Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Mise en place d'outils de Supervision

Clément ESTIENNE

SFR Business

Responsable entreprise : Alexandre Lerpiniere

Responsable académique : Sébastien Sanchez

2019

Table des matières

1 Introduction

Dans le cadre de mon stage de fin d'année, j'ai été amené à passer dix semaines dans l'entreprise SFR Business situé au 389 avenue du Club Hippique, Aix-en-Provence, dans le service de Déploiement Clients et plus précisément dans leur laboratoire.
Durant ce stage j'ai pu découvrir le monde professionnel, le comportement à adopter dans une équipe ainsi que les automatismes que l'on doit développer.

Ma mission a été de mettre en place des outils ayant pour objectif une meilleure organisation et maintenance du laboratoire. En effet, les ingénieurs réseau SFR utilisent ce lieu pour mettre en place des maquettes avant une installation chez un client, et les configurations des équipements sont amenées à changer régulièrement. J'ai donc commencé par installer un serveur syslog* Splunk afin de centraliser l'historique des commandes et configurations rentré dans chaque machine.

J'ai pu ensuite mettre en place une solution de monitoring*, pour cela j'ai effectué une étude comparative de plusieurs outils pouvant répondre aux critères de ma mission afin de sélectionner le plus adéquat, ce qui a amené ma décision d'installer Zabbix. Grâce à cet outil, j'ai cartographié le réseau du laboratoire et j'ai mis en place une solution de surveillance et d'alerte en cas d'incident. Pour finir, j'ai installé deux switch* 3750, que j'ai raccordés aux deux outils mis en place précédemment.

Dans la suite de ce rapport, je commencerai par présenter SFR Business dans sa globalité, je détaillerai l'ensemble de mon travail ainsi que les difficultés que j'ai pu rencontrer et je conclurai en résumant mon travail effectué et en détaillant ce que ce stage m'a apporté.

2 Présentation de l'entreprise

2.1 Historique

SFR Business a été créée le 20 septembre 2008, sous le nom de SFR Business Team, lors de l'achat de Neuf Cegetel par SFR qui propose aux entreprises des solutions mobiles et fixes. Elle prend son nom actuel lors de sa fusion en 2015 avec Completel et Telindus France, pour former une nouvelle marque destinée aux professionnels. Elle compte aujourd'hui plus de 3000 collaborateurs et 150 000 entreprises clientes.

2.2 Activités

SFR Business propose et déploie une palette unique de services alliant des offres convergentes fixes mobiles et des solutions sur-mesure : téléphonie, données, Réseaux d'entreprise, des objets. Elle se positionne également comme un expert de la Sécurité informatique. Ces solutions simples et performantes permettent aux entreprises, de la TPE, Très Petite Entreprise, à la multinationale, en passant par les administrations, de faire de la transformation numérique un levier de développement à part entière.

2.3 Organisation

J'ai intégré l'équipe Méditerranée & Centre-Est de Bertrand HONORE. Elle correspond à l'ex Telindus France, rachetée par SFR pour concurrencer Orange cyber sécurité, et vient de déménager dans l'agence d'Aix-en-Provence.

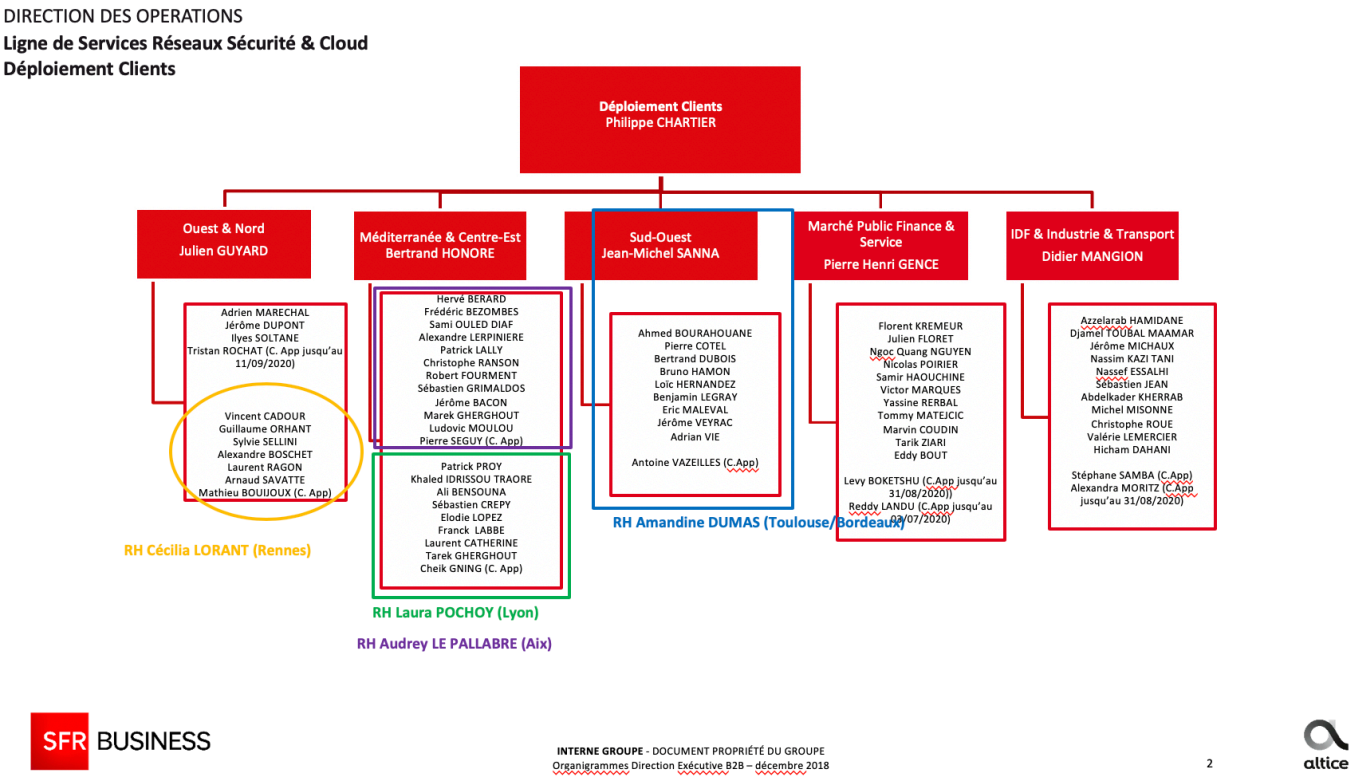


Figure 1 : Organigramme SFR Business – Service Réseaux Sécurité & Cloud – Déploiement Clients

3 Présentation du sujet du stage

3.1 Enoncé du stage

Alexandre, mon maître de stage, m'a confié deux missions principales. La première était de mettre en place un serveur de syslog Splunk afin de centraliser en un point les changements de configurations des équipements réseau du laboratoire et ainsi permettre une traçabilité de ces modifications.
La seconde mission était d'installer un serveur de monitoring afin de surveiller en temps réel l'utilisation CPU*, Central Processing Unit, l'utilisation de la mémoire des équipements. Si un de ceux-ci rencontre un problème, le serveur Zabbix devra alors notifier par e-mail un des administrateurs.
Si ces deux missions étaient portées à leur terme, alors je devrais installer deux switch 3750 dans leur laboratoire et les faire fonctionner avec les deux outils installés au préalable.

3.2 Problématique

Au-delà d'un projet d'administration système, c'était un projet professionnel. Il y a donc une partie très importante qui s'est ajoutée, la documentation. En effet, j'ai dû documenter l'ensemble de mon travail de façon très précise afin que même une personne sans formation dans ce domaine puisse compléter une installation totale de l'outil et sache aussi comment l'utiliser.
Pour mes deux missions, j'ai donc dû m'auto former, installer et configurer l'application, me familiariser avec celle-ci et enfin documenter entièrement mon travail.
Ma plus grande difficulté a donc été cette partie de documentation, c'était quelque chose de nouveau pour moi et j'ai dû m'y reprendre plus d'une dizaine de fois avant de produire quelque chose qui convenait à mon maître de stage. Mais j'ai beaucoup appris sur le fonctionnement du milieu professionnel, quand on conçoit une machine, un réseau, une application, on se doit de documenter son travail pour donner les moyens aux clients de se dépanner eux-mêmes en cas de problème.

3.3 Introduction à Splunk et Zabbix

3.3.1 Splunk

Splunk collecte, indexe et met en corrélation des données en temps réel dans des archives recherchables, permettant de générer des graphiques, des rapports, des alertes, des tableaux de bord et des infographies. Cet outil peut servir notamment à recueillir les syslogs d'équipements réseau tels qu'un routeur*, un switch, ou encore un firewall*.
Splunk peut accueillir des applications et modules afin d'être encore plus efficace et d'opérer avec des marques spécifiques comme Cisco ou Palo Alto. Il va mettre en forme les syslogs récupérés afin de faciliter la détection de pannes ou même de prévoir celles-ci.

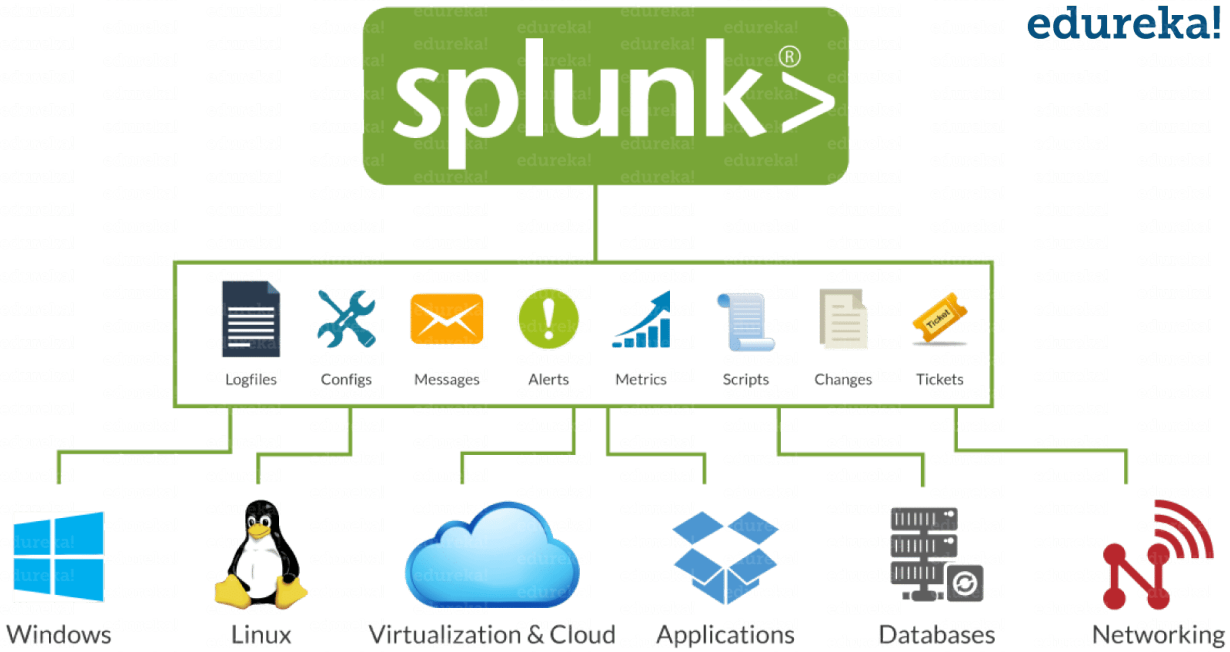


Figure 2 : Schéma Splunk

Comme nous pouvons le voir sur ce schéma (Figure 2), Splunk fonctionne avec des systèmes et applications variés.

3.3.2 Zabbix

Zabbix est un logiciel libre permettant de surveiller l'état de divers services réseau, serveurs et autres matériels réseau, produisant des graphiques dynamiques de consommation des ressources.

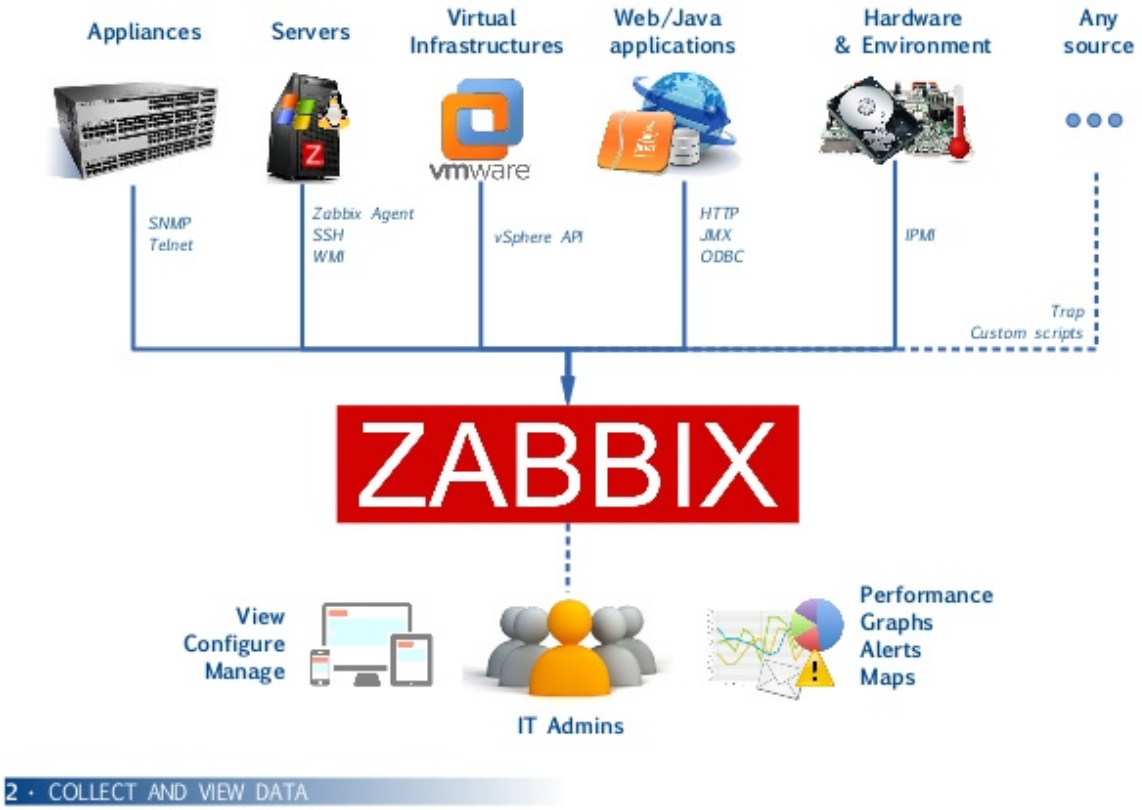


Figure 3 : Schéma Zabbix

Cet outil permet de monitorer une variété très large de systèmes différents via un agent que l'on installe sur les machines souhaitées, ou alors via différents protocoles comme le protocole SNMP*, Simple Network Management Protocol.
J'ai dû utiliser SNMPv2* selon le souhait de ma direction. Pour utiliser cette solution, il faut coupler ce protocole à des modèles qui vont mettre en forme les données récupérées par Zabbix. Comme splunk, il supporte un grand nombre de systèmes différents (Figure 3), il peut par exemple monitorer un routeur Cisco et une imprimante.

4 Présentation du travail réalisé

4.1 Préparation de l'environnement de travail

Afin d'installer Splunk et Zabbix, j'ai dû créer deux VM*, Virtual Machine, dans l'environnement VMware de mon service via un outil nommé vCenter. Au préalable, on m'a créé un pool de ressources* nommé CLES (CLement EStienne).

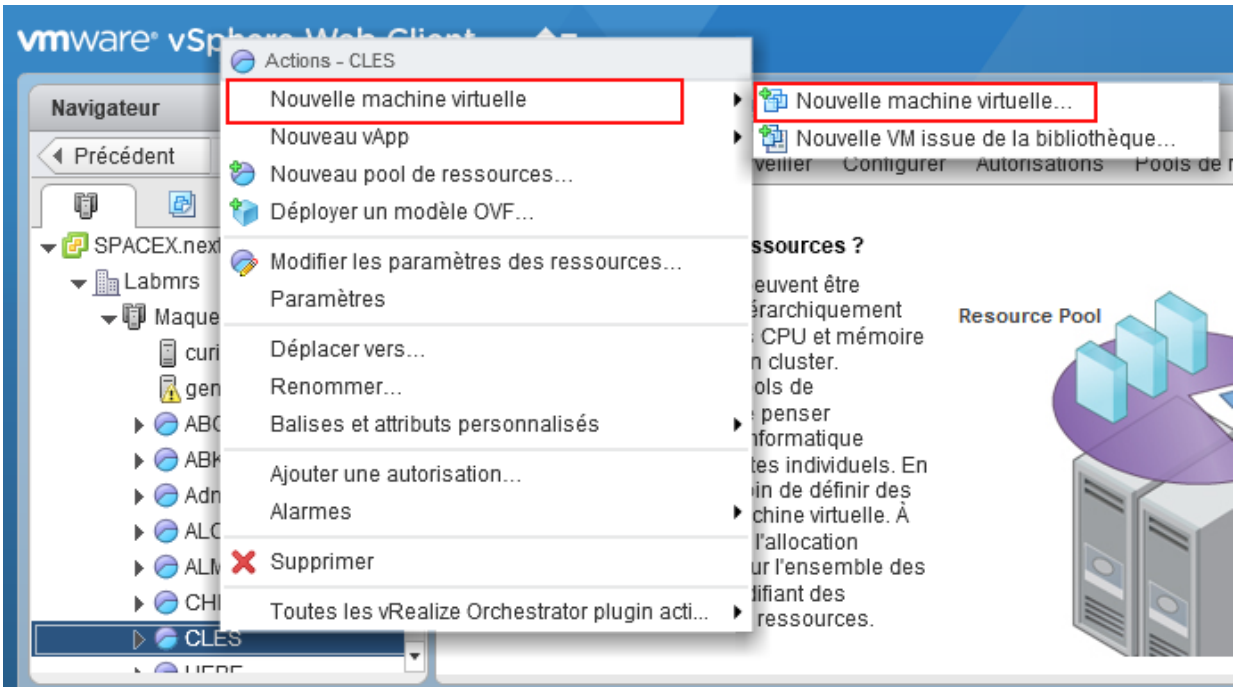


Figure 4 : Création d'une VM sur vCenter

J'ai donc pu entamer la création de mes VM (Figure 4), il y a plusieurs étapes pendant lesquels on va sélectionner le serveur qui va stocker le disque de ces VM et ou on va sélectionner les caractéristiques CPU, mémoire, stockage, réseau, etc. (Figure5).

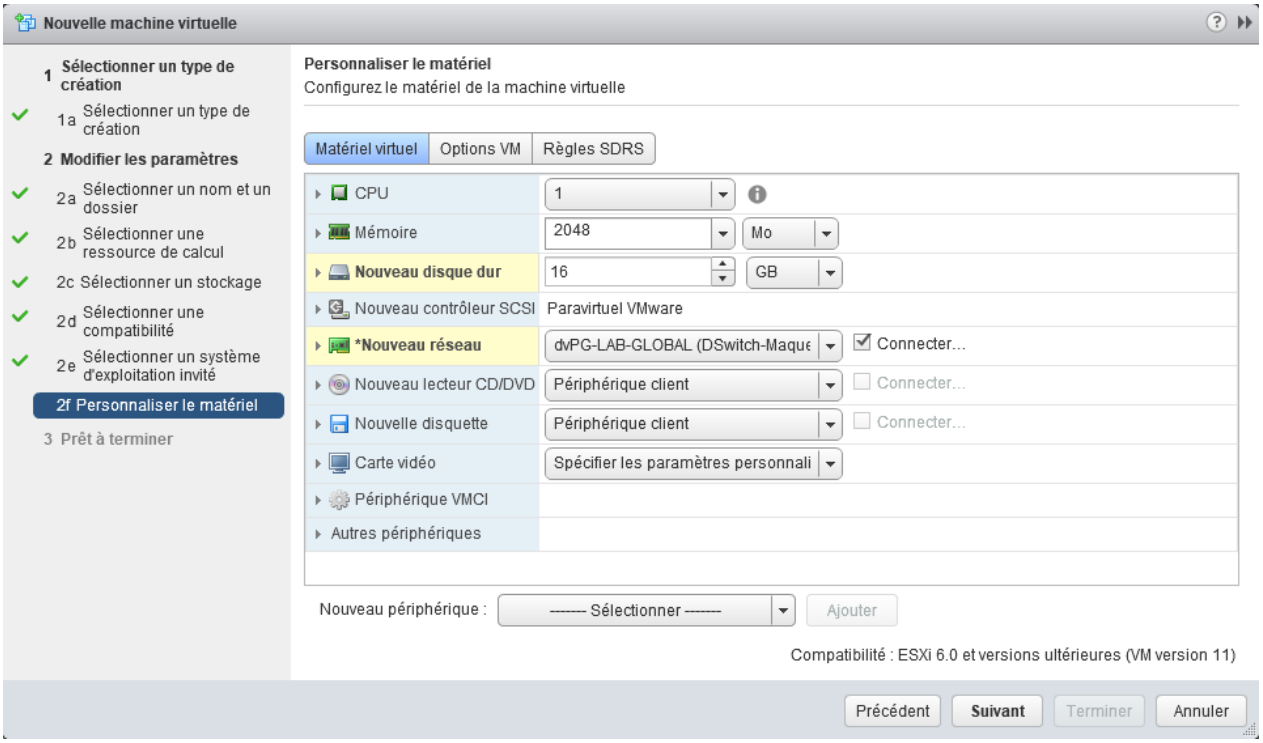


Figure 5 : Sélection des caractéristiques d'une VM

Comme système d'exploitation*, on m'a laissé le choix et j'ai donc décidé d'utiliser Debian 9 que j'ai l'habitude d'utiliser.

Je leur ai attribué une IP que j'ai dû au préalable réserver sur le PHP Ipam*, IP Address Management, de mon agence (Figure 6).

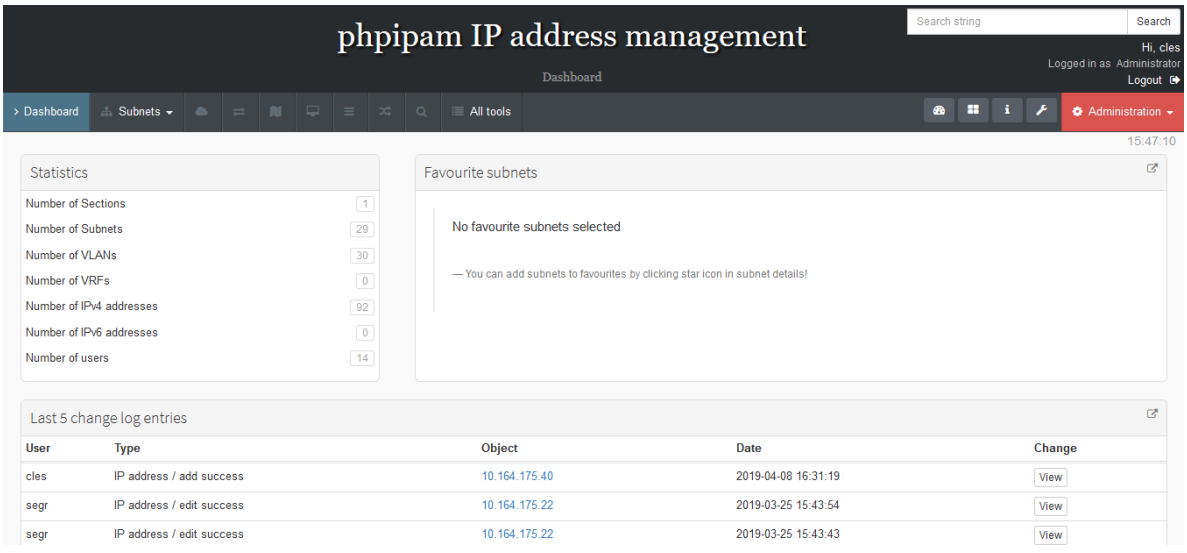


Figure 6 : Interface PHP Ipam

Sur cet outil, tous les utilisateurs du laboratoire doivent réserver une IP, donner un nom et une description à leur réservation. Cette solution permet une meilleure organisation au sein du service.

4.2 Serveur syslog Splunk

4.2.1 Installation de Splunk

L'installation de splunk fut rapide, il m'a suffi de télécharger l'archive de la dernière version sur le site de splunk, de la décompresser dans le répertoire /opt/splunk, et de me rendre dans /opt/splunk/bin pour rentrer la commande ./splunk start. Cela permet de lancer le processus splunk et d'entamer la procédure d'installation, notamment par la création d'un mot de passe administrateur.
Après avoir lancé le processus, il a fallu se connecter à l'interface web (Figure 7) à l'adresse http://IP:8000 et rentrer ses identifiants afin de commencer la configuration de cet outil.

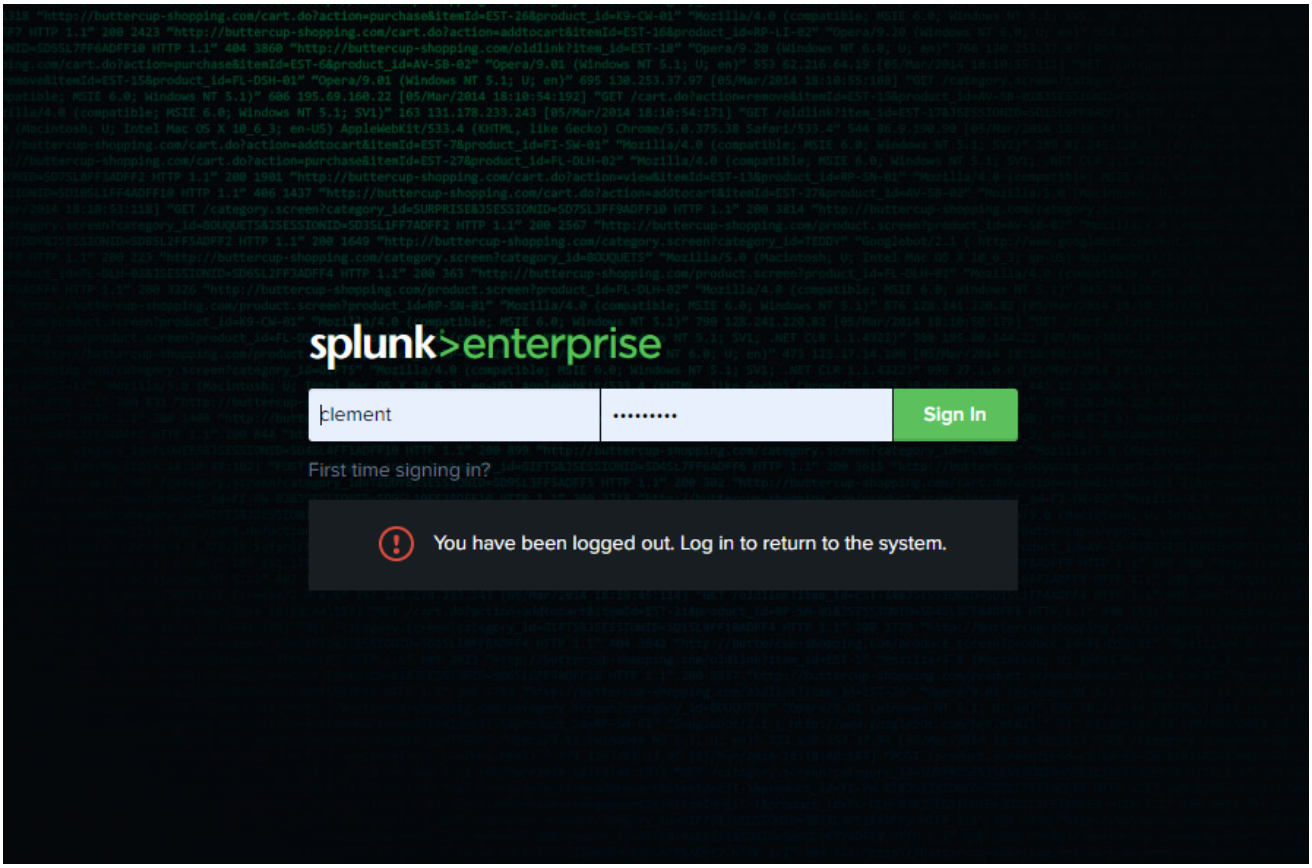


Figure 7 : Interface web Splunk

4.2.2 Configuration de Splunk

Pour rendre Splunk fonctionnel dans le laboratoire de SFR, j'ai dû suivre plusieurs étapes de configuration pour remplir le cahier des charges de mon projet.
Tout d'abord le protocole utilisé par l'interface web de Splunk devait être https*, HyperText Transfer Protocol Secure, et non http*, HyperText Transfer Protocol. Il a donc fallu activer le support SSL*, Secure Sockets Layer, Splunk nous facilite la tâche car il suffit d'activer ce support via un bouton.
Secondement, j'ai dû relier le système d'authentification de Splunk au serveur LDAP*, Lightweight Directory Access Protocol, du service pour que les administrateurs puissent se connecter avec leur compte. Cette étape était un peu plus complexe, mais grâce à l'aide d'Alexandre j'y suis parvenu.
Pour que les équipements puissent envoyer leurs syslogs au serveur que nous venons d'installer, il faut que celui-ci puisse les recevoir, il m'a donc fallu configurer un port d'écoute, le port par défaut étant le port UDP*, User Datagram Protocol, 514, et j'ai dû sélectionner le type de données à recevoir, ici des syslogs.
La configuration du serveur était à ce moment la basique mais fonctionnelle. J'ai donc pu commencer à le tester. Pour cela j'ai configuré le cœur de réseau du laboratoire pour qu'il puisse envoyer ses syslogs au serveur Splunk. Quelques commandes ont suffi :

conf t
logging facility local 7 (7 étant la valeur par défaut)
logging (@Ip du serveur Splunk)
End

Logging facility corresponds aux différents niveau de gravité des logs (Figure 8)

N	Niveau	Signification
0	Emerg	Système inutilisable
1	Alert	Une intervention immédiate est nécessaire
2	Crit	Erreur critique pour le système
3	Err	Erreur de fonctionnement
4	Warning	Avertissement
5	Notice	Événement normal méritant d'être signalé
6	Informational	Pour information seulement
7	Debug	Déboggage

Figure 8 : Niveau logging facility

À la fin de la journée, j'ai pu observer tout ce qui avait été fait sur le cœur de réseau.

Splunk permet d'installer des applications développées par les constructeurs telles que Cisco ou Palo Alto. Ces applications vont permettre une mise en forme des syslogs reçus, elles sont disponibles sur le site de splunk ou peuvent être directement installées via l'interface web.
Il y a 3 types d'équipements que voulaient surveiller mon service, les switch Cisco, les firewall Palo Alto et le service de virtualisation VMware, cependant ce dernier inondait le serveur splunk et il a fallu abandonner cette idée. Pour Cisco et Palo Alto, j'ai installé les applications proposées.

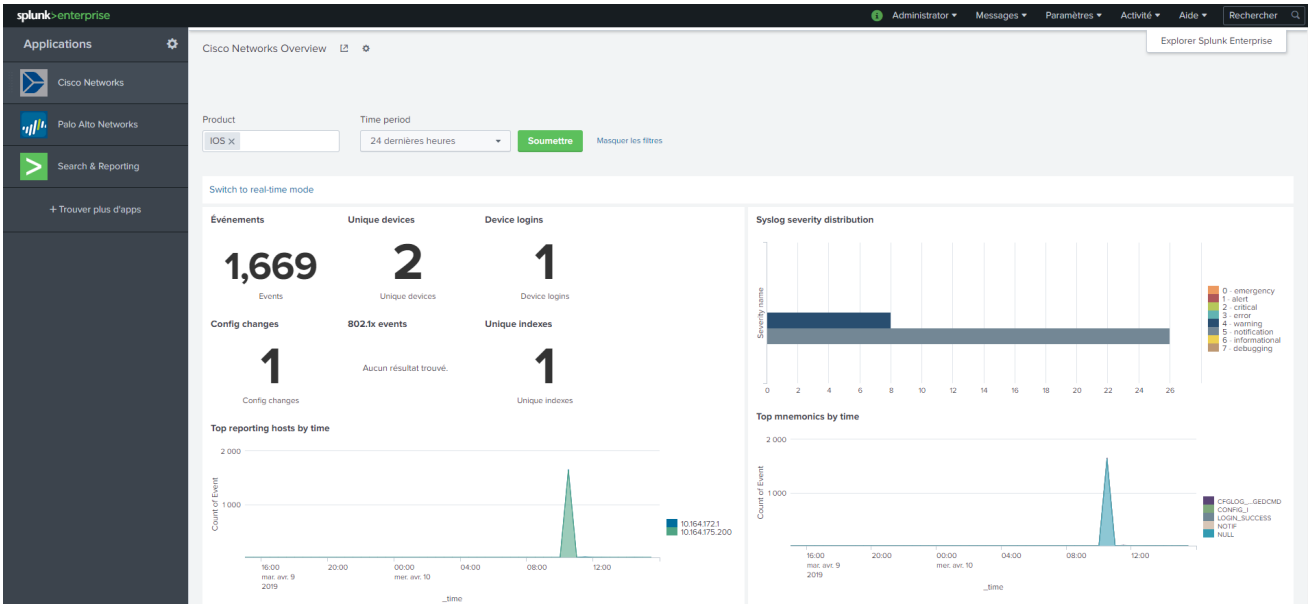


Figure 9 : Tableau de bord – Application Cisco Splunk

Sur le tableau de bord Cisco (Figure 9), différents graphiques sont affichés, ce qui permet une meilleure compréhension de l'état actuel de l'équipement ainsi qu'un historique détaillé de chaque action de la machine ou d'un utilisateur.

4.3 Étude comparative des outils de monitoring

Afin de sélectionner le meilleur outil de monitoring pour le laboratoire SFR, il m'a été demandé de faire des recherches et de rédiger une étude comparative.
Dans ce rapport, j'ai donc comparé 5 outils :

- Icinga2
- Nagios
- Centreon
- Zabbix
- Shinken

Pour être sélectionner, ces outils devaient être gratuits, supporter le protocole SNMP, pouvoir envoyer des alertes mails en cas de problème sur une machine monitor et avoir une interface graphique web claire et complète.
Pour chaque solution, je me suis informé dans un premier temps directement sur leur site respectif, puis dans un second temps sur des forums.

J'ai ensuite présenté mon rapport à Alexandre, mon maître de stage, pour qu'il puisse décider de quels outils j'allais installer.
Le choix final fut entre Icinga2 et Zabbix et Alexandre choisit Zabbix.

Ce document est disponible en annexe.

4.4 Serveur de monitoring Zabbix

4.4.1 Installation de Zabbix

Pour installer Zabbix, il m'a fallu installer plusieurs choses sur ma VM :

- Apache 2 :

  Le logiciel libre Apache HTTP Server (Apache) est apparu en avril 1995 et est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web. Il est distribué selon les termes de la licence Apache.
  L'installation reste classique (apt install apache2). Comme pour splunk, l'interface web de zabbix devra être en https. Il m'a donc fallu activer le module ssl de apache2, supprimer la configuration de site par défaut et activer la configuration ssl.

- PHP :

  PHP, **P**HP: **H**ypertext **P**reprocessor, est un langage de programmation principalement utilisé pour produire des pages web de manière dynamique. Il est donc, dans la très grande majorité des cas, couplé à un serveur HTTP (comme Apache) pour la communication avec le client web.
  Pour l'installation de Zabbix, j'ai eu besoin de 3 modules de PHP : `php-bcmath, php-mbstring et php-xml.`

- MariaDB :

  MariaDB est un système de gestion de base de données édité sous licence GPL. Il s'agit d'un fork communautaire de MySQL. En 2009, à la suite du rachat de MySQL par Sun Microsystems et des annonces du rachat de Sun Microsystems par Oracle Corporation. Michael Widenius, fondateur de MySQL, quitte cette société pour lancer le projet MariaDB, dans une démarche visant à remplacer MySQL tout en assurant la compatibilité des deux projets.
  MariaDB va permettre à Zabbix l'indexation de données. J'ai donc dû créer une base donnée pour Zabbix.

Après avoir installé ces 3 éléments, j'ai pu débuter l'installation de Zabbix en ajoutant le repository* de celui-ci, puis en installant zabbix-server-mysql et zabbix-frontend-php.

Pour compléter l'installation, j'ai dû me connecter à l'interface web de Zabbix à l'adresse https://IP/zabbix et suivre les étapes affichées (Figure 10).

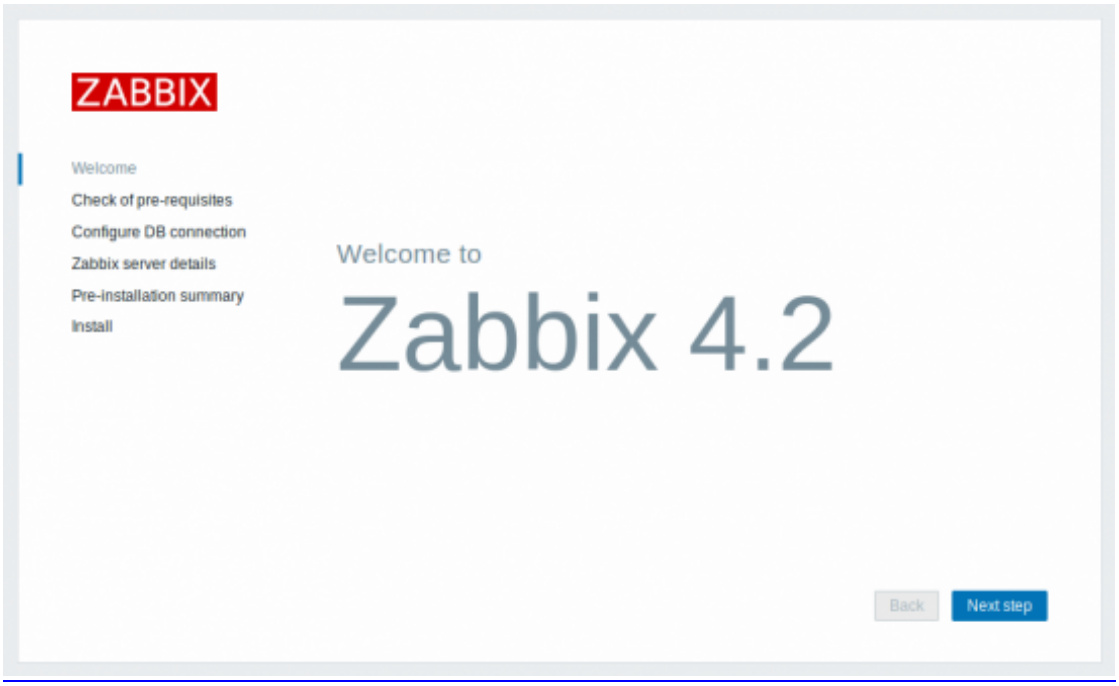


Figure 10 : Installation web de Zabbix

4.4.2 Configuration de Zabbix

Comme pour Splunk, j'ai dû relier l'authentification de Zabbix au serveur LDAP. Pour des raisons inconnues, cette étape fut plus fastidieuse que pour Splunk.
J'ai ensuite relié tous les équipements du laboratoire en SNMPv2 au serveur Zabbix afin de les monitorer. Pour cela j'ai dû tous les configurer avec la même communauté SNMP que j'ai nommée MONITOR-SFRLAB.
Pour ajouter un hôte à Zabbix, je devais le nommer, lui attribuer un groupe et donner son interface SNMP, donc son IP suivit du port SNMP, le 161 (Figure 11).

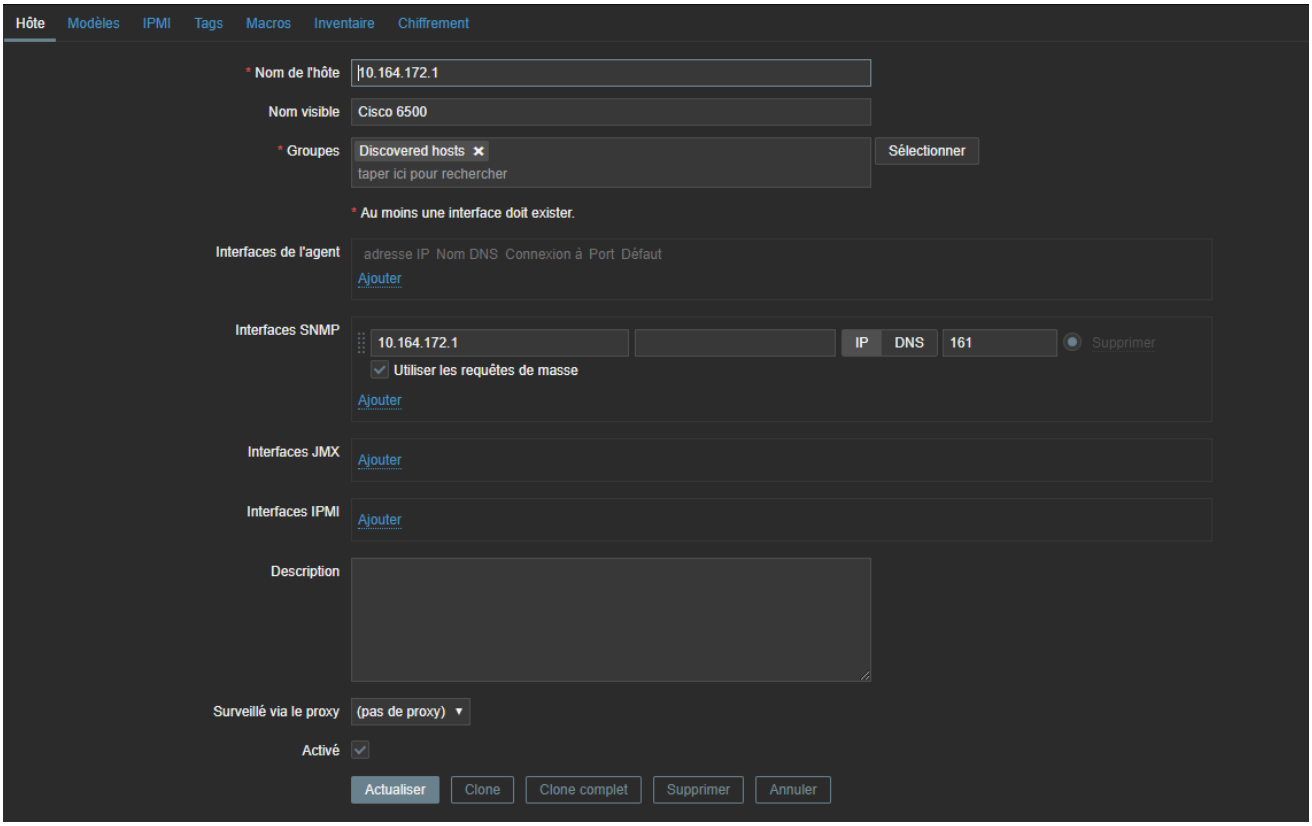


Figure 11 : Ajout d'un hôte sur Zabbix

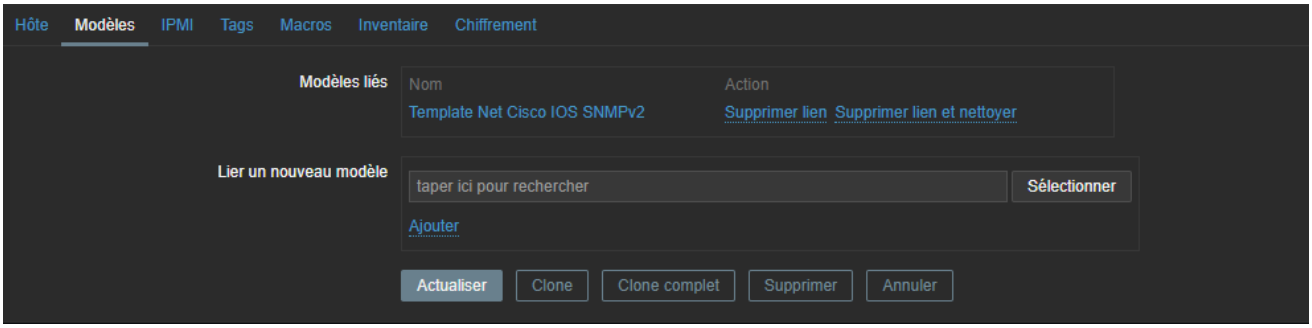


Figure 12 : Ajout d'un hôte sur Zabbix – Modèles

Il m'a fallu lui attribuer un modèle (Figure 12), comme expliqué précédemment, correspondant au type et à la marque de l'équipement.

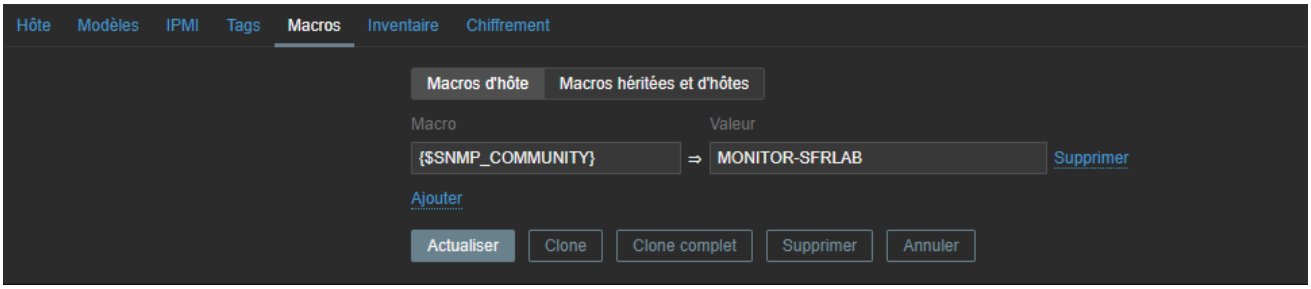


Figure 13 : Ajout d'un hôte sur Zabbix – Macros

Et enfin, la dernière étape, j'ai dû créer une macro* {$SNMP_COMMUNITY} (Figure13) correspondant à la communauté SNMP utilisée dans le laboratoire (MONITOR-SFRLAB).

La procédure est similaire pour tout type d'équipement sauf pour les serveurs VMware où elle est un peu plus complexe.

Pour chaque équipement monitoré, il a fallu créer un tableau de bord.

Figure 14 : Tableau de bord NAS Synology

Par exemple, j'ai dû créer un tableau de bord pour un NAS*,Network Attached Storage, qui affiche des informations sur le matériel, les problèmes rencontrés, l'utilisation CPU, l'utilisation mémoire, et l'utilisation des disques (Figure 14) .

Après avoir ajouté tous les équipements sur Zabbix et créé un tableau de bord pour chacun d'entre eux, il me restait deux étapes.
La première a été de configurer les alertes mails, la seconde a été de mapper le réseau du laboratoire.

Pour les alertes mails, j'ai dû créer un compte Gmail pour zabbix afin d'utiliser le serveur SMTP*,Simple Mail Transfer Protocol, de Google.

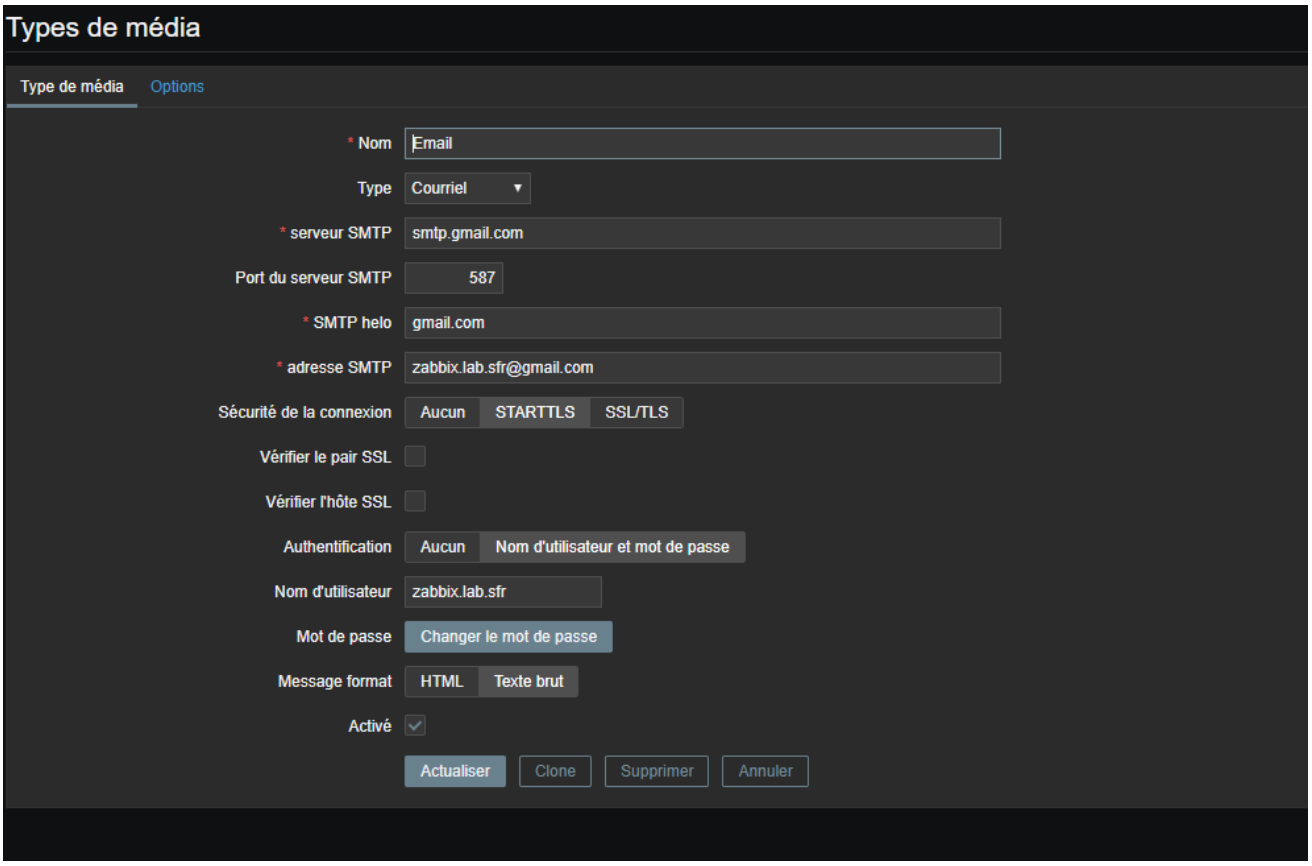


Figure 15 : Configuration SMTP Zabbix

Sur Zabbix, il a fallu configurer la solution d'envoi de mails avec les informations fournies par Gmail (Figure 15).

Pour les alertes mails, il est possible de configurer à partir de quelle sévérité de problèmes zabbix doit alerter un administrateur.

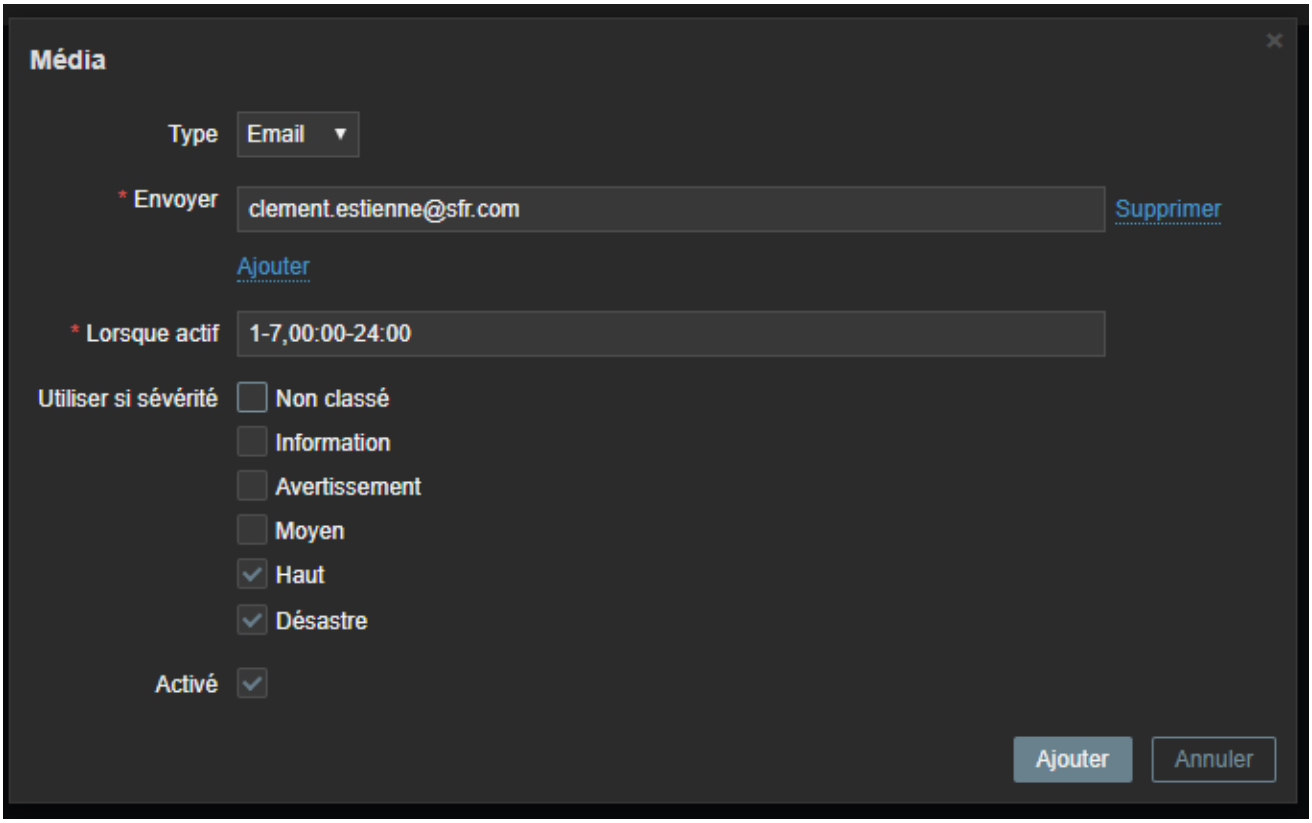


Figure 16 : Configuration Alerte Mail

Dans la configuration d'utilisateur, on sélectionne l'utilisateur pour qui on veut configurer des alertes et on sélectionne ses horaires d'activité ainsi que la sévérité des problèmes à signaler (Figure 16).

Pour mapper mon réseau, j'ai utilisé l'outil graphique de Zabbix qui permet très simplement de placer dans nos équipements au préalable ajoutés.

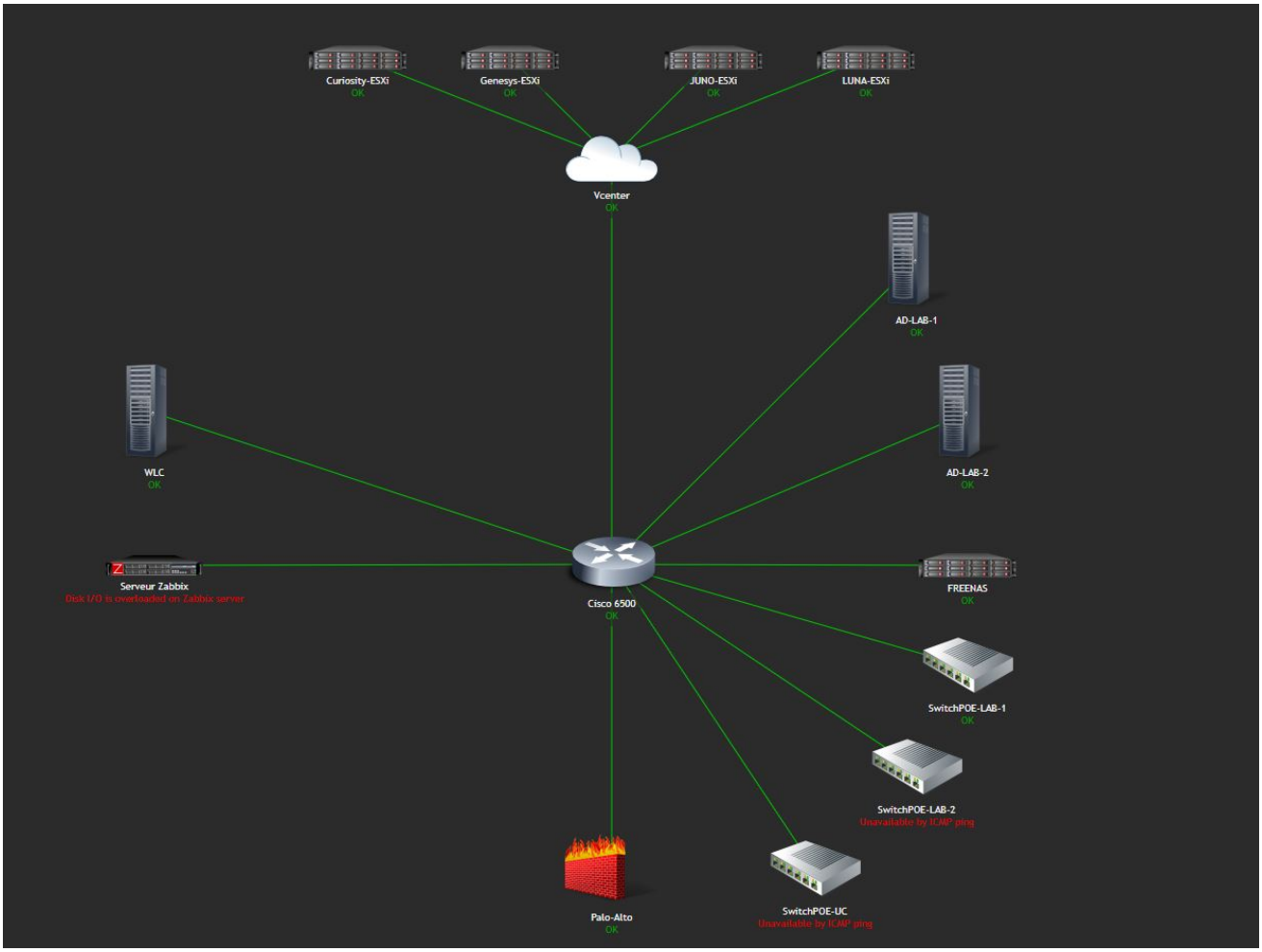


Figure 17 : Carte du réseau du laboratoire

J'ai par la suite intégré cette carte à tous les tableaux de bord, et j'ai fait en sorte que lorsque l'on clique sur un équipement, on peut avoir une option nous redirigeant sur le tableau de bord de l'équipement en question.

4.5 Installation Switch Cisco 3750

Ma dernière mission a été d'installer deux switch Cisco 3750 dans le laboratoire.
Afin que les ingénieurs testant leur maquette puissent travailler de façon plus ergonomique, j'ai installé au-dessus des paillasses des étagères métalliques pour placer les switch en hauteur et ne pas encombrer l'espace de travail.

La première difficulté rencontrée a été de ne pas avoir les identifiants pour pouvoir reconfigurer ces switch. J'ai donc dû réinitialiser le mot de passe. Pour cela, j'ai éteins électriquement mes switch et je les ai rallumés en restant appuyé sur le bouton mode situé à l'avant de ceux-ci.
Tout cela m'a permis d'initialiser manuellement la mémoire flash de mes switch, renommer le fichier de configuration (config.text) et enfin rebooter sans charger de configuration.
J'ai pu ainsi changer la configuration pour une nouvelle, fournie par Sébastien Grimaldos.
La dernière étape a été de passer l'interface connectée par câble au cœur du réseau en mode trunk* via les commandes :
int Gi2/0/24
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 20

Figure 18 : Installation Switch 3750

5 Conclusion

Durant ces 10 semaines de stages, j'ai mis en place deux outils de supervisions, Splunk et Zabbix.
La vraie expérience n'a pas été l'installation de ces solutions, mais de comment documenter son travail afin de partager son savoir avec son équipe et avec des clients. C'était un aspect du métier qui m'était inconnu jusqu'à présent.

J'ai pu découvrir ce qu'était réellement le travail en équipe, apprendre à compter sur ses collègues et à s'entre aider.

J'ai également été confronté à des difficultés techniques, que j'ai réglé en m'auto formant, et aussi à des difficultés sociales, faire l'effort d'aller dire bonjour à tout le monde a été quelque chose de nouveau pour moi.
Ces difficultés m'ont permis de grandir et de me préparer au monde de l'entreprise et de m'adapter à des situations que je ne pensai pas rencontrer.

Ce stage a donc été une réussite pour toutes ces raisons, et a permis de confirmer mon souhait de continuer dans ce domaine. Je me sens encore plus à l'aise dans le choix de poursuite d'étude que j'ai choisie dans le domaine de l'administration des réseaux et systèmes.

6 Remerciements

Je tiens avant tout à remercier mon maître de stage Alexandre LERPINIERE pour ses conseils durant mon stage.

Je tiens à remercier également Pierre SEGUY et Sébastien GRIMALDOS pour leur aide ainsi que Bertrand HONORE pour m'avoir accueilli au sein de son équipe.

De manière plus générale, je remercie tout le service Réseau de SFR Business d'avoir contribué à rendre mon expérience de stagiaire dans le monde professionnel enrichissante dans beaucoup de domaines.

7 Glossaire

Syslog, est un protocole définissant un service de journaux d'événements d'un système informatique.

Monitoring, est une activité de surveillance et de mesure d'une activité informatique. On parle aussi de supervision.

Switch, est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels.

CPU, est un composant présent dans de nombreux dispositifs électroniques qui exécute les instructions machine des programmes informatiques.

Routeur, est un équipement réseau informatique assurant le routage des paquets.

Firewall, est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau

SNMP, est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseau et matériels à distance.

SNMPv2, Version 2 du protocole SNMP

VM, est un environnement d'application ou de système d'exploitation installé sur un logiciel qui imite un matériel dédié.

Pool de ressources, un pool de ressources est une abstraction logique pour une gestion flexible des ressources.

Système d'exploitation, est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.

HTTP/HTTPS, est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (S pour secured) est la variante du HTTP sécurisée par l'usage des protocoles SSL.

SSL, est un protocole de sécurisation des échanges sur Internet

LDAP, est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire.

UDP, est un des principaux protocoles de télécommunication utilisés par Internet.

Repository, est un stockage centralisé et organisé de données.

Macro, est une liste d'ordres préalablement enregistrés et correspondants à des tâches qui doivent être régulièrement effectuées par l'ordinateur.

NAS, est. Un serveur de stockage en réseau.

SMTP, est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.

Trunk, est un lien physique permettant le transit de plusieurs VLANs.

8 Bibliographie

SFR Business : https://www.sfrbusiness.fr/

Splunk : https://www.splunk.com

Zabbix : https://www.zabbix.com/

Firewall.cx : http://www.firewall.cx/cisco-technical-knowledgebase/cisco-switches/1164-cisco-catalyst-3750-x-3560-x-password-recovery.html

TechExpertTips : https://techexpert.tips/fr/

9 Table des illustrations

Institut Universitaire de Technologie,
Aix-Marseille Université

ANNEXES
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Mise en place d'outils de Supervision

Clément ESTIENNE

SFR Business

Responsable entreprise : Alexandre Lerpiniere

Responsable académique : Sébastien Sanchez

2019

Comparatif des outils de supervision

Dans ce comparatif nous allons voir quel outil convient le mieux au monitoring du lab SFR.
Nous allons comparer 5 outils :

- Icinga2
- Nagios
- Centreon
- Zabbix
- Shinken

Icinga2

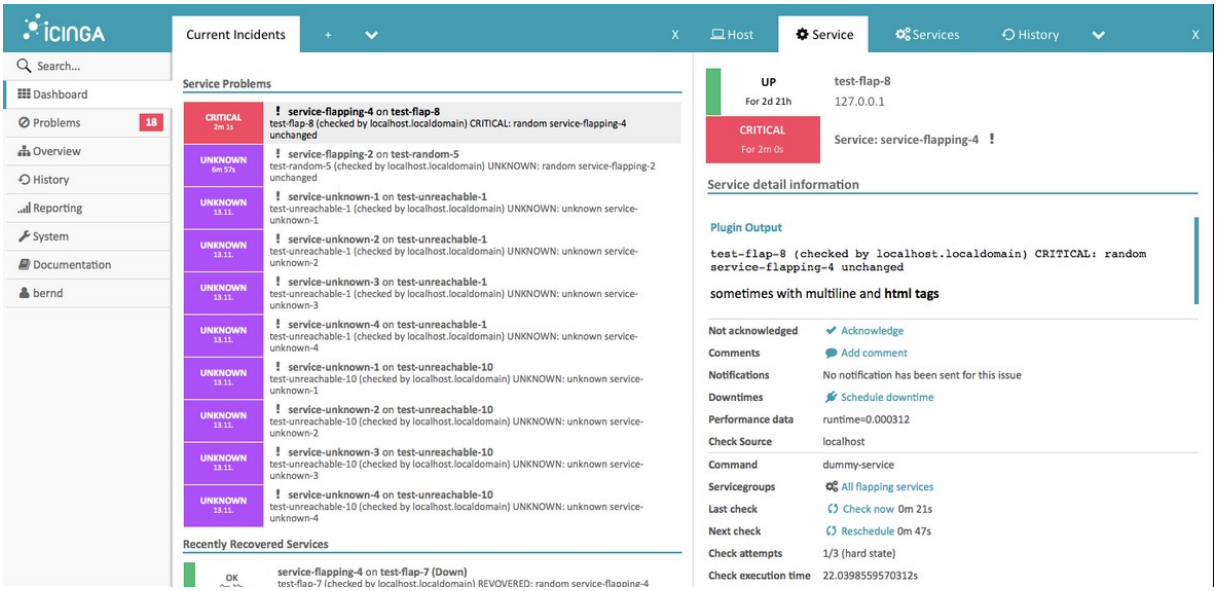
Historique :
Lancé le 15 mai 2009, Icinga fait partie des projets de Supervision Open Source dérivé du coeur du célèbre outil de supervision Nagios. Il est à l'époque le premier fork dans ce domaine, né du mécontentement des développeurs et contributeurs de Nagios qui ne voient plus évoluer le projet.

L'équipe recomposée fait évoluer le fork pendant 5 ans avant de sortir une nouvelle version baptisée Icinga 2 en juin 2014. Construit à partir de zéro, Icinga 2 est une réécriture complète de l'outil de supervision basé sur le langage C++ qu'on ne pourra alors plus qualifier de fork. En effet, plutôt que de continuer de développer à partir du Nagios Core, comme c'est le cas des versions 1.x, l'équipe de développement a décidé de repartir à zéro afin de repartir sur de nouvelles bases et notamment pouvoir construire une architecture modulaire par exemple avec Shinken.

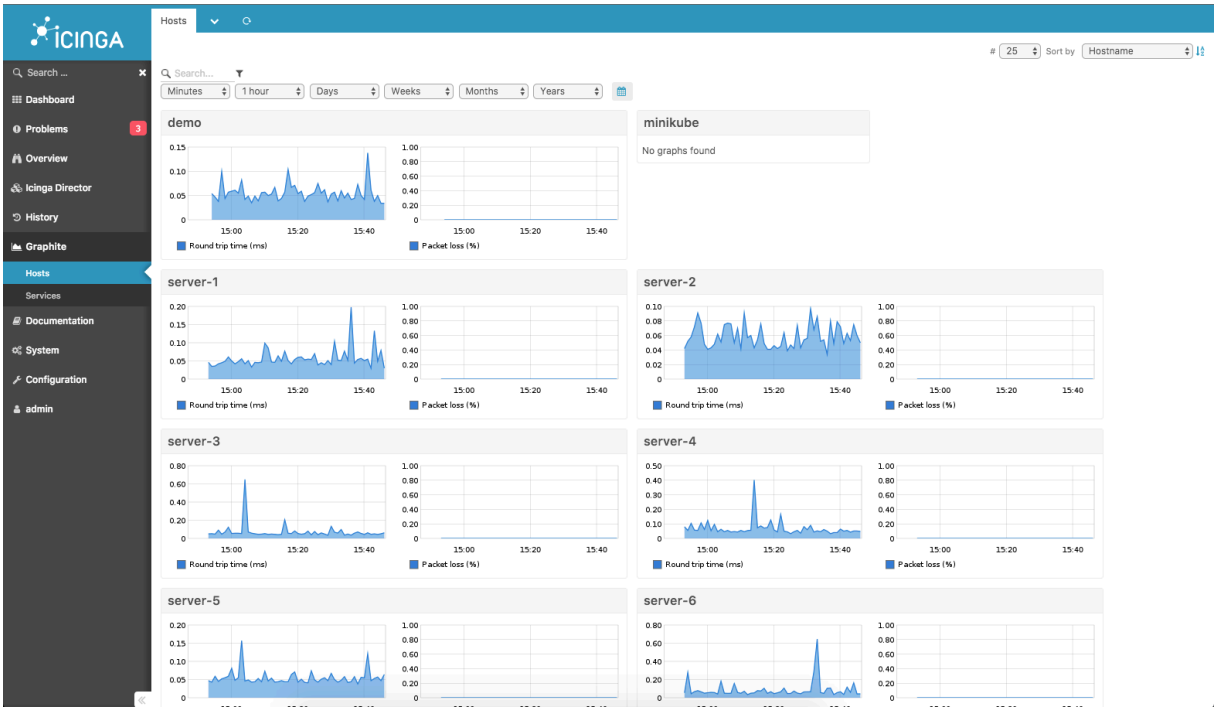
Fonctionnalité :

Icinga2 possède une architecture modulaire, ce qui permet de l'adapter à ses besoins, et de le rendre aussi complet que d'autres outils.
Au niveau base de données, Icinga2 prend en charge Oracle et PostgreSQL en plus de MySQL pour l'historisation des données.

L'interface web d'Icinga2 se veut claire et moderne :



Elle ne permet pas cependant d'afficher des graphiques etc, c'est que là que sa modularité rentre en jeu. Grâce à Graphite, on peut amener cette fonctionnalité à Icinga2 :



Il est aussi possible de créer ou d'installer des plugins qui sont disponibles sur la plateforme de partage d'Icinga2 : https://exchange.icinga.com/

Installation :
L'installation d'Icinga2 se veut simple. On peut l'installer via un repository, les mises à jour pourront donc se faire très facilement. Cependant depuis le changement du comportement de MySql, l'installation se complique un petit peu mais cela est indépendant du programme d'installation d'Icinga2.

Conclusion :
Icinga2 est donc un outil de supervision modulaire, et qui grâce aux applications déjà existantes et à sa communauté très active, devient très attractif.

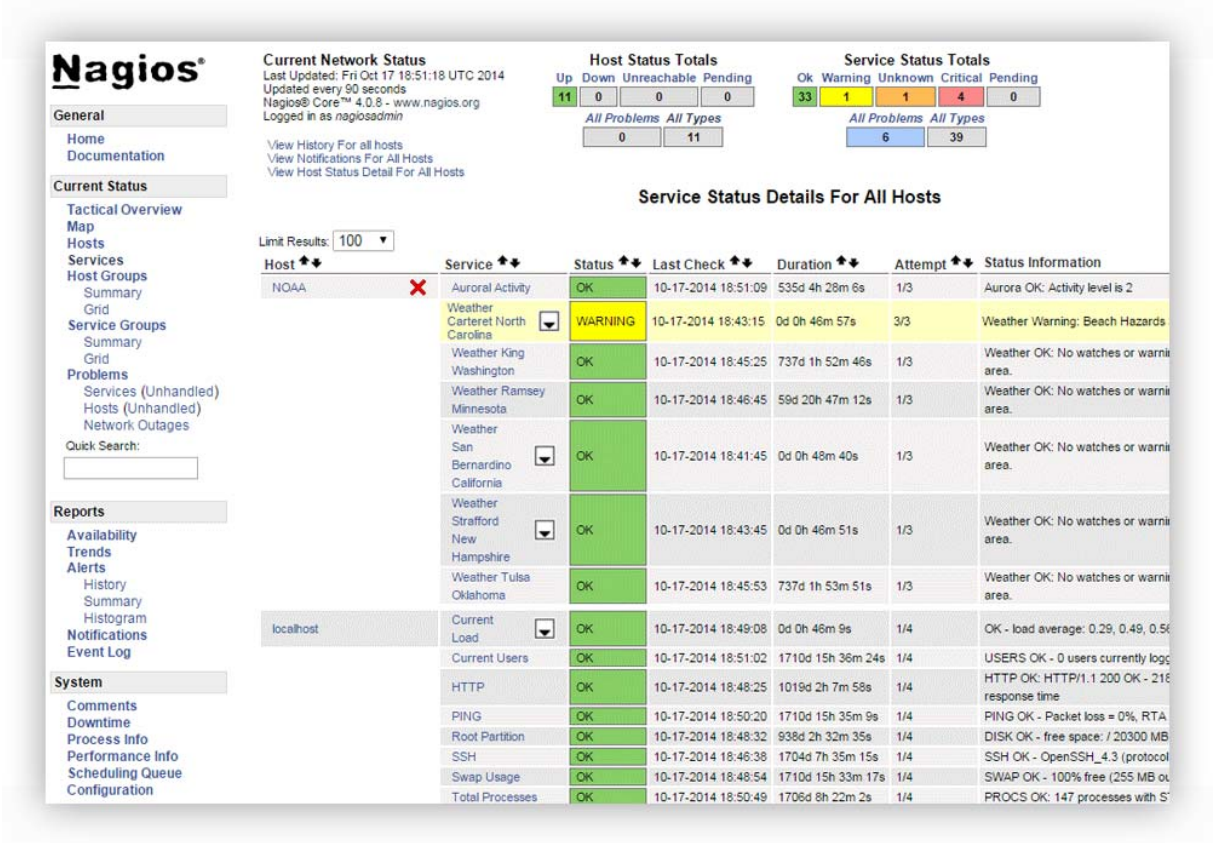
	Icinga2	Nagios	Centreon	Zabbix	Shinken
SNMP	Oui				
SNMP TRAP	Oui				
Interface graphique claire et complète	Claire et complète via l'installation de modules				

Nagios

Historique :
Nagios (anciennement Net saint) est un logiciel de supervision de réseaux créé en 1999 par Ethan Galstad. Il est considéré comme étant la référence des solutions de supervision Open Source. C'est un outil très complet pouvant s'adapter à n'importe quel type d'utilisation avec des possibilités de configurations très poussées. La modularité et la forte communauté (> 250 000) qui gravitent autour de Nagios (en participant au développement de nombreux plugins et addons) offrent des possibilités en termes de supervision qui permettent aujourd'hui de pouvoir superviser pratiquement n'importe quelle ressource.
Vu le manque de réactivité du développeur principal de Nagios et sa volonté de ne plus diffuser tous les modules sous licence libre, certains développeurs actifs sur le projet ont fait diverger Nagios pour créer Icinga.

Fonctionnalité :
À son installation, Nagios est capable de remplir beaucoup de tâches différentes, son développement n'est pas autant focalisé sur la modularité qu'Icinga.
Il est cependant possible d'installer une grande quantité de plugins afin d'optimiser son utilisation ou afin de lui permettre de répondre à une problématique en particulier.

L’interface web est assez dépassée et ses menus ne sont pas très optimisés.



Installation :
Le problème principal de Nagios est d’être un projet et non un produit. Son installation n’est donc jamais quasi la même.

Conclusion :
Nagios Core est gratuit, mais reste assez vieux. Les nouvelles versions de Nagios sont payantes (2000$ minimum). L’outil reste très complet, mais trop compliqué à mettre en place et à faire évoluer, la compagnie qui l’a développé se focalise sur ses solutions payantes.

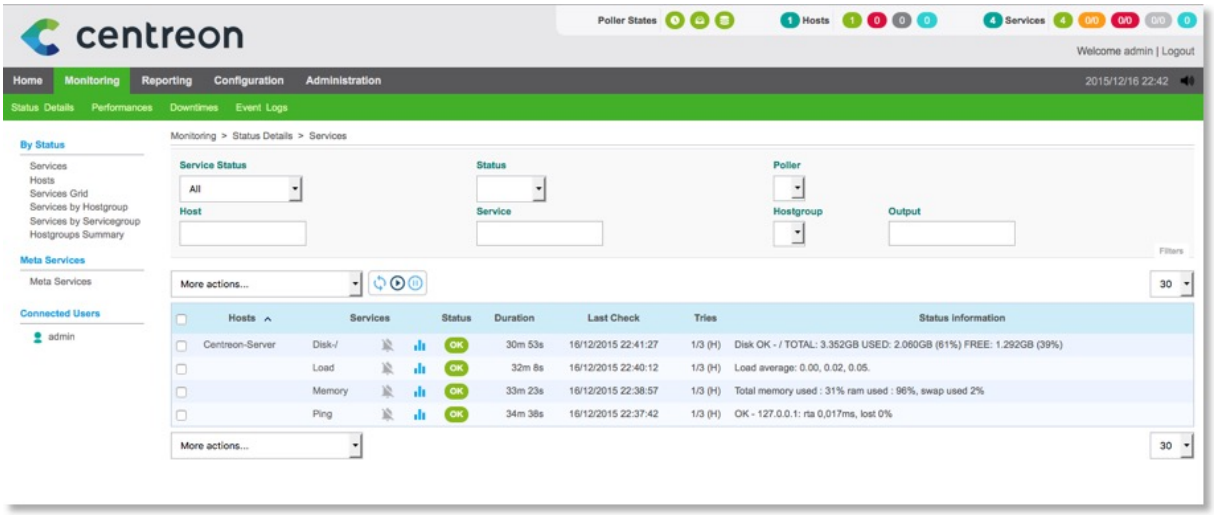
	Icinga2	Nagios	Centreon	Zabbix	Shinken
SNMP	Oui	Oui			
SNMP TRAP	Oui	Oui			
Interface graphique claire et complète	Claire et complète via l’installation de modules	Non			

Centreon

Historique :
Centreon (anciennement Oréon), a été créé en 2003 par des Français souhaitant améliorer Nagios, il a été repris par une nouvelle entreprise nommée Merethis. Il se présente comme une évolution de celui-ci pour tout d'abord son interface, mais aussi ses fonctionnalités. Il s'appuie également sur les technologies Apache et PHP pour l'interface web, MySQL pour le stockage des données de configuration et de supervision.

Fonctionnalité :
Centreon est ce que l'on peut qualifier d'usine à gaz, il est très complet et ne dispose que de quelques modules additionnels. Il possède un système de widgets permettant de compléter des fonctionnalités déjà existantes.

L'interface de Centreon est très bien organisée et assez claire :



Elle reste assez classique et s'aligne sur les standards des autres outils de supervision.

Installation :
Centreon est assez particulier à installer, mais cela reste assez simple. On peut tout d'abord l'installer via un dépôt sur un OS compatible ou alors télécharger leur propose ISO de centOS7 pour une installation propre. Cette solution facilite aussi les mises à jour de l'outil.

Conclusion :
Centreon est un très bon outil de supervision, il est complet et propose une configuration poussée ainsi qu'une personnalisation de son interface web via des widgets. Le problème principal de Centreon est les ressources qu'il demande pour bien fonctionner, il est très gourmand.

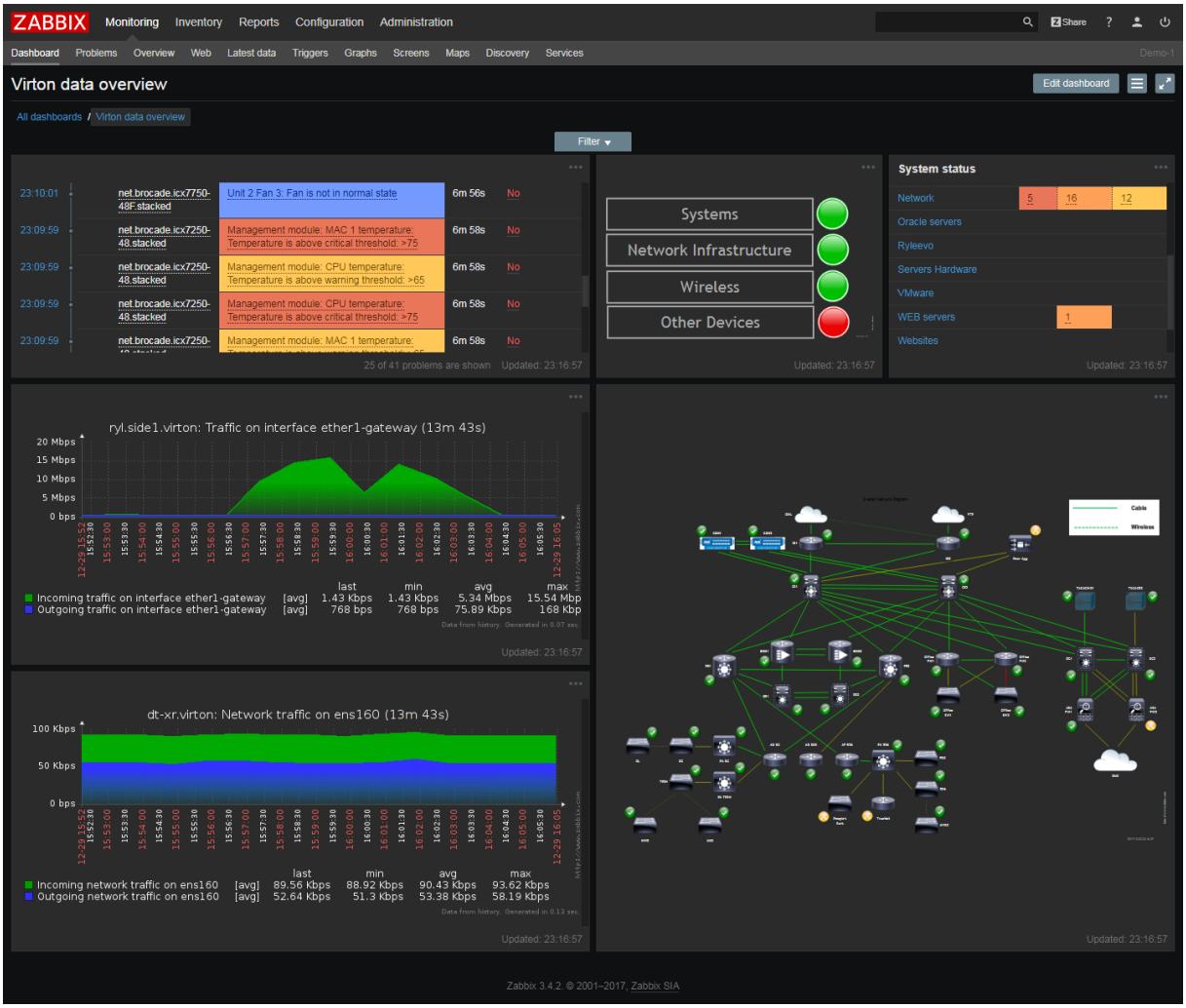
	Icinga2	Nagios	Centreon	Zabbix	Shinken
SNMP	Oui	Oui	Oui		
SNMP TRAP	Oui	Oui	Oui		
Interface graphique claire et complète	Claire et complète via l'installation de modules	Non	Oui		

Zabbix

Historique :
Zabbix a vu le jour en 1998 développé par Alexei Vladishev, sous la forme d'un projet interne, afin de répondre aux besoins de supervision d'une banque. C'est seulement à partir de 2001 que le logiciel passe sous licence GPL, avec la sortie d'une première version alpha de Zabbix 1.0. Après plusieurs années de développement, la version finale 1.0 est disponible le 23 mars 2004.
Zabbix est une application libre (open source) de supervision des systèmes et des réseaux en infrastructure IT, développée en C. L'interface web est quant à elle, développée en PHP et en JavaScript.

Fonctionnalité :
Zabbix est avec Centreon sûrement l'outil de monitoring le plus complet. S'il ne peut pas remplir une tâche, un plugin est disponible pour y remédier.

Son interface est assez intuitive et propose un système de template afin de personnaliser à son goût celle-ci.



Installation :
Il est possible d'installer Zabbix en ajoutant son repository. Son installation est donc facile ainsi que son évolutivité.

Conclusion :
À l'image de Centreon, Zabbix est un outil de supervision complet et puissant mais reste tout aussi lourd. Son interface est cependant plus complète et plus intuitive.

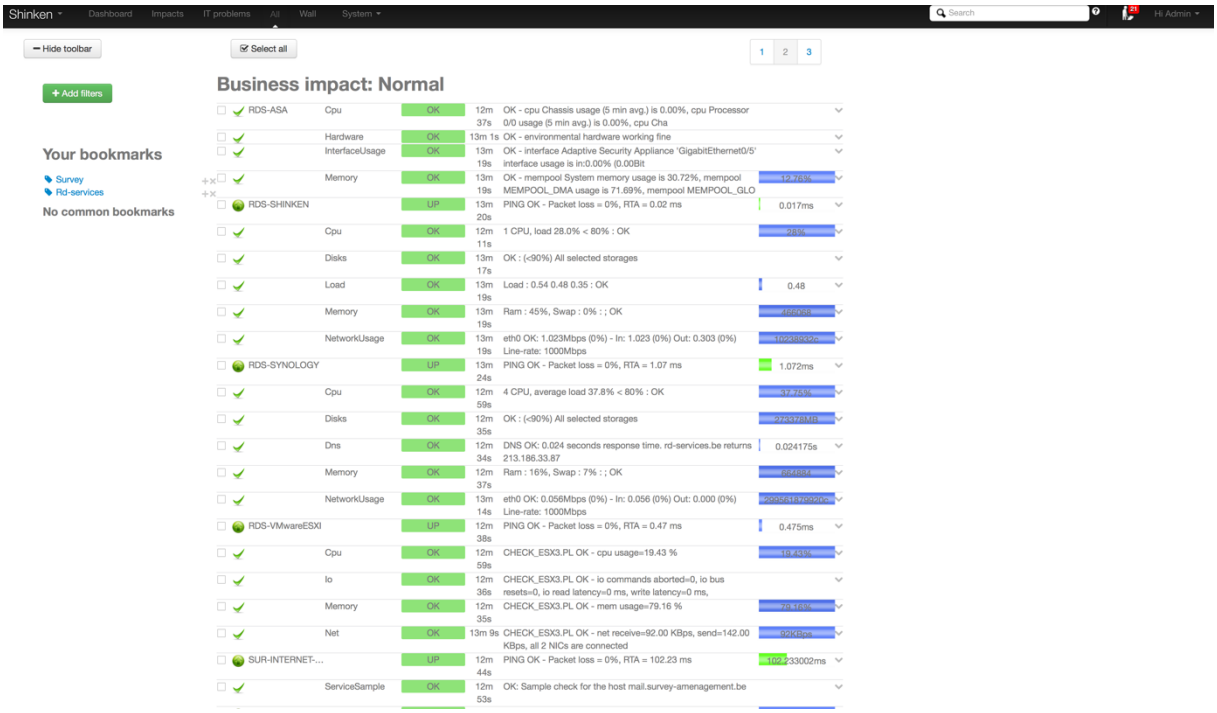
	Icinga2	Nagios	Centreon	Zabbix	Shinken
SNMP	Oui	Oui	Oui	Oui	
SNMP TRAP	Oui	Oui	Oui	Oui	
Interface graphique claire et complète	Claire et complète via l'installation de modules	Non	Oui	Oui	

Shinken

Historique :
Démarré comme une preuve de concept pour Nagios sur les architectures distribuées, le programme a rapidement démontré des performances et une flexibilité bien plus importantes que son aîné Nagios. À la suite d'un refus en décembre 2009 des développeurs de Nagios de voir Shinken devenir la nouvelle branche de développement de Nagios dans le futur. Shinken peut désormais être considéré comme un projet indépendant de système de surveillance système et réseau.
Cette solution est basée sur Nagios Core et développé en Python.

Fonctionnalité :
Shinken se veut être un outil de monitoring modulaire comme Icinga2. Il est toujours basé sur Nagios Core et reste donc compatible avec les plugins Nagios. Les fonctionnalités se rapprochent de celles d'Icinga2, elles sont donc basiques. Pour répondre à chaque problématique, il va falloir passer par des plugins.

L'interface rappelle un peu celle d'Inciga2 :



Elle reste très claire avec un nombre assez réduit de menus, contrairement à Centreon ou Zabbix.

Installation :
Shinken a besoin d'un environnement Python installé sur son OS.
Il est disponible sur Pypi, on peut donc simplement l'installer via la commande pip.

Conclusion :
Shinken est comparable à Icinga2, il propose une architecture modulaire assez intéressante, lui permettant d'être léger tout en répondant aux attentes les plus particulières .

	Icinga2	Nagios	Centreon	Zabbix	Shinken
SNMP	Oui	Oui	Oui	Oui	Oui
SNMP TRAP	Oui	Oui	Oui	Oui	Oui
Interface graphique claire et complète	Claire et complète via l'installation de modules	Non	Oui	Oui	Claire et complète via l'installation de modules