Année Universitaire : 2017 / 2018





**MESUPRES**

---------------------

**CENTRE NATIONAL DE TELE-ENSEIGNEMENT à MADAGASCAR**

---------------------

**MENTION : INFORMATIQUE**

-------------------------

**PARCOURS : RESEAUX ET SYSTEMES**

RAPPORT DE STAGE

en vue de l’obtention

du DIPLOME de Licence en Informatique Réseaux et système

**SUPERVISION RESEAUX et MONITORING des ASI**

*par* : RANARISON Hajanirina Santatra

*Encadreur Professionnel :* Monsieur HERINIAINA Naly

REMERCIEMENTS

Je tiens à exprimer ici mes sincères remerciements à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce stage de fin d’étude :

•Monsieur RAVELOMANANA Mamy : Président de l’Université d’Antananarivo.

•Monsieur DJOHARY Andrianambinina : Directeur National du CNTEMAD.

•Monsieur RAKOTOMALALA Mamy Alain : Chef de département.

•A la société JOUVE Madagascar qui m’a accueilli durant ce stage.

•Monsieur HERINIAINA Naly Responsable des Systèmes d’Information de la société JOUVE, mon encadreur professionnel, qui m’apporté de l’aide et les moyens nécessaires au bon déroulement de mon stage.

•Monsieur Antsa et Jean Fils Administrateurs Réseaux et Systèmes au sein de la société JOUVE, pour leur aide quotidienne tout au long de mon stage.

•A l’ensemble du personnel de JOUVE, pour leur accueil et pour m’avoir permis de réaliser ce stage dans un cadre agréable.

•Enfin toutes les personnes qui ont participé à la réalisation de ce stage et ce rapport.

TABLES DES MATIERES

NOTATIONS……………………………………………………………………………………....7

INTRODUCTION GENERALE…………………………………………………………………...8

CHAPITRE1 : PRESENTATION DU CNTEMAD ET L’ENTREPRISE D’ACCUEIL…………9

1. Présentation du CNTEMAD……………………………………………………………………..9

1.1. Contact et localisation………………………………………………………………….9

1.2. Présentation générale………………………………………………………………….10

1.3. Filières des formations existantes et diplômes………………………………………..10

2. Présentation du JOUVE Madagascar…………………………………………………………...12

2.1. Contact et localisation………………………………………………………………...12

2.2. Présentation générale………………………………………………………………….12

2.3. Historique de la société ………………………………………………………………12

2.4. Expertises, Missions et objectif ….…….……………………………………………13

CHAPITRE2 : PRESENTATION DU STAGE, ETUDE DE L’EXISTANT ET THEORIQUE DES SOLUTIONS………………………………………………………………………………...14

1. Présentation du stage……………………………………………………………………………14

1.1. Missions confiées……………………………………………………………………..16

1.1.1. Problématiques……………………………………………………………...16

1.1.2. Les travaux demandés……………………………………………………… 17

1.1.3. Les objectifs du stage………………………………………………………. 18

1.2. Etude de l’existant…………………………………………………………………… 18

2. Etude théorique……………………………………………………………………………… 19

2.1. Supervision ou Monitoring………………………………………………………… 19

2.1.1. Définition………………………………………………………………… 19

2.1.2. Différente niveau………………………………………………………… 19

2.1.3. Les enjeux de la surveillance réseau………………………………………. 20

2.2. Les Protocoles de supervision………………………………………………………. 21

2.2.1. ICMP………………………………………………………………………. 21

2.2.2. SNMP……………………………………………………………………… 21

2.2.2.1. Présentation générale…………………………………………….. 21

2.2.2.2. Capacités et avantages……………………………………… … 22

2.2.2.3. Les composants de SNMP……………………………………… 22

2.2.2.4. Les fonctionnements…………………………………………….. 22

2.2.2.5. Les requêtes SNMP……………………………………………… 22

2.2.2.6 Les réponses de SNMP…………………………………….. …… 22

2.2.2.7. Les alertes……………………………………………………….. 24

2.2.2.8. L’évolution de la version SNMP………………………………… 24

2.2.3. Les MIBS………………………………………………………….. 25

3. Les solutions existantes……………………………………………………………………… 26

3.1. Les logiciels Open Source…………………………………………………………… 26

3.1.1. Nagios……………………………………………………………………… 26

3.1.2. Zabbix……………………………………………………………………… 27

3.1.3. Centreon……………………………………………………………………. 27

3.1.4. Check MK………………………………………………………………….. 28

3.2. Les logiciels de monitoring propriétaires……………………………………………. 28

3.3. Le solution que nous avons choisie………………………………………… ……...29

CHAPITRE3 : REALISATION ET MISE EN PLACE DE LA SOLUTION DE SUPERVISION………………………………………………………………………………… 30

1. Environnement de travail……………………………………………………………………… 30

1.1. Environnement matériel…………………………………………………………… 30

1.1.1. Onduleur ARCHIMOD HE……………………………………………….. 30

1.1.2. L’interface réseau …………………………………………………………. 31

1.2. Environnement Logiciel…………………………………………………………… 33

2. Solution1 : Supervision de l’onduleur via l’interface web (http)…………………………… 34

2.1. Accès au CS121 de l’onduleur via la console…………………………………… 34

2.2. Accès au CS121 de l’onduleur via l’interface Web………………………………. 35

2.2.1. Configuration réseau et sécurité………………………………………… 36

2.2.2. SNMP…………………………………………………………………… 37

2.2.3. Courriel…………………………………………………………………. 37

2.2.4. Serveur de synchronisation…………………………………………… 39

2.2.5. Alarmes et Evénements……………………………………………….........39

2.2.6. Etat de l’onduleur…………………………………………………………. 40

2.2.7. Logfile…………………………………………………………………….. 40

3. Solution2 : Supervision de l’onduleur via Centreon…………………………………………. 43

3.1. Les outils de supervision……………………………………………………………. 43

3.2. Connexion à l’interface Web ……………………………………………………….. 44

3.3. Installation de Centreon-plugins…………………………………………………… 44

3.4. Création des commandes dans l’interface web centreon……………………………. 46

3.5. Création des modèles de services……………………………………………………. 47

3.6. Création d’un modèle d’hôte………………………………………………………… 49

3.7. Ajout de l’hôte ou l’onduleur à superviser………………………………………….. 50

3.8. Journaux d’événements……………………………………………………………… 52

3.9. Alerte mail…………………………………………………………………………… 53

CONCLUSION GENERALE……………………………………………………………………. 55

ANNEXE………………………………………………………………………………………… 56

BIBLIOGRAHIE………………………………………………………………………………… 67

PAGE DE RENSEIGNEMENTS...........……………………………….…………………………68 RESUME ………………………………………………………………………………………….69

NOTATIONS

Abréviations :

* ASI : Alimentation Sans Interruption
* IP  : Internet Protocol
* ICMP : Internet Control Message Protocol
* TCP : Transmission Control Protocol
* UDP : User Datagram Protocol
* SSH : Secure Shell
* VPN : Virtual Private Network
* http : Hypertext Transfer Protocol
* ARP : Adress Resolution Protocol
* DNS : Domain Name System
* SMTP : Simple Mail Transfer Protocol
* NTP : Network Time Protocol
* FTP : File Transfer Protocol
* UPSTCP : Uninterruptible Power Supply TCP

INTRODUCTION GENERALE

A la fin de la troisième année de formation informatique réseau et système au CNTEMAD, chaque étudiant doit réaliser un stage dans une entreprise. Ce stage est nécessaire afin de valider l’obtention du diplôme et a pour objectif de préparer l’étudiant à son insertion dans la vie professionnelle. Il permet de pratiquer et d’approfondir les connaissances acquises durant la formation.

Les réseaux et les systèmes d’alimentation jouent un grand rôle au bon fonctionnement de nombreux entreprises et établissements. Toute panne ou indisponibilité peut avoir une lourde conséquence au niveau financière qu’organisationnel. La supervision continue du réseau et de système d’alimentation est donc indispensable dans toute entreprise. Elle permet de voir de manière globale le fonctionnement du réseau et de prévenir les problèmes matériels et logiciels. C’est pour cela que nous avons réalisé notre stage sur « la supervision réseaux et monitoring des ASI ».

Dans ce rapport, nous commencerons par une présentation du CNTEMAD et la société JOUVE Madagascar. En suite, on va voir la présentation du stage, les problématiques, l’étude de l’existant et l’étude théorique des différentes solutions. Enfin, nous terminerons par la réalisation du projet et les résultats obtenus.

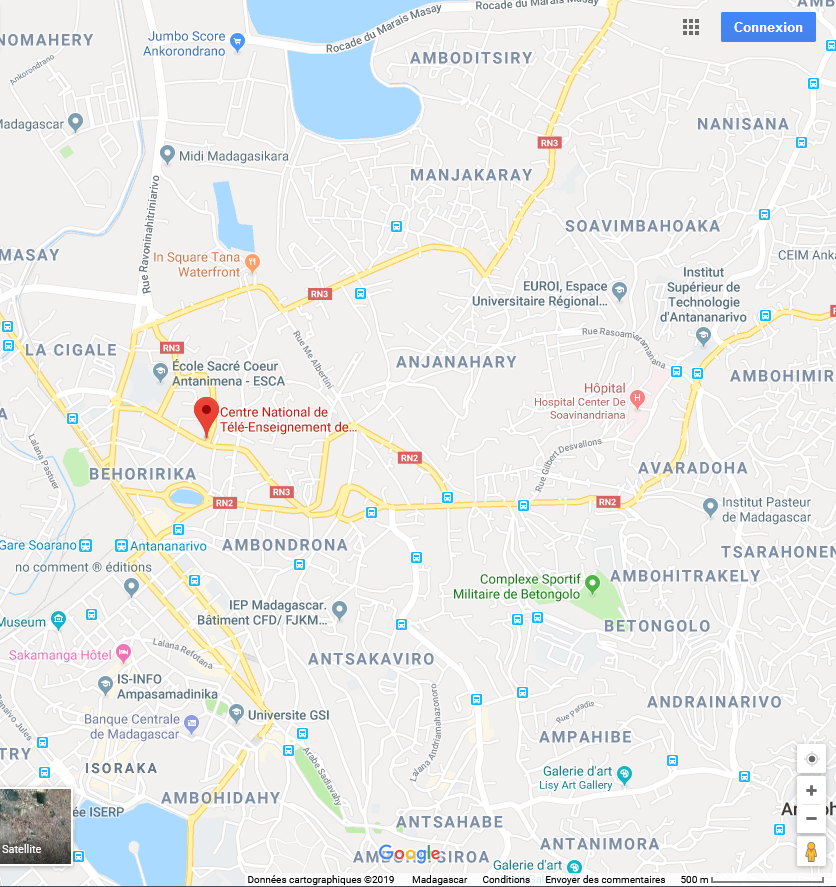
CHAPITRE 1 : PRESENTATION DU CNTEMAD ET DE L’ENTREPRISE D’ACCUEIL

Ce premier chapitre nous permet de savoir les informations concernant l’école CNTEMAD et notre entreprise d’accueil.

D’abord nous commencerons par la présentation du CNTEMAD ; sa localisation, ses formations et d’autres. En suite nous présenterons la société JOUVE Madagascar, une présentation générale, sa localisation, son histoire et ses missions.

**1. Présentation du CNTEMAD [1]**

***1.1 Contact et localisation*** [1]



***Figure 1.01*** : Localisation de CNTEMAD, google Map

L’école CNTEMAD avait plus de 33 centres régionaux répartis dans les 22 régions de Madagascar. Le siège central se situe à l’adresse Lot IVC 6 Ankadifotsy de la région Analamanga code postale 101 Antananarivo. Pour le contact, on peut envoyer une lettre à l’adresse postale P. B 78 ou appeler les numéros suivants : +261 20 22 600 57 ou +261 20 22 360 90.

***1.2 Présentation générale*** [1]

Le Centre National de Télé-Enseignement de Madagascar (CNTEMAD) est un établissement public à caractère scientifique, sous tutelle technique du MESupReS, œuvrant dans le domaine de l’enseignement supérieur, qui fut fondé, en 1992, suivant le décret 92-953 du 04/11/92, afin d’assister et d’accompagner, étroitement, l’administration des universités publiques malgaches dans leurs taches fondamentales, qui seraient : d’accueillir, de former, puis de valoriser les parcours (via les diplômes) de tout citoyen bachelier en quête de cursus universitaire.

Outre le fait de dispenser des formations universitaires habilitées aux marginalisés de l’université (marginalisés pour fautes de moyens et d’infrastructures), le CNTEMAD a œuvré pour la promotion de l’enseignement supérieur malgache, à travers le télé-enseignement, auquel il fut le pionnier. Par le biais de cette pratique, le CNTEMAD a définitivement ôté la notion d’éloignement géographique aux contraintes majeures des étudiants ; qu’il a été constaté, par conséquent, un fort accroissement du taux de fréquentation, à l’enseignement supérieur, des bacheliers. Un fait qui aurait généré une émergence surprenante de nouvelles générations d’intellectuels et de professionnels à Madagascar.

Le CNTEMAD est régi sous l’administration d’un conseil composé par des représentants : ministériels (MESupReS, MinFoP), de la fédération des chambres du commerce malgache et de l’Enseignement Supérieur malgache (présidents et doyens de facultés).

Son système d’administration est basé sur les politiques managériales d’un Directeur National, assisté par cinq sous-directeurs.

Afin d’assurer une totale couverture de la grande île en formation accréditée, le CNTEMAD est déconcentré en 34 centres régionaux de télé-enseignement.

Chaque année, on compte dans les seize mille (16.000) le nombre d’apprenants qui s’inscrivent au CNTEMAD.

***1.3 Filières des formations existantes et diplômes délivrés*** [1]

Les formations qui y sont dispensées se distinguent en deux domaines :

* Les Sciences de l’Ingénieur
* Les Sciences de la Société.

Le domaine des Sciences de l’ingénieur est étalé en trois mentions :

* Informatique :

•Base de Données et Génie Logiciel

•Réseau et Système

* Le Génie Industriel :

•Génie Electrique et Information industrielle

• Génie Industriel et Maintenance

* La Télécommunication :

•Génie des Réseaux et Transmission

• Génie des Radiocommunications

Le Second domaine est, quant à lui, étalé en :

* Droit :

•Droit Privé

• Droit Public

* Economie :

•Science Economique

•Licence professionnelle : assurance, banque, finance

•Economie et Gouvernance des Territoires

•Economie et Politique de l’Environnement et de l’Energie

* Commerce :

• Import/Export PME/PMI

•Echanges Internationaux

* Communication :

• Communication

•Information et Communication des Entreprises

* Gestion :

•Gestion Généraliste

•Gestion Spécialiste

Toutes ces mentions comprendront par la suite des ensembles de parcours, constitués par des groupes d’unité d’enseignement. Aux termes de leurs cursus, le CNTEMAD délivre à ses apprenants des diplômes de Licence ou de Master, cautionnés par le MESupRes et reconnus par le MinFop.

**2. Présentation du JOUVE Madagascar**

***2.1 Localisation***

Le siège social de la société JOUVE Madagascar se situe à Anosizato, Antananarivo,

Lot III U 134 A Ter Anosizato Est I.

***2.2 Présentation générale***

JOUVE Madagascar est une société à Responsabilité Limitée Unipersonnelle dont l’activité est le traitement de données informatiques. C’est une des filiales du groupe multinational JOUVE. Elle emploie actuellement 700 personnes répartis sur 2 sites : Antananarivo et Antsirabe.

***2.3 Historique de la société***

La société JOUVE Madagascar a été crée en 1995 et portait le nom « MADAGASCAR INFORMATIQUE SYSTEME » ou « MIS » SARL. Elle avait comme activité principale le traitement de données informatiques, opérant à titre de zone franche informatique.

Suivant le projet de rachat par le groupe JOUVE, puis la fusion au cours de l’année 2012 entre la société MIS et la société INFOSCRIBE, la dénomination à été changée par « JOUVE Madagascar » entrainant le changement du siège social à Anosizato, puis et la création du site « JOUVE Madagascar Antsirabe » entant que backup.

Actuellement, la société JOUVE Madagascar est une société à responsabilité limité unipersonnelle et emploi plus de sept cent personnes réparties sur ces deux sites, et dont l’activité reste toujours le traitement de données informatiques.

***2.4. Expertises, Missions et objectifs***

2.4.1. Expertises

La société JOUVE offre plusieurs expertises pour ses clients :

* Conseil en Stratégie et Digitale

La transformation digitale et le Data driven Strategy Consulting sont deux expertises qui garantissent les parcours digitaux et l’exploitation des données des clients.

* UX / UI, Agence Digitale

Data-driven UX : les équipes de JOUVE assurent l’exploitation des données des clients et elle apporte aussi des aides pour ses clients afin d’optimiser ses parcours d’achat et d’acquisition.

ASO et Acquisition mobile : la JOUVE accompagne ses clients dans la mise en œuvre de stratégie media et dans l’ajustement des moyens à déployer pour atteindre les résultats tout au long de ses campagnes.

* Mobile et Web

JOUVE offre 4 solutions mobiles et web pour ses clients :

•Applications Mobiles avec des technologies UX-UI, simple et personnalisée pour ciblés les utilisateurs.

•Sites Web responsive design, personnalisé et multi-langue.

•Hosting et cloud sont nécessaires pour héberger les applications et sauvegarder des données clients sensibles dans des environnements ultra sécurisés.

•IA et Maching e-learning : La JOUVE met toute son expertise au service des données cognitives et invente les usages de demain.

* Optimisation de processus métier

La JOUVE accompagne ses clients dans la transformation des processus métier en proposant des services de dématérialisation cross-canal, des plateformes de GED, des workflow documentaires.

* Data et Analytics

Ingénierie de données : transformation des données d’un état brute et de qualité variable à un état homogène et exploitable.

Big Data,SEO et Smart Search : intelligence et fiabilité deviennent critique dans la stratégie Big data des organisations

Data visualisation : l’équipe de design capitalise sur leurs outils de graphe et de visualisation pour offrir une nouvelle possibilité aux données des clients.

* Technologique

JOUVE investit chaque années dans le R&D pour résoudre les problèmes des ses clients. Ses solutions de RAD/LAD sont reconnues comme les meilleurs du marché et il est également un acteur de référence sur le contrôle et la vérification d’identité.

* Formation et e-learning

Les rédacteurs de JOUVE ont acquis une solide expertise pour rédiger des contenus et des cours pour les écoles primaire, secondaire, l’enseignement supérieur et le développement professionnel.

* Imprimé et services associés

JOUVE est le pionner de l’impression à la demande. L’imprimerie JOUVE dispose d’une force de frappe dès 50ex jusqu'à plusieurs milliers, couplant l’offset UV et le numérique noir. Il offre une impression quadrichromie haute qualité grâce à la complémentarité de offset direct drive, du jet encre et du numérique.

2.4.2. Missions et objectifs

Les missions principales de JOUVE sont :

* Accélérer les échanges des entreprises avec ses clients, fluidifies les parcours utilisateurs et développer des solutions web et mobiles robustes.
* Aident des entreprises à accélérer sa transformation digitale et proposent des usages disruptifs.
* Transforme et valorisent les données des clients et propose des datas fiables, sécurisées et validées.
* Intervenir dans les parcours digitaux des entreprises pour offrir à ses utilisateurs finaux une expérience personnalisée et fluide.

L’objectif principal est de pouvoir dominer le marché du traitement de donnée informatique à Madagascar.

Conclusion

Durant ce chapitre, nous nous sommes intéressées par la présentation de CNTEMAD et de l’entreprise d’accueil. Nous verrons dans le chapitre suivant la présentation du stage, l’infrastructure existant, les problématiques et les solutions proposés.

CHAPITRE 2 :

PRESENTATION DU STAGE, ETUDE DE L’EXISTANT ET THEORIQUE DES SOLUTIONS

Dans ce second chapitre, nous présentons en première lieu les missions confiées, les problématiques et les objectifs du stage. Ensuite, nous décrirons l’infrastructure existante du JOUVE Madagascar, et enfin une étude théorique concernant la supervision réseau et proposition de solution.

**1. Présentation du stage**

A mon arrivé chez JOUVE, j’ai été intégré dans la branche infrastructure réseau et système. Cette branche est composée de 3 personnes : le Responsable des systèmes d’informations et deux administrateurs réseaux et systèmes qui garantissent le bon fonctionnement du réseau de parc informatique de l’entreprise. Après une visite dans l’entreprise pour se familiariser avec le personnel, on m’a présenté mon projet de stage qui est la supervision réseau et des ASI (Alimentation Sans Interruption) ou onduleur. Ce stage est donc basé principalement sur la mise en place d’un outil de supervision réseaux.

***1.1. Missions confiées***

Groupe Jouve est une entreprise française de service numérique et d'impression, spécialisée dans l'acquisition, la valorisation et la diffusion d'informations. L'entreprise associe 4 métiers intégrant toute la chaîne de valeur du traitement du contenu, associés à une capacité de production industrielle importante. Elle possède un grand parc informatique composé des serveurs, des postes clients, des imprimantes, des onduleurs ... etc. la gestion de l’alimentation des équipements va donc devenir complexe s’il n’y a pas de solution de supervision pour prévenir les problèmes et les pannes. Toutes perturbations et interruptions au niveau des systèmes d’alimentation affectent directement le réseau et la qualité des services de l’entreprise.

1.1.1. Problématiques

Les 2 sites hébergent plus de 800 ordinateurs/serveurs. Pour garantir un haut niveau de disponibilité du Jouve Madagascar, la sécurité des sites repose pour une grande part sur son alimentation électrique et celle-ci doit être en conséquence hautement sécurisée. Les ASI (Alimentations statiques sans interruption), ou onduleurs, associés à des groupes électrogènes sont présents sur les 2 sites et restent essentiels, et leur technologie et leurs caractéristiques évoluent pour suivre les besoins des utilisateurs.

Nous assurons la continuité de service par:

- des tableaux MT et BT spécifiés et testés de façon à garantir les niveaux de disponibilité et de maintenabilité quelle que soit la phase du cycle de vie ;

- l’appareillage de commande et de protection intégrant des possibilités de mesure et de communication;

-des canalisations électriques préfabriquées;

-une architecture de contrôle et de monitoring associée à celle de la distribution de puissance;

- une étude de sélectivité et des réglages pour toutes les protections MT et BT des tableaux et armoires pour toutes les configurations d’alimentation : réseau, onduleurs, groupes électrogènes. Sur les sites, nous avons l'onduleur ARCHIMOD HE, un système d'alimentation sans interruption (ASI) triphasé avec la technologie PWM à haute fréquence, de type On Line à Double Conversion, architecture modulaire, possibilité de configuration N+X redondante. Il est composé de modules monophasés individuels redondants et auto-configurables, débitant une puissance nominale de 20 jusqu'à 120kW, équipé de Batteries d'accumulateurs étanches à régulation par soupape. Ces Batteries sont contenues dans l'UPS, dans un compartiment spécial, autrement dans une ou plusieurs armoires extérieures. Les ASI et leurs batteries vont assurer en cas de coupure l’alimentation des sites mais ces ASI ne sont pas monitoré et nous ne pouvons pas prévenir les pannes de cet équipement.

1.1.2. Les travaux demandés

Pour résoudre les problèmes mentionnés précédemment, le Directeur SI lance un projet de supervision de l’onduleur ARCHIMOD HE. Ce projet a pour but de surveiller l’état global de l’onduleur et de ses batteries.

Nos travaux se divisent en plusieurs parties :

* L’analyse des besoins
* L’étude de faisabilité
* Proposition des solutions
* Installation et paramétrages
* Configuration sur Centreon
* Test et essai
* Rédaction du compte rendu

1.1.3. Les objectifs du stage

Les différents objectifs de notre projet sont :

- Faire en sorte que l'onduleur ARCHIMOD HE soit accessible via la console et en réseau via l'interface web

- Superviser l'onduleur via Centreon par la surveillance des sondes

- Créer un alerte mail en cas de défaillance de l'onduleur

- Visualiser l'état des batteries (état d'utilisation et état des matériels)

***1.2 Etude de l’existant***

Le système d’alimentation de la société JOUVE Madagascar est composé de :

- Source d’entrée triphasée venant de la JIRAMA

- Des groupes électrogènes qui assurent l’alimentation des sites en cas de coupure de l’électricité de la JIRAMA

- Des onduleurs pour éviter les interruptions

Avant chaque poste/serveur de la société JOUVE est équipée d’un petit onduleur qui assure leur disponibilité en cas de coupure de l’électricité. La maintenance et la surveillance des onduleurs sont des tâches très difficiles à cause de leurs nombres. Pour améliorer le système d’alimentation, la société JOUVE a décidé de remplacer les petits onduleurs par un onduleur modulaire ARCHIMOD HE d’une puissance de 20KVA à 120KVA pour alimenter tous les postes dans le site. ARHIDMOD HE est un onduleur modulaire triphasé doté d’une interface réseau CS121 et une interface pour le monitoring.

**2. Etude théorique**

Une fois la présentation du stage faite et l’infrastructure existante exposée, il fallait trouver des solutions pour résoudre notre problématique. Nous allons donc voir quelques études théoriques concernant les techniques existantes dans le domaine de supervision réseau.

***2.1. Supervision ou Monitoring*** [5]

2.1.1. Définition [2]

Le monitoring est l’anglicisme du terme surveillance et définit la mesure d’une activité (humaine, économique, électrique, d’un organe, etc.). En informatique, le monitoring désigne la mesure (et parfois les systèmes ou appareils de mesure) d’un système électronique ou électrique dans le cadre de la supervision d’un parc.

La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l’état des réseaux et de leurs composants. Ces données seront ensuite traitées et affichées afin de mettre en lumière d’éventuels problèmes.

La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d’alerte (email ou SMS par exemple) les administrateurs.

Plusieurs actions sont ainsi réalisées : Acquisitions de données, analyse, puis visualisation et réaction.

Un tel processus est réalisé à plusieurs niveaux d’un parc de machines : Au niveau interconnexions (Réseau), au niveau de la machine elle-même(Système) et au niveau des services offerts par cette machine (Applications).

2.1.2. Différente niveau

Supervision réseau :

Par le terme réseau on entend ici l’aspect communication entre les machines. Le rôle est de s’assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d’erreurs). C’est dans ce cadre que l’on va vérifier par exemple si une adresse IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.

Supervision système :

La surveillance se cantonne dans ce cas à la machine elle-même et en particulier ses ressources. Si l’on souhaite par exemple contrôler la mémoire utilisée ou la charge processeur sur le serveur voir analyser les fichiers de logs système.

Supervision applicative :

Cette technique est plus subtile, c’est elle qui va nous permette de vérifier le fonctionnement d’une application lancée sur une machine. Cela peut être par exemple une tentative de connexion sur le port de l’application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l’analyse de logs applicatifs.

2.1.3. Les enjeux de la surveillance réseau

La surveillance continue de son réseau informatique est indispensable dans toute entreprise à partir de quelque dizaine de personnes. C’est une taille critique à partir de laquelle une panne de réseau peut entraîner une perte d’activité préjudiciable pour l’entreprise. A titre d’exemple, si un réseau est indisponible ou difficilement accessible 1% du temps alors c’est 87h de travail qui est impactées (à multiplier par le nombre d’employés).

Il est donc très important de pouvoir détecter les risques d’incidents ou les optimisations à réaliser avant de faire face à un problème technique grave.

La surveillance de l’activité réseau permet par ailleurs d’être correctement informé en cas de problème et de mettre en place le bon plan d’action rapidement.

L’autre volet de la supervision réseau concerne la sécurité de celui-ci. En effet, la cybercriminalité, les virus, les phishing et d’autres intrusions causent des dommages qui s’élèvent à quasiment plusieurs millions. Pour lutter efficacement contre ces attaques en constante augmentation (particulièrement sur les réseaux mobiles), la DSI doit se munir de technologies lui permettant de connaître ses forces, ses faiblesses mais aussi de pouvoir réagir vite lors d’une tentative. Le rôle de la supervision est donc de garantir un niveau de qualité continu souvent

nommé SLA pour Service Level Agreement, prévenir les risques de rupture de services, d’intrusion et réagir vite aux incidents.

***2.2. Les protocoles de supervision***

Il existe des protocoles réseau qui permettent de récupérer des informations sur le parc informatique. Nous allons en étudier deux particulièrement importants qui possèdent des rôles très différents mais qui ont un point en commun : ils sont tout deux largement utilisés par les logiciels de supervision.

2.2.1. ICMP (Internet Control Message Protocol)

ICMP est un protocole de couche réseau (coche 3 du modèle OSI) qui vient palier à l’absence du message d’erreur du protocole IP (Internet Protocol). En effet si il ya un incident de transmission les équipements intermédiaires vont utiliser ce protocole pour prévenir la machine émettrice. Les paquets ICMP sont encapsulés dans des paquets IP (malgré qu’ils soient au même niveau OSI), et peuvent contenir des bouts de paquets IP pour citer celui ayant généré l’erreur.

Afin de catégoriser les erreurs, elles sont divisés en types eux-mêmes parfois redivisés en codes. Par exemple le type 3 représente un destinataire inaccessible : il existe 16 codes différents en fonction de la raison pour laquelle le destinataire n’est pas joignable.

C’est un protocole très simple, qui n’a pas pour fonction directe la supervision d’un réseau mais qui est utilisé comme source d’information sur la qualité du réseau ou sur la présence d’une machine.

2.2.2. SNMP (Simple Network Management Protocol) [4]

2.2.2.1. Présentation générale

SNMP c’est un protocole de gestion de réseaux proposé par l’IETF 1988, il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux.

SNMP est un protocole relativement simple mais il est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications, les bases de données, les serveurs, les logiciels, etc.

C’est un standard pour TCP/IP.



***Figure 2.01*** : Fonctionnements SNMP

2.2.2.2. Capacités et Avantages

Permet de répondre à un grand nombre de besoins :

Capacité

-Disposer d’une cartographie du réseau,

-Fournir un inventaire précis de chaque machine,

-Mesurer la consommation d’une application,

-Signaler les dysfonctionnements

Avantages

-Protocole très simple, facile d’utilisation,

-Permet une gestion à distance des différentes machines,

-Le modèle fonctionnel pour la surveillance et pour la gestion est extensible,

-Indépendant de l’architecture des machines administrées.

2.2.2.3. Les composants de SNMP

-Eléments actifs du réseau : c’est les équipements ou les logiciels que l’on cherche à gérer.

- Des agents SNMP : chargés de superviser un équipement. Ils sont installés sur tout type d’équipement.

-La station de supervision (manager) : exécute les applications de gestion qui contrôlent les éléments réseaux.

-La MIB (Management Information Base) : collection d’objets résidant dans une base d’information virtuelle.

-Le protocole : permet à la station de supervision d’aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments.

2.2.2.4. Les fonctionnements

-Le protocole SNMP est basé sur un fonctionnement asymétrique. Il est constitué d’un ensemble de requêtes de réponses et d’un nombre limité d’alertes.

-Le manager envoie des requêtes è l’agent, lequel retourne des réponses. Lorsqu’un événement anormal surgit sur l’élément réseau, l’agent envoie une alerte (trap) au manager.

SNMP utilise le protocole UDP [RFC768]

-Le port 161 est utilisé par l’agent pour recevoir les requêtes de la station de gestion.

-Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents.

2.2.2.5. Les requêtes SNMP

-GetRequest permet la recherche d’une variable sur un agent.

-GetNextRequest permet la recherche de la variable suivante.

-GetBulk permet la recherche d’un ensemble de variables regroupées.

-SetRequest permet de changer la valeur d’une variable sur un agent.

2.2.2.6. Les réponses de SNMP

A la suite de requêtes, l’agent répond toujours par GetReponse. Toutefois si la variable demandée n’est pas disponible, le GetReponse sera accompagné d’une erreur noSuchObject.

2.2.2.7. Les alertes (traps, notifications)

Les alertes sont envoyées quand un événement attendu se produit sur l’agent.

Celui-ci en informe la station de supervision via une trap. Les alertes possibles sont : ColdStart, WarmStart, LinkDown, LinkUp, AuthentificationFailure.

2.2.2.8 L’évolution de la version SNMP

Voici les différentes versions de SNMP :

-SNMPv1 (ancien standard) : Ceci est la première version du protocole, tel que définie dans la RFC1157. On dit que la sécurité de cette version est triviale, car la seul vérification qui est faite est basée sur la chaîne de caractères « community ».

-SNMPsec (historique) : Cette version ajoute de la sécurité au protocole SNMPv1. La sécurité est basée sur des groupes. Très peu ou aucun manufacturier n’a utilisé cette version qui est maintenant largement oubliée.

-SNMPv2p (historique) : Beaucoup de travaux on été exécutés pour faire une mise à jour de SNMPv1. Ces travaux ne portaient pas seulement sur la sécurité. Le résultat est une mise à jour des opérations du protocole, des nouvelles opérations, des nouveaux types de données. La sécurité est basée sur les groupes de SNMPsec.

-SNMPv2c (expérimental) : Cette version du protocole est appelé « community stringbased SNMPv2 ». Ceci est une amélioration des opérations de protocole et des types d’opérations de SNMPv2p et utilise la sécurité par chaine de caractères « community » de SNMPv1.

-SNMPv2u (expérimental) : Cette version du protocole utilise les opérations, les types de données de SNMPv2c et la sécurité basée sur les usagers.

-SNMPv2\* (expérimental) : Cette version combine les meilleures parties de SNMPv2p et SNMPv2u. Les documents qui décrivent cette version n’ont jamais été publiés dans 12 les RFC. Des copies de ces documents peuvent être trouvées sur le site web et SNMP Research (un des premiers à défendre de cette version).

-SNMPv3 (standard actuel) : Cette version comprend une combinaison de la sécurité basée sur les usagers et les types et les opérations de SNMPv2p, avec en plus la capacité pour les « proxies ». La sécurité est basée sur ce qui se trouve dans SNMPv2u et SNMPv2\*.

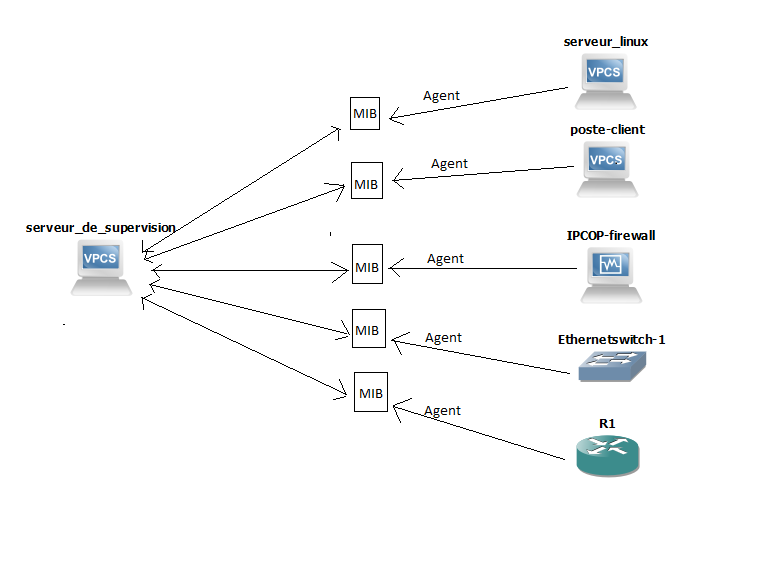
2.2.3. Les MIBS

La MIB (Management Information Base) est une base de données des informations de gestion maintenue par l’agent, auprès de laquelle le manager va venir pour s’informer.

Deux MIB publics ont été normalisées : MIB I et MIB II (dite 1 et 2). Un fichier MIB est un document texte écrit en langage ASN.1 (Abstarct Syntax Notation 1) qui décrit les variables, les tables et les alarmes gérées au sein d’une MIB.

La MIB est une structure arborescente dont chaque nœud est défini par un nombre ou OID (Object Identifier). Elle contient une partie commune à tous les agents SNMP en général, une partie commune à tous les agents SNMP d’un même type de matériel et une partie spécifique à chaque constructeur. Chaque équipement à superviser possède sa propre MIB. Non seulement la structure est normalisée, mai également les appellations des diverses rubriques.

Pour interroger les différentes variables d’activité sur un appareil, il faudra explorer son arborescence MIB. Pour accéder aux variables souhaitées, on utilisera l’OID qui désigne l’emplacement de la variable à consulter dans la MIB.



***Figure 2.02*** : Récupération des MIBs

**3. Les solutions existantes**

Une supervision efficace passe par des logiciels de monitoring qui centralisent l’information de la santé du réseau pour le compte des directions des systèmes d’information. Voici les logiciels Open Source et propriétaires les plus populaires.

***3.1. Les logiciels Open Source*** [3]

3.1.1. Nagios

(Anciennement Net Saint) est un logiciel de supervision de réseaux crée 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 configuration très poussées. La modularité et la forte communauté (>250 000) qui gravite autour de Nagios (en participant au développement de nombreux plugins et addons) offrent des possibilités en terme de supervision qui permettent aujourd’hui de pouvoir superviser pratiquement n’importe quelle ressource.

Les avantages :

-Supervision à distance peut utiliser SSH ou un tunnel SSL (notamment via un agent NRPE).

-Les plugins sont écrits dans les langages de programmation les plus adaptés à leurs tâches : scripts shell (Bash, ksh, etc.), C++, Perl, Python, Ruby, PHP, c#.

-La remontée des alertes est entièrement paramétrable grâce à l’utilisation de plugins (alerte par courrier électronique, SMS, etc..).

Les inconvénients :

-Difficile à installer et à configurer

-Dispose d’une interface compliquée

-Ne permet pas d’ajouter des hôtes via web

-Besoin d’un autre outil comme CACTI pour faciliter sa configuration

-Pas de représentations graphiques

-Les mises à jour de la configuration se font en mode « lignes de commandes » et doivent être réalisées côté supervision comme côté serveur à superviser.

3.1.2. Zabbix

C’est un outil de supervision ambitionnant de concurrencer Nagios et MRTG. Il fait la supervision technique et applicative, offre des vues graphiques (générés par RRDtools) et des alertes sur seuil. C’est une solution de monitoring complète embarquant un front-end web, un ou plusieurs serveurs distribués, et des agents multiplateformes précompilés (windows, linux, AIX, Solaris). Il est également capable de faire du monitoring SNMP et IPMI ainsi que la découverte de réseau. Il repose sur du C/C++, PHP pour la partie front end et MySQL/PostgresSQL/Oracle pour la partie BDD.

Les avantages :

-Richesse des sondes et tests possibles (supervision d’application web par exemple).

-Réalisation de graphiques, cartes ou screens. Configuration par le GUI (interface graphique).

-Mise à jour de la configuration via l’interface web Zabbix.

-Serveur Proxy Zabbix. Surveillances des sites web : temps de réponse, vitesse de transfert…

-Ses agents sont assez légères (écrits en C)

Les inconvénients :

-Interface est un peut vaste. La mise en place des templates n’est pas évidente au début : petit temps de formation nécessaire.

-L’agent zabbix communique par défaut en clair les informations, nécessite de sécuriser ces données (via VPN par exemple).

-Peu d’interfaçage avec d’autres solutions commerciales.

3.1.3. Centreon

(Anciennement Oreon). Crée en 2003 par les 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.

Les avantages :

-Une installation complète et automatique des packages nécessaire à l’utilisation de Nagios.

-Facilite la configuration de Nagios.

-Une découverte automatique du réseau via NMAP.

-affiche en Graphe le résultat des alertes, système de reporting.

Les inconvénients :

Nécessite plus de ressources matérielles que Nagios.

3.1.4. Check\_Mk

C’est une solution de Supervision open source développée par Mathias KETTNER en 2008. En réalité c’est une extension de Nagios qui est l’outil de monitoring le plus connu et le plus utilisé dans les entreprises.

Les avantages :

-Installation et configuration facile

-L’interface web est beaucoup plus intuitive et qui intègre des outils, comme PNP4Nagios et RRDTtool.

-L’interface permet une configuration entièrement graphique.

-check\_mk est capable de réaliser un inventaire automatique des services desponibles sur un hôte à superviser.

-Pas besoin de redéveloppé des sondes.

Les inconvénients :

Offre plus de services sur l’environnement Unix.

***3.2. Les logiciels de monitoring propriétaires (payants)*** [5]

A côté des outils de visualisation et de monitoring open source, les solutions propriétaires payantes sous licence comme PRTG (Paessler), OpManager ou Dynatrace sont souvent sollicitées par les entreprises avec des besoins de surveillance réseau plus avancés.

Les avantages :

* Solutions plus globales
* Périmètres techniques et fonctionnels étendus
* Support présent et réactif

Les inconvénients :

* Coût d’acquisition et de support parfois élevés
* Incompatibilités entre fournisseurs (plusieurs produits différents)
* Développements additionnels restreints et coûteux.

***3.3 La solution que nous avons choisie***

Après avoir vu toutes les solutions existantes que ce soit open source ou propriétaire nous avons décidé d’utiliser Centreon. C’est une solution open source facile à mettre en œuvre avec beaucoup de communauté en ligne en cas de problème.

CONCLUSION

Nous avons vu dans la première partie ce chapitre la présentation de stage, les problématiques, l’infrastructure existant et l’étude théorique concernant la supervision et monitoring réseau. Ensuite, les différentes solutions de supervision avec les avantages et inconvénients qui nous avons permis de choisir la solution adapté a notre problématique.

CHAPITRE 3 : REALISATION  ET MISE EN PLACE DE SOLUTION DE SUPERVISION

Dans ce dernier chapitre, nous nous intéresserons à la description des étapes de réalisation de notre solution. Nous commencerons par la description des différents environnements de travail, matériels et logiciels. Ensuite, nous décrivons les étapes de l’installation et paramétrage. Enfin, la supervision de l’onduleur via l’interface web du CS121 et Centreon.

**1. Environnement de travail**

***1.1. Environnement matériel***

Durant notre projet, nous avons eu à notre disposition :

* Un ordinateur portable
* Un ordinateur de bureau
* L’onduleur ARCHIMOD HE
* L’interface réseau CS121
* Câbles réseaux

1.1.1. Onduleur ARCHIMOD HE : [6]

ARCHIMOD HE : onduleur à architecture modulaire et extensible, avec des puissances de 20 à 120 kVA, dans une armoire rack 19".

Le système est constitué d’un ensemble de composants standard et pré-assemblés qui permettent de simplifier et d’optimiser l’étude et la réalisation des infrastructures.

La conception modulaire innovante de ces onduleurs permet d’optimiser la disponibilité de la puissance, d’augmenter la flexibilité du système et de réduire le coût total de gestion (TCO).

Module de commande: Doté d'un microprocesseur, il gère 3 modules de puissance. S’il est associé à un module d’extension de puissance, il peut en gérer jusqu’à 6, augmentant ainsi la puissance de 20 à 40 kVA. Il est doté d’un écran et d’un clavier multifonction pour surveiller les paramètres de fonctionnement de l’onduleur et pour configurer de nombreuses fonctions. Il peut être relié en parallèle à d’autres modules de commande et associé à des modules d’extension de puissance. Un indicateur d'état, rétro-éclairé, en face avant, permet un contrôle immédiat de l'état de fonctionnement du système et un port RS 232 permet de connecter un PC pour la maintenance.

Modules de puissance**:** Avec une puissance nominale de 6,7 kVA, les modules de puissance sont extrêmement compacts et maniables. Dotés d'un système plug-in et hot swap (remplaçable à chaud), ils permettent une installation et une maintenance rapides. Ils travaillent en parallèle avec tous les modules présents pour garantir la meilleure performance au système.

Module extension de puissance: Il doit être associé à un module de commande. Il permet d'augmenter la puissance de 20 à 40 kVA et d’établir une redondance individuelle sur chaque phase.

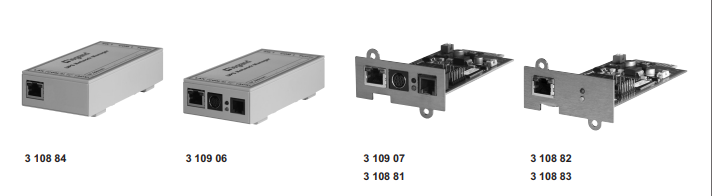
Modules batteries: Chaque module contient des batteries qui peuvent être branchées en série, formant ainsi des chaînes indépendantes ; chaque batterie présentant par ailleurs un très faible voltage CC gage de sécurité. La compacité et la fonctionnalité du module individuel (plug-in) facilitent sa manutention et les opérations d'extension sont possibles sans aucune modification de la structure du système installé.

Module distribution**:** Il permet de configurer la typologie de distribution de l'onduleur (triphasé-triphasé, triphasé-monophasé, monophasé-monophasé ou monophasé-triphasé). Il intègre les bornes de raccordement entrées/sorties, les organes de manœuvre et de protection, et la connexion pour les armoires de batteries supplémentaires. L’alimentation peut être configurée sur deux sources d’entrée séparées (principale et secourue).

Entrée des câbles: Des gaines spéciales permettent l’entrée des câbles d'entrée et de sortie, aussi bien par le haut que par le bas.

1.1.2. L’interface réseau CS121 : [7]

Le CS121 est un agent SNMP qui palie aux problèmes de distance entre un onduleur et le réseau informatique. Il se décline en 2 versions: le CS121SC et CS121BSC proposé sous forme de carte à insérer dans l'onduleur et le CS121L sous forme de boîtier externe.



***Figure 3.01*** : types carte CS121

Caractéristiques :

Haute-technologie**:** Processeurs RISC 32-Bit, Ethernet auto-détection 10/100 Mbit, 2 interfaces série RS-232 (sauf version « B »), port AUX pour 4 contacts secs de sortie/entrée pour alarmes externes (sauf version « B »).

Processeur de synchronisation et d'ordonnancement : Le processeur de synchronisation et d'ordonnancement basé sur internet permet de programmer l'on/off de la sortie Onduleurs ou des prises ou de lancer des tests de la batterie. Ceci garantit que l'Onduleurs effectue des tests réguliers de la batterie et informe l'utilisateur de tout problème par e-mail, fichier journal, etc.

Interfaces graphiques et non graphiques : Les différentes options disponibles pour la supervision et la configuration de l'adaptateur sont visuelles : Windows UPSMON, JAVAMON, UNMS, tout type de station de supervision du réseau SNMP, navigateurs internet; et non visuelles : TELNET, FTP. Le dispositif supporte également GENEREX API. L'analyse statistique est représentée graphiquement à travers le plugin GCHART pour Microsoft Internet Explorer. Ces statistiques indiquent les données de l'Onduleurs et de tous les dispositifs externes connectés, telles que la température, l'humidité, etc.

Journal : Les valeurs mesurées et les alarmes sont écrites avec des timbres horodateurs sur la mémoire rémanente de l'adaptateur CS121. La fonction de synchronisation garantit l'écriture de tous les protocoles avec des données temporelles précises.

Fonction graphique et statistiques : Le serveur CS121 fournit à ses utilisateurs une visualisation simple pour la large gamme de fonctions offertes par ses capacités de supervision et de configuration. L'adaptateur CS121 possède également le meilleur outil d'analyse graphique pour l'évaluation dynamique des données dans sa catégorie.

Services Réseau : Logiciel UPSMAN compatible pour la gestion des Alarmes. Supporte SNMP, HTTP, Telnet, ARP, TCP, UDP, DNS, SMTP, NTP, FTP, UPSTCP (UPSMON, UNMS), RCCMD, RCCMD2 (Outil d'arrêt du Multiserveur/Multi-OS et de messagerie). Base standard pour le nouveau système de gestion de réseau UNMS 2.

Email : Le client Email intégré via SMTP peut être configuré pour relayer tous les messages ou les messages Onduleurs sélectionnés. Le client Email peut également utiliser les options de messagerie du réseau pour distribuer l'information ou utiliser les fonctions internes de messagerie électronique du réseau. Compatible avec les systèmes de messagerie électronique SMTP tels que MS Exchange, Lotus et bien d'autres.

SNMP I HP OpenView : Inclut un Snap-In gratuit pour HP OpenView pour Windows. Le CS121 supporte les extensions RFC1628 MIB (Onduleurs MIB Standard) et MIB pour l'utilisation avec SITEMANAGER, SITESWITCH 4, et SENSOR MANAGER. Cela permet à l'adaptateur CS121 d'exploiter de manière optimale l'information collectée depuis les autres dispositifs disponibles à travers SNMP, comme l'ont démontré les tests effectués avec Sun Net Manager, IBM NetView, Tivoli, Unicenter, Cabletron Spectrum, ManageWise, Castle Rock et de nombreux autres systèmes de gestion de réseau basés sur SNMP. Il supporte également Ipswitch Whats UP 6 et HP/COMPAQ InsightManager.

***1.2. Environnement logiciel***

Après avoir présenté l’environnement matériel de développement, nous allons décrire brièvement les choix de logiciel et système d’exploitation utilisé.

PuTTY : est un émulateur de terminal UNIX qui permet de se connecter à distance à une machine ou un serveur, en utilisant les protocoles SSH, Telnet ou Rlogin.

Telnet : est un protocole permettant d'émuler un terminal à distance, cela signifie qu'il permet d'exécuter des commandes saisies au clavier sur une machine distante. L'outil Telnet est un implémentation du protocole Telnet, il s'agit de la traduction des spécifications en langage informatique pour créer un programme permettant d'émuler un terminal.

VMware ESXi Server : est un logiciel de virtualisation d’ordinateur développé par VMware Inc. ESXi Server est une version avancée et plus compacte de VMware ESX Server, le logiciel de virtualisation d’ordinateur de niveau entreprise de VMware. Mis en œuvre dans l'infrastructure VMware, ESXi peut être utilisé pour faciliter la gestion centralisée des applications de postes de travail et de centres de données d'entreprise.

En ce qui concerne les systèmes d’exploitation, nous avons décidé d’installer l’image iso de centreon inclus dans Centos 7 sur la VMware ESXi pour le serveur et d’utiliser windows 7 sur le poste de supervision.

**2. Solution 1 : Supervision de l’onduleur via interface WEB (http)**

***2.1 Accès au CS121 de l’onduleur via la console***

Schéma de la solution :



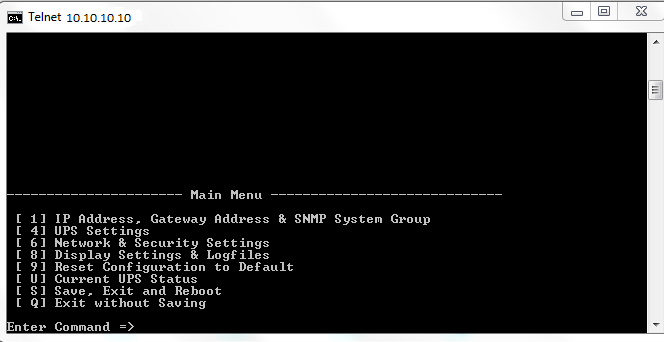
***Figure 3.02*** : Câblage de CS121 sur un ordinateur portable

En premier lieu, nous devons insérer la carte CS121 sur son emplacement dans l’onduleur après avoir modifié les commutateurs 1 et 2 en position OFF comme décrit le manuel d’utilisation. Une fois la carte connectée à l’onduleur, le voyant rouge sur la carte s’allume qui indique la procédure de démarrage. Au bout de trois minutes, le voyant vert clignote indique que la communication entre la carte et l’onduleur est établie.

Ensuite, on relie la carte et l’ordinateur portable avec un câble réseau croisé. Les voyants vert et jaune intégrés au connecteur RJ45 qui clignotent signale l’établissement de la connexion.

Pour la configuration de l’adresse IP, la CS121 est configurée par défaut 10.10.10.10 donc nous allons mettre l’ordinateur portable sur la même plage d’adresse IP que la carte en lui donnant l’adresse 10.10.10.11.

Après la configuration, on exécute une commande ping à partir de l’ordinateur portable pour vérifier si la CS121 est accessible. Si le test ping est réussi, on peut maintenant accéder l’onduleur via console en utilisant Telnet.



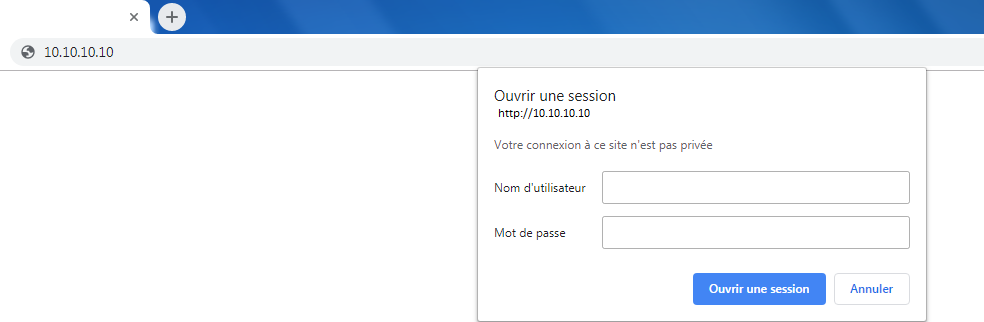
***Figure 3.03*** : Accès au CS121 avec Telnet

Nous pouvons utiliser Telnet pour faire toutes les configurations et la supervision de CS121 via console.

***2.2. Accès au CS121 de l’onduleur via interface Web (http)***

Toutes les configurations peuvent effectuées via Telnet, mais je préfère utiliser l’interface web car c’est plus pratique.

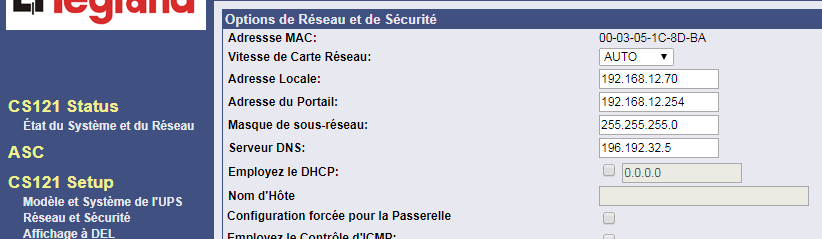
Pour accéder au CS121 via http, on va utiliser le même nom d’utilisateur et mot de passe que Telnet sur l’adresse http://10.10.10.10.



***Figure 3.04*** : Accès au CS121 via interface web

2.2.1. Configuration réseau et sécurité

Une fois connecté au CS121, on va aller sur le menu « Modèle et système » UPS pour configurer les informations de l’onduleur. En suite, dans le menu « Réseau & Sécurit& » nous devons spécifier les nouveaux paramètres réseaux de l’adaptateur CS121. Cette configuration obligatoire pour intégrer l’onduleur dans l’architecture réseau existante de l’entreprise.



***Figure 3.05*** : Configuration paramètre réseau CS121

Après toutes les modifications, il faut appliquer les paramètres avec le bouton à droite et passer au menu « Enregistrer la configuration  ». Dans ce menu, on clique sur « Sauvegarder, sortir & redémarrer » et laisser la fenêtre du navigateur web ouverte environ trois minutes pour éviter la perte des données pendant le redémarrage.

Pour activer la configuration du réseau précédant, la carte CS121 doit être retirée de l’onduleur et il faut modifier le commutateur 1 en position ON. On remet la carte dans son loge et attendre à nouveau le démarrage.

Normalement la carte n’est plus accessible avec l’adresse IP par défaut, nous utilisons maintenant l’adresse IP: 192.168.12.70 pour accéder la carte sur le réseau local.

. 2.2.2. SNMP

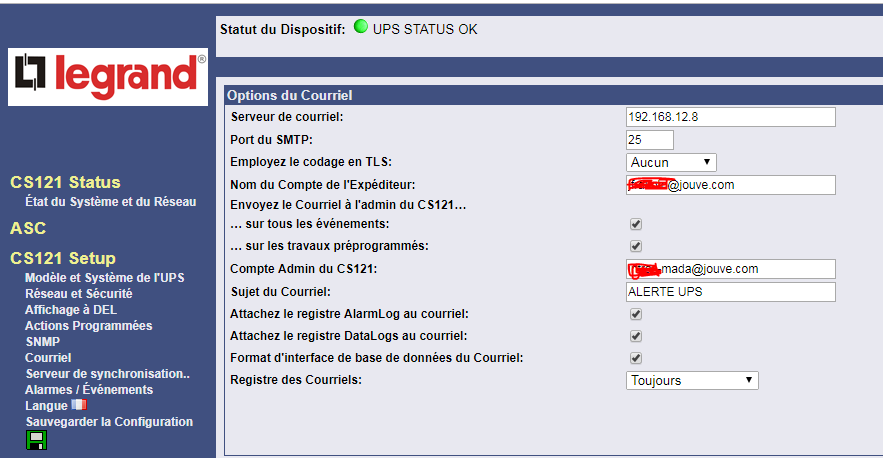
Dans ce menu, on définie les contrôles d’accès pour les communautés SNMP. Nous ne modifions pas sa valeur par défaut donc on va utiliser la SNMP v2.

2.2.3. Courriel

La configuration du courriel est très importante pour les alertes mails en cas de changement d’état de l’onduleur.

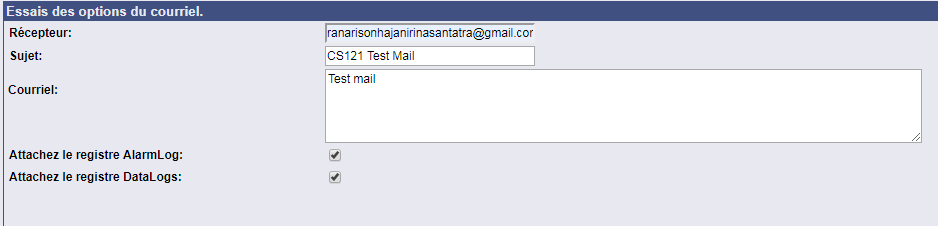
Un alerte mail est un service d’envoi automatisé d’un courrier électronique à partir d’une demande d’alerte spécifiée par un appareil (panne, changement d’état, etc). Dans notre cas l’alerte mail sert à notifier les administrateurs systèmes en cas de défaillance de l’onduleur, l’état de la batterie et plein d’autres événements qui pourrait se passer.

L’adresse IP du serveur de messagerie doit être entrée dans la case serveur de courriel et on doit spécifiés le nom de l’expéditeur et le compte administrateur qui va recevoir tous les alertes mails. On peut aussi authentifier les emails envoyé pour la sécurité.



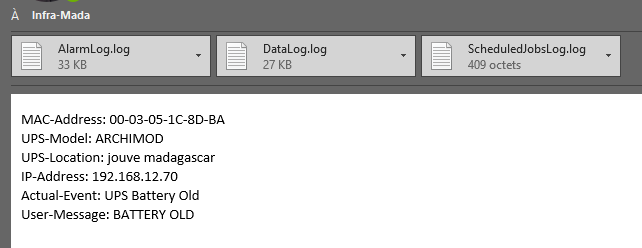
***Figure 3.06*** : Configuration du serveur de messagerie

Avec l’option « Essais du courriel », on peut faire des tests mail pour vérifier notre configuration.



***Figure 3.07*** : Test mail

Un exemple d’alerte mail :



***Figure 3.08*** Exemple alerte mail

2.2.4. Serveur de synchronisation

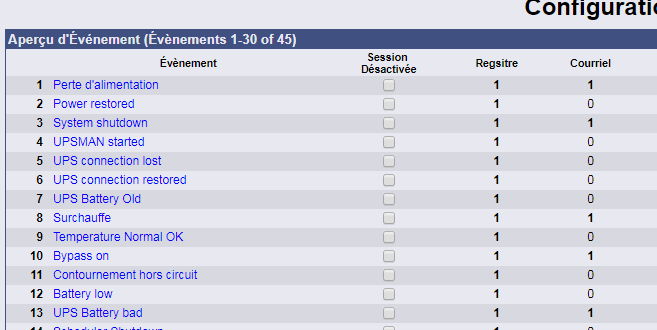
Le serveur de temps est important pour synchroniser le fichier journal de l’onduleur avec l’heure réelle. L’adaptateur peut prendre en charge jusqu’à trois adresse IP de serveur de temps différentes. On peut utiliser des serveurs du temps sur internet mais dans ce projet j’ai choisi de configurer manuellement l’heure du système.

2.2.5. Alarmes et Evénements

Les pages «alarmes et événements» sont la fonctionnalité principale de la configuration du CS121 et basées sur une combinaison d’événement et action.

Dans CS121, divers événements sont définis, comme par exemple «Powerfail», «UPS battery bad», «battery low», etc. Chaque évènement passé dans l’onduleur nous crée une action et écrit un log dans le fichier journal des alarmes.

Pour configurer nos événements et actions, on ouvre le menu «Evénements/alarmes». Le menu “Event Configuration ”affiche une vue d'ensemble sur les événements et les nombres d'actions configurées.



***Figure 3.09*** : Liste Evènements

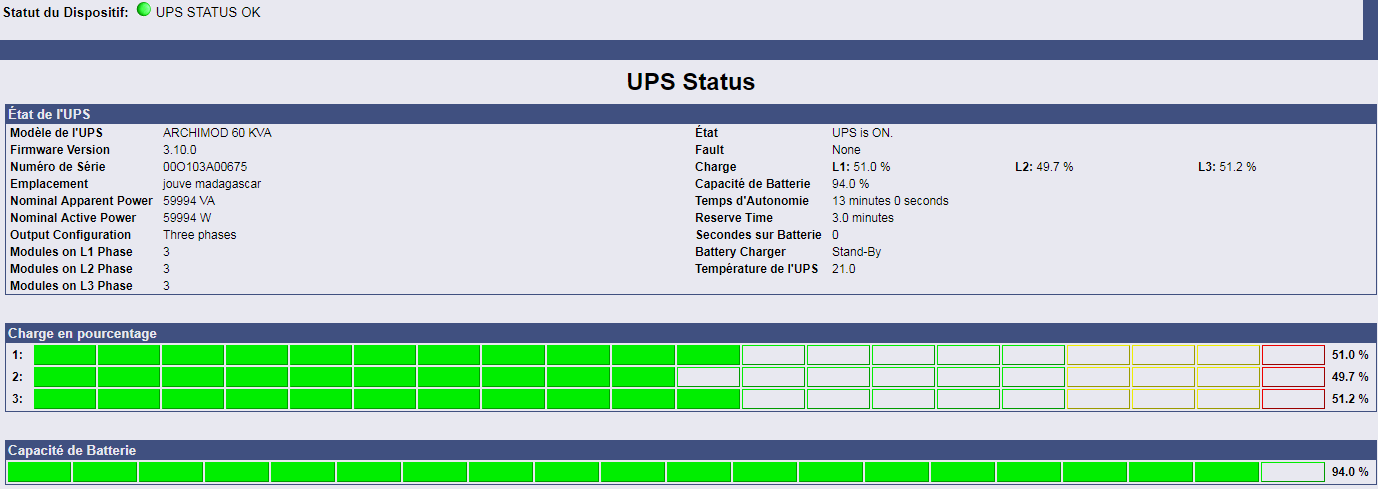
Nous pouvons configurer les événements dans le menu « éditeur d’événement ». Ce menu nous permet d’éditer, de supprimer, de tester des événements existants et d’ajouter un nouveau travail de l’événement.



***Figure 3.10*** : Editeur d’évènement

2.2.6. Etat de l’onduleur

Après toutes les configurations, on peut dire que l’onduleur est supervisé. Les trois barres indiquent les trois modules avec leur charge respective et la barre au dessous indique la capacité de la batterie.



***Figure 3.11*** : Etat de l’onduleur

2.2.7 Logfile

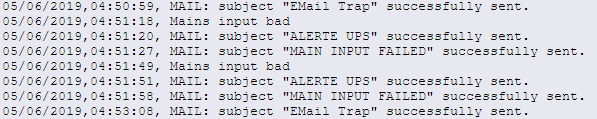
Les fichiers journaux d’événement sont très utiles pour comprendre la provenance d’une erreur ou une défaillance au niveau de l’onduleur.

Ce menu est composé d’AlarmLog, DataLog et DataLog Chart :

* AlarmLog

Le journal des alarmes contient le protocole d’alarme des événements désignés dans le ménu «alarmes et événement» et inclut les paramètres d’alarme définis par l’utilisateur du CS121.

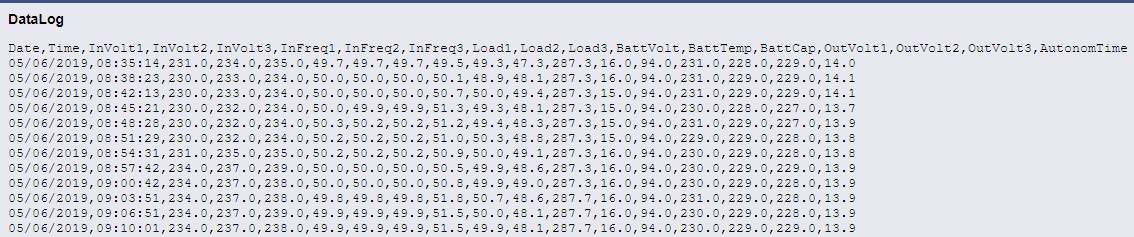
Ces entrées incluent des notifications telles que les notifications par courrier électronique définies par l’administrateur système. Pour l’explication, l’image qui suit illustre un extrait d’un fichier journal dans une période.



***Figure 3.12*** : Journal d’alarme

* DataLog

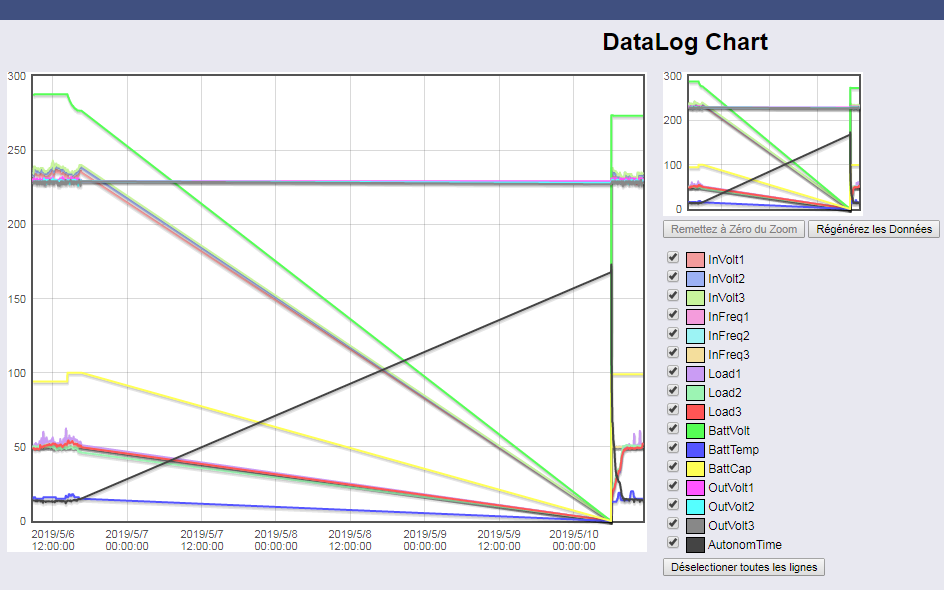
Les données de l’onduleur seront enregistrées avec l’horodatage dans le journal de données CS121(Datalog). Ces données permettent d’établir des statistiques de l’état de l’onduleur dans un intervalle de temps.



***Figure 3.13*** : Journal des données

* DataLog Chart

jChart est un tableau de contrôle pour tous les navigateur Web, qui permet de visualiser le graphique de DataLog du CS121.



***Figure 3.14*** : Graphique du journal des données

**3. Solution 2 : Supervision de l’onduleur via Centreon [9]**

Centreon est une solution de supervision open source qui nous permet de superviser différentes équipements réseaux matériel et logiciel. Dans cette partie, nous détaillerons l’installation et la configuration de Centreon.

***3.1. Les outils de supervision***

- Nous utilisons le fichier iso de Centreon 18.10 pour le serveur de supervision

L’iso Centreon 18.10 est inclus dans CentOs7, nous détaillerons les étapes de l’installation du système d’exploitation dans l’annexe de ce rapport.

- la carte CS121 supporte la norme rfc1826, donc on va installer les plugins Centreon de github qui correspond à cette norme

- Pour les alertes mails, nous choisissons postfix pour faire une relay SMTP

- Coté logiciel, nous utilisons Putty pour connecter via SSH nos serveurs de supervision et google chrome pour connecter à l’interface web de Centreon.

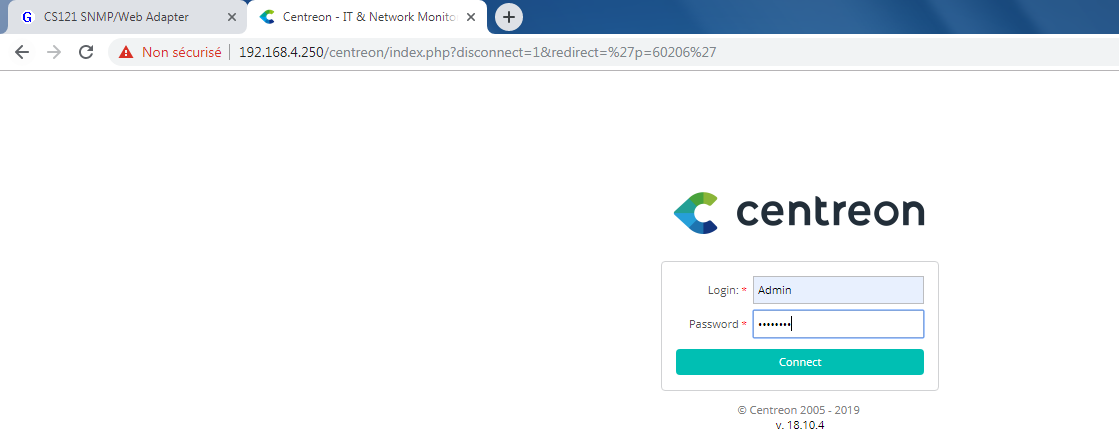
***3.2. Connexion à l’interface Web***

Pour connecter à l’interface web de Centreon, il faut se rendre à l’adresse suivant :

<http://IP_SERVEUR/centreon>

Avec IP\_SERVEUR = adresse IP de notre serveur Centreon qui est le 192.168.4.250.

En suite, renseigner le nom d’utilisateur et le mot de passe que nous avons créé à la fin de l’installation.

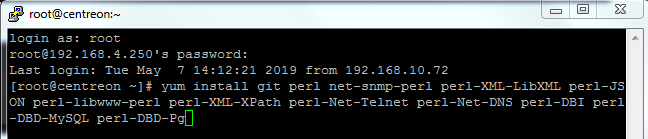


***Figure 3.15*** : Connexion à l’interface web Centreon

***3.3. Installation de Centreon-plugins*** [11] [8]

Pendant les recherches sur internet, nous avons trouvé des plugins Centreon compatibles à notre onduleur sur le site de Github. L’installation des Centreon-plugins se fait via la console donc on va se connecter au serveur avec Putty et taper des commandes.

* Installation des pré-requis



***Figure 3.16*** : Commande pour installer les pré-requis

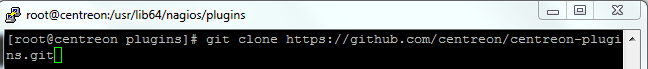
* On se rend dans le répertoire plugins

repertoire plugins

***Figure 3.17*** : Commande se rendre dans le répertoire Nagios

* Téléchargement du package Centreon-plugins

\*



***Figure 3.18*** : Commande pour télécharger les plugins

* Après on modifie le propriétaire du fichier



***Figure 3.19*** : Commande pour changer le propriétaire du fichier centreon-plugins

* Enfin, on modifie le droit d’exécution pour l’utilisateur root

droit_executerle fichier

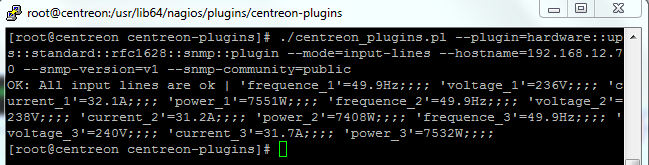
***Figure 3.20*** : Commande pour modifier le droit d’exécution

Pour superviser l’onduleur on va utiliser le plugin hardware ::ups ::standart ::rfc1628 du Centreon-plugins.

Ce plugin nous offre 5 modes :

* Le mode Alarms
* Le mode Battery-status
* Le mode Input-lines
* Le mode Output-lines
* Le mode Output-source

Un exemple de test de plugins avec le mode input-lines

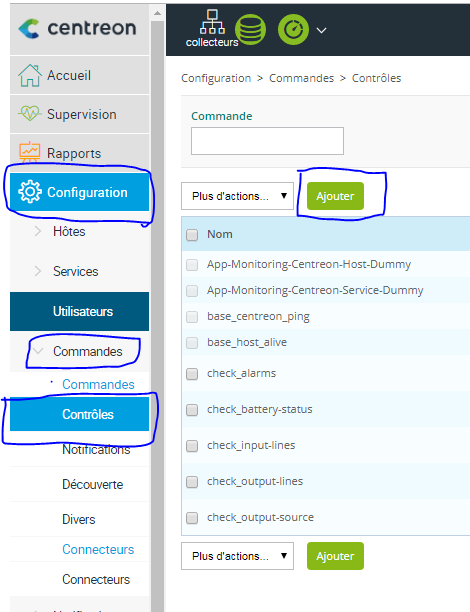


***Figure 3.21*** : Commande de teste mode de l’onduleur

***3.4. Création des commandes dans l’interface web de Centreon***

Une commande est un script lancé depuis le serveur Centreon pour interroger l'hôte distant.

Les commandes de contrôle sont la base des services. La création d’une commande se fait dans le menu configuration ->commande-> (contrôle ou notification ou découverte) ->ajouter.

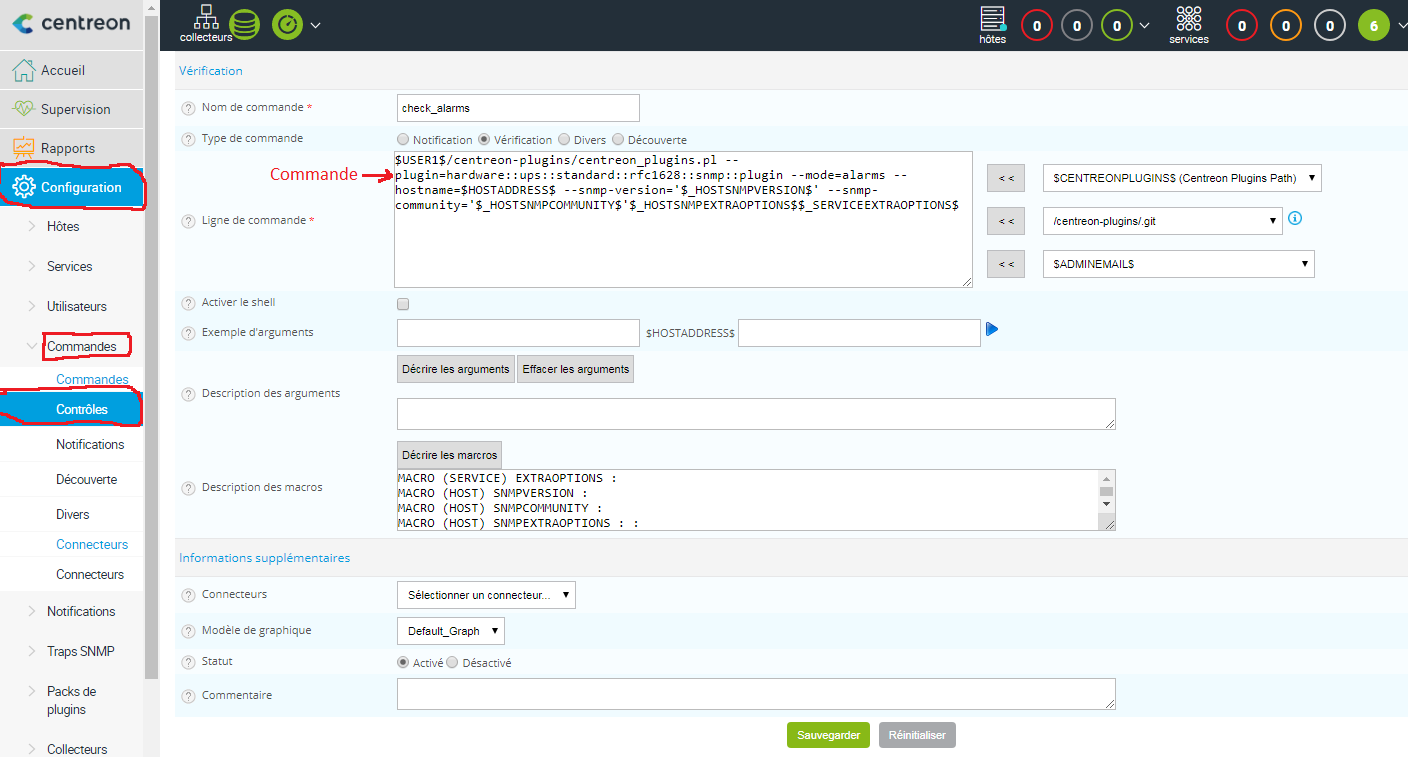


***Figure 3.22*** : Ajoute de commande Centreon

Nous devons créer cinq commandes pour les 5 modes du plugin à savoir :

* La commande check\_alarms pour savoir l’état de l’onduleur
* La commande check\_battery-status pour connaitre l’état des batteries (températures et charges)
* La commande check\_input-lines pour récupérer les valeurs des lines d’entrée de l’onduleur (fréquence, voltage, charge, courant)
* La commande check\_output\_lines pour récupérer les valeurs des lines de sortie de l’onduleur (fréquence, voltage, charge, courant)
* La commande check\_ source pour vérifier l’état de sortie

Un exemple de la création de commande check-alarms :



***Figure 3.23*** : Commande check\_alarms

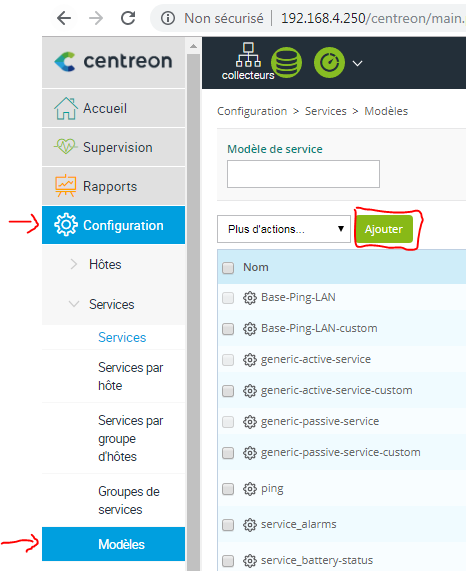
***3.5. Création des modèles de services***

Un service est l’application d’une commande, il faut la configurer pour les seuils et les notifications à envoyer en cas de problèmes ou dépassement de valeur. Les modèles de service sont tous lié au modèle d’hôte ou l’hôte pour dans la configuration de Centreon.

L’ajout de service se fait dans le menu Configuration->services->ajouter.

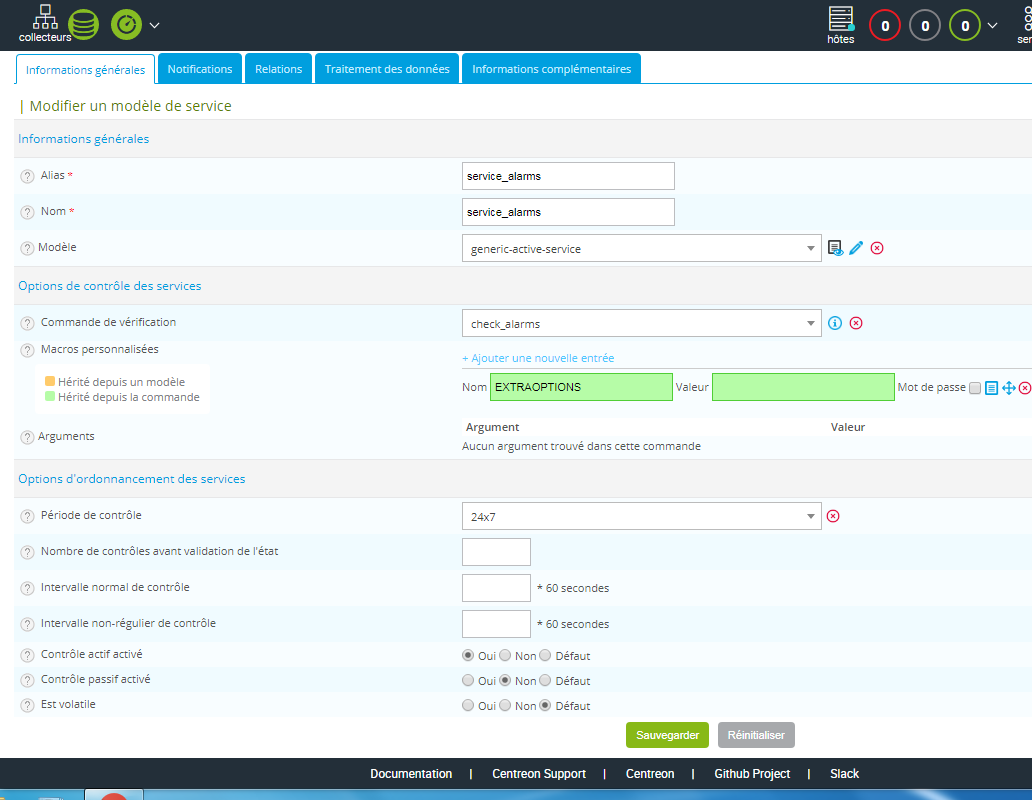
Comme dans la création de commande, nous devons aussi créer 5 modèles de services pour les 5 modes de plugins :

* Le service Alarms
* Le service Battery-status
* Le service Input-lines
* Le service Output-lines
* Le service Output-source



***Figure 3.24*** : ajout modèle de service

Un exemple de création du service Alarms :

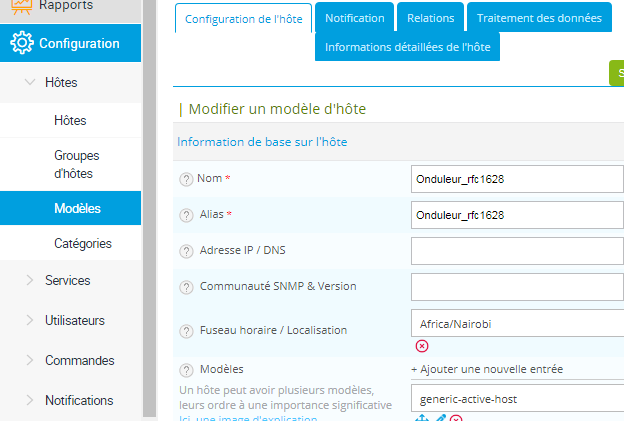


***Figure 3.25*** : Service\_alarms

***3.6. Création d’un modèle d’hôte***

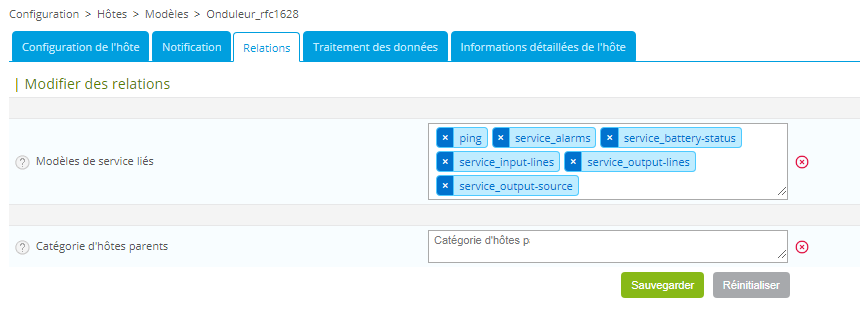
Un modèle d’hôte est nécessaire pour lier tous les services à un hôte.

L’ajout d’un modèle d’hôte se fait dans le menu Configuration->hôte->modèle->ajouter.



***Figure 3.26*** : Création modèle d’hôte

Dans l’onglet relation, on va renseigner tous les services dans la case modèle de services liés :



***Figure 3.27*** : Relier le modèle d’hôte avec les services

***3.7. Ajout de l’hôte ou l’onduleur à superviser***

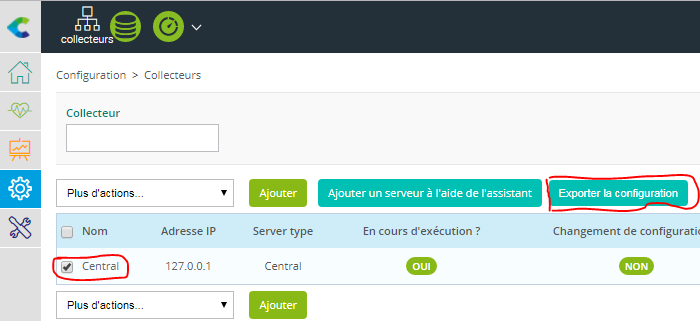
Un hôte est un matériel ou logiciel que l’on souhaite superviser, dans notre cas c’est l’onduleur ARCHIMOD HE. Chaque définition d’hôte se base sur un modèle d’hôte crée par l’administrateur ou modèle existante.

L’ajout d’hôte se fait dans le menu configuration->hôte->ajouter :



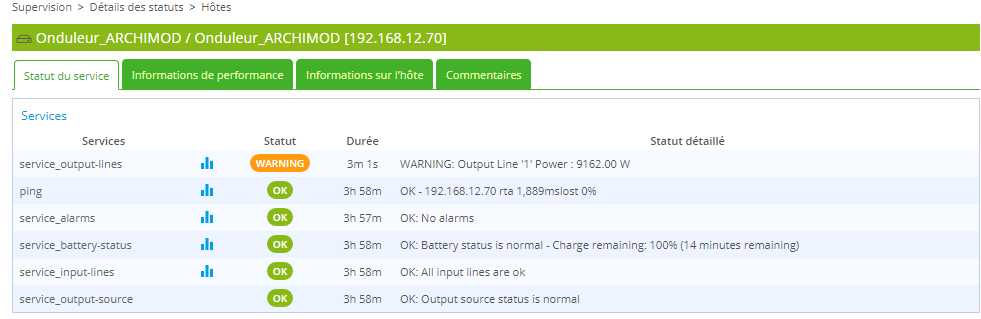
***Figure 3.28*** : Ajout de l’onduleur à surveiller

A la fin des configurations, il faut relancer et redémarrer le collecteur/poller pour qu’il prenne en compte les changements effectués. On va se rendre sur le menu configuration->collecteurs->sélectionné le collecteur->exporter la configuration :



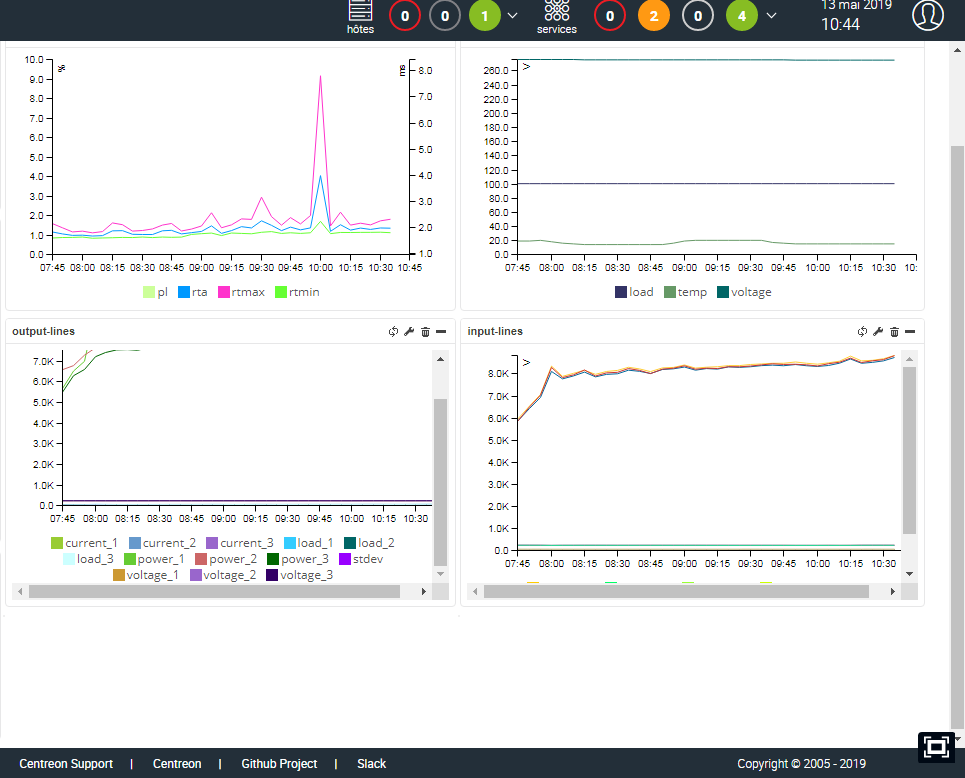
***Figure 3.29*** : Redémarrage du collecteur

L’onduleur est maintenant supervisé par Centreon :



***Figure 3.30*** : Statu de l’hôte et services

Nous pouvons avoir une vue personnalisée après l’installation des widgets :



***Figure 3.31 :*** Vue personnalisé

***3.8. Journaux d’événements***

Les journaux d’événements (aussi appelé : Event logs) permettent de :

* Visualiser les différents changements de statu et états des objets supervisés
* Voir les notifications envoyées ainsi que leurs destinataires

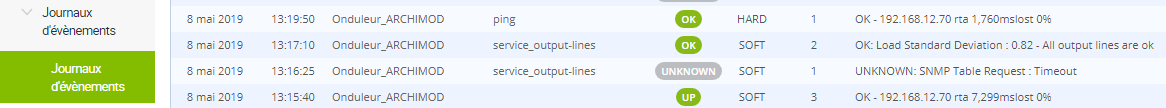
Pour visualiser nos journaux d’événements, rendez –vous dans le menu supervision->journaux d’événements.

Figure 3.32 : Journaux d’évènements

***3.9. Alerte mail***

Alerte mail ou courriel électronique d’alerte est un message généré et envoyé automatiquement à un ou plusieurs destinataires lorsque certains critères sont réunis.

Le système de notification est une des points essentiels pour les plateformes de supervision. Par défaut, la grande majorité utilise la notification par email via les daemons postfix, mail, ou exim installés sur le serveur de supervision afin d’envoyer des alertes.

Les notifications dans Centreon font appel à plusieurs éléments :

* Un postfix installé et configuré sur le serveur Centreon

Postfix est un serveur de messagerie électronique et un logiciel libre, il se charge de la livraison de messages électronique. Il est plus facile à administrer et plus sécurisé par rapport à Sendmail. Nous verrons dans annexe l’installation et configuration de Postfix.

* Les commandes utilisées pour envoyer les courriels (notify-service-by-email, notify-host-by-email)
* Des configurations au niveau des hôtes et services que nous voudrions notifier leur changement d’état
* Les contacts à notifier

Un exemple de test mail à la fin de la configuration :



***Figure 3.32*** : Alerte mail centreon

Conclusion

Nous avons découvert dans ce chapitre les aspects pratiques de notre projet, les détails des étapes de la mise en place de la solution, l’installation et la configuration des outils matériels et logiciels pour la supervision de l’onduleur en utilisant deux solutions distincts qui nous permet d’accomplir les objectifs demandés.

CONCLUSION GENERALE

Dans ce présent rapport nous avons vu en détail le déroulement des travaux effectués pendant la période du stage. L’objectif initial de ce stage a été presque accompli, ainsi que les travaux demandés. L’onduleur ARCHIMOD HE est accessible via la console et l’interface WEB. L’interface web du CS121 et de Centreon nous permettent de visualiser l’état de l’onduleur, l’état des batteries, les charges supportées et les différentes valeurs d’entrée (tension, courant,…) et sortie. Nous avons configuré le serveur de messagerie pour notifier et alerter les administrateurs par un message textuel en cas de défaillance ou de problème de l’onduleur.

Le projet que nous réalisons est déjà utilisé en production. L’onduleur ARCHIMOD HE supervisé assure l’alimentation de 90% des postes du site. Ce stage a été bénéfique pour moi, la découverte d’un nouveau domaine qui est la supervision réseau et des connaissances au niveau de virtualisation et administration serveur linux.

Enfin ce stage m’a permis de mieux comprendre le travail des administrateurs réseaux et systèmes. L’administration des serveurs, la gestion de parc informatique, la mise en place des solutions de supervisions réseaux, les sécurités et plein d’autres tâches. Les administrateurs réseaux et systèmes travaillent jour et nuit pour améliorer le niveau de disponibilité de l’entreprise. Ce stage a été une expérience professionnelle pour moi, je tiens encore une fois remercier la société JOUVE de m’avoir accueilli.

ANNEXES

ANNEXE 1 : INSTALLATION DU SERVEUR ET INTERFACE WEB DE CENTREON 18.10

**A1.1 Création de la machine virtuelle**

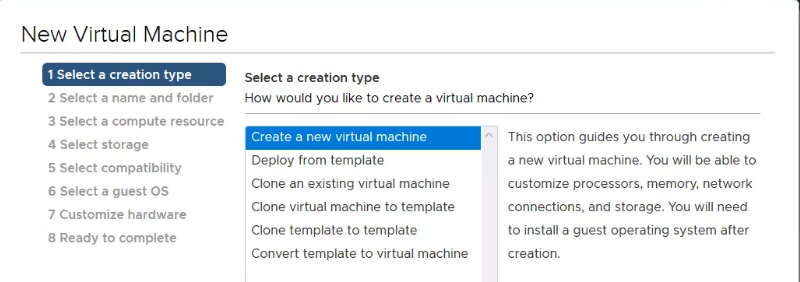


Figure A1. Création d’une nouvelle machine virtuelle

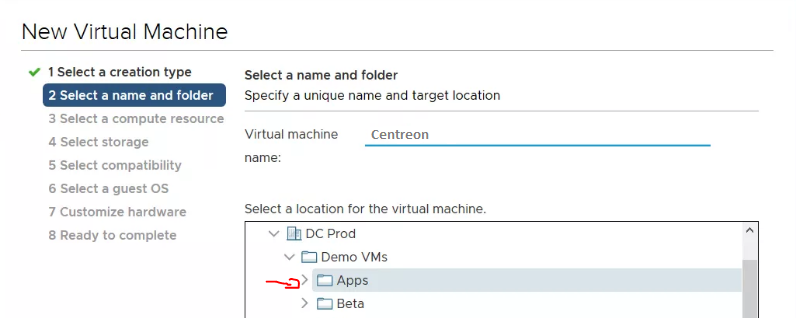


Figure A2. Nom de la machine

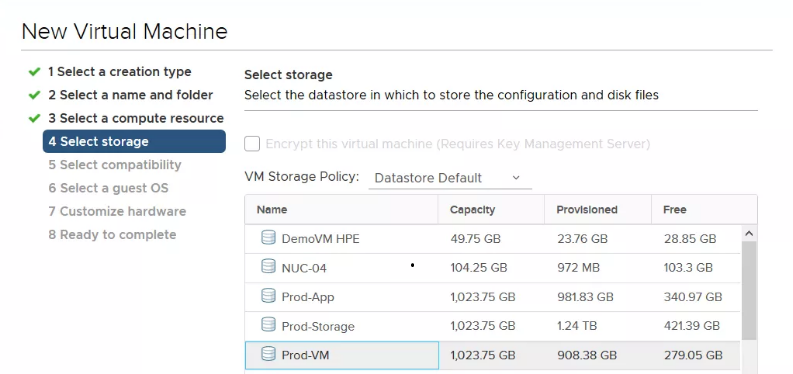


Figure A3. Emplacement de l’installation

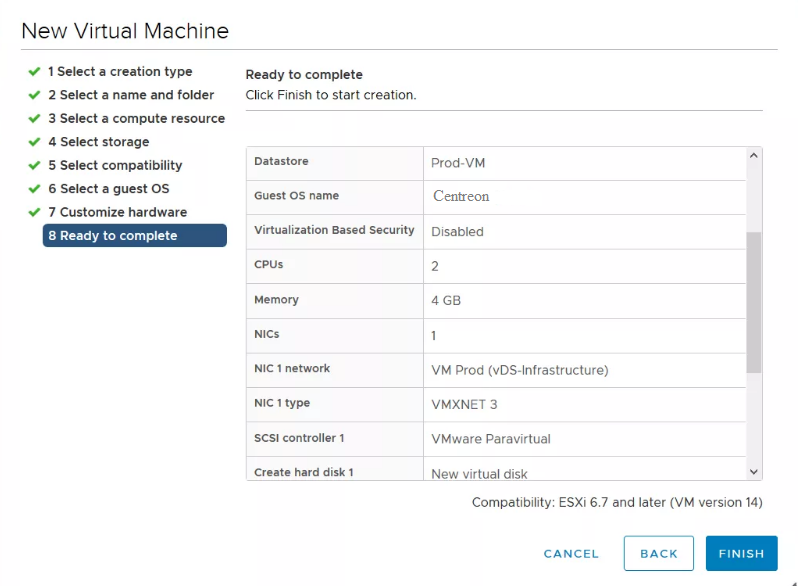


Figure A4. La machine virtuelle est prés pour l’installation

**A1.2 Installation de Centreon (Centos7) [13] [9]**

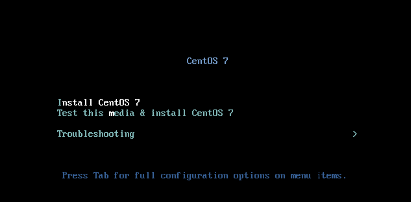


Figure A5. Démarrage de l’installation du serveur Centreon

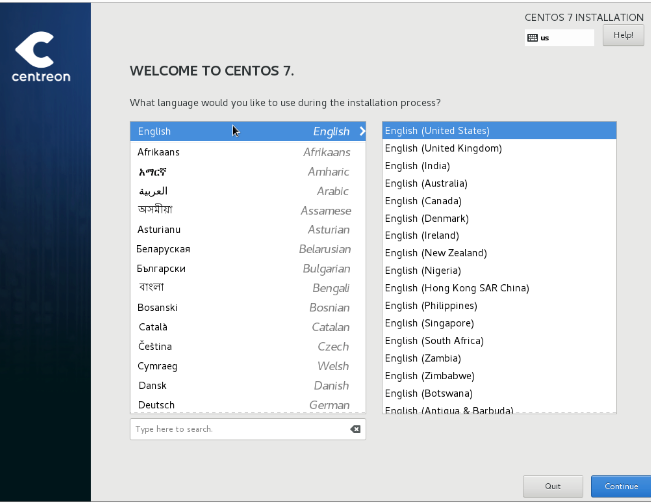


Figure A6. Choix de langue



Figure A7. Type d’installation

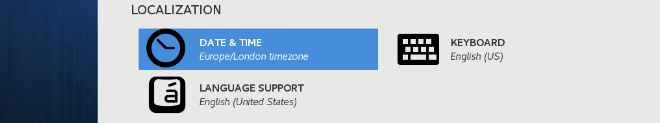


Figure A8. Configuration date et fuseau horaire

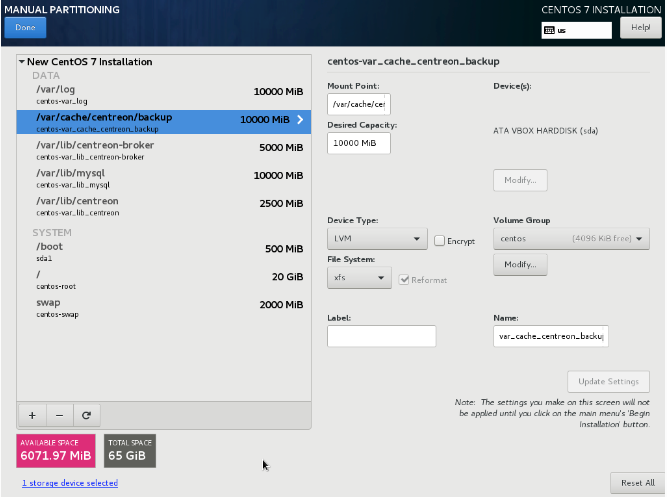


Figure A9. Partition de disque dur

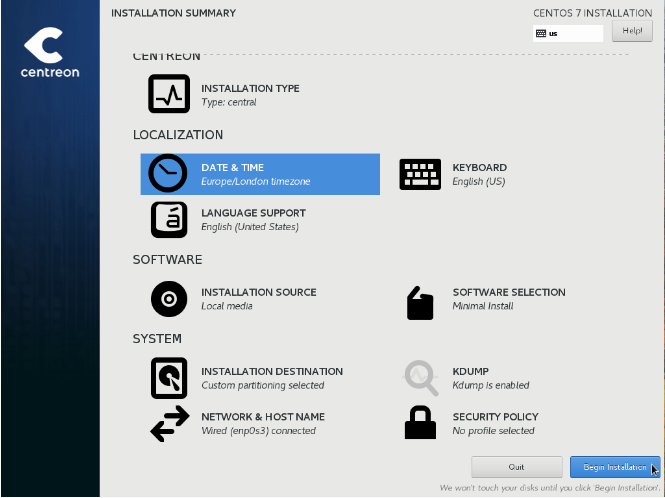


Figure A10. Fin des paramétrages et début de l’installation



Figure A11. Définition mot de passe du compte root et création nouvelle compte invitée

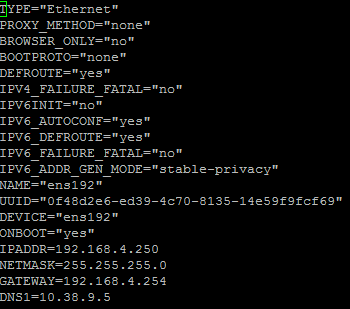


Figure A12. Configuration réseau du serveur Centreon

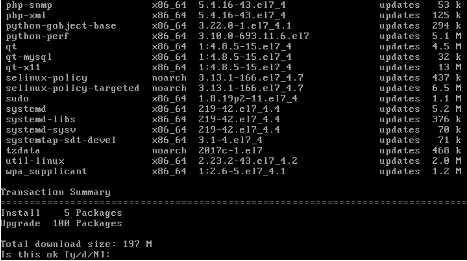


Figure A13. Mise à jour du système

**A1.3 Configuration de l’interface web de Centreon**

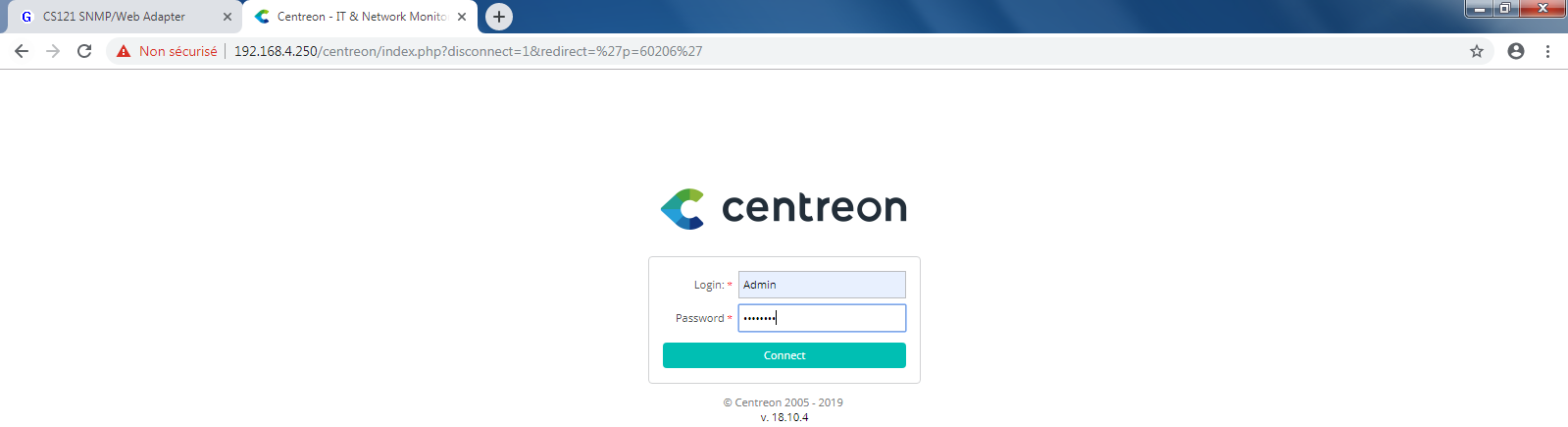


Figure A14. Connexion à l’interface web de Centreon

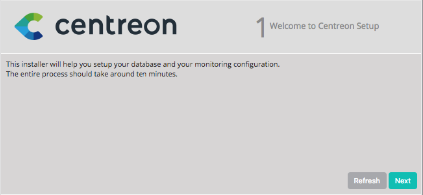


Figure A15. Configuration de l’interface web de Centreon

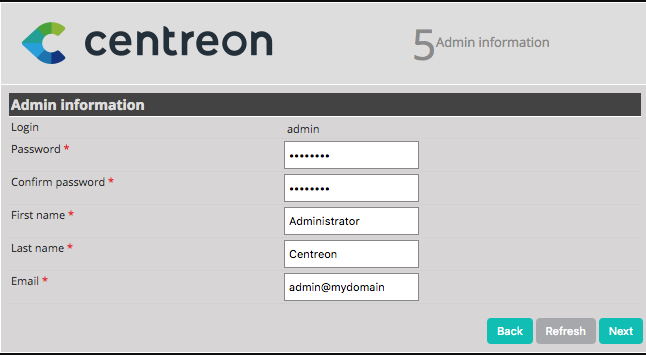


Figure A16. Définition compte Administrateur

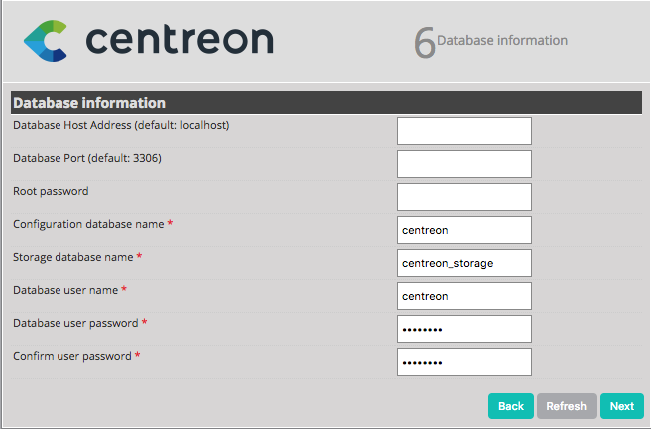


Figure A17. Configuration base de donné



Figure A18. Installation des modules



Figure A19. Fin de l’installation

ANNEXE 2 : INSTALLATION ET CONFIGURATION DU POSTFIX

**A2.1 Installation et configuration postfix [12] [13]**

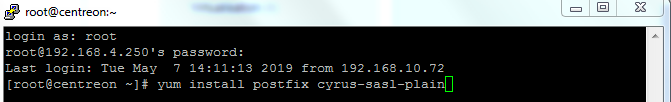


Figure A20. Installation postfix et cyrus

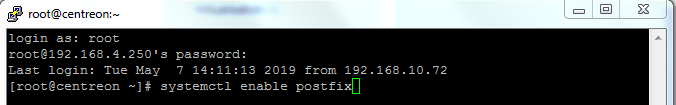


Figure A21. Activation postfix

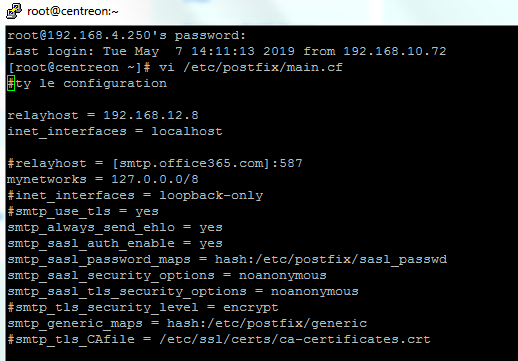


Figure A22. Configuration du fichier main.cf



Figure A23. Création du fichier sasl\_passwd



Figure A24. Modification du droit du fichier sasl\_passwd

4



Figure A25. Activation du fichier sasl\_passwd



Figure A26. Redémarrage de service postfix

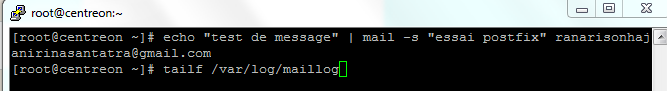


Figure A26. Teste mail à la fin de l’installation et configuration

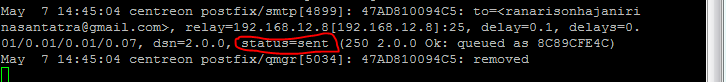


Figure A27. Confirmation d’envoi de mail dans maillog

BIBLIOGRAPHIE

[1] CNTEMAD https://www.cntemad.mg/

[2] Wikipedia-supervision réseau https:/ /fr.wikipedia.org

[3] Supinfo https://www.supinfo.com/articles/singles/3124-comparaison-outils-supervision

[4] FrameIP https://www.frameip.com/snmp/

[5] Appvizer https://www.appvizer.fr/magazine/services-informatiques/

[6] Legrand Manuel d’utilisation ARHIMOD HE https://ups.legrand.com.

[7] Generex Manuel CS121.pdf https://www.generex.com

[8] Memo-linux – supervision onduleur <https://memo-linux.com>

[9] Centreon https://centreon.com

[10] JUOVE <https://www.jouve.com>

[11] Gitbhub Centeron-plugins <https://github.com>

[12] Postfix https://www.microlinux.fr/postfix-minimal-lan-centos-7/

[13] Centos https://www.centos.com

PAGE DE RENSEIGNEMENTS



Nom  : RANARISON

Prénom(s) : Hajanirina Santatra

Adresse  : Lot III X 47 Anosibe Ouest II

[ranarisonhajanirinasantatra@gmail.com](mailto:ranarisonhajanirinasantatra@gmail.com)

+261 32 56 335 62

Titre du rapport de stage :

**SUPERVISION RESEAUX ET MONITORING DES ASI**

Nombre de pages : 62 pages

Nombre de figures : 62 Figures

Nom de la Société ou Entreprise  : JOUVE Madagascar

Contact de la Société ou Entreprise : Tel : +261 20 22 208 00 / +261 20 22 314 54

E-mail : rh-mada@jouve.com

Nom et Prénom de l’Encadreur Professionnel : HERINIAINA Naly

Contact de l’Encadreur Professionnel : nheriniaina@jouve.com

RESUME

Le présent rapport est l’aboutissement de trois mois de stage au sein de l’Entreprise JOUVE Madagascar et aussi la fin de sixième semestre en vue de l’obtention du diplôme Licence en Informatique réseau et système au CNTEMAD. Ce rapport est divisé en trois parties : la première présente le CNTEMAD et l’entreprise d’accueil ; la deuxième expose la présentation générale du stage, l’étude de l’existant et l’étude théorique des solutions ; la dernière décrit la réalisation et la mise en place des solutions de supervision de l’onduleur ARCHIMOD HE. A la fin du stage, on peut dire que tous les objectifs sont accomplis et l’onduleur en production est sous surveillance continue par les administrateurs réseaux et systèmes.

Mots clés : Monitoring, Centreon, Onduleur, Réseaux, Hôte, Service, Commande, Alerte mail, Postfix, Plugins.