interlocuteurs. Ces dimensions justifient la démarche d'automatisation et de délégation des tâches d'exploitation dans laquelle s'est engagé le CIRIL depuis plusieurs années.

Dans ce contexte et étant données les évolutions de plus en plus rapides apportées aux infrastructures administrées, la supervision était devenue une tâche fastidieuse en terme de maintenance. Afin de couvrir l'ensemble des besoins, de nombreux outils avaient été déployés au cours du temps : *netup*, *MRTG*, *Nagios*, *Cricket*, *Cacti* et des scripts maison. Ces outils étant tous indépendants, leur configuration lors des modifications de l'infrastructure engendrait un travail manuel fastidieux et inévitablement source d'erreurs. Par conséquent, la cohérence entre les outils et les équipements était également de plus en plus difficile à assurer et à vérifier.

De plus, les outils en place ne permettaient ni d'offrir un accès authentifié et personnalisé à nos correspondants, ni de s'interfacer avec notre système d'informations.

Conscient du travail que représente le développement complet d'une nouvelle solution, nous avons choisi de réutiliser un certain nombre de composants disponibles et déjà éprouvés. L'essentiel de notre travail s'est ainsi concentré sur l'intégration de logiciels libres, l'automatisation des tâches et le développement de fonctionnalités à valeurs ajoutées.

3 Système d'information centralisé

Dans le souci de concevoir une plate-forme flexible, l'ensemble des éléments participant à la configuration et à la gestion de la plate-forme est réuni en un emplacement unique : une base de donnée MySQL. Nous allons décrire ici les notions principales constituant ce système d'information.

3.1 Les métriques

La collecte des informations est la première étape dans l'élaboration d'un système de supervision. Un objet identifiant une source de données a donc été défini. Nous entendons ici par source de données la description d'une localisation permettant d'obtenir une valeur caractéristique comme une charge CPU, un débit ou encore une température. Chacun des OIDs pouvant être décrit à l'aide du protocole SNMP constitue ainsi une source de données distincte. Il existe naturellement bien d'autres façons de collecter des informations (interrogations LDAP ou SQL, résultat d'exécution d'un programme...) qui doivent être supportées. La plupart du temps un certain nombre de paramètres devra être fourni à cet objet pour réellement accéder aux données.

Etant donné qu'une simple source de données est souvent insuffisante pour décrire un comportement global, il nous a fallu regrouper plusieurs de ces objets pour définir une structure de données plus significative. Par exemple, la

définition d'une métrique⁴ comme le trafic sur une interface se décompose en plusieurs éléments :

- les débits entrant et sortant
- la vitesse du support physique associé

A partir de ces informations il sera alors possible de déterminer les pourcentages d'utilisation d'une ligne et d'en suivre l'évolution au cours du temps. Toutes les informations de même nature (définissant une métrique) seront ainsi accessibles simultanément. En outre, la définition d'une métrique spécifique également les modèles de graphes qui seront utilisés pour réaliser l'analyse visuelle des données.

La diversité des technologies et des équipements entraîne un support variable dans l'implémentation des sources de données accessibles. A titre d'exemple, certaines interfaces ne permettent pas la collecte de compteurs SNMP 64 bits pour la mesure de leur trafic. Il est alors obligatoire d'interroger les compteurs SNMP 32 bits. Cela conduit donc à créer deux définitions pour une même métrique. Le choix entre ces définitions sera ensuite réalisé de façon automatisée en fonction du type d'équipement supervisé. Ce fonctionnement évite de multiplier inutilement les métriques.

Les paramètres nécessaires à l'instanciation d'une métrique sont associés à chacune de ces définitions. En reprenant toujours le même exemple, la collecte SNMP du trafic d'une interface requiert la connaissance de l'entrée *ifDescr* correspondante.

Au final, une métrique est donc entièrement définie par :

- les sources de données qui la composent
- le type d'équipement auquel elle se rattache
- les paramètres nécessaires à son instanciation

3.2 Les services

L'ensemble des équipements supervisés est renseigné dans la base en précisant pour chacun d'eux le nom, le domaine DNS, le type, l'adresse IP d'administration, et les paramètres SNMP (version, communauté) si nécessaire. En utilisant le type d'un équipement et conformément à la démarche présentée dans la partie précédente, on sera capable de retrouver la totalité des métriques accessibles pour ce dernier. En marge de la supervision, les informations de noms et de domaines pourront également être utilisées afin de vérifier les enregistrements DNS pour les domaines concernés.

Un service représente une instance de métrique pour un équipement donné. A ce titre, il constitue l'élément de base de la supervision dans notre système. Chaque service est associé à un équipement et à une métrique définissant à eux deux l'ensemble des sources de données collectées. Par exemple, le service associant la métrique « cpu » au routeur « gw1.nancy » entraînera la collecte de trois OIDs SNMP à une fréquence donnée.

⁴ Ensemble de mesures caractérisant un comportement

Chaque service associé à une métrique qui nécessite le passage de paramètres doit définir des attributs qui fixeront les valeurs à utiliser pour ces paramètres. Le service chargé de la mesure du trafic d'une interface via SNMP devra, dans ces conditions, définir un attribut renseignant le nom de celle-ci (entrée *ifDescr*). Ces attributs peuvent également servir à stocker d'autres types d'informations. En effet, l'obtention des débits (max) d'une interface par interrogation SNMP n'étant pas toujours possible, ces attributs peuvent constituer un moyen astucieux de stockage de ces valeurs. Elles seront ensuite récupérées à chaque collecte conformément aux explications déjà fournies dans ce document.

Un service peut finalement être un service dit composé auquel cas il constitue uniquement une réunion de services pouvant eux-mêmes être composés. Ce type d'agrégation est utilisé pour superviser des fonctions plus abstraites dans leur globalité.

3.3 Les états

A chaque service est associé un état qui joue le rôle d'indicateur de surveillance. Dans la pratique cet état est matérialisé par une valeur entière qui évoluera en fonction de seuils définis par l'administrateur. Les seuils sont associés aux sources de données qui définissent la métrique du service en question. Par exemple, les sources de données nommées par convention *cpu5sec*, *cpu1min*, *cpu5min* qui sont associées à la métrique « CPU » d'un routeur peuvent définir les seuils suivants :

- *cpu1min* : Si supérieur à 90 alors état = 1
- *cpu5min* : Si supérieur à 80 alors état = 1
- *cpu5min* : Si supérieur à 90 alors état = 2

Dans ces conditions, chaque service sera par défaut supervisé par les seuils liés aux sources de données définissant sa métrique.

Dans un souci de flexibilité, il est également possible de surcharger les seuils par défaut pour un service en particulier. Si un routeur particulièrement chargé entraîne un nombre jugé trop important de changements d'états, alors les seuils peuvent être adaptés plus spécifiquement pour ce service.

Chaque changement d'état conduit à la création ou à la modification d'un événement enregistré dans la base. Ces enregistrements décrivent donc l'historique de supervision et permettront par exemple la génération de graphes d'états. Des modèles d'actions sont également associés aux services pour permettre l'exécution de traitements en réponse aux différents événements générés par la plate-forme. Un modèle est caractérisé par :

- un type d'action : envoi d'un SMS ou d'un courriel, exécution d'une commande...
- un paramètre d'action servant à représenter par exemple l'adresse du destinataire de la notification à envoyer ou la commande à exécuter.

- une liste d'états : seuls ces états conduiront à l'exécution du traitement.
- une plage horaire qui restreint l'activation du traitement à une période définie

4 Collecte et stockage des données

La fonction de collecte consiste à récupérer les valeurs pour l'ensemble des services de la plate-forme. La réalisation d'un nouveau collecteur n'a pas semblé nécessaire pour répondre aux besoins attendus. En effet, le collecteur *Cricket*⁵, déjà utilisé par le passé, est apparu comme très adapté en terme de flexibilité de configuration et de rapidité d'exécution. L'utilisation de bases « *RRDs*⁶ » comme système de stockage des données a également constitué un élément de choix.

La configuration de *Cricket* repose sur un ensemble de fichiers répartis dans une structure arborescente. Chaque branche peut ainsi être collectée séparément. Etant donné le très grand nombre de données à collecter sur Lothaire, nous avons choisi de paralléliser la collecte en divisant la configuration dans plusieurs de ces branches. Leur taille est déterminée de telle sorte que le temps total de traitement de la branche ne puisse pas dépasser la période de collecte (généralement fixée à 5 minutes) même dans le cas où chaque récupération de valeur conduit à un échec par expiration.

La configuration du collecteur est générée entièrement à partir de la base de données décrite dans la partie précédente. Une modification de la base, telle que l'ajout d'un nouveau service, entraînera automatiquement la reconstruction de la configuration. Ce fonctionnement permet d'assurer la collecte même si la base de donnée devient momentanément indisponible.

A l'issue de la collecte, les valeurs récupérées sont stockées dans des bases *RRDs* spécifiques à chaque service. Le fonctionnement de ces bases repose comme leurs noms l'indiquent sur le principe de *Round Robin*. Les bases de la plate-forme renferment quatre niveaux de détails différents pour permettre d'établir des vues très détaillées à court terme et plus globales à long terme. Pour un service collecté toutes les cinq minutes, l'intégralité des échantillons sera par exemple conservée pendant une semaine, les moyennes sur 30 minutes pendant un mois, les moyennes sur deux heures pendant un an et finalement les moyennes sur une journée pendant 3 ans. Conjointement à toutes ces moyennes sont également sauvegardées les valeurs minimum et maximum pour chacun des intervalles cités. Au final, cette solution offre un niveau de détail très intéressant pour un coût de stockage (volume) relativement faible.

La volonté de conserver les informations sur de longues périodes oblige à mener un effort particulier sur la

⁵ Utilisation du collecteur de *Cricket* : <http://cricket.sourceforge.net/>

⁶ *Round Robin Database* : <http://oss.oetiker.ch/rrdtool/>

pérennité des données. C'est pourquoi la convention de nommage des services repose sur leur sémantique plutôt que sur la réalité technique. La modification d'un paramètre lié à un service ne doit donc pas conduire à la perte ou à l'altération des données déjà collectées. Par exemple, dans le cas d'un service chargé de superviser le trafic sur une interface, une évolution de débit ou même le changement de l'interface doit être réalisé en assurant la continuité des informations.

5 Métriques supervisées

Notre projet initial de plate-forme de supervision comportait deux grands axes : disposer d'un outil robuste et polyvalent, mais également des bonnes informations au bon moment. Nous avons vu jusqu'à présent que iSup est une plate-forme hautement configurable construite sur des bases robustes.

Un travail important dans la mise en place de la supervision a consisté à déterminer les données à collecter pour chaque type d'équipement ou de service. Nous avons essayé de toujours nous tenir au « nécessaire et suffisant ». En effet, il faut toujours disposer des informations permettant de déterminer le bon fonctionnement d'un service, mais il ne faut pas pour autant s'encombrer d'informations inutiles. Trop d'information nuit à la compréhension et à la synthèse rapide.

Nous avons donc déterminé pour chaque service ou équipement les valeurs que nous souhaitons superviser et avons renseigné la base iSup. Nous avons créé des modèles de supervision afin de pouvoir appliquer automatiquement à chaque équipement les paramètres par défaut. De plus, afin de faciliter cette tâche, des *scripts* d'auto-découverte ont été développés et permettent en un temps minimum d'ajouter un nouvel équipement au parc supervisé.

A ce jour nous supervisons via iSup nos serveurs, routeurs, commutateurs, liaisons et interfaces. Nous envisageons à court terme d'y intégrer la supervision des services (VPN, DNS, messagerie...). A ce jour, environ 2000 services sont configurés dans notre plate-forme de supervision.

6 Analyse et alertes

6.1 La détection de problème

L'interprétation des informations collectées est un point essentiel dans le métier d'administrateur de réseaux et de systèmes. Il est indispensable de savoir analyser les informations recueillies afin de détecter et de prévenir les potentielles anomalies.

Cette tâche devient rapidement fastidieuse et consommatrice en temps si elle ne peut être automatisée et systématisée. Ainsi, une plate-forme de supervision doit être en mesure d'analyser les informations collectées afin de prévenir les administrateurs en cas de dysfonctionnement.

iSup a donc été conçu pour que des moteurs d'analyse puissent être développés puis associés à des services. Nous avons à ce jour implémenté plusieurs algorithmes afin de détecter les pannes et prévenir les dégradations de service :

- un mode basique, déterminant l'état d'un service en comparant les dernières valeurs collectées à des seuils,
- un mode plus évolué basé sur des dépassement de seuils sur une période glissante

Le mode évolué consiste à déterminer si un indicateur a dépassé un seuil trop longtemps pendant une période donnée, comme illustré sur la Figure 1. Prenons un exemple pour bien appréhender ce concept : « Si la CPU de mon routeur a été supérieure à 80% pendant plus de 30 minutes sur une période de 60 minutes, alors il y a un problème ». Cela revient donc à additionner les périodes pendant lesquelles un service a dépassé un seuil (les fenêtres grises t_1 , t_2 , t_3 de la Figure 1) et cela sur une durée déterminée (la fenêtre glissante bleue de la Figure 1). Si cette somme est supérieure à ce qui est toléré, alors il y a alerte.

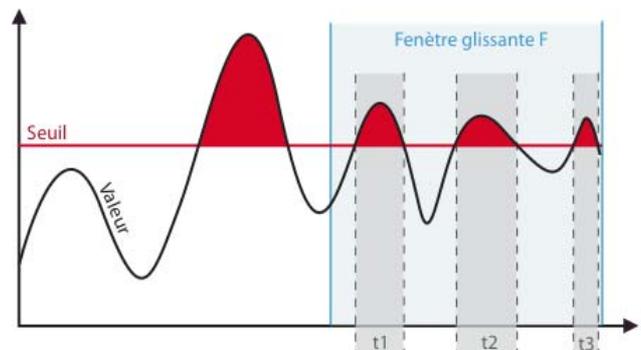


Figure 1: Détection d'alerte avec fenêtre glissante

Ces deux modes sont complémentaires : le mode basique nous renseigne sur l'état d'un service en temps réel et va plutôt être utilisé pour un résultat binaire du type « ça marche » ou « ça ne marche pas » ; le mode évolué a pour objectif de prévenir les dégradations de service en éliminant naturellement les fausses alarmes.

6.2 L'expérience humaine

L'analyse par « l'oeil humain » des métriques supervisées fait généralement intervenir un paramètre qui n'est pas pris en compte par les deux modes précédemment cités : l'expérience. Un administrateur va généralement être capable de détecter une anomalie si une courbe n'est pas « comme d'habitude ». Afin de pouvoir reproduire cette analyse, nous envisageons de développer un moteur capable de vérifier la déviation d'un paramètre par rapport à une moyenne sur une période passée. Il sera ainsi possible pour la plate-forme de supervision de déterminer si un paramètre se comporte « comme d'habitude » ou non. A titre d'exemple, un pic de charge réseau tous les soirs à l'heure des sauvegardes n'est certainement pas problématique. Par contre, le soir où ce pic n'est pas observé, il y a certainement eu un dysfonctionnement.

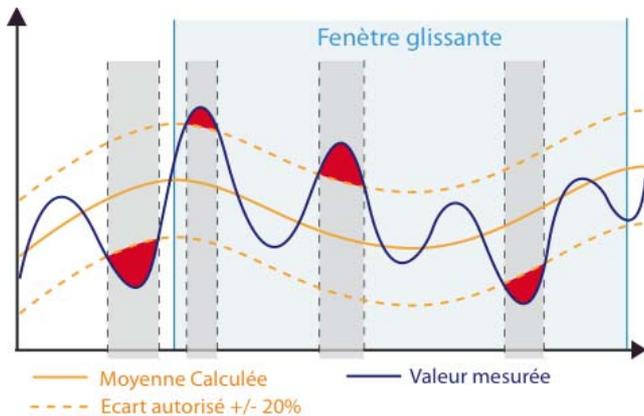


Figure 2: Détection d'alerte sur écart de la moyenne

Comme l'illustre la Figure 2, le moteur va déterminer le profil du service supervisé, puis il va appliquer l'algorithme de la fenêtre glissante pour déterminer si la valeur mesurée s'écarte trop de ce profil. Ce type d'analyse permettra de détecter les comportements anormaux et devrait automatiser un peu plus encore le travail de l'administrateur qui ne peut se concentrer que sur les indicateurs les plus importants.

Chaque service supervisé par iSup va pouvoir être analysé par un ou plusieurs moteurs, l'administrateur ayant en charge l'association moteur/service et le paramétrage du moteur pour chaque service.

6.3 L'état d'un service

L'objectif des analyses décrites précédemment étant de déterminer l'état d'un service, nous avons souhaité simplifier au maximum la compréhension du résultat, et avons opté pour un code couleur : rouge/orange/vert.

En effet, l'analyse de chaque service par un moteur va retourner l'un de ces trois états, sachant que la sémantique que nous y avons associée est la suivante :

- rouge : le service est indisponible
- orange : le service fonctionne, mais de façon dégradée
- vert : le service fonctionne correctement

Notons également que, parfois, l'état d'un service ne peut être déterminé (collecte impossible par exemple), nous avons donc introduit la couleur grise pour le représenter.

Une fois l'état de chaque service déterminé, nous pouvons passer à l'étape suivante : la génération d'alertes.

6.4 Les alertes

Une plate-forme de supervision doit être en mesure de prévenir les administrateurs en cas de dysfonctionnement important, ou en cas de potentiel problème.

Les alertes n'ont pas toutes le même niveau de criticité en fonction du service concerné et du type de problème. Un

routeur régional est généralement plus sensible qu'une borne *wifi*.

Nous avons identifié deux besoins bien distincts :

- l'alerte via message électronique
- et l'alerte par SMS.

L'alerte par SMS est destinée aux administrateurs des services critiques. Ce type d'alerte est plus particulièrement nécessaire en dehors des heures ouvrables afin d'alerter la personne d'astreinte. Ces alertes étant de la plus grande priorité, nous avons connecté à la plate-forme de supervision un boîtier permettant directement l'envoi de SMS.

Les alertes via messagerie électronique permettent de couvrir un ensemble plus large de services et surtout d'informer les équipes de permanence et/ou de support des dysfonctionnements observés.

Comme l'ensemble des fonctionnalités de la plate-forme iSup, les alertes sont configurées via des modèles, chaque service pouvant par la suite être associé à un ou plusieurs de ces modèles. Les événements générés simultanément sont agrégés afin de générer une seule notification. A titre d'exemple, nous avons aujourd'hui un modèle nous avertissant par messagerie de tous les changements d'état d'un service, et un modèle nous permettant d'envoyer un SMS à la personne d'astreinte en dehors des heures ouvrables.

Alerter est une chose, agir en est une autre. Nous avons étendu la notion d'alerte de iSup afin de pouvoir lancer une action de la même façon qu'une alerte. Finalement une alerte n'est qu'une action particulière prise par la plate-forme et nous pouvons associer un *script* à un événement. A ce jour, nous n'avons pas encore configuré d'actions agissant directement sur les équipements afin de tenter de résoudre automatiquement un problème, mais nous l'envisageons pour l'avenir.

6.5 Journalisation

Il ne faut pas oublier que chaque changement d'état d'un service ne fait pas obligatoirement l'objet d'une alerte, ou encore que les alertes peuvent se perdre. Nous avons donc souhaité conserver l'historique de l'état de chaque service. Il nous est ainsi possible de consulter à tout moment l'historique d'un service et de connaître a posteriori le résultat des analyses.

Enfin, tout événement généré par la plate-forme est automatiquement archivé dans des fichiers (*syslog*).

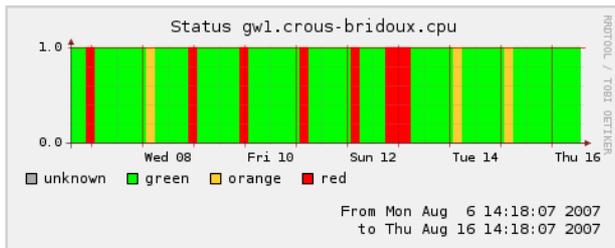


Figure 3: historique de l'état d'un service

7 La présentation des informations

7.1 Pour qui ?

La présentation des données est un point très important pour une plate-forme de supervision, c'est en quelque sorte la partie visible de l'iceberg.

La représentation des informations dépend en grande partie de la personne à qui elles sont destinées. Le besoin de personnalisation de cette présentation a également été très déterminant dans notre décision de développement maison.

Nous avons identifié dans le panel des utilisateurs de la plate-forme de supervision trois grandes catégories :

- le support de premier niveau : typiquement une *hotline* nécessitant une vue en temps réel de la disponibilité des services, afin d'orienter au mieux leurs investigations lors des appels d'utilisateurs
- les administrateurs : des personnes très techniques ayant besoin d'informations détaillées avec un historique précis mais court
- des décideurs/investisseurs ayant besoin d'une analyse sur de longues périodes, afin de connaître les tendances et surtout prévoir les évolutions

De plus, le CIRIL administre/opère les réseaux pour de nombreux établissements et essaye de toujours fournir aux administrateurs de ces établissements des outils permettant de leur déléguer les opérations courantes. Respectant cette démarche, iSup avait pour objectif de fournir aux administrateurs locaux l'accès aux informations concernant les équipements et services dont ils dépendent.

Une des contraintes était donc de proposer un accès authentifié permettant à un utilisateur de ne visualiser que les services les concernant.

7.2 Comment ?

Toutes les données collectées sont accessibles via une interface web. Chaque utilisateur est en mesure de consulter les données le concernant et a la possibilité de personnaliser son interface. Les droits des utilisateurs sont directement stockés dans la base de données de iSup.

7.2.1 Tableau de bord

La vue synthétique de premier niveau a été rendue possible grâce à la mise en place d'un tableau de bord : eBoard (Figure 4). Cette vue consiste à rassembler sur une même page les services souhaités en les symbolisant par des ronds prenant les couleurs vert/orange/rouge en fonction de leur état.

Cette vue a été rendue interactive par l'utilisation du format SVG. Ainsi, l'utilisateur obtient les informations contextuelles au service en le sélectionnant.

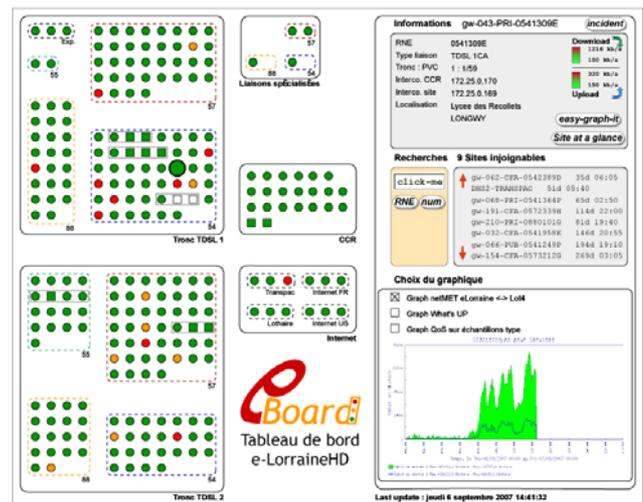


Figure 4: Tableau de bord eBoard

La vue initiale a été réalisée manuellement, les informations contextuelles et de statut sont contenues dans un fichier de données mis à jour automatiquement par iSup.

Ce tableau de bord a été initialement mis en place pour la *hotline* du réseau eLorraine⁷. Un tel outil permet de limiter les demandes de la *hotline* vers les ingénieurs en charge des services. Le projet eLorraine faisant intervenir de nombreux prestataires, eBoard permet également à la *hotline* de rapidement identifier l'origine d'un problème lors d'un appel en provenance d'un lycée.

7.2.2 Rapports détaillés et personnalisation

Au quotidien, les ingénieurs réseau et système ont besoin d'accéder à des informations techniques concernant les équipements administrés. Des données de type « nombre de *broadcast* », « niveau de remplissage des partitions » ou « pourcentage d'utilisation de la CPU » sont des données permettant d'ajuster la configuration des équipements afin d'optimiser les services.

Les données consultées doivent généralement être brutes (pas de moyenne), avec une période d'échantillonnage

⁷ Réseau des Lycées lorrains, à l'initiative du Conseil Régional de Lorraine. eLorraine représente 215 établissements reliés via des liaisons xDSL à une plate-forme régionale de collecte et de services localisée au CIRIL.

courte (au minimum de cinq minutes, voir de la minute), et enfin sur une durée relativement courte (quelques jours).

Nous avons donc développé une interface permettant de visualiser toutes les informations collectées, tout en choisissant la période à afficher. Tous les graphiques sont générés à l'aide de l'outil *RRDtool* comme l'illustre la Figure 5.

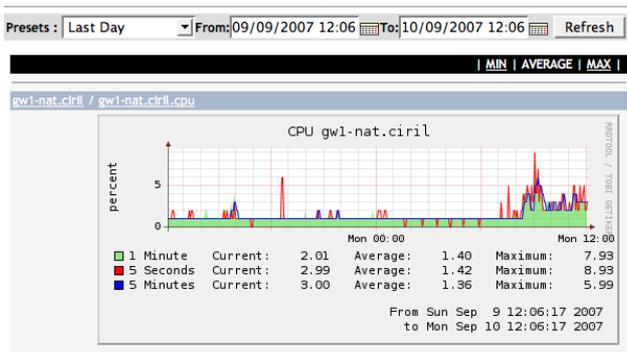


Figure 5: Graphique détaillé Figure

Pour être totalement exploitables, ces données doivent généralement être présentées en groupe, afin de déterminer s'il y a corrélation entre elles. iSup propose entre autre la notion de service composé pour pouvoir afficher sur une même vue des données à mettre en relation. Il est par exemple généralement nécessaire de visualiser sur une même page les graphiques représentant la CPU d'un routeur, le trafic et les temps de réponse sur ses liaisons afin de déterminer s'il y a une corrélation.

iSup a également pour vocation de donner aux correspondants du CIRIL la vue des informations les concernant. Tout utilisateur a généralement des centres d'intérêt variés et consulte quotidiennement les mêmes données. Nous avons donc donné la possibilité à un utilisateur de composer sa page d'accueil ; il peut y disposer ses graphiques favoris et ainsi les consulter très rapidement.

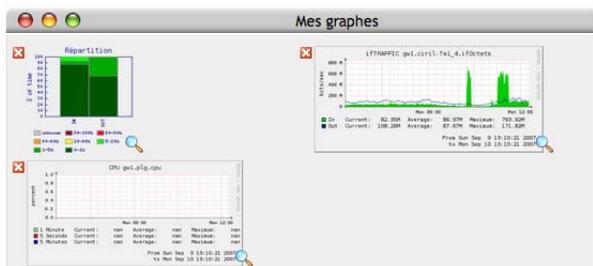


Figure 6: Page personnalisée

7.2.3 Graphiques à valeur ajoutée

Les données brutes ne sont pas toujours directement interprétables. Il est parfois nécessaire de les coupler à d'autres informations pour en tirer une information facilement exploitable. A titre d'exemple, dans le cadre des

réseaux distants (WAN) les liaisons restent très coûteuses et leur optimisation permet une répartition intelligente des ressources. Un graphique de débit ne permet pas de déterminer simplement si une liaison est saturée ou non. Il faut coupler l'information de débit à la valeur de la bande passante pour en déduire le taux d'occupation.

Des graphiques sont donc construits en temps réel par la plate-forme de supervision pour faciliter la compréhension des données collectées.

Reprenons notre exemple : un débit (habituellement exprimé en bit/s) est transformé en un pourcentage d'occupation de la bande passante, comme le montre la Figure 7.

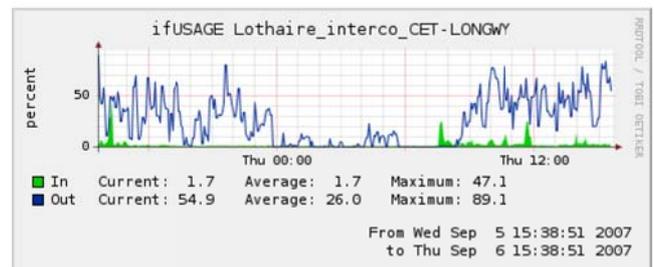


Figure 7: pourcentage d'utilisation de bande passante

Il est plus facile pour un néophyte de comprendre qu'une liaison est chargée à 80% et que cette charge augmente de 2 % tous les mois, plutôt que de parler sDSL et bits par seconde.

Dans le contexte des utilisations de ligne, il est surtout important de savoir si une ligne est saturée ou non pendant les heures ouvrées. Pour représenter cela, nous avons mis au point un graphique représentant le taux d'utilisation, comme le montre la Figure 8.

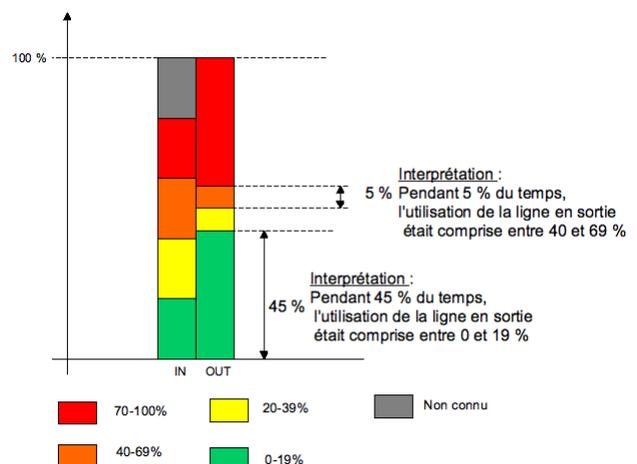


Figure 8: Graphique de répartition de charge

Sur ce graphique (histogramme empilé), chaque barre de couleur représente la part de temps pour un niveau d'utilisation donnée. De cette façon, une barre rouge (utilisation comprise entre 70 et 100%) de 50% pour un

graphique couvrant 24 heures sera interprétée de la façon suivante : « pendant 12 heures sur 24, la bande passante utilisée était comprise entre 70 et 100% ».

Ce type de graphique, cumulé sur plusieurs mois et ne tenant compte que des heures ouvrées, permet de rapidement identifier les liaisons saturées ou sous-utilisées.

Une demande prédominante de la part des institutions finançant les réseaux consiste à optimiser le budget disponible afin de rendre le meilleur service à chacun. Dans le cadre du projet eLorraine, le Conseil Régional redistribue la bande passante aux établissements les plus consommateurs, alors que les lignes les moins utilisées sont redescendues à des débits plus faibles.

7.2.4 Géolocalisation

La géolocalisation est presque devenue un phénomène de mode et présente - il faut en convenir - un attrait indéniable. La mise à disposition d'outils simples par *google* a permis de banaliser cette fonctionnalité et nous a fortement incité à ne pas nous en priver.

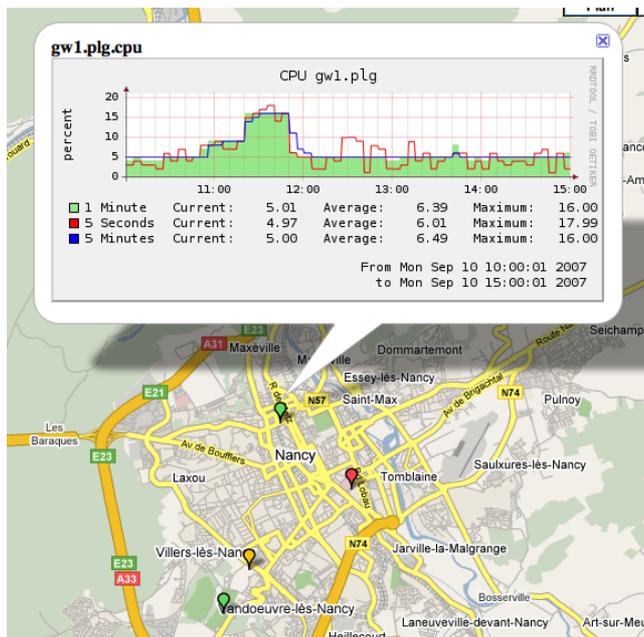


Figure 9: Géolocalisation

Il est donc possible pour chaque service de iSup de renseigner ses coordonnées GPS. Nous avons ainsi donné la possibilité aux administrateurs de construire des cartes sur lesquelles ils peuvent choisir les services à représenter. Comme illustré par la Figure 9, chaque service y est alors représenté par un point de couleur contenant des informations contextuelles directement accessibles.

8 Conclusion

L'objectif initial de ce projet est maintenant en grande partie atteint : nous disposons d'un outil central de supervision. Une simple action sur la base de données

permet la mise à jour de l'ensemble des configurations. iSup va permettre de remplacer les nombreuses applications devenues trop lourdes à maintenir. Nous disposons à ce jour d'un outil flexible, modulaire et robuste qui nous permettra de continuer à apporter de la valeur ajoutée aux rapports et analyses mis en œuvre.

Nous travaillons également à l'intégration de la supervision dans les outils d'administration que nous avons développés, afin de proposer à nos correspondants un ensemble homogène. Par exemple, il sera bientôt possible de choisir les interfaces à superviser depuis l'outil d'administration des commutateurs. De plus, la base de données des équipements étant maintenant réalisée, nous pouvons l'utiliser pour d'autres tâches de maintenance, comme la sauvegarde automatique des configurations.

