Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Le service des systèmes d'information de la Délégation Provence et Corse du CNRS

Arnaud DODERO

CNRS – Délégation Provence et Corse

Responsable entreprise : Franck LICHNOWSKI
Responsable académique : Anouch HOVSEPIAN

2018

Remerciements

Je tiens dans un premier temps à remercier l'équipe pédagogique, les responsables de la formation ainsi que ses intervenants, qui m'ont permis d'accroitre mes connaissances tout au long de ces deux années.

Je remercie également mon tuteur Monsieur Frank LICHNOWSKI pour m'avoir accepté au seins du CNRS en tant que stagiaire ainsi que pour l'aide, les conseils et le savoir-faire qu'il a su me transmettre concernant les différentes missions que j'ai pu faire. Il a su dès mon arrivée dans l'organisme m'intégrer rapidement, et me faire monter en compétence sur des sujets variés.

Je remercie également tous les membres du service Système d'information de l'organisme, M. Christophe JUILLARD, M. Michel KOURILSKY, Mme. Betty SOBRERO et M. Sébastien SORACE, et pour leur soutien et le savoir qu'ils ont pu m'apporter, facilitant ainsi mon intégration.

Table des matières

1 Introduction

Le stage en entreprise termine l'année de formation du DUT Réseaux et Télécommunications. Ce stage d'une durée de 10 semaines a pour objectif de nous faire acquérir une véritable première expérience professionnelle. Cela permet ainsi d'intégrer directement une entreprise à la fin de la formation si l'étudiant décide de ne pas poursuivre ses études.

J'ai choisi ce stage au CNRS car je trouve cet organisme fascinant, il dispose d'un large panel de métiers, que ce soit au niveau de la recherche ou dans l'accompagnement de la recherche. On y trouve beaucoup de personnes comme des chercheurs dans de nombreux domaines mais aussi des techniciens, des ingénieurs… Tous ces corps de métiers aux différents niveaux d'études se regroupent au sein d'un même campus.

C'est ainsi que j'ai décidé de rejoindre cet organisme pour finaliser mon diplôme et intégrer le service des systèmes d'information. Il a pour but de participer au développement, au maintien et à la sécurité du réseau de la délégation et du campus. Il permet aussi d'assurer une maintenance sur les éléments actifs et physique que ce soit les commutateurs, les câbles ou les routeurs. Le service est aussi très présent pour répondre aux problèmes que rencontrent les laboratoires et les autres services du campus.

C'est donc naturellement que j'ai trouvé que ce stage était fait pour moi, c'est exactement ce qui me plait dans ce métier. Mettre en place une architecture, la maintenir en fonctionnement et aider les employés.

2. Le CNRS

2.1 Présentation du CNRS

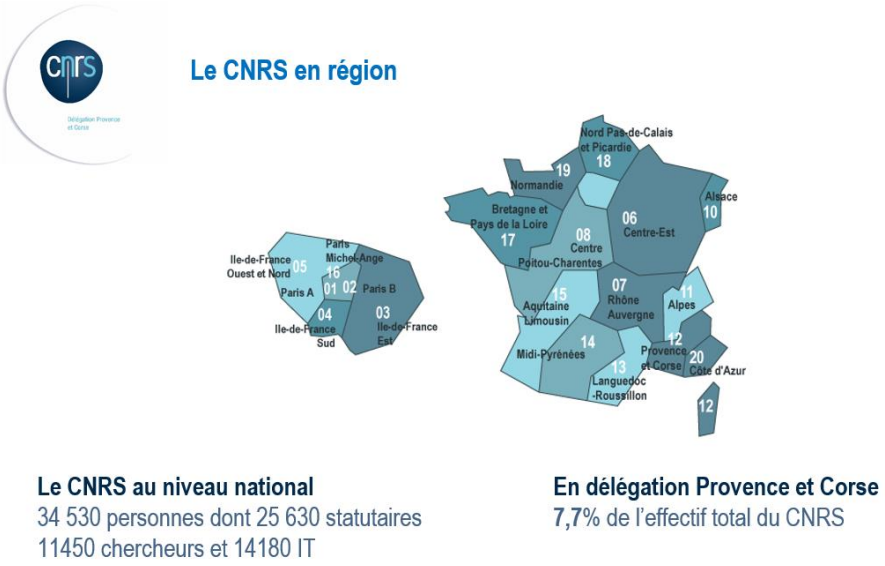
Le **CNRS**, **Centre national de la recherche scientifique**, est un organisme public de recherche fondamentale placé sous la tutelle du Ministère de l'Enseignement Supérieur et de la Recherche. Tous les domaines de la connaissance y sont représentés à travers 1 116 unités de recherche et de service labellisés dont la plupart sont gérées avec d'autres structures pour cinq ans sous la forme administrative d'« unités mixtes de recherche ».

CNRS en chiffres :

- 33 000 personnes au service de la recherche.
- 1 144 laboratoires de recherche en France et à l'étranger.
- 3,3 milliards d'euros de budget.
- 23 % de ressources propres

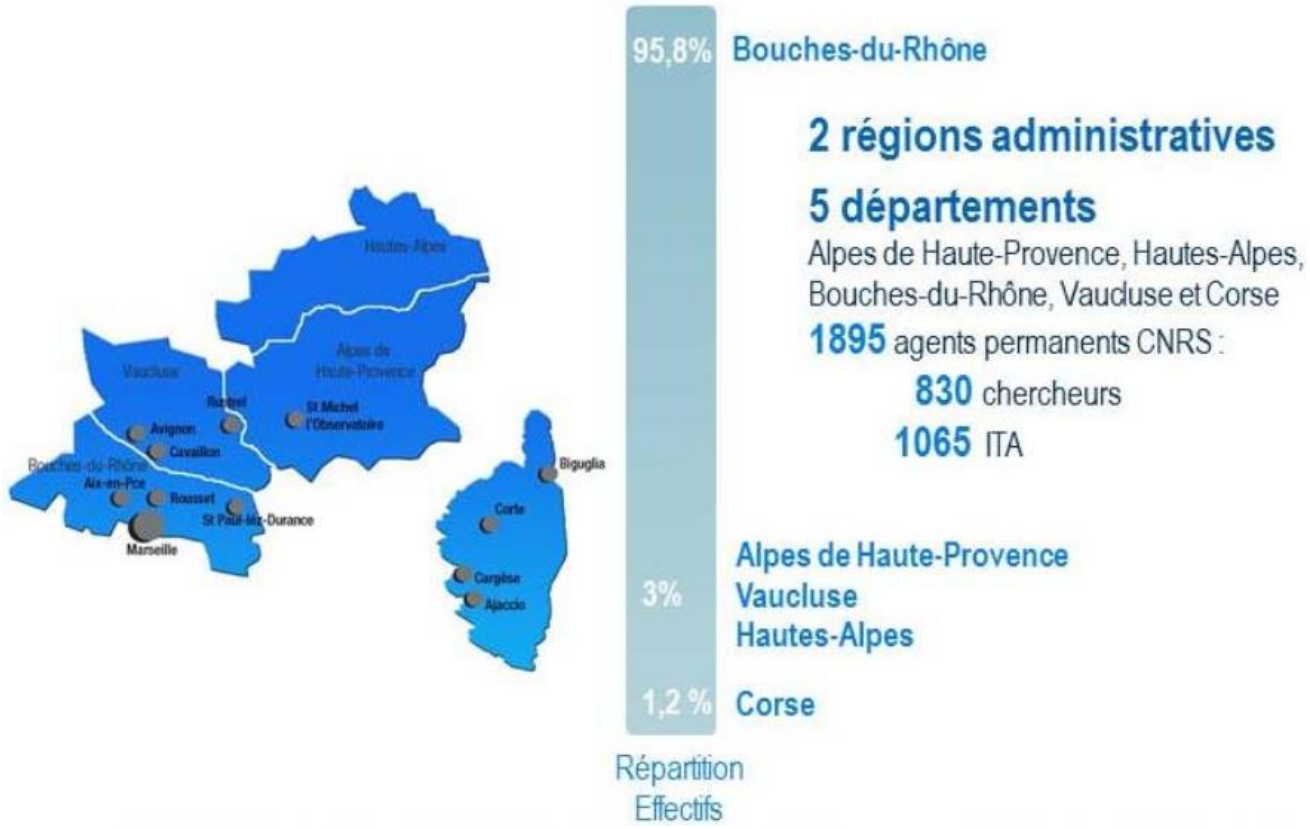
2.2 Découpage administratif

Le CNRS est décomposé au niveau national en 18 délégations régionales permettant d'assurer des missions de représentation au sein des diverses instances locales impliquées dans la recherche et l'enseignement supérieur, de gestion de proximité des laboratoires et du personnel et d'accompagnement des projets scientifiques locaux.



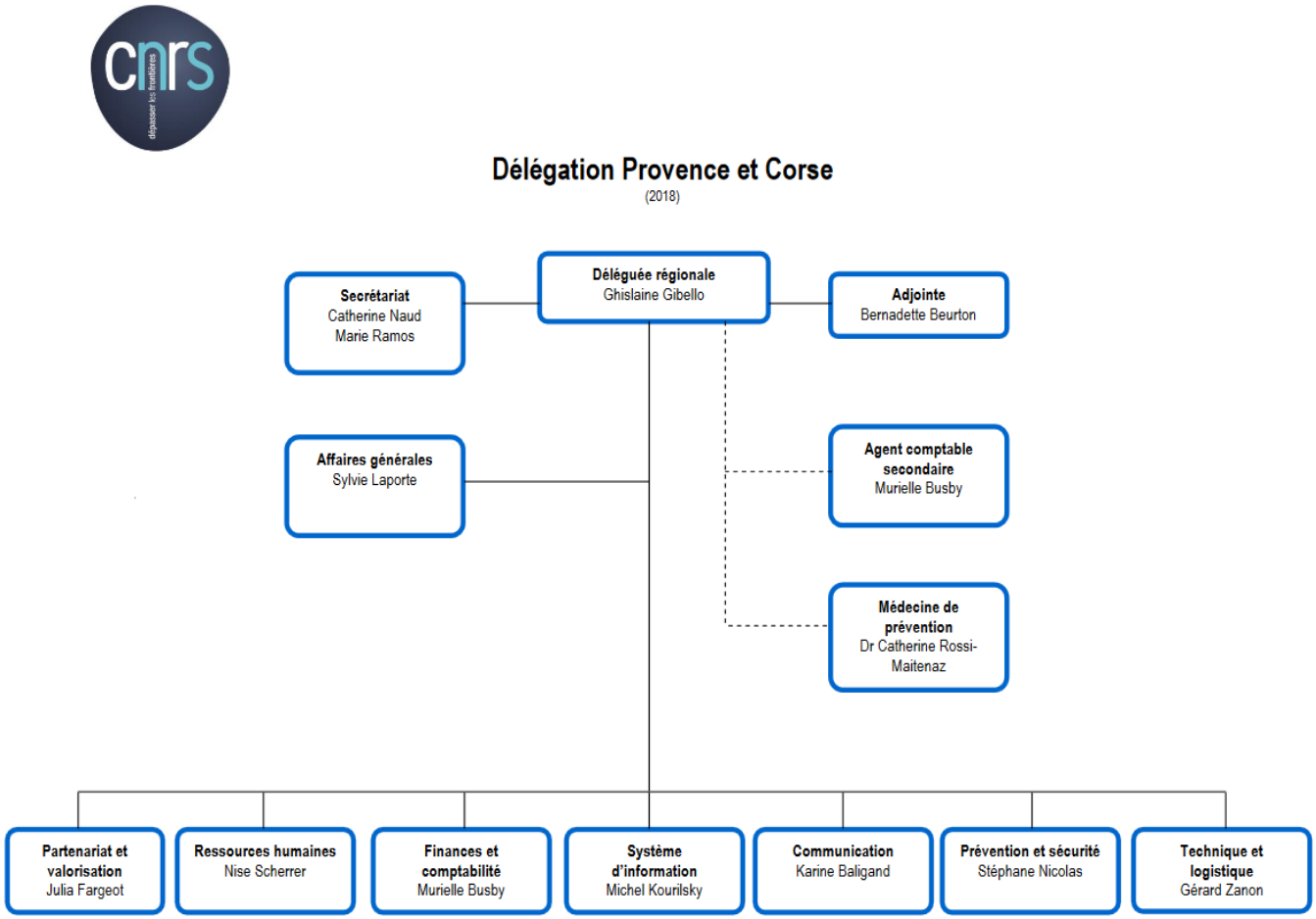
J'étais au sein de la délégation Provence et Corse qui est la 12^{éme} délégation Régionale et l'unité dans laquelle j'étais est localisée dans le centre du CNRS, 31 chemin Joseph Aiguier, dans le 9^{éme} arrondissement de Marseille.

2.3 La Délégation Provence et Corse et le campus Joseph Aiguier



Le campus Joseph Aiguier est un campus de 6 hectares regroupant des laboratoires et la délégation régionale du CNRS, pour un total de 25 bâtiments (plus de 40 sous-répartiteurs réseau) et compte environ 900 personnels, chercheurs, ingénieurs et techniciens.
Ce campus fait partie des campus propres du CNRS, c'est à dire qu'il appartient et est géré entièrement par le CNRS.
Le campus Joseph Aiguier offre à ses laboratoires et utilisateurs un réseau informatique performant, sécurisé et hautement disponible administré par des ingénieurs du CNRS, aussi bien en service de proximité (laboratoires) que pour les services campus mutualisés.

Voici l'organigramme de cette unité :



2.4 Présentation du Service des systèmes d'information : SSI

Le service dans lequel j'opérais au CNRS était le Service des Systèmes d'Information et les principales missions du service sont le déploiement régional des applications nationales mises en place par le CNRS (BFC, SIRHUS, RESEDA, INFOCENTRE...), la coordination régionale de sécurité des systèmes d'information, le conseil et l'assistance technique auprès des laboratoires et des services de la délégation, l'administration et la fourniture du service réseau pour les unités du campus Joseph Aiguier et l'administration des systèmes et du réseau de la délégation régionale.
La direction des systèmes d'information définit et met en œuvre les systèmes d'information destinés au pilotage et à la gestion des différentes activités de l'établissement.

Correspondant en laboratoire : le chargé de la sécurité des systèmes d'Information. Spécialiste des systèmes d'information, dont la mission est d'assister le directeur d'unité dans l'exercice de sa responsabilité en matière de sécurité des systèmes d'information. Il est nommé par le directeur d'unité.

2 Présentation du cadre technique général du sujet

2.1 Les Objectifs

- Acquérir une expérience professionnelle qui sera utile pour mon parcours futur.
- Découvrir et apprendre dans le monde du travail, collaborer avec d'autres personnes du métier et la vie en entreprise.
- Faire gagner du temps à l'entreprise avec le travail que j'aurai fourni.

2.2 Savoir-être

Le savoir-être à avoir afin de remplir les taches de ce stage sont :

- **L'autonomie :** Lorsque l'on est en entreprise on ne peut pas se permettre de déranger sans cesse ses collègues, car eux aussi travaillent et on ne peut pas les déranger systématiquement. Il faut être autonome et bien souvent apprendre à chercher sur internet ou dans les documentations quand on n'arrive pas à résoudre son problème.

- **Motivé :** On se doit d'être motivé car sinon les heures de travail risquent de passer bien lentement. De plus il ne faut pas abandonner, des fois cela peut se trouver compliqué de rester sur un travail de plusieurs heures sans arriver à corriger le problème. Et dès lors qu'on commence à travailler on fait beaucoup d'erreur et il faut savoir ne pas lâcher et continuer afin de rendre un travail correct.

- **Organisé :** Durant le stage j'ai eu plusieurs tâches à remplir, l'organisation et très importante pour savoir là où l'on va, par où commencer et définir des ordres de priorités.

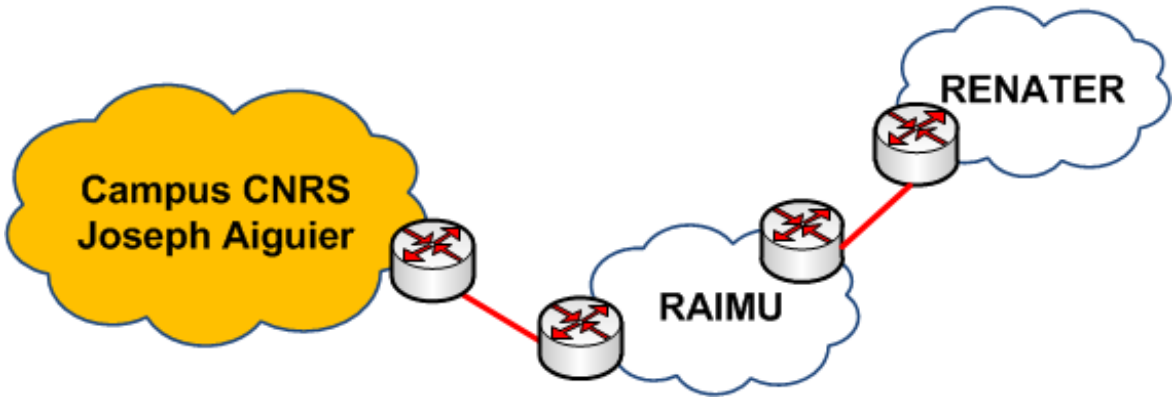
2.3 Savoir-faire

- Connaitre parfaitement les réseaux et les protocoles de routage et de sécurité (Configuration commutateurs et routeurs)
- Connaissances sur la virtualisation et les systèmes d'exploitation
- Savoir mettre en place des serveurs
- Utiliser les outils de supervision

2.4 Présentation du réseau du campus

Durant mon stage, j'ai dû accomplir différentes missions, la principale étant d'aider au renouvellement du cœur de réseau du CNRS. Or cette mission n'a pas pu avoir lieu dans les temps durant ma présence, car les caractéristiques de l'appel d'offre n'ont pas été correctement remplies par les entreprises candidates. J'ai donc eu en remplacement plusieurs autres missions qui m'ont été données.

Après une présentation des infrastructures et du schéma général du réseau, j'ai pu m'apercevoir que le CNRS disposait d'un impressionnant dispositif. Le réseau du CNRS est raccordé au réseau de collecte RAIMU (Réseau Aix Marseille Université). C'est un réseau de collecte régional dédié à l'enseignement supérieur et à la recherche. Il y a plus de 60 sites ESR (Enseignement Supérieur et la Recherche) raccordés. RAIMU est ensuite raccordé à Renater qui est le réseau national dédié à l'ESR.



Le campus offre une infrastructure permettant d'héberger et offrir divers services aux laboratoires du campus et plus généralement de la circonscription :

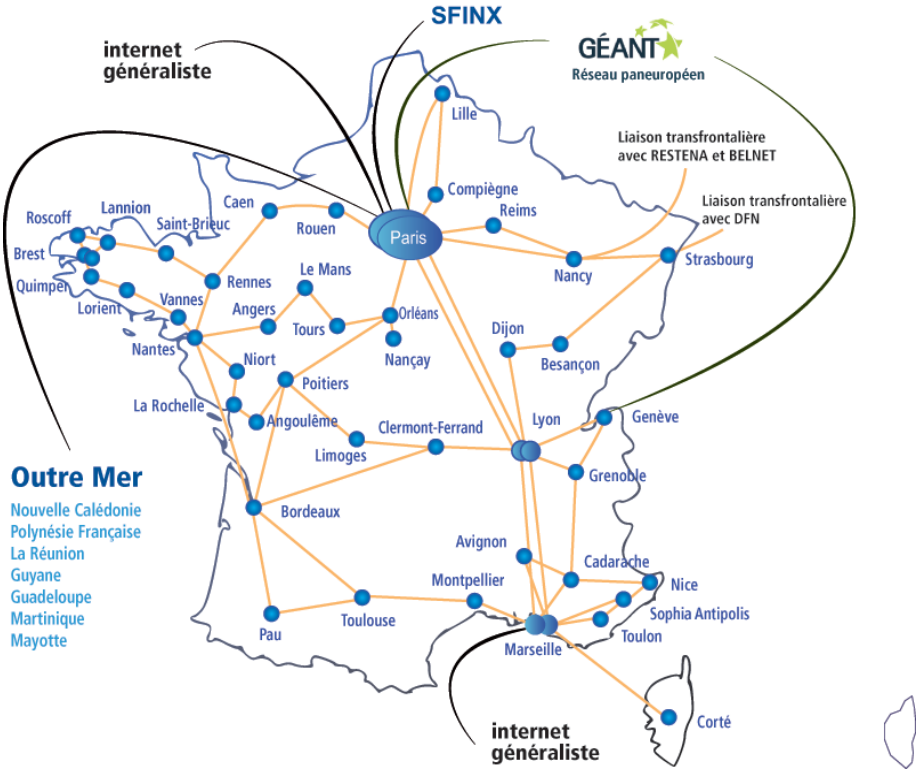
- gestionnaire de listes de messagerie multi-domaines,
- messagerie multi-domaines,
- nom de domaines (sous domaine cnrs-mrs.fr) et hébergement de domaines externes,
- hébergement de sites web,
- outils de mesure de statistiques web mutualisé,
- accès VPN mutualisé (laboratoires du campus),
- accès sans-fil (Wifi) pour les utilisateurs du campus et les visiteurs (80 bornes),
- cœur de réseau haute performance multi-gigabits,
- outils de métrologie et de supervision du réseau,
- serveur de temps de strate 2 (ntp).

Tous ces services sont hébergés sur le campus Joseph Aiguier.
L'accès à internet est donné via le Groupement d'Intérêt Public Renater.

Le logo de Renater

Il s'agit d'un réseau liant plus de 1000 sites via une liaison très haut débit (liaisons jusqu'à 10 Gbit/s, cœur de réseau à 80 Gbit/s en Île-de-France) et en IPv4 et IPv6 natifs.

RENATER est connecté au réseau pan-européen GÉANT2 (via une liaison à 10 Gbit/s). Il est également relié à Internet, en France via SFINX (à 2x10 Gbit/s), et dans le monde via 2 liaisons IP Transit à 10 Gbit/s de Paris et de Lyon.



Le réseau Renater

3 Missions et Travaux réalisés

3.1 La mise en place de mon bureau et présentation d'Active Directory

Lors de mon arrivée nous avons dû configurer un nouveau poste de travail, j'ai donc eu un bureau attitré avec un ordinateur. Christophe, qui est responsable du parc informatique, m'a montré comment le matériel était mis en place. Il a donc déclaré un nouveau PC dans l'Active Directory. Il m'a réservé une adresse IP et l'a associé avec l'adresse MAC du PC mis à ma disposition.

L'installation de Windows s'effectue lors du démarrage de l'ordinateur. En effet, le réseau reconnait la machine et se connecte sur un serveur où sont stockées les images Windows à déployer. Environ tous les 6 mois ces images sont mises à jour pour ne pas avoir à effectuer, lors de l'installation d'une nouvelle machine, toutes les mises à jour Windows jusqu'à aujourd'hui.

Il m'a ensuite montré comment étaient déployés les logiciels à distance sur les machines grâce à WAPT (solution de déploiement logiciel Open Source). Depuis son poste, il a créé plusieurs groupes de logiciels notamment un groupe base qui regroupe tous les logiciels de base à installer sur une machine comme le pack Microsoft Office, un lecteur PDF, JAVA, Adobe Flash… lors du déploiement d'une nouvelle machine. Il peut donc à distance, contrôler l'installation des logiciels sur les machines et avoir la main sur les versions des logiciels installés sur toutes les machines du campus. Ce qui permet par exemple de ne pas installer une version qui dispose de bug pour un logiciel en particulier et assurer les mises à jour de tous les logiciels.

3.2 Aide à la mise en place de la GTC

Dans un premier temps j'ai dû configurer 3 commutateurs de marque Dell dans le cadre de modifications du système de badge d'accès et de la Gestion technique Centralisée qui permet d'anticiper et d'éviter tous types de pannes en alertant les personnels d'astreinte en cas de dysfonctionnements. Ces dispositifs seront exploités par le STL (Service technique et logistique) du CNRS.

Les commutateur mis en places sont des Dell de la série N1124P-ON

La configuration se fait de la même façon que les commutateurs Cisco et les commandes se ressemblent fortement. Je n'ai donc eu pas trop de difficultés à les configurer. Le but étant de configurer les VLAN* utiles au réseau et de faire de l'etherchannel* sur les liens SFP*

Sur les deux premiers ports SFP la fibre arrivera, ils seront configurés en Etherchannel (LACP) afin de regrouper les deux ports physiques en une seule logique, ce qui permet d'assurer une redondance en cas de fibre coupée et d'augmenter le débit.
Les autres ports sont configurés dans un VLAN et pour associer le PC au bon VLAN on utilise l'adresse MAC (authentification via un serveur Radius en « mac-based »). J'ai donc configuré le commutateur en conséquence. La configuration se trouve dans l'annexe.

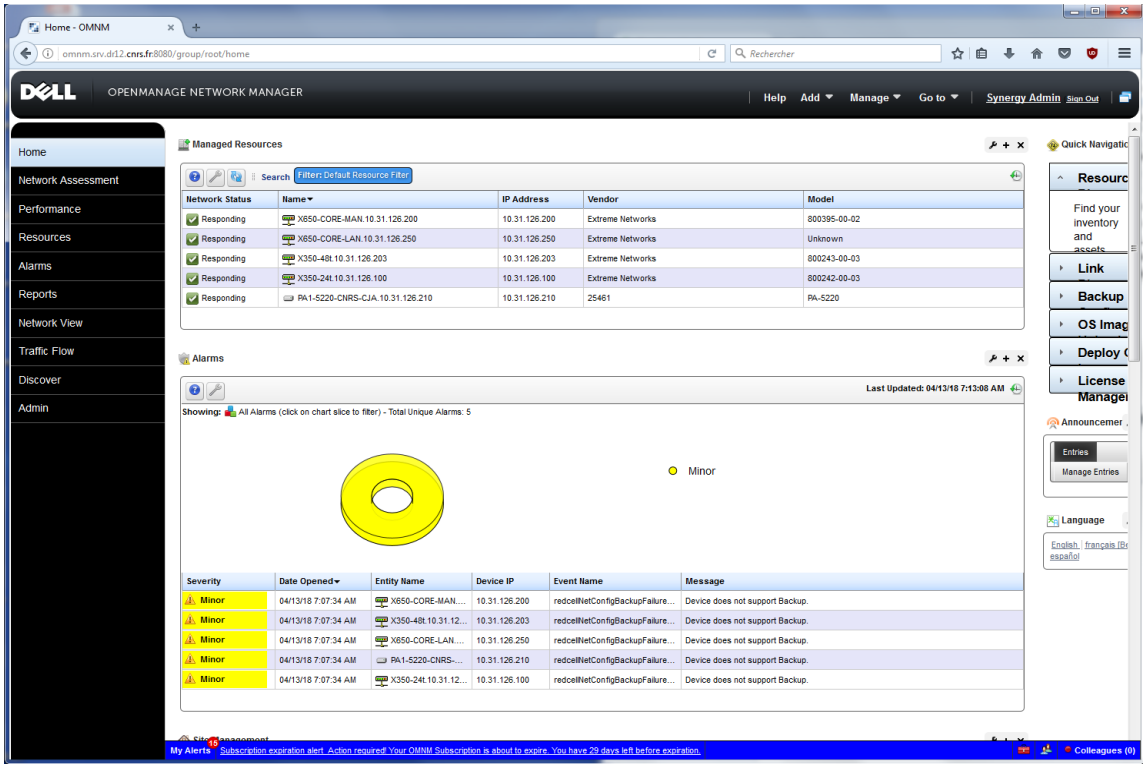
Une fois ceci fait, j'ai dû flasher la ROM, ce qui veut dire que j'ai mis à jour le système interne du commutateur. Pour cela j'ai mis le système préalablement téléchargé depuis le site du constructeur sur une clé USB grâce aux commandes suivantes et j'ai déployé la nouvelle version du système sur le commutateur :

```
en
conf
copy usb://[nom du fichier] backup
reload
```

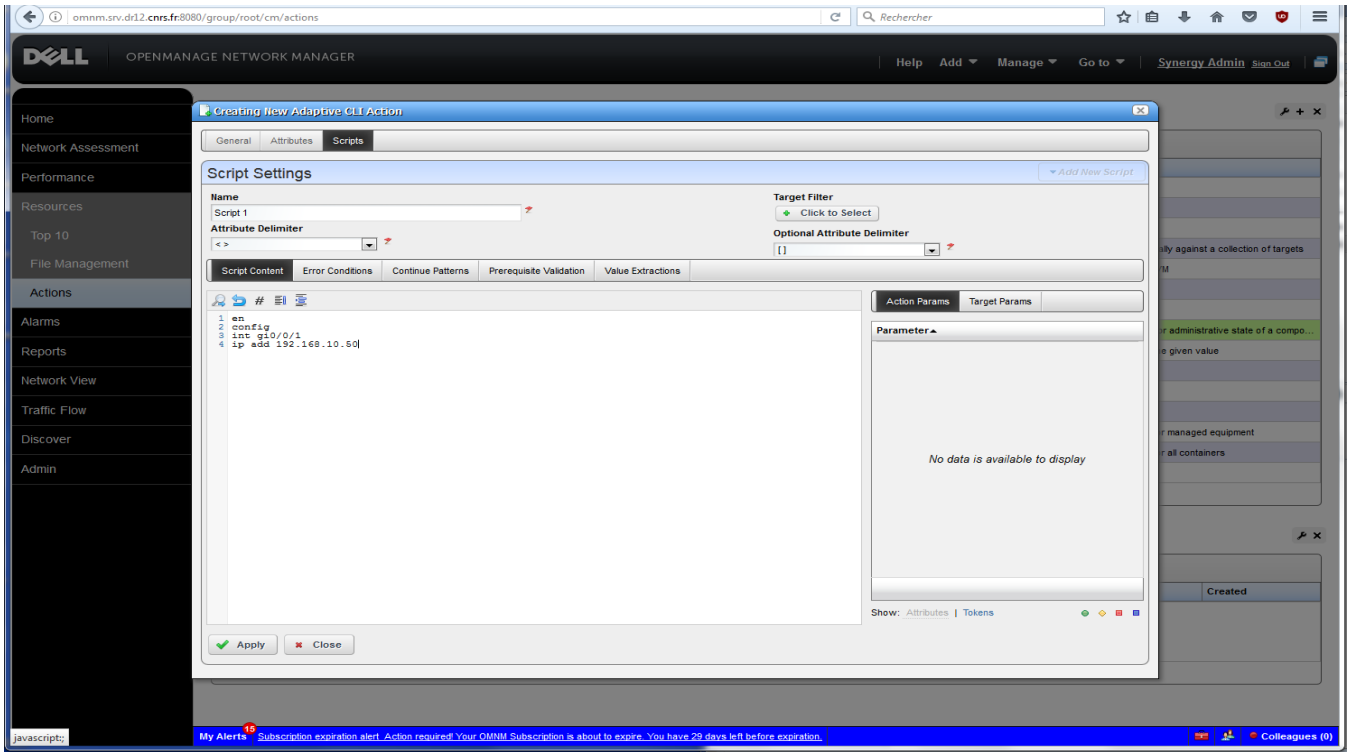
3.3 Test du logiciel de supervision avancé Dell OpenManage Network Manager (OMNM)

Afin de réfléchir à de nouveaux systèmes de supervision, mon tuteur m'a demandé de tester le logiciel proposé par Dell pour une supervision plus avancée nommé Dell OpenManage Network Manager.

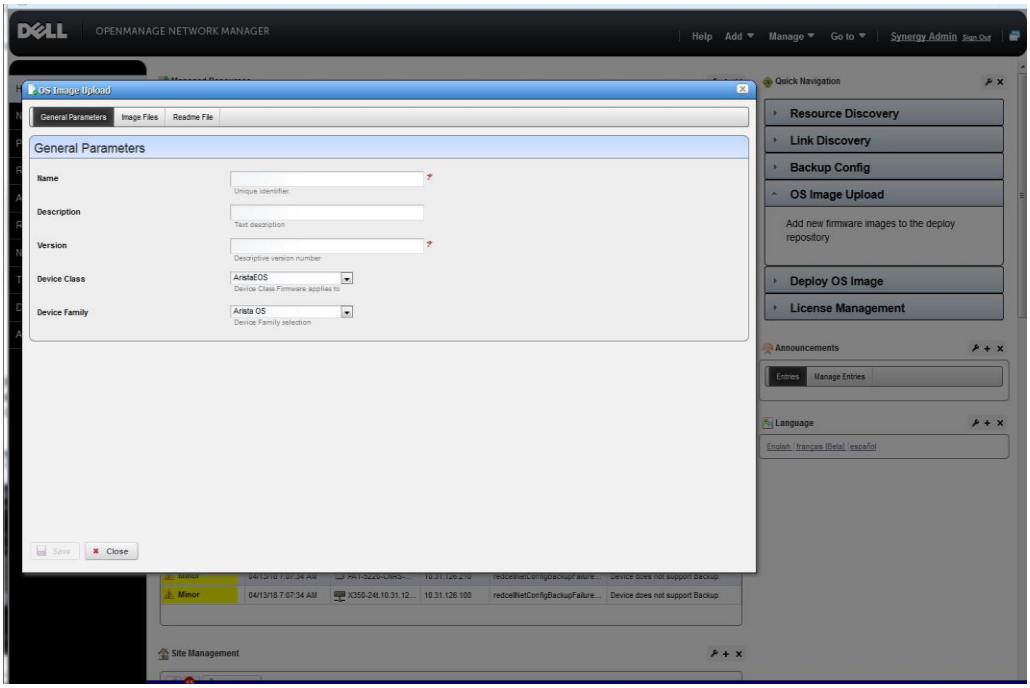
Nous avons mis en place ce système sur un serveur virtualisé (infrastructure VmWare).
Ce logiciel permet de faire de la supervision de tous les constructeurs comme on peut le faire avec des outils libres comme NAGIOS, Centreon, Icinga… Cela nous permet notamment de voir les dysfonctionnements et surcharges anormales sur les différents matériels du réseau. Lors d'un problème une alerte apparaît alors sur l'interface et on est informé de la panne. De plus on peut vérifier autant de services que l'on veut grâce au protocole SNMP.



Mais ce qui fait la différence par rapport aux autres logiciels, c'est qu'il peut aussi faire de la maintenance des appareils à distance. On peut par exemple reconfigurer un ou plusieurs commutateurs à distance. On peut aussi créer des scripts que l'on peut ensuite intégrer à des politiques de réseau afin d'automatiser la gestion. Les règles permettent de pouvoir appliquer des actions à des groupes de commutateurs qu'on aura regroupés au préalable. On peut par exemples créer des règles selon les marques avec des commandes différentes ou selon le lieu de ceux-ci. Après avoir créé tout cela, en quelques clics, on facilite le (re)paramétrage et l'exploitation d'un réseau.

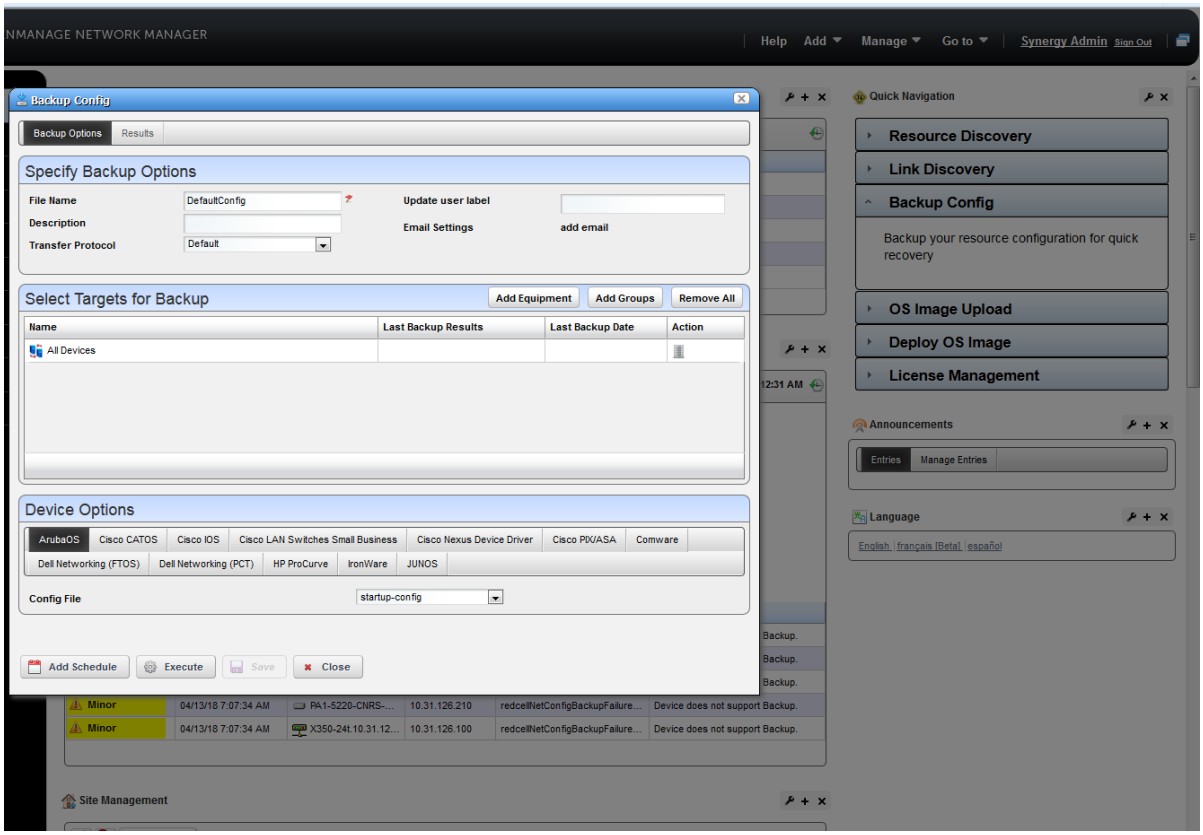


Exemple de conception d'une config à appliquer sur un groupe de commutateur

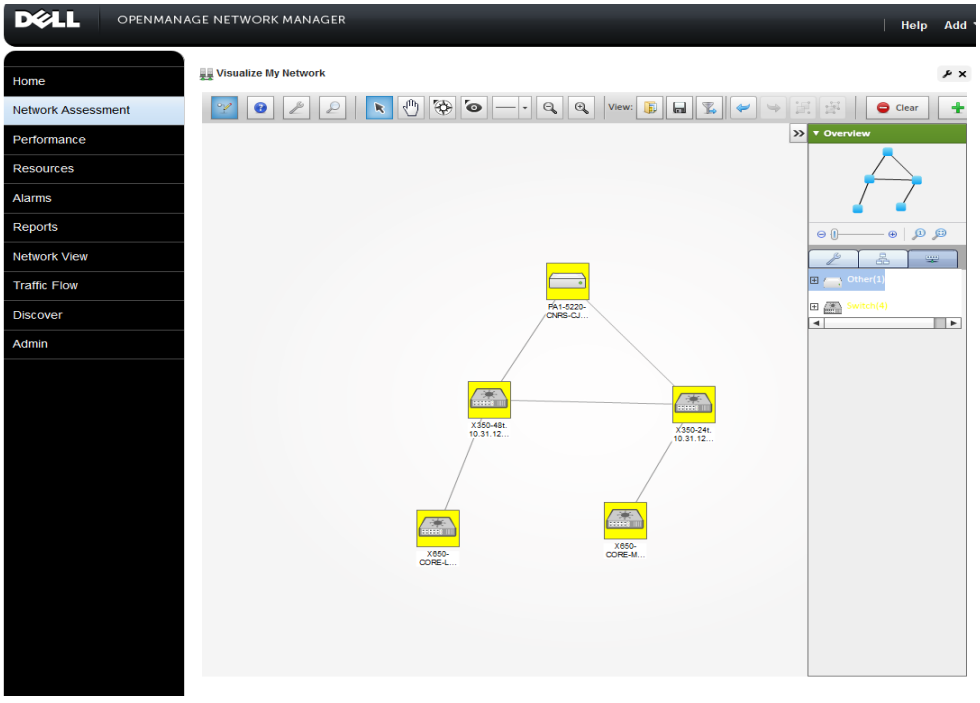


Avec OMNM on a notamment la possibilité de déployer les micro logiciels (Firmware), de façon à mettre à jour de façon distante les commutateur/routeurs. Il suffit alors de se rendre dans l'onglet de droite : Os Image et de sélectionner le groupe de routeur/commutateur pour lequel on veut faire la mise à jour (Cf. Capture d'écran de gauche).

On peut aussi bien évidemment faire des backups de la configuration et du firmware actuel, pour revenir en arrière si besoin. Onglet Backup Config > On sélectionne le groupe et le protocole.



On peut notamment dessiner un plan du réseau avec l'état actuel des éléments actifs et des liens.



De plus, on a la possibilité, d'accéder à des serveurs, d'enregistrer des configurations directement depuis le serveur de supervision.

Principaux avantages

- **Automatise la détection** des appareils et des adresses réseau IPv4 et IPv6, et fournit des informations détaillées sur leur connectivité, notamment leur capacité à produire des cartes topologiques physiques et logiques.
- **Permet de configurer et de gérer facilement** des groupes d'appareils réseau : les modifications de configuration et les déploiements de micrologiciels peuvent être effectués sur plusieurs appareils en une seule opération. De plus, de nombreuses opérations réseau peuvent être planifiées pour une exécution à des heures prédéterminées.
- L'**administrateur réseau** peut surveiller l'état et les performances du réseau, créer des tableaux de bord pour capturer des tendances et des événements importants, et en afficher la chronologie.
- Permet de **réduire le coût total de possession** en surveillant de façon proactive les problèmes du réseau, en automatisant les tâches de configuration courantes et en assurant un déploiement facile des micrologiciels.
- **Payez en fonction de vos besoins** en achetant uniquement les licences nécessaires aujourd'hui et en acquérant de nouvelles licences à mesure que votre entreprise évolue.
- **Bénéficiez d'une prise en charge fiable** avec l'envoi automatique de rapports et d'alertes lorsque le support ou la garantie du matériel arrive à expiration.
- **Rationalisez la résolution des problèmes** avec l'automatisation fournie par Dell SupportAssist. Assurez-vous que vos commutateurs Dell Networking communiquent avec le support Dell afin de réduire les étapes de dépannage et d'accélérer le temps de résolution.
- **Consultez l'état du datacenter** à l'aide de l'intégration avec Dell OpenManage Essentials qui centralise les informations relatives aux serveurs et au réseau.

Principales fonctionnalités

- Prise en charge multiplateforme avec l'installation de l'appliance virtuelle pour Windows, Linux et VMware
- Gestion multifournisseur pour les appareils Dell, mais également pour ceux des principaux fournisseurs comme Cisco, Juniper, HP, Arista, Extreme et Brocade
- Audit de conformité et correction qui identifient et corrigent les problèmes de configuration afin d'assurer la conformité
- Capacités flexibles et complètes de création de rapports pour l'inventaire, les micrologiciels, les interfaces, les ports, etc.
- Rapports d'analyse du flux du trafic qui permettent l'exportation de données sFlow au format .csv
- Mutualisation avec prise en charge de plusieurs organisations client à partir d'une instance unique
- Gestion de la configuration des appareils de type un à plusieurs et modèles pour la sauvegarde, la restauration et le déploiement des commutateurs
- Programmation avancée permettant de planifier des tâches importantes, comme les sauvegardes et les changements de configuration

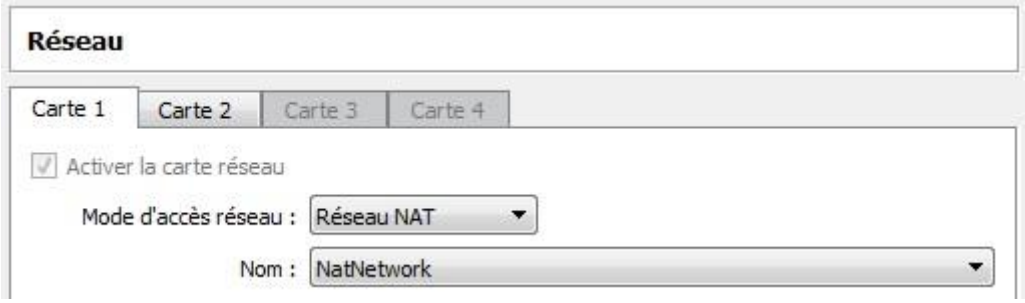
On peut donc dire que cet outil se révèle plus complet qu'un outil de supervision basique, avec notamment les fonctions supplémentaires que l'on a détaillées. Il est aussi plus facile à utiliser et à mettre en place dans la mesure où tout est inclus directement dans le logiciel. Mais cet outil n'est pas libre et n'aura peut-être jamais l'évolutivité que peut avoir un outil open-source. De plus, il faut une licence pour pouvoir l'utiliser mais cela permet de ne pas se soucier des mises à jour de sécurité et d'un support qui se fait directement par Dell. Cela peut se révéler utile pour gagner du temps et en facilité.

3.4 Test de graphite avec Centreon sur VM*

Mon tuteur de stage réfléchissait à mettre en place Graphite*, un logiciel pour extraire les données récoltées dans les logiciels de supervision comme Centreon*, l'outil permettant de superviser* le réseau CNRS. Cela permettrait de faire des graphes sur beaucoup de données comme la charge CPU, des pourcentages sur les ports ouverts, sur les pannes réseau, l'utilisation... L'idée est de mettre en place un Dashboard de supervision de réseau ou on pourra voir, en un coup d'œil, l'état en direct du réseau CNRS.
Pour mettre en place tous mes tests j'ai utilisé la virtualisation. Pour pouvoir se faire un avis sur la mise en place en réel et tester la solution.
J'ai donc installé une VM* sous Ubuntu et installé Centreon dessus. Dans une autre, j'ai installé Debian* avec graphite. La première difficulté était de pouvoir avoir accès à internet sur les VM et qu'elles puissent communiquer entre elles.

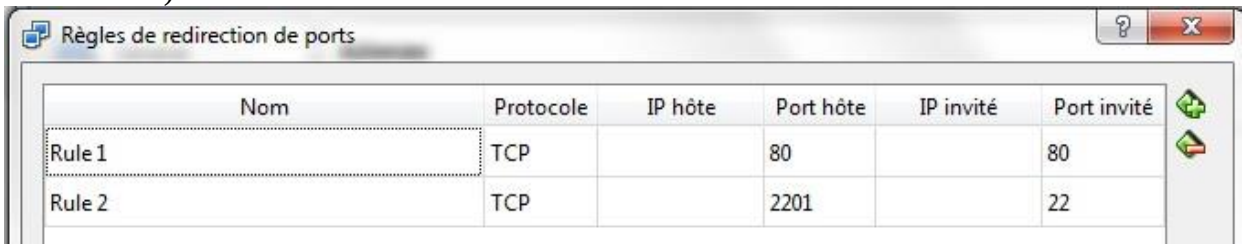
3.4.1 Configuration réseau des VM et Installation d'Ubuntu

Après avoir fait de nombreuses recherches et de tests sur les différents modes réseau pour configurer proprement les paramètres pour l'accès à internet et la communication entre les machines virtuelles j'ai trouvé les modes à appliquer :
Le premier réseau est celui des VM (Network Nat en 10.0.2.0/24), le second est celui pour communiquer avec Internet et les machines hôtes (Nat en 10.0.3.0/24).
Voici donc la configuration dans VirtualBox pour la première carte des deux VM :

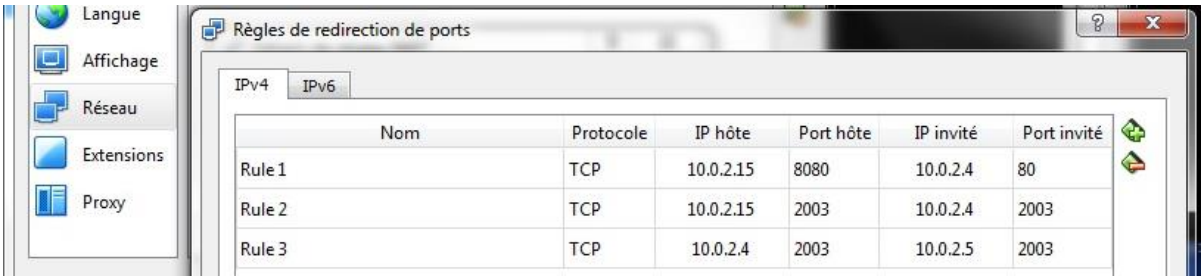


On met la seconde carte en NAT :

Il ne faut pas oublier de faire la redirection de certains ports, pour avoir accès depuis la machine hôte au serveur web (port 80 à rediriger) et pouvoir faire du SSH sur la VM (port 22 à rediriger). (Sur carte 2 NAT)

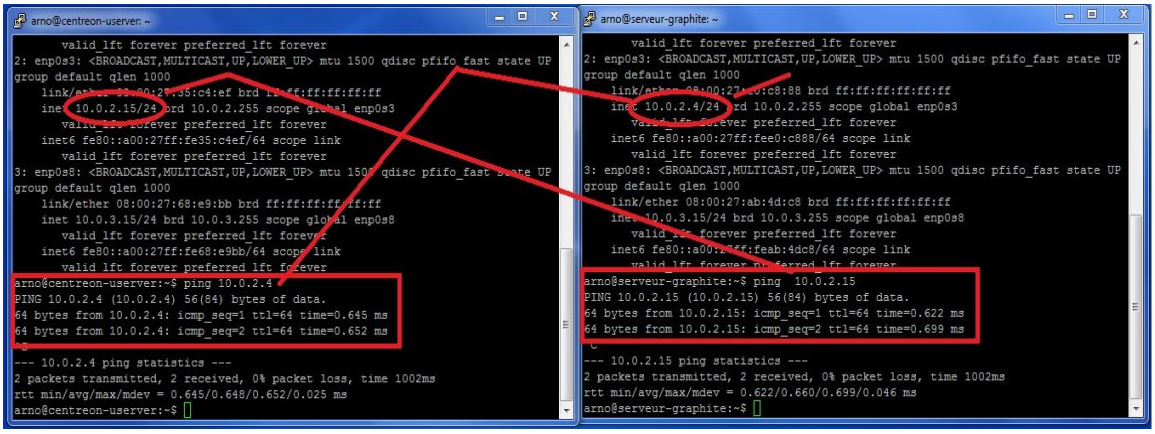


Et sur le réseau interne de la machine virtuelle, il faut rediriger ces ports-là, pour que les machines puissent se transmettre les données Centreon > Graphite.



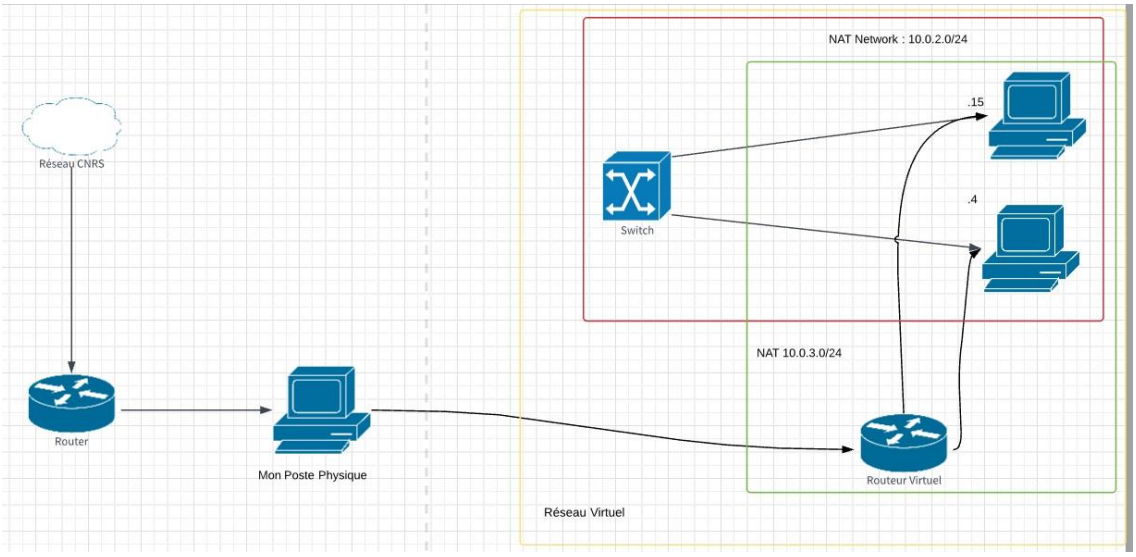
Nom	Protocole	IP hôte	Port hôte	IP invité	Port invité
Rule 1	TCP	10.0.2.15	8080	10.0.2.4	80
Rule 2	TCP	10.0.2.15	2003	10.0.2.4	2003
Rule 3	TCP	10.0.2.4	2003	10.0.2.5	2003

Après avoir installé Ubuntu serveur et après avoir effectué la configuration du réseau, il faut la tester, j'ai alors effectué un ping pour voir si les machines communiquaient entre elles.



Résultat : ça marche !

Voici un schéma du réseau :



3.4.2 Mise en place de Centreon

Centreon est une application libre (open source), Elle est basée sur Nagios (c'est ce qu'on appelle un fork). Depuis 2012, Centreon a développé son propre moteur de collecte et gestionnaire d'événements. Il est plus simple à installer et à configurer que Nagios et il offre une interface graphique Web avancée et claire. Ces principales fonctionnalités :
– Mêmes fonctionnalités que Nagios : Superviser des services réseaux (SMTP, HTTP, ICMP, SNMP…), Superviser les ressources serveurs (charge CPU, Occupation disques durs…), interface avec le protocole SNMP, remonter des alertes…
– Configuration en ligne via une API.
– Gestion des dépendances entre les services
– Visualisation des graphes et des données avancées
Plusieurs choix s'offrent à nous pour l'installation de Centreon : utiliser une image toute faite en .iso, une image virtuelle qui suffit d'importer dans Virtual Box ou alors de compiler sur un système linux de la distribution de son choix.

J'ai utilisé cette dernière solution pour l'installer sur mes machines Ubuntu. L'intérêt de cette solution est de savoir exactement les versions des dépendances que l'on a déployées et de se mettre à l'abri d'une éventuelle mise à jour qui « casserait » le fonctionnement du serveur.
Dans un premier temps, il faut installer les prérequis et récupérer les fichiers source sur le site depuis la VM. Pour cela j'ai utilisé la commande wget.

Toute la procédure de téléchargement, compilation et installation de centreon est expliquée dans l'annexe.

Après avoir configuré le logiciel, j'ai supervisé les commutateurs que j'ai installé. Pour surveiller notamment la charge CPU et l'état des commutateurs (UP ou DOWN).

Voici comment ça se présente :

Hosts	Services	Status	Duration	Last Check	Tries	Status information
Centreon-Server	Load	OK	2h 48m	2m 17s	1/3 (H)	Load average: , , .
	Ping	OK	2h 51m	4m 47s	1/3 (H)	OK - 127.0.0.1: rta 0,042ms, lost 0%
DELL_N1124P_AQ_STL	cpu-dell	OK	2h 51m	24s	1/3 (H)	OK: CPU Usage: 5.48% (5sec), 6.49% (1min), 6.69% (5min)
	Ping-Dell	OK	2h 36m	1m 54s	1/3 (H)	OK - 10.31.126.189: rta 2,262ms, lost 0%
DELL_N1124P_F_STL	cpu-dell	OK	2h 52m	1m 2s	1/3 (H)	OK: CPU Usage: 4.89% (5sec), 5.48% (1min), 5.76% (5min)
	Ping-Dell	OK	2h 49m	3m 32s	1/3 (H)	OK - 10.31.126.188: rta 2,104ms, lost 0%
DELL_N1124P_GA_STL	cpu-dell	UNKNOWN	2h 52m	1m 39s	3/3 (H)	UNKNOWN: SNMP GET Request : Timeout
	Ping-Dell	CRITICAL	2h 50m	4m 9s	3/3 (H)	CRITICAL - 10.31.126.187: rta nan, lost 100%

Hosts	Status	Services information
Centreon-Server	UP	Load Ping
DELL_N1124P_AQ_STL	UP	Ping-Dell cpu-dell
DELL_N1124P_F_STL	UP	Ping-Dell cpu-dell
DELL_N1124P_GA_STL	DOWN	Ping-Dell cpu-dell

Service int-dell2	DELL_N1124P_AQ_STL | 10.31.126.189
DELL_N1124P_AQ_STL	
Status Details	
Service Status	OK
Status information	SNMP OK - 1
Extended status information	
Performance Data	iso.3.6.1.2.1.2.2.1.8.2=1
Current Attempt	1 / 3
State Type	HARD
Last Check Type	Active
Last Check	2018/04/23 - 16:23:53
Next Scheduled Active Check	2018/04/23 - 16:28:53
Latency	0.087 seconds
Check Duration	0.197338 seconds
Last State Change	2018/04/23 - 15:21:34
Current State Duration	1h 5m
Last Service Notification	
Current Notification Number	0
Is This Service Flapping?	N/A
Percent State Change	9.210526 %
In Scheduled Downtime?	No
Last Update	2018/04/23 - 16:27:32
Executed Check Command Line	/usr/lib/nagios/plugins/check_snmp -H 10.31.126.189 -o .1.3.6.1.2.1.2.2.1.8.2 -C dr-pub -P 2c -r 1
Detailed Graph	

Pour aller plus loin, j'ai aussi voulu récupérer l'état d'une interface. Normalement on utilise les plugins Centreon qui ont déjà des commandes configurées pour chaque modèle. Or pour celui-ci, la série DELL N1100, peu répandue, il a été impossible de la trouver. J'ai donc utilisé la commande check_snmp inclus dans Centreon et j'ai rajouté l'option « –r 1 » qui permet de renvoyer un OK lorsque la commande renvoie la valeur 1 et un CRITICAL lorsque la commande renvoie la valeur 2.

Voici le résultat de tous les services configurés :

Hosts	Services	Status	Duration	Last Check	Tries	Status information
Centreon-Server	Load	OK	1M 1w	4m 13s	1/3 (H)	Load average: , , .
	Ping	OK	1M 1w	24s	1/3 (H)	OK - 127.0.0.1: rta 0,045ms, lost 0%
DELL_N1124P_AQ_STL	cpu-dell	OK	1M 1w	2m 10s	1/3 (H)	OK: CPU Usage: 7.47% (5sec), 6.27% (1min), 6.45% (5min)
	int-dell	OK	1M 1w	3m 20s	1/3 (H)	SNMP OK - 1
	int-dell2	OK	1M 1w	4m 31s	1/3 (H)	SNMP OK - 1
	int-dell3	CRITICAL	1M 1w	42s	3/3 (H)	SNMP CRITICAL - *2*
	Ping-Dell	OK	1M 6d	52s	1/3 (H)	OK - 10.31.126.189: rta 1,825ms, lost 0%
DELL_N1124P_F_STL	cpu-dell	OK	1M 1w	2m 27s	1/3 (H)	OK: CPU Usage: 9.78% (5sec), 9.70% (1min), 10.12% (5min)
	int-dell	OK	1M 1w	3m 32s	1/3 (H)	SNMP OK - 1
	int-dell2	OK	1M 1w	4m 42s	1/3 (H)	SNMP OK - 1
	int-dell3	CRITICAL	1M 1w	52s	3/3 (H)	SNMP CRITICAL - *2*

Sur cette image, on peut voir que les 2 interfaces sont OK et la troisième est DOWN, ce qui est normal car ce sont les interfaces SFP sur lesquelles nous avons relié une fibre sur chacune d'elles, celles où nous avons utilisé de l'EtherChannel (LACP).
Une fois ceci fait, nous allons utiliser graphite afin de récupérer les informations à partir de Centreon.

3.4.3 Installer Graphite

On installe les paquets pour Graphite
```
apt-get install graphite-web graphite-carbon
```

on synchronise la base de données
```
graphite-manage syncdb
```

dans /etc/default/graphite-carbon changer la variable suivante :
```
# Change to true, to enable carbon-cache on boot
CARBON_CACHE_ENABLED=True
```

Dans /etc/carbon/storage-schemas.conf. Entre les deux blocs par défaut, ajoutez ce filtre :
```
[centreon]
pattern = ^centreon\.
retentions = 60s:1d, 20m:30d, 1h:1y
```

On copie le template de configuration dans le bon dossier
```
cp /usr/share/doc/graphite-carbon/examples/storage-aggregation.conf.example
/etc/carbon/storage-aggregation.conf
```

3.4.4 Configurer Graphite

Installation du serveur web:
```
apt-get install apache2 libapache2-mod-wsgi
```

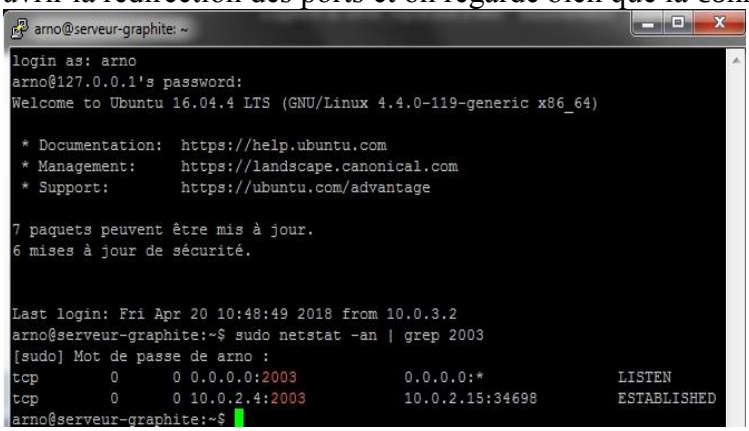
Mise en place de la configuration du site:
```
a2dissite 000-default
cp /usr/share/graphite-web/apache2-graphite.conf /etc/apache2/sites-available
a2ensite apache2-graphite
service apache2 reload
```

dans /etc/graphite/local_settings.py, changer la variable :
```
TIME_ZONE = 'Europe/Paris'
```

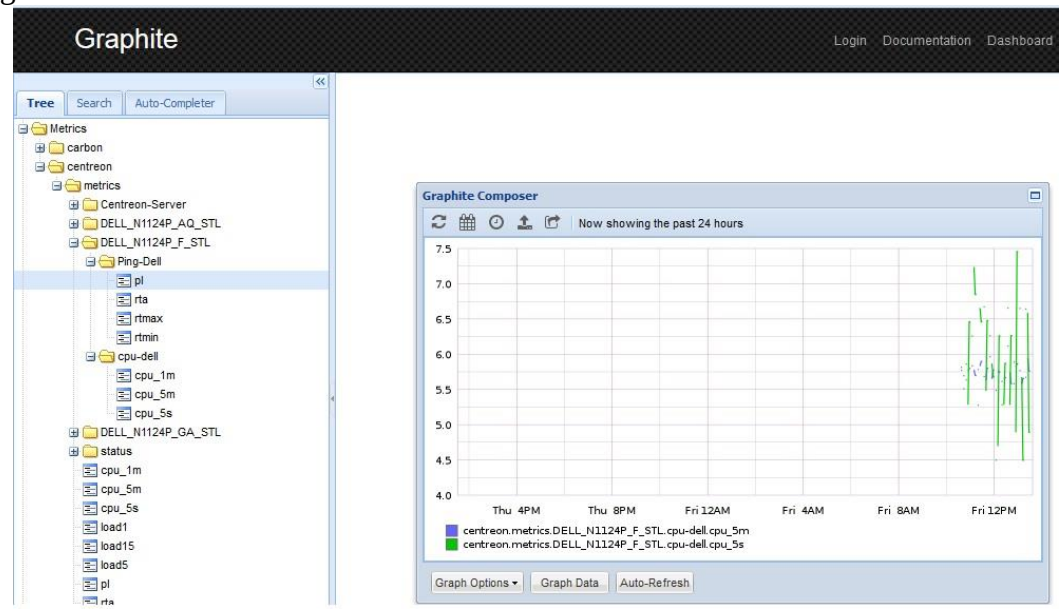
3.4.5 Configurer Centreon pour Graphite

Il suffit d'ajouter un module output de type graphite à la configuration de central-broker-master.
Cliquez sur Configuration -> Pollers -> Broker configuration.
Et d'ajouter un output Graphite dans l'interface et y mettre les informations suivantes :
```
Name:                   graphite
DB host:                10.0.2.4
DB port:                2003
Maximum queries:        1000
Metric naming:          centreon.metrics.$HOST$.$SERVICE$.$METRIC$
Status naming:          centreon.metrics.status.$HOST$.$SERVICE$
```

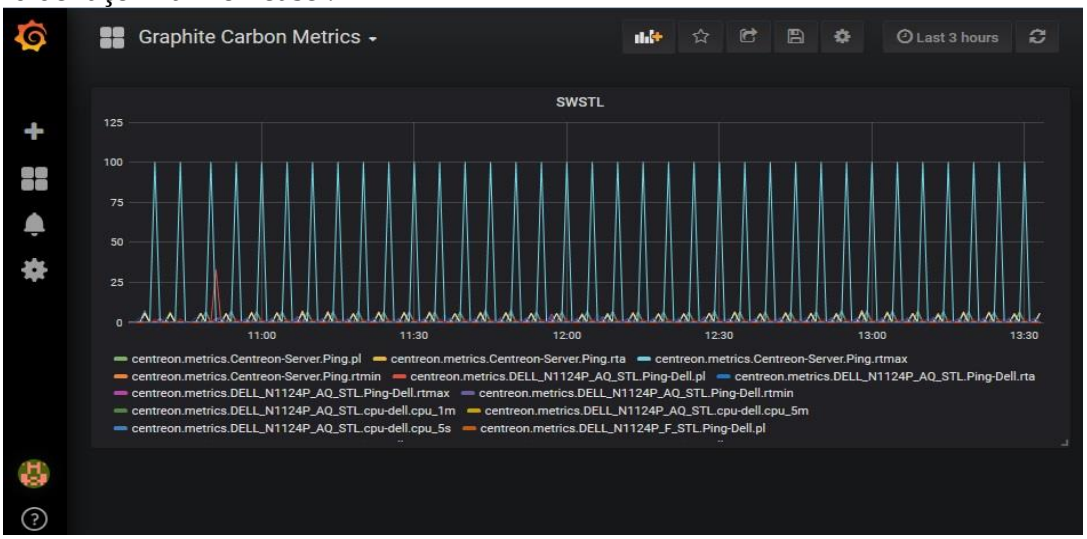
On n'oubliera pas d'ouvrir la redirection des ports et on regarde bien que la connexion soit établie :



Une fois cela mis en place, sur le serveur de graphite, on devrait avoir l'arborescence mise en place, visible à gauche :



Pour finir avec cette partie, j'ai connecté les données de Graphite sur Grafana qui est un logiciel de visualisation et de mise en forme de données métriques. C'est cet outil qui permet de créer des Dashboard de façon harmonieuse :

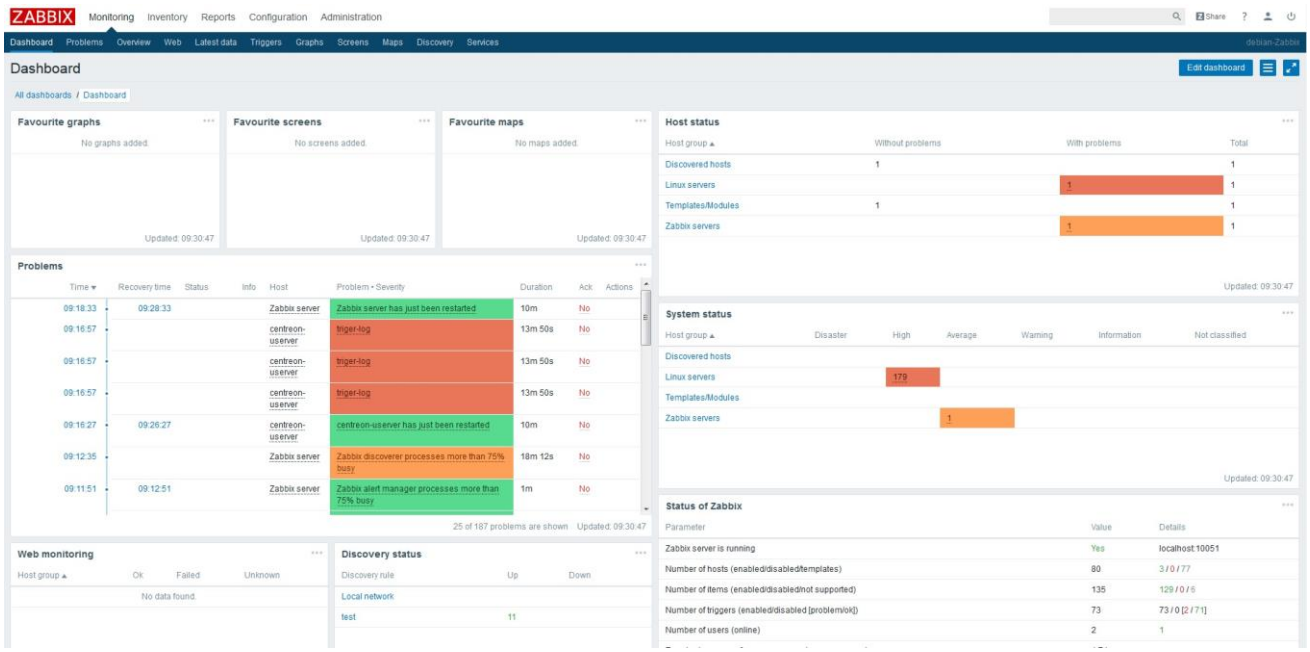


J'ai aussi comparé une autre solution de supervision, Zabbix. Nous allons voir les différences, les avantages/inconvénients.

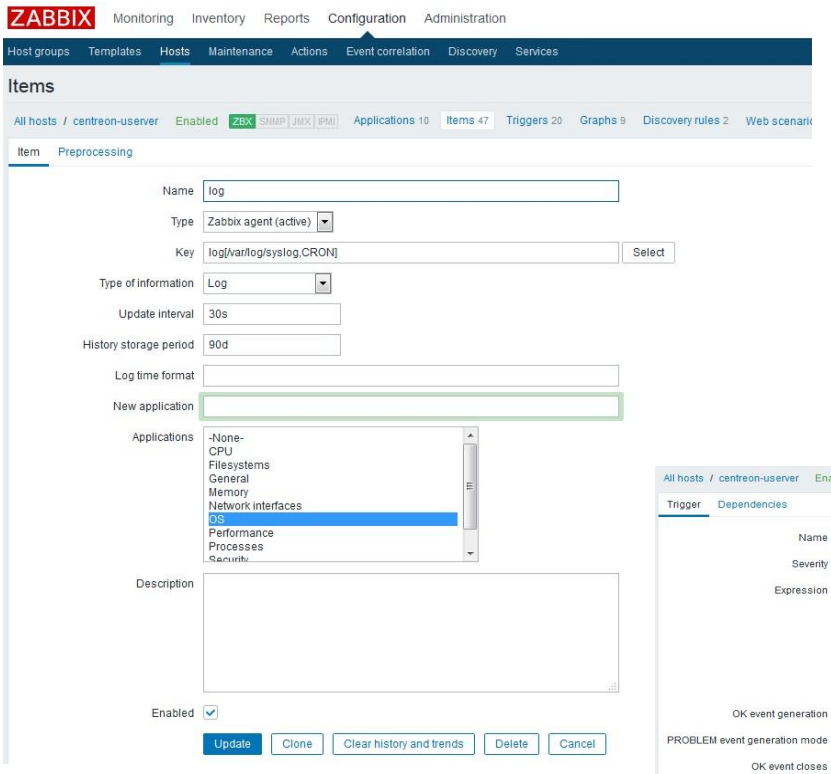
3.5 Zabbix

Zabbix comme Centreon, est un outil de supervision système open-source.

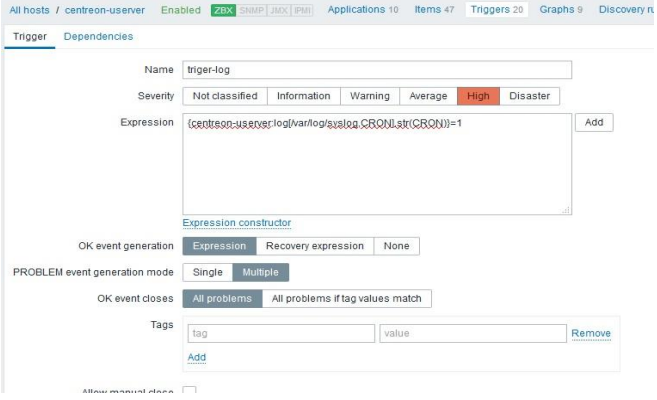
Voici à quoi ressemble l'interface Zabbix :

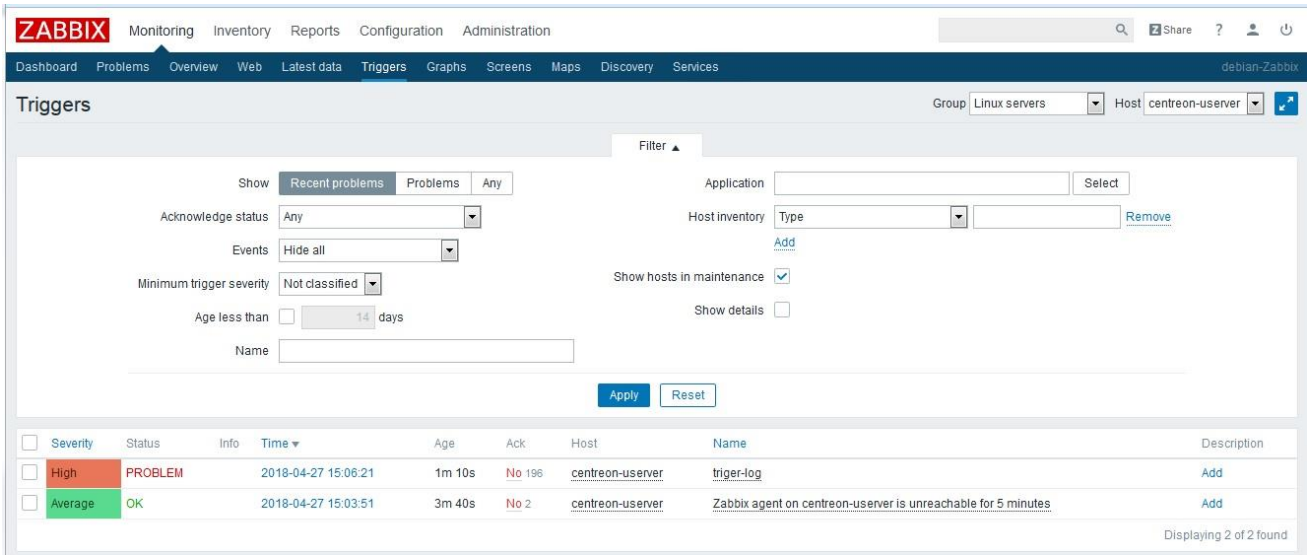


Pour commencer comme avec Centreon, j'ai ajouté les commutateurs que j'ai installé pour servir de test.
Dans Zabbix, les applications correspondent aux templates des paramètres et des commandes permettant de surveiller un service. Les items sont les commandes qui permettent de vérifier les services qui sont-elles même contenues dans les templates. On peut en ajouter manuellement.



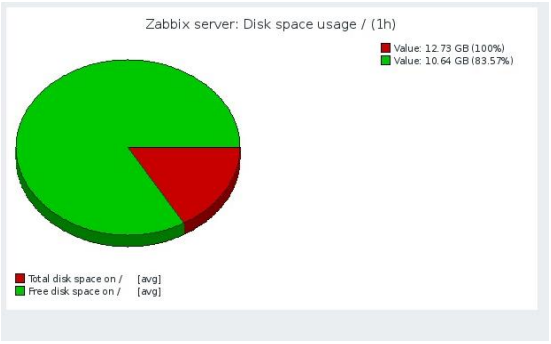
J'ai donc testé une commande permettant que dès lors qu'un mot défini s'affiche dans les logs cela fait remonter une alerte dans Zabbix. J'ai créé un nouvel item avec une commande spécifique. « log[/var/log/syslog,CRON] ». Cette commande va permettre de chercher le mot CRON dans le fichier /var/log/syslog. Afin de paramétrer l'alerte, il faut créer un « trigger ».





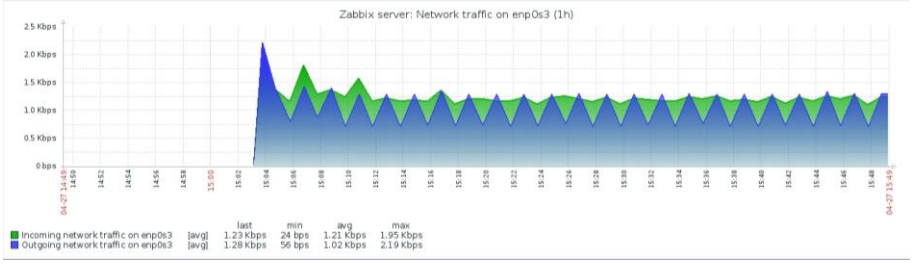
On peut notamment avoir des graphes sur plus de services que Centreon et de façon plus claire et détaillée.

Camembert sur l'occupation de l'espace disque.



Graphique sur la charge CPU

Traffic entrant/sortant de la carte réseau.



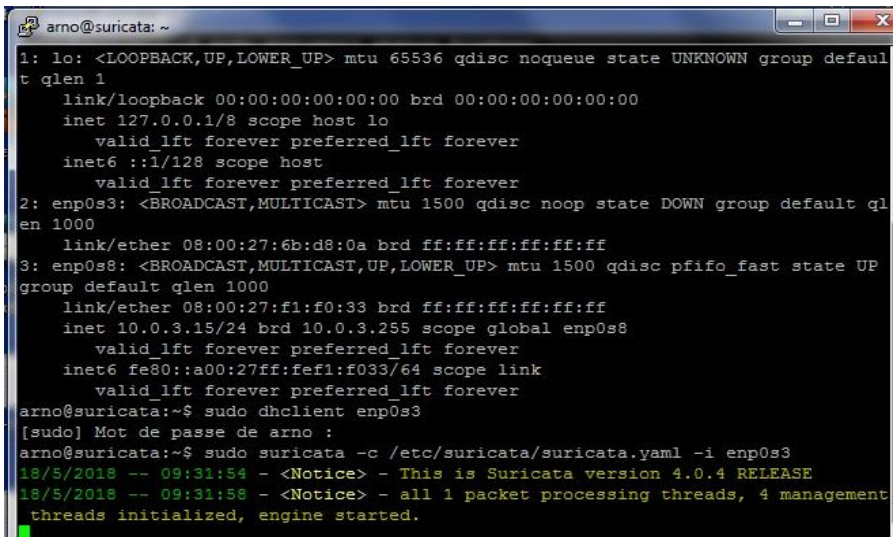
Pour faire un petit comparatif, je trouve Centreon plus facile à configurer, plus clair et plus convivial graphiquement.

De plus, Zabbix dispose de peu de connecteurs avec d'autres solutions pour extraire et analyser les données dans un autre outil.
Je résume les principaux avantages/inconvénients dans le tableau suivant :

Application	Avantages	Inconvénients
Zabbix	- Une application complète Très bien documentée. - Les interfaces de supervision et de configuration sont plus claires et plus intuitives que celle de Nagios - L'agent peut lancer des scripts afin de collecter de l'information. - Dessiner les graphes en temps réel (Mise à jours toute les 30secondes). - Gestion des droits d'accès des utilisateurs. - Configuration des notifications et des alertes faciles à l'aide de shell scripts.	- L'agent zabbix envoie par défaut en claire les informations. - Pas facile à utiliser pour un simple utilisateur. - Interface web compliquée et plein de fonctionnalités.
Centreon	- Interface Web très ergonomique. - Une Solution complète de supervision. - Très performant.	- Possibilité de rencontrer des problèmes de compatibilité. - Moins rapide que Nagios.

3.6 Test de Graylog et communication avec Suricata

Graylog est une solution open source de gestion de fichiers journaux qui stockent les messages dans une base de données Elasticsearch (pour l'indexation et la recherche des données). Cet outil permet une supervision par les logs, de détecter des erreurs sur les protocoles comme http, SSH ou autre.
Suricata est quant à lui un outils appelé IDS qui permet la prévention d'intrusion par la détection de celles-ci, il permet aussi de remonter des alertes à l'aide des logs et ainsi de faire une supervision de sécurité réseau.
Ces deux outils couplés, nous avons une solution de supervision en sécurité solide. J'ai dans un premier temps testé la solution sur une architecture virtuelle sous VirtualBox avec deux machines sur le même réseau pour me rapprocher au mieux de la situation réelle qui sera mise en place par la suite.
Dans une première VM on installe Suricata déjà présent dans les dépôts avec la commande suivante : « sudo apt install suricata »
On le lance en indiquant la bonne interface :



Dans le monde de linux il y a les paquets, que l'on peut voir comme des logiciels, qui sont présents de base dans la distribution. On peut les installer sans rien toucher en utilisant la commande apt sous debian/ubuntu, ce qui indique qu'ils sont présents dans le dépôt de base de la distribution.
Pour les paquets qui ne sont pas présents de façon native, nous avons le choix : il faut soit compiler le paquet depuis les sources soit mettre en place un dépôt externe et l'installer via apt.
Pour le cas de graylog j'ai utilisé le choix 2.

Dans une autre VM J'ai installé Graylog, pour cela j'ai utilisé un dépôt extérieur à celui de debian, celui de graylog. Pour ce faire, l'éditeur de graylog propose un package .deb permettant l'installation automatique du dépôt dans apt. Pour l'installer il suffit de télécharger le fichier .deb sur le site officiel et entrer les commandes suivantes :

```
wget https://packages.graylog2.org/repo/packages/graylog-2.4-
repository_latest.deb
sudo dpkg -i graylog-2.4-repository_latest.deb
sudo apt-get update
sudo apt-get install graylog-server
```

Pour vérifier la source du dépôt j'ai dû me rendre dans « /etc/apt/sources.list.d/ ». Un fichier qui se nomme « graylog.list » devait s'y trouver dedans avec l'adresse source du dépôt.

Il ne me manquait plus qu'à installer filebeat (un connecteur entre suricata et graylog) sur notre serveur suricata pour faire transiter les données de suricata vers le serveur de graylog.

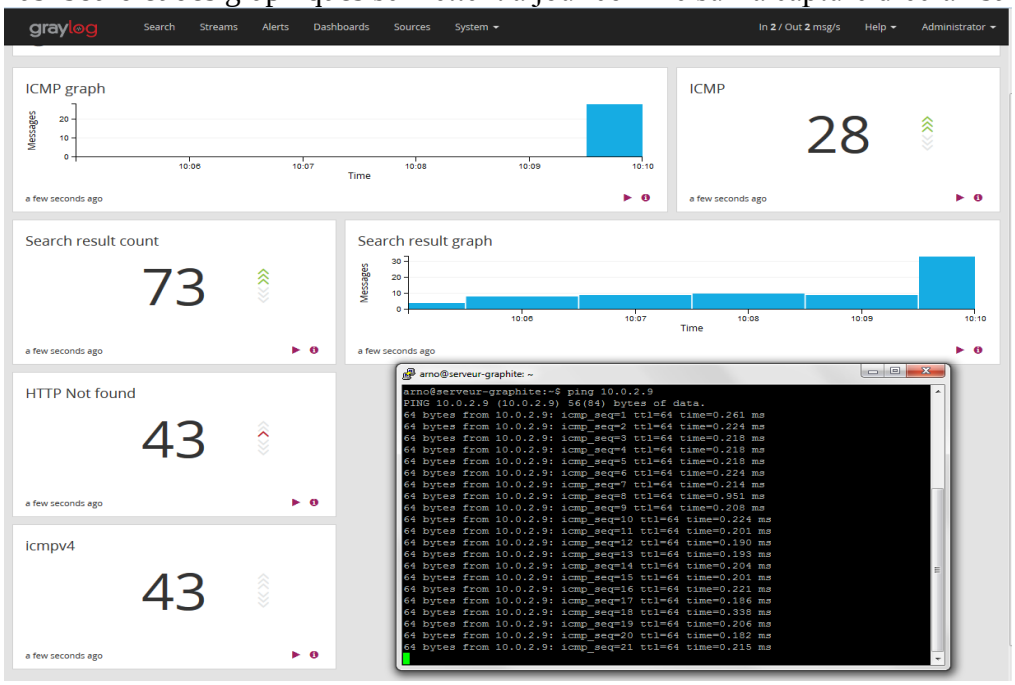
```
apt install filebeat
```

Et dans /etc/filebeat/filebeat.yml j'ai inscrit cette configuration :

```
#------------------------------ Logstash output -------------------------------
output.logstash:
  hosts: ["[adresse du serveur Graylog]:5044"]
```

Pour finir l'intégration de suricata à graylog j'ai installé un « content Pack » que j'ai trouvé sur le market place de Graylog. Il y avait un problème lors de l'importation de ce dernier, celui-ci générait une erreur. Il a donc fallu que je crée des tables de correspondances à la main car celles-ci posaient problème.

Pour tester l'infrastructure mise en place, j'ai donc ajouté des règles sur les ping (ICMP), de façon à ce que lorsqu'un ping est effectué sur le réseau, l'information soit remontée par suricata. Ainsi les valeurs du Dashboard et des graphiques se mettent à jour comme sur la capture d'écran suivante :



Après avoir essayé cela sur une machine virtuelle avec Sébastien, nous l'avons installé sur un serveur physique du CNRS avec un flux de données beaucoup plus important. Nous avons aussi procédé à la mise à jour d'ElasticSearch, ainsi que Graylog qui datait un peu. Après avoir résolu quelques soucis, notamment au niveau de la RAM, Graylog demandant beaucoup de mémoire vive, nous avons réussi à mettre en place cette solution. Dorénavant le CNRS est doté de suricata et de graylog pour prévenir les intrusions.

3.7 La migration vers un nouveau cœur de réseau

La migration n'a finalement pas eu lieu comme énoncé précédemment mais voici les étapes tels qu'elles étaient prévues :

- phase préparatoire :
  nettoyage des configurations actuelles (vlan…)

- passage de tous les liens actuels du cœur vers les extrémités en configuration 802.3ad (LACP) du 12/04 au 27/04 :
  pour cette phase je devais m'occuper de prendre les disponibilités de chacun pour qu'on procède au modifications d'architecture.
  Les informaticiens en charge des laboratoires devaient s'assurer que leurs équipements actuels puissent faire du LACP.
  Cette phase est indispensable vu que sur le nouveau cœur le LACP* (VLAG) sera activé par défaut sur tous les liens. Dans un premier temps le LACP sera assuré via un seul lien.
  Pour assurer la redondance des liens après la migration il faudra prévoir l'achat de SFP/SFP+ (en fonction du débit) pour doubler tous les liens.

- passage des comptes du cluster de pare-feux Palo Alto actuel en lecture seule prévu le 09/05
  ➔ Ce qui évite de modifier les configurations de production pendant la phase de préparation du nouveau cluster.

- récupération des configurations actuelles du cluster de pare-feux et remontée des vlans sur celui-ci. Les tests s'effectueront du 10/05 au 30/05

- Epuration des configurations actuelles sur le cœur de réseau en vue d'intégrer une configuration propre sur le futur cœur de réseau.

- mises en rack du nouveau cluster de firewall et des nouveau équipements du cœur et de routage du campus prévues le 30/05

- la migration sera effectuée à une date à déterminer.

Le schéma de la future infrastructure :

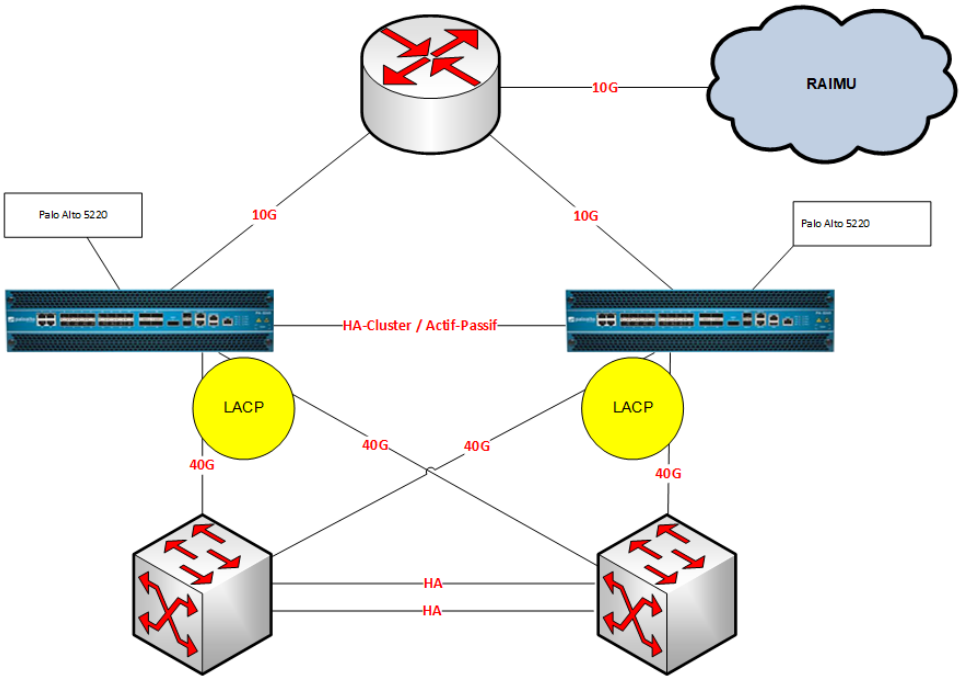


Photo des deux pare-feux en cours de configuration et de maquettage :

4 Conclusion

À travers ce stage, j'ai découvert le domaine de la supervision ainsi que de la détection d'intrusion réseau et systèmes. Ce projet m'a également permis d'appliquer et d'améliorer mes connaissances du domaine de l'administration systèmes et réseau mais aussi de la sécurité informatique.
Mes travaux sur la supervision seront bénéfiques pour le Service des Systèmes d'Information car ils ont permis d'initier une démarche d'amélioration de la surveillance et de la supervision du réseau.
Ce stage m'a beaucoup plu et m'a donné envie de continuer dans ce domaine spécifique. J'ai pris beaucoup de plaisir à monter des outils pour administrer, sécuriser et monitorer un grand réseau tel que celui du CNRS. Grace à ce stage j'ai pu découvrir la vie en entreprise, il m'a aussi aidé à savoir ce qui me plaisait pour mon futur projet professionnel.

5 Glossaire

Centreon, est un paquet open-source permettant de faire de la supervision.

Compiler, traduire un programme depuis un langage de programmation en langage CPU pour la machine

Debian/Ubuntu, sont des distribution Linux

DUT, Diplôme Universitaire de Technologie

EtherChannel , agrégation de plusieurs lien physique (câbles) afin d'augmenter la disponibilité et le débit

Firmware, est un programme intégré dans un matériel informatique (ordinateur, photocopieur, automate (API, APS), disque dur, routeur, appareil photo numérique, etc.) pour qu'il puisse fonctionner

Graphite, outils complémentaire à Centreon pour tracer des graphiques avec les données recueillies.

IDS : Intrusion Detection System

IPS : Intrusion Prevention System

LACP, protocole réseau non propriétaire permettant L'EtherChannel

SFP, small form-factor pluggable est un émetteur-récepteur compact, insérable à chaud, utilisé dans les réseaux de télécommunications et les réseaux informatiques.

SNMP : Simple Network Management Protocol

SSH : Secure Shell

Supervision : elle permet de suivre en temps réel l'état du réseau ainsi que les données relatives aux services, commutateurs, routeurs, serveurs (pannes, vitesse CPU, état des ventilateurs) via SNMP généralement, afin de pouvoir les analyser ou tester leur disponibilité.

TCP : Transport Control Protocol.

VLAN, Réseau virtuel

VM, Virtual Machine = Machine Virtuelle.

6 Bibliographie

https://fr.wikipedia.org/wiki/Centre_national_de_la_recherche_scientifique
http://www.provence-corse.cnrs.fr/
https://reseau.cnrs-mrs.fr/
http://www.sugarbug.fr/atelier/installations/ubuntu/ubuntu14_centreon_28/
https://www.zabbix.com/download?zabbix=3.4&os_distribution=debian&os_version=stretch&db=MySQL
https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Ubuntu_Installation